The Set of Differences of a Given Set

Andrew Granville; Friedrich Roesler

The American Mathematical Monthly, Vol. 106, No. 4. (Apr., 1999), pp. 338-344.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28199904%29106%3A4%3C338%3ATSODOA%3E2.0.CO%3B2-7

The American Mathematical Monthly is currently published by Mathematical Association of America.

The Set of Differences of a Given Set

Andrew Granville and Friedrich Roesler

1. INTRODUCTION. A central problem of combinatorial geometry and additive number theory is to understand the set of sums or differences of a given set of vectors. For example, given a set of m arbitrary vectors A, how big is the set $A + A := \{a + b\colon a, b \in A\}$, or the set $A - A := \{a - b\colon a, b \in A\}$? By packing the vectors close together on a lattice one can make these sets small: for example, if $A = \{a, 2a, 3a, \ldots, (m-1)a, ma\}$ then $A + A$ and $A - A$ both have $2m - 1$ elements. On the other hand, if the elements of A are appropriately spread out then we can make these sets large: for example, if $A = \{2^1, 2^2, \ldots, 2^m\}$ then $A + A$ has $(m^2 + m)/2$ elements, and $A - A$ has $m^2 - m + 1$ elements.

It may be that the sizes of $A - A$ and $A + A$ are quite different: For example if A is the set of positive integers smaller than 10^k that have only digits 1, 2, and 4 in their decimal expansions then A has 3^k elements and $A + A$ has 6^k elements, far smaller than $A - A$, which has 7^k elements. Similarly, one can construct A so that $A + A$ is far larger than $A - A$, for example by taking $A = \sum_{i=0}^{k-1} b_i 100^i$ where each b_i is allowed to take any value from the set $\{0, 2, 3, 4, 7, 11, 12, 14\}$; see [7] and [8] for more details. For the more natural example $A = \{1^2, 2^2, \ldots, n^2\}$ it can be shown, though with some difficulty, that $A - A$ is about $\log^{\kappa} n$ times as large as $A + A$, for some constant $\kappa > 0$.

Some time ago it was realized that if either $A + A$ or $A - A$ is very small then A must have some special structure: Indeed, Freiman [5] (but see [9]) showed that A must then be a subset of a small part of a lattice. There have recently been several striking and elegant advances in this area of combinatorial additive number theory; see [1], [2], and [6]. Moreover Gowers has recently given a spectacular application of Freiman's theorem, which proves the first reasonable upper bounds in Szemerédi's theorem: Given a positive integer k and a $\delta > 0$, every subset of $\{1, 2, \ldots, n\}$ with at least δn elements contains a k-term arithmetic progression, provided $n > N(k, \delta)$. Gowers gave the upper bound [13]

$$N(k, \delta) \le 2^{2^{|\log \delta|^{2^{c \cdot 2^k}}}},$$

for some constant c, a substantial improvement over bounds known previously.

Seemingly unrelated to all this is

Graham's conjecture. *For any set A of m distinct positive integers, we have*

$$\max_{a, b \in A} \frac{a}{\gcd(a, b)} \ge m.$$

Equality holds only in the following cases:

- $A = \{2, 3, 4, 6\}$.
- $A = \{k, 2k, \ldots, mk\}$ *for some integer* k.
- $A = \{l/1, l/2, \ldots, l/m\}$ *for some integer* l *divisible by the least common multiple of* $1, \ldots, m$.

This old chestnut has recently been proved correct in an outstandingly original, though long and complicated, paper by Balasubramanian and Soundararajan [3]. Their method involves very careful consideration of prime divisors of linear combinations of numbers from A. In fact Graham's conjecture had been elegantly proved for sufficiently large m by Szegedy [10] and Zaharescu [12] a decade earlier, but it took a wealth of new ideas to extend their result to all integers m.

In search of a more combinatorial proof, one might approach Graham's conjecture by asking whether there are at least m distinct integers in the set $\{a/\gcd(a, b)$: $a, b \in A\}$? If so, Graham's conjecture would follow easily. Unfortunately the answer is "no," since for

$$A = \{2, 3, 4, 6, 9, 12, 18\} \tag{1}$$

one gets the set $\{1, 2, 3, 4, 6, 9\}$.

