ACTA ARITHMETICA
LXXII.4 (1995)

Solving a linear equation in a set of integers II

by

Imre Z. Ruzsa (Budapest)

1. Introduction. We continue the study of linear equations started in Part I of this paper.

Let $(a_i)_{1\le i\le k}$ and b be integers. We try to solve the equation

$$a_1x_1 + \ldots + a_kx_k = b \tag{1.1}$$

with $x_1, \ldots, x_k$ in a prescribed set of integers.

We saw that the vanishing of the constant term b and the sum of coefficients $s = a_1 + \ldots + a_k$ had a strong effect on the behaviour of equation (1.1). The condition $b = 0$ is equivalent to homogeneity or multiplication invariance (if $x_1, \ldots, x_k$ is a solution, so is $tx_1, \ldots, tx_k$), while $s = 0$ means translation invariance (if $x_1, \ldots, x_k$ is a solution, so is $x_1 + t, \ldots, x_k + t$). We called equations with $b = s = 0$ *invariant*, and those with $b \ne 0$ or $s \ne 0$ *noninvariant*.

In Part I of the paper we studied invariant equations; now we treat noninvariant ones. We recall the principal notations.

Definition 1.1. Let

$$r(N) = \max\{|\mathcal{A}| : \mathcal{A} \subset [1, N]\}$$

over sets $\mathcal{A}$ such that equation (1.1) has no nontrivial solution with $x_i \in \mathcal{A}$, and let $R(N)$ be the analogous maximum over sets such that equation (1.1) has no solution with distinct integers $x_i \in \mathcal{A}$.

"Trivial" and "nontrivial" solutions were also defined in Part I; we recall that only invariant equations have trivial solutions, so in the noninvariant case $r(N)$ is simply the size of the maximal subset of $\{1, \ldots, N\}$ without a solution.

The vanishing of b and s affect the behaviour of $r(N)$. The following result can be considered as known.

Supported by Hungarian National Foundation for Scientific Research, Grant No. 1901.

Theorem 1.2. *If $b = s = 0$, then*

$$r(N) \le R(N) = o(N). \tag{1.2}$$

On the other hand, if $b \ne 0$ or $s \ne 0$, then $r(N) > \lambda N$ with some $\lambda > 0$ for all N large enough.

(1.2) can be proved with Roth's method, and it also follows immediately from the famous theorem of Szemerédi (1975) on arithmetical progressions. One can also adapt the methods of Heath–Brown (1987) and Szemerédi (1990) to obtain

$$r(N) \le R(N) \ll N(\log N)^{-\alpha} \tag{1.3}$$

with a positive constant α depending on the coefficients $a_1, \ldots, a_k$. The fact that $r(N) \gg N$ if $b = 0$ and $s \ne 0$ is stated by Komlós, Sulyok and Szemerédi (1975), and was known probably long before that.

Noninvariant equations have drawn little attention so far. The estimate $r(N) \gg N$ is easy, but there remain many nontrivial unsolved problems. We list what we think are the most important problems and give partial solutions. Besides, in the last two sections we give a new proof of the theorem of Komlós, Sulyok and Szemerédi (1975) on systems of linear equations in an arbitrary set. While this concerns invariant equations as well, we include it here because of the common method applied to it and to several problems on noninvariant equations.

Notation. Sets of integers will be denoted by script letters. If a letter, say $\mathcal{A}$, denotes a set, the corresponding Roman letter is used to denote its counting function without any further explanation, so that

$$A(N) = |\mathcal{A} \cap [1, N]|.$$

2. Bounds for $r(N)$. We consider the general equation

$$a_1x_1 + \ldots + a_kx_k = b, \tag{2.1}$$

where now either $b \ne 0$ or $s = a_1 + \ldots + a_k \ne 0$.

