ISRAEL JOURNAL OF MATHEMATICS **247** (2022), 697–739
DOI: 10.1007/s11856-021-2279-x

COUNTING MOD n IN PSEUDOFINITE FIELDS

BY

WILL JOHNSON

School of Mathematical Sciences, Fudan University
220 Handan Road, Shanghai 200433, China
e-mail: willij6@berkeley.edu

ABSTRACT

We show that in an ultraproduct of finite fields, the mod-n nonstandard size of definable sets varies definably in families. Moreover, if K is any pseudofinite field, then one can assign "nonstandard sizes mod n" to definable sets in K. As n varies, these nonstandard sizes assemble into a definable strong Euler characteristic on K, taking values in the profinite completion $\hat{\mathbb{Z}}$ of the integers. The strong Euler characteristic is not canonical, but depends on the choice of a nonstandard Frobenius. When $\mathrm{Abs}(K)$ is finite, the Euler characteristic has some funny properties for two choices of the nonstandard Frobenius.

Additionally, we show that the theory of finite fields remains decidable when first-order logic is expanded with parity quantifiers. However, the proof depends on a computational algebraic geometry statement whose proof is deferred to a later paper.

Received December 18, 2019 and in revised form December 5, 2020

1. Introduction

1.1. Euler characteristics. Let M be a structure and R be a ring. Let $\mathrm{Def}(M)$ denote the collection of (parametrically) definable sets in M. Recall the following definitions from [18] and [19]. An **R-valued Euler characteristic** is a function $\chi : \mathrm{Def}(M) \to R$ such that

- $\chi(\emptyset) = 0$,
- $\chi(X) = 1$ if X is a singleton,
- $\chi(X) = \chi(Y)$ if X and Y are in definable bijection,
- $\chi(X \times Y) = \chi(X) \cdot \chi(Y)$,
- $\chi(X \cup Y) = \chi(X) + \chi(Y)$ if X and Y are disjoint.

If the following additional property holds, then χ is called a **strong** Euler characteristic:

- If $f : X \to Y$ is a definable function and there is an $r \in R$ such that $\chi(f^{-1}(y)) = r$ for all y, then
$$\chi(X) = r \cdot \chi(Y).$$

For $A \subseteq M$, we say that χ is **A-definable** if the following holds:

- For any B-definable function $f : X \to Y$, let $Y_r = \{y \in Y : \chi(f^{-1}(y)) = r\}$. Then each Y_r is AB-definable, and all but finitely many Y_r are empty.[1]

We say that χ is **definable** if it is M-definable. For examples of Euler characteristics, see [18, §3, §5].

1.2. Pseudofinite Euler characteristics. A structure is **pseudofinite** if it is infinite, yet elementarily equivalent to an ultraproduct of finite structures. Pseudofinite structures have strong Euler characteristics arising from counting mod n. More precisely, if M is an ultraproduct of finite structures, there is a canonical strong Euler characteristic $\chi_n : \mathrm{Def}(M) \to \mathbb{Z}/n\mathbb{Z}$ defined in the following way. Let M be the ultraproduct $\prod_{i \in I} M_i/\mathcal{U}$, and $X = \phi(M; a)$ be a definable set. Choose a tuple $\langle a_i \rangle_{i \in I} \in \prod_{i \in I} M_i$ representing a. Then define $\chi_n(X) \in \mathbb{Z}/n\mathbb{Z}$ to be the ultralimit along $\mathcal{U}$ of the sequence
$$\langle |\phi(M_i; a_i)| + n\mathbb{Z} \rangle_{i \in I},$$
This ultralimit exists because $\mathbb{Z}/n\mathbb{Z}$ is finite. The resulting χ_n is a $\mathbb{Z}/n\mathbb{Z}$-valued strong Euler characteristic, not necessarily definable.

[1] This latter condition is automatic when M is $|R|^+$-saturated.

On an ultraproduct M of finite structures, these χ_n maps are compatible in the sense that the following diagram commutes when n divides m:

$$\begin{array}{ccc} \mathrm{Def}(M) & \xrightarrow{\chi_m} & \mathbb{Z}/m\mathbb{Z} \\ & \searrow^{\chi_n} & \downarrow \\ & & \mathbb{Z}/n\mathbb{Z} \end{array}$$

Consequently, they assemble into a map

$$\hat{\chi} : \mathrm{Def}(M) \to \hat{\mathbb{Z}},$$

where $\hat{\mathbb{Z}}$ is the ring $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$. Morally, $\hat{\chi}$ is a strong $\hat{\mathbb{Z}}$-valued Euler characteristic. If M is any structure, we will say that a map $\chi : \mathrm{Def}(M) \to \hat{\mathbb{Z}}$ is

(1) an **Euler characteristic** if all the compositions $\mathrm{Def}(M) \to \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ are Euler characteristics,
(2) a **strong** Euler characteristic if all the compositions $\mathrm{Def}(M) \to \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ are strong Euler characteristics,
(3) a **definable** Euler characteristic if all compositions $\mathrm{Def}(M) \to \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ are definable Euler characteristics.

For 2 and 3, this is an abuse of terminology.

We can repeat the discussion above with the p-adics $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ instead of $\hat{\mathbb{Z}}$. Recall that by the Chinese remainder theorem

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Giving an Euler characteristic $\hat{\chi} : \mathrm{Def}(M) \to \hat{\mathbb{Z}}$ is therefore equivalent to giving an Euler characteristic $\chi_p : \mathrm{Def}(M) \to \mathbb{Z}_p$ for every p. Moreover, $\hat{\chi}$ is strong or definable if and only if every χ_p is strong or definable, respectively.

1.3. Main results for pseudofinite fields. By a theorem of Ax [2], a field K is pseudofinite if and only if K satisfies the following three conditions:

- K is perfect,
- K is pseudo-algebraically closed: every geometrically integral variety over K has a K-point,
- $\mathrm{Gal}(K) \cong \hat{\mathbb{Z}}$, or equivalently, K has a unique field extension of degree n for each n.

Our first main result can be phrased purely in terms of pseudofinite fields.

THEOREM 1.1:

(1) *Let $K = \prod_i K_i/\mathcal{U}$ be an ultraproduct of finite fields. Then the nonstandard counting functions χ_n are $\mathrm{acl}^{eq}(\emptyset)$-definable.*
(2) *Every pseudofinite field admits an $\mathrm{acl}^{eq}(\emptyset)$-definable $\hat{\mathbb{Z}}$-valued strong Euler characteristic.*

We make several remarks:

(1) In Part 1, the $\mathrm{acl}^{eq}(\emptyset)$ is necessary: the nonstandard counting function is known to not be $\emptyset$-definable [18, Theorem 7.3].
(2) In Part 2, the Euler characteristic is not canonical, but depends on a choice of a topological generator $\sigma \in \mathrm{Gal}(K)$.

One approach to proving Theorem 1.1 would be to use étale cohomology. (See Conjecture 6.3 and the following discussion.) We will give a more elementary proof using abelian varieties and jacobians of curves.

Aside from Theorem 1.1, there is also a decidability theorem in terms of generalized parity quantifiers. For any $n \in \mathbb{N}$ and $k \in \mathbb{Z}/n\mathbb{Z}$, let $\mu^n_k x$ be a new quantifier. Interpret $\mu^n_k x : \phi(x)$ in finite structures as

The number of x such that $\phi(x)$ holds is congruent to k mod n.

In other words,

$$(M \models \mu^n_k \vec{x} : \phi(\vec{x}, \vec{b})) \iff (|\{\vec{a} : M \models \phi(\vec{a}, \vec{b})\}| \equiv k \pmod{n}).$$

For example, $\mu^2_1 x$ means "there are an odd number of x such that ..." We call μ^n_k a **generalized parity quantifier**.

Let $\mathcal{L}^{\mu}_{\mathrm{rings}}$ be the language of rings expanded with generalized parity quantifiers.

THEOREM 1.2: *Assuming Conjecture 5.2, the $\mathcal{L}^{\mu}_{\mathrm{rings}}$-theory of finite fields is decidable.*

Unfortunately, this result is conditional on Conjecture 5.2, a technical statement about definability in algebraic geometry. While the conjecture is certainly true, it is hard to give a sane proof. A complete proof will (hopefully) appear in future work [16].

1.4. MAIN RESULTS FOR PERIODIC DIFFERENCE FIELDS. The results of §1.3 can be stated more precisely in terms of difference fields. Recall that a **difference field** is a pair (K, σ) where K is a field and σ is an automorphism of K.

Definition 1.3: A difference field (K, σ) is **periodic** if every element of K has finite orbit under σ.

Periodic difference fields are not an elementary class in the language of difference fields. However, they constitute an elementary class when regarded as multi-sorted structures $(K_1, K_2, \ldots)$ where K_i is the fixed field of σ^i, with the following structure:

- The difference-field structure on each K_i.
- The inclusion map $K_n \to K_m$ for each pair n, m with n dividing m.

These multi-sorted structures were considered by Hrushovski in [14], and we will give an overview of their basic properties in §3 below.

To highlight the fact that we are no longer working in the language of difference fields, we will call these structures **periodic fields**. If $(K_1, K_2, \ldots)$ is a periodic field, we let K_∞ denote the associated periodic difference field

$$K_\infty = \varinjlim_n K_n.$$

We will abuse notation and write (K_∞, σ) when we really mean the associated periodic field $(K_1, K_2, \ldots)$.

For any q, let Fr^q denote $(\mathbb{F}_q^{\mathrm{alg}}, \phi_q)$, where ϕ_q is the qth power Frobenius. Thus $(\mathrm{Fr}^q)_n = (\mathbb{F}_{q^n}, \phi_q)$. We will call the Fr^q's **Frobenius periodic fields**. Frobenius periodic fields are "essentially finite" (every sort is finite). Consequently, ultraproducts of Frobenius periodic fields admit $\mathbb{Z}/n\mathbb{Z}$-valued strong Euler characteristics χ_n.

There is a theory ACPF whose class of models can be described in several ways:

(1) The existentially closed periodic fields.
(2) The non-Frobenius periodic fields satisfying the theory of Frobenius periodic fields.
(3) The periodic fields of the form $(K^{\mathrm{alg}}, \sigma)$, where K is pseudofinite and σ is a topological generator of $\mathrm{Gal}(K)$.

(See Propositions 3.2, 3.15, and 3.4, respectively.) In particular, ACPF is the model companion of periodic fields, and non-principal ultraproducts of Frobenius periodic fields are models of ACPF.[2]

[2] The situation is analogous to, but much simpler than, the situation with ACFA [15].

Theorem 1.1 has the following analogue for periodic fields:

THEOREM 1.4: *Let $\mathcal{C}$ be the class of Frobenius periodic fields and existentially closed periodic fields. There is a $\hat{\mathbb{Z}}$-valued strong Euler characteristic χ on (K, σ) in $\mathcal{C}$ with the following properties:*

- *χ is uniformly $\emptyset$-definable across $\mathcal{C}$.*
- *If (K, σ) is a Frobenius periodic field, then χ is the counting Euler characteristic:*

$$\chi(X) = |X|.$$

- *If (K, σ) is an ultraproduct of Frobenius periodic fields, then χ is the nonstandard counting Euler characteristic.*

There are also statements in terms of parity quantifiers. Let $\mathcal{L}_{pf}$ be the first-order language of periodic fields, and let $\mathcal{L}_{pf}^{\mu}$ be its expansion by generalized parity quantifiers.

THEOREM 1.5:

(1) Generalized parity quantifiers are uniformly eliminated on the class of Frobenius periodic fields.
(2) Assuming Conjecture 5.2, the $\mathcal{L}_{pf}^{\mu}$-theory of Frobenius periodic fields is decidable.

This statement is stronger than what we can say about finite and pseudofinite fields. In fact, generalized parity quantifiers are not uniformly eliminated on finite fields (Lemma 6.8).

1.5. A SPECIAL CASE. If p is a prime, let $\mathbb{Z}_{\neg p}$ be the prime-to-p completion of $\mathbb{Z}$:

$$\mathbb{Z}_{\neg p} = \varprojlim_{(n,p)=1} \mathbb{Z}/n\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_{\ell}.$$

If K is a field, let $\mathrm{Abs}(K)$ denote the subfield of **absolute numbers**, i.e., the relative algebraic closure of the prime field. Say that a field K is a **mock-$\mathbb{F}_q$** if K is pseudofinite and $\mathrm{Abs}(K) \cong \mathbb{F}_q$. For each prime power q, there is a unique mock-$\mathbb{F}_q$ up to elementary equivalence, by work of Ax [2, Theorems 4 and 6].

The nonstandard Euler characteristics behave in a funny way on mock-$\mathbb{F}_q$'s:

THEOREM 1.6: *Let K be a mock-$\mathbb{F}_q$, for some prime power $q = p^k$. There are two $\mathbb{Z}_{\neg p}$-valued $\emptyset$-definable strong Euler characteristics χ and $\chi^\dagger$ on K, such that:*

(1) *If V is a smooth projective variety over $\mathbb{F}_q$, then*

$$\chi(V(K)) = |V(\mathbb{F}_q)|,$$
$$\chi^\dagger(V(K)) = |V(\mathbb{F}_q)|/q^{\dim V}.$$

(2) *If X is any $\mathbb{F}_q$-definable set, then*

$$\chi(X) = |X \cap \operatorname{dcl}(\mathbb{F}_q)|.$$

In particular, $\chi(X) \in \mathbb{Z}$.

