Illinois Journal of Mathematics
Volume 49, Number 1, Spring 2005, Pages 33–43
S 0019-2082

ON ARITHMETIC COMBINATORICS AND FINITE GROUPS

NETS HAWK KATZ

Abstract. We demonstrate that a certain class of problems in linear arithmetic combinatorics is equivalent to a problem in the representation theory of finite groups which relates the sizes of various stabilizer groups.

0. Introduction

The purpose of this paper is to establish a connection between the theory of linear arithmetic combinatorics and the representation theory of finite groups. In this paper, when we refer to linear arithmetic combinatorics, we will mean the study of a certain class of statements we are about to define.

First let us clarify some notation. Let $k \geq 2$ be an integer. Let $\mathcal{L}$ and $\mathcal{S}$ be finite sets of real-valued linear functions on $\mathbb{R}^k$. Whenever

$$\rho : \mathbb{R}^k \longrightarrow \mathbb{R}$$

is a linear function and V is any vector space over $\mathbb{R}$, we may extend ρ componentwise to

$$\rho : V^k \longrightarrow V.$$

We shall not distinguish notationally between these two ρ's. Let $1 \leq \alpha \leq k$ be a positive real number. We now define a statement $S(k, \mathcal{L}, \mathcal{S}; \alpha)$.

$S(k, \mathcal{L}, \mathcal{S}; \alpha)$. *Let V be a vector space and let G be a finite set. Let*

$$r : G \longrightarrow V^k.$$

Suppose that for every $\sigma \in \mathcal{S}$ one has

$$\#(\sigma(r(G))) \leq N,$$

Received August 8, 2003; received in final form May 17, 2005.
2000 *Mathematics Subject Classification.* 05D99.
The author was partially supported by the National Science Foundation Grant DMS 0432237.

for some fixed natural number N. Suppose further that for every $\rho \in \mathcal{L}$ one has that ρ is one to one on $r(G)$. Then

$$\#(G) \leq N^{\alpha}.$$

The reader curious as to why there is no constant or logarithmic factor on the right hand side of the inequality should examine Proposition 1.3.

The goal of linear arithmetic combinatorics is to determine for which choices of $k, \mathcal{L}, \mathcal{S}$, and α, the statement $S(k, \mathcal{L}, \mathcal{S}; \alpha)$ is correct. In order to motivate this, we remind the reader of two subclasses of statements which have important applications.

We will coordinatize the linear functions on $\mathbb{R}^2$ projectively. We define for any real number r the linear map $+_r$ from $\mathbb{R}^2$ to $\mathbb{R}$ by

$$+_r(a, b) = a + rb.$$

Abusing notation, we define the map

$$+_\infty(a, b) = b.$$

For any extended real numbers $r_1, \ldots, r_n$, we define the statement $SD(r_1, \ldots, r_n; \alpha)$ by

$$SD(r_1, \ldots, r_n; \alpha) := S(2, \{+_{-1}\}, \{+_{r_1}, \ldots, +_{r_n}\}; \alpha).$$

The Sums-Differences problem, which was first introduced in [1] and further studied in [4] and [5], is to determine which of the statements $SD(r_1, \ldots, r_n; \alpha)$ are true. A simple example of such a true statement is $SD(0, 1, 2, \infty; 7/4)$. (See [4] for a short proof.)

We define the statement

$SD(\alpha)$. For all $\epsilon > 0$ there exist extended reals $r_1, \ldots, r_n$ so that $SD(r_1, \ldots, r_n; \alpha + \epsilon)$.

Currently $SD(\alpha)$ is known for all α greater than the positive real root of the polynomial $x^3 - 4x + 2$, which is approximately 1.67512... (See [5].)

Conjecture 1. *$SD(1)$.*

Conjecture 1 is important because it implies a variant of the Kakeya problem, namely that any set in $\mathbb{R}^n$ containing a unit line segment in every direction must have upper Minkowski dimension n. This is an important problem in Fourier analysis. For a survey see [10].