Unsolved problem. *For each integer $m \geq 1$, what is the least number of integers one can have in the set $\{a/\gcd(a, b)$: $a, b \in A\}$, where A is a set of m distinct positive integers?*

One can relate this problem quite closely to the vector questions asked at the beginning of the Introduction:

Let $p_1, p_2, \ldots, p_n$ be the set of primes that divide integers in A. Write each $a \in A$ in the form $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and associate to it the vector $\mathbf{a} = (a_1, \ldots, a_n)$; note that distinct integers are associated with different vectors. Now, given $a, b \in A$, evidently $\min\{a_i, b_i\}$ is the ith component of the vector associated with $\gcd(a, b)$. Thus $a_i - \min\{a_i, b_i\} = \max\{0, a_i - b_i\}$ is the ith component of the vector associated with $a/\gcd(a, b)$; we call this vector $\delta(\mathbf{a}, \mathbf{b})$. Thus we have:

Unsolved problem (restated). *For each integer $m \geq 1$, what is the least number of vectors one can have in the set $\delta(A) := \{\delta(\mathbf{a},\mathbf{b}) : \mathbf{a}, \mathbf{b} \in A\}$, where A is a set of m distinct vectors?*

Remark. We can claim that this is a restatement of the first unsolved problem only if we state that the vectors in A all have non-negative integer entries. However, through a few minor technical tricks one can drop that requirement; we leave this as a challenge to the reader.

To get the lower bound $|\delta(A)| \geq m^{1/2}$ in the unsolved problem, we first note that, for fixed $\mathbf{a} \in A$, the pairs $(\delta(\mathbf{a}, \mathbf{b}), \delta(\mathbf{b}, \mathbf{a}))$ must all be distinct since $\mathbf{b} = \mathbf{a} - \delta(\mathbf{a}, \mathbf{b}) + \delta(\mathbf{b}, \mathbf{a})$, and so there are no less than m distinct pairs. Thus there are either $\geq m^{1/2}$ distinct values for $\{\delta(\mathbf{a}, \mathbf{b}) : \mathbf{b} \in A\}$ or for $\{\delta(\mathbf{b}, \mathbf{a}) : \mathbf{b} \in A\}$, else there would be less than m distinct pairs $(\delta(\mathbf{a}, \mathbf{b}), \delta(\mathbf{b}, \mathbf{a}))$, giving a contradiction.

One can get a better lower bound for $\delta(A)$ if A is a set of vectors in the plane:

Theorem 1. *If $A \subset \mathbb{R}^2$ is a set of $m \geq 1$ distinct vectors then $\delta(A)$ has at least $(m/2)^{2/3}$ vectors. In fact there exists $\mathbf{a} \in A$ such that there are at least $(m/2)^{2/3}$ distinct vectors amongst $\{\delta(\mathbf{b}, \mathbf{a}) : \mathbf{a} \in A\}$.*

Perhaps such a lower bound holds in higher dimension. We postpone the proof of this and other results until subsequent sections.

The example given in (1) is a translation of the set $A = \{(x, y) \in \mathbb{Z}^2 : 0 \leq x, y \leq 2, 1 \leq x + y \leq 3\}$, given by Freiman and Lev (taking $n = 2, p_1 = 2, p_2 = 3$). They generalized this to $A = \{(x, y) \in \mathbb{Z}^2 : x, y \geq 0, L < x + y \leq U\}$ with $L = ((2m)^{2/3} - (2m)^{1/3})/2 + O(1)$ and $U = ((2m)^{2/3} + (2m)^{1/3})/2 + O(1)$. Then

$\delta(A) = \{(x, y) \in \mathbb{Z}^2 : x, y \geq 0, x + y < U - L\} \cup \{(t, 0), (0, t) \in \mathbb{Z}^2 : 0 \leq t \leq U\}$, which has $\sim (3/2)(2m)^{2/3}$ elements. Thus the lower bound in Theorem 1 is best possible up to a factor of $3 \cdot 2^{1/3}$. Moreover from these remarks, combined with those directly above the statement of Theorem 1, we obtain the following partial result concerning our unsolved problem:

Theorem 2. *If A is any set of $m \geq 1$ distinct vectors with $|\delta(A)|$ minimal, then $(3/2)(2m)^{2/3} \gtrsim |\delta(A)| \geq m^{1/2}$.*

The function $a/\gcd(a, b)$ in the unsolved problem is not symmetric in a and b. It thus might seem more natural to study the number of distinct values in $\{ab/\gcd(a, b)^2 : a, b \in A\}$. In this case we can prove a best possible result:

Theorem 3. *For any set of natural numbers A, there are at least $|A|$ natural numbers in the set $\{ab/\gcd(a, b)^2 : a, b \in A\}$.*

Remark. We show in Section 3 that the proof of Theorem 4 (which implies Theorem 3) can be modified to prove that equality holds only for the following sets A: Let $q_1, q_2, \ldots, q_k$ be positive rational numbers, with each $q_i = r_i/s_i \neq 1$ and $\gcd(r_i, s_i) = 1$ such that $\gcd(r_i s_i, r_j s_j) = 1$ if $i \neq j$. Let S be a subgroup of $(\mathbb{Z}/2\mathbb{Z})^k$. Then A is the set of integers $bq_1^{i_1} q_2^{i_2} \cdots q_k^{i_k}$ where the i_j satisfy $l_j \leq i_j \leq u_j$, for some lower and upper bounds l_j and u_j, with $(i_1, i_2, \ldots, i_k) \in S$, and b chosen so that these numbers are indeed all integers.

A simple example is when $A = \{d : d|n\}$ for any positive integer n. A more exotic example is $A = \{md^2 : d|n, m = 1 \text{ or } b\}$ where squarefree $b > 1$ divides n.

We may rewrite the question in Theorem 3 as a problem about sets of vectors: The ith component of the vector, $d(\mathbf{a}, \mathbf{b})$, associated with $ab/\gcd(a, b)^2$ is

$$a_i + b_i - 2\min\{a_i, b_i\} = |a_i - b_i|.$$

Therefore

$$d(\mathbf{a}, \mathbf{b}) = \delta(\mathbf{a}, \mathbf{b}) + \delta(\mathbf{b}, \mathbf{a}) = (|a_1 - b_1|, |a_2 - b_2|, \ldots, |a_n - b_n|)$$

since $\mathbf{a} - \mathbf{b} = \delta(\mathbf{a}, \mathbf{b}) - \delta(\mathbf{b}, \mathbf{a})$. Thus Theorem 3 is equivalent to the following result (which we shall prove in the next section):

Theorem 4. *If A is a finite set of distinct vectors in $\mathbb{R}^n$ then $D(A) = \{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in A\}$ has at least as many distinct vectors as A.*

These vector questions may all be thought of as problems about the set of distinct differences $\{\Delta(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in A\}$ for some naturally defined "difference" function Δ between two vectors. Moreover, each of our questions has a number theoretic interpretation; the set of values $\{\mathbf{a} - \mathbf{b}\}$ corresponds simply to looking at all ratios a/b of the corresponding integers. It is perhaps of interest to consider other difference functions that relate elementary number theory to vector problems, though we have been unable to identify any others that are particularly appealing:

Perhaps the most obvious difference function between two vectors is the Euclidean distance, $(|a_1 - b_1|^2 + |a_2 - b_2|^2 + \cdots + |a_n - b_n|^2)^{1/2}$. Unfortunately there is no straightforward number theoretic interpretation for the associated problem about integers. Moreover any set of orthonormal vectors has the property that the set of distances between pairs of vectors is $\{0, 1\}$. However, Erdős [4] restricted his attention to a set A of m distinct points in the plane. He noted that

for the points in the k-by-k integer lattice, where $k = \sqrt{m} + O(1)$, we have $\#\{|\mathbf{a} - \mathbf{b}| : \mathbf{a}, \mathbf{b} \in A\} \sim cm/\sqrt{\log m}$ for some constant $c > 0$, and asked whether this is best possible, up to the value of c? The best result in this direction, due to Székely [11], is that there exists some $\mathbf{b} \in A$ such that $\#\{|\mathbf{a} - \mathbf{b}| : \mathbf{a} \in A\} \geq c'm^{4/5}$, for some constant $c' > 0$.

2. PROOFS OF THE THEOREMS. Although we found several proofs of Theorem 1, we decided to present here the following elegant proof communicated to us by Sudakov:

Proof of Theorem 1 (Sudakov). Let x_1 be the smallest element of $X = \{x : (x, y) \in A\}$, the x-coordinates of points in A, and let $Y = \{y : (x, y) \in A\}$, the y-coordinates of points in A. Then $\delta(A)$ contains points with x-coordinate $x - x_1$ for each $x \in X$, so $|\delta(A)| \geq |X|$ (and therefore we take $\mathbf{a}$ to be any element of A with x-coordinate equal to x_1) . Similarly $|\delta(A)| \geq |Y|$. Thus our result is proved true unless $|X|, |Y| < (m/2)^{2/3}$, which we now assume.