(3) *If X is any $\mathbb{F}_q$-definable set, then $\chi^\dagger(X) \in \mathbb{Q}$.*

1.6. RELATED WORK. Many people have considered non-standard sizes of definable sets in pseudofinite fields [1, 5, 8, 18, 19]. Non-standard sizes modulo p were considered by Krajíček, who used them to prove the existence of non-trivial strong Euler characteristics on pseudofinite fields [18]. However, most research has focused on ordered Euler characteristics ([1, 19]) and the real standard part of non-standard sizes ([5, 8]). These topics can be seen as "non-standard sizes modulo the infinite prime."

Dwork [7] and Kiefe [17] consider the behavior of $|\phi(\mathbb{F}_q)|$ as q varies. Their work can be used to calculate the non-standard mod-n sizes of $\emptyset$-definable sets in pseudofinite fields of positive characteristic.

There are several variations on the notion of an Euler characteristic. One can consider an Euler characteristic $\chi(D)$ defined only for $\emptyset$-definable sets D. (In this setting, it no longer makes sense to talk about strong or definable Euler characteristics.) More generally, if T is an incomplete theory, one can consider Euler characteristics defined on the class of definable functors (i.e., formulas up to logical equivalence). If k is a field of characteristic 0 and T is the theory of pseudofinite fields extending k, then Denef and Loeser define such an Euler characteristic on formulas, taking values in $K_0(\mathrm{Mot}_{k,\mathbb{Q}^{\mathrm{alg}}}) \otimes \mathbb{Q}$, where $K_0(\mathrm{Mot}_{k,\mathbb{Q}^{\mathrm{alg}}})$ is a certain Grothendieck group of Chow motives [6, Proposition 3.4.4]. The Denef–Loeser Euler characteristic should be closely related to ours; see Remark 6.4.

Almost everything in §3 is well-known to experts. The results specific to periodic fields appear in Hrushovski's paper [14].

1.7. NOTATION. If K is a field, then K^{alg} (resp. K^{sep}) denotes the algebraic (resp. separable) closure, and $\mathrm{Gal}(K)$ denotes the absolute Galois group

$$\mathrm{Gal}(K^{\mathrm{sep}}/K) = \mathrm{Aut}(K^{\mathrm{sep}}/K).$$

We let

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

denote the profinite completion of $\mathbb{Z}$. The finite field with q elements is denoted $\mathbb{F}_q$.

A **variety** over K is a finite-type separated reduced scheme over K, not necessarily irreducible or quasi-projective. If V is a variety, then $V(K)$ denotes the set of K-points of V. A scheme X over K is **geometrically integral** or **geometrically irreducible** if $X \times_K K^{\mathrm{alg}}$ is integral or irreducible. A **curve** over K is a geometrically integral 1-dimensional smooth projective variety over K.

Remark 1.7: If K is a perfect field and V is a variety, then geometrically irreducible is equivalent to geometrically integral.

ACKNOWLEDGMENT. The author would like to thank Tianyi Xu, for helpful discussions about recursive ind-definability, Tom Scanlon, who read an earlier version of this paper appearing in the author's dissertation, and the anonymous referee, who offered countless helpful comments and introduced the author to some of the important related papers.

This material is based upon work supported by the National Science Foundation under Grant No. DGE-1106400 and Award No. DMS-1803120. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

2. Review of abelian varieties

Let A be an abelian variety over some field K. For any $n \in \mathbb{N}$, let $A[n]$ denote the group of n-torsion in $A(K^{\mathrm{alg}})$, viewed as an abelian group with $\mathrm{Gal}(K)$-action. Let $T_\ell A$ denote the ℓth Tate module [21, §18]. If $g = \dim A$, then there

are non-canonical isomorphisms

$$T_\ell A \approx \mathbb{Z}_\ell^{2g}$$

for all $\ell \neq \mathrm{char}(K)$. In particular, $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. If $p = \mathrm{char}(K)$, then

$$T_p A \approx \mathbb{Z}_p^r$$

for some r known as the **p-rank** of A. The p-rank is at most g. Similar statements hold for the torsion subgroups:

$$A[\ell^k] \approx (\mathbb{Z}/\ell^k)^{2g}, \qquad \ell \neq \mathrm{char}(K);$$
$$A[p^k] \approx (\mathbb{Z}/p^k)^r, \qquad p = \mathrm{char}(K).$$

An **isogeny** on A is a surjective endomorphism $f : A \to A$. An isogeny f has a well-defined degree $\deg(f)$, which can be described in two ways:

- The length of the scheme-theoretic kernel of f (a finite group scheme over K).
- The degree of the fraction field extension.

If $f : A \to A$ is a non-surjective endomorphism, then $\deg(f)$ is defined to be 0.

Any endomorphism $f : A \to A$ induces an endomorphism $T_\ell(f)$ on the Tate modules. We can talk about the determinant and trace of this endomorphism.

Fact 2.1 (cf. [21, Theorem 19.4] or [20, Proposition I.10.20]): *If $f : A \to A$ is any endomorphism, and $\ell \neq \mathrm{char}(K)$, then* $\deg(f) = \det T_\ell(f)$.

Corollary 2.2: *If $\alpha_1, \ldots, \alpha_{2g}$ denote the eigenvalues of $T_\ell(f)$, then for any polynomial $P(X) \in \mathbb{Z}[X]$,*

$$\deg(P(f)) = \prod_{i=1}^{2g} P(\alpha_i).$$

Because the left-hand side is an integer independent of ℓ, it follows that the α_i are algebraic numbers which do not depend on ℓ.

The numbers $\alpha_1, \ldots, \alpha_{2g}$ are called the **characteristic roots** of the endomorphism f. The characteristic roots govern the counting of points on curves over finite fields:

FACT 2.3 ([20, Theorem III.11.1]): *Let C be a curve over a finite field $\mathbb{F}_q$, and let J be its Jacobian. Then*

$$|C(\mathbb{F}_q)| = 1 - \left(\sum_{i=1}^{2g} \alpha_i\right) + q$$

where the α_i are the characteristic roots of the qth power Frobenius endomorphism $\phi_q : J \to J$.

COROLLARY 2.4: *In the setting of Theorem 2.3, if ℓ is prime-to-q, then*

$$|C(\mathbb{F}_q)| \equiv 1 - \mathrm{Tr}(\phi_q | J[\ell^k]) + \mathrm{Tr}(\phi_q | \mathbb{G}_m[\ell^k]) \pmod{\ell^k}$$

where $\mathbb{G}_m$ denotes the multiplicative group, $\mathbb{G}_m[\ell^k]$ denotes the group of ℓ^kth roots of unity (in $\mathbb{F}_q^{\mathrm{alg}}$), and $\mathrm{Tr}(\sigma|M)$ denotes the trace of an endomorphism σ of some free $\mathbb{Z}/\ell^k$-module M.

2.1. BAD CHARACTERISTIC. We would like an analogue of Corollary 2.4 in the case of bad characteristic $\ell = p$.

LEMMA 2.5: *Let $P(x)$ and $Q(x)$ be two monic polynomials in $\mathbb{Q}_p[x]$. Let $\beta_1, \ldots, \beta_m \in \mathbb{Q}_p^{\mathrm{alg}}$ be the roots of $P(x)$, and $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}_p^{\mathrm{alg}}$ be the roots of $Q(x)$. Suppose that*

$$v_p\left(\prod_{i=1}^{m} F(\beta_i)\right) \le v_p\left(\prod_{i=1}^{n} F(\alpha_i)\right) \tag{1}$$

holds for every $F(x) \in \mathbb{Z}[x]$. Then $\{\beta_1, \ldots, \beta_m\}$ is a submultiset of $\{\alpha_1, \ldots, \alpha_m\}$, i.e., $P(x)$ divides $Q(x)$.

Proof. This follows by a similar argument to [20, Lemma I.10.21]. We leave the necessary modifications as an exercise to the reader. ∎

Recall that the degree of an isogeny $f : A \to A$ is equal to the degree of the fraction field extension, and therefore factors into separable and inseparable parts:

$$\deg(f) = \deg_s(f) \cdot \deg_i(f).$$

Moreover, $\deg_s(f)$ is the size of the set-theoretic kernel of f [21, §6, Application 3].

FACT 2.6: *For any ℓ (possibly $\ell = p$),*

$$v_\ell(\det T_\ell(\phi)) = v_\ell(|\ker \phi|) = v_\ell(\deg_s(\phi)).$$

Fact 2.6 is implicit in the proof of [21, Theorem 19.4] or [20, Theorem I.10.20].

LEMMA 2.7: *Let A be an abelian variety over $\mathbb{F}_q$ for $q = p^k$. Let $\beta_1, \ldots, \beta_r$ be the eigenvalues of $T_p(\phi_q)$, for ϕ_q the qth power Frobenius on A.*

(1) *$\{\beta_1, \ldots, \beta_r\}$ is a submultiset of the characteristic roots $\{\alpha_1, \ldots, \alpha_r\}$ of ϕ_q.*
(2) *Each β_i has valuation zero in $\mathbb{Q}_p^{\mathrm{alg}}$.*

Proof. By Corollary 2.2 and Fact 2.6, the following holds for any polynomial $F(x) \in \mathbb{Z}[x]$:

$$v_p\left(\prod_{i=1}^{r} F(\beta_i)\right) = v_p(\det T_p(F(\phi_q))) = v_p(\deg_s(F(\phi_q)))$$
$$\leq v_p(\deg(F(\phi_q))) = v_p\left(\prod_{i=1}^{2g} F(\alpha_i)\right).$$

Then (1) follows by Lemma 2.5. For (2), note that the β_i are integral over $\mathbb{Z}_p$ because they are the eigenvalues of a linear map $\mathbb{Z}_p^r \to \mathbb{Z}_p^r$. Integrality implies that $v_p(\beta_i) \geq 0$. Moreover, the map $\mathbb{Z}_p^r \to \mathbb{Z}_p^r$ is invertible, because the qth power Frobenius is a bijection on points. Therefore, the β_i^{-1} are also integral, of nonnegative valuation. ∎

LEMMA 2.8: *There is a computable function $h_1(d, d', p, s)$ with the following property. Let (K, v) be an algebraically closed valued field of mixed characteristic $(0, p)$. Let $Q(x)$ be a monic polynomial of degree d, with roots $\alpha_1, \ldots, \alpha_d$. Suppose $d' \leq d$ and suppose that $v(Q(p^i)) \geq v(p^{id'})$ for $1 \leq i \leq h_1(d, d', p, s)$. Then at least d' of the α_i satisfy $v(\alpha_i) \geq v(p^s)$.*

Proof. Because ACVF is recursively enumerable, it suffices to prove that $h_1(d, d', p, s)$ exists for fixed d, d', p, s. If $h_1(d, d', p, s)$ fails to exist, then by compactness there is $(K, v) \models \mathrm{ACVF}_{0,p}$ and a monic polynomial $Q(x)$ of degree d such that

$$\forall i \in \mathbb{N} : v(Q(p^i)) \geq v(p^{id'}),$$

but fewer than d' of the roots of $Q(x)$ have valuation greater than $v(p^s)$. Let $Q(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$. Then for all but finitely many i, we have

$$id' = v(p^{id'}) \leq v(Q(p^i)) = \min_{0 \leq j \leq d} v(a_j p^{ij}) = \min_{0 \leq j \leq d} (v(a_j) + ij).$$

Therefore, $v(a_j) \geq \mathbb{N}$ for $j < d'$. By Newton polygons, at most $d - d'$ of the roots of $Q(x)$ have valuation less than $v(p^s)$, a contradiction. ∎

LEMMA 2.9: *Let G be a finite connected commutative group scheme of length n over $\mathbb{F}_q$. If $n < q$, then the qth-power Frobenius morphism $G \to G$ is the zero endomorphism.*

Proof. Well-known (and easy). ∎

FACT 2.10: *Let G be a commutative finite group scheme over a field K.*

- *Let G' be a finite subgroup scheme. Then the length of G' divides the length of G.*
- *Let G^0 denote the connected component of G. Then*

$$\ell(G^0) = \ell(G)/|G(K^{\mathrm{alg}})|.$$

The first point follows from [22, Theorems 10.5-10.7]. The second point follows by the proof of [22, Proposition 15.3].

LEMMA 2.11: *Suppose A is a g-dimensional abelian variety over $\mathbb{F}_q$. Suppose $q > p^{2gi}$. Let r be the p-rank of A. Let ϕ_q denote the qth power Frobenius endomorphism of A. Then $\deg(\phi_q - p^i)$ is divisible by $p^{i(2g-r)}$.*

Proof. Take $\ell \neq p$. By Fact 2.1, $\deg(p^i) = p^{2gi}$ because $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. Let G denote the scheme-theoretic kernel of the multiplication-by-p^i endomorphism of A. Then G is a finite group scheme of length $\deg(p^i) = p^{2gi}$. By definition of p-rank, $G(\mathbb{F}_q^{\mathrm{alg}}) \approx (\mathbb{Z}/p^i)^r$, so $G(\mathbb{F}_q^{\mathrm{alg}})$ has size p^{ir}. Therefore, the connected component G^0 of G has length $p^{2gi}/p^{ir} = p^{i(2g-r)}$, by Fact 2.10.

