More differences than multiple sums

Imre Z. Ruzsa

Graz

Dicsovery

Differences vs. k-fold sums

We compare the difference set $A - A$ to the set

$$kA = A + \ldots + A, \;\; k \text{ times}$$

Main result: there is $A \subset \mathbb{Z}$ such that

$$|kA| < |A - A|^{\alpha_k}, \;\; \alpha_k < 1.$$

Also, there is $A \subset \mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ such that

$$A - A = \mathbb{Z}_q, \;\; |kA| < q^{\alpha_k}.$$

History: Haight(1973): for all k and m there is a q and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$ and kA avoids m consecutive residues. Used this to show the existence of a set B of reals such that $B - B = \mathbb{R}$ but $\lambda(kB) = 0$ for all k.

Ways to compare sums and differences

$$F_k(q) = \min\{|kA| : A \subset \mathbb{Z}_q,\ A - A = \mathbb{Z}_q\},\ \text{(modular)}$$

$$G_k(q) = \min\left\{|kA| : A \subset \mathbb{Z}, A - A \supset \{a+1, \ldots, a+q\} \text{ for some } a\right\},$$
(interval)

$$H_k(q) = \min\{|kA| : A \subset \mathbb{Z}, |A - A| \geq q\} \text{ (cardinality)}.$$

$$\alpha_k = \inf_{q \geq 2} \frac{\log G_k(q)}{\log q}.$$

Theorem (all the same:)

$$\lim \frac{\log F_k(q)}{\log q} = \lim \frac{\log G_k(q)}{\log q} = \lim \frac{\log H_k(q)}{\log q} = \alpha_k.$$

Main result

$$\lim \frac{\log F_k(q)}{\log q} = \lim \frac{\log G_k(q)}{\log q} = \lim \frac{\log H_k(q)}{\log q} = \alpha_k.$$

Theorem (Main result.)

$$1 - \frac{1}{2^k} \leq \alpha_k < 1.$$

Reasons for "all the same"

Reasons: monotonicity, submultiplicavity, inequalities.

Lemma (Monotonicity.)

If $q < q'$, then

$$G_k(q) \leq G_k(q'), \text{ (interval)}$$

$$H_k(q) \leq H_k(q') \text{ (cardinality)}.$$

Problem

Is F_k (modular) monotonically increasing?

Conjecture

No. Probably it depends on the multiplicative structure of q.

Submultiplicativity

Lemma

If $q = q_1 q_2$, *then*

$$F_k(q) \leq F_k(q_1)F_k(q_2) \textit{ if } \gcd(q_1, q_2) = 1,$$

$$G_k(q) \leq G_k(q_1)G_k(q_2) \textit{ always},$$

$$H_k(q) \leq H_k(q_1)H_k(q_2) \textit{ always}.$$

Monotonicity and submultiplicativity imply that lim = inf for G and H (interval, cardinality).

Problem

Does $F_k(q) \leq F_k(q_1)F_k(q_2)$ *hold for not coprime integers?*

Comparisons

Lemma

For all q we have

$$F_k(q) \leq G_k(q),$$

$$H_k(q) \leq G_k(q),$$

$$G_k(q) \leq G_k(2q+1) \leq 2kF_k(q).$$

$$F_k(q) \leq c_k(\log q)^{k/2} H_k(q).$$

This implies that all three limits are $=$.

Problem

Is $F_k(q) \leq c_k H_k(q)$*? Is* $H_k(q) \leq F_k(q)$*?*

What is this good for?

As lim = inf, to prove that $\alpha_k < 1$ it is enough to find a **single** q with $G_k(q) < q$;
and as $G_k(q) \leq 2kF_k(q)$, it is enough to find a **single** q with

$$F_k(q) < \frac{q}{2k};$$

so it is enough to prove the following, seemingly weaker result.

Lemma

For every positive integer k and positive ε there is a positive integer q and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$, $|kA| < \varepsilon q$.

