MORE DIFFERENCES THAN MULTIPLE SUMS

IMRE Z. RUZSA

Abstract. We compare the size of the difference set $A - A$ to that of the set $kA$ of $k$-fold sums. We show the existence of sets such that $|kA| < |A - A|^{\alpha_k}$ with $\alpha_k < 1$.

1. Introduction

The aim of this paper is to compare the size of the difference set $A - A$ and the size of

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

(we shall write $k \cdot A = \{ka : a \in A\}$ for a set of multiples).

Much has been written about the most natural case $k = 2$. Freiman and Pigaev \cite{1} proved that $|2A|^{4/3} \leq |A - A| \leq |2A|^{4/3}$. These are still the best exponents known, though there is no reason to expect that either of them is exact. For other aspects and generalizations see the papers \cite{3,11,5,13} and the books \cite{7,14,12}.

We will show the existence of sets of integers such that $|kA| < |A - A|^{\alpha_k}$ with $\alpha_k < 1$, and of subsets of $\mathbb{Z}_q$, the set of residues modulo $q$ for all sufficiently large $q$ such that

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

As far as I know, the only paper to deal with this problem is Haight’s \cite{3}, who proved the existence, for arbitrary prescribed positive integers $k$ and $l$, of a $q$ and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$ and $kA$ avoids $l$ consecutive residues, and used this to show the existence of a set $B$ of reals such that $B - B = \mathbb{R}$ but $kB$ is of measure 0 for all $k$.

Clearly if $|kA| < q^{\alpha_k}$, then there will be gaps of size $> q^{1 - \alpha_k}$, so the above result implies Haight’s. On the other hand, it is not difficult to deduce our result from Haight’s either, so the two are essentially equivalent. I also acknowledge that, while the details will be rather different, the main idea is taken from Haight’s paper.

Haight’s work remained rather unnoticed. A reason is that it was well ahead of its time, before additive combinatorics became a fashionable subject; it is not an easy reading either.

In Section 6 we shall consider the opposite question about the maximal possible size of $kA$ compared to $A - A$.

2. The main results

We shall consider three ways of comparing sums and differences. For positive integers $k$ and $q$, $q > 1$ write

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

$$G_k(q) = \min \{|kA| : A \subset \mathbb{Z}, A - A \supset \{a + 1, \ldots, a + q\} \text{ for some } a\}.$$
\[ H_k(q) = \min \{|kA| : A \subset \mathbb{Z}, |A - A| \geq q \}. \]

Put
\[ \alpha_k = \inf_{q \geq 2} \frac{\log G_k(q)}{\log q}. \]

**Theorem 2.1.**
\[ \lim \frac{\log F_k(q)}{\log q} = \lim \frac{\log G_k(q)}{\log q} = \lim \frac{\log H_k(q)}{\log q} = \inf_{q \geq 2} \frac{\log H_k(q)}{\log q} = \alpha_k. \]

One possible quantity is missing from the list.

**Problem 2.2.** Is \[ \inf_{q \geq 2} \frac{\log F_k(q)}{\log q} = \alpha_k ? \]

**Theorem 2.3.**
\[ 1 - 2^{-k} \leq \alpha_k < 1 \]

for all \( k \).

The exact value is not known except the obvious \( \alpha_1 = 1/2 \). The bound \( \alpha_2 \geq 3/4 \) is Freiman and Pigaev’s [1]. The upper bound from the construction below will be of type 1-1/tower.

3. Properties of \( F, G, H \)

We list some properties of these functions that together will imply Theorem 2.1.

**Lemma 3.1.** (Monotonicity.) If \( q < q' \), then
\[ G_k(q) \leq G_k(q'), \]
\[ H_k(q) \leq H_k(q'). \]

(Obvious, but important.)

**Problem 3.2.** Is \( F_k \) monotonically increasing?

**Conjecture 3.3.** No. Probably it depends on the multiplicative structure of \( q \), not just its size.

**Lemma 3.4.** (Submultiplicativity.) Let \( q = q_1 q_2 \). We have
\[ F_k(q) \leq F_k(q_1)F_k(q_2) \text{ if } \gcd(q_1, q_2) = 1, \]
\[ G_k(q) \leq G_k(q_1)G_k(q_2) \text{ always}, \]
\[ H_k(q) \leq H_k(q_1)H_k(q_2) \text{ always}. \]

**Proof.** Let \( A_1, A_2 \) be sets that give the value of our function for \( q_1 \) and \( q_2 \), resp.

To see (3.1) notice that \( \mathbb{Z}_q \) is isomorphic to the direct product \( \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \), and the set \( A = A_1 \times A_2 \) gives the bound for \( F(q) \).