We define a series of sets $A_1 = A \supset A_2 \supset \cdots \supset A_k$, and then let L_i be the set of *lines* of A_i, that is, the sets of points $\{(x, y) \in A_i\}$ for each $x \in X_i := \{x : (x, y) \in A_i\}$, and the sets of points $\{(x, y) \in A_i\}$ for each $y \in Y_i := \{y : (x, y) \in A_i\}$. The average number of points on each line in L_i is $r_i := 2|A_i|/(|X_i| + |Y_i|)$. Suppose there is a line in L_i that has less than $r_i/2$ points; we obtain the set A_{i+1} by removing the points of that line from the set A_i. Notice that $r_i < r_{i+1}$. We continue with this process until we reach the set A_k, in which every line in L_k has at least $r_k/2 \geq r_1/2 = m/(|X| + |Y|) \geq (m/2)^{1/3}$ points.

Let x_0 be the smallest element of X_k. Let y_0 be the smallest element of $Y_0 = \{y : (x_0, y) \in A_k\}$, a set that is the same size as the line $\{(x_0, y) : y \in Y_0\}$ of A_k and hence has size at least $(m/2)^{1/3}$. Let $B \subset A_k \subset A$ be the union, over each $y \in Y_0$, of the lines $\{(x, y) \in A_k\}$ of L_k. Each of these lines contains at least $(m/2)^{1/3}$ elements, so that B has at least $(m/2)^{2/3}$ elements. Now $\delta(\mathbf{b}, (x_0, y_0)) = \mathbf{b} - (x_0, y_0)$ for each $\mathbf{b} \in B$, so that these δ values are distinct. Therefore $|\delta(A)| \geq |\delta(B)| \geq |B|$ (and $\mathbf{a} = (x_0, y_0)$). ∎

Proof of theorem 4 We use induction on n and then on the size of the set A. If A has just one element then $D(A)$ contains only the zero vector, and so has exactly as many distinct vectors as A. If $n = 1$ and $A = \{a_1 < a_2 < a_3 < \cdots < a_m\}$ then $\{0, a_2 - a_1, a_3 - a_1, \ldots, a_m - a_1\} \subseteq D(A)$. This subset of $D(A)$ has exactly as many distinct vectors as A, so $|D(A)| \geq |A|$.

We may now assume that $|A| > 1$ and $n > 1$. Define

$$B = \{(x_1, \ldots, x_{n-1}) : \text{ there exists } x_n \text{ with } (x_1, \ldots, x_{n-1}, x_n) \in A\},$$

the projection of A onto the first $n - 1$ dimensions. Since B is a finite, non-empty set of distinct vectors in $\mathbb{R}^{n-1}$, we can invoke the induction hypothesis to obtain

$$|D(B)| \geq |B|. \tag{2}$$

Now, for each $\mathbf{b} \in B$, let

$$A_{\mathbf{b}} = \{x_n : (\mathbf{b}, x_n) \in A\} \text{ and let } a_{\mathbf{b}} = \max\{x : x \in A_{\mathbf{b}}\},$$

so $A_{\mathbf{b}}$ is the set of numbers that give the nth coordinate of a vector in A when appended to the $n - 1$ coordinates of $\mathbf{b}$, and $a_{\mathbf{b}}$ is the largest such number. Finally, let $C = A - \{(\mathbf{b}, a_{\mathbf{b}}) : \mathbf{b} \in B\}$. That is, we get C by removing exactly one vector from A for each $\mathbf{b} \in B$, namely the vector $(\mathbf{b}, a_{\mathbf{b}})$; in other words by "skimming off the highest point which projects onto $\mathbf{b}$, for each $\mathbf{b} \in B$." Therefore

$$|C| = |A| - |B|. \tag{3}$$

Since $|C| < |A|$ we deduce, from the induction hypothesis, that

$$|D(C)| \geq |C|. \tag{4}$$

We may describe $D(A)$ and $D(C)$ in terms of the elements of $D(B)$ and the elements of the sets $A_{\mathbf{b}}$:

$$D(A) = \cup_{D \in D(B)}\{(D, |a - a'|) : d(\mathbf{b}, \mathbf{b}') = D \text{ with } a \in A_{\mathbf{b}} \text{ and } a' \in A_{\mathbf{b}'}\}.$$

