pachpp_312_25

Algebraic Methods in Additive Combinatorics

Péter Pál Pach

Doctoral dissertation submitted to the
Hungarian Academy of Sciences

Budapest, 2025

Contents

1 Introduction

During the past decades the polynomial method became a powerful tool that led to the solution of several important open problems, like Dvir's proof [35] of the finite field Kakeya conjecture, the result of Guth and Katz [65] on Erdős' distinct distances problem or the solution of the cap set problem [31, 41]. The cap set problem asks for the size of the largest subset of the vector space $\mathbb{F}_3^n$ avoiding 3-term arithmetic progressions. It became a keystone problem whose solution was expected to (and eventually) led to the solution of many other problems in Combinatorics and Number Theory, furthermore, in other fields of Mathematics, as well. While the cap set problem strongly suggested that the polynomial method might be applicable, since the condition that x, y and z form an arithmetic progression can be simply expressed as the equation $x - 2y + z = 0$, for several years almost all of the results were obtained by Fourier analytic techniques. Also note that the equation $x-2y+z$ is symmetric in the variables when we investigate the problem over $\mathbb{F}_3$, since in this case the equation has the form $x + y + z = 0$.

Most of the results obtained by polynomial techniques in the 1990s and 2000s built on Alon's Combinatorial Nullstellensatz [2], however, in case of the cap set problem a new variant was needed. Very briefly, the main idea was introducing a new kind of rank for hypermatrices (though this rank behaviour appeared only implicitly in the original papers), which still satisfies that the rank of a diagonal hypermatrix is the number of nonzero entries on its main diagonal. If a set A contains only trivial (constant) 3-term arithmetic progressions, then the "characteristic function" of 3-term arithmetic progressions (restricted to $A\times A\times A$) is a diagonal tensor, so bounding the rank of this tensor yields the desired bound on the size of the set A.

Although, in the recent solution of the Alon-Jaeger-Tarsi conjecture [90] (and also in the follow-up paper [91]) we also applied a new variant of the polynomial method, its nature is quite different from the previously mentioned variant: it uses group ring identities in a certain way. Manipulations with polynomials also play a crucial part in some of the works of the author in arithmetic Ramsey theory [74, 80, 92], but these ideas and methods are also quite diverse.

Therefore, in this thesis the author decided to give a detailed description of the above-mentioned (Croot-Lev-Pach) polynomial method which was first used to bound the maximal possible size of progression-free sets in groups like $\mathbb{Z}_m^n$, discuss the known bounds and present further applications of the technique.

In the first section we will discuss the motivations coming from number theory to investigate progression-free sets in the finite field setting, for more details we refer to the review paper [32] of Croot, Lev and the author that we follow in this section. We also refer to the discussions of Gowers [59] and Grochow [64].

1.1 Roth's problem on three-term progressions

In 1953 K. F. Roth [106] proved that the largest subset of $[n] := \{1, 2, \ldots, n\}$ containing no three-term arithmetic progression $x, x + d, x + 2d$ has size $o(n)$. Working through his proof (suitably interpreted) one can even get a quantitative bound of the form $O(n/\log\log n)$. This naturally leads to the following question.

Roth's Problem. What is the size of the largest subset $S \subseteq [n]$ containing no three-term arithmetic progressions?

Most of the progress on this problem since Roth's seminal work makes heavy use of a "density increment argument" pioneered by him. The idea is that if we assume that $S \subseteq [n]$ has no three-term progression, and if $|S| = \alpha n$ and $n > N_0(\alpha)$, then one can show that there exists an arithmetic progression

$$P := \{a, a + d, a + 2d, \ldots, a + kd\} \subseteq [n],$$

where $k > n^{1/2-o(1)}$, such that

$$|S \cap P| \geq \alpha(1 + c\alpha)|P|$$

for some $c > 0$. By translating and rescaling, we obtain a progression-free set $S' \subseteq [n']$ for some $|n'| > n^{1/2-o(1)}$ such that $|S'| \geq \alpha(1 + c\alpha)|n'|$. Iterating this (staying above the $N_0(\alpha)$ threshold for the interval length), eventually we reach a contradiction if $\alpha > c'/\log\log n$, because if α is this big, one of the sets S'' so constructed would have to have density 1, yet also is progression-free. Thus, if the original S is progression-free, then $|S| \ll n/\log\log n$.

Further refinements on the idea included achieving a greater density increment per iteration relative to the length of the interval [68, 116], resulting in bounds for progression-free sets of the type $|S| < n(\log n)^{-\delta}$, for some $0 < \delta < 1/2$. Replacing density-increments on sub-progressions (as in Roth's method) with density-increments on so-called Bohr-neighbourhoods, Bourgain [18] achieved a bound of the form $|S| \ll n\sqrt{\frac{\log\log n}{\log n}}$. Then in a series of papers by himself [19] and Sanders [110, 111] the bound was improved to $|S| < n(\log n)^{-1+o(1)}$. Improving this bound even a little bit (lowering the -1 to $-1-\varepsilon$) would establish the special case $k = 3$ of the following famous conjecture [47], which if proved would give a far-reaching generalization of Szemerédi's Theorem [115].

Erdős-Turán Conjecture on k-term arithmetic progressions. If A is a set of positive integers such that $\sum_{a \in A} 1/a$ diverges, then for every $k \geq 2$, the set A contains a k-term arithmetic progression.

The best quantitative bounds in the direction of addressing this theorem in the general case (for all values of k) are due to Leng, Sah, and Sawhney [76], who

recently proved that for every $k \geq 5$ there exists some $c_k > 0$ such that the largest subset S of $[n]$ having no k-term arithmetic progressions has size

$$|S| \ll n \exp(-(\log\log n)^{c_k}).$$

This improved upon Gowers's bounds [58] that $|S| \ll n(\log\log n)^{-2^{-2^{k+9}}}$. In the case $k = 4$, Green and Tao [62, 63] established the bound $|S| \ll n(\log n)^{-c}$ for some $0 < c < 1$.

Bloom and Sisask [15] were the first to prove the above conjecture for $k = 3$, building on the work of Bateman and Katz [9], by showing that for $n > N_0$ the largest progression-free set $S \subseteq [n]$ has size $|S| < n(\log n)^{-1-\varepsilon}$ (for some explicit $\varepsilon > 0$). Then, in a remarkable breakthrough, Kelley and Meka [73, 16] improved this to

$$|S| < n \exp(-c(\log n)^{1/12}),$$

which Bloom and Sisask [17] refined to give

$$|S| < n \exp(-c'(\log n)^{1/9}).$$

These bounds are not far off from the best possible, since from the work of Behrend [10] it was known that there exists a three-term progression-free set $S \subseteq [n]$ satisfying

$$|S| > n \exp(-(2\sqrt{\log 4} + o(1))\sqrt{\log n}).$$

This was improved by Elkin [40] by a small factor tending to infinity, and then recently Elsholtz, Hunter, Proske, and Sauermann [44] gave a substantial further improvement

$$|S| > n \exp(-(C + o(1))\sqrt{\log n}),$$

where $C = 2\sqrt{\log(24/7)\log(2)} < 2\sqrt{\log 4}$.

1.2 Finite field settings

As we saw, the main difficulty in Roth's original approach was getting a high enough density increment of the set along progressions, relative to their (the progressions) size. Meshulam [83] considered what this argument gives in the case where instead of working with subsets of intervals in the integers, one works with subsets of the finite field vector space $\mathbb{F}_p^n$. The case $p = 3$ is known as the *cap set problem.*

In Meshulam's treatment of the general case $\mathbb{F}_p^n$, rather than getting a density increment inside a sub-progression at each iteration (of Roth's argument), one gets a density increment on affine subspaces (translates of subspaces) $t + V$ where $\dim(V) = n - 1$. Since these affine subspaces are of size p^{n-1}, one can run the density increment argument for more steps than if one's sets S were drawn from

integer intervals $[N]$ when $N \approx p^n$. Furthermore, the whole argument is more elegant and simpler than in the integer case, while also containing many of the same, or analogous difficulties. In fact, this is true of many additive combinatorial problems [60, 95, 123]. Thus, it is often fruitful when trying to solve a problem over $\mathbb{Z}$, to first see what we can prove for an $\mathbb{F}_p^n$ analogue of that problem.

In the end, Meshulam proved that the largest subset $S \subseteq \mathbb{F}_p^n$ without three-term progressions (or solutions to $x - 2y + z = 0$) satisfies

$$|S| < \frac{c_p p^n}{n}.$$

Meshulam's proof uses Fourier methods, but in [78] Lev developed a purely combinatorial approach to achieve the same bounds.

Significantly improving upon Meshulam's bound was considered a major challenge, and Terry Tao [118] even once referred to the overall problem of understanding the size of sets without three-term progressions in $\mathbb{F}_3^n$ as "perhaps my favorite open question".

Bateman and Katz were the first to make major progress on it, proving that there exists some $\varepsilon > 0$ such that in the case $p = 3$ one has $|S| \ll 3^n/n^{1+\varepsilon}$. Then Ellenberg and Gijswijt [41], building on our work in [31], used algebraic methods to prove that for every prime $p \geq 3$ there exists $\delta_p > 0$ such that $|S| \ll (p - \delta_p)^n$. Further algebraic generalizations of the method were given by Tao, Sawin [112, 119] and Petrov [96].

More recently, Kelley and Meka [73] have developed a combinatorial argument (one ingredient of which being [30]) to prove weaker bounds, but still much stronger than other combinatorial and Fourier-analytic approaches, achieving $|S| \ll 2^{-\kappa_p n^{1/9}} p^n$.

Lower bounds were proved by Edel [36] for $p = 3$ giving the existence of a set S without three-term progressions that satisfies $|S| > (2.217389)^n$. This was improved by Tyrrell [121] to $|S| > (2.218)^n$, by Romera-Paredes et al [105] to $|S| > (2.2202)^n$, and by Naslund [87] to $|S| > (2.2208)^n$. Recently, Elsholtz, Hunter, Proske, and Sauermann [44] achieved a general lower bound of the shape $|S| > (cp)^n$ for some $c > 1/2$, for all primes $p \geq 3$.

1.3 Notations

Throughout the thesis, the standard notation $\ll$, $\gg$ and respectively O and Ω is applied to positive quantities in the usual way. That is, $X \gg Y$, $Y \ll X$, $X = \Omega(Y)$ and $Y = O(X)$ all mean that $X \geq cY$, for some absolute constant $c > 0$. If both $X \ll Y$ and $Y \ll X$ hold, we write $X = \Theta(Y)$. If the constant c depends on a quantity t, we write $X \ll_t Y$, $Y = O_t(Y)$, and so on. We also use the Landau o notation.

The standard dot product of vectors $x, y \in \mathbb{F}_q^n$ is denoted by $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$. For brevity, we also write xy for the dot product, if it does not cause any confusion.

We use the notation $[n] := \{1, 2, \dots, n\}$ and the Kronecker delta function as

$$\delta_{x,y} = \delta_x(y) = \delta(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}.$$

By a (nontrivial) k-term arithmetic progression in $\mathbb{Z}_m^n$ we mean a k-term arithmetic progression $a, a+d, \dots, a+(k-1)d$ (with $a, d \in \mathbb{Z}_m^n$) consisting of distinct elements, and for brevity we call it a k-AP. A set avoiding k-term arithmetic progressions is called k-AP-free. The size of the largest k-AP-free subset of $\mathbb{Z}_m^n$ is denoted $r_k(\mathbb{Z}_m^n)$ and the largest k-AP-free subset of $\{1, 2, \dots, n\}$ is denoted $r_k(n)$.

We will work with linear and affine subspaces of $\mathbb{F}_2^n$. If L is a linear subspace of dimension d, for brevity we will say that L is a d-subspace. The smallest linear subspace containing the vectors $v_1, \dots, v_k$ will be denoted by $\langle v_1, \dots, v_k \rangle$.

Similarly, if L is an affine subspace of dimension d, we will say that L is an affine d-subspace and the smallest affine subspace containing $v_1, \dots, v_k$ will be denoted by $\langle v_1, \dots, v_k \rangle_{aff}$.

For a subset $A \subseteq \mathbb{Z}_m^n$ we use the notation $A + A = \{a + a' : a, a' \in A\}$ for the sumset and $A \hat{+} A = \{a + a' : a, a' \in A, a \neq a'\}$ for the restricted sumset.

1.4 Organization of the dissertation

In Section 2 we discuss in detail results about the maximal possible size of progression-free sets in groups $\mathbb{Z}_m^n$, also addressing the analogous problems about caps and line-free sets. Section 3 contains the proofs of our asymptotic bounds and some necessary tools: in these cases we are interested in bounds when m is fixed and $n \to \infty$. In Section 4 we give lower and upper bounds on $r_3(\mathbb{Z}_4^n)$, presenting the polynomial technique from [31] in a slightly reformulated way. We also determine exact values of $r_3(\mathbb{Z}_4^n)$ and $r_4(\mathbb{Z}_4^n)$ in small dimensions. Section 5 contains analogous results for $\mathbb{Z}_6^n$, however, somewhat surprisingly, due to the special structure of $\mathbb{Z}_6$, in this case we are able to provide exponentially small upper bounds for the size avoiding 6-term arithmetic progressions, as well. Section 6 contains the proofs of our results on line-free sets, that is, sets avoiding p-term arithmetic progressions in $\mathbb{F}_p^n$. Finally, in Section 7 we give a brief introduction of the so-called slice rank method – a symmetric reformulation of our polynomial technique from [31, 41] given by Tao –, and present applications of it.

2 Progression-free sets

In this section we discuss results about the size of progression-free sets in groups of the form $\mathbb{Z}_m^n$. For more details we refer to [45, 93, 94] that we follow in this section.

There has been great interest in finding progression-free sets in $\mathbb{Z}_m^n$, especially when $m = 3$ or 4. (Note that the cases when m is odd or even slightly differ in nature, and since the case $m = 2$ is trivial, the two smallest cases are $m = 3$ and $m = 4$, respectively.) When $m = 3, 4, 5$ the properties "no arithmetic progression of length 3 modulo m" and "no 3 points on any line" are equivalent. The last property is also well known under the name caps (or cap sets). In spite of this great interest in progression-free sets and caps there is not much literature on progression-free sets in $\mathbb{Z}_m^n$, in the case of general $m > 3$, and of general progressions of length k. Furthermore, very few explicit values of the maximal sizes of such sets are known. Although there is certainly an extensive literature in the related area of finite geometry over finite fields, but in literature from an additive combinatorial point of view we are essentially aware of an exercise in the book by Tao and Vu, and a paper by Lin and Wolf, details below.

In this section we will discuss lower- and upper bounds in various cases, and find exact values in the case $m = 4$, which are comparable in size to the known values for $m = 3$.

However, before we get to this, we briefly summarize a number of related questions. The problem of finding sets $S \subseteq \mathbb{Z}_m^n$ with or without a given property has been frequently investigated. Often, one is actually interested in the maximal size of $|S|$. Also, sometimes even the one-dimensional case has been of fundamental interest. Let us recall some of the properties that have been investigated.

1) Erdős and Turán [52] raised the problem of studying the maximal size $r_k(n)$ of sets in $\{1, \dots, n\}$ without an arithmetic progression of length k. There are important contributions by Behrend, Bloom and Sisask, Bourgain, Gowers, Green, Kelley and Meka, Roth, Salem and Spencer, Sanders, Szemerédi, Tao [10, 18, 58, 61, 73, 106, 108, 110, 115]. In particular, the proof of $r_k(n) = o(n)$, as N tends to infinity, and quantitative versions thereof, turned out to be very influential in this area. It is interesting to note that the size of progression-free sets even enters the complexity of matrix multiplication, see [14, 28, 122].

   The question of arithmetic progressions has also been studied modulo m, see e.g. Croot [29]. In this setting "modulo m" one has to clarify if elements of the progression can occur more than once. For example $(1, 3, 1, 3)$ can possibly be considered as a progression of length 4 modulo $m = 4$. In this thesis, however, we study "proper arithmetic progressions" meaning that all elements in the progression are *distinct*, unless otherwise stated, and the quantity $r_k(\mathbb{Z}_m^n)$ was defined accordingly in Subsection 1.3.

2) Assume that S does not have k elements $x_1, \dots, x_k \in \mathbb{Z}_m^n$ that satisfy (for fixed

constants $a_1, \dots, a_k \in \mathbb{Z}$) a linear equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0 \in \mathbb{Z}_m^n.$$

(a) The case $n = 1, k = m, a_1 = a_2 = \cdots = a_k = 1$ was first investigated by Erdős, Ginzburg and Ziv [48], who proved that for any $2m-1$ elements in $\mathbb{Z}_m$, where in this problem repetition is allowed, there exists a subset of m elements with sum $0 \in \mathbb{Z}_m$. (There are hundreds of papers on generalizations and variants, the general topic is called "zero sums in finite abelian groups"). In the case $n = 2$ there has been important work by Reiher [103]. The multidimensional case with $n \geq 3$ is widely open, even though there are lower bounds by Edel, Elsholtz et al [37, 38, 42], and upper bounds by Alon and Dubiner [4], Naslund [85] and Hegedüs [69].

(b) The case $x_1 + x_2 - x_3 = 0, x_i \in S$ corresponds to sum-free sets. In the one-dimensional case $S \subset \{1, \dots, m\}$ it is known that the maximal size is $|S| = \lfloor \frac{m}{2} \rfloor + 1$, if all x_i are distinct, or $|S| = \lfloor \frac{m+1}{2} \rfloor$, if $x_1 = x_2$ is allowed. In the case modulo a prime m it follows from the Cauchy-Davenport theorem that the maximal size satisfies $|S| \leq \frac{m+1}{3}$ (x_i all distinct).

In the multidimensional case of an integer grid there are partial results by Cameron [24], Elsholtz and Rackham [46].

3) The case of no geometric line (of m points) in the integer grid $\{1, \dots, m\}^n$ is known as Moser's cube problem, see [84, 98]. A closely related problem is finding the maximal number of lattice points in the same cube $\{1, \dots, m\}^n$, but without any combinatorial line. The famous upper bound by Hales-Jewett [66] of $o(m^n)$ points, when m is fixed and n tends to infinity, became very influential.

In this thesis, we concentrate on sets $S \subseteq \mathbb{Z}_m^n$ of maximal size $|S| = r_k(\mathbb{Z}_m^n)$ with no k distinct elements in arithmetic progression. Observe that an arithmetic progression of length k can be expressed by means of $k-2$ linked linear conditions $x_i - 2x_{i+1} + x_{i+2} = 0$ $(i = 1, \dots, k-2)$.

The multidimensional case of no 3 points in arithmetic progression has been frequently studied, especially modulo $m = 3$. As we already mentioned before, here the questions of "no zero sums $x_1 + x_2 + x_3 = 0$" and "no arithmetic progression $x_1 + x_3 = 2x_2$" turn out to be equivalent as $1 \equiv -2 \bmod 3$ and the problem is known as the "cap set problem". There were important contributions by Brown and Buhler [21], Frankl, Graham and Rödl [56], Meshulam [83], Lev [77], Bateman and Katz [9], Croot, Lev and the author [31], Ellenberg and Gijswijt [41].

For a long time it was an important open problem if there is a $\delta > 0$ such that $|S| < (3-\delta)^n$ holds, for all progression-free sets $S \subset \mathbb{Z}_3^n$. Various authors mentioned this statement with varying degree of certainty or doubt (see Alon and Dubiner [3], [4], Green [60], Kalai [72], Edel [36], Tao [118]), until the solution by

Croot, Lev and the author [31] when $m = 4$, and finally Ellenberg and Gijswijt [41] when $m = 3$.

Meshulam's [83] long-standing bound $r_3(\mathbb{Z}_m^n) = O(\frac{m^n}{n})$ for odd values of $m \geq 3$ was extended by Lev [77] to even values $m \geq 4$. Improving this, Sanders [109] proved the following result:

$$r_3(\mathbb{Z}_4^n) = O\left(\frac{4^n}{n \log^c n}\right),$$

for some positive c. Green and Tao [61] wrote that $c = 2^{-22}$ is admissible. Introducing an entirely new approach, based on the polynomial method rather than Fourier techniques, Croot, Lev and the author [31] proved an exponentially smaller bound.

Let H denote the binary entropy function; that is,

$$H(x) = -x \log_2 x - (1-x) \log_2 (1-x), \quad x \in (0,1),$$

where $\log_2 x$ is the base-2 logarithm of x. Let us set

$$\gamma := \max\left\{\frac{1}{2}\big(H(0.5-\varepsilon) + H(2\varepsilon)\big) \colon\ 0 < \varepsilon < 0.25\right\} \approx 0.926.$$

Theorem 2.1 (Croot-Lev-Pach [31]). *If $n \geq 1$ and $A \subseteq \mathbb{Z}_4^n$ is 3AP-free, then $|A| \leq 4^{\gamma n}$, where $4^\gamma \approx 3.61$.*

We note that the exponential reduction in Theorem 2.1 was the first of its kind for problems of this sort.

For a finite abelian group $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ with positive integers $m_1 \mid m_2 \mid \cdots \mid m_k$, denote by $\mathrm{rk}_4(G)$ the number of indices $i \in [1,k]$ with $4 \mid m_i$. Since, writing $n := \mathrm{rk}_4(G)$, the group G is a union of $4^{-n}|G|$ cosets of a subgroup isomorphic to $\mathbb{Z}_4^n$, as a direct consequence of Theorem 2.1 we get the following corollary.

Corollary 2.2 (Croot-Lev-Pach [31]). *If A is 3AP-free subset of a finite abelian group G, then, writing $n := \mathrm{rk}_4(G)$, we have $|A| \leq 4^{-(1-\gamma)n}|G|$.*

The new methods introduced in [31] also led to the result $r_3(\mathbb{Z}_3^n) \leq 2.756^n$ by Ellenberg and Gijswijt [41]. As it has been mentioned before, the problem about cap sets has applications to the complexity of matrix multiplication, see [5, 14].

The corresponding problem on lower bounds of progression-free sets in $G = (\mathbb{Z}_3^n, +)$ has also been studied in detail. It is known that there is a set S with $|S| > 2.2208^n = |G|^\beta$ with $\beta = \frac{\log 2.2208}{\log 3} \approx 0.72625$. (See Edel [36] for the history of known bounds, not yet including the very recent improvements by Tyrrell [121], Paredes et al [105] and Naslund [87].)

For a lower bound when $m = 4$ Sanders [109] proved the following: there exists $S \subseteq G = (\mathbb{Z}_4^n, +)$ which does not contain a proper three term arithmetic progression with

$$|S| \gg |G|^{2/3} \approx 2.519^n.$$

This result follows from finding an example in $\mathbb{Z}_4^3$ with 16 elements and using a product construction. (Note that $\sqrt[3]{16} = 2.519\ldots$.)

We give a better lower bound on $r_3(\mathbb{Z}_4^n)$. In the construction we use binary codes with certain minimum distances. Let $A(m,d)$ denote the largest possible size of a (possibly non-linear) code in $\mathbb{F}_2^m$ with minimum distance at least d. Note that $A(m,1) = 2^m$ (all vectors can be taken) and $A(m,2) = 2^{m-1}$ (all codewords can be taken with even Hamming-weight). Here we give two links to tables of exact values of maximal codes or bounds: `https://www.win.tue.nl/~aeb/codes/binary-1.html` and `http://www.codetables.de/`
We prove the following bound:

Theorem 2.3 (Elsholtz-Pach [45]). *For $n > 1$ we have*

$$r_3(\mathbb{Z}_4^n) \geq \max_{0 \leq t \leq n} \sum_{i=t+1}^{n} \binom{n}{i} A(i, i-t).$$

As a consequence of this result one can prove a quite good lower bound for $r_3(\mathbb{Z}_4^n)$.

Corollary 2.4 (Elsholtz-Pach [45]).

$$r_3(\mathbb{Z}_4^n) \gg \frac{3^n}{\sqrt{n}},$$

which implies that there exists a progression-free set $S \subseteq \mathbb{Z}_4^n$ with

$$|S| \gg 4^{0.7924n}.$$

The exponent 0.7924 is not only much larger than the previous one of 2/3, but it is also much larger than the corresponding one 0.72625 when $m = 3$. This can be interpreted that the progression-free sets in $\mathbb{Z}_4^n$ are denser than those in $\mathbb{Z}_3^n$. The ultimate reason for this is that there is a geometrically well structured subset, namely $\{0,1,2\}^n$, on which we can find a very dense progression-free subset. As two elements from the same coset of the subgroup $\{0,2\}^n$ forbid 2^n other points, namely an affine copy of $\{0,2\}^n$, it comes handy that this forbidden set has some geometric-algebraic structure.

This corollary is the first nontrivial case of the lower bound constructions and is suitable for discussing various methods. We first prove it as a direct application of Theorem 2.3.

Proof of Corollary 2.4 (Proof 1). Calculations show that the optimal choice for t in Theorem 2.3 satisfies $t \sim 2n/3$. In particular, for $2 \leq n \leq 10$ the optimal choice is $t = \lceil (2n-5)/3 \rceil$. Note that the sum of only the first two terms in the lower bound

$$\sum_{i=t+1}^{n} \binom{n}{i} A(i, i-t),$$

with an optimal value of t, is

$$\binom{n}{t+1}2^{t+1} + \binom{n}{t+2}2^{t+1} \sim 1.5 \cdot 2^{2n/3}\binom{n}{2n/3} \sim \frac{9}{4\sqrt{\pi}} \cdot \frac{3^n}{\sqrt{n}}.$$

The total sum is not much larger as it is bounded above by $\frac{3}{\sqrt{\pi}} \cdot \frac{3^n}{\sqrt{n}}$ (see also [26]). □

The proof of Theorem 2.3 and Corollary 2.4 above may appear a bit formal. In Section 4 we explain in detail the geometric motivation of a direct proof of Corollary 2.4, i.e. the connection to Moser's cube problem and to the Behrend and Salem-Spencer constructions.

Finally, we found a quite different proof, based on weighted Sperner capacity of the 2-vertex graph with one directed edge, and vertex weights 1 and 2, but decided not to include it.