To see (3.2) take the set \( A = A_1 + q_1 \cdot A_2 \).

To see (3.3) take the set \( A = A_1 + m \cdot A_2 \) with an integer \( m \) chosen sufficiently large to avoid unwanted coincidences. \( \square \)
Problem 3.5. Does $F_k(q) \leq F_k(q_1)F_k(q_2)$ hold for not coprime integers?

Monotonicity and submultiplicativity imply that
\[
\lim_{q \to \infty} \frac{\log G_k(q)}{\log q} = \inf_{q \geq 2} \frac{\log G_k(q)}{\log q} = \alpha_k, \quad \lim_{q \to \infty} \frac{\log H_k(q)}{\log q} = \inf_{q \geq 2} \frac{\log H_k(q)}{\log q}.
\]

To prove the other equalities in Theorem 2.1 we show that these functions have the same order of magnitude.

Lemma 3.6. For all $q$ we have
\begin{align*}
(3.4) & \quad F_k(q) \leq G_k(q), \\
(3.5) & \quad H_k(q) \leq G_k(q), \\
(3.6) & \quad G_k(q) \leq G_k(2q + 1) \leq 2kF_k(q).
\end{align*}

Proof. Inequalities (3.4) and (3.5) are evident.

To show (3.6), let $A \subset \mathbb{Z}_q$ be a set such that $A - A = \mathbb{Z}_q$, $|kA| = F_k(q)$. Define $A' = \{ n : -q < n \leq q, n \mod q \in A \}$.

We claim that $A' - A'$ contains $2q + 1$ consecutive integers, namely those in the interval $[-q, q]$. Indeed, if $-q \leq m \leq q$, then there are $x, y \in A'$, $1 \leq x, y \leq q$ such that
\[ x - y \equiv m \pmod{q}. \]

Consequently one of $x - y$, $(x - q) - y$, $x - (y - q)$ will be equal to $m$, and all are elements of $A' - A'$. To estimate $|kA'|$ observe that
\[ kA' \subset [-k(q - 1), kq]. \]

This interval can be covered by $2k$ intervals of length $q$, and in each our set has at most $|kA|/q$ elements, hence $|kA'| \leq 2k|kA|$. \hfill \Box

These results partially show Theorem 2.1 except for the quantities involving $H_k$. For $H_k$ we shall give the following estimate.

Lemma 3.7. \begin{equation}
F_k(q) \leq c_k (\log q)^{k/2} H_k(q).
\end{equation}

The proof of this lemma is relegated to Section 5. To prove our main result, Theorem 2.3 we shall work with $F$ and $G$; the results about $H$ are included because it is perhaps the most natural quantity to consider.

Problem 3.8. Is $F_k(q) \leq c_k H_k(q)$? Is $H_k(q) \leq F_k(q)$?

4. The Construction

In this section we prove that $\alpha_k < 1$. We start by proving the following, seemingly weaker result.

Lemma 4.1. For every positive integer $k$ and positive $\varepsilon$ there is a positive integer $q$ and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$, $|kA| < \varepsilon q$. 

Proof. We shall describe our set in the form

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

via a function \( \varphi : \mathbb{Z}_q \to \mathbb{Z}_q \). This guarantees \( A - A = \mathbb{Z}_q \).

The set \( kA \) is the collection of all elements of the form

\[ (u(x)\varphi(x) + v(x)(x + \varphi(x))) \]

where \( u, v \) are nonnegative integer-valued functions on \( \mathbb{Z}_q \), satisfying

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

We define the level of such a pair \((u, v)\) of functions as

\[ l(u, v) = \#\{ x : u(x) + v(x) > 0 \}. \]

Clearly \( 1 \leq l(u, v) \leq k \).

