Maximal subsets free of arithmetic progressions in arbitrary sets *

Semchankau Aliaksei

October 12, 2020

Abstract

We consider the problem of determining the maximum cardinality of a subset containing no arithmetic progressions of length \( k \) in a given set of size \( n \). It is proved that it is sufficient, in a certain sense, to consider the interval \([1, \ldots, n]\). The study continues the work of Komlós, Sulyok, and Szemerédi.

1 Introduction

Let us consider an arbitrary set \( B \subseteq \mathbb{Z} \) and integer \( k \geq 3 \). We define the value \( f_k(B) \) to be the cardinality of maximal subset of \( B \), which does not contain nontrivial arithmetical progression of length \( k \) (we say arithmetical progression is trivial if all of its elements are equal). Let us consider the function

\[
\phi_k(n) := \min_{|B|=n} f_k(B).
\]

Now we introduce the function \( g_k(n) := f_k([1, 2, \ldots, n]) \). Let \( \rho_k(n) := g_k(n)/n \) be a density of maximal set free of arithmetical progressions of length \( k \) in segment \([1, \ldots, n]\). We know following estimates for \( \rho_k(n) \):

\[
\frac{1}{c_k \sqrt{\ln n}} \ll \rho_k(n) \ll \frac{1}{(\ln \ln n)^{s_k}},
\]

where \( c_k, s_k \) are positive constants, depending only on \( k \). Lower bound belongs to Behrend [Beh46], and upper bound belongs to Gowers [Gow01]. Historical retrospective on special case \( k = 3 \) can be found in works [Shk06], [Blo12].

At first sight it seems natural to expect the equality \( \phi_k(n) = g_k(n) \) to hold, although it turns out to be false already for \( n = 5, k = 3 \): \( g_3(5) = f_3([1, 2, 3, 4, 5]) = 4 > 3 = f_3(\{1, 2, 3, 4, 7\}) = \phi_3(5) \). However, intuition still predicts that \( \phi_k(n) \) does not differ much from \( g_k(n) \). In this direction it was proved by Komlós, Sulyok, and Szemerédi [KSS75] that following inequality holds:

\[
\phi_3(n) > (1/2^{15} + o(1))g_3(n), n \to \infty.
\]

*This work is supported by the Russian Science Foundation under grant 14-11-00433.
In O’Bryant’s work [OBr13] it is stated, without proof, that constant $1/2^{15}$ might be improved to $1/34$.
In here we demonstrate the following:

**Theorem 1.** For any integer $k \geq 3$ there exists such sequence $n_1 < n_2 < \ldots$ of natural numbers such that for any element $n$ in it following inequality holds:

$$\phi_k(n) > (1/4 + o(1))g_k(n).$$

Furthermore, the sequence $n_1 < n_2 < \ldots$ is rather dense in the sense that any segment of the form $[n, ne^{(ln(n))^{1/2+o(1)}}]$ contains at least one element of this sequence.

As we see this result improves bound from [KSS75] for a subsequence of $\mathbb{N}$. We obtain constant $1/4$ since we ‘compress’ given set of numbers modulo a prime number twice and keep roughly half of the elements each time. Our method differs from the one presented at [KSS75] by fewer amount of operations (consists of 2 ‘compressions’), and therefore by saving more elements of the initial set.

For natural $n$ we denote by $[n]$ the segment $[1, \ldots, n]$.

## 2 Compressing Lemmas

Let us consider some set of integers $X = \{x_1, x_2, \ldots, x_n\}$. We call set $Y = \{y_1, y_2, \ldots, y_n\}$ a **compression** of set $X$, if for any triples $(i, j, k) \in [n]^3$ equality $x_i - 2x_j + x_k = 0$ implies $y_i - 2y_j + y_k = 0$ (notice that we do not imply any order of $x_i$ and $y_i$). This definition is closely related to Freiman homomorphism, see [TV06].

Now we state a hypothesis, which we prove only in special case, which however would suffice for us.

