Linear equations and sets of integers

By

Tomasz Schoen*

Abstract

We prove two results concerning solvability of a linear equation in sets of integers. In particular, it is showed that for every $k \in \mathbb{N}$, there is a noninvariant linear equation in k variables such that if $A \subseteq \{1, \ldots, N\}$ has no solution to the equation then $|A| \le 2^{-ck/(\log k)^2} N$, for some absolute constant $c > 0$, provided that N is large enough.

1. Introduction

Denote by $r(N)$ the maximum size of a subset of $\{1, \ldots, N\}$ having no nontrivial solution (see [4] for rigorous definition of nontrivial solution) to the equation

$$a_1 x_1 + \cdots + a_k x_k = b, \tag{1}$$

and let $R(N)$ be the analogous maximum over sets without solution to (1) with distinct integers x_i. We say that an equation is *invariant* if $s = a_1 + \cdots + a_k = 0$ and $b = 0$, otherwise it is called *noninvariant.* The invariant equation $x - y = 0$ is called *trivial.* The condition $s = b = 0$ strongly affects behavior of $r(N)$ and $R(N)$. It is known [2] that for a nontrivial invariant equation

$$r(N) \leqslant R(N) = o(N) \tag{2}$$

and for noninvariant

$$N \ll r(N) \leqslant R(N).$$

Ruzsa showed [3] that for invariant equations $r(N)$ and $R(N)$ can have different order of magnitude. However, he conjectured [4] that in noninvariant case we always have

$$R(N) = r(N) + o(N). \tag{3}$$

Our first result confirm this conjecture.

Theorem 1 *For every noninariant equation we have $R(N) = r(N) + o(N)$.*

*The author is supported by MNSW grant N N201 543538

Keywords and phrases: linear equations, sets of integers.

2010 Mathematics Subject Classification: primary 11B75, secondary 11P99.

The second result of this note was also motivated by a question stated in [4]. Define

$$\lambda = \limsup \frac{r(N)}{N}$$

In noninvariant case, Ruzsa proved a lower bound for λ, which depends only on the number of unknowns k, namely

$$\lambda \geqslant (2k)^{-k}.$$

We show that there are noninvariant equations, for which the above bound is not far from best possible.

Theorem 2 *For every $k \geqslant 2$ there exists a noninvariant equation in k variables such that $\lambda < 2^{-ck/(\log k)^2}$, for some absolute constant $c > 0$.*

2. Proof of Theorem 1

We will need the following lemma.

Lemma 3 *Let $A \subseteq [N]$ and let*

$$bx = a_1x_1 + \cdots + a_jx_j \tag{4}$$

be a nontrivial invariant equation. Suppose that for every $x \in A$ there are less than k disjoint solutions (i.e. $\{y_1, \ldots, y_j\} \cap \{y'_1, \ldots, y'_j\} = \emptyset$) to the equation (4) with distinct $y_1, \ldots, y_j \in A \backslash \{x\}$. Then $|A| = o(N)$.

P r o o f. Let B be a random subset of A, taking each $x \in A$ independently with probability $p = 1/(2jk)$. For each $x \in A$ we fix $\mathcal{S}_x$, a maximal family of disjoint solutions to (4), so $|\mathcal{S}_x| < k$. Let C be the set of all $x \in B$ such that, if $(y_1, \ldots, y_j) \in \mathcal{S}_x$ then $\{y_1, \ldots, y_j\} \cap B = \emptyset$. By Bernoulii's inequality we have

$$\mathbb{E}(|C|) \geqslant p|A| - p(1 - (1 - p)^j)k|A| \geq p|A| - p^2jk|A| = |A|/(4jk).$$

Thus, there is a subset C' of A of size at least $|A|/(4jk)$ such that for every $x \in C'$ and $(y_1, \ldots, y_j) \in \mathcal{S}_x$ we have $\{y_1, \ldots, y_j\} \cap C' = \emptyset$. We claim that C' is free of solutions to (4) in distinct integers. Indeed, if $(x, y'_1, \ldots, y'_j)$ is a solution to (4) in C', then from the maximality of $\mathcal{S}_x$ it follows that $\{y_1, \ldots, y_j\} \cap \{y'_1, \ldots, y'_j\} \neq \emptyset$ for some $(y_1, \ldots, y_j) \in \mathcal{S}_x$, which is a contradiction. Hence by (2), $|C'| = o(N)$ and the assertion follows. □

P r o o f o f T h e o r e m 1. Suppose that there is a noninvariant equation (1) such that (3) does not hold. Thus, there exists a positive constant c such that for infinitely many N we have

$$R(N) \geqslant r(N) + cN.$$

Let $A \subseteq [N]$ be such that $|A| = R(N) \geqslant r(N) + cN$ and A does not contain any solution with distinct x_i.

