North-Western European Journal of Mathematics

Problems in additive number theory, V: Affinely inequivalent MSTD sets

Melvyn B. Nathanson[1]

Received: November 9, 2016/Accepted: June 26, 2017/Online: July 25, 2017

Abstract

An MSTD set is a finite set of integers with more sums than differences. It is proved that, for infinitely many positive integers k, there are infinitely many affinely inequivalent MSTD sets of cardinality k. There are several related open problems.

Keywords: MSTD sets, sumsets, difference sets.

MSC: 11B13, 05A17, 05A20, 11B75, 11P99.

1 Sums and differences

In mathematics, simple calculations often suggest hard problems. This is certainly true in number theory. Here is an example:

$$3+2=2+3 \quad \text{but} \quad 3-2 \neq 2-3.$$

This leads to the following question. Let A be a set of integers, a set of real numbers, or, more generally, a subset of an additive abelian group $\mathcal{G}$. We denote the cardinality of the set A by $|A|$. Define the *sumset*

$$A+A=\{a+a' : a,a' \in A\}$$

and the *difference set*

$$A-A=\{a-a' : a,a' \in A\}.$$

For all $a,a' \in \mathcal{G}$ with $a \neq a'$, we have $a+a'=a'+a$ because $\mathcal{G}$ is abelian. However, $a-a' \neq a'-a$ if $\mathcal{G}$ is a group, such as $\mathbb{R}$ or $\mathbb{Z}$, with the property that $2x=0$ if and only if $x=0$. It is reasonable to ask: In such groups, does every finite set have the property that the number of sums does not exceed the number of differences? Equivalently, is $|A+A| \leq |A-A|$ for every finite subset A of $\mathcal{G}$?

The answer is "no." A set with more sums than differences is called an *MSTD set*.

[1] Department of Mathematics, Lehman College (CUNY), Bronx, NY 10468, USA

As expected, most finite sets A of integers do satisfy[2] $|A+A| < |A-A|$. For example, if

$$A = \{0, 2, 3\}$$

then

$$A+A = \{0, 2, 3, 4, 5, 6\} \quad \text{and} \quad A-A = \{-3, -2, -1, 0, 1, 2, 3\}$$

with

$$|A+A| = 6 < 7 = |A-A|.$$

It is also easy to construct finite sets A for which the number of sums equals the number of differences. For example, if A is an arithmetic progression of length k in a torsion-free abelian group, that is, a set of the form

$$A = \{a_0 + id : i = 0, 1, 2, \ldots, k-1\} \tag{1}$$

for some $d \neq 0$, then the number of sums equals the number of differences:

$$A+A = \{a_0 + id : i = 0, 1, 2, \ldots, 2k-2\}$$

$$A-A = \{a_0 + id : i = -(k-1), -(k-2), \ldots, -1, 0, 1, \ldots, k-2, k-1\}$$

and

$$|A+A| = |A-A| = 2k-1.$$

In an abelian group $\mathcal{G}$, the set A is *symmetric* if there exists an element $w \in \mathcal{G}$ such that $a \in A$ if and only if $w - a \in A$. For example, the arithmetic progression (1) is symmetric with respect to $w = 2a_0 + (k-1)d$. We can prove that every finite symmetric set has the same number of sums and differences. More generally, for $0 \leq j \leq h$, consider the *sum-difference set*

$$(h-j)A - jA = \left\{ \sum_{i=1}^{h-j} a_i - \sum_{i=h-j+1}^{h} a_i : a_i \in A \text{ for } i = 1, \ldots, h \right\}.$$

For $h = 2$ and $j = 0$, this is the sumset $A+A$. For $h = 2$ and $j = 1$, this is the difference set $A-A$.

[2]Cf. Hegarty and Miller, 2009, "When almost all sets are difference dominated"; Martin and O'Bryant, 2007, "Many sets have more sums than differences".

Lemma 1 – *Let A be a nonempty finite set of real numbers with $|A| = k$. For $j \in \{0,1,2,\ldots,h\}$, there is the sum-difference inequality*

$$|(h-j)A - jA| \geq h(k-1)+1.$$

Moreover,

$$|(h-j)A - jA| = h(k-1)+1$$

if and only if A is an arithmetic progression.

Proof. If A is a set of k real numbers, then $|hA| \geq h(k-1)+1$. Moreover, $|hA| = h(k-1)+1$ if and only if A is an arithmetic progression[3].

