Fields Institute Communications 77

The Fields Institute for Research in Mathematical Sciences

Ayşe Alaca
Şaban Alaca
Kenneth S. Williams
Editors

Advances in the Theory of Numbers

Proceedings of the Thirteenth Conference of the Canadian Number Theory Association

FIELDS

Springer

Fields Institute Communications

VOLUME 77

The Fields Institute for Research in Mathematical Sciences

The Fields Institute is a centre for research in the mathematical sciences, located in Toronto, Canada. The Institute's mission is to advance global mathematical activity in the areas of research, education and innovation. The Fields Institute is supported by the Ontario Ministry of Training, Colleges and Universities, the Natural Sciences and Engineering Research Council of Canada, and seven Principal Sponsoring Universities in Ontario (Carleton, McMaster, Ottawa, Queen's, Toronto, Waterloo, Western and York), as well as by a growing list of Affiliate Universities in Canada, the U.S. and Europe, and several commercial and industrial partners.

More information about this series at http://www.springer.com/series/10503

Ayşe Alaca • Şaban Alaca • Kenneth S. Williams
Editors

Advances in the Theory of Numbers

Proceedings of the Thirteenth Conference of the Canadian Number Theory Association

The Fields Institute for Research in the Mathematical Sciences
FIELDS

Springer

Editors
Ayşe Alaca
School of Mathematics and Statistics
Carleton University
Ottawa, ON, Canada

Şaban Alaca
School of Mathematics and Statistics
Carleton University
Ottawa, ON, Canada

Kenneth S. Williams
School of Mathematics and Statistics
Carleton University
Ottawa, ON, Canada

ISSN 1069-5265 ISSN 2194-1564 (electronic)
Fields Institute Communications
ISBN 978-1-4939-3200-9 ISBN 978-1-4939-3201-6 (eBook)
DOI 10.1007/978-1-4939-3201-6

Library of Congress Control Number: 2015951981

Mathematics Subject Classification (2010): 00B20, 11-02, 11-06

Springer New York Heidelberg Dordrecht London

Cover illustration: Drawing of J.C. Fields by Keith Yeomans

Printed on acid-free paper

Springer Science+Business Media LLC New York is part of Springer Science+Business Media (www.springer.com)

Preface

The Canadian Number Theory Association (CNTA) is an informal organization of Canadian number theorists, founded in 1987 through the initiative and efforts of the late Richard Mollin of the University of Calgary. The following is a complete list of the CNTA conferences.

CNTA I	Banff Center, Banff, Alberta	1988
CNTA II	University of British Columbia	1989
CNTA III	Queen's University	1991
CNTA IV	Dalhousie University	1994
CNTA V	Carleton University	1996
CNTA VI	University of Manitoba	1999
CNTA VII	Université de Montréal	2002
CNTA VIII	University of Toronto	2004
CNTA IX	University of British Columbia	2006
CNTA X	University of Waterloo	2008
CNTA XI	Acadia University	2010
CNTA XII	University of Lethbridge	2012
CNTA XIII	Carleton University	2014

This volume contains the proceedings of the thirteenth CNTA conference, which was held at Carleton University, Ottawa, Ontario from June 16 to 20, 2014. There were 154 participants at the conference from across all continents. The scientific program of the conference consisted of one public lecture, one Ribenboim Prize lecture, ten plenary talks, 22 invited talks and 65 contributed talks, for a total of 99 talks.

The Conference Organizing Committee comprised Ayşe Alaca (Carleton), Şaban Alaca (Carleton, main organizer), Paul Mezo (Carleton), Damien Roy (Ottawa), Abdellah Sebbar (Ottawa), Gary Walsh (Ottawa), Hugh Williams (Calgary/Carleton) and Kenneth Williams (Carleton). The Scientific Advisory

Committee consisted of John Friedlander (Toronto), Steve Gonek (Rochester), Eyal Goren (McGill), Stephen Kudla (Toronto), Cameron Stewart (Waterloo), Hugh Williams (Calgary/Carleton) and Kenneth Williams (Carleton). The Ribenboim Prize Committee was made up of Adrian Iovita (Concordia), Ram Murty (Queen's) and Damien Roy (Ottawa).

The conference was supported in part by Carleton University, University of Ottawa, Centre de Recherches Mathématiques, the Tutte Institute, Number Theory Foundation, the Fields Institute and the National Science Foundation.

This volume contains written versions of some of the presentations. All papers were refereed. We thank all the authors for their considerable care and effort in preparing their manuscripts for these proceedings. Special thanks are due to the referees for their important contribution to these proceedings.

We gratefully acknowledge the faculty, staff and students of the School of Mathematics and Statistics at Carleton University for their help and support, Debbie Iscoe (Fields Institute) for her help with assembling this volume and Carole Williams for her assistance with the conference registration.

Ottawa, ON, Canada
March 2015

Ayşe Alaca
Şaban Alaca
Kenneth S. Williams

Contents

List of Lectures

Public Lecture

The Secret Life of Mathematics
La vie secrète des mathèmatiques
Jean-Marie de Koninck

Ribenboim Prize Lecture

On the mod p Langlands Program
Florian Herzig

Plenary Talks

On Langlands' Automorphic Galois Group and Weil's Explicit Formulas
James Arthur

Decompositions of Meromorphic Jacobi Forms
Kathrin Bringmann

Moments of the Riemann Zeta Function
Brian Conrey

The Arithmetic Site
Caterina Consani

Hypergeometric Functions, Modular Forms and Series for $1/\pi$
Shaun Cooper

Elliptic Curves and Class Field Theory
Henri Darmon

Small Gaps Between Primes
James Maynard

The Refined Sato-Tate Conjecture
Andrew Sutherland

Families of L-Functions and Their Symmetry
Nicholas Templier

Recovering Elliptic Curves from Their p-Torsion
Jacob Tsimerman

Invited Talks

Local Heuristics and Exact Formulas for Abelian Varieties Over Finite Fields
Jeff Achter

Cubic Irrationalities and a Ramanujan-Nagell Analogue
Mark Bauer

Partition Identities Inspired by Ramanujan
Bruce C. Berndt

The Polynomials of Mahler and Roots of Unity
Karl Dilcher

4959866698915122609810424451291 7
Michael Filaseta

Bounds on the Least Quadratic Nonresidue
Leo Goldmakher

The Frequency of Elliptic Curve Groups Over Finite Fields
Dimitris Koukoulopoulos

Diophantine Approximation by Primitive Points
Michel Laurent

Equidistribution of Polynomial Sequences in Function Fields
Yu-Ru Liu

Diophantine Equations with Generalized Fibonacci Numbers
Florian Luca

Contributed Talks

Generalized Fibonacci and Lucas Numbers of the Form $5x^2$
Olcay Karaatli

2-Adic Zeros of Additive Forms
Michael Knapp

On Erdös-Pomerance Conjecture
Wentang Kuo

Comparing the Selmer Group of an Ordinary p-Adic Representation and the Selmer Group of the Tate Dual of the Representation
Meng Fai Lim

New Bounds for $\psi(x; q, a)$
Allysa Lumley

Siegel Norm and the Character Values of Finite Groups
Amita Malik

On the Behaviour of Polynomials and Random Mappings Over Finite Fields
Roderigo Martins

Some Unconventional Results in Multiplicative Combinatorial Number Theory
Nathan McNew

Small Index Gauss Sums
Goldwyn Millar

Parity of Two Selmer Ranks of Hyperelliptic Curves Over Quadratic Extensions
Adam Morgan

The Number of Twists with Large Torsion of an Elliptic Curve
Filip Najman

Bounds for the Number of Rational Points on Curves Over Function Fields
Amilcar Pacheco

Amicable Pairs and Aliquot Cycles on Average
James Parks

Remarks on the Shape of Elliptic Curves
Hector Pasten

List of Participants

Achter, Jeff	Colorado State University
Akbary, Amir	University of Lethbridge
Alaca, Ayşe	Carleton University
Alaca, Şaban	Carleton University
Alanazi, Jamilah	Carleton University
Allen, Patrick	Northwestern University
Althagafi, Mohammed	Carleton University
Altiary, Mada	Carleton University
Arthur, James	University of Toronto
Aryan, Farzad	University of Lethbridge
Aygin, Zafer Selcuk	Carleton University
Baluyot, Siegfred	University of Rochester
Bauer, Mark	University of Calgary
Berndt, Bruce	University of Illinois
Bettin, Sandro	Université de Montréal, CRM
Bober, Jonathan	University of Bristol
Boyd, David	University of British Columbia
Bremner, Andrew	Arizona State University
Bringmann, Kathrin	University of Cologne
Bruin, Nils	Simon Fraser University
Bruni, Carmen	University of British Columbia
Candelori, Luca	McGill University
Chen, Hao	University of Washington
Cho, Peter J.	SUNY Buffalo
Chow, Sam	University of Bristol
Christie, Arron	University of Ottawa
Cloutier, Maurice-Etienne	Laval University
Conrey, Brian	American Institute of Mathematics
Consani, Caterina	Johns Hopkins University
Coons, Michael	University of Newcastle
Cooper, Shaun	Massey University

Darmon, Henri	McGill University
De Koninck, J. M.	Laval University
Dias, Dimitri	Université de Montréal
Dilcher, Karl	Dalhousie University
Dobrowolski, Edward	University of Northern British Columbia
Doyle, Greg	Carleton University
Drappeau, Sary	Université de Montréal, CRM
Dunn, Scott	University of South Carolina
Dupuy, Taylor	Hebrew University of Jerusalem
Elgarmol, Afaf	Carleton University
Ericksen, Lerry	Millville, NJ
Felix, Adam	University of Lethbridge
Filaseta, Michael	University of South Carolina
Fiorilli, Daniel	University of Michigan
Fodden, Brandon	Carleton University
Freiberg, Tristan	University of Missouri
Gafni, Ayla	Pennsylvania State University
Garcia-Fritz, Natalia	Queen's University
Ge, Fan	University of Rochester
Goldmakher, Leo	University of Toronto
Guo, Zhenyu	University of Missouri
Guy, Richard	University of Calgary
Hamieh, Alia	Queen's University
Hanson, Brandon	University of Toronto
Hare, Kevin	University of Waterloo
Hayman, Colin	Carleton University
Henriot, Kevin	Université de Montréal
Herzig, Florian	University of Toronto
Huang, Jing-Jing	University of Toronto
Hulse, Thomas	Queen's University
Jacobson, Mike	University of Calgary
Jankauskas, Jonas	University of Waterloo
Karaatli, Olcay	Sakarya University
Keita, Aminata Dite Tanti	University of Ottawa
Khan, Mizan R.	Eastern Connecticut University
Kirila, Scott	University of Rochester
Klurman, Oleksiy	Université de Montréal
Knapp, Michael	Loyola University Maryland
Kolster, Manfred	McMaster University
Koukoulopoulos, Dimitris	Université de Montréal
Lam, Winnie	University of Waterloo
Laurent, Michel	Institut de Mathématiques, Marseille
Letendre, Patrick	Laval University
Lin, Meng Fai	University of Toronto
Liu, Yu-Ru	University of Waterloo

Logan, Adam	Government of Canada
Long, Misty	Kansas State University
Luca, Florian	UNAM and WITS
Lumley, Allysa	University of Lethbridge
Lungstrum, Clayton	University of Rochester
Malik, Amita	University of Illinois
Martins, Rodrigo	UFRJ/Carleton University
Maynard, James	Université de Montréal
McKinnon, David	University of Waterloo
McNew, Nathan	Dartmouth College
Mezo, Paul	Carleton University
Millar, Goldwyn	Carleton University
Mok, Chung Pang	McMaster University
Morgan, Adam	University of Bristol
Morra, Stefano	University of Toronto
Murty, Kumar	University of Toronto
Murty, Ram	Queen's University
Musson, Matthew	Government of Canada
Najman, Filip	University of Zagreb
Ntienjem, Ebenezer	Carleton University
Omar, Ommkaltoum	Carleton University
Ouellet, Vincent	Laval University
Pacheco, Amilcar	Federal University of Rio de Janeiro
Parks, Jim	University of Lethbridge
Pasten, Hector	Queen's University
Pazuki, Fabien	Université de Bordeaux
Pigno, Vincent	Kansas State University
Pomerance, Carl	Dartmouth College
Pries, Rachel	Colorado State University
Qureshi, Claudio	Unicamp and Carleton University
Rémond, Gaël	CNRS Bordeaux
Rivard-Cooke, Martin	University of Ottawa
Roberts, David	University of Minnesota, Morris
Roe, David	University of Calgary
Rosen, Julian	University of Waterloo
Roy, Damien	University of Ottawa
Rozenhart, Pieter	Government of Canada
Rubinstein, Michael	University of Waterloo
Saber, Hicham	University of Ottawa
Saunders, J. C.	University of Waterloo
Scarfy, Justin	University of British Columbia
Scheidler, Renate	University of Calgary
Schindler, Damaris	Hausdorff Center for Mathematics, Bonn
Sebbar, Abdellah	University of Ottawa

Simons, Lloyd	Saint Michael's College
Södergren, Anders	University of Copenhagen
Sorensen, Claus	University of California, San Diego
Soydan, Gökhan	Uludag University
Sulisz, Gregory	Adrian College
Sutherland, Andrew	Massachusetts Institute of Technology
Szalay, Laszlo	University of West Hungary
Templier, Nicolas	Princeton University
Toll, Charles	National Security Agency
Trudgian, Timothy	Australian National University
Tse, Ling-Sang	University of Waterloo
Tsimerman, Jacob	Harvard University
Turner, Graeme	Carleton University
Vatwani, Akshaa	Queen's University
Vincent, Christelle	Stanford University
Voutier, Paul	London
Waldschmidt, Michel	Université Paris VI
Walji, Nahid	University of California, Berkeley
Walls, Patrick	McMaster University
Walsh, Gary	University of Ottawa
Wear, Peter	University of California, San Diego
Weatherby, Chester	Wilfrid Laurier University
Weir, Colin	Simon Fraser University
Weiss, Al	University of Alberta
Williams, Hugh	University of Calgary
Williams, Kenneth S.	Carleton University
Wong, Peng-Jie	Queen's University
Wooding, Amy	McGill University
Wu, Jing	Queen's University
Xiao, Stanley	University of Waterloo
Yamagishi, Shuntaro	University of Waterloo
Yazdani, Saroosh	University of Lethbridge
Yoon, Dong Sung	National Institute for Mathematical Sciences, South Korea
Zaman, Asif	University of Toronto

Identities for Logarithmic Means: A Survey

Bruce C. Berndt and Sun Kim

Abstract We provide a survey of identities for sums of the type $\sum_{n\le x} a(n)\log(x/n)$. In each case, $a(n)$ is an arithmetical function generated by a Dirichlet series satisfying a functional equation involving the gamma function. Moreover, all of the identities given in this paper feature infinite series of Bessel functions.

1 Introduction

Let $a(n)$ be an arithmetical function generated by a Dirichlet series satisfying a functional equation involving the gamma function $\Gamma(s)$. For example, let $r_k(n)$ denote the number of representations of the positive integer n as a sum of k squares. Then its generating function

$$\zeta_k(s) := \sum_{n=1}^{\infty} r_k(n)n^{-s}, \quad \sigma = \operatorname{Re} s > \tfrac{1}{2}k, \tag{1}$$

satisfies the functional equation

$$\pi^{-s}\Gamma(s)\zeta_k(s) = \pi^{s-k/2}\Gamma(\tfrac{1}{2}k-s)\zeta_k(\tfrac{1}{2}k-s).$$

Second, let $d(n)$ denote the number of positive divisors of the positive integer n. If $\zeta(s)$ denotes the Riemann zeta function, it is easily seen that

$$\zeta^2(s) = \sum_{n=1}^{\infty} d(n)n^{-s}, \quad \sigma > 1,$$

B.C. Berndt (✉) • S. Kim
Department of Mathematics, University of Illinois, 1409 West Green Street,
Urbana, IL 61801, USA
e-mail: berndt@illinois.edu; sunkim2@illinois.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_1

which satisfies the functional equation

$$\pi^{-s}\Gamma^2(\tfrac{1}{2}s)\zeta^2(s) = \pi^{-1+s}\Gamma^2(\tfrac{1}{2}-\tfrac{1}{2}s)\zeta^2(1-s).$$

Third, let $\tau(n)$ denote the Ramanujan tau-function. Then Ramanujan's Dirichlet series

$$f(s) := \sum_{n=1}^{\infty} \tau(n)n^{-s}, \quad \sigma > \tfrac{13}{2},$$

satisfies the functional equation

$$(2\pi)^{-s}\Gamma(s)f(s) = (2\pi)^{-(12-s)}\Gamma(12-s)f(12-s).$$

In each case, the functional equation can be used to analytically continue the Dirichlet series to the entire complex s-plane.

For an arithmetical function $a(n)$, we often desire an asymptotic formula for $\sum_{n\le x} a(n)$, or, if we divide by x, we ask for the *average order* of $a(n)$. If $a(n)$ is generated by a Dirichlet series satisfying a functional equation involving $\Gamma(s)$, then $\sum_{n\le x} a(n)$ often satisfies an identity containing an infinite series of Bessel functions [10].

For example,

$$\sum_{0\le n\le x}{}' r_2(n) = \pi x + \sum_{n=1}^{\infty} r_2(n)\left(\frac{x}{n}\right)^{1/2} J_1(2\pi\sqrt{nx})$$
$$=: \pi x + P(x), \tag{2}$$

where $P(x)$ is the "error term," and where $J_\nu(x)$ is the ordinary Bessel function of order ν defined by

$$J_\nu(z) := \sum_{n=0}^{\infty} \frac{(-1)^n}{n!\Gamma(\nu+n+1)}\left(\frac{z}{2}\right)^{\nu+2n}, \qquad 0<|z|<\infty, \qquad \nu\in\mathbb{C}. \tag{3}$$

The prime $'$ on the summation sign on the left side of (2) indicates that if x is an integer, then we count only $\frac{1}{2}r_2(x)$. One of the most famous unsolved problems in analytic number theory is the *circle problem*: find the precise order of magnitude of $P(x)$ as $x\to\infty$. It is conjectured that, for every $\epsilon>0$, $P(x) = O(x^{1/4+\epsilon})$ as x tends to ∞. A history and survey of the *circle problem* can be found in [7].

For a second example, we return to $d(n)$. First define the Bessel function $Y_\nu(z)$ of the second kind of order ν by [21, p. 64, Eq. (1)]

$$Y_\nu(z) := \frac{J_\nu(z)\cos(\nu\pi) - J_{-\nu}(z)}{\sin(\nu\pi)}, \tag{4}$$

and the modified Bessel function $K_\nu(z)$ of order ν by [21, p. 78, Eq. (6)]

$$K_\nu(z) := \frac{\pi}{2}\,\frac{e^{\pi i\nu/2}J_{-\nu}(iz) - e^{-\pi i\nu/2}J_\nu(iz)}{\sin(\nu\pi)}. \tag{5}$$

If ν is an integer n, then it is understood that we define the latter two functions by taking the limits as $\nu \to n$ in (4) and (5). Let

$$I_\nu(z) := -Y_\nu(z) - \frac{2}{\pi}K_\nu(z). \tag{6}$$

Then a famous identity of G.F. Voronoï [20] asserts that

$$\begin{aligned}\sum_{n\le x}{}' d(n) &= x\,(\log x + 2\gamma - 1) + \frac{1}{4} + \sum_{n=1}^{\infty} d(n)\left(\frac{x}{n}\right)^{1/2} I_1(4\pi\sqrt{nx}) \\ &=: x\,(\log x + 2\gamma - 1) + \frac{1}{4} + \Delta(x),\end{aligned} \tag{7}$$

where γ denotes Euler's constant and $\Delta(x)$ is the "error term." The *Dirichlet divisor problem* asks for the exact order of magnitude of $\Delta(x)$ as $x \to \infty$. Voronoï employed (7) to prove that $\Delta(x) = O(x^{1/3}\log x)$ as $x \to \infty$. It is conjectured that $\Delta(x) = O(x^{1/4+\epsilon})$, for each $\epsilon > 0$, as $x \to \infty$, and a survey of this difficult classical problem can also be found in [7].

In many cases an identity may not exist for $\sum_{n\le x} a(n)$, but it may exist for $\sum_{n\le x} a(n)(x-n)^\rho$ for sufficiently large ρ. Moreover, the weighted identity generally converges absolutely and uniformly on compact subintervals of $(0,\infty)$ making it more convenient to use than an identity for $\sum_{n\le x} a(n)$, which is discontinuous at positive integers n when $a(n) \neq 0$. Then one can apply a method of finite differences, originally due to E. Landau, to the sum $\sum_{n\le x} a(n)(x-n)^\rho$ to gain information about $\sum_{n\le x} a(n)$ [11, Theorem 4.1, pp. 106–111]. The sums $\sum_{n\le x} a(n)(x-n)^\rho$ are sometimes called Riesz means. Note that for "small" n, the contribution of $(x-n)^\rho$ is "large," while for large n, the contribution of $(x-n)^\rho$ is "small." Very roughly, arithmetic functions are "small" for "small" n and "large" for "large" n, and so $(x-n)^\rho$ acts as a "smoothing factor." In fact, W. Sierpinski [18] used an identity for $\sum_{n\le x} r_2(n)(x-n)$ to show that $P(x) = O(x^{1/3})$, as x tends to infinity.

We emphasize that the logarithmic sums $\sum_{n\le x} a(n)\log^\rho(x/n)$ can also be used in the study of the average order of certain arithmetic functions, since $\log^\rho(x/n)$ has a "smoothing" effect similar to that of $(x-n)^\rho$, for in each case, when n is "small," the contributions of these factors are "large," while when n is "large", the contributions of these factors are "small." Generally, for "small" ρ, the simplicities of the identities for $\sum_{n\le x} a(n)(x-n)^\rho$ and $\sum_{n\le x} a(n)\log^\rho(x/n)$ are comparable, but for "large" ρ, the identities for the former sum are usually more elegant than those for the latter sum. It is likely for this reason that Riesz means have been employed instead of logarithmic means in the study of the average order of arithmetic functions.

The goal of this paper is to provide a survey of identities for $\sum_{n\le x} a(n)\log(x/n)$, which, because of their intrinsic beauty, deserve to be better known than they are. We are confining our attention only to the case $\rho = 1$, because with increasing ρ, the logarithmic mean identities diminish in elegance; see, for example, [3].

2 History and Examples

To the best of our knowledge, the first logarithmic mean identity is due to A. Oppenheim [14] in 1927. Let $d(n)$ denote the number of divisors of n. Then [14, p. 342], for $x > 0$,

$$\sum_{n\le x} d(n)\log\frac{x}{n} = x\log x - x + (2\gamma-1)x + \frac{1}{4}\log x + \frac{1}{2}\log(2\pi) - \frac{1}{2\pi}\sum_{n=1}^{\infty}\frac{d(n)}{n}I_0(4\pi\sqrt{nx}), \tag{8}$$

where γ denotes Euler's constant, I_0 is defined by (6), and the series on the right-hand side of (8) converges absolutely and uniformly on compact subsets of $(0,\infty)$.

Oppenheim's proof is interesting. Let $\sigma_k(n) = \sum_{d|n} d^k$. He derives a general identity for $\sum_{n\le x}\sigma_k(n)(x-n)^\rho$ [14, p. 340], which we relate only for $|k| < \frac{1}{2}$ and $\rho = 0$. Let

$$F_\nu(z) := \cos(\tfrac{1}{2}\nu\pi)J_\nu(z) + \sin(\tfrac{1}{2}\nu\pi)I_\nu(z),$$

where $J_\nu(z)$ and $I_\nu(z)$ are defined in (3) and (6), respectively. Then

$$\sum_{n\le x}{}'\sigma_k(n) = \Phi_k(x) + \sum_{n=1}^{\infty}\sigma_k(n)\left(\frac{x}{n}\right)^{(k+1)/2}F_{k+1}(4\pi\sqrt{nx}), \tag{9}$$

where $\Phi_k(x)$ is the sum of the residues of

$$\frac{\zeta(z)\zeta(z-k)}{z}x^z.$$

Using (9), Oppenheim forms an identity for

$$L(k) := \frac{1}{k}\left\{x^k\sum_{n\le x}\sigma_{-k}(n) - \sum_{n\le x}\sigma_k(n)\right\}. \tag{10}$$

He then takes the limit of his identity for $L(k)$ as $k \to 0$. Oppenheim did not provide any details, and we will not as well, except that we will evaluate, by (10) and L'Hospital's rule,

$$\begin{aligned}\lim_{k\to 0} L(k) &= \lim_{k\to 0}\left\{x^k \log x \sum_{n\le x}\sigma_{-k}(n) - x^k \sum_{n\le x}\sum_{d|n} d^{-k}\log d - \sum_{n\le x}\sum_{d|n} d^k \log d\right\}\\ &= \log x \sum_{n\le x} d(n) - 2\sum_{n\le x}\sum_{d|n}\log d\\ &= \log x \sum_{n\le x} d(n) - \sum_{n\le x}\sum_{d|n}\log n\\ &= \sum_{n\le x} d(n)\log\frac{x}{n},\end{aligned}$$

because

$$\sum_{d|n}\log d = \sum_{d|n}\log\frac{n}{d} = \log n\, d(n) - \sum_{d|n}\log d.$$

The only other proof of (8) of which we are aware is due to the first author [3, p. 371], who deduced (8) from a general identity, established by him for $\sum_{n\le x} a(n)\log^{\rho}(x/n)$ by a method completely different from that of Oppenheim.

Oppenheim [14, p. 312] further remarks, "Similarly we can obtain identities for ... and

$$\sum_{n\le x} r_2(n)\log\frac{x}{n}."$$

However, Oppenheim provides no details. In 1954, C. Müller [13] proved that

$$\sum_{n\le x} r_2(n)\log\frac{x}{n} = \pi x - \log x - \frac{1}{4}\log\frac{\Gamma^4(1/4)}{4\pi} + O(x^{-1/4}), \tag{11}$$

as $x \to \infty$. He did not provide an exact formula for the error term on the right side of (11). L. Carlitz [9] gave a simpler proof of (11), but his method did not yield a value for the constant term in closed form on the right-hand side of (11). The first author [3, p. 372] established an identity for the first time, showing that

$$\sum_{n\le x} r_2(n)\log\frac{x}{n} = \pi x - \log x + \zeta_2'(0) - \frac{1}{\pi}\sum_{n=1}^{\infty}\frac{r_2(n)}{n} J_0(2\pi\sqrt{nx}), \tag{12}$$

where $\zeta_2'(s)$ is defined in (1). The error term in (11) follows readily from the well-known asymptotic formula [21, p. 199]

$$J_\nu(x) = \left(\frac{2}{\pi x}\right)^{1/2} \cos\left(x - \tfrac{1}{2}\nu\pi - \tfrac{1}{4}\pi\right) + O\left(\frac{1}{x^{3/2}}\right), \tag{13}$$

as $x \to \infty$. R. Ayoub and S. Chowla [2], [12, pp. 1189–1191], unaware of [3], established (11), including showing that

$$\zeta_2'(0) = -\frac{1}{4}\log\frac{\Gamma^4(1/4)}{4\pi}.$$

D. Redmond [16] generalized the work of Ayoub and Chowla by replacing $r_2(n)$ by

$$d_{\chi_1,\chi_2}(n) = \sum_{d|n} \chi_1(d)\chi_2(n/d), \tag{14}$$

where χ_1 and χ_2 are characters modulo q_1 and q_2, respectively. Thus, when $\chi_1(n) \equiv 1$ and $\chi_2(n)$ is the primitive, non-principal character modulo 4, then $d_{\chi_1,\chi_2}(n) = \frac{1}{4}r_2(n)$. If $\chi_1(n) = \chi_2(n) \equiv 1$, then $d_{\chi_1,\chi_2}(n) = d(n)$. Redmond did not prove (8) and (12), but instead established results in which the infinite series of Bessel functions are replaced by error terms. In these two examples, Redmond claimed error terms improving that of Müller and of Ayoub and Chowla in (11), and also that obtained by approximating the Bessel functions in (8) by (13). However, in [17], Redmond acknowledged that his claimed error terms are incorrect and that his methods only yield error terms that are obtained by using (13).

C. Calderón and M.J. Zárate [8] generalized Redmond's work by proving an asymptotic formula for $\sum_{n\le x} a(n)\log^k(x/n)$, where $a(n)$ is an arithmetical function (too complicated to state here) considerably generalizing (14).

U.M.A. Vorhauer [19, p. 60, Theorem 2], apparently unfamiliar with the earlier work of Müller, Carlitz, Ayoub and Chowla, Redmond, and Calderón and Zárate, also established (11). Her result was actually a special case of a general theorem in which she established an "identity" for $\sum_{n\le x} a(n)\log^k(x/n)$, where $k \ge 0$ and $a(n)$ is generated by a Dirichlet series satisfying a functional equation involving a very general product of gamma factors. Her theorem [19, p. 59, Theorem 1] is more general than the one proved in [3], where the arithmetical functions are generated by Dirichlet series satisfying functional equations involving $\Gamma^m(s)$, where m is a positive integer. However, Vorhauer's general "identity" contains an "error term," for which estimates are given, while the identity in [3] is exact and written in terms of Bessel functions. The primary purpose of Vorhauer's paper is to provide precise estimates for the "error terms."

Let us return to Ramanujan's tau-function, one of the three examples discussed in the Introduction. From [3, p. 372], we record the identity

$$\sum_{n\le x}\tau(n)\log\frac{x}{n}=\frac{2}{(4\pi)^{12}}\sum_{n=1}^{\infty}\frac{\tau(n)}{n^{12}}\int_0^{4\pi\sqrt{nx}}u^{11}J_{12}(u)du. \tag{15}$$

The identity (15) illustrates a common roadblock in establishing elegant logarithmic mean identities—the identities often involve integrals that are not readily evaluated in closed form, as is the case with the integrals on the right side of (15).

The present authors and their colleague, A. Zaharescu, have devoted considerable efforts in recent years to establishing two intriguing identities found in Ramanujan's lost notebook [15] that are connected, respectively, with the classical, unsolved *circle* and *divisor* problems. For example, see their paper [6], their survey paper [7], and an account of much of their work in the book [1] by Andrews and Berndt. We record only one of the two identities. First define

$$F(x)=\begin{cases}[x], & \text{if } x \text{ is not an integer,}\\ x-\frac{1}{2}, & \text{if } x \text{ is an integer.}\end{cases} \tag{16}$$

We offer now the first entry.

Entry 1 (p. 335). *Let $F(x)$ be defined by (16). If $0<\theta<1$ and $x>0$, then*

$$\sum_{n=1}^{\infty}F\left(\frac{x}{n}\right)\sin(2\pi n\theta)=\pi x\left(\frac{1}{2}-\theta\right)-\frac{1}{4}\cot(\pi\theta)$$
$$+\frac{1}{2}\sqrt{x}\sum_{m=1}^{\infty}\sum_{n=0}^{\infty}\left\{\frac{J_1\left(4\pi\sqrt{m(n+\theta)x}\right)}{\sqrt{m(n+\theta)}}-\frac{J_1\left(4\pi\sqrt{m(n+1-\theta)x}\right)}{\sqrt{m(n+1-\theta)}}\right\}.$$

It was natural for us to ask if there exist logarithmic mean identities corresponding to Ramanujan's two entries on page 335 of his lost notebook. Indeed, we found such analogues. However, to establish these logarithmic analogues, we first need to establish analogues of (8) for weighted divisor functions, which we now define.

For a character χ, define the weighted divisor sum

$$d_\chi(n):=\sum_{d|n}\chi(d).$$

If χ is a character modulo q, the Gauss sum $\tau(\chi)$ is defined by

$$\tau(\chi):=\sum_{h=1}^{q-1}\chi(h)e^{2\pi ih/q}.$$

Lastly, for any character χ modulo q and $\sigma > 1$, recall that the Dirichlet L-series is defined by

$$L(s,\chi) := \sum_{n=1}^{\infty} \chi(n) n^{-s}.$$

It is well-known that $L(s,\chi)$ can be analytically continued into the entire complex s-plane.

We are now ready to state two new logarithmic mean identities [5].

Theorem 2. *If χ denotes an odd primitive character modulo q, then*

$$\sum_{n\le x} d_\chi(n) \log\frac{x}{n} = xL(1,\chi) + \frac{i\tau(\chi)}{2\pi}\log(2\pi x)L(1,\overline{\chi}) - \frac{1}{2}L'(0,\chi) + \frac{i\tau(\chi)}{2\pi}\sum_{n=1}^{\infty}\frac{d_{\overline{\chi}}(n)}{n} J_0(4\pi\sqrt{nx/q}). \tag{17}$$

Theorem 3. *If χ is an even, non-principal, primitive character modulo q, then*

$$\sum_{n\le x} d_\chi(n)\log\frac{x}{n} = xL(1,\chi) - \frac{1}{2}L'(0,\chi) - \frac{\tau(\chi)}{2\pi}\sum_{n=1}^{\infty}\frac{d_{\overline{\chi}}(n)}{n} I_0(4\pi\sqrt{nx/q}). \tag{18}$$

Theorems 2 and 3 are special cases of theorems in [3], but the identities and the details of their proofs were not previously worked out until the authors did so in [5].

We are now ready to offer the logarithmic mean identity motivated by Entry 1, established with the key aid of Theorem 2, and proved by the authors in [5]. (A corresponding entry motivated by Ramanujan's second entry on page 335 of [15] and established with the help of Theorem 3 will not be given here.)

Theorem 4. *Let $x > 0$ and $0 < \theta < 1$. Then*

$$\sum_{n\le x}\log\frac{x}{n}\sum_{r|n}\sin(2\pi r\theta) = -\frac{\log(4\pi^2 x)+\gamma}{4}\cot(\pi\theta) + \pi x\left(\frac{1}{2}-\theta\right) + \frac{1}{4\pi}\big(\gamma_1(\theta)-\gamma_1(1-\theta)\big) - \frac{1}{4\pi}\sum_{\substack{m\ge 1\\ n\ge 0}}\left\{\frac{J_0\left(4\pi\sqrt{m(n+\theta)x}\right)}{(m(n+\theta))} - \frac{J_0\left(4\pi\sqrt{m(n+1-\theta)x}\right)}{(m(n+1-\theta))}\right\}, \tag{19}$$

where $\gamma_1(\theta)$ and $\gamma_1(1-\theta)$ are the Laurent series coefficients of the Hurwitz zeta function $\zeta(s,a)$, also called generalized Stieltjes constants, defined by Berndt [4, p. 152]

$$\zeta(s,a) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \gamma_n(a)(s-1)^n. \tag{20}$$

Lastly, suppose that we consider the logarithmic mean identity associated with the arithmetic function $a(n) \equiv 1$, which, of course, is generated by $\zeta(s)$. Then one can show that [3, p. 370]

$$\begin{aligned}\sum_{n\le x} \log\frac{x}{n} &= x - \frac{1}{2}\log x - \frac{1}{2}\log(2\pi) - \frac{1}{\pi}\sum_{n=1}^{\infty}\int_{2\pi nx}^{\infty} \frac{\sin u}{u}du \\ &\sim x - \frac{1}{2}\log x - \frac{1}{2}\log(2\pi) - \sum_{n=2}^{\infty} \frac{B_n(x-[x])}{(n-1)!x^{n-1}},\end{aligned} \tag{21}$$

as x tends to infinity, upon successive integrations by parts, where $B_n(x)$, $n \ge 2$, denotes the nth Bernoulli polynomial. (Complete details may be found in [3, p. 371].) The asymptotic expansion (21) is equivalent to Stirling's asymptotic series expansion for the gamma function.

We have not recorded all known logarithmic mean identities that can be found in the literature. For example, let $F(n)$ denote the number of nonzero integral ideals of norm n in either an imaginary quadratic number field or a real quadratic number field. Then in each of these cases, identities for $\sum_{n\le x} F(n)\log(x/n)$ are derived in [3]. Redmond [16] also considered the case of an imaginary quadratic number field, but with the infinite series of Bessel functions replaced by an error term.

References

1. G.E. Andrews, B.C. Berndt, *Ramanujan's Lost Notebook, Part IV* (Springer, New York, 2013)
2. R. Ayoub, S. Chowla, On a theorem of Müller and Carlitz. J. Number Theory **2**, 342–344 (1970)
3. B.C. Berndt, Identities involving the coefficients of a class of Dirichlet series, II. Trans. Am. Math. Soc. **137**, 361–374 (1969)
4. B.C. Berndt, On the Hurwitz zeta-function. Rocky Mt. J. Math. **2**, 151–157 (1972)
5. B.C. Berndt, S. Kim, Logarithmic means and double series of Bessel functions. Int. J. Number Theory. **11**, 1535–1556 (2015)
6. B.C. Berndt, S. Kim, A. Zaharescu, The circle and divisor problems, and double series of Bessel functions. Adv. Math. **236**, 24–59 (2013)
7. B.C. Berndt, S. Kim, A. Zaharescu, The circle and divisor problems, and Ramanujan's contributions through Bessel function series, in *The Legacy of Srinivasa Ramanujan: Proceedings of an International Conference in Celebration of the 125th Anniversary of Ramanujan's Birth*, University of Delhi, 17–22 December 2012, ed. by B.C. Berndt, D. Prasad (Ramanujan Mathematical Society, Mysore, 2013), pp. 111–127
8. C. Calderón, M.J. Zárate, Inversion formulas for Dirichlet series. Arch. Math. (Basel) **53**, 40–45 (1989)
9. L. Carlitz, A formula connected with lattice points in a circle. Abh. Math. Sem. Univ. Hamburg **21**, 87–89 (1957)

10. K. Chandrasekharan, R. Narasimhan, Hecke's functional equation and arithmetical identities. Ann. Math. (2) **74**, 1–23 (1961)
11. K. Chandrasekharan, R. Narasimhan, Functional equations with multiple gamma factors and the average order of arithmetical functions. Ann. Math. (2) **76**, 93–136 (1962)
12. S. Chowla, *The Collected Papers of Sarvadaman Chowla*, vol. III, ed. by J.G. Huard, K.S. Williams (Les Publications CRM, Montreal, 1999)
13. C. Müller, Eine Formel der analytischen Zahlentheorie. Abh. Math. Sem. Univ. Hamburg **19**, 62–65 (1954)
14. A. Oppenheim, Some identities in the theory of numbers. Proc. Lond. Math. Soc. **2**(1), 295–350 (1927)
15. S. Ramanujan, *The Lost Notebook and Other Unpublished Papers* (Narosa, New Delhi, 1988)
16. D. Redmond, A generalization of a theorem of Ayoub and Chowla. Proc. Am. Math. Soc. **86**, 574–580 (1982)
17. D. Redmond, Corrections and additions to "A generalization of a theorem of Ayoub and Chowla". Proc. Am. Math. Soc. **90**, 345–346 (1984)
18. W. Sierpinski, O pewnem zagadnieniu z rachunku funkcyj asymptotycznych. Prace Mat. Fiz. **17**, 77–118 (1906)
19. U.M.A. Vorhauer, Three two-dimensional Weyl steps in the circle problem, II. The logarithmic Riesz mean for a class of arithmetic functions. Acta Arith. **91**, 57–73 (1999)
20. G.F. Voronoï, Sur une fonction transcendante et ses applications à la sommation de quelques séries. Ann. École Norm. Sup. (3) **21**, 207–267, 459–533 (1904)
21. G.N. Watson, *Theory of Bessel Functions*, 2nd edn. (University Press, Cambridge, 1966)

Universal Thickening of the Field of Real Numbers

Alain Connes and Caterina Consani

To the memory of M. Krasner, in recognition of his farsightedness.

Abstract We define the universal thickening of the field of real numbers. This construction is performed in three steps which parallel the universal perfection, the Witt construction and a completion process. We show that the transposition of the perfection process at the real archimedean place is identical to the "dequantization" process and yields Viro's tropical real hyperfield $\mathbb{R}^\flat$. Then, we prove that the archimedean Witt construction in the context of hyperfields allows one to recover a field from a hyperfield, and we obtain the universal pro-infinitesimal thickening $\mathbb{R}_\infty$ of $\mathbb{R}$. Finally, we provide the real analogues of several algebras used in the construction of the rings of p-adic periods. We supply the canonical decomposition of elements in terms of Teichmüller lifts, we make the link with the Mikusinski field of operational calculus and compute the Gelfand spectrum of the archimedean counterparts of the rings of p-adic periods. In the second part of the paper we also discuss the complex case and its relation with the theory of oscillatory integrals in quantum physics.

1 Introduction

This paper establishes an analogue of the construction of the rings of periods of p-adic Hodge theory (cf. e.g. [11–13]) when a p-adic field is replaced by the field $\mathbb{R}$ of real numbers. We show that the original ideas of M. Krasner, which

A. Connes
Collège de France, 3 rue d'Ulm, Paris 75005, France

I.H.E.S., Bures-sur-Yvette, France

Ohio State University, Columbus, OH 43210, USA
e-mail: alain@connes.org

C. Consani (✉)
Department of Mathematics, The Johns Hopkins University, Baltimore, MD 21218, USA
e-mail: kc@math.jhu.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_2

were motivated by the correspondence he first unveiled between Galois theories in unequal characteristics [17], reappear unavoidably when the above analogy is developed. The interest in pursuing this construction is enhanced by our recent discovery of the *Arithmetic Site* [6] with its structure sheaf of semirings of characteristic 1, whose geometric points involve in a crucial manner the tropical semifield $\mathbb{R}_+^{\max}$. The encounter of a structure of characteristic 1 which is deeply related to the non-commutative geometric approach to the Riemann Hypothesis has motivated our search for the replacement of the p-adic constructions at the real archimedean place.

We recall that the definition of the rings of p-adic periods is based on three main steps. The first process (universal perfection) is a functorial construction which links a p-perfect field L of characteristic zero (e.g. the field $\mathbb{C}_p$ of p-adic complex numbers) to a perfect field $F(L)$ of characteristic p (cf. Appendix 2 for notations).

The second step is the p-isotypical Witt construction which defines a functorial process lifting back from characteristic p to characteristic zero (cf. Appendix 3).

Finally, in the third step one defines various rings of periods B, by making use of

- The integer ring $\mathscr{O}_F \subset F(\mathbb{C}_p)$ and other natural rings obtained from it.
- The canonical covering homomorphism $\theta : W(\mathscr{O}_F) \to \mathbb{C}_p$ (cf. Appendix 4).
- Natural norms of p-adic type and corresponding completions.

These constructions then provide, for each ring of periods, a functor from the category of p-adic Galois representations to a category of modules whose definition no longer involves the original (absolute) Galois group but trades it for an action of the Frobenius φ, a differential operator etc. There is a very rich literature covering all these topics, starting of course with the seminal, afore mentioned papers of J.-M. Fontaine; we refer to [1] for a readable introductory overview.

For the field $\mathbb{R}$ of real numbers, Galois theory is of little help since $\mathrm{Aut}(\mathbb{R})$ is the trivial group and $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathbb{Z}/2\mathbb{Z}$ is too small. However, the point that we want to emphasize in this paper is that the transposition of the above three steps is still meaningful and yields non-trivial, relevant rings endowed with a *canonical* one parameter group of automorphisms $\mathbf{F}_\lambda$, $\lambda \in \mathbb{R}_+^\times$, which replaces the Frobenius φ. More precisely, the analogues of the above three steps are

1. A dequantization process, from fields to hyperfields.
2. An extension (W-models) of the Witt construction that lifts back structures from hyperfields to fields.
3. Several completion processes which yield the relevant Banach and Frechet algebras.

We discovered that the two apparently unrelated processes of dequantization on one side (cf. [20]) and the direct transposition of the perfection process to the real archimedean place on the other, are in fact identical. The perfection process, in the case of the local field $\mathbb{R}$, starts by considering the set $F(\mathbb{R})$ made by sequences $x = (x_n)_{n\geq 0}$, $x_n \in \mathbb{R}$, which satisfy the condition $x_{n+1}^\kappa = x_n$ for all $n \in \mathbb{Z}_{\geq 0}$. Here, κ is a fixed positive *odd* rational number (i.e. $|\kappa|_2 = 1$) such that $|\kappa|_\infty < 1$.

In Sect. 2 we prove that by applying the same algebraic rules as in the construction of the field $F(L)$ in the p-adic case, one inevitably obtains a hyperfield (in the sense of M. Krasner) $\mathbb{R}^\flat$. The hyper-structure on $\mathbb{R}^\flat$ is perfect, independent of the choice of κ and it turns out that $\mathbb{R}^\flat$ coincides with the tropical real hyperfield introduced by O. Viro in [25] as the dequantization of $\mathbb{R}$. The main relevant feature of the hyperfield $\mathbb{R}^\flat$ is to be no longer rigid (unlike the field $\mathbb{R}$) and some of its properties are summarized as follows

Theorem. (*i*) *$\mathbb{R}^\flat$ is a perfect hyperfield of characteristic one, i.e. $x+x=x$, $\forall x \in \mathbb{R}^\flat$ and for any odd integer $n>0$, the map $\mathbb{R}^\flat \ni x \mapsto x^n$ is an automorphism of $\mathbb{R}^\flat$.*

(*ii*) $\mathrm{Aut}(\mathbb{R}^\flat) = \mathbb{R}_+^\times$, *with a canonical one parameter group of automorphisms θ_λ, $\lambda \in \mathbb{R}_+^\times$.*

(*iii*) *The map $x \to x_0$ defines a bijection of sets $\mathbb{R}^\flat \xrightarrow{\sim} \mathbb{R}$; the inverse image of the interval $[-1,1] \subset \mathbb{R}$ is the maximal compact sub-hyperring $\mathcal{O} \subset \mathbb{R}^\flat$.*

No mathematician will abandon with light heart the familiar algebraic framework of rings and fields for the esoteric one of hyperstructures. When Krasner introduced hyperfields (and hyperrings) motivated by the correspondence he had unveiled between the Galois theories in unequal characteristics [17], the main criticism which prevailed was that all the interesting and known examples of hyperfields (and hyperrings) are obtained as quotients K/G of a field (or ring) by a subgroup $G \subset K^\times$ of its multiplicative group, so why not to encode the structure by the (classical) pair (K,G) rather than by the hyperfield K/G. The second step (ii) in our construction exploits exactly that criticism and turns it into a construction which has the additional advantage to parallel the classical p-isotypical Witt construction.

Given a hyperfield H, a *W-model* of H is by definition a triple (K,ρ,τ) where

- K is a field
- $\rho : K \to H$ is a homomorphism of hyperfields
- $\tau : H \to K$ is a multiplicative section of ρ.

The notion of morphism of W-models is straightforward to define. A W-model of H is said to be *universal* if it is an initial object in the category of W-models of H. When such universal model exists it is unique up to canonical isomorphism and we denote it by $W(H)$. In Sect. 3 we show that the universal W-model of $\mathbb{R}^\flat$ exists and it coincides with the triple which was constructed in [3, 5], by working with the tropical semi-field $\mathbb{R}_+^{\max}$ of characteristic one and implementing some concrete formulas, involving entropy, which extend the Teichmüller formula for sums of Teichmüller lifts to the case of characteristic one. We let $W = \mathrm{Frac}(\mathbb{Q}[\mathbb{R}_+^\times])$ be the field of fractions of the group ring of the multiplicative group $\mathbb{R}_+^\times$, $\tau_W : \mathbb{R}_+^\times \to \mathbb{Q}[\mathbb{R}_+^\times] \subset W$ be the canonical group homomorphism and $\rho_W : W \to \mathbb{R}^\flat \sim \mathbb{R}$ be the map defined by

$$\rho_W\left(\sum_i \alpha_i \tau_W(x_i) \,/\, \sum_j \beta_j \tau_W(y_j)\right) = \mathrm{sign}\left(\frac{\alpha_0}{\beta_0}\right)\frac{x_0}{y_0}$$

where $x_0 = \sup\{x_i\}$, $y_0 = \sup\{y_j\}$ and $\alpha_i, \beta_j \in \mathbb{Q}$.

Theorem. *The triple* $(W = Frac(\mathbb{Q}[\mathbb{R}_+^\times]), \rho_W, \tau_W)$ *is the universal* W*-model for* $H = \mathbb{R}^\flat$. *The homomorphism* ρ_W *induces an isomorphism of hyperfields* $W/G \xrightarrow{\sim} \mathbb{R}^\flat$, *where* $G = Ker(\rho_W : W^\times \to \mathbb{R}^{\flat\times})$.

In the p-isotypical Witt construction $R \mapsto W(R)$, the respective roles of (H, K, ρ, τ) correspond to the initial perfect ring R, the p-isotypical Witt ring $W(R)$, the residue homomorphism $\rho : W(R) \to R$ and the Teichmüller lift $\tau : R \to W(R)$. It is important to underline here the fact that while homomorphisms of fields are necessarily injective this restriction no longer applies to hyperfields. This is the reason why one can work directly with fields in the definition of W-models. The subring $W_{\mathbb{Z}}(H) \subset W(H)$ generated by the range of the section τ provides then a ring theoretic structure, at the real archimedean place, and it generates the field $W(H)$. Moreover, the definition of the subring $W_{\mathbb{Z}}(R) \subset W(H)$ is meaningful for any sub-object $R \subset H$. This construction applies in particular to the maximal compact sub-hyperring $\mathscr{O} \subset \mathbb{R}^\flat$ and it provides the starting structure from where one develops the construction of the real archimedean analogues of the various rings used in p-adic Hodge theory. Finally, the functoriality of the set-up of the universal W-models yields, for $H = \mathbb{R}^\flat$, a *canonical* one parameter group of automorphisms:

$$\mathbf{F}_\lambda = W(\theta_\lambda) \in \mathrm{Aut}(W(\mathbb{R}^\flat)), \quad \lambda \in \mathbb{R}_+^\times \tag{1}$$

which are compatible with (i.e. preserve globally) the various subrings defined above. The analogue of the covering map θ is defined, likewise in the p-adic case, as the unique ring homomorphism:

$$\theta : W_{\mathbb{Q}}(\mathbb{R}^\flat) \to \mathbb{R}, \qquad \theta(\tau(x)) = x_0\,, \ \forall x = (x_n)_{n\geq 0} \in F(\mathbb{R}) = \mathbb{R}^\flat. \tag{2}$$

Using the map θ we define the universal formal pro-infinitesimal thickening of $\mathbb{R}$ as the $\mathrm{Ker}(\theta)$-adic completion of $W_{\mathbb{Q}}(\mathbb{R}^\flat)$, i.e. $\mathbb{R}_\infty = \varprojlim_n W_{\mathbb{Q}}(\mathbb{R}^\flat)/\mathrm{Ker}(\theta)^n$.

In Sect. 4, we show (cf. Theorem 3) that $\mathbb{R}_\infty$ is more substantial than the ring $\mathbb{R}[[T]]$ of formal power series with real coefficients. For each non-trivial group homomorphism $\ell : \mathbb{R}_+^\times \to \mathbb{R}$, we define a surjective ring homomorphism $\mathbb{R}_\infty \twoheadrightarrow \mathbb{R}[[T]]$. In fact we find that the real vector space $\Omega_{\mathbb{R}} = \mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ is infinite dimensional and it is inclusive of the $\mathbb{R}$-linearly independent set of natural periods $\pi_p = [p] - p$, indexed by prime numbers. Theorem 4 gives the presentation of $\Omega_{\mathbb{R}}$ by generators $\varepsilon(x)$, $x \in \mathbb{R}$, and relations $((A), (B), (C))$, which coincide with the defining relations of the argument of the $1.\frac{1}{2}$ logarithm (cf. [3, 16]) intrinsically related to the entropy function.

Theorem. *The space* $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ *is the infinite dimensional* $\mathbb{R}$*-vector space* $\Omega_{\mathbb{R}}$ *generated by the symbols* $\varepsilon(x)$, $x \in \mathbb{R}$, *with relations*

$$(A) : \varepsilon(1-x) = \varepsilon(x)$$

$$(B) : \varepsilon(x+y) = \varepsilon(y) + (1-y)\,\varepsilon\left(\frac{x}{1-y}\right) + y\,\varepsilon\left(-\frac{x}{y}\right),\ \forall y \notin \{0,1\}$$

$$(C) : x\,\varepsilon(1/x) = -\varepsilon(x)\,,\ \forall x \neq 0.$$

The above real archimedean analogue of the p-isotypical Witt construction is purely algebraic and the archimedean analogue of the p-adic topology plays a dominant role in the third step (iii) of our construction (cf. Sect. 5). This process yields $\mathbb{R}$-vector spaces and, in direct analogy with the theory of p-adic rings of periods, the definition of several Banach and Frechet algebras obtained as completions using the direct analogues of the $\|.\|_\rho$ norms of the p-adic theory (cf. Appendix 4). In Theorem 5 we show that the real archimedean analogue $B_\infty^{b,+}$ of the ring $B^{b,+}$ of p-adic Hodge theory (cf. Appendix 4) is the Banach algebra of convolution of finite real Borel measures on $[0,\infty)$. In Sect. 6 we investigate the ideals and the Gelfand spectrum of the Frechet algebras obtained from $B_\infty^{b,+}$ by completion with respect to the archimedean analogue of the norms $\|f\|_\rho$ used in p-adic Hodge theory (cf. Appendix 4). In Theorem 8 we show that the Gelfand spectrum $\mathrm{Spec}\,(B_{\mathbb{C},0}^+)$ of the Frechet algebra $B_{\mathbb{C},0}^+$ is the one point compactification $Y = \mathbb{C}^+ \cup \{\infty\}$ of the open half-plane $\mathbb{C}^+ = \{z \in \mathbb{C} \mid \Re(z) > 0\}$. It follows that the above algebras can be faithfully represented as algebras of holomorphic functions of the complex variable $z \in Y$, and moreover

- The Teichmüller lift $[x]$ of an element $x \in [-1,1]$ is given by the function $z \mapsto \mathrm{sign}(x)|x|^z$.
- For $\rho > 0$ the analogue of the $\|.\|_\rho$ norm is given, with $\alpha = -\frac{1}{\log \rho}$, by

$$\|f\|_\rho = \int_0^\infty e^{-\xi\alpha}|d\phi(\xi)|,\quad \forall f(z) = \int_0^\infty e^{-\xi z} d\phi(\xi)$$

  where the function $\phi(\xi)$ is of bounded variation.
- The one parameter group $\mathbf{F}_\lambda$ acts on $\mathbb{C}^+$ by scaling $z \to \lambda z$ and it fixes $\infty \in Y$.

In Appendix 5 we explain the relation of the point of view taken in this paper and our earlier archimedean Witt construction in the framework of perfect semi-rings of characteristic one. It is simply given by the change of variables $z = \frac{1}{T}$ as explained in (177).

Our analogy with the p-adic case is based on the following canonical decomposition of the elements of $B_\infty^{b,+}$ (cf. Sect. 5, Theorem 6; the symbol $\smile$ denotes the hyperaddition in $\mathbb{R}^\flat$, cf. (8))

Theorem. *Let $f \in B_\infty^{b,+}$. Then, there exists a real number $s_0 > -\infty$ and a real measurable function $s \geq s_0 \mapsto f_s \in [-1,1] \setminus \{0\}$, unique except on a set of Lebesgue measure zero, such that $f_s \backsim f_t = f_s$ for $s \leq t$ and so that $f = \int_{s_0}^{\infty} [f_s] e^{-s} ds$.*

We use this canonical decomposition as a substitute of the p-adic decomposition of every element $x \in B^{b,+}$ in the form $x = \sum_{n \gg -\infty} [x_n] \pi^n$, with $x_n \in \mathscr{O}_F, \forall n$ (we refer again to Appendix 4 for notations). The relation between the asymptotic expansion of $f(z)$ for $z \to \infty$ in powers of $T = \frac{1}{z}$ and the Taylor expansion at $\xi = 0$ of the function $\phi(\xi)$ of the formula $f(z) = \int_0^{\infty} e^{-\xi z} d\phi(\xi)$ is given by the Borel transform. In the simplest example $\phi(\xi) = \frac{\xi}{1+\xi}$ which corresponds to the Euler divergent series:

$$f(z) = f(1/T) \sim \sum (-1)^n n! T^n = \sum (-1)^n n! z^{-n}$$

the canonical decomposition is given by the fast convergent integral $f = \int_0^{\infty} [f_s] e^{-s} ds$ where $f_s = e^{1-e^s} \in [-1,1] \setminus \{0\}$ for all $s \geq 0$. By exploiting Titchmarsh's theorem we then show that, in general, the leading term f_{s_0} in the expansion has a multiplicative behavior in analogy with the p-adic counterpart. This part is directly related to the construction of the Mikusinski field: in Proposition 9 we provide the precise relation by constructing an embedding of the algebra B_∞^+ in the Mikusinski field $\mathfrak{M}$.

In Sect. 7 we start the development of the complex case, namely when the local field $\mathbb{R}$ is replaced by the field $\mathbb{C}$ of complex numbers. We describe an intriguing link between the process of dequantization of $\mathbb{C}$ and the oscillatory integrals which appear everywhere in physics problems. We illustrate this connection by treating in details the case of the Airy function and by showing how the asymptotic expansion of this function (already obtained by Stokes in the nineteenth century) involves an hypersum in the hyperfield quotient of a field of complex valued functions by a subgroup of its multiplicative group. More in general, in the context of gauge theories in physics, the presence of several critical points is unavoidable and for this reason we expect that the formalism deployed by the theory of hyper-structures (hyperrings and hyperfields) might shed some light on the evaluation of Feynman integrals in that context.

Motivated by the Wick rotation in quantum physics, which allows one to trade an oscillatory integral for an integral of real exponentials, we study a simple "toy model" $\mathbb{C}^\flat$ of the dequantization of the field of complex numbers by paralleling the various steps explained before for the real case. In particular, we prove that $\mathbb{C}^\flat$ is the natural perfection of the hyperfield $\mathscr{T}\mathbb{C}$ introduced by Viro. The infinite dimensional, complex vector space $\Omega_{\mathbb{C}} = \mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ naturally associated to the universal, formal pro-infinitesimal thickening $\mathbb{C}_\infty$ of $\mathbb{C}$ contains two $\mathbb{C}$-linearly independent types of periods. The first set is the natural complexification of the set of real periods π_p, while the second period ε is purely complex and it corresponds to $2i\pi$.

Appendix 1 reports a table which describes the archimedean structures that we have defined and discussed in this paper and their p-adic counterparts.

In Appendix 2 we provide a short overview of the well-known construction of universal perfection in number theory.

In Appendix 3 we develop a succinct presentation of the isotypical Witt construction $R \mapsto W(R)$ as a prelude to the theory of W-models. The objects of the basic category are triples (A, ρ, τ). The algebraic geometric meaning of ρ is clear ($\rho : A \to R$ is a ring homomorphism) while the algebraic significance of τ (a multiplicative section of ρ) only becomes conceptual by using the $\mathbb{F}_1$-formalism of monoids.

Finally, in Appendix 4 we shortly review some relevant constructions in p-adic Hodge theory which lead to the definition of the rings of p-adic periods.

2 Perfection in Characteristic One and Dequantization

In this section we prove that the functor defined by Fontaine ([11], Sect. 2.1) which associates to any p-perfect field L a perfect field $F(L)$ of characteristic p has an analogue at the real archimedean place. We find that starting with the field $\mathbb{R}$ of real numbers and taking the limit of the field laws yields unavoidably a hyperfield structure (cf. [4, 17], Sect. 2). This construction shows on one side that hyperfields appear naturally as limit of fields and it also provides on the other side an ideal candidate, namely the tropical real hyperfield $\mathbb{R}^\flat$ introduced in [25] (Sect. 7.2), as a replacement at the real archimedean place, of Fontaine's universal perfection structure. We refer to Appendix 2 for a short overview of Fontaine's original construction.

Given a p-perfect field L, one defines a perfect field $F(L)$ of characteristic p

$$F = F(L) = \{x = (x^{(n)})_{n\geq 0} | x^{(n)} \in L, (x^{(n+1)})^p = x^{(n)}\} \tag{3}$$

with the two operations ($x, y \in F$)

$$(x+y)_n = \lim_{m\to\infty} (x^{(n+m)} + y^{(n+m)})^{p^m}, \quad (xy)^{(n)} = x^{(n)} y^{(n)}. \tag{4}$$

Formulas (3) and (4) are sufficiently simple to lend themselves to an immediate generalization.

Let us start with a topological field $\mathscr{E}$ and a rational number κ and let consider the following set

$$F = F(\mathscr{E}) = \{x = (x_n)_{n\geq 0} | x_n \in \mathscr{E}, (x_{n+1})^\kappa = x_n\} \tag{5}$$

with the two operations ($x, y \in F$)

$$(x+y)_n = \lim_{m\to\infty} (x_{n+m} + y_{n+m})^{\kappa^m}, \quad (xy)_n = x_n y_n. \tag{6}$$

If $\mathscr{E}$ is a p-perfect field one has $\kappa = p$ and thus the p-adic (normalized) absolute value yields $|\kappa|_p = \frac{1}{p} < 1$. When $\mathscr{E} = \mathbb{R}$, one chooses κ such that the usual archimedean absolute value yields $|\kappa|_\infty < 1$. We assume that the 2-adic valuation of κ is zero (i.e. that the numerator and the denominator of κ are odd), so that the operation $x \mapsto x^\kappa$ is well-defined on $\mathbb{R}$. The following theorem implements the point of view of [25] to establish a precise link between the process of "dequantization" in idempotent analysis and the universal perfection construction.

Theorem 1. (1) *The map $F \ni x \to x_0 \in \mathbb{R}$ defines a bijection of sets and preserves the multiplicative structures.*
(2) *The addition defined by (6) is well defined but not associative.*
(3) *The addition given by the limit of the graphs in (6) is multivalued, associative and defines a hyperfield structure on F which coincides with the real tropical hyperfield $\mathbb{R}^\flat$ of [25].*

Proof. (1) By construction the map $x \mapsto x^\kappa$ is a bijection of $\mathbb{R}$, thus the map $F \ni x \mapsto x^{(0)} \in \mathbb{R}$ is a bijection of sets. It also preserves the multiplicative structure, due to the definition of the multiplication on F as in the second formula in (6).

(2) To avoid confusion with the ordinary addition, we denote the addition in F, as in the first formula in (6) and expressed in terms of $x_0 \in \mathbb{R}$, by $x +' y$. More explicitly, it is given by the formula

$$x +' y = \lim_{m\to\infty} (x^{\kappa^{-m}} + y^{\kappa^{-m}})^{\kappa^m}$$

and is easy to compute. In fact, it is given by

$$x +' y = \begin{cases} x, \text{ if } |x| > |y| \text{ or } x = y; \\ y, \text{ if } |x| < |y| \text{ or } x = y; \\ 0, \text{ if } y = -x. \end{cases} \tag{7}$$

In particular one finds $x +' x = x$, $\forall x \in F$. The associative law cannot hold since for any $y \in F$ with $|y| < |x|$ one has

$$(y +' x) +' -x = x +' -x = 0\,, \quad y +' (x +' -x) = y +' 0 = y\,.$$

(3) For each non negative integer m, the graph G_m of the addition conjugated by the map $x \mapsto x^{\kappa^{-m}}$ is connected (cf. Fig. 1). When $m \to \infty$ these graphs converge, as closed subsets of $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ (as Fig. 2 shows) to the graph G of the addition $\smile$ on the hyperfield $\mathbb{R}^\flat$. The obtained hyperaddition of real numbers is the following

$$x \smile y = \begin{cases} x, & \text{if } |x| > |y| \text{ or } x = y; \\ y, & \text{if } |x| < |y| \text{ or } x = y; \\ \text{[-x,x]}, & \text{if } y = -x. \end{cases} \tag{8}$$

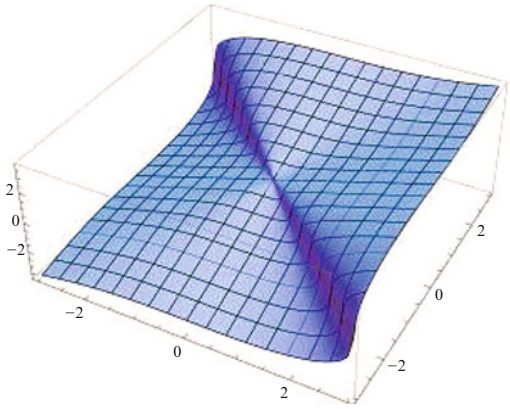


Fig. 1 Graph of the addition in $\mathbb{R}$ after conjugation by $x \mapsto x^3$, i.e. of $(x^3 + y^3)^{\frac{1}{3}}$

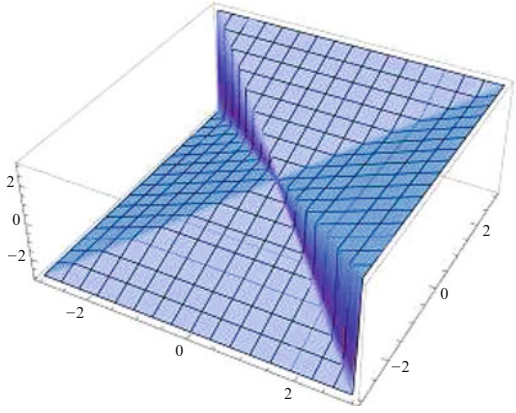


Fig. 2 Graph of the addition in $\mathbb{R}$ after conjugation by $x \mapsto x^{3^n}$ for n large. It converges to the graph of a function which is multivalued on the line $y = -x$

One can see in Fig. 2 how the limit of the graphs of the conjugates of addition becomes multivalued on the anti-diagonal $y = -x$ and fills up the interval $[-x, x]$. One checks directly that with this hyperaddition $\mathbb{R}^b$ is a hyperfield. □

Notice that replacing the sum (7) by the multivalued one (8) is the *only way* of making the latter one associative without altering the first two lines of (7). Indeed, the fact that $0 \in x + (-x)$ implies that for any y with $|y| < |x|$ one has

$$y \in y + (x + (-x)) = (y + x) + (-x) = x + (-x).$$

Remark 1. The second statement of Theorem 1 shows that there is no "formal" proof of associativity when addition is defined by (6) and assuming that the limit exists. The third statement of the theorem implies that hyperfields naturally arise when one considers limits of field structures on the same topological space, since as the proof of the statement (3) shows, the limit of univalent maps giving addition

may well fail to be univalent. The abstract reason behind the associativity of the hyperlaw given by the limit G of the graphs G_n of the conjugate $+_n$ of the addition in $\mathbb{R}$ is that for any convergent sequence $z_n \to z$, $z \in G(x,y)$ there exist convergent sequences $x_n \to x$ and $y_n \to y$ such that $z_n = x_n +_n y_n$. This is easy to see if $|y| < |x|$ or $y = x$ since (with m an odd integer)

$$\partial_x (x^m + y^m)^{1/m} = (1 + (y/x)^m)^{-1+\frac{1}{m}}.$$

If $y = -x$ the result also holds since the range of the real map $\epsilon \mapsto ((1+\epsilon)^m - 1)^{1/m}$, for $|\epsilon| \leq \frac{1}{m}$, is connected and fills up the interval $(-1,1)$ when $m \to \infty$ (m odd).

Definition 1. (1) A hyperfield H is of characteristic one if $x + x = x$, $\forall x \in H$.
(2) A hyperfield H of characteristic one is perfect if and only if for any odd integer $n > 0$, the map $H \ni x \mapsto x^n$ is an automorphism of H.

Proposition 1. (*i*) *The real tropical hyperfield $\mathbb{R}^\flat$ is perfect and of characteristic one.*
(*ii*) *The map $\lambda \mapsto \theta_\lambda$, $\theta_\lambda(x) = \mathrm{sign}(x)|x|^\lambda$, $\forall x \in \mathbb{R}$, defines a group isomorphism $\theta : \mathbb{R}_+^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{R}^\flat)$. If $\lambda = \frac{a}{b} \in \mathbb{Q}_+^\times$ is odd (i.e. both a and b are odd integers) one has $\theta_\lambda(x) = x^\lambda$, $\forall x \in \mathbb{R}$.*
(*iii*) *The compact subset $[-1,1] \subset \mathbb{R}^\flat$ is the maximal compact sub-hyperring $\mathcal{O}$ of $\mathbb{R}^\flat$.*
(*iv*) *The hyperfield $\mathbb{R}^\flat$ is complete for the distance given by $d(x,y) = |x_0 - y_0|$, for $x, y \in F = \mathbb{R}^\flat$.*

Proof. (*i*) follows from the equality $1 + 1 = 1$ which holds in $\mathbb{R}^\flat$. The perfection follows from (*ii*).
(*ii*) The maps θ_λ are automorphisms for the multiplicative structure. They also preserve the hyperaddition $\smile$ on $\mathbb{R}^\flat$. By construction, they agree with $x \mapsto x^\lambda$ when $\lambda \in \mathbb{Q}_+^\times$ is odd. Let $\alpha \in \mathrm{Aut}(\mathbb{R}^\flat)$. Since α is an automorphism of the multiplicative group $\mathbb{R}^\times = \mathbb{R}_+^\times \times \{\pm 1\}$, one has $\alpha(-1) = -1$, and α preserves globally $\mathbb{R}_+^\times$. The compatibility with the hyperaddition shows that α defines an increasing group automorphism of $\mathbb{R}_+^\times$, thus it coincides with θ_λ.
(*iii*) The compact subset $[-1,1] \subset \mathbb{R}^\flat$ is stable under multiplication and hyperaddition. For any element $x \in \mathbb{R}^\flat$ with $x \notin [-1,1]$, the integer powers x^n form an unbounded subset of $\mathbb{R}^\flat$, the maximality property then follows.
(*iv*) By Theorem 1 (1), the map $x \to x_0 \in \mathbb{R}$ defines a bijection of sets which is an isometry for the distance $d(x,y)$. The conclusion follows.

□

We refer to Appendix 2 (Proposition 16) for the p-adic counterpart of the above statements.

3 The Algebraic Witt Construction for Hyperfields

In this paper we use the following formulation of the classical p-isotypical Witt construction which associates to a perfect ring R of characteristic p the strict p-ring $W(R)$ of Witt vectors. We denote by $\rho_R : W(R) \to R$ the canonical homomorphism and $\tau_R : R \to W(R)$ the multiplicative section given by the Teichmüller lift. Next proposition is an immediate corollary of Theorem 1.2.1 of [12].

Proposition 2. *Let p be a prime number and R a perfect ring of characteristic p. The triple $(W(R), \rho_R, \tau_R)$ is the universal object among triples (A, ρ, τ) where A is a (commutative) ring, $\rho : A \to R$ is a ring homomorphism with multiplicative section $\tau : R \to A$ and the following condition holds*

$$A = \varprojlim_n A/\mathrm{Ker}(\rho)^n. \tag{9}$$

We refer to Appendix 3 for an elaboration on the nuance, due to the presence of the multiplicative lift τ in the currently used formulation, with respect to the classical notion of universal p-adic thickening. Next, we proceed in a similar manner with hyperfields, by suitably transposing the above set-up.

Definition 2. Let H be a hyperfield. A Witt-model (W-model) of H is a triple (K, ρ, τ), where K is a field, $\rho : K \to H$ is a homomorphism of hyperfields, and τ is a multiplicative section of ρ.

A morphism $(K_1, \rho_1, \tau_1) \to (K_2, \rho_2, \tau_2)$ of W-models of H is a field homomorphism $\alpha : K_1 \to K_2$ such that the following equations hold

$$\tau_2 = \alpha \circ \tau_1, \quad \rho_1 = \rho_2 \circ \alpha. \tag{10}$$

Definition 3. A W-model for a hyperfield H is universal if there exists a unique morphism from this model to any other W-model of H.

If a universal W-model exists then it is unique up-to unique isomorphism and in that case we denote it by $(W(H), \rho_H, \tau_H)$.

Next, we study the W-models for the real tropical hyperfield $H = \mathbb{R}^b$. As a first step we construct a particular W-model for H and then we shall prove that in fact it is the universal one.

Let $W = \mathrm{Frac}(\mathbb{Q}[\mathbb{R}_+^\times])$ be the field of fractions of the rational group ring $\mathbb{Q}[\mathbb{R}_+^\times]$ of the multiplicative group $\mathbb{R}_+^\times$. We let $\tau_W : \mathbb{R}_+^\times \to W$ be the canonical group homomorphism $\tau_W(x)(= [x])$ and define the map $\rho_W : W \to \mathbb{R}^b \sim \mathbb{R}$ by

$$\rho_W\left(\sum_i \alpha_i \tau_W(x_i) / \sum_j \beta_j \tau_W(y_j)\right) = \mathrm{sign}\left(\frac{\alpha_0}{\beta_0}\right)\frac{x_0}{y_0} \tag{11}$$

where $x_0 = \sup\{x_i\}$, $y_0 = \sup\{y_j\}$ and $\alpha_i, \beta_j \in \mathbb{Q}$. We extend τ_W to a multiplicative section $\tau_W : \mathbb{R}^\flat \to W$ of ρ_W by setting $\tau_W(0) = 0$ and $\tau_W(-x) = -\tau_W(x)$. It is straightforward to verify that (W, ρ_W, τ_W) is a W-model of $\mathbb{R}^\flat$ (the details are provided in the next proof). We claim that it is also the universal one, moreover it describes the full structure of the hyperfield $\mathbb{R}^\flat$ as the quotient of a field by a subgroup of its multiplicative group.

Theorem 2. *The triple* $(W = Frac(\mathbb{Q}[\mathbb{R}_+^\times]), \rho_W, \tau_W)$ *is the universal* W*-model for* $H = \mathbb{R}^\flat$.

The homomorphism ρ_W *induces an isomorphism of hyperfields* $W/G \xrightarrow{\sim} \mathbb{R}^\flat$, *where* $G = Ker(\rho_W : W^\times \to \mathbb{R}^{\flat\times})$.

Proof. First we show that the triple $(W = \mathrm{Frac}(\mathbb{Q}[\mathbb{R}_+^\times]), \rho_W, \tau_W)$ is a W-model and it also fulfills the second property. The map $\tau_W : \mathbb{R}^\flat \to W$, $x \to \tau_W(x) = [x]$ is multiplicative by construction and it is immediate to check that $\rho_W \circ \tau_W = id$, thus $\tau_W = [\,]$ is a multiplicative section of the map ρ_W defined by (11). To understand ρ_W it is useful to consider the field homomorphism $\Phi : W \to \mathscr{M}(\mathbb{C})$, where $\mathscr{M}(\mathbb{C})$ is the field of meromorphic functions on $\mathbb{C}$, defined by the formula

$$\Phi\left(\sum_i \alpha_i \tau_W(x_i) / \sum_j \beta_j \tau_W(y_j)\right)(z) = \frac{\sum_i \alpha_i x_i^z}{\sum_j \beta_j y_j^z}. \tag{12}$$

Then, keeping in mind the notation of (11), one deduces the following interpretation of ρ_W

$$\Phi(X)(z) \sim \left(\frac{\alpha_0}{\beta_0}\right)\left(\frac{x_0}{y_0}\right)^z \quad \text{when } z \to +\infty \tag{13}$$

(since for $x_j < x_0, y_j < y_0$ one has $x_j^z \ll x_0^z$, $y_j^z \ll y_0^z$ when $z \to +\infty$). One can thus state that

$$\exists a \in \mathbb{R}_+,\ \Phi(X)(2n+1) \sim a\rho_W(X)^{2n+1} \quad \text{when } n \to +\infty. \tag{14}$$

This means that one can define $\rho_W : W \to \mathbb{R}^\flat$ by the formula

$$\rho_W(X) = \lim_{n \to +\infty} (\Phi(X)(2n+1))^{1/(2n+1)}. \tag{15}$$

Notice that (15) is well defined because the odd roots are uniquely defined in $\mathbb{R}$. The map ρ_W is clearly multiplicative, next we show that it induces an isomorphism of hyperfields $W/G \xrightarrow{\sim} \mathbb{R}^\flat$, where the subgroup G is the kernel at the multiplicative level, i.e. $G = \ker(\rho_W : W^\times \to \mathbb{R}^{\flat\times})$. By definition the underlying set of G is made by the ratios $(\sum_i \alpha_i \tau_W(x_i))/(\sum_j \beta_j \tau_W(y_j)) \in W$, such that: $x_0 = y_0$ and $\mathrm{sign}(\alpha_0) = \mathrm{sign}(\beta_0)$. What remains to show is that the hyper-addition in $\mathbb{R}^\flat$ coincides with the quotient addition rule $x +_G y$ on $W/G = \mathbb{R}$. By definition one has

$$x +_G y = \{\rho_W(X + Y) |\ \rho_W(X) = x, \rho_W(Y) = y\}. \tag{16}$$

We need to consider three cases:

(a) Assume $|x| < |y|$. Then for some $a, b \in \mathbb{R}_+$ one has $\Phi(X)(2n+1) \sim ax^{2n+1}$ and $\Phi(Y)(2n+1) \sim by^{2n+1}$ and thus it follows that $\Phi(X+Y)(2n+1) \sim by^{2n+1}$. Then one gets $\rho_W(X+Y) = y$.

(b) Assume $x = y$. Then for some $a, b \in \mathbb{R}_+$ one has $\Phi(X)(2n+1) \sim ax^{2n+1}$, $\Phi(Y)(2n+1) \sim bx^{2n+1}$ and $\Phi(X+Y)(2n+1) \sim (a+b)x^{2n+1}$, thus one gets $\rho_W(X+Y) = x$, since $a + b > 0$.

(c) Assume $y = -x$. In this case, we have with $a, b \in \mathbb{R}_+$: $\Phi(X)(2n+1) \sim ax^{2n+1}$, $\Phi(Y)(2n+1) \sim by^{2n+1} = -bx^{2n+1}$. In this case we can only conclude that $|\Phi(X+Y)(2n+1)| \lesssim c|x|^{2n+1}$ which gives $|\rho_W(X+Y)| \leq |x|$. Moreover, by choosing $X = a\tau_W(x)$, $Y = b\tau_W(y)$ for suitable real a, b, we conclude that $\{x, y\} \subset x +_G y$. In fact by taking z, $|z| < |x|$, $X = \tau_W(x) + \tau_W(z)$, $Y = \tau_W(y) = -\tau_W(x)$, one gets $\rho_W(X+Y) = z$ and hence $x +_G y$ is the whole interval between x and y.

This shows that the quotient addition rule on W/G coincides with (8).

Finally, we show that the triple (W, ρ_W, τ_W) is the universal W-model for $H = \mathbb{R}^\flat$.

Let (K, ρ, τ) be a W-model for $H = \mathbb{R}^\flat$. First we prove that the field K is of characteristic zero. Indeed, one has $\rho(1) = 1$ and thus for any positive integer p one derives

$$\rho(p) \in \underbrace{\rho(1) + \cdots + \rho(1)}_{p-times} = \{1\},$$

so that $p \neq 0$, $\forall p$. Next, we note that $\tau(-1) = -1 \in K$. Indeed, since τ is multiplicative one has $\tau(-1)^2 = \tau(1) = 1$ and $\tau(-1) \neq 1$ since $(\rho \circ \tau)(-1) = -1 \neq \rho(1) = 1$. By multiplicativity of τ we thus get

$$\tau(-x) = -\tau(x) \quad \forall x \in H = \mathbb{R}^\flat. \tag{17}$$

We first define the homomorphism $\alpha : W \to K$ on $R = \mathbb{Q}[\mathbb{R}_+^\times] \subset W$. We denote an element in R as $x = \sum_i a_i \tau_W(x_i)$ with $a_i \in \mathbb{Q}$. We define $\alpha : R \to K$ by the formula

$$\alpha\left(\sum_i a_i \tau_W(x_i)\right) = \sum_i a_i \tau(x_i). \tag{18}$$

By applying the property (17) we get $\alpha(\tau_W(x)) = \tau(x)$, $\forall x \in H = \mathbb{R}^\flat$. We check now that $\alpha : R \to K$ is injective. Let $R \ni x = \sum_i a_i \tau_W(x_i) \neq 0$. Let $x_0 = \max\{x_i\}$. One then has

$$\rho(\alpha(x)) = \rho\left(\sum_i a_i \tau(x_i)\right) \in \sum_i \rho(a_i \tau(x_i)).$$

One has $\rho(a) = 1$ for $a \in \mathbb{Q}$, $a > 0$ and $\rho(-1) = -1$ and hence $\rho(a_i\tau(x_i)) = \epsilon_i\rho\tau(x_i) = \epsilon_i x_i$ with ϵ_i the sign of a_i. Thus $\rho(\alpha(x)) \in \sum_H \epsilon_i x_i = \epsilon_0 x_0 \neq 0$ and the injectivity is proven. From the injectivity just proven it follows that $\alpha : R \to K$ defines a field homomorphism $\alpha : \mathrm{Frac}(R) \to K$. By construction one has $\alpha(\tau_W(x)) = \tau(x)\ \forall x \in \mathbb{R}$.

It remains to show the second equality of (10). Consider $\rho \circ \alpha$: to show that this is equal to ρ_W it is enough to prove that they agree on R since both maps are multiplicative. Let $x = \sum_i a_i\tau_W(x_i) \in R$, then one has $\rho(\alpha(x)) \in \sum_i \rho(a_i\tau(x_i))$ and by the above argument one gets $\rho(\alpha(x)) = \epsilon_0 x_0 = \rho_W(x)$. This shows that the morphism α exists and it is unique because $\alpha(\tau_W(x))$ is necessarily equal to $\tau(x)$ so that by linearity we know α on R and hence on $\mathrm{Frac}(R)$. □

The following functoriality property will be applied later in the paper.

Proposition 3. *Let H be a hyperfield and assume that the universal W-model $W(H)$ for H exists. Then there is a canonical group homomorphism*

$$W : Aut(H) \to Aut(W(H)), \qquad W(\theta) = \alpha. \tag{19}$$

Proof. Let $\theta \in \mathrm{Aut}(H)$ be an automorphism of H. Let $(W(H) = K, \rho, \tau)$ be the universal W-model for H. Then, we consider the triple: $(K, \rho' = \theta^{-1} \circ \rho, \tau' = \tau \circ \theta)$. One sees that ρ' is a homomorphism of hyperfields, that τ' is multiplicative and that $\rho'(\tau'(x)) = \theta^{-1}(\rho(\tau(\theta(x)))) = x$. Thus $(K = W(H), \rho', \tau')$ is also a W-model of H. Then it follows from universality that there exists a field homomorphism $\alpha : K \to K$ such that the rules (10) hold, and in particular $\tau \circ \theta = \alpha \circ \tau$. From this and the fact that α is the identity when θ is the identity one deduces the existence of the group homomorphism (19). □

When $H = \mathbb{R}^\flat$ we derive from the above proposition the existence of a one parameter group of automorphisms of $W(\mathbb{R}^\flat)$ given by the (images of the) $\theta_\lambda \in \mathrm{Aut}(\mathbb{R}^\flat)$ (cf. Proposition 1). These operators form the one parameter group of Frobenius automorphisms

$$W(\theta_\lambda) = \mathbf{F}_\lambda \in \mathrm{Aut}(\mathrm{Frac}(\mathbb{Q}[\mathbb{R}_+^\times])). \tag{20}$$

The universal W-model $W(H)$ of a hyperfield H (when it exists) inherits automatically the refined structure of the *field of quotients* of a natural ring

Proposition 4. *Let H be a hyperfield with a universal W-model $(W(H), \rho, \tau)$. Let $W_{\mathbb{Z}}(H) \subset W(H)$ (resp. $W_{\mathbb{Q}}(H) \subset W(H)$) be the (integral) subring (resp. sub $\mathbb{Q}$-algebra) generated by the $\tau(x)$'s, $x \in H$. Then one has*

$$W(H) = Frac(W_{\mathbb{Z}}(H)) = Frac(W_{\mathbb{Q}}(H)). \tag{21}$$

Proof. Let $K = \mathrm{Frac}(W_{\mathbb{Z}}(H)) \subset W(H)$. The map $\tau : H \to W(H)$ has, by construction, image in K and using the restriction ρ_K of $\rho : W(H) \to H$ to K one gets a W-model (K, ρ_K, τ_K) for H. Thus by universality there exists a field

homomorphism $\alpha : W(H) \to K$ such that $\alpha \circ \tau_K(x) = \tau(x)$, $\forall x \in H$. Hence α is surjective on K (as K is generated by the $\tau(x)$'s) and also injective (as field homomorphism). Then $\alpha : W(H) \xrightarrow{\sim} K$ is a field isomorphism. A similar proof shows the second equality in (21). □

Example 1. Let $H = \text{sign} = \{0, \pm 1\}$, be the hyperfield of signs (cf. [4], Definition 2.2) then $W_{\mathbb{Z}}(\text{sign}) = \mathbb{Z}$.

Example 2. Let $H = \mathbb{R}^\flat$, then $W_{\mathbb{Q}}(\mathbb{R}^\flat) = \mathbb{Q}[\mathbb{R}_+^\times]$.

In p-adic Hodge theory (cf. [8], Sect. 5) one defines for a finite extension E of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$ and for any (real) valued complete, algebraically closed field F of characteristic p extension of an algebraically closed field $k|\mathbb{F}_q$, a ring homomorphism $\theta : W_{\mathscr{O}_E}(\mathscr{O}_F) \to \mathbb{C}_p$, $\theta(\sum_{n\geq 0}[x_n]\pi^n) = \sum_{n\geq 0} x_n^{(0)}\pi^n$ ($\pi = \pi_E$ is a chosen uniformizer of $\mathscr{O}_E$). At the real archimedean place, we have the following counterpart

Proposition 5. *There exists a unique ring homomorphism $\theta : W_{\mathbb{Q}}(\mathbb{R}^\flat) \to \mathbb{R}$ such that*

$$\theta([x]) = \theta(\tau(x)) = x^{(0)} = x, \quad \forall x \in \mathbb{R}^\flat. \tag{22}$$

Proof. It follows from Proposition 4 that $W_{\mathbb{Q}}(\mathbb{R}^\flat) = \mathbb{Q}[\mathbb{R}_+^\times]$ and thus the natural map $\mathbb{R}_+^\times \to \mathbb{R}$ extends by linearity and uniquely to a ring homomorphism ($[\,] = \tau$)

$$\theta\Big(\sum_i a_i[x_i]\Big) = \sum_i a_i x_i \in \mathbb{R}. \tag{23}$$

□

4 Universal Formal Pro-infinitesimal Thickening of the Field $\mathbb{R}$

Theorem 2 states the existence of a universal algebraic object whose definition is independent of the completeness condition (9) of Proposition 2. Given a universal object among triples (A, ρ, τ) where A is a (commutative) ring, $\rho : A \to R$ is a ring homomorphism with multiplicative section $\tau : R \to A$, the corresponding data obtained by passing to the completion $\varprojlim_n A/\text{Ker}(\rho)^n$ is automatically universal among the triples which fulfill (9). This suggests to consider the homomorphism $\theta : W_{\mathbb{Q}}(\mathbb{R}^\flat) \to \mathbb{R}$ of Proposition 5 and introduce the following

Definition 4. The universal formal pro-infinitesimal thickening $\mathbb{R}_\infty$ of $\mathbb{R}$ is the $\text{Ker}(\theta)$-adic completion of $W_{\mathbb{Q}}(\mathbb{R}^\flat)$, i.e.

$$\mathbb{R}_\infty = \varprojlim_n W_{\mathbb{Q}}(\mathbb{R}^\flat)/\text{Ker}(\theta)^n.$$

The following theorem shows that $\mathbb{R}_\infty$ has a richer structure than the ring $\mathbb{R}[[T]]$ of formal power series with real coefficients. In fact we prove that the real vector space $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ is infinite dimensional.