The endomorphism $\phi_q : A \to A$ restricts to the qth-power Frobenius endomorphism on G and G^0. By assumption, $q > p^{2ig} \geq p^{i(2g-r)}$, and so ϕ_q annihilates G^0 by Lemma 2.9.

Let G' denote the kernel of $\phi_q - p^i$. Then G^0 is a closed subgroup scheme of G'. By Fact 2.10, $\ell(G^0) = p^{i(2g-r)}$ divides $\ell(G) = \deg(\phi_q - p^i)$. ∎

PROPOSITION 2.12: *There is a computable function $h_2(p, s, g)$ with the following property. Let A be a g-dimensional abelian variety over $\mathbb{F}_q$, with*

$$q = p^k > h_2(p, s, g).$$

Let ϕ_q denote the qth power Frobenius on A. Let r be the p-rank of A. Then we can write the characteristic roots of ϕ_q as $\alpha_1, \ldots, \alpha_{2g}$, where

- *$\alpha_1, \ldots, \alpha_r$ are the eigenvalues of $T_p(\phi_q) : T_pA \to T_pA$,*
- *$v_p(\alpha_i) > v_p(p^s)$ for $i \in \{r+1, r+2, \ldots, 2g\}$.*

Proof. Define

$$h_2(p,s,g) = \max\{p^{2g\cdot h_1(2g,d',p,s)} : 0 \le d' \le 2g\},$$

where h_1 is as in Lemma 2.8. Suppose the assumptions hold. Then for any $1 \le i \le h_1(2g, 2g-r, p, s)$, we have

$$q = p^k > h_2(p,s,g) \ge p^{2g\cdot h_1(2g,2g-r,p,s)} \ge p^{2gi}.$$

By Lemma 2.11,

$$v_p(\deg(\phi_q - p^i)) \ge v_p(p^{i(2g-r)}) \quad \text{for } i \le h_1(2g, 2g-r, p, s).$$

Let $Q(x)$ be the rational polynomial whose roots are the α_i. By Corollary 2.2,

$$\deg(\phi_q - p^i) = \prod_{i=1}^{2g}(\alpha_i - p^i) = Q(p^i).$$

Thus

$$v_p(Q(p^i)) \ge v_p(p^{i(2g-r)}) \quad \text{for } i \le h_1(2g, 2g-r, p, s).$$

By definition of h_1 (Lemma 2.8), it follows that at least $2g-r$ of the roots of $Q(x)$ have p-adic valuation at least $v_p(p^s)$. Meanwhile, Lemma 2.7 gives r roots $\beta_1, \dots, \beta_r$, coming from the eigenvalues of $T_p(\phi_q)$. Each of these roots has valuation zero. There can be no overlap between the $2g-r$ roots of valuation at least $v_p(p^s)$, and the r roots coming from $T_p(\phi_q)$, so these together account for all $2g$ roots of $Q(x)$. ∎

Corollary 2.13: *There is a computable function $h(p,s,g)$ with the following property. Let C be a curve of genus g over a finite field $\mathbb{F}_q$, and let J be its Jacobian. Suppose q is a power of p, and $q > h(p,s,g)$. Then*

$$|C(\mathbb{F}_q)| \equiv 1 - \operatorname{Tr}(\phi_q | J[p^s]) + \operatorname{Tr}(\phi_q | \mathbb{G}_m[p^s]) \pmod{p^s},$$

where the notation is as in Corollary 2.4.

Proof. Take $h(p,s,g)$ to be the maximum of $h_2(p,s,g)$ and p^s. Suppose $q > h(p,s,g)$. By Fact 2.3,

$$|C(\mathbb{F}_q)| = 1 + q - \sum_{i=1}^{2g} \alpha_i.$$

Working modulo p^s, the term q vanishes, because $q > h(p,s,g) \ge p^s$. Also, $q > h_2(p,s,g)$, so by Proposition 2.12, we may assume that

- $\alpha_1, \dots, \alpha_r$ are the eigenvalues of $T_p(\phi_q)$,
- $\alpha_{r+1}, \dots, \alpha_{2g}$ have valuation at least $v_p(p^s)$.

Working modulo p^s, we can therefore ignore $\alpha_{r+1}, \ldots, \alpha_{2g}$. Thus

$$|C(\mathbb{F}_q)| \equiv 1 - \sum_{i=1}^{r} \alpha_i \pmod{p^s}.$$

The right-hand side is $1 - \mathrm{Tr}(\phi_q | J[p^s])$. Finally, observe that $\mathrm{Tr}(\phi_q | \mathbb{G}_m[p^s])$ vanishes, because $\mathbb{G}_m[p^s]$ is free of rank 0. (There is no p-torsion in the multiplicative group.) ∎

3. Review of periodic difference fields

In this section, we review the basic facts about periodic fields. The original source for these results is Hrushovski's [14]. We will follow an approach that mimics the closely related case of ACFA [4, 15].

Recall from §1.4 that a periodic field (K_∞, σ) is regarded as a multi-sorted structure $(K_1, K_2, \ldots)$ where K_n is the fixed field of σ^n on K_∞.

3.1. Existentially closed periodic fields. If (K_∞, σ) is a periodic field, then K_n/K_1 is a cyclic Galois extension of degree at most n. Say that (K_∞, σ) is **non-degenerate** if $\mathrm{Gal}(K_n/K_1) \cong \mathbb{Z}/n\mathbb{Z}$ for each n. Equivalently, $K_n \not\subseteq K_m$ for any $m < n$.

Lemma 3.1: *If (K_∞, σ) is a non-degenerate periodic field and (L_∞, σ) extends (K_∞, σ), then the natural map*

$$\psi_n : L_1 \otimes_{K_1} K_n \to L_n$$

is an isomorphism of difference rings for all $n \in \mathbb{N} \cup \{\infty\}$.

Proof. The $n = \infty$ case follows by taking the limit, so we may assume $n < \infty$. The image of ψ_n is the compositum $K_n L_1$. This is an intermediate field in the Galois extension L_n/L_1, so it must be L_m for some m dividing n. By non-degeneracy, $K_n \not\subseteq L_m$ for any $m < n$. Thus $K_n L_1 = L_n$ and the map is surjective. Non-degeneracy of K_∞ implies non-degeneracy of L_∞, and so

$$[K_n : K_1] = n = [L_n : L_1].$$

Counting dimensions, ψ_n must be injective. ∎

Recall that a field extension L/K is **regular** if $L \otimes_K K^{\mathrm{alg}}$ is a domain, or equivalently, a field. A field K is **pseudo algebraically closed** (PAC) if K is relatively existentially closed in every regular extension. An equivalent

condition is that $V(K) \neq \emptyset$ for every geometrically integral variety V over K. This property is first-order [11, Proposition 10.9].

PROPOSITION 3.2: *A periodic field (K_∞, σ) is existentially closed if and only if*

(1) $K_\infty \models \mathrm{ACF}$,
(2) (K_∞, σ) *is non-degenerate, and*
(3) K_1 *is PAC.*

Proof. Suppose (1) fails. Extend σ to an automorphism σ' of K_∞^{alg}. Then (K_∞, σ) fails to be existentially closed in $(K_\infty^{\mathrm{alg}}, \sigma')$.

Suppose (2) fails, so that $K_n = K_m$ for some $m < n$. Let σ' be the automorphism of $K'_\infty := K_\infty(x_1, \ldots, x_n)$ extending σ and mapping

$$x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_1.$$

Then (K_∞, σ) is not existentially closed in (K'_∞, σ'). Indeed, the equation $\sigma^n(x) = x \neq \sigma^m(x)$ has a solution in K'_n but not K_n.

Suppose (3) fails, so K_1 is not existentially closed in some regular extension L/K_1. The difference ring $L_\infty := L \otimes_{K_1} K_\infty$ is a field by regularity of L/K_1. Then L_∞ is a periodic field extending K_∞, and K_∞ is not existentially closed in L_∞ because K_1 is not existentially closed in L_1.

Finally, suppose (1–3) all hold. Let L_∞ be a periodic field extending K_∞. Let K_∞^* be a big ultrapower of K_∞ (in the language of periodic fields, not difference fields). It suffices to embed L_∞ into K_∞^* over K_∞. Note that

$$K_\infty^* = K_1^* \otimes_{K_1} K_\infty = K_1^* \otimes_{K_1} K_1^{\mathrm{alg}}.$$

The first equality holds by Lemma 3.1 and (2); the second equality holds by (1) and the general fact that K_∞/K_1 is algebraic. Similarly

$$L_\infty = L_1 \otimes_{K_1} K_\infty = L_1 \otimes_{K_1} K_1^{\mathrm{alg}}.$$

Then L_1/K_1 is regular, so K_1 is existentially closed in L_1 by (3). It follows that L_1 embeds into K_1^* over K_1. Tensoring with K_∞, this gives the desired embedding of periodic fields:

$$L_\infty = L_1 \otimes_{K_1} K_\infty \hookrightarrow K_1^* \otimes_{K_1} K_\infty = K_\infty^*. \qquad \blacksquare$$

The conditions of Proposition 3.2 are first order, in spite of appearances to the contrary.

Definition 3.3: **ACPF** is the theory of existentially closed periodic fields. In other words, ACPF is the model companion of periodic fields.

The name "ACPF" is not standard, but is chosen by analogy with ACFA. Recall that a field is **pseudofinite** if it is perfect, PAC, and has absolute Galois group $\hat{\mathbb{Z}}$. Models of ACPF are essentially pseudofinite fields with a choice of a generator of the Galois group:

PROPOSITION 3.4: *If K is pseudofinite and σ is a topological generator of* $\mathrm{Gal}(K)$, *then* $(K^{\mathrm{alg}}, \sigma) \models \mathrm{ACPF}$. *The periodic field* $(K^{\mathrm{alg}}, \sigma)$ *and the pseudofinite field K are bi-interpretable after naming parameters. All models of ACPF arise in this way from pseudofinite fields.*

Proof. Except for bi-interpretability, this follows from Proposition 3.2. Note that "$(K^{\mathrm{alg}}, \sigma)$" is really the multisorted structure $(K_1, K_2, \ldots)$ where K_n is the degree n extension of K. This can be interpreted in K by choosing a basis for each K_n and interpreting K_n as K^n. Conversely, K is K_1. ∎

If (K, σ) is a periodic field, let $\mathrm{Abs}(K)$ denote the "absolute numbers," the relative algebraic closure of the prime field in K. We can regard $\mathrm{Abs}(K)$ as a substructure of K. The field $\mathrm{Abs}(K)$ is algebraically closed whenever K is.

LEMMA 3.5: *Two models* $K_1, K_2 \models \mathrm{ACPF}$ *are elementarily equivalent if and only if* $\mathrm{Abs}(K_1) \cong \mathrm{Abs}(K_2)$. *More generally, if F is a substructure of K_1 and $F = F^{\mathrm{alg}}$, then any embedding of F into K_2 is a partial elementary map from K_1 to K_2.*

The proof is the same as for ACFA [4, Theorem 1.3]. Lemma 3.5 generalizes (and implies) the analogous statements for pseudofinite fields [2, Theorem 4].

3.2. DEFINABLE SETS. The following standard fact is an easy application of compactness:

FACT 3.6: *Let $\mathbb{M}$ be a monster model. Let $A \subseteq \mathbb{M}$ be small. Let $\mathcal{P}$ be a collection of A-definable subsets of $\mathbb{M}^n$ closed under positive boolean combinations. Suppose the following holds:*

For every $a, b \in \mathbb{M}^n$, if

$$\forall X \in \mathcal{P} : a \in X \implies b \in X,$$

then $\mathrm{tp}(a/A) = \mathrm{tp}(b/A)$.

Then every A-definable subset of $\mathbb{M}^n$ is in $\mathcal{P}$.

We shall need the following geometric form of almost quantifier elimination. Recall that a morphism $f : V_1 \to V_2$ of K-varieties is *quasi-finite* if the fibers of the map $V_1(K^{\mathrm{alg}}) \to V_2(K^{\mathrm{alg}})$ are finite.

PROPOSITION 3.7: *Let $(\mathbb{M}, \sigma)$ be a model of ACPF. Let (K_∞, σ) be a non-degenerate substructure, with K_1 perfect. Let X be a K_∞-definable subset of $\mathbb{M}_1^n$. Then X is the image of $V(\mathbb{M}_1) \to \mathbb{A}^n(\mathbb{M}_1)$ for some quasi-finite morphism $V \to \mathbb{A}^n$ of K_1-varieties.*

Proof. Replacing $\mathbb{M}$ with an elementary extension, we may assume $\mathbb{M}$ is $|K_\infty|^+$-saturated. Let $\mathcal{P}$ be the class of definable subsets of $\mathbb{M}_1^n$ of the specified form. We need to show that $\mathcal{P}$ contains every K_∞-definable subset of $\mathbb{M}_1^n$.