Outline of the construction

Put

$$A = \{\varphi(x), x + \varphi(x) : x \in \mathbb{Z}_q\}$$

with a function $\varphi : \mathbb{Z}_q \to \mathbb{Z}_q$ to have $A - A = \mathbb{Z}_q$.
($\varphi(x)$ is the place where we find x as a difference).

$$kA = \left\{ \sum_{x \in \mathbb{Z}_q} \Big(u(x)\varphi(x) + v(x)\big(x + \varphi(x)\big) \Big) \right\}$$

where u, v are functions $\mathbb{Z}_q \to \mathbb{Z}_{\geq 0}$ and

$$\sum_{x \in \mathbb{Z}_q} \big(u(x) + v(x)\big) = k.$$

Recursion

For a function φ and $1 \le m \le k$, $S_m(\varphi)$ denotes the set of elements that have a representation of the form

$$\sum_{x \in \mathbb{Z}_q} \Big(u(x)\varphi(x) + v(x)\big(x + \varphi(x)\big) \Big),$$

with

$$\ell(u,v) = \#\{x : u(x) + v(x) > 0\} \le m.$$

We call $\ell(u,v)$ the *level* of a pair (u,v).

$$1 \le \ell(u,v) \le k, \;\; S_1(\varphi) \subset \ldots \subset S_k(\varphi) = kA.$$

First we find a modulus and a function such that $|S_1(\varphi)| < \delta q$. Next, given two numbers $0 < \delta < \delta'$, a modulus and a function such that $|S_m(\varphi)| < \delta q$, we find a modulus q' and a function φ' such that $|S_{m+1}(\varphi')| < \delta' q'$.

Initial step

Put $q = p_0 \dots p_k$, a product of $k+1$ different primes.
$\mathbb{Z}_q = \mathbb{Z}_{p_0} \times \dots \times \mathbb{Z}_{p_k}$
Write elements of $\mathbb{Z}_q$ as vectors, $\underline{x} = (x_0, \dots, x_k)$, $x_i \in \mathbb{Z}_{p_i}$.
A pair (u, v) of level 1 is supported by a single element $\underline{x}$ and $v(\underline{x}) = k - u(\underline{x})$. Elements of $S_1(\varphi)$ are:

$$u(\underline{x})\varphi(\underline{x}) + \big(k - u(\underline{x})\big)\big(\underline{x} + \varphi(\underline{x})\big) = k\varphi(\underline{x}) + \big(k - u(\underline{x})\big)\underline{x}.$$

We make the j'th coordinate $= 0$ whenever $u(\underline{x}) = j$:

$$\varphi(x_0, \dots, x_k) = \left(-x_0, \frac{1-k}{k}x_1, \dots, \frac{j-k}{k}x_j, \dots, \frac{-1}{k}x_{k-1}, 0\right).$$

(Division in the j'th coordinate is modulo p_j.)
The number of elements with j'th coordinate $= 0$ is q/p_j, so

$$|S_1(\varphi)| \leq q \sum \frac{1}{p_j} < \delta q$$

if all $p_j > (k+1)/\delta$.

Recursive step

For some $1 \leq m < k$ we have two numbers $0 < \delta < \delta'$, a modulus q and a function such that $|S_m(\varphi)| < \delta q$.
We construct a modulus q' and a corresponding function φ' such that $|S_{m+1}(\varphi')| < \delta' q'$.
Let t be the number of pairs (u, v) of level $m+1$ on $\mathbb{Z}_q$. We put

$$q' = q p_1 p_2 \dots p_t,$$

with distinct primes $p_j \not| q$.
As before

$$\mathbb{Z}_{q'} = \mathbb{Z}_q \times \mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_t},$$

elements of $\mathbb{Z}_{q'}$ are vectors, $\underline{x} = (x_0, x_1 \dots, x_t)$, $x_0 \in \mathbb{Z}_q$, $x_i \in \mathbb{Z}_{p_i}$ for $i > 0$.
The function φ' will also be defined coordinatewise, as

$$\varphi'(\underline{x}) = \left(\varphi_0(\underline{x}), \dots, \varphi_t(\underline{x})\right), \ \varphi_0(\underline{x}) = \varphi(x_0).$$

Case of level $\leq m$

The *shadow* a pair (u', v') on $\mathbb{Z}_q'$ is a pair on $\mathbb{Z}_q$:

$$u(x) = \sum_{x_1,\dots,x_t} u'(x, x_1 \dots, x_t), \;\; v(x) = \sum_{x_1,\dots,x_t} v'(x, x_1 \dots, x_t).$$

Clearly $\ell(u, v) \leq \ell(u', v')$.
Elements of $S_{m+1}(\varphi')$ are of the form

$$\sum_{\underline{x} \in \mathbb{Z}_q'} \Big(u'(\underline{x})\varphi'(\underline{x}) + v'(\underline{x})\big(\underline{x} + \varphi'(\underline{x})\big) \Big),$$

with pairs (u', v') of level at most $m + 1$. The 0'th coordinate of this sum is exactly

$$\sum_{x \in \mathbb{Z}_q} \Big(u(x)\varphi(x) + v(x)\big(x + \varphi(x)\big) \Big),$$

where (u, v) is the shadow of (u', v'). If the level of (u, v) is at most m, then the 0'th coordinate is an element of $S_m(\varphi)$.