Define

$$\lambda_0 = \limsup \frac{r(N)}{N}, \qquad \lambda_1 = \liminf \frac{r(N)}{N}.$$

One can also consider infinite sets. Write

$$\lambda_2 = \sup \overline{d}(\mathcal{A}), \qquad \lambda_3 = \sup \underline{d}(\mathcal{A}), \qquad \lambda_4 = \sup d(\mathcal{A}),$$

where $\overline{d}$, $\underline{d}$ and d denote upper density, lower density and asymptotic density, and $\mathcal{A}$ runs over sets of positive integers in which (2.1) has no solution; in the definition of λ_4 only sets having an asymptotic density are considered.

We have obviously

$$1 \ge \lambda_0 \ge \left\{ \begin{matrix} \lambda_1 \\ \lambda_2 \end{matrix} \right\} \ge \lambda_3 \ge \lambda_4 \ge 0. \tag{2.2}$$

Our main project is to find estimates for these quantities.

THEOREM 2.1. *Let q be the smallest positive integer that does not divide* $\gcd(s,b)$. *Further, write*

$$S = \sum |a_i|.$$

We have

$$\lambda_4 \ge \lambda = \max(q^{-1}, S^{-1}, (2k)^{-k}). \tag{2.3}$$

Remark 2.2. From the three bounds given in (2.3), the first is better than the second whenever $s \ne 0$. (The prime number theorem implies that $q \ll \log |s|$.) The third has the remarkable property that it does not depend on the coefficients, only on the number of unknowns.

Proof of Theorem 2.1. First we show that $\lambda_4 \ge 1/q$. Since $q \nmid (s,b)$, at least one of the divisibilities $q \mid b$ and $q \mid s-b$ fails. Choose $t = 0$ or 1 so that $q \nmid ts - b$. Equation (2.1) has no solution within the set

$$\mathcal{A} = \{n : n \equiv t \pmod{q}\}$$

which satisfies $d(\mathcal{A}) = 1/q$.

We prove the second and third inequalities together.

Take positive numbers $\delta_1, \ldots, \delta_k$ such that

$$\delta_1 + \ldots + \delta_k = 1/2,$$

and let $U \subset [0,1)$ be the set of numbers $0 \le u < 1$ satisfying

$$\|ua_i\| < \delta_i, \qquad i = 1, \ldots, k.$$

($\|t\|$ is the distance of t from the nearest integer.) U is a very simple set, a union of finitely many intervals.

We prove that $\lambda_4 \ge \mu(U)$, where μ denotes measure. To this end let α, β be real numbers satisfying

$$\alpha b + \beta s = 1/2, \tag{2.4}$$

and put

$$\mathcal{A} = \{n : \{\alpha n + \beta\} \in U\}.$$

Here $\{x\}$ denotes the fractional part of x.

If α is irrational, then from the uniform distribution of αn modulo 1 we infer that $d(\mathcal{A}) = \mu(U)$. If $s \ne 0$, then we can fix the value of α at any irrational number and then choose β to satisfy (2.4).

If $s = 0$, then the above argument does not work, and (2.4) is equivalent to $\alpha b = 1/2$. Without restricting generality we may assume that $b > 0$.

The value $\alpha = 1/(2b)$ is fixed, and the set $\mathcal{A}$ is determined by β. It will be a union of certain residue classes modulo $2b$; let $f(\beta)$ denote the number of these classes. We have

$$f(\beta) = \sum_{j=1}^{2b} f_j(\beta),$$

where $f_j(\beta) = 1$ if $\{\alpha j + \beta\} \in U$ and 0 otherwise. We have

$$\int_0^1 f_j(\beta)\, d\beta = \mu(U),$$

hence

$$\int_0^1 f(\beta)\, d\beta = 2b\mu(U).$$

Thus for a suitable value of β we have

$$d(\mathcal{A}) = f(\beta)/(2b) \ge \mu(U).$$

Now we show that the equation has no solution in $\mathcal{A}$. Suppose that $x_1, \dots, x_k \in \mathcal{A}$ form a solution. By definition we have

$$\|a_i(\alpha x_i + \beta)\| < \delta_i,$$

hence

$$\Big\| \sum a_i(\alpha x_i + \beta) \Big\| < \sum \delta_i = 1/2.$$

On the other hand,

$$\sum a_i(\alpha x_i + \beta) = \alpha \sum a_i x_i + \beta \sum a_i = \alpha b + \beta s = 1/2,$$

a contradiction.