**Hypothesis 1.** For any $\epsilon > 0$ there is such subpolynomial function $h(n) = h_\epsilon(n)$, such that for any integer set $X$ of size $n$ there exists such $Y \subseteq X, |Y| \leq \epsilon n$, for which $X \setminus Y$ might be compressed into subset of segment $[nh(n)]$.

We prove it for all $\epsilon \in (3/4, 1)$. For the sake of transparency, we break the proof into several lemmas. Since we are only interested in behaviour of $h(n)$ for large $n$, we would only consider a case when $n$ is large enough.

**Lemma 2.1 (on compression into an interval of exponential length).** Any set of size $n$ might be compressed into a subset of the segment $[4n^{46n/2}]$.

**Proof.** Having set $X$ we want to build $Y \subseteq [4n^{46n/2}]$ such that $Y$ is a compression of $X$.

We assign to $X$ a following matrix $A$. Let us enumerate all nontrivial arithmetical progressions of length 3 in $X$:

$$(i_1, j_1, k_1), (i_2, j_2, k_2), \ldots, (i_p, j_p, k_p),$$

where $p$ is the total amount of progressions. Clearly, for any triple $(i_s, j_s, k_s)$ equality

$$x_{i_s} - 2x_{j_s} + x_{k_s} = 0$$

holds. We set $A$ to be a matrix of size $p \times n$. At $s$th row of $A$ we put 1 at $i_s$th and $k_s$th column, and $-2$ at $j_s$th column. Other entries are occupied with zeros.
For example, set $X = \{1, 2, 3, 4, 5\}$ would be assigned with the following matrix:

$$A = \begin{pmatrix} 1 & -2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 \\ 1 & 0 & -2 & 0 & 1 \end{pmatrix}$$

It is clear from the definition of matrix $A$ that

$$A \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

Furthermore, $Y$ is a compression of $X$ if and only if

$$A \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

Let us consider an arbitrary set $X$ of size $n$ and its assigned matrix $A$: $Ax = 0$, where $x = (x_1, \cdots, x_n)^T$. We would demonstrate the existence of such $y = (y_1, ..., y_n)$ such that its coordinates are distinct natural numbers not exceeding $4n^{4/3}$, satisfying $Ay = 0$.

Let us solve the equation $Ax = 0$. We choose maximal amount of linearly independent rows and put them to new matrix $A'$. Certainly, $A'x = 0 \iff Ax = 0$.

We denote size of $A'$ by $m \times n$, $m < n$ (clearly $A$ and $A'$ are degenerate, since sum of elements in each row equals 0). Let us distinguish independent (basis) variables from dependent ones. Clearly, there are exactly $m$ dependent variables among $x_1, x_2, \ldots, x_n$. Let us swap coordinates in $x = (x_1, \ldots, x_n)$ and rows in $A'$ in such a way such that first coordinates of $x$ are dependent, and last coordinates are independent. Via the Gauss elimination method we reduce the system to the following form:

$$A''x = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

(order of $x_1, x_2, \ldots$ might have changed after elimination). By Gauss elimination property there exists such nonsingular square matrix $M$ for which $A'' = MA'$. Notice that this equality would still hold if we keep only first $m$ columns of $A''$ and $A'$. Therefore, if $E$ and $D'$ are corresponding square matrices, then equality $E = MD'$ ($E$ is the identity matrix) holds. Clearly, $M = (D')^{-1}$. It is known that

$$M = (D')^{-1} = \begin{pmatrix} \frac{\text{det}(D'_{1,1})}{\text{det}(D')} & \frac{\text{det}(D'_{1,m})}{\text{det}(D')} \\ \cdots & \cdots \\ \frac{\text{det}(D'_{m,1})}{\text{det}(D')} & \frac{\text{det}(D'_{m,m})}{\text{det}(D')} \end{pmatrix}.$$
where $D_{i,j}'$ are adjoint matrices. Thus, $\| \det D' \times M \|_{\infty}$ does not exceed the absolute value of determinant of matrix consisting of elements $1,-2,0$, (with at most two $-1$ and at most one $2$ in each row), which we can bound by $(\sqrt{1^2 + 1^2 + (-2)^2})^m = 6^{m/2}$ by Hadamard inequality.