For every number t, the translated set $A' = A - t$ satisfies

$$(h-j)A' - jA' = (h-j)A - jA - (h-2j)t$$

and so

$$\Big|(h-j)A' - jA'\Big| = |(h-j)A - jA|.$$

Thus, after translating by $t = \min(A)$, we can assume that $0 = \min(A)$. In this case, we have

$$(h-j)A \cup (-jA) \subseteq (h-j)A - jA.$$

Because $(h-j)A$ is a set of nonnegative numbers and $-jA$ is a set of nonpositive numbers, we have

$$(h-j)A \cap (-jA) = \{0\}$$

and so

$$\begin{aligned} |(h-j)A - jA| &\geq |(h-j)A| + |-jA| - 1 \\ &\geq \Big((h-j)(k-1)+1\Big) + \Big(j(k-1)+1\Big) - 1 \\ &= h(k-1)+1. \end{aligned}$$

Moreover, $|(h-j)A - jA| = h(k-1)+1$ if and only if both $|(h-j)A| = (h-j)(k-1)+1$ and $|-jA| = j(k-1)+1$, or, equivalently, if and only if A is an arithmetic progression. This completes the proof. □

[3] Nathanson, 1996, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Theorem 1.6.

Theorem 1 – *Let A be a nonempty finite subset of an abelian group $\mathcal{G}$. If A is symmetric, then*

$$|(h-j)A - jA| = |hA| \tag{2}$$

for all integers $j \in \{0,1,2,\ldots,h\}$. In particular, for $h = 2$ and $j = 1$,

$$|A - A| = |A + A|.$$

Thus, symmetric sets have equal numbers of sums and differences.

Note that the nonsymmetric set

$$A = \{0,1,3,4,5,8\}$$

satisfies

$$A + A = [0,16] \setminus \{14,15\} \quad \text{and} \quad A - A = [-8,8] \setminus \{\pm 6\}$$

and so

$$|A + A| = |A - A| = 15.$$

This example[4] shows that there also exist non-symmetric sets of integers with equal numbers of sums and differences.

Proof. If $j = 0$, then $(h-j)A - jA = hA$. If $j = h$, then $(h-j)A - jA = -hA$. Equation (2) holds in both cases. Thus, we can assume that $1 \leq j \leq h-1$.

Let A be a symmetric subset with respect to $w \in \mathcal{G}$. Thus, $a \in A$ if and only if $w - a \in A$. For every integer j, define the function $f_j : \mathcal{G} \to \mathcal{G}$ by $f_j(x) = x + jw$. For all $j, \ell \in \mathbb{Z}$ we have $f_j f_\ell = f_{j+\ell}$. In particular, $f_j f_{-j} = f_0 = \mathrm{id}$ and f_j is a bijection.

Let $x = \sum_{i=1}^h a_i \in hA$, and let $a_i' = w - a_i \in A$ for $i = 1,\ldots,h$. If $1 \leq i \leq j \leq h$, then

$$\begin{aligned} f_{-j}(x) &= \left(\sum_{i=1}^{h} a_i \right) - jw \\ &= \sum_{i=1}^{h-j} a_i - \sum_{i=h-j+1}^{h} (w - a_i) \\ &= \sum_{i=1}^{h-j} a_i - \sum_{i=h-j+1}^{h} a_i' \quad \in (h-j)A - jA \end{aligned}$$

and so

$$|hA| \leq |(h-j)A - jA|.$$

[4]Due to Marica, 1969, "On a conjecture of Conway".

Let $y = \sum_{i=1}^{h-j} a_i - \sum_{i=h-j+1}^{h} a_i \in (h-j)A - jA$. For $h-j+1 \le i \le h$, let $a_i' = w - a_i \in A$. Then

$$\begin{aligned} f_j(y) &= \left(\sum_{i=1}^{h-j} a_i - \sum_{i=h-j+1}^{h} a_i \right) + jw \\ &= \sum_{i=1}^{h-j} a_i + \sum_{i=h-j+1}^{h} (w - a_i) \\ &= \sum_{i=1}^{h-j} a_i + \sum_{i=h-j+1}^{h} a_i' \quad \in hA \end{aligned}$$

and so

$$|(h-j)A - jA| \le |hA|.$$

Therefore, $|(h-j)A - jA| = |hA|$ and the proof is complete. □

Let A be a nonempty set of integers. We denote by $\gcd(A)$ the greatest common divisor of the integers in A. For real numbers u and v, we define the *interval of integers* $[u,v] = \{n \in \mathbb{Z} : u \le n \le v\}$. If u_1, v_1, u_2, v_2 are integers, then $[u_1,v_1]+[u_2,v_2] = [u_1+u_2, v_1+v_2]$.

Theorem 2 – *Let A be a finite set of nonnegative integers with $|A| \ge 2$ such that $0 \in A$ and $\gcd(A) = 1$. Let $a^* = \max(A)$. There exist integers h_1, C, and D and sets of integers $\mathscr{C}^* \subseteq [0, C+D-1]$ and $\mathscr{D}^* \subseteq [0, C+D-1]$ such that, if $h \ge 2h_1$, then the sum-difference set has the structure*

$$ja^* + (h-j)A - jA = \mathscr{C}^* \cup [C+D, ha^* - (C+D)] \cup (ha^* - \mathscr{D}^*)$$

for all integers j in the interval $[h_1, h-h_1]$. Moreover,

$$|(h-j)A - jA| = \left|(h-j')A - j'A\right|$$

for all integers $j, j' \in [h_1, h-h_1]$.