Theorem 3. (*i*) *Let $\ell : \mathbb{R}_+^\times \to \mathbb{R}$ be a group homomorphism, then the map*

$$\mathscr{T}_\ell(X)(z) := \sum_i a_i e^{\log(x_i)+(z-1)\ell(x_i)}\,,\ \forall X = \sum_i a_i[x_i] \in W_{\mathbb{Q}}(\mathbb{R}^\flat) \tag{24}$$

defines a ring homomorphism $\mathscr{T}_\ell : W_{\mathbb{Q}}(\mathbb{R}^\flat) \to C^\infty(\mathbb{R})$ to the ring of smooth real functions and

$$\theta(X) = \mathscr{T}_\ell(X)(1),\ \forall X \in W_{\mathbb{Q}}(\mathbb{R}^\flat). \tag{25}$$

(*ii*) *The Taylor expansion at $z = 1$ induces a ring homomorphism*

$$\mathbb{R}_\infty \xrightarrow{\mathscr{T}_\ell} \mathbb{R}[[z-1]], \tag{26}$$

which is surjective if $x\ell(x) + (1-x)\ell(1-x) \neq 0$ for some $x \in \mathbb{R}_+^\times$.

(*iii*) *$\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ is an infinite dimensional real vector space and the "periods" $\pi_p = [p] - p \in \mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$, for p a prime number, are linearly independent over $\mathbb{R}$.*

Proof. (*i*) For any $z \in \mathbb{R}$ the map $\log + (z-1)\ell$ defines a group homomorphism $\mathbb{R}_+^\times \to \mathbb{R}$ and the conclusion follows.

(*ii*) It follows from (*i*) and (148) that one obtains the ring homomorphism (26) since for $X \in \mathrm{Ker}(\theta)^n$ the function $\mathscr{T}_\ell(X)(z)$ vanishes of order $\geq n$ at $z = 1$. We show, under the assumption of (*ii*), that $\mathscr{T}_\ell$ as in (26) is surjective. Let $x \in \mathbb{R}$ with $x\ell(x) + (1-x)\ell(1-x) \neq 0$. One has $s(x) := 1 - [x] - [1-x] \in \mathrm{Ker}(\theta)$; the first derivative of $\mathscr{T}_\ell(s(x))(z)$ at $z = 1$ is equal to $-(x\ell(x) + (1-x)\ell(1-x))$ and it does not vanish. Using the $\mathbb{R}$-linearity which follows from $W_{\mathbb{Q}}(\mathbb{R}^\flat)/\mathrm{Ker}(\theta) = \mathbb{R}$ and by implementing the powers $s(x)^n$, one derives the surjectivity.

(*iii*) One has $\pi_n := [n] - n \in \mathrm{Ker}(\theta)$ for any integer n and hence for any prime number $n = p$. Next we show that these elements are linearly independent in $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$. The latter is a vector space over $W_{\mathbb{Q}}(\mathbb{R}^\flat)/\mathrm{Ker}(\theta) = \mathbb{R}$, and the multiplication by a real number $y \in \mathbb{R}$ is provided by the multiplication by any $s \in W_{\mathbb{Q}}(\mathbb{R}^\flat)$ such that $\theta(s) = y$. In particular we can always choose the lift of the form $s = a[b]$ where $a \in \mathbb{Q}$ and $b \in \mathbb{R}_+^\times$. Assume now that there is a linear relation of the form

$$X = \sum_i a_i[b_i]\pi_{p_i} \in \mathrm{Ker}(\theta)^2 \tag{27}$$

where $a_i \in \mathbb{Q}$, $b_i \in \mathbb{R}_+^\times$ and p_i are distinct primes. Let $\ell : \mathbb{R}_+^\times \to \mathbb{R}$ be a group homomorphism, then by using (*ii*) we see that $\mathscr{T}_\ell(X)$ vanishes at order ≥ 2 at $z = 1$, and thus $\left(\frac{d}{dz}\right)_{z=1} \mathscr{T}_\ell(X) = 0$. Using $\pi_{p_i} \in \mathrm{Ker}(\theta)$, we derive, using (24),

$$\left(\frac{d}{dz}\right)_{z=1} \mathscr{T}_\ell(a_i[b_i]\pi_{p_i}) = a_i b_i p_i \ell(p_i)$$

so that $\sum_i a_i b_i p_i \ell(p_i) = 0$. Since the logarithms of prime numbers are rationally independent, and since the additive group $\mathbb{R}$ is divisible, hence injective among abelian groups, one can construct a group homomorphism $\ell : \mathbb{R}_+^\times \to \mathbb{R}$ such that the values of $\ell(p_i)$ are arbitrarily chosen real numbers. In view of the fact that the above relation is always valid, we derive that all the coefficients $a_i b_i p_i$ must vanish and that the original relation is therefore trivial. □

Next, we extend the above construction to obtain linear forms on $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$.

Lemma 1. (*i*) *Let $\delta : W_\mathbb{Q} \to \mathbb{R}$ be a $\mathbb{Q}$-linear map such that*

$$\delta(fg) = \theta(f)\delta(g)\,,\ \forall g \in \mathrm{Ker}(\theta). \tag{28}$$

Then δ vanishes on $\mathrm{Ker}(\theta)^2$ and it defines an $\mathbb{R}$-linear form on $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$.

(*ii*) *Let $\psi : \mathbb{R} \to \mathbb{R}$ be such that $\psi(-x) = -\psi(x)$ for all $x \in \mathbb{R}$ and*

$$\psi(x(y+z)) - x\psi(y+z) = \psi(xy) - x\psi(y) + \psi(xz) - x\psi(z)\,,\ \forall x, y, z \in \mathbb{R} \tag{29}$$

then the following equality defines a $\mathbb{Q}$-linear map $\delta_\psi : W_\mathbb{Q} \to \mathbb{R}$ fulfilling (28)

$$\delta_\psi\left(\sum_j a_j[x_j]\right) := \sum_j a_j \psi(x_j)\,,\ \forall a_j \in \mathbb{Q},\ x_j \in \mathbb{R}. \tag{30}$$

Proof. (*i*) For $f, g \in \mathrm{Ker}(\theta)$, it follows from (28) that $\delta(fg) = 0$, thus δ vanishes on $\mathrm{Ker}(\theta)^2$. The action of $s \in \mathbb{R}$ on $g \in \mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ is given by fg for any $f \in W_\mathbb{Q}$ with $\theta(f) = s$. Thus the $\mathbb{R}$-linearity of the restriction of δ to $\mathrm{Ker}(\theta)$ follows from (28).

(*ii*) By construction the map δ defined by (30) is well defined since ψ is odd, and $\mathbb{Q}$-linear. To check (28) we can assume that $f = [x]$ for some $x \in \mathbb{R}$. One then has

$$\delta(fg) - \theta(f)\delta(g) = \sum_j b_j(\psi(xy_j) - x\psi(y_j))\,,\ \forall g = \sum_j b_j[y_j]. \tag{31}$$

The map $L : \mathbb{R} \to \mathbb{R}$ given by $L(y) = \psi(xy) - x\psi(y)$ is additive by (29) and thus

$$\sum_j b_j(\psi(xy_j) - x\psi(y_j)) = \sum_j b_j L(y_j) = L\Big(\sum_j b_j y_j\Big).$$

When $g \in \mathrm{Ker}(\theta)$, one derives $\theta(g) = \sum_j b_j y_j = 0$ and thus one obtains (28). □

The next statements show how the entropy appears naturally to define "periods".

Lemma 2. (*i*) *The symbol* $s(x) := 1 - [x] - [1 - x]$ *defines a map* $\mathbb{R} \to \mathrm{Ker}(\theta) \subset W_{\mathbb{Q}}(\mathbb{R}^\flat)$ *such that*

$$(a) : s(1-x) = s(x)$$

$$(b) : s(x+y) = s(y) + [1-y]s\Big(\frac{x}{1-y}\Big) + [y]s\Big(-\frac{x}{y}\Big)$$

$$(c) : [x]s(1/x) = -s(x).$$

(*ii*) *The* $\mathbb{R}$*-linear span in* $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ *of the* $s(x)$*, for* $x \in \mathbb{R}$ *generates* $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$.

Proof. (*i*) The symbol $[x]$ extends to $\mathbb{R}$ by $[-x] = -[x]$. The equality (a) holds by construction. We check (b) ((c) is checked in the same way). One has

$$[1-y]s\Big(\frac{x}{1-y}\Big) = [1-y] - [x] - [1-y-x],\ \ [y]s\Big(-\frac{x}{y}\Big) = [y] + [x] - [x+y]$$

$$[1-y]s\Big(\frac{x}{1-y}\Big) + [y]s\Big(-\frac{x}{y}\Big) = [1-y] - [1-y-x] + [y] - [x+y] = s(x+y) - s(y).$$

(*ii*) The $\mathbb{R}$-linear span in $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ of the $s(x)$ contains all the $[x+y]s(x/(x+y))$ for $x + y \neq 0$, and hence all the $[x+y] - [x] - [y]$. Let $f \in \mathrm{Ker}(\theta)$, then a non-zero integer multiple of f is of the form

$$nf = \sum_j [x_j] - \sum_k [y_k]\,,\ \ \sum_j x_j = \sum_k y_k$$

and both $\sum_j [x_j] - [\sum_j x_j]$ and $\sum_k [y_k] - [\sum_k y_k]$ belong to the $\mathbb{R}$-linear span of the $s(z)$ in $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$.

□

Theorem 4. *The space* $\mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ *is the infinite dimensional* $\mathbb{R}$*-vector space* Ω *generated by the symbols* $\varepsilon(x)$*,* $x \in \mathbb{R}$*, with relations*

$$(A) : \varepsilon(1-x) = \varepsilon(x)$$

$$(B) : \varepsilon(x+y) = \varepsilon(y) + (1-y)\,\varepsilon\Big(\frac{x}{1-y}\Big) + y\,\varepsilon\Big(-\frac{x}{y}\Big)\,,\ \ \forall y \notin \{0,1\}$$

$$(C) : x\,\varepsilon(1/x) = -\varepsilon(x)\,,\ \ \forall x \neq 0.$$

Proof. The map $\varepsilon(x) \mapsto s(x) \in \mathrm{Ker}(\theta)/\mathrm{Ker}(\theta)^2$ is well defined and surjective by Lemma 2. We show that it is injective. Let M be an $\mathbb{R}$-linear form on Ω. Next we prove that there exists $\delta : W_{\mathbb{Q}} \to \mathbb{R}$ fulfilling (28), such that

$$\delta(s(x)) = M(\varepsilon(x)) \,, \ \forall x \in \mathbb{R}. \tag{32}$$

The injectivity then follows using $\mathbb{R}$-linearity to get $M(Z) = 0$ for any Z in the kernel. We now prove (32). Let $H(x) = M(\varepsilon(x))$, then, as explained in [16] and Remark 5.3 of [3], the function $\phi(x, y) = (x + y)H(\frac{x}{x+y})$, $\phi(x, -x) = 0$, is a two cocycle on the additive group of $\mathbb{R}$, with coefficients in $\mathbb{R}$. This symmetric cocycle defines an extension in the category of torsion free divisible abelian groups, i.e. of $\mathbb{Q}$-vector spaces, and hence is a coboundary, $\phi = b\psi$. With $\psi_x(y) := \psi(xy)$ one has $b\psi_x(y, z) = \phi(xy, xz) = x\phi(y, z)$. This shows that ψ fulfills (29) and that replacing ψ by $\frac{1}{2}(\psi - \psi_{-1})$ one can assume that ψ is odd. Then δ_ψ defined in (30) fulfills (32) since $\delta_\psi(s(x)) = b\psi(x, 1 - x) = H(x)$. □

Remark 2. All Lebesgue measurable group homomorphisms $\ell : \mathbb{R}_+^\times \to \mathbb{R}$ are of the form $x \mapsto \lambda \log x$, and yield the linear form on Ω given by the entropy function. In the next Sect. 5 we investigate the ring homomorphism $\mathscr{T}_\ell$ of (24) given by the measurable choice $\ell = \log$.

5 The $\mathbb{R}$-Algebras of Analytic Functions and Their Canonical Form

This section is concerned with the *topological* step inherent to the construction of the archimedean analogue of the rings which in the p-adic case are the analogues in mixed characteristics of the ring of rigid analytic functions on the punctured unit disk in equal characteristics (cf. Appendix 4). In Sect. 3 we have seen that the structure of the $\mathbb{Q}$-algebras $W_{\mathbb{Q}}(\mathscr{O}) \subset W_{\mathbb{Q}}(\mathbb{R}^\flat)$ is inclusive of a one parameter group of automorphisms $\mathbf{F}_\lambda = W(\theta_\lambda) \in \mathrm{Aut}(W_{\mathbb{Q}}(\mathbb{R}^\flat))$ (cf. (20)) preserving $W_{\mathbb{Q}}(\mathscr{O})$, and of the ring homomorphism $\theta : W_{\mathbb{Q}}(\mathbb{R}^\flat) \to \mathbb{R}$ (cf. Proposition 5). Thus the following map defines a ring homomorphism from the Witt ring $W_{\mathbb{Q}}(\mathscr{O})$ to the ring of real valued functions of one (positive) real variable endowed with the pointwise operations

$$W_{\mathbb{Q}}(\mathscr{O}) \to \mathscr{F}(\mathbb{R}_+^\times), \quad x \to x(z) = \theta(\mathbf{F}_z(x)) \,, \ \forall z > 0. \tag{33}$$

For $x \in W_{\mathbb{Q}}(\mathscr{O})$, one has $x = \sum_i a_i[x_i]$ with $x_i \in (0, 1]$ (we keep the notation $[x] = \tau(x)$ of Sect. 3). The function $x(z) = \sum_i a_i x_i^z$, $z > 0$, is bounded by the norm $\|x\|_0 = \sum_i |a_i|$. After performing the compactification of the balls $\|x\|_0 \leq R$ of this norm for the topology of simple convergence

$$x_n \to x \iff x_n(z) \to x(z) \,, \ \forall z > 0, \tag{34}$$

one obtains the Banach algebra $B_\infty^{b,+}$ which is the real archimedean counterpart of the p-adic ring $B^{b,+}$ (cf. Appendix 4).

The main result of this section is stated in Theorem 6 that describes the canonical expansion of the elements of $B_\infty^{b,+}$. The following Sect. 5.1 prepares the ground. In Sect. 5.3 we construct the Frechet $\mathbb{R}$-algebra obtained by completion for the analogue of the $\|.\|_\rho$ norms and relate it to the Mikusinski field (cf. Sect. 5.4).

5.1 The Algebra $B_\infty^{b,+}$

We denote by NBV (Normalized and of Bounded Variation) the class of real functions $\phi(\xi)$ of a real variable ξ which are of bounded variations and normalized i.e. point-wise left continuous and tending to 0 as $\xi \to -\infty$. In fact we shall only work with functions that vanish for $\xi \leq 0$, and say that a real valued function ϕ on $(0,\infty)$ is NBV when its extension by 0 for $\xi \leq 0$ is NBV. Thus, saying that a function ϕ of bounded variation on $(0,\infty)$ is normalized just means that it is left continuous at every point of $(0,\infty)$. We refer to [21], Chap. 8.

We observe that with the notation of (8), for $a, b \in \mathbb{R}$, one has

$$a \smile b = a \Leftrightarrow |a| \geq |b|, \quad \text{and} \quad a = b \text{ if } |a| = |b|. \tag{35}$$

Throughout this section we continue to use the notation $[\,] = \tau$ of Sect. 3.

Proposition 6. (*i*) *Let $\phi(\xi)$ be a real valued, left continuous function of $\xi \in (0,\infty)$ of bounded variation and let V be its total variation. Then, there exists a measurable function $u \mapsto x_u \in [-1,1] \setminus \{0\}$ of $u \in [0,V)$ such that $x_u \smile x_v = x_u$ for $u \leq v$ and*

$$\int_0^V [x_u](z)du = \int_0^\infty e^{-\xi z} d\phi(\xi)\,, \ \forall z \in \mathbb{R}_+^\times. \tag{36}$$

Moreover the function $u \mapsto x_u$ is unique almost everywhere (i.e. except on a set of Lebesgue measure zero).

(*ii*) *Conversely, given $V < \infty$ and a measurable function $u \mapsto x_u \in [-1,1] \setminus \{0\}$ of $u \in [0,V)$, such that $x_u \smile x_v = x_u$ for $u \leq v$, there exists a unique real valued left continuous function $\phi(\xi)$, $\xi \in (0,\infty)$ of total variation V such that (36) holds.*

Proof. (*i*) Let μ be the unique real Borel measure on $[0,\infty)$ such that: $\mu([0,\xi)) = \phi(\xi)$, $\forall \xi > 0$. Then the definition of the integral on the right hand side of (36) is

$$\int_0^\infty e^{-\xi z} d\phi(\xi) = \int_0^\infty e^{-\xi z} d\mu.$$

The total variation function $T_\phi(\xi)$ which is defined as (with $\phi(0) = 0$)

$$T_\phi(\xi) = \sup\left(\sum_{j=1}^{n} |\phi(\xi_j) - \phi(\xi_{j-1})|\right), \quad 0 = \xi_0 < \xi_1 < \ldots < \xi_n = \xi$$

is equal to $|\mu|([0, \xi))$ where $|\mu|$ is the positive Borel measure on $[0, \infty)$ which is the total variation of μ (cf. [21], Theorem 8.14). We set, for $u \in [0, V)$

$$S(u) = \inf\{\xi \in (0, \infty) \mid T_\phi(\xi) > u\} \in [0, \infty). \tag{37}$$

One has $S(u) \geq S(v)$, when $u \geq v$. Moreover the function S of u is right continuous and is finite since the total variation of ϕ is $V = V(\phi) = \lim_{\xi \to \infty} T_\phi(\xi)$. Let m be the Lebesgue measure on $(0, V(\phi))$. The direct image of m by S is equal to the measure $|\mu|$. Indeed, one has

$$T_\phi(\xi) > u \iff S(u) < \xi$$

which shows that the Lebesgue measure $S(m)([0, \xi))$ of the set $\{u \mid S(u) < \xi\}$ is equal to $T_\phi(\xi) = |\mu|([0, \xi))$, $\forall \xi$. Let $h(\xi)$ be the essentially unique measurable function with values in $\{\pm 1\}$ such that $\mu = h|\mu|$ (cf. [21], Theorem 6.14). We define the function $u \mapsto x_u$ by

$$x_u = h(S(u))e^{-S(u)}, \ \forall u \in [0, V). \tag{38}$$

One has $|x_u| \geq |x_v|$ for $u \leq v$, moreover $|x_u| = |x_v| \implies x_u = x_v$, since $|x_u| = |x_v|$ implies $S(u) = S(v)$. Moreover, since $S(m) = |\mu|$ one gets

$$\int_0^V f(S(u))dm = \int_0^\infty f(\xi)|d\mu|$$

and taking $f(\xi) = h(\xi)e^{-z\xi}$ one obtains (36). The proof of the uniqueness is postponed after the proof of (ii).

(ii) Let $\sigma(u) = \text{sign}(x_u)$, $S(u) = -\log(|x_u|)$. These functions are well defined on the interval $J = [0, V)$. One has $S(u) \geq S(v)$, when $u \geq v$. Let $T(\xi)$ be defined by

$$T(\xi) = \sup\{u \in J \mid S(u) < \xi\} \in [0, V]. \tag{39}$$

$T(\xi)$ is non-decreasing and left continuous by construction, and thus it belongs to the class NBV. By hypothesis $|x_u| = |x_v| \implies x_u = x_v$, so that the function $\sigma(u) = \text{sign}(x_u)$ only depends upon $S(u)$ and can be written as $h(S(u))$ where h is measurable and takes values in $\{\pm 1\}$. We extend h to a measurable function $h : [0, \infty) \to \{\pm 1\}$. Let $\mu = hdT$ be the real Borel measure such that

$$|\mu|([0,\xi)) = T(\xi)\,, \quad \mu = h|\mu|. \tag{40}$$

Then the function $\phi(\xi) = \mu([0,\xi))$ is real valued, NBV and such that (36) holds. Indeed, one has

$$T(\xi) > u \Longleftrightarrow S_+(u) < \xi, \quad S_+(u) = \lim_{\substack{\epsilon \to 0 \\ \epsilon > 0}} S(u+\epsilon)$$

so that the map S associated to the function ϕ in the proof of (i) is equal to S_+ and thus it agrees with S outside a countable set. Hence the function x_u associated to ϕ by (38) agrees with the original x_u almost everywhere and one gets (36).

Finally, we prove the uniqueness statement of (i). It is enough to show that the function $f(z)$ given by

$$f(z) = \int_0^\infty [x_u](z)du \tag{41}$$

uniquely determines x_u almost everywhere. It follows from the above discussion that it is enough to prove that $f(z)$ uniquely determines the function $\phi(\xi)$. By [21], Theorem 8.14, the function $\phi \in$ NBV is uniquely determined by the associated measure μ. The latter is uniquely determined by f since one has

$$f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi).$$

Hence f is the Laplace transform of μ and this property determines uniquely the finite measure μ. □

The following definition introduces the real archimedean counterpart of the ring $B^{b,+}$ of p-adic Hodge theory.

Definition 5. We denote by $B_\infty^{b,+}$ the space of real functions of the form $\int_0^V [x_u]du$ where $V < \infty$, and $u \mapsto x_u \in [-1,1]$ is a measurable function of $u \in [0,V]$, such that

$$x_u \smile x_v = x_u, \quad \text{for} \quad u \leq v.$$

Then Proposition 6 shows that the functions in $B_\infty^{b,+}$ are exactly the Laplace transforms of finite real Borel measures

$$f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi). \tag{42}$$

Moreover, when expressed in terms of μ one gets

$$\|f\|_0 := \sup\{u \in [0,V] \mid x_u \neq 0\} = |\mu|([0,\infty)) \tag{43}$$

This can be seen using (39) to get

$$\sup\{u \in [0, V] \mid x_u \neq 0\} = \sup\{u \in [0, V] \mid S(u) < \infty\} = \lim_{\xi \to \infty} T(\xi) = |\mu|([0, \infty)).$$

This shows that $B_\infty^{b,+}$ is the real Banach algebra of convolution of finite real Borel measures on $[0, \infty)$. Then we obtain the following result

Theorem 5. *The space $B_\infty^{b,+}$, endowed with the pointwise operations of functions and the map $f \mapsto \|f\|_0 = \sup\{u \in \mathbb{R}_{\geq 0} \mid x_u \neq 0\}$, is a real Banach algebra.*

5.2 Canonical Form of Elements of $B_\infty^{b,+}$

In the p-adic case (cf. Appendix 4), every element $x \in B^{b,+}$ can be written uniquely in the form

$$x = \sum_{n \gg -\infty} [x_n]\pi^n\,, \quad x_n \in \mathscr{O}_F. \tag{44}$$

In the archimedean case one gets an analogous decomposition by applying Proposition 6. In the next pages we shall explain this point with care since the decomposition of the elements in $B_\infty^{b,+}$ does *not* arise by applying (36) naively.

Theorem 6. *Let $f \in B_\infty^{b,+}$. Then there exists $s_0 > -\infty$ and a measurable function, unique except on a set of Lebesgue measure zero, $s \mapsto f_s \in [-1, 1] \setminus \{0\}$, for $s > s_0$ such that $f_s \smile f_t = f_s$ for $s \leq t$ and*

$$f = \int_{s_0}^{\infty} [f_s] e^{-s} ds. \tag{45}$$

Proof. By Proposition 6 there exists a measurable function $u \mapsto x_u \in [-1, 1] \setminus \{0\}$ of $u \in [0, V)$ such that $x_u \smile x_v = x_u$ for $u \leq v$ so that

$$f = \int_0^V [x_u] du. \tag{46}$$

Define f_s by the equality

$$f_s = x_{(V - e^{-s})}\,, \quad \forall s \geq s_0 = -\log V. \tag{47}$$

The function $V - e^{-s}$ is increasing and $d(V - e^{-s}) = e^{-s} ds$, so that (45) follows from (46) by applying a change of variables. □

The scalars $\mathbb{R}$, i.e. the constant functions in $B_\infty^{b,+}$, are characterized by the condition

$$\int_{s_0}^{\infty} [f_s] e^{-s} ds \in \mathbb{R} \Longleftrightarrow f_s \in \text{sign}\,, \ \forall s \tag{48}$$

where $\text{sign} = \{-1, 0, 1\}$ is the hyperfield of signs (cf. [4]). This corresponds, in the p-adic case, to the characterization of the elements of the local field $K \subset B^{b,+}$ by the condition

$$\sum_{n \gg -\infty} [a_n] \pi^n \in K \Longleftrightarrow a_n \in k\,, \ \forall n$$

where k is the residue field of K (cf. [9], Sect. 2.1 and also Appendix 4).

In the p-adic case, the projection $\mathcal{O}_F \to k_F$ (cf. Appendix 4) induces an augmentation map ε obtained by applying the above projection to each a_n inside the expansion $f = \sum_{n \gg -\infty} [a_n] \pi^n$ (cf. (166) in Appendix 4). In the real archimedean case, the corresponding projection is the map

$$\mathbb{R}^\flat \supset [-1, 1] = \mathcal{O} \to \text{sign}, \quad x \mapsto \tilde{x} = \begin{cases} 0 \text{ if } x \in (-1, 1) \\ \pm 1 \text{ if } x = \pm 1 \end{cases}$$

When this projection is applied inside the expansion $f = \int_{s_0}^{\infty} [f_s] e^{-s} ds$ of elements in $B_\infty^{b,+}$, it yields the following

Proposition 7. *For $f \in B_\infty^{b,+}$, let $f = \int_{s_0}^{\infty} [f_s] e^{-s} ds$ be its canonical form. Then*

$$\epsilon(f) := \int_{s_0}^{\infty} [\tilde{f}_s] e^{-s} ds = \lim_{z \to +\infty} f(z) \tag{49}$$

defines a character $\epsilon : B_\infty^{b,+} \to \mathbb{R}$ of the Banach algebra $B_\infty^{b,+}$.

Proof. When $z \to \infty$, one has for any $s \geq s_0$, $[f_s](z) \to [\tilde{f}_s](z)$. Thus it follows from the Lebesgue dominated convergence theorem that (cf. (41))

$$\lim_{z \to +\infty} f(z) = \int_{s_0}^{\infty} [\tilde{f}_s] e^{-s} ds. \tag{50}$$

Since the operations in the Banach algebra $B_\infty^{b,+}$ are pointwise when the elements are viewed as functions of z, the functional ϵ is a character. □

Next, we exploit a theorem of Titchmarsh to show that the leading term of the canonical form (45) behaves multiplicatively likewise its p-adic counterpart. In particular, it will also follow that the ring $B_\infty^{b,+}$ is integral (i.e. it has no zero divisors).

Theorem 7. *The following formula defines a multiplicative map from the subset of non zero elements of* $B_\infty^{b,+}$ *to* $(0, 1]$

$$|\rho|(f) = \lim_{\epsilon \to 0+} |f_{s_0+\epsilon}|\,,\ \forall f = \int_{s_0}^{\infty} [f_s] e^{-s} ds \in B_\infty^{b,+} \setminus \{0\}. \tag{51}$$

Proof. Using (47), we can write the map $|\rho|$, with the notations of Proposition 6 as

$$|\rho|(x) = \lim_{\epsilon \to 0+} |x_\epsilon|\,,\ \forall x = \int_0^V [x_u] du.$$

By (37) one has

$$\lim_{\epsilon \to 0+} |x_\epsilon| = e^{-S(0)},\ \ S(0) = \inf\{\xi \mid T_\phi(\xi) > 0\} \in [0, \infty).$$

In terms of the measure $\mu = d\phi$, $S(0)$ is the lower bound of the support of μ. By Titchmarsh's Theorem [24] (formulated in terms of distributions [19]) one has the additivity of these lower bounds for the convolution of two measures on $[0, \infty)$

$$\inf \text{Support}(\mu_1 \star \mu_2) = \inf \text{Support}(\mu_1) + \inf \text{Support}(\mu_2)$$

and hence the required multiplicativity. □

Remark 3. One important nuance between the p-adic case and the archimedean case is in the behavior of s_0 under the algebraic operations. As in the p-adic case the quantity $V = e^{-s_0}$ defines a norm, $\|.\|_0$, but this norm is no longer ultrametric and is *sub-multiplicative* (cf. Lemma 4) while its p-adic counterpart (cf. Lemma 3(ii)) is multiplicative. It remains multiplicative for positive measures.

5.3 The Real Archimedean Norms $\|.\|_\rho$

We recall that in p-adic Hodge theory one defines, for each $\rho \in (0, 1)$, a multiplicative norm on the ring

$$B^{b,+} = W_{\mathcal{O}_K}(\mathcal{O}_F)[\frac{1}{\pi}] = \{f = \sum_{n \gg -\infty} [a_n]\pi^n \in \mathfrak{E}_{F,K} | a_n \in \mathcal{O}_F, \forall n\} \tag{52}$$

(cf. Appendix 4 for notations) by letting

$$|f|_\rho = \max_{\mathbb{Z}} |a_n| \rho^n. \tag{53}$$

To define the real archimedean counterpart of the norm $|.|_\rho$, one needs first to rewrite (53) in a slightly different manner without changing the uniform structure that it describes. Let q be the cardinality of the field of constants k so that $|\pi| = q^{-1}$. Rather than varying $\rho \in (0,1)$ we introduce a real positive parameter $\alpha > 0$ and make it varying so that $\rho^\alpha = q^{-1}$.

Lemma 3. (*i*) *For* $\rho \in (0,1)$, *we set* $\alpha = \frac{\log q}{-\log \rho}$, $\quad (\rho = q^{-1/\alpha})$. *Then, for* $f = \sum_{n \gg -\infty} [a_n]\pi^n \in B^{b,+}$ *the equality*

$$|f|_\rho^\alpha = \max_{\mathbb{Z}} |a_n|^\alpha q^{-n} \tag{54}$$

defines a multiplicative norm on $B^{b,+}$ *that describes the same uniform structure as the norm* $|.|_\rho$ *and whose restriction to* $\mathbb{Q}_p$ *is independent of* ρ.

(*ii*) *The limit, as* $\rho \to 0$, *of* $|f|_\rho^\alpha$ *is the norm* $|f|_0 = q^{-r}$, *where* r *is the smallest integer such that* $a_r \neq 0$ *(cf. [9], Sect. 3.1).*

Proof. (*i*) One has $\rho^\alpha = q^{-1}$, thus the second equality of (54) holds. Since $|\cdot|_\rho$ is a multiplicative norm the same statement holds for $|\cdot|_\rho^\alpha$. When restricted to $\mathbb{Q}_p$ the expression (54) is independent of α since one has $|a_n| \in \{0,1\} \forall n$.

(*ii*) As $\rho \to 0$, also $\alpha \to 0$ and $|f|_\rho^\alpha \overset{[}{\alpha} \to 0] \longrightarrow \max_{\substack{n \in \mathbb{Z} \\ a_n \neq 0}} q^{-n} = |f|_0$. □

In the real archimedean case, the operation of taking the "max" in (54) is replaced by an integration process. By re-scaling, we can replace $\log q$ by 1; then the archimedean analogue of (54) is given, for each $\rho \in (0,1)$ and for $\alpha = -\frac{1}{\log \rho}$ by the formula

$$\|f\|_\rho := \int_{s_0}^\infty |f_s|^\alpha e^{-s} ds\,, \ \forall f = \int_{s_0}^\infty [f_s] e^{-s} ds \in B_\infty^{b,+}. \tag{55}$$

Lemma 4. *Let* $\rho \in [0,1)$. *Equation* (55) *defines a sub-multiplicative norm on* $B_\infty^{b,+}$. *For* $\rho > 0$ *one has, with* $\alpha = -\frac{1}{\log \rho}$

$$\|f\|_\rho = \int_0^\infty e^{-\xi\alpha} |d\mu(\xi)|\,, \ \forall f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi). \tag{56}$$

For $\rho = 0$ *this norm coincides with the norm* $\|f\|_0$ *of Theorem 5.*

Proof. Using (47), we can write the functional $\|f\|_\rho$ with the notations of Proposition 6

$$\|x\|_\rho = \int_0^V |x_u|^\alpha du\,, \ \forall x = \int_0^V [x_u] du. \tag{57}$$

Using the notations of the proof of Proposition 6, one has

$$\int_0^V |x_u|^\alpha du = \int_0^V e^{-\alpha S(u)} du = \int_0^\infty e^{-\xi\alpha} |d\mu(\xi)|$$

since the image of the Lebesgue measure m on $[0, V)$ by the map S is the measure $|d\mu(\xi)|$. Thus we obtain (56). The sum of the functions associated with the measures $d\mu_j$ $(j = 1, 2)$ corresponds to the measure $d\mu_1 + d\mu_2$. Thus one derives the triangle inequality $\|f_1 + f_2\|_\rho \leq \|f_1\|_\rho + \|f_2\|_\rho$. The product of the functions corresponds to the convolution $d\mu = d\mu_1 \star d\mu_2$ of the measures

$$\int_0^\infty h(\xi) d\mu(\xi) = \int_0^\infty \int_0^\infty h(\xi_1 + \xi_2) d\mu_1(\xi_1) d\mu_2(\xi_2) \tag{58}$$

which is the projection of the product measure $d\mu_1 \otimes d\mu_2$ by the map $(\xi_1, \xi_2) \mapsto s((\xi_1, \xi_2)) = \xi_1 + \xi_2$. The module of the product measure $d\mu_1 \otimes d\mu_2$ is $|d\mu_1| \otimes |d\mu_2|$. Moreover, for $h \geq 0$ a real positive function one has

$$\int_0^\infty h|dv| = \sup\{ \left| \int_0^\infty h\psi dv \right| : |\psi| \leq 1\}.$$

It follows that the module of the projection of a measure is less than or equal to the projection of its module. Thus we derive

$$\|f_1 f_2\|_\rho = \int_0^\infty e^{\xi/\log\rho} |d\mu(\xi)| \leq \int_0^\infty e^{(\xi_1+\xi_2)/\log\rho} |d\mu_1(\xi_1)| |d\mu_2(\xi_2)| = \|f_1\|_\rho \|f_2\|_\rho$$

which proves that $\|.\|_\rho$ is sub-multiplicative. The limit case $\rho = 0$ arises by taking the limit $\alpha \to 0$ in (55), hence we obtain

$$\|f\|_0 = \int_0^V du, \quad V = \sup\{u \mid x_u \neq 0\}. \tag{59}$$

Thus $\|f\|_0$ agrees with the norm of Theorem 5. □

The norms $\|.\|_\rho$ behave coherently with the action of the automorphisms $\mathbf{F}_\lambda$, more precisely one has the equality

$$\|\mathbf{F}_\lambda(f)\|_\rho = \|f\|_{\rho^{1/\lambda}}. \tag{60}$$

Indeed, for $f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi)$ one has

$$\mathbf{F}_\lambda(f)(z) = \int_0^\infty e^{-\lambda\xi z} d\mu(\xi) = \int_0^\infty e^{-\xi z} d\mu(\xi/\lambda) \tag{61}$$

which gives (60). By construction the archimedean norms $\|.\|_\rho$ fulfill the inequality

$$\|f\|_\rho \leq \|f\|_{\rho'}\,,\ \forall \rho \geq \rho'. \tag{62}$$

In particular for $I \subset (0,1)$ a closed interval, one has, with $\rho_0 = \min I$ the smallest element of I

$$\|f\|_I = \sup_{\rho \in I} \|f\|_\rho = \|f\|_{\rho_0}. \tag{63}$$

Definition 6. We define B^+_∞ to be the Frechet algebra projective limit of the Banach algebras completion of $B^{b,+}_\infty$ for the norms $\|\cdot\|_\rho$, for $\rho \in (0,1)$.

It is straightforward to check, using (56), that B^+_∞ is the convolution algebra of measures μ on $[0,\infty)$ such that

$$\int_0^\infty e^{-\alpha\xi}|d\mu(\xi)| < \infty\,,\ \forall \alpha > 0. \tag{64}$$

Proposition 8. (*i*) *The measures which are absolutely continuous with respect to the Lebesgue measure form an ideal $J \subset B^+_\infty$.*

(*ii*) *Let $B^+_{\infty,0} \subset B^+_\infty$ be the sub-ring obtained by adjoining the unit:*

$$B^+_{\infty,0} = J + \mathbb{R} \subset B^+_\infty.$$

Then for $f \in B^+_\infty$, one has $f \in B^+_{\infty,0}$ if and only if the map $\lambda \mapsto \mathbf{F}_\lambda(f) \in B^+_\infty$ is continuous for the Frechet topology of B^+_∞.

Proof. (*i*) Follows from the well known properties of convolution of measures.

(*ii*) For $f \in B^+_{\infty,0}$ the associated measure μ is of the form $a\delta_0 + hd\xi$ where h is locally integrable and fulfills

$$\int_0^\infty e^{-\alpha\xi}|h(\xi)|d\xi < \infty\,,\ \forall \alpha > 0. \tag{65}$$

The measure associated to $\mathbf{F}_\lambda(f)$ is $a\delta_0 + h_\lambda d\xi$ where $h_\lambda(\xi) = \frac{1}{\lambda}h(\xi/\lambda)$ by (61) and one has

$$\|\mathbf{F}_\lambda(f) - \mathbf{F}_{\lambda'}(f)\|_\rho = \int_0^\infty e^{-\alpha\xi}|h_\lambda(\xi) - h_{\lambda'}(\xi)|d\xi$$

It follows that the map $\lambda \mapsto \mathbf{F}_\lambda(f) \in B^+_\infty$ is continuous for the Frechet topology of B^+_∞. The converse is proven using $\int h_n(\lambda)\mathbf{F}_\lambda(f)d\lambda \to f$ for suitable functions h_n.

□

5.4 Embedding in the Mikusinski Field $\mathfrak{M}$

In operational calculus one introduces the Mikusinski ring $\mathscr{M}(\mathbb{R}_+)$ whose elements are functions on $\mathbb{R}_+$ with locally integrable derivative, and where the product law is the Duhamel product (cf. [14]):

$$F \star G(t) = \frac{d}{dt} \int_0^t F(u)G(t-u)du. \tag{66}$$

This ring plays a main role in analysis, in view of some of its interesting properties among which we recall that $\mathscr{M}(\mathbb{R}_+)$ is an *integral ring* by the Titchmarsh's Theorem (cf. [14]) and hence it has an associated *field of fractions* $\mathfrak{M}$ called the Mikusinski field.

The following proposition states the existence of a direct relation between the Frechet algebra B_∞^+ (cf. Definition 6) and the Mikusinski field $\mathfrak{M}$. For $f \in B_{\infty,0}^+$, $f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi)$, we let

$$\mathfrak{m}(f)(\xi) = \mu([0,\xi])\,,\ \forall \xi \geq 0. \tag{67}$$

We follow the notation of *op.cit.* and denote by I the function $I(\xi) = \xi$ viewed as an element of $\mathscr{M}(\mathbb{R}_+)$.

Proposition 9. (*i*) *The map* $B_{\infty,0}^{b,+} \ni f \mapsto \mathfrak{m}(f)$ *defines an isomorphism of* $B_{\infty,0}^+$ *with a sub-ring of* $\mathscr{M}(\mathbb{R}_+)$.

(*ii*) *There exists a unique function* $\iota \in B_{\infty,0}^+$ *such that* $\mathfrak{m}(\iota) = I$, *and one has* $\iota(z) = \frac{1}{z}$, $\forall z > 0$.

(*iii*) *The isomorphism* $\mathfrak{m}$, *as in* (*i*), *extends uniquely to an injective homomorphism of the Frechet algebra* B_∞^+ *into the field* $\mathfrak{M}$.

Proof. (*i*) It is easy to check that the product (66) gives the primitive of the convolution product of the derivatives of F and G. For $f \in B_{\infty,0}^{b,+}$ the associated measure μ is of the form $F(0)\delta_0 + dF$ where $dF = F'd\xi$ and F' is locally integrable. Thus the convolution of the measures μ corresponds to the Duhamel product (66), in terms of $\mathfrak{m}(f)$. Hence, the map $f \mapsto \mathfrak{m}(f)$ is an algebra homomorphism and it is injective by construction.

(*ii*) The Lebesgue measure $d\xi$ fulfills (64), and one has

$$\int_0^\infty e^{-z\xi} d\xi = \frac{1}{z}\,,\ \forall z > 0 \tag{68}$$

thus $d\xi$ defines an element $\iota \in B_{\infty,0}^+$ such that $\mathfrak{m}(\iota) = I$.

(*iii*) We first prove the following implication

$$f \in B_\infty^+ \implies \iota \cdot f \in B_{\infty,0}^+. \tag{69}$$

Let $f \in B_\infty^+, f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi)$ with $\int_0^\infty e^{-\alpha\xi}|d\mu|(\xi) < \infty \ \forall \alpha > 0$. Let $\psi(u) = \int_0^u d\mu(\xi)$. Then one has

$$\int_0^\infty e^{-uz}\psi(u)du = \int_0^\infty \left(\int_\xi^\infty e^{-uz}du\right) d\mu(\xi) = \frac{1}{z}\int_0^\infty e^{-\xi z} d\mu(\xi)$$

where the interchange of integration is justified by Fubini's theorem. It follows that

$$(\iota \cdot f)(z) = \int_0^\infty e^{-uz}\psi(u)du$$

and, since $\psi(u)$ is locally integrable, $\iota \cdot f \in B_{\infty,0}^+$. Next one defines

$$\mathfrak{m}(f) = \frac{\mathfrak{m}(\iota \cdot f)}{I} \in \mathfrak{M}\,, \ \forall f \in B_\infty^+. \tag{70}$$

Since $\mathfrak{m}(\iota) = I$ this is the unique extension of $\mathfrak{m}$ as a homomorphism from B_∞^+ to $\mathfrak{M}$. It is well defined and yields the required injective homomorphism.

□

6 Ideals and Spectra of the Algebras B_∞^+ and $B_{\infty,0}^+$

We denote by $B_\mathbb{C}^+ = B_\infty^+ \otimes_\mathbb{R} \mathbb{C}$ and $B_{\mathbb{C},0}^+ = B_{\infty,0}^+ \otimes_\mathbb{R} \mathbb{C}$ the complexified algebras of the rings B_∞^+ and $B_{\infty,0}^+$ (cf. Sect. 5). In this section we investigate their ideals and Gelfand spectrum.

6.1 The Principal Ideals Ker θ_z

In this section we show that for $z_0 \in \mathbb{C}$, with $\Re(z_0) > 0$ the kernel of the evaluation map $f \mapsto f(z_0)$ defines a *principal* ideal of the algebras $B_\mathbb{C}^+$ and $B_{\mathbb{C},0}^+$.

We begin by stating the following lemma which allows one to divide f by the polynomial $z - z_0$, when $f(z_0) = 0$.

Lemma 5. *Any $f \in B_\mathbb{C}^+$ extends uniquely to an holomorphic function $z \mapsto f(z)$ of z, $\Re(z) > 0$.*

Let $z_0 \in \mathbb{C}$ with $\Re(z_0) > 0$. There exists a function $\mathfrak{k} \in B_{\mathbb{C},0}^+$ such that

$$f - \theta_{z_0}(f) = (z_0 - z)\mathfrak{k}. \tag{71}$$

Proof. Since $f \in B^+_{\mathbb{C}}$, there exists a complex Radon measure μ on $\mathbb{R}_+$ such that

$$f(u) = \int_0^\infty e^{-\xi u} d\mu(\xi)\,,\ \forall u > 0, \qquad \int_0^\infty e^{-\alpha\xi} |d\mu(\xi)| < \infty\,,\ \forall \alpha > 0. \tag{72}$$

The integral

$$\theta_{z_0}(f) = \int_0^\infty e^{-\xi z_0} d\mu(\xi) \tag{73}$$

is finite and bounded in absolute value by the norm $\|f\|_\rho$, for $\rho = e^{-1/\Re(z_0)}$. Let $z \neq z_0$, then one has

$$\frac{e^{-z\xi} - e^{-z_0\xi}}{z_0 - z} = \int_0^\xi e^{-(z-z_0)u - z_0\xi} du \tag{74}$$

and when $z \to z_0$ both sides of the above equality converge to the function $\xi e^{-z_0\xi}$. The equality

$$\psi(u) = \int_u^\infty e^{z_0(u-\xi)}\, d\mu(\xi)\,,\ \forall u \in \mathbb{R}_+ \tag{75}$$

defines a complex valued function whose size is controlled by

$$|\psi(u)| \leq \int_u^\infty e^{\Re(z_0)(u-\xi)}\, |d\mu(\xi)|. \tag{76}$$

Next, we show that $\int_0^\infty e^{-\alpha u} |\psi(u)| du < \infty$, for $\alpha > 0$. When $\alpha > 0$ and $\alpha < \Re(z_0)$, by implementing (74) (for $z = \alpha$ and with $\Re(z_0)$ instead of z_0) and Fubini's theorem to interchange the integrals, one has

$$\begin{aligned}\int_0^\infty e^{-\alpha u} |\psi(u)| du &\leq \int_0^\infty \int_u^\infty e^{-\alpha u} e^{\Re(z_0)(u-\xi)} |d\mu(\xi)| du \\ &= (\Re(z_0) - \alpha)^{-1} \int_0^\infty \left(e^{-\alpha\xi} - e^{-\Re(z_0)\xi}\right) |d\mu(\xi)|.\end{aligned}$$

This proves that the formula

$$\mathfrak{t}(z) = \int_0^\infty e^{-uz} \psi(u) du \tag{77}$$

defines an element $\mathfrak{t} \in B^+_{\mathbb{C},0}$ whose norm satisfies, for $\rho_0 = e^{-1/\Re(z_0)}$

$$\begin{aligned}\|\mathfrak{t}\|_\rho &\leq \int_0^\infty \int_u^\infty e^{u/\log(\rho)} e^{\Re(z_0)(u-\xi)} |d\mu(\xi)| du \\ &= (\|f\|_\rho - \|f\|_{\rho_0})/(1/\log(\rho) - 1/\log(\rho_0)).\end{aligned}$$

Moreover, using again (74) with $z \neq z_0$, one obtains

$$\frac{f(z)-f(z_0)}{z_0-z} = \int_0^\infty \frac{e^{-z\xi}-e^{-z_0\xi}}{z_0-z} d\mu(\xi) = \int_0^\infty \int_0^\xi e^{-(z-z_0)u-z_0\xi} du\, d\mu(\xi)$$

which gives

$$\mathfrak{t}(z) = \frac{f(z)-f(z_0)}{z_0-z} \tag{78}$$

and the equality (71) follows. □

Proposition 10. (*i*) *Let $z_0 \in \mathbb{C}$ with $\Re(z_0) > 0$. Then*

$$\theta_{z_0} : B_{\mathbb{C}}^+ \to \mathbb{C}, \quad \theta_{z_0}(f) = f(z_0)$$

defines a complex character of the algebra $B_{\mathbb{C}}^+$. One has $\theta_1 = \theta$.

(*ii*) *The ideal $Ker(\theta_{z_0}) \subset B_{\mathbb{C}}^+$ is generated by the function $\iota - z_0^{-1}$, with*

$$\iota(z) = \int_0^\infty e^{-\xi z} d\xi = z^{-1}\,, \ \forall z > 0. \tag{79}$$

(*iii*) *$\iota - z_0^{-1} \in B_{\mathbb{C},0}^+$ and $\iota - z_0^{-1}$ generates the ideal $Ker(\theta_{z_0}) \cap B_{\mathbb{C},0}^+ \subset B_{\mathbb{C},0}^+$.*

Proof. (*i*) follows from the first statement of Lemma 5.

(*ii*) Since one knows that

$$\int_0^\infty e^{-\xi z} d\xi = \frac{1}{z}, \qquad \int_0^\infty e^{\xi/\log(\rho)} d\xi < \infty\,, \ \forall \rho \in (0,1)$$

one derives that $\iota \in B_{\mathbb{C},0}^+$. Let $f \in B_{\mathbb{C}}^+$, then by applying Lemma 5, one sees that there exists a function $\mathfrak{t} \in B_{\mathbb{C},0}^+$ such that (71) holds. One then obtains

$$f(z) = f(z_0) + (\frac{1}{z} - \frac{1}{z_0})h(z)\,, \ \ h = -z_0(f - f(z_0)) + z_0^2\mathfrak{t} \tag{80}$$

since

$$\frac{1}{z^{-1}-z_0^{-1}} = -z_0 + \frac{1}{z_0 - z} z_0^2.$$

(*iii*) By assuming that $f \in \mathrm{Ker}(\theta_{z_0})$ we obtain the factorization $f = (\iota - z_0^{-1})h$. (*iii*) then follows since $\iota \in B_{\mathbb{C},0}^+$.

□

Lemma 6. *Let $\alpha : B^+_{\mathbb{C}} \to \mathbb{C}$ be a ring homomorphism. Then, if $T_0 = \alpha(\iota) \neq 0$ one has $\Re(T_0) > 0$ and*

$$\alpha = \theta_{z_0}, \quad z_0 = 1/T_0. \tag{81}$$

Similarly, the maps $\theta_{z_0} : B^+_{\mathbb{C},0} \to \mathbb{C}$, with $\Re(z_0) > 0$, define all the characters α of $B^+_{\mathbb{C},0}$ with $\alpha(\iota) \neq 0$.

Proof. For any $\lambda \in \mathbb{C}$ with $\Re(\lambda) \geq 0$, $\lambda \neq 0$, one has

$$\frac{T}{\lambda T + 1} = \int_0^\infty e^{-\xi/T} e^{-\lambda\xi} d\xi.$$

Thus there exists a function $h_\lambda \in B^+_{\mathbb{C},0}$ such that $(\lambda\iota + 1)h_\lambda = \iota$. Then one obtains

$$\alpha(\lambda\iota + 1)\alpha(h_\lambda) = \alpha(\iota) \neq 0$$

and $\lambda\alpha(\iota) + 1 \neq 0$ which shows that $\Re(\alpha(\iota)) > 0$. It follows from Lemma 5 that the map θ_{z_0}, $z_0 = 1/T_0$ defines a character of $B^+_{\mathbb{C}}$. Moreover for any $f \in B^+_{\mathbb{C}}$ there exists $h \in B^+_{\mathbb{C}}$ such that (80) holds i.e.

$$f = f(z_0) + (\iota - T_0)h.$$

One then obtains $\alpha(f) = f(z_0)$ since $\alpha(\iota - T_0) = 0$. □

6.2 Gelfand Spectrum of $B^+_{\mathbb{C},0}$

We are now ready to compute the Gelfand spectrum of the Frechet algebra $B^+_{\mathbb{C},0}$.

Theorem 8. *The Gelfand spectrum* $\mathrm{Spec}\,(B^+_{\mathbb{C},0})$ *is the one point compactification $Y = \mathbb{C}^+ \cup \{\infty\}$ of the open half-plane $\mathbb{C}^+ = \{z \in \mathbb{C} \mid \Re(z) > 0\}$.*

The one parameter group $\mathbf{F}_\lambda$ acts on $\mathbb{C}^+$ by scaling $z \to \lambda z$ and it fixes $\infty \in Y$.

Proof. Let $\alpha \in \mathrm{Spec}\, B^+_{\mathbb{C},0}$ be a continuous homomorphism $\alpha : B^+_{\mathbb{C},0} \to \mathbb{C}$. Let us first assume that $T_0 = \alpha(\iota) \neq 0$. Then by Lemma 6 one has $\alpha = \theta_{z_0}$, $z_0 = 1/T_0$.

Assume now that $\alpha(\iota) = 0$. Then, for any smooth function $k(\xi)$ with compact support one has

$$\int_0^\infty e^{-\xi z} k'(\xi) d\xi = k(0) + z \int_0^\infty e^{-\xi z} k(\xi) d\xi$$

This shows that if $k(0) = 0$ the associated element of $B^+_{\mathbb{C},0}$ belongs to the ideal generated by ι. Thus this ideal is dense (for the norm $\|f\|_\rho$, cf. Sect. 5.3) in the kernel of the character

$$\theta_\infty : B^+_{\mathbb{C},0} \to \mathbb{C}, \quad \theta_\infty(f) = \lim_{z\to\infty} f(z). \tag{82}$$

Thus by continuity we get $\alpha = \theta_\infty$, if $\alpha(\iota) = 0$. This shows that Spec $(B^+_{\mathbb{C},0})$ is the space of characters $\theta_z : B^+_{\mathbb{C},0} \to \mathbb{C}$, for $z \in Y = \mathbb{C}^+ \cup \{\infty\}$. The action of $\mathbf{F}_\lambda$ is such that

$$\theta_z(\mathbf{F}_\lambda(f)) = \theta_{\lambda z}(f)\,,\ \forall f \in B^+_{\mathbb{C},0},\ \lambda \in \mathbb{R}^\times_+,\ z \in Y. \tag{83}$$

□

Corollary 1. *The map $Y \ni z \mapsto \mathrm{Ker}(\theta_z) \subset B^+_{\mathbb{C},0}$ defines a bijection of Y with the space of maximal closed ideals of the Frechet algebra $B^+_{\mathbb{C},0}$.*

Proof. This follows from the generalized Gelfand-Mazur theorem which shows that for any closed maximal ideal $J \subset B^+_{\mathbb{C},0}$ there exists a continuous character $B^+_{\mathbb{C},0} \to \mathbb{C}$ whose kernel is J. □

7 The Complex Case and Oscillatory Integrals

In the real case it was simple to evaluate the asymptotic behavior of integrals of real exponentials as in Proposition 7. On the other hand, in the complex case we shall see that oscillatory integrals with several critical points provide typical examples of application of the (multi-valued) law of addition in hyperfields. Rather than developing the general case we focus on a well-known example of asymptotic behavior of integrals of imaginary exponentials, namely the case of the Airy function (see [2, 7, 23]). This function is defined by the formula (Fig. 3)

$$\mathrm{Ai}(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{i\left(\frac{s^3}{3}+xs\right)} ds. \tag{84}$$

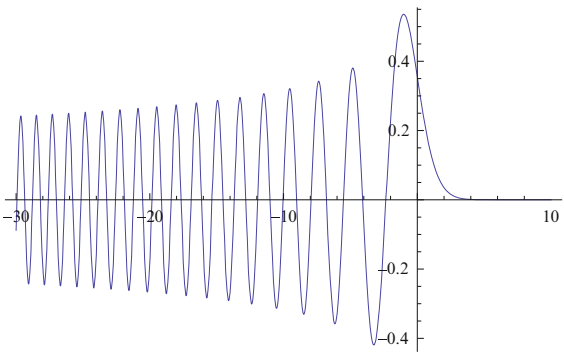


Fig. 3 Graph of the Airy function

The integral makes sense in the complex domain along a path slightly above the real axis, i.e. of the form $C = [-\infty + i\epsilon, \infty + i\epsilon]$ with $\epsilon > 0$. This function fulfills the differential equation

$$y'' - zy = 0 \tag{85}$$

and it is entire and given by the series

$$\begin{aligned} \mathrm{Ai}(z) &= 3^{-2/3} \sum_{n=0}^{\infty} \frac{z^{3n}}{9^n n! \Gamma(n + 2/3)} - 3^{-4/3} \sum_{n=0}^{\infty} \frac{z^{3n+1}}{9^n n! \Gamma(n + 4/3)} \\ &= \frac{1}{3^{2/3}\Gamma(\frac{2}{3})} - \frac{z}{3^{1/3}\Gamma(\frac{1}{3})} + \frac{z^3}{6 \times 3^{2/3}\Gamma(\frac{2}{3})} - \frac{z^4}{12\left(3^{1/3}\Gamma(\frac{1}{3})\right)} + \dots \end{aligned} \tag{86}$$

We first consider the asymptotic expansion of $\mathrm{Ai}(x)$ at infinity, on the positive real axis:

$$\mathrm{Ai}(z) \sim \frac{1}{4\pi^{3/2}} z^{-\frac{1}{4}} e^{-\frac{2}{3}z^{3/2}} \sum \frac{\Gamma(n + \frac{5}{6})\Gamma(n + \frac{1}{6})}{n!} (-3/4)^n z^{-\frac{3n}{2}} . \tag{87}$$

The series on the right hand side is not convergent and the **strong** meaning of the expansion is that the *ratio* of the left hand side by the truncated right hand side is "under control" i.e. it is of the form $1 + O(z^{-m})$, with m depending on the truncation. For instance, the ratio of $\mathrm{Ai}(\frac{1}{T})$ and the approximation

$$\begin{aligned} h_5(T) = e^{-\frac{2}{3}(\frac{1}{T})^{3/2}} \Big(&\frac{T^{1/4}}{2\sqrt{\pi}} - \frac{5T^{7/4}}{96\sqrt{\pi}} + \frac{385T^{13/4}}{9216\sqrt{\pi}} \\ &- \frac{85085T^{19/4}}{1327104\sqrt{\pi}} + \frac{37182145T^{25/4}}{254803968\sqrt{\pi}} \Big) \end{aligned}$$

is of the form $1 + O(T^{15/2})$ since the next term in the expansion is

$$-\frac{5391411025\, T^{31/4}}{12230590464\sqrt{\pi}} \sim -0.248702\, T^{31/4}$$

while the first term is $\frac{T^{1/4}}{2\sqrt{\pi}}$. The parameter T in this approximation is real and positive and one lets $T \to 0+$. For each $\alpha > 0$ we have a natural subgroup G_α of the multiplicative group of non-zero functions defined by the condition

$$G_\alpha = \{h \mid h(T) = 1 + O(T^\alpha) \text{ for } T \to 0+\}. \tag{88}$$

With this notation we can rewrite the above equivalence of the functions $\mathrm{Ai}(\frac{1}{T})$ and $h_5(T)$ as

$$\mathrm{Ai}\left(\frac{1}{T}\right)/h_5(T) \in G_\alpha\,,\ \alpha = \frac{15}{2}.$$

It is then natural to ask what kind of algebraic object one obtains if one considers the quotient of a field K of functions by the above equivalence relation (for fixed value of α). By construction G_α is a subgroup of the multiplicative group $K^\times$ and thus the quotient K/G_α is a *hyperfield*. This implies in particular that having strong expansions for two functions does not uniquely determine a strong asymptotic expansion for their sum. We illustrate this conclusion by considering the expansion of the Airy function on the negative real axis. There, the function admits zeros and the expansion is more involved and usually written in the form

$$\mathrm{Ai}(x) \sim \frac{1}{2\pi^{3/2}}(-x)^{-1/4}\Bigg(\cos\left(\frac{\pi}{4}+\frac{2x\sqrt{-x}}{3}\right)\sum_{n\,\mathrm{even}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n x^{-\frac{3n}{2}}$$
$$-\sin\left(\frac{\pi}{4}+\frac{2x\sqrt{-x}}{3}\right)\sum_{n\,\mathrm{odd}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n(-1)^{(n-1)/2}(-x)^{-\frac{3n}{2}}\Bigg). \tag{89}$$

In this case we cannot expect that the ratio of the left hand side with a truncation of the right hand side belongs to G_α for some $\alpha > 0$ (after changing variables to $x = -\frac{1}{T}$) since the equivalence relation preserves the zeros except for finitely many (since for $\alpha > 0$ and $h \in G_\alpha$ one has $h(T) = 0$ for only finitely many $T > 0$ in a neighborhood of $T = 0$). In fact, what the above asymptotic expansion suggests is that one can decompose the function $\mathrm{Ai}(-\frac{1}{T})$ as a sum of two functions which are equivalent, in the above strong sense, respectively to (with $x = -\frac{1}{T}$)

$$\frac{1}{2\pi^{3/2}}(-x)^{-1/4}\cos\left(\frac{\pi}{4}+\frac{2x\sqrt{-x}}{3}\right)\sum_{n\,\mathrm{even}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n x^{-\frac{3n}{2}}$$

and

$$-\frac{1}{2\pi^{3/2}}(-x)^{-1/4}\sin\left(\frac{\pi}{4}+\frac{2x\sqrt{-x}}{3}\right)$$
$$\sum_{n\,\mathrm{odd}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n(-1)^{(n-1)/2}(-x)^{-\frac{3n}{2}}.$$

To obtain the required decomposition of the function $\mathrm{Ai}(x)$ one uses its definition as an oscillatory integral (84), i.e. as an integral along a path slightly above the real axis, i.e. of the form $C = [-\infty + i\epsilon, \infty + i\epsilon]$ with $\epsilon > 0$. In order to obtain the decomposition for $x = -\frac{1}{T}$ real and negative, one deforms the path of integration C in the complex domain to the disjoint union of two paths C_1 and C_2 as shown

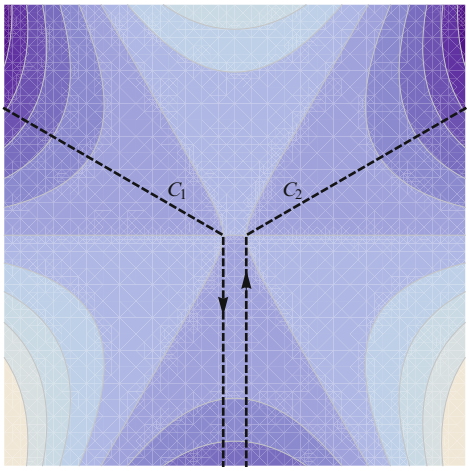


Fig. 4 For z real negative one deforms the path $C = [-\infty, \infty]$ to the disjoint union of C_1 and C_2. The levels are those of the real part of the function $\Phi(s, z)$ where $\Phi(s, z) = i\left(\frac{s^3}{3} + zs\right)$

in Fig. 4. The integrals over the paths C_j give complex conjugate numbers and this splitting as a sum $\int_C = \int_{C_1} + \int_{C_2}$ gives $\mathrm{Ai}(x) = 2\Re(\int_{C_2})$. In fact, the imaginary part $2\Im(\int_{C_2})$ gives the other Airy function $\mathrm{Bi}(x)$ which is known to be a solution of the second order linear differential equation $y'' - xy = 0$. This function can be defined directly as the following oscillatory integral

$$\mathrm{Bi}(x) = \frac{1}{\pi}\int_0^\infty \left(e^{-\left(\frac{s^3}{3} - xs\right)} + \sin\left(\frac{s^3}{3} + xs\right)\right) ds \tag{90}$$

described by the two pieces of a path C_2' going through the lower half of the imaginary axis and the right half of the real axis. $\mathrm{Bi}(x)$ is characterized, among the solutions of $y'' - xy = 0$, by

$$\mathrm{Bi}(0) = \frac{1}{3^{1/6}\Gamma(\frac{2}{3})}\,, \quad \mathrm{Bi}'(0) = \frac{3^{1/6}}{\Gamma(\frac{1}{3})}\,.$$

To obtain the required decomposition of $\mathrm{Ai}(x)$ one uses the stationary phase method to evaluate $\int_{C_2}$ where C_2 goes through the critical point $\sqrt{-x}$ with an angle of $\pi/4$ with respect to the real axis, so that it follows the line of steepest descent. This shows that the argument of the complex number $\int_{C_2} = \frac{1}{2}(\mathrm{Ai}(x) + i\mathrm{Bi}(x))$ is close to $\alpha(x) = \frac{\pi}{4} + \frac{2x\sqrt{-x}}{3}$ and thus one introduces the rotation matrix

$$R(x) = \begin{bmatrix} \cos\alpha(x) & \sin\alpha(x) \\ -\sin\alpha(x) & \cos\alpha(x) \end{bmatrix}\,, \quad \alpha(x) = \frac{\pi}{4} + \frac{2x\sqrt{-x}}{3}$$

which one applies to the column vector $\xi(x)$ with entries $(\mathrm{Ai}(x), \mathrm{Bi}(x))$. By using the inverse rotation matrix it follows that

$$\mathrm{Ai}(x) = \cos\alpha(x)\,(R(x)\xi(x))_1 - \sin\alpha(x)\,(R(x)\xi(x))_2 = \mathrm{Ai}_0(x) + \mathrm{Ai}_1(x)$$

It is exactly the decomposition of $\mathrm{Ai}(x)$ as a sum of two terms $\mathrm{Ai}_j(x)$ which gives the precise meaning to the asymptotic expansion. Indeed, the stationary phase method shows that

$$2e^{-i\alpha(x)}\int_{C_2} \sim \frac{(-x)^{-1/4}}{2\pi^{3/2}}\sum_{n=0}^{\infty}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n x^{-\frac{3n}{2}}. \tag{91}$$

Thus since $e^{-i\alpha(x)}(\mathrm{Ai}(x) + i\mathrm{Bi}(x)) = 2e^{-i\alpha(x)}\int_{C_2}$, this shows that one has

$$\mathrm{Ai}_0(x) \sim \frac{(-x)^{-1/4}}{2\pi^{3/2}}\cos\alpha(x)\sum_{n\ \mathrm{even}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n x^{-\frac{3n}{2}}. \tag{92}$$

It follows that for any $m > 0$ the ratio of the left hand side with the right hand side truncated at $n \leq m$ is of the form $1 + O(x^{-\frac{3m}{2}})$ for $x < 0$, $x \to -\infty$ as above. Similarly one shows that (Fig. 5)

$$\mathrm{Ai}_1(x) \sim -\frac{(-x)^{-1/4}}{2\pi^{3/2}}\sin\alpha(x)\sum_{n\ \mathrm{odd}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(3/4)^n(-1)^{(n-1)/2}(-x)^{-\frac{3n}{2}} \tag{93}$$

in the above strong sense. Notice that the two equivalences (92) and (93) are stronger than the original one (89) for $\mathrm{Ai}(x)$. In particular they determine *exactly* the positions of the zeros of $\mathrm{Ai}_j(x)$ for $x << 0$ as the $x_n = -\frac{1}{4}3^{2/3}(-\pi + 4n\pi)^{2/3}$ for Ai_0 and $y_n = -\frac{1}{4}3^{2/3}(\pi + 4n\pi)^{2/3}$ for Ai_1. On the other hand the zeros of the Airy function are not given by an elementary formula. Moreover even the overall sizes of the two terms $\mathrm{Ai}_j(x)$ are not the same since while $\mathrm{Ai}_0(x)$ is of the order of $(-x)^{-1/4}$ the function $\mathrm{Ai}_1(x)$ is of the order of $(-x)^{-7/4}$.

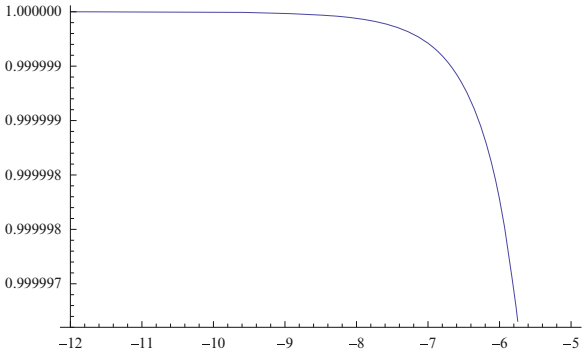


Fig. 5 The ratio of $\mathrm{Ai}_1(x)$ with its approximation using the first four terms of the asymptotic series

7.1 Strong Asymptotic Expansion of $\int_{C_2}$

We now work out the details of the stationary phase method, first for the asymptotic expansion of $\int_{C_2} = \frac{1}{2}(\mathrm{Ai}(x) + i\mathrm{Bi}(x))$ (when $x < 0$). We perform a change of variables in

$$\mathrm{Ai}(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{i\left(\frac{s^3}{3}+xs\right)}ds \tag{94}$$

and let $x = -u^{\frac{2}{3}}$ with $u > 0$ and $s = u^{\frac{1}{3}}t$. We then get

$$\mathrm{Ai}(x) = \frac{u^{\frac{1}{3}}}{2\pi}\int_{-\infty}^{\infty} e^{iu\left(\frac{t^3}{3}-t\right)}dt \tag{95}$$

and we are looking for the expansion when $u \to +\infty$. After the above change of variables the two critical points correspond now to $t = \pm 1$. For the path C_2 we take the path, in the complex domain, through the critical point $t = 1$ and such that the real part of $\frac{t^3}{3} - t$ remains constant (equal to $-\frac{2}{3}$) along the path. In this way the variation of the phase will only come from the term dt. With $t = \xi + i\eta$ one has

$$\Re\left(\frac{t^3}{3} - t\right) = \frac{\xi^3}{3} - \xi\eta^2 - \xi$$

and we take for C_2 the branch of the curve

$$\frac{\xi^3}{3} - \xi\eta^2 - \xi + \frac{2}{3} = 0$$

which is given by the formula, valid for $\xi > 0$,

$$\eta = \frac{(-1+\xi)\sqrt{2+\xi}}{\sqrt{3}\sqrt{\xi}}.$$

Along the path C_2 one has the equality (Fig. 6)

$$i\left(\frac{t^3}{3} - t\right) = -\frac{2}{3}i - \frac{1}{2}w^2, \quad w(\xi) = \frac{2(-1+\xi)(2+\xi)^{1/4}(1+2\xi)}{3^{5/4}\xi^{3/4}} \tag{96}$$

and $w(\xi)$ varies from $-\infty$ (for $\xi = 0$) to $+\infty$ for $\xi \to \infty$. One needs to compute dt and one has

$$d\eta/d\xi = \frac{1+\xi+\xi^2}{\sqrt{3}\xi^{3/2}\sqrt{2+\xi}} \tag{97}$$

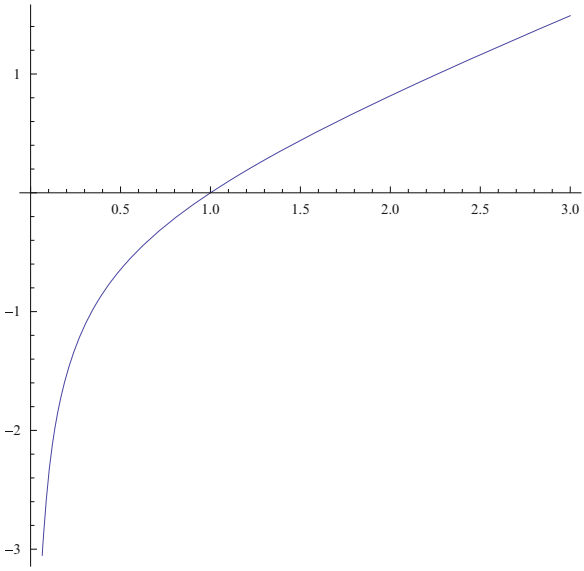


Fig. 6 The path C_2

and

$$dw/d\xi = \frac{1+3\xi^2+2\xi^3}{3^{1/4}\xi^{7/4}(2+\xi)^{3/4}}. \tag{98}$$

For $\xi \to 0$ one has

$$w \sim -(\frac{2}{3})^{\frac{5}{4}}\xi^{-\frac{3}{4}},\ \ d\eta/d\xi \sim 6^{-\frac{1}{2}}\xi^{-\frac{3}{2}},\ \ dw/d\xi \sim 3^{-\frac{1}{4}}2^{-\frac{3}{4}}\xi^{-\frac{7}{4}} \tag{99}$$

so that

$$d\xi/dw \sim c_1|w|^{-\frac{7}{4}},\ \ d\eta/dw \sim c_2|w|^{\frac{1}{4}} \tag{100}$$

For $\xi \to +\infty$ one has

$$w \sim 4\times 3^{-\frac{5}{4}}\xi^{\frac{3}{2}},\ \ d\eta/d\xi \sim 3^{-\frac{1}{2}},\ \ dw/d\xi \sim 2\times 3^{-\frac{1}{4}}\xi^{\frac{1}{2}} \tag{101}$$

so that

$$d\xi/dw \sim c_3|w|^{-\frac{1}{3}},\ \ d\eta/dw \sim c_4|w|^{-\frac{1}{3}}. \tag{102}$$

We can now justify the asymptotic expansion of $\int_{C_2}$.

Lemma 7. *When $u \to +\infty$ one has*

$$e^{-i(\frac{\pi}{4}-\frac{2}{3}u)}\int_{C_2} e^{iu\left(\frac{t^3}{3}-t\right)}dt \sim \frac{u^{-1/2}}{2\sqrt{\pi}}\sum_{n=0}^{\infty}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(\frac{3}{4}i)^n u^{-n} \tag{103}$$

Proof. Using (96) we have

$$\int_{C_2} e^{iu\left(\frac{t^3}{3}-t\right)}dt = e^{-i\frac{2}{3}u}\int_{-\infty}^{\infty} e^{-uw^2/2}g(w)dw \tag{104}$$

where the function $g(w)$ is given by

$$g(w) = g_1(w) + ig_2(w) = d\xi/dw + id\eta/dw \tag{105}$$

where one expresses ξ as a function $\xi(w)$ of $w \in \mathbb{R}$. The two functions $g_j(w)$ are smooth and $O(|w|^\ell)$ when $|w| \to \infty$ by (100) and (102). The Taylor expansion of $g(w)$ at $w = 0$ is of the form

$$g(w) = \left(\frac{1}{2}+\frac{i}{2}\right)-\frac{iw}{6}-\left(\frac{5}{96}-\frac{5i}{96}\right)w^2+\frac{w^3}{27}-\left(\frac{385}{27648}+\frac{385i}{27648}\right)w^4+\frac{7iw^5}{648}+\dots$$

and the even part $\frac{1}{2}(g(w)+g(-w))$ takes the simpler form

$$\frac{1}{2}(g(w)+g(-w)) = \frac{1+i}{2}\left(1+\frac{5iw^2}{48}-\frac{385w^4}{13824}-\frac{17017iw^6}{1990656}+\frac{1062347w^8}{382205952}+\dots\right)$$

In fact one has an equality of the form

$$\frac{1}{2}(g(w)+g(-w)) = e^{i\frac{\pi}{4}}(h_0(w)+ih_1(w)) \tag{106}$$

where $h_0(w)$ is the real part of $e^{-i\frac{\pi}{4}}\frac{1}{2}(g(w)+g(-w))$. By construction both h_j are smooth even functions and $O(|w|^\ell)$ when $|w| \to \infty$. Moreover $h_j(w) = k_j(w^2)$ where again both k_j are smooth, k_0 is even and k_1 is odd.

Let

$$f_j(u) := \int_{-\infty}^{\infty} e^{-uw^2/2}h_j(w)dw = \int_0^{\infty} e^{-uv/2}k_j(v)\frac{dv}{\sqrt{v}}. \tag{107}$$

The asymptotic expansion of $f_j(u)$ for $u \to \infty$ follows directly from the Taylor expansion of $h_j(w)$ at $w = 0$ (or of $k_j(v)$ at $v = 0$, using e.g. Watson's Lemma). It is given by the well known explicit formulas

$$f_0(u) \sim \frac{u^{-1/2}}{2\sqrt{\pi}}\sum_{n\,\text{even}}(-1)^{\frac{n}{2}}\frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!}(\frac{3}{4})^n u^{-n} \tag{108}$$

and

$$f_1(u) \sim \frac{u^{-1/2}}{2\sqrt{\pi}} \sum_{n\,\text{odd}} (-1)^{\frac{n-1}{2}} \frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!} (\frac{3}{4})^n u^{-n}. \tag{109}$$

Thus since by (104),

$$\int_{C_2} e^{iu\left(\frac{t^3}{3}-t\right)} dt = e^{i(\frac{\pi}{4}-\frac{2}{3}u)}(f_0(u) + if_1(u)) \tag{110}$$

one obtains (103). □

The above asymptotic expansions hold in the classical sense as defined by Poincaré. We shall now see that when one passes to the real part an interesting phenomenon occurs. We first need to define more precisely the notion of *strong asymptotic expansion*.

Let us consider, for $\alpha > 0$ the following multiplicative subset of functions of the variable u.

$$G_\alpha = \{h \mid h(u) = 1 + O(u^{-\alpha}) \text{ for } u \to +\infty\}. \tag{111}$$

Definition 7. Let $f(u)$, $t_n(u)$ be functions of the positive real variable u. The expansion $f(u) \sim \sum_1^\infty t_n(u)$ is called a *strong asymptotic expansion* when for any $\alpha > 0$ there exists n_α such that

$$f \in \left(\sum_1^n t_k\right) G_\alpha\,, \ \forall n \geq n_\alpha. \tag{112}$$

Proposition 11. *For $x \in \mathbb{R}$, $x < 0$, there exists a decomposition*

$$\mathrm{Ai}(x) = \mathrm{Ai}_0(x) + \mathrm{Ai}_1(x) \tag{113}$$

as a sum of two real analytic functions of x with strong asymptotic expansions

$$\mathrm{Ai}_0(-u^{\frac{2}{3}}) \sim \frac{u^{-1/6}}{2\pi^{3/2}} \cos(\frac{\pi}{4} - \frac{2}{3}u) \sum_{n\,\text{even}} (-1)^{n/2} \frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!} (3/4)^n u^{-n} \tag{114}$$

$$\mathrm{Ai}_1(-u^{\frac{2}{3}}) \sim -\frac{u^{-1/6}}{2\pi^{3/2}} \sin(\frac{\pi}{4} - \frac{2}{3}u) \sum_{n\,\text{odd}} (-1)^{\frac{(n-1)}{2}} \frac{\Gamma(n+\frac{5}{6})\Gamma(n+\frac{1}{6})}{n!} (3/4)^n u^{-n}. \tag{115}$$

Proof. One has, using (95), and deforming the path $(-\infty, \infty) + i\epsilon$ into the union of two paths C_j as in Fig. 7

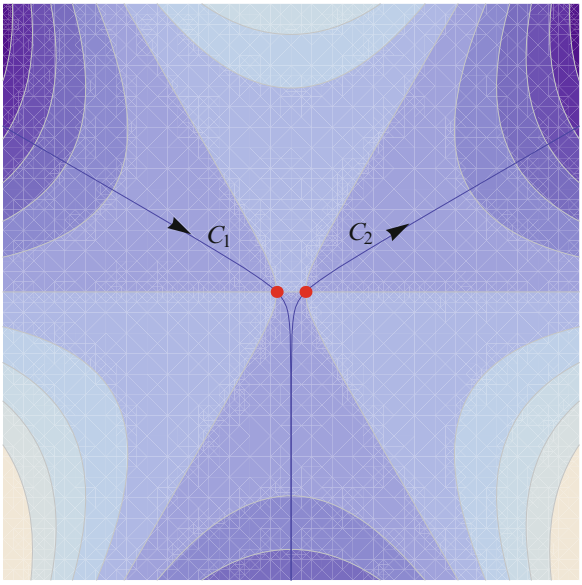


Fig. 7 The paths C_j

$$\mathrm{Ai}(-u^{\frac{2}{3}}) = \frac{u^{\frac{1}{3}}}{2\pi} \sum_j \int_{C_j} e^{iu\left(\frac{t^3}{3}-t\right)} dt. \tag{116}$$

The symmetry $s(t) = -\bar{t}$ transforms C_2 into C_1 but reverses the natural orientation. One has

$$iu\left(\frac{s(t)^3}{3} - s(t)\right) = \overline{\left(iu\left(\frac{t^3}{3} - t\right)\right)}$$

and thus the terms $\int_{C_j}$ in (116) are complex conjugate. With the notations of (107) we define

$$\mathrm{Ai}_0(x) := \frac{u^{\frac{1}{3}}}{\pi}\cos(\frac{\pi}{4} - \frac{2}{3}u) f_0(u)\,,\ \forall x = -u^{\frac{2}{3}} \tag{117}$$

and

$$\mathrm{Ai}_1(x) := \frac{u^{\frac{1}{3}}}{\pi}\sin(\frac{\pi}{4} - \frac{2}{3}u) f_1(u)\,,\ \forall x = -u^{\frac{2}{3}}. \tag{118}$$

By (116) one has

$$\mathrm{Ai}(-u^{\frac{2}{3}}) = \frac{u^{\frac{1}{3}}}{\pi} \Re\left(\int_{C_2} e^{iu\left(\frac{t^3}{3}-t\right)} dt\right) \tag{119}$$

and taking the real part of both sides of (110) one gets the decomposition (113). Using (108) and (109) one obtains the strong asymptotic expansions (114) and (115). □

Proposition 12. *There exists an element h of the algebra $B^+_{\mathbb{C},0} = B^+_{\infty,0} \otimes_{\mathbb{R}} \mathbb{C}$ such that, for any $u > 0$ one has*

$$\mathrm{Ai}(-u^{\frac{2}{3}}) = u^{\frac{1}{3}} \Re \left(e^{i(\frac{\pi}{4} - \frac{2}{3}u)} h(u) \right). \tag{120}$$

Proof. Let $h(u) = \frac{1}{\pi}(f_0(u) + if_1(u))$, then by (119) and (110) one has (120). It remains to show that each f_j belongs to $B^+_{\infty,0}$. By (107) one has

$$f_j(u) = \int_0^\infty e^{-uv/2} k_j(v) \frac{dv}{\sqrt{v}} \tag{121}$$

where the function $k_j(v)$ is smooth and of polynomial growth at ∞. It follows that the measure $d\mu_j = k_j(v)\frac{dv}{\sqrt{v}}$ is a Radon measure such that $\int_0^\infty e^{-\alpha v}|d\mu_j| < \infty$ for any $\alpha > 0$ and one obtains the conclusion using (121) and Definition 6. □

7.2 Source Term and Perturbative Treatment of the Airy Integral

In this section we investigate what happens if we treat the Airy integral by introducing a source term and by performing perturbation theory around a Gaussian: this is a familiar method in the theory of Feynman integrals. We consider the Airy integral in the form

$$F(u) = u^{-\frac{1}{3}} \mathrm{Ai}(-u^{\frac{2}{3}}) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{iu\left(\frac{t^3}{3} - t\right)} dt$$

and we introduce a source term

$$F(u, j) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{iu\left(\frac{t^3}{3} - t + jt\right)} dt \tag{122}$$

in order to understand the relative roles of the variables u and j. One has, for $t = (1-j)^{1/2}s$,

$$iu\left(\frac{t^3}{3} - t + jt\right) = iu(1-j)^{3/2}\left(\frac{s^3}{3} - s\right)$$

so that for $j < 1$ one gets

$$F(u,j) = (1-j)^{1/2} F(u(1-j)^{3/2}). \tag{123}$$

The formula (123) gives us, for $j < 1$, fixed the control of the behavior of the integral (122) when $u \to \infty$.

Next, we compare this with the perturbative method around a critical point. We choose a critical point for the action without the source, we take $t = 1$ and write $t = 1 + \phi$. We are then dealing with the exponent $iu\left(-\frac{2}{3} + j + j\phi + \phi^2 + \frac{\phi^3}{3}\right)$, and thus with the integral

$$F(u,j) = e^{iu(-\frac{2}{3}+j)} \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{iu\left(\phi^2 + \frac{\phi^3}{3} + j\phi\right)} d\phi. \tag{124}$$

We now see how this integral is treated in the perturbative manner. One first introduces a coupling constant g in front of the interaction term. The reason for doing that is to be able to proceed by integrating against a Gaussian. When $g = 0$ the integral is Gaussian and one then expands around $g = 0$ to obtain the result in general. Thus one deals with

$$F(u,j,g) = e^{iu(-\frac{2}{3}+j)} \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{iu\left(\phi^2 + g\frac{\phi^3}{3} + j\phi\right)} d\phi \tag{125}$$

so that $F(u,j) = F(u,j,1)$. One treats g as small and one looks for an asymptotic expansion in powers of g. Since the interaction term is of higher order, we get the equation $W_0 = \text{Legendre}(S)$. The change of variables is that $u = \frac{1}{\hbar}$, and the action $S(\phi)$ is given by

$$S(\phi) = \phi^2 + g\frac{\phi^3}{3}. \tag{126}$$

One computes the Legendre transform of S perturbatively. One has two solutions of the equation $\delta S/\delta\psi = -j$ which are given by

$$\psi = \frac{-1 \pm \sqrt{1-gj}}{g}$$

and the solution which is selected by the perturbative expansion is

$$\psi_+ = \frac{-1 + \sqrt{1-gj}}{g} = -\frac{j}{2} - \frac{gj^2}{8} - \frac{g^2 j^3}{16} - \frac{5g^3 j^4}{128} + O(j)^5. \tag{127}$$

One thus gets at the perturbative level

$$W_0(j) = S(\psi_+) + j\psi_+$$

and taking into account the term $e^{iu(-\frac{2}{3}+j)}$ one gets the following evaluation for the exponent

$$iu\left(-\frac{2}{3}+j+S(\psi_+)+j\psi_+\right)=iu\left(-\frac{2}{3}+j-\frac{j^2}{4}-\frac{j^3}{24}+\frac{1}{64}\left(-2g+g^2\right)j^4+O(j)^5\right)$$

where in closed form one has

$$S(\psi_+)+j\psi_+=\frac{\left(-1+\sqrt{1-gj}\right)\left(3g^2j+3g\left(-1+\sqrt{1-gj}\right)+\left(-1+\sqrt{1-gj}\right)^2\right)}{3g^3}.$$

Taking $g=1$, the above expression simplifies and one obtains

$$-\frac{2}{3}+j+S(\psi_+)+j\psi_+=-\frac{2}{3}(1-j)^{3/2}$$

which gives the exponent

$$iu\left(-\frac{2}{3}(1-j)^{3/2}\right).$$

This shows that the perturbative expansion corresponds to taking the integral over the path C_2 in the expression of the Airy function and gives a strong asymptotic expansion of this term but of course it completely ignores the contribution of C_1 which is nevertheless essential.

Let us now look at the non-perturbative behavior of the functional integral as a function of the source j. One uses the usual normalization which amounts to divide by the value at $j=0$ and thus we consider

$$\left(\frac{1}{2\pi}\int_{-\infty}^{\infty}e^{iu\left(\frac{t^3}{3}-t+jt\right)}dt\right)/\left(\frac{1}{2\pi}\int_{-\infty}^{\infty}e^{iu\left(\frac{t^3}{3}-t\right)}dt\right)=F(u,j)/F(u). \tag{128}$$

One has, using (123), and for $j<1$

$$F(u,j)/F(u)=(1-j)^{1/2}F(u(1-j)^{3/2})/F(u)=\frac{\mathrm{Ai}(-(1-j)u^{\frac{2}{3}})}{\mathrm{Ai}(-u^{\frac{2}{3}})}. \tag{129}$$

Since the denominator has many zeros which do not correspond to zeros of the numerator one obtains a function which oscillates wildly between the poles as shown in Fig. 8.

We can thus summarize the treatment of the integral with a source (122) as follows

$$F(u,j)=\frac{1}{2\pi}\int_{-\infty}^{\infty}e^{iu\left(\frac{t^3}{3}-t+jt\right)}dt \tag{130}$$

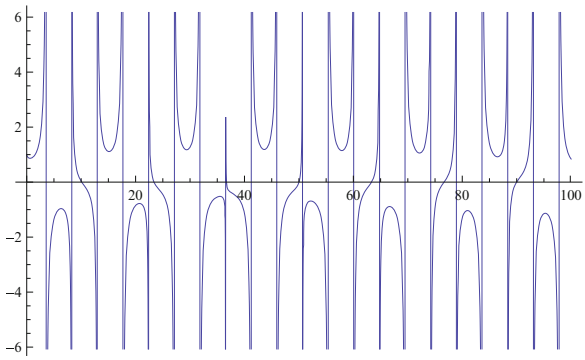


Fig. 8 The graph of $\frac{\mathrm{Ai}(-(1-j)u^{\frac{2}{3}})}{\mathrm{Ai}(-u^{\frac{2}{3}})}$ for $j = \frac{1}{2}$

1. The quotient $F(u,j)/F(u,0)$ has infinitely many poles in u when $j \neq 0$ and its logarithm does not make sense.
2. This behavior is due to the presence of two critical points which each contribute by a wave without any coherence between the two waves.
3. The perturbative treatment chooses one of the critical points and makes an expansion of the contribution of this critical point, thus giving this term up to strong equivalence.
4. The presence of several critical points forces one to add the contributions of each critical point and replaces the exact knowledge of each of these terms up to strong equivalence by a hypersum in the quotient hyperfield.

Thus one can conclude that the way the perturbative method disregards the problem of the hypersum relies in the fact that it does not compute the full integral but only a portion of it corresponding to the choice of a critical point. Clearly, a complete understanding of the process requires to consider the full integral by add up the various contributions, therefore the appearance of the hypersum cannot be avoided. In the context of gauge theories in physics, the presence of several critical points is unavoidable and for this reason we expect that the formalism deployed by the theory of hyper-structures (hyperrings and hyperfields) might shed some light on the evaluation of Feyman integrals in that context.