We have yet to estimate $\mu(U)$. A possible choice of the numbers δ_i is

$$\delta_i = \frac{|a_i|}{2S},$$

and in this case U contains the interval $(-1/(2S), 1/(2S))$ modulo one, hence $\mu(U) \ge 1/S$.

To prove the third estimate in (2.3) we put $\delta_i = 1/(2k)$ for all i. To estimate $\mu(U)$ consider the map

$$x \to (\{a_1 x\}, \dots, \{a_k x\})$$

from $[0,1)$ to $[0,1)^k$. Divide the set $[0,1)^k$ into $(2k)^k$ cubes of side $1/(2k)$. Via the above map, this induces a division of $[0,1)$ into $(2k)^k$ parts. At least one of these parts, say V, satisfies $\mu(V) \ge (2k)^{-k}$. Take an arbitrary $v \in V$. The set $V - v$ modulo 1 is a part of U, hence

$$\mu(U) \ge \mu(V) \ge (2k)^{-k}. \ \blacksquare$$

PROBLEM 2.3. Decide the cases of equality in (2.2).

It seems safe to conjecture that always $\lambda_0 = \lambda_1$, that is, the limit $\lim r(N)/N$ exists. If $s = 0$, then the equation is translation invariant, hence $r(N)$ is subadditive, which immediately implies the existence of this limit. In general, we cannot solve this innocent-looking problem.

STATEMENT 2.4. *If either all coefficients a_i are of the same sign, or* $\gcd(a_1, \ldots, a_k)$ *does not divide b, then $\lambda_0 = \ldots = \lambda_4 = 1$, otherwise $\lambda_0 < 1$.*

Proof. If all coefficients a_i are of the same sign, then there are no solutions in the set (M, ∞) for a suitable M. If $\gcd(a_1, \ldots, a_k)$ does not divide b, then there are no solutions at all.

Assume now that $(a_1, \ldots, a_k) \mid b$. This implies that there are (signed) integers $X_1, \ldots, X_k$ that form a solution of the equation. If there are both positive and negative coefficients, then there are positive integers $y_1, \ldots, y_k$ that satisfy

$$a_1 y_1 + \ldots + a_k y_k = 0.$$

The numbers $x_i = X_i + t y_i$ form a solution of the equation and they are positive for $t > t_0$. Write $X = \max X_i$ and $Y = \max y_i$.

Consider now a set $\mathcal{A} \subset [1, N]$ without solution. For each integer t with $t_0 < t < (N - X)/Y$, the numbers $X_i + t y_i$ are in $[1, N]$ and at least one is missing from $\mathcal{A}$. One missing element is counted at most k times, and consequently we have

$$|\mathcal{A}| \le N - \frac{1}{k}\left(\frac{N - X}{Y} - t_0\right),$$

which implies

$$\lambda_0 \le 1 - \frac{1}{kY} < 1. \ \blacksquare$$

Next we show that λ_0 cannot be bounded from below by a positive absolute constant.

THEOREM 2.5. *Consider the equation in $2k$ variables*

$$(x_1 - y_1) + 2(x_2 - y_2) + \ldots + 2^{k-1}(x_k - y_k) = b, \tag{2.5}$$

where the integer b is of the form

$$b = \operatorname{lcm}[1, \ldots, m] < 2^k. \tag{2.6}$$

This equation satisfies $r(N) \le N/m$; with the maximal possible choice of m we have $r(N) \le 2N/k$.

Proof. Let d be the smallest difference between consecutive terms of a set $\mathcal{A}$, say $d = x - y$, $x, y \in \mathcal{A}$. If $d > m$, then $|\mathcal{A}| < N/m$ for $N > m$.

Assume that $d \le m$; we show that equation (2.5) has a solution in $\mathcal{A}$. Write $u = b/d$; by the assumptions on b, u is an integer and $1 \le u < 2^k$. Let

$$u = \sum_{i=0}^{k-1} e_i 2^i, \qquad e_i = 0 \text{ or } 1,$$

be the binary representation of u. Let $y_i = y$ for all i, $x_i = x$ if $e_i = 1$ and $x_i = y$ if $e_i = 0$; this is a solution of (2.5).

