MSTD SETS AND FREIMAN ISOMORPHISMS

MELVYN B. NATHANSON

To Grigori Freiman on his 90th birthday

Abstract: An MSTD set is a finite set with more pairwise sums than differences. (Υ, Φ) -ismorphisms are generalizations of Freiman isomorphisms to arbitrary linear forms. These generalized isomorphisms are used to prove that every finite set of real numbers is Freiman isomorphic to a finite set of integers. This implies that there exists no MSTD set A of real numbers with $|A| \leq 7$, and, up to Freiman isomorphism and affine isomorphism, there exists exactly one MSTD set A of real numbers with |A| = 8.

Keywords: MSTD set, Freiman isomorphism, (Υ, Φ) -ismorphism, sumset, difference set, linear forms, Dirichlet's theorem, product set, quotient set, MPTQ set.

1. Sums and differences

For every nonempty subset A of an additive abelian group, we define the *sumset*

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

and the difference set

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

The observation that

$$3+2=2+3$$

but

$$3 - 2 \neq 2 - 3$$

suggests the reasonable conjecture that a finite set of integers or real numbers should have more differences, or at least as many differences, as sums, but this conjecture is false. For example, the set

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

²⁰¹⁰ Mathematics Subject Classification: primary: 11B13; secondary: 11B75, 05B20, 05A19, 05A17, 11D04

has difference set

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

and sumset

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

Note the translated difference set

$$A - A + \{14\} = [0, 28] \setminus \{1, 8, 20, 27\}.$$

We have

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

Sets with more sums than differences are called MSTD sets.

As expected, MSTD sets of integers are rare (e.g. Hegarty and Miller [3], Martin and O'Bryant [5], Zhao [12, 13]). Isolated examples and infinite families of MSTD sets of integers have been constructed (e.g. Hegarty [4], Miller, Orosz, and Scheinerman [6], Miller and Scheinerman [7], and Nathanson [9, 10]), but there is no adequate classification.

If A is an MSTD set, then every affine image of A, that is, every set of the form

$$\lambda * A + \mu = \{\lambda a + \mu : a \in A\}$$

with $\lambda, \mu \in \mathbf{R}$ and $\lambda \neq 0$ is also an MSTD set. We call the sets A and $\lambda * A + \mu$ affinely isomorphic. Using a clever algorithm and extensive computation, Hegarty [4] proved that if A is an MSTD set of integers, then $|A| \geq 8$, and if A is an MSTD set with |A| = 8, then A is affinely isomorphic to the set $\{0, 2, 3, 4, 7, 11, 12, 14\}$.

MSTD sets of integers have been studied extensively, but little is known about MSTD sets of real numbers and how they differ from MSTD sets of integers. In this paper we show that, associated to every MSTD set of real numbers, there is a "Freiman isomorphic" MSTD set of integers, and that properties of MSTD sets of real numbers may be deduced from properties of their associated integer MSTD sets. In particular, we prove that if A is an MSTD set of real numbers, then $|A| \geq 8$. We shall define *Freiman isomorphism* and, more generally, (Υ, Φ) -isomorphism, and prove that if A is a real MSTD set with |A| = 8, then A is not only Freiman isomorphic but also affinely isomorphic to the set $\{0, 2, 3, 4, 7, 11, 12, 14\}$.

2. (Υ, Φ) -isomorphisms

We begin with a simple set theoretical observation. Let U be a set, and let Υ be a function defined on U with image $\Upsilon(U) = \{\Upsilon(u) : u \in U\}$. Let V be a set, and let Φ be a function defined on V with image $\Phi(V) = \{\Phi(v) : v \in V\}$. A function $f^*: U \to V$ is an (Υ, Φ) -homomorphism if, for all $u, u' \in U$, the equation

$$\Upsilon(u) = \Upsilon(u') \tag{2.1}$$

implies that

$$\Phi(f^*(u)) = \Phi(f^*(u')). \tag{2.2}$$

Equivalently, for each $x \in \Upsilon(U)$, there exists $y \in \Phi(V)$ such that

$$f^* (\Upsilon^{-1}(x)) \subseteq \Phi^{-1}(y).$$

This implies that there is a well-defined function $F: \Upsilon(U) \to \Phi(V)$ such that

$$F(x) = \Phi(f^*(u))$$

for all $x \in \Upsilon(U)$ and $u \in \Upsilon^{-1}(x)$. Thus, the following diagram commutes:

$$\begin{array}{c|c} U & \xrightarrow{\Upsilon} \Upsilon(U) \\ f^* \downarrow & & \downarrow^F \\ V & \xrightarrow{\Phi} \Phi(V) \end{array}$$

An (Υ, Φ) -homomorphism $f^*: U \to V$ is a (Υ, Φ) -isomorphism if there is a (Φ, Υ) -homomorphism $g^*: V \to U$ such that $g^*f^* = \mathrm{id}_U$ and $f^*g^* = \mathrm{id}_V$. We call g^* the (Υ, Φ) -inverse of f^* . As a (Φ, Υ) -homomorphism, the function g^* has the following property: If $v, v' \in V$ and

$$\Phi(v) = \Phi(v') \tag{2.3}$$

then

$$\Upsilon(g^*(v)) = \Upsilon(g^*(v')). \tag{2.4}$$

Let f^* be an (Υ, Φ) -isomorphism with inverse g^* . Let $G: \Phi(V) \to \Upsilon(U)$ be the function induced by g^* . Let $u, u' \in U$ satisfy (2.2). Writing $v = f^*(u)$ and $v' = f^*(u')$, we obtain (2.3), which implies (2.4). Because $u = g^*(v)$ and $u' = g^*(v')$, we obtain (2.1). Thus, if f^* is an (Υ, Φ) -isomorphism, then (2.1) and (2.2) are equivalent.

