COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **42** (2) (2022) 203–236
DOI: 10.1007/s00493-021-4547-0

AN ANALYTIC APPROACH TO CARDINALITIES OF SUMSETS

DÁVID MATOLCSI, IMRE Z. RUZSA, GEORGE SHAKAN,
DMITRII ZHELEZOV

Received November 1, 2020
Revised January 17, 2021
Online First January 14, 2022

Let d be a positive integer and $U \subset \mathbb{Z}^d$ finite. We study

$$\beta(U) := \inf_{\substack{A,B \neq \emptyset \\ \text{finite}}} \frac{|A+B+U|}{|A|^{1/2}|B|^{1/2}},$$

and other related quantities. We employ tensorization, which is not available for the doubling constant, $|U+U|/|U|$. For instance, we show

$$\beta(U) = |U|,$$

whenever U is a subset of $\{0,1\}^d$. Our methods parallel those used for the Prékopa–Leindler inequality, an integral variant of the Brunn–Minkowski inequality.

1. Introduction

The aim of this study is to understand the nature of structures in $\mathbb{Z}^d$, the presence of which implies that the sumset must be large. The archetype is Freiman's theorem that if a set $A \subset \mathbb{Z}^d$ is proper d-dimensional, then

$$|A+A| \geq (d+1)|A| - \binom{d+1}{2}. \tag{1}$$

The assumption on dimension can be expressed as $S_d \subset A$ for a d-dimensional simplex S_d. In general, the *induced doubling* of a set U is the quantity

$$\inf_{A \supset U} \frac{|A+A|}{|A|};$$

Mathematics Subject Classification (2010): 11B13, 11B75 our main aim is to give lower estimates for it and related quantities. Applications for the sum-product problem, related to the work of [1], will be the subject of another paper.

While our main interest is in $\mathbb{Z}^d$, we shall mostly formulate our results for general, typically torsion-free commutative groups. Since we work with finite sets and a finitely generated torsion-free group is isomorphic to some $\mathbb{Z}^d$, it is not more general, but we rarely need the coordinates.

In the first part we work with sets, in the second part we study a weighted version which will be necessary for the proof of the main results. By introducing a weighted analog, we will be able to use *tensorization*: that is we prove a d dimensional inequality by induction on dimension alongside a two point inequality. This is a method commonly used in analysis, for instance, in the Prékopa–Leindler inequality [14] and Beckner's inequality [3]. We discuss this more below, but also invite the reader to the excellent survey paper of Gardner [4].

Part I: sets

2. Main results

Let U be a finite set in a commutative group G. We modify the above definition of induced doubling to use sums of different sets, which are often better behaved.

Definition 2.1 (Induced doubling). The *induced doublings* of U are the quantities

$$\alpha(U) = \inf_{A \supset U, B \supset U} \frac{|A+B|}{\sqrt{|A||B|}},$$

the (unrestricted) *induced doubling*;

$$\alpha'(U) = \inf_{A \supset U, B \supset U,\ |A|=|B|} \frac{|A+B|}{|A|},$$

the *isometric induced doubling*;

$$\alpha''(U) = \inf_{A \supset U} \frac{|A+A|}{|A|},$$

the *isomeric induced doubling.*

Conjecture 2.2. In the above definitions, the infimum is a minimum.

We rarely can estimate induced doubling directly, typically, it will be through a related quantity involving the sum of three sets.

Definition 2.3 (Induced tripling β). The *triplings* of U are the quantities

$$\beta(U) = \inf_{A,B} \frac{|A+B+U|}{\sqrt{|A||B|}},$$

the *(unrestricted) tripling*;

$$\beta'(U) = \inf_{A,B,\ |A|=|B|} \frac{|A+B+U|}{\sqrt{|A||B|}},$$

the *isometric tripling*;

$$\beta''(U) = \inf_{A} \frac{|A+A+U|}{|A|},$$

the *isomeric tripling.*

These infima may and may not be minima. Estimates we later derive for β are weaker than the obvious $\max(|A|,|B|)$ when the sizes of A and B are rather different. Thus, we also consider an asymmetric version as follows.

Definition 2.4 (Asymmetric induced tripling β_p). For $1<p<\infty$ we put

$$\beta_p(U) = \inf_{A,B} \frac{|A+B+U|}{|A|^{1/p}|B|^{1-1/p}}.$$

Thus $\beta(U)=\beta_2(U)$. We shall estimate these quantities rather preciesly for sets contained in *quasicubes*, which we define recursively as follows.

Definition 2.5 (Quasicubes). A 0-dimensional quasicube is any singleton.

Let U be a finite set in a commutative group G. We say that U is a d-dimensional quasicube, if there is a proper subgroup G' such that U is contained in two distinct cosets, say $G'+x$ and $G'+y$, both $U\cap(G'+x)$ and $U\cap(G'+y)$ are $(d-1)$-dimensional quasicubes and $x-y$ is of infinite order in the factor-group G/G'.

For instance, in $\mathbb{Z}^2$ any four points that lie on two distinct parallel lines (i.e., a trapezoid) form a quasicube. A d-dimensional quasicube has 2^d elements, and its dimension is indeed d according to the following definition.

Definition 2.6 (Set dimension). Let A be a finite set in a commutative group G. Let H be the subgroup generated by $A-A$, that is, the smallest group H with the property that A lies in a single coset of H. As a finitely generated group, H is isomorphic to some $H'\times\mathbb{Z}^d$, where H' is a torsion group. We call $d=\dim A$ the dimension of A.

The central result of the present paper is that subsets of quasicubes induce large additive doubling and tripling. Indeed much of what we prove was known for cubes in [7], but their geometric methods do no extend to quasicubes (or subsets of quasicubes).

Theorem 2.7 (Subsets of quasicubes have maximal β). *Let U be a d-dimensional quasicube in any commutative group. For every $V \subset U$ we have*

$$\beta(V) = |V|, \quad \alpha(V) \geq |V|^{1/2}. \tag{2}$$

In particular,

$$\beta(U) = 2^d, \quad \alpha(U) \geq 2^{d/2}.$$

A short streamlined self-contained proof of Theorem 2.7 can also be found in a follow up paper of Green and the authors [6].

The main innovation of the tripling β is that it allows one to efficiently account for the additive expansion of the lower dimensional subsets (fibers) of U in a recursive fashion. The core estimate is Theorem 11.1, where we show that a certain functional is minimized by geometric progressions.

The power of Theorem 2.7 comes from the fact that the estimates (2) do not depend on the dimension of U or V. It is utilised in [15] to give a structural result for sets with up to polynomially large additive doubling, the regime not amenable for traditional methods like Fourier analysis. The structural result was in turn used in [9] and [15] as a drop-in replacement for the notoriously involved multi-scale device introduced by Bourgain and Chang [1] to tackle the Erdős–Szemerédi conjecture.

In comparison, the authors of [1] implicitly analysed a quantity similar to α but resorted to iterative dyadic pigeonholing, with compounded logarithmic losses leading to a significantly worse estimate. In particular, such an analysis would give non-trivial bounds only for well-balanced quasicubes with all the lower-dimensional fibers being of comparable size and thus extracting structural information using methods of [1] had been problematic.

As a corollary of Theorem 2.7, it follows that iterated sumsets of quasicube sumsets grow logarithmically, which is essentially sharp.

Corollary 2.8 (Quasicubes have large iterated sumset). *Let U be a d-dimensional quasicube in any commutative group. For every $V \subset U$ and $k \geq 2$ we have*

$$|(2^k - 1)V| \geq |V|^k.$$

Proof. The base case $k=2$ follows from the definition of β and Theorem 2.7. For larger k, one has

$$\begin{aligned}|(2^k-1)V| &= |(2^{k-1}-1)V+(2^{k-1}-1)V+V|\\ &\geq |(2^{k-1}-1)V|\beta(V) \geq |V|^k.\end{aligned}$$ ∎

The trivial bound

$$\beta(U) \leq \min(|U|, 2^d) \tag{3}$$

holds for any set U of dimension d, so the induced tripling (i.e. β) of quasicube subsets is as large as it gets. We conjecture that this holds for a larger class of sets.

Conjecture 2.9 (Log-span conjecture). Let V be a finite set with the property that for any $k \leq \dim V$, any k-dimensional subset of V has at most 2^k elements. Then

$$\beta(V) = |V| \tag{4}$$

and in particular,

$$\alpha(V) \geq |V|^{1/2}.$$

We conjecture that in fact β is determined by the linear dependence matroid of the set in question, in the following sense.

Conjecture 2.10 (Linear matroid conjecture). Let U, V be finite sets of equal cardinality in any group, $\varphi\colon U \to V$ a bijection. If for every $U' \subset U$ we have $\dim \varphi(U') \leq \dim U'$, then $\beta(V) \leq \beta(U)$. In particular, if always $\dim \varphi(U') = \dim U'$, then $\beta(V) = \beta(U)$.

Note that Conjecture 2.9 would follow quickly from Conjecture 2.10 and Theorem 2.7.