The estimation $m \ge k/2$ follows from Chebyshev's estimate on primes and the prime number theorem yields $m \sim \log 2^k = (\log 2)k$. ∎

Problem 2.6. Find an equation with small λ_0 and $s \ne 0$.

Let

$$s^+ = \sum_{a_i > 0} a_i, \qquad s^- = \sum_{a_i < 0} |a_i|.$$

Without restricting generality we may assume that $s^+ \ge s^-$. By considering the integers in the interval

$$\left(\frac{s^-}{s^+} N, N \right]$$

we obtain

$$\lambda_1 \ge \frac{s^+ - s^-}{s^+}.$$

For an integer $m > 1$, let $\varrho(m)$ denote the maximal cardinality of a set $\mathcal{B}$ of residue classes modulo m such that the congruence

$$a_1 x_1 + \ldots + a_k x_k \equiv b \pmod m \tag{2.7}$$

has no solution with $x_i \in \mathcal{B}$, and put

$$\varrho = \sup \frac{\varrho(m)}{m}. \tag{2.8}$$

By considering the set of integers satisfying $a \equiv u \pmod m$ for some $u \in \mathcal{B}$ we see that $\lambda_1 \ge \varrho(m)$ for any m, thus $\lambda_1 \ge \varrho$.

Problem 2.7. Is it true that always

$$\lambda_0 = \lambda_1 = \max\left(\varrho, \frac{s^+ - s^-}{s^+} \right) ?$$

Problem 2.8. When is the supremum in (2.8) a maximum?

It may not be, as the following example shows. Consider the equation $x = 2y$. We show that $\varrho(m) \le (2m-1)/3$. Let $\mathcal{B}$ be a set such that congruence (2.4) has no solution in $\mathcal{B}$, $|\mathcal{B}| = l$. For each $x \in \mathcal{B}$ consider the residues $2x$. These lie outside $\mathcal{B}$ and each $z \notin \mathcal{B}$ has at most two representations in this form. Furthermore, $0 \notin \mathcal{B}$, and the residue 0 has only one representation in the form $0 = 2y$, $y \in \mathcal{B}$, because one of the at most two solutions is 0 itself. This yields $l \le 2(m-l)-1$ or $l \le (2m-1)/3$, as claimed. Now by considering $m = 2^{2q+1}$ and the set of residues in the form $2^{2i}(2j+1)$, $0 \le i \le q$, we see that $\varrho(m) \ge (2m-1)/3$ for these values of m, and consequently $\varrho = 2/3$.

Recall that we defined

$$R(N) = \max |\mathcal{A}|$$

over sets $\mathcal{A} \subset [1, N]$ of integers such that equation (2.1) has no solution with *distinct* numbers $x_i \in \mathcal{A}$. In Section 3 of Part I we saw that the behaviour of $r(N)$ and $R(N)$ can be very different in the invariant case. We think that this does not happen for noninvariant equations.

Conjecture 2.9. We always have

$$R(N) = r(N) + o(N).$$

Any lower bound for $r(N)$ automatically yields a lower bound for $R(N)$. In the only nontrivial upper bound we gave, in Theorem 2.5, we can prove only a weaker bound for $R(N)$ with a modification of the method.

3. Infinite sets. For Sidon's equation ($x + y = u + v$), the problems for finite and infinite sets behave very differently. In the noninvariant case the difference is less dramatic but still does exist.

λ_1 and λ_2 may be different. Consider, for instance, the equation $x = y + az$ with an integer $a > 1$. This equation has no solution in the interval

$$\left(\frac{N}{a+1}, N\right],$$

hence $\lambda_1 \ge a/(a+1)$ (one can show that $\lambda_0 = \lambda_1 = a/(a+1)$). On the other hand, we have $\lambda_2 \le 1/2$. Indeed, let $\mathcal{A}$ be a set without solution. Fix any number $d \in \mathcal{A}$. There are no integers $x, y \in \mathcal{A}$ satisfying $x - y = ad$, that is, the sets $\mathcal{A}$ and $\mathcal{A} + ad$ are disjoint. This implies $2A(N) \le N + ad$, whence $\lambda_2 \le 1/2$. (If a is odd, then $\lambda_2 = \lambda_3 = \lambda_4 = 1/2$ follows from the previous observation and Theorem 2.1.)