We now define our second class of examples. If $i, j \in \{1, \ldots k\}$, we define linear functions ρ_i and ρ_{ij} on $\mathbb{R}^k$ by

$$\rho_i(x) = x_i\,; \quad \rho_{ij}(x) = x_i + x_j.$$

We define

$$SE(k; \alpha) := S(k, \{\rho_i\}, \{\rho_{ij}\}; \alpha).$$

Further, we define

$SE(\alpha)$. *For all $\epsilon > 0$ there exists a $k > 0$ with $SE(k; \alpha + \epsilon)$.*

The family SE arose in the paper [8] in connection with Erdös' famous distance problem (see [2]), which asks how few distinct distances there can be between N points in the plane. [8] showed the $SE(\alpha)$ implies $\Omega(N^{4/(5-1/\alpha)-})$ distances. The problem was further studied in [9], [3], and [6]. Currently the best known result is $SE((24-7e)/(10-3e))$. (See [6].) Some counterexamples are given in [7]. They show that the best conceivable result is

Conjecture 2. $SE(2)$.

In general, if one thinks about how to build a counterexample to one of the statements $S(k, \mathcal{L}, \mathcal{S}; \alpha)$, one realizes that there are several different layers of structure involved. There is the choice of the vector space V and the exact values of the map r. But what turns out to be more fundamental is the set G and the incidence geometry of the level sets of the functions $\sigma(r(G))$. We consider now the special case where this is part of a Tits geometry. In other words, the case in which G is a finite group and the level sets are cosets of certain subgroups.

$GS(k, \mathcal{L}, \mathcal{S}; \alpha)$. *Let G be a finite group and let V be a vector space on which it is represented (on the left). Let $w = (v_1, \ldots, v_k) \in V^k$. Suppose that for every $\sigma \in \mathcal{S}$ there is a subgroup $H_\sigma \subset G$ with*

$$[G : H_\sigma] \leq N,$$

and with $\sigma(w)$ fixed by H_σ. Suppose further that for every $\rho \in \mathcal{L}$ one has that $\rho(w)$ is not fixed by any element of G other than the identity. Then

$$\#(G) \leq N^\alpha.$$

We are now ready to state our main result.

Theorem 0.1.

$$S(k, \mathcal{L}, \mathcal{S}; \alpha) \iff GS(k, \mathcal{L}, \mathcal{S}; \alpha).$$

One direction is immediate. To get the other, we will lift a counterexample to $S(k, \mathcal{L}, \mathcal{S}; \alpha)$ to the group of permutations on G.

In Section 1, we will review some generalities about the classes of problems $S(k, \mathcal{L}, \mathcal{S}; \alpha)$ and $GS(k, \mathcal{L}, \mathcal{S}; \alpha)$. In Section 2, we will prove the main theorem. In Section 3 we will present some group-theoretic counterexamples to statements in the family SD.

Acknowledgments. The author would like to thank Elizabeth Housworth, Alex Iosevich, Mike Larsen, and John Shareshian for helpful discussions.

1. Preliminaries

In this section, we remind the reader of some of the standard features of problems in the family $S(k, \mathcal{L}, \mathcal{S}; \alpha)$.

Let G be a set, V a vector space, and r a map from G to V. We say that (G, V, r) is an $S(k, \mathcal{L}, \mathcal{S})$ example of order N provided that for every $\sigma \in \mathcal{S}$ one has

$$\#(\sigma(r(G))) \leq N,$$

and for every $\rho \in \mathcal{L}$ one has that ρ is one to one on $r(G)$.

Similarly, let G be a group, $\{H_\sigma\}_{\sigma \in \mathcal{S}}$ be a family of subgroups of G, V a vector space on which G is represented, and $w \in V^k$. We say that $(G, \{H_\sigma\}, V, w)$ is a $GS(k, \mathcal{L}, \mathcal{S})$ example of order N provided that for each $\sigma \in \mathcal{S}$ we have $[G : H_\sigma] \leq N$ and $\sigma(w)$ is fixed by every element in H_σ, while for every $\rho \in \mathcal{L}$ one has that $\rho(w)$ is not fixed by any element of G.