Lemma 1. Let U, V, and W be sets, and let Υ, Φ , and χ be functions on U, V, and W, respectively. If f^* is an (Υ, Φ) -homomorphism (resp. (Υ, Φ) -isomorphism) from U to V and if f_1^* is a (Φ, χ) -homomorphism (resp. (Φ, χ) -isomorphism) from V to W, then $f_1^*f^*$ is an (Υ, χ) -homomorphism (resp. (Υ, χ) -isomorphism) from U to W.

Proof. This follows immediately from the definitions.

Let |X| denote the cardinality of the set X. For every set U and function Υ on U, we define the representation function of $x \in \Upsilon(U)$ as follows:

$$r_{\Upsilon,U}(x) = \left|\left\{u \in U : \Upsilon(u) = x\right\}\right| = \left|\Upsilon^{-1}(x)\right|.$$

Theorem 1. Let U and V be sets, let Υ be a function on U, and let Φ be a function on V. If $f^*: U \to V$ is an (Υ, Φ) -isomorphism, then

(i) The induced function $F: \Upsilon(U) \to \Phi(V)$ is a bijection, and so

$$|\Upsilon(U)| = |\Phi(V)|.$$

(ii) For all $x \in \Upsilon(U)$,

$$r_{\Upsilon,U}(x) = r_{\Phi,V}(F(x)).$$

Proof. Let g^* be the (Υ, Φ) -inverse of f^* . If $x \in \Upsilon(U)$ and $u \in \Upsilon^{-1}(x)$, then

$$GF(x) = GF\Upsilon(u) = G\Phi f^*(u) = \Upsilon g^* f^*(u) = \Upsilon(u) = x.$$

Similarly, FG(y) = y for all $y \in \Phi(V)$, and so $G = F^{-1}$. Thus, F is a bijection and $|\Upsilon(U)| = |\Phi(V)|$.

For all $x \in \Upsilon(U)$, we have

$$u \in \Upsilon^{-1}(x)$$

if and only if

$$F\Upsilon(u) = F(x)$$

if and only if

$$\Phi f^*(u) = F(x)$$

if and only if

$$f^*(u) \in \Phi^{-1}(F(x)).$$

Because $f^*: U \to V$ is a bijection, we have $|\Upsilon^{-1}(x)| = |\Phi^{-1}(F(x))|$, or, equivalently, $r_{\Upsilon,U}(x) = r_{\Phi,V}(F(x))$. This completes the proof.

3. Linear forms

A linear form with coefficients in a ring R is a function of the form

$$\Upsilon(t_1,\ldots,t_h) = \sum_{j=1}^h v_j t_j$$

where $v_j \in R$ for j = 1, ..., h. The linear form is nonzero if $v_j \neq 0$ for some j. The study of sums and differences is the study of the special linear forms $t_1 + t_2$ and $t_1 - t_2$, but it is natural to consider more general linear forms. We begin with functions of h variables that are sums of functions of one variable.

Theorem 2. Let R be a ring, let M be an R-module, let A be a subset of M, and let A^h denote the set of all h-tuples of elements of A. Let S be a ring, let N be an S-module, let B be a subset of N, and let B^h denote the set of all h-tuples of elements of B. For every function $f: A \to B$, define $f^*: A^h \to B^h$ by

$$f^*(a_1,\ldots,a_h) = (f(a_1),\ldots,f(a_h)).$$

Let $\Upsilon_1(t_1), \ldots, \Upsilon_h(t_h)$ be functions defined on A, and let $\Phi_1(t_1), \ldots, \Phi_h(t_h)$ be functions defined on B. The functions

$$\Upsilon(t_1,\ldots,t_h) = \sum_{j=1}^h \Upsilon_j(t_j)$$

and

$$\Phi(t_1,\ldots,t_h) = \sum_{j=1}^h \Phi_j(t_j)$$

are defined on A^h and B^h , respectively.

For every subset J of $H = \{1, 2, ..., h\}$, let

$$\Upsilon_J(t_1,\ldots,t_h) = \sum_{j\in H\setminus J} \Upsilon_j(t_j) - \sum_{j\in J} \Upsilon_j(t_j)$$

and

$$\Phi_J(t_1,\ldots,t_h) = \sum_{j \in H \setminus J} \Phi_j(t_j) - \sum_{j \in J} \Phi_j(t_j).$$

The functions Υ_J and Φ_J are functions on A^h and B^h , respectively. If $f^*: A^h \to B^h$ is an (Υ, Φ) -isomorphism, then, for every subset $J \subseteq H$, the function $f^*: A^h \to B^h$ is also an (Υ_J, Φ_j) -isomorphism, and

$$|\Upsilon_J(A^h)| = |\Phi_J(B^h)|.$$

Proof. If $(a_1, \ldots, a_h) \in A^h$ and $(a'_1, \ldots, a'_h) \in A^h$ and if

$$\Upsilon_J(a_1,\ldots,a_h) = \Upsilon_J(a_1',\ldots,a_h')$$

then

$$\sum_{j \in H \backslash J} \Upsilon_j(a_j) - \sum_{j \in J} \Upsilon_j(a_j) = \sum_{j \in H \backslash J} \Upsilon_j(a_j') - \sum_{j \in J} \Upsilon_j(a_j')$$

and so

$$\sum_{j \in H \backslash J} \Upsilon_j(a_j) + \sum_{j \in J} \Upsilon_j(a_j') = \sum_{j \in H \backslash J} \Upsilon_j(a_j') + \sum_{j \in J} \Upsilon_j(a_j).$$

Let

$$u_j = \begin{cases} a_j & \text{if } j \in H \setminus J \\ a'_i & \text{if } j \in J \end{cases}$$

and

$$u'_{j} = \begin{cases} a'_{j} & \text{if } j \in H \setminus J \\ a_{j} & \text{if } j \in J. \end{cases}$$