Let us list the obtained lower bounds up to dimension 10:

Corollary 2.5 (Elsholtz-Pach [45])**.**

$$2 \le r_3(\mathbb{Z}_4^1),\ 6 \le r_3(\mathbb{Z}_4^2),\ 16 \le r_3(\mathbb{Z}_4^3),\ 42 \le r_3(\mathbb{Z}_4^4),\ 124 \le r_3(\mathbb{Z}_4^5),$$

$$344 \le r_3(\mathbb{Z}_4^6),\ 960 \le r_3(\mathbb{Z}_4^7),\ 2832 \le r_3(\mathbb{Z}_4^8),\ 7880 \le r_3(\mathbb{Z}_4^9),\ 22232 \le r_3(\mathbb{Z}_4^{10}).$$

Let us explain this with two examples: when $n = 5$, choose $t = 2$. Then

$$\begin{aligned} r_3(\mathbb{Z}_4^5) &\ge \tbinom{5}{3}A(3,1) + \tbinom{5}{4}A(4,2) + \tbinom{5}{5}A(5,3) \\ &= 10 \cdot 8 + 5 \cdot 4 + 1 \cdot 4 = 80 + 40 + 4 = 124, \end{aligned}$$

which is best possible by Theorem 2.11. When $n = 8$, choose $t = 4$.

$$\begin{aligned} r_3(\mathbb{Z}_4^8) &\ge \tbinom{8}{5}A(5,1) + \tbinom{8}{6}A(6,2) + \tbinom{8}{7}A(7,3) + \tbinom{8}{8}A(8,4) \\ &= 56 \cdot 32 + 28 \cdot 32 + 8 \cdot 16 + 1 \cdot 16 = 2832. \end{aligned}$$

In the case of $\mathbb{Z}_3^n$ the bound from [41] has been improved by Jiang [71] by a factor of $\sqrt{n}$, so the following is known:

$$2.2208\ldots^n \ll r_3(\mathbb{Z}_3^n) \le 2.755\ldots^n/\sqrt{n}, \quad [87,\ 41,\ 71]$$

$$3^n/\sqrt{n} \ll r_3(\mathbb{Z}_4^n) \le 3.61\ldots^n, \quad [45,\ 31],$$

and for primes $p \ge 3$ and some positive constant δ_p

$$r_3(\mathbb{Z}_p^n) \le (p - \delta_p)^n \quad [41].$$

Indeed the argument yields the bound

$$r_3(\mathbb{Z}_p^n) \le (J(p)p)^n, \quad [14]$$

where

$$J(p) = \frac{1}{p} \min_{0<t<1} \frac{1 - t^p}{(1-t)\, t^{(p-1)/3}}. \tag{1}$$

Furthermore, it is known that $J(s)$ is decreasing and $\lim_{s\to\infty} J(s) = 0.8414\ldots$ (see equation (4.11) of [14]).

Remark 2.6. *As $J(s)$ is decreasing and $J(3) \le 0.9184$, with the additional consideration of composite m (see below), one can conclude, that for every $m \ge 3$ the following holds (see e.g. [14] and [97]):*

$$r_3(\mathbb{Z}_m^n) \le (0.9184m)^n. \tag{2}$$

For m not being a power of 2 this also holds: if p is an odd prime divisor of m, then $r_3(\mathbb{Z}_m^n) \le (m/p)^n r_3(\mathbb{Z}_p^n) \le (m/p)^n (pJ(p))^n \le (0.9184m)^n$. For integers divisible by 4 this follows from [31], since $r_3(\mathbb{Z}_m^n) \le (m/4)^n r_3(\mathbb{Z}_4)^n \le (0.91m)^n$.

For prime power values of m there have been some improvements on the trivial corollaries of the prime case, like $r_3(\mathbb{Z}_9^n) \le 3^n r_3(\mathbb{Z}_3^n)$. Namely, the method was adapted to odd prime powers [14, 96, 114] giving the bound

$$r_3(\mathbb{Z}_m^n) \le (mJ(m))^n.$$

For instance, the trivial bound $r_3(\mathbb{Z}_9^n) \le 3^n r_3(\mathbb{Z}_3^n) \le 8.268^n$ is improved to $r_3(\mathbb{Z}_9^n) \le 7.847^n$ by this result.

In the technically more difficult even case there has also been an improvement for $m = 2^3 = 8$. For $r_3(\mathbb{Z}_8^n)$ the trivial implication is

$$r_3(\mathbb{Z}_8^n) \le 2^n r_3(\mathbb{Z}_4^n) \le 7.222^n,$$

however, Petrov and Pohoata [97] could prove that the stronger bound $r_3(\mathbb{Z}_8^n) \le 7.09^n$ also holds.

It is easy to see that the sequence $(r_3(\mathbb{Z}_m^n))^{1/n}$ converges to some limit $\alpha_{3,m}$. The main idea behind this observation is that with the help of the product construction one can bubble up constructions found in small dimensions. (See also Lemma 2.13). Namely, if A avoids 3AP's in dimension n, then the t-fold direct product $\underbrace{A \times A \times \cdots \times A}_{t}$ also avoids 3AP's in dimension tn.

As $\alpha_{3,m} < m$ we may say that 3AP-free sets in $\mathbb{Z}_m^n$ are *exponentially small* when $m \ge 3$. Prior to the paper [94], for longer progressions it has not yet been decided in *any* of the cases $4 \le k \le m$ whether $r_k(\mathbb{Z}_m^n)$ is also exponentially small or of order of magnitude $(m - o(1))^n$ (as $n \to \infty$). In Section 5 we will prove that whenever $6 \mid m$ and $k \in \{4, 5, 6\}$ the quantity $r_k(\mathbb{Z}_m^n)$ is exponentially small, specially,

$$r_6(\mathbb{Z}_6^n) \le 5.709^n.$$

It is tempting to also formulate this statement as $\lim(r_6(\mathbb{Z}_6^n))^{1/n} \le 5.709$, however, somewhat surprisingly, we do not see a proof of the statement that $r_6(\mathbb{Z}_6^n)^{1/n}$ converges (although we believe it surely does). The convergence is not immediate, because the product construction does not work in general. When $k = 3$ or m is a prime power, the t-fold direct product $\underbrace{A \times A \times \cdots \times A}_{t}$ avoids k-AP's when A itself is k-AP-free, however, for general k and m this fails to hold. Let us illustrate

this by the case $k = 6, m = 6$. In dimension 1 we clearly have $r_6(\mathbb{Z}_6) = 5$, and, for instance, the set $A = \{0, 1, 2, 3, 4\}$ is 6AP-free. By taking $A \times A = \{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3, 4\}$ we obtain a 25-element subset of $\mathbb{Z}_6^2$ which contains the following 6AP:

$$(0, 0), (2, 3), (4, 0), (0, 3), (2, 0), (4, 3).$$

Although the product construction is not applicable, the value of $r_6(\mathbb{Z}_6^2)$ still turns out to be $25 = 5^2$, however, we will show that $r_6(\mathbb{Z}_6^3) < 125 = (r_6(\mathbb{Z}_6))^3$.

We prove the following bounds:

Theorem 2.7 (Pach-Palincza [94]). *For sets without arithmetic progression of length* 6 *we have the following results in small dimensions:*

$$r_6(\mathbb{Z}_6^1) = 5, \quad r_6(\mathbb{Z}_6^2) = 25, \quad 117 \le r_6(\mathbb{Z}_6^3) \le 124.$$

Theorem 2.8 (Pach-Palincza [94]). *For sets without arithmetic progression of length* 6 *we have the following results:*

$$4.44^n \le 2^n r_3(\mathbb{Z}_3^n) \le r_6(\mathbb{Z}_6^n) \le 5.709^n,$$

assuming that n is sufficiently large.

If $6 \mid m$, then $\mathbb{Z}_6^n$ is a subgroup of $\mathbb{Z}_m^n$, and by using the bound from Theorem 2.8 in each of the $(m/6)^n$ cosets, the following corollary is obtained:

Corollary 2.9 (Pach-Palincza [94]). *If $6 \mid m$ and $k \in \{4, 5, 6\}$, then*

$$r_k(\mathbb{Z}_m^n) \le (0.948m)^n,$$

if n is sufficiently large.

Finally, we provide another upper bound for $r_6(\mathbb{Z}_6^n)$ in terms of $r_3(\mathbb{Z}_3^n)$.

Theorem 2.10 (Pach-Palincza [94]). *For sets without arithmetic progression of length* 6 *we have the following result:*

$$r_6(\mathbb{Z}_6^n) \le 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}.$$

Note that by using the bound $r_3(\mathbb{Z}_3^n) \le 2.756^n$, Theorem 2.10 implies that $r_6(\mathbb{Z}_6^n) \le 5.75^n$ which bound is worse than the one in Theorem 2.8. However, if $r_3(\mathbb{Z}_3^n) \le 2.69^n$, then Theorem 2.10 gives a better estimate than Theorem 2.8.

We shall mention that although the method could be applied for any finite field $\mathbb{F}_q$ with $q = p^\alpha$; since $r_3(\mathbb{F}_q^n) = r_3(\mathbb{F}_p^{\alpha n})$ the relevant cases are those when the prime power q is a prime. (The resulting upper bound from the application to $\mathbb{F}_{p^\alpha}$ is worse than the bound coming from the case of $\mathbb{F}_p$.)

There are only very few explicit values known. In the case of cap sets modulo $m = 3$ the following is known:

$$r_3(\mathbb{Z}_3^1) = 2, r_3(\mathbb{Z}_3^2) = 4, r_3(\mathbb{Z}_3^3) = 9, r_3(\mathbb{Z}_3^4) = 20, r_3(\mathbb{Z}_3^5) = 45, r_3(\mathbb{Z}_3^6) = 112.$$

Note that the 4-dimensional case corresponds to the card game SET. The author of the 6-dimensional result (Potechin [100]) and the authors of the *classification* of the unique 5-dimensional maximum cap [39], (required for the 6-dimensional case by Potechin) mentioned that they used computer calculations. Y. Edel informed us that for the paper [39] the computation time was a few weeks.

We determine the exact values in case of $\mathbb{Z}_4^n$ up to dimension 5 for 3AP-free sets and up to dimension 4 for 4AP-free sets:

Theorem 2.11 (Elsholtz-Pach [45])**.** *For sets without arithmetic progression of length* 3 *we have the following results:*

$$r_3(\mathbb{Z}_4^1) = 2,\ r_3(\mathbb{Z}_4^2) = 6,\ r_3(\mathbb{Z}_4^3) = 16,\ r_3(\mathbb{Z}_4^4) = 42,\ r_3(\mathbb{Z}_4^5) = 124.$$

Theorem 2.12 (Elsholtz-Pach [45])**.** *For sets without arithmetic progression of length* 4 *we have the following results:*

$$r_4(\mathbb{Z}_4^1) = 3,\ r_4(\mathbb{Z}_4^2) = 10,\ r_4(\mathbb{Z}_4^3) = 36,\ r_4(\mathbb{Z}_4^4) = 128.$$

As mentioned before, it is well known that results of this type can be lifted to higher dimensions and yield asymptotic results by a simple product construction, compare also Proposition 3.5 [38] in the similar setting of zero-sum free sets.

Lemma 2.13. *Let q be a prime power.*

a) Let $S_1 \subset \mathbb{Z}_q^{n_1}$ and $S_2 \subset \mathbb{Z}_q^{n_2}$ be k-progression-free sets, then $S_1 \times S_2 \subset \mathbb{Z}_q^{n_1+n_2}$ is also k-progression-free, consequently:

$$r_k(\mathbb{Z}_q^{n_1+n_2}) \geq r_k(\mathbb{Z}_q^{n_1})\, r_k(\mathbb{Z}_q^{n_2}).$$

b) A repeated application of part a) gives:

$$r_k(\mathbb{Z}_q^{nt}) \geq \left(r_k(\mathbb{Z}_q^{n})\right)^t.$$

Lifting the largest known *exact values* $r_3(\mathbb{Z}_4^5) = 124$ and $r_4(\mathbb{Z}_4^4) = 128$ gives:

Corollary 2.14.

$$r_3(\mathbb{Z}_4^n) \gg 2.622^n, \quad r_4(\mathbb{Z}_4^n) \gg 3.363^n.$$

The first result is considerably weaker than Corollary 2.4, while the second one is the strongest that is currently known. The product construction only makes use of "local" information from small dimensions. The "relative density" for the high dimensional problem is the same as for the low dimensional base-example that was lifted. Lifting for example the bound $r_3(\mathbb{Z}_4^{10}) \geq 22232$ (which is not known to be sharp), gives a better estimate $r_3(\mathbb{Z}_4^n) \gg 2.720\ldots^n$. But for $k = 3$ it is better to use the "global" information from the digits giving the lower bound $\frac{3^n}{\sqrt{n}}$. However,

for $k = m = 4$ we do not know how to replace the product construction by a better strategy.

In many cases we present constructions much better than the product construction. These use "global" properties i.e. making full use of the actual dimension n. With our current understanding this only works when $k < m$. For $k = m$ the product construction appears to be the strongest available method, see also Edel [36].

These proofs describe a set explicitly in terms of its coordinate entries, similar to the constructions by Salem and Spencer [108], and Behrend [10]. Salem and Spencer constructed progression-free sets in the integers by representing integers in an m-ary digit system, when m is odd, and using the digits $0 \le a_i \le (m-1)/2$ a fixed number of times, namely with frequency n/d for integers of length n. Restricting the digits avoids wrapping over modulo m. Behrend constructed large progression-free sets in the integers by mapping a high-dimensional sphere, which by convexity is progression-free, to the integers. He also represented integers in an m-ary system with digits $0 \le a_i \le (m-1)/2$, where m is odd, and fixed value $\sum_{i=1}^{n} a_i^2$. In the integer case the optimization of the values of m and n shows that Behrend's construction is greatly superior. In our setting we make use of both ideas, and observe that m, n are fixed by the problem, and the method of Behrend, when applicable, is only slightly stronger, but a bit more complicated.

Proposition 2.15. *Let $q \ge k \ge 3$ where the prime power q and k are fixed. The limit*

$$\alpha_{k,q} := \lim_{n\to\infty} \left(r_k(\mathbb{Z}_q^n)\right)^{1/n}$$

exists.

It follows from Theorems 2.16 and 2.17 that

$$\left\lceil \frac{m+1}{2} \right\rceil \le \alpha_{k,m} \le m.$$

For $k = 3$ more is known: $\alpha_{3,p} \le J(p)p$, when $m = p$ is an odd prime, and $J(p)$ was defined by (1).

Tao and Vu [120, exercise 10.1.3] observe that there is a construction in $\mathbb{Z}_m^n$ with at least $\frac{[m/2]^n}{m^2 n^2}$ points without 3-progression (based on Behrend's construction).[1]

Lin and Wolf [79] proved the following: If m is a prime and $k \le m$, then

$$r_k(\mathbb{Z}_m^n) \ge \left(m^{2(k-1)} + m^{k-1} - 1\right)^{\frac{n}{2k}} \approx m^{\frac{(k-1)n}{k}}.$$

Their proof makes use of a product construction, as explained in Lemma 2.13. They also have some results, when m is a pure prime power, but this refers to finite fields $\mathbb{F}_m$, which are different from $\mathbb{Z}_m$. In particular, when m is prime and

[1] It seems they possibly intended the denominator to be $m^2 n$ (in our notation).

m^{k-1} is large, and n increases, the exponential growth of the lower bound is based on the constant $m^{\frac{k-1}{k}}$ compared to the obtained $\lfloor \frac{m+2}{2} \rfloor$ here.

We now give our general theorems, which improve the above lower bound and remove the prime condition on m:

Theorem 2.16 (Elsholtz-Pach [45]). *Let $m \geq 5$ be odd. There exists some $C_m > 0$ such that*

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+1}{2}\right)^n.$$

Moreover, with

$$\sigma_m = \sqrt{\frac{1}{2880}(m^4 + 4m^3 - 14m^2 - 36m + 45)}$$

one can choose $C_m = \frac{1}{3\sqrt{3}\sigma_m}$. For large m one has $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}m^2}$.

The case $m = 5$ also improves the asymptotic lower bound of affine caps, for details see Section 2.1. In the case $m = 3$ this would give a lower bound of $\gg \frac{2^n}{\sqrt{n}}$ only which is smaller than the trivial lower bound by taking all 2^n elements with coordinate entries 0 or 1. Also note that in view of $r_k(\mathbb{Z}_m^n) \geq r_3(\mathbb{Z}_m^n)$ the theorem trivially induces lower bounds for any $k \geq 3$ (also in the theorem below).

A crucial idea again is to avoid any product construction and to use one more digit than Tao and Vu [120, exercise 10.1.3] used, with some extra constraints, which are less costly (if m is constant and n increases). Their lower bound $\frac{m^n}{2^n} \cdot \frac{1}{m^2 n^2}$ in case $m = 4$ would also be weaker than the trivial progression-free set $\{0,1\}^n$ with 2^n elements.

Theorem 2.17 (Elsholtz-Pach [45]). *Let $m \geq 4$ be even. There exists some $C_m > 0$ such that*

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+2}{2}\right)^n.$$

With

$$\sigma_m = \sqrt{\frac{m^4 + 8m^3 + 4m^2 - 48m}{2880}}$$

one can choose $C_m = \frac{1}{3\sqrt{3}\sigma_m}$. For large m one has $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}m^2}$.

(A version of this result, in the special case $m = 8$ has also been observed in [97], having seen a precursor of [45]. Their main concern is an improvement of the upper bound.)

As is well known from Behrend's construction there are good reasons to restrict to half of the available digits. In the above cases we go up to one element more than half of the digits. In the cases of even m one additionally has to study progressions of type $0\frac{m}{2}0$ carefully. In the examples below we go even further, and note that those progressions which actually use the reduction modulo m cause quite a bit of extra work. (For example, in the case $r_4(\mathbb{Z}_{11}^n)$ we have to care about progressions of type $1, 6, 0, 5$ modulo 11.)

Theorem 2.18 (Elsholtz-Pach [45]). *The following holds:*

$$r_4(\mathbb{Z}_{11}^n) \gg \frac{7^n}{n^3}.$$

(No attempt was made to reduce the exponent 3.) For comparison Lin and Wolf [79] have a lower bound of about about 6.04^n. (For fixed k the improvement increases, as m increases.)

It is clear that on a case by case study one can prove related results for several individual values of m and k. Here we present two further cases where these ideas are generalized to infinite families $m = p^s, k = p^{s-1}+1$ (or $k = p^{s-2}+1$ respectively), where p is prime. It should be noted that in this case the set of digits used is not consecutive, but makes use of the structure of orbits of length p, and hence the algebraic structure. As can be seen, several good properties are preserved: many progression types can be excluded by the Salem-Spencer "same-frequency property", and the "all-elements-distinct" property (i.e. proper progressions).

Theorem 2.19 (Elsholtz-Pach [45]). *Let $m = p^s$ be a pure prime power, $s \geq 2$. Let $k = p^{s-1}+1$. Then there exist constants $C_m > 0$ and $0 < c_m \leq m/2$ such that the following holds:*

$$r_k(\mathbb{Z}_m^n) \geq C_m \frac{(m-p+1)^n}{n^{c_m}}.$$

Corollary 2.20 (Elsholtz-Pach [45]). *There exist positive constants C_m and $c_m \leq m/2$ such that the following holds:*

$$r_3(\mathbb{Z}_4^n) \geq C_4 \frac{3^n}{n^{c_4}},$$

$$r_5(\mathbb{Z}_8^n) \geq C_8 \frac{7^n}{n^{c_8}},$$

$$r_{10}(\mathbb{Z}_{27}^n) \geq C_{27} \frac{25^n}{n^{c_{27}}},$$

$$r_{26}(\mathbb{Z}_{125}^n) \geq C_{125} \frac{121^n}{n^{c_{125}}},$$

$$r_{102}(\mathbb{Z}_{101^2}^n) \geq C_{10201} \frac{10101^n}{n^{c_{10201}}}.$$

Theorem 2.21 (Elsholtz-Pach [45]). *Let $m = p^s$ be a pure prime power, $s \geq 3$. Let $k = p^{s-2}+1$. Then there exist constants $C_m > 0$ and $0 < c_m \leq m/2$ such that the following holds:*

$$r_k(\mathbb{Z}_m^n) \geq C_m \frac{(m-2p^2+2p)^n}{n^{c_m}}.$$

For $p = 2$, this is certainly not best possible. By Theorem 2.17 for $m = 8, k = 3$ one can use 5 digits, rather than 4.

Corollary 2.22 (Elsholtz-Pach [45]). *There exist positive constants C_m and $c_m \le m/2$ such that the following holds:*

$$r_{p+1}(\mathbb{Z}_{p^3}^n) \ge C_{p+1}\frac{(p^3-2p^2+2p)^n}{n^{c_{p+1}}},$$
$$r_4(\mathbb{Z}_{27}^n) \ge C_{27}\frac{15^n}{n^{c_{27}}},$$
$$r_{82}(\mathbb{Z}_{729}^n) \ge C_{729}\frac{717^n}{n^{c_{729}}},$$
$$r_6(\mathbb{Z}_{125}^n) \ge C_{125}\frac{85^n}{n^{c_{125}}},$$
$$r_{26}(\mathbb{Z}_{625}^n) \ge C_{625}\frac{585^n}{n^{c_{625}}}.$$

We are not aware of any earlier results of this type.

We now briefly discuss some aspects of the proofs of the exact values and of a conditional upper bound.

For the estimates of $r_3(\mathbb{Z}_4^n)$ we shall need a reformulation of the problem which is presented in Section 4.1. Let us say that a system of subsets $A(x) \subseteq \mathbb{F}_2^n$ $(x \in \mathbb{F}_2^n)$ satisfies property $(*)$, if the following implication holds:

$$\forall x \in \mathbb{F}_2^n \ (y \in x + A(x)\hat{+}A(x) \implies A(y) = \varnothing). \qquad (*)$$

(Note that for $A(x) = \varnothing$ we define $x + A(x)\hat{+}A(x) := \varnothing$.) In Lemma 4.1 we will show that the largest possible total size of a system of subsets satisfying property $(*)$ is exactly $r_3(\mathbb{Z}_4^n)$. Hence, estimating the maximal total size of a system of subsets $\{A(x) : x \in \mathbb{F}_2^n\}$ satisfying $(*)$ is equivalent with our original question.

As it turns out it is very useful that we can reduce the case of arbitrary subsets $A(x)$ to the case of subspaces. We do not know, if this can be done for higher dimension, but for the low dimensions studied here explicitly this is a quite powerful method.

In this case, the upper bound $O(3^n)$ is quite close to the general lower bound in the unrestricted case, namely $r_3(\mathbb{Z}_4^n) \gg 3^n/\sqrt{n}$.

Theorem 2.23 (Elsholtz-Pach [45]). *If the system of subsets $A(x)$ satisfies $(*)$ and all non-empty subsets $A(x)$ are subspaces, then*

$$\sum_{x\in\mathbb{F}_2^n} |A(x)| \le 3^n.$$

Note that for $n = 1$ any 2-element subset forms a progression-free subset in $\mathbb{Z}_4^n$. If $n \in \{2,3,4\}$, then the extremal construction is also unique in the following sense:

Theorem 2.24 (Elsholtz-Pach [45]). *Let $n \in \{2,3,4\}$. If the systems of subsets $\{A(x) : x \in \mathbb{F}_2^n\}$ and $\{A'(x) : x \in \mathbb{F}_2^n\}$ both have total size $r_3(\mathbb{Z}_4^n)$ and they satisfy $(*)$, then there is an invertible affine linear transformation $\varphi : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ and vectors $c(x) \in \mathbb{Z}_2^n$ $(x \in \mathbb{Z}_2^n)$ such that $A'(x) = A(\varphi(x)) + c(x)$ for every $x \in \mathbb{Z}_2^n$.*

2.1 Caps

An affine cap in $AG(n,q)$ is a set in $\mathbb{F}_q^n$ with no three points on a line. Here we set $m = q$, and study sets without three points on a line in $\mathbb{Z}_m^n$. In other words, when $m = q$ is a prime, caps in $\mathbb{Z}_m^n$ and $AG(n,q)$ are the same. The condition "no three points on a line" can be expressed by linear equations of the type $ax + by + cz = 0$ (where $a + b + c = 0$). As we see below when $m = 3, 5$ it is enough to consider the case of arithmetic 3-progressions, $x - 2y + z = 0$. The case $m = 4$ does not correspond to affine caps, as $\mathbb{Z}_4 \neq \mathbb{F}_4$, but in $\mathbb{Z}_m$ with $m = 3, 4, 5$ any line with three points actually contains 3 points in arithmetic progression. To see this modulo $m = 5$, one just has to examine all cases in one dimension. There are obvious cases such as $\{0, 1, 2\}$ or $\{0, 2, 4\}$. The crucial case is that also the example $\{0, 1, 3\} \subset \mathbb{Z}_5$ is a progression, as $1, 3, 5 = 0$ is a progression.

Modulo $m = 3$ the cap set problem is known even from the popular card game SET. The size of the caps in dimension up to 6 are:

$$r_3(\mathbb{Z}_3) = 2, r_3(\mathbb{Z}_3^2) = 4, r_3(\mathbb{Z}_3^3) = 9, r_3(\mathbb{Z}_3^4) = 20, r_3(\mathbb{Z}_3^5) = 45, r_3(\mathbb{Z}_3^6) = 112.$$

More generally modulo prime $m = q$ the following is known about affine caps in $\mathbb{Z}_m^n = AG(n,q)$ (we would like to thank Yves Edel for this collection):
in dimension
$n = 2$: one has $m + 1$ points (a so called oval),
$n = 3$: one has m^2 points (which is the affine part of an ovoid in projective space),
$n = 4, m = 5$ at least 65 points (which is the affine part of a projective cap of 66 points, see [12],
$n = 5, m = 5$ one has at least 195 points,[2]
$n = 6$: one has at least $m^4 + m^2 - 1$ points, see Edel [36].

For large dimensions, the best lower bound constructions are due to Edel [36] and are based on a tensor product construction of this best cap in dimension 6. For prime m, this gives a lower bound of $r_3(\mathbb{Z}_m^n) \geq m^{n(\log_m(m^4+m^2-1))/6}$ (which is also the construction of Lin and Wolf [79]) and this gives an asymptotic exponent of about 2/3.

Some refinements are known, when $q = 3$ or $q = 4$ (finite field case, different from $\mathbb{Z}_4$). Edel [36] writes: "No better lower bound seems to be known for general q, except for the ternary and quaternary cases."

Especially in the case $m = 3$ there have been a number of refinements to an exponent of 0.72625. The progress over the record 0.7218 from 30 years ago (see [23]) seems small, but this progress is, of course, on a logarithmic scale.

When $m = 5$, the above lifting from dimension 6 gives a lower bound of $5^{0.6705n} \approx 2.9421^n$ points. In contrast, Theorem 2.16 above gives the lower bound of $C_5 3^n/\sqrt{n} \approx 5^{0.6826n}$ points. It may be possible to optimise the constant C_5 in

[2] in fact, here the caps in $PG(5,5)$ and $AG(5,5)$ have the same number of points, see `https://www.mathi.uni-heidelberg.de/~yves/Matritzen/CAPs/Matrizen/(195,5,5).html`

the construction modulo 5, similar to the case $m = 4$ in Theorem 2.3. In any case this improvement appears to be the first improvement for any affine cap in $AG(n, m)$, when $m = q \geq 5$.