Denote by A' the set of all elements $x \in A$, for which every nontrivial invariant equation

$$(a_{i_1} + \dots + a_{i_j})x = a_{i_1}y_1 + \dots + a_{i_j}y_j,$$

$1 \le i_1 < \dots < i_j \le k$, has at least k disjoint solutions with distinct $y_1, \dots, y_j \in A$. By Lemma 3 we have

$$|A'| > r(N),$$

provided that N is large enough, so that there is a solution to $a_1x_1 + \dots + a_kx_k = b$ in A'. By $A' \subseteq A$ some of x_i must be equal. We rearrange the equation in the following way (if necessary renumber the coefficients)

$$(a_1 + \dots + a_{i_1})x_1 + \dots + (a_{i_{n-1}+1} + \dots + a_{i_n})x_n = b, \tag{5}$$

where $x_i \neq x_j$ for $i \neq j$. Possibly, there are expressions of the form $(a_{i_j} + a_{i_j+1})x_j$ with $a_{i_j} = -a_{i_j+1}$ (so they are equal zero). We join all them to another one, which is not of this form corresponding with, say x_u, by replacing all x_j by x_u. Since our equation is noninvariant it is always possible. Finally, we can assume that there are no expressions $(a_{i_j}+a_{i_j+1})x_j$, $a_{i_j} = -a_{i_j+1}$ in (5). For each $1 \leqslant u \leqslant n$ the equation

$$(a_{i_{u-1}+1} + \dots + a_{i_u})x_u = a_{i_{u-1}+1}y_{i_{u-1}+1} + \dots + a_{i_u}y_{i_u}, \tag{6}$$

has at least k disjoint solutions with distinct $y_{i_{u-1}+1}, \dots, y_{i_u} \in A$. Thus, for every $1 \leqslant u \leqslant n$ we can select a solution $y_{i_{u-1}+1}, \dots, y_{i_u}$ in such way that

$$\{y_{i_{u-1}+1}, \dots, y_{i_u}\} \cap \{y_{i_{v-1}+1}, \dots, y_{i_v}\} = \emptyset,$$

for all $1 \leqslant u < v \leqslant n$. Finally, plugging (6) into (5) we obtain $a_1y_1 + \dots + a_ky_k = b$ with distinct integers $y_i \in A$, which is a contradiction. $\square$

3. Equations with small λ

Ruzsa [4] proved the following inequalities

$$\lambda \geqslant \max\{q^{-1}, S^{-1}, (2k)^{-k}\},$$

where q is the smallest positive integer that does not divide $\gcd(s, b)$ and $S = \sum |a_i|$. There are equations, which satisfy equality $\lambda = 1/q$ or $\lambda = 1/S$. It is easy to see that $\lambda = 1/q = 1/2$ for the equation $x + y = z$ and $\lambda = 1/S = 1/2$ for the equation $x - y = 2$. We show that there are equations with λ close to the third bound. Our approach is partially based on the main idea of the proof of Theorem 1 in [5].

The Fourier coefficients of a set $A \subseteq \mathbb{Z}_m$ are defined by

$$\widehat{A}(r) = \sum_{a \in A} e^{-2\pi i r a/m},$$

for every $r \in \mathbb{Z}_m$. Parseval's formula states that $\sum_{r=0}^{m-1} |\widehat{A}(r)|^2 = |A|n$. For a set $T \subseteq \mathbb{Z}$, let $\mathsf{C}(T)$ be the smallest cardinality of a multiset $\Gamma \subseteq \mathbb{R}$ such that

$$T \subseteq \operatorname{Span}(\Gamma) = \Big\{ \sum_{\gamma \in \Gamma} \varepsilon_\gamma \gamma : \varepsilon_\gamma \in \{-1, 0, 1\} \Big\}.$$

In proof of Theorem 2 we will make use of some lemmas. The first one is the well-known result of Chang [1].

Lemma 4 *Let* $A \subseteq \mathbb{Z}_m$, $|A| = \delta m$ *and* $\Lambda = \{r \in \mathbb{Z}_n : |\widehat{A}(r)| \geqslant \varepsilon|A|\}$. *Then there is a set* $\Gamma \subseteq \mathbb{Z}_m$ *such that* $|\Gamma| \ll \varepsilon^{-2}\log(1/\delta)$ *and* $\Lambda \subseteq \mathrm{Span}(\Gamma)$.

Lemma 5 *For every positive integer* t *we have* $\mathsf{C}(\{1,2,\dots,2^t\}) \geqslant (t+1)/\log(2t+3)$.