Proof. Because $A \subseteq [0,a^*]$, we have $hA \subseteq [0, ha^*]$ for all nonnegative integers h. By a fundamental theorem of additive number theory[5], there exists a positive integer $h_0 = h_0(A)$ and there exist nonnegative integers C and D and sets of integers $\mathscr{C} \subseteq [0, C-2]$ and $\mathscr{D} \subseteq [0, D-2]$ such that, for all $h \ge h_0$, the sumset hA has the rigid structure

$$hA = \mathscr{C} \cup [C, ha^* - D] \cup (ha^* - \mathscr{D}). \tag{3}$$

Let

$$h_1 = h_1(A) = \max\left(h_0, \frac{2C+D}{a^*}, \frac{C+2D}{a^*}\right). \tag{4}$$

Let $h \geq 2h_1$. If $j \in [h_1, h-h_1]$, then

$$j \geq h_1 \quad \text{and} \quad h-j \geq h_1.$$

Let $r = h-j$. Applying the structure (3) on the previous page, we obtain the sumsets

$$rA = \mathscr{C} \cup [C, ra^* - D] \cup (ra^* - \mathscr{D})$$

and

$$jA = \mathscr{C} \cup [C, ja^* - D] \cup (ja^* - \mathscr{D}).$$

Rearranging the identity for jA gives

$$ja^* - jA = \mathscr{D} \cup [D, ja^* - C] \cup (ja^* - \mathscr{C}).$$

We have

$$\begin{aligned} [C+D, ha^* - (C+D)] &= [C, ra^* - D] + [D, ja^* - C] \\ &\subseteq rA + (ja^* - jA). \end{aligned}$$

It follows from (4) that

$$\begin{aligned} \min(ja^* - \mathscr{C}) &\geq ja^* - (C-2) \\ &> ja^* - C \\ &\geq h_1 a^* - C \\ &\geq (2C+D) - C = C+D. \end{aligned}$$

Similarly,

$$\min(ra^* - \mathscr{D}) > ra^* - D \geq C + D.$$

These lower bounds imply that for

$$n \in [0, C+D-1] \quad \text{and} \quad j \in [h_1, h-h_1]$$

we have $n \in rA + (ja^* - jA)$ if and only if

$$n \in (\mathscr{C} + \mathscr{D}) \cup (\mathscr{C} + [D, ja^* - C]) \cup (\mathscr{D} + [C, ra^* - D])$$

if and only if

$$n \in (\mathscr{C} + \mathscr{D}) \cup (\mathscr{C} + [D, C+D]) \cup (\mathscr{D} + [C, C+D]).$$

Therefore,

$$\begin{aligned}\mathscr{C}^* &= [0, C+D-1] \cap ((\mathscr{C}+\mathscr{D}) \cup (\mathscr{C}+[D, C+D]) \cup (\mathscr{D}+[C, C+D])) \\ &= [0, C+D-1] \cap (rA + (ja^* - jA))\end{aligned}$$

for all $j \in [h_1, h-h_1]$. Similarly, there exists a set $\mathscr{D}^* \subseteq [0, C+D-1]$ such that

$$ha^* - \mathscr{D}^* = [ha^* - (C+D)+1), ha^*] \cap (rA + (ja^* - jA))$$

for all $j \in [h_1, h-h_1]$. Therefore,

$$\begin{aligned}ja^* + (h-j)A - jA &= (rA + (ja^* - jA)) \\ &= \mathscr{C}^* \cup [C+D, ha^* - (C+D)] \cup (ha^* - \mathscr{D}^*)\end{aligned}$$

for all $j \in [h_1, h-h_1]$. This completes the proof. □

Problem 1 – *Let A be a set of k integers. For $j = 0, 1, \ldots, h$, let*

$$f_{A,h}(j) = |(h-j)A - jA|.$$

- *Is* $\max\Big(f_{A,h}(j) : j = 0, 1, \ldots, h\Big) = f_{A,h}\left(\left[\frac{h}{2}\right]\right)$ *?*
- *Is the function $f_{A,h}(j)$ unimodal?*

Although the conjecture that a finite set of integers has no more sums than differences is reasonable, the conjecture is false. Here are three counterexamples. The set

$$A = \{0, 2, 3, 4, 7, 11, 12, 14\}$$

with $|A| = 8$ and with sumset

$$A + A = [0, 28] \setminus \{1, 20, 27\}$$

and difference set

$$A - A = [-14, 14] \setminus \{6, -6, 13, -13\}$$

satisfies

$$|A + A| = 26 > 25 = |A - A|.$$

Note that $A = \{0, 2, 3, 7, 11, 12, 14\} \cup \{4\}$, where the set $\{0, 2, 3, 7, 11, 12, 14\}$ is symmetric. This observation is exploited in Nathanson[6].