As the case of affine caps modulo primes (or prime powers) has been well studied in the literature it seems somewhat surprising to us that the quite simple construction of vectors with $n/3$ of the entries being 1, and the other $2n/3$ of the entries being 0 or 2 has not been observed before, which still asymptotically breaks the record. The reason may be that the improvement actually can only be seen for $n \geq 138$. Even with an improved constant C_5 one will not see the improvement for small dimensions.

2.2 Line-free sets

In the intersection of finite geometry and extremal combinatorics numerous problems about finding maximal subsets of affine or projective spaces avoiding certain configurations have been studied. For instance, in case of the previously discussed cap set problem 3-term arithmetic progressions coincide with affine lines, thus progression-free sets are the same as line-free sets.

It is a natural question to ask for bounds on the cardinality of subsets of the n-dimensional affine space over an arbitrary finite field $\mathbb{F}_q$ that do not contain a full line.

Since in the case when p is a prime, p-progressions in $\mathbb{F}_p^n$ correspond to lines in the n-dimensional affine space, therefore, we are interested in bounds on $r_p(\mathbb{F}_p^n)$.

For the general case surprisingly only few results on $r_p(\mathbb{F}_p^n)$ are known. There is the trivial lower bound $r_p(\mathbb{F}_p^n) \geq (p-1)^n$ achieved by a hypercube of side length $p-1$. Jamison [70] and Brouwer and Schrijver [20] independently proved that this is sharp for $n = 2$. For $n = 3$ the only improvement to this construction was by a single point described in the post of Zare in a mathoverflow thread [124]. We prove the following lower bounds:

Theorem 2.25 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43])**.**
Let $p \geq 5$ be a prime, then

$$r_p(\mathbb{F}_p^3) \geq (p-1)^3 + p - 2\sqrt{p} = p^3 - 3p^2 + 4p - 2\sqrt{p} - 1.$$

This can be improved in some special cases.

Theorem 2.26 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43])**.**
Let p be a prime with $p \equiv 7 \pmod{24}$, then

$$r_p(\mathbb{F}_p^3) \geq (p-1)^3 + (p-1) = p^3 - 3p^2 + 4p - 2.$$

Moreover, $r_7(\mathbb{F}_7^3) \geq 225$.

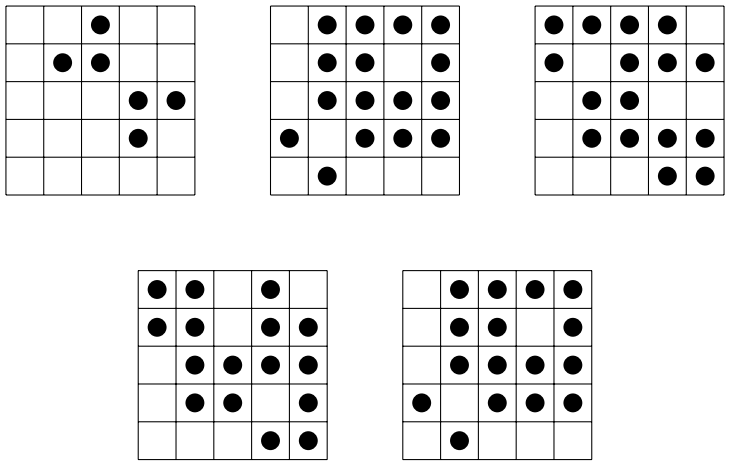


Figure 1: A line-free set showing $r_p(\mathbb{F}_p^3) \geq 70$

The simple upper bound $r_p(\mathbb{F}_p^n) \leq p^n - \frac{p^n-1}{p-1}$ was given by Aleksanyan and Papikian [1] and was achieved by removing at least one point from each line going through a fixed point. In particular $r_p(\mathbb{F}_p^3) \leq p^3 - p^2 - p - 1$. The stronger bounds $r_p(\mathbb{F}_p^n) \leq p^n - 2p^{n-1} + 1$ and $r_p(\mathbb{F}_p^3) \leq p^3 - 2p^2 + 1$ can be obtained by a result of Sziklai [117, Proposition 4.1] (see also [7], [13]). We give the following new bounds:

Theorem 2.27 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]). *Let $p \geq 3$ be a prime, $k \in \{3, 4, \ldots, p\}$ and $n \in \mathbb{N}$, then*

$$r_k(\mathbb{F}_p^{n+1}) \leq \frac{2(p^{n+1}-1)r_k(\mathbb{F}_p^n) + p^n - \sqrt{4(p^{n+1}-1)r_k(\mathbb{F}_p^n)(p^n - r_k(\mathbb{F}_p^n)) + p^{2n}}}{2p^n}.$$

The three-dimensional case gives the following corollary.

Corollary 2.28 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]). *Let $p \geq 3$ be a prime, then*

$$r_p(\mathbb{F}_p^3) \leq \frac{2p^5 - 4p^4 + 2p^3 - p^2 + 4p - 2 - \sqrt{8p^6 - 20p^5 + 17p^4 - 12p^3 + 20p^2 - 16p + 4}}{2p^2},$$

in particular,

$$r_p(\mathbb{F}_p^3) \leq p^3 - 2p^2 - (\sqrt{2} - 1)p + 2.$$

For other dimensions, there is the lower bound $r_p(\mathbb{F}_p^{2p}) \geq p(p-1)^{2p-1}$ due to Frankl et al [56], using large sunflower-free sets.

We found a 70-point 5AP-free set in $\mathbb{F}_5^3$ via a branch and cut approach (see Figure 1) and showed the following upper bounds for small primes.

Theorem 2.29 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]). $r_5(\mathbb{F}_5^3) < 74$.

Theorem 2.30 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).
$r_7(\mathbb{F}_7^3) < 243$.

According to Lemma 2.13 one can use the product $S_1 \times S_2$ of two line-free sets $S_1 \subseteq \mathbb{F}_p^{n_1}$, $S_2 \subseteq \mathbb{F}_p^{n_2}$ to get a line-free set in the higher dimension $n_1 + n_2$. This construction also provides us the lower bound $|S_1|^{1/n_1}$ for $\alpha_p := \lim_{n\to\infty}(r_p(\mathbb{F}_p^n))^{1/n}$, and therefore the asymptotic lower bound $(|S_1|^{1/n_1} - o(1))^n$ for $r_p(\mathbb{F}_p^n)$ (see also e.g. [33], [93]). The strongest known lower bound for general p is

$$\alpha_p \geq p^{1/2p}(p-1)^{(2p-1)/2p}$$

using the results of Frankl et al [56], however for small primes the new three-dimensional lower bounds $r_5(\mathbb{F}_5^3) \geq 70$ and $r_7(\mathbb{F}_7^3) \geq 225$ give better lower bounds, namely, $\alpha_5 \geq 4.121$ and $\alpha_7 \geq 6.082$.

We also show the following explicit lower bound for arbitrary dimension (see Table 1 for comparisons).

Theorem 2.31 (Elsholtz-Führer-Füredi-Kovács-Pach-Simon-Velich [43]).
Let $p \geq 3$ be a prime, then $r_p(\mathbb{F}_p^n) \geq (p-1)^n + \frac{n-2}{2}(p-1)(p-2)^{n-3}$.

p	5	7	11	13	17
$n = 3$	4.041	6.027	10.016	12.013	16.010
$n = 4$	4.046	6.034	10.022	12.019	16.014
$n = 5$	4.041	6.034	10.024	12.020	16.016
$n = 6$	4.034	6.031	10.024	12.021	16.017
$n = 7$	4.027	6.028	10.023	12.020	16.017
$n = 2p$	4.090	6.066	10.043	12.037	16.028

Table 1: The bases a for the lower bounds $r_p(\mathbb{F}_p^n) \geq a^n$ that can be achieved by Theorem 2.31 for small primes. The last row gives bounds that can only be used for dimensions at least $2p$, using the results of Frankl et al. [56].

3 Proofs of the asymptotic lower bounds

In this section we prove the asymptotic lower bounds. We will use several times that the central multinomial coefficients can be approximated by Stirling's formula:

Lemma 3.1. *Let $d \geq 2$ be an integer. There exists a constant c_d such that*

$$\binom{dn}{n,\ldots,n} \sim c_d \frac{d^{dn}}{n^{(d-1)/2}}.$$

Here we give a geometrically inspired proof of Corollary 2.4.

Proof of Corollary 2.4 (Proof 2): The crucial idea is that an arithmetic progression of length 3 (with 3 distinct points) in $\mathbb{Z}_4^n$ has a uniquely defined middle point. (For comparison, this is not the case in $\mathbb{Z}_3^n$.)

We relate the problem to a problem posed by Leo Moser [84]. Find in $H = \{0,1,2\}^n$ the maximal set of elements without "three on a line" (which is also known as Moser's cube problem). Observe that in this case there is no reduction modulo 3. Let $f(n)$ denote the largest such number in $H = \{0,1,2\}^n$. It is known that $f(1) = 2, f(2) = 6, f(3) = 16$, (see Chvátal [27]), $f(4) = 43$ (see Chandra [25]), $f(5) = 124, f(6) = 353$ [98]. In dimensions 1, 2, 3 and 5 these values are the same as $r_3(\mathbb{Z}_4^n)$, but in dimension 4 one has that $r_3(\mathbb{Z}_4^4) = 42 < f(4) = 43$.

A simple observation by Komlós [75] shows that $f(n) \gg \frac{3^n}{\sqrt{n}}$, and the implicit constant was refined again by Chvátal [26]. The construction by Chvátal relates the problem to coding theory and gives $f(5) \geq 124$, for example.

Let us adapt Komlós' [75] observation to our situation: the set

$$S = \{(x_1,\ldots,x_n) \in \{0,1,2\}^n : x_i = 1 \text{ for } m = \lfloor n/3 \rfloor \text{ values } i\}$$

has the claimed number of elements and has no three points on a line.

Now, let us count the number of such points. Let n be a multiple of 3, then by Stirling's formula S has

$$\begin{aligned} |S| &= 2^{n-m}\tbinom{n}{m} = 2^{2n/3}\tbinom{n}{n/3} \\ &\sim 2^{2n/3}\frac{\sqrt{2\pi n}n^n}{e^n}\frac{e^{n/3}}{\sqrt{2\pi n/3}(n/3)^{n/3}}\frac{e^{2n/3}}{\sqrt{2\pi 2n/3}(2n/3)^{2n/3}} \gg \frac{3^n}{\sqrt{n}} \end{aligned}$$

elements. When $n \equiv 1,2 \bmod 3$ we have the same order of magnitude, up to a constant factor, for example, by filling the extra 1 or 2 coordinates with entries from $\{0,1\}$. Further observe that for three points P_1, P_2, P_3 to be on a line (in this order), in each coordinate
either i) all entries are the same,
or ii) the entries are $0,1,2$ or $2,1,0$ (in this order). Since the number of "middle entries 1" is constant for all points, there cannot be an arithmetic progression of three distinct digits.

Let us embed the set S from $\{0,1,2\}^n$ canonically into $G = (\mathbb{Z}_4^n, +)$. Think of G as the lattice points $\{0,1,2,3\}^n$ but now with reduction modulo 4 in each coordinate. Observe that the set S does not have a single "3" entry. An arithmetic progression of length 3 modulo 4 that does not make use of $x_i = 3$ in any coordinate must be of one of the types listed below. In a given coordinate the digits are:
i) the same,
ii) or are $0,1,2$ or $2,1,0$ in this order,
iii) or $0,2,0$, or $2,0,2$.

We will show that the set $S \subset \mathbb{Z}_4^n$ does not contain a proper 3-progression. Suppose S does contain three distinct points P_1, P_2, P_3 in arithmetic progression. The case i) where all entries are the same does not play any role. Let us look at those coordinates where the entries differ. Since all points have the same number of 1 entries, let us study, where one of the three elements uses a "1", but another point does not: For this, the only possibilities are $0,1,2$ and $2,1,0$. But here only the middle point P_2 can make use of a 1. So, the two points P_1 and P_3 cannot make use of their 1's, unless all three entries are identically 1. This means that all three points have their 1's in exactly the same position, and that there is no coordinate with a progression 012 or 210. So, let us look at the other coordinates. The only possibilities left are 020 or 202. But then P_1 and P_3 would be the very same point, which is a contradiction to the definition of a proper progression. □

Proof of Proposition 2.15. The idea of this proof might go back to Shannon [113], see also Davis and Maclagan [33]. Let $\alpha_{k,m}(n) = (r_k(\mathbb{Z}_m^n))^{1/n}$, so that we have the following properties: By the product construction (Lemma 2.13) we have

$$r_k(\mathbb{Z}_m^{n_1}) r_k(\mathbb{Z}_m^{n_2}) \le r_k(\mathbb{Z}_m^{n_1+n_2}),$$

that is,

$$\alpha_{k,m}(n_1)^{n_1} \alpha_{k,m}(n_2)^{n_2} \le \alpha_{k,m}(n_1+n_2)^{n_1+n_2},$$

and therefore

$$n_1 \log \alpha_{k,m}(n_1) + n_2 \log \alpha_{k,m}(n_2) \le (n_1+n_2) \log \alpha_{k,m}(n_1+n_2).$$

Therefore, the sequence $\{n \log \alpha_{k,m}(n)\}_{n=1}^{\infty}$ is superadditive.

By Fekete's Lemma on superadditive sequences the limit $\lim_{n\to\infty} \log \alpha_{k,m}(n)$ exists and equals $\sup_n \log \alpha_{k,m}(n)$.

□

Proof of Theorem 2.16: Let us first prove a slightly weaker result based on the Salem-Spencer construction [108] for sets of integers without 3AP's. Recall that

m is odd and that we only need to study $k = 3$. Assume first that n is a multiple of $(m+1)/2$. Choose vectors with digits

$$a_i \in \left\{0, 1, 2, \ldots, \frac{m-1}{2}\right\}$$

with exactly n_i entries of digit i, where $i \in \left\{0, 1, 2, \ldots, \frac{m-1}{2}\right\}$. The number of such vectors is maximized when $n_i = \frac{n}{(m+1)/2}$ for every i. This gives at least $C_m(\frac{m+1}{2})^n \frac{1}{n^{c_m}}$ points, for positive constants C_m and c_m. If n is not a multiple of $(m+1)/2$ one can fill the remaining coordinates with entries $0 \le a_i \le \frac{m-1}{2}$, which slightly weakens the constant C_m.

We show that there is no arithmetic 3-progression: by the choice of the allowed digits, if the digit $a > 0$ occurs, then the digit $m - a \equiv -a \bmod m$ is forbidden, so 0 is never in the centre of a proper 3-progression. As all vectors have the same number of 0 entries, all of these digits 0 must occur in the same coordinate position, giving a trivial 000-progression. By continuing this, all nontrivial 3-progressions, without the digit 0 do not have a digit 1 in the centre, and hence the digit 1 can only come from a 111-progression.

To do an explicit example, let $m = 11, k = 3$, we use the digits: $0, 1, 2, 3, 4, 5$. A complete list of all possible 3-progressions of these digits is:

$$\begin{cases} 000, 111, 222, 333, 444, 555, \\ 012, 024, 123, 135, 234, 210, 345, 321, 420, 432, 531, 543. \end{cases}.$$

As there are three distinct points, there must be a proper 3-progression of three distinct digits abc. As the digit 0 is never in the centre of any of these nontrivial 3-progressions, and as all vectors have the same number of 0 entries, the digit can only occur in the trivial way: 000. This leaves the following shorter list of nontrivial 3-progressions:

$$123, 135, 234, 321, 345, 432, 531, 543.$$

Now the digit 1 is never in the centre, and 1 can only occur in the trivial 111 progression, leaving the list $234, 345, 432, 543$. Now, the digit 2 is never in the centre, so 2 can only occur as 222, leaving $345, 543$. Now 3 is never in the centre, which gives the final contradiction.

Note that initially we have restricted the frequency of all digits $0, 1, 2, 3, 4, 5$, but we can now observe that restricting the frequency of the digits $0, 1, 2, 3$ is enough.

Based on a comment of a referee of paper [45], we can also observe that one gets some saving on the number of restrictions, when fixing the total number of occurrences of "digit is 0 or 5". As there is no 0 or 5 in the centre position one can remove 0 and 5 so that the list of nontrivial progressions

$$012, 024, 123, 135, 234, 210, 345, 321, 420, 432, 531, 543$$

immediately shrinks to $123,234,321,432$. Now a second condition such as "the total number of occurrences of 1 and 4 is constant" also forbids these cases, so we have used only two restrictions. In general it seems that about $m/4$ such restrictions of joint occurrence of digits a and $(m-1)/2-a$ are sufficient.

We now prove the theorem in its full strength, based on Behrend's construction. The number of elements used is only larger by a factor n^c.

Let m be odd, and n be a multiple of $(m+1)/2$. Let

$$S_R = \left\{(a_1,\dots,a_n) : a_i \in \{0,1,\dots,(m-1)/2\},\ \sum_{i=1}^{n}\left(a_i - \frac{m-1}{4}\right)^2 = R\right\}.$$

Here S_R can be thought of as a sphere about centre $((m-1)/4,\dots,(m-1)/4))$ with R as squared radius. We prove that all S_R are progression-free and there exists an S_R of size at least

$$C_m \frac{1}{\sqrt{n}}\left(\frac{m+1}{2}\right)^n.$$

Suppose there are three distinct points P_1, P_2, P_3 in arithmetic progression. None of the progressions in a fixed coordinate makes use of the reduction modulo m, so the convexity of the geometric sphere gives a contradiction. But let us look at this arithmetically: Let the progression in the i-th coordinate be a_i-d_i, a_i, a_i+d_i. Then for the three points one has that

$$\sum_{i=1}^{n}\left(a_i - d_i - \frac{m-1}{4}\right)^2 = \sum_{i=1}^{n}\left(a_i - \frac{m-1}{4}\right)^2 = \sum_{i=1}^{n}\left(a_i + d_i - \frac{m-1}{4}\right)^2.$$

Then

$$\sum_{i=1}^{n}\left(\left(a_i + d_i - \frac{m-1}{4}\right)^2 + \left(a_i - d_i - \frac{m-1}{4}\right)^2 - 2\left(a_i - \frac{m-1}{4}\right)^2\right) = 0.$$

This yields $\sum_{i=1}^{n} 2d_i^2 = 0$. Hence $d_i = 0$ for all i. In other words, the three points are identical, which is a contradiction.

The size of large sets S_R follows from the observation that most elements in $(a_1,\dots,a_n) \in [0, \frac{m-1}{2}]^n$ have a value of $R = \sum_{i=1}^{n}(a_i - \frac{m-1}{4})^2$ in an interval of size the standard deviation around the mean value. To make this more precise, we follow Elkin [40] and consider $a_i - \frac{m-1}{4}$ as independent random variables $Y_1,\dots,Y_n$, distributed uniformly in $\{-(m-1)/4,\dots,(m-1)/4\}$, and

$$Z_i = Y_i^2\ (i \in \{1,\dots,n\}), \quad Z = \sum_{i=1}^{n} Z_i.$$

The expected value is

$$\mu_m := \mathbb{E}(Z_i) = \frac{1}{(m+1)/2}\sum_{i=-(m-1)/4}^{(m-1)/4} i^2 = \frac{1}{48}m^2 + \frac{1}{24}m - \frac{1}{16}$$

and $\mathbb{E}(Z) = n\mathbb{E}(Z_i)$. The variance is

$$\begin{aligned}\mathrm{Var}(Z_i) &= \mathbb{E}(Z_i^2) - \mathbb{E}(Z_i)^2 \\ &= \tfrac{m^4}{1280} + \tfrac{m^3}{320} - \tfrac{11m^2}{1920} - \tfrac{17m}{960} + \tfrac{5}{256} - \left(\tfrac{1}{48}m^2 + \tfrac{1}{24}m - \tfrac{1}{16}\right)^2 \\ &= \tfrac{1}{2880}\left(m^4 + 4m^3 - 14m^2 - 36m + 45\right),\end{aligned}$$

and $\mathrm{Var}(Z) = n\mathrm{Var}(Z_i)$.

The standard deviation is $\sigma_m = \sqrt{\mathrm{Var}(Z_i)}$ and $\sigma_Z = \sqrt{\mathrm{Var}(Z)} = \sigma_m\sqrt{n}$, where σ_m depends only on m. By Chebychev's inequality

$$\mathbb{P}(|Z - \mathbb{E}(Z)| > a\sigma_Z) \le \frac{1}{a^2}.$$

With $a = \sqrt{3}$ we see that for at least two thirds of all elements in $[0, \frac{m-1}{2}]^n$ the sum of digit squares-distances from the centre point $\left(\frac{m-1}{4}, \ldots, \frac{m-1}{4}\right)$ is in the interval $[\mu_m n - a\sigma_Z, \mu_m n + a\sigma_Z]$. By the pigeonhole principle there exists a squared radius R with frequency at least $\frac{C_m}{\sqrt{n}}\left(\frac{m+1}{2}\right)^n$, where

$$C_m = \frac{2}{3 \cdot 2\sqrt{3}\sigma_m} = \frac{1}{3\sqrt{3}\sigma_m}.$$

Note that $\sigma_5 = \frac{\sqrt{2}}{3}, \sigma_7 = 1, \sigma_9 = \sqrt{\frac{14}{5}}$. As the proof only makes use of effective bounds, the result is valid for all odd $m \ge 5$ and all n. If the odd value m tends to infinity, then, asymptotically $\sigma_m \sim \frac{m^2}{24\sqrt{5}}$ holds, giving the claimed value of C_m. □

Remark 3.2. *While the Salem-Spencer type construction with all frequencies of the digits being constant is completely explicit, the above Behrend-type proof uses the pigeonhole principle, which is not explicit, and in algorithmic terms slow, as one would need to search for a good value R. However, a result of Rankin [101] gives entirely explicit bounds on the number of representations of numbers as a sum of n squares of bounded size. In particular this shows that not only there are good values R but that* all *values R in the interval are good, when weakening the constant C_m by a small factor only. In particular, one can choose $R = \lfloor \mu n \rfloor$. In another direction, as the above argument does not make use of reduction modulo m, it seems possible to implement the improvement by Elkin [40], which might gain an extra factor, maybe of size n^c. Elkin observed that 3-progressions in a suitable union of spheres (annulus) are geometrically quite restricted. One can then prove that there is a large subset of this union which is progression-free.*

Proof of Theorem 2.17: Again, we first prove a sightly weaker version based on the Salem-Spencer construction. This proof is similar to the previous case, but as m is even there is one extra complication to care for. Assume first that n is a multiple of $(m+2)/2$, and that there is an arithmetic progression of three distinct points.

Choose vectors with exactly n_i entries of digit i, where $i \in \{0, 1, 2, \ldots, \frac{m}{2}\}$. The number of such vectors is maximized when $n_i = \frac{n}{(m+2)/2}$ for every i. This gives at least $(\frac{m+2}{2})^n \frac{C'_m}{n^{c_m}}$ points. If n is not a multiple of $(m+2)/2$ one can fill the remaining coordinates with 0 entries, which will slightly weaken the constant C'_m.

Working out the set of all nontrivial 3-progressions, one observes that the boundary values 0 and $m/2$ occur as values in the middle position only in the progressions of type $0\frac{m}{2}0$, $\frac{m}{2}0\frac{m}{2}$ or constant progressions. This means that the values of 0 or $\frac{m}{2}$ can occur in constant 3-progressions, 000, $\frac{m}{2}\frac{m}{2}\frac{m}{2}$ and in the same number of progressions of types $0\frac{m}{2}0$ and $\frac{m}{2}0\frac{m}{2}$. Hence other nontrivial progressions using 0 or $\frac{m}{2}$ (e.g. like 012) never occur.

By definition of a proper 3-progression we search for three *distinct* points, this means there must be somewhere another nontrivial progression abc with three distinct digits in $\{1, 2, \ldots, \frac{m}{2} - 1\}$. One can then continue iteratively as before, and conclude that there is no nontrivial 3-progression of 3 distinct points. (As in the case of odd m it is possible to reduce the number of restrictions, for example by fixing the joint occurrences of digits a and $m/2 - a$.)

Let us define the Behrend-sphere:

$$S_R = \left\{ (a_1, \ldots, a_n) : a_i \in \{0, 1, \ldots, m/2\}, \sum_{i=1}^{n} \left(a_i - \frac{m}{4} \right)^2 = R \right\}.$$

We prove that S_R is 3-progression-free in $\mathbb{Z}_m^n$. The estimate on the number of points is as in the case of odd m above.

Suppose there are three distinct points P_1, P_2, P_3 in arithmetic progression. The nonconstant progressions in a fixed coordinate do not make use of the reduction modulo m, with the two exceptions of $0\frac{m}{2}0$ and $\frac{m}{2}0\frac{m}{2}$. Let $n_1, n_2, \ldots, n_s$ denote the number of coordinates with a fixed progression-pattern such as 000, 012, 024 etc. Of these, let n_1 count the pattern $0\frac{m}{2}0$ and and n_2 count the pattern $\frac{m}{2}0\frac{m}{2}$. As all other patterns do not wrap over modulo m let n_i count the pattern $p_i - d_i, p_i, p_i + d_i$.

Hence $\sum_{i=1}^{s} n_i = n$. The points $(a_1, \ldots, a_n)$ in S_R lie on a sphere with centre $(m/4, \ldots, m/4)$. Let the progression pattern of the j-th coordinates be p_j –

$d_j, p_j, p_j + d_j$. Then for the three points P_1, P_2, P_3 one has that

$$n_1\frac{m^2}{16} + n_2\frac{m^2}{16} + \sum_i n_i\left(p_i - d_i - \frac{m}{4}\right)^2 = n_1\frac{m^2}{16} + n_2\frac{m^2}{16} + \sum_i n_i\left(p_i - \frac{m}{4}\right)^2 =$$
$$= n_1\frac{m^2}{16} + n_2\frac{m^2}{16} + \sum_i n_i\left(p_i + d_i - \frac{m}{4}\right)^2.$$

Then

$$\sum_{i=3}^{s} n_i\left(\left(p_i + d_i - \frac{m}{4}\right)^2 + \left(p_i - d_i - \frac{m}{4}\right)^2 - 2\left(p_i - \frac{m}{4}\right)^2\right) = 0.$$

This yields $\sum\limits_{i=3}^{s} n_i 2d_i^2 = 0$. Hence for all nonconstant patterns with $i \geq 3$ one has that $n_i = 0$. The three points only consist of patterns aaa, $0\frac{m}{2}0$ or $\frac{m}{2}0\frac{m}{2}$. Therefore the first and the third point are exactly the same point, in contradiction to the assumption.