Note that $\mathcal{P}$ is closed under finite unions, because we can form coproducts $V_1 \sqcup V_2$ in the category of K_1-varieties. Similarly, $\mathcal{P}$ is closed under finite intersections, because of fiber products $V_1 \times_{\mathbb{A}^n} V_2$. Therefore, we can use Fact 3.6. Let a, b be two points in $\mathbb{M}_1^n$. Suppose that for every $X \in \mathcal{P}$,

$$a \in X \implies b \in X.$$

We must show $\mathrm{tp}(a/K_\infty) = \mathrm{tp}(b/K_\infty)$. Let $(K_1(a)^{\mathrm{alg}})_1$ denote the fixed field of the periodic difference field $K_1(a)^{\mathrm{alg}} \subseteq \mathbb{M}_\infty$.

CLAIM 3.8: *Let c be an m-tuple from $(K_1(a)^{\mathrm{alg}})_1$ and $\phi(x; y)$ be a quantifier-free $\mathcal{L}_{\mathrm{rings}}(K_1)$-formula such that $\phi(a; c)$ holds. Then there is an m-tuple d from $\mathbb{M}_1$ such that $\phi(b; d)$ holds.*

Proof of Claim 3.8. Strengthening $\phi(x; y)$, we may assume that

- $\phi(x; y)$ witnesses that $y \in K_1(x)^{\mathrm{alg}}$,
- $\phi(\mathbb{M}_\infty)$ defines a locally closed subvariety W of $\mathbb{A}^{n+m}$.

Then the projection $W \to \mathbb{A}^n$ is a quasi-finite morphism of varieties over K_1. Let $X \in \mathcal{P}$ be the image of $W(\mathbb{M}_1) \to \mathbb{A}^n(\mathbb{M}_1)$. Then

$$(a; c) \in W(\mathbb{M}_1) \implies a \in X \implies b \in X \implies (b; d) \in W(\mathbb{M}_1)$$

for some m-tuple $d \in \mathbb{M}_1$. ∎

By saturation, the Claim holds even when c is an infinite tuple and $\phi(x; y)$ is a type. Letting c enumerate $(K_1(a)^{\mathrm{alg}})_1$ and $\phi(x; y)$ be the complete type of (a, c) over K_1, we obtain an embedding of fields

$$(K_1(a)^{\mathrm{alg}})_1 \hookrightarrow \mathbb{M}_1$$

mapping a to b and K_1 to K_1 pointwise. By Lemma 3.1, we can apply the functor $- \otimes_{K_1} K_\infty$ and obtain an embedding of periodic fields

$$K_1(a)^{\mathrm{alg}} \hookrightarrow \mathbb{M}_\infty$$

sending a to b, and K_∞ to K_∞ pointwise. By Lemma 3.5, this is a partial elementary map, so $\mathrm{tp}(a/K_\infty) = \mathrm{tp}(b/K_\infty)$. ∎

Proposition 3.7 is similar in spirit to Kiefe's quantifier elimination [17, §3], but stronger in that we are restricting to positive boolean combinations of images. It is also quite similar to the quantifier elimination using Galois stratifications (e.g., [6, Theorem 2.3.1]).

In Proposition 3.7, note that $\dim(V) \leq n$, because the geometric fibers of $V \to \mathbb{A}^n$ are finite. In the 1-dimensional case, V is essentially a collection of curves:

Fact 3.9: *Let K be a perfect field, and V be a 1-dimensional variety over K. In other words, $V(K^{\mathrm{alg}})$ is 1-dimensional as a definable set in K^{alg}. Then there exist curves*[3] *$C_1, C_2, \ldots, C_n$ and a definable bijection between a cofinite subset of $V(K)$ and a cofinite subset of $\coprod_{i=1}^n C_i(K)$.*

3.3. The theory of Frobenius periodic fields. Recall the Frobenius periodic fields $\mathrm{Fr}^q = (\mathbb{F}_q^{\mathrm{alg}}, \phi_q)$, where ϕ_q is the qth power Frobenius. There is an analogy

finite fields : pseudofinite fields :: Frobenius periodic fields : e.c. periodic fields.

Ax showed that a field K is pseudofinite if and only if it is elementarily equivalent to a non-principal ultraproduct of finite fields. The analogous thing happens here.

Definition 3.10: $\widetilde{\mathrm{ACPF}}$ is the theory of periodic fields K_∞ such that

(1) $K_\infty \models \mathrm{ACF}$,
(2) K_∞ is non-degenerate,
(3) K_1 is a model of the theory T_{fin} of finite fields,
(4) if K_1 has size $q < \infty$, then σ acts as the qth power Frobenius on K_∞.

Ax showed that the models of T_{fin} are exactly the finite and pseudofinite fields.

[3] Geometrically irreducible, smooth, and projective as always.

LEMMA 3.11: *The models of* $\widetilde{\text{ACPF}}$ *are exactly the models of* ACPF *and the Frobenius periodic fields.*

Proof. If $(K_\infty, \sigma) \models \text{ACPF}$, then Axioms (1) and (2) hold by definition, (3) holds because K_1 is pseudofinite by Proposition 3.4, and (4) is vacuous, as pseudofinite fields are infinite. If (K, σ) is the qth Frobenius periodic field Fr^q, then all the axioms are trivial. Conversely, suppose $(K_\infty, \sigma) \models \widetilde{\text{ACPF}}$. If $|K_1| = q < \infty$, then Axiom (1) forces

$$K_\infty \cong \mathbb{F}_q^{\text{alg}}$$

and Axiom (4) forces

$$(K_\infty, \sigma) \cong \text{Fr}^q\,.$$

If K_1 is infinite, then (3) forces K_1 to be pseudofinite, hence PAC. Then (1) and (2) ensure $(K_\infty, \sigma) \models \text{ACPF}$. ∎

COROLLARY 3.12: *If* (K_∞, σ) *is a non-principal ultraproduct of Frobenius periodic fields, then* $(K_\infty, \sigma) \models \text{ACPF}$.

LEMMA 3.13: *If* $(K_\infty, \sigma) \models \text{ACPF}$ *and* K_∞ *has characteristic 0, then* (K_∞, σ) *is elementarily equivalent to an ultraproduct of Frobenius periodic fields* Fr^p *with* p *prime.*

Proof. For each prime p, let $\tilde{F}_p$ be the periodic field $(\mathbb{Q}_p^{\text{un}}, \sigma)$, where $\mathbb{Q}_p^{\text{un}}$ is the maximal unramified algebraic extension of $\mathbb{Q}_p$, and σ induces the pth power Frobenius on the residue field. By the Chebotarev density theorem, there is a non-principal ultraproduct $(\tilde{F}^*, \sigma)$ of $\tilde{F}_p$ such that

$$(\text{Abs}(\tilde{F}^*), \sigma) \cong (\text{Abs}(K), \sigma).$$

Now $\tilde{F}^*$ has a σ-invariant valuation whose residue field is an ultraproduct F^* of Frobenius periodic fields Fr^p. Then F^* has characteristic 0, the valuation is equicharacteristic 0, and the residue map gives an isomorphism

$$(\text{Abs}(\tilde{F}^*), \sigma) \cong (\text{Abs}(F^*), \sigma).$$

By Lemma 3.5 and Corollary 3.12, $(K, \sigma) \equiv (F^*, \sigma)$. ∎

LEMMA 3.14: *If* $(K_\infty, \sigma) \models \text{ACPF}$ *and* K *has characteristic* $p > 0$*, then* K *is elementarily equivalent to a non-principal ultraproduct of Frobenius periodic fields* Fr^q*, with* q *ranging over powers of* p.

Proof. Similar to Lemma 3.13, but easier (no valuations or Chebotarev). ∎

PROPOSITION 3.15:

(1) *A periodic field (K, σ) is existentially closed if and only if it is elementarily equivalent to a non-principal ultraproduct of Frobenius periodic fields.*
(2) *The elementary class generated by Frobenius periodic fields consists of the Frobenius periodic fields and existentially closed periodic fields.*
(3) $\widetilde{\text{ACPF}}$ *is the theory of Frobenius periodic fields.*

Let T_{prime} be the theory of finite prime fields $\mathbb{F}_p$. Ax showed that the models of T_{prime} are exactly the finite prime fields and the pseudofinite fields of characteristic 0. Analogously, one can show:

PROPOSITION 3.16:

(1) *A periodic field (K, σ) is existentially closed of characteristic 0 if and only if it is elementarily equivalent to a non-principal ultraproduct of prime Frobenius periodic fields.*
(2) *The elementary class generated by prime Frobenius periodic fields consists of:*
   - *Prime Frobenius periodic fields.*
   - *Existentially closed periodic fields of characteristic* 0.
(3) *The theory of prime Frobenius periodic fields is axiomatized by* $\widetilde{\text{ACPF}}$ *and the statement that $K_1 \models T_{\text{prime}}$.*

4. Proof of the main theorem

4.1. THE IMPLICIT DEFINITION. Using Beth implicit definability, Krajíček proves that if a theory admits a unique R-valued strong Euler characteristic χ, then χ is definable [18, Theorem 7.2]. We will use a similar strategy to define our strong $\hat{\mathbb{Z}}$-valued Euler characteristic. We will use the following two variants of Beth implicit definability:

FACT 4.1 ([13, Theorem 6.6.4]): *Let $L^+ \supseteq L^-$ be languages. Let T^- be an L^- theory and T^+ be an L^+ theory extending T^-. Let $\phi(x)$ be an L^+ formula. Suppose that whenever $N \models T^-$, and M_1^+ and M_2^+ are two expansions of N to a model of T^+, that $\phi(M_1^+) = \phi(M_2^+)$. Then there is an L^--formula $\psi(x)$ such that $T^+ \vdash \phi \leftrightarrow \psi$.*

COROLLARY 4.2: *Let $L^+ \supseteq L^-$ be languages. Let T^- be an L^- theory and T^+ be an L^+ theory extending T^-. Suppose that:*

- *T^- is the theory of some (non-elementary) class $\mathcal{C}$ of L^--structures.*
- *Every model of T^- has at most one expansion to a model of T^+.*
- *Every model in $\mathcal{C}$ has at least one expansion to a model of T^+.*

Then every model of T^- has a unique expansion to a model of T^+, and T^+ is a definitional expansion of T^-.

Proof. If $M \models T^-$, then M is elementarily equivalent to an ultraproduct

$$M \equiv M' = \prod_{i \in I} M_i/\mathcal{U}$$

of structures $M_i \in \mathcal{C}$. Each M_i can be expanded to a model of T^+, so the same holds for the ultraproduct M'. By Fact 4.1 and the assumptions, the T^+-structure on M' is $\emptyset$-definable from the T^--structure. Therefore the T^+-structure transfers along the elementary equivalence $M' \equiv M$, giving a T^+-structure on M. So every model of T^- expands to a model of T^+ in a unique way. By Fact 4.1, T^+ is a definitional expansion of T^-. ∎

We will apply both versions of implicit definability in the following context:

- The language L^- is the language of periodic fields.
- The theory T^- is $\widetilde{\text{ACPF}}$, the theory of Frobenius periodic fields as in §3.3.
- $\mathcal{C}$ is the class of Frobenius periodic fields.
- The language L^+ is the expansion of L^- by a new predicate $P_{\phi,n,k}(\vec{y})$ for every formula $\phi(\vec{x};\vec{y}) \in L^-$, every $n \in \mathbb{N}$, and every $k \in \mathbb{Z}/n\mathbb{Z}$. (Compare with the proof of [18, Theorem 7.2].)

The theory T^+ is T^- plus the following axioms:

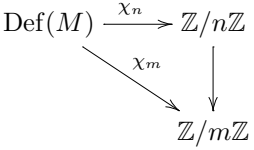
(1) For every ϕ, n, and b, there is a unique $k \in \mathbb{Z}/n\mathbb{Z}$ such that $P_{\phi,n,k}(b)$ holds.

(2) If $\phi(K;b) = \phi'(K;b')$, then

$$P_{\phi,n,k}(b) \iff P_{\phi',n,k}(b').$$

(3) If X is a definable set $\phi(K;b)$, let $\chi_n(X)$ denote the unique k such that $P_{\phi,n,k}(b)$ holds. (This is well-defined by (1) and (2).) Then χ_n is a strong Euler characteristic for each n.

(4) The diagram



commutes when m divides n.

(5) Let C be a genus-g curve over K_1, and let J be its Jacobian. Let p^k be a prime power. Let h be the function from Corollary 2.13. If $\mathrm{char}(K) \neq p$ or if $|K_1| > h(g,p,k)$, then $\chi_{p^k}(C(K_1))$ is given by the formula

$$\chi_{p^k}(C(K_1)) = 1 - \mathrm{Tr}(\sigma|J[p^k]) + \mathrm{Tr}(\sigma|\mathbb{G}_m[p^k]).$$

Here, if G is a commutative group variety over K_1, then $\mathrm{Tr}(\sigma|G[n])$ denotes the trace of the action of σ on the group of n-torsion in $G(K_\infty)$.

Axioms (1)–(4) encode the statement that χ is a $\hat{\mathbb{Z}}$-valued strong Euler characteristic, and Axiom (5) determines its value on curves over K_1. We discuss why Axiom (5) is first-order in §5.