Similarly, since $C_{\mathbf{b}} = A_{\mathbf{b}} - \{a_{\mathbf{b}}\}$, we obtain

$$D(C) = \cup_{D \in D(B)}\{(D, |c - c'|) : d(\mathbf{b}, \mathbf{b}') = D \text{ with } c \in C_{\mathbf{b}} \text{ and } c' \in C_{\mathbf{b}'}\}.$$

Now comes the key observation in our argument: For any pair $\mathbf{b}, \mathbf{b}' \in B$, the largest difference $|a - a'|$ with $a \in A_{\mathbf{b}}$ and $a' \in A_{\mathbf{b}'}$, must have $a = a_{\mathbf{b}}$ or $a' = a_{\mathbf{b}'}$. Thus this largest difference does not appear among the set of differences $\{|c - c'| : c \in C_{\mathbf{b}}, c' \in C_{\mathbf{b}'}\}$. We deduce that, for any $D \in D(B)$, the set

$$\{|c - c'| : d(\mathbf{b}, \mathbf{b}') = D \text{ with } c \in C_{\mathbf{b}} \text{ and } c' \in C_{\mathbf{b}'}\}$$

does not contain the largest element of

$$\{|a - a'| : d(\mathbf{b}, \mathbf{b}') = D \text{ with } a \in A_{\mathbf{b}} \text{ and } a' \in A_{\mathbf{b}'}\},$$

so it is a proper subset, and is thus smaller. Comparing the sizes of $D(A)$ and $D(C)$, and taking this observation into account, we obtain

$$\begin{aligned} |D(C)| &\leq \sum_{D \in D(B)} \left(\#\{|a - a'| : d(\mathbf{b}, \mathbf{b}') = D \text{ with } a \in A_{\mathbf{b}} \text{ and } a' \in A_{\mathbf{b}'}\} - 1\right) \\ &\leq |D(A)| - |D(B)|. \end{aligned} \tag{5}$$

Combining (2), (3), (4), and (5) gives

$$|D(A)| \geq |D(B)| + |D(C)| \geq |B| + |C| = |A|,$$

as required.

3. WHEN DOES EQUALITY HOLD IN THEOREM 4? As we indicated at the beginning of the Introduction, equality typically holds in inequalities such as Theorem 4, only when the vectors in A form part of a lattice. Let $\mathbb{I}_k$ be the set of all subsets I of $\mathbb{Z}^k$ of the form $R \cap \Lambda$, where R is some rectangular box with sides parallel to the axes, and Λ is a lattice with $(2\mathbb{Z})^k \subseteq \Lambda \subseteq \mathbb{Z}^k$. More specifically the points $(i_1, i_2, \ldots, i_k) \in S$, with each i_j contained in some interval $[l_j, u_j]$, and S a subgroup of $(\mathbb{Z}/2\mathbb{Z})^k$. One can easily verify that equality holds in Theorem 4 for any $A \in \mathbb{I}_k$; in fact equality holds if and only if A is a suitable translation of some $I \in \mathbb{I}_k$:

Proposition 1. *If $A \subset \mathbb{R}^n$ with $|D(A)| = |A|$ then there exist $\mathbf{a}, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbb{R}^n$, with the gth component of $\mathbf{v}_j$ non-zero for at most one j for each g, such that $A = \{\mathbf{a} + \sum_{j=1}^k i_j \mathbf{v}_j : (i_1, i_2, \ldots, i_k) \in I\}$, where $I \in \mathbb{I}_k$.*

Before we indicate how to deduce this from our proof of Theorem 4, we first note the following results:

Proposition 2. *If A and B are two sets of distinct real numbers then $\#\{|a - b| : a \in A, b \in B\} \geq \min\{|A|, |B|\}$. If equality holds then either*

- *$A = B$ is an arithmetic progression; or*
- *$B = \{a + (2i + 1)d : 1 \leq 2i + 1 \leq 2N - 1\}$ with $A_0 = \{a + 2id : 0 \leq 2i \leq 2N\}$, and then A is either A_0, or A_0 less any one element; or*
- *$A = \{m - a, m + a\}$ and $B = \{m - b, m + b\}$ for some $a > b > 0$.*

The inequality in Proposition 2 can be proved by taking c to be the smallest number from either set (say from B), and then by noting that the numbers $a - c, a \in A$, are distinct, positive real numbers. That the enumerated cases are the only ones in which equality holds may be proved by induction on $\min\{|A|, |B|\}$, using the induction hypothesis on the smaller sets created by removing the largest number from each of A and B.