Theorem 2.11 (Discrete Prékopa–Leindler for quasicubes). *Fix* $1 < p < \infty$ *and let* q *be the conjugate exponent defined via*

$$1/p + 1/q = 1.$$

Let U *be a* d*-dimensional quasicube in any commutative group and* $V \subset U$*. We have*

$$\beta_p(V) \geq c_p^d |V|, \quad \text{where } c_p = \frac{p^{1/p} q^{1/q}}{2} \leq 1.$$

The flexibility of choosing p allows us to deduce the following discrete Brunn–Minkowski inequality.

Corollary 2.12 (Discrete Brunn–Minkowski for quasicubes). *Let U be a subset of a d-dimensional quasicube in any commutative group. For any finite sets A, B we have*

$$|A+B+U|^{1/d} \geq \frac{|U|}{2^d}\left(|A|^{1/d}+|B|^{1/d}\right).$$

Note if U is a quasicube, then $|U|=2^d$, and we obtain

$$|A+B+U|^{1/d} \geq |A|^{1/d}+|B|^{1/d}.$$

This result was obtained for cubes by Green and Tao [7, Lemma 2.4]. Their methods, which rely on the continuous Brunn–Minkowski inequality, seem to not generalize to quasicubes. We remark that our results are somewhat in a similar spirit to that of [2, Section 5], where lower bounds for sumsets of subsets of $\{0,\ldots,M-1\}^d$ are provided.

The reader may also see [8,12,10,11] for other work on discrete-type Brunn–Minkowski inequalities. For instance, in [8], they prove an inequality of the form

$$|\overline{A}+B| \geq |A|^{1/d}+|B|^{1/d}, \tag{5}$$

for finite and non-empty subsets of $\mathbb{Z}^d$. One can check that $\overline{U}$ has much different structure than U for general quasicubes. Indeed Theorem 2.7 is most useful for small and medium-sized subsets of a quasicube, while $\overline{U}$ always essentially contains a quasicube and thus is of size exponential in the dimension. Some comparison of (5) to [7] may be found at the end of [11]. Also in [11], they study lower bounds for $|A+B|$ where A and B are the intersection of a convex set with $\mathbb{Z}^d$. For instance, they prove the following.

Theorem 2.13 ([11]). *Let $K, L \subset \mathbb{R}^d$ be non-empty and bounded. Then for any $\lambda \in (0,1)$, one has*

$$|(\lambda\cdot K+(1-\lambda)\cdot L+(-1,1)^d)\cap\mathbb{Z}^d| \geq \lambda|K\cap\mathbb{Z}^d|^{1/d}+(1-\lambda)|L\cap\mathbb{Z}^d|^{1/d}.$$

Theorem 2.13 is another successful instance of the Brunn–Minkowski inequality and is well suited for integers defined by bounded sets. While there are several differences to the current work, the main one is that the structure in the additional summand, $(-1,1)^d$, present in Theorem 2.13 is relaxed considerably. We do highlight, however, that in Theorem 2.7 and Theorem 2.13, one proceeds by formulating a functional analog and tensorization.

Proof of Corollary 2.12. Apply the inequality from Theorem 2.11,

$$|A+B+U| \geq \frac{|U|c_p^d}{2^d}|A|^{1/p}|B|^{1/q}$$

with the optimal choice of p which is defined by

$$1/p = \frac{|A|^{1/d}}{|A|^{1/d}+|B|^{1/d}}. \qquad \blacksquare$$

Theorem 2.11 can be viewed as a discrete Prékopa–Leindler inequality, which we recall (see also [4, Theorem 4.2]).

Theorem 2.14 (Prékopa–Leindler [14]). *Let* $0<\lambda<1$ *and*

$$g, h, F\colon \mathbb{R}^d \to \mathbb{R},$$

be non-negative measurable functions satisfying for all $x, y \in \mathbb{R}^d$

$$F((1-\lambda)x+\lambda y) \geq f(x)g(y).$$

Then

$$\int F \geq \|f\|_p \|g\|_q,$$

with $p=1/\lambda$ *and* $1/p+1/q=1$.

Note that Theorem 2.14 can be used to deduce the Brunn–Minkowski inequality, in a similar manner to Corollary 2.12. Theorem 2.11 can be intepreted to be a discrete analog of Theorem 2.14.

3. Inequalities between doublings and triplings

We conjecture that the defined six quantities are actually only two, and connected by simple inequalities.

Conjecture 3.1 (Doubling-tripling conjecture). For every finite set U in any commutative group we have

$$\alpha(U)=\alpha'(U)=\alpha''(U) \leq \beta(U)=\beta'(U)=\beta''(U) \leq \alpha(U)^2.$$

We list some properties.

Statement 3.2 (Basic Inequalities). *Let V be a finite set in a commutative group G, $|V|=n$, $\dim V=d$. We have*

$$\alpha(V) \le \alpha'(V) \le \alpha''(V) \begin{cases} < 2^d, \\ \le (n+1)/2, \end{cases}$$

$$d+1 \le \beta(V) \le \beta'(V) \le \beta''(V) \begin{cases} \le 2^d, \\ \le n. \end{cases}$$

Proof. The inequalities

$$\alpha(V) \le \alpha'(V) \le \alpha''(V), \quad \beta(V) \le \beta'(V) \le \beta''(V)$$

follow immediately from the definitions. Taking $A=V$ in the definition of $\alpha''(V)$, we have

$$\alpha''(V) \le \frac{|V+V|}{|V|} \le \frac{1}{|V|}\binom{|V|+1}{2} = \frac{n+1}{2}.$$

Taking $A=\{0\}$ in the definition of $\beta''(V)$, we find that

$$\beta''(V) \le |V| = n.$$

Since V has dimension d, we may assume

$$V \subset H' \times \mathbb{Z}^d.$$

Thus for large enough N, we have $V \subset A$, where

$$A := H' \times \{-N, \dots, N\}^d.$$

Since

$$\frac{|A+A|}{|A|} \to 2^d \quad \text{as } N \to \infty,$$

we find that $\alpha''(V) \le 2^d$. Also,

$$A + A + V \subset H' \times \left\{-2N - \max_{v\in V} |v|_\infty, \dots, 2N + \max_{v\in V} |v|_\infty\right\}^d,$$

and so

$$\beta''(V) \le \frac{|A+A+V|}{|A|} \to 2^d \quad \text{as } N \to \infty.$$

Note that $\beta(V) \ge d+1$ follows from the more general Theorem 2.7 which we prove later. ∎

Statement 3.3 (Basic Inequalities II). *For every finite set U in any commutative group we have*

$$\alpha(U) \le \beta(U),\ \alpha'(U) \le 4\beta'(U),\ \alpha''(U) \le 3\beta''(U), \tag{6}$$

$$\beta(U) \le \alpha(U)^2,\ \beta''(U) \le \alpha(U)^3, \tag{7}$$

$$\alpha''(U) \le \alpha(U)^2,\ \beta''(U) \le \beta''(U+U) \le \beta(U)^2. \tag{8}$$

Proof. We may assume $U \subset G = H' \times \mathbb{Z}^d$. If $d=0$, then all

$$1 = \alpha(U) = \alpha'(U) = \alpha''(U) = \beta(U) = \beta'(U) = \beta''(U),$$

so we may assume $d \ge 1$.

We first show the second inequality in (6). Let A, B be such that $|A| = |B|$ and let k be a large integer. Since $d \ge 1$, we may choose a $x \in G$ be such that the sets

$$A + x, \dots, A + kx,$$

are disjoint, and

$$B + x \dots, B + kx,$$

are also disjoint. Indeed, there is a group homomorphism $\pi\colon G \to \mathbb{Z}$ and so such it is enough to establish such an x for subsets of $\mathbb{Z}$. But here we may choose x larger than $\max A - \min A$. Put

$$A' = U \cup \bigcup_{i=1}^{k} (A + ix),\ B' = U \cup \bigcup_{i=1}^{k} (B + ix).$$

These sets satisfy

$$U \subset A', B' \quad \text{and} \quad |A'| = |B'| \ge k|A|.$$

We have

$$A' + B' = (U+U) \cup \bigcup_{i=1}^{k} (A+U+ix) \cup \bigcup_{i=1}^{k} (B+U+ix) \cup \bigcup_{i=2}^{2k} (A+B+ix). \tag{9}$$

As $|A+U|, |B+U|, |A+B|$ are all smaller than $|A+B+U|$, we find

$$|A' + B'| \le |U + U| + (4k-1)|A + B + U|.$$

Thus

$$\frac{|A' + B'|}{|A'|} \le \frac{|U + U|}{k|A|} + \left(4 - \frac{1}{k}\right) \frac{|A + B + U|}{|A|}.$$

As this is true for any A and B with $|A| = |B|$, we find

$$\alpha'(U) \le \frac{|U + U|}{k} + 4\beta'(U),$$

and the second statement of (6) follows from letting $k \to \infty$.

The proof of the third statement of (6), that is $\alpha''(U)\le 3\beta''(U)$, proceeds similarly. The only difference is we take $A=B$ so some parts of (9) coincide and the 4 is reduced to 3.

We could use the same approach to show $\alpha(U)\le 4\beta(U)$. The proof below due to Thomas Bloom allows one to get rid of the factor. We need the following from [13].