Proof. Suppose that $\Gamma \subseteq \mathbb{R}$, $|\Gamma| = \mathsf{C}(\{1,2,\dots,2^t\})$ and $\{1,2,\dots,2^t\} \subseteq \mathrm{Span}(\Gamma)$. Since each integer $0 \leqslant n \leqslant 2^{t+1}-1$ can be written as $n = \sum_{i=0}^{t}\varepsilon_i 2^i$, $\varepsilon_i \in \{-1,0,1\}$ it follows that

$$n = \sum_{\gamma\in\Gamma}\varepsilon_\gamma\gamma, \tag{7}$$

for some $\varepsilon_\gamma \in \{0,\pm1,\dots,\pm(t+1)\}$. Thus, there are at least 2^{t+1} distinct sums of the form (7), so that

$$(2t+3)^{|\Gamma|} \geqslant 2^{t+1},$$

hence

$$\mathsf{C}(\{1,2,\dots,2^t\}) \geqslant \frac{t+1}{\log(2t+3)},$$

which completes the proof. □

Denote by $d(A)$ the asymptotic density (if exists) of $A \subseteq \mathbb{N}$. The next lemma was proved in [4].

Lemma 6 *If* $s = 0$ *and* $b \neq 0$, *then*

$$\lambda = \sup d(A),$$

where A *runs over sets of positive integers in which (1) has no solution and* $d(A)$ *exists.*

Proof of Theorem 2. Let $c' > 0$ be a small constant to be specify later. First we consider the case of even $k \geq 6$, write $k = 2l+2$. Let $a_i = 2^i$ for all $i \leqslant t = c'k/(\log k)^2$, $a_{t+1} = \cdots = a_l = 1$ and $b = (2^t)!$. We show that for the equation

$$a_1(x_1-y_1) + \cdots + a_l(x_l-y_l) + (x_{l+1}-y_{l+1}) = b \tag{8}$$

we have $\lambda < 2^{-ck/(\log k)^2}$. By Lemma 6 there exists a set $A \subseteq \mathbb{N}$ having no solution to (8) such that $d(A) \geqslant \lambda/2 > 0$. Hence, by Szemerédi's theorem [6] there are arbitrarily long arithmetic progressions in A. Clearly, for a given $n \in \mathbb{N}$ there exists an arithmetic progression of length at least $2\sum|a_i| + |b| + 1$ and the step at least n in A. Let $d, d+m, \dots, d+Lm$ be such progression. Then $0, \pm m, \dots, \pm Lm \in A - A$ and notice that the congruence

$$a_1(x_1-y_1) + \cdots + a_l(x_l-y_l) \equiv b \pmod m \tag{9}$$

has no solution in $B = A \cap \{1,\dots,m-1\}$. Indeed, if there is a solution $x_i, y_i \in B$ of (9), then

$$a_1(x_1-y_1) + \cdots + a_l(x_l-y_l) = b + jm$$

for some $|j| \leqslant 2\sum|a_i|+|b|$. Thus, $jm \in A-A$, so that

$$a_1(x_1-y_1)+\cdots+a_l(x_l-y_l)+(x_{l+1}-y_{l+1})=b$$

for some $x_{l+1}, y_{l+1} \in A$, which contradicts the choice of A. For m large enough we have $|B| \geqslant (\lambda/3)m$. Thus, to finish the proof it is enough to show that $|B|:=\delta m < 2^{-ck/(\log k)^2}m$. Since B contains no solution to (9) it follows that

$$\sum_{r=0}^{m-1}\prod_{i=1}^{l}|\widehat{B}(a_ir)|^2e^{2\pi irb/m}=0.$$

Therefore

$$-|B|^{2k}=\sum_{r=1}^{m-1}\prod_{i=1}^{l}|\widehat{B}(a_ir)|^2e^{2\pi irb/m} \geqslant -\sum_{\cos(2\pi rb/m)<0}\prod_{i=1}^{l}|\widehat{B}(a_ir)|^2.$$

An important property of $b=(2^t)!$ is that if $\cos(2\pi rb/m)<0$ then $\gcd(r,m)<m/a_l$. Let

$$\prod_{i=1}^{l}|\widehat{B}(a_ir_0)|=\max_{\cos(2\pi rb/m)<0}\prod_{i=1}^{l}|\widehat{B}(a_ir)|,$$

then by Hölder's inequality

$$|B|^{2l} \leqslant \prod_{i=1}^{l}|\widehat{B}(a_ir_0)|^{\frac{2l-2}{l}}\sum_{r=1}^{m-1}\prod_{i=1}^{l}|\widehat{B}(a_ir)|^{2/l} \leqslant \prod_{i=1}^{l}|\widehat{B}(a_ir_0)|^{\frac{2l-2}{l}}\prod_{i=1}^{l}\Big(\sum_{r=1}^{m-1}|\widehat{B}(a_ir)|^2\Big)^{1/l}.$$