We have $(u_1, ..., u_h), (u'_1, ..., u'_h) \in A^h$, and

$$\Upsilon(u_1,\ldots,u_h)=\Upsilon(u_1',\ldots,u_h').$$

Because f^* is an (Υ, Φ) -homomorphism, it follows that

$$\Phi(f^*(u_1, \dots, u_h)) = \Phi(f^*(u'_1, \dots, u'_h)).$$

Expanding the left and right sides of this equation, we obtain

$$\Phi(f^*(u_1, \dots, u_h)) = \Phi(f(u_1), \dots, f(u_h))
= \sum_{j \in H \setminus J} \Phi_j(f(u_j)) + \sum_{j \in J} \Phi_j(f(u_j))
= \sum_{j \in H \setminus J} \Phi_j(f(a_j)) + \sum_{j \in J} \Phi_j(f(a'_j))$$

and

$$\begin{split} \Phi(f^*(u_1', \dots, u_h')) &= \Phi(f(u_1'), \dots, f(u_h')) \\ &= \sum_{j \in H \setminus J} \Phi_j(f(u_j')) + \sum_{j \in J} \Phi_j(f(u_j')) \\ &= \sum_{j \in H \setminus J} \Phi_j(f(a_j')) + \sum_{j \in J} \Phi_j(f(a_j)). \end{split}$$

Therefore,

$$\Phi_J(f^*(a_1, \dots, a_h)) = \sum_{j \in H \setminus J} \Phi_j(f(a_j)) - \sum_{j \in J} \Phi_j(f(a_j))$$
$$= \sum_{j \in H \setminus J} \Phi_j(f(a_j')) - \sum_{j \in J} \Phi_j(f(a_j'))$$
$$= \Phi_J(f^*(a_1', \dots, a_h')).$$

Similarly, because $(f^*)^{-1}$ is a (Φ, Υ) -homomorphism,

$$\Phi_J(f^*(a_1,\ldots,a_h)) = \Phi_J(f^*(a_1',\ldots,a_h'))$$

implies that

$$\Upsilon_J(a_1,\ldots,a_h) = \Upsilon_J(a_1',\ldots,a_h')$$

and so f^* is also an (Υ_J, Φ_J) -isomorphism for all $J \subseteq H$. Applying Theorem 1 completes the proof.

4. Linear forms with rational coefficients

In this section we consider the special case $\Upsilon = \Phi$, and write, simply, Φ -homomorphism instead of (Φ, Φ) -homomorphism, and Φ -isomorphism instead of (Φ, Φ) -isomorphism.

Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be finite sets of real numbers with $|A| = |B| = k \ge 2$, and let $f: A \to B$ be a bijection such that $f(a_i) = b_i$ for all $i = 1, \ldots, k$. Let $\Phi(t_1, \ldots, t_h)$ be a nonzero linear form with rational coefficients. The function f will be called a Φ -isomorphism if the function $f^*: A^h \to B^h$ is a Φ -isomorphism. This means that, for all h-tuples $(a_{i_1}, \ldots, a_{i_h}), (a_{i_{h+1}}, \ldots, a_{i_{2h}}) \in A^h$, we have

$$\Phi(a_{i_1}, \dots, a_{i_h}) = \Phi(a_{i_{h+1}}, \dots, a_{i_{2h}})$$

if and only if

$$\Phi(b_{i_1},\ldots,b_{i_h}) = \Phi(b_{i_{h+1}},\ldots,b_{i_{2h}}).$$

The sets A and B are Φ -isomorphic if there exists a Φ -isomorphism $f: A \to B$. The following result generalizes Corollary 8.1 of Nathanson [8].

Theorem 3. Let

$$\Phi(t_1,\ldots,t_h) = \sum_{j=1}^h \varphi_j t_j$$

be a nonzero linear form with rational coefficients. Every finite subset of \mathbf{Z}^d is Φ -isomorphic to a set of positive integers.

Proof. Let m be a common multiple of the denominators of the rational numbers $\varphi_1, \ldots, \varphi_h$. The linear form

$$\hat{\Phi}(t_1,\ldots,t_h) = m\Phi(t_1,\ldots,t_h) = \sum_{j=1}^h m\varphi_j t_j$$

has integer coefficients. For all h-tuples of lattice points or real numbers, we have $\hat{\Phi}(a_1,\ldots,a_h)=\hat{\Phi}(a_{h+1},\ldots,a_{2h})$ if and only if $\Phi(a_1,\ldots,a_h)=\Phi(a_{h+1},\ldots,a_{2h})$. Thus, we can assume that the coefficients $\varphi_1,\ldots,\varphi_h$ are integers.

For i = 1, ..., d, let $\pi_i : \mathbf{R}^d \to \mathbf{R}$ be the projection of a vector onto its *i*th coordinate. Let A be a nonempty finite subset of \mathbf{Z}^d , and let

$$a^* = \max(\{|\pi_i(a)| : a \in A \text{ and } i = 1, \dots, d)\}.$$

Let

$$\varphi^* = \max\left(\{|\varphi_j| : j = 1, \dots, h\}\right)$$

and let λ be a real number such that

$$\lambda > 2a^* \varphi^* h + 1 \tag{4.1}$$

We shall prove that the linear form $f_{\lambda}: \mathbf{R}^d \to \mathbf{R}$ defined by

$$f_{\lambda}(x_1,\ldots,x_d) = \sum_{i=1}^d x_i \lambda^{i-1}$$

is a Φ -isomorphism from A into \mathbf{R} . If λ is an integer, then f is a Φ -isomorphism from A into \mathbf{Z} .