[5] Nathanson, 1972, "Sums of finite sets of integers";
Nathanson, 1996, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*.

[6] Nathanson, 2007b, "Sets with more sums than differences".

The set

$$B = \{0, 1, 2, 4, 7, 8, 12, 14, 15\}$$

with $|B| = 9$ and with sumset

$$B + B = [0, 30] \setminus \{25\}$$

and difference set

$$B - B = [-15, 15] \setminus \{9, -9\}$$

satisfies

$$|B + B| = 30 > 29 = |B - B|.$$

The set

$$C = \{0, 1, 2, 4, 5, 9, 12, 13, 14, 16, 17, 21, 24, 25, 26, 28, 29\}$$

with $|C| = 17$ and with sumset

$$C + C = [0, 58]$$

and difference set

$$C - C = [-29, 29] \setminus \{\pm 6, \pm 18\}$$

satisfies

$$|C + C| = 59 > 55 = |C - C|.$$

Set B appears in Marica[7] and set C in Freiman and Pigarev[8].

An *MSTD set* in an abelian group $\mathcal{G}$ is a finite set that has more sums than differences. MSTD sets of integers have been extensively investigated in recent years, but they are still mysterious and many open problems remain. MSTD sets of real numbers and MSTD sets in arbitrary abelian groups have also been studied. In this paper we consider only MSTD sets contained in the additive groups $\mathbb{Z}$ and $\mathbb{R}$. There are constructions of various infinite families of MSTD sets of integers[9], but there is no complete classification.

Problem 2 – *A fundamental problem is to classify the possible structures of MSTD sets of integers and of real numbers.*

[7] Marica, 1969, "On a conjecture of Conway".

[8] Freiman and Pigarev, 1973, "The relation between the invariants R and T".

[9] E.g. Hegarty, 2007, "Some explicit constructions of sets with more sums than differences"; Miller, Orosz, and Scheinerman, 2010, "Explicit constructions of infinite families of MSTD sets"; Nathanson, 2007a, *Problems in additive number theory. I, Additive Combinatorics*.

Let $\mathcal{G}$ denote $\mathbb{R}$ or $\mathbb{Z}$. For all $\lambda, \mu \in \mathcal{G}$ with $\lambda \neq 0$, we define the *affine map* $f : \mathcal{G} \to \mathcal{G}$ by

$$f(x) = \lambda x + \mu.$$

An affine map is one-to-one. Subsets A and B of $\mathcal{G}$ are *affinely equivalent* if there exists an affine map $f : A \to B$ or $f : B \to A$ that is a bijection.

Let $k \geq 2$ and let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a set of integers such that

$$a_0 < a_1 < \cdots < a_{k-1}.$$

Let

$$d = \gcd(\{a_i - a_0 : i = 1, \ldots, k-1\})$$

and

$$a'_i = \frac{a_i - a_0}{d}$$

for $i = 0, 1, \ldots, k-1$. Let $A' = \left\{a'_0, a'_1, \ldots, a'_{k-1}\right\}$. We have

$$0 = a'_0 < a'_1 < \cdots < a'_{k-1}.$$

Note that

$$\min(A') = 0 \quad \text{and} \quad \gcd(A') = 1.$$

We call A' the *normal form* of A.

Consider the affine map $f(x) = dx + a_0$. We have

$$A = \left\{da'_i + a_0 : i = 0, 1, \ldots, k-1\right\} = \left\{f(a'_i) : i = 0, 1, \ldots, k-1\right\} = f(A')$$

and so $f : A' \to A$ is a bijection and the sets A and A' are affinely equivalent.

A property of a set is an *affine invariant* if, for all affinely equivalent sets A and B, the set A has the property if and only if the set B has the property.

The property of being an MSTD set is an affine invariant. Let f be an affine map on $\mathcal{G}$. For all $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4} \in \mathcal{G}$, the following statements are equivalent:

$$a_{i_1} - a_{i_2} = a_{i_3} - a_{i_4}$$
$$a_{i_1} + a_{i_4} = a_{i_2} + a_{i_3}$$
$$f(a_{i_1}) + f(a_{i_4}) = f(a_{i_2}) + f(a_{i_3})$$
$$f(a_{i_1}) - f(a_{i_2}) = f(a_{i_3}) - f(a_{i_4}).$$

This implies that if A is an MSTD set, then $B = f(A)$ is an MSTD set for every affine map f. Thus, to classify MSTD sets of real numbers or of integers, it suffices to classify them up to affine maps.