Proposition 3. *Suppose that $I \in \mathbb{I}_k$ and that $f : I \to \mathbb{R}$ is a map for which $|f(\mathbf{i}) - f(\mathbf{j})|$ is a function of $d(\mathbf{i}, \mathbf{j})$ only. Then there exist constants α and β such that, for every $\mathbf{i} \in I$, either $f(\mathbf{i}) = \alpha + \beta i_j$ for some fixed j, or $f(\mathbf{i}) = \alpha$ or β depending on whether or not $\mathbf{i} \in T$, where T is a subgroup of S of index 2.*

Proposition 3 is easily proved by induction on k.

Sketch of the proof of proposition 1. If $|A| = 1$ then clearly $|D(A)| = 1$. If $n = 1$ then A is an arithmetic progression, by Proposition 2. We now proceed with the same induction as in the proof of Theorem 4, and then by induction on $h(= h(A))$, the maximum of $|A_{\mathbf{b}}|, \mathbf{b} \in B$. For $h = 1$, we know that B has the structure stated in Proposition 1 by induction, since $|D(B)| = |B|$ as in the proof of Theorem 4. Define $f(\mathbf{i}) = a_{\mathbf{b}}$ where $\mathbf{b} = \mathbf{a} + \sum_{j=1}^{k} i_j \mathbf{v}_j$. The result follows from Proposition 3.

Now suppose $h > 1$ and write $A^{(1)} = A$. By the proof of Theorem 4 we know that $|D(B^{(1)})| = |B^{(1)}|$ and $|D(A^{(2)})| = |A^{(2)}|$ where $B^{(1)} = B$ and $A^{(2)} = C$. We now apply the proof of Theorem 4 to $A^{(2)}$ and then to $A^{(3)}$, etc., to find a sequence of sets $A^{(1)} \supsetneq A^{(2)} \supsetneq \cdots \supsetneq A^{(h)}$ with each $h(A^{(j)}) = h + 1 - j$ and $|D(A^{(j)})| = |A^{(j)}|$. Note that $B^{(j)} = \{\mathbf{b} \in B : |A_{\mathbf{b}}| \geq j\}$.

We first prove Proposition 1 for $A^* := \{(\mathbf{b}, x) : \mathbf{b} \in B^{(h)}, x \in A_{\mathbf{b}}\}$. From the proof of Theorem 4 (taking $D = 0$) we see that there are no more than h elements in the union of all sets $\{|a - a'| : a, a' \in A_{\mathbf{b}}\}$. If $|A_{\mathbf{b}}| = h$ then, by Proposition 2, $A_{\mathbf{b}}$ must be an arithmetic progression; and the arithmetic progressions for any two such sets must have the same common difference. Moreover if $|A_{\mathbf{b}}| = |A_{\mathbf{b}'}| = h$ then $\#\{|a - a'| : a \in A_{\mathbf{b}}, a' \in A_{\mathbf{b}'}\} \leq h$ by the proof of Theorem 4, and so either $A_{\mathbf{b}} = A_{\mathbf{b}'}$ or they are two disjoint, but interwoven, arithmetic progressions, by Proposition 2. Thus the sets $A_{\mathbf{b}}$ of size h are either all identical (in which case A^* satisfies Proposition 1 by the induction hypothesis), or there are two possible such sets $A_{\mathbf{b}}$. In this case we may write each $\mathbf{b} = \mathbf{a} + \sum_{j=1}^{k} i_j \mathbf{v}_j$ by the induction hypothesis, and let $f(\mathbf{i})$ be the smallest element in $A_{\mathbf{b}}$. By Proposition 3 we deduce that Proposition 1 holds for A^*.