Let (a_1, \ldots, a_h) and $(a_{h+1}, \ldots, a_{2h})$ be h-tuples of lattice points in A. The identity

$$\Phi(a_1, \dots, a_h) - \Phi(a_{h+1}, \dots, a_{2h}) = \sum_{j=1}^h \varphi_j(a_j - a_{h+j})$$

$$= \left(\sum_{j=1}^h \varphi_j \pi_1(a_j - a_{h+j}), \dots, \sum_{j=1}^h \varphi_j \pi_d(a_j - a_{h+j})\right) \in \mathbf{Z}^d$$

implies that

$$\Phi(a_1,\ldots,a_h) = \Phi(a_{h+1},\ldots,a_{2h})$$

if and only if

$$\sum_{j=1}^{h} \varphi_j \pi_i (a_j - a_{h+j}) = 0 \quad \text{for all } i = 1, \dots, d.$$
 (4.2)

We have

$$f_{\lambda}\left(\Phi(a_1,\ldots,a_h)\right) = f_{\lambda}\left(\Phi(a_{h+1},\ldots,a_{2h})\right)$$

if and only if

$$f_{\lambda} \left(\Phi(a_1, \dots, a_h) - \Phi(a_{h+1}, \dots, a_{2h}) \right) = 0$$

if and only if

$$f_{\lambda}\left(\sum_{j=1}^{h}\varphi_{j}\pi_{1}(a_{j}-a_{h+j}),\ldots,\sum_{j=1}^{h}\varphi_{j}\pi_{d}(a_{j}-a_{h+j})\right)=0$$

if and only if

$$\sum_{i=1}^{d} \left(\sum_{j=1}^{h} \varphi_j \pi_i (a_j - a_{h+j}) \right) \lambda^{i-1} = 0.$$
 (4.3)

Suppose that

$$\sum_{i=1}^{h} \varphi_j \pi_i (a_j - a_{h+j}) \neq 0$$

for some $i \in \{1, ..., d\}$. Let r be the greatest integer such that $\sum_{j=1}^{h} \varphi_j \pi_r(a_j - a_{h+j}) \neq 0$, or, equivalently, such that

$$\left| \sum_{j=1}^{h} \varphi_j \pi_r(a_j - a_{h+j}) \right| \ge 1. \tag{4.4}$$

Rewriting (4.3), we obtain

$$-\sum_{j=1}^{h} \varphi_j \pi_r(a_j - a_{h+j}) \lambda^{r-1} = \sum_{i=1}^{r-1} \left(\sum_{j=1}^{h} \varphi_j \pi_i(a_j - a_{h+j}) \right) \lambda^{i-1}.$$

Applying inequality (4.4), the triangle inequality, and inequality (4.1), we obtain

$$\lambda^{r-1} \leq \left| \sum_{j=1}^{h} \varphi_j \pi_r(a_j - a_{h+j}) \lambda^{r-1} \right|$$

$$= \left| \sum_{i=1}^{r-1} \left(\sum_{j=1}^{h} \varphi_j \pi_i(a_j - a_{h+j}) \right) \lambda^{i-1} \right|$$

$$\leq \sum_{i=1}^{r-1} \sum_{j=1}^{h} \varphi_j(|\pi_i(a_j)| + |\pi_i(a_{h+j})|) \lambda^{i-1}$$

$$\leq \sum_{i=1}^{r-1} 2a^* \varphi^* h \lambda^{i-1}$$

$$< 2a^* \varphi^* h \frac{\lambda^{r-1}}{\lambda - 1}$$

$$< \lambda^{r-1}$$

which is absurd. Therefore,

$$f_{\lambda}\left(\Phi(a_1,\ldots,a_h)\right) = f_{\lambda}\left(\Phi(a_{h+1},\ldots,a_{2h})\right)$$

if and only if condition (4.2) is satisfied. that is, if and only if

$$\Phi(a_1,\ldots,a_h) = \Phi(a_{h+1},\ldots,a_{2h}).$$

Thus, f_{λ} is a Φ -isomorphism from A to a set of real numbers, which, by translation, is Φ -isomorphic to a set of positive real numbers. Choosing a positive integer λ completes the proof.

We shall give three different proofs of the following fundamental theorem. The first uses linear programming, the second uses diophantine approximation, and the third reduces the proof to Theorem 3.

Theorem 4. Let

$$\Phi(t_1,\ldots,t_h) = \sum_{j=1}^h \varphi_j t_j$$

be a nonzero linear form with rational coefficients. Every nonempty finite set A of real numbers is Φ -isomorphic to a set of positive integers.

Proof. There is nothing to prove if |A| = 1, so we can assume that $A = \{a_1, \ldots, a_k\}$ is a finite set of real numbers with $|A| = k \ge 2$.

The first proof uses a linear programming argument of Alon and Kleitman [1, Prop. 4.1']. To every pair of h-tuples $(a_{i_1}, \ldots, a_{i_h}), (a_{i_{h+1}}, \ldots, a_{i_{2h}}) \in A^h$, we construct a linear equation or linear inequality in 2k variables $t_1, \ldots, t_k, t_{k+1}, \ldots, t_{2k}$ as follows: If

$$\Phi(a_{i_1}, \dots, a_{i_h}) = \Phi(a_{i_{h+1}}, \dots, a_{i_{2h}})$$

then we have the equation

$$\Phi(t_{i_1},\ldots,t_{i_h}) - \Phi(t_{i_{h+1}},\ldots,t_{i_{2h}}) = 0.$$

If

$$\Phi(a_{i_1},\ldots,a_{i_b}) < \Phi(a_{i_{b+1}},\ldots,a_{i_{2b}})$$

then we have the inequality

$$\Phi(t_{i_1},\ldots,t_{i_h}) - \Phi(t_{i_{h+1}},\ldots,t_{i_{2h}}) < 0.$$

If

$$\Phi(a_{i_1},\ldots,a_{i_h}) > \Phi(a_{i_{h+1}},\ldots,a_{i_{2h}})$$

then we have the inequality

$$\Phi(t_{i_1},\ldots,t_{i_h}) - \Phi(t_{i_{h+1}},\ldots,t_{i_{2h}}) > 0.$$

This procedure gives a system of k^{2h} equations and inequalities with rational coefficients for which the set $A = \{a_1, \ldots, a_k\}$ is a solution in real numbers. It follows that the system also has a solution $\hat{B} = \{\hat{b}_1, \ldots, \hat{b}_k\}$ in rational numbers.