7.3 A Toy Model: The Hyperfield $\mathbb{C}^\flat$

The choice of a critical point in the asymptotic expansions which one performs in quantum physics to interpret the result in a classical manner is guided by the Wick rotation whose effect is to replace an integral of imaginary exponentials by an integral of real exponentials. This process is justified in quantum field theory where one then rotates back by analytic continuation from the Euclidean formulation to

the Minkowski space physical description. This suggests to select the critical points using the following total ordering on $\mathbb{C}$. Let $\mathbb{C}_+ \subset \mathbb{C}$ be defined by

$$\mathbb{C}_+ = \{z \in \mathbb{C} \mid \Re(z) \geq 0 \text{ and } \Im(z) \geq 0 \text{ if } \Re(z) = 0\} \tag{131}$$

We write $z \leq z'$ for $z' - z \in \mathbb{C}_+$. This defines a total order relation compatible with addition.

7.3.1 The Hyperfield $\mathbb{C}^\flat$

As a set $\mathbb{C}^\flat = (\mathbb{C} \bigsqcup \mathbb{C}) \cup \{0\}$ is the union of two copies of $\mathbb{C}$ and $\{0\}$. We write its non-zero elements as $\epsilon\, e(z)$ where $\epsilon = \pm 1$ and $z \in \mathbb{C}$. The multiplicative structure is defined by $\epsilon e(z) \cdot \epsilon' e(z') := \epsilon\epsilon' e(z + z')$ and the additive structure is given by

$$\epsilon\, e(z) + \epsilon'\, e(z') = \begin{cases} \epsilon\, e(z), & \text{if } z' < z; \\ \epsilon'\, e(z'), & \text{if } z < z'; \\ \epsilon\, e(z) & \text{if } z = z', \epsilon = \epsilon'; \\ \{0\} \cup \{\epsilon'' e(z'') \mid z'' \leq z\}, & \text{if } z = z', \epsilon = -\epsilon'. \end{cases} \tag{132}$$

One checks that these laws define a hyperfield structure on $\mathbb{C}^\flat$. Moreover as in the real case one obtains

Proposition 13. *The hyperfield $\mathbb{C}^\flat$ is perfect of characteristic one.*

7.3.2 Description of $\mathbb{C}^\flat$ as Perfection of $\mathbb{C}$

We shall use an analogous formula as in the real case where we take $\kappa = \frac{1}{3}$ in Theorem 1. The only difference is that in the complex case we require that the sequence $(x^{(j)})_{j\in\mathbb{Z}}$ of complex numbers $x^{(j)} \in \mathbb{C}$, is doubly infinite and *convergent* when $j \to -\infty$. This nuance makes no difference in the real case since any sequence $(x^{(j)})_{j\geq 0}$ of real numbers such that $x^{(j+1)} = (x^{(j)})^3\,,\ \forall j$, uniquely extends to a doubly infinite sequence $(x^{(j)})_{j\in\mathbb{Z}}$ fulfilling $x^{(j+1)} = (x^{(j)})^3\,,\ \forall j$, and the obtained sequence is automatically convergent when $j \to -\infty$ (and its limit belongs to $\{-1, 0, 1\}$).

Theorem 9. *One has a canonical isomorphism of $\mathbb{C}^\flat$ with doubly infinite sequences $x^{(j)} \in \mathbb{C}$ as follows*

$$\mathbb{C}^\flat \xrightarrow{\surd} \{(x^{(j)})_{j\in\mathbb{Z}}, \text{ convergent for } j \to -\infty \mid x^{(j+1)} = (x^{(j)})^3\,,\ \forall j \in \mathbb{Z}\} \tag{133}$$

The map $\surd$ associates to 0 the sequence $x^{(j)} = 0$ and to $x = \epsilon\, e(z) \in \mathbb{C}^\flat$ the sequence $x^{(j)} = \epsilon\, e^{3^j z}$.

Proof. The map $\sqrt{}$ which associates to $x = \epsilon\, e(z) \in \mathbb{C}^\flat$ the sequence $x^{(j)} = \epsilon\, e^{3^j z}$ is well defined since $(x^{(j)})^3 = x^{(j+1)}$ as 3 is odd, while $x^{(j)} \to \epsilon$ as $j \to -\infty$. We show that the map $\sqrt{}$ is bijective. It is injective because the sequence $x^{(j)} = \epsilon\, e^{3^j z}$ determines both ϵ and z by the equalities

$$\epsilon = \lim_{j\to-\infty} x^{(j)}\,,\quad z = \lim_{j\to-\infty} 3^{-j}\left(\epsilon\, x^{(j)} - 1\right).$$

Let now $x^{(j)}$ be a doubly infinite sequence of complex numbers as in (133). If $x^{(0)} = 0$ then all $x^{(j)}$ are 0. Assume that $x^{(0)} \neq 0$ and let $\mu = |x^{(0)}|$. Then one has $|x^{(-j)}| = \mu^{1/3^j} \to 1$ when $j \to \infty$. The limit $\epsilon = \lim_{j\to-\infty} x^{(j)}$ fulfills $\epsilon \neq 0$ and

$$\epsilon^3 = \lim (x^{(j-1)})^3 = \lim x^{(j)} = \epsilon$$

so that $\epsilon = \pm 1$. Replacing $x^{(j)}$ by $-x^{(j)}$ we can assume that $\epsilon = 1$ i.e. that $x^{(j)} \to 1$ when $j \to -\infty$. Since $x^{(j)} \to 1$ one has $|x^{(j)} - 1| < 1$ for $j \leq j_0$ and thus

$$x^{(j)} = e^{z_0/3^{j_0-j}}\,,\ \forall j \leq j_0,\ \ z_0 = \log(x^{(j_0)}) \tag{134}$$

where $\log(x^{(j_0)})$ is defined by the convergent series

$$\log(x^{(j_0)}) = -\sum_1^\infty \frac{(1 - x^{(j_0)})^n}{n}.$$

Thus one gets, with $z = 3^{-j_0} z_0$ the equality $x^{(j)} = e^{3^j z}$, $\forall j$, and hence the surjectivity of $\sqrt{}$. □

It is important to have an explicit formula for the natural extension of the sequence $x^{(j)}$ to a continuous, one parameter family $x(t) \in \mathbb{C}$, $t \in \mathbb{R}$.

Corollary 2. *Let $x^{(j)}$ be a non-zero sequence of complex numbers such that $(x^{(j)})^3 = x^{(j+1)}$ for all $j \in \mathbb{Z}$ and which is convergent for $j \to -\infty$. There exists a unique continuous one parameter family $x(t) \in \mathbb{C}$, $t \in \mathbb{R}$ such that*

- *$x(3^j) = x^{(j)}$, $\forall j \in \mathbb{Z}$.*
- *$x(kt) = x(t)^k$ for all odd $k \in \mathbb{Z}$.*

Let $\epsilon = \lim_{j\to-\infty} x^{(j)}$. Then one has for any $t > 0$

$$x(t) = \epsilon \prod (\epsilon\, x^{(j)})^{a_j}\,,\ \forall a_j \in \{0, 1, 2\},\ \sum a_j\, 3^j = t. \tag{135}$$

Proof. The existence of the $x(t)$ follows from Theorem 9. Its uniqueness follows from the density in $\mathbb{R}$ of the $a\, 3^{-k}$ where $a \in \mathbb{Z}$ is odd. To prove (135) one can assume that $\epsilon = \lim x^{(j)}$ is 1. One then has $x(t) = e^{zt}$ for some $z \in \mathbb{C}$ and (135) follows. Note that the infinite product is absolutely convergent since $\sum_{j\leq 0} |\epsilon\, x^{(j)} - 1| < \infty$. □

The product of two convergent sequences is convergent and thus it is immediate to get the product of two elements of $\mathbb{C}^\flat$ from their representation as doubly infinite sequences

$$(x^{(j)})_{j\in\mathbb{Z}}.(y^{(j)})_{j\in\mathbb{Z}} = (x^{(j)}y^{(j)})_{j\in\mathbb{Z}}. \tag{136}$$

For the addition, the natural formula to try is (as in the p-adic and real cases)

$$(x+y)^{(i)} = \lim_{j\to\infty}(x^{(i+j)}+y^{(i+j)})^{3^{-j}} \tag{137}$$

however, one needs to handle here the ambiguity in the extraction of roots of order a power of 3. When $|x^{(0)}| > |y^{(0)}|$ this is easily done since, for $j \geq 0$

$$x^{(i+j)}+y^{(i+j)} = x^{(i+j)}\left(1+(y^{(i)}/x^{(i)})^{3^j}\right)$$

while for $j \to \infty$ one has, since $|y^{(i)}/x^{(i)}| < 1$

$$\left(1+(y^{(i)}/x^{(i)})^{3^j}\right)^{3^{-j}} \to 1 \tag{138}$$

using the unique extraction of roots in a neighborhood of 1. Thus this gives

$$(x+y)^{(i)} = x^{(i)} \text{ if } |x^{(0)}| > |y^{(0)}|. \tag{139}$$

What is new in the complex case is that in the case when $|x^{(0)}| = |y^{(0)}|$ (i.e. when the two sequences have the same modulus) it is the behavior of $x(t)+y(t)$ on the *imaginary* axis (i.e. for $it \to +\infty$) which allows one to get the hypersum. The required analytic continuation in the parameter t connects with the Wick rotation of quantum physics. Note that there is nevertheless also a direct manner to decide, assuming $y \neq -x$, which between x and y is the hypersum $x+y$, this is achieved by considering the behavior of the sequences $(x^{(j)})_{j\geq 0}$ and $(y^{(j)})_{j\geq 0}$ for $j \to -\infty$. When $|x| \neq |y|$ it is the sequence of largest modulus. When $|x| = |y|$ one considers the sequence

$$u(j) = x^{(j)}/y^{(j)}, \quad j \to -\infty,$$

of complex numbers of modulus 1 and the hypersum is x (resp. y) when the sequence rotates in a clockwise (resp. anticlockwise) manner for $j \to -\infty$.

7.3.3 $\mathbb{C}$ as the Quotient of $\mathbb{C}^\flat$ by the Euler Relation $e^{i\pi} = -1$

We show that $\mathbb{C}^\flat$ appears naturally as the perfection of the hyperfield $\mathscr{T}\mathbb{C}$ of Viro tropical complex numbers (cf. [25]). The multiplicative structure of $\mathscr{T}\mathbb{C}$ is the same

as for ordinary complex numbers and we recall the definition of the hypersum $a \smile b$ in the case of Viro tropical complex numbers. One sets

1. If $|a| < |b|$: $a \smile b = b$; if $|a| > |b|$: $a \smile b = a$.
2. If $|a| = |b|$ and $a \neq -b$, with $a = re^{i\alpha}, b = re^{i\beta}$ and $|\alpha - \beta| < \pi$

$$a \smile b = \{re^{i\varphi} \mid |\alpha - \varphi| + |\varphi - \beta| = |\alpha - \beta|\}$$

3. If $a + b = 0$: $a \smile b$ is the closed disk $\{c \in \mathbb{C} \mid |c| \leq |a|\}$.

The hyperfield $\mathscr{T}\mathbb{C}$ is not perfect. This conclusion is obvious since the map $x \mapsto x^n$ is not bijective say for $n = 3$.

Proposition 14. (*i*) *The following map* $\mathrm{ev} : \mathbb{C}^\flat \to \mathscr{T}\mathbb{C}$ *is a hyperfield homomorphism*

$$\mathrm{ev}(\epsilon e(z)) := \epsilon e^z\,,\ \forall \epsilon \in \{\pm 1\},\ z \in \mathbb{C},\ \ \mathrm{ev}(0) = 0. \tag{140}$$

Moreover (with the notations of Theorem 9) one has $\mathrm{ev}(x) = x^{(0)}$ *for all* $x \in \mathbb{C}^\flat$.

(*ii*) *The hyperfield homomorphism* ev *is surjective and at the level of the multiplicative groups one has the exact sequence*

$$1 \to (-e(i\pi))^{\mathbb{Z}} \to \mathbb{C}^{\flat\times} \xrightarrow{\mathrm{ev}} \mathbb{C}^\times \to 1. \tag{141}$$

Proof. The map $\mathrm{ev} : \mathbb{C}^\flat \to \mathscr{T}\mathbb{C}$ is multiplicative, we need to check that it is compatible with the hyperaddition. Let $x = \epsilon e(z), x' = \epsilon e(z')$, we show that

$$\mathrm{ev}(x + x') \subset \mathrm{ev}(x) \smile \mathrm{ev}(x'). \tag{142}$$

Assume first that $\Re(z) < \Re(z')$. Then one has $z' - z \in \mathbb{C}_+$ and thus $x + x' = x'$ by (132). One has $|\mathrm{ev}(x)| = e^{\Re(z)}$ and thus $|\mathrm{ev}(x)| < |\mathrm{ev}(x')|$ so that $\mathrm{ev}(x) \smile \mathrm{ev}(x') = \mathrm{ev}(x')$. This shows that (142) holds when $\Re(z) \neq \Re(z')$. Assume now that $\Re(z) = \Re(z')$. Then $|\mathrm{ev}(x)| = |\mathrm{ev}(x')|$ and the definition of the hypersum $\smile$ shows that in this case $\mathrm{ev}(x) \smile \mathrm{ev}(x') \supset \{\mathrm{ev}(x), \mathrm{ev}(x')\}$. This shows, using (132), that (142) holds when $x' \neq -x$. Assume now that $x' = -x$. Then $\mathrm{ev}(x) = -\mathrm{ev}(x')$ and $\mathrm{ev}(x) \smile \mathrm{ev}(x')$ is the closed disk $\{c \in \mathbb{C} \mid |c| \leq |\mathrm{ev}(x)|\}$. With $x = \epsilon\, e(z)$ one has

$$x + x' = \{0\} \cup \{\epsilon'' e(z'') \mid z'' \leq_P z\}.$$

But $z'' \leq_P z$ implies $\Re(z'') \leq \Re(z)$ and hence $|\mathrm{ev}(\epsilon'' e(z''))| = e^{\Re(z'')} \leq e^{\Re(z)} = |\mathrm{ev}(x)|$ so that $\mathrm{ev}(\epsilon'' e(z''))$ belongs to the closed disk $\{c \in \mathbb{C} \mid |c| \leq |\mathrm{ev}(x)|\}$. We thus get (142) in this case also and this shows that the map ev is a hyperfield homomorphism.

For the second statement note that the map ev is a group homomorphism $\mathbb{C}^{\flat\times} \xrightarrow{\mathrm{ev}} \mathbb{C}^\times$ and its kernel is the cyclic group generated by the element $-e(i\pi) \in \mathbb{C}^\flat$. □

7.3.4 Universal W-Model of $\mathbb{C}^\flat$

The hyperfield $\mathbb{C}^\flat$ admits a universal W-model. Given finitely many elements $z_j \in \mathbb{C}$ we denote by $\vee z_j$ the unique largest element for the total order associated to $\mathbb{C}_+$. The following formula defines a homomorphism ρ from the group ring $R = \mathbb{Q}[\mathbb{C}]$ to $\mathbb{C}^\flat$

$$\rho(\sum_1^n a_j \epsilon_j u(z_j)) := \epsilon_k \, e(z_k) \, , \; z_k = \vee z_j \tag{143}$$

which extends to a homomorphism of hyperfields from the field $K = \mathrm{Frac}(R)$ to $\mathbb{C}^\flat$.

Theorem 10. *The triple $(W = K, \rho, \tau_W)$ is the universal W-model for $H = \mathbb{C}^\flat$. The homomorphism ρ induces an isomorphism of hyperfields $W/G \xrightarrow{\sim} \mathbb{C}^\flat$, where $G = \ker(\rho : W^\times \to \mathbb{C}^{\flat\times})$.*

Proof. The proof is similar to the proof of Theorem 2 and is left to the reader. □

7.3.5 The Map $\theta_\mathbb{C}$ and the Ring $\mathbb{C}_\infty$

We proceed as in the real case and construct the universal formal pro-infinitesimal thickening of the field $\mathbb{C}$. Theorem 10 gives not only the field $W(\mathbb{C}^\flat)$ but also the subalgebra $W_\mathbb{Q}(\mathbb{C}^\flat)$ generated by the Teichmüller lifts $[x]$ for $x \in \mathbb{C}^\flat$.

Proposition 15. *There exists a unique ring homomorphism $\theta_\mathbb{C} : W_\mathbb{Q}(\mathbb{C}^\flat) \to \mathbb{C}$ such that ($[\,] = \tau$)*

$$\theta_\mathbb{C}([x]) = \theta_\mathbb{C}(\tau(x)) = \mathrm{ev}(x), \quad \forall x \in \mathbb{C}^\flat. \tag{144}$$

Proof. By construction $W_\mathbb{Q}(\mathbb{C}^\flat)$ is the subalgebra (over $\mathbb{Q}$) generated by the Teichmüller lifts $[x]$ for $x \in \mathbb{C}^\flat$. With $x = \epsilon e(z)$ one has $[x] = \epsilon \, u(z)$ and thus one gets that $W_\mathbb{Q}(\mathbb{C}^\flat) = \mathbb{Q}[\mathbb{C}]$. Thus the natural map $u(z) \mapsto e^z$ extends by linearity and uniquely to a ring homomorphism

$$\theta_\mathbb{C}(\sum_i a_i [x_i]) = \sum_i a_i \mathrm{ev}(x_i) \in \mathbb{C}. \tag{145}$$

□

As in the real case, this suggests to consider the homomorphism $\theta_\mathbb{C} : W_\mathbb{Q}(\mathbb{C}^\flat) \to \mathbb{C}$ of Proposition 15 and introduce the following

Definition 8. The universal formal pro-infinitesimal thickening $\mathbb{C}_\infty$ of $\mathbb{C}$ is the $\mathrm{Ker}(\theta_\mathbb{C})$-adic completion of $W_\mathbb{Q}(\mathbb{C}^\flat)$, i.e.

$$\mathbb{C}_\infty = \varprojlim_n W_\mathbb{Q}(\mathbb{C}^\flat)/\mathrm{Ker}(\theta_\mathbb{C})^n.$$

We shall now proceed as in the real case to show that $\mathrm{Ker}(\theta_{\mathbb{C}})/\mathrm{Ker}(\theta_{\mathbb{C}})^2$ is an infinite dimensional complex vector space. Our main goal will be that to construct explicitly a two dimensional complex space of linear forms on $\mathrm{Ker}(\theta_{\mathbb{C}})/\mathrm{Ker}(\theta_{\mathbb{C}})^2$. We introduce the following vector spaces over $\mathbb{C}$

Definition 9. We let $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C})$ be the complex vector space of all *additive* maps $L : \mathbb{C} \to \mathbb{C}$, and $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C},\mathbb{C}) \subset \mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C})$ the two dimensional subspace of $\mathbb{R}$-linear maps.

One has by definition

$$(a\phi + b\psi)(z) := a\phi(z) + b\psi(z) \in \mathbb{C}\,,\ \forall a,b,z \in \mathbb{C}\,,\ \phi,\psi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C}).$$

Note that $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C},\mathbb{C}) \subset \mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C})$ is also the subspace of additive maps which are measurable and that it is only by the virtue of the axiom of choice that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C})$ is infinite dimensional, while only the elements of the subspace $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C},\mathbb{C})$ can be concretely exhibited. We write the elements of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C},\mathbb{C})$ in the form

$$L(z) = az + b\bar{z}\,,\ \forall z \in \mathbb{C} \tag{146}$$

so that (a,b) are the natural coordinates in this complex vector space.

Lemma 8. (*i*) *Let* $\ell \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C})$*, then the map*

$$\mathscr{T}_\ell(X)(u) := \sum_i a_i e^{z_i + u\ell(z_i)}\,,\ \forall X = \sum_i a_i u(z_i) \in W_{\mathbb{Q}}(\mathbb{C}^\flat) \tag{147}$$

defines a ring homomorphism $\mathscr{T}_\ell : W_{\mathbb{Q}}(\mathbb{C}^\flat) \to \mathscr{E}$ *to the ring of entire functions of the variable* $u \in \mathbb{C}$ *and*

$$\theta_{\mathbb{C}}(X) = \mathscr{T}_\ell(X)(0),\ \forall X \in W_{\mathbb{Q}}(\mathbb{C}^\flat). \tag{148}$$

(*ii*) *Let* $\ell \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{C},\mathbb{C})$*. Then the following formula defines a linear form on* $\mathrm{Ker}(\theta_{\mathbb{C}})/\mathrm{Ker}(\theta_{\mathbb{C}})^2$

$$\mathrm{Ker}(\theta_{\mathbb{C}}) \ni X \mapsto \delta_\ell(X) = \left(\frac{d}{du}\mathscr{T}_\ell(X)(u)\right)_{u=0} \tag{149}$$

Proof. (*i*) For each $u \in \mathbb{C}$ the map $z \mapsto e^{z+u\ell(z)}$ is a group homomorphism from the additive group $\mathbb{C}$ to the multiplicative group $\mathbb{C}^\times$. Thus this map extends to a ring homomorphism from the group ring $W_{\mathbb{Q}}(\mathbb{C}^\flat) = \mathbb{Q}[\mathbb{C}]$ to $\mathbb{C}$. This shows that $\mathscr{T}_\ell$ is a homomorphism to the algebra of functions with pointwise operations. Since $\mathscr{T}_\ell(X)$ is a finite linear combination of exponential functions of u it is an entire function. One checks (148) using the definition (144) of $\theta_{\mathbb{C}}$.

(*ii*) First the right hand side of (149) vanishes when $X \in \mathrm{Ker}(\theta_{\mathbb{C}})^2$ since the entire function $\mathscr{T}_\ell(X)(u)$ admits a zero of order at least two at $u = 0$ as can be seen using (148). This shows that δ_ℓ is well defined. It is clearly additive. Let us show that it is $\mathbb{C}$-linear. For the structure of complex vector space on $W_{\mathbb{Q}}(\mathbb{C}^\flat)/\mathrm{Ker}(\theta_{\mathbb{C}}) = \mathbb{C}$, the multiplication by a complex number $y \in \mathbb{C}$ is provided by the multiplication by any $s \in W_{\mathbb{Q}}(\mathbb{C}^\flat)$ such that $\theta_{\mathbb{C}}(s) = y$. We then have, with $X \in \mathrm{Ker}(\theta_{\mathbb{C}})$, the expansion at $u = 0$

$$\mathscr{T}_\ell(sX)(u) = \mathscr{T}_\ell(s)(u)\mathscr{T}_\ell(X)(u) = \theta_{\mathbb{C}}(s)\delta_\ell(X)u + O(u^2).$$

This shows that δ_ℓ is $\mathbb{C}$-linear. □

7.3.6 The Periods ϵ and π_p

As in Theorem 3 one can use Lemma 8 to show that the "periods" of the form $\pi_p = [e(\log p)] - p$ are linearly independent elements of $\mathrm{Ker}(\theta_{\mathbb{C}})/\mathrm{Ker}(\theta_{\mathbb{C}})^2$. Next, we construct another "period" which is purely complex. We start with the analogue of the element $\epsilon \in F(\mathbb{C}_p)$ of the p-adic Hodge theory. We define in our case

$$\varepsilon := e(2i\pi) \in \mathbb{C}^\flat. \tag{150}$$

The natural square root $\varepsilon^{(2)}$ of ε is $\varepsilon^{(2)} = e(i\pi) \in \mathbb{C}^\flat$ and one has

$$\theta_{\mathbb{C}}([\varepsilon]) = 1, \ \ \omega \in \mathrm{Ker}(\theta_{\mathbb{C}}), \ \omega = ([\varepsilon] - 1)/([\varepsilon^{(2)}] - 1). \tag{151}$$

The last part follows from $\omega = 1 + [\varepsilon^{(2)}]$ and the fact that $e^{i\pi} = -1$. Now that we have these various "periods" we can evaluate on them the natural linear forms δ_ℓ on $\mathrm{Ker}(\theta_{\mathbb{C}})/\mathrm{Ker}(\theta_{\mathbb{C}})^2$ given by elements of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C})$.

Lemma 9. *For $L \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C})$ given by (146) one has*

$$\delta_L(\pi_p) = (a + b)p \log(p), \ \ \delta_L(\omega) = i\pi(b - a). \tag{152}$$

Proof. Let $\ell = L$ with L given by (146). One has

$$\delta_L(\pi_p) = \left(\frac{d}{du}\right)_{u=0} \mathscr{T}_\ell([e(\log p)] - p)(u) = \left(\frac{d}{du}\right)_{u=0} e^{\log p + uL(\log p)} = pL(\log p)$$

which gives $(a + b)p \log(p)$ by (146). Similarly

$$\delta_L(\omega) = \left(\frac{d}{du}\right)_{u=0} \mathscr{T}_\ell(1 + [\varepsilon^{(2)}])(u) = \left(\frac{d}{du}\right)_{u=0} e^{i\pi + uL(i\pi)} = -L(i\pi)$$

which gives $i\pi(b - a)$ by (146). □

Appendix 1

The following table reports the archimedean structures that we have defined and discussed in this paper and their p-adic counterparts (cf. [9]).

p-adic case	Archimedean case
$\mathbb{F}_p$	$\mathrm{sign} = \{-1, 0, 1\}$ hyperfield of signs
$F = F(\mathbb{C}_p)$	$F(\mathbb{R}) = \mathbb{R}^\flat \subset \mathbb{C}^\flat = F(\mathbb{C})$
$\epsilon \in F(\mathbb{C}_p)$	$\varepsilon := e(2i\pi) \in \mathbb{C}^\flat = F(\mathbb{C})$
$\mathscr{O}_F = \varprojlim_{x \mapsto x^p} \mathscr{O}_{\mathbb{C}_p}$	$\mathscr{O} = \varprojlim_{x \mapsto x^\kappa} [-1, 1] \subset \varprojlim_{z \mapsto z^\kappa} \{z, \lvert z\rvert \leq 1\}$
$B^{b,+} = W_{\mathscr{O}_K}(\mathscr{O}_F)[1/\pi]$	$B_\infty^{b,+} = \{f(z) = \int_0^\infty e^{-\xi z} d\mu(\xi) \mid \mu$ finite real measure$\}$
$x = \sum_{n \gg -\infty} [x_n]\pi^n \in B^{b,+}$	$f = \int_{s_0}^\infty [f_s] e^{-s} ds \in B_\infty^{b,+}, f_s \backsim f_t = f_s$ for $s \leq t$
$W_{\mathscr{O}_K}(\mathscr{O}_F) = \{x \in B^{b,+} \mid x = \sum_{n \geq 0} [x_n]\pi^n\}$	$\{f \in B_\infty^{b,+} \mid \lVert f\rVert_0 \leq 1\} = \{f \in B_\infty^{b,+} \mid f = \int_0^\infty [f_s] e^{-s} ds\}$
$\theta : B^{b,+} \to \mathbb{C}_p$	$\theta : B_\infty^{b,+} \to \mathbb{R}, \quad \theta_{\mathbb{C}} : W_{\mathbb{Q}}(\mathbb{C}^\flat) \to \mathbb{C}$
$\varphi(\sum_{n \gg -\infty} [x_n]\pi^n) = \sum_{n \gg -\infty} [x_n^q]\pi^n$	$\mathbf{F}_\lambda(\int_{s_0}^\infty [f_s] e^{-s} ds) = \int_{s_0}^\infty [f_s^\lambda] e^{-s} ds$
$\lvert x\rvert_\rho^\alpha = \max_{\mathbb{Z}} \lvert x_n\rvert^\alpha q^{-n}$	$\lVert f\rVert_\rho = \int_{s_0}^\infty \lvert f_s\rvert^\alpha e^{-s} ds$

Appendix 2

In this appendix we give a short overview of the well-known construction of universal perfection in number theory: we refer to [10], Chap. V, Sect. 1.4; [11, 26], Sect. 2.1; [9], Sect. 2.4 for more details.

The universal perfection is a procedure which associates, in a canonical way, a perfect field $F(L)$ of characteristic p to a p-perfect field L. This construction is particularly relevant when $\mathrm{char}(L) = 0$, since it determines the first step toward the definition of a universal, Galois equivariant cover of L (cf. Appendix 4).

We recall that a field L is said to be p-perfect if it is complete with respect to a non archimedean absolute value $|\ |_L$, L has a residue field of characteristic p and the endomorphism of $\mathscr{O}_L/p\mathscr{O}_L$, $x \to x^p$ is surjective. Furthermore, the field L is said to be strictly p-perfect if $\mathscr{O}_L$ is not a discrete valuation ring.

Starting with a p-perfect field L, one introduces the set

$$F(L) = \{x = (x^{(n)})_{n\in\mathbb{N}} |\ x^{(n)} \in L;\ (x^{(n+1)})^p = x^{(n)}\}. \tag{153}$$

If $x, y \in F(L)$, one sets

$$(x + y)^{(n)} = \lim_{m\to\infty} (x^{(n+m)} + y^{(n+m)})^{p^m}; \qquad (xy)^{(n)} = x^{(n)}y^{(n)}. \tag{154}$$

We recall from [9] (cf. Sect. 2.4) the following result

Proposition 16. *Let L be a p-perfect field. Then $F(L)$ with the above two operations is a perfect field of characteristic p, complete with respect to the absolute value defined by $|x| = |x^{(0)}|_L$. Moreover if $\mathfrak{a} \subset \mathfrak{m}_L$ is a finite type (i.e. principal) ideal of $\mathscr{O}_L$ containing $p\mathscr{O}_L$, then the map reduction mod. $\mathfrak{a}$ induces an isomorphism of topological rings*

$$\mathscr{O}_{F(L)} \xrightarrow{\sim} \varprojlim_{n\in\mathbb{N}} \mathscr{O}_L/\mathfrak{a}, \qquad x = (x^{(n)})_{n\in\mathbb{N}} \mapsto \bar{x} = (x^{(n)} mod.\ \mathfrak{a})_{n\in\mathbb{N}} \tag{155}$$

where the transition maps in the projective limit are given by the ring homomorphism $\bar{x} \to \bar{x}^p$.

In other words, the bijection (155) allows one to transfer (uniquely) the natural (perfect) algebra structure on $\varprojlim_{v\to v^p} \mathscr{O}_L/\mathfrak{a}$ over the inverse limit set $\mathscr{O}_{F(L)} = \varprojlim_{x\mapsto x^p} \mathscr{O}_L$ of p-power compatible sequences $x = (x^{(n)})_{n\geq 0}$, $x^{(n)} \in \mathscr{O}_L$. Indeed, one shows that for any $v = (v_n) \in \varprojlim_{v\to v^p} \mathscr{O}_L/\mathfrak{a}$ and arbitrary lifts $x_n \in \mathscr{O}_L$ of $v_n \in \mathscr{O}_L/\mathfrak{a} \forall n \geq 0$, the limit $x^{(n)} = \lim_{m\to\infty} x_{n+m}^{p^m}$ exists in $\mathscr{O}_L \forall n \geq 0$ and is independent of the choice of the lifts x_n. This lifting process is naturally multiplicative, whereas the additive structure on $\varprojlim_{v\to v^p} \mathscr{O}_L/\mathfrak{a}$ lifts on $\mathscr{O}_{F(L)}$ as (154).

Appendix 3

In this appendix we provide, for completeness, a proof of Proposition 2. We recall that a pro-infinitesimal thickening of a ring R (cf. [12], Sect. 1.1.1 with $\Lambda = \mathbb{Z}$) is a surjective ring homomorphism $\theta : A \to R$, such that the ring A is Hausdorff and complete for the $\mathrm{Ker}(\theta)$-adic topology i.e.

$$A = \varprojlim_n A/\mathrm{Ker}(\theta)^n. \tag{156}$$

As a minor variant, we consider triples (A, θ, τ), where $\theta : A \to R$ is a ring homomorphism with multiplicative section $\tau : R \to A$ and condition (156) holds.

A morphism from the triple (A_1, θ_1, τ_1) to the triple (A_2, θ_2, τ_2) is given by a ring homomorphism $\alpha : A_1 \to A_2$ such that

$$\tau_2 = \alpha \circ \tau_1, \quad \theta_1 = \theta_2 \circ \alpha. \tag{157}$$

Let R be a perfect ring of characteristic p and let $W(R)$ be the p-isotypical Witt ring of R. Let $\rho_R : W(R) \to R$ be the canonical homomorphism and $\tau_R : R \to W(R)$ the multiplicative section given by the Teichmüller lift.

By construction one has $\mathrm{Ker}(\rho_R) = pW(R)$ and condition (156) holds.

We show that for any triple (A, ρ, τ) fulfilling (156), there exists a unique ring homomorphism from $(W(R), \rho_R, \tau_R)$ to (A, ρ, τ) (Compare with Theorem 4.2 of [15] and Theorem 1.2.1 of [12]). The ring A with the sequence of ideals $\mathfrak{a}_n = \mathrm{Ker}(\rho)^n$ fulfills the hypothesis of [22] (II, Sect. 4, Proposition 8). Thus it follows from [22] (II, Sect. 5, Proposition 10) that there exists a (unique) ring homomorphism $\alpha : W(R) \to A$ such that $\rho \circ \alpha = \rho_R$. Moreover the uniqueness of the multiplicative section shown in [22] (II, Sect. 4, Proposition 8) proves that one has $\tau = \alpha \circ \tau_R$. This completes the proof of Proposition 2.

Next we show that the notion of thickening involving a multiplicative section τ is in general different from the classical notion.

Consider $R = \mathbb{Z}$. Then, for any surjective ring homomorphism $\theta : A \to R$, the map $\mathbb{Z} \ni n \mapsto n1_A$ is the unique homomorphism from the pair $(\mathbb{Z}, id)$ to the pair (A, θ). It follows that the pair $(\mathbb{Z}, id)$ is the *universal pro-infinitesimal thickening of* $\mathbb{Z}$. This no longer holds when one involves the multiplicative section τ.

Given a ring R, we consider R-triples (A, ρ, τ) where $\rho : A \to R$ is a ring homomorphism, $\tau : R \to A$ is a multiplicative section (i.e. a morphism of monoids such that $\tau(0) = 0$ and $\tau(1) = 1$) and one also assumes (156). A morphism between two triples is a ring homomorphism $\alpha : A_1 \to A_2$ such that $\rho_1 = \rho_2 \circ \alpha$ and $\tau_2 = \alpha \circ \tau_1$.

Proposition 2 shows that when R is a perfect ring of characteristic p there exists an initial object in the category of R-triples. For $R = \mathbb{Z}$ the triple $(\mathbb{Z}, id, id)$ is a $\mathbb{Z}$-triple but it is not the universal one. The latter is in fact obtained using the ring $\mathbb{Z}[[\{\delta_p\}]] \otimes (\mathbb{Z} \oplus \mathbb{Z}_2 e)$ of formal series with independent generators $\delta_p = [p] - p$,

for each prime p and an additional generator $e = [-1] + 1$ such that $e^2 = 2e$. The augmentation defines a surjection $\epsilon : A \to \mathbb{Z}$, $\rho(e) = 0$, and there exists a unique multiplicative section τ, $\tau(1) = 1$, such that

$$\tau(p) = p + \delta_p\,,\ \forall p \text{ prime},\ \tau(-1) = -1 + e. \tag{158}$$

Proposition 17. *The triple* $(\mathbb{Z}[[\{\delta_p\}]] \otimes (\mathbb{Z} \oplus \mathbb{Z}_2 e), \epsilon, \tau)$ *is the universal* $\mathbb{Z}$*-triple. The map*

$$D : \mathbb{Z} \to \mathrm{Ker}(\epsilon)/\mathrm{Ker}(\epsilon)^2,\ \ D(n) := \tau(n) - n \tag{159}$$

fulfills the Leibnitz rule and its component on δ_p *coincides with the map* $\frac{\partial}{\partial p} : \mathbb{Z} \to \mathbb{Z}$ *defined in [18].*

Proof. By construction one has $\delta_p \in \mathrm{Ker}(\epsilon)$ and thus $\epsilon \circ \tau = id$. Consider first the subring $\mathbb{Z}[\{\delta_p\}][e]$ freely generated by the $\delta_p = [p] - p$ for each prime p and an additional generator $e = [-1] + 1$ such that $e^2 = 2e$. Given a $\mathbb{Z}$-triple (A, ρ, τ), there exists a unique ring homomorphism

$$\alpha : \mathbb{Z}[\{\delta_p\}][e] \to A\,,\ \ \alpha(\delta_p) = \tau(p) - p\,,\ \alpha(e) = \tau(-1) + 1. \tag{160}$$

This ring homomorphism extends uniquely, by continuity, to a homomorphism

$$\alpha : \varprojlim_n \mathbb{Z}[\{\delta_p\}][e]/\mathrm{Ker}(\epsilon)^n \to A = \varprojlim_n A/\mathrm{Ker}(\rho)^n$$

and this shows that $(\mathbb{Z}[[\{\delta_p\}]] \otimes (\mathbb{Z} \oplus \mathbb{Z}_2 e), \epsilon, \tau)$ is the universal $\mathbb{Z}$-triple.

The second assertion follows from [18] (cf. Theorem 1) and the identity

$$[nm] - nm = ([n] - n)m + n([m] - m) + ([n] - n)([m] - m)\,,\ \forall n, m \in \mathbb{Z}.$$

□

Appendix 4

In this appendix we shortly review some relevant constructions in p-adic Hodge theory which lead to the definition of the rings of p-adic periods. The main references are [8, 9].

We fix a non-archimedean locally compact field K of characteristic zero with a *finite* residue field k of characteristic p: $q = |k|$. Let v_K be the (discrete) valuation of K normalized by $v_K(K^*) = \mathbb{Z}$.

Let F be any *perfect* field containing k. We assume that F is complete for a given (non-trivial) absolute value $|\ |$. By $W(F)$ and $W(k)$ we denote the rings of isotypical Witt-vectors.

There exists a *unique* (up-to a unique isomorphism) field extension $\mathfrak{E}_{F,K}$ of K, complete with respect to a *discrete* valuation v extending v_K such that:

- $v(\mathfrak{E}_{F,K}^*) = v_K(K^*) = \mathbb{Z}$
- F is the residue field of $\mathfrak{E}_{F,K}$.

One sees that $\mathfrak{E}_{F,K}$ can be identified with $K \otimes_{W(k)} W(F)$. Thus, if π is a *chosen* uniformizing parameter of K, then an element of $\mathfrak{E}_{F,K}$ can be written *uniquely* as $\mathfrak{e} = \sum_{n \gg -\infty} [a_n]\pi^n$, $a_n \in F$. In particular $\mathfrak{e} \in K$ if and only if $a_n \in k \forall n$.

Let $\mathscr{O}_{\mathfrak{E}_{F,K}}$ be the (discrete) valuation ring of $\mathfrak{E}_{F,K}$. Each element of $\mathscr{O}_{\mathfrak{E}_{F,K}}$ can be written *uniquely* as $\sum_{n \geq 0} [a_n]\pi^n$, $a_n \in F$. The projection map $\mathscr{O}_{\mathfrak{E}_{F,K}} \twoheadrightarrow F$ has a unique multiplicative section i.e. the Teichmüller map $a \mapsto [a] = 1 \otimes (a, 0, 0, \ldots, 0, \ldots)$.

There is a *universal* (local) subring $W_{\mathscr{O}_K}(\mathscr{O}_F) \subset \mathscr{O}_{\mathfrak{E}_{F,K}}$ which describes the *unique* π-adic torsion-free lifting of the perfect $\mathscr{O}_K$-algebra $\mathscr{O}_F$. If K_0 denotes the maximal unramified extension of $\mathbb{Q}_p$ inside K, there is a *canonical* isomorphism:

$$\mathscr{O}_K \otimes_{\mathscr{O}_{K_0}} W(\mathscr{O}_F) \xrightarrow{\sim} W_{\mathscr{O}_K}(\mathscr{O}_F),\ 1 \otimes [a]_F \mapsto [a].$$

If A is any separated and complete π-adic $\mathscr{O}_K$-algebra with field of fractions L and $F = F(L)$ (cf. Appendix 3 for notation), there is a ring homomorphism

$$\theta : W_{\mathscr{O}_K}(\mathscr{O}_{F(L)}) \longrightarrow A, \qquad \sum_{n \geq 0} [x_n]\pi^n \mapsto \sum_{n \geq 0} x_n^{(0)} \pi^n. \tag{161}$$

In the particular case of the algebra $A = \mathscr{O}_F = \mathscr{O}_{F(\mathbf{C}_K)}$ ($\mathbf{C}_K$ = completion of a fixed algebraic closure of K), the surjective ring homomorphism $\theta_0 : \mathscr{O}_F \twoheadrightarrow \mathscr{O}_{\mathbf{C}_K}/(p)$, $\theta_0((x^{(n)})_{n \geq 0}) = x^{(0)}$ lifts to a surjective ring homomorphism of $\mathscr{O}_K$-algebras

$$\theta : W_{\mathscr{O}_K}(\mathscr{O}_{F(\mathbf{C}_K)}) \twoheadrightarrow \mathscr{O}_{\mathbf{C}_K}, \qquad \sum_{n \geq 0} [x_n]\pi^n \mapsto \sum_{n \geq 0} x_n^{(0)} \pi^n \tag{162}$$

which is *independent* of the choice of the uniformizer π.

The valued field $(\mathfrak{E}_{F,K}, |\cdot|)$ ($|\cdot|$ non discrete) contains two further sub-$\mathscr{O}_K$-algebras which are also independent of the choice of a uniformizer $\pi \in \mathscr{O}_K$. They are

$$B^{b,+} := W_{\mathscr{O}_K}(\mathscr{O}_F)[\frac{1}{\pi}] = \{x = \sum_{n \gg -\infty} [x_n]\pi^n \in \mathfrak{E}_{F,K} | x_n \in \mathscr{O}_F, \forall n\} \tag{163}$$

and if $a \in \mathfrak{m}_F \setminus \{0\} \subset \mathscr{O}_F$, the ring $B^b := B^{b,+}[\frac{1}{[a]}]$ which can be equivalently described as

$$B^b = B^b_{F,K} = \{f = \sum_{n \gg -\infty} [x_n]\pi^n \in \mathfrak{E}_{F,K} | \exists C > 0, |x_n| \leq C, \forall n\}. \tag{164}$$

If a p-perfect field L contains K as a closed subfield, the ring homomorphism (161) extends to a surjective homomorphism of K-algebras

$$\theta : B^b_{F(L),K} \to L, \qquad \theta(\sum_{n\gg-\infty}[x_n]\pi^n) = \sum_{n\gg-\infty} x_n^{(0)}\pi^n \tag{165}$$

which is independent of the choice of π. If moreover L is a strictly p-perfect field, then $|F(L)| = |L|$ and the kernel of the map θ in (165) is a prime ideal of $B^b_{F(L),K}$ of degree one. One has

$$\theta(B^{b,+}_{F(L),K}) = L \quad \text{and} \quad \theta(W_{\mathscr{O}_K}(\mathscr{O}_{F(L)})) = \mathscr{O}_L.$$

Let $\mathfrak{E}_0 = \mathfrak{E}_{k_F,K}$. Then the projection $\mathscr{O}_F \to k_F$, $x \to \bar{x}$ induces an augmentation map

$$\varepsilon : B^{b,+} \to \mathfrak{E}_0, \qquad \varepsilon(\sum_{n\gg-\infty}[x_n]\pi^n) = \sum_{n\gg-\infty}[\bar{x}_n]\pi^n \tag{166}$$

with $\varepsilon(W_{\mathscr{O}_K}(\mathscr{O}_F)) = \mathscr{O}_{\mathfrak{E}_0}$. $E = \{\sum_{n\gg-\infty}[x_n]\pi^n |\ x_n \in k_F, \forall n\}$ is a local sub-field of $B^{b,+}$.

One introduces for $r \in \mathbb{R}_{\geq 0}$ the family of valuations on $B^{b,+}$:

$$x = \sum_{n\gg-\infty}[x_n]\pi^n, \qquad v_r(x) = \inf_{n\in\mathbb{Z}}\{v(x_n) + nr\} \in \mathbb{R} \cup \{+\infty\}$$

and defines B^+ as the completion of $B^{b,+}$ for the family of norms $(q^{-v_r})_{r>0}$ ($q = |k|$), $r \in v(F)$.

An equivalent definition of these multiplicative norms is given as follows: for $\mathbb{R} \ni \rho \in [0,1]$ one defines

$$|x|_\rho = \max_{n\in\mathbb{Z}}|x_n|\rho^n \tag{167}$$

$$|x|_0 = q^{-r},\ r \text{ smallest integer}, x_r \neq 0; \qquad |x|_1 = \sup_{n\in\mathbb{Z}}|x_n|.$$

In view of the description of B^b given in (164), the norms (167) are well-defined on the larger ring B^b. The completion B of B^b for these norms, as $\rho \in (0,1)$, contains $B^+[\frac{1}{[a]}]$ for any chosen $a \in \mathfrak{m}_F \setminus \{0\}$.

B is the analogue in mixed characteristics of the ring of rigid analytic functions on the punctured unit disk in equal characteristics.

The subalgebra $B^+ \subset B$ is characterized by the condition

$$B^+ = \{b \in B \mid |b|_1 \leq 1\}. \tag{168}$$

The extension of rings $B^+ \subset B^+[\frac{1}{[a]}]$ gives a perfect control of the divisibility as explained in [8], Theorem 6.55. A remarkable property of this construction is that the Frobenius endomorphism on $B^{b,+}$

$$\varphi : B^{b,+} \to B^{b,+}, \quad \varphi(\sum_{n \gg -\infty} [x_n]\pi^n) = \sum_{n \gg -\infty} [x_n^q]\pi^n$$

extends to a Frobenius *automorphism* on B^b and on B^+ thus to a *continuous* Frobenius *automorphism* $\varphi : B \xrightarrow{\sim} B$ (i.e. the unique K-automorphism which induces $x \mapsto x^q$ on F) which satisfies $|\varphi(f)|_{\rho^q} = (|f|_\rho)^q$, $\forall \rho \in (0,1)$.

The homomorphism (165) (in particular for $L = \mathbf{C}_K$) extends to a *canonical continuous* universal (Galois equivariant) cover of L

$$\theta : B \twoheadrightarrow L.$$

Appendix 5

In this appendix we explain the connection of the above construction with the archimedean analogue of the Witt construction in the framework of perfect semirings of characteristic one [3, 5]. Given a multiplicative cancellative perfect semiring R of characteristic 1, one keeps the same multiplication but deforms the addition into the following operation

$$x +_w y = \sum_{\alpha \in I} w(\alpha) x^\alpha y^{1-\alpha}\,, \ I = (0,1) \cap \mathbb{Q}, \tag{169}$$

which is commutative provided $w(1-\alpha) = w(\alpha)$, $\forall \alpha \in I$, and associative provided that the following equation holds

$$w(\alpha)w(\beta)^\alpha = w(\alpha\beta)w(\gamma)^{(1-\alpha\beta)}\,, \ \ \gamma = \frac{\alpha(1-\beta)}{1-\alpha\beta} \qquad \forall \alpha, \beta \in I. \tag{170}$$

By applying Theorem 5.4 in [3], one sees that the positive symmetric solutions to (170) are parameterized by $\rho \in R$, $\rho > 1$, and they are given by the following formula involving the entropy S,

$$w(\alpha) = \rho^{S(\alpha)}, \qquad S(\alpha) = -\alpha \log(\alpha) - (1-\alpha)\log(1-\alpha)\,, \ \forall \alpha \in I. \tag{171}$$

We apply this result to the semi-field $\mathbb{R}_+^{\max}$ of tropical geometry. We write the elements $\rho \in \mathbb{R}_+^{\max}$, $\rho > 1$, in the convenient form $\rho = e^T$ for some $T > 0$. In this way, we can view $w(\alpha)$ as the function of T given by

$$w_T(\alpha) = w(\alpha, T) = e^{TS(\alpha)} \qquad \forall \alpha \in I\,. \tag{172}$$

By performing a direct computation one obtains for $x, y > 0$ that the perturbed sum $x +_{w_T} y$ is given by

$$x +_{w_T} y = \left(x^{1/T} + y^{1/T}\right)^T . \tag{173}$$

The formula (173) shows that the sum of two elements of $\mathbb{R}_+^{\max}$, computed by using w_T, is a function which depends explicitly on the variable T. The functions $[x](T) = x$ (for $x \in \mathbb{R}_+^{\max}$) which are constant in T describe the Teichmüller lifts. The sum of such functions is no longer constant in T. In particular one can compute the sum of n constant functions all equal to 1:

$$1 +_{w_T} 1 +_{w_T} \cdots +_{w_T} 1 = n^T \tag{174}$$

which shows that the sum of n terms equal to the unit of the structure is given by the function of the variable T: $T \mapsto n^T$.

Proposition 18. *The following map χ is a homomorphism from the semi-ring R generated by the functions $T \mapsto \alpha^T$, $\alpha \in \mathbb{Q}_+$, and the Teichmüller lifts to the algebra of real-valued functions from $(0, \infty)$ to $\mathbb{R}_+$ with pointwise sum and product*

$$\chi(f)(T) = f(T)^{1/T} , \ \forall T > 0. \tag{175}$$

The range of the map χ is the semi-ring of finite linear combinations, with positive rational coefficients, of Teichmüller lifts of elements $x \in \mathbb{R}_+^{\max}$ given in the χ-representation by

$$\chi([x])(T) = x^{1/T} , \ \forall T > 0 , \ \forall x \in \mathbb{R}_+^{\max} \tag{176}$$

The following defines a homomorphism from R to $W_{\mathbb{Q}}(\mathbb{R}^{\flat})$,

$$f \mapsto \beta(f), \ \ \beta(f)(z) = \chi(f)(\frac{1}{z}) . \tag{177}$$

Proof. The proof is straightforward using [3]. □

Thus (177) gives the translation from the framework of [3, 5] to the framework of the present paper.

Acknowledgements The second author was partially supported by the NSF grant DMS 1069218 and would like to thank the Collège de France for some financial support.

References

1. L. Berger, An introduction to the theory of p-adic representations, in *Geometric Aspects of Dwork Theory*, vols. I, II (Walter de Gruyter GmbH Co. KG, Berlin, 2004), pp. 255–292
2. M. Berry, Stokes' phenomenon, smoothing a Victorian discontinuity. IHES Publ. **68**, 211–221 (1989)
3. A. Connes, The Witt construction in characteristic one and quantization, in *Noncommutative Geometry and Global Analysis*. Contemporary Mathematics, vol. 546 (American Mathematical Society, Providence, 2011) pp. 83–113
4. A. Connes, C. Consani, The hyperring of adèle classes. J. Number Theory **131**, 159–194 (2011)
5. A. Connes, C. Consani, Characteristic one, entropy and the absolute point, in *Noncommutative Geometry, Arithmetic, and Related Topics*. The Twenty-First Meeting of the Japan-US Mathematics Institute, Baltimore 2009 (Johns Hopkins University Press, Baltimore, 2012), pp. 75–139
6. A. Connes, C. Consani, The arithmetic site. C. R. Math. Ser. I **352**, 971–975 (2014)
7. R.B. Dingle, *Asymptotic Expansions: Their Derivation and Interpretation* (Academic, New York/London, 1973)
8. L. Fargues, J.-M. Fontaine, *Courbes et Fibrés Vectoriels en Théorie de Hodge p-Adique*. Preprint (2011)
9. L. Fargues, J.-M. Fontaine, Vector bundles and p-adic Galois representations. AMS/IP Stud. Adv. Math. **51**, 77–113 (2011)
10. J.-M. Fontaine, *Groupes p-Divisibles sur les Corps Locaux*. Asterisque, vol. 47–48 (Sociéte Mathematique de France, Paris, 1977)
11. J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate. Ann. Math. **115**, 529–577 (1982)
12. J.-M. Fontaine, Le corps des périodes p-adiques. Asterisque **223**, 59–111 (1994) [With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988)]
13. J.-M. Fontaine, Arithmétique des représentations galoisiennes p-adiques. Asterisque **295**, 1–115 (2004)
14. H. Glaeske, A. Prudnikov, K. Skornik, *Operational Calculus and Related Topics*. Analytical Methods and Special Functions, vol. 10 (Chapman Hall/CRC, Boca Raton, 2006)
15. A. Grothendieck, *Groupes de Barsotti-Tate et cristaux de Dieudonné*. Séminaire de Mathématiques Supérieures, vol. 45 (Été, 1970) (Les Presses de l'Université de Montréal, Montreal, 1974), 155 pp.
16. M. Kontsevich, *The* $1\frac{1}{2}$*-Logarithm* (Friedrich Hirzebruchs Emeritierung, Bonn, 1995)
17. M. Krasner, Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique 0 (French), in *Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956* (Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris, 1957), pp. 129–206
18. N. Kurokawa, H. Ochiai, M. Wakayama, Absolute derivations and zeta functions, in *Kazuya Kato's Fiftieth Birthday*. Documenta Mathematica, Extra Volume (2003), pp. 565–584
19. J.L. Lions, Supports de produits de composition, I (French). C. R. Acad. Sci. Paris **232**, 1530–1532 (1951)
20. G. Litvinov, Tropical mathematics, idempotent analysis, classical mechanics and geometry, in *Spectral Theory and Geometric Analysis*. Contemporary Mathematics, vol. 535 (American Mathematical Society, Providence, 2011), pp. 159–186
21. W. Rudin, *Real and Complex Analysis* (McGraw-Hill, New York, 1987)
22. J.P. Serre, *Corps Locaux* (French), Deuxième édn. (Publications de l'Université de Nancago, No. VIII (Hermann, Paris, 1968), 245 pp.

23. G.G. Stokes, On the critical values of the sums of periodic series. Trans. Camb. Phil. Soc. **8**, 533–610 (1847) [Reprinted in Mathematical and Physical Papers (ref. [4]), vol. I, pp. 236–313]
24. E.C. Titchmarsh, The zeros of certain integral functions. Proc. Lond. Math. Soc. **25**, 283–302 (1926)
25. O. Viro, *Hyperfields for Tropical Geometry I, Hyperfields and Dequantization* (2010)
26. J.P. Wintenberger, Le corps des normes de certaines extensions infinies de corps locaux; applications. Ann. Sci. École Norm. Sup. (4) **16**(1), 59–89 (1983)

Moments of Zeta and Correlations of Divisor-Sums: II

Brian Conrey and Jonathan P. Keating

Abstract This is Part II of our examination of the second and fourth moments and shifted moments of the Riemann zeta-function on the critical line using long Dirichlet polynomials and divisor correlations.

1 Introduction

In part I, see [2], we completed the analysis of the second moment of the Riemann zeta-function using the long Dirichlet polynomial method of Goldston and Gonek [3] and we initiated the study of the fourth moment by this approach. In particular we calculated the contributions from the off-diagonal terms arising from coefficient correlations of the form $\sum_{n\le X} d(n)d(n+h)$ and identified the terms that are missed in this approach. In this paper we show how to evaluate these new terms that were missing and in doing so we introduce a new technique that is a discrete analog of the circle method. This analysis gives a concrete introduction to how we will approach higher moments through this circle method approach. In a subsequent paper we will show how to obtain the "full-moment" conjecture for the $2k$th moment of $\zeta(s)$ on the critical line, i.e. the full polynomial of degree k^2 which comprises the main term. The idea for this method originates in the work of Bogomolny and Keating; see [1].

Thus, we will calculate the contribution of what we call the type II sums (after [1]) which arise in the evaluation of

$$\int_0^\infty \psi\left(\frac{t}{T}\right) \sum_{m\le X} \frac{\tau_{\alpha,\beta}(m)}{m^s} \sum_{n\le X} \frac{\tau_{\gamma,\delta}(n)}{n^{1-s}}\, dt$$

B. Conrey (✉)
American Institute of Mathematics, 360 Portage Ave, Palo Alto, CA 94306, USA

School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
e-mail: conrey@aimath.org

J.P. Keating
School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
e-mail: j.p.keating@bristol.ac.uk

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_3

where $s = 1/2 + it$ and $\tau_{\alpha,\beta}(n) = \sum_{de=n} d^{-\alpha} e^{-\beta}$. (See [2] for further notation and introduction.) To describe the type II sums we observe that integrating term-by-term we find that the above is

$$T \sum_{m,n \le X} \frac{\tau_{\alpha,\beta}(m)\tau_{\gamma,\delta}(n)}{\sqrt{mn}} \hat{\psi}\left(\frac{T}{2\pi} \log(m/n)\right) = T\mathscr{D} + T\mathscr{O} + \mathscr{E}$$

where $\mathscr{D}$ is the diagonal

$$\mathscr{D} = \hat{\psi}(0) \sum_{n \le X} \frac{\tau_{\alpha,\beta}(n)\tau_{\gamma,\delta}(n)}{n};$$

$\mathscr{O}$ is the off-diagonal

$$\mathscr{O} = \sum_{\substack{m \ne n \\ 0 < |m-n| < m/\tau}} \frac{\tau_{\alpha,\beta}(m)\tau_{\gamma,\delta}(n)}{\sqrt{mn}} \hat{\psi}\left(\frac{T}{2\pi} \log(m/n)\right);$$

and $\mathscr{E} \ll T^{\epsilon}$ is an error term; here $\tau = T^{1-\epsilon}$ and the Fourier transform is defined by

$$\hat{\psi}(v) = \int_{\mathbb{R}} \psi(u) e(uv)\, du$$

where $e(x) = \exp(2\pi i x)$.

If we evaluate $\mathscr{O}$ here in the traditional manner, e.g., as in [3], we would now solve the shifted convolution problem which consists of evaluating

$$\sum_{n \le x} \tau_{\alpha,\beta}(n)\tau_{\gamma,\delta}(n+h)$$

and summing by parts. This analysis was carried out in I. Here we use a new approach. We first make use of the fact that $\tau_{\alpha,\beta}$ and $\tau_{\gamma,\delta}$ are convolutions to write

$$\mathscr{O} = \sum_{\substack{m_1 m_2, n_1 n_2 \le X \\ 0 < |m_1 m_2 - n_1 n_2| < m_1 m_2/\tau}} \frac{m_1^{-\alpha} m_2^{-\beta} n_1^{-\gamma} n_2^{-\delta}}{m_1 m_2} \hat{\psi}\left(\frac{T}{2\pi} \log((n_1 n_2)/(m_1 m_2)\right).$$

Now we embark on a discrete analog of the circle method which basically consists of approximating a ratio, say m_1/n_1, by a rational number with a small denominator, say M/N, and then summing all of the terms with m_1/n_1 close to M/N; finally we sum over M and N.

To this end we introduce a parameter Q and subdivide the interval $[0, 1]$ into Farey intervals associated with the fractions M/N with $1 \le M \le N \le Q$ and $(M, N) = 1$ from the Farey sequence $\mathscr{F}_Q$. The Farey interval $\mathscr{M}_{M,N}$ determined by the fraction M/N is defined to be

$$\mathscr{M}_{M,N} = \left[\frac{M}{N} - \frac{M+M''}{N+N''}, \frac{M}{N} + \frac{M+M'}{N+N'}\right)$$

where $\frac{M''}{N''}, \frac{M}{N}, \frac{M'}{N'}$ are three consecutive terms in the Farey sequence $\mathscr{F}_Q$. Now given such an M and N we sum over the terms m_1 and n_1 for which $m_1/n_1 \in \mathscr{M}_{M,N}$; for such a pair we define

$$h_1 := m_1 N - n_1 M.$$

The possible range of h_1 may be computed by

$$|h_1| = \left|\frac{m_1}{n_1} - \frac{M}{N}\right| n_1 N \leq \left(\frac{M}{N} - \frac{M+M''}{N+N''}\right) n_1 N = \frac{n_1}{N+N''} \approx \frac{n_1}{Q}$$

since adjacent denominators satisfy $Q < N + N'' < 2Q$. In general, the rapid decay of $\hat{\psi}$ governs the range of h_1 and h_2 defined below.

Also, we note that if Q is not too large then $m_1/n_1 \in \mathscr{M}_{M,N}$ implies that $n_2/m_2 \in \mathscr{M}_{M,N}$ as well. This is because the distance from m_1/n_1 to n_2/m_2 is

$$\left|\frac{m_1}{n_1} - \frac{n_2}{m_2}\right| = \frac{|m_1 m_2 - n_1 n_2|}{n_1 m_2} \leq \frac{m_1 m_2}{\tau n_1 m_2} \leq \frac{1}{\tau}.$$

On the other hand

$$\left|\frac{M}{N} - \frac{M'}{N'}\right| \gg \frac{1}{Q^2}$$

so if $Q^2 = o(\tau)$ then our assertion follows.

Now we define

$$h_2 := m_2 M - n_2 N.$$

We have

$$m_1 m_2 MN - n_1 n_2 MN = h_1 m_2 M + h_2 m_1 N - h_1 h_2$$

so that

$$\frac{m_1 m_2 - n_1 n_2}{m_1 m_2} = \frac{h_1}{m_1 N} + \frac{h_2}{m_2 M} - \frac{h_1 h_2}{m_1 m_2 MN}$$

and

$$\log \frac{n_1 n_2}{m_1 m_2} = \frac{h_1}{m_1 N} + \frac{h_2}{m_2 M} + O\left(\frac{h_1 h_2}{m_1 m_2 MN}\right).$$

The error term is negligible so we have now arranged the sum as

$$\sum_{\substack{M\le N\le Q\\(M,N)=1}}\sum_{h_1,h_2}\sum_{\substack{m_1m_2\le X\\(*_1),(*_2)}}\frac{m_1^{-\alpha}m_2^{-\beta}n_1^{-\gamma}n_2^{-\delta}}{m_1m_2}\hat{\psi}\left(\frac{Th_1}{2\pi m_1N}+\frac{Th_2}{2\pi m_2M}\right)$$

where

$$(*_1): m_1N-n_1M=h_1 \qquad \text{and} \qquad (*_2): m_2M-n_2N=h_2$$

Note that for a given m_1, n_1 and h_1 the condition $(*_1)$ implies that $m_1/n_1 \in \mathscr{M}_{M,N}$ so we don't need to write that condition.

2 Smoothing the Sums over M and N

We introduce another smooth weight function $\phi(y)$, which is an approximation to the characteristic function $\chi_{(0,1]}(y)$ to help with the summation over M and N. In the next section we will encounter sums of the form

$$S_Q(\xi,\eta):=\sum_{\substack{1\le M\le N\\(M,N)=1}}\phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right)M^{-1-\xi}N^{-1-\eta}$$

for a finite set of choices of ξ and η which are of the form

$$\epsilon_1\alpha+\epsilon_2\beta+\epsilon_3\gamma+\epsilon_4\delta$$

where the $\epsilon_i \in \{-1,0,1\}$. For our weight function ϕ we require that

$$\phi(y)=\frac{1}{2\pi i}\int_{(1)}\tilde{\phi}(s)y^{-s}\,ds$$

where $\tilde{\phi}(s)$ has the properties that

$$\operatorname*{Res}_{s=0}\tilde{\phi}(s)=1 \qquad \text{and} \qquad \tilde{\phi}(\xi)=0$$

for all of the eligible values of ξ that arise, and that $\tilde{\phi}(s)$ is analytic in $\Re s \ge -1/2$ and has rapid decay vertically in this region. In practice $S_Q(\xi,\eta)$ will be combined with $S_Q(\eta,\xi)$ to obtain

$$S_Q(\xi,\eta)+S_Q(\eta,\xi)=\phi\left(\frac{1}{Q}\right)^2+\sum_{(M,N)=1}\phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right)M^{-1-\xi}N^{-1-\eta}$$

The second term is

$$\sum_d \frac{\mu(d)}{d^{2+\xi+\eta}} \sum_M \phi\left(\frac{Md}{Q}\right) M^{-1-\xi} \sum_N \phi\left(\frac{Nd}{Q}\right) N^{-1-\eta}$$
$$= \sum_d \frac{\mu(d)}{d^{2+\xi+\eta}} \left(\frac{1}{2\pi i}\int_{(1)} \tilde{\phi}(w)\zeta(w+1+\xi)\left(\frac{Q}{d}\right)^w dw\right)$$
$$\times\left(\frac{1}{2\pi i}\int_{(1)} \tilde{\phi}(z)\zeta(z+1+\eta)\left(\frac{Q}{d}\right)^z dz\right).$$

The first integral is $= \zeta(1+\xi) + O((Q/d)^{-1/3})$ as can be seen by moving the path of integration to the left to $\Re w = -1/3$ and accounting for the residue at the pole $w = 0$; note that since $\tilde{\phi}(-\xi) = 0$, there is no pole at $w = -\xi$. Thus, altogether we have

$$S_Q(\xi,\eta) + S_Q(\eta,\xi) = \phi\left(\frac{1}{Q}\right)^2 + \frac{\zeta(1+\xi)\zeta(1+\eta)}{\zeta(2+\xi+\eta)} + O(Q^{-1/3}). \tag{1}$$

3 The Case of $h_2 = 0$

We remark first of all that the terms with $h_1 = h_2 = 0$ are precisely the diagonal terms. Now we consider what happens if $h_2 = 0$ and $h_1 \neq 0$. We call this a "semi-diagonal" term after [1].

If $h_2 = 0$ then $m_2 M = n_2 N$. Since $(M,N) = 1$ it follows that $m_2 = N\ell$ and $n_2 = M\ell$ for some ℓ. Thus we have

$$\sum_{\substack{M\leq N\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) \sum_{h_1} \sum_{\substack{m_1,n_1,\ell\\(*_1)\\n_1\geq|h_1|Q}} \frac{m_1^{-\alpha}(N\ell)^{-\beta}n_1^{-\gamma}(M\ell)^{-\delta}}{m_1 m_2} \hat{\psi}\left(\frac{Th_1}{2\pi m_1 N}\right)$$

where

$$(*_1) : m_1 N - n_1 M = h_1.$$

We replace m_1 by a smooth variable u_1 and n_1 by $m_1 N/M$. We have $u_1 \ell N = m_1 m_2 \leq X$ and so our sum is

$$\sum_{\substack{M\leq N\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) M^{-\delta+\gamma-1} N^{-\beta-\gamma-1}$$
$$\times \sum_{h_1}\sum_{\ell} \ell^{-1-\beta-\delta} \int_{u_1\ell\leq\frac{X}{N}} u_1^{-1-\alpha-\gamma} \hat{\psi}\left(\frac{Th_1}{2\pi u_1 N}\right) du_1.$$

We save the term with $h_1 = 0$ for later and we group the terms with h_1 and $-h_1$ together and use $\hat{\psi}(-v) = \overline{\hat{\psi}(v)}$. We make the substitution $v_1 = \frac{Th_1}{2\pi u_1 N}$ in the integral and switch the integral over v_1 with the sum over h_1 and ℓ. Then (with $h_1 > 0$) we have that

$$\frac{\ell N T h_1}{2\pi v_1 N} = u_1 \ell N \le X$$

implies that

$$\ell h_1 \le \frac{2\pi X v_1}{T}.$$

Thus we have

$$\sum_{\substack{M\le N\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) M^{-\delta+\gamma-1} N^{\alpha-\beta-1} \int_0^\infty v_1^{-1+\alpha+\gamma} (2\Re\hat{\psi}(v_1))$$
$$\times \sum_{h_1\ell \le \frac{2\pi X v_1}{T}} h_1^{-\alpha-\gamma} \ell^{-1-\beta-\delta}\, dv_1.$$

The sum over h_1 and ℓ is

$$\frac{1}{2\pi i}\int_{(2)} \zeta(s+1+\beta+\delta)\zeta(s+\alpha+\gamma)\left(\frac{2\pi v_1 X}{T}\right)^s \frac{ds}{s}$$

Together with the integral over v_1 this is

$$\int_0^\infty v_1^{-1+\alpha+\gamma}\hat{\psi}(v_1)\frac{2}{2\pi i}\int_{(2)} \zeta(s+1+\beta+\delta)\zeta(s+\alpha+\gamma)\left(\frac{2\pi v_1 X}{T}\right)^s \frac{ds}{s}\, dv_1.$$

Now, as we've seen before, if $\Re s > 0$ then

$$\int_0^\infty (2\Re\hat{\psi}(v)) v^s\, dv = \chi(1-s)\int_0^\infty \psi(t) t^{-s}\, dt.$$

Thus, the above is

$$\int_0^\infty t^{-1-\alpha-\gamma}\psi(t)\frac{2}{2\pi i}\int_{(2)} \zeta(s+1+\beta+\delta)\zeta(1-s-\alpha-\gamma)\left(\frac{2\pi X}{tT}\right)^s \frac{ds}{s}\, dt$$

We move the s-path left to $\Re s = -1/2$, thus crossing the poles at $s = 0$, $s = -\alpha-\gamma$ and $s = -\beta-\delta$. Thus the above is

$$\int_0^\infty t^{-1-\alpha-\gamma}\psi(t)\Bigg(\zeta(1+\beta+\delta)\zeta(1-\alpha-\gamma)-\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\left(\frac{2\pi X}{tT}\right)^{-\beta-\delta}}{\beta+\delta}$$
$$+\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\left(\frac{2\pi X}{tT}\right)^{-\alpha-\gamma}}{\alpha+\gamma}\Bigg)\,dt$$

and altogether we have

$$\sum_{\substack{M\le N\\(M,N)=1}}\phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right)M^{-\delta+\gamma-1}N^{\alpha-\beta-1}$$
$$\times\int_0^\infty t^{-1-\alpha-\gamma}\psi(t)\Bigg(\zeta(1+\beta+\delta)\zeta(1-\alpha-\gamma)$$
$$-\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\left(\frac{2\pi X}{tT}\right)^{-\beta-\delta}}{\beta+\delta}+\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\left(\frac{2\pi X}{tT}\right)^{-\alpha-\gamma}}{\alpha+\gamma}\Bigg)\,dt$$

All of the above is predicated on $m_1/n_1 < 1$. The contribution from the terms where $n_1 < m_1$ will be exactly as above but with the quadruple $(\alpha,\beta,\gamma,\delta)$ replaced with $(\gamma,\delta,\alpha,\beta)$. In particular, $\alpha+\gamma$ will be replaced by $\beta+\gamma$ prior to summing over M and N. This will give another term

$$\sum_{\substack{M\le N\\(M,N)=1}}\phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right)M^{\alpha-\beta-1}N^{-\delta+\gamma-1}$$
$$\times\int_0^\infty t^{-1-\beta-\delta}\psi(t)\Bigg(\zeta(1+\beta+\delta)\zeta(1-\alpha-\gamma)$$
$$-\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\left(\frac{2\pi X}{tT}\right)^{-\beta-\delta}}{\beta+\delta}+\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\left(\frac{2\pi X}{tT}\right)^{-\alpha-\gamma}}{\alpha+\gamma}\Bigg)\,dt$$

Now we consider what happens when $h_1 = 0$ and $h_2 \neq 0$. These terms will contribute the "complements" to the above two expressions so that we will be in the situation described in (1) and so we can execute the sums over M and N as described there, replacing the sums over M and N by ratios of zeta functions with small error terms. Thus, we obtain

$$\int_0^\infty t^{-1-\alpha-\gamma}\psi(t)\Bigg(\frac{\zeta(1+\beta+\delta)\zeta(1-\alpha-\gamma)\zeta(1-\gamma+\delta)\zeta(1-\alpha+\beta)}{\zeta(2-\alpha+\beta-\gamma+\delta)}$$
$$-\left(\frac{2\pi X}{tT}\right)^{-\beta-\delta}\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\zeta(1-\alpha+\beta)\zeta(1-\gamma+\delta)}{(\beta+\delta)\,\zeta(2-\alpha+\beta-\gamma+\delta)}$$
$$+\left(\frac{2\pi X}{tT}\right)^{-\alpha-\gamma}\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\zeta(1-\alpha+\beta)\zeta(1-\gamma+\delta)}{(\alpha+\gamma)\,\zeta(2-\alpha+\beta-\gamma+\delta)}\Bigg)\,dt$$

and the complementary term with $\alpha+\gamma$ replaced by $\beta+\delta$ and vice-versa.

This is identical with one of the one-swap terms identified by descending as previously described.

There are further semi-diagonal terms. If we do the exact same analysis as throughout this entire section but now focusing on the ratio m_1/n_2 instead of m_1/n_1 then the effect will be to switch the roles of γ and δ in the expression above. Then we end up with two more terms and a total of four terms. These terms are identical with the four terms obtained by the "descent" method described in Sect. 8 of Conrey and Keating [2].

A question of whether we have over-counted some terms may arise. But the "duplicate" terms for which $m_1/n_1 \in \mathscr{M}_{M,N}$ and simultaneously $m_1/n_2 \in \mathscr{M}_{M',N'}$ with $N \le Q$ and $N' \le Q$ contribute an insignificant amount to the total and so may be regarded as part of the error term.

4 The Case of $h_1h_2 \neq 0$

Now we consider

$$\sum_{\substack{M\le N\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) \sum_{h_1h_2\neq 0} \sum_{\substack{m_1m_2\le X\\(*_1),(*_2)}} \frac{m_1^{-\alpha}m_2^{-\beta}n_1^{-\gamma}n_2^{-\delta}}{m_1m_2}\hat{\psi}\left(\frac{Th_1}{2\pi m_1N}+\frac{Th_2}{2\pi m_2M}\right).$$

In this case we have a bound for h_2 similar to that for h_1:

$$|h_2| \ll \frac{m_2}{Q} \ll \frac{n_2M}{QN}.$$

In particular, we have

$$|h_1h_2| \ll \frac{n_1n_2M}{Q^2N} \ll \frac{X}{Q^2}.$$

Now we replace the sums over m_1, m_2, n_1, n_2 subject to $(*_1)$ and $(*_2)$ by their averages. As before, we replace m_1 by u_1 and now we replace m_2 by u_2. We replace n_1 and n_2 by u_1N/M and u_2M/N respectively. We then have

$$\sum_{\substack{M\le N\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) M^{\gamma-\delta-1}N^{\delta-\gamma-1}$$

$$\times \sum_{h_1h_2\neq 0} \int_{u_1u_2\le X} u_1^{-\alpha-\gamma-1}u_2^{-\beta-\delta-1}\hat{\psi}\left(\frac{Th_1}{2\pi u_1N}+\frac{Th_2}{2\pi u_2M}\right)du_1\,du_2.$$

Now there are four cases to consider according to the four sign choices of h_1 and h_2. We make the substitutions

$$v_1 = \frac{T|h_1|}{2\pi u_1 N} \qquad \text{and} \qquad v_2 = \frac{T|h_2|}{2\pi u_2 M}$$

and move the sums over h_1 and h_2 to the inside. The condition $u_1 u_2 \le X$ implies that

$$\frac{T^2|h_1 h_2|}{4\pi^2 v_1 v_2 MN} = u_1 u_2 \le X$$

or

$$|h_1 h_2| \le \frac{4\pi^2 XMN v_1 v_2}{T^2}.$$

We get

$$\left(\frac{T}{2\pi}\right)^{-\alpha-\beta-\gamma-\delta} \sum_{\substack{M\le N\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) M^{\gamma+\beta-1} N^{\delta+\alpha-1}$$

$$\times \iint_{v_1,v_2} v_1^{\alpha+\gamma-1} v_2^{\beta+\delta-1} \sum_{0<|h_1h_2|\le \frac{4\pi^2 XMN v_1 v_2}{T^2}} h_1^{-\alpha-\gamma} h_2^{-\beta-\delta}$$

$$\times \Big(\hat\psi(v_1+v_2) + \hat\psi(v_1-v_2) + \hat\psi(-v_1+v_2) + \hat\psi(-v_1-v_2)\Big)\, dv_1\, dv_2.$$

Using

$$\hat\psi(v_1+v_2) = \int_0^\infty \psi(t) e(t(v_1+v_2))\, dt$$

we see that

$$\hat\psi(v_1+v_2) + \hat\psi(v_1-v_2) + \hat\psi(-v_1+v_2) + \hat\psi(-v_1-v_2)$$
$$= \int_0^\infty \psi(t)\big(e(tv_1)+e(-tv_1)\big)\big(e(tv_2)+e(-tv_2)\big)\, dt;$$

Also

$$\sum_{h_1h_2\le \frac{4\pi^2 XMN v_1 v_2}{T^2}} h_1^{-\alpha-\gamma} h_2^{-\beta-\delta} = \frac{1}{2\pi i}\int_{(2)} \zeta(s+\alpha+\gamma)\zeta(s+\beta+\delta) \frac{\left(\frac{4\pi^2 XMN v_1 v_2}{T^2}\right)^s}{s}\, ds$$

and

$$\int_0^\infty v_1^{s+\alpha+\gamma-1}(e(tv_1)+e(-tv_1))\, dv_1 = t^{-s-\alpha-\gamma}\chi(1-s-\alpha-\gamma),$$

and similarly for the integral over v_2. Incorporating these, we have simplified things to

$$\left(\frac{T}{2\pi}\right)^{-\alpha-\beta-\gamma-\delta} \sum_{\substack{M\le N\le Q\\(M,N)=1}} \phi\left(\frac{M}{Q}\right)\phi\left(\frac{N}{Q}\right) M^{\gamma+\beta-1}N^{\delta+\alpha-1}$$

$$\times \int_0^\infty \psi(t)t^{-\alpha-\beta-\gamma-\delta}\frac{1}{2\pi i}\int_{(2)} \zeta(1-s-\alpha-\gamma)\zeta(1-s-\beta-\delta)\frac{(\frac{4\pi^2XMN}{t^2T^2})^s}{s}\,ds\,dt.$$

The above expression is unchanged if (α,γ) is interchanged with (β,δ). So the result of summing terms for which $n_1/m_1 \le 1$ rather than $m_1/n_1 \le 1$ allows for summing over M and N as in Sect. 9; we obtain

$$\left(\frac{T}{2\pi}\right)^{-\alpha-\beta-\gamma-\delta}\frac{1}{(2\pi i)^2}\int_{z,w}\tilde{\phi}(z)\tilde{\phi}(w)\frac{\zeta(1-\beta-\gamma-s+z)\zeta(1-\alpha-\delta-s+w)}{\zeta(2-\alpha-\beta-\gamma-\delta-2s+z+w)}$$
$$\times\int_0^\infty \psi(t)t^{-\alpha-\beta-\gamma-\delta}\frac{1}{2\pi i}\int_{(2)}\zeta(1-s-\alpha-\gamma)\zeta(1-s-\beta-\delta)$$
$$\times\frac{(\frac{X}{t^2T^2})^sQ^{z+w}}{s}\,ds\,dw\,dz\,dt.$$

Moving the s-path to the right to ∞ and the z and w paths to the left to $-1/4$, say we obtain

$$\int_0^\infty \psi(t)\Bigg(\left(\frac{tT}{2\pi}\right)^{-\alpha-\beta-\gamma-\delta}\frac{\zeta(1-\alpha-\gamma)\zeta(1-\beta-\delta)\zeta(1-\beta-\gamma)\zeta(1-\alpha-\delta)}{\zeta(2-\alpha-\beta-\gamma-\delta)}$$
$$+X^{-\alpha-\gamma}\left(\frac{tT}{2\pi}\right)^{\alpha-\beta+\gamma-\delta}\frac{\zeta(1+\alpha-\beta+\gamma-\delta)\zeta(1+\alpha-\beta)\zeta(1+\gamma-\delta)}{(\alpha+\gamma)\,\zeta(2+\alpha-\beta+\gamma-\delta)}$$
$$+X^{-\beta-\delta}\left(\frac{tT}{2\pi}\right)^{-\alpha+\beta-\gamma+\delta}\frac{\zeta(1-\alpha+\beta-\gamma+\delta)\zeta(1-\alpha+\beta)\zeta(1-\gamma+\delta)}{(\beta+\delta)\,\zeta(2-\alpha+\beta-\gamma+\delta)}$$
$$+X^{-\alpha-\delta}\left(\frac{tT}{2\pi}\right)^{\alpha-\beta-\gamma+\delta}\frac{\zeta(1-\gamma+\delta)\zeta(1+\alpha-\beta-\gamma+\delta)\zeta(1+\alpha-\beta)}{(\alpha+\delta)\zeta(2+\alpha-\beta-\gamma+\delta)}$$
$$+X^{-\beta-\gamma}\left(\frac{tT}{2\pi}\right)^{-\alpha+\beta+\gamma-\delta}\frac{\zeta(1-\alpha+\beta)\zeta(1-\alpha+\beta+\gamma-\delta)\zeta(1+\gamma-\delta)}{(\beta+\gamma)\zeta(2-\alpha+\beta+\gamma-\delta)}\Bigg)\,dt$$

with an error term of $O(Q^{-1/4})$. This expression is exactly what we were hoping for; it is identical to the "two-swap" terms found in the descent approach (see Conrey and Keating [2], section 9).

5 Conclusion

We have shown how to reproduce the complete conjecture for the shifted fourth moment of ζ by analyzing the mean square of long Dirichlet polynomials whose coefficients are convolutions of two smooth arithmetic functions. In the next paper we will carry this analysis out for coefficients which are convolutions of an arbitrary number of convolutions and use this to reproduce the full conjecture for the $2k$th moment of ζ for an arbitrary k.

Acknowledgements We gratefully acknowledge support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms. Research of the first author was also supported by the American Institute of Mathematics and by a grant from the National Science Foundation. JPK is grateful for the following additional support: a grant from the Leverhulme Trust, a Royal Society Wolfson Research Merit Award, a Royal Society Leverhulme Senior Research Fellowship, and a grant from the Air Force Office of Scientific Research, Air Force Material Command, USAF (number FA8655-10-1-3088). He is also pleased to thank the American Institute of Mathematics for hospitality during a visit where this work started.

References

1. E.B. Bogomolny, J.P. Keating, Random matrix theory and the Riemann zeros I: three- and four-point correlations. Nonlinearity **8**(6), 1115–1131 (1995)
2. B. Conrey, J.P. Keating, Moments of zeta and correlations of divisor-sums: I. Philos. Trans. A **373**(2040), 20140313, 11 pp (2015)
3. D.A. Goldston, S.M. Gonek, Mean value theorems for long Dirichlet polynomials and tails of Dirichlet series. Acta Arith. **84**(2), 155–192 (1998)

A Note on the Theorem of Maynard and Tao

Tristan Freiberg

Abstract In a recent and much celebrated breakthrough, Maynard and Tao have independently proved a certain approximation to the prime k-tuple conjecture. We have subsequently seen numerous interesting applications of the Maynard–Tao sieve method, and in this short survey we will discuss some of its consequences for patterns in the gaps between consecutive primes. These include a conjecture of Erdős and Turán (as pointed out by Granville), and a conjecture of Chowla (first proved by Shiu in 1997). More recently it has been realized that the Maynard–Tao sieve method does not only produce small gaps between primes, but, as we will also discuss, it may be combined with a construction of Erdős–Rankin for producing large gaps between consecutive primes, resulting in small, medium and large gaps between consecutive primes.

1 Introduction

In 1904, as an extension of Dirichlet's theorem on primes in arithmetic progressions, Dickson [6] posed the question:

> Do there exist m linear forms $a_1n + b_1, \ldots, a_mn + b_m$ which give m prime numbers for the same value of n, as n runs through an infinite succession of positive integers?

To the surprise and delight of many, Dickson's question turns out to be within the scope of our knowledge of the distribution of primes in progressions.

The most recent chapter of this story begins 101 years after Dickson posed his question, with the groundbreaking work of Goldston–Pintz–Yıldırım [16]. They provided a conditional[1] affirmative answer in the case where $m = 2$. Their work was reinvigorated by the outstanding work of Zhang [38], who provided an unconditional affirmative answer for $m = 2$. Most recently, an extraordinary breakthrough

[1] Their condition being that the primes have level of distribution greater than $1/2$ (see (10) below).

T. Freiberg (✉)
Department of Mathematics, University of Missouri, Columbia, MO 65211, USA
e-mail: freibergt@missouri.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_4

of Maynard [21] and Tao[2] has finally settled the question, unconditionally, for all m. We refer the reader to the expository article of Granville [17] for an account of this recent history and the ideas involved.

Thanks to the work of Maynard et al., we now know that for every m, there do exist m-tuples of linear forms that infinitely often produce m primes. However, we do not know of any particular m-tuple that does this (except, of course, in the case $m = 1$). Nevertheless, the mere existence of such m-tuples has many interesting consequences, some of which have been given by Granville [17]. The theme of this note is "consecutive primes in tuples", and as a sample corollary of Maynard's work, we will demonstrate the following result, which was first given by the author, Banks and Turnage-Butterbaugh [2, Corollary 3]. Regarding applications in connection with consecutive primes, we would be remiss not to mention here the substantial work of Baker and Pollack [1], Pollack [27], and Pollack and Thompson [28].

Theorem 1. *Let $p_1 = 2 < p_2 = 3 < \cdots$ be the sequence of all primes. Let a and q be a coprime pair of integers, and let $m \geq 2$ be an integer. For infinitely many n, we have*

$$p_{n+1} \equiv \cdots \equiv p_{n+m} \equiv a \bmod q \quad \text{and} \quad p_{n+m} - p_{n+1} \leq qB_m,$$

where $B_m = \mathrm{e}^{8m+5}$. In fact, there is an absolute constant c such that one can take $B_m = cm^3\mathrm{e}^{4m}$, and one can take $B_2 = 600$.

It was Chowla who conjectured that there should be infinitely many pairs of consecutive primes $p_n \equiv p_{n+1} \equiv a \bmod q$. (See Guy's book [18, A4].) This conjecture, and its extension to "strings" of consecutive, congruent primes of arbitrary length m, without the constraint that they lie in a bounded-length interval, was first proved in a splendid paper of Shiu [35]. In the special case where $m = 2$, by combining the ideas of Shiu and Goldston–Pintz–Yıldırım, the author [12, Theorem 3] proved a conditional version of Theorem 1 (with a weaker bound for B_2), and unconditionally [13, Theorem 1.1] that there are infinitely many "Shiu strings" $p_n \equiv p_{n+1} \equiv a \bmod q$ with $d_n/\log n$ arbitrarily small (cf. Sect. 3), where $d_n = p_{n+1} - p_n$. Quantitative results were also given in [13, 35], but have been superseded by Maynard's result [22, Theorem 3.3].

Theorem 1 is an almost immediate consequence of Maynard's original work in [21]. The basic observation is that if $0 = h_1 < h_2 < \cdots < h_k$ are integers and if, for every integer h in $[0, B] \setminus \{h_1, \ldots, h_k\}$, $\nu_0 + h \equiv 0 \bmod \ell_h$ for some small prime ℓ_h, then, for all such h, $n + h \equiv 0 \bmod \ell_h$ for every $n \equiv \nu_0 \bmod \prod_h \ell_h$. Thus, thanks to Maynard, we can produce certain configurations of primes in intervals, while forcing the other integers in those intervals to be composite. As Granville pointed out,[3] this idea can be used to establish an old conjecture of Erdős and

[2] Maynard [21] writes: "Terence Tao (private communication) has independently proven Theorem 1.1 [...] at much the same time."

[3] Private communication.

Turán [8] (also see [9] and Guy's book [18, A11]) concerning the gaps d_n between consecutive primes. The conjecture—now a theorem—is that there are infinitely many arbitrarily long increasing sequences $d_n < d_{n+1} < \cdots < d_{n+m}$, and likewise for decreasing sequences $d_n > d_{n+1} > \cdots > d_{n+m}$. This result and some variants of it are proved in detail in [2].