Lemma 3.4 (Petridis). *Let X,Y,Z be finite subsets of a commutative group with the property that for all $X'\subset X$, we have*

$$\frac{|X'+Y|}{|X'|}\ge \frac{|X+Y|}{|X|}.$$

Then

$$|X+Y+Z||X|\le |X+Y||X+Z|.$$

Let $A,B\subset G$ be finite with the property that for any $A'\subset A$ and $B'\subset B$

$$\frac{|A+B+V|}{|A|^{1/2}|B|^{1/2}}\le \frac{|A'+B+V|}{|A'|^{1/2}|B|^{1/2}},\quad \frac{|A+B+V|}{|A|^{1/2}|B|^{1/2}}\le \frac{|A+B'+V|}{|A|^{1/2}|B'|^{1/2}}. \tag{10}$$

Using this Lemma, we proceed to prove that $\alpha(V)\le\beta(V)$.

By a standard limiting argument we may assume WLOG that the infimum in the definition of $\beta(V)$ is taken over A,B satisfying (10). This implies in particular that for any $A'\subset A$

$$\frac{|A+B+V|}{|A|}\le \frac{|A'+B+V|}{|A'|}.$$

Applying Lemma 3.4 with $X=A$, $Y=B+V$ and $Z=V$, we conclude

$$|A+B+V+V||A|\le |A+B+V||A+V|,$$

and rearranging gives

$$\frac{|A+V+B+V|}{|A+V|^{1/2}|B+V|^{1/2}}\left(\frac{|B+V|^{1/2}|A|^{1/2}}{|B|^{1/2}|A+V|^{1/2}}\right)\le \frac{|A+B+V|}{|A|^{1/2}|B|^{1/2}}.$$

Applying with the roles of A and B swapped, we also find

$$\frac{|A+V+B+V|}{|A+V|^{1/2}|B+V|^{1/2}}\left(\frac{|A+V|^{1/2}|B|^{1/2}}{|A|^{1/2}|B+V|^{1/2}}\right)\le \frac{|A+B+V|}{|A|^{1/2}|B|^{1/2}},$$

and so

$$\frac{|A+V+B+V|}{|A+V|^{1/2}|B+V|^{1/2}}\le \frac{|A+B+V|}{|A|^{1/2}|B|^{1/2}}.$$

A shifted version of V is included in both $A+V$ and $B+V$, so

$$\alpha(V) \leq \frac{|(A+V)+(B+V)|}{|A+V|^{1/2}|B+V|^{1/2}}.$$

Thus we conclude that

$$\alpha(V) \leq \beta(V).$$

For (7) and (8) we need Plünnecke's inequality.

Lemma 3.5 (Plünnecke). *Let X and Y be subsets of a commutative group. Let k be a positive integer and $|X+Y| = c|X|$. Then there is a $X' \subset X$ such that*

$$|X' + kY| \leq c^k |X'|.$$

In particular,

Lemma 3.6 (Plünnecke). *Let X, Y be finite sets of an additive group. Then there is $X' \subset X$ such that*

$$|Y+Y| \leq |X'+Y+Y| \leq |X'| \frac{|X+Y|^2}{|X|^2} \leq \frac{|X+Y|^2}{|X|}.$$

We now proceed to (7). Let A, B be any sets containing U. After swapping the roles of A and B, we may suppose $|A| \leq |B|$. By Lemma 3.5, there is an $A' \subset A$ such that

$$|A' + 2B| \leq \left(\frac{|A+B|}{|A|}\right)^2 |A'|.$$

As $A' + B + U \subset A' + 2B$, we conclude

$$\beta(U) \leq \frac{|A'+B+U|}{\sqrt{|A'||B|}} \leq \sqrt{\frac{|A'|}{|A|}} \frac{|A+B|^2}{|A||B|} \leq \frac{|A+B|^2}{|A||B|}.$$

As A and B are arbitrary, we conclude

$$\beta(U) \leq \alpha(U)^2.$$

We approach the first inequality in (8) similarly. Let A and B be arbitrary sets containing U. Then by Lemma 3.6

$$\frac{|B+B|}{|B|} \leq \frac{|A+B|^2}{|A||B|},$$

and $\alpha''(U) \leq \alpha(U)^2$ follows.

We now proceed to the second statement of (7). Let A and B be sets containing U with $|B| \le |A|$. By Lemma 3.5 we may find an $A' \subset A$ such that

$$|B+B+U| \le |A'+3B| \le \left(\frac{|A+B|}{|A|}\right)^3 |A|.$$

Dividing both sides by $|B|$ and using $|B| \le |A|$ gives $\beta''(U) \le \alpha(U)^3$.

We now proceed to the second statements of (8). First, $\beta''(U) \le \beta''(2U)$ follows immediately from the definitions. Let A, B be arbitrary with $|B| \le |A|$. We find, by Lemma 3.5, a $B' \subset B$ such that

$$|B' + 2(A+U)| \le \left(\frac{|A+B+U|}{|B|}\right)^2 |B'|,$$

and hence

$$\frac{|2A+2U|}{|A|} \le \frac{|A+B+U|^2}{|A||B|}$$

and so $\beta''(2U) \le \beta(U)^2$ follows. ∎

Problem 3.7. How tight are these inequalities? For the discrete cube $K_d = \{0,1\}^d$ we have $\beta(K_d) = 2^d$, $2^{d/2} \le \alpha(K_d) \le (3/2)^d$, so $\beta \le \alpha^2$ is pretty tight, the exponent is definitely not lower than $\log 2/\log(3/2)$.

4. The independence problem

In the preceding sections we tacitly assumed that the ambient group G is fixed, and the sets A, B in the definition of the α's and β's are taken from this group. Sometimes we shall consider different groups, and the possibility of dependence arises.

For this section we change the notations to $\alpha(U,G)$, to indicate the ambient group (and similarly for all other parameters).

Conjecture 4.1 (The independence hypothesis). Let G be a group, G' its subgroup, $U \subset G'$ and let ϑ be any of the functionals $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$. We have

$$\vartheta(U,G) = \vartheta(U,G').$$

We cannot even answer Conjecture 4.1 even in the following simple special case. Let $G = \mathbb{Z}^d$, and assume that $U \subset p \cdot \mathbb{Z}^d$. Do we get the same values of $\alpha, \alpha', \alpha'', \beta', \beta''$ if we restrict A, B to be subsets of $p \cdot \mathbb{Z}^d$?

The only case where we can show this in generality is for β.

Theorem 4.2 (Independence for β). *Let G be a group, G' its subgroup, $U \subset G'$. We have*

$$\beta(U,G) = \beta(U,G').$$

Proof. Take $A, B \subset G$ and split them according to cosets of G', say

$$A = \bigcup A_i, \ B = \bigcup B_j.$$

Assume that A_1 is the largest of the A_i and similarly for B. The sets $A_1 + B_j + U$ are disjoint (as j varies), and hence

$$|A+B+U| \geq \sum_j |A_1 + B_j + U| \geq \beta(U,G')\sqrt{|A_1|}\sum_j \sqrt{|B_j|}.$$

By symmetry of A and B,

$$|A+B+U| \geq \beta(U,G')\sqrt{|B_1|}\sum_i \sqrt{|A_i|}.$$

Forming the geometric mean of the above two inequalities and using Hölder of the form

$$\sum x_i^2 \leq (\max x_i) \sum x_i$$

separately for the numbers $|A_i|$ and $|B_j|$, we obtain the desired result. ∎

An important special case is easily seen.

Statement 4.3 (Cartesian products with torsion). *Let G be a group, $G = G' \times H$ with H torsion-free, $U \subset G'$ and let ϑ be any of the functionals $\alpha, \alpha', \alpha'', \beta', \beta''$. We have*

$$\vartheta(U,G) = \vartheta(U,G').$$

In particular, this implies that by embedding $\mathbb{Z}^d$ into $\mathbb{Z}^k$ with $k > d$ these values do not change.

Proof. If G' is a torsion group, then all these functionals have value 1. Assume this is not the case, and fix a $g \in G'$ of infinite order.

Take $A, B \subset G$. We are going to construct $A', B' \subset G'$ such that

$$|A' + B'| = |A+B|, \ |A' + B' + U| = |A+B+U|,$$

and the restrictions used to define $\alpha, \alpha', \alpha'', \beta', \beta''$ are preserved.

Let H' be the subgroup of H generated by the elements in the H-projection of $A \cup B$. Since H is torsion-free, we have $H' \cong \mathbb{Z}^d$ for some d. Let

$e_1,\dots,e_d$ be a system of generators for H'. For fixed integers $m_1,\dots,m_d$ (to be chosen later) define a homomorphism $\varphi\colon G'\times H'\to G'$ by

$$\varphi(x, y_1e_1 + \ldots + y_de_d) = x + (m_1y_1 + \ldots + m_dy_d)g.$$

Put $A'=\varphi(A)$, $B'=\varphi(B)$. It is clear that for $m_1,\dots,m_d$ large enough (and dependent on A,B,U), φ is one-to-one on $A,B,A+B,A+B+U$ and the claim follows. ∎

5. Torsion

The presence of torsion is the source of difficulties. We conjecture it should not matter much.

Conjecture 5.1. Let G be a group, H its torsion subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism, $U\subset G$, $U'=\varphi(U)\subset G'$ and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta',\beta''$. We have

$$\vartheta(U') = \vartheta(U).$$

Remark 5.2. The case of β follows from Statement 5.3 below and supermultiplicativity (Theorem 7.4) as β is always at least 1.