4.2. Uniqueness. The "existence" part of Corollary 4.2 has already been verified:

Proposition 4.3: *If Fr^q is a Frobenius periodic field, and χ is the counting Euler characteristic, then χ satisfies T^+. In particular, Fr^q admits an expansion to a model of T^+.*

Proof. Examining the definition of T^+, Axioms (1)–(4) merely say that χ is a $\hat{\mathbb{Z}}$-valued strong Euler characteristic, which is trivial. Axiom (5) holds by Corollaries 2.4 and 2.13. ∎

Therefore, it remains to prove the "uniqueness" part. Our goal is to show that on any $(K,\sigma) \models \widetilde{\mathrm{ACPF}}$, there is at most one $\hat{\mathbb{Z}}$-valued Euler characteristic satisfying the axioms of T^+. Until Proposition 4.7, we will restrict our attention to models of ACPF.

Remark 4.4: In Axiom (5) of T^+, the condition "$|K_1| > h(g,p,k)$" is automatic when K_1 is infinite, i.e., when $(K_\infty,\sigma) \models \mathrm{ACPF}$. Therefore, for models of ACPF, Axiom (5) says the following: for any curve C over K_1 with Jacobian J,

$$\chi_{p^k}(C(K_1)) = 1 - \mathrm{Tr}(\sigma|J[p^k]) + \mathrm{Tr}(\sigma|\mathbb{G}_m[p^k]).$$

By the Chinese remainder theorem, this formula determines $\chi_n(C)$ for any n.

LEMMA 4.5: *Let (K_∞, σ) be a model of* ACPF*, admitting two expansions to a model of T^+. Let χ and χ' be the corresponding $\hat{\mathbb{Z}}$-valued strong Euler characteristics. Then $\chi(X) = \chi'(X)$ for every unary definable set $X \subseteq K_1$.*

Proof. Say that a definable set is **good** if $\chi(X) = \chi'(X)$. Finite sets are good. If X is in definable bijection with Y and X is good, then so is Y. A disjoint union of two good sets is good. If S is a cofinite subset of X, then S is good if and only if X is good. Consequently, if a cofinite subset of X is in definable bijection with a cofinite subset of Y, then X is good if and only if Y is good.

If C is a curve over K_1, then $C(K_1)$ is good, by Remark 4.4. Any disjoint union of sets of this form is also good. By Fact 3.9, the set $V(K_1)$ is good for any 1-dimensional variety X over K_1.

Now let X be a definable subset of $(K_1)^1$. By Proposition 3.7, X is the image of $V_1(K_1) \to \mathbb{A}^1(K_1)$ for some morphism $V_1 \to \mathbb{A}^1$ of K_1-varieties with geometrically finite fibers. Let V_n denote the n-fold fiber product

$$\underbrace{V_1 \times_{\mathbb{A}^1} V_1 \times_{\mathbb{A}^1} \cdots \times_{\mathbb{A}^1} V_1}_{n \text{ times}}.$$

Each of the morphisms $V_n \to \mathbb{A}^1$ has geometrically finite fibers, so each variety V_n is 1-dimensional. Hence each set

$$Y_n := V_n(K_1)$$

is good. Note that Y_n is the n-fold fiber product of Y_1 over X.

Let m be a bound on the size of the fibers of $Y_1 \to X$. For $1 \leq k \leq m$, let X_k denote the set of $a \in X$ such that $f^{-1}(a)$ has size k. Let α_k and β_k denote $\chi(X_k)$ and $\chi'(X_k)$.

Because χ and χ' are strong Euler characteristics,

$$\chi(Y_n) = \sum_{k=1}^{m} \alpha_k k^n,$$
$$\chi'(Y_n) = \sum_{k=1}^{m} \beta_k k^n,$$

for all n. As the Y_n's are good,

$$\sum_{k=1}^{m} \alpha_k k^n = \sum_{k=1}^{m} \beta_k k^n$$

for $n=1,\ldots,m$. By invertibility of the Vandermonde matrix $\langle k^n\rangle_{1\leq k\leq m,\,1\leq n\leq m}$, and the fact that $\hat{\mathbb{Z}}$ has no $\mathbb{Z}$-torsion, it follows that $\alpha_k=\beta_k$ for all k. Consequently,

$$\chi(X)=\sum_{k=1}^{m}\alpha_k=\sum_{k=1}^{m}\beta_k=\chi'(X). \tag{2}$$

Therefore X is good. ∎

The proof method of Lemma 4.5 is essentially due to Kiefe [17, Proof of Lemma 8].

LEMMA 4.6: *For any n, the following statements are true:*

- (S_n) *Let (K_∞,σ) be a model of ACPF, admitting two expansions to a model of T^+. Let χ and χ' be the corresponding $\hat{\mathbb{Z}}$-valued strong Euler characteristics. Then $\chi(X)=\chi'(X)$ for every definable subset $X\subseteq(K_1)^n$.*
- (T_n) *If (K_∞,σ) is a model of ACPF, admitting an expansion to a model of T^+, and χ is the corresponding $\hat{\mathbb{Z}}$-valued strong Euler characteristic, then for every definable family $\{X_a\}_{a\in Y}$ of subsets of $(K_1)^n$, for every $m\in\mathbb{N}$ and for every $k\in\mathbb{Z}/m\mathbb{Z}$, the set*

$$\{a\in Y(K):\chi(X_a)\equiv k\pmod m\}$$

is definable in the L^--reduct (K_∞,σ).

Proof. Statement S_1 is Lemma 4.5. The implication $S_n \implies T_n$ follows by Beth implicit definability. It suffices to show

$$(S_1 \text{ and } S_n \text{ and } T_n) \implies S_{n+1}.$$

Assume the left hand side. Let $(K_\infty,\sigma),\chi,\chi'$, and $X\subseteq K_1\times(K_1)^n$ be as in the statement of S_{n+1}. Fix $m\in\mathbb{N}$; we claim $\chi_m(X)=\chi'_m(X)$. For $t\in K_1$, let

$$X_t=\{\vec{x}\in(K_1)^n:(t,\vec{x})\in X\}.$$

By statements S_n and T_n, the sets

$$Y_k=\{t\in K_1:\chi(X_t)\equiv k\pmod m\},$$
$$Y'_k=\{t\in K_1:\chi'(X_t)\equiv k\pmod m\}$$

are equal and definable. Because χ and χ' are strong Euler characteristics,

$$\chi_m(X) = \sum_{k \in \mathbb{Z}/m\mathbb{Z}} k \cdot \chi_m(Y_k),$$

$$\chi'_m(X) = \sum_{k \in \mathbb{Z}/m\mathbb{Z}} k \cdot \chi'_m(Y'_k).$$

Then $\chi_m(Y_k) = \chi'_m(Y_k)$ by statement S_1, so putting things together,

$$\chi_m(X) = \chi'_m(X).$$

As m was arbitrary, S_n holds. ∎

PROPOSITION 4.7: *If (K, σ) is a model of $\widetilde{\text{ACPF}}$, then there is at most one expansion of (K, σ) to a model of T^+.*

Proof. If (K, σ) is a Frobenius periodic field, then K_∞ is essentially finite and there is at most one $\hat{\mathbb{Z}}$-valued Euler characteristic. So assume $(K_\infty, \sigma) \models \text{ACPF}$. Let χ, χ' be two $\hat{\mathbb{Z}}$-valued Euler characteristics satisfying T^+. Note that the sort K_n is in definable bijection with $(K_1)^n$. If X is any definable set in K_∞, then X is therefore in definable bijection with a definable subset $Y \subseteq (K_1)^m$ for some m. By statement S_m of Lemma 4.6,

$$\chi(X) = \chi(Y) = \chi'(Y) = \chi'(X). \qquad \blacksquare$$

By Corollary 4.2 and Proposition 4.3, we conclude

PROPOSITION 4.8: *If (K, σ) is a model of $\widetilde{\text{ACPF}}$, then there is a unique expansion of (K, σ) to a model of T^+.*

THEOREM (Theorem 1.4): *Let $\mathcal{C}$ be the class of Frobenius periodic fields and existentially closed periodic fields. There is a $\hat{\mathbb{Z}}$-valued strong Euler characteristic χ on (K, σ) in $\mathcal{C}$ with the following properties:*

- *χ is uniformly $\emptyset$-definable across $\mathcal{C}$.*
- *If (K, σ) is a Frobenius periodic field, then χ is the counting Euler characteristic:*
$$\chi(X) = |X|.$$
- *If (K, σ) is an ultraproduct of Frobenius periodic fields, then χ is the nonstandard counting Euler characteristic.*

Definition 4.9: The **canonical Euler characteristic** on $(K, \sigma) \models \widetilde{\text{ACPF}}$ is the $\hat{\mathbb{Z}}$-valued Euler characteristic of Theorem 1.4.

5. A digression on definability and computability

This section discusses some of the technical issues related to Axiom (5) in the definition of T^+. If one is willing to sweep these issues under the rug, this section can be skipped.

LEMMA 5.1: *The theory T^+ of §4.1 is first-order.*

Proof sketch. The difficulty lies in expressing Axiom (5) via first-order axioms. The assertion

> J is the Jacobian of C

can be expressed as

> J is a smooth projective group variety that is birationally equivalent (over K_1) to $\mathrm{Sym}^g C$, the gth symmetric product of C.

Indeed, the Jacobian is a smooth projective group variety because it is an abelian variety, and it is birationally equivalent to $\mathrm{Sym}^g C$ by the construction of the Jacobian in [23, §V.1]. By Theorem I.3.8 in [20], any birational map between two projective group varieties extends to an isomorphism.

Even the following statement is rather non-trivial to express:

> C is a (smooth projective) curve of genus g.

Smoothness can be witnessed by covering projective space with Zariski open patches on which C is cut out by a system of equations whose matrix of partial derivatives has rank no higher than the codimension of C. Geometric irreducibility can be witnessed as in the appendix of [10]. Genus can be determined by counting zeros and poles on a meromorphic section of the tangent bundle. Alternatively, genus can be calculated by projecting into the plane, calculating the delta invariants of the singularities, and applying the degree-genus formula.

Hopefully, everything will be spelled out in greater detail in [16]. ∎

CONJECTURE 5.2: *The theory T^+ of §4.1 is recursively axiomatizable.*

Conjecture 5.2 is almost certainly true, by the method of Lemma 5.1. However, it is surprisingly difficult to write out a proof that is both rigorous and human-readable. In future work ([16]), I will develop a toolbox for working with recursively ind-definable sets. This toolbox enables a smooth proof of Conjecture 5.2 along the lines of Lemma 5.1.

Alternatively, there may be clever algebraic proofs of Conjecture 5.2. But it would be more conceptually satisfying to explain why the informal argument can be formalized, rather than cheating and appealing to algebraic tricks.

6. Further results

6.1. Uniform definability of the counting Euler characteristic. Theorem 1.4 implies that the counting Euler characteristic is uniformly definable across all Frobenius periodic fields. This can be restated more explicitly as follows:

Corollary 6.1: *For any formula $\phi(x;y)$ in the language of periodic fields, any $n \in \mathbb{N}$, and any $k \in \mathbb{Z}/n\mathbb{Z}$, there is a formula $\psi_{\phi,n,k}(y)$ such that for any Frobenius periodic field Fr^q and any tuple b from Fr^q,*

$$\mathrm{Fr}^q \models \psi_{\phi,n,k}(b) \iff |\phi(\mathrm{Fr}^q; b)| \equiv k \pmod{n}$$

6.2. Evaluation on curves.

Proposition 6.2: *Let (K_∞, σ) be a model of* ACPF*. Let C be a curve over K_1, and J be the jacobian. For any prime ℓ (possibly the characteristic), the ℓ-adic component of $\chi(C(K_1))$ is determined by the trace of the action of σ on the ℓ-adic Tate modules of J and the multiplicative group $\mathbb{G}_m$:*

$$1 - \mathrm{Tr}(\sigma|T_\ell J) + \mathrm{Tr}(\sigma|T_\ell \mathbb{G}_m).$$

Proof. This follows directly from Axiom 5 of T^+, and Remark 4.4. ∎

For $\ell \neq \mathrm{char}(K)$, there should be a generalization using ℓ-adic étale cohomology with compact supports:

Conjecture 6.3: *Let (K_∞, σ) be a model of ACPF, let V be a variety over K_1, and let ℓ be a prime different from the characteristic. Then the ℓ-adic component of $\chi(V(K_1))$ is given by the formula*

$$\sum_{i=0}^{2\dim(V)} (-1)^i \,\mathrm{Tr}(\sigma^{-1}|H_c^i(V;\mathbb{Q}_\ell)),$$

where $H_c^i(V;\mathbb{Q}_\ell)$ denotes the ℓ-adic cohomology with compact supports.

I suspect that Conjecture 6.3 is trivial with the right tools. If I understand correctly, the conjecture holds for Frobenius periodic fields, because of Grothendieck's trace formula [9, Chapter II, Theorem 4.2]. As long as Conjecture 6.3 can be stated as a conjunction of first-order sentences, it transfers to models of ACPF by Proposition 3.15. Thus, the only thing needing verification is that the groups $H^i_c(V;\mathbb{Z}/\ell^k)$ depend definably on V. This should follow easily from the base change theorem for direct images with proper support [9, Chapter 1, Theorem 8.7(1)].