2 Results and Deduction of Theorem 1

We consider k-tuples

$$\mathscr{H}(x) = \{g_i x + h_i\}_{i=1}^k = \{g_1 x + h_1, \ldots, g_k x + h_k\}$$

of linear forms in $\mathbb{Z}[x]$, each having positive leading coefficient. We call $\mathscr{H}(x)$ *admissible* if and only if

$$\forall \text{ primes } p, \quad \#\{n \bmod p : \textstyle\prod_{i=1}^k (g_i n + h_i) \equiv 0 \bmod p\} < p. \tag{1}$$

Dickson [6] noted that if

$$\mathscr{H}(n) = \{g_i n + h_i\}_{i=1}^k = \{g_1 n + h_1, \ldots, g_k n + h_k\}$$

is to contain k primes for infinitely many positive integers n, $\mathscr{H}(x)$ must be admissible. Throughout, we will tacitly assume that the k linear forms $g_i x + h_i$ are distinct and have positive leading coefficients g_i, so that $\mathscr{H}(n)$ contains k distinct positive integers for all sufficiently large integers n. If $\mathscr{H}(x)$ is admissible then $\prod_{i=1}^k (g_i, h_i) = 1$, so these assumptions may be written succinctly as

$$g_1, \ldots, g_k > 0 \quad \text{and} \quad \textstyle\prod_{1 \le i < j \le k} (g_i h_j - g_j h_i) \neq 0. \tag{2}$$

Conjecture 1 (Prime k-tuple conjecture). For any admissible k-tuple

$$\mathscr{H}(x) = \{g_i x + h_i\}_{i=1}^k$$

satisfying (2), there exist infinitely many positive integers n such that $\mathscr{H}(n)$ consists of k primes.

The following formulation of the theorem of Maynard and Tao has been given by Granville [17, Theorem 6.4].

Theorem 2 (Maynard–Tao). *Fix any positive integer m. There is a number k_m, depending only on m, such that the following holds for any integer $k \ge k_m$. For any admissible k-tuple*

$$\mathscr{H}(x) = \{g_i x + h_i\}_{i=1}^k$$

satisfying (2), there exist infinitely many integers n such that $\mathscr{H}(n)$ contains at least m primes. One can take any k_m satisfying $k_m \log k_m > \mathrm{e}^{8m+4}$.

Call an m-tuple $\{g_i x + h_i\}_{i=1}^m$ a "Dickson m-tuple" if there are infinitely many n for which $\{g_i n + h_i\}_{i=1}^m$ contains m primes. Let $\mathscr{H}(x) = \{g_i x + h_i\}_{i=1}^k$ be an admissible k-tuple with $k \geq k_m$, where $k_m \log k_m > \mathrm{e}^{8m+4}$. Thus, $\mathscr{H}(x)$ contains $\binom{k}{k_m}$ k_m-tuples, all of which are admissible and so, by the Maynard–Tao theorem, contain at least one Dickson m-tuple. But each Dickson sub-m-tuple of $\mathscr{H}(x)$ is contained in exactly $\binom{k-m}{k-k_m}$ sub-k_m-tuples of $\mathscr{H}(x)$. Hence,

$$\#\{\mathscr{J}(x) \subseteq \mathscr{H}(x) : \mathscr{J}(x) \text{ is a Dickson } m\text{-tuple}\} \geq \binom{k}{k_m} \Big/ \binom{k-m}{k-k_m}. \tag{3}$$

Thus, as a proportion of the total number of m-tuples contained in $\mathscr{H}(x)$, the number of m-tuples contained in $\mathscr{H}(x)$ for which the prime m-tuple conjecture holds is at least $(k_m)^{-m}$. This basic counting argument can be found in Maynard's paper [21, Theorem 1.2], as well as Granville's article [17, Corollary 1.4].

As Granville [17, Corollary 1.4 et seq.] points out, in the case where $g_i = g$ for each i, all of this still holds if we require that the primes in $\mathscr{H}(n)$ be *consecutive* primes. That is, we have the following version of the Maynard–Tao theorem.

Theorem 3 (Maynard–Tao). *Fix any positive integer m. There is a number k_m, depending only on m, such that the following holds for any integer $k \geq k_m$. For any admissible k-tuple*

$$\mathscr{H}(x) = \{g_i x + h_i\}_{i=1}^k$$

satisfying (2), there exist infinitely many integers n such that $\mathscr{H}(n)$ contains at least m consecutive primes. One can take any k_m satisfying $k_m \log k_m > \mathrm{e}^{8m+4}$.

Call an m-tuple $\{gx + h_i\}_{i=1}^m$ a "Dickson* m-tuple" if there are infinitely many n for which $\{gn + h_i\}_{i=1}^m$ contains m *consecutive* primes. Essentially repeating the argument that gave (3), we see that if $\mathscr{H}(x) = \{gx + h_i\}_{i=1}^k$ is an admissible k-tuple with $k \geq k_m$, where $k_m \log k_m > \mathrm{e}^{8m+4}$, then

$$\#\{\mathscr{J}(x) \subseteq \mathscr{H}(x) : \mathscr{J}(x) \text{ is a Dickson* } m\text{-tuple}\} \geq \binom{k}{k_m} \Big/ \binom{k-m}{k-k_m}, \tag{4}$$

the right-hand side being at least $(k/k_m)^m$.

We deduced Theorem 3 in [2], originally with[4] $k_m = \mathrm{e}^{\mathrm{e}^{12m}}$, but as Granville[5] pointed out, k_m need not be larger in Theorem 3 than it is in Theorem 2. Indeed, Theorem 3 follows at once from Theorem 2 and the following basic proposition. Let us denote the set of all primes by

$$\mathbb{P} = \{p_1 = 2 < p_2 = 3 < p_3 = 5 < \cdots\}.$$

Proposition 1. *Let $\mathscr{H}(x) = \{g_i x + h_i\}_{i=1}^k$ be an admissible k-tuple satisfying (2), and let B be a positive integer. There exists an integer U, depending only on $\mathscr{H}(x)$ and B, and an integer ν_0, such that*

$$\mathscr{H}(Ux + \nu_0) = \{g_i(Ux + \nu_0) + h_i\}_{i=1}^k$$

is admissible and, for all sufficiently large integers n,

$$\mathbb{P} \cap \left(\bigcup_{i=1}^k \mathscr{I}_B(g_i(Un + \nu_0) + h_i) \right) = \mathbb{P} \cap \{g_i(Un + \nu_0) + h_i\}_{i=1}^k, \tag{5}$$

where

$$\mathscr{I}_B(g_i(Un + \nu_0) + h_i) = [g_i(Un + \nu_0) + h_i - B, g_i(Un + \nu_0) + h_i + B]$$

is the closed interval of length $2B$, centered at $g_i(Un + \nu_0) + h_i$.

The following proof is given in [2]. The basic idea behind the construction is essentially the same as the one involved in producing gaps between primes by considering runs of composite integers of the form $n! + 2, \ldots, n! + n$.

Proof (Proof of Proposition 1). Let

$$\mathscr{P} = \{\ell_{ab} : 1 \le a \le k, |b| \le B\}$$

be any $k \times (2B + 1)$ array of distinct primes ℓ_{ab} that do not divide

$$D_B(\mathscr{H}) = g_1 \cdots g_k \prod_{\substack{1 \le i,j \le k \\ g_i x + h_i + h \notin \mathscr{H}(x) \\ g_j x + h_j + h \notin \mathscr{H}(x)}} \prod_{|h| \le B} (g_i h_j - g_j h_i + g_i h).$$

Of course we want $D_B(\mathscr{H})$ to be nonzero, and this is the reason for the conditions $g_a x + h_a + h \notin \mathscr{H}(x)$, $a = i, j$. To see that $D_B(\mathscr{H}) \neq 0$, note that since $\mathscr{H}(x)$ is admissible, $\prod_{i=1}^k (g_i, h_i) = 1$, so $g_a h_b - g_b h_a + g_a h = g_a(h_b + h) - h_a(g_b) = 0$ if and

[4] We used the *ad hoc* construction of the original version of this note: if $\ell_1 < \cdots < \ell_k$ are primes such that $k < \ell_1$ and $\ell_k < \ell_1^2$, and if $Q = (\ell_1 \cdots \ell_k)^{-1} \prod_{p \le \ell_k} p$, then $\{Qx + \ell_i\}_{i=1}^k$ is admissible, and whenever it produces primes they must be consecutive. To guarantee the existence of the k primes ℓ_i with $\ell_k < \ell_1^2$, we applied the Maynard–Tao theorem to an admissible K-tuple with K sufficiently large in terms of k.

[5] See terrytao.wordpress.com/2013/11/22/ polymath8b-ii-optimising-the-variational-problem-and-the-sieve/ #comment-254079.

only if $g_a = g_b$ and $h_a = h_b + h$, in which case $g_b x + h_b + h = g_a x + h_a \in \mathscr{H}(x)$. Let

$$U = \prod_{\ell_{ab} \in \mathscr{P}} \ell_{ab}$$

and, using the Chinese remainder theorem, choose an integer ν_0 satisfying the following congruence conditions:

$$\forall \ell_{ab} \in \mathscr{P}, \quad g_a \nu_0 + h_a + b \equiv \begin{cases} 0 & \mod \ell_{ab} \quad \text{if } g_a x + h_a + b \notin \mathscr{H}(x), \\ n_{ab} & \mod \ell_{ab} \quad \text{if } g_a x + h_a + b \in \mathscr{H}(x), \end{cases} \tag{6}$$

where $n_{ab} \bmod \ell_{ab}$ is any congruence class mod ℓ_{ab} such that

$$\prod_{i=1}^{k} (g_i n_{ab} + h_i) \not\equiv 0 \mod \ell_{ab}, \tag{7}$$

which exists because $\mathscr{H}(x)$ is admissible. For every n and any $1 \le a \le k$, $|b| \le B$, we have

$$g_a x + h_a + b \notin \mathscr{H}(x) \implies g_a(Un + \nu_0) + h_a + b \equiv 0 \mod \ell_{ab},$$

so $g_a(Un+\nu_0)+h_a+b$ is prime for at most one n. Hence (5) holds for all sufficiently large n.

Let us verify that the k-tuple

$$\mathscr{H}(Ux + \nu_0) = \{g_i(Ux + \nu_0) + h_i\}_{i=1}^{k}$$

is admissible. If $p \nmid U$ then the solutions $n \bmod p$ to the congruence

$$\prod_{i=1}^{k} (g_i U n + g_i \nu_0 + h_i) \equiv 0 \mod p \tag{8}$$

are in one-to-one correspondence with the solutions to $\prod_{i=1}^{k}(g_i n + h_i) \equiv 0 \mod p$, of which there are less than[6] p as $\mathscr{H}(x)$ is admissible. Now suppose $p \mid U$, that is $p = \ell_{ab}$ for some $\ell_{ab} \in \mathscr{P}$. Then there are no solutions to (8). For if $g_a x + h_a + b \in \mathscr{H}(x)$, then by (6) and (7), the left-hand side of (8) is nonzero mod ℓ_{ab}, and if $g_a x + h_a + b \notin \mathscr{H}(x)$, we have the following. By (6),

$$g_i U n + g_i \nu_0 + h_i \equiv 0 \mod \ell_{ab}$$

[6] In fact the number of solutions is k, because $p \nmid U$ implies $p \nmid g_1 \cdots g_k \prod_{1 \le i < j \le k} (g_i h_j - g_j h_i)$, so we have $\prod_{i=1}^{k}(g_i n + h_i) \equiv 0 \mod p$ if and only if $n \equiv -g_i^{-1} h_i \mod p$ for some i, and these k congruence classes are all distinct mod p.

for some i if and only if

$$g_i\nu_0 + h_i \equiv 0 \equiv g_a\nu_0 + h_a + b \bmod \ell_{ab},$$

which holds only if

$$g_a(g_i\nu_0 + h_i) \equiv g_i(g_a\nu_0 + h_a + b) \bmod \ell_{ab},$$

that is

$$g_a h_i - g_i h_a - g_i b \equiv 0 \bmod \ell_{ab},$$

which is contrary to the assumption that $\ell_{ab} \nmid D_B(\mathscr{H})$. □

In the special case where $\mathscr{H}(x) = \{gx + h_i\}_{i=1}^k$ and $B = \max_{i\neq j}|h_j - h_i|$, applying Theorem 2 to the "augmented" k-tuple $\mathscr{H}(Ux+\nu_0)$ of Proposition 1 gives Theorem 3. Indeed, from Proposition 1 we deduce the following.

Proposition 2. *The following statements are equivalent.*

(i) *For every admissible k-tuple of the form $\mathscr{H}(x) = \{gx + h_i\}_{i=1}^k$, there exist infinitely many integers n such that $\mathscr{H}(n)$ contains at least m primes.*
(ii) *For every admissible k-tuple of the form $\mathscr{H}(x) = \{gx + h_i\}_{i=1}^k$, there exist infinitely many integers n such that $\mathscr{H}(n)$ contains at least m* consecutive *primes.*

Remark 1. Let $\mathscr{H}(x) = \{gx + h_i\}_{i=1}^k$ be an admissible k-tuple with $h_1 < \cdots < h_k$. Theorem 2 actually applies to certain subsets $\mathbb{P}'$ of $\mathbb{P}$ that have positive relative density and positive level of distribution. Thus, we can prove that if k is large enough in terms of m, as well as in terms of the relative density and level of distribution of $\mathbb{P}'$, then for infinitely many n,

$$|\mathbb{P} \cap [gn + h_1, gn + h_k]| = |\mathbb{P} \cap \mathscr{H}(n)| \geq |\mathbb{P}' \cap \mathscr{H}(n)| \geq m.$$

However, we cannot in general exclude the possibility that for all sufficiently large n, $|\mathbb{P} \cap \mathscr{H}(n)| \geq 2|\mathbb{P}' \cap \mathscr{H}(n)|$. That is, we cannot in general conclude that $\mathbb{P}' \cap \mathscr{H}(n)$ infinitely often contains a pair consecutive primes, p_r and p_{r+1}.

In Table 1, k is an integer such that (i) (equivalently (ii)) of Proposition 2 is known to hold for the corresponding m, and B_m is a number such that an admissible k-tuple

$$\{x + 0, x + h_2, \ldots, x + h_k\} \quad \text{with} \quad 0 < h_2 < \cdots < h_k \leq B_m$$

is known to exist. Thus,

$$\liminf_{n\to\infty}(p_{n+m} - p_{n+1}) \leq B_m. \tag{9}$$

In the last four rows of Table 1, c denotes some positive constant (possibly a different constant in each instance). The results in rows marked [EH] are conditional on the Elliott–Halberstam conjecture, which we will now explain.

The primes are evenly distributed among the possible arithmetic progressions to a given modulus q. Very loosely, the primes are said to have level of distribution θ if this equidistribution is already apparent among the primes up to $q^{1/\theta+\epsilon}$, if not for all q then at least for almost all q. The celebrated Bombieri–Vinogradov theorem states that the primes have level of distribution $1/2$. It is not known if the primes have level of distribution greater than $1/2$, but the Elliott–Halberstam conjecture asserts that the primes have level of distribution 1.

More precisely, let

$$\Delta(N;q,a) = \pi(N;q,a) - \frac{\pi(N)}{\phi(q)},$$

be the discrepancy between $\pi(N;q,a)$, that is, the number of primes $p \leq N$ with $p \equiv a \bmod q$, and the "expected" number of such primes, viz. $\pi(N)/\phi(q)$ (assuming $(q,a) = 1$). We say that the primes have level of distribution θ if, for any given $A > 1$ and any given $\epsilon > 0$, we have

$$\sum_{q \leq N^{\theta-\epsilon}} \max_{(q,a)=1} |\Delta(N;q,a)| \ll N(\log N)^{-A}. \tag{10}$$

(The notation $X \ll Y$ signifies that $|X| \leq c|Y|$ for some constant c, which in the case of (10) may depend on ϵ and A.) Since $\pi(N) \sim N/\log N$ as $N \to \infty$ by the prime number theorem, this means that on average over moduli $q \leq N^{\theta-\epsilon}$, the discrepancy $\Delta(N;q,a)$ is small compared to $\pi(N)/\phi(q)$.

Proof (Proof of Theorem 1). If a and q are a coprime pair of positive integers and

$$\{x+0, x+h_2, \ldots, x+h_k\}, \quad 0 < h_2 < \cdots < h_k$$

is an admissible k-tuple, then

$$\mathscr{H}(x) = \{qx+a, q(x+h_2)+a, \ldots, q(x+h_k)+a\}$$

is also admissible. Choosing U and ν_0 as in Proposition 1, we see that if the interval

$$[N, N+qh_k], \quad N = q(Un+\nu_0)+a$$

contains any primes, they all lie in $\mathscr{H}(Un+\nu_0)$, all of whose elements are congruent to a mod q. By Theorem 2, $\mathscr{H}(Un+\nu_0)$ contains at least m primes for infinitely many n, provided k is sufficiently large in terms of m. Applying the results of Table 1 completes the proof. □

Table 1 Bounded length intervals containing primes

	m	k	B_m	Reference
[EH]	2	6	16	GPY [16]
	2	3,500,000	70,000,000	Zhang [38]
	2	632	4680	Polymath [29]
	2	105	600	Maynard [21]
	2	50	246	Polymath [30]
[EH]	2	5	12	Maynard [21]
[EH]	3	105	600	Maynard [21]
[EH]	3	54	270	Polymath [30]
	m	$[e^{8m+4}]$	e^{8m+5}	Granville [17]
	m	$[cm^2e^{4m}]$	cm^3e^{4m}	Maynard [21]
[EH]	m	$[cm^2e^{2m}]$	cm^3e^{2m}	Maynard [21]
	m	$[ce^{(4-28/157)}]$	$cme^{(4-28/157)m}$	Polymath [30]
[EH]	m	$[ce^{2m}]$	cme^{2m}	Polymath [30]

Remark 2. One may deduce the aforementioned conjecture of Erdős and Turán concerning increasing and decreasing runs of prime gaps by considering k-tuples of the form $\{x, x+h, \dots, x+h^k\}$ or $\{x, x-h, \dots, x-h^k\}$.

The major development of Goldston, Pintz and Yıldırım (GPY) in [16] paved the way for all of the results in Table 1. They established, on[7] [EH], that any admissible 6-tuple of linear forms infinitely often produces at least two primes. As the 6-tuple $\{x, x+4, x+6, x+10, x+12, x+16\}$ is admissible, this meant one could conditionally take $B_2 = 16$ in (9). Briefly, the GPY method runs as follows.

Let an admissible k-tuple $\mathscr{H}(x) = \{x+h_1, \dots, x+h_k\}$ be given. Let (λ_d) be a sequence of real numbers, so that $\nu(n) = \big(\sum_{d|n} \lambda_d\big)^2$ is always nonnegative, and set $\nu_{\mathscr{H}}(n) = \nu\big((n+h_1)\cdots(n+h_k)\big)$. Letting $\mathbf{1}_{\mathbb{P}}$ denote the indicator function of the set $\mathbb{P}$ of all primes, consider the sum

$$S_{\mathscr{H}}(N;m) = \sum_{N<n\le 2N} \Big(\sum_{i=1}^{k} \mathbf{1}_{\mathbb{P}}(n+h_i) - (m-1)\Big)\nu_{\mathscr{H}}(n). \tag{11}$$

If $S_{\mathscr{H}}(N;m) > 0$ then we can conclude that $|\mathscr{H}(n)\cap\mathbb{P}| \ge m$ for some n in the range $N < n \le 2N$. GPY discovered a system of weights (λ_d) for which $S_{\mathscr{H}}(N;2) > 0$ for all sufficiently large N, assuming (the unproven conjecture) that $\theta > 1/2$, and provided that k is sufficiently large in terms of θ.

For reasons to do with level of distribution, (λ_d) is assumed to be supported on the positive integers $d \le R = N^{(\theta-\epsilon)/2}$. A typical choice for λ_d $(d \le R)$ would be

$$\lambda_d = \mu(d)\big(\log(R/d)\big)^k.$$

[7] In fact, a level of distribution of $\theta = 0.971$ suffices.

With such a choice, for $N < n \leq 2N$, the divisor sum $\sum_{d|n} \lambda_d$ approximates the generalized von Mangoldt function

$$\Lambda_k(n) = \sum_{d|n} \mu(d)\big(\log(n/d)\big)^k,$$

which vanishes if n has more than k prime factors. That is, $\nu_{\mathscr{H}}(n)$ essentially detects those $n \in (N, 2N]$ for which $n + h_1, \dots, n + h_k$ are all prime. However, with this choice the above positivity argument always fails.

GPY considered, more generally,

$$\lambda_d = \mu(d)F(\log R/d)$$

for a smooth compactly supported function $F : [0, \infty) \to \mathbb{R}$. They found that by choosing $F(x) = x^{k+l}$, the above positivity argument succeeded (with $m = 2$), assuming $\theta > 1/2$, k sufficiently large in terms of θ and $l \approx \sqrt{k}$. GPY also used their weight to prove an important unconditional result, as we will see in the next section.

Zhang [38] was the first to prove unconditionally that $\liminf_{n\to\infty}(p_{n+1} - p_n)$ is bounded, not by showing that the primes have level of distribution greater than $1/2$, but by working a substitute of the Bombieri–Vinogradov theorem into GPY's proof, which had the effect of going beyond the level of $1/2$. Zhang [38] showed that for an admissible k-tuple $\mathscr{H}(x) = \{x + h_i\}_{i=1}^k$, there exist infinitely many integers n such that $\mathscr{H}(n)$ contains at least two primes, provided $k \geq 3.5 \times 10^6$, and consequently that one could take $B_2 = 7 \times 10^7$ in (9). Zhang's proof was subsequently refined in a Polymath project [29] to the point where one could take $B_2 = 4680$. More precisely, it was established that admissible 632-tuples contain at least two primes infinitely often, and there is an admissible 632-tuple $\mathscr{H}(x)$ with $\mathscr{H}(0) \subseteq [0, 4680]$.

Maynard [21] broke the next major barrier by establishing the existence of infinitely many bounded-length intervals containing more than two primes. Maynard achieved this chiefly by considering a more flexible system of weights $(\lambda_{d_1,\dots,d_k})$ than GPY's, in which

$$\nu_{\mathscr{H}}(n) = \Bigg(\sum_{d_i|n+h_i\ \forall i} \lambda_{d_1,\dots,d_k}\Bigg)^2$$

may depend on each term of the product $(n+h_1)\cdots(n+h_k)$ individually. Moreover, Maynard's proof only requires that the primes have level of distribution $\theta > 0$, which means that it applies to subsequences of the primes for which only weaker level of distribution results are known hold. For instance, Thorner [36] has shown that there are infinitely often bounded gaps between primes in a given Chebotarev class, and established a number of interesting applications of this result in itself.

In [17], Granville uses explicit bounds for $\pi(N)$ to show that if $2k \log k > 10^5$, then $\pi(2k \log k) - \pi(k) > k$. Thus, for such k, we can choose k primes larger than k, but less than $2k \log k$, to form an admissible k-tuple. So, for any $m \geq 1$, if k is

the smallest integer satisfying $k \log k > \mathrm{e}^{8m+4}$, one can find an admissible k-tuple $\mathscr{H}(x) = \{x + h_i\}_{i=1}^{k}$ such that $\mathscr{H}(0) \subset [1, 2k \log k]$. Thus, (9) holds with $B_m = \mathrm{e}^{8m+5}$ by the Maynard–Tao theorem.

Maynard [21] does better than this for large m: there is an absolute constant c such that the Maynard–Tao theorem holds with any $k > cm^2\mathrm{e}^{4m}$ and (9) holds with $B_m = cm^3\mathrm{e}^{4m}$. Moreover, for specific m one can be explicit. Thus, Maynard [21] shows, for instance, that any admissible 105-tuple produces at least two primes infinitely often, and there is such a tuple that "fits" in an interval of length 600, whence one can take $B_2 = 600$. A Polymath project [30] has refined and optimized aspects of Maynard's proof and obtained still better bounds (see Table 1).

3 Small, Medium and Large Gaps Between Consecutive Primes

Recall that $d_n = p_{n+1} - p_n$ denotes the nth prime gap. In [16], GPY used their sieve weights to establish, unconditionally, the longstanding conjecture that

$$\liminf_{n\to\infty} \frac{d_n}{\log n} = 0.$$

The prime number theorem implies that $p_n \sim n \log p_n \sim n \log n$ as $n \to \infty$, so the normalized nth prime gap $d_n/\log n$ is approximately 1 on average. GPY's result then tells us that $d_n/\log n$ is infinitely often arbitrarily small. At the opposite end of the spectrum, the result

$$\limsup_{n\to\infty} \frac{d_n}{\log n} = \infty$$

goes back to Westzynthius [37].

What about limit points of the sequence $\{d_n/\log n : n \geq 2\}$ in-between these two extremes? We denote this set of limit points by $\mathbf{L}$. Perhaps surprisingly, no other limit point is known—not even 1 is known to be in $\mathbf{L}$ (the prime number theorem implies the existence of a limit point less than or equal to 1). However, as Erdős wrote in [10, p. 4]: "It seems certain that the sequence $d_n/\log n$ is everywhere dense in $(0, \infty)$."

Indeed, based on the prime number theorem, which implies that

$$\sum_{N<n\leq 2N} \mathbf{1}_{\mathbb{P}}(n) \sim \int_N^{2N} \frac{\mathrm{d}t}{\log t} \qquad (N \to \infty),$$

Cramér proposed that for large N, the sequence $(\mathbf{1}_{\mathbb{P}}(n) : N < n \leq 2N)$ should behave like a sequence $(X_n : N < n \leq 2N)$ of independent random variables X_n,

where $X_n = 1$ with probability $1/\log N$, and $X_n = 0$ with probability $1 - 1/\log N$. Thus, Cramér's statistical model suggests that the gaps between consecutive primes should follow an exponential distribution: for any given $b > a \geq 0$, we expect that

$$\#\{N < n \leq 2N : d_n/\log N \in (a, b]\} \sim N \int_a^b \mathrm{e}^{-t}\mathrm{d}t \qquad (N \to \infty).$$

Gallagher [14] showed that this prediction would follow from a certain uniform version of the Hardy–Littlewood prime k-tuple conjecture—obviously well beyond current ideas.

Erdős [10] and Ricci [33] were able to show that $\mathbf{L}$ has positive Lebesgue measure, or more precisely that if λ denotes the Lebesgue measure on $\mathbb{R}$, then $\lambda([0, 2] \cap \mathbf{L}) > 1/8$. Goldston and Ledoan [15] have recently shown that, for any $T > 1$, the method used by Erdős yields $\lambda([0, T] \cap \mathbf{L}) > (1/\mathscr{C})(1 - 1/T)$, where $\mathscr{C}$ is any overestimate in the sieve upper bound for the number of generalized twin primes. (One can take $\mathscr{C} = 7/2$ by work of Bombieri et al. [4].) Using Zhang's breakthrough [38], Pintz [25] has shown that there is a small (ineffective) positive constant η such that $\mathbf{L} \supseteq [0, \eta]$. None of these results demonstrates the existence of a finite limit point greater than 1. This was a challenge posed by Erdős, which was first answered by Hildebrand and Maier [19]. In fact, they showed that there is a positive constant c for which $\lambda([0, T] \cap \mathbf{L}) \geq c\,T$ holds for all sufficiently large T, and hence that $\mathbf{L}$ contains arbitrarily large limit points.

In [3, Theorem 1.1], the author, Banks and Maynard show that for any given sequence of $k = 9$ nonnegative real numbers $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_k$, we have

$$\{\beta_j - \beta_i : 1 \leq i < j \leq k\} \cap \mathbf{L} \neq \emptyset. \tag{12}$$

The reader may deduce, using properties of Lebesgue measure, that asymptotically at least 12.5 % of all nonnegative real numbers belong to $\mathbf{L}$, that is

$$\lambda([0, T] \cap \mathbf{L}) \gtrsim T/8 \quad (T \to \infty).$$

The basic philosophy behind [3] is that the Maynard–Tao sieve method, which produces small gaps between primes, can be combined with a construction of Erdős [7] and Rankin [31] for producing unusually large gaps between primes, yielding gaps between consecutive primes of any desired intermediate size. We paraphrase the following proof outline from [3, Sect. 3].

The Erdős–Rankin construction produces long intervals $(n, n+z]$ containing only composite integers. This is accomplished by choosing a set of integers $\{a_p : p \leq y\}$, one for each prime $p \leq y < z$, so that for every integer $g \in (0, z]$, the congruence $g \equiv a_p \bmod p$ holds for at least one $p \leq y$. By the Chinese remainder theorem one can find an integer ν_0, uniquely determined modulo $P(y) = \prod_{p \leq y} p$, such that $\nu_0 \equiv -a_p \bmod p$ for every $p \leq y$. Now suppose $n \equiv \nu_0 \bmod P(y)$ and $n > y$. For any $g \in (0, z]$ we have $g \equiv a_p \bmod p$ for some $p \mid P(y)$, and so $g + n \equiv a_p - a_p \equiv 0 \bmod p$; hence, $g + n$ is composite for each $g \in (0, z]$. We say that the progression

$\nu_0 \bmod P(y)$ *sieves out* intervals of the form $(n, n+z]$, where $n \equiv \nu_0 \bmod P(y)$ and $n > y$. Noting that $\log P(y) \sim y$ by the prime number theorem, the goal is to maximize the ratio z/y.

As we have seen, the Maynard–Tao theorem has established the existence of m-tuples of primes in k-tuples of integers the form $\mathscr{H}(n) = \{n + h_1, \dots, n + h_k\}$, whenever[8] $\mathscr{H} = \{h_1, \dots, h_k\}$ is admissible and k is large enough in terms of m. It turns out that in the Maynard–Tao theorem one can restrict n to lie in an arithmetic progression—in fact this simplifies certain estimates in its proof.

Given a sufficiently large number N and a modulus $W = \prod_{p \le D_0} p$, where D_0 grows slowly with N, one can take $n \in (N, 2N]$ with $n \equiv \nu_0 \bmod W$, provided that ν_0 is an integer for which $(\nu_0 + h_i, W) = 1$ for each i. Instead of the sum in (11), one aims to show positivity of

$$\sum_{\substack{N < n \le 2N \\ n \equiv \nu_0 \bmod W}} \left(\sum_{i=1}^{k} \mathbf{1}_{\mathbb{P}}(n + h_i) - (m-1) \right) \nu_{\mathscr{H}}(n). \tag{13}$$

Choosing the progression $\nu_0 \bmod W$ carefully, one can use it to sieve out all integers in intervals of the form $(n, n+z]$ with $n \equiv \nu_0 \bmod W$ *except* for the integers in $\mathscr{H}(n)$. Used in this way, the Maynard–Tao theorem produces *consecutive* m-tuples of primes in intervals of *bounded length*, more or less as in Proposition 1 above.

The results of Banks et al. [3] require a modification of the above ideas to obtain consecutive primes in $\mathscr{H}(n) = \{n + h_1, \dots, n + h_k\}$, $n \in (N, 2N]$, with differences $h_j - h_i$ of order $\log N$. To do this, we give a uniform version of the Maynard–Tao theorem [3, Theorem 4.3], in which the elements of $\mathscr{H}$ are allowed to grow with N. We also need to be able to take D_0 as large as $\epsilon \log N$, which is problematic for reasons related to level of distribution.

In the original work of Maynard [21], $D_0 = \log_3 N$, hence W is less than a power of $\log_2 N$, though one could take $D_0 = \log_2 N$ (W less than a power of $\log N$) without affecting the proof. In our case W may be as large as a small power of N, and so our extension of the Maynard–Tao theorem requires a modification of the Bombieri–Vinogradov theorem that exploits the fact that the arithmetic progressions with which we are concerned have moduli that are all multiples of the smooth integer W. Specifically, instead of (10) we really only need a bound of the shape[9]

$$\sum_{\substack{r \le N^{\theta-\delta} \\ (r,W)=1}} \mu(r)^2 \max_{(rW,a)=1} |\Delta(N; rW, a)| \ll \frac{N}{\phi(W)(\log N)^A}. \tag{14}$$

[8] Let us write $\mathscr{H} = \{h_1, \dots, h_k\}$ now, instead of $\mathscr{H}(x) = \{x + h_1, \dots, x + h_k\}$ as in Sect. 2.

[9] Actually, we need to restrict the sum to moduli rW that avoid multiples of any "exceptional moduli" arising from putative Siegel zeros—a technical complication, which we ignore here for the sake of exposition.

In [3, Theorem 4.2] we essentially prove that (14) holds for any $\delta > 0$ and $A > 0$, with $\theta = 1/2$. (We have $W = \prod_{p \le D_0} p$ with $D_0 = \epsilon \log N$, and we require ϵ to be sufficiently small in terms of δ and A.) This result makes use of standard zero density estimates, combined with state of the art bounds due to Chang [5] for character sums to smooth moduli.

The next step is to use a slight modification of the Erdős–Rankin construction to find an arithmetic progression $\nu_0 \bmod W$ that sieves out the integers in an interval $(0, z]$, *except* for precisely k integers $h_1, \dots, h_k \in (0, z]$ that constitute our admissible k-tuple. As it turns out, we are able to choose $\mathscr{H}$ so that for each j and any given $\beta_k \ge \cdots \ge \beta_1 \ge 0$, we have $h_j = (\beta_j + \epsilon + o(1)) \log N$. As in the Erdős–Rankin construction, we select the integers $\{a_p : p \le y\}$, $y \le z$, in stages according to their size. We take $0 < y_1 < y_2 < y < z$, say, where y_1 and y_2 are parameters to be chosen optimally later.

First, we put $a_p = 0$ for primes $p \in (y_1, y_2]$. Next, we use a "greedy sieve" to choose the a_p optimally for the small primes $2 < p \le y_1$, that is, we successively choose a_p so that $g \equiv a_p \bmod p$ for the maximum possible number of $g \in (0, z]$ that have remain "unsifted" thus far. Since we do not know the congruence classes $a_p \bmod p$ for the smallest primes, our approach does not work in general for all k-tuples $\mathscr{H} = \{h_1, \dots, h_k\}$; we find it convenient to select our k-tuple only after sieving by primes $p \le y_2$. We choose the numbers h_i from among the primes in $(y, z]$. (This is why we do not use $p = 2$ "greedily"—if we had $a_2 = 1$ then only even integers would remain unsifted.) It is clear that each $h_i \not\equiv a_p \bmod p$ for all $p \in (y_1, y_2]$ since for those primes we have $a_p = 0$. We can also guarantee that $h_i \not\equiv a_p \bmod p$ for the small primes $p \le y_1$ if we select primes h_i in a suitable arithmetic progression $\nu_0 \bmod P_1$, where $P_1 = \prod_{2 < p \le y_1} p$. We choose $y_1 = (\log y)^{1/4}$, so such primes exist by (Page's version of) the prime number theorem for arithmetic progressions.

The reader may note that the results of Table 1 suggest that we could only hope to show positivity of the sum (13) for large N and $m = 1$ if $k \ge 50$, and yet we claim (12) holds for any $\beta_k \ge \cdots \ge \beta_1 \ge 0$ with $k = 9$. Indeed, to obtain the numerically superior result, we actually employ an extra inclusion-exclusion argument and sieve upper bound, which was considered by contributors to the Polymath project [30].

We suppose k is a sufficiently large multiple of 9 and

$$\mathscr{H} = \mathscr{H}_1 \cup \cdots \cup \mathscr{H}_9$$

is a partition of $\mathscr{H} = \{h_1, \dots, h_k\}$ into 9 sets each of size $k/9$. Instead of the sum in (13), we consider

$$\sum_{\substack{N < n \le 2N \\ n \equiv \nu_0 \bmod W}} \Bigg(\sum_{i=1}^{k} \mathbf{1}_{\mathbb{P}}(n + h_i) - 1 - \sum_{j=1}^{9} \sum_{\substack{h, h' \in \mathscr{H}_j \\ h < h'}} \mathbf{1}_{\mathbb{P}}(n + h) \mathbf{1}_{\mathbb{P}}(n + h') \Bigg) \nu_{\mathscr{H}}(n).$$

If this is positive then some n must make a positive contribution, and this happens only when there exist two elements $h_i' \in \mathscr{H}_i$ and $h_j' \in \mathscr{H}_j$, $i \neq j$, such that $n + h_i'$ and $n + h_j'$ are both prime.

We cannot obtain asymptotic estimates for the new terms corresponding to $\mathbf{1}_{\mathbb{P}}(n+h)\mathbf{1}_{\mathbb{P}}(n+h')$, but we have

$$\mathbf{1}_{\mathbb{P}}(n+h') \le \big(\textstyle\sum_{d|n+h'} \hat{\lambda}_d\big)^2$$

if $\hat{\lambda}_d$ are real weights with $\hat{\lambda}_1 = 1$, and we can obtain an asymptotic upper bound for sums of the form

$$\sum_{\substack{N<n\le 2N \\ n\equiv \nu_0 \bmod W}} \mathbf{1}_{\mathbb{P}}(n+h)\big(\textstyle\sum_{d|n+h'} \hat{\lambda}_d\big)^2 \nu_{\mathscr{H}}(n),$$

for suitable $(\hat{\lambda}_d)$. The estimates are such that all of this works with a partition of $\mathscr{H}$ into no less than 9 sets. We refer the reader to [3, Sect. 4.2] for details.

We ultimately choose k nonnegative numbers

$$\beta_1, \dots, \beta_1, \beta_2, \dots, \beta_2, \dots, \beta_9, \dots, \beta_9$$

(each β_j repeated $k/9$ times), and using our modified Erdős–Rankin construction to construct an admissible k-tuple $\mathscr{H}$ such that $\mathscr{H} = \mathscr{H}_1 \cup \cdots \cup \mathscr{H}_9$ is a partition with each $\mathscr{H}_j$ of size $k/9$ and having all of its elements of size $(\beta_j + \epsilon + o(1)) \log N$.

As we mentioned, the purpose of the Erdős–Rankin construction is to produce gaps between consecutive primes that are as large as possible. In 1935 Erdős [7] showed that

$$d_n \gg (\log n)(\log_2 n)(\log_3 n)^{-2}$$

for infinitely many n. In 1938 Rankin [31] extended this to

$$d_n/F(n) \ge c - o(1) \tag{15}$$

for infinitely many n, where

$$F(n) = (\log n)(\log_2 n)(\log_4 n)(\log_3 n)^{-2},$$

originally with $c = 1/3$. Nearly 25 years later, Schönhage [34] showed that (15) holds for infinitely many n if $c = \mathrm{e}^{\gamma}/2$, and Rankin [32] subsequently showed this holds with $c = \mathrm{e}^{\gamma}$.

In 1979, Erdős offered his largest ever prize of $10,000 to anyone who could show that

$$\limsup_{n\to\infty} d_n/F(n) = \infty. \tag{16}$$

Until very recently, only two improvements on Rankin's record had been made. The first was due to Maier and Pomerance [20], who showed that in (15) one can take $c = c_0 e^{\gamma}$, where $c_0 = 1.312\ldots$ is the solution of the equation $4/c_0 - e^{-4/c_0} = 3$. The second was due to Pintz [24], who showed that $c = 2e^{\gamma}$ is admissible.

Finally, by turning the basic idea of Banks et al. [3] around, that is, by incorporating the Maynard–Tao sieve machinery into the Erdős–Rankin construction, Maynard [23] has succeeded in establishing (16). This has also been shown using different methods independently by Ford et al. [11]. Maynard has even indicated a way to replace $F(n)$ in (16) by a function that grows faster by a factor of $(\log_3 n)^{1+o(1)}$.

The obvious question now is: what about other limit points of the sequence $d_n/F(n)$, or for that matter of $d_n/f(n)$ for any sufficiently slowly growing function f? In fact, our method in [3] applies to limit points $\mathbf{L}_f$ of $\{d_n/f(n) : n \geq n_f\}$, for any increasing function f such that $f(2N) - f(N) \ll 1$ for all sufficiently large N, and such that $f(N) \leq (\log N)(\log_3 N)(\log_4 N)^{-1}$ for all large N. It is possible to do better—this question has been addressed by Pintz [26]. We expect that one can show that $\mathbf{L}_f$ contains 12.5 % or more of the nonnegative reals as long as $f(N) \leq F(N)$.

Acknowledgements For their input or commentary, we thank William Banks, Andrew Granville, James Maynard, Caroline Turnage-Butterbaugh, and the referee.

References

1. R.C. Baker, P. Pollack, Bounded gaps between primes with a given primitive root, II. Forum Math. (2014, to appear), 19 pp. [arXiv:1407.7186]
2. W.D. Banks, T. Freiberg, C.L. Turnage-Butterbaugh, Consecutive primes in tuples. Acta Arith. **167**, 261–266 (2015)
3. W.D. Banks, T. Freiberg, J. Maynard, On limit points of the sequence of normalized prime gaps. Preprint (2014), 25 pp. [arXiv:1404.5094]
4. E. Bombieri, J.B. Friedlander, I.H. Iwaniec, Primes in arithmetic progressions to large moduli. Acta Math. **156**, 203–251 (1986)
5. M.C. Chang, Short character sums for composite moduli. J. Anal. Math. **123**, 1–33 (2014)
6. L.E. Dickson, A new extension of Dirichlet's theorem on prime numbers. Messenger Math. **33**, 155–161 (1904)
7. P. Erdős, On the difference of consecutive primes. Q. J. Math. Oxf. Ser. **6**, 124–128 (1935)
8. P. Erdős, P. Turán, On some new questions on the distribution of prime numbers. Bull. Am. Math. Soc. **54**, 371–378 (1948)
9. P. Erdős, On the difference of consecutive primes. Bull. Am. Math. Soc. **54**, 885–889 (1948)
10. P. Erdős, Some problems on the distribution of prime numbers, in *C. I. M. E. Teoria dei numeri*. Math. Congr. (Varenna, 1954/1955), 8 pp.
11. K. Ford, B. Green, S. Konyagin, T. Tao, Large gaps between consecutive prime numbers. Preprint (2014), 31 pp. [arXiv:1408.4505]
12. T. Freiberg, Strings of congruent primes in short intervals. Ph.D. Thesis, Université de Montréal, 2010, 127 pp.
13. T. Freiberg, Strings of congruent primes in short intervals. J. Lond. Math. Soc. **84**(2), 344–364 (2011)
14. P.X. Gallagher, On the distribution of primes in short intervals. Mathematika **23**, 4–9 (1976)

15. D.A. Goldston, A.H. Ledoan, Limit points of normalized consecutive prime gaps, in *Analytic Number Theory in Honor of Helmut Maier's 60th Birthday*, ed. by C. Pomerance, M. Rassias (Springer, New York, 2015)
16. D.A. Goldston, J. Pintz, C.Y. Yıldırım, Primes in tuples I. Ann. Math. **170**(2), 819–862 (2009)
17. A. Granville, Primes in intervals of bounded length. Bull. Am. Math. Soc. **52**, 171–222 (2015)
18. R. Guy, *Unsolved Problems in Number Theory*, 3rd edn. (Springer, New York, 2004)
19. A. Hildebrand, H. Maier, Gaps between prime numbers. Proc. Am. Math. Soc. **104**, 1–9 (1988)
20. H. Maier, C. Pomerance, Unusually large gaps between consecutive primes. Trans. Am. Math. Soc. **322**, 201–237 (1990)
21. J. Maynard, Small gaps between primes. Ann. Math. **181**(2), 383–413 (2015)
22. J. Maynard, Dense clusters of primes in subsets. Preprint (2014), 35 pp. [arXiv:1405.2593]
23. J. Maynard, Large gaps between primes. Preprint (2014), 14 pp. [arXiv:1408.5110]
24. J. Pintz, Very large gaps between consecutive primes. J. Number Theory **63**, 286–301 (1997)
25. J. Pintz, Polignac numbers, conjectures of Erdős on gaps between primes, arithmetic progressions in primes, and the bounded gap conjecture. Preprint (2013), 14 pp. [arXiv:1305.6289]
26. J. Pintz, On the distribution of gaps between consecutive primes. Preprint (2014), 16 pp. [arXiv:1407.2213]
27. P. Pollack, Bounded gaps between primes with a given primitive root. Algebra Number Theory **8**, 1769–1786 (2014)
28. P. Pollack, L. Thompson, Arithmetic functions at consecutive shifted primes. Int. J. Number Theory **11**, 1477–1498 (2015)
29. D.H.J. Polymath, New equidistribution estimates of Zhang type, and bounded gaps between primes. Algebra Number Theory **8**, 2067–2199 (2014)
30. D.H.J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes. Res. Math. Sci. **1**, 1–83 (2014)
31. R.A. Rankin, The difference between consecutive prime numbers. J. Lond. Math. Soc. **s1–13**, 242–247 (1938)
32. R.A. Rankin, The difference between consecutive prime numbers V. Proc. Edinb. Math. Soc. (2) **13**, 331–332 (1963)
33. G. Ricci, Recherches sur l'allure de la suite $\{(p_{n+1} - p_n)/\log p_n\}$, in *Colloque sur la Théorie des Nombres*, Bruxelles, 1955 (G. Thone, Liège, 1956), pp. 93–106
34. A. Schönhage, Eine Bemerkung zur Konstruktion grosser Primzahllücken. Arch. Math. **14**, 29–30 (1963)
35. D.K.L. Shiu, Strings of congruent primes. J. Lond. Math. Soc. (2) **61**(2), 359–373 (2000)
36. J. Thorner, Bounded gaps between primes in Chebotarev sets. Res. Math. Sci. **1**, 16 (2014)
37. E. Westzynthius, Über die Verteilung der Zahlen, die zu den n ersten Primzahlen teilerfremd sind. Commentat. Phys. Math. **5**, 1–37 (1931)
38. Y. Zhang, Bounded gaps between primes. Ann. Math. (2) **179**, 1121–1174 (2014)

A Prime Analogue of Roth's Theorem in Function Fields

Yu-Ru Liu and Craig V. Spencer

Abstract Let $\mathbb{F}_q[t]$ denote the polynomial ring over the finite field $\mathbb{F}_q$, and let $\mathscr{P}_R$ denote the subset of $\mathbb{F}_q[t]$ containing all monic irreducible polynomials of degree R. For non-zero elements $\mathbf{r} = (r_1, r_2, r_3)$ of $\mathbb{F}_q$ satisfying $r_1 + r_2 + r_3 = 0$, let $D(\mathscr{P}_R) = D_{\mathbf{r}}(\mathscr{P}_R)$ denote the maximal cardinality of a set $A_R \subseteq \mathscr{P}_R$ which contains no non-trivial solution of $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in A_R$ $(1 \leq i \leq 3)$. By applying the polynomial Hardy-Littlewood circle method, we prove that $D(\mathscr{P}_R) \ll_q |\mathscr{P}_R|/(\log\log\log|\mathscr{P}_R|)$.

1 Introduction

For $n \in \mathbb{N} = \{1, 2, \cdots\}$, let $D_3([1, n])$ denote the maximal cardinality of an integer subset of $[1, n]$ containing no non-trivial 3-term arithmetic progressions. In a fundamental paper, Roth [20] proved that $D_3([1, n]) \ll n/\log\log n$. His result was later improved by Heath-Brown [8], Szemerédi [24], Bourgain [3, 4] and Sanders [21, 22]. In 2014, Bloom [2] showed that $D_3([1, n]) \ll n(\log\log n)^4/\log n$, which gives the best upper bound up to date. Szemerédi [23] proved that subsets of the natural numbers with positive upper density contain arbitrarily long arithmetic progressions, and in 2001, Gowers [5] proved a quantitative version of Szemerédi's theorem.

One can consider analogous questions with $[1, n]$ replaced by $P[1, n]$, the set of positive primes up to n. Let $D_3(P[1, n])$ denote the maximal cardinality of an integer subset of $P[1, n]$ containing no non-trivial 3-term arithmetic progression, and let $\pi(n)$ denote the cardinality of $P[1, n]$. In [6], Green proved that

Y.-R. Liu (✉)
Faculty of Mathematics, Department of Pure Mathematics, University of Waterloo, Waterloo, ON, Canada N2L 3G1
e-mail: yrliu@math.uwaterloo.ca

C.V. Spencer
Department of Mathematics, Kansas State University, 138 Cardwell Hall, Manhattan, KS 66506, USA
e-mail: cvs@ksu.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_5

$$D_3(P[1,n]) \ll \pi(n)\left(\frac{\log\log\log\log\log\pi(n)}{\log\log\log\log\pi(n)}\right)^{1/2}.$$

In [7], Green and Tao proved that subsets of the primes with positive upper density contain arbitrarily long arithmetic progressions.

Let $\mathbb{F}_q[t]$ denote the ring of polynomials over the finite field $\mathbb{F}_q$. For $R \in \mathbb{N} = \{1,2,\ldots\}$, let $\mathscr{P}_R$ be the subset of $\mathbb{F}_q[t]$ containing all monic irreducible polynomials of degree R. Let $\mathbf{r} = (r_1, r_2, r_3)$ be non-zero elements of $\mathbb{F}_q$ satisfying $r_1 + r_2 + r_3 = 0$. Let $(x_1, x_2, x_3) \in \mathbb{F}_q[t]^3$ be a solution of $r_1x_1 + r_2x_2 + r_3x_3 = 0$. We say that (x_1, x_2, x_3) is a *trivial* solution if $x_1 = x_2 = x_3$. Otherwise, we say that (x_1, x_2, x_3) is a *non-trivial* solution. Let $D(\mathscr{P}_R) = D_{\mathbf{r}}(\mathscr{P}_R)$ denote the maximal cardinality of a set $A_R \subseteq \mathscr{P}_R$ for which there is no non-trivial solution of $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in A_R$ $(1 \le i \le 3)$, and let $|\mathscr{P}_R|$ denote the cardinality of $\mathscr{P}_R$. In this paper, we prove the following theorem.

Theorem 1. *For $R \in \mathbb{N}$,*

$$D(\mathscr{P}_R) \ll_q \frac{|\mathscr{P}_R|}{\log\log\log\log|\mathscr{P}_R|}.$$

Here the implicit constant depends only on q.

In the special case that $\mathbf{r} = (1,-2,1)$ and $\gcd(2,q) = 1$, the number $D(\mathscr{P}_R)$ denotes the maximal cardinality of a set $A_R \subseteq \mathscr{P}_R$ which contains no non-trivial 3-term arithmetic progression. In large part, this paper will follow the approach of Green. Our improvement over the analogous bound for $\mathbb{Z}$ stems from nice properties of Bohr sets in $\mathbb{F}_q[t]$ and the availability of a stronger bound for Roth's theorem in $\mathbb{F}_q[t]$ (see [14]) than in $\mathbb{Z}$. It is worth noting that when studying equations of the form $r_1x_1 + \cdots + r_sx_s = 0$ where $r_1 + \cdots + r_s = 0$ and $s \ge 4$, in [14], the authors proved that

$$D(\mathscr{P}_R) \ll_q \frac{|\mathscr{P}_R|}{(\log|\mathscr{P}_R|)^{s-3}},$$

which provides a strong bound compared to Theorem 1. Also, Lê has proved a function field analogue of Green and Tao's theorem on arithmetic progressions of primes (see [11]). While his method provides results about more general configurations in the irreducible polynomials of $\mathbb{F}_q[t]$, the approach of this paper produces stronger quantitative bounds on $D(\mathscr{P}_R)$. In addition, several estimates of exponential sums in this paper are essential to various additive combinatorial problems in function fields, including the results in [12].

In 2011, the above mentioned bound of Green was improved by Helfgott and de Roton [9] to

$$|\tilde{A}_R| \ll |\tilde{\mathscr{P}}_R|\frac{\log\log\log|\tilde{\mathscr{P}}_R|}{(\log\log|\tilde{\mathscr{P}}_R|)^{1/3}}.$$

Recently, Naslund [16] showed that for any $\epsilon > 0$,

$$|\tilde{A}_R| \ll |\tilde{\mathscr{P}}_R|\left(\frac{1}{\log\log|\tilde{\mathscr{P}}_R|}\right)^{1-\epsilon}.$$

In future work, we will show how their methods can be implemented over $\mathbb{F}_q[t]$ to improve Theorem 1.

2 Basic Setup

We start this section by introducing the Fourier analysis of $\mathbb{F}_q[t]$. Let $\mathbb{K} = \mathbb{F}_q(t)$ be the field of fractions of $\mathbb{F}_q[t]$, and let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K}$ at ∞. We may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i\le r} a_i t^i$ for some $r \in \mathbb{Z}$ and $a_i = a_i(\alpha) \in \mathbb{F}_q$ $(i \le r)$. If $a_r \neq 0$, we define $\operatorname{ord}\alpha = r$ and we write $\langle\alpha\rangle$ for $q^{\operatorname{ord}\alpha}$. We adopt the conventions that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. Also, it is often convenient to refer to $a_{-1}(\alpha)$ as being the residue of α, an element of $\mathbb{F}_q$ that we denote by $\operatorname{res}\alpha$. For a real number R, we let $\hat{R}$ denote q^R. Hence, for $x \in \mathbb{F}_q[t]$, $\langle x\rangle < \hat{N}$ if and only if $\operatorname{ord} x < N$. Furthermore, we let $\mathbb{T}$ denote the compact additive subgroup of $\mathbb{K}_\infty$ defined by $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \langle\alpha\rangle < 1\}$. Given any Haar measure $d\alpha$ on $\mathbb{K}_\infty$, we normalize it in such a manner that $\int_{\mathbb{T}} 1\, d\alpha = 1$. Thus if $\mathfrak{N}$ is the subset of $\mathbb{K}_\infty$ defined by $\mathfrak{N} = \{\alpha \in \mathbb{K}_\infty : \operatorname{ord}\alpha < -N\}$, then the measure of $\mathfrak{N}$, $\operatorname{mes}(\mathfrak{N})$, is equal to $\hat{N}^{-1}$.

We are now equipped to define the exponential function on $\mathbb{F}_q[t]$. Suppose that the characteristic of $\mathbb{F}_q$ is p. Let $e(z)$ denote $e^{2\pi i z}$ and let $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map. There is a non-trivial additive character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\operatorname{tr}(a)/p)$. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ by defining, for each element $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q(\operatorname{res}\alpha)$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$, established in [10, Lemma 1], takes the shape

$$\int_{\mathbb{T}} e(h\alpha)\, d\alpha = \begin{cases} 1, & \text{when } h = 0, \\ 0, & \text{when } h \in \mathbb{F}_q[t] \setminus \{0\}. \end{cases}$$

For $N \in \mathbb{N}$, let $\mathscr{S}_N$ denote the subset of $\mathbb{F}_q[t]$ containing all monic polynomials of degree N. For $b, m \in \mathbb{F}_q[t]$ with m monic, $\langle b\rangle < \langle m\rangle \le N$ and $(b, m) = 1$, define a set

$$\begin{aligned} X = \Lambda_{b,m,N} &= \{n \in \mathscr{S}_N \mid mn + b \text{ is irreducible}\} \qquad (1) \\ &\cong \{n' \in S_{N+\operatorname{ord} m} \mid n' \text{ is irreducible and } n' \equiv b \pmod m\}. \end{aligned}$$

Thus by the prime number theorem in arithmetic progression in $\mathbb{F}_q[t]$ [19, Theorem 4.8],

$$|X| = \frac{\hat{N}\langle m\rangle}{(N+\operatorname{ord} m)\phi(m)} + O\left(\frac{\hat{N}^{1/2}\langle m\rangle^{1/2}}{N+\operatorname{ord} m}\right), \tag{2}$$

where $\phi(m) = \left|\left\{n \in \mathbb{F}_q[t] \,|\, \operatorname{ord} n < \operatorname{ord} m \text{ and } (n,m) = 1)\right\}\right|$. Define a function $\lambda_{b,m,N} : \mathscr{S}_N \to \mathbb{C}$ supported on X by setting

$$\lambda_{b,m,N}(n) = \begin{cases} \frac{(N+\operatorname{ord} m)\phi(m)}{\hat{N}\langle m\rangle}, & \text{when } n \in X, \\ 0, & \text{otherwise.} \end{cases}$$

In the following, we will abuse our notation and view $\lambda_{b,m,N}$ as a measure on X. By (2), we have

$$\lambda_{b,m,N}(X) = \sum_{n\in X} \lambda_{b,m,N}(n) = 1 + o(1).$$

For functions $h_1, h_2 : \mathscr{S}_N \to \mathbb{C}$, we define an inner product

$$\langle h_1, h_2\rangle_X = \sum_{n\in\mathscr{S}_N} h_1(n)\overline{h_2(n)}\lambda_{b,m,N}(n).$$

We will use the wedge symbol to denote the Fourier transforms on both $\mathbb{T}$ and $\mathscr{S}_N$. More precisely, for $f : \mathbb{T} \to \mathbb{C}$ and $h : \mathscr{S}_N \to \mathbb{C}$, the functions $f^\wedge : \mathscr{S}_N \to \mathbb{C}$ and $h^\wedge : \mathbb{T} \to \mathbb{C}$ are defined by

$$f^\wedge(n) = \int_{\mathbb{T}} f(\theta)e(-n\theta)\,d\theta \qquad \text{and} \qquad h^\wedge(\theta) = \sum_{n\in\mathscr{S}_N} h(n)e(n\theta).$$

Also, we define the convolution of two functions $f : \mathbb{T} \to \mathbb{C}$ and $g : \mathbb{T} \to \mathbb{C}$ to be

$$(f * g)(\rho) = \int_{\mathbb{T}} f(\theta)g(\rho-\theta)\,d\theta.$$

For any measure space Y, let $B(Y)$ denote the space of continuous functions on Y and define an operator $T : B(X) \to B(\mathbb{T})$ by

$$T : h \longmapsto (h\lambda_{b,m,N})^\wedge.$$

A dual operator $T^* : B(\mathbb{T}) \to B(X)$ of T is defined by

$$T^* : f \longmapsto f^\wedge|_X.$$

We have

$$\langle Th, f\rangle_{\mathbb{T}} = \langle h, T^*f\rangle_X.$$

Also, the map $TT^* : B(\mathbb{T}) \to B(\mathbb{T})$ is given by

$$TT^* : f \longmapsto f * \lambda^{\wedge}_{b,m,N}.$$

Furthermore, for an operator T and positive numbers a and b, we define

$$\|T\|_{a\to b} = \sup_f \frac{\|Tf\|_b}{\|f\|_a},$$

where $\|\cdot\|_a$ denotes the L^a norm and f ranges over continuous functions that map to $\mathbb{C}$. A main step in proving Theorem 1 will be deriving a restriction theorem for monic irreducible polynomials. Namely, we will prove the following theorem.

Theorem 2. *Suppose that $\delta > 2$ is a real number. Then there exists a constant $C(q,\delta)$, depending only on q and δ, such that*

$$\|T\|_{2\to\delta} \le C(q,\delta)\hat{N}^{-1/\delta}.$$

As an application of Theorem 2, we are able to derive the Hardy-Littlewood majorant property for function fields. Namely, we will establish the following theorem.

Theorem 3. *Let $(a_x)_{x\in\mathscr{P}_R}$ be any sequence of complex numbers with $|a_x| \le 1$ for all $x \in \mathscr{P}_R$. For a real number $\delta \ge 2$, we have*

$$\Big\| \sum_{x\in\mathscr{P}_R} a_x e(x\theta)\Big\|_\delta \le C'(q,\delta)\Big\| \sum_{x\in\mathscr{P}_R} e(x\theta)\Big\|_\delta,$$

where $C'(q,\delta)$ is a constant depending only on q and δ.

Note that in the special case when δ is an even integer, by considering the underlying Diophantine equation, one can show that Theorem 3 holds with $C'(q,\delta) = 1$.

For a real number $\delta > 1$, let δ' denote the unique real number satisfying $1/\delta + 1/\delta' = 1$. Since

$$\begin{aligned}\|Tf\|_\delta &= \sup_{\|g\|_{\delta'}=1} \langle Tf, g\rangle = \sup_{\|g\|_{\delta'}=1} \langle f, T^*g\rangle \le \|f\|_2 \sup_{\|g\|_{\delta'}=1} \|T^*g\|_2 \\ &= \|f\|_2 \sup_{\|g\|_{\delta'}=1} \langle g, TT^*g\rangle^{1/2} \le \|f\|_2 \|TT^*\|^{1/2}_{\delta'\to\delta},\end{aligned} \tag{3}$$

to prove Theorem 2, it suffices to bound the quantity

$$\|TT^*\|_{\delta'\to\delta} = \sup_{\|f\|_{\delta'}=1} \|f * \lambda^{\wedge}_{b,m,N}\|_\delta. \tag{4}$$

In this paper, ϖ will be used to denote a monic irreducible polynomial. For a polynomial $x \in \mathbb{F}_q[t]$, we say that x is $\hat{Q}$-*rough* if for all monic irreducible polynomials ϖ with $\varpi | x$, we have $\langle \varpi \rangle > \hat{Q}$. For $Q \in \mathbb{N}$, define

$$\lambda_{b,m,N}^{(Q)}(n) = \begin{cases} \hat{N}^{-1} \prod_{\substack{\langle \varpi \rangle \leq \hat{Q} \\ \varpi \nmid m}} \left(1 - 1/\langle \varpi \rangle\right)^{-1}, & \text{if } n \in \mathscr{S}_N \text{ and } mn + b \text{ is } \hat{Q}\text{-rough}, \\ 0, & \text{otherwise.} \end{cases}$$

By a sieve argument, one can show that

$$\sum_{n \in \mathscr{S}_N} \lambda_{b,m,N}^{(Q)}(n) = 1 + o(1).$$

Also, we define $\lambda_{b,m,N}^{(0)}(n) = 0$ for all $n \in \mathscr{S}_N$. Let $A = 4/(\delta - 2)$. For a positive integer $K = [A \log_q N]$ and $1 \leq Q \leq K$, let

$$\psi_Q = \lambda_{b,m,N}^{(Q)} - \lambda_{b,m,N}^{(Q-1)} \quad (1 \leq Q \leq K) \qquad \text{and} \qquad \psi_{K+1} = \lambda_{b,m,N} - \lambda_{b,m,N}^{(K)}.$$

Since $\sum_{i=1}^{K+1} \psi_i = \lambda_{b,m,N}$, by the triangle inequality, to bound $\|TT^*\|_{\delta' \to \delta}$, it suffices to consider

$$\sup_{\|f\|_{\delta'}=1} \|f * \psi_j^{\wedge}\|_{\delta} \quad (1 \leq j \leq K+1).$$

To obtain the above bound, we will apply the Riesz-Thorin interpolation theorem [17, 25] with the following bounds which we will prove in the next two sections:

$$\|f * \psi_Q^{\wedge}\|_{\infty} \ll_{q,\delta} \hat{Q}^{-1} \|f\|_1 \qquad \text{and} \qquad \|f * \psi_Q^{\wedge}\|_2 \ll_{q,\delta} N\hat{N}^{-1} \|f\|_2.$$

Notation For $k \in \mathbb{N}$, let $f(k)$ and $g(k)$ be functions of k. If $g(k)$ is positive and there exists a constant $c > 0$ such that $|f(k)| \leq cg(k)$, we write $f(k) \ll g(k)$. In the following, all implicit constants depend at most on q and δ. In Sect. 6, while δ is fixed, all implicit constant depends at most on q. Throughout, the letter ϵ will denote a sufficiently small positive number. We adopt the convention that whenever ϵ appears in a statement, then we are implicitly asserting that for each $\epsilon > 0$, the statement holds for sufficiently large values of the main parameter. Note that the "value" of ϵ may consequently change from statement.

3 An L^2-L^2 Estimate

We first state Merten's theorem for $\mathbb{F}_q[t]$.

Lemma 4 ([13, Lemma 2]). *For $Q \in \mathbb{N}$, we have*

$$\prod_{\langle \varpi \rangle \le \hat{Q}} \left(1 - 1/\langle \varpi \rangle\right)^{-1} \ll Q.$$

Lemma 5. *For a function $f : \mathbb{T} \to \mathbb{C}$ and $1 \le Q \le K$,*

$$\|f * \psi_Q^{\wedge}\|_2 \ll Q\hat{N}^{-1} \|f\|_2.$$

Also, one has

$$\|f * \psi_{K+1}^{\wedge}\|_2 \ll N\hat{N}^{-1} \|f\|_2.$$

Proof. Note that for $1 \le Q \le K+1$,

$$\|f * \psi_Q^{\wedge}\|_2 = \|f^{\wedge}\psi_Q\|_2 \le \|\psi_Q\|_\infty \|f^{\wedge}\|_2 = \|\psi_Q\|_\infty \|f\|_2.$$

For $1 \le Q \le K$, by Lemma 4,

$$\begin{aligned}
\|\psi_Q\|_\infty &\le \|\lambda_{b,m,N}^{(Q)}\|_\infty + \|\lambda_{b,m,N}^{(Q-1)}\|_\infty \\
&= \hat{N}^{-1} \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid m}} \left(1 - 1/\langle \varpi \rangle\right)^{-1} + \hat{N}^{-1} \prod_{\substack{\langle \varpi \rangle \le \widehat{Q-1} \\ \varpi \nmid m}} \left(1 - 1/\langle \varpi \rangle\right)^{-1} \\
&\ll Q\hat{N}^{-1} + (Q-1)\hat{N}^{-1} \ll Q\hat{N}^{-1}.
\end{aligned}$$

Similarly,

$$\|\psi_{K+1}\|_\infty \le \|\lambda_{b,m,N}\|_\infty + \|\lambda_{b,m,N}^{(K)}\|_\infty \ll \frac{\phi(m)(N + \operatorname{ord} m)}{\hat{N}\langle m \rangle} + K\hat{N}^{-1} \ll N\hat{N}^{-1}.$$

Thus the lemma follows.

4 An L^1-L^∞ Estimate

For a function $f : \mathbb{T} \to \mathbb{C}$ and $1 \le Q \le K+1$, we have

$$\|f * \psi_Q^{\wedge}\|_\infty \le \|\psi_Q^{\wedge}\|_\infty \|f\|_1.$$

The goal of this section is to apply the Hardy-Littlewood circle method to establish the following proposition.

Proposition 6. *For $1 \leq Q \leq K$, we have*

$$\|\lambda_{b,m,N}^{\wedge} - \lambda_{b,m,N}^{(Q)^{\wedge}}\|_{\infty} \ll \hat{Q}^{-1}.$$

Note that

$$\|\lambda_{b,m,N}^{\wedge} - \lambda_{b,m,N}^{(0)^{\wedge}}\|_{\infty} = \|\lambda_{b,m,N}^{\wedge}\|_{\infty} \ll 1.$$

Thus by combining Proposition 6 with the triangle inequality, we obtain the following lemma.

Lemma 7. *For a function $f : \mathbb{T} \to \mathbb{C}$ and $1 \leq Q \leq K+1$,*

$$\|f * \psi_Q^{\wedge}\|_{\infty} \ll \hat{Q}^{-1}\|f\|_1.$$

Let $B = 2A + 12$. Note that for all $\alpha \in \mathbb{T}$, by Dirichlet's theorem for $\mathbb{F}_q[t]$ [10, Lemma 3], there exist $a, g \in \mathbb{F}_q[t]$ with g monic, $(a, g) = 1$, $\langle \alpha - a/g \rangle < N^B/(\langle g \rangle \hat{N})$ and $\langle g \rangle \leq \hat{N}/N^B$. We define the major arcs $\mathfrak{M}$ and the minor arcs $\mathfrak{m}$ as follow:

$$\mathfrak{M} = \bigcup_{\substack{\langle g \rangle \leq N^B \\ (a,g)=1 \\ g \text{ monic}}} \mathfrak{M}_{a,g} \qquad \text{and} \qquad \mathfrak{m} = \mathbb{T} \setminus \mathfrak{M},$$

where

$$\mathfrak{M}_{a,g} = \left\{\alpha \in \mathbb{T} \,|\, \langle \alpha - a/g \rangle < N^B/\langle g \rangle \hat{N}\right\}.$$

In order to prove Proposition 6, we will separate our analysis into major arc contributions and minor arc contributions.

4.1 Major Arc Estimates

In the following, we consider a function $h : \mathscr{S}_N \to \mathbb{C}$ which satisfies the following condition:

- **Condition*** Let $r, g \in \mathbb{F}_q[t]$ with g monic, $\langle r \rangle < \langle g \rangle$ and $\langle g \rangle \leq N^B$. Let $L = N - \lceil B \log_q N \rceil$. For $r' \in \mathscr{S}_N$ with $r' \equiv r \pmod{g}$, let

  $$Y = \left\{r' + lg \,|\, \langle l \rangle < \hat{L}\right\} \subseteq \mathscr{S}_N.$$

  Then

  $$\sum_{n \in Y} h(n) = \frac{\hat{L}}{\hat{N}} \left(\gamma_{r,g}(h) + O(E(h))\right),$$

  where $\gamma_{r,g}(h)$ is a constant depending on h and $E(h)$ is an error term of size $o(1)$.

Let

$$\varrho(\beta) = \hat{N}^{-1} \sum_{n \in \mathscr{S}_N} e(\beta n).$$

Lemma 8. *Suppose that* $\langle \beta \rangle < N^B/\langle g \rangle \hat{N}$ *and that* $r, g \in \mathbb{F}_q[t]$ *with* g *monic,* $\langle r \rangle < \langle g \rangle$ *and* $\langle g \rangle \le N^B$. *For* $h : \mathscr{S}_N \to \mathbb{C}$ *satisfying Condition*, we have*

$$\sum_{\substack{n \in \mathscr{S}_N \\ n \equiv r \pmod g}} h(n) e(\beta n) = \langle g \rangle^{-1} \gamma_{r,g}(h) \varrho(\beta) + O\big(\langle g \rangle^{-1} E(h)\big).$$

Proof. For $n \in \mathscr{S}_N$ with $n \equiv r \pmod g$, we can write $n = g(yt^L + l) + r$ with y monic, $\langle y \rangle = \hat{N}/\langle g \rangle \hat{L}$ and $\langle l \rangle < \hat{L}$. Moreover, for $\langle l \rangle < \hat{L}$, we have

$$\langle \beta(gl + r) \rangle < \frac{N^B}{\langle g \rangle \hat{N}} \cdot \langle g \rangle \cdot \frac{\hat{N}}{q^{1 + \lceil B \log_q N \rceil}} \le \frac{1}{q},$$

which implies that $e(\beta(gl + r)) = 1$. Thus by applying Condition* with $r' = gyt^L + r$,

$$\begin{aligned}
\sum_{\substack{n \in \mathscr{S}_N \\ n \equiv r \pmod g}} h(n) e(\beta n) &= \sum_{\substack{\langle y \rangle = \hat{N}/\langle g \rangle \hat{L} \\ y \text{ monic}}} \sum_{\langle l \rangle < \hat{L}} h\big(g(yt^L + l) + r\big)\, e\big(\beta(g(yt^L + l) + r)\big) \\
&= \sum_{\substack{\langle y \rangle = \hat{N}/\langle g \rangle \hat{L} \\ y \text{ monic}}} e(\beta g y t^L) \sum_{\langle l \rangle < \hat{L}} h\big(gyt^L + lg + r\big) \\
&= \frac{\hat{L}}{\hat{N}} \gamma_{r,g}(h) \sum_{\substack{\langle y \rangle = \hat{N}/\langle g \rangle \hat{L} \\ y \text{ monic}}} e(\beta g y t^L) + O\big(\langle g \rangle^{-1} E(h)\big).
\end{aligned}$$

In addition, for $\langle z \rangle < \langle gt^L \rangle = \langle g \rangle \hat{L}$, we have

$$\langle \beta z \rangle < \frac{N^B}{\langle g \rangle \hat{N}} \cdot \langle z \rangle \le \frac{N^B}{\langle g \rangle \hat{N}} \cdot \frac{\langle g \rangle \hat{N}}{q^{1 + \lceil B \log_q N \rceil}} \le \frac{1}{q},$$

which implies that $e(\beta z) = 1$. Thus

$$\begin{aligned}
\sum_{\substack{\langle y \rangle = \hat{N}/\langle g \rangle \hat{L} \\ y \text{ monic}}} e(\beta g y t^L) &= \frac{1}{\langle g \rangle \hat{L}} \sum_{\langle z \rangle < \langle gt^L \rangle} \sum_{\substack{\langle y \rangle = \hat{N}/\langle g \rangle \hat{L} \\ y \text{ monic}}} e\big(\beta(gyt^L + z)\big) \\
&= \frac{1}{\langle g \rangle \hat{L}} \sum_{n \in \mathscr{S}_N} e(\beta n) = \frac{\hat{N}}{\langle g \rangle \hat{L}} \varrho(\beta).
\end{aligned}$$

By combining the above estimates, we have

$$\sum_{\substack{n\in\mathscr{S}_N\\ n\equiv r(\mathrm{mod}\ g)}} h(n)e(\beta n) = \langle g\rangle^{-1}\gamma_{r,g}(h)\varrho(\beta) + O\big(\langle g\rangle^{-1}E(h)\big).$$

This completes the proof of the lemma.

Lemma 9. *Let $h : \mathscr{S}_N \to \mathbb{C}$ satisfy Condition*. For $a, g \in \mathbb{F}_q[t]$ with g monic, $(a, g) = 1$ and $\langle g\rangle \le N^B$, define*

$$\sigma_{a,g}(h) = \sum_{\langle r\rangle<\langle g\rangle} e\left(\frac{ar}{g}\right)\gamma_{r,g}(h).$$

Then for $\alpha \in \mathfrak{M}_{a,g}$,

$$h^\wedge(\alpha) = \langle g\rangle^{-1}\sigma_{a,g}(h)\varrho\left(\alpha - \frac{a}{g}\right) + O\big(E(h)\big).$$

Proof. Write $\alpha = a/g + \beta$ with $\langle\beta\rangle < N^B\langle g\rangle^{-1}\hat{N}^{-1}$. Then by Lemma 8,

$$\begin{aligned} h^\wedge(\alpha) &= \sum_{n\in\mathscr{S}_N} h(n)e(n\alpha)\\ &= \sum_{\langle r\rangle<\langle g\rangle} e\left(\frac{ra}{g}\right) \sum_{\substack{n\in\mathscr{S}_N\\ n\equiv r(\mathrm{mod}\ g)}} h(n)e(\beta n)\\ &= \langle g\rangle^{-1}\varrho(\beta) \sum_{\langle r\rangle<\langle g\rangle} e\left(\frac{ra}{g}\right)\gamma_{r,g}(h) + O\big(\langle g\rangle\langle g\rangle^{-1}E(h)\big)\\ &= \langle g\rangle^{-1}\varrho(\beta)\sigma_{a,g}(h) + O\big(E(h)\big). \end{aligned}$$

Thus the lemma follows.

In the following, we will show that the functions $\lambda_{b,m,N}$ and $\lambda^{(Q)}_{b,m,N}$ $(1 \le Q \le K)$ satisfy Condition*. We first recall a result of Rhin.

Lemma 10 (Rhin [18, Theorem 4]). *Let $c, d \in \mathbb{F}_q[t]$ with c monic and $(c, d) = 1$. For $D, M \in \mathbb{N}$, we denote by $N(c, d; M, D)$ the number of monic irreducible polynomials ϖ of order M satisfying $\varpi \equiv c\,(\mathrm{mod}\, d)$ and $\mathrm{ord}\,(\varpi t^{\mathrm{ord}\, c} - ct^{\mathrm{ord}\, m}) < -D + \mathrm{ord}\,\varpi + \mathrm{ord}\, c$. Then*

$$N(c, d; M, D) = \frac{\hat{M}}{M\phi(d)\hat{D}} + O\big((\mathrm{ord}\, d + D + 1)\hat{M}^{1/2}\big).$$

Lemma 11. *Let $r, g \in \mathbb{F}_q[t]$ with g monic, $\langle r\rangle < \langle g\rangle$ and $\langle g\rangle \le N^B$. Then $\lambda_{b,m,N}$ satisfies Condition* with*

$$\gamma_{r,g}(\lambda_{b,m,N}) = \begin{cases} \frac{\phi(m)\langle g\rangle}{\phi(mg)}, & \text{if } (mr+b, mg) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$E(\lambda_{b,m,N}) = N^{B+1+\epsilon}\langle m\rangle^{1/2+\epsilon}\hat{N}^{-1/2}.$$

Proof. Recall the definition of X in (1). Let $r' \in \mathscr{S}_N$ with $r' \equiv r \pmod g$ and $Y = \{r' + lg \mid \langle l\rangle < \hat{L}\} \subseteq \mathscr{S}_N$. For $n = r' + lg \in Y$, $\lambda_{b,m,N}(n) = 0$ if and only if $mn + b \notin X$.

(1) Suppose that $(mr + b, mg) \neq 1$. We assume that $N^B < \hat{N}$. Then there exists a monic irreducible polynomial ϖ such that $\varpi | (mr + b, mg)$. Write $n = r + l'g + lg$ for some $l' \in \mathbb{F}_q[t]$. Then the polynomial

$$mn + b = m(r + l'g + lg) + b = (mr + b) + mg(l + l')$$

has a factor ϖ. If $mn + b \in X$, then $\varpi = mn + b$. Since

$$\langle\varpi\rangle \le \langle mg\rangle \le \langle m\rangle N^B < \langle m\rangle\hat{N} = \langle mn + b\rangle,$$

we have $\varpi \neq mn + b$. Thus we have $mn + b \notin X$. It follows that

$$\sum_{n\in Y} \lambda_{b,m,N}(n) = 0.$$

Thus the lemma follows in this case.

(2) Suppose that $(mr + b, mg) = 1$. Consider

$$N_{r'} = N_{r'}(m, g, L) = \#\{n = r' + lg \mid \langle l\rangle < \hat{L} \text{ and } mn + b \in X\},$$

which is equal to the number of monic irreducible polynomials ϖ with $\operatorname{ord}\varpi = N + \operatorname{ord} m$, $\varpi \equiv mr' + b \pmod{mg}$ and $\langle\varpi - (mr' + b)\rangle < \hat{L}\langle mg\rangle$. We now apply Lemma 10 with $c = mr' + b$, $d = mg$, $M = N + \operatorname{ord} m = \operatorname{ord} c$ and $D = N - L - \operatorname{ord} g$. Since $L = N - \lceil \log_q N^B\rceil$, we have

$$\begin{aligned} N_{r'} &= \frac{\hat{N}\langle m\rangle\hat{L}\langle g\rangle}{(N + \operatorname{ord} m)\phi(mg)\hat{N}} + O\Big(\big((\operatorname{ord} g + \operatorname{ord} m) + (N - L - \operatorname{ord} g) + 1\big)\hat{N}^{1/2}\langle m\rangle^{1/2}\Big) \\ &= \frac{\hat{L}\langle mg\rangle}{(N + \operatorname{ord} m)\phi(mg)} + O\big((\operatorname{ord} m + \lceil B\log_q N\rceil)\hat{N}^{1/2}\langle m\rangle^{1/2}\big). \end{aligned}$$

It follows that

$$\begin{aligned}
&\sum_{n\in Y}\lambda_{b,m,N}(n)\\
&=\frac{\phi(m)(N+\operatorname{ord} m)}{\hat{N}\langle m\rangle}\Big(\frac{\hat{L}\langle mg\rangle}{(N+\operatorname{ord} m)\phi(mg)}+O\big((\operatorname{ord} m+\lceil B\log_q N\rceil)\hat{N}^{1/2}\langle m\rangle^{1/2}\big)\Big)\\
&=\frac{\hat{L}}{\hat{N}}\Big(\frac{\phi(m)\langle g\rangle}{\phi(mg)}+O\Big(\frac{\hat{N}\phi(m)(N+\operatorname{ord} m)}{\hat{L}\hat{N}\langle m\rangle}(\operatorname{ord} m+B\log_q N)\hat{N}^{1/2}\langle m\rangle^{1/2}\Big)\Big)\\
&=\frac{\hat{L}}{\hat{N}}\Big(\frac{\phi(m)\langle g\rangle}{\phi(mg)}+O\Big(\frac{N^{B+1+\epsilon}\langle m\rangle^{1/2+\epsilon}}{\hat{N}^{1/2}}\Big)\Big).
\end{aligned}$$

Thus the lemma also follows in this case.

Lemma 12. *Suppose that $a, g\in\mathbb{F}_q[t]$ with g monic, $(a,g)=1$ and $\langle g\rangle\le N^B$. For σ defined as in Lemma 9, one has*

$$\sigma_{a,g}(\lambda_{b,m,N})=\begin{cases}\frac{\langle g\rangle\mu(g)}{\phi(g)}e\big(\frac{-ab\bar{m}}{g}\big), & \text{if } (m,g)=1,\\ 0, & \text{otherwise.}\end{cases}$$

Here, we write $\bar{m}$ for the multiplicative inverse of m modulo g and $\mu(\cdot)$ the Möbius function on $\mathbb{F}_q[t]$.

Proof. By Lemma 11, we have

$$\begin{aligned}
\sigma_{a,g}(\lambda_{b,m,N})=\sum_{\langle r\rangle<\langle g\rangle}e\left(\frac{ar}{g}\right)\gamma_{r,g}(\lambda_{b,m,N})&=\frac{\phi(m)\langle g\rangle}{\phi(mg)}\sum_{\substack{\langle r\rangle<\langle g\rangle\\(mr+b,mg)=1}}e\left(\frac{ar}{g}\right)\\
&=\frac{\phi(m)\langle g\rangle}{\phi(mg)}\sum_{\substack{\langle r\rangle<\langle g\rangle\\(mr+b,g)=1}}e\left(\frac{ar}{g}\right).
\end{aligned}$$

For $z\in\mathbb{Z}$ with $z\ge 0$, if $\varpi^z|g$ and $\varpi^{z+1}\nmid g$, we write that $\varpi^z\|g$. Let

$$g_0=\prod_{\varpi^z\|g,\,\varpi\nmid m}\varpi^z,$$

and $g_1=g/g_0$. If $\varpi|m$, then $\varpi\nmid(mr+b)$. Thus $(mr+b,mg)=(mr+b,g_0)$, and

$$\sum_{\substack{\langle r\rangle<\langle g\rangle\\(mr+b,g)=1}}e\left(\frac{ar}{g}\right)=\sum_{\substack{\langle r\rangle<\langle g\rangle\\(mr+b,g_0)=1}}e\left(\frac{ar}{g}\right).$$

By writing $r = ug_0 + v$ with $\langle u\rangle < \langle g_1\rangle$ and $\langle v\rangle < \langle g_0\rangle$, we have

$$\sum_{\substack{\langle r\rangle<\langle g\rangle\\(mr+b,g_0)=1}} e\left(\frac{ar}{g}\right) = \sum_{\substack{\langle v\rangle<\langle g_0\rangle\\(mv+b,g_0)=1}} e\left(\frac{av}{g}\right) \sum_{\langle u\rangle<\langle g_1\rangle} e\left(\frac{au}{g_1}\right).$$

Since

$$\sum_{\langle u\rangle<\langle g_1\rangle} e\left(\frac{au}{g_1}\right) = \begin{cases} 1, & \text{if } \langle g_1\rangle = 1,\\ 0, & \text{otherwise,}\end{cases}$$

it follows that

$$\sum_{\substack{\langle v\rangle<\langle g_0\rangle\\(mv+b,g_0)=1}} e\left(\frac{av}{g}\right) \sum_{\langle u\rangle<\langle g_1\rangle} e\left(\frac{au}{g_1}\right) = \begin{cases} \displaystyle\sum_{\substack{\langle v\rangle<\langle g\rangle\\(mv+b,g)=1}} e\left(\frac{av}{g}\right), & \text{if } g_1 = 1,\\ 0, & \text{otherwise.}\end{cases}$$

One has that $(g, m) = 1$ if and only if $g_1 = 1$. When $(g, m) = 1$, we have $\frac{\phi(m)\langle g\rangle}{\phi(mg)} = \frac{\langle g\rangle}{\phi(g)}$. Therefore, to prove the lemma, it is enough to show that when $(g, m) = 1$, we have

$$\sum_{\substack{\langle v\rangle<\langle g\rangle\\(mv+b,g)=1}} e\left(\frac{av}{g}\right) = \mu(g)e\left(\frac{-ab\bar{m}}{g}\right).$$

Suppose that $(g, m) = 1$. Let $w = mv+b$. Then $(w-b)\bar{m} \equiv v \pmod g$. By checking that $\displaystyle\sum_{\substack{\langle w\rangle<\langle g\rangle\\(w,g)=1}} e\left(\frac{aw\bar{m}}{g}\right)$ is a multiplicative function in g, one can verify that

$$\sum_{\substack{\langle w\rangle<\langle g\rangle\\(w,g)=1}} e\left(\frac{aw\bar{m}}{g}\right) = \mu(g).$$

Thus

$$\begin{aligned}\sum_{\substack{\langle v\rangle<\langle g\rangle\\(mv+b,g)=1}} e\left(\frac{av}{g}\right) = \sum_{\substack{\langle w\rangle<\langle g\rangle\\(w,g)=1}} e\left(\frac{a(w-b)\bar{m}}{g}\right) &= e\left(\frac{-ab\bar{m}}{g}\right) \sum_{\substack{\langle w\rangle<\langle g\rangle\\(w,g)=1}} e\left(\frac{aw\bar{m}}{g}\right)\\ &= \mu(g)e\left(\frac{-ab\bar{m}}{g}\right).\end{aligned}$$

This completes the proof of the lemma.

Lemma 13. *Let $r, g \in \mathbb{F}_q[t]$ with g monic, $\langle r\rangle < \langle g\rangle$ and $\langle g\rangle \le N^B$. For $1 \le Q \le K$, the function $\lambda_{b,m,N}^{(Q)}$ satisfies Condition* with*

$$\gamma_{r,g}(\lambda_{b,m,N}^{(Q)}) = \begin{cases} \prod\limits_{\substack{\langle \varpi\rangle \le \hat{Q} \\ \varpi \nmid m}} \left(1 - 1/\langle \varpi\rangle\right)^{-1} \prod\limits_{\substack{\langle \varpi\rangle \le \hat{Q} \\ \varpi \nmid mg}} \left(1 - 1/\langle \varpi\rangle\right), & \text{if } (mr+b, mg) \text{ is } \hat{Q}\text{-rough,} \\ 0, & \text{otherwise,} \end{cases}$$

and

$$E(\lambda_{b,m,N}^{(Q)}) = \hat{N}^{-1/(2A)+\epsilon} + \hat{N}^{-1/2+\epsilon},$$

where $A = 4/(\delta - 2)$ is defined as in Sect. 2.

Proof. Let $r' \in \mathscr{S}_N$ with $r' \equiv r \pmod g$ and $Y = \left\{r' + lg \,|\, \langle l\rangle < \hat{L}\right\} \subseteq \mathscr{S}_N$. Since $(b, m) = 1$, if $\varpi \in \mathbb{F}_q[t]$ is a monic irreducible polynomial with $\varpi | m$, then $\varpi \nmid (mn + b)$. Thus it suffices to consider ϖ with $\varpi \nmid m$. Let $\varpi_1, \ldots, \varpi_R \in \mathbb{F}_q[t]$ denote the monic irreducible polynomials with $\langle \varpi_i\rangle \le \hat{Q}$ and $\varpi_i \nmid m$ $(1 \le i \le R)$. For $n = r' + lg \in Y$, $\lambda_{b,m,N}^{(Q)}(n) = 0$ if and only if $\varpi_i | (mn + b)$ for some $1 \le i \le R$.

(1) Suppose that $(mr + b, mg)$ is not $\hat{Q}$-rough. Then there exists some ϖ_i such that $\varpi_i | (mr + b, mg)$. Write $n = r + l'g + lg$ for some $l' \in \mathbb{F}_q[t]$. Thus the polynomial $mn + b = (mr + b) + mg(l + l')$ has a factor ϖ_i. Hence, $\lambda_{b,m,N}^{(Q)}(n) = 0$ and the lemma follows in this case.

(2) Suppose that $(mr + b, mg)$ is $\hat{Q}$-rough, i.e., $\varpi_i \nmid (mr + b, mg)$ $(1 \le i \le R)$. Let X_i denote the event that $\varpi_i | (mn + b)$ for $n \in Y$, and let $\mathbb{P}(X_i) = |X_i|/\hat{L}$ be the probability of X_i occurring. We denote by X_i^c the complement of X_i. Note that

$$\sum_{n \in Y} \lambda_{b,m,N}^{(Q)}(n) = \frac{1}{\hat{N}} \prod_{\substack{\langle \varpi\rangle \le \hat{Q} \\ \varpi \nmid m}} \left(1 - 1/\langle \varpi\rangle\right)^{-1} \cdot \left| \bigcap_{i=1}^{R} X_i^c \right| = \frac{\hat{L}}{\hat{N}} \prod_{\substack{\langle \varpi\rangle \le \hat{Q} \\ \varpi \nmid m}} \left(1 - 1/\langle \varpi\rangle\right)^{-1} \cdot \mathscr{V},$$

where

$$\mathscr{V} = \mathbb{P}\left(\bigcap_{i=1}^{R} X_i^c \right).$$

It remains to estimate $\mathscr{V}$.