The result thus holds when $A^* = A$, that is, when there are h elements in every $A_{\mathbf{b}}$, or equivalently when $B^{(1)} = B^{(h)}$. If not then there exists $\mathbf{b} \in B^{(j)} \setminus B^{(j+1)}$ for some $j, 1 \leq j \leq h - 1$. Let $\mathbf{b}'$ be any point in $B^{(j+1)}$ and $D := d(\mathbf{b}', \mathbf{b})$. The induction hypothesis ensures that each $B^{(i)}$ is a lattice as described in the hypothesis of Proposition 1, and this particular lattice structure implies that there do not exist $\beta, \beta' \in B^{(j+1)}$ with $d(\beta, \beta') = D$. Therefore $\#\{|a - a'| : a \in A_{\mathbf{b}}, a' \in A_{\mathbf{b}'}\} = |A_{\mathbf{b}}|$, by the proof of Theorem 4. Using Proposition 2 we deduce that $A_{\mathbf{b}}$ and $A_{\mathbf{b}'}$ are interwoven disjoint arithmetic progressions, whose union is also an arithmetic progression. Thus $h(A_{\mathbf{b}'}) = j + 1$, so taking $\mathbf{b}' \in B^{(h)}$ we see that $j = h - 1$, and moreover all such sets $A_{\mathbf{b}'}, \mathbf{b}' \in B^{(h)}$ must be the identical arithmetic progression. But the same argument applies to every $\mathbf{b} \in B^{(h-1)}$, and so each such $A_{\mathbf{b}}$ is the same arithmetic progression interwoven between the elements in each $A_{\mathbf{b}'}$ with $\mathbf{b}' \in B^{(h)}$. Thus Proposition 1 holds for A.

4. FURTHER QUESTIONS. Proposition 2 inspires, and provides the answer in one dimension to, the following open problem: If A and B are finite sets of distinct vectors in $\mathbb{R}^n$ then show that the order of the set $D(A, B) = \{d(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in A, \mathbf{b} \in B\}$ is at least $\min\{|A|, |B|\}$. This translates to finding a lower bound for the order of $\{ab/\gcd(a, b)^2 : a \in A, b \in B\}$ where A and B are sets of distinct positive integers.

Probably even more difficult would be to find a good lower bound for the order of $\{a/\gcd(a, b), b/\gcd(a, b) : a \in A, b \in B\}$. Generalizing Graham's Conjecture, we conjecture that the largest element of this set is $\geq \min\{|A|, |B|\}$ (the authors of [3] have informed us that they retract the claim at the end of the introduction to [3], which would have implied this conjecture).

ACKNOWLEDGMENT. We thank Seva Lev and Carl Pomerance for their helpful comments, and Sudakov for communicating his proof of Theorem 1.

REFERENCES

1. N. Alon, M. Nathanson, and I. Ruzsa, Adding distinct congruence classes modulo a prime, *J. Number Theory* **102** (1995) 250–255.
2. Y. Bilu, Addition of sets of integers of positive density, *J. Number Theory* **64** (1997) 233–275.
3. R. Balasubramanian and K. Soundararajan, On a conjecture of R. L. Graham, *Acta Arith.* **75** (1996) 1–38.
4. P. Erdős, On sets of distances of n points, *Amer. Math. Monthly* **53** (1946) 248–250.
5. G. Freiman, Foundations of a structural theory of set addition, *Transl. Math. Monographs* **37** (1973).
6. V. Lev, Structure theorem for multiple addition and the Frobenius problem, *J. Number Theory* **58** (1996) 79–88.
7. I. Z. Ruzsa, Sets of sums and differences, *Sém. Théorie Nombres Paris* (1984) 267–273.
8. I. Z. Ruzsa, On the number of sums and differences, *Acta Math. Hung* **59** (1992) 439–447.
9. I. Z. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.* **65** (1994) 379–388.
10. M. Szegedy, The solution of Graham's greatest common divisor problem, *Combinatorica* **6** (1986) 67–71.
11. L. A. Székely, Crossing numbers and hard Erdős problems in discrete geometry, *Combin. Probab. Comput.* **6** (1997) 353–358.
12. A. Zaharescu, On a conjecture of Graham, *J. Number Theory* **27** (1987) 33–40.
13. W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, *Geom. Funct. Anal.* **8** (1998) 529–551.

ANDREW GRANVILLE is the Barrow Professor of Mathematics at the University of Georgia. He is a regular contributor to the MONTHLY, and was a recipient of the MAA's Hasse prize in 1995. His main research is in number theory and related topics.
University of Georgia, Athens, Georgia 30602-7403
andrew@math.uga.edu

FRIEDRICH ROESLER Harvard class of '68, was born in Saxony at the end of the second world war. He studied in Münster (Germany), Cambridge, and London and received his Ph.D. from the University of Münster. Since 1983 he has been a professor of mathematics at the Technical University of Munich. His current research interests lie in number theory and algebra,
Zentrum Mathematik der Technischen Universität München, Arcisstrasse 21, 80290 München, Germany
roesler@mathematik.tu-muenchen.de