Problem 3.1. Is there an absolute constant C such that we always have $\lambda_2 \ge C\lambda_1$?

The quantity ϱ was defined in (2.8). We have obviously $\lambda_4 \ge \varrho$.

Problem 3.2. Is it true that always $\lambda_2 = \lambda_3 = \lambda_4 = \varrho$?

If $s = 0$, then the equality of the λ_i's can be asserted.

Theorem 3.3. *If $s = 0$ and $b \ne 0$, then $\lambda_0 = \lambda_1 = \lambda_2 = \lambda_3 = \lambda_4$.*

Proof. The proof is based on translating and combining solution-free sets. There are several ways to express this idea, a popular one applies compactness in the space $\{0,1\}^{\mathbb{Z}}$. We use the method developed in Ruzsa (1978). We recall some concepts and results from this paper.

By a *homogeneous system* we mean a collection $\mathbf{H}$ of finite sets of integers such that for every $A \in \mathbf{H}$ all the subsets and translates of A belong to $\mathbf{H}$ as well. The *counting function* of a homogeneous system $\mathbf{H}$ is defined as

$$H(x) = \max_{A\in\mathbf{H}} |A \cap [1,x]|.$$

The *density* of $\mathbf{H}$ is the limit

$$d(\mathbf{H}) = \lim_{x\to\infty} H(x)/x,$$

which always exists.

Lemma 3.4. *For an arbitrary homogeneous system* $\mathbf{H}$ *there is a set* A *of positive integers such that* A *has asymptotic density*, $d(A) = d(\mathbf{H})$ *and every translate of every finite subset of* A *belongs to* $\mathbf{H}$.

This is Theorem 4 of Ruzsa (1978).

Now let $\mathbf{S}$ be the collection of all finite sets of integers in which (2.1) has no solution. Then $\mathbf{S}$ is a homogeneous system and its density is λ_0. By the lemma above, there is a set $\mathcal{A}$ of density $d(\mathcal{A}) = d(\mathbf{S}) = \lambda_0$ such that all finite subsets of $\mathcal{A}$ belong to $\mathbf{S}$. This is equivalent to saying that equation (2.1) has no solution in $\mathcal{A}$, hence $\lambda_4 = \lambda_0$. The other equalities follow from the obvious inequalities listed in (2.2). ∎

The case $s \neq 0$, when there is no obvious connection between values of $r(n)$, may be more difficult.

4. Equations in a general set.

Besides solutions of an equation

$$a_1x_1 + \ldots + a_kx_k = b \tag{4.1}$$

in a subset of the first N integers, one can ask about solution-free subsets of an arbitrary set.

Definition 4.1. We define $r'(N)$ as the largest number m with the following property: every set $\mathcal{B}$ of N integers contains a subset $\mathcal{A} \subset \mathcal{B}$ of m elements such that equation (4.1) has no nontrivial solution in $\mathcal{A}$. We define $R'(N)$ similarly, admitting only solutions with k distinct integers x_j.

We have obviously $r'(N) \le r(N)$ and $R'(N) \le R(N)$. Komlós, Sulyok and Szemerédi (1975) proved that in both cases the difference is at most a constant factor. In this section we give a different proof of their result, based on ideas similar to that of Theorem 2.1. This also leads to an improvement in the values of the constants.

We consider the invariant and noninvariant cases separately. In the noninvariant case we know that $r(N) \gg N$ (Theorem 2.1), and instead of comparing $r'(N)$ and $r(N)$ we shall estimate $r'(N)$ directly. We prove essentially the same lower bound for $r'(N)$ as we did for $r(N)$ in Theorem 2.1.