(2.1) If $\varpi_i | g$, then $mn + b \equiv mr + b \not\equiv 0 \pmod{\varpi_i}$, i.e., $\varpi_i \nmid (mn + b)$. Thus $\mathbb{P}(X_i) = 0$.

(2.2) Suppose that $\varpi_i \nmid g$. Since $\varpi_i \nmid m$, we have $(\varpi_i, mg) = 1$. If $\hat{L} \ge \langle \varpi\rangle$, as l varies with $\langle l\rangle < \hat{L}$, then $mn + b = (mr' + b) + lmg$ runs through all

residue classes modulo ϖ_i. Thus we have $\mathbb{P}(X_i) = 1/\langle \varpi_i \rangle$. On the other hand, if $\hat{L} < \langle \varpi \rangle$, then either 0 or 1 choices of l will give $\varpi_i | (mn + b)$. Thus $\mathbb{P}(X_i) = O(\hat{L}^{-1})$. From the above estimates, we have

$$\mathbb{P}(X_i) = \frac{\epsilon_i}{\langle \varpi_i \rangle} + O(\hat{L}^{-1}),$$

where

$$\epsilon_i = \begin{cases} 0, & \text{if } \varpi_i | g, \\ 1, & \text{otherwise.} \end{cases}$$

By the inclusion-exclusion formula, we have

$$\mathscr{V} = \sum_{s=0}^{R} (-1)^s \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} + O\left(\hat{L}^{-1} \sum_{s=1}^{R} \binom{R}{s} \right).$$

Note that for any $K' \in \mathbb{N}$, by considering the even terms of the above alternating sum, we have

$$\begin{aligned} \mathscr{V} &\le \sum_{s=0}^{2K'} (-1)^s \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} + O\left(\hat{L}^{-1} \sum_{s=1}^{2K'} \binom{R}{s} \right) \\ &= \prod_{i=1}^{R} \left(1 - \frac{\epsilon_i}{\langle \varpi_i \rangle} \right) + O\Big(\sum_{s=2K'+1}^{R} \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} \Big) \\ &\quad + O\left(\hat{L}^{-1} \sum_{s=1}^{2K'} \binom{R}{s} \right). \end{aligned}$$

Similarly, by considering the odd terms of the alternating sum, we have

$$\begin{aligned} \mathscr{V} &\ge \sum_{s=0}^{2K'-1} (-1)^s \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} + O\left(\hat{L}^{-1} \sum_{s=1}^{2K'-1} \binom{R}{s} \right) \\ &= \prod_{i=1}^{R} \left(1 - \frac{\epsilon_i}{\langle \varpi_i \rangle} \right) + O\Big(\sum_{s=2K'}^{R} \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} \Big) \\ &\quad + O\left(\hat{L}^{-1} \sum_{s=1}^{2K'-1} \binom{R}{s} \right). \end{aligned}$$

Thus for any $J \in \mathbb{N}$, we have

$$\mathscr{V} = \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid mg}} \big(1 - 1/\langle \varpi \rangle\big) + O\bigg(\sum_{s=J}^{R} \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} \bigg)$$

$$+ O\bigg(\hat{L}^{-1} \sum_{s=1}^{J} \binom{R}{s} \bigg).$$

To estimate the error terms, note that

$$\hat{L}^{-1} \sum_{s=1}^{J} \binom{R}{s} \ll \hat{L}^{-1} R^{J+1}.$$

Also, for $J \le s \le R$,

$$\sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} \le \frac{1}{s!} \bigg(\sum_{i=1}^{R} \frac{1}{\langle \varpi_i \rangle} \bigg)^s \le \frac{1}{s!} \bigg(\sum_{\langle \varpi \rangle \le \hat{Q}} \frac{1}{\langle \varpi \rangle} \bigg)^s$$

$$\le \frac{1}{s!} \big(\ln Q + c \big)^s.$$

The last inequality follows from Lemma 4 with c some fixed constant. It follows that for $J > 3(\ln Q + c)$,

$$\begin{aligned}
&\sum_{s=J}^{R} \sum_{1 \le i_1 < \cdots < i_s \le R} \prod_{j=1}^{s} \frac{\epsilon_{i_1} \cdots \epsilon_{i_s}}{\langle \varpi_{i_1} \rangle \cdots \langle \varpi_{i_s} \rangle} \\
&\le \sum_{s=J}^{R} \frac{1}{s!} (\ln Q + c)^s \\
&\le \frac{(\ln Q + c)^J}{J!} \bigg(1 + \frac{\ln Q + c}{J+1} + \frac{(\ln Q + c)^2}{(J+1)(J+2)} + \cdots \bigg) \\
&\le \frac{(\ln Q + c)^J}{J!} \big(1 + 1/3 + 1/3^2 + \cdots \big) \\
&\ll \bigg(\frac{e \ln(e^c Q)}{J} \bigg)^J.
\end{aligned}$$

The last inequality follows from Stirling's formula, namely that $J! = \sqrt{2\pi J}(J/e)^J\big(1 + O(1/J)\big)$. Thus we have

$$\mathscr{V} = \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid mg}} \big(1 - 1/\langle \varpi \rangle\big) + O\bigg(\bigg(\frac{e \ln(e^c Q)}{J} \bigg)^J + \hat{L}^{-1} R^{J+1} \bigg).$$

Since $R \ll \hat{Q} \ll N^A$, by choosing $J = N/(2A \log_q N)$, we have

$$\left(\frac{e \ln(e^c Q)}{J}\right)^J \ll \hat{N}^{-1/(2A)+\epsilon} \qquad \text{and} \qquad \hat{L}^{-1} R^{J+1} \ll \hat{N}^{-1/2+\epsilon}.$$

Thus

$$\mathscr{V} = \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid mg}} \big(1 - 1/\langle \varpi \rangle\big) + O\big(\hat{N}^{-1/(2A)+\epsilon} + \hat{N}^{-1/2+\epsilon}\big).$$

By Lemma 4, we have

$$\prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid m}} \big(1 - 1/\langle \varpi \rangle\big)^{-1} \le \prod_{\langle \varpi \rangle \le \hat{Q}} \big(1 - 1/\langle \varpi \rangle\big)^{-1} \ll Q \ll \log_q N.$$

It follows that

$$\begin{aligned} &\sum_{n \in Y} \lambda^{(Q)}_{b,m,N}(n) \\ &= \frac{\hat{L}}{\hat{N}} \Bigg(\prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid m}} \big(1 - 1/\langle \varpi \rangle\big)^{-1} \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid mg}} \big(1 - 1/\langle \varpi \rangle\big) + O\big(\hat{N}^{-1/(2A)+\epsilon} + \hat{N}^{-1/2+\epsilon}\big) \Bigg). \end{aligned}$$

This completes the proof of the lemma.

For a polynomial $x \in \mathbb{F}_q[t]$, we say that x is $\hat{Q}$-*smooth* if for all monic irreducible polynomials ϖ with $\varpi | x$, we have $\langle \varpi \rangle \le \hat{Q}$.

Lemma 14. *Suppose that $a, g \in \mathbb{F}_q[t]$ with g monic, $(a, g) = 1$ and $\langle g \rangle \le N^B$. Also, suppose that $1 \le Q \le K$. For σ defined as in Lemma 9, one has*

$$\sigma_{a,g}(\lambda^{(Q)}_{b,m,N}) = \begin{cases} \frac{\langle g \rangle \mu(g)}{\phi(g)} e\big(\frac{-ab\bar{m}}{g}\big), & \text{if } (m, g) = 1 \text{ and } g \text{ is } \hat{Q}\text{-smooth}, \\ 0, & \text{otherwise}, \end{cases}$$

where $\bar{m}$ is the multiplicative inverse of m modulo g.

Proof. By Lemma 13, we have

$$\begin{aligned} \sigma_{a,g}(\lambda^{(Q)}_{b,m,N}) &= \sum_{\langle r \rangle < \langle g \rangle} e\left(\frac{ar}{g}\right) \gamma_{r,g}(\lambda^{(Q)}_{b,m,N}) \\ &= \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid m}} \big(1 - 1/\langle \varpi \rangle\big)^{-1} \prod_{\substack{\langle \varpi \rangle \le \hat{Q} \\ \varpi \nmid mg}} \big(1 - 1/\langle \varpi \rangle\big) \sum_{\substack{\langle r \rangle < \langle g \rangle \\ (mr+b, mg) \text{ is } \hat{Q}\text{-rough}}} e\left(\frac{ar}{g}\right). \end{aligned}$$

Note that if $(m,g)=1$ and g is $\hat{Q}$-smooth, then

$$\prod_{\substack{\langle\varpi\rangle\le\hat{Q}\\ \varpi\nmid m}}\left(1-1/\langle\varpi\rangle\right)^{-1}\prod_{\substack{\langle\varpi\rangle\le\hat{Q}\\ \varpi\nmid mg}}\left(1-1/\langle\varpi\rangle\right)=\langle g\rangle/\phi(g).$$

Thus to prove the lemma, it is enough to show that

$$\sum_{\substack{\langle r\rangle<\langle g\rangle\\ (mr+b,mg)\text{ is }\hat{Q}\text{-rough}}}e\left(\frac{ar}{g}\right)=\begin{cases}\mu(g)e\left(\frac{-ab\bar{m}}{g}\right), & \text{if } (m,g)=1 \text{ and } g \text{ is } \hat{Q}\text{-smooth},\\ 0, & \text{otherwise.}\end{cases}$$

Let

$$g_2=\prod_{\substack{\langle\varpi\rangle\le\hat{Q}\\ \varpi^z\| g,\ \varpi\nmid m}}\varpi^z,$$

and $g_3=g/g_2$. If $\varpi|m$, then $\varpi\nmid(mr+b)$. Thus $(mr+b,mg)=(mr+b,g)$, and

$$\sum_{\substack{\langle r\rangle<\langle g\rangle\\ (mr+b,mg)\text{ is }\hat{Q}\text{-rough}}}e\left(\frac{ar}{g}\right)=\sum_{\substack{\langle r\rangle<\langle g\rangle\\ (mr+b,g_2)=1}}e\left(\frac{ar}{g}\right).$$

Note that $(m,g)=1$ and that g is $\hat{Q}$-smooth if and only if $g_3=1$. Then using a similar argument as the one in the proof of Lemma 12 (with g_0 replaced by g_2 and g_1 replaced by g_3), we can show that

$$\sum_{\substack{\langle r\rangle<\langle g\rangle\\ (mr+b,g_2)=1}}e\left(\frac{ar}{g}\right)=\begin{cases}\mu(g)e\left(\frac{-ab\bar{m}}{g}\right), & \text{if } (m,g)=1 \text{ and } g \text{ is } \hat{Q}\text{-smooth},\\ 0, & \text{otherwise.}\end{cases}$$

This completes the proof of the lemma.

We now summarize the major arc contribution to Proposition 6.

Lemma 15. *For $1\le Q\le K$, we have*

$$\sup_{\alpha\in\mathfrak{M}}|\lambda^{\wedge}_{b,m,N}(\alpha)-\lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha)|\ll\hat{Q}^{-1}.$$

Proof. Let $\alpha\in\mathfrak{M}$. Then there exists $a,g\in\mathbb{F}_q[t]$ with g monic, $(a,g)=1$, $\langle\alpha-a/g\rangle<N^B/\left(\langle g\rangle\hat{N}\right)$ and $\langle g\rangle\le\hat{N}/N^B$. By combining Lemmas 9, 11, 12, 13 and 14, if g is $\hat{Q}$-smooth, we have

$$|\lambda^{\wedge}_{b,m,N}(\alpha)-\lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha)|\ll N^{B+1+\epsilon}\langle m\rangle^{1/2+\epsilon}\hat{N}^{-1/2}+\hat{N}^{-1/(2A)+\epsilon}+\hat{N}^{-1/2+\epsilon}\ll\hat{Q}^{-1}.$$

If g is not $\hat{Q}$-smooth, then there exists an irreducible polynomial ϖ with $\langle \varpi \rangle > \hat{Q}$ and $\varpi | g$. It follows that $\phi(g) \geq \phi(\varpi) = \langle \varpi \rangle - 1 \gg \hat{Q}$. Thus we have

$$\begin{aligned} |\lambda^{\wedge}_{b,m,N}(\alpha) - \lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha)| &\leq |\lambda^{\wedge}_{b,m,N}(\alpha)| + |\lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha)| \\ &\ll 1/\phi(g) + N^{B+1+\epsilon} \langle m \rangle^{1/2+\epsilon} \hat{N}^{-1/2} + \hat{N}^{-1/(2A)+\epsilon} + \hat{N}^{-1/2+\epsilon} \\ &\ll \hat{Q}^{-1}. \end{aligned}$$

This completes the proof of the lemma.

4.2 Minor Arc Estimates

We will now turn our attention to obtaining a minor arc estimate for $\lambda_{b,m,N}(\alpha)$. We will obtain the following result.

Lemma 16. *Suppose that $\langle m \rangle \leq N$. One has*

$$\sup_{\alpha \in \mathfrak{m}} |\lambda^{\wedge}_{b,m,N}(\alpha)| \ll N^{6-B/2} = N^{-A},$$

where $A = 4/(\delta - 2)$ and $B = 2A + 12$ are defined as in Sects. 2 and 3.

In order to prove this lemma, we need to establish more notation. Whenever a sum has a superscript $+$, which will look like $\sum^{+}$, the sum will be restricted to monic polynomials. Let $R \in \mathbb{N}$, and let U be a parameter with $1 \leq U < R/2$. Define τ_x by

$$\tau_x = \sum_{\substack{d|x \\ \langle d \rangle \leq \hat{U}}}^{+} \mu(d). \tag{5}$$

Let

$$\Lambda(y) = \begin{cases} \operatorname{ord} \varpi, & \text{when } y = \varpi^l \text{ for some monic, irreducible polynomial } \varpi \text{ and } l \in \mathbb{N}, \\ 0, & \text{otherwise.} \end{cases}$$

We now will present a sequence of lemmas concerning the weighted exponential sum

$$\sum_{\substack{\langle y \rangle \leq \hat{R} \\ y \equiv b \,(\mathrm{mod}\, m)}}^{+} \Lambda(y) e(\alpha y);$$

from these lemmas, we will be able to extract Lemma 16. Due to the underlying shape of Dirichlet series in $\mathbb{F}_q[t]$, we are unable to take an approach similar to that in [1]. Instead, we will follow the ideas of [26, Chap. 3].

Lemma 17. *Let $\upsilon(x,y)$ denote a function on $\mathbb{F}_q[t]^2$. Then we have*

$$\sum_{\hat{U}<\langle y\rangle\le\hat{R}}^{+}\upsilon(1,y)+\sum_{\hat{U}<\langle x\rangle\le\hat{R}}^{+}\sum_{\hat{U}<\langle y\rangle\le\hat{R}/\langle x\rangle}^{+}\tau_x\upsilon(x,y)=\sum_{\langle d\rangle\le\hat{U}}^{+}\sum_{\hat{U}<\langle y\rangle\le\hat{R}/\langle d\rangle}^{+}\sum_{\langle z\rangle\le\hat{R}/\langle yd\rangle}^{+}\mu(d)\upsilon(dz,y).$$

Proof. By writing $x=dz$, we have

$$\begin{aligned}\sum_{\langle d\rangle\le\hat{U}}^{+}\sum_{\hat{U}<\langle y\rangle\le\hat{R}/\langle d\rangle}^{+}\sum_{\langle z\rangle\le\hat{R}/\langle yd\rangle}^{+}\mu(d)\upsilon(dz,y)&=\sum_{\hat{U}<\langle x\rangle\le\hat{R}}^{+}\sum_{\hat{U}<\langle y\rangle\le\hat{R}/\langle x\rangle}^{+}\upsilon(x,y)\sum_{\substack{d|x\\ \langle d\rangle\le\hat{U}}}^{+}\mu(d)\\&\quad+\sum_{\langle x\rangle\le\hat{U}}^{+}\sum_{\hat{U}<\langle y\rangle\le\hat{R}/\langle x\rangle}^{+}\upsilon(x,y)\sum_{\substack{d|x\\ \langle d\rangle\le\hat{U}}}^{+}\mu(d).\end{aligned}\tag{6}$$

For $\langle x\rangle\le\hat{U}$, we have

$$\sum_{\substack{d|x\\ \langle d\rangle\le\hat{U}}}^{+}\mu(d)=\begin{cases}1, & \text{when } x=1,\\ 0, & \text{otherwise.}\end{cases}$$

Thus

$$\sum_{\langle x\rangle\le\hat{U}}^{+}\sum_{\hat{U}<\langle y\rangle\le\hat{R}/\langle x\rangle}^{+}\upsilon(x,y)\sum_{\substack{d|x\\ \langle d\rangle\le\hat{U}}}^{+}\mu(d)=\sum_{\hat{U}<\langle y\rangle\le\hat{R}}^{+}\upsilon(1,y).\tag{7}$$

The lemma now follows from (5), (6) and (7).

Let

$$S_1(\alpha)=\sum_{\substack{\langle y\rangle\le\hat{U}\\ y\equiv b\,(\mathrm{mod}\,m)}}^{+}\Lambda(y)e(\alpha y),\qquad S_2(\alpha)=\sum_{\substack{\langle xy\rangle\le\hat{R}\\ \langle x\rangle\le\hat{U}\\ xy\equiv b\,(\mathrm{mod}\,m)}}^{+}\mu(x)(\mathrm{ord}\,y)e(\alpha xy),$$

$$S_3(\alpha)=\sum_{\substack{\langle xy\rangle\le\hat{R}\\ \langle x\rangle\le\hat{U}^2\\ xy\equiv b\,(\mathrm{mod}\,m)}}^{+}\sum_{\substack{x=uv\\ \langle u\rangle,\langle v\rangle\le\hat{U}}}^{+}\mu(u)\Lambda(v)e(\alpha xy),$$

and

$$S_4(\alpha)=\sum_{\substack{\langle xy\rangle\le\hat{R}\\ \langle x\rangle,\langle y\rangle>\hat{U}\\ xy\equiv b\,(\mathrm{mod}\,m)}}^{+}\tau_x\Lambda(y)e(\alpha xy).$$

Lemma 18. *One has*

$$\sum_{\substack{\langle y\rangle\leq\hat{R}\\ y\equiv b\,(\mathrm{mod}\,m)}}^{+}\Lambda(y)e(\alpha y)=S_1(\alpha)+S_2(\alpha)-S_3(\alpha)-S_4(\alpha).$$

Proof. Let

$$\upsilon(x,y)=\begin{cases}\Lambda(y)e(\alpha xy), & \text{when } xy\equiv b\,(\mathrm{mod}\,m),\\ 0, & \text{otherwise.}\end{cases}$$

We first notice that

$$\sum_{\substack{\langle y\rangle\leq\hat{R}\\ y\equiv b\,(\mathrm{mod}\,m)}}^{+}\Lambda(y)e(\alpha y)=S_1(\alpha)+\sum_{\hat{U}<\langle y\rangle\leq\hat{R}}^{+}\upsilon(1,y).$$

Thus we are left to show that

$$\sum_{\hat{U}<\langle y\rangle\leq\hat{R}}^{+}\upsilon(1,y)+S_4(\alpha)=S_2(\alpha)-S_3(\alpha).$$

Applying Lemma 17, we have

$$\sum_{\hat{U}<\langle y\rangle\leq\hat{R}}^{+}\upsilon(1,y)+S_4(\alpha)=\sum_{\langle d\rangle\leq\hat{U}}^{+}\sum_{\hat{U}<\langle y\rangle\leq\hat{R}/\langle d\rangle}^{+}\sum_{\langle z\rangle\leq\hat{R}/\langle yd\rangle}^{+}\mu(d)\upsilon(dz,y).\tag{8}$$

Since

$$S_3(\alpha)=\sum_{\langle d\rangle\leq\hat{U}}^{+}\sum_{\langle y\rangle\leq\hat{U}}^{+}\sum_{\langle z\rangle\leq\hat{R}/\langle yd\rangle}^{+}\mu(d)\upsilon(dz,y),$$

by combining this with (8), we find that

$$\begin{aligned}\sum_{\hat{U}\leq\langle y\rangle\leq\hat{R}}^{+}\upsilon(1,y)+S_4(\alpha)&=\sum_{\langle d\rangle\leq\hat{U}}^{+}\sum_{\langle y\rangle\leq\hat{R}/\langle d\rangle}^{+}\sum_{\langle z\rangle\leq\hat{R}/\langle yd\rangle}^{+}\mu(d)\upsilon(dz,y)-S_3(\alpha)\\&=\sum_{\langle d\rangle\leq\hat{U}}^{+}\sum_{\langle y\rangle\leq\hat{R}/\langle d\rangle}^{+}\sum_{\substack{\langle z\rangle\leq\hat{R}/\langle yd\rangle\\ dyz\equiv b\,(\mathrm{mod}\,m)}}^{+}\mu(d)\Lambda(y)e(\alpha dyz)-S_3(\alpha)\\&=\sum_{\langle d\rangle\leq\hat{U}}^{+}\sum_{\substack{\langle w\rangle\leq\hat{R}/\langle d\rangle\\ dw\equiv b\,(\mathrm{mod}\,m)}}^{+}\mu(d)e(\alpha dw)\sum_{v|w}^{+}\Lambda(v)-S_3(\alpha)\end{aligned}$$

$$= \sideset{}{^+}\sum_{\langle d\rangle \le \hat{U}} \sideset{}{^+}\sum_{\substack{\langle w\rangle \le \hat{R}/\langle d\rangle \\ dw \equiv b \,(\mathrm{mod}\, m)}} \mu(d)(\mathrm{ord}\, w) e(\alpha dw) - S_3(\alpha)$$

$$= S_2(\alpha) - S_3(\alpha).$$

The lemma now follows.

We will now obtain upper bounds for the sums $S_1(\alpha)$, $S_2(\alpha)$, $S_3(\alpha)$ and $S_4(\alpha)$.

Lemma 19. *One has*

$$S_1(\alpha) \ll \hat{U}U.$$

Proof. By applying the triangle inequality and the trivial bound, we have

$$S_1(\alpha) \ll \sideset{}{^+}\sum_{\substack{\langle y\rangle \le \hat{U} \\ y \equiv b \,(\mathrm{mod}\, m)}} \Lambda(y) \ll \hat{U}U.$$

Lemma 20. *Suppose that $\langle \alpha - a/g\rangle < \langle g\rangle^{-2}$ with $(a, g) = 1$. Assume that $S, R \in \mathbb{N}$ with $S \le R$. Then for any real number T with $T \le \hat{R}/\hat{S}$, we have*

$$\sideset{}{^+}\sum_{\langle x\rangle \le \hat{S}} \left| \sideset{}{^+}\sum_{T < \langle y\rangle \le \hat{R}/\langle x\rangle} e(\alpha xy) \right| \ll \hat{R}S\langle g\rangle^{-1} + \hat{S}R + \langle g\rangle(RS + \mathrm{ord}\, g).$$

Proof. By the triangle inequality, we have

$$\sideset{}{^+}\sum_{\langle x\rangle \le \hat{S}} \left| \sideset{}{^+}\sum_{T < \langle y\rangle \le \hat{R}/\langle x\rangle} e(\alpha xy) \right| \le \sideset{}{^+}\sum_{\langle x\rangle \le \hat{S}} \sum_{W=0}^{R-\mathrm{ord}\, x} \left| \sideset{}{^+}\sum_{\langle y\rangle = \hat{W}} e(\alpha xy) \right|. \tag{9}$$

Also, it was proved in [10, Lemma 7] that

$$\left| \sideset{}{^+}\sum_{\langle y\rangle = \hat{W}} e(\alpha xy) \right| = \begin{cases} \hat{W}, & \text{when } \langle \|\alpha x\|\rangle < \hat{W}^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Thus we have

$$\sideset{}{^+}\sum_{\langle x\rangle \le \hat{S}} \sum_{W=0}^{R-\mathrm{ord}\, x} \left| \sideset{}{^+}\sum_{\langle y\rangle = \hat{W}} e(\alpha xy) \right|$$

$$= \sideset{}{^+}\sum_{\langle x\rangle \le \hat{S}} \sum_{W=0}^{\min(R-\mathrm{ord}\, x,\, -\mathrm{ord}\, \|\alpha x\| - 1)} \hat{W}$$

$$\begin{aligned}
&\ll \sum_{\langle x\rangle\le \hat{S}}^{+} \min\left(\hat{R}/\langle x\rangle, \langle\|\alpha x\|\rangle^{-1}\right)\\
&\ll \sum_{\langle x\rangle<\langle g\rangle}^{+} \langle\|\alpha x\|\rangle^{-1} + \sum_{W=\operatorname{ord} g}^{S} \sum_{\langle x\rangle=\hat{W}}^{+} \min\left(\hat{R}/\langle x\rangle, \langle\|\alpha x\|\rangle^{-1}\right)\\
&= E_1 + E_2, \qquad (10)
\end{aligned}$$

where

$$E_1 = \sum_{\langle x\rangle<\langle g\rangle}^{+} \langle\|\alpha x\|\rangle^{-1} \qquad \text{and} \qquad E_2 = \sum_{W=\operatorname{ord} g}^{S} \sum_{\langle x\rangle=\hat{W}}^{+} \min\left(\hat{R}/\langle x\rangle, \langle\|\alpha x\|\rangle^{-1}\right).$$

We first bound E_1. For $\langle x\rangle < \langle g\rangle$, since $\langle \alpha - a/g\rangle < \langle g\rangle^{-2}$, we have

$$\left\langle \alpha x - \frac{ax}{g}\right\rangle < \frac{\langle x\rangle}{\langle g\rangle^2} < \frac{1}{\langle g\rangle}.$$

Since $\langle\|ax/g\|\rangle \ge \langle g\rangle^{-1}$, we deduce that

$$\langle\|\alpha x\|\rangle = \left\langle \Big\| \frac{ax}{g} + \big(\alpha - \frac{a}{g}\big)x\Big\|\right\rangle = \left\langle \Big\| \frac{ax}{g}\Big\| + \big(\alpha - \frac{a}{g}\big)x\right\rangle = \left\langle \Big\| \frac{ax}{g}\Big\|\right\rangle.$$

Since $(a, g) = 1$, we have

$$\begin{aligned}
E_1 \le \sum_{\langle x\rangle<\langle g\rangle} \langle\|\alpha x\|\rangle^{-1} &= \sum_{\langle x\rangle<\langle g\rangle} \left\langle \Big\| \frac{ax}{g}\Big\|\right\rangle^{-1} = \sum_{\langle y\rangle<\langle g\rangle} \left\langle \Big\| \frac{y}{g}\Big\|\right\rangle^{-1}\\
&\ll \sum_{W=0}^{\operatorname{ord} g-1} \hat{W}\Big(\frac{\langle g\rangle}{\hat{W}}\Big) \ll \langle g\rangle(\operatorname{ord} g). \qquad (11)
\end{aligned}$$

We are now left to bound E_2. Note that

$$\begin{aligned}
E_2 &= \sum_{W=\operatorname{ord} g}^{S} \Bigg(\sum_{\substack{\langle x\rangle=\hat{W}\\ \langle\|\alpha x\|\rangle^{-1}\ge \hat{R}/\hat{W}}}^{+} \frac{\hat{R}}{\hat{W}} + \sum_{V=0}^{R-W-1} \sum_{\substack{\langle x\rangle=\hat{W}\\ \langle\|\alpha x\|\rangle^{-1}=\hat{V}}}^{+} \hat{V}\Bigg)\\
&\le \sum_{W=\operatorname{ord} g}^{S} \sum_{V=0}^{R-W} \sum_{\substack{\langle x\rangle=\hat{W}\\ \langle\|\alpha x\|\rangle^{-1}\ge \hat{V}}}^{+} \hat{V} \le \sum_{W=\operatorname{ord} g}^{S} \sum_{V=0}^{R-W} \sum_{\substack{\langle x\rangle<q\hat{W}\\ \langle\|\alpha x\|\rangle<q\hat{V}^{-1}}} \hat{V}.
\end{aligned}$$

By [10, Lemma 7], we deduce that

$$E_2 \ll \sum_{W=\operatorname{ord} g}^{S} \sum_{V=0}^{R-W} \sum_{\langle x\rangle<q\hat{W}} \Big| \sum_{\langle y\rangle<\hat{V}q^{-1}} e(\alpha xy)\Big|.$$

We now apply [15, Lemma 11.1] to get

$$\sum_{\langle x\rangle<q\hat{W}} \Big| \sum_{\langle y\rangle<\hat{V}q^{-1}} e(\alpha xy)\Big| \ll \hat{W}\hat{V}\Big(\langle g\rangle^{-1} + \hat{W}^{-1} + \hat{V}^{-1} + \langle g\rangle\hat{W}^{-1}\hat{V}^{-1}\Big).$$

Using this bound, we see that

$$\begin{aligned} E_2 &\ll \sum_{W=\operatorname{ord} g}^{S} \sum_{V=0}^{R-W} \hat{W}\hat{V}\Big(\langle g\rangle^{-1} + \hat{W}^{-1} + \hat{V}^{-1} + \langle g\rangle\hat{W}^{-1}\hat{V}^{-1}\Big) \\ &\ll \sum_{W=\operatorname{ord} g}^{S} \Big(\hat{R}\langle g\rangle^{-1} + \hat{R}\hat{W}^{-1} + \hat{W}R + \langle g\rangle R\Big) \\ &\ll \hat{R}S\langle g\rangle^{-1} + \hat{S}R + \langle g\rangle RS. \end{aligned} \tag{12}$$

The lemma now follows by combining (9)–(12).

Lemma 21. *Suppose that* $\langle \alpha - a/g\rangle < \langle g\rangle^{-2}$ *with* $(a, g) = 1$ *and* $\operatorname{ord} m < U$. *Then one has*

$$S_2(\alpha) \ll \hat{U}\langle m\rangle R^2 + \hat{R}R^2\langle g\rangle^{-1} + \langle g\rangle R(R^2 + \operatorname{ord} g).$$

Proof. Note that

$$\begin{aligned} S_2(\alpha) &= \sideset{}{^+}\sum_{\substack{\langle xy\rangle\le\hat{R}\\ \langle x\rangle\le\hat{U}\\ xy\equiv b\,(\mathrm{mod}\,m)}} \mu(x)(\operatorname{ord} y)e(\alpha xy) \\ &= \sideset{}{^+}\sum_{\langle x\rangle\le\hat{U}} \mu(x) \sideset{}{^+}\sum_{\substack{\langle y\rangle\le\hat{R}/\langle x\rangle\\ xy\equiv b\,(\mathrm{mod}\,m)}} e(\alpha xy)\int_1^{\langle y\rangle}\frac{dt}{t\log q} \\ &= \sideset{}{^+}\sum_{\langle x\rangle\le\hat{U}} \mu(x)\int_1^{\hat{R}/\langle x\rangle}\Bigg(\sideset{}{^+}\sum_{\substack{t<\langle y\rangle\le\hat{R}/\langle x\rangle\\ xy\equiv b\,(\mathrm{mod}\,m)}} e(\alpha xy)\Bigg)\frac{dt}{t\log q}. \end{aligned}$$

By two applications of the triangle inequality, we get

$$S_2(\alpha) \ll \sideset{}{^+}\sum_{\langle x\rangle\le\hat{U}} \int_1^{\hat{R}/\langle x\rangle} \Bigg|\sideset{}{^+}\sum_{\substack{t<\langle y\rangle\le\hat{R}/\langle x\rangle\\ xy\equiv b\,(\mathrm{mod}\,m)}} e(\alpha xy)\Bigg|\frac{dt}{t}.$$

Switching the leftmost sum with the integral in the last expression, we obtain

$$S_2(\alpha) \ll \int_1^{\hat{R}} \sum_{\langle x\rangle \le \min(\hat{U}, \hat{R}/t)}^{+} \Big| \sum_{\substack{t<\langle y\rangle \le \hat{R}/\langle x\rangle \\ xy \equiv b \,(\mathrm{mod}\, m)}}^{+} e(\alpha xy)\Big| \frac{dt}{t} \ll \int_1^{\hat{R}} \sum_{\substack{\langle x\rangle \le \hat{U} \\ (x,m)=1}}^{+} \Big| \sum_{\substack{t<\langle y\rangle \le \hat{R}/\langle x\rangle \\ y \equiv \bar{x}b \,(\mathrm{mod}\, m)}}^{+} e(\alpha xy)\Big| \frac{dt}{t},$$

where $\bar{x}$ is the multiplicative inverse of x modulo m. We now split the sum over y into two sums depending on whether or not $\langle y\rangle \le \langle m\rangle$. Write $y = \bar{x}b + my'$ and $x' = mx$. Then by the triangle inequality, we have

$$\begin{aligned} S_2(\alpha) &\ll \int_1^{\hat{R}} \hat{U}\langle m\rangle \frac{dt}{t} + \int_1^{\hat{R}} \sum_{\substack{\langle x\rangle \le \hat{U} \\ (x,m)=1}}^{+} \Big| \sum_{\substack{\max(t,\langle m\rangle)<\langle y\rangle \le \hat{R}/\langle x\rangle \\ y \equiv \bar{x}b \,(\mathrm{mod}\, m)}}^{+} e(\alpha xy)\Big| \frac{dt}{t} \\ &\ll \hat{U}\langle m\rangle R + \int_1^{\hat{R}} \sum_{\substack{\langle x\rangle \le \hat{U} \\ (x,m)=1}}^{+} \Big| \sum_{\max(t/\langle m\rangle,1)<\langle y'\rangle \le \hat{R}/\langle mx\rangle}^{+} e(\alpha mxy')\Big| \big|e(\alpha b)\big| \frac{dt}{t} \\ &\ll \hat{U}\langle m\rangle R + \int_1^{\hat{R}} \sum_{\langle x'\rangle \le \hat{U}\langle m\rangle}^{+} \Big| \sum_{\max(t/\langle m\rangle,1)<\langle y'\rangle \le \hat{R}/\langle x'\rangle}^{+} e(\alpha x'y')\Big| \frac{dt}{t}. \end{aligned}$$

Since $\operatorname{ord} m < U < R$, by Lemma 20, we deduce that

$$\begin{aligned} S_2(\alpha) &\ll \hat{U}\langle m\rangle R + \int_1^{\hat{R}} \Big(\hat{R}(U + \operatorname{ord} m)\langle g\rangle^{-1} + \hat{U}\langle m\rangle R \\ &\quad + \langle g\rangle((U + \operatorname{ord} m)R + \operatorname{ord} g)) \frac{dt}{t} \\ &\ll \hat{U}\langle m\rangle R^2 + \hat{R}R^2\langle g\rangle^{-1} + \langle g\rangle R(R^2 + \operatorname{ord} g). \end{aligned}$$

This completes the proof of the lemma.

Lemma 22. *Suppose that* $\langle \alpha - a/g\rangle < \langle g\rangle^{-2}$ *with* $(a, g) = 1$ *and* $\operatorname{ord} m < U$. *Then one has*

$$S_3(\alpha) \ll \hat{R}R^2\langle g\rangle^{-1} + \hat{U}^2\langle m\rangle R^2 + \langle g\rangle R(R^2 + \operatorname{ord} g).$$

Proof. For any $\langle x\rangle \le \hat{U}^2$, we have

$$\sum_{\substack{x=uv \\ \langle u\rangle,\langle v\rangle \le \hat{U}}}^{+} \mu(u)\Lambda(v) \ll \sum_{v|x}^{+} \Lambda(v) = \operatorname{ord} x \ll R.$$

Write $y = \bar{x}b + my'$ and $x' = mx$, where $\bar{x}$ is the multiplicative inverse of x modulo m. Then from the above inequality, we deduce that

$$\begin{aligned}
S_3(\alpha) &= \sideset{}{^+}\sum_{\substack{\langle xy\rangle\le \hat{R}\\ \langle x\rangle\le \hat{U}^2\\ xy\equiv b\,(\mathrm{mod}\,m)}} \sideset{}{^+}\sum_{\substack{x=uv\\ \langle u\rangle,\langle v\rangle\le \hat{U}}} \mu(u)\Lambda(v)e(\alpha xy)\\
&\ll \sideset{}{^+}\sum_{\langle x\rangle\le \hat{U}^2} \Big| \sideset{}{^+}\sum_{\substack{x=uv\\ \langle u\rangle,\langle v\rangle\le \hat{U}}} \mu(u)\Lambda(v)\Big| \cdot \Big| \sideset{}{^+}\sum_{\substack{\langle y\rangle\le \hat{R}/\langle x\rangle\\ xy\equiv b\,(\mathrm{mod}\,m)}} e(\alpha xy)\Big|\\
&\ll R \sideset{}{^+}\sum_{\substack{\langle x\rangle\le \hat{U}^2\\ (x,m)=1}} \Big| \sideset{}{^+}\sum_{\substack{\langle y\rangle\le \hat{R}/\langle x\rangle\\ y\equiv \bar{x}b\,(\mathrm{mod}\,m)}} e(\alpha xy)\Big|\\
&= R \sideset{}{^+}\sum_{\substack{\langle x\rangle\le \hat{U}^2\\ (x,m)=1}} \Big| \sideset{}{^+}\sum_{\langle y'\rangle\le \hat{R}/\langle mx\rangle} e(\alpha mxy')\Big|\\
&\ll R \sideset{}{^+}\sum_{\langle x'\rangle\le \hat{U}^2\langle m\rangle} \Big| \sideset{}{^+}\sum_{\langle y'\rangle\le \hat{R}/\langle x'\rangle} e(\alpha x'y')\Big|.
\end{aligned}$$

Since $\operatorname{ord} m < U < R$, by Lemma 20, we obtain that

$$\begin{aligned}
S_3(\alpha) &\ll R\big(\hat{R}(2U+\operatorname{ord} m)\langle g\rangle^{-1} + \hat{U}^2\langle m\rangle R + \langle g\rangle((2U+\operatorname{ord} m)R + \operatorname{ord} g)\big)\\
&\ll \hat{R}R^2\langle g\rangle^{-1} + \hat{U}^2\langle m\rangle R^2 + \langle g\rangle R(R^2+\operatorname{ord} g).
\end{aligned}$$

This completes the proof of the lemma.

Lemma 23. *Suppose that* $\langle \alpha - a/g\rangle < \langle g\rangle^{-2}$ *with* $(a,g)=1$ *and* $\operatorname{ord} m \le U$. *Then one has*

$$S_4(\alpha) \ll \hat{R}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{-1/2} + \hat{R}R^{9/2}\langle m\rangle\hat{U}^{-1/2} + \hat{R}^{1/2}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{1/2}.$$

Proof. By writing $x = y_1z$, $z = rs$ and $y_1 = uv$, we have

$$\begin{aligned}
\sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv \tilde{x}\,(\mathrm{mod}\,m)}} |\tau_x|^2 &\le \sideset{}{^+}\sum_{\langle x\rangle=\hat{V}} \tau_x^2 \le \sideset{}{^+}\sum_{\langle x\rangle=\hat{V}} \Big(\sideset{}{^+}\sum_{y|x} 1\Big)^2 = \sideset{}{^+}\sum_{\langle y_1\rangle\le\hat{V}} \sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ y_1|x}} \sideset{}{^+}\sum_{y_2|x} 1\\
&= \sideset{}{^+}\sum_{\langle y_1\rangle\le\hat{V}} \sideset{}{^+}\sum_{\langle z\rangle=\hat{V}/\langle y_1\rangle} \sideset{}{^+}\sum_{y_2|y_1z} 1\\
&\le \sideset{}{^+}\sum_{\langle y_1\rangle\le\hat{V}} \sideset{}{^+}\sum_{d_1|y_1} \sideset{}{^+}\sum_{\langle z\rangle=\hat{V}/\langle y_1\rangle} \sideset{}{^+}\sum_{d_2|z} 1 = \sideset{}{^+}\sum_{\langle y_1\rangle\le\hat{V}} \sideset{}{^+}\sum_{d_1|y_1} \sideset{}{^+}\sum_{\substack{r,s\\ \langle rs\rangle=\hat{V}/\langle y_1\rangle}} 1\\
&\ll \hat{V}V \sideset{}{^+}\sum_{\langle y_1\rangle\le\hat{V}} \sideset{}{^+}\sum_{d_1|y_1} \langle y_1\rangle^{-1} = \hat{V}V \sideset{}{^+}\sum_{\substack{u,v\\ \langle uv\rangle\le\hat{V}}} \langle uv\rangle^{-1} \ll \hat{V}V^3.
\end{aligned} \tag{13}$$

Note that

$$S_4(\alpha) = \sideset{}{^+}\sum_{\substack{\langle xy\rangle\le \hat{R}\\ \langle x\rangle,\langle y\rangle>\hat{U}\\ xy\equiv b\,(\mathrm{mod}\,m)}} \tau_x \Lambda(y) e(\alpha xy)$$

$$= \sum_{\substack{U<V,W<R-U\\ V+W\le R}} \sum_{\substack{\tilde{x},\tilde{y}\\ \tilde{x}\tilde{y}\equiv b\,(\mathrm{mod}\,m)}} \sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} \tau_x \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}} \Lambda(y) e(\alpha xy).$$

Applying the Cauchy-Schwarz inequality and (13), we obtain that

$$\begin{aligned} S_4(\alpha) &\ll \sum_{\substack{U<V,W<R-U\\ V+W\le R}} \sum_{\substack{\tilde{x},\tilde{y}\\ \tilde{x}\tilde{y}\equiv b\,(\mathrm{mod}\,m)}} \Bigg(\sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} |\tau_x|^2 \Bigg)^{1/2} \\ &\quad \times \Bigg(\sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} \Bigg| \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}} \Lambda(y) e(\alpha xy) \Bigg|^2 \Bigg)^{1/2} \\ &\ll \sum_{\substack{U<V,W<R-U\\ V+W\le R}} \sum_{\substack{\tilde{x},\tilde{y}\\ \tilde{x}\tilde{y}\equiv b\,(\mathrm{mod}\,m)}} \hat{V}^{1/2} V^{3/2} \Bigg(\sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} \Bigg| \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}} \Lambda(y) e(\alpha xy) \Bigg|^2 \Bigg)^{1/2}. \end{aligned} \tag{14}$$

One has

$$\begin{aligned} &\sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} \Bigg| \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}} \Lambda(y) e(\alpha xy) \Bigg|^2 \\ &= \sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} \sideset{}{^+}\sum_{\substack{\langle y_1\rangle=\langle y_2\rangle=\hat{W}\\ y_1\equiv y_2\equiv\tilde{y}\,(\mathrm{mod}\,m)}} \Lambda(y_1)\Lambda(y_2) e(\alpha x(y_1-y_2)) \\ &= \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}} \sum_{\substack{\langle h\rangle<\hat{W}\\ h\equiv 0\,(\mathrm{mod}\,m)}} \Lambda(y)\Lambda(y+h) \sideset{}{^+}\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}} e(\alpha xh). \end{aligned} \tag{15}$$

For $(\tilde{x}, m) = (\tilde{y}, m) = 1$, $V + W \le R$ and $\langle m\rangle \le \min(\hat{V}, \hat{W})$, since $|\Lambda(z)| \le \operatorname{ord} z$, by writing $h = mh'$, $x = \tilde{x} + mx'$ and $h'' = m^2h'$, we have

$$\begin{aligned}
&\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}}^{+}\ \sum_{\substack{\langle h\rangle<\hat{W}\\ h\equiv 0\,(\mathrm{mod}\,m)}}\Lambda(y)\Lambda(y+h)\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}}^{+}e(\alpha xh)\\
&\quad\ll W^2\sum_{\substack{\langle y\rangle=\hat{W}\\ y\equiv\tilde{y}\,(\mathrm{mod}\,m)}}^{+}\ \sum_{\substack{\langle h\rangle<\hat{W}\\ h\equiv 0\,(\mathrm{mod}\,m)}}\Big|\sum_{\substack{\langle x\rangle=\hat{V}\\ x\equiv\tilde{x}\,(\mathrm{mod}\,m)}}^{+}e(\alpha xh)\Big|\\
&\quad=\frac{\hat{W}W^2}{\langle m\rangle}\sum_{\langle h'\rangle<\hat{W}/\langle m\rangle}\Big|\sum_{\langle x'\rangle=\hat{V}/\langle m\rangle}^{+}e(\alpha m^2x'h')\Big|\\
&\quad\ll\frac{\hat{W}W^2}{\langle m\rangle}\sum_{\langle h''\rangle<\hat{W}\langle m\rangle}\Big|\sum_{\langle x'\rangle=\hat{V}/\langle m\rangle}^{+}e(\alpha x'h'')\Big|.
\end{aligned}\tag{16}$$

When $V+W\le R$ and $U\le\min(V,W)$, it follows from [15, Lemma 11.1] that

$$\begin{aligned}
\sum_{\langle h''\rangle<\hat{W}\langle m\rangle}\Big|\sum_{\langle x'\rangle=\hat{V}/\langle m\rangle}^{+}e(\alpha x'h'')\Big|&\le\sum_{\langle h''\rangle<\hat{W}\langle m\rangle}\Big|\sum_{\langle x'\rangle<q\hat{V}/\langle m\rangle}e(\alpha x'h'')\Big|\\
&\ll\hat{W}\hat{V}\big(\langle g\rangle^{-1}+\hat{W}^{-1}\langle m\rangle^{-1}+\hat{V}^{-1}\langle m\rangle+\langle g\rangle(\hat{W}\hat{V})^{-1}\big)\\
&\ll\hat{R}\langle g\rangle^{-1}+\hat{R}\langle m\rangle\hat{U}^{-1}+\langle g\rangle.
\end{aligned}\tag{17}$$

Upon combining (14)–(17), we have

$$\begin{aligned}
S_4(\alpha)&\ll\sum_{\substack{U<V,W<R-U\\ V+W\le R}}\ \sum_{\substack{\tilde{x},\tilde{y}\\ \tilde{x}\tilde{y}\equiv b\,(\mathrm{mod}\,m)}}\hat{V}^{1/2}V^{3/2}\hat{W}^{1/2}W\langle m\rangle^{-1/2}\big(\hat{R}\langle g\rangle^{-1}\\
&\quad+\hat{R}\langle m\rangle\hat{U}^{-1}+\langle g\rangle\big)^{1/2}\\
&\ll\sum_{\substack{U<V,W<R-U\\ V+W\le R}}\hat{R}^{1/2}R^{5/2}\langle m\rangle^{1/2}\big(\hat{R}\langle g\rangle^{-1}+\hat{R}\langle m\rangle\hat{U}^{-1}+\langle g\rangle\big)^{1/2}\\
&\ll\hat{R}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{-1/2}+\hat{R}R^{9/2}\langle m\rangle\hat{U}^{-1/2}+\hat{R}^{1/2}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{1/2}.
\end{aligned}$$

Lemma 24. *Suppose that $\langle m\rangle\le\hat{R}^{2/5}R$, $\langle g\rangle<\hat{R}\langle m\rangle$ and $\langle\alpha-a/g\rangle<\langle g\rangle^{-2}$ with $(a,g)=1$. Then one has*

$$\begin{aligned}
\sum_{\substack{\langle y\rangle\le\hat{R}\\ y\equiv b\,(\mathrm{mod}\,m)}}^{+}\Lambda(y)e(\alpha y)&\ll\hat{R}^{4/5}\langle m\rangle R^4+\langle g\rangle R^3+\hat{R}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{-1/2}\\
&\quad+\hat{R}^{1/2}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{1/2}.
\end{aligned}$$

Proof. We deduce from Lemmas 18, 19, 21, 22 and 23 that when $\operatorname{ord} m \le U$, we have

$$\sum_{\substack{\langle y\rangle\le \hat{R}\\ y\equiv b \,(\mathrm{mod}\, m)}}^{+} \Lambda(y)e(\alpha y) \ll \hat{U}^2\langle m\rangle R^2 + \langle g\rangle R(R^2+\operatorname{ord} g) + \hat{R}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{-1/2}$$
$$+ \hat{R}R^{9/2}\langle m\rangle\hat{U}^{-1/2} + \hat{R}^{1/2}R^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{1/2}.$$

The lemma now follows by setting $\hat{U} = \hat{R}^{2/5}R$.

We will now derive Lemma 16 from Lemma 24.

Proof (of Lemma 16). Note that

$$\lambda^{\wedge}_{b,m,N}(\alpha) = \frac{(N+\operatorname{ord} m)\phi(m)}{\hat{N}\langle m\rangle} \sum_{\substack{\langle n\rangle=\hat{N}\\ mn+b \text{ irred}}}^{+} e(\alpha n)$$
$$= \frac{\phi(m)}{\hat{N}\langle m\rangle}\sum_{\langle n\rangle=\hat{N}}^{+}\Lambda(mn+b)e(\alpha n)$$
$$+ O\Big(\frac{N+\operatorname{ord} m}{\hat{N}}\Big(\sum_{\substack{\langle \varpi\rangle=(\hat{N}\langle m\rangle)^{1/2}\\ \varpi \text{ irred}}}^{+}\frac{1}{2} + \sum_{\substack{\langle \varpi\rangle=(\hat{N}\langle m\rangle)^{1/3}\\ \varpi \text{ irred}}}^{+}\frac{1}{3}+\cdots\Big)\Big)$$
$$= \frac{\phi(m)}{\hat{N}\langle m\rangle}\sum_{\langle n\rangle=\hat{N}}^{+}\Lambda(mn+b)e(\alpha n) + O\big(\hat{N}^{-1/2}\langle m\rangle^{1/2}\big).$$

By writing $x = mn+b$, we have

$$\lambda^{\wedge}_{b,m,N}(\alpha) = \frac{\phi(m)e(-\alpha b/m)}{\hat{N}\langle m\rangle}\sum_{\substack{\langle x\rangle=\hat{N}\langle m\rangle\\ x\equiv b\,(\mathrm{mod}\, m)}}^{+}\Lambda(x)e(\alpha x/m) + O\big(\hat{N}^{-1/2}\langle m\rangle^{1/2}\big).$$

By the triangle inequality, we deduce that

$$\lambda^{\wedge}_{b,m,N}(\alpha) \ll \hat{N}^{-1}\Big(\Big|\sum_{\substack{\langle x\rangle\le\hat{N}\langle m\rangle\\ x\equiv b\,(\mathrm{mod}\, m)}}^{+}\Lambda(x)e(\alpha x/m)\Big| + \Big|\sum_{\substack{\langle x\rangle\le q^{-1}\hat{N}\langle m\rangle\\ x\equiv b\,(\mathrm{mod}\, m)}}^{+}\Lambda(x)e(\alpha x/m)\Big|\Big)$$
$$+ \hat{N}^{-1/2}\langle m\rangle^{1/2}. \tag{18}$$

Let $\alpha \in \mathfrak{m}$. By Dirichlet's approximation theorem, there exist $a, g \in \mathbb{F}_q[t]$ with g monic, $\langle g\rangle \le \hat{N}\langle m\rangle/N^B$, $(a,g)=1$ and $\langle \alpha/m - a/g\rangle < N^B/(\langle mg\rangle\hat{N}) \le \langle g\rangle^{-2}$. Let $d=(g,m)$. Then

$$\left\langle \alpha - \frac{am/d}{g/d} \right\rangle < \frac{N^B}{\langle g\rangle \hat{N}} \le \frac{N^B}{\langle g/d\rangle \hat{N}}.$$

Since $\alpha \in \mathfrak{m}$, we must have $\langle g/d\rangle > N^B$, which implies that $\langle g\rangle > N^B\langle d\rangle \ge N^B$. By Lemma 24 and (18), we have

$$\begin{aligned}
&\lambda^{\wedge}_{b,m,N}(\alpha)\\
&\ll \hat{N}^{-1}\big(\hat{N}^{4/5}\langle m\rangle^{9/5}N^4 + \langle g\rangle N^3 + \hat{N}N^{9/2}\langle m\rangle^{3/2}\langle g\rangle^{-1/2} + \hat{N}^{1/2}N^{9/2}\langle m\rangle\langle g\rangle^{1/2}\big)\\
&\qquad + \hat{N}^{-1/2}\langle m\rangle^{1/2}\\
&\ll \hat{N}^{-1/5}N^{29/5} + N^{4-B} + N^{6-B/2} + \hat{N}^{-1/2}N^{1/2} \ll N^{6-B/2} = N^{-A}.
\end{aligned}$$

This completes the proof of the lemma.

We will next prove a minor arc estimate for $\lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha)$.

Lemma 25. *Let $1 \le Q \le K$ and $\langle m\rangle \le N$. Suppose that $\langle \alpha - a/g\rangle < \langle g\rangle^{-2}$ with $(a,g) = 1$. Then one has*

$$|\lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha)| \ll \log_q N\Big(N\langle g\rangle^{-1} + \hat{N}^{-1}\langle g\rangle(N^2 + \operatorname{ord} g) + \hat{N}^{-1/(3A)}N\Big).$$

Proof. Let $\{\varpi_1, \dots, \varpi_R\}$ denote the set of monic, irreducible polynomials ϖ with $\langle \varpi\rangle \le \hat{Q}$ and $\varpi \nmid m$. By the inclusion-exclusion principle, we have

$$\lambda^{(Q)^{\wedge}}_{b,m,N}(\alpha) = \sum_{n\in\mathscr{I}_N} \lambda^{(Q)}_{b,m,N}(n)e(\alpha n) = \hat{N}^{-1}\prod_{i=1}^{R}(1 - 1/\langle \varpi_i\rangle)^{-1}h(\alpha), \tag{19}$$

where

$$h(\alpha) = \sum_{s=0}^{R}(-1)^s \sum_{1\le i_1<\cdots<i_s\le R} \sideset{}{^+}\sum_{\substack{\langle y\rangle = \hat{N}\langle m\rangle/\langle \varpi_1\cdots\varpi_s\rangle \\ \varpi_{i_1}\cdots\varpi_{i_s}y \equiv b \,(\mathrm{mod}\, m)}} e\left(\alpha\left(\frac{\varpi_{i_1}\cdots\varpi_{i_s}y - b}{m}\right)\right). \tag{20}$$

By Lemma 4, we have

$$\prod_{i=1}^{R}\big(1 - 1/\langle \varpi_i\rangle\big)^{-1} \ll Q \ll \log_q N. \tag{21}$$

Let $J = N/(2A\log_q N)$. If $0 \le s \le J$, since $\langle \varpi_i\rangle \le \hat{Q} \le N^A$, we have

$$\prod_{j=1}^{s}\langle \varpi_{i_j}\rangle \le N^{AN/(2A\log_q N)} = N^{N/(2\log_q N)} = \hat{N}^{1/2}.$$

Therefore, by writing $y = \bar{x}b + my'$, where $\bar{x}$ is the multiplicative inverse of x modulo m, it follow from Lemma 20 that

$$\begin{aligned}
&\sum_{0\le s\le J}(-1)^s \sum_{1\le i_1<\cdots<i_s\le R} \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{N}\langle m\rangle/\langle \varpi_1\cdots\varpi_s\rangle\\ \varpi_{i_1}\cdots\varpi_{i_s}y\equiv b\,(\mathrm{mod}\,m)}} e\Big(\alpha\Big(\frac{\varpi_{i_1}\cdots\varpi_{i_s}y-b}{m}\Big)\Big)\\
&\quad\ll \sideset{}{^+}\sum_{\substack{\langle x\rangle\le \hat{N}^{1/2}\\ (x,m)=1}}\Big|\sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{N}\langle m\rangle/\langle x\rangle\\ xy\equiv b\,(\mathrm{mod}\,m)}} e\Big(\frac{\alpha xy}{m}\Big)\Big| \ll \sideset{}{^+}\sum_{\langle x\rangle\le\hat{N}^{1/2}}\Big|\sideset{}{^+}\sum_{\langle y'\rangle=\hat{N}/\langle x\rangle} e\big(\alpha xy'\big)\Big| \qquad (22)\\
&\quad\ll \hat{N}N\langle g\rangle^{-1}+\hat{N}^{1/2}N+\langle g\rangle(N^2+\mathrm{ord}\,g).
\end{aligned}$$

For $s > J$, we have

$$\begin{aligned}
&\sum_{J<s\le R}(-1)^s \sum_{1\le i_1<\cdots<i_s\le R} \sideset{}{^+}\sum_{\substack{\langle y\rangle=\hat{N}\langle m\rangle/\langle \varpi_1\cdots\varpi_s\rangle\\ \varpi_{i_1}\cdots\varpi_{i_s}y\equiv b\,(\mathrm{mod}\,m)}} e\Big(\alpha\Big(\frac{\varpi_{i_1}\cdots\varpi_{i_s}y-b}{m}\Big)\Big)\\
&\ll \sum_{J<s\le R}\sum_{1\le i_1<\cdots<i_s\le R}\hat{N}\langle m\rangle/\langle \varpi_{i_1}\cdots\varpi_{i_s}\rangle \qquad (23)\\
&\ll \hat{N}\langle m\rangle\sum_{J<s\le R}(s!)^{-1}\big(\langle\varpi_1\rangle^{-1}+\cdots+\langle\varpi_R\rangle^{-1}\big)^s\\
&\ll \hat{N}\langle m\rangle\sum_{J<s\le R}(s!)^{-1}(C_1\log_q\log_q N)^s,
\end{aligned}$$

where the last inequality follows from Lemma 4. By Stirling's formula, we have $s! = \sqrt{2\pi s}\big(\frac{s}{e}\big)^s\big(1+O\big(\frac{1}{s}\big)\big)$. Thus for $s > J = N/2A\log_q N$, we have

$$\begin{aligned}
\sum_{J<s\le R}(s!)^{-1}(C_1\log\log N)^s &\ll \sum_{J<s\le R} s^{-1/2}\Big(\frac{C_1 e\log_q\log_q N}{s}\Big)^s\\
&\ll \sum_{J<s\le R}\Big(\frac{2A\log_q N}{N}\Big)^{1/2}\Big(\frac{2C_1Ae\log_q N\log_q\log_q N}{N}\Big)^s\\
&\ll \Big(\frac{\log_q N}{N}\Big)^{1/2}\sum_{J<s\le R}N^{s\left(-1+o(1)\right)}\\
&\ll \Big(\frac{\log_q N}{N}\Big)^{1/2}N^{\left(-1+o(1)\right)N/(2A\log_q N)}\\
&\ll \Big(\frac{\log_q N}{N}\Big)^{1/2}\hat{N}^{-1/(2A)+o(1)} \ll \hat{N}^{-1/(3A)}. \qquad (24)
\end{aligned}$$

By combining (19)–(24), we deduce that

$$|\lambda_{b,m,N}^{(Q)^\wedge}(\alpha)| \ll \hat{N}^{-1}\log_q N\big(\hat{N}N\langle g\rangle^{-1} + \hat{N}^{1/2}N + \langle g\rangle(N^2+\operatorname{ord} g) + \hat{N}^{1-1/(3A)}\langle m\rangle\big)$$
$$\ll \log_q N\big(N\langle g\rangle^{-1} + \hat{N}^{-1}\langle g\rangle(N^2+\operatorname{ord} g) + \hat{N}^{-1/(3A)}N\big).$$

Lemma 26. *Let $1 \le Q \le K$ and $\langle m\rangle \le N$. One has*

$$\sup_{\alpha\in\mathfrak{m}} |\lambda_{b,m,N}^{(Q)^\wedge}(\alpha)| \ll N^{2-B}\log_q N \ll N^{-A}.$$

Proof. Let $\alpha \in \mathfrak{m}$. By Dirichlet's approximation theorem, there exist $a, g \in \mathbb{F}_q[t]$ with g monic, $\langle g\rangle \le \hat{N}/N^B$, $(a,g)=1$ and $\langle \alpha - a/g\rangle < N^B/(\langle g\rangle\hat{N}) \le \langle g\rangle^{-2}$. Since $\alpha \in \mathfrak{m}$, we have $\langle g\rangle > N^B$. By Lemma 25,

$$|\lambda_{b,m,N}^{(Q)^\wedge}(\alpha)| \ll \log_q N\big(N\langle g\rangle^{-1} + \hat{N}^{-1}\langle g\rangle(N^2+\operatorname{ord} g) + \hat{N}^{-1/(3A)}N\big)$$
$$\ll N^{2-B}\log_q N \ll N^{-A}.$$

We now summarize the minor arc contribution in Proposition 6.

Lemma 27. *For $1 \le Q \le K$, we have*

$$\sup_{\alpha\in\mathfrak{m}} \big|\lambda_{b,m,N}^{\wedge}(\alpha) - \lambda_{b,m,N}^{(Q)^\wedge}(\alpha)\big| \ll N^{-A} \ll \hat{Q}^{-1}.$$

Proof. The lemma follows by combining Lemmas 16 and 26 and noting that

$$N^{-A} \ll \hat{K}^{-1} \ll \hat{Q}^{-1}.$$

Note that by combining Lemmas 15 and 27, we obtain Proposition 6.

5 Proofs of Theorems 2 and 3

We will first prove Theorem 2.

Proof (of Theorem 2). By Lemmas 5 and 7, for $1 \le Q \le K$, we have

$$\|f * \psi_Q^\wedge\|_\infty \ll \hat{Q}^{-1}\|f\|_1 \qquad \text{and} \qquad \|f * \psi_Q^\wedge\|_2 \ll Q\hat{N}^{-1}\|f\|_2.$$

By the Riesz-Thorin interpolation theorem [17, 25], we interpolate between these two bounds to find that for $\delta \ge 2$, we have

$$\|f * \psi_Q^\wedge\|_\delta \ll \hat{Q}^{-1+2/\delta}Q^{2/\delta}\hat{N}^{-2/\delta}\|f\|_{\delta'}.$$

Similarly, since

$$\|f * \psi_{K+1}^{\wedge}\|_\infty \ll \widehat{(K+1)}^{-1}\|f\|_1 \ll N^{-A}\|f\|_1 \quad \text{and} \quad \|f * \psi_{K+1}^{\wedge}\|_2 \ll N\hat{N}^{-1}\|f\|_2,$$

for $\delta > 2$, we have

$$\|f * \psi_{K+1}^{\wedge}\|_\delta \ll N^{A(-1+2/\delta)+2/\delta}\hat{N}^{-2/\delta}\|f\|_{\delta'}.$$

Upon recalling that $A = 4/(\delta - 2)$, we have

$$\|f * \psi_{K+1}^{\wedge}\|_\delta \ll N^{-2/\delta}\hat{N}^{-2/\delta}\|f\|_{\delta'}.$$

By the triangle inequality,

$$\|f * \lambda_{b,m,N}^{\wedge}\|_\delta \ll \sum_{Q=1}^{K+1}\|f * \psi_Q^{\wedge}\|_\delta \ll \hat{N}^{-2/\delta}\|f\|_{\delta'}.$$

Therefore, by (3) and (4), we have

$$\|T\|_{2\to\delta} \le \sup_{\|f\|_{\delta'}=1}\|f * \lambda_{b,m,N}^{\wedge}\|_\delta^{1/2} \ll \hat{N}^{-1/\delta}.$$

This completes the proof of the theorem.

We will now deduce Theorem 3 from Theorem 2.

Proof (of Theorem 3). When $\delta = 2$, the theorem follows from Parseval's inequality. Hence, we assume that $\delta > 2$. Let $(a_x)_{x\in\mathscr{P}_R}$ be a sequence of complex numbers with $|a_x| \le 1$ for $x \in \mathscr{P}_R$. Let

$$f(x) = \begin{cases} a_x, & \text{if } x \in \mathscr{P}_R, \\ 0, & \text{otherwise.} \end{cases}$$

Then, by setting $\lambda_{b,m,N} = \lambda_{0,1,R}$, it follows from Theorem 2 that

$$\left(\int_{\mathbb{T}}\Big|\sum_{x\in\mathscr{P}_R} a_x\frac{R}{\hat{R}}e(\alpha x)\Big|^\delta d\alpha\right)^{1/\delta} = \|Tf\|_\delta \ll \hat{R}^{-1/\delta}\|f\|_2 = \hat{R}^{-1/\delta}\left(\sum_{x\in\mathscr{P}_R}|a_x|^2\frac{R}{\hat{R}}\right)^{1/2} \ll \hat{R}^{-1/\delta}.$$

Thus

$$\Big\|\sum_{x\in\mathscr{P}_R} a_x e(x\theta)\Big\|_\delta = \left(\int_{\mathbb{T}}\Big|\sum_{x\in\mathscr{P}_R} a_x e(\alpha x)\Big|^\delta d\alpha\right)^{1/\delta} \ll \hat{R}^{1-1/\delta}R^{-1}. \tag{25}$$

Also, for $\langle\beta\rangle < q^{-1}\hat{R}^{-1}$ and $x \in \mathscr{P}_R$, we have $\langle\beta x\rangle < q^{-1}$, implying that

$$\begin{aligned}\Big\| \sum_{x\in\mathscr{P}_R} e(x\theta)\Big\|_\delta &= \bigg(\int_{\mathbb{T}} \Big|\sum_{x\in\mathscr{P}_R} e(\alpha x)\Big|^\delta d\alpha\bigg)^{1/\delta} \\ &\geq \bigg(\int_{\langle\beta\rangle<q^{-1}\hat{R}^{-1}} \Big|\sum_{x\in\mathscr{P}_R} e(\beta x)\Big|^\delta d\beta\bigg)^{1/\delta} \\ &\gg \bigg(\int_{\langle\beta\rangle<q^{-1}\hat{R}^{-1}} \hat{R}^\delta R^{-\delta} d\beta\bigg)^{1/\delta} \gg \hat{R}^{1-1/\delta}R^{-1}.\end{aligned} \tag{26}$$

The theorem now follows by combining (25) and (26).

6 Proof of Theorem 1

To prove Theorem 1, we will employ the W-trick (see [7] for a discussion of the method). Namely, we will pass to an arithmetic progression with common difference equal to a product of small irreducible polynomials and this will allow us to avoid some obstacles modulo small irreducible polynomials. It is worth noting that if one is able to avoid using the W-trick, the resulting bound in Theorem 1 could be improved to $D_{\mathbf{r}}(\mathscr{P}_R) \ll |\mathscr{P}_R|/\log_q|\mathscr{P}_R|$.

Lemma 28. *Let $r_1, r_2, r_3 \in \mathbb{F}_q$ with $r_1 + r_2 + r_3 = 0$. Suppose that $A_R \subseteq \mathscr{P}_R$ and that there is no non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_1, x_2, x_3 \in A_R$. Suppose also that $|A_R| > \eta\hat{R}/R$ for some $\eta \in \mathbb{R}$ with $\eta > 0$. Let*

$$W = \Big[\log_q\Big(\frac{\log_q R}{4}\Big)\Big] \qquad \text{and} \qquad m = \prod_{\langle\varpi\rangle\leq\hat{W}} \varpi.$$

Set $\hat{N} = \hat{R}/\langle m\rangle$. Then for N sufficiently large, there exists $\mathscr{A} \subseteq \mathscr{S}_N$ such that

- *There is no non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_1, x_2, x_3 \in \mathscr{A}$,*
- *There exists some $b \in \mathbb{F}_q[t]$ with $(b, m) = 1$ and $\lambda_{b,m,N}(\mathscr{A}) \geq \eta$.*

Proof. Let 1_{A_R} denote the characteristic function of the set A_R. We have

$$\sum_{\substack{\langle b\rangle<\langle m\rangle\\(b,m)=1}} \sum_{\substack{x\in S_R\\ x\equiv b\,(\mathrm{mod}\,m)}} 1_{A_R}(x) \geq \eta\hat{R}/R.$$

By the pigeonhole principle, there exists $b \in \mathbb{F}_q[t]$ with $\langle b\rangle < \langle m\rangle$ and $(b, m) = 1$ such that

$$\sum_{\substack{x\in S_R\\ x\equiv b\,(\mathrm{mod}\,m)}} 1_{A_R}(x) \geq \frac{\eta\hat{R}}{\phi(m)R}.$$

Let $\mathscr{A} = \{n \in \mathscr{S}_N \mid mn + b \in A_R\}$. Thus

$$\lambda_{b,m,N}(\mathscr{A}) = \frac{(N + \operatorname{ord} m)\phi(m)}{\hat{N}\langle m\rangle} \sum_{n\in\mathscr{S}_N} 1_{A_R}(mn + b) \geq \eta.$$

Since $r_1 + r_2 + r_3 = 0$ and there is no non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_1, x_2, x_3 \in A_R$, it follows that there is no non-trivial solutions to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_1, x_2, x_3 \in \mathscr{A}$. This completes the proof of the lemma.

In order to apply Lemma 28 with the earlier work in this paper, we need to bound $\langle m\rangle$ in terms of N. Note that

$$\operatorname{ord} m = \sum_{\langle\varpi\rangle\leq\hat{W}} \operatorname{ord}\varpi = \sum_{K=1}^{W} K\big(\hat{K}/K + O(\hat{K}^{1/2}/K)\big) = q(q-1)^{-1}\hat{W} + O(\hat{W}^{1/2}).$$

Since $W = \big[\log_q\big(\frac{\log_q R}{4}\big)\big]$, for R sufficiently large in terms of q, we have

$$\operatorname{ord} m \in \Big[\frac{\log_q R}{4.1q}, \frac{\log_q R}{1.9}\Big];$$

from which we derive that

$$\hat{N} = \hat{R}/\langle m\rangle \in \big[\hat{R}R^{-1/1.9}, \hat{R}R^{-1/(4.1q)}\big].$$

In addition, we have $\langle m\rangle \leq R^{1/1.9} \leq N$ and $W \ll \log_q \log_q N$.

For a set $\mathscr{A} \subseteq \mathscr{S}_N$ and a monic irreducible polynomial ϖ of degree N, we embed $\mathscr{A}$ into $\mathbb{F}_q[t]/\varpi\mathbb{F}_q[t]$ via the bijection $x \to x\,(\mathrm{mod}\,\varpi)$. Also, we define Fourier analysis for $\mathbb{F}_q[t]/\varpi\mathbb{F}_q[t]$: if $f, g : \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \to \mathbb{C}$ and $r \in \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t]$, we write

$$\tilde{f}(r) = \sum_{\langle x\rangle<\langle\varpi\rangle} f(x)e(rx/\varpi) \qquad \text{and} \qquad (f * g)(r) = \sum_{\langle x\rangle<\langle\varpi\rangle} f(x)g(r-x).$$

We define functions $\kappa, \lambda : \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \to \mathbb{C}$ by

$$\kappa(x) = \begin{cases} 1, & \text{if there exists } y \in \mathscr{A} \text{ such that } x \equiv y\,(\mathrm{mod}\,\varpi),\\ 0, & \text{otherwise,}\end{cases}$$

and $\lambda(x) = \lambda_{b,m,N}(y)$, where y is the unique element of $\mathscr{S}_N$ with $x \equiv y \pmod{\varpi}$. We also define a function $a : \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \to \mathbb{C}$ by $a(x) = \kappa(x)\lambda(x)$. First, we estimate the function $\tilde{\lambda}$.

In what follows, we will fix $\delta = 5/2$. Thus all implicit constants below depend at most on q.

Lemma 29. *We have*

$$\sup_{z \not\equiv 0 \pmod{\varpi}} |\tilde{\lambda}(z)| \ll (\log_q N)^{-1}.$$

Proof. Note that $\tilde{\lambda}(z) = \lambda^{\wedge}_{b,m,N}(z/\varpi)$. For $z/\varpi \in \mathfrak{m}$, by Lemma 16, we have

$$\tilde{\lambda}(z) \ll N^{-A} \ll (\log_q N)^{-1}.$$

Thus we are left to prove the lemma for the case that $z/\varpi \in \mathfrak{M}_{a,g} \subseteq \mathfrak{M}$. By Lemmas 9, 11 and 12, we have

$$\tilde{\lambda}(z) = \begin{cases} \frac{\mu(g)}{\phi(g)} e\Big(\frac{-ab\bar{m}}{g}\Big) \varrho\Big(\frac{z}{\varpi} - \frac{a}{g}\Big) + O\Big(\frac{N^{B+1+\epsilon}\langle m\rangle^{1/2+\epsilon}}{\hat{N}^{1/2}}\Big), & \text{if } (g,m) = 1, \\ O\Big(\frac{N^{B+1+\epsilon}\langle m\rangle^{1/2+\epsilon}}{\hat{N}^{1/2}}\Big), & \text{otherwise.} \end{cases}$$

Because

$$\frac{N^{B+1+\epsilon}\langle m\rangle^{1/2+\epsilon}}{\hat{N}^{1/2}} \ll (\log_q N)^{-1},$$

it is enough to show that when $(g,m) = 1$, we have

$$\phi(g)^{-1} \varrho\Big(\frac{z}{\varpi} - \frac{a}{g}\Big) \ll (\log_q N)^{-1}.$$

For $\langle g\rangle = 1$, since $z \not\equiv 0 \pmod{\varpi}$,

$$\phi(g)^{-1} \varrho\Big(\frac{z}{\varpi} - \frac{a}{g}\Big) = \varrho(z/\varpi) = \hat{N}^{-1} \sum_{x \in \mathscr{S}_N} e(zx/\varpi) = 0.$$

For $\langle g\rangle > 1$, note that $|\varrho(\alpha)| \le 1$ for all $\alpha \in \mathbb{T}$. When $\langle g\rangle > 1$ and $(g,m) = 1$, by the definition of m, there exists a monic irreducible polynomial ϖ' with $\varpi' | g$ and $\langle \varpi'\rangle > \hat{W}$. Thus

$$\phi(g)^{-1} \le \phi(\varpi')^{-1} \ll \hat{W}^{-1} \ll (\log_q N)^{-1}.$$

This completes the proof of the lemma.

We now prove a discrete version of the majorant property with $\delta = 5/2$. Note that the proof below can be adapted to give a discrete majorant property for any $\delta > 2$.

Lemma 30. *There exists an absolute constant $C''(q)$ such that*

$$\sum_{\langle z\rangle<\langle \varpi\rangle} |\tilde{a}(z)|^{5/2} \le C''(q).$$

Proof. For $\langle \varpi\rangle = \hat{N} > 1$, $x \in \mathscr{S}_N$ and $\langle\theta\rangle < 1$, we have $e\big(\frac{x(z+\theta)}{\varpi}\big) = e\big(\frac{xz}{\varpi}\big)e\big(\frac{t^N\theta}{\varpi}\big)$. Thus for all $\langle\alpha\rangle < \hat{N}$, by writing $\alpha = z + \theta$ with $z \in S_{N-1}$ and $\theta \in \mathbb{T}$, we have

$$\begin{aligned}\sum_{\langle z\rangle<\langle \varpi\rangle} |\tilde{a}(z)|^{5/2} &= \sum_{\langle z\rangle<\langle \varpi\rangle} \Big| \sum_{x\in\mathscr{S}_N} \kappa(x)\lambda(x)e(zx/\varpi)\Big|^{5/2} \\ &= \int_{\langle\alpha\rangle<\hat{N}} \Big| \sum_{x\in\mathscr{S}_N} \kappa(x)\lambda(x)e(\alpha x/\varpi)\Big|^{5/2} d\alpha.\end{aligned} \tag{27}$$

By writing $\alpha = \varpi\gamma$, we deduce that

$$\int_{\langle\alpha\rangle<\hat{N}} \Big| \sum_{x\in\mathscr{S}_N} \kappa(x)\lambda(x)e(\alpha x/\varpi)\Big|^{5/2} d\alpha = \hat{N}\int_{\mathbb{T}} \Big| \sum_{x\in\mathscr{S}_N} \kappa(x)\lambda_{b,m,N}(x)e(\gamma x)\Big|^{5/2} d\gamma. \tag{28}$$

By Theorem 2,

$$\begin{aligned}&\Big(\int_{\mathbb{T}} \Big| \sum_{x\in\mathscr{S}_N} \kappa(x)\lambda_{b,m,N}(x)e(\gamma x)\Big|^{5/2} d\gamma\Big)^{2/5} \\ &\quad = \|T\kappa\|_{5/2} \ll \hat{N}^{-2/5}\|\kappa\|_2 \\ &\quad = \hat{N}^{-5/2}\Big(\sum_{x\in\mathscr{S}_N} |\kappa(x)|^2\lambda_{b,m,N}(x)\Big)^{1/2} \ll \hat{N}^{-5/2}.\end{aligned} \tag{29}$$

By combining (27)–(29), we find that

$$\sum_{\langle z\rangle<\langle \varpi\rangle} |\tilde{a}(z)|^{5/2} \ll 1.$$

This completes the proof of the lemma.

Let ς be a real parameter satisfying $0 \le \varsigma \le 1$ and define

$$\mathscr{Z} = \mathscr{Z}(\varsigma) = \big\{z \in \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \,\big|\, |\tilde{a}(z)| \ge \varsigma\big\}.$$

Let $k = |\mathscr{Z}|$ and write $\mathscr{Z} = \{z_1, \dots, z_k\}$. We now are able to define a Bohr set

$$\mathscr{B} = \mathscr{B}(\mathscr{Z}) = \Big\{x \in \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \,\Big|\, \Big\langle \Big\| \frac{xz_i}{\varpi} \Big\| \Big\rangle < q^{-1} \ (1 \le i \le k)\Big\}.$$

Define a function $\beta : \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \to \mathbb{C}$ by

$$\beta(x) = \begin{cases} |\mathscr{B}|^{-1}, & \text{if } x \in \mathscr{B}, \\ 0, & \text{otherwise.} \end{cases}$$

We define a function $a_1 : \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \to \mathbb{C}$ by $a_1(x) = (a * \beta * \beta)(x)$.

Lemma 31. *There exists a positive constant $C_2(q)$ such that whenever $k \le \log_q \log_q N$, we have $\|a_1\|_\infty \le C_2(q)\hat{N}^{-1}$.*

Proof. From the definition of a_1 and Lemma 29, we have

$$\begin{aligned} a_1(x) = \big(a * \beta * \beta\big)(x) &\le \big(\lambda * \beta * \beta\big)(x) = \hat{N}^{-1} \sum_{\langle y\rangle < \langle \varpi\rangle} \tilde{\lambda}(y)\tilde{\beta}(y)^2 e\big(-xy/\varpi\big) \\ &\le \hat{N}^{-1}\tilde{\lambda}(0)\tilde{\beta}(0)^2 + \hat{N}^{-1} \sum_{\substack{\langle y\rangle < \langle \varpi\rangle \\ y \ne 0}} \tilde{\lambda}(y)\tilde{\beta}(y)^2 e\big(-xy/\varpi\big) \\ &\ll \hat{N}^{-1} + \hat{N}^{-1} \sup_{y \not\equiv 0 \,(\mathrm{mod}\, \varpi)} |\tilde{\lambda}(y)| \sum_{\langle y\rangle < \langle \varpi\rangle} |\tilde{\beta}(y)|^2 \\ &\ll \hat{N}^{-1} + (\log_q N)^{-1}|B|^{-1}. \end{aligned}$$

Recall that $\mathscr{Z} = \{z_1, \dots, z_k\}$. Consider the mapping $\Gamma : \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t] \to \mathbb{T}^k$ defined by

$$\Gamma(x) = \big(\|xz_1/\varpi\|, \dots, \|xz_k/\varpi\|\big).$$

Let

$$\mathscr{G} = \big\{(\alpha_1, \dots, \alpha_k) \in \mathbb{T}^k \mid \langle \alpha_i\rangle < q^{-1} \ (1 \le i \le k)\big\}.$$

By the pigeonhole principle, there exists an element $(v_1, \dots, v_k) \in \mathbb{F}_q^k$ where

$$\mathscr{H} = \{x \,(\mathrm{mod}\, \varpi) \mid \Gamma(x) - (v_1, \dots, v_k) \in \mathscr{G}\}$$

contains at least $\hat{N}q^{-k}$ elements. Let $y \in \mathscr{H}$. Then for any $y' \in \mathscr{H}$, we have $\Gamma(y - y') \in \mathscr{G}$. Hence, $|B| \ge \hat{N}q^{-k}$, implying that

$$|a_1(x)| \ll \hat{N}^{-1} + (\log_q N)^{-1}\hat{N}^{-1}q^k \ll \hat{N}^{-1}.$$

We will now prove upper and lower bounds for the sum

$$\hat{N}^{-1} \sum_{\langle z\rangle<\langle \varpi\rangle} \tilde{a}_1(r_1 z)\tilde{a}_1(r_2 z)\tilde{a}_1(r_3 z),$$

and we will then deduce Theorem 1 by comparing these upper and lower bounds.

Lemma 32. *Suppose that there is no non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in \mathscr{A}$ $(1 \le i \le 3)$. Then*

$$\hat{N}^{-1} \sum_{\langle z\rangle<\langle \varpi\rangle} \tilde{a}_1(r_1 z)\tilde{a}_1(r_2 z)\tilde{a}_1(r_3 z) \ll \hat{N}^{-2}N^2 + \hat{N}^{-1}\varsigma^{1/2}.$$

Proof. Since there is no non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in \mathscr{A}$ $(1 \le i \le 3)$, we have

$$\begin{aligned}
\hat{N}^{-1} \sum_{\langle z\rangle<\langle \varpi\rangle} \tilde{a}(r_1 z)\tilde{a}(r_2 z)\tilde{a}(r_3 z) &= \sum_{\langle x_1\rangle<\langle \varpi\rangle} \sum_{\langle x_2\rangle<\langle \varpi\rangle} a(x_1)a(x_2)a(-r_1r_3^{-1}x_1 - r_2r_3^{-1}x_2) \\
&= \sum_{\langle x\rangle<\langle \varpi\rangle} a(x)^3 \le \sum_{y\in\mathscr{S}_N} \lambda_{b,m,N}(y)^3 \\
&\ll \frac{(N+\operatorname{ord} m)^2\phi(m)^2}{\hat{N}^2\langle m\rangle^2} \ll N^2\hat{N}^{-2}.
\end{aligned}$$

Since $\tilde{a}_1 = \tilde{a}\tilde{\beta}^2$, it follows that

$$\begin{aligned}
&\hat{N}^{-1} \sum_{\langle z\rangle<\langle \varpi\rangle} \tilde{a}_1(r_1 z)\tilde{a}_1(r_2 z)\tilde{a}_1(r_3 z) \\
&\quad= \hat{N}^{-1} \sum_{\langle z\rangle<\langle \varpi\rangle} \Big(\tilde{a}_1(r_1 z)\tilde{a}_1(r_2 z)\tilde{a}_1(r_3 z) - \tilde{a}(r_1 z)\tilde{a}(r_2 z)\tilde{a}(r_3 z)\Big) \\
&\qquad + O(N^2\hat{N}^{-2}) \\
&\quad= \hat{N}^{-1} \sum_{\langle z\rangle<\langle \varpi\rangle} \tilde{a}(r_1 z)\tilde{a}(r_2 z)\tilde{a}(r_3 z)\Big(\tilde{\beta}(r_1)^2\tilde{\beta}(r_2)^2\tilde{\beta}(r_3)^2 - 1\Big) \\
&\qquad + O(N^2\hat{N}^{-2}).
\end{aligned} \tag{30}$$

Note that when $z \in \mathscr{Z}$ and $r \in \mathbb{F}_q$, since $\langle \|rzx/\varpi\| \rangle < q^{-1}$ for all $x \in \mathscr{B}$, we have

$$\tilde{\beta}(rz) = |\mathscr{B}|^{-1} \sum_{x\in\mathscr{B}} e(rzx/\varpi) = 1.$$

Thus

$$\sum_{z\in\mathscr{Z}} \tilde{a}(r_1 z)\tilde{a}(r_2 z)\tilde{a}(r_3 z)\Big(\tilde{\beta}(r_1 z)^2\tilde{\beta}(r_2 z)^2\tilde{\beta}(r_3 z)^2 - 1\Big) = 0. \tag{31}$$

Note that for all $z \pmod{\varpi}$,

$$\left|\tilde{\beta}(r_1 z)^2 \tilde{\beta}(r_2 z)^2 \tilde{\beta}(r_3 z)^2 - 1\right| \leq 2.$$

By combining Hölder's inequality with Lemma 30, we have

$$\begin{aligned} &\sum_{\substack{\langle z\rangle < \langle \varpi\rangle \\ z \notin \mathscr{L}}} \tilde{a}(r_1 z)\tilde{a}(r_2 z)\tilde{a}(r_3 z)\left(\tilde{\beta}(r_1 z)^2 \tilde{\beta}(r_2 z)^2 \tilde{\beta}(r_3 z)^2 - 1\right) \\ &\qquad \ll \sup_{\substack{\langle z\rangle < \langle \varpi\rangle \\ z \notin \mathscr{L}}} |\tilde{a}(z)|^{1/2} \sum_{\langle z\rangle < \langle \varpi\rangle} |\tilde{a}(z)|^{5/2} \ll \varsigma^{1/2}. \end{aligned} \tag{32}$$

The lemma now follows by combining (30)–(32).

Lemma 33. *Suppose that $k \leq \log_q \log_q N$. Then there exists a positive constant $C_5 = C_5(q)$ such that*

$$\hat{N}^{-1} \sum_{\langle z\rangle < \langle \varpi\rangle} \tilde{a}_1(r_1 z)\tilde{a}_1(r_2 z)\tilde{a}_1(r_3 z) \gg \eta^4 \hat{N}^{-1} q^{-C_5/\eta}.$$

Proof. Let

$$\mathscr{A}' = \left\{x \in \mathbb{F}_q[t]/\varpi \mathbb{F}_q[t] \;\middle|\; a_1(x) \geq \frac{\eta}{2\hat{N}}\right\}.$$

By Lemma 31, there exists a constant $C_2 = C_2(q) > 1$ such that $\|a_1\|_\infty \leq C_2 \hat{N}^{-1}$. Thus by Lemma 28,

$$\begin{aligned} |\mathscr{A}'|\frac{C_2}{\hat{N}} + (\hat{N} - |\mathscr{A}'|)\frac{\eta}{2\hat{N}} &\geq \sum_{\langle x\rangle < \langle \varpi\rangle} a_1(x) \\ &= \sum_{\langle x\rangle < \langle \varpi\rangle} (a * \beta * \beta)(x) \\ &= \sum_{\langle y\rangle < \langle \varpi\rangle} \beta(y) \sum_{\langle z\rangle < \langle \varpi\rangle} \beta(z-y) \sum_{\langle x\rangle < \langle \varpi\rangle} a(x-z) \\ &\geq \eta \sum_{\langle y\rangle < \langle \varpi\rangle} \beta(y) \sum_{\langle z\rangle < \langle \varpi\rangle} \beta(z-y) = \eta. \end{aligned}$$

Hence, we have

$$|\mathscr{A}'| \geq \eta \hat{N}/(2C_2 - \eta) \geq C_3 \eta \hat{N},$$

where $C_3 = 1/(2C_2) \in (0,1)$. Let S denote the number of non-trivial solutions to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in \mathscr{A}'$ $(1 \le i \le 3)$. Then one has

$$\hat{N}^{-1} \sum_{\langle z\rangle < \langle \varpi\rangle} \tilde{a}_1(r_1z)\tilde{a}_1(r_2z)\tilde{a}_1(r_3z) \ge \frac{C_3^3\eta^3 S}{\hat{N}^3}. \tag{33}$$

Let $M \in \mathbb{N}$. By [14, Theorem 1], there exists a positive constant $C_4 = C_4(q)$ such that if $M \ge C_4/\eta$, then any subset of S_M of density at least $C_3\eta/2$ contains a non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$. Furthermore, since $r_i \in \mathbb{F}_q$ $(1 \le i \le 3)$, the same is true for any space isomorphic to S_M as a vector space over $\mathbb{F}_q$. Now, let $M < N$. There are $\hat{N}(\hat{N}-1)$ choices of (u,v) where $u \in \mathscr{S}_N$ and $0 < \langle v\rangle < \hat{N}$. Consider arithmetic progressions of the form $W_{u,v} = \{u + vl \,|\, \langle l\rangle < \hat{M}\} \subset \mathbb{F}_q[t]/\varpi\mathbb{F}_q[t]$. Let $\mathscr{U} = \{(u,v) \,\big|\, |W_{u,v} \cap \mathscr{A}'| > C_3\eta\hat{M}/2\}$. Note that $|W_{u,v} \cap \mathscr{A}'| \le \hat{M}$ for all u and v. Upon noting that every element $x \in \mathscr{A}'$ lies inside exactly $(\hat{N}-1)\hat{M}$ sets $W_{u,v}$, we have

$$|\mathscr{U}|\hat{M} + \big(\hat{N}(\hat{N}-1) - |\mathscr{U}|\big)C_3\eta\hat{M}/2 \ge (\hat{N}-1)\hat{M}|\mathscr{A}'| \ge C_3\eta\hat{N}(\hat{N}-1)\hat{M}.$$

It follows that

$$|\mathscr{U}| \ge C_3\eta\hat{N}(\hat{N}-1)/(2 - C_3\eta) \ge C_3\eta\hat{N}(\hat{N}-1)/2.$$

Thus there are at least $C_3\eta\hat{N}(\hat{N}-1)/2$ sets $W_{u,v}$ for which $\mathscr{A}' \cap W_{u,v}$ has density at least $C_3\eta/2$. Provided that $C_4/\eta \le M < N$, each set $W_{u,v}$ with $(u,v) \in \mathscr{U}$ contains a non-trivial solution to $r_1x_1 + r_2x_2 + r_3x_3 = 0$. Note that for any non-trivial solution $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in \mathscr{A}'$ $(1 \le i \le 3)$, there are at most $\hat{M}^2$ choices of (u,v) so that $(x_1,x_2,x_3) \in W_{u,v}^3$. Therefore, provided that $\lceil C_4/\eta\rceil < N$, by setting $M = \lceil C_4/\eta\rceil$, we have

$$S \ge \frac{C_3\eta\hat{N}(\hat{N}-1)}{2\hat{M}^2} \gg \eta\hat{N}^2 q^{-2C_4/\eta}. \tag{34}$$

The lemma follows by combining (33) and (34) and setting $C_5 = 2C_4$.