In the group of integers, Hegarty[10] proved that that there exists no MSTD set of cardinality less than 8, and that every MSTD set of cardinality 8 is affinely equivalent to the set $\{0,2,3,4,7,11,12,14\}$.

Let $\mathcal{H}(k,n)$ denote the number of affinely inequivalent MSTD sets of integers of cardinality k contained in the interval $[0,n]$. Thus, Hegarty proved that $\mathcal{H}(k,n) = 0$ for $k \leq 7$ and all positive integers n, that $\mathcal{H}(8,n) = 0$ for $n \leq 13$, and that $\mathcal{H}(8,n) = 1$ for $n \geq 14$.

Problem 3 – *Why does there exist no MSTD set of integers of size 7?*

Problem 4 – *Let $k \geq 9$. Compute $\mathcal{H}(k,n)$. Describe the asymptotic growth of $\mathcal{H}(k,n)$ as $n \to \infty$.*

Problem 5 – *For fixed n, describe the behavior of $\mathcal{H}(k,n)$ as a function of k. For example, is $\mathcal{H}(k,n)$ a unimodal function of k? Note that $\mathcal{H}(k,n) = 0$ for $k > n$.*

For fixed k, the function $\mathcal{H}(k,n)$ is a monotonically increasing function of n. Denoting by $\mathcal{H}(k)$ the number of affinely inequivalent MSTD sets of cardinality k, we have

$$\mathcal{H}(k) = \lim_{n\to\infty} \mathcal{H}(k,n).$$

Thus, $\mathcal{H}(k) = \infty$ if there exist infinitely many affinely inequivalent MSTD sets of integers of cardinality k.

For every finite set A of integers, define

$$\Delta(A) = |A - A| - |A + A|.$$

The set A is an MSTD set if and only if $\Delta(A) < 0$.

Lemma 2 – *Let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a set of k integers with*

$$0 = a_0 < a_1 < \cdots < a_{k-1}.$$

If a_k is an integer such that

$$2a_{k-1} < a_k$$

and if

$$A' = A \cup \{a_k\}$$

then

$$\Delta(A') - \Delta(A) = k - 1.$$

[10] Hegarty, 2007, "Some explicit constructions of sets with more sums than differences".

Proof. We have

$$A' + A' = (A + A) \cup \{a_k + a_i : i = 0, 1, \ldots, k\}.$$

Because $\max(A + A) = 2a_{k-1} < a_k < a_k + a_1 < \cdots < a_k + a_{k-1} < 2a_k$ we have

$$\left|A' + A'\right| = |A + A| + k + 1.$$

Similarly,

$$A' - A' = (A - A) \cup \{\pm(a_k - a_i) : i = 0, 1, \ldots, k - 1\}.$$

Because $\max(A - A) = a_{k-1} < a_k - a_{k-1} < a_k - a_{k-2} < \cdots < a_k - a_1 < a_k$ and $\min(A - A) = -a_{k-1} > -a_k + a_{k-1} > \cdots > -a_k + a_1 > -a_k$ we have

$$\left|A' - A'\right| = |A - A| + 2k.$$

Therefore,

$$\begin{aligned} \Delta(A') &= \left|A' - A'\right| - \left|A' + A'\right| \\ &= (|A - A| + 2k) - (|A + A| + k + 1) \\ &= \Delta(A) + k - 1. \end{aligned}$$

This completes the proof. □

Lemma 3 – *Let B be an* MSTD *set of integers with*

$$|B + B| \geq |B - B| + |B|.$$

There exist infinitely many affinely inequivalent MSTD *sets of integers of cardinality $|B| + 1$, that is, $\mathcal{H}(|B| + 1) = \infty$.*

Proof. Let $|B| = \ell$. Translating the set B by $\min(B)$, we can assume that $0 = \min(B)$. Let $b_{\ell-1} = \max(B)$. The inequality

$$|B + B| \geq |B - B| + |B|$$

is equivalent to

$$\Delta(B) \leq -\ell.$$

For every integer $b_\ell > 2b_{\ell-1}$ and $B' = B \cup \{b_\ell\}$, Lemma 2 on the preceding page implies that

$$\Delta(B') = \Delta(B) + \ell - 1 \leq -1$$

and so

$$\left|B' - B'\right| < \left|B' + B'\right|.$$

Therefore, B' is an MSTD set of integers of cardinality $\ell + 1$. If $b'_\ell > b_\ell > 2b_{\ell-1}$, then the sets $B \cup \{b_\ell\}$ and $B \cup \left\{b'_\ell\right\}$ are affinely inequivalent, and so $\mathcal{H}(\ell + 1) = \infty$. □

Lemma 4 – *Let A be a nonempty finite set of nonnegative integers with $a^* = \max(A)$. Let m be a positive integer with*

$$m > 2a^*.$$

If n is a positive integer and

$$B = \left\{ \sum_{i=0}^{n-1} a_i m^i : a_i \in A \text{ for all } i = 0, 1, \ldots, n-1 \right\} \tag{5}$$

then

$$|B| = |A|^n, \quad |B+B| = |A+A|^n \quad \text{and} \quad |B-B| = |A-A|^n.$$

Proof. The first two identities follow immediately from the uniqueness of the m-adic representation of an integer.