We estimate C_m as above: for $i = 1, \ldots, n$ consider $Y_i = a_i - \frac{m}{4}$ as independent random variables, distributed uniformly in $\{-m/4, \ldots, m/4\}$, and

$$Z_i = Y_i^2 \ (i \in \{1, \ldots, n\}), Z = \sum_{i=1}^{n} Z_i.$$

The expected value is

$$\mu_m := \mathbb{E}(Z_i) = \frac{1}{(m+2)/2}\sum_{i=-m/4}^{m/4} i^2 = \frac{1}{48}m^2 + \frac{1}{12}m$$

and $\mathbb{E}(Z) = n\mathbb{E}(Z_i)$. The variance is

$$\begin{array}{rcl} \mathrm{Var}(Z_i) & = & \mathbb{E}(Z_i^2) - \mathbb{E}(Z_i)^2 \\ & = & \frac{m^4}{1280} + \frac{m^3}{160} + \frac{m^2}{120} - \frac{m}{60} - \left(\frac{1}{48}m^2 + \frac{1}{12}m\right)^2 \\ & = & \frac{1}{2880}\left(m^4 + 8m^3 + 4m^2 - 48m\right), \end{array}$$

and $\mathrm{Var}(Z) = n\mathrm{Var}(Z_i)$.

The standard deviation is $\sigma_m = \sqrt{\mathrm{Var}(Z_i)}$ and $\sigma_Z = \sqrt{\mathrm{Var}(Z)} = \sigma_m\sqrt{n}$, where σ_m depends only on m. By Chebychev's inequality

$$\mathbb{P}(|Z - \mathbb{E}(Z)| > a\sigma_Z) \leq \frac{1}{a^2}.$$

With $a = \sqrt{3}$ we see that for at least two thirds of all elements in $[0, \frac{m}{2}]^n$ the sum of digit squares-distances from the centre point $\left(\frac{m}{4}, \ldots, \frac{m}{4}\right)$ is in the interval $[\mu_m n - a\sigma_Z, \mu_m n + a\sigma_Z]$. By the pigeonhole principle there exists a squared radius R with frequency at least $\frac{C_m}{\sqrt{n}}\left(\frac{m+2}{2}\right)^n$, where

$$C_m = \frac{2}{3 \cdot 2\sqrt{3}\sigma_m} = \frac{1}{3\sqrt{3}\sigma_m}.$$

Note that $\sigma_4 = \frac{\sqrt{2}}{3}, \sigma_6 = 1, \sigma_8 = \sqrt{\frac{14}{5}}$. As the proof only makes use of effective bounds, the result is valid for all even $m \geq 4$ and all n. If the even value of m tends to infinity, then asymptotically $\sigma_m \sim \frac{m^2}{24\sqrt{5}}$ holds, giving the claimed value of C_m.

Note that the values of the constants in the two cases m odd and even are quite similar.

□

Proof of Theorem 2.18. Let n be a multiple of 7 and $D = \{0, 1, 2, 3, 4, 5, 6\}$. Let

$$S = \{(a_1, \ldots, a_n) : a_i \in D \text{ and for each } j \in D \text{ there are } n/7 \text{ values } i \in \{1, \ldots, n\} \text{ with } a_i = j\}.$$

The list of trivial and nontrivial arithmetic progressions of length 4 with digits in D modulo 11 is:

$$\begin{cases} 0000, 1111, 2222, 3333, 4444, 5555, 6666 \\ 0\underline{1}23, 0246, 123\underline{4}, 16\underline{0}5, \underline{2}345, 3456, 32\underline{1}0, \underline{4}321, 5\underline{0}61, 543\underline{2}, 6420, 6543 \end{cases}$$

Let $d(a_1a_2a_3a_4)$ denote the number of coordinates, where the pattern $a_1a_2a_3a_4$ occurs among the 4 points which are in arithmetic progression. Note that the digit 0 occurs in all 4 positions with the same frequency. Applying this to positions 3 and 1 we see that the number of occurrences of a pattern 1605 equals the sum of the number of occurrences of patterns 0123 and 0246 together. (See underlined symbols in the list of patterns.) Also looking at digit 1 at positions 2 and 1, and combining these gives:

$$\begin{aligned} &(1) \quad d(1605) = d(0123) + d(0246) \\ &(2) \quad d(0123) = d(1605) + d(1234) = d(0123) + d(0246) + d(1234), \\ &\qquad \text{which implies:} \\ &(3) \quad d(1234) = 0. \end{aligned}$$

As 1234 is the *only* nontrivial progression with digit 4 in the last position, all 4's must occur in form of a trivial progression, 4444. Therefore,

$$d(0246) = d(1234) = d(2345) = d(3456) = d(4321) = d(5432) = d(6420) = d(6543) = 0.$$

This leaves only the following nontrivial progressions.

$$0123, 1605, 3210, 5061$$

Here we observe that there are no digits 2 or 6 at the boundary, and also no digits 3 or 5 in the positions 2 and 3. So, in each coordinate there can only be

a constant progression, which contradicts that we have a proper progression of distinct points in S.

The number of elements in S is the multinomial coefficient

$$\binom{n}{n/7, n/7, n/7, n/7, n/7, n/7, n/7} = \frac{n!}{((n/7)!)^7} \sim C\frac{7^n}{n^3}$$

for some constant $C > 0$, by Stirling's formula. If n is not a multiple of 7, say $n = 7r + i$, one adds $i \leq 6$ further coordinates with constant digits, which only weakens the overall lower bound by a small factor. □

Proof of Theorem 2.19. In this situation we do not take the digits consecutively, but make use of the algebraic structure of $(\mathbb{Z}_m, +)$. In particular, p^{s-1} generates a subgroup of order p, and k-progressions in $\mathbb{Z}_m$ with gap size divisible by p have the property that the first element is the same as the last element. We choose the digits as follows:

$$D = \mathbb{Z}_m \setminus \{ip^{s-1} - 1 : i = 2, \ldots, p\}.$$

Observe that D contains $p^{s-1} - 1$ complete cycles of length p, and one extra element, and so

$$|D| = (p^{s-1} - 1)p + 1 = p^s - p + 1.$$

There are three types of progressions of length $k = p^{s-1} + 1$ in D:

1. Type I progressions have a non-zero gap size divisible by p. In this case the first element and the last element of the progression are the same.

2. For Type II progressions the gap size is not divisible by p. In this case all residue classes modulo p^{s-1} occur, and the first and last elements are the same modulo p^{s-1}, but cannot be the same modulo $m = p^s$. The residue class $p^{s-1} - 1 \bmod m$ must occur, as D contains only one element from the residue class $-1 \bmod p^{s-1}$. We observe that no such k-progression can start with $p^{s-1} - 1$, as it would have to end at *another* element $-1 \bmod p^{s-1}$, which is impossible.

3. Type III progressions are constant.

So far this was the part which generalized the algebraic situation from $m = 4$ to prime powers. The last part is the set-theoretic trick inspired by Salem and Spencer.

Let $|D| \mid n$ and let

$$S = \left\{ (a_1, \ldots, a_n) : a_i \in D, \forall d \in D : |\{j \in [1, n] : a_j = d\}| = \frac{n}{|D|} \right\}.$$

The number $|S|$ of elements is the multinomial coefficient

$$\binom{n}{n/|D|,\ldots,n/|D|} \sim C_m \frac{|D|^n}{n^{(|D|-1)/2}}$$

according to Lemma 3.1. Suppose that S contains a *proper* arithmetic progression of length $k = p^{s-1} + 1$.

Let us study the occurrence of the digit $p^{s-1} - 1$ in the first vector. It cannot be part of a type I or type II progression, and hence must be a constant type III progression. Therefore all coordinate entries $p^{s-1} - 1$ in all vectors occur in the same positions. In all other coordinates we only have type I and type III progressions. For these the first and the last elements are the same, modulo m. Hence there cannot be a *proper* arithmetic progression of length k, which by definition consists of k distinct elements.

□

Proof of Theorem 2.21. Recall that $m = p^s, s \geq 3, k = p^{s-2} + 1$. Let

$$D_1 = \left\{p^{s-2}i : i = 0,\ldots,p^2 - 1\right\},$$

$$D_2 = \left\{p^{s-1}i + j : i \in \{0,\ldots,p-1\}, j \in \{1,\ldots,p-1\}\right\}$$

and $D_3 = \{0,1,2,\ldots,p-1\}$. Choose the digits:

$$D = (\mathbb{Z}_m \setminus (D_1 \cup D_2)) \cup D_3.$$

Observe that

$$|D| = p^s - p^2 - p(p-1) + p = p^s - 2p^2 + 2p.$$

For example, when $m = 27, k = 4$, then

$$D = \{0,1,2,4,5,7,8,13,14,16,17,22,23,25,26\}.$$

There are four types of progressions of length $k = p^{s-2} + 1$ in D:
Type I progressions with gap size p^t, $2 \leq t < s$, which therefore contain a cycle of length p^{s-t}. Here the first element and the last element is the same. Note that the class 0 cannot be part of such a progression, as the element $p^t \cdot p^{s-1-t} = p^{s-1}$ is not in D.
Type II: progressions of gap size p. They must use exactly one of the digits in $D_3 \setminus \{0\}$, but cannot use it in the first or last position: starting with $d \in D_3 \setminus \{0\}$ and gap size p the longest progression size is $k - 1$, as otherwise a digit in D_2 would be needed, which is impossible. Also the progression cannot contain 0, as it would then also contain $p \cdot p^{s-2}$, which is impossible. (Example, $m = 27$: the longest progression with gap size 3 is: $22, 25, 1, 4, 7$.)
Type III progressions have a gap size coprime to p, and do not contain any cycle. They consist of $k = p^{s-2} + 1$ distinct digits, and in particular go through all residue

classes modulo p^{s-2}, and therefore contain the special element 0. But note that no such progression can start with 0, as it would also have to end at *another* element $0 \bmod p^{s-2}$, which is impossible.
Type IV progressions are constant.

Note that progressions starting with 0 must be of type IV. Now let $|D|$ divide n and let

$$S = \left\{ (a_1, \ldots, a_n) : a_i \in D, \forall d \in D : |\{j \in [1,n] : a_j = d\}| = \frac{n}{|D|} \right\}.$$

The number $|S|$ of elements is the multinomial coefficient

$$\binom{n}{n/|D|, \ldots, n/|D|} \sim C_m \frac{|D|^n}{n^{(|D|-1)/2}}.$$

As all elements contain the same number of 0 entries, the constant progressions (type IV) are the only ones that contain any 0 entry.

Now suppose that S has a proper progression of length $k = p^{s-2} + 1$. All k elements contain in $\frac{n}{|D|}$ positions an entry $d \in D_3$. Looking at the first element of the progression we see that these progressions starting with $d \in D_3$ can only be of type IV, i.e. constant. Hence all digits D_3 cannot take part in any nontrivial progression. With all other digits in $\mathbb{Z}_m \setminus (D_1 \cup D_2)$ and with all progression types we observe that the first and the last elements are the same. Altogether, the set S of vectors does not have a *proper* arithmetic progression of length k, which by definition consists of k distinct elements. □

4 Progression-free sets in $\mathbb{Z}_4^n$

In this section we give bounds for $r_3(\mathbb{Z}_4^n)$ and $r_4(\mathbb{Z}_4^n)$. For proving the upper bound $r_3(\mathbb{Z}_4^n) \le 3.611^n$ with Croot, Lev and the author [31] developed a new variant of the polynomial method. Here we will follow the proof from [31], but we present it in a slightly different way. Due to the structure of $\mathbb{Z}_4^n$, if a, b, c is a 3AP, then $c - a = 2(b - a)$ must lie in the subgroup generated by its involutions: $\{0, 2\}^n \cong \mathbb{F}_2^n$. (Note that this subgroup is both the image and the kernel of the doubling endomorphism of $\mathbb{Z}_4^n$ defined by $g \mapsto 2g$ $(g \in \mathbb{Z}_4^n)$.) This makes it natural to reformulate the problem of finding $r_3(\mathbb{Z}_4^n)$ as an extremal problem about a system of subsets of $\mathbb{F}_2^n$ satisfying a certain condition. Though this reformulation does not play a crucial role in our proof, we believe it may be helpful to explicitly state it, as in [31] it was used only implicitly.

4.1 Subset reformulation for 3AP-free-ness

In this section we give a "subset formulation" for the question of determining $r_3(\mathbb{Z}_4^n)$. As an application, we give yet another proof to Corollary 2.4, then we prove Theorem 2.23.

Let us say that a system of subsets $A(x) \subseteq \mathbb{F}_2^n$ $(x \in \mathbb{F}_2^n)$ satisfies property $(*)$, if the following implication holds:

$$\forall x \in \mathbb{F}_2^n \ (y \in x + A(x)\hat{+}A(x) \implies A(y) = \varnothing). \qquad (*)$$

(Note that for $A(x) = \varnothing$ we define $x + A(x)\hat{+}A(x) := \varnothing$.)
Let $r_3'(n)$ denote the maximal possible size of $\sum_{x \in \mathbb{F}_2^n} |A(x)|$, if the system of subsets $\{A(x) : x \in \mathbb{F}_2^n\}$ satisfies $(*)$.

The proof of Lemma 4.1 (below) shows that property $(*)$ nicely captures the condition that the "corresponding" $A \subseteq \mathbb{Z}_4^n$ is 3AP-free.

Lemma 4.1. *For every $n \ge 1$ we have $r_3(\mathbb{Z}_4^n) = r_3'(n)$.*

Proof. Let $F = \{0, 2\}^n \le \mathbb{Z}_4^n$ and $R = \{0, 1\}^n \subseteq \mathbb{Z}_4^n$. Every element $a \in \mathbb{Z}_4^n$ can be written as $a = f + r$ $(f \in F, r \in R)$ in a unique way. Let $A \subseteq \mathbb{Z}_4^n$. Let us assign to every $x = 2r \in F$ (where $r \in R$) a subset $A(x) \subseteq F$ in the following way:

$$A(x) = \{y \in F : r + y \in A\}.$$

Three distinct elements

$$a_1 = f_1 + r_1, \ a_2 = f_2 + r_2, \ a_3 = f_3 + r_3$$

(where $f_i \in F, r_i \in R$) form an arithmetic progression (in this order) if and only if $a_1 + a_3 = 2a_2$, that is, if $f_1 + f_3 + r_1 + r_3 = 2r_2$. As $f_1, f_3, 2r_2 \in F$, this implies $r_1 = r_3$, so the condition gives $2r_2 = 2r_1 + f_1 + f_3$. Such elements can be found

in A if and only if for distinct $x = 2r_1, y = 2r_2 \in F$ we have $y \in x + A(x)\hat{+}A(x)$ and $A(y) \neq \varnothing$. Note that $F \cong \mathbb{F}_2^n$, and this is equivalent with the condition that the system of subsets satisfies property $(*)$. Furthermore, $|A| = \sum |A(x)|$, so the maximal possible size of a 3AP-free subset of $\mathbb{Z}_4^n$ is equal to the maximal possible total size of a system of subsets $A(x)$ satisfying property $(*)$. □

Now, as an illustration, we give an alternative – different from the proofs presented in Section 3 – proof (using the subset reformulation) for Corollary 2.4, then we prove Theorem 2.23.

Alternative proof of Corollary 2.4. For $x \in \mathbb{F}_2^n$ let $\mathrm{supp}(x) = \{i : x_i \neq 0\}$. Let us fix some $r \in \{0, 1, \dots, n\}$. Let $A(x) = \{v : \mathrm{supp}(v) \subseteq \mathrm{supp}(x)\}$, if $|\mathrm{supp}(x)| = r$ and $A(x) = \varnothing$, otherwise. We claim that the system of subsets $A(x)$ satisfies $(*)$. Indeed, if $y \in x + A(x)\hat{+}A(x)$, then $|\mathrm{supp}(x)| = r$, thus $\mathrm{supp}(y) \subsetneq \mathrm{supp}(x)$ yields $A(y) = \varnothing$.

The total size of the subsets $A(x)$ is $\binom{n}{r}2^r$. The optimal choice is $r = \lceil 2n/3 \rceil$ yielding

$$r_3(\mathbb{Z}_4^n) \geq \binom{n}{r}2^r \gg 3^n/\sqrt{n}.$$

□

Proof of Theorem 2.23. For $0 \leq k \leq n$ let X_k contain those x for which $A(x)$ is a subspace of codimension k. If there is an $A(x)$ of codimension 0, that is, $A(x) = \mathbb{F}_2^n$, then all the other $A(y)$ sets are empty, thus the total size of the subsets is only 2^n. From now on, we assume that each nonempty subset is a subspace of positive codimension.

Let us fix k. For $x \in X_k$ let $x^{(1)}, \dots, x^{(k)}$ be a basis for the orthogonal complement of $A(x)$, that is, $A(x) = \{z : \forall\ 1 \leq i \leq k :\ zx^{(i)} = 0\}$.

Let $\hat{x} = (x, 1) \in \mathbb{F}_2^{n+1}$ and $\hat{x}^{(i)} = (x^{(i)}, 1 + xx^{(i)}) \in \mathbb{F}_2^{n+1}$. Now, for every $x \in X_k$ we have $\hat{x}\hat{x}^{(i)} = 1$. If $x \neq y \in X_k$, then $y \notin x + A(x)\hat{+}A(x)$, thus for some $1 \leq i \leq k$ we have $(x + y)x^{(i)} = 1$. However, this implies that $(\hat{x} + \hat{y})\hat{x}^{(i)} = 1$, that is, $\hat{y}\hat{x}^{(i)} = 0$. Let

$$u(x) = \hat{x} \otimes \hat{x} \otimes \cdots \otimes \hat{x} \in (\mathbb{F}_2^{n+1})^{\otimes k}$$

and

$$v(x) = \hat{x}^{(1)} \otimes \hat{x}^{(2)} \otimes \cdots \otimes \hat{x}^{(k)} \in (\mathbb{F}_2^{n+1})^{\otimes k}.$$

If $x, y \in X_k$, then $u(x)v(y) = \delta_{xy}$, so the vectors $(u(x), v(x))$ (with $x \in X_k$) form a biorthogonal system of vectors, specially, the $u(x)$ vectors are linearly independent. However, all the $u(x)$ vectors lie in a subspace of dimension $\sum_{i=1}^{k}\binom{n+1}{i}$, thus $|X_k| \leq \sum_{i=1}^{k}\binom{n+1}{i}$. Therefore, the total size of the subsets $A(x)$ is at most

$$\sum_{k=1}^{n}\sum_{i=1}^{k}\binom{n+1}{i}2^{n-k} \leq 6 \cdot 3^n.$$

Now we use the tensor power trick to get rid of the factor 6. Let us assume that in $\mathbb{F}_2^n$ the system of subsets $A(x)$ satisfies $(*)$ and all the non-empty subsets are subspaces. Let $S = \sum |A(x)|$. Now, we can define a system of subsets in $\mathbb{F}_2^{nt}$ as follows. For $(x_1, x_2, \dots, x_t) \in \mathbb{F}_2^{nt}$ let

$$A((x_1, x_2, \dots, x_t)) = A(x_1) \times A(x_2) \times \cdots \times A(x_t).$$

It is easy to check that this system satisfies $(*)$, all the non-empty subsets are subspaces and the total size of the subspaces is S^t. Therefore, $S^t \le 6 \cdot 3^{nt}$, thus $S \le 6^{1/t} 3^n$. This holds for every t, so the statement is proven.

□

4.2 Reformulation for 4AP-free-ness

A similar subset reformulation can be given for 4AP-free-ness. Let us say that a system of subsets $A(x) \subseteq \mathbb{F}_2^n$ $(x \in \mathbb{F}_2^n)$ satisfies property $(**)$, if the following implication holds:

$$\forall x, y \in \mathbb{F}_2^n \ (x + y \in (A(x) + A(x)) \cap (A(y) + A(y)) \implies x = y) \qquad (**)$$

(Note that for $A(x) = \varnothing$ we define $A(x) + A(x) := \varnothing$.)
Let $r_4'(n)$ denote the maximal possible size of $\sum\limits_{x \in \mathbb{F}_2^n} |A(x)|$, if the system of subsets $\{A(x) : x \in \mathbb{F}_2^n\}$ satisfies $(**)$.

Lemma 4.2. *For every $n \ge 1$ we have $r_4(\mathbb{Z}_4^n) = r_4'(n)$.*

Proof. Similarly to the proof of Lemma 4.1 let us write every element $a \in \mathbb{Z}_4^n$ in the form $a = f + r$ (where $f \in F := \{0, 2\}^n, r \in R := \{0, 1\}^n$). Let $A \subseteq \mathbb{Z}_4^n$. Let us assign to every $x = 2r \in F$ (where $r \in R$) a subset $A(x) \subseteq F$ in the following way:

$$A(x) = \{y \in F : r + y \in A\}.$$

Now four distinct elements

$$a_1 = f_1 + r_1, \ a_2 = f_2 + r_2, \ a_3 = f_3 + r_3, \ a_4 = f_4 + r_4$$

(where $f_i \in F, r_i \in R$) form an arithmetic progression (in this order) if and only if $a_1 + a_3 = 2a_2$ and $a_2 + a_4 = 2a_3$, that is, if $f_1 + f_3 + r_1 + r_3 = 2r_2$ and $f_2 + f_4 + r_2 + r_4 = 2r_3$. This implies $r_1 = r_3$ and $r_2 = r_4$, so the condition gives $2r_2 = 2r_1 + f_1 + f_3$ and $2r_1 = 2r_2 + f_2 + f_4$. Such elements exist in A if and only if for distinct elements $x = 2r_1, y = 2r_2 \in F$ we have $y \in x + A(x) \hat{+} A(x)$ and $x \in y + A(y) \hat{+} A(y)$. Note that $F \cong \mathbb{F}_2^n$. Hence, A is 4AP-free if and only if the system of subsets $\{A(x) : x \in F\}$ satisfies property $(**)$.

Furthermore, $|A| = \sum |A(x)|$, so the maximal possible size of a 4AP-free subset of $\mathbb{Z}_4^n$ is the same as the maximal possible total size of a family of subsets $A(x)$ satisfying property $(**)$. □

4.3 Lower bound for $r_3(\mathbb{Z}_4^n)$

Proof of Theorem 2.3. For a point $a \in \mathbb{Z}_4^n$ define $T(a) = \{i \in [n] : a_i \in \{0,2\}\}$.
If $a, b, c \in \{0,1,2\}^n$ form an arithmetic 3-progression, then for $i \in [n]$ we have:

$$(a_i, b_i, c_i) \in \{(0,0,0), (0,1,2), (0,2,0), (1,1,1), (2,0,2), (2,1,0), (2,2,2)\}.$$

Hence $T(a) = T(c) \supseteq T(b)$ and a and c differ only at positions $i \in T(a) \backslash T(b)$.

Fix t and let $S \subseteq \{0,1,2\}^n$ be such that $|T(a)| \geq t$ for every $a \in S$ and such that $\{a \in S : T(a) = T\}$ has minimum Hamming distance at least $|T| - t + 1$ for every T with $|T| \geq t$. Then S does not contain a proper 3-progression, since, if $a, b, c \in S$ form a 3-progression, then for the Hamming-distance of a and c we have the bound

$$d(a,c) \leq |T(a) \backslash T(b)| = |T(a)| - |T(b)| \leq |T(a)| - t,$$

which implies that $a = c$.

We can construct such S as follows. For every $T \subseteq [n]$ of size $i \geq t$ we take a binary code in $\{0,2\}^T$ of size $A(i, i-t)$ of minimum distance $i-t$ and add symbols '1' in the positions $[n] \backslash T$ to get a code A_T.
The set $S = \bigcup_{|T| \geq t} A_T$ gives the stated lower bound.

□

4.4 Upper bound for $r_3(\mathbb{Z}_4^n)$

We recall that the degree of a multivariate polynomial is the largest sum of the exponents of all of its monomials. The polynomial is *multilinear* if it is linear in every individual variable.

The proof of Theorem 2.1 is based on the following lemma.

Lemma 4.3. *Suppose that $n \geq 1$ and $d \geq 0$ are integers, P is a multilinear polynomial in n variables of total degree at most d over a field $\mathbb{F}$, and $A \subseteq \mathbb{F}^n$ is a set with*

$$|A| > 2 \sum_{0 \leq i \leq d/2} \binom{n}{i}.$$

If $P(a-b) = 0$ for all $a, b \in A$ with $a \neq b$, then also $P(0) = 0$.