For a function \( \varphi \) and \( 1 \leq m \leq k \), let \( S_m(\varphi) \) denote the set of elements that have a representation of the form \((\text{4.1})\) with \( l(u, v) \leq m \) (in particular, \( S_k(\varphi) = kA \)). The construction will proceed recursively. First we show how to find a modulus and a function such that \( |S_1(\varphi)| < \delta q \). Next we show that, given two numbers \( \delta, \delta' \) such that \( 0 < \delta < \delta' \), a modulus and a function such that \( |S_m(\varphi)| < \delta q \), we can find a modulus \( q' \) and a corresponding function \( \varphi' \) such that \( |S_{m+1}(\varphi')| < \delta' q' \).

For the first step we will take a product of \( k + 1 \) different primes, \( q = p_0 \ldots p_k \) and identify \( \mathbb{Z}_q \) with the direct product \( \mathbb{Z}_{p_0} \times \ldots \times \mathbb{Z}_{p_k} \). We shall write elements of \( \mathbb{Z}_q \) as vectors, \( \underline{x} = (x_0, \ldots, x_k) \), \( x_i \in \mathbb{Z}_{p_i} \). A pair \((u, v)\) of level 1 is supported by a single element \( \underline{x} \); necessarily \( v(x) = k - u(x) \). Hence elements of \( S_1(\varphi) \) are of the form

\[ u(x)\varphi(x) + (k - u(x))(x + \varphi(x)) = k\varphi(x) + (k - u(x))\underline{x}. \]

We will achieve that whenever \( u(\underline{x}) = j \), the \( j' \)th coordinate of this sum will vanish. To this end we put

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

Here division in the \( j' \)th coordinate is meant modulo \( p_j \), and in order that this make sense we assume \( p_j > k \) for all \( j \).

The number of elements where the \( j' \)th coordinate vanishes is exactly \( q/p_j \), consequently we have

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

if we select primes so that \( p_j > (k + 1)/\delta \).

For the inductive step, assume that for some \( 1 \leq m < k \) we are given two numbers \( \delta, \delta' \) such that \( 0 < \delta < \delta' \), a modulus \( q \) and a function such that \( |S_m(\varphi)| < \delta q \). We shall construct a modulus \( q' \) and a corresponding function \( \varphi' \) such that \( |S_{m+1}(\varphi')| < \delta' q' \).

Let \( t \) be the number of pairs \((u, v)\) of level \( m + 1 \) on \( \mathbb{Z}_q \). Our new number will be of the form

\[ q' = qp_1p_2 \ldots p_t, \]
with distinct primes $p_j$, not dividing $q$. We identify $\mathbb{Z}_q$ with the direct product $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_t}$. We shall write elements of $\mathbb{Z}_q'$ as vectors, $\underline{x} = (x_0, x_1, \ldots, x_i)$, $x_0 \in \mathbb{Z}_q$, $x_i \in \mathbb{Z}_{p_i}$ for $i > 0$. The function $\varphi'$ will also be defined coordinatewise, as

$$\varphi'(\underline{x}) = (\varphi_0(x), \ldots, \varphi_t(x)).$$

We put $\varphi_0(x) = \varphi(x_0)$.

Given a pair $(u', v')$ on $\mathbb{Z}_q'$, we define its shadow on $\mathbb{Z}_q$ by the formula

$$u(x) = \sum_{x_1, \ldots, x_i} u'(x, x_1, \ldots, x_i), \quad v(x) = \sum_{x_1, \ldots, x_i} v'(x, x_1, \ldots, x_i).$$

Clearly the level of $(u, v)$ does not exceed the level of $(u', v')$.

Elements of $S_{m+1}(\varphi')$ are of the form

$$(4.2) \quad \sum_{x \in \mathbb{Z}_q} \left( u'(\underline{x}) \varphi'(\underline{x}) + v'(\underline{x})(x + \varphi'(\underline{x})) \right),$$

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

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

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

Now we consider the case when the level of $(u, v)$, as well as of $(u', v')$, is $m + 1$. Let $(u_1, v_1), \ldots, (u_t, v_t)$ be a list of all pairs $(u, v)$ of level $m + 1$. We shall achieve that the $j$'th coordinate vanish whenever the shadow of $(u', v')$ is $(u_j, v_j)$.