We write

$$s = \sum a_i, \qquad S = \sum |a_i|, \qquad \lambda = \max(S^{-1}, (2k)^{-k}). \tag{4.2}$$

THEOREM 4.2. *Assume that either $b \ne 0$ or $\sum a_i \ne 0$. With the number λ of* (4.2) *we have $r'(N) \ge \lambda(N-1)$ for every N.*

Proof. We define U as in the proof of Theorem 2.1, take two reals satisfying (2.4) and define $\mathcal{A}$ by

$$\mathcal{A} = \{n \in \mathcal{B} : \{\alpha n + \beta\} \in U\}.$$

The same argument yields that equation (4.1) has no solution in $\mathcal{A}$. We need to estimate $|\mathcal{A}|$.

If $s \ne 0$, we can rewrite (2.4) as

$$\beta = \frac{1}{2s} - \frac{\alpha b}{s},$$

therefore

$$\alpha n + \beta = \gamma(sn - b) + \frac{1}{2s}, \tag{4.3}$$

where $\gamma = \alpha/s$. The set $\mathcal{A}$ is determined uniquely by γ; write $|\mathcal{A}| = f(\gamma)$. We have

$$f(\gamma) = \sum_{n \in \mathcal{B}} f_n(\gamma),$$

where $f_n(\gamma) = 1$ if $\gamma(sn-b)+1/(2s) \in U$ and 0 otherwise. For a fixed $n \in \mathcal{B}$ the measure of those $\gamma \in [0,1)$ for which this condition holds is equal to $\mu(U)$ unless $sn - b = 0$, that is, with at most one exception. Consequently,

$$\int_0^1 f(\gamma)\, d\gamma \ge \mu(U)(N-1),$$

so with a suitable selection of γ we have

$$|\mathcal{A}| = f(\gamma) \ge \mu(U)(N-1) \ge \lambda(N-1)$$

as claimed.

If $s = 0$, then we fix $\alpha = 1/(2b)$ and obtain the same result by averaging in β, as we did in the proof of Theorem 2.1. ∎

Since the four numbers $r(N)$, $r'(N)$, $R(N)$ and $R'(N)$ are all between $\lambda(N-1)$ and N, they have the same order of magnitude. For invariant equations the order of magnitude of these quantities is unknown but a comparison is possible even in a more general situation. Instead of a single equation we consider a system of equations

$$a_{j1}x_1 + \ldots + a_{jk}x_k = 0, \qquad j = 1, \ldots, J, \tag{4.4}$$

with integral coefficients a_{ji}. We assume that the system is invariant, that is,

$$\sum_{i=1}^{k} a_{ji} = 0$$

for every $1 \le j \le J$.

We generalize the concept of a nontrivial solution as follows. For every k-tuple $x_1, \ldots, x_k$ of integers we define its *coincidence matrix* as the $k \times k$ matrix (δ_{ij}) in which $\delta_{ij} = 1$ if $x_i = x_j$ and 0 otherwise. Now assume that a subset $\varDelta$ of all $n \times n$ 0-1 matrices is given. We call a solution *admissible* if its coincidence matrix belongs to $\varDelta$. If $\varDelta$ has only one element, the identity matrix, we get the notion of solutions with different values of the unknowns. It is natural, but not necessary, to assume that the identity matrix belongs to $\varDelta$.

Definition 4.3. Let a system (4.4) of equations and a set $\varDelta$ of $n \times n$ 0-1 matrices be given. We define $r(N)$ as the maximal cardinality of a set $\mathcal{A} \subset [1, N]$ of integers such that the system (4.4) has no solution with $x_i \in \mathcal{A}$ whose coincidence matrix belongs to $\varDelta$. We define $r'(N)$ as the maximal integer m with the property that every set $\mathcal{B}$ of integers, $|\mathcal{B}| = N$, contains a subset $\mathcal{A}$ with $|\mathcal{A}| = m$, such that the system (4.4) has no solution with $x_i \in \mathcal{A}$ whose coincidence matrix belongs to $\varDelta$.