Proof. Let $m := \sum_{0 \leq i \leq d/2} \binom{n}{i}$, and let $\mathcal{K} = \{K_1, \ldots, K_m\}$ be the collection of all sets $K \subseteq [n]$ with $|K| \leq d/2$. Writing for brevity

$$x^I := \prod_{i \in I} x_i, \quad x = (x_1, \ldots, x_n) \in \mathbb{F}^n, \ I \subseteq [n],$$

there exist coefficients $C_{I,J} \in \mathbb{F}$ $(I, J \subseteq [n])$ depending only on the polynomial P, such that for all $x, y \in \mathbb{F}^n$ we have

$$P(x-y) = \sum_{\substack{I,J\subseteq[n]\\ I\cap J=\emptyset\\ |I|+|J|\le d}} C_{I,J}\, x^I y^J$$

$$= \sum_{I\in\mathcal{K}} x^I \sum_{\substack{J\subseteq[n]\setminus I\\ |J|\le d-|I|}} C_{I,J}\, y^J + \sum_{J\in\mathcal{K}} \left(\sum_{\substack{I\subseteq[n]\setminus J\\ d/2<|I|\le d-|J|}} C_{I,J}\, x^I \right) y^J.$$

The right-hand side can be interpreted as the scalar product of the vectors $u(x), v(y) \in \mathbb{F}^{2m}$ defined by

$$u_i(x) = x^{K_i}, \quad u_{m+i}(x) = \sum_{\substack{I\subseteq[n]\setminus K_i\\ d/2<|I|\le d-|K_i|}} C_{I,K_i}\, x^I$$

and

$$v_i(y) = \sum_{\substack{J\subseteq[n]\setminus K_i\\ |J|\le d-|K_i|}} C_{K_i,J}\, y^J, \quad v_{m+i}(y) = y^{K_i}$$

for all $1 \le i \le m$. Consequently, if we had $P(a-b) = 0$ for all $a, b \in A$ with $a \ne b$, while $P(0) \ne 0$, this would imply that the vectors $u(a)$ and $v(b)$ are orthogonal if and only if $a \ne b$. As a result, the vectors $u(a)$ would be linearly independent (an equality of the sort $\sum_{a\in A} \lambda_a u(a) = 0$ with the coefficients $\lambda_a \in \mathbb{F}$ after a scalar multiplication by $v(b)$ yields $\lambda_b = 0$, for any $b \in A$).
Finally, the linear independence of $\{u(a)\colon a \in A\} \subseteq \mathbb{F}^{2m}$ implies $|A| \le 2m$, contrary to the assumptions of the lemma. □

Remark 4.4. *It is easy to extend the lemma relaxing the multilinearity assumption to the assumption that P has bounded degree in each individual variable. Specifically, denoting by $f_\delta(n,d)$ the number of monomials $x_1^{i_1}\dots x_n^{i_n}$ with $0 \le i_1,\dots,i_n \le \delta$ and $i_1+\dots+i_n \le d$, if P has all individual degrees not exceeding δ, and the total degree not exceeding d, then $|A| > 2f_\delta(n, \lfloor d/2 \rfloor)$ along with $P(a-b) = 0$ $(a, b \in A,\ a \ne b)$ imply $P(0) = 0$. Moreover, taking $\delta = d$, or $\delta = |\mathbb{F}| - 1$ for $\mathbb{F}$ finite, one can drop the individual degree assumption altogether.*

Remark 4.5. *The lower bound on $|A|$ can not be significantly weakened according to the following example. Let $\mathbb{F} = \mathbb{F}_2$ and $P(x) \in \mathbb{F}_2[x_1,\dots,x_n]$ be the sum of multilinear monomials of degree at most d, that is, $P(x) = \sum_{\substack{I\subseteq[n]\\ |I|\le d}} x^I$. Let $A \subseteq \mathbb{F}_2^n$ be the set of vectors that contain at most $d/2$ ones, then $|A| = \sum_{0\le i\le d/2} \binom{n}{i}$.*
In $A\hat{+}A$ each vector has at most d ones, thus by the binomial theorem P vanishes on $A\hat{+}A$, but $P(0) = 1 \ne 0$.

We will use the estimate

$$\sum_{0\le i\le z}\binom{n}{i} < 2^{nH(z/n)} \tag{3}$$

valid for all integer $n \ge 1$ and real $0 < z \le n/2$; see, for instance, [81, Ch. 10, §11, Lemma 8].

Recall, that for integer $n \ge d \ge 0$, the sum $\sum_{i=0}^{d}\binom{n}{i}$ is the dimension of the vector space of all multilinear polynomials in n variables of total degree at most d over the two-element field $\mathbb{F}_2$. In particular, the dimension of the vector space of *all* multilinear polynomials in n variables over $\mathbb{F}_2$ is equal to the dimension of the vector space of all $\mathbb{F}_2$-valued functions on $\mathbb{F}_2^n$, and it follows that any non-zero multilinear polynomial represents a non-zero function. These basic facts are used in the proof of Proposition 4.6 below.

Proposition 4.6. *Suppose that $n \ge 1$ and the system of subsets $A(x) \subseteq \mathbb{F}_2^n$ ($x \in \mathbb{F}_2^n$) satisfies property $(*)$. Let $0 < \varepsilon < 0.25$ and*

$$B := \{x : |A(x)| \ge 2^{nH(0.5-\varepsilon)+1}\}.$$

Then $|B| < 2^{nH(2\varepsilon)}$.

Proof. For the sake of contradiction assume that $|B| \ge 2^{nH(2\varepsilon)}$, equivalently, for the complement $\overline{B} = \mathbb{F}_2^n \setminus B$ we have $|\overline{B}| \le 2^n - 2^{nH(2\varepsilon)}$.

Let $d := m - \lceil 2\varepsilon n\rceil$ and $\mathcal{P}$ be the vector space of multilinear polynomials of degree at most d in n variables:

$$\mathcal{P} = \{p \in \mathbb{F}_2[x_1,\dots,x_n] : \deg p \le d,\ p \text{ is multilinear}\}.$$

Since

$$\dim\mathcal{P} = \sum_{i=0}^{d}\binom{n}{i} = 2^n - \sum_{i=0}^{\lceil 2\varepsilon n\rceil-1}\binom{n}{i} > 2^n - 2^{nH(2\varepsilon)} \ge |\overline{B}|,$$

the kernel of the evaluation mapping $\mathcal{P} \to \mathbb{F}_2^{\overline{B}}$ is nontrivial, that is, some $0 \not\equiv p \in \mathbb{F}_2[x_1,\dots,x_n]$ of degree at most d vanishes on $\overline{B}$.

Note that

$$2\sum_{i\le d/2}\binom{n}{i} < 2^{nH(0.5-\varepsilon+1)}.$$

Since the system satisfies property $(*)$, for every $b \in B$ we have $b + A(b)\hat{+}A(b) \subseteq \overline{B}$, so $p(b+x)$ vanishes on $A(b)\hat{+}A(b)$. Lemma 4.3 yields that $0 = p(b+0) = p(b)$. Hence, $p \equiv 0$, which contradicts our assumption, completing the proof. □

Proof of Theorem 2.1. For $x \geq 0$, let $N(x)$ denote the number of subsets $A(x)$ containing at least x elements; thus $N(x) = 0$ for $x > 2^n$, and we can write

$$\sum |A(x)| = \int_0^{2^{n+1}} N(x)\,dx. \tag{4}$$

Trivially, we have $N(x) \leq 2^n$ for all $x \geq 0$, so that

$$\int_0^{2^{nH(1/4)+1}} N(x)\,dx \leq 2^{(H(1/4)+1)n+1} < 2 \cdot 4^{\gamma n}. \tag{5}$$

On the other hand, the substitution $x = 2^{nH(0.5-\varepsilon)+1}$ gives

$$\int_{2^{nH(1/4)+1}}^{2^{n+1}} N(x)\,dx = n \int_0^{1/4} 2^{nH(0.5-\varepsilon)+1} N(2^{nH(0.5-\varepsilon)+1}) \log \frac{0.5+\varepsilon}{0.5-\varepsilon}\,d\varepsilon, \tag{6}$$

and applying Proposition 4.6, the integral in the right-hand side can be estimated as

$$2n \int_0^{1/4} 2^{n(H(0.5-\varepsilon)+H(2\varepsilon))} \log \frac{0.5+\varepsilon}{0.5-\varepsilon}\,d\varepsilon < 3n \int_0^{1/4} 2^{n(H(0.5-\varepsilon)+H(2\varepsilon))}\,d\varepsilon < n \cdot 4^{\gamma n}. \tag{7}$$

From (4)–(7) we get $|A| < (n+2) \cdot 4^{\gamma n}$, and to conclude the proof we use the tensor power trick: for integer $k \geq 1$, the set $A \times \cdots \times A \subseteq \mathbb{Z}_4^{kn}$ is progression-free and therefore

$$|A|^k < (kn+2) \cdot 4^{\gamma kn}$$

by what we have just shown. This readily implies the desired result. □

In the rest of this subsection we present the adaptation of the proof to the setting of odd primes. We present the proof in a slightly different form compared to the paper of Ellenberg and Gijswijt [41]. In the context of 3AP-free subset of $\mathbb{F}_q^n$ (where q is an odd prime power) Lemma 4.3 shall be formulated in the following way:

Lemma 4.7. *Let $p \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of degree at most d and assume that p vanishes on the restricted sumset $A \hat{+} A$ for some $A \subseteq \mathbb{F}_q^n$. Then p vanishes on all but at most $2f_q(n, d/2)$ many elements of $2 * A := \{2a : a \in A\}$, where $f_q(n, D)$ denotes the number of monomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ whose total degree is at most D and each individual degree is at most $q-1$, that is,*

$$f_q(n, D) = |\{(i_1, \ldots, i_n) \in \{0, 1, \ldots, q-1\}^n, i_1 + \cdots + i_n \leq D\}|.$$

The only modification in the proof of Lemma 4.3 is that in the representation $p(x+y) = \sum c_{I,J} x^I y^J = \langle u(x), v(y) \rangle$ we have that I and J are *multisets*, then for getting the desired bound one shall use that $\{u(a) : P(2a) \neq 0\}$ is a linearly independent system of vectors. (Note that over $\mathbb{F}_2$ for every a we have $2a = 0$, thus the conclusion there was $P(0) = 0$ assuming A is large enough.)

Now, let $A \subseteq \mathbb{F}_q^n$ be a 3AP-free set and define $B := 2 * A = \{2a : a \in A\}$. Let $\mathcal{P}$ denote the space of those polynomials in $\mathbb{F}_q[x_1, \dots, x_n]$ whose total degree is at most d and each individual degree is at most $q-1$.

Let $\mathcal{P}_0 := \{p \in \mathcal{P} : p\big|_{\overline{B}} \cong 0\} \leq \mathcal{P}$ be the kernel of the evaluation mapping on $\overline{B}$. Observe that by the dimension theorem

$$\dim\mathcal{P}_0 \geq \dim\mathcal{P} - |\overline{B}| = |A| - (q^n - f_q(n,d)) = |A| - f_q(n,(q-1)n-d-1).$$

As A is 3AP-free, $A\hat{+}A \subseteq \overline{B}$, since $a+a' = 2a''$ with $a, a', a'' \in A, a \neq a'$ would imply that a, a'', a' is a 3AP contained in A. Therefore, by Lemma 4.7 we obtain that every $p \in \mathcal{P}_0$ vanishes on $\mathbb{F}_q^n$ with the exception of at most $2f_q(n, d/2)$ points. By using that in a k-dimensional subspace there is always a vector with at least k nonzero coordinates we have that

$$\dim\mathcal{P}_0 \leq 2f_q(n, d/2).$$

Comparing the lower- and upper bounds for $\dim\mathcal{P}_0$ we get that

$$|A| \leq 2f_q(n, d/2) + f_q(n,(q-1)n-d-1).$$

The optimal choice for d is $d \approx \frac{2(q-1)n}{3}$, which yields the bound $|A| \leq (qJ(q))^n$ discussed in Section 2. Notice that the main difference is that in the proof for $\mathbb{Z}_4$ we needed the existence of one single, not everywhere 0 polynomial from $\mathcal{P}_0$, while for $\mathbb{F}_q$ it is also needed that the same dimension counting argument implies that the dimension of $\mathcal{P}_0$ is large.

4.5 3AP-free subsets of $\mathbb{Z}_4^n$, if $n \leq 5$

In this subsection we give a brief outline of the main strategy for proving Theorem 2.11. If we take a look at condition $(*)$ or $(**)$, then heuristically it seems to be a good idea to use sets with small doubling, since $(*)$ and $(**)$ seem to be less restrictive for these sets. Subspaces have a small doubling, and working with them is easier. An important step will be to show that it can be assumed (up to dimension $n \leq 5$) that in a maximal configuration all the (non-empty) subsets are subspaces. To arrive at this all-subspace state, we can use arguments of the following type: if $A(x) + A(x) \supseteq V$ for a large subspace V (where "large" means that $|V| \geq |A(x)|$), then we can replace $A(x)$ by V, since $(*)$ (or $(**)$) remains true (that is, the corresponding subset is still 3AP/4AP-free) and the total size of the subsets is larger (not smaller). So the general plan is to replace the subsets with subspaces, and then solve the subspace version of the problem. If the dimension is small, then for almost all subsets $A(x)$ we can do this reduction step easily, there are just a few cases, when $A(x)+A(x)$ does not contain a sufficiently large subspace. However, even in these exceptional cases $A(x)+A(x)$ turns out to be too large, so these cases can be excluded, as well. As the dimension increases, both the reduction step and handling the all-subspace problem is getting more

difficult. The 5-dimensional case is considerably more difficult than the previous cases, the proof of this is presented in a separate subsection. Now, we continue with the proof of the cases $1 \le n \le 4$.

4.6 Proof of Theorem 2.11 in the cases $n \le 4$ and of Theorem 2.24

Proof of Theorem 2.11 in the cases $n \le 4$. According to Lemma 4.1 and Corollary 2.5 it suffices to show that

$$r_3'(1) \le 2,\ r_3'(2) \le 6,\ r_3'(3) \le 16,\ r_3'(4) \le 42.$$

Case 1: $n = 1$**.**

If the dimension is 1, then it is trivial that every 2-element subset of $\mathbb{Z}_4$ is 3AP-free and any three elements form a 3AP, so $r_3(\mathbb{Z}_4) = 2$.

We continue with some general observations that are going to be used when the dimension is at least 2. Let us take a system of subsets $A(x)(\subseteq \mathbb{F}_2^n)$ (indexed by elements $x \in \mathbb{F}_2^n$) satisfying $(*)$. For brevity let $S = \sum_{x\in\mathbb{F}_2^n} |A(x)|$.

Observation 1. If $2^{n-1} < |A(x)|$ for some $x \in \mathbb{F}_2^n$, then by the pigeon-hole principle $x + A(x) + A(x) = \mathbb{F}_2^n$. Since, for every $y \in \mathbb{F}_2^n$ we have $(x + A(x)) \cap (y + A(x)) \ne \varnothing$, so, for some $a_1, a_2 \in A(x)$ we have $x + a_1 = y + a_2$, that is, $y = x + a_1 + a_2 \in x + A(x) + A(x)$. Therefore, $x + A(x)\hat{+}A(x) = \mathbb{F}_2^n \setminus \{x\}$, so all the subsets are empty except $A(x)$, thus $S = |A(x)| \le 2^n$. Hence, in this case the statement holds.

From now on, let us assume that $|A(x)| \le 2^{n-1}$ for every x.

Observation 2. Let $A(x)$ be a nonempty subset: $0 < |A(x)| \le 2^{n-1}$. It can be assumed that $0 \in A(x)$, since changing $A(x)$ to a translate of itself, $A(x) + c$, preserves the sumset $A(x) + A(x)$.

Observation 3. If $|A(x)| \in \{1, 2\}$, then $A(x)$ is automatically a subspace, as $0 \in A(x)$. If $|A(x)| \in \{3, 4\}$, let u and v be two different nonzero elements of $A(x)$, that is, $A(x) \supseteq \{0, u, v\}$. Clearly, for $A'(x) = \langle u, v\rangle$ we have $A(x)\hat{+}A(x) \supseteq A'(x)\hat{+}A'(x)$, so we may replace $A(x)$ by the 2-dimensional linear subspace $A'(x)$. This way $(*)$ is still satisfied, and either S does not change or it increases by 1.

Now we consider the cases $n = 2, 3, 4$ one by one.

Case 2: $n = 2$**.**

Now, we continue with the case when the dimension is 2. If none of the subsets is empty, then all of them can have size at most 1, thus $S \le 4$. Otherwise, by Observation 1 we can assume that every nonempty subset has size at most 2, thus $S \le 6$, since there must be an empty set.

Case 3: $n = 3$**.**

If the dimension is 3, then let e_1, e_2, e_3 be a basis for $\mathbb{F}_2^3$.

According to Observations 1-3 we can assume that all subsets have size at most 4 and every nonempty subset is a subspace (of dimension at most 2).

Let k denote the number of 2-subspaces and ℓ the number of empty sets. If $k = 0$, then $S \le 2 \cdot 8 = 16$, and we are done. Note that in fact $S < 16$, since either all subsets have size at most 1 or at least one of them is empty.

So we can assume that $k > 0$. If $A(x) = \langle u, v \rangle$ is a 2-subspace, then

$$A(x+u), A(x+v), A(x+u+v)$$

are all empty, that is, we can assign an "empty triple" $\{x+u, x+v, x+u+v\}$ to each 2-subspace. To different 2-subspaces we assign different triples, as the sum of the elements in the triple is x. That is, $k \le \binom{\ell}{3}$. We have $S \le 4k + 2(8-k-\ell) = 16 + 2k - 2\ell \le 16 + 2\binom{\ell}{3} - 2\ell \le 16$, if $\ell \le 4$, equality holds if and only if $\ell = 4$. If $5 \le \ell$, then $S \le 3 \cdot 4 = 12$. Therefore, $S \le 16$ is shown and the maximum occurs when $k = \ell = 4$.

We continue with the 4-dimensional case.

Case 4: $n = 4$**.**

We will show that if the system of subsets $\{A(x) \subseteq \mathbb{F}_2^4 \mid x \in \mathbb{F}_2^4\}$ satisfies $(*)$, then $\sum_{x \in \mathbb{F}_2^4} |A(x)| \le 42$.

At first it is going to be shown that "in most of the cases" it can be assumed that all the nonempty $A(x)$ subsets are linear subspaces, then we will prove the statement for the special case when the non-empty $A(x)$ subsets are all linear subspaces and finally cover the remaining cases.

By Observations 1-3 we can assume that all subsets have size at most 8 and every nonempty subset of size at most 4 is a subspace (of dimension at most 2).

Let $5 \le |A(x)| \le 8$. As $\dim\langle A(x)\rangle \ge 3$, we may choose three linearly independent vectors from $A(x)$. Let these be f_1, f_2, f_3 and let $A'(x) = \langle f_1, f_2, f_3 \rangle$. As $0, f_1, f_2, f_3 \in A(x)$, we have that

$$\{0, f_1, f_2, f_3, f_1+f_2, f_1+f_3, f_2+f_3\} \subseteq A(x) + A(x),$$

that is, $A(x)+A(x)$ contains all the elements of the subspace $\langle f_1, f_2, f_3 \rangle$, possibly with the exception of $f_1 + f_2 + f_3$.

We claim that if there exists some $0 \neq g \in (A(x) \cap A'(x)) \setminus \{f_1, f_2, f_3\}$, then $A(x) + A(x) \supseteq \langle f_1, f_2, f_3 \rangle$. To see this, we only need to show that $f_1 + f_2 + f_3 \in A(x) \hat{+} A(x)$. However, either $g = f_i + f_j$ (with some distinct $i, j \in \{1,2,3\}$) and $f_1+f_2+f_3 = g+f_k$ (where $\{i,j,k\} = \{1,2,3\}$) or $g = f_1+f_2+f_3$ and $f_1+f_2+f_3 = g+0$ is a good representation. Therefore, in this case we can replace $A(x)$ by $\langle f_1, f_2, f_3 \rangle$. It remains to check the case when any four vectors in $A(x) \setminus \{0\}$ are linearly independent.

Step 1. Assuming that $A(x)$ is not a subspace, and any four vectors in $A(x) \setminus \{0\}$ are linearly independent we prove $S < 42$ under the additional assumption that at most two subsets have size 8.

Without loss of generality it can be assumed that $\{0, f_1, f_2, f_3, f_4\} \subseteq A(x)$, where f_1, f_2, f_3, f_4 is a basis. The 3-subspaces spanned by three out of these basis vectors cover $\mathbb{F}_2^4$ with the exception of $f_1 + f_2 + f_3 + f_4$. That is, if $|A(x)| \neq 5$, then

$$A(x) = \{0, f_1, f_2, f_3, f_4, f_1 + f_2 + f_3 + f_4\},$$

but in this case $A(x)\hat{+}A(x) \supseteq A'(x)\hat{+}A'(x)$ for $A'(x) = \langle f_1, f_2, f_3\rangle$, so we can replace $A(x)$ by a larger set $A'(x)$.

So, it suffices to check the case when $A(x) = \{0, f_1, f_2, f_3, f_4\}$. The system of subsets $\{A(y) \mid y \in \mathbb{F}_2^4\}$ can be replaced by a "translate" of itself: $\{A'(y) \mid y \in \mathbb{F}_2^4\}$ where $A'(y) = A(y + c)$ for some fixed $c \in \mathbb{F}_2^4$ (not depending on y). So by taking $c = x$ we may suppose that $A(0) = \{0, f_1, f_2, f_3, f_4\}$. Then $|0 + A(0)\hat{+}A(0)| = 10$, so at least 10 subsets are empty. The size of $A(0)$ is 5 and the size of the other five (possibly) nonempty subsets is at most 8. If at least two out of these five subsets have size at most 5, then $S \leq 5 + 5 + 5 + 3 \cdot 8 = 39 < 42$. If this does not hold, then at least four of them are of size 8. We will cover this case later: indeed, it is going to be shown that if at least three subsets are of size 8, then $S < 42$.

Step 2. From now on, we will assume that

- either all the nonempty $A(x)$ sets are linear subspaces of dimension at most 3, or
- some of the subsets are of size 5, but there are at least three subsets of size 8,

and show that $S \leq 42$ in these cases, too.

Let h be the number of 3-subspaces. We distinguish 4 subcases.

Subcase 1 ($h = 0$). In this case all of the subsets are of size at most 4. If $A(x) = \langle u, v\rangle$ is a 2-dimensional subspace for some x, then $A(x)\hat{+}A(x) = \{u, v, u + v\}$, thus $A(x + u), A(x + v)$ and $A(x + u + v)$ are all empty. So for each 2-subspace $A(x)$ we can assign an "empty triple", since the subsets assigned to the elements of $x + A(x)\hat{+}A(x)$ are all empty. Moreover, the triple $\{x + u, x + v, x + u + v\}$ determines x, since the sum of the vectors in the triple is x. Let k be the number of 2-subspaces and ℓ be the number of empty subsets (among the $A(x)$ sets). As empty triples can be assigned to the 2-subspaces by an injective mapping, we have $k \leq \binom{\ell}{3}$.
Hence,

$$S \leq 4k + 2(16 - k - \ell) = 32 + 2k - 2\ell \leq 32 + 2\binom{\ell}{3} - 2\ell.$$

If $\ell \leq 4$, then this yields $S \leq 32$. Moreover, for $\ell = 5$ we obtain that $S \leq 42$.
If $\ell \geq 6$, then $S \leq 10 \cdot 4 = 40$.
In all cases we obtained that $S \leq 42$.

Subcase 2 ($h = 1$). Let $|A(0)| = 8$. As $|0 + A(0)\hat{+}A(0)| = 7$, at least 7 subsets are empty and consequently $S \leq 8 + (16 - 1 - 7) \cdot 4 = 40$.

Subcase 3 ($h = 2$). Let $A(u)$ and $A(v)$ be the two 3-subspaces. Then $U = u + A(u) + A(u)$ and $V = v + A(v) + A(v)$ are 3-dimensional affine subspaces.
If $U \cap V = \varnothing$, then $U \cup V = \mathbb{F}_2^4$ and $A(x) = \varnothing$ for all $x \notin \{u, v\}$, so $S \leq 2 \cdot 8 = 16$. Otherwise, $U \cap V$ is a 2-dimensional affine subspace, so $|(U \cup V) \setminus \{u, v\}| = (16 - 4) - 2 = 10$, that is, at least 10 subsets are empty. Then $S \leq 2 \cdot 8 + 4 \cdot 4 = 32$.

Subcase 4 ($h \geq 3$). Finally, let us assume that $A(u), A(v), A(w)$ are 3-subspaces. Note that in this case it can happen that some of the nonempty subsets are not subspaces (these sets have size 5 and contain 5 affine independent vectors). According to Subcase 3, at least 10 subsets are empty. If at least 11 subsets are empty, then $S \leq 5 \cdot 8 = 40$, and we are done.

So it can be assumed that exactly 10 subsets are empty. Let

$$U = u + A(u) + A(u),\ V = v + A(v) + A(v),\ W = w + A(w) + A(w).$$

Since there are only 10 empty subsets, from the argument of Subcase 3 it follows that these are exactly the 10 subsets $A(x)$ which are assigned to the 10 elements $x \in (U \cup V) \setminus \{u, v\}$. However, $U, V, U \cap V$ are all affine subspaces, so the sum of the vectors in U adds up to 0 and the same holds for V and $U \cap V$. Thus the sum of the vectors in $U \cup V$ is also 0. Hence, the sum of all vectors to which the empty set is assigned is $u + v$. However, we can repeat this argument with U and W and get that the sum is also equal to $u + w$, which is a contradiction. We are done.

□

Proof of Theorem 2.24. We are going to use the implications of the previous proof.

When $n = 2$, one of the sets must be empty and all other sets must have size 2 in order to get 6 elements. If, say, $A(x_0) = \varnothing$, then for any $x \neq x_0$ the set $A(x)$ must contain two elements whose difference is x. Two such configurations can always be mapped to each other in the required way.

When $n = 3$, then we need four empty sets and four 2-subspaces to get the total size of 16. Assume that $A(x_1) = A(x_2) = A(x_3) = A(x_4) = \varnothing$. We claim that x_1, x_2, x_3, x_4 are affinely independent. Otherwise they form an affine 2-subspace, however, taking some $x \notin \{x_1, x_2, x_3, x_4\}$ the affine 2-subspace $x + A(x) + A(x)$ would have to contain exactly three of x_1, x_2, x_3, x_4 (and x as the fourth element) which is impossible. Therefore, x_1, x_2, x_3, x_4 are affine independent, and by some affine linear transformation φ they can be mapped to $0, e_1, e_2, e_3$, for simplicity. Now, we can assume that 0 is contained in every nonempty $A(x)$ (by suitable translations). Then it follows that $A(e_i + e_j) = \langle e_i, e_j \rangle$, for $1 \leq i < j \leq 3$ and $A(e_1 + e_2 + e_3) = \langle e_1 + e_2, e_2 + e_3 \rangle$.

Finally, let $n = 4$. Note that $S = 42$ can hold only in Subcase 1 when $k = 10, \ell = 5$.

From the proof it follows that $S = 42$ is possible only if there are exactly five empty sets, ten 2-subspaces and one 1-subspace. Moreover, if u_1, u_2, u_3, u_4, u_5 are the vectors to which the empty set is assigned, then the 3-term sums made out of these 5 vectors have to be all distinct. Clearly, by applying a suitable affine linear transformation φ we can assume that $u_1 = 0$ and u_2, u_3, u_4 are linearly independent. If $u_5 \in \langle u_2, u_3, u_4 \rangle$, then all the 10 triple sums lie in a 3-subspace, so they can not be all distinct. Thus u_2, u_3, u_4, u_5 are linearly independent. Therefore, by renaming $u_1, \ldots, u_5$ (if necessary), let $A(0) = A(e_1) = A(e_2) = A(e_3) = A(e_4) = \varnothing$, where e_1, e_2, e_3, e_4 is a basis. The set $A(e_1+e_2+e_3+e_4)$ can not be a 2-subspace, since all vectors in it must have Hamming-weight at least 3 to satisfy

$$e_1 + e_2 + e_3 + e_4 + A(e_1 + e_2 + e_3 + e_4)\hat{+}A(e_1 + e_2 + e_3 + e_4) \subseteq \{0, e_1, e_2, e_3, e_4\}.$$

So it is the unique 1-subspace, for instance $A(e_1 + e_2 + e_3 + e_4) = \langle e_1 + e_2 + e_3 + e_4 \rangle$ is an appropriate choice, but $\langle e_i + e_j + e_k \rangle$ is also fine with any 3-subset $\{i, j, k\}$ of $\{1, 2, 3, 4\}$. By permuting $0, e_1, e_2, e_3, e_4$ with a suitable affine linear transformation we may assume that $A(e_1 + e_2 + e_3 + e_4) = \langle e_1 + e_2 + e_3 + e_4 \rangle$.