Observe that the level of a pair $(u', v')$ and that of its shadow can be equal only if there is no coincidence among the 0'th coordinate of those elements for which $u'(\underline{x}) + v'(\underline{x}) > 0$; the sum defining the shadow has always at most one nonzero term. Consequently for all $\underline{x} = (x_0, x_1, \ldots, x_i)$ either $(u'(\underline{x}), v'(\underline{x})) = (0, 0)$ or $(u'(\underline{x}), v'(\underline{x})) = (u_j(x_0), v_j(x_0))$. Thus all nonzero terms in the sum $(4.2)$ are of the form

$$u_j(x_0) \varphi(x) + v_j(x_0)(x + \varphi(x)).$$

The $j$'th coordinate of this summand is

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

This will vanish if we define

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

the division being understood modulo $p_j$.

This construction ensures that either the 0'th coordinate is in $S_m(\varphi)$ or another coordinate vanishes. Hence

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

if we choose primes satisfying $p_j > t/(\delta' - \delta)$.

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 $S_k(\varphi) = kA$. \qed
Remark 1. For the initial step I know several constructions, some of which yield smaller values of $q$; I chose this one because it anticipates the inductive step.

Proof of Theorem 2.3. By virtue of Theorem 2.1, to prove the upper bound it is sufficient to find a single $q$ such that $G_k(q) < q$; and by inequality (3.6), it suffices to find a single $q$ such that $F_k(q) < q/k$, which is the previous lemma with $\varepsilon = 1/k$.

To demonstrate the lower bound we show that for any finite set in any group we have

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

We use induction on $k$. The case $k = 1$ is evident. To go from $k$ to $k + 1$ we use the inequality [9] (see also [7],[14],[12])

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

with $Y = Z = A$, $X = -kA$. □

5. From integers to residues

In this section we prove Lemma 3.7.

We start with an arbitrary set $A$ of integers, and in several steps we turn it into a set of residues modulo $q$. Our tool will be the following projection-like transformation, which depends on a real parameter $t$:

$$\pi_t(n) = \lfloor q\{tn\} \rfloor.$$ 

(We suppress the parameter $q$, which will be fixed through the section.) The values of $\pi_t$ are integers in $[1, q)$, and $\pi_t$ has a quasi-additivity property:

$$\pi_t(x + y) = \pi_t(x) + \pi_t(y) + r, \ r \in \{0, 1, -q, 1 - q\}.$$ 

Lemma 5.1. Let $S$ be a set of integers, $|S| = q$. There is a $t \in (0, 1)$ such that

$$|\pi_t(S)| > q/3.$$ 

Proof. We select $t \in [0, 1)$ randomly with uniform distribution. Let $z$ be the number of pairs $m, n \in S$ such that $\pi_t(m) = \pi_t(n)$. For a fixed pair $(m, n)$ the probability that $\pi_t(m) = \pi_t(n)$ is 1 if $m = n$, and at most $2/q$ if $m \neq n$. To see the latter claim note that if $\pi_t(m) = \pi_t(n)$, then

$$|\{tm\} - \{tn\}| < 1/q,$$

hence $|t(m - n)| < 2/q$, which has probability $2/q$. Hence the expectation of $z$ is

$$\leq q + \frac{2}{q}q(q - 1) < 3q.$$ 

Select any $t$ for which $z < 3q$. For an integer $j \in [0, q)$ let $r_j$ be the number of integers $n \in S$ such that $\pi_t(n) = j$. The inequality of arithmetic and square means yields

$$z = \sum r_j^2 \geq \frac{(\sum r_j)^2}{|\pi_t(S)|} = \frac{q^2}{|\pi_t(S)|},$$

hence $|\pi_t(S)| \geq q^2/z > q/3$ as wanted. □
**Lemma 5.2.** Let $A \subset \mathbb{Z}_q$ be a nonempty set, $|A| \geq tq$, $0 < t < 1$, and let $k$ be a positive integer. There are sets $B_1, \ldots, B_k \subset \mathbb{Z}_q$ such that

$$A + B_1 + \ldots + B_k = \mathbb{Z}_q$$

and

$$|B_i| \leq m = \left\lceil \left( \frac{\log q}{t} \right)^{1/k} \right\rceil.$$