Statement 5.3 (Projections and torsion). *Let G be a group, H its torsion subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism, $U\subset G$, $U'=\varphi(U)\subset G'$ and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta,\beta',\beta''$. We have*

$$\vartheta(U') \ge \vartheta(U).$$

Proof. For concreteness, let us prove Statement 5.3 for the case of β, as for the other functionals the argument is similar.

For an arbitrary $\epsilon>0$ there are $A',B'\subset G'$ such that

$$\frac{|A'+B'+U'|}{|A'|^{1/2}|B'|^{1/2}} \le \beta(U') + \epsilon.$$

WLOG we may assume H is of finite order. Take $A:=\phi^{-1}(A')$ and $B:=\phi^{-1}(B')$, so that $|A|=|H||A'|$ and $|B|=|H||B'|$. At the same time clearly,

$$|A+B+U| \le |A'+B'+U'||H|,$$

so

$$\beta(U) \le \frac{|A+B+U|}{|A|^{1/2}|B|^{1/2}} \le \beta(U') + \epsilon.$$

The claim follows as ϵ can be taken arbitrarily close to zero. ∎

Statement 5.4 (The trivial lower bounds). *Let G be a group, H its torsion subgroup, $U \subset G$. If U is contained in a single coset of H, then*

$$\alpha(U) = \alpha'(U) = \alpha''(U) = \beta(U) = \beta'(U) = \beta'(U) = 1,$$

otherwise

$$\beta(U) \geq 2, \ \alpha(U) \geq 3/2.$$

Proof. The statement is trivial when U is contained in a coset of H.

Otherwise, we may assume WLOG that U contains the union of $\{0\} \oplus U_0$ and $\{1\} \oplus U_1$ with some $U_0, U_1 \subset G/\mathbb{Z}$. We also write

$$A = \bigsqcup_{i=1}^{N} a_i \oplus A_i$$

and

$$B = \bigsqcup_{j=1}^{M} b_j \oplus B_j$$

with $A_i, B_j \subset G/\mathbb{Z}$ and some N, M, so that the integers $\{a_i\}$ and $\{b_j\}$ are monotone increasing. Then $|A+B+U|$ contains the disjoint union of

$$\begin{aligned}
&(a_1 + b_1) \oplus (A_1 + B_1 + U_0),\\
&(a_1 + b_1 + 1) \oplus (A_1 + B_1 + U_1), \ldots, (a_N + b_1 + 1) \oplus (A_N + B_1 + U_1),\\
&(a_N + b_2 + 1) \oplus (A_N + B_2 + U_1), \ldots, (a_N + b_M + 1) \oplus (A_N + B_M + U_1).
\end{aligned}$$

Since in any group

$$|A_i + B_j + U_k| \geq \max\{|A_i|, |B_j|\},$$

we conclude that

$$|A + B + U| \geq \sum_{i=1}^{N} |A_i| + \sum_{j=1}^{M} |B_j| = |A| + |B| \geq 2|A|^{1/2}|B|^{1/2}.$$

In a similar way, for an arbitrary $A \supset U$ holds

$$|A + B| \geq |A| + |B| - \min\{|A_1|, |A_N|, |B_1|, |B_M|\} \geq \frac{3}{2}|A|^{1/2}|B|^{1/2},$$

and hence $\beta(U) \geq 2$ and $\alpha(U) \geq 3/2$. ∎

6. Projection and compression

By *projection* we mean the application of any homomorphism. We think projections never increase the value of our α's and β's.

Conjecture 6.1 (Projection conjecture). Let G be a group, H its subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism, $U\subset G$, $U'=\varphi(U)\subset G'$ and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta',\beta''$. We have

$$\vartheta(U')\le\vartheta(U).$$

Remark 6.2. For β_p the conjecture follows from Theorem 7.5 as $\beta_p\ge 1$ always.

Remark 6.3. Essentially this means the following. Given sets $A,B\subset G$ (subject to certain conditions, depending on which of the functionals we consider) we need to find $A',B'\subset G'$ such that

$$\frac{|A'+B'|}{\sqrt{|A'||B'|}}\le\frac{|A+B|}{\sqrt{|A||B|}}$$

for the α's, or

$$\frac{|A'+B'+U'|}{|A'|^{1/p}|B'|^{1-1/p}}\le\frac{|A+B+U|}{|A|^{1/p}|B|^{1-1/p}}$$

for the β's. The natural approach of taking $A'=\varphi(A)$, $B'=\varphi(B)$ may not work even when $G=\mathbb{Z}^2$, $G'=\mathbb{Z}$.

We establish an important special case.

Theorem 6.4 (Projection conjecture with no torsion). *Let G be a group, H its subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism, $U\subset G$, $U'=\varphi(U)\subset G'$ and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta_p,\beta',\beta''$. If H is torsion-free, then*

$$\vartheta(U')\le\vartheta(U).$$

Definition 6.5. Let G be a group, H its subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism. The *compression along φ* is the mapping C_φ of finite subsets of G into finite subsets of $G'\times\mathbb{Z}$ defined as follows. Let $A\subset G$ be a finite set. We put

$$C_\varphi(A)=\bigcup_{x\in\varphi(A)}(x\times\{0,1,\dots,|A\cap\varphi^{-1}(x)|-1\}.$$

That is, each part of A in a coset of H is replaced by an interval of the same size. If $G=\mathbb{Z}^d$ and $H=\mathbb{Z}^k$ with $k<d$, then we can naturally represent the compression in $\mathbb{Z}^d$, which is the classical usage of this term.

In what follows we will write $\varphi_A^{-1}(x)$ as an alias for $\varphi^{-1}(x)\cap A$. For a given set A and $x\in G'$, such a set is called the *fiber* of A above x. One can say that the compression operator "normalizes" each fiber of A by replacing it with an initial segment in $\mathbb{Z}$.

Clearly, $|C_\varphi(A)|=|A|$ always.

Statement 6.6 (Compressions shrink sumsets). *Let G be a group, H its subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism, $A,B\subset G$. If H is torsion-free, then*

$$C_\varphi(A)+C_\varphi(B)\subset C_\varphi(A+B).$$

Proof. The claim is standard and can be adopted from e.g. [5].

Let $z\in\varphi(C_\varphi(A)+C_\varphi(B))$. There are $z_a\in\varphi(A)$ and $z_b\in\varphi(B)$ such that $z=z_a+z_b$. By the Cauchy-Davenport inequality and the definition of the compression,

$$\begin{aligned}|\varphi^{-1}_{C_\varphi(A)+C_\varphi(B)}(z)| &= |\varphi_A^{-1}(z_a)|+|\varphi_B^{-1}(z_b)|-1\\ &\le |\varphi_A^{-1}(z_a)+\varphi_B^{-1}(z_b)|\le|\varphi^{-1}_{C_\varphi(A+B)}(z)|,\end{aligned}$$

and the claim follows. ∎

Theorem 6.7 (Compressions). *Let G be a group, H its subgroup, $G'=G/H$ the factor group, $\varphi\colon G\to G'$ the natural homomorphism, $U\subset G$, and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta_p,\beta',\beta''$. If H is torsion-free, then*

$$\vartheta(C_\varphi(U))\le\vartheta(U).$$

Proof. Indeed, the previous statement implies that

$$\frac{|C_\varphi(A)+C_\varphi(B)|}{\sqrt{|C_\varphi(A)||C_\varphi(B)|}}\le\frac{|A+B|}{\sqrt{|A||B|}}$$

and

$$\frac{|C_\varphi(A)+C_\varphi(B)+C_\varphi(U)|}{|C_\varphi(A)|^{1/p}|C_\varphi(B)|^{1-1/p}}\le\frac{|A+B+U|}{|A|^{1/p}|B|^{1-1/p}}.$$

Also, the restrictions are preserved (if $A\supset U$, then $C_\varphi(A)\supset C_\varphi(U)$; if $|A|=|B|$, then $|C_\varphi(A)|=|C_\varphi(B)|$). ∎

Proof of Theorem 6.4. We can naturally embed G' into $G'\times\mathbb{Z}$ as $G'\times\{0\}$. With this embedding we have $U'\subset C_\varphi(U)$, hence

$$\vartheta(U,G)\ge\vartheta(C_\varphi(U),G'\times\mathbb{Z})\ge\vartheta(U',G'\times\mathbb{Z})=\vartheta(U',G');$$

in the last step we apply Statement 4.3. ∎

7. Direct product

The behaviour of our quantities under direct product and a somewhat more general operation (*tensorization*, see Theorem 7.5 below) is important for our applications.

Conjecture 7.1 (Multiplicativity hypothesis). Let $G=G_1\times G_2$, $V_1\subset G_1$, $V_2\subset G_2$, $U=V_1\times V_2$, and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta_p,\beta',\beta''$. We have

$$\vartheta(U)=\vartheta(V_1)\vartheta(V_2).$$

Submultiplicativity is easy.