Case of level $= m + 1$

Assume $\ell(u,v) = \ell(u',v') = m+1$.
Let $(u_1,v_1),\dots,(u_t,v_t)$ be a list of pairs (u,v) of level $m+1$.
We make the j'th coordinate $= 0$ whenever the shadow of (u',v') is (u_j,v_j).
$\ell(u,v) = \ell(u',v')$ happens only if the elements with $u'(\underline{x}) + v'(\underline{x}) > 0$ have all different 0'th coordinates.
So for all $\underline{x} = (x_0, x_1 \dots, x_t)$ either $\big(u'(\underline{x}), v'(\underline{x})\big) = (0,0)$ or $\big(u'(\underline{x}), v'(\underline{x})\big) = \big(u_j(x_0), v_j(x_0)\big)$.
So all nonzero terms in the sum

$$\sum_{\underline{x}\in\mathbb{Z}_q'} \Big(u'(\underline{x})\varphi'(\underline{x}) + v'(\underline{x})\big(\underline{x} + \varphi'(\underline{x})\big)\Big),$$

are of the form

$$u_j(x_0)\varphi'(\underline{x}) + v_j(x_0)\big(\underline{x} + \varphi'(\underline{x})\big).$$

(Case of level $= m+1$, cont'd)
All nonzero terms in the sum

$$\sum_{\underline{x}\in\mathbb{Z}'_q}\Big(u'(\underline{x})\varphi'(\underline{x})+v'(\underline{x})\big(\underline{x}+\varphi'(\underline{x})\big)\Big),$$

are of the form

$$u_j(x_0)\varphi'(\underline{x})+v_j(x_0)\big(\underline{x}+\varphi'(\underline{x})\big).$$

The j'th coordinate of this summand is

$$u_j(x_0)\varphi_j(\underline{x})+v_j(x_0)\big(x_j+\varphi_j(\underline{x})\big).$$

This will vanish if we define

$$\varphi_j(\underline{x})=\begin{cases}-\frac{v_j(x_0)}{u_j(x_0)+v_j(x_0)} & \text{if } u_j(x_0)+v_j(x_0)>0,\\ 0 & \text{if } u_j(x_0)+v_j(x_0)=0,\end{cases}$$

division modulo p_j.

Counting

Either the 0'th coordinate is in $S_m(\varphi)$ or another coordinate vanishes. So

$$\frac{|S_{m+1}(\varphi')|}{q'} \leq \frac{|S_m(\varphi)|}{q} + \sum_{j=1}^{t} \frac{1}{p_j} < \delta + \sum_{j=1}^{t} \frac{1}{p_j} < \delta',$$

if all primes satisfy $p_j > t/(\delta' - \delta)$.
To prove the Lemma we start with $\delta = \varepsilon/(k+1)$ and proceed by finding moduli and functions with $|S_m(\varphi)|/q < (m+1)\varepsilon/(k+1)$. After k steps we have the desired bound for the size of $S_k(\varphi) = kA$.

Lower estimate

For any finite set in any group we have

$$|kA| \geq |A - A|^{1-2^{-k}}.$$

Induction on k; $k = 1$ is evident.
To go from k to $k + 1$ use the inequality

$$|X||Y - Z| \leq |Y - X||Y - Z|$$

with $Y = Z = A$, $X = -kA$.

The other side

How **big** can kA be compared to $A - A$?

$$f_k(q) = \min\{|A - A| : A \subset \mathbb{Z}_q, kA = \mathbb{Z}_q\},$$

$$g_k(q) = \min\left\{|A-A| : A \subset \mathbb{Z}, kA \supset \{a+1, \ldots, a+q\} \text{ for some } a\right\},$$

$$h_k(q) = \min\{|A - A| : A \subset \mathbb{Z}, |kA| \geq q\}.$$

Put

$$\beta_k = \inf_{q \geq 2} \frac{\log g_k(q)}{\log q}.$$

Theorem

$$\lim \frac{\log f_k(q)}{\log q} = \lim \frac{\log g_k(q)}{\log q} = \lim \frac{\log h_k(q)}{\log q} = \beta_k.$$

Theorem

(a)
$$\frac{2}{k} - \frac{1}{k^2} \leq \beta_k \leq \frac{2}{k}$$
for all k.

(b) *$k\beta_k$ is increasing.*

Problem

Is always $\beta_k < 2/k$?

Conjecture

Yes.

Problem

(Case $k = 4$.) Is always $|4A| \leq |A - A|^2$?

The End