Since $A'$ also consists of elements $-2,1,0$, equality $A'' = MA'$ implies that all elements of $\det D'A''$ are integers with absolute values not exceeding $2m6^{m/2} \leq 2n6^{n/2}$.

Now we turn to construction of desired $y = (y_1,...,y_m)$, satisfying all the conditions above. Let us consider equation $A''x = 0$ and denote its first $m$ elements by $w_1,...,w_m$, and remaining by $z_1,...,z_t$, $m + t = n$. We have:

$$A''x = 0 \iff \begin{pmatrix} 1 & 0 & 0 & \cdots & w_1 \\ 0 & 1 & 0 & \cdots & w_m \\ 0 & 0 & 1 & \cdots & z_1 \\ & & & \cdots & \vdots \\ & & & & z_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

or

$$w_1 + a_{1,1}z_1 + a_{1,2}z_2 + \cdots + a_{1,t}z_t = 0,$$

$$\vdots$$

$$w_m + a_{m,1}z_1 + a_{m,2}z_2 + \cdots + a_{m,t}z_t = 0.$$

We know that any $a_{i,j}$ becomes integer when multiplied by $\det D'$ not exceeding $2n6^{n/2}$ by absolute value. From here we obtain that for any $w_i$ there exists such $\alpha_{i,1}, \alpha_{i,2},...,\alpha_{i,t}$ (negative correspondent elements of $A''$, multiplied by $\det D'$), such that

$$w_i = \frac{\alpha_{i,1}z_1 + \cdots + \alpha_{i,t}z_t}{\det D'},$$

where all of $\alpha_{i,j}$ are integer and bounded by $2n6^{n/2}$ in absolute value.

We now aim to find such a solution $w_1,\cdots,w_m,z_1,\cdots,z_t$, where all variables are distinct, natural and do not exceed $4n^46^{n/2}$.

Now we demonstrate that it is possible to choose from multidimensional cube $[0,K-1]^t$, (where $K = n^2$), such $t$-tuple $(z_1,...,z_t)$, so that all elements in $y = (z_1,...,z_t,w_1,...,w_m)$ would be distinct. Indeed, amount of possible points belonging to cube is $K^t$. Any equality of the form $z_i = z_j, z_i = w_j, w_i = w_j$ determines a hyperplane of the form $\alpha_1z_1 + \cdots + \alpha_tz_t = 0$ - clearly, all integer points belonging to hyperplane can be projected onto the face of hypercube (and projections are integers, too). Therefore there are at most $K^{t-1}$ integer points on any hyperplane. In total, there are at most $C_n^2K^{t-1} < K^t$ points in total.

Having this coordinates $(z_1,...,z_t)$ we construct corresponding $w_1,...,w_m$, multiply all elements of $y = (z_1,\cdots,w_1,\cdots)$ by $\det D'$ and obtain an integer-valued vector, whose maximal element does not exceed either $n^2 \times \det D' \leq n^2 \times 6^{n/2}$, (if it was one of $z_i$), or $n \times \max(\alpha) \times \max(z_i) \leq n \times 2n6^{n/2} \times n^2 = 2n^46^{n/2}$ (if it was one of $w_i$) — and therefore we can bound maximal element as $2n^46^{n/2}$. To get rid off negative numbers, we shift coordinates of $y$ `to right' to obtain set of naturals, with maximal element not exceeding $2 \times 2n^46^{n/2}$.

**Remark 1.** Clearly, one cannot get rid off exponential multiplier $c^n$, since there is not such compression for set $\{0,1,2,4,...,2^n\}$ that would make maximal element less than $2^n$. 

4
Lemma 2.2 (on compression into subset of segment of cubic length). If set $X$ of size $n$ belongs to segment $[1, \ldots, M]$, where $M = 4n^46^{n/2}$, then there exists such subset $X' \subseteq X$, $|X'| \geq |X|/2$ which might be compressed into subset of segment $[n^3]$.