The remaining 10 sets need to be 2-subspaces. For $A(e_i + e_j)$ the unique appropriate choice is $A(e_i + e_j) = \langle e_i, e_j \rangle$, with this choice

$$e_i + e_j + A(e_i + e_j)\hat{+}A(e_i + e_j) = \{0, e_i, e_j\}$$

holds. For $A(e_i + e_j + e_k)$ the unique appropriate choice is

$$A(e_i + e_j + e_k) = \langle e_i + e_j, e_i + e_k \rangle = \{0, e_i + e_j, e_j + e_k, e_k + e_i\},$$

with this choice $e_i + e_j + e_k + A(e_i + e_j + e_k)\hat{+}A(e_i + e_j + e_k) = \{e_i, e_j, e_k\}$ is satisfied. □

4.7 Proof of $r_3(\mathbb{Z}_4^5) = 124$

We will show that if the system of subsets $\{A(x) \subseteq \mathbb{F}_2^5 \mid x \in \mathbb{F}_2^5\}$ satisfies $(*)$, then $S := \sum_{x \in \mathbb{F}_2^5} |A(x)| \leq 124$.

Again, by Observations 1-3 we can assume that all subsets have size at most 16 and every nonempty subset of size at most 4 is a subspace (of dimension at most 2).

Now, let us assume that $8 < |A(x)| \leq 16$. The set $A(x)$ must contain at least 4 linearly independent vectors. (Note that by Observation 2 we have $0 \in A(x)$.)

Step 1. First, let us assume that a set $A(x)$ with size $8 < |A(x)| \leq 16$ spans a 4-dimensional subspace. Our aim is to show it can be assumed that $A(x)$ itself is a 4-subspace.

Let $f_1, f_2, f_3, f_4 \in A(x)$ be linearly independent. Then $A(x)\hat{+}A(x)$ contains all the pairwise sums $f_i + f_j$. If $f_1 + f_2 + f_3 + f_4$ also lies in $A(x)$, then $A(x) + A(x) = \langle f_1, f_2, f_3, f_4 \rangle$, since the 3-term sums like $f_1 + f_2 + f_3$ can be obtained as $(f_1 + f_2 + f_3 + f_4) + f_4 = f_1 + f_2 + f_3$ and $f_1 + f_2 + f_3 + f_4 = (f_1 + f_2 + f_3 + f_4) + 0 \in A(x)\hat{+}A(x)$. Hence, if $f_1 + f_2 + f_3 + f_4 \in A(x)$, then $A(x)$ can be replaced by $A'(x) = \langle f_1, f_2, f_3, f_4 \rangle$.

Now, let us assume that $f_1 + f_2 + f_3 + f_4 \notin A(x)$. Let us call the 2-term sums $f_i + f_j$ (with $i \neq j$) *pairs* and the 3-term sums $f_i + f_j + f_k$ (with i, j, k distinct) *triples*. The pair $f_i + f_j$ can be identified with the set of indices $\{i, j\}$, let us call this subset $\{i, j\} \subseteq \{1, 2, 3, 4\}$ also a *pair*, and similarly the 3-element subset $\{i, j, k\}$ will be called a *triple* corresponding to the vector $f_i + f_j + f_k$. As the size of $A(x)$ is at least 9, the set $A(x)$ must contain at least $(9 - 4 - 1 =)4$ elements among the six pairs and four triples.

Now, we will prove that (at least) one of the following cases holds:

(i) $A(x)$ contains two disjoint pairs, for instance: $f_1 + f_2, f_3 + f_4 \in A(x)$,

(ii) $A(x)$ contains a pair and a triple such that their intersection has size 1, for instance: $f_1 + f_2$ and $f_2 + f_3 + f_4$,

(iii) $A(x)$ contains all triples,

(iv) $A(x)$ contains a triple and all the three pairs contained in it, for instance: $f_1 + f_2 + f_3, f_1 + f_2, f_1 + f_3, f_2 + f_3 \in A(x)$.

For the sake of contradiction let us assume that none of (i-iv) holds. Since we need at least four more vectors, at least one triple is contained in $A(x)$, by symmetry we shall assume that $f_1 + f_2 + f_3 \in A(x)$. Note that the pairs $f_1 + f_4, f_2 + f_4, f_3 + f_4$ are not in $A(x)$, since (ii) does not hold. Therefore, there must be (at least) one more triple in $A(x)$, otherwise (iv) would hold. We may assume that $f_1 + f_2 + f_4 \in A(x)$. Now, it follows that the pairs $f_1 + f_3, f_2 + f_3$ are not in $A(x)$. However, $A(x)$ must contain at least one pair, this pair can only be $f_1 + f_2$ (since the other five pairs are already excluded). The two remaining triples ($f_1 + f_3 + f_4$ and $f_2 + f_3 + f_4$) intersect the pair $f_1 + f_2$ in a single element, so they are not contained in $A(x)$ which contradicts that $A(x)$ contains at least 4 elements from the 4 triples and 6 pairs.

Finally, we show that the equality $A(x) + A(x) = \langle f_1, f_2, f_3, f_4 \rangle$ holds in all of the four cases (i)-(iv).

In case (i) we have $f_1 + f_2 + f_3 + f_4 = (f_1 + f_2) + (f_3 + f_4)$ and each triple contains either $\{1, 2\}$ or $\{3, 4\}$, thus they can be expressed like $f_1 + f_2 + f_3 = (f_1 + f_2) + f_3$.

In case (ii) we have $f_1 + f_2 + f_3 + f_4 = f_1 + (f_2 + f_3 + f_4)$, the triples $\{1, 2, 3\}$ and $\{1, 2, 4\}$ can be obtained like $f_1 + f_2 + f_3 = (f_1 + f_2) + f_3$, furthermore, $f_2 + f_3 + f_4 = 0 + (f_2 + f_3 + f_4)$ and $f_1 + f_3 + f_4 = (f_1 + f_2) + (f_2 + f_3 + f_4)$, as all $f_1, f_2, f_3, f_4 \in A(x)$.

In case (iii) all the triples can be written like $f_1 + f_2 + f_3 = (f_1 + f_2 + f_3) + 0$ and $f_1 + f_2 + f_3 + f_4 = (f_1 + f_2 + f_3) + f_4$.

In case (iv) all the triples can be written like $f_1 + f_2 + f_3 = (f_1 + f_2 + f_3) + 0$ or $(f_1 + f_2 + f_4) = (f_1 + f_2) + f_4$ and $f_1 + f_2 + f_3 + f_4 = (f_1 + f_2 + f_3) + f_4$.

Thus in all cases we get $A(x) + A(x) = \langle f_1, f_2, f_3, f_4\rangle$. Hence, if $A(x)$ is a set of size at least 9 (and at most 16) such that $A(x)$ is not a 4-subspace, then we can assume that $\dim\langle A(x)\rangle = 5$.

Step 2. We show that it can be assumed that there is no subset for which $8 < |A(x)| \leq 16$ and $\dim\langle A(x)\rangle = 5$. Our aim is to show that $A(x)$ can be replaced by a 4-subspace. Together with Step 1 this implies that we can assume that all sets having size larger than 8 are 4-subspaces. Moreover, we show that there can be at most one such subset.

Our aim is to show that either there is a 4-subspace $A'(x)$ such that $A'(x) \subseteq A(x) + A(x)$ or the total size S of the sets is at most 124.

Let us assume that $0, f_1, f_2, f_3, f_4, f_5 \in A(x)$, where $f_1, \ldots, f_5$ is a basis. Then all singletons f_i and pairs $f_i + f_j$ lie in $A(x)\hat{+}A(x)$. If a 4-term sum, like $f_1 + f_2 + f_3 + f_4$ lies in $A(x)$, then $A(x) + A(x)$ contains $\langle f_1, f_2, f_3, f_4\rangle$ and we are done: $A(x)$ can be replaced by $\langle f_1, f_2, f_3, f_4\rangle$. More generally we can formulate the following observation:

Observation 4. If it is possible to choose 6 vectors $w_1, \ldots, w_6$ from $A(x)$ in such a way that they span a 4-dimensional affine subspace and their sum is 0, then $A(x)$ can be replaced by a 4-subspace, since translating $A(x)$ by w_6 and taking $f_1 = w_1 + w_6, f_2 = w_2 + w_6, \ldots, f_4 = w_4 + w_6$ gives $w_5 + w_6 = f_1 + f_2 + f_3 + f_4$, so this case can be handled in the same way as the previous case.

Therefore, $f_1 + f_2 + f_3 + f_4 + f_5 \notin A(x)$, since $\{f_1, f_2, f_3, f_4, f_5, f_1 + f_2 + f_3 + f_4 + f_5\}$ adds up to 0. Thus the remaining elements of $A(x)$ are all pairs and triples. We claim that the following cases can be excluded with the help of Observation 4:

(i) there are two disjoint pairs, e.g. $f_1 + f_2, f_3 + f_4 \in A(x)$,

(ii) there are two triples intersecting each other in a single element, e.g. $f_1 + f_2 + f_3, f_3 + f_4 + f_5 \in A(x)$,

(iii) there is a pair and a triple intersecting each other in a single element, e.g. $f_1 + f_2, f_2 + f_3 + f_4 \in A(x)$.

In case (i) $f_1 + f_2 + f_3 + f_4 + (f_1 + f_2) + (f_3 + f_4) = 0$.
In case (ii) $(f_1 + f_2 + f_3) + (f_3 + f_4 + f_5) + f_1 + f_2 + f_4 + f_5 = 0$.
In case (iii) $(f_1 + f_2) + (f_2 + f_3 + f_4) + f_1 + f_3 + f_4 + 0 = 0$.

Finally, let us assume that (i)-(iii) do not hold. From (i) it follows that the pairs either form a star or a triangle. If they form a triangle, let us assume that it is $f_1 + f_2, f_2 + f_3, f_1 + f_3$. Since $f_1 + f_2 + f_3 \in A(x)$ would imply $\langle f_1, f_2, f_3, f_4\rangle \subseteq A(x) + A(x)$, we have $f_1 + f_2 + f_3 \notin A(x)$. Furthermore, (iii) implies that none of the other triples is in $A(x)$. Hence, $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1 + f_2, f_2 + f_3, f_1 + f_3\}$, we will refer to this as case (a). From now on, we assume that the pairs in $A(x)$ form a star.

If this star contains 4 vectors, e.g. $f_1+f_2, f_1+f_3, f_1+f_4, f_1+f_5 \in A(x)$, then $A(x)$ can not contain any triples because of (iii). (Case (b).)

If this star contains 3 vectors, e.g. $f_1+f_2, f_1+f_3, f_1+f_4$, then $A(x)$ can not contain any triples because of (iii). (Case (c).)

If this star contains 2 vectors, e.g. f_1+f_2, f_1+f_3. At least one triple must lie in $A(x)$ and (iii) implies that this triple is $f_1+f_2+f_3$. (Case (d).)

If only one pair is in $A(x)$, e.g. $f_1+f_2 \in A(x)$. There are at least two more vectors (thus triples) in $A(x)$. If one of them is $f_3+f_4+f_5$, then the other triple intersects the pair $\{1,2\}$ or the triple $\{3,4,5\}$ in one element, contradicting (ii) or (iii). Thus, by (iii) these two triples must contain $\{1,2\}$, which gives case (e).

If there are no pairs, then there are at least three triples. Any two of them have an intersection of size 2, giving case (f) or case (g).

We summarize this below.

(a) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2, f_2+f_3, f_1+f_3\}$

(b) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2, f_1+f_3, f_1+f_4, f_1+f_5\}$

(c) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2, f_1+f_3, f_1+f_4\}$

(d) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2, f_1+f_3, f_1+f_2+f_3\}$

(e) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2, f_1+f_2+f_3, f_1+f_2+f_4\}$

(f) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2+f_3, f_1+f_2+f_4, f_1+f_2+f_5\}$

(g) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5, f_1+f_2+f_3, f_1+f_2+f_4, f_1+f_3+f_4\}$

Note that the size of $A(x)$ is 10 in case (b) and 9 in the remaining cases (a) and (c)-(g). Also, the size of $A(x)\hat{+}A(x)$ is 21 in cases (b), (c), (e), (f) and 22 in cases (a), (d), (g).

Let us assume that there is at least one subset $A(x)$ having size at least 9 and not being a 4-subspace. Then at least 21 subsets out of the 32 sets $A(y)$ are empty, so at most 11 subsets are non-empty. Let k denote the number of 4-subspaces among the subsets $A(x)$. Then $S = \sum |A(y)| \le 16k + 10(11-k) = 110+6k$. If $k \le 2$, then this is at most 122. So let us assume that there are at least three 4-subspaces, namely, $A(y), A(z), A(u)$. Let $K = y + A(y), L = z + A(z), M = u + A(u)$, then K, L, M are affine subspaces of dimension 4.

If two of them are disjoint, for instance $K \cap L = \varnothing$, then $K \cup L = \mathbb{F}_2^5$, giving that $A(t) = \varnothing$ for every $t \notin \{y, z\}$, which is a contradiction. So any two of them intersect nontrivially, and then any pairwise intersection is a 3-dimensional affine subspace. As $y \notin L \cup M$, we have that $(K \cap L) \cap (K \cap M) \neq \varnothing$, since both of them is an 8-element subset of the 15-element set $K \setminus \{y\}$, hence $K \cap L \cap M \neq \varnothing$. Then $K \cap L \cap M$ has size 4 or 8. By inclusion-exclusion principle, in both cases

$$|K \cup L \cup M| = |K| + |L| + |M| - |K \cap L| - |K \cap M| - |L \cap M| + |K \cap L \cap M| \ge 28,$$

thus, at least $28 - 3 = 25$ subsets are empty and $S \leq 7 \cdot 16 = 112$.

Therefore, it can be assumed that all subsets having at least 9 elements are 4-subspaces, moreover there are at most 2 such subsets. If there are 2 such subsets $A(x)$ and $A(y)$, then

$$|A(x) \cup A(y)| = |A(x)| + |A(y)| - |A(x) \cap A(y)| \geq 16 + 16 - 8 = 24,$$

so at least $24 - 2 = 22$ subsets are empty and $S \leq 2 \cdot 16 + 8 \cdot 8 = 96$. Hence, it can be assumed that there is at most one 4-subspace.

Step 3. Now we show that if $|A(x)| \in [5, 8]$, then it can be assumed that $A(x)$ is either a 3-subspace or a set of 5 or 6 affine independent points.

Let us assume that $4 < |A(x)| \leq 8$. If $\langle A(x) \rangle$ has dimension 3, then $A(x)$ can be replaced with this 3-subspace. If $\dim\langle A(x) \rangle = 4$, then it can be assumed that $0, f_1, f_2, f_3, f_4 \in A(x)$. If at least one more element is in $A(x)$, then $A(x) + A(x)$ contains a 3-subspace and we can replace $A(x)$ by this 3-subspace, otherwise $A(x) = \{0, f_1, f_2, f_3, f_4\}$, we will refer to this case as case (A).

If $\dim\langle A(x) \rangle = 5$, then it can be assumed that $0, f_1, f_2, f_3, f_4, f_5 \in A(x)$. If at least one more element with Hamming-weight at most 4 is in $A(x)$, then $A(x) + A(x)$ contains a 3-subspace. If $f_1 + f_2 + f_3 + f_4 + f_5 \in A(x)$, then $\langle f_1 + f_2, f_2 + f_3, f_3 + f_4 \rangle \subseteq A(x) + A(x)$, otherwise $A(x) = \{0, f_1, f_2, f_3, f_4, f_5\}$, we will refer to this case as case (B).

Hence, it can be assumed that if there is a subset $A(x)$ (with size in $[5, 8]$) which is not a subspace, then it contains 5 or 6 affine independent points:

(A) $A(x) = \{0, f_1, f_2, f_3, f_4\}$

(B) $A(x) = \{0, f_1, f_2, f_3, f_4, f_5\}$

Note that the size of $A(x)$ in these cases is either 5 or 6.

Step 4. We show that it can be assumed that all subsets have size at most 8.

Note that we have already seen (in Step 2) that there can be at most one 4-subspace, so let us assume that there exists a (unique) 4-subspace $A(y)$. Then $|A(y) \hat{+} A(y)| = 15$, so there are at least 15 empty subsets. All the other subsets are 3-subspaces or have size at most 6. If there is no 3-subspace, then $S \leq 16 + 16 \cdot 6 = 112$, and we are done. Let $A(x)$ be a 3-subspace and $K = y + A(y), L = x + A(x)$. As $|K \cap L| \leq 4$, we have $|K \cup L| \geq 16 + 8 - 4 = 20$, so there are at least $20 - 2 = 18$ empty subsets, thus at most 14 non-empty ones implying $S \leq 16 + 13 \cdot 8 = 120$, and we are done. Therefore, none of the subsets can be a 4-subspace, and consequently all the subsets have size at most 8.

Step 5. We show that it can be assumed that all nonempty subsets are subspaces of dimension at most 3 or a set of 5 or 6 affine independent points. Furthermore, the number of empty sets among the $A(x)$ subsets is at most 16 and there exists a subset of size at least 5.

If $0 < |A(x)| \leq 4$, then by Observations 1-3 it can be assumed that $A(x)$ is a subspace.

Now, we can assume that all the subsets have size at most 8 and all those non-empty subsets that are not subspaces are of type (A) or (B).

If there are at least 17 empty subsets, then $S \leq 8 \cdot 15 = 120$, so it can be assumed that at most 16 subsets are empty.

If there is no subset with size larger than 2, then $S \leq 64$. If there is no subset with size larger than 4, then there must be a subset with size 4 and there are at most 29 non-empty sets, so $S \leq 29 \cdot 4 = 116$. So there is a subset of size at least five, this can be either of type (A) or (B) or a 3-subspace.

Now our aim is to show that we can assume that there is no subset of type (A) neither of type (B).

Step 6. We show that there is no subset of type (B).

Let us assume that there is a subset of type (B). Without loss of generality this is $A(0) = \{0, e_1, e_2, e_3, e_4, e_5\}$. Then

$$A(0)\hat{+}A(0) = \{e_1, \dots, e_5, e_1 + e_2, \dots, e_4 + e_5\} =: T,$$

that is, $A(0)\hat{+}A(0)$ has size 15 and $A(e_i) = \varnothing, A(e_i + e_j) = \varnothing$ for every $i \neq j$. As $17 \cdot 6 = 102 = 124 - 22$, at least 11 subsets are 3-subspaces. Let $A(x)$ be a 3-subspace and $K := x + A(x)$. As $A(0) \neq \varnothing$, we have $0 \notin K$. We claim that $K \setminus \{x\} \nsubseteq T$.

For the sake of contradiction, let us assume the contrary.
Let $U = (e_1 + e_2 + e_3 + e_4 + e_5)^{\perp}$ and $\overline{U} = \mathbb{F}_2^5 \setminus U$. As $|T \cap \overline{U}| = 5$, the set $K \cap \overline{U}$ can not be a 3-subspace. If $K \cap \overline{U}$ is a 2-subspace, then without loss of generality, $x = e_1 + e_2 + e_3$ and $K \cap \overline{U} = \{e_1 + e_2 + e_3, e_1, e_2, e_3\}$. However, none of the translates of this set is contained in $K \cap U$, thus we must have $K \subseteq U$, which leads to a contradiction, as well.

Hence, there exists some $y \notin T$ such that $A(y) = \varnothing$, so the number of the empty subsets is at least 16. If the number of 3-subspaces is at most 14, then $S \leq 14 \cdot 8 + 2 \cdot 6 = 124$, and we are done. So we can suppose that the number of 3-subspaces is at least 15 and one subset has size 6. The set $A(e_1 + e_2 + e_3 + e_4 + e_5)$ is not a 3-subspace, since any affine 3-subspace containing $e_1 + e_2 + e_3 + e_4 + e_5$ contains at least 2 more elements that are not in T. Hence $A(e_1 + e_2 + e_3 + e_4 + e_5)$ is the 16th empty subset. Now, we claim that $A(e_1 + e_2 + e_3 + e_4)$ is not a 3-subspace. This holds, since any affine 3-subspace containing $e_1 + e_2 + e_3 + e_4$ has at least one more element outside of $T \cup \{e_1 + e_2 + e_3 + e_4 + e_5\}$.

Therefore, there is no subset of type (B).

Step 7. We show that there is no subset of type (A).

Let us assume that there is a subset of type (A), it can be assumed that it is $A(0) = \{0, e_1, e_2, e_3, e_4\}$. Then $|A(0)| = 5$ and

$$A(0)\hat{+}A(0) = \{e_1, \dots, e_4, e_1 + e_2, \dots, e_3 + e_4\}$$

has size 10. That is, we already have 10 empty subsets.

For brevity let us write $A(i_1 i_2 \dots i_\ell)$ for $A(e_{i_1} + e_{i_2} + \dots + e_{i_\ell})$, if

$$\{i_1, i_2, \dots, i_\ell\} \subseteq \{1, 2, 3, 4, 5\}.$$

(For instance, $A(1) = A(e_1), A(123) = A(e_1 + e_2 + e_3)$, and so on.)

Let us assume first that the total size of the subsets

$$A(123), A(124), A(134), A(234), A(1234)$$

is at most 32.

Consider the following 16 subsets: $A(z + e_5)$ $(z \in \langle e_1, e_2, e_3, e_4\rangle)$. Let k denote the number of 3-subspaces among these and ℓ the number of empty ones. If $S \geq 125$, then $\sum |A(z + e_5)| \geq 125 - 5 - 32 = 88$, thus $8k + 5(16 - k - \ell) \geq 88$, and then

$$3k \geq 5\ell + 8. \tag{8}$$

If $A(z+e_5)$ is a 3-subspace, then $K_z = z+e_5+A(z+e_5)$ is an affine 3-subspace containing $z + e_5$. The 1-codimensional affine subspace $R = \{x : xe_5 = 1\}$ contains either all 8 elements of K_z or 4 elements of K_z. In the first case we get 7 new empty subsets, so the total number of empty subsets is at least 17 and we are done: $S \leq 15 \cdot 8 = 120$. So for every 3-subspace K_z exactly 4 elements of K_z lie in R. The sum of these 4 vectors is 0, so the sum of the three vectors in $(K_z \cap R) \setminus \{z+e_5\}$ is $z+e_5$. Hence, for every 3-subspace K_z we get an "empty triple" of vectors from R, therefore,

$$\binom{\ell}{3} \geq k. \tag{9}$$

By (8) and (9) we obtain that $\ell(\ell-1)(\ell-2)/2 \geq 5\ell + 8$, which yields $\ell \geq 6$. Then (8) implies that $k \geq 13$, which is a contradiction, since $6 + 13 > 16 = |R|$.

Hence, it can be assumed that the total size of the sets

$$A(123), A(124), A(134), A(234), A(1234)$$

is at least 33, on the other hand, it is clearly at most 40. It follows that none of them is empty and at least three of them are 3-subspaces, so we can assume that $A(123)$ is a 3-subspace. $A(123) \leq \langle e_1, e_2, e_3, e_4\rangle$ is not possible, since then $e_1 + e_2 + e_3 + A(123)$ would contain $e_1 + e_2 + e_4$ or $e_1 + e_3 + e_4$ or $e_2 + e_3 + e_4$ or $e_1 + e_2 + e_3 + e_4$. Indeed, if an affine 3-subspace of $\langle e_1, e_2, e_3, e_4\rangle$ contains $e_1 + e_2 + e_3$ but none of the other 4 vectors, then it is $\langle e_1, e_2, e_3\rangle$, however, $\langle e_1, e_2, e_3\rangle$ contains 0, as well, which is a contradiction.

So $e_1+e_2+e_3+A(123)$ intersects nontrivially R, so $|(e_1+e_2+e_3+A(123)) \cap R| = 4$, thus at least 4 subsets (among subsets $A(x)$ with $x \in R$) are empty: $\ell \geq 4$. Note that the sum of the four corresponding vectors is 0. Also, note that in this case (similarly to (8) in the previous case) we shall assume that

$$3k \geq 5\ell. \tag{10}$$

Now (10) yields that at least 7 such subsets are 3-subspaces: $k \geq 7$. Then (9) implies that the number of empty ones is at least 5. Again, by (10) we get $k \geq 9$. If $\ell = 5$, then we have $\binom{5}{3} = 10$ triples, but there is a 4-term zero-sum, so 4 triples can not be "empty triples", thus there is a 6th empty subset: $\ell \geq 6$, and by (10) we obtain that $k \geq 10$. So $\sum |A(z+e_5)| = 10 \cdot 8 = 80$. As $125 - 5 - 80 = 40$, all the sets $A(123), A(124), A(134), A(234), A(1234)$ must be 3-subspaces. If

$$v \in \{e_1+e_2+e_3, e_1+e_2+e_4, e_1+e_3+e_4, e_2+e_3+e_4, e_1+e_2+e_3+e_4\},$$

then $v + A(v)$ intersects R in 4 vectors whose sum is 0. It can be checked that this set of 4 vectors can not be the same for all the 5 possible v-s. (Otherwise $\mathbb{F}_2^5 \setminus R$ would contain at least 15 vectors to which the empty set is assigned, however, there are only 10 such vectors.) So there must be at least two such 4-element sets. Their intersection has size at least 2, since we have only 6 vectors in R to which the empty set is assigned, and also at most 2, otherwise they would be the same. Let $A(z_1+e_5), \ldots, A(z_6+e_5)$ be the empty ones, and let us assume that the two 4-zero-sum-sets are $\{z_1, \ldots, z_4\}$ and $\{z_3, \ldots, z_6\}$. Then $z_1 + z_2 = z_3 + z_4 = z_5 + z_6$. 20 triples can be chosen out of these 6 vectors, but just 8 of them can be "empty triples", which is a contradiction.

Therefore, we can assume that there is no subset of type (A), that is, all the nonempty subsets are subspaces of dimension at most 3. According to Step 5 there must be at least one 3-subspace among the subsets, as Steps 6-7 imply that all the sets of size at least 5 are 3-subspaces.

Step 8. We show that the number of empty subsets is at least 13.