We are now in a position to prove Theorem 1.

Proof (of Theorem 1). Let η, A_R, $\mathscr{A}$, N and R be defined as in Lemma 28, where R is sufficiently large in terms of q. Suppose that there is no non-trivial solutions to $r_1x_1 + r_2x_2 + r_3x_3 = 0$ with $x_i \in \mathscr{A}$ $(1 \le i \le 3)$. Recall that $k = |\mathscr{Z}| = \big|\{\langle z\rangle < \langle \varpi\rangle \,\big|\, |\tilde{a}(z)| \ge \varsigma\}\big|$. By Lemma 30,

$$k\varsigma^{5/2} \le \sum_{\langle x\rangle < \langle \varpi\rangle} |\tilde{a}(x)|^{5/2} \ll 1.$$

Since $k \ll \varsigma^{-5/2}$, there exists a positive constant $C_6 = C_6(q)$ such that, upon setting $\varsigma = C_6(\log_q \log_q N)^{-2/5}$, we have $k \leq \log_q \log_q N$. By Lemmas 32 and 33,

$$\begin{aligned}\eta^4 \hat{N}^{-1} q^{-C_5/\eta} &\ll \hat{N}^{-1} \sum_{\langle z \rangle < \langle \varpi \rangle} \tilde{a}_1(r_1 z)\tilde{a}_1(r_2 z)\tilde{a}_1(r_3 z) \\ &\ll \hat{N}^{-2}N^2 + \hat{N}^{-1}\varsigma^{1/2} \\ &\ll \hat{N}^{-2}N^2 + \hat{N}^{-1}(\log_q \log_q N)^{-1/5} \\ &\ll \hat{N}^{-1}(\log_q \log_q N)^{-1/5}.\end{aligned}$$

Thus $\eta^4 q^{-C_5/\eta} \ll (\log_q \log_q N)^{-1/5}$, which implies that

$$\log_q \log_q \log_q N \ll -\log_q \eta + \frac{1}{\eta} \ll \frac{1}{\eta}.$$

From the above inequality, we can deduce that $\eta \ll (\log_q \log_q \log_q N)^{-1}$. Therefore, we have

$$\frac{|A_R|}{|\mathscr{P}_R|} \ll \frac{1}{\log_q \log_q \log_q N} \ll \frac{1}{\log_q \log_q \log_q R} \ll \frac{1}{\log_q \log_q \log_q \log_q |\mathscr{P}_R|}.$$

Theorem 1 now follows.

Acknowledgements The research of the first author is supported in part by an NSERC discovery grant. The research of the second author is supported in part by NSA Young Investigator Grants #H98230-10-1-0155, #H98230-12-1-0220, and #H98230-14-1-0164.

The authors are grateful to Trevor Wooley for many valuable discussions during the completion of this work and to Frank Thorne for providing a reference to [18]. They also would like to thank the referee for many valuable comments. This work was completed when the second author visited the University of Waterloo in 2007 and 2008, and he would like to thank the Department of Pure Mathematics for their hospitality.

References

1. A. Balog, A. Perelli, Exponential sums over primes in an arithmetic progression. Proc. Am. Math. Soc. **93**, 578–582 (1985)
2. T.F. Bloom, Translation invariant equations and the method of Sanders. Bull. Lond. Math. Soc. **44**, 1050–1067 (2012)
3. J. Bourgain, On triples in arithmetic progression. Geom. Funct. Anal. **9**, 968–984 (1999)
4. J. Bourgain, Roth's theorem on progressions revisited. J. Anal. Math. **104**, 155–206 (2008)
5. W.T. Gowers, A new proof of Szemerédi's theorem. Geom. Funct. Anal. **11**, 465–588 (2001)
6. B.J. Green, Roth's theorem in the primes. Ann. Math. **161**, 1609–1636 (2005)
7. B.J. Green, T.C. Tao, The primes contain arbitrarily long arithmetic progressions. Ann. Math. **167**, 481–547 (2008)

8. D.R. Heath-Brown, Integer sets containing no arithmetic progressions. J. Lond. Math. Soc. **35**, 385–394 (1987)
9. H.A. Helfgott, A. de Roton, Improving Roth's theorem in the primes. Int. Math. Res. Not. **2011**, 767–783 (2011)
10. R.M. Kubota, Waring's problem for $\mathbf{F}_q[x]$. Diss. Math. (Rozpr. Mat.) **117**, 60pp (1974)
11. T.H. Lê, Green-Tao theorem in function fields. Acta Arith. **147**, 129–152 (2011)
12. T.H. Lê, C.V. Spencer, Difference sets and the irreducibles in function fields. B. Lond. Math. Soc. **43**, 347–358 (2011)
13. Y.-R. Liu, A generalization of the Turán and Erdös-Kac theorem. Ph.D. thesis, Harvard University, 2003
14. Y.-R. Liu, C.V. Spencer, A generalization of Roth's theorem in function fields. Int. J. Number Theory **5**, 1149–1154 (2009)
15. Y.-R. Liu, T.D. Wooley, Waring's problem in function fields. J. Reine Angew. Math. **638**, 1–67 (2010)
16. E. Naslund, On improving Roth's theorem in the primes. Mathematika **61**, 49–62 (2015)
17. M. Riesz, Sur les maxima des formes bilinéaires et sur les fonctionnelles linéaires. Acta Math. **49**, 465–497 (1927)
18. G. Rhin, Répartition modulo 1 dans un corps de séries formelles sur un corps fini. Diss. Math. (Rozpr. Mat.) **95**, 75pp (1972)
19. M. Rosen, *Number Theory in Function Fields* (Springer, New York, 2002)
20. K.F. Roth, On certain sets of integers. J. Lond. Math. Soc. **28**, 104–109 (1953)
21. T. Sanders, On Roth's theorem on progressions. Ann. Math. **174**, 619–636 (2011)
22. T. Sanders, On certain other sets of integers. J. Anal. Math. **116**, 53–82 (2012)
23. E. Szemerédi, On sets of integers containing no k elements in arithmetic progression. Acta Arith. **27**, 199–245 (1975)
24. E. Szemerédi, Integer sets containing no arithmetic progressions. Acta Math. Hungar. **56**, 155–158 (1990)
25. G.O. Thorin, Convexity theorems generalizing those of M. Riesz and Hadamard with some applications. Comm. Sem. Math. Univ. Lund [Medd. Lunds Univ. Mat. Sem.] **9**, 1–58 (1948)
26. R.C. Vaughan, *The Hardy-Littlewood Method*, 2nd edn. (Cambridge University Press, Cambridge, 1997)

The Distribution of Self-Fibonacci Divisors

Florian Luca and Emanuele Tron

Abstract Consider the positive integers n such that n divides the n-th Fibonacci number, and their counting function A. We prove that

$$A(x) \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x}.$$

1 Introduction

The Fibonacci numbers notoriously possess many arithmetical properties in relation to their indices. In this context, Fibonacci numbers divisible by their index constitute a natural subject of study, yet there are relatively few substantial results concerning them in the literature.

Let $\mathscr{A} = \{a_n\}_{n\in\mathbb{N}}$ be the increasing sequence of natural numbers such that a_n divides F_{a_n}: this is OEIS A023172, and it starts

$$1,\ 5,\ 12,\ 24,\ 25,\ 36,\ 48,\ 60,\ 72,\ 96,\ 108,\ 120,\ 125,\ 144,\ 168,\ 180,\ \ldots$$

(as they have no common name, we dub them *self-Fibonacci divisors*). Let moreover $A(x) := \#\{n \leq x : n \in \mathscr{A}\}$ be its counting function.

This kind of sequence has already been considered by several authors; we limit ourselves to mentioning the current state-of-the-art result, due to Alba González–Luca–Pomerance–Shparlinski.

Proposition 1 ([1], Theorems 1.2 and 1.3). *It holds that*

$$\left(\frac{1}{4}+o(1)\right)\log x \leq \log A(x) \leq \log x - (1+o(1))\sqrt{\log x \log\log x}.$$

F. Luca (✉)
School of Mathematics, University of the Witwatersrand, PO Box 2050, Wits, South Africa
e-mail: florian.luca@wits.ac.za

E. Tron
Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy
e-mail: emanuele.tron@sns.it

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_6

We improve the upper bound above as follows.

Theorem 1. *We have that*

$$\log A(x) \le \log x - \left(\frac{1}{2} + o(1)\right) \frac{\log x \log\log\log x}{\log\log x}. \tag{1}$$

The main element of the proof is a new classification of self-Fibonacci divisors.

We now recall some basic facts about Fibonacci numbers. All statements in the next lemma are well-known and readily provable.

Lemma 1. *Define $z(n)$ to be the least positive integer such that n divides $F_{z(n)}$ (the* Fibonacci entry point*, or* order of appearance*, of n). Then the following properties hold.*

- *$z(n)$ exists for all $n \in \mathbb{N}$. In fact, $z(n) \le 2n$.*
- *For every $a, b \in \mathbb{N}$, $\gcd(F_a, F_b) = F_{\gcd(a,b)}$.*
- *For every prime p, $z(p)$ divides $p - \left(\frac{p}{5}\right)$, $\left(\frac{p}{5}\right)$ being the Legendre symbol.*
- *If a divides b, then $z(a)$ divides $z(b)$.*
- *For every $a, b \in \mathbb{N}$ one has $z(\mathrm{lcm}(a,b)) = \mathrm{lcm}(z(a), z(b))$. In particular, $\mathrm{lcm}(z(a), z(b))$ divides $z(ab)$.*
- *For every prime p and every $n \in \mathbb{N}$, $z(p^n) = p^{\max(n-e(p),0)} z(p)$, where $e(p) := v_p(F_{z(p)}) \ge 1$ and v_p is the usual p-adic valuation.*

From now on, we shall use the above properties without citing them.

Next comes a useful result concerning the p-adic valuation of Fibonacci numbers.

Lemma 2 ([4], Theorem 1). *The following equalities hold.*

$$v_2(F_n) = \begin{cases} 0, & \text{if } n \equiv 1, 2 \pmod 3; \\ 1, & \text{if } n \equiv 3 \pmod 6; \\ 3, & \text{if } n \equiv 6 \pmod{12}; \\ v_2(n) + 2, & \text{if } n \equiv 0 \pmod{12}. \end{cases}$$

$$v_5(F_n) = v_5(n).$$

For $p \ne 2, 5$ prime,

$$v_p(F_n) = \begin{cases} v_p(n) + e(p), & \text{if } n \equiv 0 \pmod{z(p)}; \\ 0, & \text{if } n \not\equiv 0 \pmod{z(p)}. \end{cases}$$

To end the section, we point out an interesting feature of the upper bound in Theorem 1: it should be, up to a constant factor of the secondary term, best possible.

A squarefree integer n is a self-Fibonacci divisor if and only if $z(p)$ divides n for every prime p that divides n. This is certainly true if $p - \left(\frac{p}{5}\right)$ divides n for every prime factor p of n. This is indeed strongly reminiscent of Korselt's criterion for Carmichael numbers: one should therefore expect heuristics for self-Fibonacci divisors similar to those for Carmichael numbers to be valid; in particular Pomerance's [7], which would predict

$$\log A(x) = \log x - (1 + o(1)) \frac{\log x \log\log\log x}{\log\log x}.$$

The reader should compare this with Theorem 4 of [3], which states that, if $\mathscr{L}(x)$ is the number of composite integers n up to x for which n divides $F_{n-\left(\frac{n}{5}\right)}$, then

$$\log \mathscr{L}(x) \leq \log x - \left(\frac{1}{2} + o(1)\right) \frac{\log x \log\log\log x}{\log\log x}.$$

2 Arithmetical Characterisation

In this section, we show how $\mathscr{A}$ can be partitioned into subsequences that admit a simple description.

Note that n divides F_n if and only if $z(n)$ divides n and set

$$\mathscr{A}_k := \{n \in \mathbb{N} : n/z(n) = k\}.$$

Our next task is to prove the following characterisation of the $\mathscr{A}_k$'s. Let $c(k) := \min \mathscr{A}_k$ whenever $\mathscr{A}_k$ is not empty.

Theorem 2. *$\mathscr{A}_k$ is empty if k is divisible by 8, 5 or $p^{e(p)+1}$ for an odd prime p. Otherwise, if $k = 2^{\alpha_t+1} \prod_{\substack{i=1 \\ p_i \neq 2}}^{t} p_i^{\alpha_i}$ is its factorisation,*

- $\mathscr{A}_k = \left\{ c(k) \cdot 5^{\beta_1} \cdot \prod_{\substack{i=1 \\ p_i \neq 2,5}}^{t} p_i^{\beta_{i+1}} \right\}$ *as $(\beta_1, \ldots, \beta_{t+1})$ ranges over $\mathbb{N}^{t+1}$ with the conditions that either $\beta_{i+1} \geq 0$ if $\alpha_i = e(p_i)$, or $\beta_{i+1} = 0$ if $\alpha_i < e(p_i)$, for every $i \geq 1$, if k is odd or 2 times an odd number;*
- $\mathscr{A}_k = \left\{ c(k) \cdot 5^{\beta_1} \cdot 2^{\beta_{t+2}} \cdot \prod_{\substack{i=1 \\ p_i \neq 2,5}}^{t} p_i^{\beta_{i+1}} \right\}$ *with $(\beta_1, \ldots, \beta_{t+2})$ ranging over $\mathbb{N}^{t+2}$ as before, if k is a multiple of 4.*

Proof. We shall henceforth implicitly assume that *the primes we deal with are distinct from* 2 *and* 5, and all the proofs when some prime is 2 or 5 are easily adapted using the part of Lemma 2 regarding the 2-adic and 5-adic valuations.

Suppose that, for some n, $n/z(n) = k$, and p^d is the exact power of p that divides k. Upon writing $k = p^d k'$ and $n = p^d n'$, with k' coprime to p, this becomes $n'/k' = z(p^d n')$. In particular,

$$d + v_p(n') \le v_p(F_{z(p^d n')}) = v_p(F_{n'/k'}) \le v_p(n') + e(p),$$

which is absurd if $d \ge e(p) + 1$, so that $\mathscr{A}_k = \varnothing$ if $p^{e(p)+1}$ divides k.

If on the other hand k fulfills the conditions for $\mathscr{A}_k$ to be nonempty, we want to know for which $m \in \mathbb{N}$, given $n \in \mathscr{A}_k$, mn is itself in $\mathscr{A}_k$: this will give the conclusion, once we know that all the numbers in the sequence are multiples of a smallest number $c(k)$ which belongs itself to $\mathscr{A}_k$. The proof of this latter fact is deferred to Theorem 3 since it fits better within that setting.

Suppose we have $n \in \mathscr{A}_k$, and take $m = p_1^{a_1} \cdots p_w^{a_w}$ with $a_i > 0$ for each i; set $n = p_1^{\lambda_1} \cdots p_w^{\lambda_w} n'$ with n' coprime to m and $\lambda_i \ge 0$ for each i.

If $\lambda_i > 0$ for all i, then one has

$$k = \frac{n}{z(n)} = \frac{p_1^{\lambda_1} \cdots p_w^{\lambda_w} n'}{z(p_1^{\lambda_1} \cdots p_w^{\lambda_w} n')}$$

$$= \frac{p_1^{\lambda_1} \cdots p_w^{\lambda_w} n'}{\operatorname{lcm}(p_1^{\max(\lambda_1 - e(p_1),0)} z(p_1), \ldots, p_w^{\max(\lambda_w - e(p_w),0)} z(p_w), z(n'))}.$$

The p_i-adic valuation of this expression is $v_{p_i}(k)$, so in the denominator either $\max(\lambda_i - e(p_i), 0)$ is the greatest power of p_i, or some of $z(p_1), \ldots, z(p_w), z(n')$ has p-adic valuation $\lambda_i - v_{p_i}(k) \ge \lambda_i - e(p_i)$. Furthermore, one has $\lambda_i \ge v_{p_i}(k)$, as n has to be a multiple of k.

Now, the number

$$\frac{mn}{z(mn)} = \frac{p_1^{\lambda_1 + a_1} \cdots p_w^{\lambda_w + a_w} n'}{z(p_1^{\lambda_1 + a_1} \cdots p_w^{\lambda_w + a_w} n')}$$

$$= \frac{p_1^{\lambda_1 + a_1} \cdots p_w^{\lambda_w + a_w} n'}{\operatorname{lcm}(p_1^{\max(\lambda_1 + a_1 - e(p_1),0)} z(p_1), \ldots, p_w^{\max(\lambda_w + a_w - e(p_w),0)} z(p_w), z(n'))}$$

is equal to k if and only if its p_i-adic valuation is $v_{p_i}(k)$ for each i, that is

$$v_{p_i}(k) = \lambda_i + a_i - \max(\lambda_i + a_i - e(p_i), \lambda_i - v_{p_i}(k)).$$

Suppose that the first term in the max is the greater, that is $a_i \ge e(p_i) - v_{p_i}(k)$. The above equality reduces to $v_{p_i}(k) = e(p_i)$: so in this case each value $\ge e(p_i) - v_{p_i}(k)$ for a_i (with any value of λ_i) is admissible, if $v_{p_i}(k) = e(p_i)$, and no value is admissible if $0 \le v_{p_i}(k) < e(p_i)$.

Suppose that the second term is the greater, that is $a_i < e(p_i) - v_{p_i}(k)$. The equality reduces to $a_i = 0$, which is impossible.

Finally, if $\lambda_i = 0$ for some $i \leq w$, it is no longer true that $z(p_i^{\lambda_i}) = p_i^{\max(\lambda_i - e(p_i),0)} z(p_i)$, but one has $v_{p_i}(z(n)) = \lambda_i - v_{p_i}(k) = 0 = v_{p_i}(z(n'))$, so the above proof carries on with minor changes.

Starting from $c(k)$ and building all the members of $\mathscr{A}_k$ by progressively adding prime factors, we find exactly the statement of the theorem. □

In the remainder of this section, we show that $c(k)$ admits a more explicit description.

Theorem 3. *Whenever $c(k)$ exists, we have that $c(k) = k \operatorname{lcm}\left\{z^{(i)}(k)\right\}_{i=1}^{\infty}$, $z^{(i)}$ being the i-th iterate of z.*

Proof. To prove first that such an expression is well-defined, we show that the sequence of iterates of z eventually hits a fixed point.

First note that, for $k = \prod_i p_i^{\alpha_i}$, $z(k) = \operatorname{lcm}\left\{p_i^{\max(\alpha_i - e(p_i),0)} z(p_i)\right\}_i$: this is a divisor of $\frac{k}{\operatorname{rad}(k)} \operatorname{lcm}\{z(p_i)\}_i$, where $\operatorname{rad}(k) = \prod_i p_i$ is the radical of k. Consider now the largest prime factor P of k: if $P \geq 7$, its exponent in the previous expression decreases by at least 1 at each step, since the largest prime factor of $z(P)$ is strictly smaller than P. Consequently, after at most $v_P(k)$ steps, the exponent of P would have vanished. By iterating the argument concerning the largest prime factor at each step, after a finite number ℓ of steps, $z^{(\ell)}(k)$ will have only prime factors smaller than 7; set $z^{(\ell)}(k) = 2^a 3^b 5^c$.

Recall now Theorem 1.1 of [6]: the fixed points of z are exactly the numbers of the form 5^f and $12 \cdot 5^f$. By noting that $z(2^a) = 3 \cdot 2^{a-2}$, $z(3^b) = 4 \cdot 3^{b-1}$, $z(5^c) = 5^c$, we get that $z(2^a 3^b 5^c) = 2^{\max(a-2,2)} 3^{\max(b-1,1)} 5^c$. Since we can continue this until $a \leq 2$ and $b \leq 1$, we are left with a few cases to check to show that the sequence of iterates indeed reaches a fixed point.

As $c(k)$ must be a multiple of k, call $T := c(k)/k$. Consider next the obvious equalities

$$T = z(kT),$$

$$z(T) = z^{(2)}(kT),$$

$$z^{(2)}(T) = z^{(3)}(kT),$$

$$\vdots$$

Write $x \overset{\text{div}}{\leftarrow} y$ for the statement "y divides x". Then one has

$$\begin{aligned} T &= z(kT) \\ &\overset{\text{div}}{\leftarrow} z(\operatorname{lcm}(k, T)) \\ &= \operatorname{lcm}(z(k), z(T)) \\ &= \operatorname{lcm}(z(k), z^{(2)}(kT)) \\ &\overset{\text{div}}{\leftarrow} \operatorname{lcm}(z(k), z(\operatorname{lcm}(z(k), z(T)))) \\ &= \operatorname{lcm}(z(k), \operatorname{lcm}(z^{(2)}(k), z^{(2)}(T))) \\ &= \operatorname{lcm}(z(k), z^{(2)}(k), z^{(3)}(kT)) \\ &\vdots \\ &= \operatorname{lcm}(z(k), z^{(2)}(k), z^{(3)}(k), \dots). \end{aligned}$$

Note that we have not used yet that kT is the smallest member of $\mathscr{A}_k$; this means the above reasoning works for any member of $\mathscr{A}_k$, so that any number in $\mathscr{A}_k$ is a multiple of $k \operatorname{lcm}(z(k), z^{(2)}(k), z^{(3)}(k), \dots)$. If we manage to prove that $k \operatorname{lcm}(z(k), z^{(2)}(k),\ z^{(3)}(k), \dots)$ is in $\mathscr{A}_k$, we will obtain the divisibility argument we needed in the proof of Theorem 2.

Thus, we want to prove that $T = \operatorname{lcm}\left\{z^{(i)}(k)\right\}_{i=1}^{\infty}$ works; it is enough to prove that the divisibilities we previously derived are equalities, or in other words that $z(kT) = z(\operatorname{lcm}(k, T))$ for T defined this way.

If $k = \prod_i p_i^{\alpha_i}$ with $1 \le \alpha_i \le e(p_i)$ for each i, then

$$\begin{aligned} T &= \operatorname{lcm}\left(z\left(\prod_i p_i^{\alpha_i}\right),\ z^{(2)}\left(\prod_i p_i^{\alpha_i}\right),\ \dots\right) \\ &= \operatorname{lcm}\left(\operatorname{lcm}\left\{z\left(p_i^{\alpha_i}\right)\right\}_i,\ \operatorname{lcm}\left\{z^{(2)}\left(p_i^{\alpha_i}\right)\right\}_i,\ \dots\right) \\ &= \operatorname{lcm}\left(\left\{z\left(p_i^{\alpha_i}\right)\right\}_i,\ \left\{z^{(2)}\left(p_i^{\alpha_i}\right)\right\}_i,\ \dots\right) \end{aligned}$$

and

$$z(kT) = z\left(\left(\prod_i p_i^{\alpha_i}\right) \operatorname{lcm}\left(z\left(\prod_i p_i^{\alpha_i}\right),\ z^{(2)}\left(\prod_i p_i^{\alpha_i}\right),\ \dots\right)\right).$$

We would like to bring the $\prod_i p_i^{\alpha_i}$ into the least common multiple, but some power of p_i could divide the iterated entry point of some other prime to a higher power. Define then $m(p_h)$ to be the largest exponent of a power of p_h that divides $z^{(i)}(p_j)$ as i and j vary; thus

$$
\begin{aligned}
& z\left(\left(\prod_i p_i^{\alpha_i}\right) \operatorname{lcm}\left(z\left(\prod_i p_i^{\alpha_i}\right),\ z^{(2)}\left(\prod_i p_i^{\alpha_i}\right),\ \ldots\right)\right) \\
=& z\left(\operatorname{lcm}\left(\left\{p_i^{m(p_i)+\alpha_i}\right\}_i,\ z\left(\prod_i p_i^{\alpha_i}\right),\ z^{(2)}\left(\prod_i p_i^{\alpha_i}\right),\ \ldots\right)\right) \\
=& \operatorname{lcm}\left(\left\{z\left(p_i^{m(p_i)+\alpha_i}\right)\right\}_i,\ \left\{z^{(2)}\left(p_i^{\alpha_i}\right)\right\}_i,\ \left\{z^{(3)}\left(p_i^{\alpha_i}\right)\right\}_i,\ \ldots\right).
\end{aligned}
$$

We need this to be equal to

$$
\begin{aligned}
&\operatorname{lcm}\left(\left\{z\left(p_i^{\alpha_i}\right)\right\}_i,\ \left\{z^{(2)}\left(p_i^{\alpha_i}\right)\right\}_i,\ \left\{z^{(3)}\left(p_i^{\alpha_i}\right)\right\}_i,\ \ldots\right) \\
&\qquad = \operatorname{lcm}(z(k), z(T)) = z(\operatorname{lcm}(k, T)).
\end{aligned}
$$

All that is left to do now is to remark that this is true if and only if their p_i-adic valuations are equal for each i, or in other words, as p_i is coprime to $z(p_i^{\alpha_i}) = z(p_i)$,

$$\max(m(p_i) + \alpha_i - e(p_i)), m(p_i)) = m(p_i),$$

and this is evident. □

3 The Proof of Theorem 1

Let $x \geq 10$. One of our ingredients is the following result from [3].

Lemma 3 ([3], Theorem 3). *As $x \to \infty$,*

$$\#\{n \leq x : z(n) = m\} \leq x^{1-(1/2+o(1))\log\log\log x/\log\log x},$$

uniformly in m.

Let $n \in \mathscr{A}(x)$. By Theorem 2, every self-Fibonacci divisor is of the form $c(k)m$, where m is composed of primes that divide k. Thus, write $n = c(k)m$, where every prime factor of m divides k. Let $C(x) := x^{\log\log\log x/\log\log x}$. We distinguish two cases.

Case 1. $k \leq x/C(x)$.

Let $\mathscr{A}_1(x)$ be the subset of such $n \in \mathscr{A}(x)$. We fix k and count possible m's because $c(k)$ is determined by k; we use an idea similar to the one of the proof of Theorem 4 in [2]. Clearly, m has at most $\omega(k)$ distinct prime factors. Define next $\Psi(x, y)$ to be the number of positive integers $\ell \leq x$ whose largest prime factor $P(\ell)$ satisfies the inequality $P(\ell) \leq y$, and let p_s be the s-th prime. If $\mathscr{P}_k$ is the set of the prime divisors of k, the quantity of numbers $m \leq x$ all of whose prime factors are in $\mathscr{P}_k$ is of course at most $\Psi(x, p_{\omega(k)}) \leq \Psi(x, 2\log x)$ for x large enough.

Here we used the fact that $p_s < s(\log s + \log\log s)$ for all $s \geq 6$ (Theorem 3 of [8]) together with $\omega(k) < 2\log k/\log\log k$ for all $k \geq 3$. Classical estimates on $\Psi(x,y)$, such as the one of de Bruijn (see, for example, Theorem 2 on page 359 in [9]), show that if we put

$$Z := \frac{\log x}{\log y}\log\left(1+\frac{y}{\log x}\right) + \frac{y}{\log y}\log\left(1+\frac{\log x}{y}\right),$$

then the estimate

$$\log\Psi(x,y) = Z\left(1+O\left(\frac{1}{\log y}+\frac{1}{\log\log(2x)}\right)\right) \tag{2}$$

holds uniformly in $x \geq y \geq 2$. The above estimates (2) with $y = 2\log x$ imply that there are at most $C(x)^{(3\log 3-2\log 2+o(1))/\log\log\log x} = C(x)^{o(1)}$ values of m for any fixed k. Summing up over k, we get that

$$\#\mathscr{A}_1(x) \leq C(x)^{o(1)} \sum_{k\leq x/C(x)} 1 \leq \frac{x}{C(x)^{1+o(1)}} \qquad (x \text{ large}). \tag{3}$$

Case 2. $x/C(x) < k \leq x$.

Here, we have $kz(k) \leq c(k) \leq x$, whence $z(k) \leq C(x)$. Fix $z(k) = z$ in $[1, C(x)]$. By Lemma 3, if we put $\mathscr{B}_z := \{n \in \mathbb{N} : z(n) = z\}$, then the inequality

$$\#\mathscr{B}_z(t) \leq t/C(t)^{1/2+o(1)} \qquad \text{holds as} \quad t \to \infty. \tag{4}$$

We now let $k \in \mathscr{B}_z$. Then $n \leq x$ is a multiple of kz. The number of such n is $\lfloor x/kz \rfloor \leq x/kz$. Summing up the above inequality over $k \in \mathscr{B}_z$ and using partial summation and (4), we have

$$\begin{aligned}
\frac{x}{z}\sum_{\substack{k\in\mathscr{B}_z\\ x/C(x)<k\leq x}}\frac{1}{k} &= \frac{x}{z}\int_{x/C(x)}^{x}\frac{\mathrm{d}\#\mathscr{B}_z(t)}{t} \\
&= \frac{x}{z}\left(\frac{\#\mathscr{B}_z(t)}{t}\Big|_{t=x/C(x)}^{t=x} + \int_{x/C(x)}^{x}\frac{\#\mathscr{B}_z(t)}{t^2}\mathrm{d}t\right) \\
&\leq \frac{x}{z}\left(\frac{\#\mathscr{B}_z(x)}{x} + \int_{x/C(x)}^{x}\frac{\mathrm{d}t}{tC(t)^{1/2+o(1)}}\right) \\
&= \frac{x}{z}\left(\frac{1}{C(x)^{1/2+o(1)}} + \frac{1}{C(x)^{1/2+o(1)}}\int_{x/C(x)}^{x}\frac{\mathrm{d}t}{t}\right) \\
&= \frac{(1+o(1))x\log C(x)}{zC(x)^{1/2+o(1)}} = \frac{x}{zC(x)^{1/2+o(1)}},
\end{aligned}$$

where in the above calculation we used the fact that

$$C(t)^{1/2+o(1)} = C(x)^{1/2+o(1)} \quad \text{uniformly in} \quad t \in [x/C(x), x] \quad \text{as} \quad x \to \infty.$$

We now sum over $z \in [1, C(x)]$, and obtain that

$$\begin{aligned} \#\mathscr{A}_2(x) &\le \frac{x}{C(x)^{1/2+o(1)}} \sum_{1 \le z \le C(x)} \frac{1}{z} \\ &= \frac{(1+o(1))x \log C(x)}{C(x)^{1/2+o(1)}} = \frac{x}{C(x)^{1/2+o(1)}} \qquad (x \to \infty). \end{aligned} \tag{5}$$

The desired conclusion now follows from (3) and (5).

4 Comments

Of course, the methods we presented apply equally well to other Lucas sequences, where analogues of Theorems 2, 3 and 1 hold; we chose to display the Fibonacci case, when the classification takes a particularly simple form.

To conclude, we make some observations to promote future progress. The problem of finding lower bounds for $A(x)$ requires completely different ideas; one can prove that

$$\log A(x) = \log \#\{n \le x : c(n) \le x,\ n \text{ squarefree}\} + O\left(\frac{\log x \log\log\log x}{\log\log x}\right),$$

so that in order to prove $A(x) = x^{1+O(\log\log\log x/\log\log x)}$ unconditionally one would need to build many squarefree n with small $c(n)$. The best we managed to prove is that $\log c(n) < 3P(n)$ (by double counting), and $\log c(n) < 7\sum_{p|n}(\log p)^2$ (by induction), but neither of these is sufficient. This hints at building numbers n for which their prime factors share most of their Pratt-Fibonacci trees (Pratt trees built with the factors of $z(p)$ as children of a node p^δ, taken with their exponents).

The set of numbers n with small $c(n)$ is both small and large in a certain sense: it has asymptotic density 0 and exponential density 1, conjecturally.

It is likely that $c(n)$ is quite large for most n. Recall that putting

$$F(n) := \operatorname{rad}\left(\prod_{k \ge 1} \phi^{(k)}(n)\right),$$

then in [5] it is proved that the inequality

$$F(n) > n^{(1+o(1))\log\log n/\log\log\log n}$$

holds for n tending to infinity through a set of asymptotic density 1. Since $c(n)$ is quite similar to $F(n)$, we conjecture that a like result holds for $c(n)$ as well.

Acknowledgements We are especially grateful to the referee for improving the argument in Sect. 3, to P. Leonetti for helping formulate Theorem 3, and to C. Sanna for pointing out a flaw in an earlier version of Theorem 2. We also thank B. Cloitre, K. Ford, D. Marques, C. Pomerance, G. Tenenbaum, L. Versari.

References

1. J.J. Alba González, F. Luca, C. Pomerance, I.E. Shparlinski, On numbers n dividing the nth term of a linear recurrence. Proc. Edinb. Math. Soc. **55.2**, 271–289 (2012)
2. P. Erdős, F. Luca, C. Pomerance, On the proportion of numbers coprime to a given integer, in *Proceedings of the Anatomy of Integers Conference*, Montréal, March 2006, ed. by J.-M. De Koninck, A. Granville, F. Luca. CRM Proceedings and Lecture Notes, vol. 46, pp. 47–64 (2008)
3. D.M. Gordon, C.Pomerance, The distribution of Lucas and elliptic pseudoprimes. Math. Comput. **57**, 825–838 (1991)
4. J.H. Halton, On the divisibility properties of Fibonacci numbers. Fibonacci Q. **4.3**, 217–240 (1966)
5. F. Luca, C. Pomerance, *Combinatorial Number Theory*. Irreducible Radical Extensions and Euler-function Chains (de Gruyter, Berlin, 2007), pp. 351–361
6. D. Marques, Fixed points of the order of appearance in the Fibonacci sequence. Fibonacci Q. **50.4**, 346–351 (2012)
7. C. Pomerance, On the distribution of pseudoprimes. Math. Comput. **37**, 587–593 (1981)
8. J.B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers. Ill. J. Math. **6.1**, 64–94 (1962)
9. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory* (Cambridge University Press, Cambridge, 1995)

Some Remarks on Automorphy and the Sato-Tate Conjecture

M. Ram Murty and V. Kumar Murty

Abstract We present an informal account of the evolution of the Sato-Tate conjecture and describe some recent work of the authors that it gave rise to.

1 The Conjecture

Let E be an elliptic curve defined over the rationals of conductor N. For any prime p not dividing N, we may consider the number of points N_p on the reduction of E mod p. Following Hasse, we have the inequality

$$|N_p - (p+1)| \leq 2\sqrt{p}.$$

Thus, we may write the integer

$$a_p = N_p - (p+1)$$

as

$$a_p = 2\sqrt{p}\cos(\theta_p),\ 0 \leq \theta_p \leq \pi.$$

The Sato-Tate conjecture describes the distribution of the "angles of Frobenius" θ_p as p varies. if E has complex multiplication, one expects that the angles are essentially equidistributed (after one takes into account the fact that for half the primes, namely those that do not split in the field of multiplication, $\theta_p = \pi/2$). If E does not have complex multiplication, then the Sato-Tate conjecture predicts a skewed distribution, namely

M.R. Murty
Department of Mathematics, Queen's University, Kingston, ON, Canada K7L 3N6
e-mail: murty@mast.queensu.ca

V.K. Murty (✉)
Department of Mathematics, University of Toronto, Toronto, ON, Canada M5S 2E4
e-mail: murty@math.toronto.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_7

$$\#\{p \leq x : \theta_p \in [\alpha, \beta]\} \sim \left(\frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2\theta \, d\theta\right)\pi(x)$$

where $\pi(x)$ as usual denotes the total number of primes $p \leq x$. The integral can of course be evaluated, and so the right hand side may also be written

$$\left(\frac{\beta-\alpha}{\pi} - \frac{1}{2\pi}(\sin 2\beta - \sin 2\alpha)\right)\pi(x).$$

The Sato-Tate conjecture is actually a theorem now due to the work of Barnet-Lamb et al. [1].

2 Origin of the Conjecture

Where does such a conjecture come from? Mikio Sato was led to it by numerical calculations. This is described in the beautiful article [11]. It also occurs in Tate's 1964 talk [14] at the Woods Hole Summer Institute on Algebraic Geometry organized by the American Mathematical Society. In that talk, he formulated the following conjecture about algebraic cycles on algebraic varieties. Let X be a smooth projective variety over a number field K. Let $L \supseteq K$ be a finite extension. Consider the Abelian group $A^i(X;L)$ generated by codimension i subvarieties (modulo homological equivalence) which are homologically equivalent to one defined over L. The ℓ-adic cycle class gives a map

$$A^i(X;L) \otimes \mathbb{Q}_\ell \to H_\ell^{2i}(\overline{X})(i).$$

Here, $\overline{X}$ is the base-change of X to an algebraic closure $\overline{K}$ of K, and $H_\ell^*(\overline{X})$ is the ℓ-adic cohomology of X. This is a finite dimensional $\mathbb{Q}_\ell$-vector space on which there is a continuous action of $\mathrm{Gal}(\overline{K}/K)$. In the case X is an Abelian variety, we have

$$H_\ell^*(\overline{X}) = \wedge H_\ell^1(\overline{X}).$$

Moreover, $H_\ell^1(\overline{X})$ is the $\mathbb{Q}_\ell$-dual of the Tate module $V_\ell(X)$ defined by

$$V_\ell(X) = \lim X[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

This is a $\mathrm{Gal}(\overline{K}/K)$ module in the evident way as $\mathrm{Gal}(\overline{K}/K)$ acts on $X[\ell^n]$.

The cyclotomic character

$$\chi_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mu_{\ell^\infty})$$

gives the action of Galois on ℓ-power roots of unity. The Tate twist $H_\ell^k(\overline{X})(i)$ is the Galois module $H_\ell^k(\overline{X}) \otimes \chi_\ell^i$.

The cycle class map is Galois equivariant, and so the image lies in the subspace of $H^{2i}_\ell(\overline{X})(i)$ fixed by $\mathrm{Gal}(\overline{K}/L)$.

Conjecture 1 (Tate Conjecture 1). The map

$$A^i(X;L) \otimes \mathbb{Q}_\ell \to H^{2i}_\ell(\overline{X})(i)^{\mathrm{Gal}(\overline{K}/L)}$$

is surjective.

This conjecture is still open in general, though there is now a vast literature on establishing it in special cases. One can get a (by now partial) picture of what is known from Tate's article [15] in the Motives volume.

In [14], Tate computed that for $X = E^m$, with E an elliptic curve defined over $K = \mathbb{Q}$, we have

$$\dim A^i(X,L) = \begin{cases} \binom{m}{i}^2 & \text{if } E \text{ has } CM \\ \binom{m}{i}^2 - \binom{m}{i-1}\binom{m}{i+1} & \text{if } E \text{ does not have } CM. \end{cases} \tag{1}$$

Here $L = \mathbb{Q}$ in the non CM case, and L is the field of multiplication in the CM case. To do this calculation, he did first the case $i = 1$ and then proved that A^i is generated by A^1. Soon afterwards, Mumford introduced the Mumford-Tate group and using the invariant theory of this group, the calculation becomes somewhat simpler.

Let us consider Tate's formula (1) in some special cases. For example, for $m = 2$ and $i = 1$, we have $X = E \times E$ and the codimension 1 cycles are (up to algebraic equivalence) $E \times \{0\}$, $\{0\} \times E$, and the diagonal Δ. In the CM case one has, in addition, the graph Δ_{CM} of the complex multiplication. Thus, the dimension of $A^1(X;L)$ is either 4 or 3 depending on whether E does or does not have CM. Here, we can take $L = \mathbb{Q}$ if E does not have CM. If E does have CM, the field L should contain the CM field.

Similarly, for $m = 3$, and $i = 1$, and E without CM, we have $X = E \times E \times E$. Denoting by E_1, E_2 and E_3 the three copies of E, we have the 6 generic cycles $E \times E \times \{0\}, E \times \{0\} \times E, \{0\} \times E \times E, \Delta_{12} \times E, E \times \Delta_{23}$ and $\Delta_{13} \times E$ where Δ_{ab} is the diagonal in $E_a \times E_b$. Note that

$$6 = \binom{3}{1}^2 - \binom{3}{0}\binom{3}{2}.$$

3 *L*-Functions

For a smooth projective variety over K, consider the Euler product

$$\Phi_i(X,s) = \prod_v \det(I - Frob_v | H^i_\ell(\overline{X})^{I_v}(Nv)^{-s})^{-1}.$$

Here the product is over finite primes v of K. This converges for $\Re(s) > 1 + \frac{i}{2}$. Thus, when $X = E$ and $i = 1$, we have the Hasse L-function of E:

$$\Phi_1(E,s) \;=\; \prod_v \left(1 - \frac{e^{i\theta_v}}{(Nv)^{s-\frac{1}{2}}}\right)^{-1} \left(1 - \frac{e^{-i\theta_v}}{(Nv)^{s-\frac{1}{2}}}\right)^{-1}.$$

For L a finite extension of K, we may also consider the base change $X_{/L}$ (in other words, X viewed as a variety over L) and in this case, we have the corresponding Euler product $\Phi_i(X_{/L}, s)$.

Conjecture 2 (Tate Conjecture 2). $\Phi_{2i}(X_{/L}, s)$ has a pole at $s = 1 + i$ of order equal to $\dim A^i(X, L)$.

In particular, (1) and the above conjecture predict that

$$-\mathrm{ord}_{s=k+1}\Phi_{2k}(E^m_{/L}, s) \;=\; \begin{cases} \binom{m}{k}^2 & \text{if } E \text{ has } CM \\ \binom{m}{k}^2 - \binom{m}{k-1}\binom{m}{k+1} & \text{if } E \text{ does not have } CM. \end{cases}$$

Here, $L = \mathbb{Q}$ if E does not have CM and the field of multiplication in the CM case. Tate also suggests that $\Phi_{2k+1}(X, s)$ does not have a pole or zero at the edge of its critical strip, namely

$$s = 1 + \frac{1}{2}(2k+1) \;=\; k + \frac{3}{2}.$$

These analytic conjectures are motivated by analogy with Artin L-functions and by the Birch and Swinnerton-Dyer conjecture. Again, for $X = E^m$, he computes

$$\Phi_k(X,s) \;=\; \prod_{0 \le i \le k/2} M_{k-2i}(s - \frac{k}{2})^{\binom{m}{i}\binom{m}{k-i}}.$$

Here,

$$M_0(s) \;=\; \zeta(s)$$

and for $k > 0$,

$$M_k(s) \;=\; \prod_v \left(1 - \frac{e^{ik\theta_v}}{(Nv)^s}\right)^{-1} \left(1 - \frac{e^{-ik\theta_v}}{(Nv)^s}\right)^{-1}.$$

If $E_{/\mathbb{Q}}$ has CM, the M_k are Hecke L-functions and we know they have analytic continuation to $\Re(s) = 1$ and are non-vanishing on that line. Hence, with L the CM field, the order of pole at $s = k+1$ of $\Phi_{2k}(E^m_{/L}, s)$ is the contribution from $i = k$ and this is

$$\binom{m}{k}^2 \;=\; \dim A^k(E^m, L).$$

Now consider the case $E_{/\mathbb{Q}}$ does not have CM. Let c_k denote the order of M_k at $s = 1$ (assuming that M_k is meromorphic at $s = 1$). Then, we have $c_0 = 1$. Moreover, as

$$\Phi_2(X, s) = M_2(s-1)^{\binom{m}{0}\binom{m}{2}} M_0(s-1)^{\binom{m}{1}\binom{m}{1}}$$

we expect that $c_2 = -1$. Also, we expect $c_{2k} = 0$ for all $k > 1$. Indeed, we have

$$\Phi_{2k}(X, s) \;=\; \prod_{0 \le i \le k} M_{2k-2i}(s-k)^{\binom{m}{i}\binom{m}{2k-i}}.$$

The factors on the right corresponding to $i = k$ and $i = k-1$ account for the expected pole of the left hand side.

Suppose also that $c_{2k+1} = 0$ for all $k \ge 0$. Then by a Tauberian argument, we might expect

$$\frac{1}{\pi(x)} \sum_{p \le x} \left(e^{ik\theta_p} + e^{-ik\theta_p}\right) \;\longrightarrow\; c_k.$$

Consider

$$F(x) = \frac{1}{\pi} \sum c_k \cos kx.$$

This should then be the distribution function for the θ_v. In other words,

$$F(x) = \frac{1}{\pi}\,(1 - \cos 2x) \;=\; \frac{2}{\pi} \sin^2 x.$$

4 Modular Forms

At the time, arguing by analogy, Serre formulated a conjecture to describe the distribution of the "angles of Frobenius" for any holomorphic cusp form of weight $k \ge 2$, level N and trivial character that is a normalized eigenform for the Hecke operators. For such a form f, let us write

$$f(z) = \sum_{n \ge 1} a_f(n) e^{2\pi i n z}$$

for the Fourier expansion at the cusp $i\infty$. Let us suppose that it is not of CM-type (in the sense of Ribet). That is, there does not exist a Dirichlet character χ with the property that $a_f(p) = \chi(p) a_f(p)$ for almost all p. Then, the Sato-Tate conjecture formulated by Serre in this context is as follows. As before, we can write

$$a_f(p) = 2p^{(k-1)/2} \cos\theta_p$$

for some $\theta_p \in [0, \pi]$. Then

$$\#\{p \leq x : \theta_p \in [\alpha, \beta]\} \sim \left(\frac{2}{\pi}\int_\alpha^\beta \sin^2\theta d\theta\right)\pi(x).$$

At the time that Serre proposed this, the Taniyama conjecture was not yet proven and so it could not be considered a generalization of the original Sato-Tate conjecture for elliptic curves.

5 The Symmetric Power L-Functions

We now know that the M_k do *not* have good analytic properties and the "correct" L-functions to consider are

$$L_k(s) = \prod_v \prod_{j=0}^{k} \left(1 - \frac{e^{i\theta_v(k-2j)}}{(Nv)^s}\right)^{-1}.$$

The product converges absolutely for $\Re(s) > 1$ so defines an analytic function in that half plane. There is a simple relation between the L_k and the M_k. We have

$$L_0(s) = M_0(s) = \zeta(s)$$

$$L_1(s) = M_1(s) = L(E, s + \frac{1}{2})$$

$$L_2(s) = \prod_v \left(1 - \frac{e^{2i\theta_v}}{(Nv)^s}\right)^{-1}\left(1 - \frac{1}{(Nv)^s}\right)^{-1}\left(1 - \frac{e^{-2i\theta_v}}{(Nv)^s}\right)^{-1}$$

which can be rewritten as

$$L_2(s) = M_0(s)M_2(s).$$

We note that if the middle factor in the above Euler product for L_2 were removed, we would get good analytic properties for the resulting function only in the CM case. In general, we have the relations

$$L_{2k}(s) = M_0(s)M_2(s)M_4(s)\cdots M_{2k}(s)$$

and

$$L_{2k+1}(s) = M_1(s)M_3(s)M_5(s)\cdots M_{2k+1}(s)$$

Using the L_m, Serre proposed a conjectural approach to proving this. If it can be shown that all the $L_m(s)$ are analytic for $\Re s \geq 1$ and non vanishing on the line $\Re(s) = 1$, then Serre showed [12] that Tauberian theorems could be used to deduce the above conjecture. Soon afterwards, Ogg [9] showed that if one had the analytic

continuation of the L_m for $\Re(s) > \frac{1}{2} - \epsilon$ for some $\epsilon > 0$, then the non-vanishing on the line $\Re(s) = 1$ could be deduced. In the work of the second author [5], it was shown that non-vanishing was in fact a consequence of the analytic continuation just to $\Re(s) \geq 1$.

In [6], it is shown that if we had the analytic continuation of all the L_m at $s = 1$ (that is, just the point and not the whole line), we could deduce the following weaker version of the Sato-Tate conjecture, namely

$$\sum_{\substack{p \leq x \\ \theta_p \in [\alpha, \beta]}} \frac{\log p}{p} \sim \left(\frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \theta \, d\theta \right) \log x.$$

The question of how to prove the analytic continuation remained. A conjectural approach to proving it was provided by Langlands.

6 Langlands' Conjecture

Now let us restrict to the case $E_{/\mathbb{Q}}$ does not have CM and consider the family of L-functions $L_m(s)$ introduced above.

Conjecture 3 (Langlands, 1970). There exists $\pi_m \in \mathcal{A}(GL_{m+1})$ a cuspidal automorphic representation such that

$$L(s, \pi_m) = L_m(s)$$

for all $m \geq 1$.

Given the known analytic properties of the standard L-function associated to a cuspidal automorphic representation of GL_m, a consequence of Langlands' conjecture would be the analytic continuation of the $L_m(s)$ for all s.

It is interesting to note that the Sato-Tate conjecture (both the original version as well as Serre's generalization) was proved by Barnet-Lamb et al. [1]. However, this was achieved without proving Langlands' conjecture. What the authors of [1] *did* prove is the *potential* automorphy of the symmetric power L-functions. This means that when the corresponding Galois representation is restricted to a subgroup of finite index, it's L-function is the L-function of an automorphic representation. This, therefore, still leaves open the automorphy of the $L_m(s)$ itself.

Conjecture 3 is a special case of the Langlands Functoriality conjecture. Indeed, beginning with an automorphic representation π of $\mathrm{G}L_2$, and considering the m-th symmetric power of the standard representation

$$r_m : \mathrm{G}L_2(\mathbb{C}) \to \mathrm{G}L_{m+1}(\mathbb{C})$$

the Langlands L-function $L(s, \pi, r_m)$ is $L_m(s)$. Viewing r_m as a map between the complex L-groups of GL_2 and GL_{m+1}, functoriality would predict the existence of a π_m as above.

For $m = 2$, this is the work of Shimura and Gelbart-Jacquet. For $m = 3$ this is due to Kim and Shahidi [4] and for $m = 4$, to Kim [3]. The main result of our work is to show that the holomorphy for all m follows from the automorphy of a restricted class of Rankin-Selberg products, as we explain below. (After this work was completed, we learnt[1] of recent work of Clozel and Thorne [2] that outlines a similar strategy. However, there seem to be differences as the approach of these authors involves local conditions and deformations of Galois representations. Using their approach, they have now proved the automorphy of L_m for $m \leq 8$.)

7 Rankin-Selberg Convolution

Another instance of functoriality is the Rankin-Selberg convolution. Denote by $\mathcal{A}_0(n, F)$ the set of cuspidal automorphic representations of GL_n over F and let $\pi_i \in \mathcal{A}_0(n_i, F)$ for $i = 1, 2$ and assume both are unitary. The Rankin-Selberg convolution provides an L-function $L(s, \pi_1 \times \pi_2)$ which by the work of Jacquet and Shalika extends to a function analytic everywhere except possibly at $s = 1$ where it has a simple pole if and only if $\pi_1 \simeq \pi_2^*$ (the dual of π_2). Another special case of functoriality would be the following hypothesis.

Conjecture 4. There exists a map

$$H_F(n_1, n_2) : \mathcal{A}_0(n_1, F) \times \mathcal{A}_0(n_2, F) \to \mathcal{A}(n_1 n_2, F)$$

in which a pair (π_1, π_2) is mapped to π_3 in such a way that

$$L(s, \pi_3) = L(s, \pi_1 \times \pi_2).$$

It is known that $H_F(n, 1)$ exists for all n. This is due to Godement-Jacquet. The work of Ramakrishnan [10] shows that $H_F(2, 2)$ exists and the work of Kim and Shahidi [4] shows that $H_F(2, 3)$ exists. Our main result is the following.

Theorem 1. *Suppose $H_{\mathbb{Q}}(n, 2)$ exists for all n. Then all the L_m are automorphic.*

[1] Thanks to Florian Herzig for informing us of this.

8 Brief Outline of the Proof

We will outline the main steps in the proof of Theorem 1. The details will be presented elsewhere. We note that contrary to the expectation that the proof of the analytic continuation of the L_m could be used to prove the Sato-Tate conjecture, our argument *uses* the Sato-Tate theorem to deduce the analytic continuation.

There are three main steps of the proof. The first is to define the notion of *virtual automorphy*. We say that a Dirichlet series

$$F(s) = \sum a_n n^{-s}$$

is *virtually automorphic* if

$$F(s) = \prod L(s, \pi_j)^{b_j}$$

where each π_j is an element of $\mathcal{A}(n_j, \mathbb{Q})$ for some positive integer n_j and some $b_j \in \mathbb{Z}$. We say it is virtually cuspidal if all the π_j in the above factorization are in $\mathcal{A}_0(n_j, \mathbb{Q})$. Now, we use the hypothesis $H(n, 2)$ to show that the L_m are virtually cuspidal.

In the second step, we have a natural notion of Rankin-Selberg convolution $F \times G$ of two virtually cuspidal Dirichlet series F and G. Using this, and the self-duality of the L_m, we deduce that

$$L_m \times L_m = \prod_{j,k} L(s, \pi_j \times \pi_k^*)^{b_j b_k}.$$

The right hand side has a pole at $s = 1$ of order $= \sum b_j^2$ using a result of Shahidi on Rankin-Selberg convolutions.

The third step is to show that the left hand side in fact has a simple pole at $s = 1$ as a consequence of the Sato-Tate theorem and an application of a Tauberian theorem. This implies that only one of the b_j is non-zero and must in fact be ± 1. It can be deduced (using the location of trivial zeros) that it is in fact equal to 1 and thus L_m is automorphic. The details are presented in [7].

9 Variants

Let $S(N, k)$ denote the space of holomorphic cusp forms of weight k for $\Gamma_0(N)$ and denote by $T_n = T_n(N, k)$ the n-th Hecke operator acting on $S(N, k)$. Then the eigenvalues of the normalized operator $T_p/p^{(k-1)/2}$ lie in the interval $[-2, 2]$. The Sato-Tate conjecture (in the general form given to it by Serre) concerns the distribution of these eigenvalues as N and k are fixed and p varies. In [13], Serre began a study of the distribution properties when p is fixed and N and k vary.

In particular, he proved that for a sequence (N_λ, k_λ) with $N_\lambda + k_\lambda \to \infty$, and for p a prime that does not divide any of the N_λ, the eigenvalues of $T_p(N_\lambda, k_\lambda)/p^{(k_\lambda-1)/2}$ are distributed in $[-2, 2]$ according to the measure

$$\mu_p = \frac{p+1}{\pi} \frac{(1-x^2/4)^{\frac{1}{2}}}{(p^{\frac{1}{2}} + p^{-\frac{1}{2}})^2 - x^2} dx.$$

This was made effective in the work of the first author and Sinha [8]. Denote by $s(N, k)$ the dimension of $S(N, k)$. Let $a_{p,i}$ for $1 \leq i \leq s(N, k)$ denote the eigenvalues of T_p acting on $S(N, k)$ (counted with multiplicity). Then, in ([8], Theorem 2), it is proved that

$$\frac{1}{s(N,k)} \#\{1 \leq i \leq s(N,k) : \frac{a_{p,i}}{p^{(k-1)/2}} \in [\alpha, \beta]\} = \int_\alpha^\beta \mu_p + \mathbf{O}(\frac{\log p}{\log kN})$$

where the implied constant is effectively computable.

Acknowledgements It is a pleasure to thank Florian Herzig for some helpful comments and especially for bringing [2] to our attention.

References

1. T. Barnet-Lamb, D. Geraghty, M. Harris, R. Taylor, A family of Calabi-Yau varieties and potential automorphy II. Publ. Res. Inst. Math. Sci. **7**, 29–98 (2011)
2. L. Clozel, J. Thorne, Level raising and symmetric power functionality, I. Preprint (2013)
3. H. Kim, Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. J. Am. Math. Soc. **16**, 139–183 (2003)
4. H. Kim, F. Shahidi, Functorial products for $GL_2 \times GL_3$ and the symmetric cube for GL_2. Ann. Math. **155**, 837–893 (2002)
5. V.K. Murty, On the Sato-Tate conjecture, in *Number Theory Related to Fermat's Last Theorem*, ed. by N. Koblitz. Progress in Mathematics, vol. 26 (Birkhauser, Boston, 1982)
6. V.K. Murty, On the Sato-Tate conjecture II, in *On Certain L-Functions*, ed. by J. Arthur et al. Clay Mathematics Proceedings, vol. 13 (American Mathematical Society, Providence, 2011), pp. 471–482
7. M.R Murty, V.K. Murty, Automorphy and the Sato-Tate conjecture. Preprint (2013)
8. M.R. Murty, K. Sinha, Effective equidistribution of eigenvalues of Hecke operators. J. Number Theory **129**, 681–714 (2009)
9. A. P. Ogg, A remark on the Sato-Tate conjecture. Invent. Math. **9**, 198–200 (1969/1970)
10. D. Ramakrishnan, Modularity of the Rankin-Selberg L-series and multiplicity one for SL_2. Ann. Math. **152**, 45–111 (2000)
11. P. Schapira, Mikio Sato: a visionary of mathematics. Not. Am. Math. Soc. **54**, 243–245 (2007)
12. J.-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves* (Benjamin, New York, 1968)
13. J.-P. Serre, Répartition asymptotique des valeurs propres de l'operateur de Hecke T_p. J. Am. Math. Soc. **10**, 75–102 (1997)
14. J. Tate, Algebraic cycles and poles of Zeta functions, in *Arithmetic Algebraic Geometry*, ed. by O. Schilling, (Harper and Row, New York, 1965), pp. 93–110
15. J. Tate, Conjectures on algebraic cycles in ℓ-adic cohomology, in *Motives*, Part 1, ed. by U. Jannsen et al. Proceedings of Symposia in Pure Mathematics, vol. 55 (American Mathematical Society, Providence, 1994), pp. 71–83

Division Polynomials with Galois Group $SU_3(3).2 \cong G_2(2)$

David P. Roberts

Abstract We use a rigidity argument to prove the existence of two related degree 28 covers of the projective plane with Galois group $SU_3(3).2 \cong G_2(2)$. Constructing corresponding two-parameter polynomials directly from the defining group-theoretic data seems beyond feasibility. Instead we provide two independent constructions of these polynomials, one from 3-division points on covers of the projective line studied by Deligne and Mostow, and one from 2-division points of genus three curves studied by Shioda. We explain how one of the covers also arises as a 2-division polynomial for a family of G_2 motives in the classification of Dettweiler and Reiter. We conclude by specializing our two covers to get interesting three-point covers and number fields which would be hard to construct directly.

1 Introduction

Suppose Y is a variety over $\mathbb{Q}$ with bad reduction at a set S of primes. For any prime ℓ, there are associated number fields coming from the mod ℓ cohomology of the topological space $Y(\mathbb{C})$. On the one hand, these number fields are interesting because their Galois groups tend to be Lie-type groups and their bad reduction is constrained to be within $S \cup \{\ell\}$. On the other hand, defining polynomials for these number fields are often beyond computational reach, even for quite simple Y and very small ℓ. In this paper, we work out some remarkable examples in this framework, with our computations of defining polynomials being *ad hoc* and just within the limits of feasibility.

1.1 Section-by-Section Overview

Section 2 provides background on the theoretical context, presenting it as a generalization of the familiar passage from an elliptic curve to one of its division

D.P. Roberts (✉)
Division of Science and Mathematics, University of Minnesota, Morris, MN 56267, USA
e-mail: roberts@morris.umn.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_8

polynomials. It then gives information on the Lie-type group which plays the central role for us, namely $SU_3(3).2 \cong G_2(2)$. Finally, the section reviews an earlier construction of a one-parameter polynomial for this Galois group due to Malle and Matzat [12, p. 412].

Section 3 explains how a rigidity argument gives two canonical degree 28 covers of surfaces defined over $\mathbb{Q}$, each with Galois group $SU_3(3).2 \cong G_2(2)$. In our notation, these covers are

$$\pi_1 : X_1 \to U_{3,1,1}, \qquad \pi_2 : X_2 \to U_{3,2}.$$

The bases are respectively $U_{3,1,1} = M_{0,5}/S_3$ and $U_{3,2} = M_{0,5}/(S_3 \times S_2)$, these being moduli spaces of five partially distinguishable points in the projective line. We explain how the covers are related by a cubic correspondence deduced from an exceptional isomorphism $U_{2,1,1,1} \cong U_{2,1,2}$ first studied by Deligne and Mostow [5, Sect. 10]. Standard methods, as illustrated in [14], might let one construct the covers π_i directly if certain curves had genus zero. However these methods are obstructed by the fact that these curves have positive genus.

Sections 4, 5, and 6 concern varietal sources for our covers. Section 4 starts with two different two-parameter families of covers of the projective line considered by Deligne and Mostow [4]. Via the group $SU_3(3).2$, these families of curves yield π_1 and π_2 from 3-division points. We use the second family to compute a defining polynomial $F_2(a, b, x)$ for π_2, and then transfer this knowledge to also obtain a polynomial $F_1(p, q, x)$ for π_1. Section 5 starts with a large family of genus three curves studied by Shioda [16]. This family already has an explicit 2-division polynomial $S(r_1, r_3, r_4, r_5, r_6, r_7, r_9, z)$ with Galois group $Sp_6(2)$. We find appropriate loci in the parameter space where the Galois group drops to the subgroup $G_2(2)$, and thereby independently get alternative polynomials $S_1(p, q, z)$ and $S_2(a, b, z)$ for the two covers. Section 6 explains how $F_1(p, q, z)$ also arises as the 2-division polynomial of a family of motives with motivic Galois group G_2 studied by Dettweiler and Reiter [6]. Sections 4, 5, and 6 each close with a subsection explicitly relating L-polynomials modulo the relevant prime ℓ to our division polynomials.

Section 7 shifts the focus away from varietal sources and onto specializations of our explicit polynomials. Specializing to suitable lines, we get 14 new degree 28 three-point covers with Galois group $SU_3(3).2 \cong G_2(2)$. These covers all have positive genus, and it would be difficult to construct them directly by the standard techniques of three-point covers.

Section 8 specializes to points, finding 376 different degree 28 number fields with Galois group $SU_3(3).2 \cong G_2(2)$ and discriminant of the form $2^j 3^k$. Again it would be difficult to construct these fields by techniques within algebraic number theory itself. We show that a thorough analysis of ramification in these fields is possible, despite the relatively large degree, by presenting such an analysis of the field with the smallest discriminant.

1.2 Computer Platforms

The bulk of the calculations for this paper were carried out in *Mathematica* [19]. However most calculations with number fields were done in *Pari* [17] while most calculations with L-functions were done in *Magma* [2].

Many of the statements in this paper can only be confirmed with the assistance of a computer. To facilitate verification and further exploration on the reader's part, a commented *Mathematica* file on the author's homepage accompanies this paper. It contains some of the formulas and data presented here.

1.3 Relation to a Similar Paper

The polynomials $F_1(p, q, x)$ and $F_2(a, b, x)$ are similar in nature to the polynomials $g_{27}(u, v, x)$ and $g_{28}(u, v, x)$ of [14] which have Galois groups $W(E_6)$ and $W(E_7)^+$ respectively. However [14] and this paper focus on different theoretical topics to avoid duplication. The discussion of monodromy and the universality of specialization sets in [14] applies after modification to the new base schemes $U_{3,1,1}$ and $U_{3,2}$ here. Similarly, our general discussion of division polynomials here could equally well be illustrated by $g_{27}(u, v, x)$ and $g_{28}(u, v, x)$.

2 Background

This section provides some context for our later considerations.

2.1 Division Polynomials

Classical formulas [18, p. 200] let one pass directly from an elliptic curve $Y : y^2 = x^3 + ax + b$ to division polynomials giving x-coordinates of their n-torsion points. Initializing via $f_1 = 1$ and $f_2 = 2$, these division polynomials f_n for $n \geq 3$ are computable by recursion:

$$\begin{aligned}
f_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
f_4 &= 4x^6 + 20ax^4 + 80bx^3 - 20a^2x^2 - 16abx - 4a^3 - 32b^2,\\
f_{2m} &= f_m \left(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2\right)/2,\\
f_{4m+1} &= (x^3 + ax + b)^2 f_{2m+2}f_{2m}^3 - f_{2m-1}f_{2m+1}^3,\\
f_{4m+3} &= f_{2m+3}f_{2m+1}^3 - (x^3 + ax + b)^2 f_{2m}f_{2m+2}^3.
\end{aligned}$$

Special cases give particularly interesting number fields. For example, at $(a, b) = (-1/3, 19/108)$ the degree sixty polynomial $f_{11} \in \mathbb{Q}[x]$ has Galois group $GL_2(11)/\{\pm 1\}$ and field discriminant -11^{109}.

On an abstract level, there are interesting number fields from n-torsion points on any abelian variety over $\mathbb{Q}$. More generally, from any variety Y over $\mathbb{Q}$ there are interesting field extensions from the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the cohomology groups $H^m(Y(\mathbb{C}), \mathbb{Z}/n\mathbb{Z})$. However for most pairs (Y, n), there is nothing remotely as explicit as the above recursion relations. In fact, there is presently no way at all to produce explicit division polynomials describing these fields.

2.2 The group $SU_3(3).2 \cong G_2(2)$

The Atlas [3] provides a wealth of group-theoretic information about the group $SU_3(3).2 \cong G_2(2)$. In particular, this group has the form $\Gamma.2$, where Γ has order $6048 = 2^5 3^3 7$ and is the 12th smallest non-abelian simple group.

Table 1 presents some of the information that is most important to us. The left half corresponds to the 14 conjugacy classes in Γ. The six classes $1A$, $2A$, $3A$, $3B$, $4C$, and $6A$ are rational, while the remaining classes are conjugate in pairs over the quadratic fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(i)$ respectively. When one considers the full group $\Gamma.2$, these pairs collapse and one has 16 conjugacy classes, ten in Γ and six in $\Gamma.2 - \Gamma$, with $12c$ and $12d$ two classes conjugate over $\mathbb{Q}(\sqrt{-3})$.

Of particular importance to us is that $\Gamma.2$ embeds as a transitive subgroup of the alternating group A_{28}. The cycle partition λ_{28} associated to a conjugacy class is given in Table 1. The group $\Gamma.2$ also embeds as a transitive subgroup of A_{36} and the corresponding λ_{36} are given. We use the degree 36 embedding only occasionally. For example, it is useful for distinguishing $3A$ from $3B$ via cycle partitions. As a convention, if we do not refer explicitly to degree we are working with the degree 28 embedding.

As just discussed, Table 1 has information about permutation representations of $\Gamma.2$. We are also interested in linear representations, and some group-theoretic information is contained in the small tables at the end of Sect. 4.3 (for characteristic 3), at the end of Sect. 5.5 (for characteristic 2), and in Fig. 3 (for characteristic zero).

2.3 Rigidity and Covers

Some fundamental aspects of our general context are as follows. Let G be a finite centerless group and let $C = (C_1, \ldots, C_z)$ be a list of conjugacy classes in G. Define

$$\overline{\Sigma}(C) = \{(g_1, \ldots, g_z) \in C_1 \times \cdots \times C_z : g_1 \cdots g_z = 1\},$$
$$\Sigma(C) = \{(g_1, \ldots, g_z) \in \overline{\Sigma}(C) : \langle g_1, \ldots, g_z \rangle = G\}.$$

Table 1 Information about conjugacy classes in $\Gamma.2$

Classes in Γ			
C	$\lvert C\rvert$	λ_{28}	λ_{36}
$1A$	1	1^{28}	1^{36}
$2A$	63	$y2^{12}1^4$	$2^{12}1^{12}$
$3A$	56	3^91	3^{12}
$3B$	672	3^91	$3^{11}1^3$
$4AB$	$2 \cdot 63$	4^61^4	4^62^6
$4C$	378	4^62^2	$4^62^41^4$
$6A$	504	6^431	6^43^4
$7AB$	$2 \cdot 864$	7^4	7^51
$8AB$	$2 \cdot 756$	$8^32^11^2$	8^34^3
$12AB$	$2 \cdot 504$	12^231	12^26^2

Classes in $\Gamma.2 - \Gamma$			
C	$\lvert C\rvert$	λ_{28}	λ_{36}
$2b$	252	$2^{12}1^4$	$2^{16}1^4$
$4d$	252	4^61^4	4^62^6
$6b$	2016	6^431	$6^53^12^11$
$8c$	1512	8^34	$8^34^221^2$
$12cd$	$2 \cdot 1008$	12^231	12^26^2

The group G acts on these sets by simultaneous conjugation and the action is free on $\Sigma(C)$. The mass of C is $\overline{\mu}(C) := |\overline{\Sigma}(C_1, \ldots, C_z)|/|G|$. A classical formula, presented in e.g. [12, Theorem 5.8], gives the mass as a sum over irreducible characters of G,

$$\overline{\mu}(C) = \frac{|C_1| \cdots |C_z|}{|G|^2} \sum_{\chi} \frac{\chi(C_1) \cdots \chi(C_z)}{\chi(1)^{z-2}}. \tag{1}$$

We say that C is rigid if $\mu(C) := |\Sigma(C)|/|G| = 1$ and strictly rigid if moreover $\overline{\mu}(C) = 1$.

Let $G \subseteq S_n$ now be a transitive permutation realization of G such that the centralizer of G in S_n is trivial. Let $\tau_1, \ldots, \tau_z$ be distinct points in the complex projective line, connected by suitable paths to a fixed base point. A tuple $(g_1, \ldots, g_z) \in \Sigma(C)$ then determines a degree n cover of the projective line with monodromy group G and local monodromy transformation g_i about the point τ_i. The genus g_n of the degree n cover is calculated via the cycle partitions $\lambda_i \vdash n$ by the general formula

$$|\lambda_1| + \cdots + |\lambda_z| = (z-2)n + 2 - 2g_n. \tag{2}$$

Here $|\lambda_i|$ indicates the number of parts of λ_i.

Let $M_{0,w}$ be the moduli space of w labeled distinct points in the projective line. This is a very explicit space, as τ_1, τ_2, and τ_3 can be uniquely normalized to 0, 1, and ∞ respectively. The group S_w acts on $M_{0,w}$ by permuting the points. If $\nu = (\nu_1, \ldots, \nu_r)$ sums to w then we let $S_\nu = S_{\nu_1} \times \cdots \times S_{\nu_r}$ and put $U_\nu = M_{0,w}/S_\nu$.

When $C = (C_1, \ldots, C_z)$ is rigid and the τ_i move in $M_{0,z}$, all the covers of the projective line fit together into a single cover of $M_{0,z+1}$. Moreover, under simple conditions as exemplified below, this cover is guaranteed to be defined over $\mathbb{Q}$. When $z = 3$, the space $M_{0,3}$ is just a single point and $M_{0,4}$ identified with $\mathbb{P}^1 - \{0, 1, \infty\}$, with τ_4 serving as coordinate. This case has been extensively treated in the literature. When $z \geq 4$ the situation is more complicated and a primary purpose of [14] and the present paper is to give interesting examples. When some adjacent C_i coincide, the cover descends to a cover of the corresponding quotient U_ν of $M_{0,z+1}$.

2.4 The Malle-Matzat Cover

Malle and Matzat computed the cover coming from the strictly rigid genus zero triple $(4d, 2b, 12AB)$ belonging to the group $\Gamma.2$. This Malle-Matzat cover is similar, but much simpler, than the covers π_1 and π_2 that we are about to consider. Accordingly we discuss it here as a model, and use it later as well for comparison.

Identifying the degree 28 covering curve X with $\mathbb{P}^1_x$, the cover $\mathbb{P}^1_x \to \mathbb{P}^1_t$ is then given by the explicit degree 28 rational function

$$t = \frac{-\left(x^4 + 20x^3 + 114x^2 + 68x + 13\right) \cdot \left(x^6 - 6x^5 - 435x^4 - 308x^3 + 15x^2 + 66x + 19\right)^4}{2^2 3^9 \left(x^2 + 4x + 1\right)^{12} (2x + 1)}.$$

The partitions $\lambda_1 = 4^6 1^4$ and $\lambda_3 = 12^2 3\,1$ are visible as root multiplicities of the numerator and denominator respectively. Rewriting the equation as

$$m(t, x) = 0, \tag{3}$$

the partition $\lambda_2 = 2^{12} 1^4$ likewise appears as the root multiplicities of $m(1, x)$.

The discriminant of the monic polynomial $m(t, x)$ is

$$D_m(t) = 2^{576} 3^{630} t^{18} (t - 1)^{12}. \tag{4}$$

It is a perfect square, in conformity with the fact that $\Gamma.2$ lies in the alternating group A_{28}. Thus $D_m(t)$ is not useful in seeing how the .2 enters Galois-theoretically. In fact, the order two quotient group corresponds to the extension of $\mathbb{Q}(t)$ generated by $\sqrt{t(1-t)}$.

The general theory of three-point covers says that $X \to \mathbb{P}_t$ has bad reduction within the primes dividing $|\Gamma.2|$, namely 2, 3, and 7. A particularly interesting

feature of $D_m(t)$ is that it reveals that in fact the Malle-Matzat cover has good reduction at 7. In [13, Sect. 8], we explained how the Malle-Matzat polynomial is a 3-division polynomial for a family of varieties with bad reduction only in $\{2, 3\}$, and this connection explains the good reduction at 7.

3 Rigid Covers of $U_{3,1,1}$ and $U_{3,2}$

This section explains how general theory gives the existence of our two main covers $\pi_1 : X_1 \to U_{3,1,1}$ and $\pi_2 : X_2 \to U_{3,2}$ and the cubic relation between them.

3.1 Five Strictly Rigid Quadruples

For a fixed number of ramifying points z and a fixed ambient group G, the mass formula (1) lets one find all C with $\overline{\mu}(C) = 1$. From any explicit tuple $(g_1, \ldots, g_z) \in \overline{\Sigma}(C)$, one gets $\mu(C) = 1$ or 0 according to whether $\langle g_1, \ldots, g_z \rangle$ is all of G or not. Carrying out this mechanical procedure for $z = 3$ and $G = \Gamma.2$ gives several strictly rigid triples, with only the Malle-Matzat triple having genus zero. For $z = 3$ and $G = \Gamma$, one gets yet more rigid triples. None of these have genus zero and some of them appear in Table 2 below.

Applying this mechanical procedure for $z = 4$ yields the following result:

Proposition 3.1. *There are no strictly rigid quadruples in $\Gamma.2$. Up to reordering and conjugation by the outer involution of Γ, there are five strictly rigid quadruples in Γ:*

$(3A,\ 3A,\ 3A,\ 4B)$: *(genus 9),* $(4A,\ 4A,\ 4A,\ 2A)$: *(genus 6),*
$(4A,\ 4A,\ 4A,\ 4B)$: *(genus 9),*
$(2A,\ 2A,\ 3A,\ 4A)$: *(genus 3),* $(4A,\ 4A,\ 3A,\ 3A)$: *(genus 9).*

Moreover, there are no other rigid quadruples C with $\overline{\mu}(C) < 4$. □

The list of all quadruples considered in the process of proving the proposition makes clear that the five quadruples presented stand quite apart from all the others. For the case $G = \Gamma.2$, the quadruples C with the smallest $\overline{\mu}(C)$ are $(4d, 2b, 2A, 2A)$, $(4d, 2b, 3A, 2A)$, $(4d, 3d, 4AB, 2A)$, $(2b, 2b, 3A, 2A)$, and $(4d, 4d, 3A, 2A)$. The corresponding $(\mu(C), \overline{\mu}(C))$ are $(0, 2.750)$, $(3, 3.000)$, $(0, 3.375)$, $(0, 3.500)$, and $(3, 3.\overline{666})$. For the case of $G = \Gamma$, there are 15 other C with $\overline{\mu}(C) \in [1, 2)$; all have $\mu(C) = 0$. Likewise, there are 12 C with $\overline{\mu}(C) \in [2, 3)$; four have $\mu(C) = 0$ and eight have $\mu(C) = 2$. Continuing the trend, there are eight C with $\overline{\mu}(C) \in [3, 4)$; two have $\mu(C) = 0$ while six have $\mu(C) = 3$. In particular, as asserted by the proposition, $\mu(C) = 1$ does not otherwise occur in the range $\overline{\mu}(C) < 4$; we expect that $\mu(C) = 1$ does not occur either for $\overline{\mu}(C) \geq 4$.

3.2 The Two Covers

In this section, we explain how the left-listed quadruples in Proposition 3.1 all give rise to the same cover $\pi_1 : X_1 \to U_{3,1,1}$ while the right-listed quadruples both give rise to the same cover $\pi_2 : X_2 \to U_{3,2}$. Figure 1 provides a visual overview of our explanation.

3.2.1 The Base Variety $M_{0,5}$

Let

$$M_{0,5} = \operatorname{Spec} \mathbb{Q}\left[s, t, \frac{1}{s(s-1)t(t-1)(s-t)}\right]$$

be the moduli space of five distinct ordered points in the projective line. The description on the right arises because the five points can be normalized to 0, 1, ∞, s, t by a unique fractional linear transformation.

A naive completion of $M_{0,5}$ is $\overline{M}_{0,5} = \mathbb{P}^1_s \times \mathbb{P}^1_t$. The top subfigure in each column on Fig. 1 gives a schematic representation of the real torus $\overline{M}_{0,5}(\mathbb{R})$. As usual, one should imagine the subfigure inscribed in a square, with the torus obtained by identifying left and right sides, and also top and bottom sides. Here and in the rest of Fig. 1, coordinate axes are distinguished by darker lines and lines which are at infinity in our particular coordinates are indicated by dotting.

A more natural completion $\hat{M}_{0,5}$ of $M_{0,5}$ is obtained from blowing up $\overline{M}_{0,5}$ at the three triple points $(0,0)$, $(1,1)$, and (∞,∞). The natural action of S_5 on $M_{0,5}$ extends uniquely to $\hat{M}_{0,5}$. Reflecting this equivariance, lines in $\hat{M}_{0,5} - M_{0,5}$ are naturally labeled by two-element subsets of $\{0, 1, \infty, s, t\}$. Another reflection of equivariance is that elements of $\{0, 1, \infty, s, t\}$ index fibrations over genus zero curves. The fibrations p_s and p_t are projections to the t and s axes respectively. The smooth fibers of p_0 and p_1 are the lines going through $(1,1)$ and $(0,0)$ respectively of slope different from 0, 1, ∞. The smooth fibers of p_∞ are certain hyperbolas going through both $(0,0)$, $(1,1)$. Note how each fibration partitions the ten lines of $\hat{M}_{0,5} - M_{0,5}$ into four sections and six half-fibers, the latter coming in three pairs to form the singular fibers.

Consider (01), (st), and (01∞) in their action on $M_{0,5}$. The group $S_3 \times S_2$ that they generate acts on the naive compactification $\overline{M}_{0,5}$. This action can be readily visualized in terms of our pictures of $M_{0,5}(\mathbb{R})$: (01) is a half-turn about the point $(1/2, 1/2)$, (st) is a reflection in the diagonal line, and (01∞) is a simultaneous one-third turn of the coordinate circles $\mathbb{P}^1_s(\mathbb{R})$ and $\mathbb{P}^1_t(\mathbb{R})$.

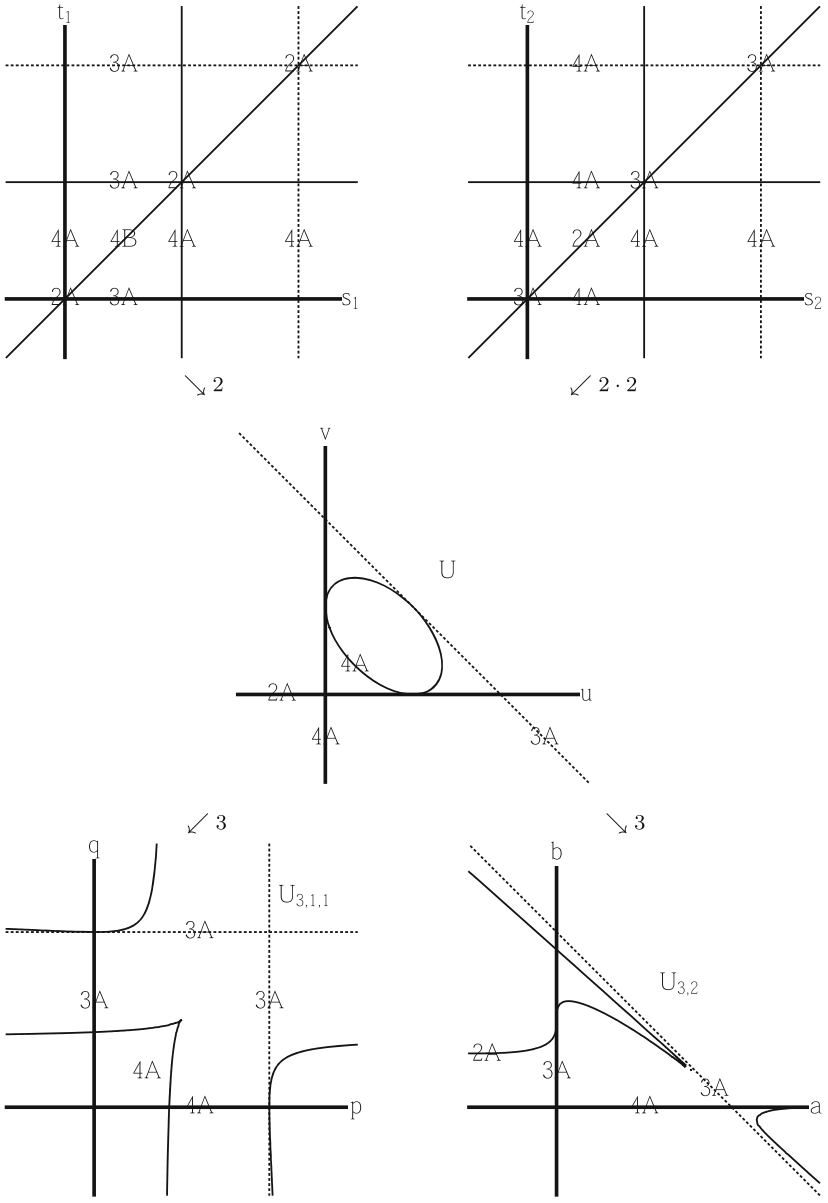


Fig. 1 Base varieties, ramification divisors, and associated conjugacy classes

3.2.2 Quotients of $M_{0,5}$

Figure 1 schematically indicates five planes, each with their own coordinates, as indicated by axis-labeling. The maps between these planes have the degrees indicated in Fig. 1, and are given by the following formulas:

$$(u,v) = \left(\frac{(s_1-1)s_1}{(t_1-1)t_1}, \frac{(s_1-t_1)^2}{(t_1-1)t_1}\right), \qquad (u,v) = \left((s_2-t_2)^2, (s_2+t_2-1)^2\right),$$

$$(p,q) = \left(\frac{3(2u-v+1)}{(u-v+2)^2}, \frac{3u(u-v+2)}{(2u-v+1)^2}\right), \quad (a,b) = \left(\frac{-768u^3}{W^2}, \frac{9\Delta}{W}\right).$$

Here $\Delta = u^2+v^2+1-2u-2v-2uv$ is a quantity which will play a recurring role, while $W = u^2-10uv+6u+9v^2-18v+9$ is a quantity which appears explicitly here only. Two moduli interpretations of (u,v), identifying U with $U_{2,1,1,1}$ and $U_{2,1,2}$ respectively, are given in (8) and (9) below. The moduli interpretation of (p,q) appears in (6) and (7) below. The moduli interpretation of (a,b) is less direct, but arises from the relation (5) below. The four maps displayed above are consequences of these moduli relations.

Our considerations are mainly birational, and so it is not of fundamental importance how we complete the various planes. As the diagrams indicate, three times we complete to a product $\mathbb{P}^1 \times \mathbb{P}^1$ of projective lines, while twice we complete to a projective plane $\mathbb{P}^2$. We are starting with two copies of the same variety, with $U^i_{1^5}$ having coordinates s_i and t_i. The other varieties are quotients:

$$U = U^1_{1^5}/\langle(01)\rangle, \qquad U = U^2_{1^5}/\langle(01),(st)\rangle,$$

$$U_{3,1,1} = U^1_{1^5}/\langle(01),(01\infty)\rangle, \qquad U_{3,2} = U^2_{1^5}/\langle(01),(01\infty),(st)\rangle.$$

Blowing up some of the intersection points would yield more natural completions, but we will not be pursuing our covers at this level of detail.

The natural double cover $U_{3,1,1} \to U_{3,2}$ is given in our coordinates by

$$(a,b) = \left(p^2q^2-6pq+4p+4q-3, pq\right). \tag{5}$$

Inserting this map on the bottom row of Fig. 1 would of course make the bottom triangle not commute, as even degrees would be wrong. Because of this lack of commutativity, the behavior of X_1 over curves and points in Fig. 5 is not directly related to the behavior of X_2 over the pushed-forward curves and points in Fig. 6.

3.2.3 Covers of $M_{0,5}$

The five rigid tuples of Proposition 3.1 enter Fig. 1 through our associating conjugacy classes in Γ to lines. On the top-left subfigure, from any fixed choice

of $s \in \mathbb{C} - \{0, 1\}$ one has a cover of $\mathbb{P}^1_t(\mathbb{C})$ ramified at 0, 1, ∞, and s. The local monodromy classes associated to moving in a counter-clockwise loop in the t-plane about these singularities form the ordered quadruple $(3A, 3A, 3A, 4B)$. On the top-right subfigure they form $(4A, 4A, 4A, 2A)$.

But now by rigidity one has local monodromy classes associated to all ten lines of $\hat{M}_{0,5} - M_{0,5}$. Using the monodromy considerations of [14], we have computed these classes. The classes are placed in the top two subfigures of Fig. 1. Interchanging the roles of s and t, one sees that the cover of $M_{0,5}$ indicated by the top-left subfigure also arises from $(4A, 4A, 4A, 4B)$. However the top right cover now just arises in a new way from the original quadruple $(4A, 4A, 4A, 2A)$. Via any of the three remaining projections $p_0, p_1\, p_\infty$, the covers represented by the top-left and top-right subfigures arise respectively from $(2A, 2A, 3A, 4A)$ and $(4A, 4A, 3A, 3A)$.

3.2.4 Descent to Covers of $U_{3,1,1}$ and $U_{3,2}$

The labeling by conjugacy classes on both the top-left and top-right copies of $M_{0,5}$ is visibly stable under the action of $S_3 = \langle (01), (01\infty) \rangle$. Moreover on the top-right, the labeling is also stable under the diagonal reflection (st). One therefore has descent, to a cover $\pi_1 : X_1 \to U_{3,1,1}$ on the left and a cover $\pi_2 : X_2 \to U_{3,2}$ on the right.