If $y \in B - B$, then there exist $x = \sum_{i=0}^{n-1} a_i m^i \in B$ and $\tilde{x} = \sum_{i=0}^{n-1} \tilde{a}_i m^i \in B$ such that

$$y = x - \tilde{x} = \sum_{i=0}^{n-1} (a_i - \tilde{a}_i) m^i = \sum_{i=0}^{n-1} d_i m^i$$

where $d_i \in A - A$ for all $i = 0, 1, \ldots, n-1$.

Let $d_i, d_i' \in A - A$ for $i = 0, 1, \ldots, n-1$. We have $|d_i| \leq a^*$, $\left|d_i'\right| \leq a^*$, and so

$$\left|d_i - d_i'\right| \leq 2a^* \leq m - 1.$$

Define $y, y' \in B - B$ by $y = \sum_{i=0}^{n-1} d_i m^i$ and $y' = \sum_{i=0}^{n-1} d_i' m^i$. Suppose that $y = y'$. If $d_{r-1} \neq d_{r-1}'$ for some $r \in \{1, \ldots, n\}$ and $d_i = d_i'$ for $i = r, \ldots, n-1$, then

$$0 = y - y' = \sum_{i=0}^{n-1} (d_i - d_i') m^i = \sum_{i=0}^{r-1} (d_i - d_i') m^i$$

and so

$$(d_{r-1}' - d_{r-1}) m^{r-1} = \sum_{i=0}^{r-2} (d_i - d_i') m^i.$$

Taking the absolute value of each side of this equation, we obtain

$$m^{r-1} \leq \left|d_{r-1}' - d_{r-1}\right| m^{r-1} = \left| \sum_{i=0}^{r-2} (d_i - d_i') m^i \right|$$

(Cont. next page)

$$\leq 2a^* \sum_{i=0}^{r-2} m^i$$

$$< \left(\frac{2a^*}{m-1}\right) m^{r-1} \leq m^{r-1}$$

which is absurd. Therefore, $y = y'$ if and only if $d_i = d_i'$ for all $i = 0, 1, \ldots, n-1$, and so $|B - B| = |A - A|^n$. This completes the proof. □

Hegarty and Miller; Martin and O'Bryant[11] used probability arguments to prove that there are infinitely many MSTD sets of cardinality k for all sufficiently large k. The following theorem gives a constructive proof that, for infinitely many k, there exist infinitely many affinely inequivalent MSTD sets of integers of cardinality k.

Theorem 3 – *If there exists an* MSTD *set of integers of cardinality k, then $\mathcal{H}(k^n + 1) = \infty$ for all integers $n \geq k$.*

Proof. For all integers $n \geq k \geq 1$, we have $2k - 1 \geq k$ and

$$n(2k-1)^{n-1} \geq k \cdot k^{n-1} = k^n.$$

Let A be a nonempty set of integers of cardinality k. After an affine transformation, we can assume that $\min(A) = 0$, $\gcd(A) = 1$, and $\max(A) = a^*$. Moreover,

$$A - A \supseteq \{0\} \cup \{\pm a : a \in A \setminus \{0\}\}$$

and so

$$|A - A| \geq 2k - 1.$$

Choose $m > 2a^*$ and $n \geq k$, and define the set B by Equation (5) on the preceding page.

If A is an MSTD set, then $|A + A| \geq |A - A| + 1$. Applying Lemma 4 on the preceding page, we obtain $|B| = k^n$ and

$$\begin{aligned} |B + B| &= |A + A|^n \\ &\geq (|A - A| + 1)^n \\ &> |A - A|^n + n|A - A|^{n-1} \\ &\geq |A - A|^n + n(2k-1)^{n-1} \\ &\geq |A - A|^n + k^n \\ &= |B - B| + |B|. \end{aligned}$$

Applying Lemma 3 on p. 131 with $\ell = k^n$, we see that B is an MSTD set. Because we have infinitely many choices of m and n, it follows that $\mathcal{H}(k^n + 1) = \infty$. This completes the proof. □

Problem 6 – *Compute the smallest k such that $\mathcal{H}(k) = \infty$. We know only that $k \geq 9$.*

Problem 7 – *Do there exist infinitely many affinely inequivalent* MSTD *sets of integers of cardinality k for all sufficiently large k?*

[11] Hegarty and Miller, 2009, "When almost all sets are difference dominated";
Martin and O'Bryant, 2007, "Many sets have more sums than differences".