Statement 7.2 (Sub-multiplicativity). *Let $G=G_1\times G_2$, $V_1\subset G_1$, $V_2\subset G_2$, $U=V_1\times V_2$, and let ϑ be any of the functionals $\alpha,\alpha',\alpha'',\beta_p,\beta',\beta''$. We have*

$$\vartheta(U)\le\vartheta(V_1)\vartheta(V_2).$$

Proof. We show only for $\vartheta=\alpha$, the rest being similar. Let A_1,B_1 be arbitrary sets containing V_1 and A_2,B_2 be arbitrary sets containing V_2. Then $A_1\times A_2$ and $B_1\times B_2$ contain $V_1\times V_2$ and so

$$\alpha(V_1\times V_2)\le\frac{|A_1\times A_2+B_1\times B_2|}{(|A_1||B_1||A_2||B_2|)^{1/2}}=\frac{|A_1+B_1||A_2+B_2|}{(|A_1||B_1||A_2||B_2|)^{1/2}}.$$

Thus

$$\alpha(V_1\times V_2)\le\alpha(V_1)\alpha(V_2).\qquad\blacksquare$$

The multiplicativity hypothesis, Conjecture 7.1, would have consequences for the comparison problems of Section 3.

Statement 7.3. *Let U be a subset of a commutative group.*
If Conjecture 7.1 holds for α', then $\alpha(U)=\alpha'(U)\le\beta'(U)$.
If Conjecture 7.1 holds for α'', then $\alpha''(U)\le\beta''(U)$.
If Conjecture 7.1 holds for β', then $\beta(U)=\beta'(U)$.

Proof. The inequalities

$$\alpha'(U)\le\beta'(U),\quad \alpha''(U)\le\beta''(U),$$

follow from (6), that is

$$\alpha'(U)\le 4\beta'(U),\quad \alpha''(U)\le 3\beta''(U),$$

and Conjecture 7.1 with the tensor power trick. We prove only the first of the two inequalities, the second follows similarly. Indeed for any $n\ge1$, first using Conjecture 7.1 for α' and then Statement 7.2 for β', we find

$$\alpha'(U)^n = \alpha'(U^n) \leq 4\beta'(U^n) \leq 4\beta'(U)^n.$$

Thus

$$\alpha'(U) \leq 4^{1/n}\beta'(U),$$

and the result follows from allowing $n \to \infty$. We now show that Conjecture 7.1 implies

$$\alpha(U) = \alpha'(U).$$

By Statement 3.2, it is enough to show $\alpha'(U) \leq \alpha(U)$. Let A and B be sets containing U. Then $A \times B$ and $B \times A$ contain $U \times U$ and are of the same size, so

$$\alpha'(U^2) \leq \frac{|A \times B + B \times A|}{|A||B|} = \frac{|A+B|^2}{|A||B|}.$$

The result then follows from Conjecture 7.1 for α'. The inequality $\beta(U) = \beta'(U)$ is similar. ∎

We are far from knowing the multipliciativity of α, as we cannot even compute $\alpha(\{0,1\}^d)$. We do know multiplicativity of β.

Theorem 7.4 (Multiplicativity of β). *Let $G = G_1 \times G_2$, $V_1 \subset G_1$, $V_2 \subset G_2$, $U = V_1 \times V_2$. We have*

$$\beta_p(U) = \beta_p(V_1)\beta_p(V_2).$$

This will follow from supermultiplicativity, which we shall establish in a more general setting.

Theorem 7.5 (β along fibers). *Let G be a group, H its subgroup, $G' = G/H$ the factor group, $\varphi\colon G \to G'$ the natural homomorphism, $U \subset G$, $V = \varphi(U)$. We have*

$$\beta_p(U) \geq \beta_p(V) \min_{x \in V} \beta_p\bigl(U \cap \varphi^{-1}(x)\bigr).$$

If H is a direct factor, this can be reformulated as follows.

Corollary 7.6. *Let $G = G_1 \times G_2$, $V \subset G_1$, and for each $x \in V$ given a set $W_x \subset G_2$. Put*

$$U = \bigcup_{x \in V} \{x\} \times W_x.$$

We have

$$\beta_p(U) \geq \beta_p(V) \min_{x \in V} \beta_p(W_x).$$

Theorem 7.5 (and thus Theorem 7.4 and Corollary 7.6) will be proved in a yet more general form in Section 10. It turns out that a functional analog of β that we introduce shortly, provides greater flexibility for carrying out an induction argument.

Part II: functions

8. Functional tripling

We shall consider nonnegative-valued functions in the space $\ell^1(G)$. A set A naturally corresponds to the function 1_A.

Definition 8.1. The *max-convolution* of the non-negative functions $f, g \in \ell^1(G)$ is

$$(f \mathbin{\overline{*}} g)(x) = \max_t f(t)g(x-t).$$

This generalizes the notion of sumset. For the indicator functions $1_A, 1_B$ of sets A, B we have

$$1_A \mathbin{\overline{*}} 1_B = 1_{A+B}.$$

One can replace the notion of cardinality of a set with the ℓ^1 norm of a function. However, we have a more robust notion.

Definition 8.2. The *level sets* of a function f are the sets

$$\mathcal{F}(t) = \{x \in G \colon f(x) \geq t\}.$$

The *distribution function* of f is the function $F \colon \mathbb{R}^+ \to \mathbb{Z}$ given by

$$F(t) = |\mathcal{F}(t)|.$$

Note that this is different from the definition used in probability theory.

Definition 8.3. Let f, g be functions with distribution functions F, G. If $F = G$, we call them *identically distributed* and write $f \sim g$.

Definition 8.4. The *functional triplings* of a function f are the quantities

$$\gamma(f) = \inf_{g,h} \frac{\|f \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1}{\|g\|_2 \, \|h\|_2},$$

the *unrestricted tripling*;

$$\gamma_p(f) = \inf_{g,h} \frac{\|f \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1}{\|g\|_p \, \|h\|_q},$$

its asymmetric variant, where $1/p + 1/q = 1$;

$$\gamma'(f) = \inf_{g \sim h} \frac{\|f \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1}{\|g\|_2 \, \|h\|_2},$$

the *isometric tripling*;

$$\gamma''(f) = \inf_{g} \frac{\|f \mathbin{\overline{*}} g \mathbin{\overline{*}} g\|_1}{\|g\|_2^2},$$

the *isomeric tripling.*

Conjecture 8.5.

$$\gamma = \gamma' = \gamma''.$$

Tripling of sets can be expressed via functional tripling.

Theorem 8.6 (Function and Set analog of β are the same). *Let U be any finite set in a commutative group. We have*

$$\beta_p(U) = \gamma_p(1_U),\ \beta'(U) = \gamma'(1_U),\ \beta'(U) = \gamma''(1_U).$$

Proof. We prove only $\beta_p(U) = \gamma_p(1_U)$, as the other equalities follow similarly (in fact the definitions of γ', γ'' are designed just for this). We have

$$\frac{|A+B+U|}{|A|^p|B|^q} = \frac{\|1_U \mathbin{\overline{*}} 1_A \mathbin{\overline{*}} 1_B\|_1}{\|1_A\|_p \|1_B\|_q},$$

and the inequality $\gamma_p(1_U) \le \beta_p(U)$ follows from taking an infimum over A and B.

To prove the reverse inequality, we need a lemma, which is a multiplicative analog of Prékopa–Leindler, Theorem 2.14.

Lemma 8.7 (Multiplicative Prékopa–Leindler). *Let a, b, c be measurable functions $\mathbb{R}_+ \to [0,1]$ and $1 < p, q < \infty$ are Hölder conjugates, that is*

$$\frac{1}{p} + \frac{1}{q} = 1.$$

Assume that for any $u, v \in \mathbb{R}_+$

$$c(uv) \ge a(u)b(v).$$

Then

$$\|c\|_1 \ge \left(\int_0^1 a^p(t^{1/p})dt\right)^{1/p} \left(\int_0^1 b^q(t^{1/q})dt\right)^{1/q}.$$

Proof. Define

$$h(x) := c(e^{-x})e^{-x}$$

and further

$$f(x) := a^p(e^{-x/p})e^{-x} \tag{11}$$

$$g(x) := b^q(e^{-x/q})e^{-x}. \tag{12}$$

We then have that for any $x, y > 0$

$$h\left(x/p + y/q\right) \ge f^{1/p}(x) g^{1/q}(y),$$

so by the Prékopa–Leindler inequality, Theorem 2.14,

$$\|h\|_1 \ge \|f\|_1^{1/p} \|g\|_1^{1/q}.$$

The claim follows after the change of variables $t = e^{-x}$. ∎

We want to prove that for any non-negative functions g,h

$$\|1_V \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1 \geq \beta(V)\|g\|_p\|h\|_q.$$

After rescaling, we may assume $\max g = \max h = 1$. Let

$$S(t) := \{z\colon 1_V \mathbin{\overline{*}} g \mathbin{\overline{*}} h(z) \geq t\}.$$

Further define the distribution functions

$$G(t) := \{z\colon g(z) \geq t\}$$

and

$$H(t) := \{z\colon h(z) \geq t\}.$$

For any u,v then have the inclusion

$$G(u) + H(v) + V \subset S(uv),$$

so

$$|S(uv)| \geq \beta_p(V)|G(u)|^{1/p}|H(v)|^{1/q}.$$

It follows from Lemma 8.7 that

$$\|1_V \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1 \geq \beta_p(V)\left(\int_0^1 G(t^{1/p})dt\right)^{1/p}\left(\int_0^1 H(t^{1/q})dt\right)^{1/q}.$$

The result now follows from the layer-cake principle of the form

$$\int F(t^{1/p})dt = \int f(t)^p dt.$$ ∎

9. The independence problem

The independence problem arises as it did for sets.