PROPOSITION 1.1. *Suppose (G, V, r) is an $S(k, \mathcal{L}, \mathcal{S})$ example of order N with $\#(G) = K$. Then there exists (G', V', r'), an $S(k, \mathcal{L}, \mathcal{S})$ example of order N^2 with $\#(G') = K^2$. Similarly suppose $(G, \{H_\sigma\}, V, w)$ is a $GS(k, \mathcal{L}, \mathcal{S})$ example of order N with $\#(G) = K$. Then there exists $(G', \{H'_\sigma\}, V', w')$, a $GS(k, \mathcal{L}, \mathcal{S})$ example of order N^2 with $\#(G') = K^2$.*

Proof. To prove the first part, we let $G' = G \times G$, $V' = V^2$, and $r'(g_1, g_2) = (r(g_1), r(g_2))$.

To prove the second part, we let $G' = G \times G$, $H'_\sigma = H_\sigma \times H_\sigma$, and we let V' be the representation $V \oplus V$, and $w' = (w, w)$. □

An immediate consequence of the proposition is:

COROLLARY 1.2. *Suppose that $S(k, \mathcal{L}, \mathcal{S}; \alpha)$ is false. Then we can find arbitrarily large N and (G, V, r), an $S(k, \mathcal{L}, \mathcal{S})$ example of order N with $\#(G) > N^\alpha$. Suppose that $GS(k, \mathcal{L}, \mathcal{S}; \alpha)$ is false. Then we can find arbitrarily large N and $(G, \{H_\sigma\}, V, w)$, a $GS(k, \mathcal{L}, \mathcal{S})$ example with $\#(G) > N^\alpha$.*

PROPOSITION 1.3. *Fix $k, \mathcal{L}, \mathcal{S}$. Then for some $\beta \geq 0$ we have*

$$\{\alpha : S(k, \mathcal{L}, \mathcal{S}; \alpha)\} = [\beta, \infty).$$

Similarly for some $\gamma \geq 0$ we have

$$\{\alpha : GS(k, \mathcal{L}, \mathcal{S}; \alpha)\} = [\gamma, \infty).$$

We will show later that $\gamma = \beta$.

Proof. It is clear that $S(k, \mathcal{L}, \mathcal{S}; \beta) \implies S(k, \mathcal{L}, \mathcal{S}; \alpha)$ and $GS(k, \mathcal{L}, \mathcal{S}; \beta) \implies GS(k, \mathcal{L}, \mathcal{S}; \alpha)$ whenever $\beta < \alpha$. We thus need only show the sets are closed.

Let

$$\beta = \inf\{\alpha : S(k, \mathcal{L}, \mathcal{S}; \alpha)\}.$$

Let (G, V, r) be an $S(k, \mathcal{L}, \mathcal{S})$ example of order N. Then

$$\#(G) \leq N^{\alpha},$$

for all $\alpha > \beta$. Taking the infimum over these inequalities, we get

$$\#(G) \leq N^{\beta}.$$

An identical argument proves the second part. □

Next, we will show that the freedom to choose any real vector space V plays no role whatsoever in the problem of determining whether $S(k, \mathcal{L}, \mathcal{S}; \alpha)$ is true.

We define the following statements:

$\mathbb{R}S(k, \mathcal{L}, \mathcal{S}; \alpha)$. *Let G be a finite set. Let*

$$r : G \longrightarrow \mathbb{R}^k.$$

Suppose that for every $\sigma \in \mathcal{S}$ one has

$$\#(\sigma(r(G))) \leq N,$$

for some fixed natural number N. Suppose further that for every $\rho \in \mathcal{L}$ one has that ρ is one to one on $r(G)$. Then

$$\#(G) \leq N^{\alpha}.$$

We say that (G, r) is an $\mathbb{R}S(k, \mathcal{L}, \mathcal{S})$ example of order N provided that $(G, \mathbb{R}, r)$ is an $S(k, \mathcal{L}, \mathcal{S})$ example of order N.

PROPOSITION 1.4. $S(k, \mathcal{L}, \mathcal{S}; \alpha) \iff \mathbb{R}S(k, \mathcal{L}, \mathcal{S}; \alpha)$.