2 An incomplete history

Marica wrote the first paper on sets with more sums than differences. His paper starts with a quotation from unpublished mimeographed notes of Croft[12]:

> Problem 7 of Section VI of H. T. Croft's "Research Problems" (August, 1967 edition) is by J. H. Conway:
>
> A is a finite set of integers $\{a_i\}$. $A+A$ denotes $\{a_i+a_j\}$, $A-A$ denotes $\{a_i-a_j\}$. Prove that $A-A$ always has more numbers than $A+A$ unless A is symmetrical about 0.[13]

I have been unable to obtain a copy of these notes. Conway (personal communication) says that he did not make this conjecture, and, in fact, produced a counterexample. The smallest MSTD set is $\{0,2,3,4,7,11,12,14\}$, but I do not know where this set first appeared. The first published example of an MSTD set is Marica's set $\{1,2,3,5,8,9,13,15,16\}$. There is a related note of Spohn[14]. Freiman and Pigarev (1973) is another significant early work.

Nathanson[15] introduced the term *MSTD sets*. There is important early work of Roesler[16] and Ruzsa[17], and the related paper of Hennecart, Robert, and Yudin[18]. Steve Miller and his students and colleagues have contributed greatly to this subject[19].

There has also been great interest in the Lebesgue measure of sum and difference sets[20].

---

[12] Croft, 1967, "Research problems, Problem 7, Section VI".

[13] Marica, 1969, "On a conjecture of Conway".

[14] Spohn, 1971, "On Conway's conjecture for integer sets".

[15] Nathanson, 2007a, *Problems in additive number theory. I, Additive Combinatorics*.

[16] Roesler, 2000, "A mean value density theorem of additive number theory".

[17] Ruzsa, 1978, "On the cardinality of $A+A$ and $A-A$";
Ruzsa, 1984, "Sets of sums and differences";
Ruzsa, 1992, "On the number of sums and differences".

[18] Hennecart, Robert, and Yudin, 1999, "On the number of sums and differences".

[19] Do, Kulkarni, Miller, Moon, and Wellens, 2015, "Sums and differences of correlated random sets";
Do, Kulkarni, Miller, Moon, Wellens, and Wilcox, 2015, "Sets characterized by missing sums and differences in dilating polytopes";
Iyer et al., 2012, "Generalized more sums than differences sets";
Iyer et al., 2014, "Finding and counting MSTD sets";
Miller, Orosz, and Scheinerman, 2010, "Explicit constructions of infinite families of MSTD sets";
Miller, Robinson, and Pegado, 2012, "Explicit constructions of large families of generalized more sums than differences sets";
Miller and Scheinerman, 2010, "Explicit constructions of infinite families of MSTD sets";
Zhao, 2010a, "Constructing MSTD sets using bidirectional ballot sequences";
Zhao, 2010b, "Counting MSTD sets in finite abelian groups";
Zhao, 2011, "Sets characterized by missing sums and differences".

[20] E.g. Oxtoby, 1971, *Measure and category. A survey of the analogies between topological and measure spaces*;

References

Croft, H. T. (1967). "Research problems, Problem 7, Section VI". Mimeographed notes, University of Cambridge (cit. on p. 134).

Do, T., A. Kulkarni, S. J. Miller, D. Moon, and J. Wellens (2015). "Sums and differences of correlated random sets". *J. Number Theory* **147**, pp. 44–68 (cit. on p. 134).

Do, T., A. Kulkarni, S. J. Miller, D. Moon, J. Wellens, and J. Wilcox (2015). "Sets characterized by missing sums and differences in dilating polytopes". *J. Number Theory* **157**, pp. 123–153 (cit. on p. 134).

Freiman, G. A. and V. P. Pigarev (1973). "The relation between the invariants R and T". In: *Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (Russian)*. Moscow: Kalinin. Gos. Univ., pp. 172–174 (cit. on pp. 128, 134).

Hegarty, P. V. (2007). "Some explicit constructions of sets with more sums than differences". *Acta Arith.* **130**, pp. 61–77 (cit. on pp. 128, 130).

Hegarty, P. V. and S. J. Miller (2009). "When almost all sets are difference dominated". *Random Structures Algorithms* **35** (1), pp. 118–136 (cit. on pp. 122, 133).

Hennecart, F., G. Robert, and A. Yudin (1999). "On the number of sums and differences". *Astérisque* (258), pp. xiii, 173–178 (cit. on p. 134).

Iyer, G. et al. (2012). "Generalized more sums than differences sets". *J. Number Theory* **132** (5), pp. 1054–1073 (cit. on p. 134).