Write

$$S = \max_j \sum_{i=1}^{k} |a_{ji}|.$$

Theorem 4.4. *For every system of equations and every set $\varDelta$ of admissible coincidence matrices we have*

$$r'(N) \ge \frac{4}{S^2 + 4} r(N). \tag{4.5}$$

Proof. Take a set $\mathcal{A}^* \subset [1, N]$ such that $|\mathcal{A}^*| = r(N)$ and (4.4) has no admissible solution in $\mathcal{A}^*$. We put $\varepsilon = 1/S$ and $m = NS/2$. (S is even, since $\sum_i a_{ji} = 0$, thus m is an integer.) We define the set U as

$$U = \bigcup_{y \in \mathcal{A}^*} \left(\frac{y - \varepsilon}{m}, \frac{y + \varepsilon}{m} \right) = \bigcup I_y.$$

We take two real numbers α and β and define a set $\mathcal{A} \subset \mathcal{B}$ as follows. If for any $y \in \mathcal{A}^*$ there is an $n \in \mathcal{B}$ such that $\{\alpha n + \beta\} \in I_y$, then we put one of these numbers n (say, the smallest) into $\mathcal{A}$. We have definitely

$$\mathcal{A} \subset \mathcal{A}' = \{n \in \mathcal{B} : \{\alpha n + \beta\} \in U\}.$$

We show that (4.4) has no admissible solution in $\mathcal{A}$. Assume that $x_1, \ldots, x_k$ is a solution. We have

$$\alpha x_i + \beta = z_i + \frac{y_i + \varepsilon_i}{m}, \tag{4.6}$$

where $|\varepsilon_i| < \varepsilon$, $y_i \in \mathcal{A}^*$ and the z_i's are integers. Moreover, since we selected only one $n \in \mathcal{B}$ for each interval, the coincidence matrix of $y_1, \ldots, y_k$ is the same as that of $x_1, \ldots, x_k$.

Equation (4.6) implies that

$$\sum a_{ji}\left(z_i + \frac{y_i + \varepsilon_i}{m}\right) = 0$$

for every j. Multiplying this equation by m we see that $\sum a_{ji}\varepsilon_i$ must be an integer. Since this number is less in absolute value than

$$\varepsilon \sum |a_{ji}| \le \varepsilon S = 1,$$

its value is 0. We conclude that

$$\sum a_{ji}\left(z_i + \frac{y_i}{m}\right) = 0.$$

This shows that $\sum a_{ji}y_i/m$ is always an integer. Since $\sum_i a_{ji} = 0$, we have

$$\left|\sum a_{ji}y_i\right| = \left|\sum a_{ji}\left(y_i - \frac{N+1}{2}\right)\right| \le S\frac{N-1}{2}.$$

Hence

$$\left|\sum a_{ji}y_i/m\right| \le S\frac{(N-1)/2}{m} < 1,$$

and consequently its value is 0. We proved that $y_1, \ldots, y_k$ also forms a solution, a contradiction.

We now estimate $|\mathcal{A}|$. Write $|\mathcal{A}| = f(\alpha, \beta)$, $|\mathcal{A}'| = g(\alpha, \beta)$. Finally, let $h(\alpha, \beta)$ be the number of those pairs (n, n'), $n, n' \in \mathcal{B}$, for which $\{\alpha n + \beta\}$ and $\{\alpha n' + \beta\}$ are in a common interval I_y, $y \in \mathcal{A}^*$.

It is easy to compute an average of g. We have $g(\alpha, \beta) = \sum_{n \in \mathcal{B}} g_n(\alpha, \beta)$, where $g_n(\alpha, \beta) = 1$ if $\{\alpha n + \beta\} \in U$ and 0 otherwise. Now we have $\int_0^1 g_n(\alpha, \beta)\, d\beta = \mu(U)$ for every n and α, and consequently

$$\int_0^1 \int_0^1 g(\alpha, \beta)\, d\alpha\, d\beta = N\mu(U).$$

One can hope that if the numbers $\{\alpha n + \beta\}$ do not often lie in the same I_y, that is, h is not too big, then f is not much smaller than g. An exact expression is the following. Let $\phi_y = \phi_y(\alpha, \beta)$ denote the number of integers $n \in \mathcal{B}$ such that $\{\alpha n + \beta\} \in I_y$. We have