Proof. It is immediate that $S(k, \mathcal{L}, \mathcal{S}; \alpha) \implies \mathbb{R}S(k, \mathcal{L}, \mathcal{S}; \alpha)$. We must show the opposite direction.

Suppose that (G, V, r) is an $S(k, \mathcal{L}, \mathcal{S})$ example of order N and that $\#(G) > N^{\alpha}$. We will use this to construct an equally large $\mathbb{R}S(k, \mathcal{L}, \mathcal{S})$ example.

We introduce a collection of formal variables

$$\{x_{g,j}\}_{g \in G, 1 \leq j \leq k}.$$

We will allow our linear functions to act formally on the k-tuples $x_g = (x_{g,1}, \ldots, x_{g,n})$. We will introduce a system of equations among the formal variables

$$\mathcal{E} = \{\sigma(x_{g_1}) = \sigma(x_{g_2}) : \sigma(r(g_1)) = \sigma(r(g_2)\}.$$

Notice that $x_g = r(g)$ is a V-valued solution to the system of equation $\mathcal{E}$. Also note that for every $\rho \in \mathcal{L}$ we have $\rho(r(g_1)) \neq \rho(r(g_2))$ for g_1, g_2 distinct. Therefore $\mathcal{E}$ does not imply any of the equations

$$\rho(x_{g_1}) = \rho(x_{g_2}),$$

for g_1, g_2 distinct.

Let K be the vector space of real-valued solutions to $\mathcal{E}$. Let L_{ρ,g_1,g_2} be the set of real-valued solutions to $\mathcal{E}$ which also satisfy

$$\rho(x_{g_1}) = \rho(x_{g_2}).$$

When g_1, g_2 are distinct, we have that L_{ρ,g_1,g_2} is a hyperplane in K. No real vector space is a finite union of hyperplanes. Therefore the set

$$M = K \backslash \left(\bigcup_{\rho \in \mathcal{L}, g_1 \neq g_2 \in G} L_{\rho,g_1,g_2} \right),$$

is nonempty. Pick any solution $m \in M$. Then (G, m) is the desired $\mathbb{R}S(k, \mathcal{L}, \mathcal{S})$ example of order N. □

We codify a consequence of the above proof as a corollary.

COROLLARY 1.5. *Let (G, V, r) be an $S(k, \mathcal{L}, \mathcal{S})$ example of order N. Then there exists (G, s), an $\mathbb{R}S(k, \mathcal{L}, \mathcal{S})$ example of order N, so that for each $\sigma \in \mathcal{S}$, the functions $\sigma(r(.))$ and $\sigma(s(.))$ have the same level sets.*

We now define a scalar version of the $GS(k, \mathcal{L}, \mathcal{S}; \alpha)$ problem. Let G be a group. If H is a subgroup, a left coset is the set gH where $g \in G$.

$\mathbb{R}GS(k, \mathcal{L}, \mathcal{S}; \alpha)$. *Let G be a finite group. Let $r : G \longrightarrow \mathbb{R}^k$. Suppose that for every $\sigma \in \mathcal{S}$ there is a subgroup $H_\sigma \subset G$ with*

$$[G : H_\sigma] \leq N,$$

and suppose that $\sigma(r(g))$ is constant on the left cosets of H_σ. Suppose moreover that (G, r) is an $\mathbb{R}S(k, \mathcal{L}, \mathcal{S})$ example of order N. Then

$$\#(G) \leq N^\alpha.$$

We of course define such a triple $(G, \{H_\sigma\}, r)$ to be an $\mathbb{R}GS(k, \mathcal{L}, \mathcal{S})$ example of order N.

PROPOSITION 1.6. $GS(k, \mathcal{L}, \mathcal{S}; \alpha) \iff \mathbb{R}GS(k, \mathcal{L}, \mathcal{S}; \alpha)$.