Proof. Let us consider first prime numbers $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. Let us take the minimal prime number which does not divide any difference in $X$ and denote it by $p_{k+1}$. Then for any $p_k, t \leq k$, there are such distinct $x_i, x_j, x_t$ such that $p_t|(x_i - x_j)$. From here we obtain

$$2 \times 3 \times 5 \times \cdots \times p_k \prod_{i \neq j}(x_i - x_j).$$

From here we obtain the following bound (via using $p_k > k$, $|x_i - x_j| < M$):

$$2 \times 3 \times \cdots \times k \leq M^{n^2-n}.$$

Apply log to both parts:

$$k \ln k - k \leq \frac{n^2-n}{2} \ln M,$$

from where it is easy to observe that $p_{k+1} < 2n^3$ for large enough $n$.

Thus, there exists such prime $p \leq 2n^3$ which does not divide any difference in $X$. Let us now consider a set $X' = \{x_1 \pmod{p}, x_2 \pmod{p}, \ldots\}$. It has size $n$, and belongs to segment $[0, \ldots, p-1]$, therefore intersects by half with one of the segments $L_1 = [0, \ldots, p/2]$, and $L_2 = [p/2, p-1]$ (it is clear, that if elements form a progression in $X$, then so their images do in $X' \cap L_i$, provided that all of them belong to this image), and therefore we can remove at most half of the elements such that remaining set is compressible into subset of segment $[n^3]$.

Lemma 2.3 (on compression into subset of segment of almost-linear length). If set $X$ of size $n$ belongs to segment $[8n^3]$, then for any $\epsilon > 0$ there exists $X' \subseteq X$, $|X'| \geq (1/2 - \epsilon)|X|$ such that $|C_n \ln n|$, where $C_n$ is a constant, depending only on $\epsilon$.

Proof. For $n$ sufficiently large we consider prime numbers in segment $[2n, \ldots, 2cn \ln n]$, where $c$ is a positive constant. By Tchebyshev theorem, when $n$ is large enough, this segment would contain at least $cn$ prime numbers. We number them as $p_1, p_2, \ldots, p_s$, $s > cn$. Consider triples $(i, j, t)$, where $i, j, t$ are such that $p_t|(x_i - x_j)$. Notice that each pair $(i, j)$ of indexes participates in at most 2 triples, since $|x_i - x_j| < 8n^3$ and cannot be divisible by 3 or more distinct prime numbers exceeding $2n$. Therefore, there are at most $n^2$ such triples. By Dirichlet’s box principle some $p_t$ corresponds to at most $n^2/cn = n/c$ triples. We remove from $X$ all $x_i, x_j$, belonging to any of this triples, and remaining set $X_r$ would have size at least $|X| - 2n^2/cn \geq |X| - 2n^2$.

For set $X_r$ it is true that difference of any two distinct elements is not divisible by any prime $p_t < 2cn \ln n$, and in the same spirit as in previous lemma we remove from $X_r$ at most half of the elements such that remaining set might be compressed into subset $X'$ of segment $[2cn \ln n]$. Since we can take constant $c$ arbitrary large (and, accordingly, take $n > n(c)$), we have proved the desired assertion for any $\epsilon > 0$.

Now we turn to a proof of the Hypothesis 1 in the special case $\epsilon \in (3/4, 1)$:
Proof. We assume that $\epsilon \in (3/4, 1)$. First we compress set $X$ of $n$ elements into subset of segment $[4n^{1/2}6^{n/2}]$ by Lemma 2.1. Then we throw away at most half of the elements and compress $X$ into subset of segment $[n^3]$ by Lemma 2.2. Now we fix some $\delta > 0$ and apply Lemma 2.3 to $X \subseteq [1, \ldots, n^3] \sim [1, \ldots, 8(\frac{n}{2})^3]$, throw away at most $(\frac{1}{2} + \delta)\frac{n}{2}$ elements and compress remaining elements into the segment $[1, C\delta^2 \frac{n}{2}]$. In total we loose at most

$$\frac{n}{2} + (\frac{1}{2} + \delta)\frac{n}{2} = (\frac{3}{4} + \frac{\delta}{2})n$$

elements, so we take $\delta$ such that inequality $\frac{3}{4} + \frac{\delta}{2} \leq \epsilon$ holds. Obviously, $\delta := 2\epsilon - \frac{3}{2} > 0$ would work. \hfill \square