3.3 Summarizing Diagram

We now shift attention from Figs. 1 to 2. The lowest varieties $U_{3,1,1}$, $U_{3,2}$ and their common cubic covering by U from Fig. 1 are redrawn in the left part of Fig. 2. The two copies of $M_{0,5}$ from the top of Fig. 1 now play a secondary role and are suppressed. In their place, the degree 28 coverings X_1 and X_2 discussed above are now explicitly indicated. Also Fig. 2 contains their common base change to $X_0 \to U$.

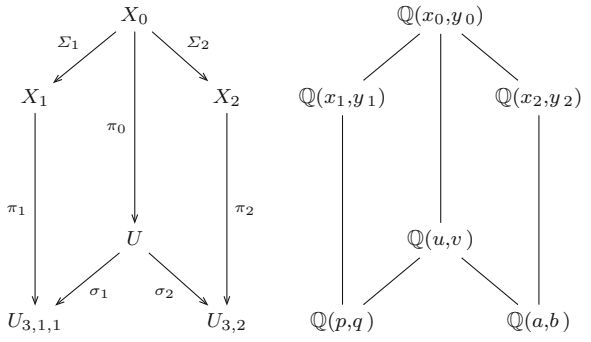


Fig. 2 *Left*: the covers π_1 and π_2, as related by the cover π_0. *Right*: corresponding function fields

The left part of Fig. 2 commutes, and so the upper maps Σ_i, like the lower maps σ_i from Fig. 1, have degree three. Note that while the top-left part of Fig. 2 has been canonically defined, we do not yet have an explicit description for any of the surfaces X_i or maps Σ_i. We do not yet have an explicit description of the vertical maps π_i either. In particular, we have not yet discussed the coordinates x_i, y_i from the top-right part of Fig. 2.

4 3-Division Polynomials of Deligne-Mostow Covers

Here we first recognize $\pi_1 : X_1 \to U_{3,1,1}$ and $\pi_2 : X_2 \to U_{3,2}$ as associated to 3-division points on certain Deligne-Mostow covers. Using this connection, we compute π_2 directly and then deduce explicit formulas for π_0 and π_1. The last section calculates some sample L-polynomials and illustrates how their mod 3 reductions are determined by our equations for the π_i.

4.1 Local Monodromy Agreement

Deligne and Mostow's treatises [4, 5] concern curves presented in the form $y^n = f(\text{parameters}, x)$ and the dependence of their period integrals on the parameters. Their table in Sect. 14.1 of [4] has 36 lines, each corresponding to a family. Their lines 3 and 2, written using our parameters p and q on $U_{3,1,1}$, are

$$y^4 = x^2(px^3 + 3x^2 + 3x + q), \tag{6}$$

$$y^4 = x(px^3 + 3x^2 + 3x + q)^2. \tag{7}$$

In both cases, the complex roots of $f(x)$ are the three roots α_1, α_2, and α_3 of $px^3 + 3x^2 + 3x + q$ and $\alpha_4 = 0$. A series solution for each equation in the variable $x - \alpha_4 = x$ is

$$y = q^{1/4}x^{1/2}\left(1 + \frac{3x}{4q} - \frac{27x^2}{32q^2} + \cdots\right), \quad y = q^{1/2}x^{1/4}\left(1 + \frac{3x}{2q} - \frac{9x^2}{8q^2} + \cdots\right).$$

The important quantity for us is the leading exponent associated with α_4, namely $\mu_4 = 1/2$ and $\mu_4 = 1/4$ in the two cases. Similarly, expanding in the local coordinates $x - \alpha_i$ for $i \in \{1, 2, 3\}$, one has $\mu_1 = \mu_2 = \mu_3$. In the two cases, these exponents are $1/4$ and $1/2$ respectively.

Corresponding to the title of [5] containing just $PU(1, n)$ rather than more general $PU(m, n)$, Deligne and Mostow are interested in the case when the sum of the μ_j corresponding to roots of $f(x)$ is in $(1, 2)$. A leading exponent at ∞, here μ_5, is then

defined so that the sum of all μ_i is 2. So, summarizing in the two cases, the exponent vector is

$$(\mu_1, \mu_2, \mu_3, \mu_4, \mu_5) = \left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}\right), \quad (\mu_1, \mu_2, \mu_3, \mu_4, \mu_5) = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{4}, \frac{1}{4}\right).$$

These are the quantities actually presented on lines 3 and 2 of the Deligne-Mostow table. From $\mu_4 = \mu_5$ one has descent from $U_{3,1,1}$ to $U_{3,2}$ in the second case, but not the first.

Switch notation to $(\mu_0, \mu_1, \mu_\infty, \mu_s, \mu_t)$ to agree with the previous section. The local monodromies about the divisor of D_{jk}, as classes in $GL_3(\mathbb{C})$, are represented by

$$m_{jk} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & \exp(2\pi i(\mu_j + \mu_k)) \end{pmatrix}.$$

Here the off-diagonal 1 can be replaced by 0, except in the case $\mu_j + \mu_k \in \mathbb{Z}$, i.e. $\mu_j + \mu_k = 1$.

Global monodromy is in fact in a unitary subgroup of $GL_3(\mathbb{Z}[i])$. The matrix m_{jk} has infinite order if $\mu_j + \mu_k = 1$, and otherwise has the finite order $\text{denom}(\mu_j + \mu_k) \in \{2, 4\}$. Reducing to $PU_3(\mathbb{F}_3) \subset PGL_3(\mathbb{F}_9)$, the infinite order m_{jk} acquire order 3 and the finite order m_{jk} maintain their order. Moreover, not just the orders but even the conjugacy classes can be shown to agree with those presented at the top of Fig. 1. Thus the rigid covers of the previous section are realized as 3-division covers.

4.2 Explicit Equations

The following theorem gives equations describing the three covers π_0, π_1, and π_2. A preliminary comment about the contrast between curves and surfaces is in order. Requiring automorphisms to fix $\mathbb{C}$ pointwise, $\text{Aut}(\mathbb{C}(x))$ is just $PGL_2(\mathbb{C})$ while $\text{Aut}(\mathbb{C}(x, y))$ is the infinite-dimensional Cremona group. A consequence is that any given $F : \mathbb{P}^1 \to \mathbb{P}^1$ is already in a good form. Furthermore, one has only a total of six degrees of freedom in adjusting domain and target coordinates in order to get a particularly nice form, like that of the Malle-Matzat cover. However a given $F : \mathbb{P}^2 \to \mathbb{P}^2$ may be in far from best form, and adjusting coordinates to improve the form seems to be more of an art than a science. The theorem gives the best form we could find in each case, but does not exclude the possibility that there are more concise forms.

Theorem 4.1. *The surfaces X_0, X_1, and X_2 are all rational. There are coordinate functions (x_i, y_i) on X_i so that the top five maps in the left half of Fig. 2 are as follows:*

The three covers with domain X_0. *Abbreviate* $(x, y) = (x_0, y_0)$ *and*

$$\begin{aligned}
g_4 &= 15x^2 - 4yx - 4x + 5,\\
g_{6a} &= 9xy^2 + y^2 + 18xy - 18y - 66x + 6,\\
g_{6b} &= 225x^2 - 30yx - 30x - 2y^2 + 6y + 33,\\
g_{7a} &= 15yx^2 + 65x^2 - 2y^2x - 4yx - 2x + 5y + 5,\\
g_{7b} &= 45yx^2 - 105x^2 + 6y^2x - 8yx - 14x - 5y - 5,\\
g_9 &= 225x^3 - 30yx^2 - 105x^2 + y^2x + 22yx + 21x + y^2 - 8y - 9,\\
g_{10} &= 225x^2y^2 + 1200x^2y + 2850x^2 + 250xy^2 - 1500x + 2y^4 + 8y^3 + 37y^2\\
&\quad -192y + 402,\\
g_{17} &= 2025x^3y^2 + 24300x^3y + 39150x^3 + 540x^2y^3 + 1845x^2y^2 - 180x^2y\\
&\quad -29610x^2 - 18xy^4 + 168xy^3 - 213xy^2 - 252xy + 9522x + 10y^4\\
&\quad +60y^3 - 105y^2 + 900y - 2070,\\
g_{18} &= 50625x^5 - 3375yx^4 + 30375x^4 - 675y^2x^3 + 2025yx^3 + 2700x^3\\
&\quad +75y^3x^2 + 2025yx^2 + 5850x^2 - 2y^4x - 18y^3x + 33y^2x - 513yx\\
&\quad +63x + 15y^3 - 30y^2 + 270y + 315.
\end{aligned}$$

Then Σ_1, π_0, *and* Σ_2 *are given by*

$$x_1 = -\frac{g_{17}}{g_{6a}g_{6b}}, \qquad y_1 = \frac{45g_{10}(x+1)\left(9x^2-2x+1\right)}{g_4 g_{6a} g_{6b}},$$

$$u = \frac{g_{6b}^6 x^4(x+1)}{25g_{6a}^3 g_{7a}^2\left(9x^2-2x+1\right)}, \qquad v = \frac{g_{18}^2 g_4^2 g_9}{25g_{6a}^3 g_{7a}^2\left(9x^2-2x+1\right)},$$

$$x_2 = \frac{1}{x+1}, \qquad y_2 = \frac{g_4 g_{7a}}{5g_{7b}(x+1)^2}.$$

The cover π_1. *Abbreviate* $(x, y) = (x_1, y_1)$ *and*

$$\begin{aligned}
h_{11} &= 2x^5 + 4x^4 - 12x^3y + 8x^3 + 9x^2y + 16x^2 - 24xy + 8x + 3y^3\\
&\quad +18y + 16,\\
h_{26} &= 4x^7 + 48x^6y + 7x^6 - 72x^5y^2 + 24x^5 + 48x^4y^3 - 63x^4y^2 + 288x^4y\\
&\quad +42x^4 - 12x^3y^4 - 288x^3y^2 + 48x^3 - 3x^2y^4 + 192x^2y^3 - 252x^2y^2\\
&\quad +576x^2y + 84x^2 - 24xy^4 - 288xy^2 + 32x + 3y^6 - 6y^4 + 192y^3\\
&\quad -252y^2 + 384y + 56.
\end{aligned}$$

Then π_1 is given by

$$p = \frac{3h_{26}}{h_{11}^2}, \qquad q = \frac{3h_{11}y\left(3x^2 - y^2 + 6\right)^4}{h_{26}^2}.$$

The cover π_2. *Abbreviate $(x, y) = (x_2, y_2)$ and*

$$\begin{aligned} f_9 &= 144x^3y - 408x^2y - 12x^2 + 8xy^2 + 388xy + 20x - 9y^2 - 126y - 9, \\ f_{14} &= 36x^4y^2 - 288x^3y^2 - 504x^3y + 816x^2y^2 + 1236x^2y - 12x^2 + 2xy^3 \\ &\quad -840xy^2 - 1038xy + 20x - 9y^3 + 297y^2 + 297y - 9. \end{aligned}$$

Then π_2 is given by

$$a = \frac{3f_9^3}{f_{14}^2\left(12x^2 - 20x + 9\right)}, \qquad b = \frac{36x^4y^2}{f_{14}}.$$

Proof. We will sketch our construction only, as there were many complicated variable changes to reduce to the relatively concise formulation given in the theorem. We first found π_2 as follows. Via (7), the genus three curve $Y_2(p, q)$ is presented as a quartic cover of $\mathbb{P}^1_x$. Replacing x by t^2 in (7) and factoring, one gets a presentation of $Y_2(p, q)$ as a double cover of the t-line $\mathbb{P}^1_t$:

$$y^2 = pt^7 + 3t^5 + 3t^3 + qt.$$

Three-torsion points on the Jacobian of $Y_2(p, q)$ are related to unramified abelian triple covers of $Y_2(p, q)$. Such a triple cover arises as a base-change of certain ramified non-abelian triple covers of $\mathbb{P}^1_t$.

Consider now a partially-specified triple cover of $\mathbb{P}^1_t$, given by

$$(at + \mu)z^3 + (bt - \lambda\mu)z^2 + t(c + t)z + t(d - t) = 0.$$

The discriminant of this polynomial with respect to z is a septic polynomial in t with zero constant term. Setting it equal to $k(pt^7 + 3t^5 + 3t^3 + qt)$ imposes the necessary ramification condition. It also gives seven equations in the seven unknowns a, b, c, d, λ, μ, and k, all dependent on the two parameters p and q.

The equations corresponding to the coefficients of t^2, t^4, and t^6 let one eliminate d and μ and reduce the remaining equation to

$$\begin{aligned} &-9a^2\lambda^2 + 162a^2\lambda - 729a^2 + 18ab\lambda^2 + 180ab\lambda - 486ab + 120ac\lambda \\ &\qquad -216ac + 3b^2\lambda^2 + 34b^2\lambda + 27b^2 + 24bc\lambda + 72bc + 32c^2 = 0. \end{aligned}$$

The system consisting of this equation and the equations coming from the coefficients of t^1, t^3, t^5, and t^7 is very complicated to solve. Nonetheless, one can eliminate

all the remaining variables, at the expense of putting in the new parameters x_2 and y_2. Conveniently, p and q enter the final formulas symmetrically and can then be replaced by a and b via (5), yielding our presentation of π_2.

Our formula for π_0 was then obtained via base-change. To get π_1 we first built a double cover $\tilde{X}_0$ of X_0 which is a Galois sextic cover of the yet-to-be explicitized X_1. Then we explicitized X_1 by taking invariants under the Galois action, $X_1 = \tilde{X}_0/S_3$. □

There is a standard way to pass from bivariate rational functions as in the theorem to univariate polynomials which are more traditional in number theory. Namely, suppose given a cover of rational surfaces via say $u = A(x,y)/B(x,y)$ and $v = C(x,y)/D(x,y)$. Assuming x indeed generates the field extension, one can express the cover in terms of x alone via a resultant

$$F(u,v,x) = \mathrm{Res}_y(A(x,y) - uB(x,y), C(x,y) - vD(x,y)).$$

Carrying this out in our context gives $F_0(u,v,x)$, $F_1(p,q,x)$ and $F_2(a,b,x)$. Expanded out, they have 1606, 772, and 209 terms respectively. Interchanging the roles of x and y, one gets polynomials $G_0(u,v,y)$, $G_1(p,q,y)$, and $G_2(a,b,y)$ with 4941, 1469, and 951 terms respectively. In general, keeping either just x or just y is unlikely to minimize the number of terms. More likely the minimum can only be obtained by keeping some third variable $z \in \mathbb{Q}(x,y)$. There do not seem to be standard procedures to find these best variables.

4.3 *L-Polynomials of Deligne-Mostow Covers and Their Reduction Modulo* 3

To explicitly illustrate the 3-division nature of the main polynomials $F_1(p,q,x)$ and $F_2(a,b,x)$, we pursue the polynomial $F_0(u,v,x)$ describing their common base-change. Cubically base-changed to the u-v plane, the Deligne-Mostow covers in question after some twisting become as follows:

$$Y_1(u,v): \quad vy^4 = x^2(x-1)^3(vx^2 + (1-u-v)x + u) \qquad \text{(genus 4)}, \tag{8}$$

$$Y_2(u,v): \quad 4y^4 = \left(x^2 + 2x + 1 - \frac{4}{v}\right)^2 \left(x^2 - 2x + 1 - \frac{4u}{v}\right) \qquad \text{(genus 3)}, \tag{9}$$

$$E(u,v): \quad y^2 = (x-1)(vx^2 + (1-u-v)x + u) \qquad \text{(genus 1)}.$$

The quadratic subcover of $Y_1(u,v)$ is the elliptic curve $E(u,v)$ while the quadratic subcover of $Y_2(u,v)$ has genus zero.

Our monodromy considerations give a relation between $Y_1(u,v)$ and $Y_2(u,v)$. The twisting factors v and 4 in the equations above are included so that we can give a clean statement of this relation on a more refined level:

$$L_p(Y_1(u,v),x) = L_p(Y_2(u,v),x)L_p(E(u,v),x). \tag{10}$$

Here u and v are rational numbers and p is any prime good for all three curves. Each L-polynomial $L_p(Y,x)$ is the numerator of the corresponding zeta-function $\zeta_p(Y,x)$, obtained by determining the point counts $|Y(\mathbb{F}_{p^f})|$ for f up through genus(Y). Our computations below obtain this L-polynomial via *Magma*'s command `ZetaFunction` [2].

The factorization (10) has the following explicit form:

$$L_p(Y_1(u,v),x) = (1 + ax + bx^2 + cx^3 + pbx^4 + p^2ax^5 + p^3x^6)(1 + dx + px^2).$$

For $p \equiv 1$ (4), both factors in turn split over $\mathbb{Q}(i)$ as the product of two conjugate polynomials. For $p \equiv 3$ (4), the coefficients a, c, and d all vanish, so that each factor is an even polynomial. Taking $(u,v) = (-4,-3)$ as a running example, these two cases are represented by the first two good primes:

$$\begin{aligned} L_5(Y_1(-4,-3),x) &= \left(1 - x^2 - 16x^3 - 5x^4 + 125x^6\right)\left(1 - 2x + 5x^2\right), \\ &= N\left(1 + ix - (1-2i)x^2 - (10+5i)x^3\right) N(1 - (1+2i)x), \\ L_7(Y_1(-4,-3),x) &= \left(1 + 5x^2 + 35x^4 + 343x^6\right)\left(1 + 7x^2\right). \end{aligned}$$

Here and below, $N(f) = f\bar{f}$ is the product of a polynomial f and its conjugate $\bar{f}$.

Consider now $L_p(Y_2(u,v),x) = N(1 + \alpha x + \beta x^2 + \gamma x^3)$ in $\mathbb{F}_3[x]$ for varying $p \equiv 1$ (4). To twist into a situation governed by $SU_3(3)$ we replace x by $-\gamma^5 x$ to obtain the modified polynomial $\hat{L}_p(Y_2(u,v),x) = N(1 - \alpha\gamma^5 x + \beta\gamma^2 x^2 - x^3) \in \mathbb{F}_3[x]$. Similarly, for $p \equiv 3$ (4), consider $L_p(Y_2(u,v),x) = 1 + bx^2 + bpx^4 + p^3x^6$ in $\mathbb{F}_3[x]$. To twist into a situation governed by $SU_3(3).2 - SU_3(3)$, we replace x^2 by px^2 obtaining $\hat{L}_p(Y_2(u,v),x) = 1 + bpx^2 + bpx^4 + x^6 \in \mathbb{F}_3[x]$. For $5 \le p \le 97$, the polynomials $\hat{L}_p(Y_2(-4,-3),x)$ are calculated directly by `ZetaFunction` to be

Class(p)	$\lambda_{28}(p)$	$\hat{L}_p(Y_2(-4,-3),x) \in \mathbb{F}_3[x]$	Primes p
$3B$	$3^9 1$	$N\left(1 - x^3\right)$	89
$7AB$	7^4	$N\left(1 - (1+i)x + (1-i)x^2 - x^3\right)$	5, 13, 29, 53, 61, 73, 97
$8AB$	$8^3 2\, 1^2$	$N\left(1 - ix - ix^2 - x^3\right)$	37, 41
$12AB$	$12^2 3\, 1$	$N\left(1 + (1-i)x - (1+i)x^2 - x^3\right)$	17
$6b$	$6^4 3\, 1$	$\left(1 + x^2\right)^3$	11, 19
$8c$	$8^3 4$	$\left(1 + x^2\right)\left(1 + 2x + 2x^2\right)\left(1 + x + 2x^2\right)$	43, 67, 79, 83
$12c, 12d$	$12^2 3\, 1$	$(1+x)^2(1+2x)^2\left(1 + x^2\right)$	7, 23, 31, 47, 59, 71.

For general (u,v), the fact that $F_0(u,v,x)$ functions as a 3-division polynomial is seen by the fact that $\hat{L}_p(Y_2(u,v),x) \in \mathbb{F}_3[x]$ depends only the conjugacy class in $\Gamma.2$ determined by p. Up to small ambiguities, as described in Table 1, this conjugacy class is determined by the class of p modulo 4 and the factorization partition $\lambda_{28}(p)$ of $F_0(u,v,x) \in \mathbb{F}_p[x]$.

5 2-Division Polynomials of Shioda Quartics

In this section, we recognize $\pi_1 : X_1 \to U_{3,1,1}$ and $\pi_2 : X_2 \to U_{3,2}$ as 2-division polynomials for certain genus three Shioda curves. The last section calculates some sample L-polynomials and illustrates how their mod 2 reductions are determined by our equations for the π_i.

5.1 The Shioda $W(E_7)^+$ Polynomial

In [15], Shioda exhibits multiparameter polynomials for the Weyl groups $W(E_6)$, $W(E_7)$, and $W(E_8)$. He proves in Theorem 7.2 that these polynomials are generic, in the sense that any $W(E_n)$ extension of a characteristic zero field F is given by some specialization of the parameters.

The case of $W(E_7) \cong W(E_7)^+ \times C_2$ is explained in greater detail in [16] and goes as follows. Fix a parameter vector $r = (r_1, r_3, r_4, r_5, r_6, r_7, r_9) \in \mathbb{C}^7$ and consider the equation

$$y^2 = x^3 + (w^3 + r_4 w + r_6)x + (r_1 w^4 + r_3 w^3 + r_5 w^2 + r_7 w + r_9). \tag{11}$$

The vanishing of the right side defines a quartic curve Q_r in the w-x plane. The equation itself defines a $K3$ surface in x-y-w space mapping to the w-line with elliptic curves as fibers. Now consider the substitutions

$$x = zw + b, \qquad y = cw^2 + dw + e,$$

which make each side of (11) a quartic polynomial in w. Equating like coefficients, (11) then becomes five equations in the five unknowns z, b, c, d, and e. There are 56 solutions, paired according to the negation operator $(z, b, c, d, e) \mapsto (z, b, -c, -d, -e)$. Much of the interest in Shioda's theory comes from regarding these solutions as generators for the rank seven Mordell-Weil group of the generic fiber.

Our interest instead is that the 28 lines $x = zw + b$ are exactly the 28 bitangents of Q_r. The variables b, c, d, and e can be very easily eliminated and one gets Shioda's degree 28 generic polynomial for the rotation subgroup $W(E_7)^+$:

$$\begin{aligned} &S(r, z) = \\ &z^{28} - 8r_1 z^{27} + 72r_3 z^{25} + 60r_4 z^{24} + (-504r_5 + 432r_1 r_4)z^{23} + \\ &(384r_1^2 r_4 - 1248r_1 r_5 + 540r_3^2 - 540r_6)z^{22} + \cdots \end{aligned}$$

Expanded out as an element of $\mathbb{Z}[r, z] := \mathbb{Z}[r_1, r_3, r_4, r_5, r_6, r_7, r_9, z]$, there are 1784 terms. The polynomial is weighted homogeneous when the variable z is given

weight 1 and each parameter r_i is given weight i. The polynomial discriminant of $S(r, z)$ factors over $\mathbb{Q}$ as $\Delta(r) = D(r)C(r)^2$, with $D(r)$ a source of ramification and $C(r)$ an irrelevant artifact of our coordinates.

5.2 Using $\Gamma.2 \subset W(E_7)^+$

The group $\Gamma.2$ is a subgroup of $W(E_7)^+$. Since genericity implies descent-genericity [11], any degree 28 extension K/F with Galois group $\Gamma.2$ is of the form $F[x]/S(r, z)$ for suitable $r \in F^7$. For the Malle-Matzat polynomial $m(t, x)$, we considered various $t \in \mathbb{Q}$ and conducted a very modest search over different polynomials of small height defining the same field as $\mathbb{Q}[x]/m(t, x)$. For a few t, we found a polynomial of the form $S(r, z)$ for certain $r \in \mathbb{Q}^7$. Some of these seven-tuples had similar shapes, and interpolating these only we found that the Malle-Matzat family seemed also to be given by

$$S(0, -27t^2, -81t^2, 243t^3, 243t^3, -729t^4, 729t^5, z) = 0. \tag{12}$$

The correctness of this alternative equation is algebraically confirmed by eliminating t from the pair of Eqs. (3), (12), to obtain the relation

$$z = \frac{(x-1)^2\left(x^4 + 20x^3 + 114x^2 + 68x + 13\right) \cdot \left(x^6 - 6x^5 - 435x^4 - 308x^3 + 15x^2 + 66x + 19\right)^2}{243\left(x^2 + 4x + 1\right)^8}. \tag{13}$$

Thus Eq. (12) realizes the Malle-Matzat polynomial as a 2-division polynomial for an explicit family of genus three curves.

The simplicity of the equational form (12) is striking, especially taking into account that all the positive integers printed are powers of 3. Expanding the family out as a polynomial in $\mathbb{Z}[t, z]$ hides the simplicity, as there are 75 terms.

5.3 A Search for $\Gamma.2$ Specializations

Given the simplicity of (12), we searched for similar families as follows. We considered one-parameter polynomials of the form $S(r, z)$ with $r_i = a_i t^{e_i}$. Here the $e_i \in \mathbb{Z}_{\geq 0}$ are fixed and the constants a_i yet unspecified. We looked at many $(e_1, e_3, e_4, e_5, e_6, e_7, e_9)$ near-proportional to $(1, 3, 4, 5, 6, 7, 9)$ so as to ensure that $D(a_1 t^{e_1}, \ldots, a_9 t^{e_9})$ has the form $t^a d(t)$ with $d(t)$ of small degree. When a particular exponent e_i made a proportionality $(e_1, \ldots, e_9) \propto (1, \ldots, 9)$ not so close, we set a_i equal to zero, rendering e_i irrelevant.

We then worked modulo 5, letting $(a_1, \ldots, a_9)$ run over relevant possibilities in $\mathbb{F}_5^7$. If k of the a_i are set equal to zero, we looked at just 4^{5-k} possibilities: we kept the other a_i nonzero, and homogeneity and the scaling $t \mapsto ut$ each saved a factor of 4. We examined each one-parameter family $S(a_1 t^{e_1}, \ldots, a_9 t^{e_9}, z)$ by specializing to $t \in \mathbb{F}_{5^j}$ and factoring in $\mathbb{F}_{5^j}[z]$. In the rare cases when all factorization patterns λ_{28} for $j = 1, 2$, and 3 corresponded to elements of $\Gamma.2$, as on Table 1, we proceeded under the expectation that $S(a_1 t^{e_1}, \ldots, a_9 t^{e_9}, z) = 0$ defines a cover with Galois group in $\Gamma.2$.

For 15 $(e_1, \ldots, e_9)$ we found exactly one $(a_1, \ldots, a_9)$ which works. For five $(e_1, \ldots, e_9)$ we found several $(a_1, \ldots, a_9)$ which work, suggestive of a two-parameter family. We then reinspected these five $(e_1, \ldots, e_9)$ in characteristic seven, imposing also that the covers sought be tame. The case $(e_1, e_3, e_4, e_5, e_6, e_7, e_9) = (0, 1, 1, \star, 2, 2, 2)$ seemed to give a two-parameter family in both characteristics, satisfying the tameness condition at 7; here the $\star$ means that we are setting $a_5 = 0$. Standardizing coordinates, the two-parameter families seemed to match well, and there remained the task of lifting to characteristic zero.

We first found that $S(1, 0, 3t, 0, 0, 0, -t^2, z) \in \mathbb{Q}[t, z]$ defines a 3-point cover, giving us hope that coefficients might be even simpler than in (12). Finally we found a good two-parameter family $S_0(u, v, z) = 0$ where

$$S_0(u, v, z) = S(1, u - v + 1, -3u, 0, u(-u + v - 1), u(-u + v - 1), -u^2, z). \tag{14}$$

The discriminant of $S_0(u, v, z)$ is

$$D(u, v) = 2^{216} 3^{108} u^{42} v^{24} (u^2 - 2uv - 2u + v^2 - 2v + 1)^2$$

times the square of a large-degree irreducible polynomial in $\mathbb{Z}[u, v]$.

5.4 Explicit Polynomials

Our computation of $S_0(u, v, z)$, as just described, is completely independent of the considerations of the previous section. In fact we found $S_0(u, v, z)$ before we found its analog $F_0(u, v, x)$ from the previous section. It might have been possible to directly descend $S_0(u, v, z)$ to $S_1(p, q, z)$ and $S_2(a, b, z)$ below. However instead we obtained these new S_i from the corresponding F_i: we took lots of specialization points, applied *Pari*'s `polred` to obtain alternate polynomials, selected those that are of the form $S(r_1, r_3, r_4, r_5, r_6, r_7, r_9, z)$, and interpolated those that seemed to fit a common pattern.

Theorem 5.1. *Abbreviate* $d = p^2q^2 - 6pq + 4p + 4q - 3$, $A = 256/a$, *and* $B = (b-1)/8$. *The covers* π_0, π_1, *and* π_2 *are also given respectively via the polynomials* $S_0(u, v, z)$,

$$S_1(p,q,z) = S(\begin{array}{r} 0, \\ d^2p, \\ 3d^2p^2(q-1), \\ 3d^3p^2, z), \\ -d^3p^2\left(3p^2q^2 - 9pq + 4q + 2p\right), \\ -3d^4p^3(q-1), \\ d^5p^4\left(2pq^2 - 3q + 1\right), \end{array}$$

$$S_2(a,b,z) = S(\begin{array}{r} 1, \\ 3\left(AB^2 + 2\right), \\ -3\left(8AB^2 + AB + 1\right), \\ -3\left(5AB^2 + AB - 4\right), z). \\ -8A^2B^4 - A^2B^3 - 184AB^2 - 31AB - A - 2, \\ -56A^2B^4 - 7A^2B^3 - 199AB^2 - 58AB - 4A + 10, \\ -440A^2B^4 - 103A^2B^3 - 6A^2B^2 - 693AB^2 - 183AB - 12A + 3, \end{array}$$

Proof. We describe Case 0, as the other cases are similar except that the analog of (15) is much more complicated. Analogously to (13), one needs to find z in the function field $\mathbb{Q}(x,y)$ of X_0 satisfying $S_0(u,v,z) = 0$. To find a candidate z, one takes a sufficiently large collection of $\{(x_i, y_i)\}$ of ordered pairs in $\mathbb{Q}^2$. One next obtains the pairs $(u_i, v_i) = \pi_0(x_i, y_i)$. Discarding the very rare cases where $S_0(u_i, v_i, z) \in \mathbb{Q}[z]$ has more than one rational root, one defines z_i to be the unique rational root of $S_0(u_i, v_i, z)$. The desired z is then obtained by interpolation, being

$$z = \frac{(3x-1)g_{6a}}{g_{6b}} = \frac{(3x-1)\left(9xy^2 + 18xy - 66x + y^2 - 18y + 6\right)}{225x^2 - 30xy - 30x - 2y^2 + 6y + 33}. \tag{15}$$

Correctness is confirmed by verifying that $S_0(u(x,y), v(x,y), z(x,y))$ indeed simplifies to zero in $\mathbb{Q}(x,y)$. □

Fully expanded out, $S_0(u,v,z)$, $S_1(p,q,z)$, and $S_2(a,b,z)$ respectively have 551, 7299, and 1053 terms. Thus given Shioda's master polynomial S, our S_i admit the relatively concise presentations given in (14) and Theorem 5.1. Without S, the new S_i are of comparable complexity to the previous F_i, in the sense of number of terms.

5.5 *L-Polynomials of Shioda Quartics and Their Reduction Modulo 2*

To illustrate the 2-division nature of the polynomials $S_0(u,v,z)$, $S_1(p,q,z)$, and $S_2(a,b,z)$, one could take any parameter pair for which the corresponding polynomial is separable. As in Sect. 4.3, we work with $(u,v) = (-4,-3)$.

The images of (u, v) in the lower planes are $(p, q) = \sigma_1(-4, -3) = (-12, -3/4)$ and $(a, b) = \sigma_2(-4, -3) = (192, 9)$. By plugging into the three parts of Theorem 5.1, and scaling by $r_i \mapsto r_i/9^i$ in the middle case, one gets indices

$$\begin{aligned} I_0(-4,-3) &= (1, \quad 0, \quad 12, \quad 0, \quad 0, \quad 0, \quad -16), \\ I_1(-12,-3/4) &= (0, -12, -84, -144, \quad 720, -1008, \quad 7872), \\ I_2(192,9) &= (1, \quad 10, -39, \quad -12, -306, \quad -450, -2157). \end{aligned}$$

Taking these vectors as $(r_1, r_3, r_4, r_5, r_6, r_7, r_9)$ and substituting into the right side of (11), one gets three quartic plane curves, to be denoted here simply Q_0, Q_1, and Q_2.

As in Sect. 4.3, each of the genus three curves Q_i has good L-polynomials

$$L_p(Q_i, x) = 1 + ax + bx + cx^3 + pbx^4 + p^2ax^5 + p^3x^6.$$

Using *Magma*'s `ZetaFunction` again, and taking the first two good primes in each case, one gets

$$\begin{aligned} L_5(Q_0, x) &= 1 + x + 3x^2 + x^3 + \cdots, \quad L_7(Q_0, x) = 1 - x + 4x^2 - 11x^3 + \cdots, \\ L_5(Q_1, x) &= 1 + x + 3x^2 + x^3 + \cdots, \quad L_7(Q_1, x) = 1 - x + 8x^2 - x^3 + \cdots, \\ L_5(Q_2, x) &= 1 + x + x^2 + 11x^3 + \cdots, \quad L_7(Q_2, x) = 1 - x + 8x^2 - x^3 + \cdots. \end{aligned}$$

One has coincidences $L_5(Q_0, x) = L_5(Q_1, x)$ and $L_7(Q_1, x) = L(Q_2, x)$, with the second polynomial being reducible: $(1 - x + 7x^2)(1 + x^2 + 49x^4)$. The generic behavior is that all three $L_p(Q_i, x)$ are different and their splitting fields are disjoint extensions of $\mathbb{Q}$, each with Galois group the wreath product $S_2 \wr S_3$ of order 48.

The behavior of the curves here differs sharply from the behavior of the curves in Sect. 4.3. To describe this difference, we will use the language of motives, referring to the unconditional theory of [1]. Note however, that the language of Jacobians would suffice for the current comparison. Similarly, one could use the alternative language of Artin representations for Sect. 6.3. But for uniformity, and certainly to include the general case as represented by Sect. 6.4, the language of motives is best.

The difference between they Y_i of Sect. 4.3 and the Q_i here goes as follows. The two curves Y_i from Sect. 4.3 give rise to a single rank six motive $M = H^1(Y_2, \mathbb{Q}) \subset H^1(Y_1, \mathbb{Q})$. Moreover the potential automorphism $(x, y) \mapsto (x, iy)$ causes the motivic Galois group of M to be the ten-dimensional conformal unitary group $CU_3.2$. In contrast, the motives $M_i = H^1(Q_i, \mathbb{Q})$ here are all different, as is clear from their different L-polynomials. Moreover, their motivic Galois groups are all as big as possible, the full 22-dimensional conformal symplectic group CSp_6.

While the different $L_p(Q_i, x) \in \mathbb{Z}[x]$ have very little to do with each other, their reductions to $\mathbb{F}_2[x]$ coincide, as illustrated with primes $5 \le p \le 97$:

Class(p)	$\lambda_{28}(p)$	$L_p(Q_i, x) \in \mathbb{F}_2[x]$	Primes p
$3B$	$3^9 1$	$(x+1)^2\left(x^2+x+1\right)^2$	89
$7AB$	7^4	$\left(x^3+x+1\right)\left(x^3+x^2+1\right)$	5, 13, 29, 53, 61, 73, 97
$8AB$	$8^3 21^2$	$(x+1)^6$	37, 41
$12AB$	$12^2 31$	$\left(x^2+x+1\right)^3$	17
$6b$	$6^4 31$	$(x+1)^2\left(x^2+x+1\right)^2$	11, 19
$8c$	$8^3 4$	$(x+1)^6$	43, 67, 79, 83
$12c, 12d$	$12^2 31$	$\left(x^2+x+1\right)^3$	7, 23, 31, 47, 59, 71

This table shows very clearly how $S_0(-4,-3,z)$ functions as a 2-division polynomial. All three S_i, arbitrarily specialized, similarly capture the mod 2 behavior of corresponding L-polynomials.

6 2-Division Polynomials of Dettweiler-Reiter G_2 Motives

This section explains how the cover $\pi_1 : X_1 \to U_{3,1,1}$ is related to rigidity in the algebraic group G_2 in two ways. The last section presents some sample analytic calculations with L-functions.

6.1 Rigidity in General

In the mid 1990s, Katz [10] developed a powerful theory of rigidity of tuples $(g_1, \ldots, g_z)$ satisfying $g_1 \cdots g_z = 1$ in ambient groups of the form $GL_n(E)$, with E being an algebraically closed field. There is presently developing a theory of rigidity of tuples in $G(E)$ for other ambient algebraic groups G; particularly relevant for us is [6], where G is either G_2 or SO_7. In general, if G is simple modulo its finite center we say that a tuple $(C_1, \ldots, C_z)$ is numerically rigid if

$$\sum_{i=1}^{z} \mathrm{cd}_G(C_i) = (z-2)\dim(G). \tag{16}$$

Here for C_i a conjugacy class containing an element g_i, the integer $\mathrm{cd}_G(C_i) = \mathrm{cd}_G(g_i)$ is the dimension of the centralizer of g_i in $G(E)$.

The Malle-Matzat case provides a convenient example in Katz's original context. As explained in [13, Sect. 8], after a quadratic base change the class triple $(4b, 2b, 12AB)$ becomes $(12A, 2A, 12B)$ in $\Gamma = SU_3(\mathbb{F}_3)$. Pushed forward to $SL_3(\overline{\mathbb{F}}_3)$, the classes $12A$ and $12B$ are regular and so have centralizer dimension $\mathrm{rank}(SL_3) = 2$. The class $2A$ is a reflection and has centralizer $GL_2(\overline{\mathbb{F}}_3)$ with dimension 4. The rigidity condition (16) becomes $2 + 4 + 2 = 1 \cdot 8$ and is thus satisfied.

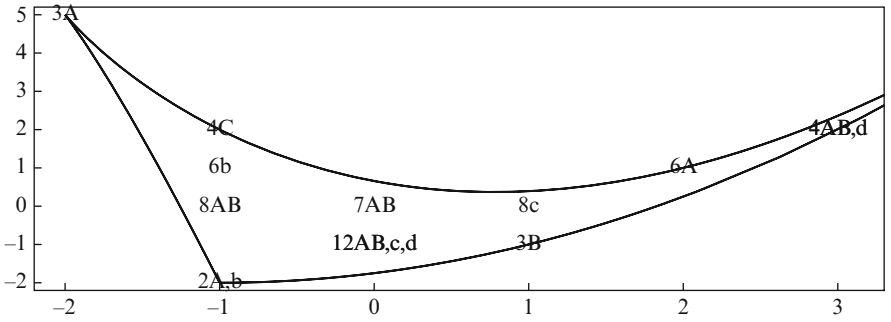


Fig. 3 The image of the class-set $G_2(2)^\natural$ inside the class space $G_2^{c\natural}$

6.2 *Groups $G_2(2)$ and G_2-Rigidity*

Our group $\Gamma.2 = G_2(2)$ embeds into the fourteen-dimensional compact Lie group G_2^c. Figure 3 illustrates the associated map $G_2(2)^\natural \to G_2^{c\natural}$ on the level of conjugacy classes, which is no longer injective. The fundamental characters χ and ϕ of G_2 have degrees 7 and 14 respectively, and the set $G_2^{c\natural}$ becomes the indicated triangular region in the χ-ϕ plane. The unique class in $G_2(2)^\natural$ which is outside the window is the identity class $1A$ at the point $(\chi, \phi) = (7, 14)$.

We have drawn Fig. 3 to facilitate the analysis of rigidity in $G_2(\mathbb{C})$. First consider classes which intersect the compact group G_2^c, and are thus represented by points in the closed triangular region drawn in the figure. If g represents one of the vertex classes labeled by $1A$, $3A$, and $2A, b$ respectively, its centralizer has type G_2, SL_3, and $SL_2 \times SL_2$, thus dimension 14, 8, and 6 respectively. For g representing a class otherwise on the boundary, the centralizer has type GL_2 and hence dimension 4. For g in the interior, the class is regular and so the centralizer dimension is $\text{rank}(G_2) = 2$. For general semisimple elements in $G_2(\mathbb{C})$ the situation is the same: centralizer dimensions are 14, 8, and 6 for the three special classes already considered, 4 for classes on the algebraic curve corresponding to the boundary, and 2 otherwise.

6.3 *G_2-Rigidity of $(3A, 3A, 3A, 4B)$*

The first-listed quadruple for π_1 in Proposition 3.1 is $(3A, 3A, 3A, 4B)$. Using the determinations associated to Fig. 3, the left side of (16) becomes $8+8+8+4 = 28$ which agrees with the right side $(4-2)14 = 28$. Thus $(3A, 3A, 3A, 4B)$ is G_2-rigid. We are not pursuing this connection here, but it seems possible to write down a corresponding rank seven differential equation with finite monodromy. From the algebraic solutions to this differential equation, one could perhaps construct the cover $X_1 \to U_{3,1,1}$ in a third way.

6.4 *Orthogonal Rigidity of a Lift of* (2A, 2A, 3A, 4A)

The last-listed quadruple for π_1 in Proposition 3.1 is $(2A, 2A, 3A, 4A)$. This tuple fails to be G_2-rigid, as now the left side of (16) is $6 + 6 + 8 + 3 = 24$ which is less than 28. However one does have rigidity of a lift as follows.

The following matrices were sent to me by Stefan Reiter in July 2013.

$$a = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ -3 & 1 & & 1 & & & & \\ 3 & -1 & & & 1 & & & \\ 9 & -3 & & & & 1 & & \\ -1 & & 3 & -1 & 2 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & & & & & & \\ & 1 & & & & & & \\ & & 1 & 1 & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & & & & 3 & -1 & \\ & 1 & & & 9 & -3 & \\ & & -2 & 1 & & & \\ & & -9 & 4 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & -3 & 1 & & & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & & & & & \\ & 1 & & & & & \\ & & 1 & 1 & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & -1 & & & & & -3 \\ 3 & -2 & & & & & \\ & & 1 & -1 & & & 3 \\ & & 3 & -2 & & & 6 \\ & & & & 1 & -1 & -3 \\ & & & & 3 & -2 & \\ & & & & & & 1 \end{pmatrix} \sim \begin{pmatrix} \omega & & & & & & \\ & \omega & & & & & \\ & & \omega & & & & \\ & & & \overline{\omega} & & & \\ & & & & \overline{\omega} & & \\ & & & & & \overline{\omega} & \\ & & & & & & 1 \end{pmatrix}$$

$$d = \begin{pmatrix} 10 & -5 & & & 9 & -5 & -6 \\ 15 & -8 & & & 18 & -9 & -9 \\ & & 1 & & & & \\ -3 & 4 & -3 & 1 & -6 & 3 & 3 \\ 9 & -5 & & & 10 & -5 & -6 \\ 18 & -9 & & & 15 & -8 & -9 \\ -2 & 1 & & & -2 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & & & & & \\ & 1 & 1 & & & & \\ & & 1 & & & & \\ & & & 1 & 1 & & \\ & & & & 1 & 1 & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

These matrices satisfy $abcd = 1$ and they generate a subgroup of $GL_7(\mathbb{C})$ with Zariski closure of the form $G_2(\mathbb{C})$. On the one hand, reduced to $GL_7(\mathbb{F}_2)$, these matrices generate a copy of $G_2(2)'$ with a, b, c, and d respectively in $2A$, $2A$, $3A$ and $4A$. On the other hand, considered in $GL_7(\mathbb{C})$, the matrices have Jordan canonical forms as listed on the right, with $\omega = \exp(2\pi i/3)$.

Consider $a, b, c, d \in G_2(\mathbb{C}) \subset SO_7(\mathbb{C}) \subset SL_7(\mathbb{C})$. Centralizer dimensions are calculated in [6, Sect. 3] and the numerics associated with (16) are as follows.

G	$\mathrm{cd}_G(a)$	$+$	$\mathrm{cd}_G(b)$	$+$	$\mathrm{cd}_G(c)$	$+$	$\mathrm{cd}_G(d)$				$2\dim(G)$
G_2	8	$+$	8	$+$	8	$+$	4	$=$	28	$=$	28
SO_7	13	$+$	13	$+$	9	$+$	7	$=$	42	$=$	42
SL_7	28	$+$	28	$+$	28	$+$	16	$=$	90	$<$	96

Thus the quadruple $([a], [b], [c], [d])$ is $G_2(\mathbb{C})$- and $SO_7(\mathbb{C})$-rigid. However it is not $SL_7(\mathbb{C})$-rigid, and so does not fit into Katz's original framework.

Dettweiler and Reiter classify tuples of classes in $G_2(\mathbb{C})$ which are $SO_7(\mathbb{C})$ rigid in [6]. Thus $([a], [b], [c], [d])$ is in their classification. In fact, it appears as the first line of the table in Sect. 5.4. Being $SO_7(\mathbb{C})$-rigid is a stronger condition than being $G_2(\mathbb{C})$-rigid. It implies from [6] that there is a corresponding rank seven motive over $\mathbb{Q}(p, q)$ with motivic Galois group G_2.

6.5 *Division Polynomials and L-Functions*

In Sects. 4.3 and 5.5 we have discussed L-polynomials $L_p(M, x)$ for certain motives $M = H^1(\text{curve}, \mathbb{Q})$. Putting these L-polynomials together, including also L-polynomials at bad primes, one gets a global L-function

$$L(M, s) = \prod_p L_p(M, p^{-s})^{-1}. \tag{17}$$

This L-function is expected to have standard analytic properties, including an analytic continuation and a functional equation with respect to $s \leftrightarrow 2 - s$. Normalizing the motives from Sects. 6.3 and 6.4 to have weight 0, one likewise expects good analytic properties of corresponding $L(M, s)$, involving now functional equations $s \leftrightarrow 1 - s$.

We do not know yet how to compute L-polynomials in the context of Sect. 6.4, where the motivic Galois group is generically the fourteen-dimensional algebraic group G_2. However the computation of L-polynomials is feasible in the setting of Sect. 6.3 where the motivic Galois group is just the finite group $G_2(2)$. In fact, as commented already in Sect. 5.5, we are using motivic language mainly because it is the natural general context for division polynomials. The particular motives from Sect. 6.3 correspond to finite-image Galois representations and so this language could be avoided.

In the setting of Sects. 4, 5, and 6.3, analytic computations with global L-functions (17) are possible on a numerical level. To illustrate this, we consider the motive M from Sect. 6.3 associated to the specialization point used in Sects. 4.3 and 5.5, namely $(u, v) = (-4, -3)$. This motive corresponds to the seven-dimensional irreducible representation of $G_2(2)$ into $SO(7)$. It is natural here to twist by the Dirichlet character χ given on odd primes p by $\chi(p) = (-1)^{(p-1)/2}$. The twisted motive M' corresponding to the other seven-dimensional irreducible representation of $G_2(2)$. At the level of good L-polynomials, passing back and forth between M and M' means replacing x by $\chi(p)x$.

Let $p \geq 5$ be a prime. The corresponding Frobenius class Fr_p can usually be deduced from Table 1 from the mod p factorization partition of $S_0(-4, -3, z)$ and the class of p modulo 4. To make the necessary distinction between $3A$ and $3B$, we use the factorization partition of the resolvent $f_{36}(4, x)$ presented in (19). The (χ, ϕ)-coordinates of Fr_p on Fig. 3 then yield the L-polynomial

$$L_p(M, x) = 1 - ax + bx^2 - cx^3 + cx^4 - bx^5 + ax^6 - x^7.$$

Here $a = \chi$, $b = \chi + \phi$, and $c = a + a^2 - b$.

The necessary 2-adic and 3-adic analysis for obtaining conductors and bad L-polynomials is begun in Proposition 8.2 below. For $L(M, s)$ the conductor is $2^{20}3^{12}$, the decomposition of the exponents as a sum of seven slopes being as follows.

$$\text{At 2: } 20 = 6 \cdot 3 + 2. \qquad \text{At 3: } 12 = 6 \cdot \frac{11}{6} + 1.$$

Since all slopes are positive, the bad L-polynomials are $L_2(M, x) = L_3(M, x) = 1$. For $L(M', s)$, the slopes are all the same except the 2-adic slope 2 is now 0, so that the conductor drops to $2^{18}3^{12}$. Slopes of 0 contribute to the degree of L-polynomials, and in this case $L_2(M', x) = 1 - x$ while still $L_3(M', x) = 1$.

In principle, *Magma*'s Artin representation and L-function packages [2], both due to Tim Dokchister, should do all the above automatically, given simply $S_0(-4, -3, z)$ as input. However the inertia groups at 2 and 3 are currently too large, and so *Magma* can only be used with the above extra information at the bad primes. It then outputs numerical values for arbitrary s, on the assumption that standard conjectures hold. Particularly interesting s include those of the form $\frac{1}{2} + it$ with t real, i.e. those on the critical line. Here one multiplies L by a phase factor depending analytically on t to obtain a new function L^* taking real values only. Figure 4 presents plots for our two cases, numerically identifying zeros on the critical line.

To obtain analogous plots of $L^*(M, \frac{w+1}{2} + it)$ for a general weight w motive, such as the weight one motives from Sects. 4.3 and 5.5, division polynomials do not at all suffice. Here one needs the much more complete information obtained from point counts, like the $L_p(M, x)$ presented in Sects. 4.3 and 5.5 for $p = 5$ and $p = 7$. However division polynomials can still be of assistance in obtaining the needed information at the bad primes.

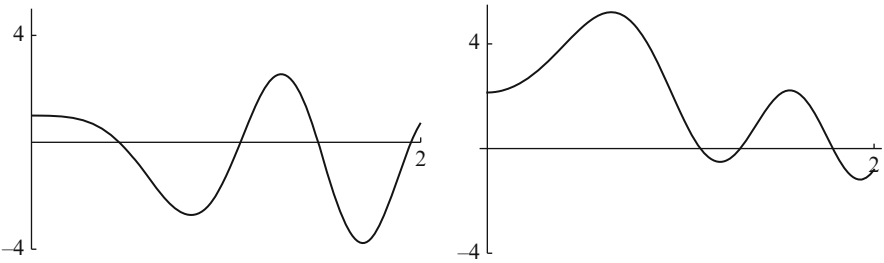


Fig. 4 Graphs of $L^*(M, \frac{1}{2} + it)$ (*left*) and $L^*(M', \frac{1}{2} + it)$ (*right*)

7 Specialization to Three-Point Covers

In Sect. 7.1 we find projective lines P in $\overline{U}_{3,1,1}$ and $\overline{U}_{3,2}$ suitably intersecting the discriminant locus in only three points. In Sect. 7.2 we consider the covers obtained by the preimages under π_1 and π_2 of these lines. We thereby construct some of the three-point covers $X_P \to P$ mentioned in Sect. 3.1. As stated previously, it would be hard to construct these covers directly because these X_P always have positive genus. In Sect. 7.3 we apply quadratic descent twice to a cover $X_P \to P$ coming from a curve $P \subset U_{3,1,1}$ and recover the Malle-Matzat cover (3).

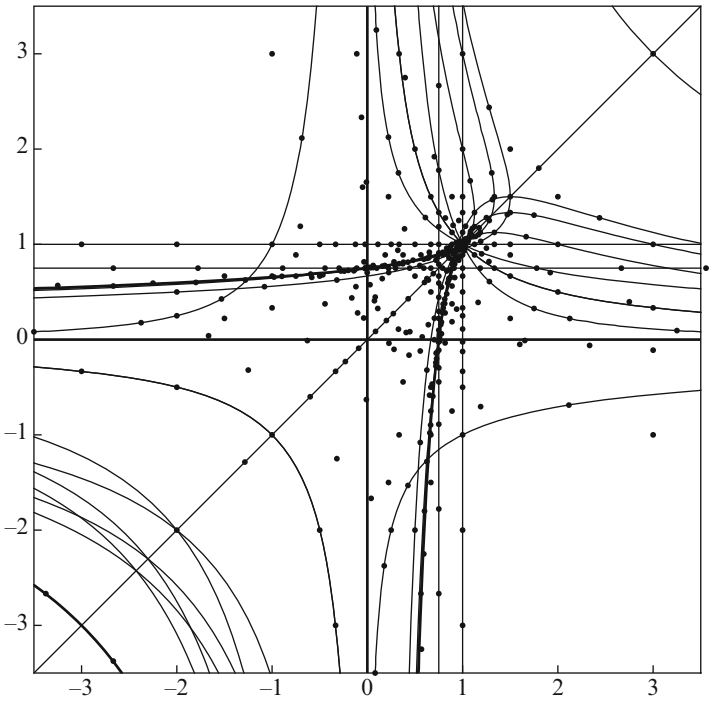
7.1 Curves in $\overline{U}_{3,1,1}$ and $\overline{U}_{3,2}$

The top half of Fig. 5 is a window on the real points of the naive completion $\overline{U}_{3,1,1} = \mathbb{P}^1_p \times \mathbb{P}^1_q$. The discriminant locus $Z_{3,1,1}$ consists of the two coordinate axes, the two lines at infinity, and the solution curve D_1 of

$$p^2q^2 - 6pq + 4p + 4q - 3 = 0.$$

The five lightly drawn straight lines intersect $Z_{3,1,1}$ in just three points, not counting multiplicities. The ten other lightly drawn curves have the same three-point property, although it is not visually evident. The points drawn in Fig. 5 will be discussed in the next section.

The bottom half of Fig. 5 names and parametrizes the 15 lightly drawn curves in the top half. Each name is a superscripted letter. The five bulleted curves are the straight lines. There are other natural coordinate systems on the p-q-plane, and each of the other curves appears as a line in at least one of these coordinate systems. We are emphasizing the coordinates p and q because they make the natural involution of $U_{3,1,1}$ completely evident as $p \leftrightarrow q$. The three curves labeled T^* are stable under this involution. The remaining 12 curves form six interchanged pairs: $T' \leftrightarrow T''$. Six of the 15 curves are images of lines in the cubic cover U. These source lines in U are indicated by a, b, c, d, e, and f.



		p	q
G'	•	t	1
H'	•	$8t/9$	$3/4$
I'		$(9t-5)/4$	$1/p^2$
J'		$(t+3)/4$	$(4p-3)/p^2$
K'	a	$(t+2)/3$	$(3p-2)/p^2$
L'	e	$3(t+4)/16$	$9(4p-3)/8p^2$
F^*	$\bullet f$	$3/(4t-1)$	$3/(4t-1)$
M^*		t	$1/t$
B^*	b	$-3t$	$-3/t$

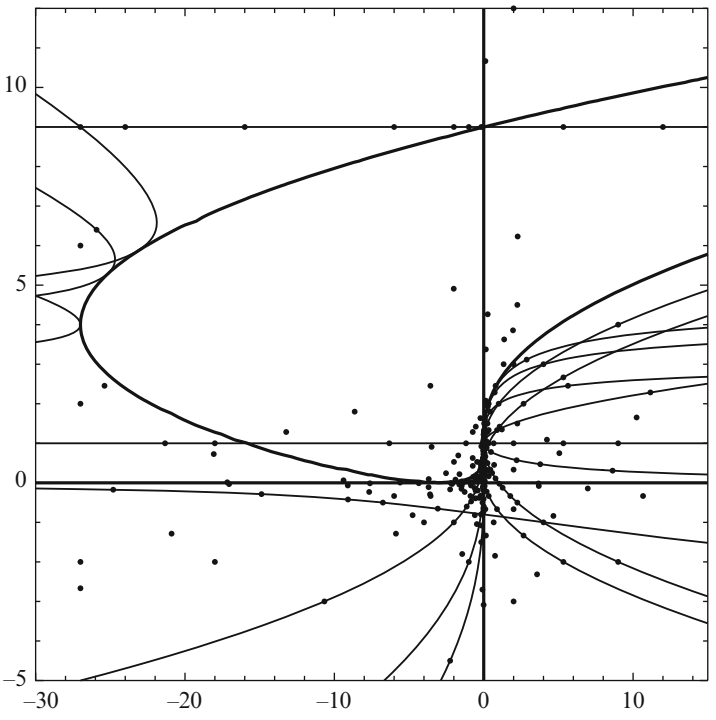
		p	q
G''	•	1	t
H''	•	$3/4$	$8t/9$
I''		$1/q^2$	$(9t-5)/4$
J''		$(4q-3)/q^2$	$(t+3)/4$
K''	c	$(3q-2)/q^2$	$(t+2)/3$
L''	d	$9(4q-3)/8q^2$	$3(t+4)/16$

Fig. 5 *Top*: the p-q plane $U_{3,1,1}(\mathbb{R})$. Discriminant loci (*thick*), bases of three-point covers (*thin*), and specialization points are drawn in. *Bottom*: parametrizations of the bases for three-point covers

Figure 6 is the analog of Fig. 5 for $\overline{U}_{3,2} = \mathbb{P}^2_{a,b}$ and we will describe it more briefly, focusing on differences. The discriminant locus $Z_{3,2}$ has four components, the two coordinate axes, the line at infinity, and the curve D_2 with equation

$$a^2 - 2ab^2 + 12ab + 6a + b^4 - 12b^3 + 30b^2 - 28b + 9 = 0.$$

The light curves each intersect the discriminant locus in three points, where this time a contact point with D_2 does not count if the local intersection number is even. Despite the relaxing of the three-point condition, we have found only 12 such curves. The five curves A, B, C, E, and F are images of generically bijective maps from curves a, b, c, e, and f in U. Curve d in U double covers B, and so does not



	a	b
A	$-27(b-1)^3/(5b-9)$	$9(t-1)/(5t-9)$
$B\bullet$	$-48(t-1)$	9
C	$-(b-9)(5b-9)/27$	$9(t-1)/(5t-1)$
E	$-(b-1)^3/(b-3)$	$3(t-1)/(t-3)$
F	$-3/\left(9t^2-7t+1\right)^2$	$\frac{9(t-1)t}{9t^2-7t+1}$
$M\bullet$	$-16t$	1

	a	b
G	$(b-1)^2$	t
H	$b(3b-2)/3$	$2t/3$
I	$(b-1)^2(5b+4)/b$	$4/(9t-5)$
J	$-(b-1)^2b/3(b-4)$	$4t/(t+3)$
K	$-(b-1)^3/(b-3)$	$3t/(t+2)$
L	$\frac{-b^2(10b-9)}{27(2b-9)}$	$9t/2(t+4)$

Fig. 6 *Top*: the *a*-*b* plane $U_{3,2}(\mathbb{R})$. Discriminant loci (*thick*), bases of three-point covers (*thin*), and specialization points are drawn in. *Bottom*: parametrizations of the bases for three-point covers

have its own entry on Fig. 6. For $T = G, H, I, J, K$, and L, the curve $T \subset U_{3,2}$ comes from T' and T'' in $U_{3,1,1}$ via (5). Finally $M \subset U_{3,2}$ is double-covered by M^* in $U_{3,1,1}$.

7.2 Three-Point Covers with Galois Group $\Gamma.2$

The previous section concerned the base varieties $U_{3,1,1}$ and $U_{3,2}$ only. For quite general covers $X \to U_\nu$, one gets three-point covers $X_P \to P$ by specialization to the $P \subset X_\nu$ listed there. We now apply this theory to our particular covers $\pi_1 : X_1 \to U_{3,1,1}$ and $\pi_2 : X_2 \to U_{3,2}$. Because of the explicit parametrizations in Figs. 5 and 6, our bases are now coordinatized projective lines $\mathbb{P}^1 = \mathbb{P}^1_t$.

Table 2 Sixteen three-point covers obtained from π_1 and π_2 by specialization

X_0	X_{311}	X_{32}	C_0	C_1	C_∞	g_{28}	g_{36}	$\bar{\mu}$	μ
	H''		$4A$	$4B$	$3B$	−−	−−	$0.\overline{3}$	0
	I''		$4A$	$12A$	$2A$	−−	−−	$0.\overline{3}$	0
b	B^*	B	$6A$	$2A$	$8A$	1	0	1	1
		M	$12A$	$2A$	$8B$	2	2	1	1
		G	$4A$	$6A$	$3B$	2	2	1	1
	H', G''		$12A$	$4A$	$3B$	2	5	1	1
e	L'	E, K	$4C$	$4A$	$8A$	3	3	1	1
	G'	H	$3A$	$12A$	$3B$	3	5	1	1
a	K'	A	$4A$	$8A$	$8B$	4	7	1	1
c	K''	C, I	$3A$	$8A$	$6A$	4	6	1	1
d	L''		$6A$	$4A$	$6A$	4	5	1	1
f	F^*, I'	F	$4A$	$8B$	$12B$	5	8	1	1
	J'		$4A$	$12A$	$8B$	5	8	1	1
		L	$12A$	$3A$	$8A$	5	8	1	1
	M^*	J	$6A$	$12A$	$8B$	7	10	5	5
	J''		$12A$	$12A$	$6A$	8	11	$4.08\overline{3}$	3

Table 2 gives the results. The first two lines illustrate the general phenomenon where Galois groups sometimes become smaller under specialization. Here the covers have Galois groups of order 216 and 432 respectively, thus of index 56 and 28 in $\Gamma.2$. The covers $X_{28} \to \mathbb{P}^1$ each split into a genus one cover $X_{27} \to \mathbb{P}^1$ and the trivial cover $\mathbb{P}^1 \to \mathbb{P}^1$.

The next fourteen lines each give a cover $X_{28} \to \mathbb{P}^1$ with Galois group all of $\Gamma.2$. They are sorted by the genus g_{28} of this cover. In most cases, more than one base curve $\mathbb{P}^1$ yield isomorphic covers, after suitable permutations of the three cusps $\{0, 1, \infty\}$. The local monodromy classes in Γ always correspond to the first-listed parametrized base. These classes are unambiguously determined, except for a simultaneous interchange $4A \leftrightarrow 4B$, $8A \leftrightarrow 8B$, $12A \leftrightarrow 12B$, coming from the outer automorphism of Γ. We always normalize by making the first-listed interchanged class have an A in its name.

Thus for example, specializing $S_1(p, q, x)$ at $(p, q) = (-3t, -3/t)$ from the B^* line of Fig. 5, one gets a polynomial in $\mathbb{Z}[t, x]$ with 554 terms. The local monodromy partitions are $(6A, 2A, 8A)$ as printed. Alternatively, specializing $S_2(a, b, x)$ at $(a, b) = (-48(t-1), 9)$ from the B line of Fig. 6, one gets a polynomial in $\mathbb{Z}[t, x]$ now with 252 terms. The monodromy partitions are the same, except for the reordering $(C_0, C_1, C_\infty) = (2A, 6A, 8A)$.

Having specialized from two parameters down to one, it is now much more reasonable to print polynomials giving equations $f_{28}(t,x) = 0$ and $f_{36}(t,x) = 0$ corresponding to the covers in any of the last fourteen lines of Table 2. We do this only in the case where genera are the smallest, namely the third line:

$$\begin{aligned} f_{28}(t,x) = \\ &-t\left(3x^4 - 252x^3 + 222x^2 - 692x - 5\right) \cdot \\ &\quad \left(81x^{12} + 2106x^{11} + 26001x^{10} + 73332x^9 + 268515x^8 + 574938x^7\right. \\ &\quad \left. +618759x^6 + 400896x^5 + 184140x^4 + 52752x^3 + 8952x^2 + 576x - 32\right)^2 \\ &+2^{10}(1-t)(4x+1)\left(9x^4 + 18x^3 + 48x^2 + 18x + 1\right)^6 \\ &+3^9(1-t)t(x-2)^8x^2\left(x^2+8\right)\left(x^2 - 2x - 1\right)^8, \end{aligned} \tag{18}$$

$$\begin{aligned} f_{36}(t,x) = \\ &\left(4x^4 - 3\right)^3\left(4x^4 - 12x^2 + 12x - 3\right)^6 \\ &-3^9t(x-1)^4\left(2x^2-1\right)^8\left(2x^2 - 2x + 1\right)^4. \end{aligned} \tag{19}$$

Here the genera, namely $(g_{28}, g_{36}) = (1,0)$, are the reverse of those of the Malle-Matzat covers.

7.3 Recovering the Malle-Matzat Cover

The Malle-Matzat cover can be constructed from the last line of Table 2 via two quadratic descents as follows. The given cover $X_1 \to \mathbb{P}^1_t$ has ramification invariants $(12A, 12A, 6A)$. Quotienting out by the involution $t \leftrightarrow 1-t$ on the base and its unique lift to X_1, one gets the descended cover $X_2 \to \mathbb{P}^1_s$, with $s = 4t(1-t)$. The ramification invariants of this cover are $(12A, 2A, 12B)$. Quotienting now by $s \leftrightarrow 1/s$ on the base and its unique lift to X_2, one gets the twice descended cover $X_3 \to \mathbb{P}^1_u$, with $u = -(s-1)^2/4s$. The ramification invariants of this cover are $(4b, 2b, 12AB)$, showing that it is the Malle-Matzat cover.

In other words,

$$m\left(\frac{(2t-1)^4}{16(t-1)t}, x\right) \quad \text{and} \quad S_1\left(\frac{16t}{(t+3)^2}, \frac{t+3}{4}, z\right)$$

are two different polynomials defining the same degree 28 extension of $\mathbb{Q}(t)$. The left one is a quartic base-change of the Malle-Matzat polynomial $m(u,x)$ while the right is a specialization of $S_1(p,q,z)$.

8 Specialization to Number Fields

In this final section, we discuss specialization to number fields with discriminant of the form 2^j3^k. Section 8.1 discusses fields obtained by specializing the π_i. Section 8.2 continues this discussion, involving also similar fields from other sources. Section 8.3 discusses analysis of ramification in general, with a field having Galois group $PGL_2(7)$ serving as an example. Section 8.4 concludes by analyzing the ramification of a particularly interesting field with Galois group $SU_3(3).2 \cong G_2(2)$.

8.1 Specializing the Covers π_i

In this section, we restrict attention to number fields with Galois group $\Gamma.2$ and discriminant of the form 2^j3^k. Consider first the cover $X_0 \to U$. We have found 216 ordered pairs (u, v) such that the corresponding number field $\mathbb{Q}[x]/F_0(u, v, x)$ has Galois group $\Gamma.2$ and discriminant of the form 2^j3^k. Different specialization points can give isomorphic fields, and we found 147 number fields in this process.

Next consider the covers $\pi_1 : X_1 \to U_{3,1,1}$ and $\pi_2 : X_2 \to U_{3,2}$. Beyond images of specialization points in $U(\mathbb{Q})$, we found 248 pairs (p, q) and 177 pairs (a, b) giving fields with Galois group $\Gamma.2$ and discriminant of the form 2^j3^k. We obtained 62 new fields arising from both covers, 95 new fields arising from π_1 only, and 72 new fields arising from π_2 only. Thus we found in total 376 fields with Galois group $\Gamma.2$ and discriminant of the form 2^j3^k.

Figure 7 indicates the pairs (j, k) arising from field discriminants 2^j3^k of one of these 376 fields. The area of the disk at (j, k) is proportional to the number of fields giving rise to (j, k). In 36 cases, this field is unique. The largest multiplicity is 19,

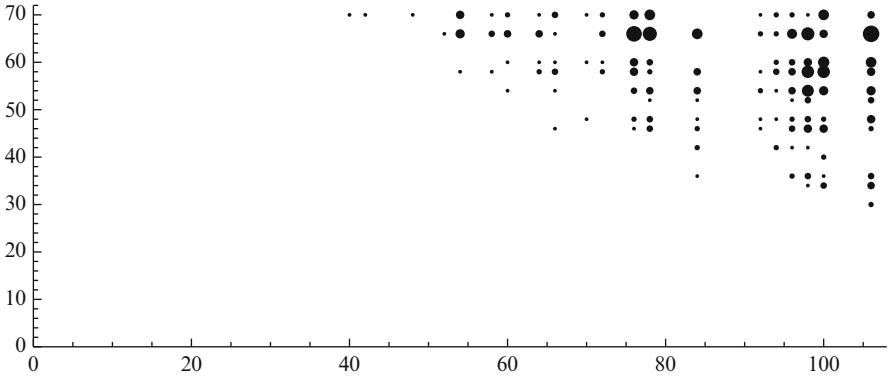


Fig. 7 Pairs (j, k) arising from field discriminants 2^j3^k from specializations of $F_1(p, q, x)$ and $F_2(a, b, x)$

arising from $(j,k) = (106,66)$. The smallest discriminant is $2^{66}3^{46}$, coming from just one field. This field arises from eight sources,

$$\begin{aligned}(u,v) &= (-4,-3), \left(-\frac{1}{2},1\right), \left(\frac{1}{2},3\right), (4,-3), (-32,1), \left(-\frac{32}{81},\frac{49}{81}\right),\\ (p,q) &= \left(1,\frac{1}{2}\right),\\ (a,b) &= \left(-\frac{27}{4},-\frac{1}{2}\right).\end{aligned} \tag{20}$$

The largest discriminant $2^{106}3^{70}$ arises from four fields.

The phenomenon of several specialization points giving rise to a single field is quite common in our collection of covers π_i. The octet in (20) is the most extreme instance, but there are many other multiplets as altogether $216 + 248 + 177 = 641$ different specialization points give rise to only 376 fields. This repetition phenomenon is discussed for a different cover in [13, Sect. 6], where it is explained by a Hecke operator. It would be of interest to give a similar automorphic explanation of the very large drop $641 \to 376$. Ideally, such a description would follow through on one of the main points of view of Deligne and Mostow [4, 5], by describing all our surfaces via uniformization by the unit ball in $\mathbb{C}^2$.

8.2 *Summary of Known Fields*

We specialized the Malle-Matzat cover in [13, Sect. 8] to obtain fields with discriminant of the form 2^j3^k. From $t = 1/2$ we obtained a field with Galois group Γ, while from 41 other t we obtained 41 other fields with Galois group $\Gamma.2$. While in our covers π_i the .2 always corresponds to the quadratic field $\mathbb{Q}(i)$, in the Malle-Matzat cover general $\mathbb{Q}(\sqrt{\partial})$ arise.

Sorting all the known fields by $\partial \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, including two additional fields from [14] with $\partial = 2$ and $\partial = 6$, one has the following result.

Proposition 8.1. *There are at least* 409 *degree 28 fields with Galois group Γ or $\Gamma.2$ and discriminant of the form 2^j3^k. Sorted by the associated quadratic algebra $\mathbb{Q}[x]/(x^2-\partial)$, these lower bounds are*

∂	-6	-3	-2	-1	1	2	3	6
#	5	6	6	381	1	7	2	1.

Two aspects of our incomplete numerics are striking. First, it is somewhat surprising that there are at least 408 number fields with Galois group $\Gamma.2$ and discriminant 2^j3^k. By way of contrast, the number of fields with Galois group S_7, S_8, and S_9 and discriminant $\pm 2^j3^k$ is exactly 10, at least 72, and at least 46 respectively [9]. Second, the imbalance with respect to ∂ is quite extreme. We have not been exhaustive in

specializing our covers and we expect that the 381 could be increased somewhat. By exhaustively specializing Shioda's $W(E_7)^+$ family, in principle one could obtain the correct values on the bottom row. Our expectation however is that most fields have already been found and so the imbalance favoring $\mathbb{Q}(i)$ is maintained in the complete numerics.

8.3 *Analysis of Ramification*

In general, let K be a degree n number field with discriminant d and root discriminant $\delta = |d|^{1/n}$. It is important to simultaneously consider the Galois closure K^{gal}, its discriminant D and its root discriminant $\Delta = |D|^{1/N}$. For a given field K, one has $\delta \leq \Delta$. To emphasize the fact that the large field K^{gal} is never directly seen in computations, we call Δ the Galois root discriminant or GRD of K. A GRD Δ is typically much harder to compute than the corresponding root discriminant δ, as it requires good knowledge of higher inertia groups at each ramifying prime.

For sufficiently simple K, ramification is thoroughly analyzed by the website associated to [7], and the GRD Δ is automatically computed. The 409 fields K contributing to Proposition 8.1 are not in the simple range, and we will present one *ad hoc* computation of a GRD Δ in the next section. As an illustration of the general method, we first consider an easier case here.

For the easier case, take $t = -1$ in (18), which corresponds to $(p, q) = (3, 3)$ via B^* and $(a, b) = (-48, 9)$ via B, both of which come from $(u, v) = (1, 2)$. The discriminant and root discriminant of $K = \mathbb{Q}[x]/f_{28}(-1, x)$ are $d = 2^{92}3^{24}$ and $\delta \approx 25.007$ respectively. This root discriminant is much smaller than the minimum $(2^{66}3^{46})^{1/28} \approx 31.147$ appearing in Sect. 8.1. The field K was excluded from consideration in Sect. 8.1 because the Galois group is not $\Gamma.2$ but rather the 336-element subgroup $PGL_2(7)$. This drop in Galois group is confirmed by the factorization of the resolvent into irreducibles: $f_{36}(-1, x) = xf_{14}(x)f_{21}(x)$.

The group $PGL_2(7)$ can be embedded in S_8, which means that K^{gal} can also be given as the splitting field of a degree eight polynomial. Such a degree eight polynomial was already found in [8, Table 8.2]:

$$f(x) = x^8 - 6x^4 - 48x^3 - 72x^2 - 48x - 9.$$

The analysis of ramification is then done automatically by the website associated to [7], returning for each prime p a slope content symbol SC_p of the form $[s_1, \ldots, s_k]_t^u$. This means that the decomposition group D_p has order $p^k tu$, the inertia subgroup I_p has order $p^k t$, and the wild inertia subgroup P_p has order p^k. The wild slopes s_i are then rational numbers greater than one measuring wildness of ramification, as explained in [7, Sect. 3.4].

In our $PGL_2(7)$ example, also taking weighted averages to get Galois mean slope [7, Sect. 3.7], the result is

$$SC_2 = [2, 3, 7/2, 9/2]_1^1, \qquad GMS_2 = \frac{1}{16} \cdot 2 + \frac{1}{8} \cdot 3 + \frac{1}{4} \cdot \frac{7}{2} + \frac{1}{2} \cdot \frac{9}{2} = \frac{29}{8},$$
$$SC_3 = [\,]_7^6, \qquad GMS_3 = \frac{6}{7}.$$

The Galois root discriminant is then $\Delta = 2^{29/8}3^{6/7} \approx 31.637$. This Galois root discriminant is the fifth smallest currently on [9] from a field with Galois group $PGL_2(7)$.

8.4 A Lightly Ramified Number Field

Let K be the number field coming from the eight specialization points (20). Applying *Pari*'s `polredabs` [17] to get a canonical polynomial, this field is $K = \mathbb{Q}[x]/f(x)$ with

$$\begin{aligned} f(x) = {} & \\ & x^{28} - 4x^{27} + 18x^{26} - 60x^{25} + 165x^{24} - 420x^{23} + 798x^{22} - 1440x^{21} \\ & +2040x^{20} - 2292x^{19} + 2478x^{18} - 756x^{17} - 657x^{16} + 1464x^{15} - 4920x^{14} \\ & +3072x^{13} - 1068x^{12} + 3768x^{11} + 1752x^{10} - 4680x^9 - 1116x^8 + 672x^7 \\ & +1800x^6 - 240x^5 - 216x^4 - 192x^3 + 24x^2 + 32x + 4. \end{aligned}$$

The field K arises from (18) with either $t = 4$ or $t = 32/81$, so we also have its resolvent $K_{36} = \mathbb{Q}[x]/f_{36}(4, x)$ from (19). Since one of the eight specialization points in (20) is $(u, v) = (-4, -3)$, we have also seen this field already in the three sections about L-polynomials, Sects. 4.3, 5.5, and 6.5. ÿ Let K^{gal} be the splitting field of K. Calculation of slope contents is not automatically done by the website of [7] because degrees are too large. The proof of the following proposition illustrates the types of considerations which are built into [7] for smaller degrees.

Proposition 8.2. *The decomposition groups of K^{gal} at the ramified primes have invariants as follows:*

$$SC_2 = [2, 2, 2, 3, 3]_1^3, \qquad GMS_2 = \frac{7}{32} \cdot 2 + \frac{3}{4} \cdot 3 = \frac{43}{16},$$
$$SC_3 = [13/8, 13/8, 11/6]_8^2, \qquad GMS_3 = \frac{1}{27} \cdot \frac{7}{8} + \frac{8}{27} \cdot \frac{13}{8} + \frac{2}{3} \cdot \frac{11}{6} = \frac{125}{72}.$$

Thus the root discriminant of K^{gal} is $\Delta = 2^{43/16}3^{125/72} \approx 43.386$.

Proof. The computation is easier at the prime $p = 3$ and so we do it first. The field K factors 3-adically as $K_{27} \times \mathbb{Q}_3$ with K_{27} having discriminant 3^{46}. The exponent

arises from three slopes $s_1 \le s_2 \le s_3$ via $46 = 2s_1 + 6s_2 + 18s_3$. One of the two degree 63 resolvents, computed by *Magma*, factors 3-adically as $K_{54} \times K_9$, with $K_9 \cong \mathbb{Q}_3[x]/(x^9 + 6x^5 + 6)$ having slope content $[13/8, 13/8]_8^2$. This forces the remaining slope of K_{27} to be $s_3 = 11/6$. The inertia group D_3 is thus the maximal subgroup $3_+^{1+2} : 8 : 2$ of $\Gamma.2$, with slope content $[13/8, 13/8, 11/6]_8^2$.

Moving on to the prime 2, the field K factors 2-adically as $K_{16} \times K_{12}$. Here K_{16} is totally ramified of discriminant 2^{42}. The complement K_{12} contains the unramified cubic extension of $\mathbb{Q}_2$ and has discriminant 2^{24}. Since the group $S_{16} \times (S_4 \wr C_3)$ does not contain an element of cycle structure either $8^3 21$ or $8^3 4$, the decomposition group D_2 cannot contain an element of order eight. Thus D_2 cannot contain a Sylow 2-subgroup of $\Gamma.2$. So even though $\mathrm{ord}_2(|\Gamma.2|) = 6$, there can be at most five wild slopes.

The resolvent K_{36} factors as $K_{16} \times K_{12} \times K_8$, with $K_8 \cong \mathbb{Q}_2[x]/(x^8 + 2x^7 + 2)$ having discriminant 2^{14} and slope content $[2, 2, 2]_1^3$. Thus we have found three slopes to be 2, 2, and 2. If we can find two more wild slopes we will have identified all wild slopes.

The field K_8 and the sextic field $K_6 = \mathbb{Q}_2[x]/(x^6 + x^2 + 1)$ with discriminant 2^6 have the same splitting field. The latter is a subfield of K_{12} showing that $(24-6)/6 = 3$ is a fourth 2-adic slope. In fact, since both involutions in $\Gamma.2$ have cycle type $2^{12}1^4$ and therefore must appear in the degree 12 factor, 3 is the largest wild slope.

The quartic subfield of K_8 is $K_4 = \mathbb{Q}_2[x]/(x^4 + 2x^3 + 2x^2 + 2)$ with discriminant 2^6. Computation shows it is a subfield of K_{16}. So the remaining slope s satisfies $1 \cdot 2 + 2 \cdot 2 + 4 \cdot s + 8 \cdot 3 = 42$ and must also be 3. The tame degree I_2/P_2 can only be 1, as the only other possibility $t = 3$ would force $u = 2$ and $\Gamma.2$ does not contain a solvable subgroup of order a multiple of $2^6 3^2 = 576$. Thus D_2 has order 96 and slope content $[2, 2, 2, 3, 3]_1^3$. □

The Galois root discriminant $\Delta \approx 43.386$ is very low, as is clear from the discussion in [8], as updated in [9, Table 9.1]. In fact, the field K^{gal} is a current record-holder, in the sense that all known Galois fields with smaller root discriminants involve only simple groups of size smaller than 6048 in their Galois groups.

Acknowledgements It is a pleasure to thank Zhiwei Yun for a conversation about G_2-rigidity from which this paper grew. It is equally a pleasure to thank Michael Dettweiler and Stefan Reiter for helping to make the direct connections to their work [6]. We are also grateful to the Simons Foundation for research support through grant #209472.

References

1. Y. André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, Panoramas et Synthèses, vol. 17 (Société Mathématique de France, Paris, 2004), xii+261 pp.
2. W. Bosma, J.J. Cannon, C. Fieker, A. Steel (eds.), *Handbook of Magma Functions*, Edition 2.19 (2012). http://magma.maths.usyd.edu.au/magma/handbook/

3. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *Atlas of Finite Groups*. (Oxford University Press, Oxford, 1985)
4. P. Deligne, G.D. Mostow, *Monodromy of Hypergeometric Functions and Nonlattice Integral Monodromy*. Publications Mathématiques de l'IHÉS, No. 63 (1986), pp. 5–89.
5. P. Deligne, G.D. Mostow, *Commensurabilities Among Lattices in PU*$(1, n)$. Annals of Mathematics Studies, vol. 132 (Princeton University Press, Princeton, 1993), viii+183 pp.
6. M. Dettweiler, S. Reiter, The classification of orthogonally rigid G_2-local systems and related differential operators. Trans. Am. Math. Soc. **366**(11), 5821–5851 (2014)
7. J.W. Jones, D.P. Roberts, A database of local fields. J. Symb. Comput. **41**(1), 80–97 (2006). Database at http://math.la.asu.edu/~jj/localfields/
8. J.W. Jones, D.P. Roberts, Galois number fields with small root discriminant. J. Number Theory **122**(2), 379–407 (2007)
9. J.W. Jones, D.P. Roberts, A database of number fields. Lond. Math. Soc. J. Comput. Math. **17**(1), 595–618 (2014). Database at http://hobbes.la.asu.edu/NFDB/
10. N.M. Katz, *Rigid Local Systems*. Annals of Mathematics Study, vol. 138 (Princeton University Press, Princeton, 1996)
11. G. Kemper, Generic polynomials are descent-generic. Manuscripta Math. **105**(1), 139–141 (2001)
12. G. Malle, B.H. Matzat, *Inverse Galois Theory* (Springer, New York, 1999)
13. D.P. Roberts, An *ABC* construction of number fields, in *Number Theory*. CRM Proceedings Lecture Notes, vol. 36 (American Mathematical Society, Providence, 2004), pp. 237–267
14. D.P. Roberts, *Covers of $M_{0,5}$ and number fields* (in preparation)
15. T. Shioda, *Theory of Mordell-Weil Lattices*. Proceedings of the International Congress of Mathematicians, vols. I, II (Kyoto, 1990) (Mathematical Society of Japan, Tokyo, 1991) pp. 473–489
16. T. Shioda, Plane quartics and Mordell-Weil lattices of type E_7. Comment. Math. Univ. St. Paul. **42**(1), 61–79 (1993)
17. The PARI group, Bordeaux. *PARI/GP*. Version 2.3.4 (2009)
18. H. Weber, Lehrbuch der Algebra III, 3rd edn. (Chelsea, New York, 1961)
19. Wolfram Research, Inc., *Mathematica*, Version 10.0 Champaign (2014)

A Variant of Weyl's Inequality for Systems of Forms and Applications

Damaris Schindler

Abstract We give a variant of Weyl's inequality for systems of forms together with applications. First we use this to give a different formulation of a theorem of B.J. Birch on forms in many variables. More precisely, we show that the dimension of the locus V^* introduced in this work can be replaced by the maximal dimension of the singular loci of forms in the linear system of the given forms. In some cases this improves on the aforementioned theorem of Birch.

Second, we improve on a theorem of W.M. Schmidt which states that the number of integer points inside a given box, that lie on the variety given by a system of homogeneous forms of the same degree, satisfies the asymptotic behaviour as predicted by the classical circle method, as soon as the so called h-invariant of the system is sufficiently large. In this direction we generalise previous improvements of R. Dietmann on systems of quadratic and cubic forms to systems of forms of general degree.

1 Introduction

We consider a system of homogeneous forms $f_i(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ of degree d. For convenience we write $\mathbf{x} = (x_1, \dots, x_n)$ and ask for the number of integer solutions to the system of Diophantine equations given by

$$f_i(\mathbf{x}) = 0, \quad 1 \leq i \leq r.$$

More precisely, we fix a box $\mathscr{B} \subset \mathbb{R}^n$ which is contained in the unit box centred at the origin and we let $P \geq 1$ be some real parameter. Then we define the counting function

$$N(P) = \sharp\{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \in P\mathscr{B},\ f_i(\mathbf{x}) = 0,\ 1 \leq i \leq r\}.$$

D. Schindler (✉)
Hausdorff Center for Mathematics, Endenicher Allee 62–64, 53115 Bonn, Germany
e-mail: damaris.schindler@hcm.uni-bonn.de

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_9

This counting function has received a lot of attention (see for example [2, 10]), and is a central object of investigation in number theory. If the number of variables n is relatively large compared to the number of equations and the degree d, then the Hardy-Littlewood circle method has proved to be a valuable tool in obtaining asymptotic formulas for the counting function $N(P)$.

A very general result in this direction has been obtained by Birch in [2]. He introduces a locus called V^* which is the affine variety given by

$$\operatorname{rank}\left(\frac{\partial f_i(\mathbf{x})}{\partial x_j}\right)_{\substack{1\le i\le r\\ 1\le j\le n}} < r.$$

In his work [2] Birch provides an asymptotic formula for $N(P)$ as soon as

$$n - \dim V^* > r(r+1)(d-1)2^{d-1}.$$

A main ingredient in most applications of the circle method, as for example that in [2], is a form of Weyl's inequality. In this paper we present a variant of Weyl's inequality for systems of forms, and give two applications of our new form of Weyl's inequality.

First this allows us to replace the dimension of the locus V^* in Birch's theorem on system of forms by a quantity which appears to be more natural in this context, and bounds the previously used quantity from below. For an integer vector $\mathbf{b} \in \mathbb{Z}^r$ we let $f_{\mathbf{b}} = b_1 f_1 + \ldots + b_r f_r$ be the form in the pencil of $f_1, \ldots, f_r$ associated to $\mathbf{b}$. For any homogeneous form g we write $\operatorname{Sing}(g)$ for the singular locus (in affine space) of the form $g = 0$. We can now state a variant of Birch's theorem on forms in many variables as follows.

Theorem 1. *Assume that*

$$n - \max_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} (\dim \operatorname{Sing}(f_{\mathbf{b}})) > r(r+1)(d-1)2^{d-1}.$$

Then we have the asymptotic formula

$$N(P) = \mathfrak{S}\mathscr{J}P^{n-rd} + O(P^{n-rd-\delta}), \tag{1}$$

for some $\delta > 0$. Here $\mathfrak{S}$ and $\mathscr{J}$ are the singular series and singular integral.

This is essentially the main theorem of Birch's work [2] where the quantity $\dim V^*$ is replace by $\max_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}}(\dim \operatorname{Sing}(f_{\mathbf{b}}))$. In other words we can now describe the singularity of the system of forms f_i, $1 \le i \le r$ by the maximal dimension of the singular loci of forms in the pencil. To our knowledge, it is hard to find a satisfactory geometric interpretation for the locus V^* (see for example work of Aleksandrov and Moroz [1] into this direction).

Furthermore, we point out that for any non-trivial form $f_{\mathbf{b}}$ in the pencil, the dimension of the singular locus $\dim \mathrm{Sing}(f_{\mathbf{b}})$ is always bounded by $\dim V^*$. Indeed, the singular locus of the form $f_{\mathbf{b}}$ is given by

$$b_1 \frac{\partial f_1}{\partial x_i}(\mathbf{x}) + \ldots + b_r \frac{\partial f_r}{\partial x_i}(\mathbf{x}) = 0, \quad 1 \le i \le n.$$

If some vector $\mathbf{x}$ is contained in $\mathrm{Sing}(f_{\mathbf{b}})$, then these relations imply that the rank of the matrix $(\frac{\partial f_i}{\partial x_j})$ can be at most r. This shows that $\mathrm{Sing}(f_{\mathbf{b}}) \subset V^*$, and $\dim \mathrm{Sing}(f_{\mathbf{b}}) \le \dim V^*$ for any non-zero vector $\mathbf{b}$.