By Parseval formula we have

$$\sum_{r=1}^{m-1}|\widehat{B}(a_ir)|^2 \leqslant a_i\sum_{r=0}^{m-1}|\widehat{B}(r)|^2=a_im|B|$$

so that

$$\prod_{i=1}^{l}|\widehat{B}(a_ir_0)| \geqslant \delta^{\frac{l}{2l-2}}|B|^l\prod_i a_i^{-\frac{1}{2l-2}} \geqslant \delta 2^{-t^2/l}|B|^l. \tag{10}$$

Let $\Lambda=\{a_1r_0,\dots,a_lr_0\}$ and $\Lambda'=\{a_ir_0 : |\widehat{B}(a_ir_0)| \geqslant |B|/2\}$, then from (10) it follows that $|\Lambda\setminus\Lambda'| \leqslant \log(1/\delta)+t^2/l$. By Lemma 4 there exists a set $Y \subseteq \mathbb{Z}_m$ such that $|Y| \ll \log(1/\delta)$ and $\Lambda' \subseteq \mathrm{Span}(Y)$. Thus, for $X=Y\cup(\Lambda\setminus\Lambda')$ we have $\Lambda\subseteq\mathrm{Span}(X)$ and $|X| \ll \log(1/\delta)+t^2/l$.

Put $d=\gcd(r_0,m)$ and write $r_0=r_1d$. Furthermore, denote by $0 \leqslant s \leqslant m-1$ the integer such that $r_1s\equiv 1 \pmod m$ and let $(a)_m$ stands for an integer $0 \leqslant h \leqslant m-1$ such that $h \equiv a \pmod m$. As we mentioned before $a_ld<m$. We show that the span of

$$\Gamma=\frac{1}{d}\cdot(s\cdot X)_m\cup\frac{1}{d}\cdot\{m,2m,\dots,2^{\lfloor\log|X|\rfloor}m\}\subseteq\mathbb{R}$$

covers $\{a_1,\dots,a_l\}$. Indeed, for every i there is a choice of $\varepsilon_\gamma\in\{-1,0,1\}$ such that

$$\sum_{\gamma\in X}\varepsilon_\gamma\gamma\equiv a_ir_0 \pmod m,$$

hence

$$\sum_{\gamma\in X}\varepsilon_\gamma s\gamma \equiv a_i d \pmod m.$$

Therefore, for every i, there is an integer n_i and a choice of $\varepsilon_\gamma \in \{-1,0,1\}$ satisfying

$$\sum_{\gamma\in X}\varepsilon_\gamma (s\gamma)_m = a_i d + n_i m.$$

Observe that

$$|n_i| \leqslant \frac{1}{m}\Big|\sum_{\gamma\in X}\varepsilon_\gamma (s\gamma)_m\Big| + \frac{1}{m}|a_i d| \leqslant |X|(m-1)/m + 1 < |X| + 1.$$

Thus, for some $\varepsilon_j \in \{-1,0,1\}$ we have

$$a_i = \frac{1}{d}\sum_{\gamma\in X}\varepsilon_\gamma (s\gamma)_m - \frac{1}{d}n_i m = \sum_{\gamma\in X}\varepsilon_\gamma \frac{1}{d}(s\gamma)_m + \sum_{j=0}^{\lfloor\log|X|\rfloor}\varepsilon_j \frac{1}{d}2^j m,$$

so that $\{a_1,\dots,a_l\} \subseteq \mathrm{Span}(\Gamma)$. However, by Lemma 5, $\mathsf{C}(\{a_1,\dots,a_l\}) \gg t/\log t$, so $|\Gamma| = |X| + \lfloor\log|X|\rfloor + 1 \gg t/\log t$. Hence

$$\log(1/\delta) \gg t/\log t - t^2/k \gg k/(\log k)^2,$$

provided that c' is sufficiently small.

To finish the proof, we need to show the theorem for odd k, write $k = 2l+3 \geqslant 7$. In this case, it is easy to see that the required inequality is satisfied for the equation

$$a_1(x_1-y_1) + \cdots + a_l(x_l-y_l) + (x+y-2z) = b. \qquad \square$$

References

[1] M.-C. Chang, Polynomial bounds in Freiman's theorem, *Duke Math. J.,* **113** (2002), 399–419.

[2] K. F. Roth, On certain sets of integers, *J. London Math. Soc.,* **28** (1953), 104–109.

[3] I. Z. Ruzsa, Solving linear equations in sets of integers. I, *Acta Arith.,* **65** (1993), 259–282.

[4] I. Z. Ruzsa, Solving linear equations in sets of integers. II, *Acta Arith.,* **72** (1995), 385–397.

[5] T. Schoen, Linear equations in $\mathbb{Z}_p$, *Bull. London Math. Soc.,* **37** (2005), 495–501.

[6] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arth.,* **27** (1975), 199–245.

Faculty of Mathematics and Computer Science,
Adam Mickiewicz University,
Umultowska 87, 61-614 Poznań, Poland
schoen@amu.edu.pl