Multiplying an equation or an inequality by a positive number preserves the equation or inequality. If m is a positive common multiple of the denominators of the rational numbers in the set \hat{B} , then $B=m*\hat{B}=\{m\hat{b}_1,\ldots,m\hat{b}_k\}$ is a finite set of integers that also solves the system of equations and inequalities. Thus, the set B has the property that, for all h-tuples $(a_{i_1},\ldots,a_{i_h}),(a_{i_{h+1}},\ldots,a_{i_{2h}})\in A^h$, we have

$$\Phi(a_{i_1}, \dots, a_{i_h}) = \Phi(a_{i_{h+1}}, \dots, a_{i_{2h}})$$

if and only if

$$\Phi(b_{i_1}, \dots, b_{i_h}) = \Phi(b_{i_{h+1}}, \dots, b_{i_{2h}})$$

and so the real set A and the integer set B are Φ -isomorphic. Because translation of a set is a Φ -isomorphism, we obtain a solution set of positive integers. This completes the first proof of Theorem 4.

The second proof uses diophantine approximation. We can assume that the linear form Φ is nonzero with integer coefficients, and so

$$\varphi^* = \max(|\varphi_j| : j = 1, \dots, h) \ge 1.$$

The image under Φ of a finite set A of real numbers is the set

$$\Phi(A) = \left\{ \Phi(a_{i_1}, \dots, a_{i_h}) : (a_{i_1}, \dots, a_{i_h}) \in A^h \right\}$$
$$= \left\{ \sum_{j=1}^h \varphi_j a_{i_j} : a_{i_j} \in A \text{ for } j = 1, \dots, h \right\}.$$

We have $|\Phi(A)| \geq 2$ because $|A| \geq 2$ and Φ is nonzero. It follows that

$$\delta^* = \min(|x - x'| : x, x' \in \Phi(A) \text{ and } x \neq x') > 0.$$

Let

$$0<\varepsilon<\frac{\min(\delta^*,1)}{2h\varphi^*}.$$

By Dirichlet's theorem (Hardy-Wright [2, Theorem 201]), for every $\varepsilon > 0$, there is a positive integer q and a set

$$B = \{b_1, \dots, b_k\}$$

of integers such that

$$|qa_i - b_i| < \varepsilon$$

for all i = 1, ..., k. We define

$$\theta_i = qa_i - b_i$$

for i = 1, ..., k. For every h-tuple $(a_{i_1}, ..., a_{i_h}) \in A^h$, we have

$$|\Phi(\theta_{i_1}, \dots, \theta_{i_h})| \le \sum_{j=1}^h |\varphi_j| |\theta_{i_j}| \le h\varphi^* \varepsilon < \frac{\min(\delta^*, 1)}{2}.$$

$$(4.5)$$

Define the functions $f:A\to B$ and $f^*:A^h\to B^h$ by

$$f(a_i) = b_i$$
 and $f^*(a_{i_1}, \dots, a_{i_h}) = (b_{i_1}, \dots, b_{i_h}).$

Let $(a_{i_1}, \ldots, a_{i_h}), (a_{i_{h+1}}, \ldots, a_{i_{2h}})$ be h-tuples in A^h . Using the linearity of Φ , we have

$$\Phi(a_{i_1}, \dots, a_{i_h}) = \Phi(a_{i_{h+1}}, \dots, a_{i_{2h}})$$

if and only if

$$\begin{split} \Phi(b_{i_1},\dots,b_{i_h}) + \Phi(\theta_{i_1},\dots,\theta_{i_h}) &= \Phi(b_{i_1}+\theta_{i_1},\dots,b_{i_h}+\theta_{i_h}) \\ &= \Phi(qa_{i_1},\dots,qa_{i_h}) \\ &= q\Phi(a_{i_1},\dots,a_{i_h}) \\ &= q\Phi(a_{i_{h+1}},\dots,a_{i_{2h}}) \\ &= \Phi(qa_{i_{h+1}},\dots,qa_{i_{2h}}) \\ &= \Phi(b_{i_{h+1}}+\theta_{i_{h+1}},\dots,b_{i_{2h}}+\theta_{i_{2h}}) \\ &= \Phi(b_{i_{h+1}},\dots,b_{i_{2h}}) + \Phi(\theta_{i_{h+1}},\dots,\theta_{i_{2h}}) \end{split}$$

if and only if

$$\Phi(b_{i_1},\ldots,b_{i_h}) - \Phi(b_{i_{h+1}},\ldots,b_{i_{2h}}) = \Phi(\theta_{i_{h+1}},\ldots,\theta_{i_{2h}}) - \Phi(\theta_{i_1},\ldots,\theta_{i_h}).$$

Recall inequality (4.5). Because $\Phi(b_{i_1},\ldots,b_{i_h})$ and $\Phi(b_{i_{h+1}},\ldots,b_{i_{2h}})$ are integers, if $\Phi(b_{i_1},\ldots,b_{i_h}) \neq \Phi(b_{i_{h+1}},\ldots,b_{i_{2h}})$, then

$$1 \leq |\Phi(b_{i_1}, \dots, b_{i_h}) - \Phi(b_{i_{h+1}}, \dots, b_{i_{2h}})|$$

$$\leq |\Phi(\theta_{i_{h+1}}, \dots, \theta_{i_{2h}})| + |\Phi(\theta_{i_1}, \dots, \theta_{i_h})|$$

$$\leq 1$$

which is absurd. Therefore, $\Phi(a_{i_1},\ldots,a_{i_h})=\Phi(a_{i_{h+1}},\ldots,a_{i_{2h}})$ implies $\Phi(b_{i_1},\ldots,b_{i_h})=\Phi(b_{i_{h+1}},\ldots,b_{i_{2h}})$, and the function $f:A\to B$ is a Φ -homomorphism.