**Proof.** Select $B_1$ randomly, with equal probability from all $\binom{q}{m}$ $m$-element subsets of $\mathbb{Z}_q$. The probability that an element of $\mathbb{Z}_q$ is not in $A + B_1$ is

$$\left( \frac{q - |A|}{m} \right) / \binom{q}{m} < (1 - t)^m.$$

Hence the expectation of $|\mathbb{Z}_q \setminus (A + B_1)|$ is $< (1 - t)^m q$. Fix $B_1$ so that

$$|\mathbb{Z}_q \setminus (A + B_1)| < (1 - t)^m q.$$ 

Now repeat the process with $A + B_1$ in the place of $A$ to find $B_2$, and so on. After $k$ steps the number of elements outside $A + B_1 + \ldots + B_k$ will be

$$< (1 - t)^m q < e^{-tm^k} q < 1.$$

□

The case $k = 1$ of this lemma is a theorem of Lorentz [6] (see also [4]).

**Proof of Lemma 3.7.** Let $A$ be a set of integers such that $|A - A| \geq q$ and $|kA| = H_k(q)$. Put $A_1 = \pi_t(A)$ with a number $t$ such that $|\pi_t(A - A)| > q/3$. The quasi-additivity property implies that

$$\pi_t(A - A) \subset (A_1 - A_1) + \{0, -1, q, q - 1\}.$$ 

Let $A_2 \subset \mathbb{Z}_q$ be the image of $A_1$. The above inclusion shows that $(A_2 - A_2) + \{0, -1\}$ contains the image of $\pi_t(A - A)$, hence

$$|A_2 - A_2| \geq |\pi_t(A - A)|/2 > q/6.$$ 

Similarly $kA_2$ is contained in the image of $\pi_t(kA) + \{0, 1, \ldots, k - 1\}$, hence

$$|kA_2| \leq k|kA| = kH_k(q).$$ 

By Lemma 5.2 applied to the set $A_2$, there are sets $B_1, B_2 \subset \mathbb{Z}_q$ such that $(A_2 - A_2) + B_1 + B_2 = \mathbb{Z}_q$ and $|B_i| < c\sqrt{\log q}$. Our set will be $A_3 = A_2 + (B_1 \cup -B_2)$. This set satisfies $A_3 - A_3 = \mathbb{Z}_q$ and

$$|kA_3| \leq |kA_2||k(B_1 \cup -B_2)| < (c \log q)^{k/2}|kA_2| \leq k(c \log q)^{k/2}H_k(q).$$

□
6. THE OTHER SIDE

In this section we consider the question about the maximal possible size of \( kA \) compared to \( A - A \). Most results and proofs are completely analogous, and we shall not give details.

For positive integers \( k \) and \( q > 1 \) write

\[
\begin{aligned}
  f_k(q) &= \min \{|A - A| : A \subset \mathbb{Z}_q, kA = \mathbb{Z}_q\}, \\
  g_k(q) &= \min \{|A - A| : A \subset \mathbb{Z}, kA \supset \{a + 1, \ldots, a + q\} \text{ for some } a\}, \\
  h_k(q) &= \min \{|A - A| : A \subset \mathbb{Z}, |kA| \geq q\}.
\end{aligned}
\]

Put

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

**Theorem 6.1.**

\[
\lim \frac{\log f_k(q)}{\log q} = \lim \frac{\log g_k(q)}{\log q} = \lim \frac{\log h_k(q)}{\log q} = \inf_{q \geq 2} \frac{\log h_k(q)}{\log q} = \beta_k.
\]

Again, I cannot decide whether

\[
\inf_{q \geq 2} \frac{\log f_k(q)}{\log q} = \beta_k.
\]

The proof of this result proceeds through analogues of Lemmas 3.1, 3.4, 3.6, 3.7.

**Lemma 6.2.** *(Monotonicity.)* If \( q < q' \), then

\[
\begin{aligned}
  g_k(q) &\leq g_k(q'), \\
  h_k(q) &\leq h_k(q').
\end{aligned}
\]

**Problem 6.3.** Is \( f_k \) monotonically increasing?

**Conjecture 6.4.** No. Probably it depends on the multiplicative structure of \( q \), not just its size.

**Lemma 6.5.** *(Submultiplicativity.)* Let \( q = q_1q_2 \). We have

\[
\begin{aligned}
  f_k(q) &\leq f_k(q_1)f_k(q_2) \text{ if } \gcd(q_1, q_2) = 1, \\
  g_k(q) &\leq g_k(q_1)g_k(q_2) \text{ always}, \\
  h_k(q) &\leq h_k(q_1)h_k(q_2) \text{ always}.
\end{aligned}
\]