3 Proof of Theorem 1

In what follows, we would need a following lemma:

Lemma 3.1 (on lower-bound for density). For any natural $a, b$ and natural $k \geq 3$ the following inequality holds:

$$\rho_k(3ab) \geq \rho_3(a)\rho_k(b)/3.$$  

Proof. Let us bisect a segment of length $3ab$ into segments of length $3b$. Let us choose among them those, whose numbers correspond to maximal subset of segment $[a]$, free of arithmetical progressions of length 3 (clearly, there would be exactly $g_3(a) = a\rho_3(a)$ of such segments). We bisect chosen segments into subsegments of length $b$, and only keep ‘middle’ ones. Then we take a maximal subset free of arithmetical progressions of length $k$ of size $g_k(b) = b\rho_k(b)$ in each of these middle subsegments. Clearly, the union of all those subsets does not contain any arithmetical progression of length $k$, and therefore $\rho_k(3ab) \geq g_3(a)g_k(b)/3ab = \rho_3(a)\rho_k(b)/3$. \hfill \square

Before proving Theorem 1, we need following inequality:

Lemma 3.2. For large enough natural $n$, natural $k \geq 3$ and positive real $\alpha \in (0, 1/4)$, the following inequality holds:

$$\phi_k(n) > \alpha n \rho_k(C\alpha n \ln n).$$

Proof. Let us consider an arbitrary set $X$ of $n$ elements. By special case of Hypothesis 1 with $1 - \frac{1+\alpha}{2} \to \epsilon$, one can remove at most $\epsilon n$ elements in such a way, so that remaining set might be compressed into subset $A$ of segment $[C_\alpha n \ln n]$ of size $\frac{1+\alpha}{2}n$. Let us set $m := C_\alpha n \ln n$. Now we consider $\epsilon > 0$ such that $\frac{1+\alpha}{2}(1 - \epsilon) > \alpha$. Let us show that there exists such natural number $s$, depending only on $\alpha$, with the following property: if one considers maximal subset free of arithmetical progressions of length $k$ (which we denote by $T$) in the segment $[m + 1, m + (s + 1)m]$, then there is such a shift $A + x$ of set $A$, which has large intersection with $T$ (clearly, $|T| = (s + 1)m\rho_k((s + 1)m))$:

$$|(A + x) \cap T| \geq (1 - \epsilon)|A|\rho_k((s + 1)m).$$

(1)

Indeed, let us consider shifts of $A$ ‘to the right’: $A + 1, A + 2, \ldots, A + sm$. Notice that any element of $T$, located left to $m + sm$, belongs to exactly $|A|$ shifts. Let $T_1 := T \cap [m + 1, m + sm]$ and $T_2 := T \cap [m + sm + 1, m + (s + 1)m]$. Clearly $|T| = |T_1| + |T_2|$. Let us assume that (1) does not
hold. By Dirichlet’s box principle some shift of $A$ intersects $T$ by at least $|T||A|/sm$ elements, and therefore one can conclude that $|T||A|/sm \leq (1-\epsilon)|A|\rho_k((s+1)m)$, and therefore $|T_2| \geq |T| - |T_1| \geq (1+se)\rho_k((s+1)m)$ elements of $T$.

By Lemma 3.1 (we assume that $s+1$ is divisible by 3) we see $\rho_k(m) \geq (1+se)\rho_k((s+1)m) \geq (1+se)\rho_3((s+1)/3)\rho_k(m)$ (we derive leftmost inequality from the fact that set free of progressions of length $k$ cannot have density more than $\rho_k(m)$ on segment of length $m$). Therefore, to get a contradiction, it is enough to take $s$ to be that large so that inequality $(1+se)\rho_3((s+1)/3) \geq 1$ holds.