Conversely,

$$\Phi(b_{i_1},\ldots,b_{i_h}) = \Phi(b_{i_{h+1}},\ldots,b_{i_{2h}})$$

if and only if

$$\Phi(qa_{i_1} - \theta_{i_1}, \dots, qa_{i_h} - \theta_{i_h}) = \Phi(qa_{i_{h+1}} - \theta_{i_{h+1}}, \dots, qa_{i_{2h}} - \theta_{i_{2h}})$$

if and only if

$$q(\Phi(a_{i_1},\ldots,a_{i_h}) - \Phi(a_{i_{h+1}},\ldots,a_{i_{2h}})) = \Phi(\theta_{i_1},\ldots,\theta_{i_h}) - \Phi(\theta_{i_{h+1}},\ldots,\theta_{i_{2h}}).$$

Because q is a positive integer, if $\Phi(a_{i_1},\ldots,a_{i_k}) \neq \Phi(a_{i_{k+1}},\ldots,a_{i_{2k}})$, then

$$\delta^* \leq |\Phi(a_{i_1}, \dots, a_{i_h}) - \Phi(a_{i_{h+1}}, \dots, a_{i_{2h}})|$$

$$\leq q |\Phi(a_{i_1}, \dots, a_{i_h}) - \Phi(a_{i_{h+1}}, \dots, a_{i_{2h}})|$$

$$\leq |\Phi(\theta_{i_1}, \dots, \theta_{i_h})| + |\Phi(\theta_{i_{h+1}}, \dots, \theta_{i_{2h}})|$$

$$< \min(\delta^*, 1) \leq \delta^*$$

which is absurd. Therefore, $\Phi(b_{i_1},\ldots,b_{i_h})=\Phi(b_{i_{h+1}},\ldots,b_{i_{2h}})$ implies $\Phi(a_{i_1},\ldots,a_{i_h})=\Phi(a_{i_{h+1}},\ldots,a_{i_{2h}})$, and the function f is a Φ -isomorphism.

By translation of B, we obtain a set of positive integers that is Φ -isomorphic to A. This completes the second proof.

The third proof is the simplest. Let A be a nonempty finite set of real numbers that is not a set of integers. The additive group G generated by A is a torsion-free finitely generated abelian group, and so G is a free abelian group of rank d for some positive integer d. Let $f: G \to \mathbf{Z}^d$ be a group isomorphism. The restriction of the function f to A is a Φ -isomorphism from A to a finite set of lattice points in \mathbf{Z}^d . By Theorem 3, this set of lattice points is Φ -isomorphic to a finite set of positive integers. This completes the proof.

5. MSTD sets of real numbers and of integers

In the special case h=2 and the linear form

$$\Phi(t_1, t_2) = t_1 + t_2$$

a Φ -isomorphism is called a *Freiman isomorphism*. The construction of Theorem 2 applied to the form $\Phi(t_1, t_2) = t_1 + t_2$, with $J = \{2\} \subseteq H = \{1, 2\}$, gives the linear form

$$\Phi_J(t_1, t_2) = t_1 - t_2.$$

For every subset A of an additive abelian group, we have the sumset $A + A = \Phi(A)$ and the difference set $A - A = \Phi_J(A)$.

Theorem 5. Every finite set A of real numbers is Freiman isomorphic to a set B of positive integers. If A is an MSTD set of real numbers, then B is an MSTD set of positive integers.

Proof. Applying Theorem 4 to the linear form $\Phi(t_1, t_2) = t_1 + t_2$, we see that, for every finite set $A = \{a_1, \ldots, a_k\}$ of real numbers with |A| = k, there is a set $B = \{b_1, \ldots, b_k\}$ of positive integers and a function $f: A \to B$ with $f(a_i) = b_i$ for $i = 1, \ldots, k$, such that, for all $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4} \in A$,

$$a_{i_1} + a_{i_2} = a_{i_3} + a_{i_4}$$

if and only if

$$b_{i_1} + b_{i_2} = b_{i_3} + b_{i_4}.$$

Thus, A and B are Freiman isomorphic.

Using Theorem 2 with $H = \{1, 2\}$ and $J = \{2\}$, we have

$$a_{i_1} - a_{i_2} = a_{i_3} - a_{i_4}$$

if and only if

$$b_{i_1} - b_{i_2} = b_{i_3} - b_{i_4}.$$

It follows that

$$|A + A| = |B + B|$$

and

$$|A - A| = |B - B|$$

and so B is an MSTD set of integers if A is an MSTD set of real numbers.

Theorem 6. If A is an MSTD set of real numbers, then $|A| \ge 8$. If A is an MSTD set of real numbers and |A| = 8, then A is Freiman isomorphic to the set $\{0, 2, 3, 4, 7, 11, 12, 14\}$.

Proof. This follows immediately from Hegarty's theorem that, if B is an MSTD set of integers, then $|A| \geq 8$, and if B is an MSTD set of integers and |A| = 8, then B is affinely isomorphic to the set $\{0, 2, 3, 4, 7, 11, 12, 14\}$.

An additive abelian group G is 2-divisible if for every $a \in G$ there exists $x \in G$ such that 2x = a. We write x = a/2. For example, the group $\mathbb{Z}/3\mathbb{Z}$ is 2-divisible.