**Lemma 6.6.** For all \( q \) we have

\[
\begin{aligned}
  f_k(q) &\leq g_k(q), \\
  h_k(q) &\leq g_k(q), \\
  g_k(q) &\leq g_k(2q + 1) \leq 4f_k(q).
\end{aligned}
\]

**Lemma 6.7.**

\[
\begin{aligned}
  f_k(q) &\leq c_k(\log q)^{2/k}h_k(q).
\end{aligned}
\]
Problem 6.8. Is $f_k(q) \leq c_k h_k(q)$? Is $h_k(q) \leq f_k(q)$?

Theorem 6.9. (a): 
\[ \frac{2}{k} - \frac{1}{k^2} \leq \beta_k \leq \frac{2}{k} \]
for all $k$.
(b): $k \beta_k$ is increasing.

Proof. For the lower estimate we show that 
\[ |kA| < |A - A|^{k^2/(2k-1)} \]
for every finite set in any commutative group. Write $|A| = n$, $|A - A| = tn$. By a Plünecke-type inequality (see e.g. [8], [10], [7], [14], [13]) we get 
\[ |kA| \leq t^k n, \]
and obviously 
\[ |kA| < n^k. \]
By multiplying the $k'$th power of (6.8) and $(k - 1)$'th power of (6.9) and taking $k^2$th root we get the desired bound.

For the upper estimate take a generic set without any coincidence among the $k$-fold sums.

Claim (b) follows from the fact that $|kA|^{1/k}$ is a decreasing function of $k$, see [2]. □

Claim (b) above leaves two possibilities: either always $\beta_k < 2/k$, or $\beta_k = 2/k$ after a point.

Problem 6.10. Is always $\beta_k < 2/k$?

Conjecture 6.11. Yes.

As far as I know, the only known case is $k = 2$. I think the case $k = 4$ is particularly interesting:

Problem 6.12. Is always $|4A| \leq |A - A|^2$?

References
1. G. Freiman and V. P. Pigaev, The relation between the invariants $R$ and $T$ (Russian), Kalinin. Gos. Univ. Moscow (1973), 172–174.
2. Katalin Gyarmati, M. Matolcsi, and I. Z. Ruzsa, A superadditivity and submultiplicativity property for cardinalities of sumsets, Combinatorica 30 (2010), 163–174.
3. J. A. Haight, Difference covers which have small $k$-sums for any $k$, Mathematika 20 (1973), 109–118.
4. H. Halberstam and K. F. Roth, Sequences, Clarendon, London, 1966, 2nd ed. Springer, 1983.
5. F. Hennecart, G. Robert, and A. Yudin, On the volume of sums and differences, Structure theory of set addition, Astérisque, vol. 258, Soc. Mat. France, 1999, pp. 173–178.
6. G. G. Lorentz, On a problem of additive number theory, Proc. Amer. Math. Soc. 5 (1954), 838–841.
7. M. B. Nathanson, Additive number theory: Inverse problems and the geometry of sumsets, Graduate texts in Math., vol. 165, Springer, New York, Berlin, Heidelberg, 1996.
8. H. Plünnecke, Eine zahlentheoretische anwendung der graphtheorie, J. Reine Angew. Math. 243 (1970), 171–183.
9. I. Z. Ruzsa, On the cardinality of $A + A$ and $A - A$, Combinatorics (Keszthely 1976), Coll. Math. Soc. J. Bolyai, vol. 18, North-Holland – Bolyai Társulat, Budapest, 1978, pp. 933–938.
10. , An application of graph theory to additive number theory, Scientia, Ser. A 3 (1989), 97–109.
11. ______, *On the number of sums and differences*, Acta Math. Sci. Hungar 59 (1992), 439–447.
12. ______, *Many differences, few sums*, Ann. Univ. Eötvös 51 (2008), 27–38.
13. ______, *Sumsets and structure*, Combinatorial number theory and additive group theory, Advanced courses in mathematics, CRM Barcelona, Birkhäuser, Basel – Boston – Berlin, 2009, pp. 87–210.
14. T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.