Remark 6.4: Fix a field k of characteristic 0. Denef and Loeser [6] assign to each formula ϕ in the language of k-algebras an invariant $\chi_c(\phi)$ depending only on the realizations of ϕ in pseudofinite fields extending k. The invariant $\chi_c(\phi)$ is a virtual motive, i.e., an element of $K_0(\mathrm{Mot}_{k,\mathbb{Q}^{\mathrm{alg}}}) \otimes \mathbb{Q}$, where $K_0(\mathrm{Mot}_{k,\mathbb{Q}^{\mathrm{alg}}})$ is the Grothendieck group of Chow motives over k with coefficients in $\mathbb{Q}^{\mathrm{alg}}$. Let K be a pseudofinite field extending k, let σ be a topological generator of $\mathrm{Gal}(K)$, let $\hat{\chi}$ be the associated $\hat{\mathbb{Z}}$-valued strong Euler characteristic, and let ℓ be a prime. Generalizing Conjecture 6.3, one expects the ℓ-adic part of $\hat{\chi}(\phi(K))$ to be given by $F(\chi_c(\phi))$, where $F : K_0(\mathrm{Mot}_{k,\mathbb{Q}^{\mathrm{alg}}}) \otimes \mathbb{Q} \to \mathbb{Q}_\ell$ is the ring homomorphism sending (the class of) a motive M to the trace of σ^{-1} acting on the ℓ-adic realization of M.

6.3. Pseudofinite fields.

Lemma 6.5: *Let K be a pseudofinite field and σ be a topological generator of* $\mathrm{Gal}(K)$. *The canonical $\hat{\mathbb{Z}}$-valued definable strong Euler characteristic on $(K^{\mathrm{alg}},\sigma)$ restricts to an $\mathrm{acl}^{eq}(\emptyset)$-definable strong Euler characteristic on K.*

Proof. The structure $(K^{\mathrm{alg}},\sigma)$ and the field K have equivalent categories of (parametrically) definable sets, by the bi-interpretability of Proposition 3.4. Therefore, the definable strong Euler characteristic on $(K^{\mathrm{alg}},\sigma)$ determines a definable strong Euler characteristic χ' on K.

To prove $\mathrm{acl}^{eq}(\emptyset)$-definability of χ', we may pass to an elementary extension and assume K and $(K^{\mathrm{alg}},\sigma)$ are monster models. The Euler characteristic χ' is not determined in an $\mathrm{Aut}(K)$-invariant way, because of the choice of σ. However, there are only boundedly many choices for σ. Therefore χ' has only boundedly many conjugates under $\mathrm{Aut}(K)$, so χ' is $\mathrm{acl}^{eq}(\emptyset)$-definable. ∎

THEOREM (Theorem 1.1):

(1) *Let $K = \prod_i K_i/\mathcal{U}$ be an ultraproduct of finite fields. Then the nonstandard counting functions χ_n are $\mathrm{acl}^{eq}(\emptyset)$-definable.*
(2) *Every pseudofinite field admits an $\mathrm{acl}^{eq}(\emptyset)$-definable $\hat{\mathbb{Z}}$-valued strong Euler characteristic.*

Proof. Part 2 is Lemma 6.5. For part 1, given an ultraproduct $K = \prod_i \mathbb{F}_{q_i}/\mathcal{U}$, let $(L, \sigma) = \prod_i \mathrm{Fr}^{q_i}/\mathcal{U}$ be the corresponding ultraproduct of Frobenius periodic fields. Then $K \cong L_1$. The nonstandard counting functions on K are induced by the canonical Euler characteristic on (L_∞, σ). Therefore the nonstandard counting functions on K are $\mathrm{acl}^{eq}(\emptyset)$-definable, by Lemma 6.5. ∎

6.4. ELIMINATION OF PARITY QUANTIFIERS. Let $\mu^n_k x$ be a generalized parity quantifier, as in §1.3. Let $\mathcal{L}^\mu_{\mathrm{rings}}$ and $\mathcal{L}^\mu_{pf}$ be the language of rings and the language of periodic fields, respectively, expanded with generalized parity quantifiers.

PROPOSITION 6.6 (Theorem 1.5.(1)): *Frobenius periodic fields uniformly eliminate generalized parity quantifiers. If $\phi(\vec{x})$ is a formula in $\mathcal{L}^\mu_{pf}$, then there is a formula $\phi'(\vec{x}) \in \mathcal{L}_{pf}$ such that for any Frobenius periodic field Fr^q and any tuple $\vec{a}$,*

$$\mathrm{Fr}^q \models \phi(\vec{a}) \iff \mathrm{Fr}^q \models \phi'(\vec{a}).$$

Proof. Proceed by induction on the complexity of $\phi(\vec{x})$. We may assume $\phi(\vec{x})$ has the form

$$\mu^n_k \vec{y} : \psi(\vec{x}, \vec{y}),$$

for some formula $\psi(\vec{x}, \vec{y}) \in \mathcal{L}_{pf}$. In this case, we can eliminate μ^n_k by Corollary 6.1. ∎

Example 6.7: The $\mathcal{L}^\mu_{pf}$-sentence

$$\tau \overset{\mathrm{def}}{\iff} \mu^5_2 x \in K_1 : x = x$$

is equivalent in Frobenius periodic fields Fr^q to the $\mathcal{L}_{pf}$-sentence

$$\tau' \overset{\mathrm{def}}{\iff} 5 \neq 0 \wedge \forall x \in K_4 : (x^5 = 1 \to \sigma(x) = x^2).$$

To see this, break into cases according to the congruence class of q modulo 5. Note that $\mathrm{Fr}^q \models \tau \iff q \equiv 2 \pmod 5$.

- If $q \equiv 0 \pmod 5$, then Fr^q has characteristic 5, so τ' and τ are both false.
- If $q \equiv 2 \pmod 5$, then Fr^q does not have characteristic 5, and

$$\forall x \in K_\infty : (x^5 = 1 \to x^q = x^2),$$

  so τ and τ' are both true.
- If $q \equiv j \pmod 5$ for $j \neq 0, 2$, then Fr^q does not have characteristic 5. Let x be a primitive fifth root of unity. Then $x \in K_4$, because $\mathrm{Gal}(K_1(x)/K_1)$ is a subgroup of

$$(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}.$$

  Also,

$$x^q = x^j \neq x^2,$$

  and so τ' is false.

In contrast to Proposition 6.6, generalized parity quantifiers are *not* eliminated in finite fields:

LEMMA 6.8: *There is no $\mathcal{L}_{\mathrm{rings}}$-sentence ρ equivalent to the following $\mathcal{L}^{\mu}_{\mathrm{rings}}$-sentence in every finite field:*

$$\mu^5_2 x : x = x.$$

Proof. Suppose ρ exists. Then the following are equivalent for any model $(K_\infty, \sigma) \models \widetilde{\mathrm{ACPF}}$:

- K_1 satisfies ρ.
- K_∞ does not have characteristic 5, and the action of σ on the fifth roots of unity is given by

$$\sigma(\omega) = \omega^2.$$

Now take (K_∞, σ) satisfying ACPF and the two equivalent conditions. (For example, we can take K_∞ to be a non-principal ultraproduct of Fr^p where p ranges over primes congruent to 2 mod 5. A non-principal ultrafilter exists by Dirichlet's theorem.) Then K_1 satisfies ρ, and σ acts on the fifth roots of unity by squaring. Consider a dual model

$$(K^\dagger_\infty, \sigma) \cong (K_\infty, \sigma^{-1}).$$

From the axioms of ACPF, it is clear that $(K_\infty^\dagger, \sigma) \models$ ACPF. Since σ acts on fifth roots by squaring, σ^{-1} acts by cubing:

$$\sigma^{-1}(\omega) = \omega^3,$$

as 2 and 3 are multiplicative inverses modulo 5. So $(K_\infty^\dagger, \sigma)$ does not satisfy the two equivalent conditions, and in particular, $K_1^\dagger \not\models \rho$. But this is absurd, since $K_1^\dagger$ is isomorphic as a field to K_1. ∎

Remark 6.9: The proof of Lemma 6.8 actually proves something stronger: parity quantifiers are not eliminated on the class of prime fields $\mathbb{F}_p$. The non-elimination of parity quantifiers in finite fields was originally proven in [18, Theorem 7.3], using a slightly different method.

6.5. Decidability. Recall the theory T^+ of §4.1. For the rest of this section, we assume Conjecture 5.2.

Lemma 6.10: *(Assuming Conjecture 5.2.) There is a computable function which takes a formula $\phi(\vec{x})$ in the language of T^+ and outputs a formula $\phi'(\vec{x})$ in the language of periodic fields, such that*

$$T^+ \vdash \phi \leftrightarrow \phi'.$$

Proof. By Conjecture 5.2, the theory $\widetilde{\text{ACPF}}$ of §3.3 and the theory T^+ of §4.1 are recursively axiomatized.

For each ϕ, an equivalent formula ϕ' exists by Beth implicit definability (Fact 4.1) and the existence and uniqueness of the expansion to T^+ (Proposition 4.8). An algorithm can find ϕ' by searching all consequences of T^+ until it finds one of the form

$$\forall \vec{x} : \phi(\vec{x}) \leftrightarrow \phi'(\vec{x})$$

with ϕ' a formula in the pure language of periodic fields. ∎

Corollary 6.11: *(Assuming Conjecture 5.2.)*

(1) *In Corollary 6.1, the formula $\psi_{\phi,n,k}$ can be chosen to depend computably on ϕ.*
(2) *In Proposition 6.6, the elimination of generalized parity quantifiers can be carried out computably—the formula ϕ' can be chosen to depend computably on ϕ.*

Proof.

(1) Corollary 6.1 is an instance of Lemma 6.10, so the conversion can be done computably.
(2) As in the proof of Proposition 6.6, one converts a $\mathcal{L}^{\mu}_{pf}$-formula into a pure $\mathcal{L}_{pf}$-formula by recursion on the formula. ∎

THEOREM (Theorems 1.5.(2) and 1.2): *(Assuming Conjecture 5.2.)*

(1) *The $\mathcal{L}^{\mu}_{pf}$-theory of Frobenius periodic fields is decidable.*
(2) *The $\mathcal{L}^{\mu}_{\text{rings}}$-theory of finite fields is decidable.*

Proof. First note that the ($\mathcal{L}_{pf}$-)theory of Frobenius periodic fields is decidable. By Proposition 3.15, the theory is completely axiomatized by $\widetilde{\text{ACPF}}$. Therefore, the theory is computably enumerable. The theory is also co-computably enumerable. Indeed, a sentence τ is not part of the theory if and only if $\text{Fr}^q \models \neg\tau$ for some q. There is an algorithm taking q and τ and outputting whether or not $\text{Fr}^q \models \tau$, because Fr^q is essentially finite. So we can enumerate all the statements that fail in some Frobenius periodic field, which is the complement of the theory of Frobenius periodic fields. Thus the theory of Frobenius periodic fields is decidable, as claimed.

Now given a $\mathcal{L}^{\mu}_{pf}$-sentence τ, we can computably convert it into an equivalent $\mathcal{L}_{pf}$-sentence τ', and use the previous paragraph to computably determine whether or not τ' holds in every Frobenius periodic field. This proves the first point.

The second point follows, because there is a computable way to convert an $\mathcal{L}^{\mu}_{\text{rings}}$-sentence τ into a $\mathcal{L}^{\mu}_{pf}$-sentence τ' such that

$$(K_\infty, \sigma) \models \tau' \iff K_1 \models \tau$$

for any essentially finite periodic field (K_∞, σ). Taking K_∞ to be Fr^q, we see that

$$\text{Fr}^q \models \tau' \iff \mathbb{F}_q \models \tau.$$

Therefore, τ holds in every finite field if and only if τ' holds in every Frobenius periodic field. Then we can apply the oracle for the first point to τ'. ∎

7. Mock-finite fields

Recall that $\mathrm{Abs}(K)$ denotes the substructure of **absolute numbers** of K—the elements algebraic over the prime field.

Definition 7.1: A field K is **mock-finite** if K is pseudofinite and $\mathrm{Abs}(K)$ is finite.

We will see that mock-finite fields admit particularly nice Euler characteristics.

Definition 7.2: A field K is a **mock-$\mathbb{F}_q$** if K is pseudofinite and $\mathrm{Abs}(K) \cong \mathbb{F}_q$.

Note that K is mock-finite if and only if K is a mock-$\mathbb{F}_q$ for some q. For fixed q, the theory of mock $\mathbb{F}_q$'s is consistent and complete [2, Theorems 4 and 6].

LEMMA 7.3: *Let K be a mock-$\mathbb{F}_q$. Then the restriction homomorphism*

$$\mathrm{Gal}(K) \to \mathrm{Gal}(\mathbb{F}_q)$$

is an isomorphism. Consequently, there is a unique topological generator $\sigma \in \mathrm{Gal}(K)$ extending the qth power Frobenius $\phi_q \in \mathrm{Gal}(\mathbb{F}_q)$.