This is possible since $\rho_3(n) \geq \frac{1}{k^{3\sqrt{\log n}}}k^{3\sqrt{\log n}}$, denominator is subpolynomial, and the function $(1+se)\rho_3(\frac{s+1}{3})$ has polynomial growth on $s$. So, we obtained required $s$ depending on $\epsilon$ and $k$, or on $\alpha$ and $k$.

So, now we have desired inequality $\phi_k(n) > \frac{1}{4+\alpha}(1-\epsilon)n\rho_k((s+1)m) > \alpha\rho_k(H_{\alpha,k}n\ln n)$.

Now we turn to Theorem 1:

**Proof.** Let us suppose that statement of Theorem 1 does not hold for some $k \geq 3$. Therefore, there exists some $\epsilon > 0$, such that for any $o(1)$ there is some segment $I = [m, me^{(\ln m)^{1/2+o(1)}}]$, such that for any $n \in I$ inequality $\phi_k(n) < (1/4-\epsilon)g_k(n)$ holds. On the other side, by Lemma 3.2, any $n \in I$ satisfies $(1/4-\epsilon)g_k(n) \geq \alpha\rho_k(C_{\alpha,k}n\ln n)$, where $\alpha > (1/4-\epsilon)$ (one can set $\alpha := 1/4-\epsilon/2$). From here we obtain that for some constant $c > 1$ ($c := \frac{1}{1/4-\epsilon}$) inequality $\rho_k(n) > c\rho_k(C_{c,k}n\ln n)$ takes place whenever $n \in I$.

Now we build the sequence $t_1 = m, t_2 = Ct_1\ln t_1, t_3 = Ct_2\ln t_2, \ldots$ (we continue while $t_i \in I$ holds — clearly, there are at least $(\ln m)^{1/2+o(1)}$ such $t_i$).

Therefore, $\rho_k(t_1) > c\rho_k(t_2) > c^2\rho_k(t_3) > \cdots$

Now, combining lower bound for $\rho_k(n)$, and the fact that sequence of $t_i$ has at least $(\ln m)^{1/2+o(1)}$ elements, the bound $\rho_k(t_1) \geq c^{t_i-1}\rho_k(t_i)$ would yield a contradiction for the last $t_i$ in the list. 

**References**

[Beh46] F. A. Behrend. “On Sets of Integers Which Contain No Three Terms in Arithmetical Progression”. *Proceedings of the National Academy of Sciences* 32.12 (1946), pp. 331–332. DOI: 10.1073/pnas.32.12.331. URL: https://www.pnas.org/content/32/12/331.

[Blo12] Thomas F. Bloom. “Translation invariant equations and the method of Sanders”. *Bulletin of the London Mathematical Society* 44.5 (2012), pp. 1050–1067. DOI: 10.1112/blms/bds045. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/blms/bds045.

[Gow01] W. T. Gowers. “A new proof of Szemerédi’s theorem”. *Geom. Funct. Anal.* 11.3 (2001), 465–588 (2001), erratum 11, no. 4, 869. DOI: https://doi.org/10.1007/s00039-001-0332-9.

[KSS75] J. Komlós, M. Sulyok, and E. Szemerédi. “Linear problems in combinatorial number theory”. *Acta Mathematica Academiae Scientiarum Hungarica* 26 (1975), pp. 113–121. DOI: https://doi.org/10.1007/BF01895954.

[OBr13] K. O’ Bryant. “Thick Subsets that Do Not Contain Arithmetic Progressions”. *Integers* 13 (2013), A18. DOI: 10.1515/9783110298161.249. arXiv: 0912.1494 [math.NT].
[Shk06] Ilya Shkredov. “Szemerédi’s theorem and problems on arithmetic progressions”. Uspekhi Mat. Nauk 61 (Jan. 2006), pp. 111-178. DOI: 10.4213/rm5293.

[TV06] T. Tao and V. Vu. “Additive Combinatorics”. Vol. 105. Cambridge Univ. Press, Cambridge, 2006.

A.S. Semchankau
The Steklov Institute of Mathematics
119991, Russian Federation, Moscow, Ulitsa Gubkina, 8
aliaksei.semchankau@gmail.com