Proof. Suppose we are given $(G, \{H_\sigma\}, V, w)$, a $GS(k, \mathcal{L}, \mathcal{S})$ example of order N. Then define the function $r : G \longrightarrow V^k$ by

$$r(g) = gw,$$

where we consider V^k as being the k-fold direct sum of the representation v. Then (G, V, r) is an $S(k, \mathcal{L}, \mathcal{S})$ example. Notice that for each $\sigma \in \mathcal{S}$ we have that $\sigma(r(.))$ is constant on left cosets of H_σ. We apply Corollary 1.5 to obtain an $\mathbb{R}GS(k, \mathcal{L}, \mathcal{S})$ example of the same size.

Conversely suppose we are given $(G, \{H_\sigma\}, r)$, an $\mathbb{R}GS(k, \mathcal{L}, \mathcal{S})$ example of order N. We let V be the set of functions on G considered as the right regular

representation. Then r can be viewed as an element of V^k. We claim that $(G, \{H_\sigma\}, V, r)$ is a $GS(k, \mathcal{L}, \mathcal{S})$ example of order n.

We now prove the claim. For each $\sigma \in \mathcal{S}$, we know that $\sigma(r(.))$ is constant on the left cosets of H_σ. Therefore it is fixed by each element of H_σ acting in the right regular representation. On the other hand, for each $\rho \in \mathcal{L}$ we have that $\rho(r(.))$ is an injective real-valued function on G. Therefore no nontrivial permutation of the domain can fix it. □

2. Proof of Theorem 0.1

We proceed to prove the main theorem.

First we will show

$$S(k, \mathcal{L}, \mathcal{S}; \alpha) \implies GS(k, \mathcal{L}, \mathcal{S}; \alpha).$$

Suppose that $(G, \{H_\sigma\}, V, w)$ is a $GS(k, \mathcal{L}, \mathcal{S})$ example of order N and $\#(G) > N^\alpha$. Then define $r : G \longrightarrow V^k$ by

$$r(g) = gw.$$

By hypothesis, (G, V, r) is an $S(k, \mathcal{L}, \mathcal{S})$ example of order N. But since $\#(G) > N^\alpha$, we have reached a contradiction.

Now we need only show

$$GS(k, \mathcal{L}, \mathcal{S}; \alpha) \implies S(k, \mathcal{L}, \mathcal{S}; \alpha).$$

In fact, by Proposition 1.3, we need only show that for any $\epsilon > 0$,

$$GS(k, \mathcal{L}, \mathcal{S}; \alpha) \implies S(k, \mathcal{L}, \mathcal{S}; \alpha + \epsilon).$$

First we record a pair of elementary estimates on factorials. This could also be done by invoking Stirling's formula.

LEMMA 2.1. *For any $\epsilon > 0$, when N is sufficiently large, we have*

$$N^{(1-\epsilon)N} < N! < N^N.$$

Proof. The second inequality is obvious since $N!$ is a product of N factors all but one of which is less than N.

To get the first inequality, just observe that

$$\left(\frac{\epsilon}{3}N\right)^{N(1-\epsilon/2)} \leq N!,$$

since $N!$ has more than $N(1-\epsilon/2)$ factors larger than $(\epsilon/3)N$. Since $(\epsilon/3)^{-N}$ grows more slowly in N than $N^{\epsilon N/2}$, the proof is complete. □

LEMMA 2.2. *Fix $\rho < 1$. For any $\delta > 0$, when M is a sufficiently large natural number, the following is true. Let K be a natural number with $K \leq$*

$M^{1-\rho}$. Let $j_1, \dots, j_K$ be natural numbers with $j_1 + \cdots + j_K = M$. Then

$$\prod_{l=1}^{K} j_l! > (M!)^{\rho-\delta}.$$

Proof. Pick $\eta > 0$ very, very small depending only on δ. Then

$$\sum_{l: j_l \leq \eta M/K} j_l \leq \eta M.$$

Therefore

$$\sum_{l: j_l > \eta M/K} j_l \geq (1 - \eta M).$$

Now

$$\begin{aligned}
\prod_{l=1}^{K} j_l! &\geq \prod_{l: j_l > \eta M/K} j_l! \\
&\geq \prod_{l: j_l > \eta M/K} j_l^{(1-\eta) j_l} \\
&\geq \prod_{l: j_l > \eta M/K} \left(\eta \frac{M}{K}\right)^{(1-\eta) j_l} \\
&\geq \eta^M M^{\rho (1-\eta)^2 M}.
\end{aligned}$$