For this section we change the notations to $\gamma(U,G)$ etc. to indicate the ambient group.

Theorem 9.1 (Ambient group does not change γ). *Let G be a group, G' its subgroup, $U \subset G'$. We have*

$$\gamma_p(1_U,G) = \gamma_p(1_U,G').$$

Proof. This follows from Theorem 8.6 and Theorem 4.2. ∎

Conjecture 9.2 (Functional independence hypothesis). Let G be a group, G' its subgroup, $f \in \ell^1(G')$ and let ϑ be any of the functionals γ', γ''. We have

$$\vartheta(f,G) = \vartheta(f,G').$$

10. Direct product

Theorem 10.1 (Multiplicativity). *Let* $G = G_1 \times G_2$, $f_1 \in \ell^1(G_1)$, $f_2 \in \ell^1(G_2)$, *and define* $f \in \ell^1(G)$ *by* $f(x,y) = f_1(x) f_2(y)$. *We have*

$$\begin{gathered}\gamma_p(f) = \gamma_p(f_1)\gamma_p(f_2),\\ \gamma'(f) \le \gamma'(f_1)\gamma'(f_2),\\ \gamma''(f) \le \gamma''(f_1)\gamma''(f_2).\end{gathered}$$

Proof. The $\le$ inequalities all follow from the fact that (with g_i, h_i defined similarly to f_i)

$$f \mathbin{\overline{*}} g \mathbin{\overline{*}} h(x,y) \le f_1 \mathbin{\overline{*}} g_1 \mathbin{\overline{*}} h_1(x) f_2 \mathbin{\overline{*}} g_2 \mathbin{\overline{*}} h_2(y)$$

for any $x \in G_1$ and $y \in G_2$.

The reverse inequality for γ_p follows from a much more general Theorem 10.2 (and Theorem 10.3) towards which we immediately proceed. ∎

Theorem 10.2 (Tensorization). *Let* G *be a group,* H *a subgroup,* $G' = G/H$ *the factor group,* $\varphi\colon G \to G'$ *the natural homomorphism,* $f \in \ell^1(G)$. *Define* $f_\varphi \in \ell^1(G')$ *by*

$$f_\varphi(x) := \gamma_p\big(f|_{\varphi^{-1}(x)}\big).$$

We have $\gamma_p(f) \ge \gamma_p(f_\varphi)$.

Proof. Let $g, h \in \ell^{‘}(G)$ be non-negative. We have

$$\begin{aligned}\|f \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1 &= \sum_{z\in G} \max_{x_1+x_2+x_3=z} f(x_1)g(x_2)h(x_3)\\ &= \sum_{z_1\in G'} \sum_{z\in z_1+H} \max_{\substack{w_1,w_2,w_3\in G'\\ w_1+w_2+w_3=z_1}} \max_{\substack{x_1+x_2+x_3=z\\ x_i\in H+w_i}} f(x_1)g(x_2)h(x_3) \qquad (13)\\ &\ge \sum_{z_1\in G'} \max_{\substack{w_1,w_2,w_3\in G'\\ w_1+w_2+w_3=z_1}} \sum_{z\in z_1+H} \max_{\substack{x_1+x_2+x_3=z\\ x_i\in H+w_i}} f(x_1)g(x_2)h(x_3).\end{aligned}$$

Define the functions g', h' on G' as follows

$$g'(w_2) := \|g|_{\varphi^{-1}(w_2)}\|_p, h'(w_3) := \|h|_{\varphi^{-1}(w_3)}\|_q.$$

One can further estimate (13)

$$\begin{aligned}&\ge \sum_{z_1\in G'} \max_{\substack{w_1,w_2,w_3\in G'\\ w_1+w_2+w_3=z_1}} f_\varphi(w_1)g'(w_2)h'(w_3)\\ &\ge \gamma_p(f_\varphi)\|g\|_p\|h\|_q.\end{aligned}$$

The last inequality follows from the observation that

$$\|g'\|_p = \|g\|_p, \|h'\|_q = \|h\|_q.$$ ∎

We can specialize Theorem 10.2 to cartesian products.

Theorem 10.3. *Let* $G=G_1\times G_2$*,* f *a function on* G*. For* $x\in G_1$*, define* $f_x(y)=f(x,y)$*, functions on* G_2*. Let* $g(x)=\gamma_p(f_x)$*, a function on* G_1*. We have* $\gamma_p(f)\ge\gamma_p(g)$*.*

Proof. We let $\varphi\colon G_1\times G_2\to G_1$ by projection. Then

$$f_\varphi(x)=\gamma(f_x),$$

and so the result follows from Theorem 10.2. ∎

We are now ready to prove Theorem 7.5.

Theorem 7.5. Let U be as in the statement and $f=1_U=:U$. Then, by Theorem 8.6, for $x\in V$

$$f_\varphi(x):=\gamma_p\left(f|_{\varphi^{-1}(x)}\right)=\beta_p(U\cap\varphi^{-1}(x)).$$

In particular, we have the point-wise bound

$$f_\varphi(x)\ge 1_V(x)\min_{t\in V}\beta_p(U\cap\varphi^{-1}(t)),$$

so again by Theorem 8.6 and homogenity

$$\gamma_p(f_\varphi)\ge\beta_p(V)\min_{t\in V}\beta_p(U\cap\varphi^{-1}(t)).$$

The result now follows from Theorem 10.2, as

$$\beta_p(U)=\gamma_p(f)\ge\gamma_p(f_\varphi)\ge\beta_p(V)\min_{x\in V}\beta_p(U\cap\varphi^{-1}(x)).$$ ∎

11. Functional tripling for functions supported on quasicubes

The goal of this section is to prove Theorem 2.7. The basic strategy is to use tensorization to reduce to a two-point inequality.

It is enough to show $\beta(V)=|V|$, since then by (7), $\alpha(V)\ge|V|^{1/2}$ follows.

We let U be a d dimensional quasicube, defined in Definition 2.5. Thus U is d dimensional as thus we may assume

$$U\subset H'\times\mathbb{Z}^d,$$

where H' is a torsion subgroup. We first show we may assume $H'=\{0\}$. Let π be the projection to $\mathbb{Z}^d$. Then by induction, it follows that $|\pi(U)|=|U|$.

Thus for $V \subset U$, to prove Theorem 2.7, it is enough to show

$$\beta(\pi(V)) \geq |V|,$$

as $\beta(V) \geq \beta(\pi(V))$ by Theorem 7.5. By Theorem 4.2, we may assume

$$V \subset U \subset \mathbb{Z}^d.$$

Central to our study will be the following.

Theorem 11.1 (γ for two-point functions). *For* $0 \leq \delta \leq 1$,

$$f_\delta := 1_{\{0\}} + \delta 1_{\{1\}}.$$

Then

$$\gamma(f_\delta) = \delta + 1,$$

and more generally,

$$\gamma_p(f_\delta) \geq \frac{p^{1/p} q^{1/q}}{2}(1+\delta).$$

We remark that the stronger

$$\gamma_p(f_\delta) \geq (\delta^c + 1)^{1/c}, \quad 2^{1/c} = p^{1/p} q^{1/q}$$

is probably true, though we do not require it (see this mathoverflow post [16]). Such a result would be useful for quasicubes that are asymmetrical in size. We also remark that Prékopa [14, Equation 2.4] proved Theorem 11.1 in the special case $p = q = 2$ and $\delta = 1$ and his proof extends to the $\delta = 0$ case.

We now present an important family of examples. First, they are a natural guess for minimizers of $\gamma_p(f_\delta)$ and indeed show that Theorem 11.1 is best possible. Secondly, in the proof of Theorem 11.1 below, we show that to bound $\gamma_p(f_\delta)$ from below it is enough to consider g and h, from Definition 8.4, from the following.

Example 11.2. Fix $0<\delta<1$. Let $g=(1,\delta,\dots,\delta^r)$ and $h=(1,\delta,\dots,\delta^s)$. Then

$$\|f_\delta \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1 = \sum_{j=0}^{r+s+1} \delta^j = \frac{1-\delta^{r+s+2}}{1-\delta},$$

while

$$\|g\|_p^p = \frac{1-\delta^{p(r+1)}}{1-\delta^p},$$

and

$$\|h\|_q^q = \frac{1-\delta^{q(s+1)}}{1-\delta^q}.$$

Note that

$$\frac{1-\delta^{r+s+2}}{(1-\delta^{p(r+1)})^{1/p}(1-\delta^{q(s+1)})^{1/q}} \geq 1. \tag{14}$$

Indeed, this follows from the inequality

$$(1-xy) \geq (1-x^p)^{1/p}(1-y^q)^{1/q}, \quad 0 \leq x, y \leq 1,$$

which is an application of Hölder's inequality applied to the vectors

$$(x^n)_{n\in\mathbb{Z}_{\geq 0}}, \quad (y^n)_{n\in\mathbb{Z}_{\geq 0}}.$$

Thus (14) is minimized by allowing $r,s\to\infty$ and so

$$\frac{\|f_\delta \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1}{\|g\|_p\|h\|_q} \geq \frac{(1-\delta^p)^{1/p}(1-\delta^q)^{1/q}}{1-\delta}.$$

In the most important case, that is $p=q=2$, we have

$$\frac{\|f_\delta \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1}{\|g\|_2\|h\|_2} \geq 1+\delta,$$

while the more general case is a bit harder.