Proof. The restriction homomorphism is surjective because $\mathbb{F}_q$ is relatively algebraically closed in K. Both Galois groups are isomorphic to $\hat{\mathbb{Z}}$, and any continuous surjective homomorphism $\hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ is an isomorphism. ∎

Definition 7.4: If K is a mock-$\mathbb{F}_q$, the **mock Frobenius automorphism** is the unique $\sigma \in \mathrm{Gal}(K)$ extending the qth-power Frobenius $\phi_q \in \mathrm{Gal}(\mathbb{F}_q)$.

If p is a prime, let $\mathbb{Z}_{\neg p}$ be the prime-to-p completion of $\mathbb{Z}$:

$$\mathbb{Z}_{\neg p} = \varprojlim_{(n,p)=1} \mathbb{Z}/n\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell.$$

Definition 7.5: Let K be a mock-finite field, and σ be the mock Frobenius automorphism.

(1) The **principal Euler characteristic** on K is the $\mathbb{Z}_{\neg p}$-valued Euler characteristic induced by σ.
(2) The **dual Euler characteristic** on K is the $\mathbb{Z}_{\neg p}$-valued Euler characteristic induced by σ^{-1}.

The reason for the prime-to-p restriction will become clear soon.

LEMMA 7.6: *The principal and dual Euler characteristics are $\emptyset$-definable.*

Proof. They are definable by Lemma 6.5, and $\mathrm{Aut}(K/\emptyset)$-invariant by construction. ∎

7.1. Mock-frobenius periodic fields.

Definition 7.7: A periodic field (K, σ) is a **mock-**Fr^q if $(K, \sigma) \models \mathrm{ACPF}$ and $\mathrm{Abs}(K, \sigma) \cong \mathrm{Fr}^q$.

Proposition 7.8: *Let q be a prime power.*

(1) *The theory of mock-Fr^q periodic fields is consistent and complete.*
(2) *If K is a mock-$\mathbb{F}_q$ and σ is the mock Frobenius, then $(K^{\mathrm{alg}}, \sigma)$ is a mock-Fr^q. Every mock-Fr^q arises this way.*

Proof. (1) Mock-Fr^q fields exist because we can embed Fr^q into an existentially closed periodic field. Any two mock-Fr^q fields are elementarily equivalent by Lemma 3.5.
(2) Clear from Proposition 3.4 and the definitions. ∎

7.2. The principal Euler characteristic. Dwork proved the following part of the Weil conjectures, in [7].

Fact 7.9 (Dwork): *If V is a variety over $\mathbb{F}_q$, then there are non-zero algebraic integers $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_{m'}$ such that for every n,*

$$|V(\mathbb{F}_{q^n})| = \alpha_1^n + \cdots + \alpha_m^n - \beta_1^n - \cdots - \beta_{m'}^n.$$

There is no assumption that V is smooth, proper, or connected.

Fix a copy $\mathbb{Q}^{\mathrm{alg}}$ of the algebraic numbers. For each prime ℓ, fix an extension of the ℓ-adic valuation v_ℓ from $\mathbb{Q}$ to $\mathbb{Q}^{\mathrm{alg}}$. Note that v_ℓ is non-negative on the algebraic integers.

Lemma 7.10: *Let V, α_i, β_j be as in Fact 7.9. Let (K_∞, σ) be a mock Fr^q, and let χ_ℓ be the ℓ-adic part of the canonical Euler characteristic on K. Then*

$$\chi_\ell(V(K_1)) = \alpha_1' + \cdots + \alpha_m' - \beta_1' - \cdots - \beta_{m'}', \tag{3}$$

where

$$\alpha_i' = \begin{cases} \alpha_i, & v_\ell(\alpha_i) = 0, \\ 0, & v_\ell(\alpha_i) > 0; \end{cases}$$

$$\beta_i' = \begin{cases} \beta_i, & v_\ell(\beta_i) = 0, \\ 0, & v_\ell(\beta_i) > 0. \end{cases}$$

In other words, $\chi_\ell(V(K_1))$ is obtained from $|V(\mathbb{F}_q)|$ by dropping the terms of positive ℓ-adic valuation.

Proof. Take a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{N}$, concentrating on the sets $1+n\mathbb{Z}$ for every non-zero ideal $n\mathbb{Z}$. It suffices to prove the following two Claims:

CLAIM 7.11: *The ultralimit of $|V(\mathbb{F}_{q^n})|$ in $\mathbb{Z}_\ell$ is given by the right-hand side of* (3).

CLAIM 7.12: *The ultralimit of $|V(\mathbb{F}_{q^n})|$ in $\mathbb{Z}_\ell$ is given by the left-hand side of* (3).

Claim 7.11 follows from a direct calculation. Claim 7.12 holds because the theory of K is the limit of the theory of Fr^{q^n} as $n \to \mathcal{U}$. We leave the details as an exercise to the reader. ∎

LEMMA 7.13: *Let (K_∞, σ) be a mock-Fr^q.*

(1) *If C is a curve over $\mathbb{F}_q$, and $\alpha_1, \ldots, \alpha_{2g}$ are the characteristic roots of the qth-power Frobenius, then the prime-to-p part of $\chi(C(K_1))$ equals $|C(\mathbb{F}_q)|$.*
(2) *If V is a 1-dimensional variety over $\mathbb{F}_q$, then the prime-to-p part of $\chi(V(K_1))$ equals $|V(\mathbb{F}_q)|$.*
(3) *If X is an Fr^q-definable subset of K_1, then the prime-to-p part of $\chi(X)$ equals $|X \cap \mathbb{F}_q|$.*

Proof.

(1) By the Weil conjectures for curves [12, Appendix C, §1], we know that

$$C(\mathbb{F}_{q^n}) = 1 - \alpha_1^n - \cdots - \alpha_{2g}^n + q^n$$

for all n. Moreover, the Poincaré duality part of the Weil conjectures gives an equality of multi-sets:

$$\{\alpha_1, \ldots, \alpha_{2g}\} = \{q/\alpha_1, \ldots, q/\alpha_{2g}\}.$$

It follows that each α_i has ℓ-adic valuation 0, for ℓ prime-to-p. Therefore, by Lemma 7.10, the ℓ-adic part of $\chi(C(K_1))$ agrees with $|C(\mathbb{F}_q)|$.

(2) An exercise using Part (1) and Fact 3.9 (applied to the field $\mathbb{F}_q$).

(3) By Proposition 3.7, there is a quasi-finite morphism $V \to \mathbb{A}^1_{\mathbb{F}_q}$ of $\mathbb{F}_q$-varieties such that X is the image of

$$V(K_1) \to \mathbb{A}^1(K_1) = K_1.$$

For each n, let V_n be the fiber product of n copies of V over $\mathbb{A}^1$. Then $V_n \to \mathbb{A}^1_{\mathbb{F}_q}$ is still quasi-finite, so V_n has dimension at most 1. By Part (2), $\chi(V_n(K_1)) = |V_n(\mathbb{F}_q)|$.

Now use the argument of Lemma 4.5. Let $f : V(K_1) \to X$ be the surjection induced by $V \to \mathbb{A}^1$. Let X_k be the definable set of $a \in X$ such that the fiber $f^{-1}(a)$ has size k. Note that if $a \in X \cap \mathbb{F}_q$, then every point in the fiber is field-theoretically algebraic over a, hence in $V(\mathbb{F}_q)$.

The upshot is that the fibers of $V(\mathbb{F}_q) \to (X \cap \mathbb{F}_q)$ have size k over $X_k \cap \mathbb{F}_q$, and more generally the fibers of $V_n(\mathbb{F}_q) \to (X \cap \mathbb{F}_q)$ have size k^n over $X_k \cap \mathbb{F}_q$. Therefore,

$$|V_n(\mathbb{F}_q)| = \sum_k k^n \cdot |X_k \cap \mathbb{F}_q|,$$
$$\chi(V_n(K_1)) = \sum_k k^n \cdot \chi(X_k),$$

where the second line is as in the proof of Lemma 4.5. By Part (2), the left hand sides agree. By the invertibility of Vandermonde matrices, it follows that $\chi(X_k) = |X_k \cap \mathbb{F}_q|$. Summing over k, we see

$$\chi(X) = |X \cap \mathbb{F}_q|. \qquad \blacksquare$$

PROPOSITION 7.14: *Let K be a mock-$\mathbb{F}_q$. Let χ be the principal Euler characterisic on K. For any $\mathbb{F}_q$-definable set $X \subseteq K^n$, we have*

$$\chi(X) = |X \cap \mathbb{F}_q^n|.$$

In particular, $\chi(X) \in \mathbb{Z}$.

Proof. Proceed by induction on n. For the base case $n=1$, expand K to a mock-Fr^q by Proposition 7.8.(2), and then apply Lemma 7.13.(3). Suppose $n>1$. For $a \in K_1$, let X_a denote the slice of X over a:

$$X_a = \{\vec{b} \in (K_1)^{n-1} : (a, \vec{b}) \in X\}.$$

Fix ℓ^k, and work with χ modulo ℓ^k. For $i \in \mathbb{Z}/\ell^k$, let S_i be the set of $a \in K_1$ such that $\chi(X_a) \equiv i \pmod{\ell^k}$. Each set S_i is $\mathbb{F}_q$-definable, so by induction $\chi(S_i) = |S_i \cap \mathbb{F}_q|$. Now for $a \in S_i \cap \mathbb{F}_q$, the set X_a is $\mathbb{F}_q$-definable, so by

induction $\chi(X_a) = |X_a \cap \mathbb{F}_q^{n-1}|$. Then the following holds modulo ℓ^k:

$$\begin{aligned}\chi(X) &\equiv \sum_{i\in\mathbb{Z}/\ell^k} i\cdot\chi(S_i) \equiv \sum_{i\in\mathbb{Z}/\ell^k} i\cdot|S_i\cap\mathbb{F}_q| \\ &\equiv \sum_{i\in\mathbb{Z}/\ell^k}\sum_{a\in S_i\cap\mathbb{F}_q} i \equiv \sum_{i\in\mathbb{Z}/\ell^k}\sum_{a\in S_i\cap\mathbb{F}_q}\chi(X_a) \\ &\equiv \sum_{a\in\mathbb{F}_q}\chi(X_a) \equiv \sum_{a\in\mathbb{F}_q}|X_a\cap\mathbb{F}_q^{n-1}|.\end{aligned}$$

The final sum is $|X \cap \mathbb{F}_q^n|$. ∎

This lets us simplify Lemma 7.10:

COROLLARY 7.15: *Let V, α_i, β_j be as in Fact 7.9. Let F be a mock $\mathbb{F}_q$, and χ be its principal Euler characteristic. Then*

$$\chi(V(F)) = \alpha_1 + \cdots + \alpha_m - \beta_1 - \cdots - \beta_{m'}.$$

This implies something about the numbers appearing in Dwork's theorem.

COROLLARY 7.16: *If V is a variety over $\mathbb{F}_q$, then the α_i and β_j of Fact 7.9 have ℓ-adic valuation zero for ℓ prime-to-q.*

Proof. Let α_i' and β_i' be as in Lemma 7.10. Let F be a mock-$\mathbb{F}_q$, and χ_ℓ be the ℓ-adic part of the principal Euler characteristic. Comparing Lemma 7.10 and Corollary 7.15, we see that

$$\alpha_1' + \cdots + \alpha_m' - \beta_1' - \cdots - \beta_{m'}' = \alpha_1 + \cdots + \alpha_m - \beta_1 - \cdots - \beta_{m'}.$$

Replacing $\mathbb{F}_q$ with $\mathbb{F}_{q^n}$ changes α_i to α_i^n and α_i' to $(\alpha_i')^n$. Therefore, the following holds for any $n \geq 1$:

$$(\alpha_1')^n + \cdots + (\alpha_m')^n - (\beta_1')^n - \cdots - (\beta_{m'}')^n = \alpha_1^n + \cdots + \alpha_m^n - \beta_1^n - \cdots - \beta_{m'}^n.$$

Comparing Poincaré series, one gets equality of multisets

$$\{\alpha_1', \ldots, \alpha_m'\} = \{\alpha_1, \ldots, \alpha_m\},$$
$$\{\beta_1', \ldots, \beta_{m'}'\} = \{\beta_1, \ldots, \beta_{m'}\}.$$

Therefore, none of the α_i' or β_i' are zero, and every α_i and β_i has ℓ-adic valuation 0. ∎

Remark 7.17: Corollary 7.16 can be proven using ℓ-adic cohomology, but the proof given here is more elementary.

7.3. The dual Euler characteristic. Let K be a mock-$\mathbb{F}_q$. Recall that the **dual Euler characteristic** on K is the prime-to-q part of the canonical Euler characteristic induced by σ^{-1}, where σ is the mock Frobenius.

Lemma 7.18: *Let V be a variety over $\mathbb{F}_q$, and let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_{m'}$ be the algebraic integers from Fact 7.9. Let K be a mock-$\mathbb{F}_q$ and let $\chi^\dagger$ be the dual Euler characteristic. Then*

$$\chi^\dagger(V(K)) = \alpha_1^{-1} + \cdots + \alpha_m^{-1} - \beta_1^{-1} - \cdots - \beta_{m'}^{-1}.$$

Moreover, this value is rational.