Theorem 7. Let $A^* = \{0, 2, 3, 4, 7, 11, 12, 14\}$, and let B be a subset of a 2-divisible group such that B is Freiman isomorphic to A. If $f: A^* \to B$ is a Freiman isomorphism, then f is the affine map

$$f(x) = x\left(\frac{f(2) - f(0)}{2}\right) + f(0)$$
(5.1)

for all $x \in A^*$.

Proof. Because f is a Freiman isomorphism,

$$4+0=2+2$$

implies that

$$f(4) + f(0) = f(2) + f(2)$$

and so

$$f(4) = 2f(2) - f(0) = \frac{4f(2) - 2f(0)}{2}.$$

Similarly, 3 + 3 = 2 + 4 implies that

$$f(3) = \frac{f(2) + f(4)}{2} = \frac{3f(2) - f(0)}{2}.$$

The equation 7 + 0 = 4 + 3 implies that

$$f(7) = \frac{7f(2) - 5f(0)}{2}.$$

The equation 11 + 0 = 7 + 4 implies that

$$f(11) = \frac{11f(2) - 9f(0)}{2}.$$

The equation 14 + 0 = 7 + 7 implies that

$$f(14) = \frac{14f(2) - 12f(0)}{2}.$$

The equation 12 + 2 = 14 + 0 implies that

$$f(12) = \frac{12f(2) - 10f(0)}{2}.$$

We see that

$$f(x) = \frac{xf(2) - (x - 2)f(0)}{2} = x\left(\frac{f(2) - f(0)}{2}\right) + f(0)$$

for all $x \in A^*$. This completes the proof.

The following result is due to Moshe Newman [11].

Theorem 8 (Newman). Every MSTD set A of real numbers with |A| = 8 is affinely isomorphic to the set $A^* = \{0, 2, 3, 4, 7, 11, 12, 14\}$.

Proof. By Theorem 6, the set A of real numbers is Freiman isomorphic to A^* . Let $A = \{a_1, a_2, \ldots, a_8\}$, where $a_1 < a_2 < \cdots < a_8$. Define the affine map $g : \mathbf{R} \to \mathbf{R}$ by

$$g(x) = \frac{2(x - a_1)}{a_2 - a_1}.$$

Let $b_i = g(a_i)$ for i = 1, ..., 8, and let $B = g(A) = \{b_1, ..., b_8\}$. Note that $b_1 = f(a_1) = 0$ and $b_2 = f(a_2) = 2$, and that $b_1 < b_2 < \cdots < b_8$. The set B of real numbers is affinely isomorphic to A and Freiman isomorphic to A^* . Let

$$f:A^* \to B$$

be a Freiman isomorphism. By Theorem 7, the function f is an affine map of the form (5.1). If f(2) > f(0), then f is strictly increasing, and so f(0) = 0 and f(2) = 2. This implies that f(x) = x for all $x \in A^*$, and so $A^* = B$ is affinely isomorphic to A.

If f(2) < f(0), then f is strictly decreasing, and f(0) = 14 and f(2) = 12. This implies that f(x) = 14 - x for $x \in A^*$, and so $B = 14 - A^* = \{0, 2, 3, 7, 10, 11, 12, 14\}$, which is also affinely isomorphic to A^* . This completes the proof.

6. More products than quotients

Let B be a set of positive real numbers. We define the *product set*

$$B \cdot B = \{b \cdot b' : b, b' \in B\}$$

and the quotient set

$$B/B = \{b/b' : b, b' \in B\}.$$

The observation that

$$3 \cdot 2 = 2 \cdot 3$$

but

$$\frac{3}{2} \neq \frac{2}{3}$$

suggests that a finite set of positive real numbers should have more quotients, or at least as many quotients, as products, but it easy to show that there do exist sets with more products than quotients. Such sets are called MPTQ sets.

Here is a simple construction of MPTQ sets. Let A be a set of real numbers. For every positive real number c, let

$$c^A = \{c^a : a \in A\}.$$

The function $a \mapsto c^a$ is a Freiman isomorphism from the additive set A to the multiplicative set c^A . The set A is an MSTD set of real numbers if and only if $c^A = \{c^a : a \in A\}$ is an MPTQ set of positive real numbers. Moreover, if A is an MSTD set of positive integers and if c > 1 is an integer, then c^A is an MPTQ set of positive integers.

Conversely, let B be a set of positive real numbers. For every positive real number c, let

$$\log_c B = \{\log_c b : b \in B\}.$$

The function $b \mapsto \log_c b$ is a Freiman isomorphism from the multiplicative set B to the additive set $\log_c B$. The set B is an MPTQ set of positive real numbers if and only if $\log_c B$ is an MSTD set of real numbers.

7. Problems

Hegarty gave a computational proof of the theorem that an MSTD set of integers must contain at least 8 elements. A large number of cases must be checked, and a computer checks them. This calculation does not explain why the result is true.

Problem 1. Is there a proof of Hegarty's theorem that explains why an MSTD set of integers cannot have 7 elements?

A subset A of an abelian group G is symmetric if there exists an element $s \in G$ such that $A = \{s - a : a \in A\}$. For example, every finite arithmetic progression is symmetric.