For the second inequality, we have applied Lemma 2.1 with ηM^ρ sufficiently large. Moreover, we may assume that we have picked M sufficiently large so that

$$\eta^M \geq M^{-\eta \rho M}.$$

Thus we have

$$\prod_{l=1}^{K} j_l! \geq M^{((1-\eta)^2 - \eta)\rho M}.$$

By the correct choice of η,

$$(1-\eta)^2 - \eta > 1 - \frac{\delta}{\rho},$$

and applying the easy half of Lemma 2.1 we have completed the proof. □

We are now ready to complete the proof of Theorem 0.1. Given a large (G, V, r), an $S(k, \mathcal{L}, \mathcal{S})$ example of order N with $\#(G) > N^{\alpha+\epsilon}$, we must construct $(G', \{H_\sigma\}, V', w)$, a $GS(k, \mathcal{L}, \mathcal{S})$ example of some order N' with $\#(G') \geq (N')^\alpha$. Recall that by Corollary 1.2 we can always find a large $S(k, \mathcal{L}, \mathcal{S})$ example.

We let V' be the space of V-valued functions on G. We let G' be the permutation group of the elements of G and H_σ be the subgroup of permutations that fix the level sets of $\sigma(r(.))$. We set $w' = r$, where we consider r as a k-tuple of V-valued functions on G. Clearly H_σ is exactly the group of permutations fixing $\sigma(w')$. On the other hand, for any $\rho \in \mathcal{L}$, we have that $\rho(w')$ is injective from G to V so that no nontrivial permutation fixes it. We have established that $(G', \{H_\sigma\}, V', w')$ is a $GS(k, \mathcal{L}, \mathcal{S})$ example and we are left to estimate the orders.

Then H_σ is in fact the direct product of the permutation groups of the individual level sets. We may apply Lemma 2.2 with $M = N^{\alpha+\epsilon}$ and with $\rho = 1 - \frac{1}{\alpha+\epsilon}$. We conclude that for each $\sigma \in \mathcal{S}$, we have that

$$\#(H_\sigma) > \#(G')^{1-\frac{1}{\alpha+\epsilon}-\delta}.$$

Since δ was chosen arbitrarily, we may have chosen it so small that we get

$$\#(H_\sigma) > \#(G')^{1-1/\alpha},$$

which is the same as

$$\#(G') > \left(\frac{\#(G')}{\#(H_\sigma)}\right)^{\alpha},$$

which was to be shown. □

3. Some examples

In this section, we describe a family of group-theoretic sums-differences examples which motivated this study. To be precise, for certain sets $\{r_1, \ldots, r_n\}$ of numbers, we will produce $\mathbb{R}GS(2, \{+_{-1}\}, \{+_{r_j}\}_{j=1}^n)$ examples, which from now on we will refer to as $GSD(r_1, \ldots, r_n)$ examples.

Example 1. The following is a very well known $GSD(0, 1, \infty)$ example (see, e.g., [1], [6]). Rusza [7] found a much stronger example.

Let $G = S_3$, the group of permutations on three elements. Notice that this is also D_3, the dihedral group on three elements, which is the group of symmetries of the equilateral triangle. We must define w and $\mathbb{R}^2$-valued function on G.

We let

$$w(e) = (0,1);\ w((12)) = (0,3);\ w((13)) = (3,1);$$
$$w((23)) = (1,0);\ w((123)) = (1,3);\ w(132) = (3,0).$$

Then letting

$$H_{+_0} = \{e, (12)\}; H_{+_\infty} = \{e, (13)\}; H_{+_1} = \{e, (23)\},$$

we have an example of order 3 (and size 6).

EXAMPLE 2. The following is a $GSD(0,1,2,\infty)$ example, which as far as we know has not been published before.

Let $G = D_4 = \{e, (13), (24), (13)(24), (1234), (12)(34), (1432), (14)(23)\}$ be the dihedral group on 4 elements.