Lemma 11.3 (Minimizer for γ_p). *Let* $0<\delta<1$ *and*

$$g=h=(1,\delta,\delta^2,\dots,).$$

Then we have

$$\frac{\|f_\delta \mathbin{\overline{*}} g \mathbin{\overline{*}} h\|_1}{\|g\|_p\|h\|_q} \geq \frac{p^{1/p}q^{1/q}}{2}(1+\delta).$$

Proof. Similar to the $p=q=2$ case above it suffices to show that

$$\frac{(1-\delta^p)^{1/p}(1-\delta^q)^{1/q}}{1-\delta} \geq \frac{p^{1/p}q^{1/q}}{2}(1+\delta)$$

or

$$(1-\delta^p)^{1/p}(1-\delta^q)^{1/q} \geq \frac{p^{1/p}q^{1/q}}{2}(1-\delta^2).$$

This follows upon applying Hölder's inequality:

$$\int_\delta^1 s^2\frac{ds}{s} \leq \left(\int_\delta^1 s^p\frac{ds}{s}\right)^{1/p}\left(\int_\delta^1 s^q\frac{ds}{s}\right)^{1/q}. \qquad \blacksquare$$

Proof of Theorem 2.7 and Theorem 2.11. We first show how Theorem 11.1 implies Theorem 2.7. Thus we assume $p=q=2$. By the discussion at the beginning at the current section we may assume that $V\subset\mathbb{Z}^d$. By Theorem 4.2 we can further assume that in fact $V\subset\mathbb{Q}^d$. Since β is invariant under bijective linear transformations of $\mathbb{Q}^d$, after a suitable translation and choosing a basis $\{e_i\}$ for the ambient group $\mathbb{Q}^d$ (now viewed as a linear space) one can WLOG write

$$V = 0\oplus V_0\cup e_1\oplus V_1,$$

where V_0 and V_1 are $d-1$ dimensional quasicubes.

Now, we again use the independence of the ambient group (Theorem 4.2) to reduce the ambient group to the one generated by V, so that now $V\subset G:=\mathbb{Z}e_1\times\mathbb{Z}^{d-1}$.

Let $A,B\subset\mathbb{Z}^d$ and write

$$A=\bigcup_i ie_1\oplus A_i,\quad B=\bigcup_j je_1\oplus B_j.$$

We claim that $\gamma(1_V)=|V|$ and in particular,

$$|A+B+V|\geq\|f\,\overline{*}\,g\,\overline{*}\,h\|_1, \tag{15}$$

where

$$f=|V_0|1_{\{0\}}+|V_1|1_{\{1\}},\quad g(i)=|A_i|^{1/2},\quad h(j)=|B_j|^{1/2}.$$

We induct on the dimension on V. The base case follows directly from Theorem 11.1 and homogenity of γ.

We let π_1 be projection onto the first coordinate and

$$X_k = \pi_1^{-1}(k) \cap (A+B+V).$$

Then, X_k contains all the fiber sumsets as long as the first coordinate equals k, so

$$\begin{aligned}
|X_k| &= \max\{\max_{i+j=k} |A_i+B_j+V_0|, \max_{i+j=k-1} |A_i+B_j+V_1|\} \\
&\geq \max\{\max_{i+j=k} \beta(V_0)|A_i|^{1/2}|B_j|^{1/2}, \max_{i+j=k-1} \beta(V_1)|A_i|^{1/2}|B_j|^{1/2}\} \\
&= \max\{\max_{i+j=k} \gamma(1_{V_0})|A_i|^{1/2}|B_j|^{1/2}, \max_{i+j=k-1} \gamma(1_{V_1})|A_i|^{1/2}|B_j|^{1/2}\} \\
&= \max\{\max_{i+j=k} |V_0||A_i|^{1/2}|B_j|^{1/2}, \max_{i+j=k-1} |V_1||A_i|^{1/2}|B_j|^{1/2}\} \\
&= f \overline{*} g \overline{*} h(k).
\end{aligned}$$

Summing over k gives (15). By Theorem 11.1, we have

$$|A+B+V| \geq \|f \overline{*} g \overline{*} h\|_1 \geq (|V_1|+|V_2|)\|f\|_2\|g\|_2 = |V||A|^{1/2}|B|^{1/2},$$

which implies Theorem 2.7.

We now handle the case of general p. Everything proceeds the same as in the $p=2$ case, except the induction claim is

$$\gamma_p(1_V) \geq \frac{|V|p^{d/p}q^{d/q}}{2^d}.$$

Theorem 2.11 now follows from Theorem 8.6. ■

We now proceed to the proof of Theorem 11.1. We first need the following lemma.

Lemma 11.4 (γ and permutations). *Let $f,g,h\colon \mathbb{Z}\to\mathbb{R}$ be non-negative functions with finite support. Let σ,τ,ρ be permuations of the support of f,g,h, respectively. Set*

$$f_\sigma(x) := f \circ \sigma(x),$$

and similarly for g and h. Then

$$\|f_\sigma \overline{*} g_\tau \overline{*} h_\rho\|_1,$$

is minimized for a choice of permutations that makes each function non-increasing.

Proof. We may suppose, after translation, that the smallest element of the support is zero for all three functions. Put $F := f \overline{*} g \overline{*} h$ and let σ, τ, ρ be some permutations such that f_σ, g_τ, h_ρ are non-increasing. Note that $G := f_\sigma \overline{*} g_\tau \overline{*} h_\rho$ is then also non-increasing. Let s be a sufficiently large number and order the sequence $F(0), \dots, F(s)$ (which will end with zeroes) via

$$F_0 \geq \dots \geq F_s. \tag{16}$$

We claim that for $0 \leq v \leq s$

$$f_\sigma \overline{*} g_\tau \overline{*} h_\rho(v) = G(v) \leq F_v,$$

and the result follows from this claim. Let m, n, r be such that $m+n+r=v$ and

$$f_\sigma(m) g_\tau(n) h_\rho(r) = G(v).$$

It follows by the choice of σ, τ, ρ, that for any $i \leq m$, $j \leq n$, $k \leq r$

$$\begin{aligned} G(v) &= f_\sigma(m) g_\tau(n) h_\rho(r) \\ &\leq f_\sigma(i) g_\tau(j) h_\rho(k) \\ &= f(\sigma(i)) g(\tau(j)) h(\rho(k)) \\ &\leq F(\sigma(i) + \tau(j) + \rho(k)). \end{aligned}$$

It follows that for any

$$t \in \{\sigma(0), \dots, \sigma(m)\} + \{\tau(0), \dots, \tau(n)\} + \{\rho(0), \dots, \rho(r)\} \tag{17}$$

holds

$$G(v) \leq F(t).$$

But the sumset on the RHS of (17) is of size at least $m+n+r+1$, by the Cauchy-Davenport inequality. Thus, there are at least $v+1$ values in the sequence (16) that are no less than $G(v)$, and hence

$$G(v) \leq F_v. \qquad \blacksquare$$

Proof of Theorem 11.1. We aim to show that for non-negative valued g and h in $\ell_1(\mathbb{Z})$

$$\frac{\|f_\delta \overline{*} g \overline{*} h\|}{\|g\|_p \|h\|_q} \geq c_\delta = \frac{(1-\delta^p)^{1/p}(1-\delta^q)^{1/q}}{1-\delta}. \tag{18}$$

We remind the reader that c_δ is the infimum of (18) over all g, h of the form

$$g = (1, \delta, \dots, \delta^r), \quad h = (1, \delta, \dots, \delta^s), \tag{19}$$

as shown in Example 11.2.

We suppose there is a $g,h \in \ell^1(\mathbb{Z})$ such that (18) is smaller than c_δ. By continuity, we may suppose both g and h have finite support. By Lemma 11.4, we may permute g,h so they are both non-increasing. After translation of the supports, we suppose

$$g = (g_0, \dots g_r), \quad h = (h_0, \dots, h_s).$$

We further assume that $r+s$ is minimally chosen. Thus

$$\frac{\|f_\delta \mathbin{\bar{*}} u \mathbin{\bar{*}} v\|_1}{\|u\|_p \|v\|_q} \geq c_\delta,$$

for any u and v satisfying

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| < r + s + 2.$$

By compactness, there exists g,h which minimize (18) subject to $\operatorname{supp}(g) \subseteq \{0,\dots,r\}$, $\operatorname{supp}(h) \subseteq \{0,\dots,s\}$, and

$$\|g\|_p = 1, \quad \|h\|_q = 1. \tag{20}$$

Because the value of (18) doesn't change by multiplying g and h by constant, this is also a minimum over all g and h where $\operatorname{supp}(g) \subseteq \{0,\dots,r\}$ and $\operatorname{supp}(h) \subseteq \{0,\dots,s\}$

Set

$$p(x) = f_\delta \mathbin{\bar{*}} g \mathbin{\bar{*}} h(x).$$

Let

$$Q_1 \subset \{0, \dots, r\}, \quad Q_2 \subset \{0, \dots, s\}.$$

We let $R(Q_1)$ be the set of all indices $n \in \{0,\dots,r+s+1\}$ such that if

$$p_n = f_i g_j h_k, \quad (i + j + k = n),$$

then $j \in Q_1$, and similarly for Q_2. We now analyze what happens when we replace g with g_t which we get by multiplying all $g(i)$ by $(1-t)$ where $i \in Q_1$. (t is a small enough positive real number.)