$$f = \sum_{\phi_y \neq 0} 1, \qquad g = \sum \phi_y, \qquad h = \sum \phi_y^2,$$

and the inequality of arithmetic and square means yields

$$g(\alpha, \beta)^2 \le f(\alpha, \beta) h(\alpha, \beta).$$

By integrating this inequality we obtain

$$\begin{aligned}\int_0^1\int_0^1 g(\alpha,\beta)^2\,d\alpha\,d\beta &\le \int_0^1\int_0^1 h(\alpha,\beta) f(\alpha,\beta)\,d\alpha\,d\beta \\ &\le \max f \cdot \int_0^1\int_0^1 h(\alpha,\beta)\,d\alpha\,d\beta.\end{aligned}$$

We also know that

$$\int_0^1\int_0^1 g(\alpha,\beta)^2\,d\alpha\,d\beta \ge \Big(\int_0^1\int_0^1 g(\alpha,\beta)\,d\alpha\,d\beta\Big)^2 = N^2\mu(U)^2.$$

Combining these inequalities we find

$$\max f(\alpha,\beta) \ge \frac{N^2\mu(U)^2}{\int_0^1\int_0^1 h(\alpha,\beta)\,d\alpha\,d\beta}. \tag{4.7}$$

Our next task is to estimate the integral of h.

We can express h as

$$h(\alpha,\beta) = \sum h_{nn'}(\alpha,\beta),$$

where $h_{nn'}(\alpha,\beta) = 1$ if $\{\alpha n + \beta\}$ and $\{\alpha n' + \beta\}$ are in a common interval I_y, and 0 otherwise. They can be in the same I_y only if $\|\alpha(n-n')\| \le 2\varepsilon/m$, and consequently we have

$$\int_0^1 h_{nn'}(\alpha,\beta)\,d\beta \le \begin{cases} 0 & \text{if } \|\alpha(n-n')\| > 2\varepsilon/m, \\ \mu(U) & \text{otherwise.}\end{cases} \tag{4.8}$$

The measure of those α for which the condition $\|\alpha(n-n')\| \le 2\varepsilon/m$ holds is 1 if $n = n'$ and $2\varepsilon/m$ if $n \neq n'$, thus (4.8) implies

$$\int_0^1\int_0^1 h_{nn'}(\alpha,\beta)\,d\alpha\,d\beta \le \begin{cases} \mu(U) & \text{if } n = n', \\ 2\varepsilon\mu(U)/m & \text{if } n \neq n'.\end{cases}$$

On summing these estimates we obtain

$$\int_0^1\int_0^1 h(\alpha,\beta)\,d\alpha\,d\beta \le N\mu(U)+N(N-1)\frac{2\varepsilon\mu(U)}{m} \le N\mu(U)(1+2\varepsilon N/m).$$

Substituting this estimate into (4.7) we get

$$\max f(\alpha,\beta) \ge \frac{N\mu(U)}{1+2\varepsilon N/m}.$$

In view of $\mu(U)=2\varepsilon r(N)/m$, $\varepsilon=1/S$ and $m=NS/2$ this is equivalent to (4.5). ■

References

D. R. Heath-Brown (1987), *Integer sets containing no arithmetic progression*, J. London Math. Soc. 35, 385–394.

J. Komlós, M. Sulyok and E. Szemerédi (1975), *Linear problems in combinatorial number theory*, Acta Math. Hungar. 26, 113–121.

I. Z. Ruzsa (1978), *On difference sets*, Studia Sci. Math. Hungar. 13, 319–326.

I. Z. Ruzsa (1993), *Solving a linear equation in a set of integes I*, Acta Arith. 65, 259–282.

E. Szemerédi (1975), *On sets of integers containing no k elements in arithmetic progression*, ibid. 27, 199–245.

E. Szemerédi (1990), *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. 56, 155–158.

MATHEMATICAL INSTITUTE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST, PF. 127
H-1364 HUNGARY
E-mail: H1140RUZ@ELLA.HU

Received on 18.10.1994
and in revised form on 19.12.1994 (2681)