Define

$$w(e) = (-16, 31);\ w((13)) = (-16, 26);\ w((24)) = (34, 6);$$
$$w((13)(24)) = (34, 1);\ w((1234)) = (4, 6);\ w((12)(34)) = (4, 31);$$
$$w((1432)) = (14, 26);\ w((14)(23)) = (14, 1).$$

Let

$$H_{+_0} = \{e, (13)\};\ H_{+_{infty}} = \{e, (12)(34)\};$$
$$H_{+1} = \{e, (14)(23)\};\ H_{+2} = \{e, (24)\}.$$

Then we have an example of order 4 (and size 8).

EXAMPLE $n-2$. Example 1 is not hard to discover without a group theoretic point of view. Example 2 solves a problem that is overdetermined and we came across it by first discovering the range of w by trial and error and with great difficulty.

However, once one has the group theoretic point of view, it becomes apparent why these examples exist and why one has an analogous example for every dihedral group.

The group D_n is the symmetry group of the regular n-gon and is therefore represented on the plane. It contains n reflections and n rotations (counting the identity). Each reflection preserves a line through the origin. We call these the *fixed lines*. Any point in the plane not on the fixed lines is not preserved by any element of the group.

Let v_1 and v_2 be two points in the plane and suppose that the line l passing through them does not contain the origin. Suppose moreover that the direction of the line, $v_1 - v_2$, is not preserved by any element of the group. Then l intersects each fixed line. Number the fixed lines $l_1, \ldots, l_n$. Hence for each fixed line l_j there is a real r_j different from -1 so that $(v_1 + r_j v_2)/(r_j + 1)$ is on the fixed line (unless v_2 is on the line, in which case we take $r_j = \infty$). We denote by $H_{+_{r_j}}$ the subgroup of order 2 generated by the reflection preserving l_j. We let $w = (v_1, v_2)$. Then $(G, \{H_{+_{r_j}}\}, w)$ is a $GS(2, \{+_{-1}\}, \{+_{r_j}\}_{j=1}^n)$ example of order n (and size $2n$). Now, by Proposition 1.6, there must exist such a $GSD(r_1, \ldots, r_n)$ example.

REFERENCES

[1] J. Bourgain, *On the dimension of Kakeya sets and related maximal inequalities*, Geom. Funct. Anal. **9** (1999), 256–282. MR 1692486 (2000b:42013)

[2] P. Erdös, *On sets of distances of n points*, Amer. Math. Monthly **53** (1946), 248–250. MR 0015796 (7,471c)

[3] N. H. Katz, *An improvement of a lemma of Tardos*, Combinatorica, submitted.
[4] N. H. Katz and T. Tao, *Bounds on arithmetic projections, and applications to the Kakeya conjecture*, Math. Res. Lett. **6** (1999), 625–630. MR 1739220 (2000m:28006)
[5] ———, *New bounds for Kakeya problems*, J. Anal. Math. **87** (2002), 231–263. MR 1945284 (2003i:28006)
[6] N. H. Katz and G. Tardos, *A new entropy inequality for the Erdős distance problem*, Towards a theory of geometric graphs, Contemp. Math., vol. 342, Amer. Math. Soc., Providence, RI, 2004, pp. 119–126. MR 2065258 (2005f:52033)
[7] I. Z. Ruzsa, *A problem on restricted sumsets*, Towards a theory of geometric graphs, Contemp. Math., vol. 342, Amer. Math. Soc., Providence, RI, 2004, pp. 245–248. MR 2065267 (2005g:11030)
[8] J. Solymosi and C. D. Tóth, *Distinct distances in the plane*, Discrete Comput. Geom. **25** (2001), 629–634. MR 1838423 (2002c:52020)
[9] G. Tardos, *On distinct sums and distinct distances*, Adv. Math. **180** (2003), 275–289. MR 2019225 (2004j:11025)
[10] T. Wolff, *Recent work connected with the Kakeya problem*, Prospects in mathematics (Princeton, NJ, 1996), Amer. Math. Soc., Providence, RI, 1999, pp. 129–162. MR 1660476 (2000d:42010)

Department of Mathematics, Indiana University, Bloomington, IN 47405, USA
E-mail address: nhkatz@indiana.edu