Let $1 \leq k$ be the number of 3-subspaces and ℓ the number of empty subsets. Let us colour the elements of $\mathbb{F}_2^5$: x is coloured red, if $A(x) = \varnothing$ and x is coloured blue, if $A(x)$ is a 3-subspace. (If $A(x)$ is a subspace of dimension at most 2, then x is not coloured.) Let $\tilde{A}(x) = x + A(x)$, specially, if x is blue, then $\tilde{A}(x)$ is a 3-dimensional affine subspace containing x and seven red vectors.

If $125 \leq S$, then $125 \leq 8k + (32 - k - \ell)4$ which yields $\ell \leq k$. Now we are going to show that $\ell \geq 13$. If x is blue, then in $\tilde{A}(x)$ there are two kinds of triples: the 2-subspace spanned by them either contains x or not. The number of triples in $\tilde{A}(x) \setminus \{x\}$ is 35 and 7 of these triples span a 2-subspace containing x. These triples are not contained in any other affine 3-subspace $\tilde{A}(y)$.

Furthermore, we claim that if $\ell < 13$, then a triple can appear in at most two 3-subspaces. For the sake of contradiction, let us assume that a triple is contained in $K \cap L \cap M$, where $K = \tilde{A}(x), L = \tilde{A}(y), M = \tilde{A}(z)$ are 3-subspaces. Let H be the 2-subspace spanned by this triple, then $H = K \cap L \cap M$ and $K \setminus H$, $L \setminus H$, $M \setminus H$ are disjoint, thus $|K \cup L \cup M| = 16$. However, in $K \cup L \cup M$ all the vectors are red except x, y, z, hence $16 - 3 = 13 \leq \ell$, which is a contradiction.

Now, since each triple appears in at most two 3-subspaces, we obtain that

$$7\ell + \frac{28\ell}{2} \leq 7k + \frac{28k}{2} \leq \binom{\ell}{3},$$

thus

$$126 \le (\ell - 1)(\ell - 2),$$

implying that $\ell \ge 13$.

Therefore, $k \ge \ell \ge 13$, as we claimed.

Step 9. We show that if $A(x), A(y), A(z)$ are 3-subspaces (with distinct x, y, z), then $A(x) \cap A(y) \cap A(z)$ is not an affine 2-subspace.

Now, for the sake of contradiction, assume that there are three 3-subspaces, $A(x), A(y), A(z)$ whose intersection is an affine 2-subspace L. Without loss of generality we can assume that L is a linear (2-)subspace. Note that

$$\tilde{A}(x) = L \cup (L + x), \quad \tilde{A}(y) = L \cup (L + y), \quad \tilde{A}(z) = L \cup (L + z).$$

Note that $\mathbb{F}_2^5$ can be partitioned into 8 translates of L. Every affine 3-subspace contains the same number of vectors from those L-translates that have a nonempty intersection with it. That is, given a 2-subspace L, we can distinguish three types of affine 3-subspaces, we are going to say that a 3-subspace is of

- type-1, if it contains 1-1 vector from each L-translate,
- type-2, if it contains 2-2 vectors from four L-translates (and none from the remaining four L-translates),
- type-4, if it contains 4-4 vectors from two L-translates (and none from the remaining six L-translates).

In $M = L \cup (L + x) \cup (L + y) \cup (L + z)$ there are 13 red elements, namely, all the vectors except x, y, z. If $t \notin M$ is blue, then $\tilde{A}(t)$ is a 3-subspace of type-1, type-2 or type-4 which contains t and seven red vectors.

If at least two L-translates do not contain any red vector, then the elements of these translates can not be blue, so $k \le 11$, which is a contradiction. Hence, there is at most one L-translate without any red vector. In particular, this means that $\ell \ge 16$, since there are 13 red vectors in M and at least 3 red vectors outside of M.

Thus $k = \ell = 16$. Let us assume that the red vectors outside of M are v_1, v_2, v_3, these vectors must be in different L-translates. Let $L' = \{u_1, u_2, u_3, u_4\}$ be the unique L-translate not containing any red vector. If $v_1 + v_2 + v_3 \in L'$, then at most one of the $A(u_i)$ sets can be a 3-subspace (namely, $A(v_1 + v_2 + v_3)$), which is a contradiction. Now assume that $v_1 + v_2 + v_3 \notin L'$. By symmetry we can assume that $v_1 + v_2 + v_3 \notin L + x$ also holds. But then the union of the $\tilde{A}(u_i) = \langle u_i, v_1, v_2, v_3 \rangle_{aff}$ sets (that are all affine 3-subspaces of type-1) cover $L + x$ and the (unique) u_i for which $x \in \tilde{A}(u_i)$ can not be blue (since x is not red). Hence, no three-wise intersection of 3-subspaces can be a 2-subspace.

Step 10. Now we know that $13 \le \ell \le k$ and no three-wise intersection of 3-subspaces is a 2-subspace. We finish the proof of the upper bound 124 by verifying the statement in these cases.

Let N be the number of those pairs of 3-subspaces whose intersection is a 2-subspace. Then

$$35k \le \binom{\ell}{3} + 4N, \tag{11}$$

since each of the k 3-subspaces contains 35 empty triples. Hence, for $\ell < 16$ we have $N > 0$, that is, two of the 3-subspaces assigned to blue vectors intersect each other in a 2-subspace. In the following subcases we always take two such subsets first.

Subcase 1. If $\ell = 13$, then we can assume that L is a linear 2-subspace and $\tilde{A}(x) = L \cup (L + x), \tilde{A}(y) = L \cup (L + y)$ are 3-subspaces corresponding to blue vectors x and y. At least 2 translates of L does not contain any red vector, and in these translates there can not be any blue vectors, either. So the number of blue vectors is at most $32 - 13 - 8 = 11$, which is a contradiction.

Subcase 2. If $\ell = 14$, then again let L be a linear 2-subspace and $\tilde{A}(x) = L \cup (L+x), \tilde{A}(y) = L \cup (L+y)$ be 3-subspaces corresponding to blue vectors x and y. Note that in $L \cup (L + x) \cup (L + y)$ there are 10 red vectors. We have 4 more red vectors, say, v_1, v_2, v_3, v_4, which must lie in different L-translates. (Otherwise, there would be two L-translates without any red vector, which would imply that the 8 vectors in these translates are not coloured, contradicting that the number of non-coloured vectors is at most 4.)

Note that all the 3-subspaces assigned to some blue vector different from x, y are of type-1 or type-2. To get a 3-subspace of type-2 we need to take 2-2 red vectors from $L, L+x, L+y$. Moreover, these pairs must determine parallel vectors in these three L-translates (that is, in each pair the sum of the two vectors is the same), so there are at most 6 such subspaces. A type-1 3-subspace must correspond to a (blue) vector from the last L-translate, so there are at most 4 such subspaces. Hence $k \le 4 + 6 + 2 = 12$, which is a contradiction.

Subcase 3. Let us assume that $\ell = 15$. Again, we can assume that for some linear 2-subspace L the sets $A(x) = L \cup (L + x), A(y) = L \cup (L + y)$ are two 3-subspaces. Let $L_4, \dots, L_8$ be the remaining five L-translates. They contain altogether 5 red vectors. If at least two of them do not contain any red vector, then in these two L-translates there aren't any blue vectors either, so the number of blue vectors is at most 9, which is a contradiction. So without the loss of generality it can be assumed that either (i) L_4 contains two red vectors and each of L_5, L_6, L_7 contains exactly one vector: v_i in L_i $(5 \le i \le 7)$ or (ii) each of $L_4, \dots, L_8$ contains exactly one red vector: v_i in L_i $(4 \le i \le 8)$.

In case (i) let α, β be the two directions that are different from the direction determined by the two red vectors of L_4. That is, α and β are those two nonzero elements of L that are different from the sum of the two red vectors in L_4. Let us consider the following 6 vectors in L_5, L_6, L_7: $v_i + \alpha, v_i + \beta$ (for $5 \le i \le 7$). If such a vector is blue, then the corresponding 3-subspace is of type-2, moreover, L_1, L_2, L_3 contain one-one red pair of this 3-subspace, and in each pair the sum is the same, either α or β. There are only 4 such triples (of pairs of vectors) meaning that at

least two of the vectors $v_i+\alpha, v_i+\beta$ $(5 \le i \le 7)$ are not blue. To get 15 blue vectors all vectors in L_8 must be blue (as there are at most 2 non-coloured vectors). Note that the corresponding 3-subspaces must be of type-1. If $v_5 + v_6 + v_7 \in L_8$, then there can be at most one blue element in L_8 (namely $v_5+v_6+v_7$). If $v_5+v_6+v_7 \notin L_8$, then by symmetry we can also assume that $v_5 + v_6 + v_7 \notin L_2$. If $t \in L_8$ is blue, then the corresponding 3-subspace is $\tilde{A}(t) = \langle v_5, v_6, v_7, t\rangle_{aff}$, but these four 3-subspaces cover L_2, which contradicts that L_2 contains only 3 red vectors.

In case (ii) there are two 3-subspaces of type-4. To get a 3-subspace of type-2, we have to choose one-one red pair from L_1, L_2, L_3 in such a way that these pairs determine parallel directions. This can be done in 6 ways, and every affine 3-subspace is determined by 6 points of it, so there are at most six 3-subspaces of type-2. To get a 3-subspace of type-1 we have to choose a red vector from all but one of the L-translates. First assume that no four-element subset of $\{v_4, \dots, v_8\}$ is a 2-subspace. Then the (at least) four red vectors chosen to be in this 3-subspace from $\{v_4, \dots, v_8\}$ determine uniquely a 3-subspace, so the number of 3-subspaces of type-1 is at most 5, thus $k \le 2+6+5 = 13$, which is a contradiction. Now assume that a 4-element subset, say, $\{v_4, v_5, v_6, v_7\}$ forms a 2-subspace. Each 3-subspace of type-1 contains at least 3 elements of $\{v_4, v_5, v_6, v_7\}$, hence all of them contain all these four vectors. Then the blue vector is in $L_8 \setminus \{v_8\}$, so there are at most 3 such subspaces, thus, $k \le 2 + 6 + 3 = 11$, which is a contradiction.

Subcase 4. Finally, let us assume that $\ell = k = 16$, that is, all vectors are either red or blue. First we show that there are two 3-subspaces whose intersection is a 2-subspace. For the sake of contradiction, assume the contrary. Let S_1, S_2, S_3, S_4 be four 3-subspaces assigned to blue vectors. If every pairwise intersection has size less than 4 (that is, the intersection is either empty or has size 2), then

$$|S_1 \cup S_2 \cup S_3 \cup S_4| \ge \sum |S_i| - \sum |S_i \cap S_j| \ge 4 \cdot 8 - 6 \cdot 2 = 20, \tag{12}$$

so $S_1 \cup S_2 \cup S_3 \cup S_4$ contains at least $20 - 4 = 16$ red vectors. Since there are only 16 red vectors, we must have equality in (12), so each pairwise intersection has size 2 and each triple-intersection has size 0. Clearly, these hold for any four 3-subspaces assigned to blue vectors. Pick such a 3-subspace, for instance, S_1. Then the other fifteen 3-subspaces have to intersect S_1 in pairwise disjoint pairs, which is impossible. Therefore, there are two 3-subspaces whose intersection is a 2-subspace.

Hence, we can assume that this 2-subspace is a linear 2-subspace L and the sets $A(x) = L \cup (L + x), A(y) = L \cup (L + y)$ are two 3-subspaces corresponding to blue vectors x and y. Let $L_4, \dots, L_8$ be the remaining five L-translates. These contain 6 more red vectors. As there can be at most one L-translate without any red vector, we can assume that the number of red vectors among them is i) 3-1-1-1-0 or ii) 2-2-1-1-0 or iii) 2-1-1-1-1.

In case i) let v_5, v_6, v_7 be the red vectors in L_5, L_6, L_7. If $v_5+v_6+v_7 \in L_8$, then in L_8 there is at most one blue vector (namely, $v_5+v_6+v_7$), which is a contradiction. Assume that $v_5 + v_6 + v_7 \notin L_8$. We can assume that $v_5 + v_6 + v_7 \notin L_2$. If $t \in L_8$ is

blue, then $\tilde{A}(t) = \langle t, v_5, v_6, v_7 \rangle_{aff}$, but these cover L_2, which contradicts that L_2 contains a blue element.

In case ii) let us assume that the direction $0 \neq \alpha \in L$ is different from the direction(s) determined by the pairs in L_4, L_5. Let $v_6 \in L_6, v_7 \in L_7$ be the red vectors in these translates. Consider the blue vectors $v_6 + \alpha$ and $v_7 + \alpha$. The 3-subspaces corresponding to them are of type-2, and both of them contain one-one pair from L_1, L_2, L_3, moreover, all these pairs determine direction α. In L_2 and L_3 these pairs are uniquely determined. In L_1 there are two choices (two disjoint pairs). However, these two pairs in L_1 together with the pairs from L_2 and L_3 determine two pairs in the same L-translate, which contradicts the existence of such a pair in both L_6 and L_7.

Finally, we consider case iii). Let $\ell_1 = 0, \ell_2 = e_3, \ell_3 = e_4, \ell_4 = e_3 + e_4, \ell_5 = e_5, \ell_6 = e_3 + e_5, \ell_7 = e_4 + e_5, \ell_8 = e_3 + e_4 + e_5$ and $L = \langle e_1, e_2 \rangle$. For every $1 \leq i \leq 8$ let $L_i = L + \ell_i$. We can assume that L_1 contains 4 red vectors and L_2, L_3 contain 3-3 red vectors.

First assume that the L-translate containing 2 red vectors is L_4, we can assume that these vectors are $e_3 + e_4$ and $e_1 + e_3 + e_4$. Let t be a blue vector in one of the four L-translates $L_5, \ldots, L_8$. Then $\tilde{A}(t)$ is either of type-2 or type-1. However, only L_1, L_2, L_3, L_4 contain at least two red vectors, which means that any 3-subspace of type-2 must contain at least 6 vectors from $L_1 \cup L_2 \cup L_3 \cup L_4$, which is a 4-subspace, thus the remaining two vectors of the 3-subspace must also lie in this subspace, too. So $\tilde{A}(t)$ is of type-1. As $L_5 \cup L_6 \cup L_7 \cup L_8$ is an affine 4-subspace, it intersects $\tilde{A}(t)$ in an affine 2-subspace. Therefore, if, say, $t \in L_8$, then t and the red vectors from L_5, L_6, L_7 form an affine 2-subspace, that is, t is the sum of these three red vectors. But then in L_8 the only blue vector is t, which is a contradiction.

Hence, L_4 contains one red vector. By symmetry, we can assume that L_5 contains 2 red vectors and these are e_5 and $e_1 + e_5$. Let the red vector in L_i be $\ell_i + t_i$ for $i \in \{4, 6, 7, 8\}$.

Let $i \in \{6, 7, 8\}$. We claim that $\tilde{A}(\ell_i + t_i + e_2)$ and $\tilde{A}(\ell_i + t_i + e_1 + e_2)$ must be of type-1. Otherwise, $\tilde{A}(\ell_i + t_i + e_2)$ or $\tilde{A}(\ell_i + t_i + e_1 + e_2)$ would contain at least two vectors from $L_5 \cup L_6 \cup L_7 \cup L_8$, so it would have to contain two more red vectors from one of the L-translates L_5, L_6, L_7, L_8, these could only be e_5 and $e_5 + e_1$ from L_5. But then the blue vector $\ell_i + t_i + e_1$ would also lie in the 3-subspace (to get parallel pairs from the different translates), a contradiction. Hence, $\tilde{A}(\ell_i + t_i + e_2)$ and $\tilde{A}(\ell_i + t_i + e_1 + e_2)$ are of type-1.

Consider $\tilde{A}(\ell_6 + t_6 + e_2)$ and $\tilde{A}(\ell_6 + t_6 + e_1 + e_2)$. Each of these two subspaces contain either e_5 or $e_5 + e_1$ and they contain $\ell_7 + t_7$ and $\ell_8 + t_8$. As the intersection of $\tilde{A}(\ell_6 + t_6 + e_2) \cap \tilde{A}(\ell_6 + t_6 + e_1 + e_2)$ with the 1-codimensional affine subspace $L_5 \cup L_6 \cup L_7 \cup L_8$ must be of size 2, they contain different elements from L_5. Without loss of generality we can assume that $\tilde{A}(\ell_6 + t_6 + e_2)$ contains e_5. Then $e_5 + (\ell_6 + t_6 + e_2) + (\ell_7 + t_7) + (\ell_8 + t_8) = 0$, that is, $t_6 + t_7 + t_8 = e_2$. Now $\tilde{A}(\ell_6 + t_6 + e_2)$

and $\tilde{A}(\ell_6+t_6+e_2+e_1)$ are determined, since they must contain ℓ_4+t_4:

$$\tilde{A}(\ell_6+t_6+e_2) = \{\ell_1+t_4+t_8, \ell_2+t_4+t_6+t_8+e_2, \ell_3+t_4+t_7+t_8, \ell_4+t_4, \ell_5, \ell_6+t_6+e_2, \ell_7+t_7, \ell_8+t_8\},$$

$$\tilde{A}(\ell_6+t_6+e_2+e_1) = \{\ell_1+t_4+t_8+e_1, \ell_2+t_4+t_6+t_8+e_2+e_1, \ell_3+t_4+t_7+t_8, \ell_4+t_4, \ell_5+e_1, \ell_6+t_6+e_2+e_1, \ell_7+t_7, \ell_8+t_8\}.$$

Similarly, the type-1 3-subspaces containing 2-2 blue vectors from L_7 and L_8 are:

$$\{\ell_1+t_4+t_8, \ell_2+t_4+t_6+t_8, \ell_3+t_4+t_7+t_8+e_2, \ell_4+t_4, \ell_5, \ell_6+t_6, \ell_7+t_7+e_2, \ell_8+t_8\},$$
$$\{\ell_1+t_4+t_8, \ell_2+t_4+t_6+t_8, \ell_3+t_4+t_7+t_8+e_2+e_1, \ell_4+t_4, \ell_5+e_1, \ell_6+t_6, \ell_7+t_7+e_2+e_1, \ell_8+t_8\},$$
$$\{\ell_1+t_4+t_8+e_2, \ell_2+t_4+t_6+t_8+e_2, \ell_3+t_4+t_7+t_8+e_2, \ell_4+t_4, \ell_5, \ell_6+t_6, \ell_7+t_7, \ell_8+t_8+e_2\},$$
$$\{\ell_1+t_4+t_8+e_2+e_1, \ell_2+t_4+t_6+t_8+e_2+e_1, \ell_3+t_4+t_7+t_8+e_2+e_1, \ell_4+t_4, \ell_5+e_1, \ell_6+t_6, \ell_7+t_7, \ell_8+t_8+e_2+e_1\}.$$

So the set of red vectors in L_2 is $\{\ell_2+t_4+t_6+t_8, \ell_2+t_4+t_6+t_8+e_2, \ell_2+t_4+t_6+t_8+e_2+e_1\}$ and in L_3 is $\{\ell_3+t_4+t_7+t_8, \ell_3+t_4+t_7+t_8+e_2, \ell_3+t_4+t_7+t_8+e_2+e_1\}$.

Now consider $\ell_8+t_8+e_1$ which is a blue vector in L_8. Note that $\tilde{A}(\ell_8+t_8+e_1)$ is of type-2 (otherwise the three 3-subspaces corresponding to blue vectors from L_8 would have a 2-subspace intersection, contradicting Step 9). Also, it must contain ℓ_8+t_8. As it contains at least 2 vectors from the 1-codimensional affine subspace $L_5 \cup L_6 \cup L_7 \cup L_8$, it must contain two more, which can only be ℓ_5 and ℓ_5+e_1. The remaining two red pairs are in two of L_1, L_2, L_3. As $L_8 = L_5 + (e_3+e_4)$, these two L-translates must be L_2 and L_3. Also, the difference of the vectors from the same L-translate must be e_1, so the 3-subspace is:

$$\{\ell_2+t_4+t_6+t_8+e_2, \ell_2+t_4+t_6+t_8+e_2+e_1, \ell_3+t_4+t_7+t_8+e_2, \ell_3+t_4+t_7+t_8+e_2+e_1, \ell_5, \ell_5+e_1, \ell_8+t_8, \ell_8+t_8+e_1\}.$$

As $\{\ell_2+t_4+t_6+t_8+e_2, \ell_2+t_4+t_6+t_8+e_2+e_1\} = \{\ell_5, \ell_5+e_1\}+e_5+e_3+t_4+t_6+t_8+e_2$, we get that $\{\ell_8+t_8, \ell_8+t_8+e_1\}+e_5+e_3+t_4+t_6+t_8+e_2 = \{\ell_3+t_4+t_6+e_2, \ell_3+t_4+t_6+e_2+e_1\}$ has to coincide with $\{\ell_3+t_4+t_7+t_8+e_2, \ell_3+t_4+t_7+t_8+e_2+e_1\}$. However, this leads to $t_6+t_7+t_8 \in \{0, e_1\}$, which is a contradiction.

4.8 4AP-free subsets of $\mathbb{Z}_4^n$

Proof of Theorem 2.12. According to Lemma 4.2 it suffices to show that $r'_4(1) = 3, r'_4(2) = 10, r'_4(3) = 36$ and $r'_4(4) = 128$. In other words, we will show that if

the system of subsets $\{A(x) \subseteq \mathbb{F}_2^n \mid x \in \mathbb{F}_2^n\}$ satisfies $(**)$, then $S = \sum_{x \in \mathbb{F}_2^n} |A(x)|$ is at most 3, 10, 36, 128 for $n = 1, 2, 3, 4$, respectively. Then, we will present constructions of these sizes.

By the pigeon-hole principle we get that $A(x) + A(x) = \mathbb{F}_2^n$, if $|A(x)| > 2^{n-1}$. Hence, $|A(x)| > 2^{n-1}$ holds for at most one x, since $x \neq y$ and $2^{n-1} < |A(x)|, |A(y)|$ would imply that $x + y \in (A(x) + A(x)) \cap (A(y) + A(y)) = \mathbb{F}_2^n$, contradicting $(**)$.

This observation immediately yields that $S \leq 2^n + (2^n - 1)2^{n-1} = 2^{2n-1} + 2^{n-1}$. For $n = 1, 2, 3$ we obtain the claimed upper bounds $3, 10, 36$, respectively.

Hence, for $n = 4$ we obtain that $S \leq 136$, now we will show that $S \leq 128$ also holds. We have already seen (in the proof of Theorem 2.11) that it can be assumed that all the nonempty $A(x)$ subsets are linear subspaces or a set of 5 affine independent points. If all the subsets are of size at most 8, then clearly $S \leq 16 \cdot 8 = 128$. So we can assume that one of them is $\mathbb{F}_2^4$, without loss of generality let $A(0) = \mathbb{F}_2^4$. It can be assumed that the number of 3-subspaces among the $A(x)$ sets is at least 13, since otherwise $S \leq 16 + 12 \cdot 8 + 3 \cdot 5 = 127$. If $A(x)$ is a 3-subspace, then for some (uniquely determined) $\varphi(x) \in \mathbb{F}_2^4$ we have $A(x) = (\varphi(x))^\perp$. As

$$x + 0 \notin (A(x) + A(x)) \cap (A(0) + A(0)) = A(x),$$

we obtain that $x\varphi(x) = 1$. We claim that φ is injective, that is, if $A(x)$ and $A(y)$ are 3-subspaces (with $x \neq y$), then $\varphi(x) \neq \varphi(y)$. Otherwise, $(x + y)\varphi(x) = x\varphi(x) + y\varphi(y) = 1 + 1 = 0$, so $x + y \in A(x)$ and similarly $x + y \in A(y)$. So this would lead to $x + y \in (A(x) + A(x)) \cap (A(y) + A(y))$, which contradicts property $(**)$. Therefore, φ is injective. Also, if $A(x)$ and $A(y)$ are 3-subspaces (and $x \neq y$), then $x\varphi(y) = 0$ or $y\varphi(x) = 0$, since $x\varphi(y) = y\varphi(x) = 1$ would imply that $(x + y)\varphi(x) = 0 = (x + y)\varphi(y)$ and so $x + y \in (A(x) + A(x)) \cap (A(y) + A(y))$, which would contradict property $(**)$.

Now, let us assume that for some z the set $A(z)$ is a set of 5 affine independent points. Let $X = \{x \in \mathbb{F}_2^4 \mid x + z \in A(z) \hat{+} A(z)\}$. As $z = z + 0 \notin (A(z) \hat{+} A(z)) \cap (A(0) \hat{+} A(0)) = A(z) \hat{+} A(z)$, we have $X \subseteq \mathbb{F}_2^4 \setminus \{0, z\}$. Note that $A(z) \hat{+} A(z)$ contains $\binom{5}{2}$ (distinct) sums, thus we have $|X| = 10$. For all $x \in X$ we have $x + z \notin A(x) \hat{+} A(x)$. We know that at least 13 subsets are 3-subspaces, so there are at most three subsets that are not 3-subspaces: $A(0), A(z)$ and possibly one more. Thus for at least 9 elements of X the set $A(x)$ is a 3-subspace. For such an x the condition $x + z \notin A(x) \hat{+} A(x)$ implies that $1 = (x + z)\varphi(x) = 1 + z\varphi(x)$, hence $z\varphi(x) = 0$. As φ is injective, this would mean that the 3-subspace $(z)^\perp$ contains at least 9 different vectors, which is a contradiction. Hence, it can be assumed that all the nonempty $A(x)$ sets are linear subspaces.

At least 14 of the $A(x)$ subsets are 3-subspaces, since otherwise $S \leq 16 + 13 \cdot 8 + 2 \cdot 4 = 128$ clearly holds, as $|A(x)| \leq 4$ for every $x \neq 0$ for which $A(x)$ is not a 3-subspace. Therefore, the mapping φ is defined on $\mathbb{F}_2^4 \setminus \{0\}$ with the exception of at most one point. Also, φ is injective, so it can be extended to a bijective mapping from $\mathbb{F}_2^4 \setminus \{0\}$ to $\mathbb{F}_2^4 \setminus \{0\}$.