Hence Theorem 1 formally implies Birch's theorem in [2]. Furthermore, there are examples of systems where Theorem 1 is stronger than Birch's main theorem in [2]. For simplicity of notation let

$$u = u(\mathbf{f}) := \max_{\mathbf{b} \in \mathbb{Z}^r \setminus \{\mathbf{0}\}} (\dim \mathrm{Sing}(f_{\mathbf{b}})).$$

Let $k \ge r - 1$ be some integer and consider the system of quadratic forms

$$Q_i(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{k} x_j y_{ji}, \quad 1 \le i \le r,$$

in the $k(r+1)$ variables x_j for $1 \le j \le k$ and y_{ji} for $1 \le i \le r$ and $1 \le j \le k$. A short computation reveals that

$$\dim V^* = k(r-1) + r - 1 = u + r - 1.$$

Note also that once we choose k sufficiently large, Theorem 1 is indeed applicable. On the other hand these examples are essentially sharp. If we work over the complex numbers then we have

$$V^* = \cup_{\mathbf{b} \in \mathbb{C}^r \setminus \{\mathbf{0}\}} \mathrm{Sing}(f_{\mathbf{b}}),$$

and this leads to the bound $\dim V^* \le u_{\mathbb{C}} + r - 1$, where

$$u_{\mathbb{C}} := \max_{\mathbf{b} \in \mathbb{C}^r \setminus \{\mathbf{0}\}} (\dim \mathrm{Sing}(f_{\mathbf{b}})).$$

Since being published in 1962, Birch's work [2] has received a lot of attention and has been generalised in multiple directions. It seems natural to expect that our observation and new formulation of the main result in Theorem 1 can in an analogous way be transferred to most of these generalisations and developments. Some examples to mention are work of Brandes [3] on forms representing forms and the vanishing of forms on linear subspaces. Furthermore, the analogue of the locus V^* in work of Skinner [11], which generalises Birch's theorem on forms in many

variables to the number field situation, and work of the author [7] on bihomogeneous forms, could very likely be replaced by a non-singularity condition on forms of the linear system. Another result and application in this direction is a paper of Lee [6] on a generalisation to function fields $\mathbb{F}_q[t]$.

As a second application of our new form of Weyl's inequality for systems of forms, we can strengthen a theorem of Schmidt [10], which provides an asymptotic formula for the counting function $N(P)$ as soon as a so-called h-invariant of the system is sufficiently large. As a special case of this we recover the results of Dietmann's work [4] on systems of quadratic and cubic forms.

For a homogeneous form $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ we define the h-invariant of f to be the least integer h such that f can be written in the form

$$f(\mathbf{x}) = \sum_{i=1}^{h} g_i(\mathbf{x}) g_i'(\mathbf{x}),$$

with forms $g_i(\mathbf{x})$ and $g_i'(\mathbf{x})$ of positive degree with rational coefficients. For a system $\mathbf{f}$ of homogeneous forms $f_i(\mathbf{x})$, $1 \le i \le r$, of degree d, we define the h-invariant $h(\mathbf{f})$ to be the minimum of the h-invariant of any form in the rational linear system of the forms, i.e. we set $h(\mathbf{f}) = \min_{\mathbf{b} \in \mathbb{Z}^r \setminus \{\mathbf{0}\}} h(f_{\mathbf{b}})$.

We say that a system of forms $\mathbf{f}$ of degree d is a Hardy-Littlewood system if the conclusion on the asymptotic formula for the counting function $N(P)$ as in Eq. (1) in Theorem 1 holds. If the h-invariant of a system of homogeneous forms of the same degree is sufficiently large, then Schmidt proves in his work [10] that $\mathbf{f}$ is a Hardy-Littlewood system. As we shall indicate in Sect. 2, his results easily imply the following theorem, which we state here for convenience.

Theorem 2 (Schmidt, 1985, See [10]). *There exists a function $\phi(d)$ with the following property. If the system $\mathbf{f}$ of homogeneous forms of degree $d > 1$ has a h-invariant which is bounded below by*

$$h(\mathbf{f}) > \phi(d)(r(r+1)(d-1)2^{d-1} + (d-1)r(r-1)),$$

then the system $\mathbf{f}$ is a Hardy-Littlewood system. Furthermore, one has $\phi(2) = \phi(3) = 1$, $\phi(4) = 3$, $\phi(5) = 13$ and $\phi(d) < (\log 2)^{-d} d!$ in general.

Note that the function $\phi(d)$ is exactly the function occurring in Proposition III_C in Schmidt's work [10].

Our new form of Weyl's inequality improves on this theorem in the following way.

Theorem 3. *Let $\phi(d)$ be the function as in Theorem 2. If the system $\mathbf{f}$ of homogeneous forms of degree $d > 1$ has a h-invariant which is bounded below by*

$$h(\mathbf{f}) > \phi(d) r(r+1)(d-1)2^{d-1},$$

then $\mathbf{f}$ *is a Hardy-Littlewood system. In the case* $d = 2$ *one may replace the condition on the h-invariant of the system by the assumption that the rank of each form in the rational linear system of the quadratic forms is bounded below by* $2r(r + 1)$.

The special cases of degree $d = 2$ and $d = 3$ in Theorem 3 reduce to Theorem 1 and Theorem 2 in Dietmann's paper [4]. In the quadratic case Dietmann improves on previous results of Schmidt in [8] in reducing the lower bound in the rank condition from $2r^2 + 3r$ to only $2r^2 + 2r$, and in the cubic case he reduces the lower bound on the h-invariant from $10r^2 + 6r$ (see Schmidt's paper [9]) to $8r^2 + 8r$. In fact, our new form of Weyl's inequality takes up the main idea in Dietmann's work [4].

As Dietmann points out in [4], the h-invariant can in some ways be seen as a generalisation of the rank of a quadratic form to higher degree forms. By diagonalising a quadratic form one sees that its h-invariant is bounded by its rank. However, we note that these two notions do not coincide for the case of quadratic forms, as examples built up from forms like $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2)$ show. Hence we need to formulate the case $d = 2$ in Theorem 3 separately in order to obtain the full strength of the theorem in this case.

As another example we consider the case of systems of forms $\mathbf{f}$ of degree $d = 4$. In this case one has $\phi(4) = 3$ and Theorem 3 implies that the expected asymptotic formula for $N(P)$ holds as soon as

$$h(\mathbf{f}) > 3r(r + 1) \times 3 \times 2^3 = 9 \times (8r^2 + 8r).$$

Schmidt obtains the same result in his paper [10] (see Theorem 2 above) under the stronger condition

$$h(\mathbf{f}) > \phi(4)(r(r + 1)(d - 1)2^{d-1} + (d - 1)r(r - 1)) = 9(9r^2 + 7r). \tag{2}$$

We finally remark that if the system of forms $f_i(\mathbf{x})$, $1 \leq i \leq r$, in Theorem 1 or Theorem 3 forms a complete intersection, and if there exist non-singular real and p-adic points on the variety X given by these forms, then the singular series $\mathfrak{S}$ and the singular integral $\mathscr{J}$ are both positive. In particular, this implies the existence of rational points on the variety X as soon as there are non-singular solutions at every place of $\mathbb{Q}$ including infinity.

The structure of this paper is as follows. We recall a version of Weyl's inequality from [2] in the next section and present in Lemma 2 our new variant of Weyl's inequality for systems of forms. We use this in the last section to deduce Theorems 1 and 3, and we explain the improvements of Theorem 3 compared to Theorem 2.

After Dietmann posted [4] on the ArXiv, containing the new variant of Weyl's inequality and its application to systems of quadratic and cubic forms, he (in the revised published version [5]) and the author independently generalized his work to systems of forms of higher degree, and to Birchs theorem, obtaining the same conclusions Theorems 1 and 3. Most of our reference to his work hence refers to the earlier version [4], and now Lemma 2 could also be deduced from the later version [5].

2 A Variant of Weyl's Inequality

For some n-dimensional box $\mathscr{B}$, some real vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r)$ and some large real number P we define the exponential sum

$$S(\boldsymbol{\alpha}) = \sum_{\mathbf{x} \in P\mathscr{B} \cap \mathbb{Z}^n} e\left(\sum_{i=1}^{r} \alpha_i f_i(\mathbf{x}) \right).$$

If $f(\mathbf{x})$ is some homogeneous form of degree d, then we let $\Gamma_f(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)})$ be its unique associated symmetric multilinear form satisfying $\Gamma_f(\mathbf{x}, \dots, \mathbf{x}) = d! f(\mathbf{x})$. Moreover, if $f_i(\mathbf{x})$, $1 \le i \le r$, form a system of homogeneous forms of degree d as before, then we let $\Gamma_i(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)})$, $1 \le i \le r$, be the associated multilinear forms. We introduce the sup-norm $|\mathbf{x}| = \max_{1 \le i \le n} |x_i|$ on the vector space $\mathbb{R}^n$, and write $\|\gamma\| = \min_{y \in \mathbb{Z}} |\gamma - y|$ for the least distance of a real number γ to an integer. Furthermore, we write here and in the following $\mathbf{e}_j$ for the j-th unit vector in n-dimensional affine space. Then we let $N(P^{\xi}; P^{-\eta}; \boldsymbol{\alpha})$ be the number of integer vectors $\mathbf{x}^{(2)}, \dots, \mathbf{x}^{(d)}$ with $|\mathbf{x}^{(2)}|, \dots, |\mathbf{x}^{(d)}| \le P^{\xi}$ and

$$\left\| \sum_{i=1}^{r} \alpha_i \Gamma_i(\mathbf{e}_j, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(d)}) \right\| < P^{-\eta}, \quad 1 \le j \le n.$$

We start our considerations with recalling Lemma 2.4 from Birch's work [2].

Lemma 1 (Lemma 2.4 in [2]). *Let $k > 0$ be a real parameter. For fixed $0 < \theta \le 1$ one of the following alternatives hold.*

(i) $|S(\boldsymbol{\alpha})| < P^{n-k}$, *or*
(ii) $N(P^{\theta}; P^{-d+(d-1)\theta}; \boldsymbol{\alpha}) \gg P^{(d-1)n\theta - 2^{d-1}k - \varepsilon}$, *for any $\varepsilon > 0$.*

The main idea is to treat the condition (ii) differently than in Birch's work [2], following a similar idea as taken up in the paper [4]. Before stating our new version of Weyl's inequality, we need to introduce the g-invariant of a homogeneous form.

We define $\mathscr{M}_f$ to be the variety in affine $(d-1)n$-space given by

$$\Gamma_f(\mathbf{e}_j, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(d)}) = 0, \quad 1 \le j \le n,$$

and write $\mathscr{M}_f(P)$ for the number of integer points on $\mathscr{M}_f$ with coordinates all bounded by P. Then we define the g-invariant $g(f)$ of the form f to be the largest real number such that

$$\mathscr{M}_f(P) \ll P^{(d-1)n - g(f) + \varepsilon},$$

holds for all $\varepsilon > 0$. Note that this number $g(f)$ coincides with the g-invariant that Schmidt associates to a single form f in [10].

Lemma 2. *Let* $\tilde{g} = \inf_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} g(f_{\mathbf{b}})$ *and let* $0 < \theta \leq 1$ *be fixed. Then we either have the bound*

(i) $|S(\boldsymbol{\alpha})| < P^{n-2^{-d+1}\tilde{g}\theta+\varepsilon}$, *or*

(ii) (major arc approximation for $\boldsymbol{\alpha}$ *with respect to the parameter* θ*) there exist natural numbers* $a_1, \ldots, a_r$ *and* $1 \leq q \ll P^{r(d-1)\theta}$ *with* $\gcd(q, a_1, \ldots, a_r) = 1$ *and*

$$|q\alpha_i - a_i| \ll P^{-d+r(d-1)\theta}, \quad 1 \leq i \leq r.$$

Proof. Let the notation be as in Lemma 1 and assume that alternative (ii) in Lemma 1 holds.

We consider the matrix ψ of size $r \times (nN(P^\theta; P^{-d+(d-1)\theta}; \boldsymbol{\alpha}))$ with entries $\Gamma_i(\mathbf{e}_j, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(d)})$ in the ith row. The columns are indexed by $(j, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(d)})$, where $1 \leq j \leq n$ and $\mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(d)}$ run through all tuples of integer vectors counted by $N(P^\theta; P^{-d+(d-1)\theta}; \boldsymbol{\alpha})$. We distinguish two cases.

Case (a): Assume that $\operatorname{rank}(\psi) = r$. Then there is a $r \times r$-minor $\tilde{\psi}$ of full rank, which we say is given by

$$\tilde{\psi} = (\tilde{\psi}_{i,l})_{1\leq i,l\leq r} = (\Gamma_i(\mathbf{e}_{j_l}, \mathbf{x}_l^{(2)}, \ldots, \mathbf{x}_l^{(d)}))_{1\leq i,l\leq r}.$$

In particular, we have $\| \sum_{i=1}^r \alpha_i \tilde{\psi}_{i,l} \| < P^{-d+(d-1)\theta}$, for all $1 \leq l \leq r$. Hence, we can write

$$\sum_{i=1}^r \alpha_i \tilde{\psi}_{i,l} = \tilde{a}_l + \tilde{\delta}_l,$$

with integers $\tilde{a}_l$ and real numbers $\tilde{\delta}_l$ with $|\tilde{\delta}_l| < P^{-d+(d-1)\theta}$. Let $\tilde{\psi}^{\mathrm{adj}}$ be the adjoint matrix to $\tilde{\psi}$, which satisfies $\tilde{\psi}^{\mathrm{adj}}\tilde{\psi} = (\det\tilde{\psi})\,\mathrm{id}$, and let $q = \det\tilde{\psi}$. Since $\tilde{\psi}$ was assumed to be of rank r, its determinant q is non-zero. Furthermore we note that $|q| \ll P^{r\theta(d-1)}$. Now we can use the adjoint matrix $\tilde{\psi}^{\mathrm{adj}}$ to find a good approximation for $\boldsymbol{\alpha}$ by rational numbers with small denominator. Indeed, we have

$$\begin{aligned}\left| q\alpha_i - \sum_{l=1}^r \tilde{\psi}_{i,l}^{\mathrm{adj}} \tilde{a}_l \right| &\leq \sum_{l=1}^r |\tilde{\psi}_{i,l}^{\mathrm{adj}}||\tilde{\delta}_l| \\ &\ll P^{\theta(r-1)(d-1)} P^{-d+(d-1)\theta}.\end{aligned}$$

We set $a_i = \sum_{l=1}^r \tilde{\psi}_{i,l}^{\mathrm{adj}} \tilde{a}_l$. After removing common factors of q and the integers a_i, we obtain integers $q, a_1, \ldots, a_r$ with $\gcd(q, a_1, \ldots, a_r) = 1$ and $1 \leq q \ll P^{r(d-1)\theta}$, such that

$$|q\alpha_i - a_i| \ll P^{-d+r(d-1)\theta}, \quad 1 \leq i \leq r.$$

In this case the conclusion (ii) of the Lemma holds.

Case (b): Assume that $\operatorname{rank}(\psi) < r$. Then the r rows of ψ are linearly dependent over $\mathbb{Q}$, and thus there exist integers $b_1, \dots, b_r \in \mathbb{Z}$, not all zero, such that

$$\sum_{i=1}^{r} b_i \Gamma_i(\mathbf{e}_j, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(d)}) = 0,$$

for all $1 \le j \le n$ and for all tuples $\mathbf{x}^{(2)}, \dots, \mathbf{x}^{(d)}$ counted by $N(P^\theta; P^{-d+(d-1)\theta}; \boldsymbol{\alpha})$.We note that

$$\sum_{i=1}^{r} b_i \Gamma_i(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)}) = \Gamma_{f_\mathbf{b}}(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)})$$

is the multilinear form associated to the form $f_\mathbf{b}(\mathbf{x}) = \sum_{i=1}^{r} b_i f_i(\mathbf{x})$. We recall the definition of the variety $\mathscr{M}_f$ stated before this lemma, and deduce from the lower bound on $N(P^\theta; P^{-d+(d-1)\theta}; \boldsymbol{\alpha})$, that we have

$$\mathscr{M}_{f_\mathbf{b}}(P^\theta) \gg P^{(d-1)n\theta - 2^{d-1}k - \varepsilon}, \tag{3}$$

for any $\varepsilon > 0$. By definition of the g-invariant $g(f_\mathbf{b})$ we see that Eq. (3) implies that

$$(d-1)n - 2^{d-1}k/\theta - \varepsilon \le (d-1)n - g(f_\mathbf{b}) + \varepsilon,$$

for any $\varepsilon > 0$. Hence we have $2^{-d+1} g(f_\mathbf{b})\theta \le k$ for some $\mathbf{b} \in \mathbb{Z}^r \setminus \{\mathbf{0}\}$, and the first alternative of the lemma holds.

We remark that Lemma 2 has recently also appeared in the form of Lemma 2 in [5].

3 Applications

The main goal of this section is to prove Theorems 1 and 3. Before we show how Lemma 2 implies Theorems 1 and 3 we recall some very general results from Schmidt's work [10], which simplify our following arguments.

For this we first recall the Hypothesis on $\mathbf{f}$ introduced in Sect. 4 in [10] for the case of forms of same degree.

Hypothesis 4 (Hypothesis on f with Parameter Ω) *Let $\mathscr{B}$ be some box and $\Delta > 0$ and assume that P is sufficiently large depending on the system $\mathbf{f}$, the parameter Ω, the box $\mathscr{B}$ and Δ. Then one either has the upper bound*

i) $|S(\boldsymbol{\alpha})| \le P^{n-\Delta\Omega}$, *or*
ii) there are natural numbers $q \le P^\Delta$ and $a_1, \dots, a_r$ such that

$$|q\alpha_i - a_i| \le P^{-d+\Delta}, \quad 1 \le i \le r.$$

In his work [10] Schmidt shows that this hypothesis is enough to verify that the Hardy-Littlewood circle method can be applied to the counting function $N(P)$ related to the system of equations $\mathbf{f}$. One of his main results is the following, which we only state for the special case of forms of the same degree, since this is all we use in this paper.

Theorem 5 (Proposition I in [10], Second Part). *Suppose the system* $\mathbf{f}$ *satisfies Hypothesis 4 with respect to some parameter*

$$\Omega > r + 1.$$

Then $\mathbf{f}$ *is a Hardy-Littlewood system.*

In combination with our new version of Weyl's inequality in Lemma 2 we obtain the following useful corollary.

Corollary 1. *Assume that* $\mathbf{f}$ *is a system of homogeneous forms of the same degree with*

$$\inf_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} g(f_{\mathbf{b}}) > r(r+1)(d-1)2^{d-1}.$$

Then the asymptotic formula for $N(P)$ *as predicted by the circle method holds, i.e.* $\mathbf{f}$ *is a Hardy-Littlewood system.*

Proof. First we note that Lemma 2 implies Hypothesis 4 with respect to any parameter

$$\Omega < 2^{-d+1}r^{-1}(d-1)^{-1}\tilde{g}.$$

This is clear by the formulation of Lemma 2 for the range $0 < \Delta \leq r(d-1)$ if we set $\Delta = r(d-1)\theta$. In the case where $\Delta > r(d-1)$ alternative (ii) in Hypothesis 4 is automatically satisfied by Dirichlet's approximation principle.

Now Proposition I in [10] applies as stated in Theorem 5, which completes the proof of the Corollary.

Next we relate the g-invariant of a homogeneous form to the dimension of its singular locus, and thereby establish the new formulation of Birch's theorem on forms in many variables as stated in Theorem 1.

Proof (Proof of Theorem 1). Consider some vector $\mathbf{b} \in \mathbb{Z}^r \setminus \{\mathbf{0}\}$ and its associated form $f_{\mathbf{b}}$ in the pencil of $f_i(\mathbf{x})$, $1 \leq i \leq r$. We note that the intersection of the affine variety $\mathscr{M}_{f_{\mathbf{b}}}$ with the diagonal $\mathscr{D}$ given by

$$\mathbf{x}^{(2)} = \ldots = \mathbf{x}^{(d)},$$

is isomorphic to the singular locus of the form $f_{\mathbf{b}}$. Hence we obtain by the affine intersection theorem that

$$\dim \operatorname{Sing}(f_{\mathbf{b}}) = \dim(\mathscr{D} \cap \mathscr{M}_{f_{\mathbf{b}}}) \geq \dim \mathscr{D} + \dim \mathscr{M}_{f_{\mathbf{b}}} - (d-1)n.$$

This shows that

$$\dim \mathrm{Sing}(f_{\mathbf{b}}) \geq \dim \mathscr{M}_{f_{\mathbf{b}}} - (d-1)n + n,$$

which implies that

$$g(f_{\mathbf{b}}) \geq n - \dim \mathrm{Sing}(f_{\mathbf{b}}).$$

Taking the infimum over all non-zero integer tuples $\mathbf{b}$ we obtain

$$\inf_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} g(f_{\mathbf{b}}) \geq n - \max_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} (\dim \mathrm{Sing}(f_{\mathbf{b}})),$$

and hence Lemma 2 holds with $\tilde{g}$ replaced by $n - \max_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}}(\dim \mathrm{Sing}(f_{\mathbf{b}}))$. This shows that in Lemma 4.3 in Birch's work [2], the quantity K which is defined in his setting as

$$2^{d-1}K = n - \dim V^*,$$

can be replaced by

$$2^{d-1}K = n - \max_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} (\dim \mathrm{Sing}(f_{\mathbf{b}})).$$

Now Theorem 1 follows identically as the main theorem in Birch's paper [2]. Alternatively we can apply Corollary 1 to obtain the desired result.

Next we turn towards the proof of Theorem 3 which improves on the previous known results in Theorem 2. However, since Theorem 2 is not contained in this formulation in the paper [10], we first give a short deduction of it from the results of [10]. Indeed, Schmidt concludes in his remark after Proposition II_0 that the expected asymptotic formula in Theorem 2 for $N(P)$ holds as soon as a so called g-invariant $g(\mathbf{f})$ of the system $\mathbf{f}$ is larger than

$$g(\mathbf{f}) > 2^{d-1}(d-1)r(r+1). \tag{4}$$

His Corollary after Proposition III states that there is the relation

$$h(\mathbf{f}) \leq \phi(d)(g(\mathbf{f}) + (d-1)r(r-1)). \tag{5}$$

Hence the condition

$$h(\mathbf{f}) > \phi(d)(r(r+1)(d-1)2^{d-1} + (d-1)r(r-1)),$$

in Theorem 2 implies that (4) holds and thus the conclusion of Theorem 2 follows.

The main difference in the use of our new version of Weyl's inequality in comparison to Schmidt's work is that we can state everything in terms of the g-invariant of a single form. In his work [10] Schmidt uses a form of Weyl's inequality where the infimum of all g-invariants of the elements of the rational linear system is replaced by his so called g-invariant $g(\mathbf{f})$ of the whole system. This is in complete analogy with the replacement of the locus V^* in Birch's work [2] by the maximal dimension of the singular loci of elements in the rational linear system as in Theorem 1.

Proof (Proof of Theorem 3). For a single form f, Eq. (17.2) in [10] implies that

$$h(f) \leq \phi(d)g(f), \tag{6}$$

which should be compared to the relation (5) for systems of forms. For a single form we do not need the term $\phi(d)(d-1)r(r-1)$, which is present for the relation referring to the whole system of forms in Eq. (5). This explains our improvement of Theorem 3 compared to Theorem 2.

Assume now that the assumptions of Theorem 3 are satisfied, i.e.

$$h(\mathbf{f}) > \phi(d)r(r+1)(d-1)2^{d-1}.$$

Recall that we have defined $h(\mathbf{f}) = \min_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} h(f_{\mathbf{b}})$. Hence we obtain together with Eq. (6) the relation

$$\inf_{\mathbf{b}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} g(f_{\mathbf{b}}) > r(r+1)(d-1)2^{d-1}.$$

Now we apply Corollary 1 to complete the proof of Theorem 3 for the case of degree $d \geq 3$.

For the case of systems of quadratic forms we note that the g-invariant of a single quadratic form f is bounded below by its rank. Indeed, let some quadratic form f be given by some $n \times n$-matrix A. Then the variety $\mathscr{M}_f$ is given by the system of linear equations $A\mathbf{x} = 0$, and we deduce that

$$\mathscr{M}_f(P) \ll P^{n-\mathrm{rank}(A)},$$

which shows that $g(f) \geq \mathrm{rank}(A)$. Now we apply Corollary 1 as in the case $d \geq 3$.

Acknowledgements The author would like to thank Prof. T.D. Browning for comments on an earlier version of this paper, Prof. P. Salberger for helpful discussions, and the referees for a careful reading of the manuscript and their suggestions.

References

1. A.G. Aleksandrov, B.Z. Moroz, Complete intersections in relation to a paper of B.J. Birch. Bull. Lond. Math. Soc. **34**, 149–154 (2002)
2. B.J. Birch, Forms in many variables. Proc. R. Soc. A **265**, 245–263 (1962)
3. J. Brandes, Forms representing forms and linear spaces on hypersurfaces. Proc. Lond. Math. Soc. **108**, 809–835 (2014)
4. R. Dietmann, Weyl's inequality and systems of forms. Available at arXiv:1208.1968v1 (2012). http://arxiv.org/abs/1208.1968v1.Cited9Aug2012
5. Dietmann, R.: Weyl's inequality and systems of forms. Q. J. Math **66** (1), 97–110 (2015)
6. S.-L.A. Lee, Birch's theorem in function fields. Available at arXiv: 1109.4953 (2011). http://arxiv.org/abs/1109.4953.Cited27Sept2011
7. D. Schindler, Bihomogeneous forms in many variables. J. Théorie Nombres Bord. **26**, 483–506 (2014)
8. W.M. Schmidt, Simultaneous rational zeros of quadratic forms, in *Seminar on Number Theory*, Paris 1980–1981 (Paris, 1980/1981), Progress in Mathematics, vol. 22 (Birkhäuser, Boston, 1982), pp. 281–307
9. W.M. Schmidt, On cubic polynomials IV. Systems of rational equations. Monatsh. Math. **93**, 329–348 (1982)
10. W.M. Schmidt, The density of integer points on homogeneous varieties. Acta Math. **154**(3–4), 243–296 (1985)
11. C.M. Skinner, Forms over number fields and weak approximation. Comput. Math. **106**, 11–29 (1997)

The Breuil-Schneider Conjecture: A Survey

Claus M. Sorensen

Abstract This note is a survey of the Breuil-Schneider conjecture, based on the authors 30 min talk at the 13th conference of the Canadian Number Theory Association (CNTA XIII) held at Carleton University, June 16–20, 2014. We give an overview of the problem, and describe certain recent developments by the author and others.

1 Prelude: The Fontaine-Mazur Conjecture

Let $\tilde{F}$ be a number field,[1] with absolute Galois group $\Gamma_{\tilde{F}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\tilde{F})$. The p-adic representations of $\Gamma_{\tilde{F}}$, which arise naturally, come from algebraic geometry. More precisely, if $X_{/\tilde{F}}$ is a (smooth projective) variety, one would look at irreducible constituents $r : \Gamma_{\tilde{F}} \to \mathrm{GL}_n(\mathbb{Q}_p)$ of the cohomology $H^\bullet_{\text{ét}}(X \times_{\tilde{F}} \bar{\mathbb{Q}}, \bar{\mathbb{Q}}_p(t))$. It is now known that such r are "*geometric*", which by definition means the following:

- $r_w := r|_{\Gamma_{\tilde{F}_w}}$ is unramified[2] at all but finitely many places $w \nmid p$.
- r_w is potentially semistable at all places $w|p$.

The Fontaine-Mazur conjecture (Conjecture 1 in [23]) is the converse: These local conditions guarantee that r occurs in the cohomology of some X, up to Tate twist.

In recent years, Emerton and Kisin have made impressive progress on this for odd two-dimensional representations of $\Gamma_{\mathbb{Q}}$—as a result of the proof of Serre's conjecture [32], by Khare and Wintenberger! To give the flavor, Emerton shows the following result (see Theorem 1.2.4 in [21]).

[1] This is the notation we will eventually use in Sect. 5 below, to distinguish it from $F/\mathbb{Q}_p$.

[2] Here we tacitly fix algebraic closures $\bar{F} \hookrightarrow \bar{F}_w$ extending $F \hookrightarrow F_w$, in order to identify the decomposition group $\Gamma_{F_w} = \mathrm{Gal}(\bar{F}_w/F_w)$ with a subgroup of Γ_F. We say r_w is *unramified* if its restriction to the inertia group $I_{F_w} = \mathrm{Gal}(\bar{F}_w/F_w^{nr})$ is trivial.

C.M. Sorensen (✉)
Department of Mathematics, UC San Diego, La Jolla, CA, USA
e-mail: csorensen@ucsd.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_10

Theorem 1.1 (Emerton). *Let $r : \Gamma_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ be an irreducible odd representation, $p > 2$. Assume $\bar{r}|_{\Gamma_{\mathbb{Q}(\xi_p)}}$ is irreducible, and that $\bar{r}|_{\Gamma_{\mathbb{Q}_p}}$ is "generic". If r is geometric, with distinct Hodge-Tate weights, then (up to a Tate twist) $r = r_f$ for some cuspidal eigenform f of weight $k \geq 2$.*

Remark 1. We write $\bar{r}$ for the reduction of r modulo p. Let us add a few details. By the compactness of $\Gamma_{\mathbb{Q}}$, the image of r lies in $\mathrm{GL}_2(\mathscr{O}_E)$ for some finite extension $E/\mathbb{Q}_p$. Composition with $\mathscr{O}_E \twoheadrightarrow \kappa_E = \mathscr{O}_E/\varpi_E\mathscr{O}_E$ yields the "naive" reduction mod p into $\mathrm{GL}_2(k_E) \subset \mathrm{GL}_2(\bar{\mathbb{F}}_p)$. The Brauer-Nesbitt principle tells us its *semi-simplification* is independent of the choice of stable $\mathscr{O}_E$-lattice in E^2. This semisimple representation is what we denote by $\bar{r}$. Of course, in Theorem 1.1 $\bar{r}$ is irreducible, so it's given by any of its naive reductions. The notion of $\bar{r}|_{\Gamma_{\mathbb{Q}_p}}$ being "generic" is a bit ad hoc. Here we take it to mean that $\bar{r}|_{\Gamma_{\mathbb{Q}_p}} \sim \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & * \\ & \bar{\varepsilon}_{cyc} \end{pmatrix}$; even after twisting by a character, and * may or may not be zero. (Here $\bar{\varepsilon}_{cyc}$ is the mod p cyclotomic character.)

Since there is a motive attached to f, by Scholl and others [36], one knows how to carve out $r = r_f$ in the cohomology of some (Kuga-Sato) variety $X_{/\mathbb{Q}}$.

Very broadly speaking, the proof of 1.1 has two steps. The **first** step is essentially Serre's conjecture, which combined with "big" $R = \mathbb{T}$ theorems of Böckle [8] tells us that at least r comes from a *p-adic* modular form; we say r is *pro*-modular (closely related to the modularity of $\bar{r}$). The **second** step is to establish *classical* modularity of r, using that $r|_{\Gamma_{\mathbb{Q}_p}}$ is potentially semistable of regular weight. This is where the p-adic local Langlands correspondence $\Pi(\cdot)$ for $\mathrm{GL}_2(\mathbb{Q}_p)$ comes in. It goes from two-dimensional p-adic representation of $\Gamma_{\mathbb{Q}_p}$ to unitary p-adic Banach space representations of $\mathrm{GL}_2(\mathbb{Q}_p)$, and its "inverse" has a nice clean description via Colmez's so-called Montreal functor. We're applying $\Pi(\cdot)$ to the restriction $r|_{\Gamma_{\mathbb{Q}_p}}$. Emerton shows in [21] that it satisfies local-global compatibility, which basically says that

$$\Pi(r|_{\Gamma_{\mathbb{Q}_p}}) \hookrightarrow \mathrm{Hom}_{\Gamma_{\mathbb{Q}}}(r, \hat{H}^1),$$

where $\hat{H}^1$ is a huge Banach-space of p-adic modular forms (the completed cohomology of the tower of modular curves). The condition at p ensures that $\Pi(r|_{\Gamma_{\mathbb{Q}_p}})$ has so-called "locally algebraic" vectors—much more on these in the next section! Hence so does $\mathrm{Hom}_{\Gamma_{\mathbb{Q}}}(r, \hat{H}^1)$. But the locally algebraic vectors in $\hat{H}^1$ have a description in terms of classical modular forms, and this essentially finishes the proof.

This is meant to motivate the search for a p-adic local Langlands correspondence for $\mathrm{GL}_n(F)$, for finite extensions $F/\mathbb{Q}_p$, and other groups. The Breuil-Schneider conjecture is one of the initial steps towards a precise formulation of what one is looking for.

2 Motivation: p-Adic Local Langlands for $\mathrm{GL}_2(\mathbb{Q}_p)$

The *classical* local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ is a bijection between certain two-dimensional Weil-Deligne representations of $W_{\mathbb{Q}_p}$ and irreducible smooth representations of $\mathrm{GL}_2(\mathbb{Q}_p)$. Here the coefficient field E is unspecified. One can take the complex numbers $\mathbb{C}$, the ℓ-adic numbers $\bar{\mathbb{Q}}_\ell$ for $\ell \neq p$, or even $\bar{\mathbb{Q}}_p$—which we eventually will. The topology of E plays no role in the correspondence. A natural source of Weil-Deligne representations are Galois representations. This is where the topology of E plays a huge role. Thus, for $\ell \neq p$, with any continuous representation $\rho : \Gamma_{\mathbb{Q}_p} = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\bar{\mathbb{Q}}_\ell)$ one can associate a Weil-Deligne representation $\mathrm{WD}(\rho)$, and hence an irreducible smooth representation $\pi_{sm}(\rho)$ of $\mathrm{GL}_2(\mathbb{Q}_p)$ over $\bar{\mathbb{Q}}_\ell$. Moreover, one can *recover* ρ from $\pi_{sm}(\rho)$. This completely fails for $\ell = p$, and this is what leads to the p-adic local Langlands correspondence. The classical local Langlands correspondence for $\mathrm{GL}(2)$ has been dealt with in detail in [7]. For $\mathrm{GL}(n)$ there are several good expositions. We mention [31, 41].

In what follows we will fix our coefficient field E, which we take to be a finite extension $E/\mathbb{Q}_p$. Suitably normalized, classical local Langlands is $\Gamma_{\mathbb{Q}_p}$-equivariant and can therefore be defined over E (as opposed to $\bar{\mathbb{Q}}_p$). If we restrict ourselves to potentially semistable representations $\rho : \Gamma_{\mathbb{Q}_p} \to \mathrm{GL}_2(E)$, a recipe of Fontaine associates a Weil-Deligne representation $\mathrm{WD}(\rho)$, and hence $\pi_{sm}(\rho)$ still makes sense. See [10, 29] for details on how this goes. However, $\rho \rightsquigarrow \pi_{sm}(\rho)$ is no longer reversible. In addition, we have the Hodge-Tate weights, which we will assume are distinct, $\mathrm{HT}(\rho) = \{w_1 < w_2\}$. These correspond to an irreducible algebraic representation $\pi_{alg}(\rho)$ of $\mathrm{GL}_2(\mathbb{Q}_p)$—the one of highest weight $t \mapsto t_1^{w_2-1}t_2^{w_1}$ (relative to the upper-triangular Borel). More concretely,

$$\pi_{alg}(\rho) = \det{}^{w_1} \otimes_E \mathrm{Sym}^{w_2-w_1-1}(E^2).$$

Still, one cannot reconstruct ρ from $\pi_{sm}(\rho)$ and $\pi_{alg}(\rho)$. In a nutshell, the problem is the following: In p-adic Hodge theory, the potentially semistable ρ are classified by linear algebra data which includes a certain Hodge *filtration*—and this is lost in the process of constructing $\pi_{alg}(\rho)$. We only see its jumps.

The p-adic local Langlands correspondence takes *any* continuous representation $\rho : \Gamma_{\mathbb{Q}_p} \to \mathrm{GL}_2(E)$ and attaches a Banach E-space $\Pi(\rho)$ with a unitary $\mathrm{GL}_2(\mathbb{Q}_p)$-action. Consult [16] for the most recent developments (for small p). This map $\rho \rightsquigarrow \Pi(\rho)$ is reversible, and compatible with classical local Langlands in the following sense: When ρ is potentially semistable, with distinct Hodge-Tate weights,

$$\boxed{\Pi(\rho)^{alg} = \pi_{alg}(\rho) \otimes_E \pi_{sm}(\rho)}. \tag{1}$$

Furthermore, $\Pi(\rho)^{alg} = 0$ otherwise. Here the superscript *alg* indicates taking the locally algebraic vectors—an invariant subspace between the smooth vectors and

the locally analytic vectors. Recall that a vector is smooth if some compact open subgroup acts trivially. Analogously, a vector is locally algebraic if some compact open subgroup acts polynomially. (A good go-to source for these notions, as well as local analyticity, is Breuil's ICM article [11].)

When ρ is irreducible, $\Pi(\rho)$ is known to be topologically irreducible, and therefore the completion of $\pi_{alg}(\rho) \otimes_E \pi_{sm}(\rho)$ relative to a suitable $\mathrm{GL}_2(\mathbb{Q}_p)$-invariant norm $\|\cdot\|$, which somehow "corresponds" to the lost filtration.

For $\mathrm{GL}_n(\mathbb{Q}_p)$, or even $\mathrm{GL}_2(F)$ for finite extensions $F/\mathbb{Q}_p$, the p-adic local Langlands correspondence remains elusive. The Breuil-Schneider conjecture is in some sense a "first approximation", which uses (1) as a guiding principle: The right-hand side can be defined for any potentially semistable representation $\rho : \Gamma_F \to \mathrm{GL}_n(E)$, with distinct Hodge-Tate weights, and the conjecture is that $\pi_{alg}(\rho) \otimes_E \pi_{sm}(\rho)$ admits at least one $\mathrm{GL}_n(F)$-invariant norm. The resulting completions should be closely related to the yet undefined $\Pi(\rho)$—at least in the irreducible case.

Of course, ultimately one would want more than the mere *existence* of an invariant norm $\|\cdot\|$ on $\pi_{alg}(\rho) \otimes_E \pi_{sm}(\rho)$. In general it will *not* be unique (up to equivalence), but should correspond to the possible compatible Hodge filtrations. In the case of $\mathrm{GL}_2(\mathbb{Q}_p)$ this is exemplified by the connection to $\mathscr{L}$-invariants.

Example 1. Let $\mathscr{E}_{/\mathbb{Q}_p}$ be a semistable elliptic curve. That is, its reduction mod p has a nodal singularity (as opposed to a cusp). This can always be achieved by passing to a finite extension. By the theory of the Tate curve, any such $\mathscr{E}$ has p-adic uniformization; meaning there's a unique $q \in \bar{\mathbb{Q}}_p^\times$ with $|q| < 1$ such that $\mathscr{E}(\bar{\mathbb{Q}}_p) \simeq \bar{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$, respecting the $\Gamma_{\mathbb{Q}_p}$-action. The Galois action $\rho_{\mathscr{E},p}$ on the Tate module

$$V_p(\mathscr{E}) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(\mathscr{E}) \simeq \mathbb{Q}_p^{\oplus 2}, \quad T_p(\mathscr{E}) := \varprojlim_n \mathscr{E}[p^n] \simeq \mathbb{Z}_p^{\oplus 2},$$

can then be made explicit in terms of the parameter q—or rather the $\mathscr{L}$-invariant,

$$\mathscr{L} = \mathscr{L}_{\mathscr{E}} = \log(q)/\mathrm{ord}(q).$$

(Here log is the Iwasawa-log, with $\log(p) = 0$.) This $\mathscr{L}$ is *encoded* in $\rho_{\mathscr{E},p}$ via p-adic Hodge theory; it can be read off from the Hodge-filtration (see [5] for the explicit relation). In this example, $\mathrm{HT}(\rho_{\mathscr{E},p}) = \{0, 1\}$, so $\pi_{alg}(\rho_{\mathscr{E},p}) = 1$ and $\pi_{alg}(\rho_{\mathscr{E},p}) = St$; the Steinberg representation (up to an unramified quadratic twist). Recall that,

$$St = St_{\mathrm{GL}_2(\mathbb{Q}_p)} = \mathscr{C}^\infty(\mathbb{P}^1(\mathbb{Q}_p))/\{\text{constants}\}.$$

The sup-norm on St is certainly $\mathrm{GL}_2(\mathbb{Q}_p)$-invariant, and "corresponds" to $\mathscr{L} = 0$ (that is, $q = p$). In [6], it is shown how any $\mathscr{L}$ defines an invariant norm $\|\cdot\|_{\mathscr{L}}$ on St, such that $\Pi(\rho_{\mathscr{E},p}) = St^\wedge$ (the completion). In fact, more generally, in loc. cit. Breuil defines a unitary Banach space representation $B(k, \mathscr{L})$ of $\mathrm{GL}_2(\mathbb{Q}_p)$, for any $k \geq 2$ and $\mathscr{L} \in \bar{\mathbb{Q}}_p$. The dual $B(k, \mathscr{L})'$ is a certain space of $\log_{\mathscr{L}}$-rigid functions on the p-adic upper half-plane $\Omega = \mathbb{C}_p \backslash \mathbb{Q}_p$. Furthermore,

$$B(k,\mathscr{L})^{alg} = |\det|^{\frac{k-2}{2}} \cdot \mathrm{Sym}^{k-2} \otimes St.$$

(Breuil shows this for $k = 2$ and for $k > 2$ when $\mathscr{L}$ comes from a modular form; but it's now known in general due to subsequent work of Colmez and others.) These Banach representations $B(k,\mathscr{L})$ correspond to the semistable *non*-crystalline representations $\rho : \Gamma_{\mathbb{Q}_p} \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$, with weights $\{0, k-1\}$, under the p-adic local Langlands correspondence. It might be worth emphasizing that a very special feature for $\mathrm{GL}_2(\mathbb{Q}_p)$, is that for (irreducible) *crystalline* representations ρ, the invariant norm on $\pi_{alg}(\rho) \otimes_E \pi_{sm}(\rho)$ *is* in fact unique up to equivalence—this is extremely important in local-global compatibility; which explains how $\Pi(\rho)$ "sits" in completed cohomology when ρ arises from a p-adic modular form—see [21].

3 The Breuil-Schneider Conjecture: The Statement

Besides the coefficient field $E/\mathbb{Q}_p$, we now fix a base field $F/\mathbb{Q}_p$. We assume throughout that E is large enough to contain the Galois closure of F. Now suppose $\rho : \Gamma_F \to \mathrm{GL}_n(E)$ is a potentially semistable representation, with labeled Hodge-Tate weights $\mathrm{HT}_\tau(\rho) = \{w_{1,\tau} < \cdots < w_{n,\tau}\}$, for each embedding $\tau : F \hookrightarrow E$. As in Sect. 2, one defines a smooth E-representation $\pi_{sm}(\rho)$ of $\mathrm{GL}_n(F)$ via the classical local Langlands correspondence for GL_n plus Fontaine. There is a small wrinkle here, which we are tempted to gloss over: There is an issue with *genericity*—not in the sense of the Introduction, but in the (usual) sense of $\pi_{sm}(\rho)$ having a *Whittaker* model.[3] When $\pi_{sm}(\rho)$ is *non*-generic, one should really replace it by a generic (but reducible) principal series, of which it is quotient. For instance, in the GL_2-case, if ρ is the trivial representation one would take $\pi_{sm}(\rho)$ to be the non-split extension of 1 by Steinberg. For the most part we will sweep this under the rug, and usually assume ρ is generic (i.e., that $\pi_{sm}(\rho)$ is generic).

For each τ, we let $\pi_{alg,\tau}(\rho)$ be the irreducible algebraic representation of $\mathrm{GL}_n(F)$ of highest weight $(w_{n,\tau} - (n-1), \ldots, w_{1,\tau})$ relative to the upper-triangular Borel. Then let $\pi_{alg}(\rho) = \otimes_{\tau \in \mathrm{Hom}(F,E)} \pi_{alg,\tau}(\rho)$, with $\mathrm{GL}_n(F)$ acting diagonally. The Breuil-Scneider recipe, from [10], takes the tensor product, and gives a locally algebraic representation (again, with $\mathrm{GL}_n(F)$ acting diagonally):

Definition 3.1. $\mathrm{BS}(\rho) := \pi_{alg}(\rho) \otimes_E \pi_{sm}(\rho)$.

Upon a closer look, this definition works in greater generality. It only depends on the data $\mathrm{WD}(\rho)$ and $\mathrm{HT}_\tau(\rho)$ associated with ρ. In other words, we could start with data $\mathscr{D} = (\mathrm{WD}, \mathrm{HT}_\tau)$, consisting of a Weil-Deligne representation WD, and tuples of integers $\mathrm{HT}_\tau = \{w_{1,\tau} < \cdots < w_{n,\tau}\}$, and define $\mathrm{BS}(\mathscr{D})$ as above. The main conjecture of [10] is as follows (Conjecture 4.3 on p. 18 in loc. cit.).

[3] Meaning the representation $\pi_{sm}(\rho)$ embeds into $\mathrm{Ind}_{U_n}^{\mathrm{GL}_n}(\psi)$ for some additive character $\psi \neq 1$.

Conjecture 3.2 (Breuil, Schneider). The data $\mathscr{D}$ arises from a potentially semistable representation if and only if $\mathrm{BS}(\mathscr{D})$ admits a $\mathrm{GL}_n(F)$-invariant norm.

The "if" part of this conjecture is completely known [29], and is due to Y. Hu—who proved a stronger result: First, WD arises from an étale (ϕ, N)-module D in a standard way (see 2.2 in [29]). As part of his Orsay Ph.D. thesis, Hu translated the existence of an admissible filtration on D, with jumps HT_τ, into a purely group-theoretic condition known as the "Emerton condition" (in the vein of Theorem 1 in [25], which deals with the crystalline case). We rephrase part of Theorem 1.2 (or the slightly more general Theorem 2.12, p. 12) in [29] in our notation:

Theorem 3.3 (Hu). *$\mathscr{D}$ comes from a potentially semistable representation if and only if the Emerton condition holds: For every parabolic P, with Haar modulus δ_P,*

$$|(\delta_P^{-1}\chi)(z)|_p \leq 1, \quad \forall z \in Z_M^+, \quad \forall \chi \hookrightarrow J_P(\mathrm{BS}(\mathscr{D})). \tag{2}$$

Here Z_M^+ is the contracting monoid in the center of the Levi $M = M_P$, and $J_P(\cdot)$ is Emerton's locally analytic Jacquet functor (introduced and studied in [20]).

Let us add a few words on the contracting monoid (see p. 33 in [20] for more details): Once and for all, fix a compact open subgroup $N_0 \subset N = N_P$, and let $M^+ = \{m \in M | mN_0m^{-1} \subset N_0\}$. Then $Z_M^+ = M^+ \cap Z_M$. In the case of GL_n, taking P to be the standard parabolic corresponding to the partition $n = n_1 + \cdots + n_r$, it's given by

$$Z_M^+ = \{\mathrm{diag}(t_1 \cdot I_{n_1}, \ldots, t_r \cdot I_{n_r}) : |t_1| \leq \cdots \leq |t_r|\}.$$

It may also be worth pointing out that since $\mathrm{BS}(\mathscr{D}) = \pi_{alg}(\mathscr{D}) \otimes_E \pi_{sm}(\mathscr{D})$ is locally algebraic, we strictly speaking don't need the locally analytic extension of the Jacquet functor here: By Proposition 4.3.6, p. 63, in [20],

$$J_P(\mathrm{BS}(\mathscr{D})) \simeq \pi_{alg}(\mathscr{D})^{N_P} \otimes \pi_{sm}(\mathscr{D})_{N_P}.$$

Here the N_P-invariants $\pi_{alg}(\mathscr{D})^{N_P}$ is an irreducible algebraic representation of M_P, and the N_P-coinvariants $\pi_{sm}(\mathscr{D})_{N_P}$ is the usual Jacquet module in smooth representation theory (up to a twist).

It is relatively easy to show that (2) is satisfied if $\mathrm{BS}(\mathscr{D})$ carries an invariant norm, which is how the condition arose in the first place. This takes care of the so-called "easy" direction of Conjecture 3.2. The "only if" part is still open; the existence of a norm on $\mathrm{BS}(\rho)$. The purpose of this note is to report on recent progress in this direction. Note that asking for a norm amounts to asking for a (separated) *lattice*: Given $\|\cdot\|$, look at the unit ball Λ. Conversely, given Λ, look at its "gauge" $\|x\| = q_E^{-v_\Lambda(x)}$, where $v_\Lambda(x)$ is the largest v such that $x \in \varpi_E^v \Lambda$. Thus we are looking for integral structures in $\mathrm{BS}(\rho)$.

3.1 Forerunner: The Crystalline Case

For irreducible *crystalline* representations $\rho : \Gamma_{\mathbb{Q}_p} \to \mathrm{GL}_2(E)$, the p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ has a very nice description: Berger and Breuil showed that $\mathrm{BS}(\rho)$ admits a *unique* invariant norm, up to equivalence, and $\Pi(\rho)$ is the completion. See [4], or Theorem 2.3.2 on p. 8 of [5] (which is about the existence of a finite type lattice; all such are obviously commensurable).

In a precursor to [10], Schneider and Teitelbaum tried to extend this picture to higher-dimensional crystalline representations $\rho : \Gamma_F \to \mathrm{GL}_n(E)$. Here $\pi_{sm}(\rho)$ is an unramified principal series representation, corresponding to a character of the spherical Hecke algebra, $\zeta : \mathscr{H}(G,K) \to E$, where we have introduced $G = \mathrm{GL}_n(F)$ and $K = \mathrm{GL}_n(\mathscr{O}_F)$. Alternatively, one may then think of $\pi_{sm}(\rho)$ as a "universal module" (as in works of Borel, Matsumoto, Serre, Lazarus, etc.)

$$\pi_{sm}(\rho) \simeq \mathscr{C}_c(G/K) \otimes_{\mathscr{H}(G,K),\zeta} E,$$

where $\mathscr{C}_c(G/K)$ denotes the space of compactly supported E-valued continuous functions G/K (i.e, *finitely* supported functions since G/K is discrete). This can be generalized to take into account the algebraic representation $\pi_{alg}(\rho)$, which is traditionally denoted ξ. It defines a variant $\mathscr{H}_\xi(G,K)$ of the spherical Hecke algebra, consisting of $\mathrm{End}(\xi)$-valued K-biequivariant functions on G. When $\xi = 1$ one recovers $\mathscr{H}(G,K)$. Since ξ is an irreducible representation of G (as opposed to just K), there is in fact a natural isomorphism $\mathscr{H}(G,K) \xrightarrow{\sim} \mathscr{H}_\xi(G,K)$ of E-algebras, which can be used to transfer ζ to an eigensystem $\zeta : \mathscr{H}_\xi(G,K) \to E$. See p. 639 in [35]. Unwinding the definitions, one finds that

$$\mathrm{BS}(\rho) \simeq H_{\xi,\zeta} := \mathrm{ind}_K^G(\xi) \otimes_{\mathscr{H}_\xi(G,K),\zeta} E,$$

where $\mathrm{ind}_K^G = c\text{-}\mathrm{Ind}_K^G$ denotes the compact induction of the representation $\xi|_K$ (i.e., ξ-valued functions f on G such that $f(kg) = \xi(k)f(g)$, *and* such that f is compactly supported modulo K). This interpretation is useful, by virtue of $H_{\xi,\zeta}$ carrying a canonical G-invariant *seminorm*: Since K is compact, there is certainly a K-invariant norm $\|\cdot\|_\xi$ on ξ—and they are all equivalent since ξ is finite-dimensional. Thus $\mathrm{ind}_K^G(\xi)$ is endowed with the sup-norm, and finally $H_{\xi,\zeta}$ acquires the quotient *semi*-norm. Since we mod out by a subspace which may not be closed, a priori it could happen that $\|x\| = 0$ for some $x \neq 0$. A key construction in [35], p. 671, see also [34], is the following.

Definition 3.4. $B_{\xi,\zeta}$ is the Hausdorff completion of $H_{\xi,\zeta}$. That is, $(H_{\xi,\zeta}/\overline{\{0\}})^\wedge$.

Thus $B_{\xi,\zeta}$ is a unitary Banach E-representation of G, which yields $\Pi(\rho)$ when $n = 2$ and $F = \mathbb{Q}_p$. Unfortunately, in most other cases, it is not even known to be non-trivial! It would be bizarre, but we cannot rule out that 0 is dense in $H_{\xi,\zeta}$. This led to the (weaker) predecessor of Conjecture 3.2:

Conjecture 3.5 (Schneider, Teitelbaum). $B_{\xi,\zeta} \neq 0$.

For comparison, this is Conjecture 5.2 in [34]. Note that if $\mathrm{BS}(\rho) \simeq H_{\xi,\zeta}$ admits a G-invariant *norm* $\|\cdot\|'$, then in fact the canonical semi-norm on $H_{\xi,\zeta}$ must be a norm (and consequently $H_{\xi,\zeta} \hookrightarrow B_{\xi,\zeta}$ is dense): By Frobenius reciprocity, or really its "opposite"—which holds for *compact* induction, we have

$$\mathrm{Hom}_G(\mathrm{ind}_K^G(\xi), H_{\xi,\zeta}) \simeq \mathrm{Hom}_K(\xi, H_{\xi,\zeta}|_K),$$

and all maps here are automatically continuous since $\dim(\xi) < \infty$, regardless of what topology we put on $H_{\xi,\zeta}$. In particular the canonical projection $\pi : \mathrm{ind}_K^G(\xi) \to H_{\xi,\zeta}$ is automatically continuous for the $\|\cdot\|'$-topology. Thus $\ker(\pi)$ is closed.

Although in general $B_{\xi,\zeta}$ is not even known to be nonzero, it is expected to be a huge inadmissible representation, with lots of (almost) quotients, for $n > 2$ or $F \neq \mathbb{Q}_p$. The expectation is that there should be a G-map, with dense image,

$$B_{\xi,\zeta} \xrightarrow{?} \Pi(\rho),$$

for any irreducible crystalline ρ with $\pi_{alg} \leftrightarrow \xi$ and $\pi_{sm} \leftrightarrow \zeta$. There are scores of such representations in higher rank, corresponding to choices of admissible filtrations compatible with (ξ, ζ). The motto here is that $B_{\xi,\zeta}$ parametrizes the crystalline part of p-adic local Langlands.

There are other very important results in [35], but it would take us too far afield to describe them in detail here. Let it suffice to say they develop a (crystalline) theory for general split reductive groups $G_{/F}$, and prove an analogue of Theorem 3.3 in that setup. See Theorem 5.5 in [34] for a nice summary.

3.2 Miscellaneous Results

There are various partial results towards Conjecture 3.2 scattered in the literature, all proved in a purely local setting. We give a quick (possibly incomplete) overview.

- For $\mathrm{GL}_2(F)$, *de Ieso* used compact induction in [18] to produce a separated lattice in $\mathrm{BS}(\rho)$, under some technical p-smallness condition on the weight.
- For $\mathrm{GL}_2(F)$, *Assaf, Kazhdan, and de Shalit* used p-adic Fourier theory for the Kirillov model to get integral structures in two cases: (1) $\pi_{sm}(\rho)$ is unramified principal series, and $\pi_{alg}(\rho)$ is a twist of Sym^n with $n < q_F$, and (2) $\pi_{sm}(\rho)$ is tamely ramified and $n = 0$. See [1], and its prequel [30].
- For $\mathrm{GL}_2(F)$, *Vigneras* studied local systems on the tree in [40], and was able to show Conjecture 3.2 in the Steinberg case (Proposition 0.9 in loc. cit.) and made progress for tamely ramified principal series (Proposition 0.10).
- For general split reductive groups, *Grosse-Klönne* looked at the universal module for the spherical Hecke algebra, and was able to show cases of Conjecture 3.2

for unramified principal series, again under some p-smallness condition on the Coxeter number (when $F = \mathbb{Q}_p$) plus other technical assumptions. See Theorem 9.1 in [27].

4 The Indecomposable Case

When $\pi_{sm}(\rho)$ is supercuspidal (equivalently, $\mathrm{WD}(\rho)$ is absolutely irreducible), there are many ways to construct a norm on $\mathrm{BS}(\rho)$. One can write $\pi_{sm}(\rho)$ as a compactly induced representation, or take the sup-norm of matrix coefficients. (This case was already observed as Theorem 5.2 in [10].)

Note that the central character of $\mathrm{BS}(\rho)$ always takes values in $\mathscr{O}_E^\times$. In fact this is equivalent to the Emerton condition (2) when $\mathrm{WD}(\rho)$ is indecomposable (equivalently, $\pi_{sm}(\rho)$ is generalized Steinberg)—it turns out the Jacquet modules of $\pi_{sm}(\rho)$ are simple in that case, if nonzero, and as a consequence one only has to check (2) for $P = G$, which is p-adic unitarity of the central character.

This leads to the following *special case* of Conjecture 3.2, which was mentioned explicitly as Conjecture 5.5 in [10].

Conjecture 4.1. Let ρ be a potentially semistable representation, with distinct Hodge-Tate weights, such that $\mathrm{WD}(\rho)$ is indecomposable. Then $\mathrm{BS}(\rho)$ admits a $\mathrm{GL}_n(F)$-invariant norm.

The author recently proved this conjecture. In fact, he proved the following stronger result, which generalizes Conjecture 4.1 to arbitrary reductive groups [37].

Theorem 4.2 (S.). *Let $G_{/\mathbb{Q}_p}$ be a connected reductive group. Let π_{alg} be an irreducible algebraic representation of $G(\mathbb{Q}_p)$, and let π_{sm} be an essentially discrete series representation of $G(\mathbb{Q}_p)$, both defined over E. Then $\pi_{alg} \otimes_E \pi_{sm}$ admits a $G(\mathbb{Q}_p)$-invariant norm if (and only if) its central character is unitary.*

One deduces Conjecture 4.1 by taking $G = \mathrm{Res}_{F/\mathbb{Q}_p} \mathrm{GL}_n$. Indeed the generalized Steinberg representations of $\mathrm{GL}_n(F)$ are precisely the essentially discrete series representations—by which we mean some *twist* has L^2-matrix coefficients. Here lies a subtlety worth pointing out: We are working over a p-adic field E, not $\mathbb{C}$, so being L^2 only makes sense after choosing an embedding $E \hookrightarrow \mathbb{C}$. To get a good notion over E, we need to know the set of essentially discrete series is stable under $\mathrm{Aut}(\mathbb{C})$. For GL_n, this follows from the Bernstein-Zelevinsky classification (via segments of supercuspidals etc.)—see [31] for a nice overview. For a general G, it was shown by Clozel.

4.1 Sketch of the Proof of Theorem 4.2

After fiddling around with the center, and *using* that the central character takes values in $\mathscr{O}_E^\times$, one may assume G is semisimple. In turn, decomposing G^{sc} into a product of simple groups, and fiddling around with the tensor product norm (see paragraph 17, Chap. IV in [33]), one may assume G is in fact *simple* and *simply connected*. We are to show $\pi_{alg} \otimes_E \pi_{sm}$ *always* admits a norm—there is no center, hence no constraint.

Step 1. We choose a *global* model $G_{/\mathbb{Q}}$ such that $G(\mathbb{R})$ is compact. This uses a result of Borel and Harder in Galois cohomology [9], which shows that forms[4] (not necessarily inner forms) can be prescribed locally.

Step 2. We apply the trace formula for $G_{/\mathbb{Q}}$—which is as simple as the trace formula gets: There is no contribution from Eisenstein series since G is anisotropic. Since $G(\mathbb{R})$ is compact, π_{alg} is discrete series. So is π_{sm}, by hypothesis. Therefore they admit *pseudo-coefficients* [14] (functions on the group which behave like matrix-coefficients). By a now more-or-less standard argument, which goes back to Clozel [15] (which in turn builds on [17])—in much greater generality, one can "isolate" the contribution from π_{alg} and π_{sm} in the trace formula. The upshot being there exists *lots* of automorphic representations Π of $G(\mathbb{A})$ with $\Pi_\infty = \pi_{alg}$ and $\Pi_p = \pi_{sm}$ (under some fixed and suppressed embedding $E \hookrightarrow \mathbb{C}$). Here we use that G is simple to run the trace formula techniques.

Step 3. Let $\mathscr{A}_G$ be the space of automorphic forms on $G(\mathbb{A})$. Following [26], for each compact open subgroup $K \subset G(\mathbb{A}_f)$, consider the space of algebraic modular forms on G, of weight π_{alg} and level K. That is, $\mathrm{Hom}_{G(\mathbb{R})}(\pi_{alg}, \mathscr{A}_G^K)$—which contains Π_f^K as a direct summand. Indeed,

$$\mathrm{Hom}_{G(\mathbb{R})}(\pi_{alg}, \mathscr{A}_G^K) \simeq \bigoplus\nolimits_{\pi : \pi_\infty \simeq \pi_{alg}} m_G(\pi) \cdot \pi_f^K .$$

Via $E \hookrightarrow \mathbb{C}$ this space gets identified with p-adic modular forms, $\mathrm{Hom}_K(\pi_{alg}, \mathscr{C}_G)$, where $\mathscr{C}_G$ is the space of all continuous functions $G(\mathbb{Q})\backslash G(\mathbb{A}_f) \to E$, and K acts via the projection to $G(\mathbb{Q}_p)$. Thus,

$$\pi_{alg} \otimes \Pi_f^K \subset \pi_{alg} \otimes \mathrm{Hom}_K(\pi_{alg}, \mathscr{C}_G) \hookrightarrow \mathscr{C}_G^{K^p} .$$

When varying the level K_p, these maps are compatible, and give rise to a map

$$(\pi_{alg} \otimes \Pi_p) \otimes \Pi_f^{K^p} \hookrightarrow \mathscr{C}_G^{K^p} .$$

[4] Not to be confused with *automorphic* forms. For instance, the inner forms of GL(2) are the algebraic groups $D^\times$, for quaternion algebras D, whereas the outer forms of GL(2) are the unitary groups in two variables.

Passing to the limit over shrinking K^p yields $\pi_{alg} \otimes \Pi_f = (\pi_{alg} \otimes \pi_{sm}) \otimes \Pi_f^p \hookrightarrow \mathscr{C}_G$. The quotient $G(\mathbb{Q})\backslash G(\mathbb{A}_f)$ is compact, so $\mathscr{C}_G$ endowed with the sup-norm is a Banach space on which $G(\mathbb{A}_f)$ acts unitarily via right-translations. Restricting the sup-norm yields a $G(\mathbb{A}_f)$-invariant norm on $\pi_{alg} \otimes \Pi_f$—and by further restriction a $G(\mathbb{Q}_p)$-invariant norm on $\pi_{alg} \otimes \pi_{sm}$, which finishes the sketch of the proof.

Remark 2. To put things in perspective, $\mathscr{C}_G$ can be thought of as $\hat{H}^0_E$, a very degenerate case of Emerton's completed cohomology—developed in great generality in [19]. Let $H^0(K)_{\mathscr{O}_E}$ be the set of $\mathscr{O}_E$-valued functions on the finite set $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K$. When $K \supset K'$, there is a natural pull-back map $H^0(K)_{\mathscr{O}_E} \to H^0(K')_{\mathscr{O}_E}$. Fix a tame level K^p, and take full levels of the form $K = K_p K^p$, with $K_p \to 1$. The direct limit $\varinjlim_{K_p} H^0(K_p K^p)_{\mathscr{O}_E}$ is no longer ϖ_E-adically complete, so we consider its completion:

$$\hat{H}^0_{\mathscr{O}_E}(K^p) = (\varinjlim_{K_p} H^0(K_p K^p)_{\mathscr{O}_E})^\wedge, \quad \hat{H}^0_{\mathscr{O}_E} = \varinjlim_{K^p} \hat{H}^0_{\mathscr{O}_E}(K^p).$$

Thus $\hat{H}^0_{\mathscr{O}_E}$ is the unit ball in a Banach E-space $\hat{H}^0_E$, which can be identified with E-valued continuous functions on $G(\mathbb{Q})\backslash G(\mathbb{A}_f)$. Alternatively, $\hat{H}^0_{\mathscr{O}_E}(K^p)$ can be thought of as

$$\tilde{H}^0_{\mathscr{O}_E}(K^p) := \varinjlim_{K_p} \varprojlim_{s>0} H^0(K_p K^p)_{\mathscr{O}_E/\varpi_E^s \mathscr{O}_E}.$$

Indeed, the natural map $\hat{H}^0_{\mathscr{O}_E}(K^p) \to \tilde{H}^0_{\mathscr{O}_E}(K^p)$ is an isomorphism (see [19]).

5 The Automorphic Case: Local-Global Compatibility at *p*

The argument in Step 3 of Sect. 4.1 shows the following: If $G_{/\mathbb{Q}}$ is a *reductive* group, which is *compact* at infinity, and Π is an automorphic representation of $G(\mathbb{A})$ with $\Pi_\infty = \pi_{alg}$ and $\Pi_p = \pi_{sm}$, then $\pi_{alg} \otimes_E \pi_{sm}$ admits a $G(\mathbb{Q}_p)$-invariant norm.

We will apply this observation to definite unitary groups: Thus[5] $\tilde{F}/\tilde{F}^+$ is a CM extension, and B is a central simple $\tilde{F}$-algebra of dimension n^2 equipped with an anti-involution $\star$ of the second kind (which means $\star|_{\tilde{F}} = c$). Introduce $U = U(B, \star)_{/\tilde{F}^+}$ and take its restriction of scalars, $G = \mathrm{Res}_{\tilde{F}^+/\mathbb{Q}}(U)$. We assume throughout that $G(\mathbb{R}) \simeq U(n)^{\mathrm{Hom}(\tilde{F}^+, \mathbb{R})}$ is compact, and that $G(\mathbb{Q}_p)$ can be identified with $\prod_{v|p} \mathrm{GL}_n(\tilde{F}_{\tilde{v}})$ upon a choice of divisor $\tilde{v}|v$, for each place $v|p$ of $\tilde{F}^+$.

[5] We use the notation $\tilde{F}$ to distinguish it from our p-adic base field $F/\mathbb{Q}_p$.

One of the goals of the "Book Project" is to attach Galois representations to automorphic representations Π on $G(\mathbb{A})$—roughly by a base change to $\mathrm{GL}_n(\mathbb{A}_{\tilde{F}})$, descent to an indefinite unitary group U' with a Shimura variety $Sh_{U'}$, and a detailed study of the cohomology of $Sh_{U'}$. The following result is now known, due to the collaborative efforts of many people.

Theorem 5.1 ("Book Project"). *Let Π be an automorphic representation of $G(\mathbb{A})$, with Π_∞ of weight $a = (a_\tau)_{\tau \in \mathrm{Hom}(\tilde{F}^+, \mathbb{R})}$. Fix an isomorphism $\iota : \mathbb{C} \xrightarrow{\sim} \bar{\mathbb{Q}}_p$. Then there exists a unique continuous semisimple Galois representation,*

$$r_{\Pi,\iota} : \Gamma_{\tilde{F}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\tilde{F}) \longrightarrow \mathrm{GL}_n(\bar{\mathbb{Q}}_p),$$

with the following properties:

(0) $r^\vee_{\Pi,\iota} \simeq r^c_{\Pi,\iota} \otimes \epsilon_{cyc}^{n-1}$.

(1) For ***every*** *finite place v of $\tilde{F}^+$, which splits in $\tilde{F}$, and every place $w|v$,*

$$\mathrm{WD}(r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}})^{F-ss} \simeq rec_n(BC_{w|v}(\Pi_v) \otimes |\det|^{\frac{1-n}{2}}).$$

(Here $BC_{w|v}$ denotes "base change" from $U(\tilde{F}^+_v)$ to $\mathrm{GL}_n(\tilde{F}_w)$.)

(2) $r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}}$ is potentially semistable for every $w|p$, with Hodge-Tate weights

$$\mathrm{HT}_\tau(r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}}) = \{a_{\tau,j} + (n-j) : j = 1, \ldots, n\},$$

for $\tau : \tilde{F}_w \hookrightarrow \bar{\mathbb{Q}}_p$. Here our convention is that $\mathrm{HT}_\tau(\epsilon_{cyc}) = \{-1\}$.

Remark 3. In this Theorem, rec_n denotes the (classical) local Langlands correspondence for $\mathrm{GL}_n(\tilde{F}_w)$, normalized as in [28]. It's a bijection between irreducible admissible representations of $\mathrm{GL}_n(\tilde{F}_w)$ (over $\mathbb{C} \simeq \bar{\mathbb{Q}}_p$) and Frobenius-semisimple n-dimensional Weil-Deligne representations for $\tilde{F}_w$. The latter are pairs (r, N) consisting of a (nilpotent) monodromy operator N and a *semisimple* representation r of the Weil group $W_{\tilde{F}_w}$, with open kernel. They naturally arise from potentially semistable p-adic representations of $\Gamma_{\tilde{F}_w}$. When $w \nmid p$, every continuous representation is potentially semistable, and (r, N) is given by a simple formula (see [39] for details). For $w|p$ the associated (r, N) is more complicated to define, and involves Fontaine's period ring B_{dR} (see [24] for details). The Weil-representation r may not be semisimple; the *Frobenius*-semisimplification is defined to be $(r, N)^{F-ss} = (r^{ss}, N)$.

What is important to us here is the "local-global compatibility" in part (1) at the places v *dividing* p. This was proved in [2] and [3] under a certain regularity assumption, which was later removed in [12].

In [38] the author pushed the ideas from Sect. 4.1 further, combining them with Theorem 5.1, part (1) above p. A bit of book-keeping yielded the result below.

Corollary 5.2 (S). *Conjecture 3.2 holds for $\rho = r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}}$, for any place $w|p$ of $\tilde{F}$.*

The implied norm on $\mathrm{BS}(\rho)$ comes from a $G(\mathbb{Q}_p)$-equivariant embedding

$$\bigotimes_{v|p} \mathrm{BS}(r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_{\tilde{v}}}}) \hookrightarrow \mathscr{C}_G = \{G(\mathbb{Q})\backslash G(\mathbb{A}_f) \xrightarrow{cts.} \bar{\mathbb{Q}}_p\}, \tag{3}$$

obtained as in Sect. 4.1. Here the tensor product is viewed as a representation of $G(\mathbb{Q}_p)$ via the selection of places $\{\tilde{v}\}_{v|p}$. The speculation aired in [38] is that the closure of the image of (3) ought to be "closely related" to $\hat{\otimes}_{v|p}\Pi(r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_{\tilde{v}}}})$, where $\Pi(\cdot)$ should be the p-adic local Langlands correspondence for GL_n, if it exists. (At least if all the restrictions $r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_{\tilde{v}}}}$ are irreducible.)

One can make this more precise: Given an automorphic representation Π as in Theorem 5.1, there is the associated Galois representation $r_{\Pi,\iota}$ of $\Gamma_{\tilde{F}}$, which we can restrict to the various decomposition groups at p—resulting in the collection $\{r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}}\}_{w|p}$. On the other hand, the argument in Sect. 4 ("Step 3") yields a *canonical* $G(\mathbb{A}_f)$-invariant norm on $(\pi_{alg}\otimes\pi_{sm})\otimes\Pi_f^p$—using the now known result that $m_G(\Pi) = 1$. For each choice of vector $0 \neq x \in \Pi_f^p$, this gives rise to a $G(\mathbb{Q}_p)$-invariant norm $\|\cdot\|_x$ on $\pi_{alg}\otimes\pi_{sm}$, by restriction. Since Π_f^p is irreducible, it is easy to see that all these $\|\cdot\|_x$ define the same topology. Thus we may also attach to Π (and ι) a unitary Banach space representation of $G(\mathbb{Q}_p)$, namely the completion $B_{\Pi,\iota} = (\pi_{alg}\otimes\pi_{sm})^\wedge$. It is natural to speculate that $B_{\Pi,\iota}$ only depends on $\{r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}}\}_{w|p}$. That is, for two automorphic Π and Π' as above, it is natural to ask whether or not

$$r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_w}} \simeq r_{\Pi',\iota}|_{\Gamma_{\tilde{F}_w}}, \forall w|p \overset{?}{\Longrightarrow} B_{\Pi,\iota} \simeq B_{\Pi',\iota},$$

and perhaps even conversely—under favorable circumstances. This seems to be a very hard question, which lies at the very heart of extending the p-adic local Langlands correspondence to GL_n.

Another speculation in [38] was how these things vary across the eigenvariety $X = X_G$, of some fixed tame level K^p. On one hand, each point $x \in X(E)$ defines a pseudo-representation $t_x : \Gamma_{\tilde{F}} \to E$. On the other, one has the Hecke eigenspace $\mathscr{C}^{K^p}_{G,x}$, which is a Banach-Hecke module over E with a unitary $G(\mathbb{Q}_p)$-action. This way X parametrizes a bijection $t_x \leftrightarrow \mathscr{C}^{K^p}_{G,x}$, which we like to think of as some sort of p-adic "global" Langlands correspondence.

6 Patching and p-Adic Local Langlands

Recently there has been spectacular progress on Conjecture 3.2 in the principal series case, which is the deepest, by joint work of Caraiani, Emerton, Gee, Geraghty, Paškūnas, and Shin. In the preprint [13], using global methods, they construct a

candidate $\Pi(\rho)$ for a p-adic local Langlands correspondence for $\mathrm{GL}_n(F)$, and are able to say enough about it to prove new cases of Conjecture 3.2. The following is their Theorem 5.3 (a less precise version of which is Theorem B in their introduction).

Theorem 6.1 (Caraiani, Emerton, Gee, Geraghty, Paškūnas, and Shin). *Suppose $p \nmid 2n$. Let $\rho : \Gamma_F \to \mathrm{GL}_n(E)$ be a generic potentially **crystalline** representation, of regular weight. If ρ lies on an automorphic component of the corresponding potentially crystalline deformation ring $R^{\square}_{\tilde{\mathfrak{p}}}(\sigma)[1/p]$, then $\mathrm{BS}(\rho)$ admits a nonzero unitary admissible Banach completion.*

The conclusion is a little stronger than just the existence of a norm on $\mathrm{BS}(\rho)$, in that it asserts admissibility. They refer to it as "folklore" that every regular de Rham representation ρ should lie on an automorphic component. Thus they reduce Conjecture 3.2 to standard expectations in the automorphy lifting world. It should be emphasized that this condition is much weaker than saying ρ comes from an automorphic form (as in Corollary 5.2). It roughly says that it lies on the same *component* as some $r_{\Pi,\iota}|_{\Gamma_{\tilde{F}_{\tilde{\mathfrak{p}}}}}$ (identifying $\tilde{F}_{\tilde{\mathfrak{p}}} \simeq F$)—in turn more restrictive than saying the reduction $\bar{\rho}$ is automorphic. In some situations one can check this hypothesis, employing the available automorphy lifting theorems. See Corollary 5.4 on "potentially diagonalizable" ρ in [13], and their Corollary 5.5—which we quote:

Corollary 6.2 (—). *Suppose $p > 2$. Let $\rho : \Gamma_F \to \mathrm{GL}_n(E)$ be a generic potentially semistable representation, of regular weight. Further, assume that **either***

*(1) $n = 2$, and ρ is potentially Barsotti-Tate, **or***
(2) $F/\mathbb{Q}_p$ is unramified, ρ is crystalline, $p \neq n$, and the Hodge-Tate weights of ρ are in the "extended Fontaine-Laffaille range" (meaning the difference of any two weights in $\mathrm{HT}_\tau(\rho)$ is at most $p-1$).

Then $\mathrm{BS}(\rho)$ admits a nonzero unitary admissible Banach completion.

As hinted at already, they actually construct a candidate $\Pi(\rho)$ for p-adic local Langlands and verify (under the given hypotheses) that $\mathrm{BS}(\rho) \hookrightarrow \Pi(\rho)$. Moreover, they express optimism in [13], Remark 5.8, that $\mathrm{BS}(\rho)$ coincides with the space of locally algebraic vectors $\Pi(\rho)^{alg}$—evidence that $\Pi(\rho)$ is "purely local" although it is defined via choices of auxiliary global data. Convincing evidence for *Shimura curves* is provided by Emerton et al. [22].

The definition of $\Pi(\rho)$ in [13] is based on their "hypothetical formulation" of p-adic local Langlands in Sect. 6.1: Given a representation $\bar{\rho} : \Gamma_F \to \mathrm{GL}_n(k_E)$ with $\mathrm{End}_{\Gamma_F}(\bar{\rho}) = k_E$ (for simplicity) there should be a finitely generated $R_{\bar{\rho}}[[\mathrm{GL}_n(\mathcal{O})]]$-module L_∞, which is $\mathcal{O}_E$-torsion free, and such that the $\mathrm{GL}_n(\mathcal{O})$-action can be *promoted* to an $R_{\bar{\rho}}$-linear action of the full $\mathrm{GL}_n(F)$. Then p-adic local Langlands $\rho \rightsquigarrow B(\rho)$ should arise from specializing L_∞ as follows. Say $\rho : \Gamma_F \to \mathrm{GL}_n(\mathcal{O}_E)$ is a lift of $\bar{\rho}$, corresponding to a point $x \in (\mathrm{Spec} R_{\bar{\rho}})(\mathcal{O}_E)$. Then,

$$B(\rho) = (L_\infty \otimes_{R_{\bar\rho},x} \mathscr{O}_E)^d[1/p],$$

where d denotes taking the (Schikhof) dual[6] $\mathrm{Hom}^{cts.}_{\mathscr{O}_E}(-, \mathscr{O}_E)$. When $\mathrm{End}_{\Gamma_F}(\bar\rho) \neq k_E$ one would replace $R_{\bar\rho}$ by the universal framed deformation ring $R^{\square}_{\bar\rho}$, and L_∞ should be endowed with additional structure (see the footnote on p. 45 of [13]).

The construction in [13] starts off from a $\bar\rho : \Gamma_F \to \mathrm{GL}_n(k_E)$, which admits a "potentially diagonalizable" lift $\rho_{p.d.}$ to $\mathscr{O}_E$. This assumptions allows them to pass to a global setup (cf. Sect. 5 above), and suitably extend $\bar\rho$ to a representation $\Gamma_{\tilde F} \to \mathrm{GL}_n(k_E)$. Carrying out a delicate variant of the Taylor-Wiles-Kisin patching method for modular forms on G, but letting the weight and the p-part of the level vary, they construct an $R_\infty[[\mathrm{GL}_n(\mathscr{O})]]$-module M_∞ (defined on p. 15 in loc. cit.), where R_∞ is a multivariate power series ring over some local deformation ring R^{loc} (rather, a tensor product of such). Proposition 2.8 in loc. cit. establishes the key fact that the $\mathrm{GL}_n(\mathscr{O})$-action on M_∞ extends naturally to a $\mathrm{GL}_n(F)$-action.

Now, if $\rho : \Gamma_F \to \mathrm{GL}_n(\mathscr{O}_E)$ is a lift of $\bar\rho$, the definition of $\Pi(\rho)$ proceeds in the following steps: Under the identification $F \simeq \tilde F_{\tilde{\mathfrak{p}}}$ our lift ρ corresponds to a point $x : R^{\square}_{\tilde{\mathfrak{p}}} \to \mathscr{O}_E$, which we extend to a point $x' : R^{loc} \to \mathscr{O}_E$, using the given lift $\rho_{p.d.}$ at the places in S_p away from $\mathfrak{p}$. We extend x' further, and arbitrarily, to a homomorphism $y : R_\infty \to \mathscr{O}_E$. Recall that $R_\infty \simeq R^{loc}[[x_1, \ldots, x_N]]$. Then,

$$\Pi(\rho) := (M_\infty \otimes_{R_\infty,y} \mathscr{O}_E)^d[1/p].$$

(See Sect. 2.10, p. 19 in [13].) It should be stressed that $\Pi(\rho)$ is *not* known to be independent of the "globalization", nor the choice of extension y. Furthermore, in general it is not known whether $\Pi(\rho) \neq 0$.

In Sect. 6.2 of [13] they speculate that $M_\infty \overset{?}{=} R_\infty \otimes_{R_{\bar\rho}} L_\infty$.

Acknowledgements I would like to thank the organizers of CNTA XIII for a wonderful event in beautiful Ottawa, and for the opportunity to speak there. S.W. Shin read an early draft of this paper, and made comments; his feedback is greatly appreciated—as is the thorough reading of the anonymous referee.

References

1. E. Assaf, D. Kazhdan, E. de Shalit, Kirillov models and the Breuil-Schneider conjecture for $\mathrm{GL}_2(F)$. arXiv:1302.3060 (2013)
2. T. Barnet-Lamb, T. Gee, D. Geraghty, R. Taylor, Local-global compatibility for l=p, I. Ann. Fac. Sci. Toulouse Math. (6) **21**(1), 57–92 (2012)
3. T. Barnet-Lamb, T. Gee, D. Geraghty, R. Taylor, Local-global compatibility for l=p, II. Ann. Sci. École Norm. Supérieure (4) **47**(1), 165–179 (2014)

[6] An anti-equivalence between compact $\mathscr{O}_E$-modules and ϖ_E-adically *complete* $\mathscr{O}_E$-modules.

4. L. Berger, C. Breuil, Sur quelques representations potentiellement cristallines de $GL_2(\mathbb{Q}_p)$. Asterisque **330**, 155–211 (2010)
5. L. Berger, La correspondance de Langlands locale p-adique pour $GL_2(\mathbb{Q}_p)$, in *Seminaire Bourbaki*, vol. 2009/2010. Exposes 1012–1026. Asterisque, vol. 339, Exp. No. 1017 (2011), viii, 157–180
6. C. Breuil, Invariant $\mathscr{L}$ et série spéciale p-adique. Ann. Sci. École Norm. Supérieure (4) **37**(4), 559–610 (2004)
7. C. Bushnell, G. Henniart, The local Langlands conjecture for GL(2), in *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, vol. 335 (Springer, Berlin, 2006)
8. G. Böckle, On the density of modular points in universal deformation spaces. Am. J. Math. **123**(5), 985–1007 (2001)
9. A. Borel, G. Harder, Existence of discrete cocompact subgroups of reductive groups over local fields. J. Reine Angew. Math. **298**, 53–64 (1978)
10. C. Breuil, P. Schneider, First steps towards p-adic Langlands functoriality. J. Reine Angew. Math. **610**, 149–180 (2007)
11. C. Breuil, The emerging p-adic Langlands programme, in *Proceedings of the International Congress of Mathematicians*, vol. II (Hindustan Book Agency, New Delhi, 2010), pp. 203–230
12. A. Caraiani, Local-global compatibility and the action of monodromy on nearby cycles. Duke Math. J. **161**(12), 2311–2413 (2012)
13. A. Caraiani, M. Emerton, T. Gee, D. Geraghty, V. Paškūnas, S.W. Shin, *Patching and the p-adic local Langlands correspondence*. Preprint (2013)
14. L. Clozel, P. Delorme, Le theoreme de Paley-Wiener invariant pour les groupes de Lie reductifs. Invent. Math. **77**(3), 427–453 (1984)
15. L. Clozel, On limit multiplicities of discrete series representations in spaces of automorphic forms. Invent. Math. **83**(2), 265–284 (1986)
16. P. Colmez, G. Dospinescu, V. Paskunas, The p-adic local Langlands correspondence for $GL_2(\mathbb{Q}_p)$. Camb. J. Math. **2**, 1–47 (2014)
17. D. de George, N. Wallach, Limit formulas for multiplicities in $L^2(\Gamma\backslash G)$. Ann. Math. (2) **107**(1), 133–150 (1978)
18. M. De Ieso, Existence de normes invariantes pour GL_2. J. Number Theory **133**(8), 2729–2755 (2013)
19. M. Emerton, On the interpolation of systems of eigenvalues attached to automorphic Hecke eigenforms. Invent. Math. **164**(1), 1–84 (2006)
20. M. Emerton, Jacquet modules of locally analytic representations of p-adic reductive groups, I. Construction and first properties. Ann. Sci. École Norm. Supérieure (4) **39**(5), 775–839 (2006)
21. M. Emerton, Local-global compatibility in the p-adic Langlands programme for GL_2 /$\mathbb{Q}$ (Draft dated March 23, 2011). Available at http://www.math.uchicago.edu/~emerton/preprints.html
22. M. Emerton, T. Gee, D. Savitt, Lattices in the cohomology of Shimura curves. Invent. Math. Invent. Math. **200**(1), 1–96 (2015)
23. J.-M. Fontaine, B. Mazur, Geometric Galois representations, in *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, Hong Kong, 1993. Number Theory, vol. I (International Press, Cambridge, 1995), pp. 41–78
24. J.-M. Fontaine, Représentations p-adiques, in *Proceedings of the International Congress of Mathematicians*, Warsaw, 1983, vols. 1, 2 (PWN, Warsaw, 1984), pp. 475–486
25. J.-M. Fontaine, M. Rapoport, Existence de filtrations admissibles sur des isocristaux. Bull. Soc. Math. Fr. **133**(1), 73–86 (2005)
26. B. Gross, Algebraic modular forms. Isr. J. Math. **113**, 61–93 (1999)
27. E. Grosse-Klonne, On the universal module of p-adic spherical Hecke algebras. Am. J. Math. **136**(3), 599–652 (2014)
28. M. Harris, R. Taylor, *The Geometry and Cohomology of Some Simple Shimura Varieties*. With an Appendix by Vladimir G. Berkovich. Annals of Mathematics Studies, vol. 151 (Princeton University Press, Princeton, 2001)

29. Y. Hu, Normes invariantes et existence de filtrations admissibles. J. Reine Angew. Math. **634**, 107–141 (2009)
30. D. Kazhdan, E. de Shalit, Kirillov models and integral structures in p-adic smooth representations of $GL_2(F)$. J. Algebra **353**, 212–223 (2012)
31. S. Kudla, The local Langlands correspondence: the non-Archimedean case, in *Motives*, Seattle, 1991. Proceedings of Symposia in Pure Mathematics, vol. 55, Part 2 (American Mathematical Society, Providence, 1994), pp. 365–391
32. C. Khare, J.-P. Wintenberger, Serre's modularity conjecture, in *Proceedings of the International Congress of Mathematicians*, vol. II (Hindustan Book Agency, New Delhi, 2010), pp. 280–293
33. P. Schneider, *Nonarchimedean Functional Analysis*. Springer Monographs in Mathematics (Springer, Berlin, 2002), vi+156 pp.
34. P. Schneider, *Continuous Representation Theory of p-Adic Lie Groups*. International Congress of Mathematicians, vol. II (European Mathematical Society, Zurich, 2006), pp. 1261–1282
35. P. Schneider, J. Teitelbaum, Banach-Hecke algebras and p-adic Galois representations. Doc. Math. Extra Vol., 631–684 (2006)
36. A. Scholl, Motives for modular forms. Invent. Math. **100**(2), 419–430 (1990)
37. C. Sorensen, A proof of the Breuil-Schneider conjecture in the indecomposable case. Ann. Math. (2) **177**(1), 367–382 (2013)
38. C. Sorensen, Eigenvarieties and invariant norms. Pac. J. Math. **275**(1), 191–230 (2015)
39. J. Tate, Number theoretic background, in *Automorphic Forms, Representations and L-Functions* (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, 1977), Part 2. Proceedings of Symposia in Pure Mathematics, XXXIII (American Mathematical Society, Providence, 1979), pp. 3–26
40. M.-F. Vigneras, A criterion for integral structures and coefficient systems on the tree of PGL(2,F). Pure Appl. Math. Q. **4**(4), (2008) [Special Issue: In honor of Jean-Pierre Serre, Part 1, pp. 1291–1316]
41. T. Wedhorn, The local Langlands correspondence for GL(n) over p-adic fields, in *School on Automorphic Forms on GL(n)*. ICTP Lecture Notes, vol. 21 (Abdus Salam International Centre for Theoretical Physics, Trieste, 2008), pp. 237–320