Iyer, G. et al. (2014). "Finding and counting MSTD sets". In: *Combinatorial and additive number theory—CANT 2011 and 2012*. Vol. 101. Springer Proc. Math. Stat. Springer, New York, pp. 79–98 (cit. on p. 134).

Marica, J. (1969). "On a conjecture of Conway". *Canad. Math. Bull.* **12**, pp. 233–234 (cit. on pp. 124, 128, 134).

Martin, G. and K. O'Bryant (2007). "Many sets have more sums than differences". In: *Additive Combinatorics*. Vol. 43. CRM Proc. Lecture Notes. Providence, RI: Amer. Math. Soc., pp. 287–305 (cit. on pp. 122, 133).

Miller, S. J., B. Orosz, and D. Scheinerman (2010). "Explicit constructions of infinite families of MSTD sets". *J. Number Theory* **130** (5), pp. 1221–1233 (cit. on pp. 128, 134).

Miller, S. J., L. Robinson, and S. Pegado (2012). "Explicit constructions of large families of generalized more sums than differences sets". *Integers* **12** (5), pp. 935–949 (cit. on p. 134).

Piccard, 1939, *Sur les ensembles de distances des ensembles de points d'un espace Euclidien*;
Piccard, 1940, "Sur les ensembles de distances";
Piccard, 1942, *Sur des ensembles parfaits*;
Steinhaus, 1920, "Sur les distances des points dans les ensembles de mesure positive".

Miller, S. J. and D. Scheinerman (2010). "Explicit constructions of infinite families of MSTD sets". In: *Additive number theory*. Springer, New York, pp. 229–248 (cit. on p. 134).
Nathanson, M. B. (1972). "Sums of finite sets of integers". *Amer. Math. Monthly* **79**, pp. 1010–1012 (cit. on p. 127).
Nathanson, M. B. (1996). *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. **165**. Graduate Texts in Mathematics. New York: Springer-Verlag, pp. xiv+293 (cit. on pp. 123, 127).
Nathanson, M. B. (2007a). *Problems in additive number theory. I, Additive Combinatorics*. **43**. CRM Proc. Lecture Notes. Amer. Math. Soc., Providence, RI, pp. 263–270 (cit. on pp. 128, 134).
Nathanson, M. B. (2007b). "Sets with more sums than differences". *Integers* **7** (A5) (cit. on p. 127).
Oxtoby, J. C. (1971). *Measure and category. A survey of the analogies between topological and measure spaces*. Springer-Verlag, New York-Berlin (cit. on p. 134).
Piccard, S. (1939). *Sur les ensembles de distances des ensembles de points d'un espace Euclidien*. **13**. Mém. Univ. Neuchâtel. Neuchâtel: Secrétariat de l'Université (cit. on p. 135).
Piccard, S. (1940). "Sur les ensembles de distances". *C. R. Acad. Sci. Paris* **210**, pp. 780–783 (cit. on p. 135).
Piccard, S. (1942). *Sur des ensembles parfaits*. **16**. Mém. Univ. Neuchâtel. Neuchâtel: Secrétariat de l'Université (cit. on p. 135).
Roesler, F. (2000). "A mean value density theorem of additive number theory". *Acta Arith.* **96** (2), pp. 121–138 (cit. on p. 134).
Ruzsa, I. Z. (1978). "On the cardinality of $A+A$ and $A-A$". In: *Combinatorics year (Keszthely, 1976)*. Vol. 18. Coll. Math. Soc. J. Bolyai. North-Holland–Bolyai Tàrsulat, pp. 933–938 (cit. on p. 134).
Ruzsa, I. Z. (1984). "Sets of sums and differences". In: *Séminaire de Théorie des Nombres de Paris 1982–1983*. Boston: Birkhäuser, pp. 267–273 (cit. on p. 134).
Ruzsa, I. Z. (1992). "On the number of sums and differences". *Acta Math. Sci. Hungar.* **59**, pp. 439–447 (cit. on p. 134).
Spohn, W. G. (1971). "On Conway's conjecture for integer sets". *Canad. Math. Bull.* **14**, pp. 461–462 (cit. on p. 134).
Steinhaus, H. (1920). "Sur les distances des points dans les ensembles de mesure positive". *Fund. Math.* **1**, pp. 93–104 (cit. on p. 135).
Zhao, Y. (2010a). "Constructing MSTD sets using bidirectional ballot sequences". *J. Number Theory* **130**, pp. 1212–1220 (cit. on p. 134).
Zhao, Y. (2010b). "Counting MSTD sets in finite abelian groups". *J. Number Theory* **130**, pp. 2308–2322 (cit. on p. 134).
Zhao, Y. (2011). "Sets characterized by missing sums and differences". *J. Number Theory* **131**, pp. 2107–2134 (cit. on p. 134).

Contents