In $f_\delta \mathbin{\bar{*}} g_t \mathbin{\bar{*}} h$, the values corresponding to $R(Q_1)$ will be multiplied by $(1-t)$, the other values will be the same as in $f_\delta \mathbin{\bar{*}} g \mathbin{\bar{*}} h$.

$$r(t) := \frac{\|f_\delta \mathbin{\bar{*}} g_t \mathbin{\bar{*}} h\|_1}{\|g_t\|_p \|h\|_q}.$$

$r'(0)$ is the right-hand derivative of $r(t)$ at 0. By minimality, $r'(0) \geq 0$.

The right-hand derivative of $\|f \,\bar{*}\, g \,\bar{*}\, h\|_1$ at 0 is

$$-\sum_{y\in R(Q_1)} p(y)$$

and the right-hand derivative of $\|g_t\|_p$ is

$$-\frac{1}{p}\frac{1}{\|g_t\|_p^{p+1}}p(1-t)^{p-1}(-1)\sum_{x\in Q_1} g(x)^p$$

which is equal to

$$\frac{\sum_{x\in Q_1} g(x)^p}{\|g\|_p^{p+1}}$$

at 0.

So

$$0 \le r'(0) = \frac{\|p\|_1 \sum_{x\in Q_1} g(x)^p}{\|g\|_p^{p+1}\|h\|_q} - \frac{\sum_{y\in R(Q_1)} p(y)}{\|g\|_p\|h\|_q}.$$

By symmetry we get a similar inequality for any $Q_2 \subset \{0,\dots,s\}$, so by reframing the inequalities
(21)

$$\|p\|_1^{1/p} \ge \frac{\|g\|_p \left(\sum_{y\in R(Q_1)} p(y)\right)^{1/p}}{\left(\sum_{x\in Q_1} g(x)^p\right)^{1/p}}, \quad \|p\|_1^{1/q} \ge \frac{\|h\|_q \left(\sum_{y\in R(Q_2)} p(y)\right)^{1/q}}{\left(\sum_{x\in Q_2} h(x)^p\right)^{1/p}}.$$

We now define new functions,

$$a(i) = \delta^{-i}g(i), \quad b(j) = \delta^{-j}h(j).$$

We set

$$Q_1 = \{i\colon a(i) = \max a\}, \quad Q_2 = \{j\colon b(j) = \max b\}$$

and set

$$u(i) = g(i)1_{Q_1}(i), \quad v(j) = h(j)1_{Q_2}(j),$$
$$R(Q_1) \supseteq \operatorname{supp}(f_\delta \,\bar{*}\, u \,\bar{*}\, v),$$
$$R(Q_2) \supseteq \operatorname{supp}(f_\delta \,\bar{*}\, u \,\bar{*}\, v).$$

So $\sum_{y\in R(Q)} p(y) \ge \|f_\delta \,\bar{*}\, u \,\bar{*}\, v\|_1$ is true for both Q_1 and Q_2.

Combining it with (21), we get

$$\|p\|_1^{1/p} \geq \frac{\|g\|_p \|f_\delta \overline{*}\, u \,\overline{*}\, v\|_1^{1/p}}{\|u\|_p}, \quad \|p\|_1^{1/q} \geq \frac{\|h\|_q \|f_\delta \overline{*}\, u \,\overline{*}\, v\|_1^{1/q}}{\|v\|_q}. \tag{22}$$

Multiplying the two inequalities in (22), we get

$$\frac{\|f_\delta \overline{*}\, g \,\overline{*}\, h\|_1}{\|g\|_p \|h\|_q} \geq \frac{\|f_\delta \overline{*}\, u \,\overline{*}\, v\|_1}{\|u\|_p \|v\|_q}.$$

If either a or b is not constant, then u or v has a value of 0 at some point. Then by Lemma 11.4 we can rearrange it to a non-increasing order, with making

$$\frac{\|f_\delta \overline{*}\, u \,\overline{*}\, v\|_1}{\|u\|_p \|v\|_q}$$

smaller or equal after the rearrangement.

Now $|\operatorname{supp}(u)| + |\operatorname{supp}(v)| < |\operatorname{supp}(g)| + |\operatorname{supp}(h)|$, so because we started with a counterexample with minimal supports,

$$\frac{\|f_\delta \overline{*}\, u \,\overline{*}\, v\|_1}{\|u\|_p \|v\|_q} \geq c_\delta.$$

This is a contradiction, because we assumed that

$$\frac{\|f_\delta \overline{*}\, g \,\overline{*}\, h\|_1}{\|g\|_p \|h\|_q} < c_\delta.$$

So a and b must both be constant, but then (18) cannot be smaller than c_δ, as proved in Example 11.2. Thus, the ratio in (18) is at least c_δ. By Lemma 11.3,

$$c_\delta \geq p^{1/p} q^{1/q} \frac{(1+\delta)}{2}. \qquad \blacksquare$$

Acknowledgement. GS is supported by Ben Green's Simons Investigator Grant 376201. DZ is supported by a Knut and Alice Wallenberg Fellowship (Program for Mathematics 2017). IR is supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 29759, T 38396 and K129335. MD is supported by the New National Excellence Program of the National Research, Development and Innovation Fund and the Ministry for Innovation and Technology of Hungary (ÚNKP-20-1). The authors thank Máté Matolcsi, Thomas Bloom, Misha Rudnev, Oliver Roche-Newton, Ben Green and Ilya Shkredov for useful discussions.

References

[1] J. Bourgain and M.-C. Chang: On the size of k-fold sum and product sets of integers, *Journal of the American Mathematical Society* **17** (2004), 473–497.

[2] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, D. Kutzarova: Explicit constructions of RIP matrices and related problems, *Duke Mathematical Journal* **159** (2011), 145–185.

[3] W. Beckner: *Inequalities in Fourier analysis.* PhD thesis, Princeton., 1975.

[4] R. Gardner: The Brunn–Minkowski inequality, *Bulletin of the American Mathematical Society* **39** (2002), 355–405.

[5] R. J. Gardner and P. Gronchi: A Brunn–Minkowski inequality for the integer lattice, *Transactions of the American Mathematical Society* **353** (2001), 3995–4025.

[6] B. Green, D. Matolcsi, I. Ruzsa, G. Shakan and D. Zhelezov: A weighted Prékopa–Leindler Inequality and sumsets with quasicubes, preprint.

[7] B. Green and T. Tao: Compressions, convex geometry and the Freiman–Bilu theorem, *Quarterly Journal of Mathematics* **57** (2006), 495–504.

[8] M. Hernández Cifre, D. Iglesias and J. Yepes Nicolás: On a Discrete Brunn–Minkowski type inequality, *Siam Journal of Discrete Matheamatics* (2018), 1840–1856.

[9] B. Hanson, O. Roche-Newton and D. Zhelezov: On iterated product sets with shifts, II, *Algebra & Number Theory* **14** (2020), 2239–2260.

[10] B. Halikias, D. Klartag and B. Slomka: Discrete variants of Brunn–Minkowski type inequalities, preprint arXiv:1911.040392v2, 2019.

[11] A. Iglesias, D. Nicolás and J. Zvavitch: Brunn–Minkowski type inequalities for the lattice point enumerator, preprint arXiv:1911.12874, 2019.

[12] B. Klartag and J. Lehec: Poisson processes and a log-concave Bernstein theorem, *Studia Math*, 2019.

[13] G. Petridis: New proofs of Plünnecke-type estimates for product sets in groups, *Combinatorica* **32** (2012), 721–733.

[14] A. Prékopa: Logarithmic concave measures with application to stochastic programming, *Acta Scientiarum Mathematicarum* **32** (1971), 301–316.

[15] D. Pálvölgyi and D. Zhelezov: Query complexity and the polynomial Freiman-Ruzsa conjecture, preprint arXiv:2003.04648, 2020.

[16] G. Shakan: Nice proof of inequality $(1-x^p)^{1/p}(1-x^q)^{1/q} \geq (1-x)(1+x^c)^{1/c}$ where $2^{1/c} = p^{1/p}q^{1/q}$? *MathOverflow*, 2019, https://mathoverflow.net/q/343334 (version: 2019-10-08).

Dávid Matolcsi

Institute of Mathematics
Faculty of Sciences
Eötvös Loránd University
H-1117 Budapest, Hungary
`matolcsidavid@gmail.com`

Imre Z. Ruzsa, Dmitrii Zhelezov

Alfréd Rényi Institute of Mathematics
Budapest, Pf. 127
H-1364 Hungary
`ruzsa@renyi.hu, dzhelezov@gmail.com`

George Shakan

Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road, Oxford
OX2 6GG, UK
`george.shakan@gmail.com`