Proof. Similar to Lemma 7.10, but using an ultrafilter that concentrates on $-1 + n\mathbb{Z}$ for all n. Corollary 7.16 ensures that $v_\ell(\alpha_i) = 0$ for all i, so there is no need for any α_i''s or β_i''s. Rationality is an easy exercise, using the fact that

$$\alpha_1^n + \cdots + \alpha_m^n - \beta_1^n - \cdots - \beta_{m'}^n \in \mathbb{Z}$$

for all $n \in \mathbb{N}$. ∎

Proposition 7.19: *If K is a mock-$\mathbb{F}_q$ and $\chi^\dagger$ is the dual Euler characteristic on K, then $\chi^\dagger(X) \in \mathbb{Q}$ for every $\mathbb{F}_q$-definable set X.*

Proof. If X is the set of K-points in some $\mathbb{F}_q$-definable variety, this follows from Lemma 7.18.

If X is a definable subset of K^n, then Proposition 3.7 yields a quasi-finite morphism $V \to \mathbb{A}^n$ of varieties over $\mathbb{F}_q$, such that X is the image of $V(K_1) \to \mathbb{A}^n(K_1)$. Let V_n be the n-fold fiber product of V over $\mathbb{A}^1$. By the argument of Lemma 4.5, $\chi^\dagger(X)$ is given by some rational linear combination of the $\chi^\dagger(V_n(K))$. ∎

Example 7.20: If V is a d-dimensional smooth projective variety over $\mathbb{F}_q$, then the following identities of multisets hold by the Poincaré duality part of the Weil conjectures:

$$\{\alpha_1, \ldots, \alpha_m\} = \{q^d/\alpha_1, \ldots, q^d/\alpha_m\},$$
$$\{\beta_1, \ldots, \beta_{m'}\} = \{q^d/\beta_1, \ldots, q^d/\beta_{m'}\}.$$

Therefore, for K a mock-$\mathbb{F}_q$ with dual Euler characteristic $\chi^\dagger$,

$$\begin{aligned}\chi^\dagger(V(K)) &= \alpha_1^{-1} + \cdots + \alpha_m^{-1} - \beta_1^{-1} - \cdots - \beta_{m'}^{-1} \\ &= (\alpha_1 + \cdots + \alpha_m - \beta_1 - \cdots - \beta_{m'})/q^d = |V(\mathbb{F}_q)|/q^d.\end{aligned}$$

Putting everything together, we have proven:

THEOREM (Theorem 1.6): *Let K be a mock-$\mathbb{F}_q$, for some prime power $q = p^k$. There are two $\mathbb{Z}_{\neg p}$-valued $\emptyset$-definable strong Euler characteristics χ and $\chi^\dagger$ on K, such that*

(1) *If V is a smooth projective variety over $\mathbb{F}_q$, then*

$$\chi(V(K)) = |V(\mathbb{F}_q)|,$$
$$\chi^\dagger(V(K)) = |V(\mathbb{F}_q)|/q^{\dim V}.$$

(2) *If X is any $\mathbb{F}_q$-definable set, then*

$$\chi(X) = |X \cap \operatorname{dcl}(\mathbb{F}_q)|.$$

In particular, $\chi(X) \in \mathbb{Z}$.

(3) *If X is any $\mathbb{F}_q$-definable set, then $\chi^\dagger(X) \in \mathbb{Q}$.*

Example 7.20 can be generalized to arbitrary pseudofinite fields:

PROPOSITION 7.21: *Let K be a pseudofinite field, and σ be a topological generator of* $\mathrm{Gal}(K)$. *Let χ and $\chi^\dagger$ be the $\hat{\mathbb{Z}}$-valued Euler characteristics associated to σ and σ^{-1}, or the prime-to-p-parts if* $\mathrm{char}(K) = p > 0$. *Let V be a smooth projective variety over K. Then $\chi(K)$ is invertible in $\hat{\mathbb{Z}}$ or $\mathbb{Z}_{\neg p}$, and*

$$\chi^\dagger(V(K)) = \chi(V(K))\chi(K)^{-\dim(V)}. \tag{4}$$

Proof. By Axiom 5 in §4.1, $\chi(K)$ is given by the trace of σ on torsion in $\mathbb{G}_m(K^{\mathrm{alg}})$. This trace is invertible, because σ is invertible and the torsion has rank 1 (away from the characteristic). So $\chi(K)$ is invertible in $\hat{\mathbb{Z}}$ or $\mathbb{Z}_{\neg p}$. The identity (4) can be expressed by a conjunction of first-order sentences in the language of $(K^{\mathrm{alg}}, \sigma) \models \mathrm{ACPF}$. Indeed, this follows by the definability of χ and $\chi^\dagger$, and the fact that the family of smooth projective d-dimensional varieties is uniformly ind-definable. Now, when $(K^{\mathrm{alg}}, \sigma)$ is a mock Frobenius periodic field, (4) holds by Example 7.20. But every model of ACPF is elementarily equivalent to an ultraproduct of mock Frobenius periodic fields, by an argument similar to Lemma 3.13. ∎

Proposition 7.21 could probably also be derived using Conjecture 6.3.

Remark 7.22: Both Proposition 7.21 and Example 7.20 seem closely related to Bittner's duality involution on the Grothendieck group of varieties [3]. When V is a d-dimensional smooth projective variety, this involution sends $[V]$ to $[V]\cdot\mathbb{L}^{-d}$, where $\mathbb{L} = [\mathbb{A}^1]$.

8. Directions for future research

There are several immediate directions for future research. The most important next step is verifying Conjecture 5.2, completing the proof that the $\mathcal{L}^{\mu}_{\text{rings}}$-theory of finite fields is decidable (Theorem 1.2). This will hopefully be carried out in [16]. Another key task is to relate the $\mathbb{Z}_\ell$-valued Euler characteristic to ℓ-adic étale cohomology (Conjecture 6.3).

Another interesting direction is the following variant of Theorem 1.2:

CONJECTURE 8.1: *The $\mathcal{L}^{\mu}_{\text{rings}}$-theory of the rings $\mathbb{Z}/n\mathbb{Z}$ is decidable.*

Lastly, it may be possible to generalize the definability of the canonical Euler characteristic from ACPF to its expansion ACFA. Although ACFA is not pseudofinite, its models are ultraproducts of Frobenius difference fields [15], and definable sets of finite rank are naturally pseudofinite.

8.1. INTERACTIONS WITH NUMBER THEORY? We have relied heavily on algebraic geometry and number theory to prove a relatively simple model-theoretic fact. One could dream of reversing the process to obtain new results in number theory. Ultraproducts of finite fields are not the only source of pseudofinite fields. For example, if σ is chosen randomly in $\text{Gal}(\mathbb{Q})$, then $(\mathbb{Q}^{\text{alg}}, \sigma) \models \text{ACPF}$ with probability 1, by [11, §16.6]. Perhaps one can prove non-trivial facts by reasoning about nonstandard sizes of definable sets in these structures.

Unfortunately, we have probably done nothing interesting from a number-theoretic point of view. The nonstandard "sizes" on pseudofinite fields should be a simple artifact of étale cohomology, by Conjecture 6.3. Étale cohomology is already well-understood. Combinatorial facts about sizes correspond to well-known facts about cohomology. The fact that $\chi(X \times Y) = \chi(X) \cdot \chi(Y)$ corresponds to the Künneth formula. When $f : E \to B$ is a morphism, the strong Euler characteristic property allows us to calculate the "size" of E by "integrating" the "sizes" of the fibers over B. This property corresponds to the Leray spectral sequence.

One tool which might be new on the model-theoretic side is elimination of imaginaries, which holds in ACPF by work of Hrushovski [14]. When X is interpretable, or definable with quantifiers, we know that $\chi(X)$ is "integral," lying in $\hat{\mathbb{Z}}$ rather than $\hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$. There may be some number-theoretic content to this.

It feels as if there could be some connection between the canonical Euler characteristic and p-adic L-functions. The classical L-functions associated to number fields and elliptic curves are defined in terms of point counting. In some cases, these L-functions can be converted to p-adic analytic functions by extrapolating the values at negative integers. Insofar as we are counting points on varieties mod p^k, there is a spiritual connection to the p-adic part of the canonical Euler characteristic.

Moreover, p-adic integration appears in both contexts. If χ is a strong $\mathbb{Z}_p$-valued Euler characteristic, and $f : E \to B$ is a definable function, then χ induces a p-adic measure μ on B, and one can calculate $\chi(E)$ by p-adic integration

$$\chi(E) = \int_{x \in B} \chi(f^{-1}(x))\, d\mu(x).$$

This was essentially how $\chi(X)$ was calculated in Lemma 4.6. Meanwhile, p-adic integration plays a key role in the theory of p-adic L-functions. For example, the Riemann zeta function is given on negative integers by a p-adic Mellin transform: there is some $c \in \mathbb{Z}_p^\times$ and p-adic measure μ on $\mathbb{Z}_p$ such that for positive integers k,

$$\zeta(-k) = \frac{1}{1 - c^{k+1}} \int_{\mathbb{Z}_p} x^k \, d\mu(x). \tag{5}$$

This Mellin transform is the underlying reason why the Kubota–Leopoldt p-adic zeta function exists. In some cases, the measure μ can be given a pseudofinite interpretation. For example, if p is odd and α is a nonstandard integer whose p-adic standard part is $-1/2$, then $\zeta(-k)$ is given by the p-adic standard part of the sum

$$\frac{1}{2 - 2^{-k}} \sum_{n=1}^{\alpha} n^k.$$

In other words, (5) holds with $c = 1/2$ and μ equal to (half) the nonstandard counting measure on the pseudofinite set $\{1, 2, \ldots, \alpha\}$.

Thus there are several vague connections between the canonical Euler characteristic on pseudofinite fields, and p-adic L-functions. I lack the expertise to pursue this connection further.

References

[1] O. M. Alshanqiti, *Pseudo-finite rings and their generalizations*, Ph.D. thesis, University of Manchester, 2015.

[2] J. Ax, *The elementary theory of finite fields*, Annals of Mathematics **88** (1968), 239–271.

[3] F. Bittner, *The universal euler characteristic for varieties of characteristic zero*, Compositio Mathematica **140** (2004), 1011–1032.

[4] Z. Chatzidakis and E. Hrushovski, *Model theory of difference fields*, Transactions of the American Mathematical Society **351** (1999), 2997–3071.

[5] Z. Chatzidakis, L. van den Dries and A. Macintyre, *Definable sets over finite fields*, Journal für die reine und angewandte Mathematik **427** (1992), 107–135.

[6] J. Denef and F. Loeser, *Definable sets, motives, and p-adic integrals*, Journal of the American Mathematical Society **14** (2000), 429–629.

[7] B. M. Dwork, *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics **82** (1960), 631–648.

[8] R. Elwes and D. Macpherson, *A survey of asymptotic classes and measurable structures*, in *Model Theory with Applications to Algebra and Analysis. Vo. 2*, London Mathematical Society Lecture Note Series, Vol. 350 Cambridge University Press, Cambridge, 2008, pp. 125–160.

[9] E. Freitag and R. Kiehl, *Étale Cohomology and the Weil Conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 13, Springer, Berlin, 1988.

[10] J. Freitag, W. Li and T. Scanlon, *Differential Chow varieties exist*, Journal of the London Mathematical Society **95** (2016), 128–156.

[11] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 11, Springer, Berlin, 2008.

[12] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Vol. 52, Springer, New York–Heidelberg, 1977.

[13] W. Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1993.

[14] E. Hrushovski, *Pseudo-finite fields and related structures*, in *Model theory and Applications*, Quaderni di matematica, Vol. 11, Aracne, Rome, 2002.

[15] E. Hrushovski, *The elementary theory of the Frobenius automorphisms*, `https://arxiv.org/abs/math/0406514`.

[16] W. Johnson and T. Xu, *Computable ind-definability*, work in progress.

[17] C. Kiefe, *Sets definable over finite fields: their zeta-functions*, Transactions of the American Mathematical Society **223** (1976), 45–59.

[18] J. Krajíček, *Uniform families of polynomial equations over a finite field and structures admitting an euler characteristic of definable sets*, Proceedings of the London Mathematical Society **3** (2000), 257–284.

[19] J. Krajíček and T. Scanlon, *Combinatorics with definable sets: Euler characteristics and Grothendieck rings*, Bulletin of Symbolic Logic **6** (2000), 311–330.

[20] J. S. Milne, *Abelian Varieties*, Course notes, `https://www.jmilne.org/math/CourseNotes/av.html`.

[21] D. Mumford, *Abelian Varieties*, Studies in Mathematics, Vol. 5, Tata Institute of Fundamental Research, Bombay, 1970.

[22] R. Pink, *Finite group schemes and p-divisible groups*, Course notes, `http://www.math.ethz.ch/~pink/FiniteGroupSchemes.html`.

[23] J.-P. Serre, *Algebraic Groups and Class Fields*, Graduate Texts in Mathematics, Vol. 117, Springer, New York, 1988.