Lemma 2. Let

$$\Phi(t_1,\ldots,t_h) = \sum_{j=1}^h \varphi_j t_j$$

be a nonzero linear form with integer coefficients, and, for $J \subseteq H = \{1, 2, ..., h\}$, let

$$\Phi_J(t_1,\ldots,t_h) = \sum_{j\in H\setminus J} \varphi_j t_j - \sum_{j\in J} \varphi_j t_j.$$

If A is a symmetric finite subset of an abelian group G, then

$$|\Phi(A)| = |\Phi_J(A)|.$$

Proof. Because A is symmetric, there is an element $s \in G$ such that, for every $a \in A$ there is a unique $a' \in A$ with a = s - a'. Let

$$s^* = \sum_{j \in J} \varphi_j s$$

If $x \in \Phi(A)$, then there exists $(a_1, \ldots, a_h) \in A^h$ such that

$$x = \Phi(a_1, \dots, a_h)$$

$$= \sum_{j \in H \setminus J} \varphi_j a_j + \sum_{j \in J} \varphi_j a_j$$

$$= \sum_{j \in H \setminus J} \varphi_j a_j + \sum_{j \in J} \varphi_j (s - a'_j)$$

$$= \sum_{j \in J} \varphi_j s + \sum_{j \in H \setminus J} \varphi_j a_j - \sum_{j \in J} \varphi_j a'_j$$

$$\in s^* + \Phi_J(A)$$

and so $\Phi(A) \subseteq \{s^*\} + \Phi_J(A)$ and $|\Phi(A)| \le |\Phi_J(A)|$. Similarly, $\Phi_J(A) \subseteq \{-s^*\} + \Phi(A)$ and $|\Phi_J(A)| \le |\Phi(A)|$. This completes the proof.

Here is a simple problem chosen from a large class of related problems about linear forms and finite sets of integers. Consider the linear forms

$$\Phi(t_1, t_2, t_3) = t_1 + t_2 + t_3$$

and

$$\Phi_3(t_1, t_2, t_3) = t_1 + t_2 - t_3$$

For every set A of integers, we have

$$\Phi(A) = A + A + A$$
 and $\Phi_3(A) = A + A - A$.

By Lemma 2, if A is a finite symmetric set of integers, then $|\Phi(A)| = |\Phi_3(A)|$. For example, if A is an arithmetic progression of length k, then $|\Phi(A)| = |\Phi_3(A)| = 3k - 2$. If $A = \{0, 2, 3, 4, 7, 11, 12, 14\}$, then

$$\Phi(A) = \Phi_3(A) + \{14\} = [0, 42] \setminus \{1, 41\}$$

and

$$|\Phi(A)| = |\Phi_3(A)| = 41.$$

The symmetry of the form Φ and the asymmetry of the form Φ_3 suggest that $|\Phi(A)| \leq |\Phi_3(A)|$ for most finite sets of integers.

Problem 2. Describe the finite sets A of integers such that $|\Phi(A)| > |\Phi_3(A)|$.

Problem 3. Can we go beyond linear forms? Consider quadratic, cubic, and other higher degree forms, or general polynomials in h variables, such as the polynomials $t_1 + t_2^2$ and $t_1^2 + t_2^2$. Here is a sample problem. To every h-tuple $I = (i_1, \ldots, i_h)$ of nonnegative integers, we associate the monomial $t^I = t_1^{i_1} \cdots t_h^{i_h}$. Let \mathcal{I} be a finite set of h-tuples, and let

$$P(t_1,\ldots,t_h) = \sum_{I\in\mathcal{I}} \varphi_I t^I$$

be a polynomial with nonzero integer coefficients. Let $\varepsilon_I \in \{\pm 1\}$ for $I \in \mathcal{I}$, and let $\varepsilon = (\varepsilon_I)_{I \in \mathcal{I}}$. Define

$$P_{\varepsilon}(t_1,\ldots,t_h) = \sum_{I\in\mathcal{I}} \varepsilon_I \varphi_I t^I.$$

Compare the cardinalities of the sets $P_{\varepsilon}(A)$ for finite sets A of integers.

Problem 4. How can one model the behavior of polynomial images of finite sets of real numbers by finite sets of integers?

8. Acknowledgements

This paper originated in a conference in honor of Grigori Freiman at Tel Aviv University in July, 2016. I stated in my lecture that I did not know who had discovered the first example of an MSTD set, but that it might have been a set of real numbers. Noga Alon remarked that, by the method in his paper [1] with Kleitman, one can always construct an MSTD set of integers from an MSTD set of real numbers. This gave the first proof of Theorem 4. Kevin O'Bryant suggested the use of Dirichlet's theorem in the diophantine approximation proof of Theorem 4. I described both proofs in a lecture at the Integers Conference in October, 2016, and Paul Pollack observed that the structure theorem for finitely generated torsion-free abelian groups gives the third proof.

Theorems 7 and 8 are essentially due to Moshe Newman [11].

References

- [1] N. Alon and D. J. Kleitman, *Sum-free subsets*, A Tribute to Paul Erdős, Cambridge University Press, Cambridge, 1990, pp. 13–26.
- [2] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, 6th ed., Oxford University Press, Oxford, 2008.
- [3] P. Hegarty and S.J. Miller, When almost all sets are difference dominated, Random Structures Algorithms **35** (2009), no. 1, 118–136.
- [4] P.V. Hegarty, Some explicit constructions of sets with more sums than differences, Acta Arith. 130 (2007), 61–77.
- [5] G. Martin and K. O'Bryant, Many sets have more sums than differences, Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 287–305.
- [6] S.J. Miller, B. Orosz, and D. Scheinerman, Explicit constructions of infinite families of MSTD sets, J. Number Theory 130 (2010), no. 5, 1221–1233.
- [7] S.J. Miller and D. Scheinerman, Explicit constructions of infinite families of MSTD sets, Additive number theory, Springer, New York, 2010, pp. 229–248.
- [8] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer-Verlag, New York, 1996.
- [9] M.B. Nathanson, Problems in additive number theory. I, Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 263–270.
- [10] M.B. Nathanson, Sets with more sums than differences, Integers 7 (2007), A5, 24.
- [11] M. Newman, personal communication, 2016
- [12] Y. Zhao, Constructing MSTD sets using bidirectional ballot sequences, J. Number Theory 130 (2010), 1212–1220.
- [13] Y. Zhao, Sets characterized by missing sums and differences, J. Number Theory 131 (2011), 2107–2134.

 $\textbf{E-mail:} \ \ melvyn.nathanson@lehman.cuny.edu$

Received: 9 September 2016; revised: 25 July 2017