Let $H = \{x : A(x) \text{ is a 3-subspace}\}$. Then either $H = \mathbb{F}_2^4 \setminus \{0\}$ or $H = \mathbb{F}_2^4 \setminus \{0, u\}$ for some u. Let

$$N := |\{(x, y) : \ x, y \in H, \ x \neq y, \ x\varphi(y) = 0\}|.$$

At first assume that $H = \mathbb{F}_2^4 \setminus \{0\}$. As at least one of $x\varphi(y)$ and $y\varphi(x)$ is equal to 0 for every $x \neq y$, we get that $N \geq \binom{15}{2} = 105$. On the other hand

$$N \leq \sum_{x \in H} (|x^\perp| - 1) = 15 \cdot 7 = 105.$$

Therefore, $|N| = 105$ and for any two distinct elements of H exactly one of $x\varphi(y)$ and $y\varphi(x)$ is equal to 0. In other words, $x\varphi(y) + y\varphi(x) = 1$ for any two different elements $x, y \in H$. Let

$$u(x) = (1, x, \varphi(x)), \ v(x) = (1, \varphi(x), x) \in \mathbb{F}_2^9$$

for every $x \in H$. Then $u(x)v(y) = \delta_{xy}$, thus $\{u(x), v(x)\}_{x \in H}$ is a biorthogonal system, implying that $|H| \leq \dim(\mathbb{F}_2^9) = 9$, which is a contradiction.

Now assume that there is a subset $A(u)$ (with $u \neq 0$) which is not a 3-subspace: $H = \mathbb{F}_2^4 \setminus \{0, u\}$. As at least one of $x\varphi(y)$ and $y\varphi(x)$ is equal to 0 for every $x \neq y$, we get that $N \geq \binom{14}{2} = 91$. However,

$$N \leq \left(\sum_{x \in H} (|x^\perp| - 1) \right) - |u^\perp \cap H| \leq 14 \cdot 7 - 6 = 92.$$

Hence, $N \in \{91, 92\}$ and there is at most one pair of distinct elements $x, y \in H$ such that $x\varphi(y) = y\varphi(x) = 0$. By dropping out one of the two elements of this pair from H (if such a pair exists at all) we obtain a 13-element subset $H' \subseteq H$ such that $x\varphi(y) + y\varphi(x) = 1$ for every $x, y \in H'$, $x \neq y$. Again, let

$$u(x) = (1, x, \varphi(x)), \ v(x) = (1, \varphi(x), x) \in \mathbb{F}_2^9$$

for every $x \in H'$. Then $u(x)v(y) = \delta_{xy}$, thus $\{u(x), v(x)\}_{x \in H'}$ is a biorthogonal system, implying that $|H'| \leq 9$, which is a contradiction.

Hence, it is shown that $S \leq 128$.

Now we give constructions to prove the lower bounds.

Case 1: $n = 1$**.**

$A(0) = \mathbb{F}_2, A(1) = \{0\}$ give $3 \leq r_4'(1)$. (In fact, any 3-element subset of $\mathbb{Z}_4$ is free of arithmetic progressions of length 4, trivially.)

Case 2: $n = 2$**.**

Let $A(0) = \mathbb{F}_2^2 = \langle e_1, e_2 \rangle$. Furthermore, let

$$\varphi(e_1) = e_1, \varphi(e_2) = e_1 + e_2, \varphi(e_1 + e_2) = e_2.$$

Then $x\varphi(x) = 1$ for every $x \neq 0$ and $x\varphi(y) + y\varphi(x) = 1$ for every $x, y \in \mathbb{F}_2^2 \setminus \{0\}$, $x \neq y$. For $0 \neq x$ let $A(x) = (\varphi(x))^\perp$. Then $x + 0 \notin A(x)$, since $x\varphi(x) = 1$. Also, for

any two nonzero vectors x and y either $x\varphi(y) = 0$ or $y\varphi(x) = 0$. We can assume that $x\varphi(y) = 0$. (Otherwise we swap x and y.) Then $(x + y)\varphi(y) = 0 + 1$ implies that $x + y \notin A(y) = A(y) + A(y)$, so the condition $(**)$ holds. Thus $10 \le r'_4(2)$.

Case 3: $n = 3$**.**

Let $A(0) = \mathbb{F}_2^3 = \langle e_1, e_2, e_3\rangle$. Similarly to the previous case it suffices to define a bijective mapping $\varphi : \mathbb{F}_2^3 \setminus \{0\} \to \mathbb{F}_2^3 \setminus \{0\}$ such that $x\varphi(x) = 1$ for every $x \neq 0$ and $x\varphi(y) + y\varphi(x) = 1$ for every $x \neq y$. It is easy to check that the following mapping satisfies these conditions: $\varphi(e_1) = e_1, \varphi(e_2) = e_1 + e_2, \varphi(e_3) = e_1 + e_2 + e_3, \varphi(e_1+e_2) = e_2+e_3, \varphi(e_1+e_3) = e_3, \varphi(e_2+e_3) = e_1+e_3, \varphi(e_1+e_2+e_3) = e_2$. Hence, $8 + 7 \cdot 4 = 36 \le r'_4(3)$.

Case 4: $n = 4$**.**

Let $\mathbb{F}_2^4 = \langle e_1, e_2, e_3, e_4\rangle$. Let us extend the mapping $\varphi : \langle e_1, e_2, e_3\rangle \to \langle e_1, e_2, e_3\rangle$ defined in Case 3 with $\varphi(0) = 0$. For every $x \in \langle e_1, e_2, e_3\rangle$ let

$$A(x) = A(x + e_4) = (\varphi(x) + e_4)^\perp.$$

Let $x, y \in \langle e_1, e_2, e_3\rangle$ and $\alpha, \beta \in \{0, 1\}$. We have to show that

$$(x + \alpha e_4) + (y + \beta e_4) \notin A(x + \alpha e_4) \cap A(y + \beta e_4)$$

unless $x = y$ and $\alpha = \beta$. If $(x + \alpha e_4) + (y + \beta e_4) \in A(x + \alpha e_4)$, then

$$(x + y + (\alpha + \beta)e_4)(\varphi(x) + e_4) = 0,$$

that is,

$$x\varphi(x) + y\varphi(x) + \alpha + \beta = 0.$$

Similarly, $(x + \alpha e_4) + (y + \beta e_4) \in A(y + \beta e_4)$ implies that

$$y\varphi(y) + x\varphi(y) + \alpha + \beta = 0.$$

If $x = y$, then $0 = x\varphi(x) + x\varphi(x) + \alpha + \beta$ yields $\alpha = \beta$, and we are done. From now on, let us assume that $x \neq y$.

If $x = 0$, then by adding up the two equations:

$$0 = 0\varphi(0) + y\varphi(0) + y\varphi(y) + 0\varphi(y) = y\varphi(y) = 1,$$

which is a contradiction. Similarly, $y = 0$ also leads to a contradiction.

Finally, let us assume that $x \neq y$ and $x, y \neq 0$. Then by adding up the two equations we get

$$0 = x\varphi(x) + y\varphi(y) + (x\varphi(y) + y\varphi(x)) = 1 + 1 + 1 = 1,$$

which is a contradiction, too.

Hence, the system satisfies property $(**)$, and $16 \cdot 8 \le r'_4(4)$.

□

5 Progression-free sets in $\mathbb{Z}_6^n$

First we give a subset reformulation for the problems of determining $r_k(\mathbb{Z}_6^n)$ (for $k = 3, 4, 5, 6$), similar to the reformulation we had in case of $\mathbb{Z}_4^n$ in Subsections 4.1 and 4.2.

5.1 Subset reformulation

We may express $\mathbb{Z}_6^n$ as $\mathbb{Z}_6^n = F \oplus R$, where

$$F = \{0, 2, 4\} \cong \mathbb{Z}_3^n \text{ and } R = \{0, 3\}^n \cong \mathbb{Z}_2^n.$$

A sequence

$$a_1 = f_1 + r_1, a_2 = f_2 + r_2, \ldots, a_k = f_k + r_k$$

(where $f_i \in F, r_i \in R$) forms an arithmetic progression in $\mathbb{Z}_6^n$ if and only if $f_1, f_2, \ldots, f_k$ is an arithmetic progression in $\mathbb{Z}_3^n$ and $r_1, r_2, \ldots, r_k$ is an arithmetic progression in $\mathbb{Z}_2^n$, respectively. Note that if the elements are distinct, then $k \leq 6$. If $k = 3$, then the progression consists of pairwise different elements if and only if f_1, f_2, f_3 are distinct. Since the sequence $r_1, r_2, \ldots$ is alternating, for $k \in \{4, 5, 6\}$ the necessary and sufficient conditions for getting k distinct elements is that f_1, f_2, f_3 are distinct and r_1, r_2 are distinct. Using this decomposition we may reformulate the property that "a subset $A \subseteq \mathbb{Z}_6^n$ avoids k-term arithmetic progressions" in terms of a property of systems of subsets of $\mathbb{Z}_3^n$. Namely, let $A(r) = \{f \in \mathbb{Z}_3^n : f + r \in A\}$ for $r \in R$ and let us define properties $(*)_3, (*)_4, (*)_5, (*)_6$ as follows:

The system of subsets $A(r)$ $(r \in \mathbb{Z}_2^n)$ satisfies

- property $(*)_3$, if $A(r') \cup A(r'')$ is 3AP-free for every pair $r', r'' \in \mathbb{Z}_2^n$,
- property $(*)_4$, if it is not possible to choose two different indices $r', r'' \in \mathbb{Z}_2^n$ and a 3AP a, b, c in $\mathbb{Z}_3^n$ such that $a, b \in A(r')$ and $a, c \in A(r'')$,
- property $(*)_5$, if it is not possible to choose two different indices $r', r'' \in \mathbb{Z}_2^n$ and a 3AP a, b, c in $\mathbb{Z}_3^n$ such that $a, b, c \in A(r')$ and $a, b \in A(r'')$,
- property $(*)_6$, if $A(r') \cap A(r'')$ is 3AP-free for every pair of distinct indices $r', r'' \in \mathbb{Z}_2^n$.

Note that in this reformulation $\mathbb{Z}_2^n$ serves only as an index set of size 2^n, its structure does not play any role.

Let us summarize in the following statement how the reformulation can be used to study the $r_k(\mathbb{Z}_6^n)$ values.

Proposition 5.1. *Let $k \in \{3, 4, 5, 6\}$. The maximum total size of a system of subsets $A(r) \subseteq \mathbb{Z}_3^n$ $(r \in \mathbb{Z}_2^n)$ satisfying property $(*)_k$ is $r_k(\mathbb{Z}_6^n)$.*

Proof. The statements immediately follow from the structural description of arithmetic progressions in $\mathbb{Z}_6^n$. □

Let us mention that the problem of determining the size of the largest 3AP-free subset of $\mathbb{Z}_6^n$ is equivalent with doing so in case of $\mathbb{Z}_3^n$:

Proposition 5.2. *For sets without arithmetic progression of length three the following holds:*

$$r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n).$$

Proof. If $A_0 \subseteq \mathbb{Z}_3^n$ is 3AP-free, then the system $A(x) = A_0$ $(x \in \mathbb{Z}_2^n)$ satisfies property $(*)_3$, thus $r_3(\mathbb{Z}_6^n) \geq 2^n r_3(\mathbb{Z}_3^n)$.

On the other hand, if $\sum_{x \in \mathbb{Z}_2^n} |A(x)| > 2^n r_3(\mathbb{Z}_3^n)$, then for some x we have $|A(x)| > r_3(\mathbb{Z}_3^n)$, thus $A(x)$ contains a 3AP, and $(*)_3$ fails to hold. Hence, $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$. □

In fact the argument only used that 6 has residue 2 modulo 4, and in general it yields the following statement:

Proposition 5.3. *If $m = 4M + 2$ for some integer M, then*

$$r_3(\mathbb{Z}_m^n) = 2^n r_3(\mathbb{Z}_{m/2}^n).$$

While studying $r_3(\mathbb{Z}_m^n)$ there are some technical differences between the cases when m is odd and when m is divisible by 4, but the case when m is an even number not divisible by 4 simply reduces to the odd case. We shall mention that for certain composite values of m there have been some improvements on the trivial corollaries of the prime case, like $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n)$. Namely, the method was adapted to odd prime powers [14, 96, 114] and also to the technically more difficult even case for $m = 2^3 = 8$. [97] (Cf. Section 2 for a discussion of these results.)

5.2 Proofs

Proof of Theorem 2.7.

Dimension 1. Clearly, $r_6(\mathbb{Z}_6^1) = 5$. Any 5-element subset of $\mathbb{Z}_6^1$ is trivially 6AP-free.

Dimension 2. Now, we show that $r_6(\mathbb{Z}_6^2) = 25$. Using the reformulation from Section 5.1 we are interested in the maximal possible total size of a system of four subsets of $\mathbb{Z}_3^2$ satisfying property $(*)_6$. That is, we would like to determine the maximum of $\sum_{i=1}^{4} |A_i|$, where $A_i \subseteq \mathbb{Z}_3^2$ $(1 \leq i \leq 4)$ such that no 3AP is contained in at least two of the subsets A_i. The total number of 3AP's in $\mathbb{Z}_3^2$ is $\frac{9 \cdot 8}{6} = 12$, thus the four subsets $A_1,\ A_2,\ A_3,\ A_4$ can contain at most twelve 3AP's in total. It is easy to determine the smallest possible number of 3AP's that must be contained

in a subset of a given size (by hand or by a computer search). Let us summarize the results in the table below:

size of A	0	1	2	3	4	5	6	7	8	9
min #3AP in A	0	0	0	0	0	1	2	5	8	12

Let x_i denote the number of i-element subsets among A_1, A_2, A_3, A_4 (where $0 \le i \le 9$). Since each 3AP can appear in at most one set A_i, the optimal value for $\sum_{i=1}^{4} |A_i|$ can not be more than the solution of the following integer program:

$$\begin{aligned}
&\max x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 \\
&\text{subject to} \\
&x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 4 \\
&x_5 + 2x_6 + 5x_7 + 8x_8 + 12x_9 \le 12 \\
&x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9 : \text{nonnegative integers}
\end{aligned}$$

(The first constraint ensures that four subsets are chosen, and the second constraint holds, since the total number of 3AP's contained in the four subsets can not be more than the total number of 3AP's in $\mathbb{Z}_3^2$.)

By solving the above integer program we obtain that the optimal value is 25 which is attained at $x_6 = 3, x_7 = 1$ (everything else is 0). That is, to achieve 25, one of the subsets must have size 7, and the three other subsets must have size 6.

By symmetry, we may assume that $A_1 = \mathbb{Z}_3^2 \setminus \{u, v\}$, where u and v are two different elements. Let $w = -u - v$ be the third point on the line uv. Let α denote the direction of the line uv. Note that in $\mathbb{Z}_3^2$ there are four possible directions, let us denote the other three directions by β, γ and δ.

Note that A_2, A_3, A_4 must have size 6 and each of them must contain exactly two 3AP's. In $\mathbb{Z}_3^2$ there are two types of 6-element sets: the complement of a 6-element set is either an affine line or not. To contain only two 3AP's the sets A_2, A_3, A_4 must all be the complements of affine lines, in other words, each of them is a union of two parallel lines. Moreover, these lines must not be parallel with the line uv, otherwise at least one of them would be contained in two subsets (in A_1 and here).

Also, none of these lines can go through w, as this would result in a 3AP contained both in A_1 and here.

Finally, a line from A_i and a line from A_j (where $2 \le i < j \le 4$) must not be parallel to each other because of similar reasons. That is, we may assume that A_2, A_3, A_4 are the unions of two-two lines of directions β, γ, δ, respectively.

Therefore, A_2, A_3, A_4 can be characterized as follows: A_2, A_3, A_4 are all the unions of two parallel lines, where the directions of the lines are β, γ, δ respectively, furthermore each line goes through u or v. (Thus $\{A_2, A_3, A_4\}$ is uniquely determined.)

The obtained system $\{A_1, A_2, A_3, A_4\}$ satisfies the conditions, since:

- A_1 contains two 3AP's with direction α and three more 3AP's that contain w.
- None of the 3AP's contained in A_2, A_3, A_4 have direction α and none of them contains w.
- The two-two lines contained in A_2, A_3, A_4 have directions β, γ, δ, respectively.

Hence, we proved that the largest 6AP-free set in $\mathbb{Z}_6^2$ has size 25 (and it is unique in the above described sense).

Dimension 3. Analogously to the previous case, with a quick computer check we found that the minimum number of 3AP's that must be contained in subsets of $\mathbb{Z}_3^3$ of given sizes are the numbers below. (Let m_j denote the minimum number of 3AP's that must be contained in a set of size j.)

size of A (j)	0	1	2	3	4	5	6	7	8	9	10
min #3AP in A (m_j)	0	0	0	0	0	0	0	0	0	0	2

size of A (j)	11	12	13	14	15	16	17	18	19
min #3AP in A (m_j)	3	4	7	10	13	16	20	24	33

size of A (j)	20	21	22	23	24	25	26	27
min #3AP in A (m_j)	42	51	60	70	80	92	104	117

Let x_i denote the number of i-element subsets among $A_1 - A_8$ (where $0 \le i \le 27$).

Since each 3AP can appear in at most one set A_i, the optimal value for $\sum_{i=1}^{8} |A_i|$ can not be more than the solution of the following integer program:

$$\begin{aligned}
&\max \sum_{i=1}^{27} i x_i \\
&\text{subject to} \\
&\sum_{i=0}^{27} x_i = 8 \\
&\sum_{i=0}^{27} m_i x_i \le 117 \\
&x_0, x_1, \ldots, x_{27} : \text{nonnegative integers}
\end{aligned}$$

With the help of an IP solver we obtained that the optimum is 124 yielding the bound

$$r_6(\mathbb{Z}_6^3) \le 124.$$

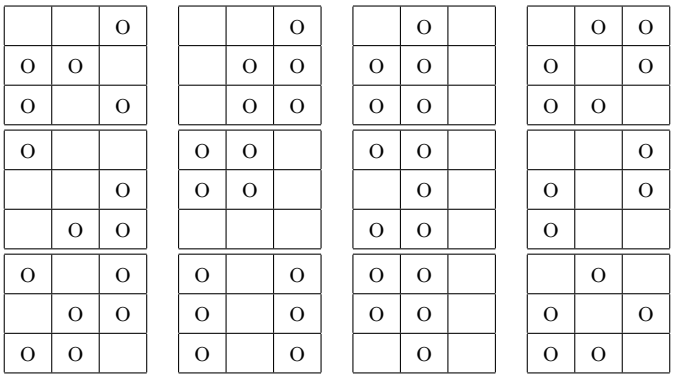


Table 2: Construction showing $r_6(\mathbb{Z}_6^3) \geq 117$

Turning to the lower bound, with computer help we found the a construction (see Table 2) where the total size of the eight subsets is 117.

Hence,

$$117 \leq r_6(\mathbb{Z}_6^3).$$

□

Proof of Theorem 2.8. The lower bound follows from Proposition 5.2 and from the best known lower bounds [87, 105] for $r_3(\mathbb{Z}_3^n)$.

To prove the upper bound it suffices to show that $\sum_{i \in I} |A_i| \leq 5.709^n$, if the system of subsets (of $\mathbb{Z}_3^n$) $\{A_i : i \in I\}$ satisfies property $(*)_6$ and $|I| = 2^n$.

We will use a supersaturation extension of the cap set result [99, Corollary 3.2]. (See also the arithmetic triangle removal lemma of Fox and Lovász [54].) This says that any subset of $\mathbb{Z}_3^n$ of density α has three-term arithmetic progression density at least α^C, where $C \approx 13.901$ is an explicit constant[3]. (Note that this

[3]Namely, $C = 1 + \frac{\log 3}{\log(3/\alpha)}$, where $\alpha = 3J(3) = 2.755\ldots$

includes counting trivial three-term arithmetic progressions.)

Let $\beta = 3/2^{1/C} \approx 2.854$, then we have $\beta^C = \frac{3^C}{2}$. The total size of subsets having size at most β^n is at most $2^n\beta^n$. Now, we consider the subsets with size larger than β^n. Let m_i denote the number of those subsets whose size lie in $(2^i\beta^n, 2^{i+1}\beta^n]$. Since each 3AP can occur in at most one set, we obtain that

$$m_i(2^i\beta^n/3^n)^C \le 1,$$

yielding that $m_i \le (3/\beta)^{Cn}2^{-iC}$. Therefore, the total size of subsets of size larger than β^n is at most

$$\sum_{i=0}^{\infty} m_i 2^{i+1}\beta^n \le \sum_{i=0}^{\infty}(3/\beta)^{Cn}2^{-iC}2^{i+1}\beta^n = (2\beta)^n\sum_{i=0}^{\infty}2^{1-(C-1)i} \le 2.001(2\beta)^n.$$

Hence, by adding up the obtained upper bounds for sets of size at most β^n and larger than β^n it is obtained that $\sum|A_i| \le 3.001(2\beta)^n$.

□

Proof of Theorem 2.10. It suffices to prove that

$$S := \sum_{i\in I}|A_i| \le 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)},$$

if the system of subsets (of $\mathbb{Z}_3^n$) $\{A_i : i \in I\}$ satisfies property $(*)_6$ and $|I| = 2^n$.

Let us enumerate the elements of $\mathbb{Z}_3^n$ by the positive integers from $[3^n]$. For $i \in I$ let v_i be the characteristic vector of A_i, that is, the jth entry of v_i is 1, if the element (from $\mathbb{Z}_3^n$) labeled by j is contained in A_i and 0 otherwise. Let $w := \sum_{i\in I} v_i$, denote the entries of w by $w_1, \dots, w_{3^n}$. Note that $w_1 + \cdots + w_{3^n} = \sum_{i\in I}|A_i| = S$.

By the Cauchy-Schwarz inequality

$$w^2 = w_1^2 + \cdots + w_{3^n}^2 \ge \frac{(w_1 + \cdots + w_{3^n})^2}{3^n} = \frac{S^2}{3^n}. \tag{13}$$

Since $A_i \cap A_j$ is 3AP-free for any two different indices $i, j \in I$ we have $v_i v_j \le r_3(\mathbb{Z}_3^n)$. Therefore,

$$w^2 = \sum_{i\in I} v_i^2 + \sum_{i,j\in I, i\ne j} v_i v_j \le S + 2^{2n}r_3(\mathbb{Z}_3^n). \tag{14}$$

By comparing (13) and (14) we obtain that $S^2 - 3^n S - 2^{2n}3^n r_3(\mathbb{Z}_3^n) \le 0$ which yields

$$S \le \frac{3^n + \sqrt{3^{2n} + 2^{2n+2}3^n r_3(\mathbb{Z}_3^n)}}{2} < 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}.$$

□

5.3 Remarks

In this section we proved that $r_6(\mathbb{Z}_6^n) \le 5.709^n$, which implies that $r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n when $6 \mid m$ and $k \in \{4,5,6\}$. Previously this was known only for the cases $3 = k \le m$, and according to our knowledge there is no pair of k, m with $3 \le k \le m$ such that $r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ is known to be true.

It would also be interesting to look for applications of our results and the underlying idea. An anonymous referee (of paper [94]) suggested a possible application to the multiplicative version of the problem. Namely, to achieve upper bounds of the shape $m/(\log m)^\varepsilon$ for the size of a subset $A \subseteq \mathbb{Z}_m$ avoiding 6-term *geometric* progressions for *typical* integers m. Let us sketch a possible argument. Let us assume that m has r distinct prime factors of residue 1 mod 3 and that $A \subseteq \mathbb{Z}_m$ does not contain any 6-term geometric progression. Note that for a *typical* m we have $r \approx 0.5 \log\log m$. Then the multiplicative group of units, $\mathbb{Z}_m^\times$, has a subgroup isomorphic to $(\mathbb{Z}_6^r, +)$. By applying the bound $r_6(\mathbb{Z}_6^r) \le 5.709^n$ in each of its cosets we get $|A \cap \mathbb{Z}_m^\times| \le (0.9515)^r \varphi(m)$, where $0.9515 = 5.709/6$ and $|\mathbb{Z}_m^\times| = \varphi(m)$. Similarly, among those elements $a \in \mathbb{Z}_m$ for which $\gcd(a,m) = d$ the set A can contain at most $\varphi(m/d)(0.9515)^{\omega'(m/d)}$, where $\omega'(m/d)$ is the number of distinct prime divisors of m/d having residue 1 mod 3. If $\omega'(m/d)$ is at least, say, $r/2$, then we have a saving of $(0.9515)^{r/2}$. Also, a calculation shows that for typical m the contribution to the sum $\sum_{d \mid m} \varphi(m/d)(0.9515)^{\omega'(m/d)}$ of those d for which $\omega'(m/d) \le r/2$ is negligible: as in these cases d is at least the product of the first $r/2$ primes. This argument yields a bound of shape $m/(\log m)^\varepsilon$ for *most* m. The resulting bound is weak if the number of prime factors (of residue 1 mod 3) of m is small. Let us consider an example. If p is a Sophie Germain prime, then to bound the maximum size of a 6-term geometric-progression-free subset of $\mathbb{Z}_{2p+1}$ one has to bound the maximum size of a subset of $\mathbb{Z}_{2p}$ avoiding 6-term arithmetic progressions, which is essentially the same as doing so in $\mathbb{Z}_p$.

Note that the case of 3-term geometric-progression-free subsets of $\mathbb{Z}_m$ was studied by McNew [82] who proved that their size is at most $\frac{m(\log\log m)^5}{\log m}$.

6 Proofs of results about line-free sets

In this section we prove our results giving bounds on the largest possible size of line-free sets.

6.1 Proofs of the upper bounds

Proof of Theorem 2.27. Let $A \subseteq \mathbb{F}_p^{n+1}$ be k-progression-free with $|A| = r_k(\mathbb{F}_p^{n+1})$. We count the number of the point pairs on every n-dimensional affine hyperplane

$$s = \left|\{(\{a,b\},S) \mid a,b \in A,\ a \neq b,\ a,b \in S,\ S \text{ is an } n\text{-dim affine hyperplane}\}\right|.$$

On every hyperplane, the number of points is at most $r_k(\mathbb{F}_p^n)$. Firstly, we assume $r_k(\mathbb{F}_p^{n+1}) \geq (p-1)r_k(\mathbb{F}_p^n)$, then the sum of number of point pairs for p parallel hyperplanes is maximal, if there are $p-1$ hyperplanes with $r_k(\mathbb{F}_p^n)$ points and one with $r_k(\mathbb{F}_p^{n+1}) - (p-1)r_k(\mathbb{F}_p^n)$.

There are $\frac{p^{n+1}-1}{p-1}$ disjoint sets of parallel hyperplanes, so

$$s \leq \left(\frac{p^{n+1}-1}{p-1}\right)\left((p-1)\binom{r_k(\mathbb{F}_p^n)}{2} + \binom{r_k(\mathbb{F}_p^{n+1}) - (p-1)r_k(\mathbb{F}_p^n)}{2}\right).$$

Note here that this inequality still holds, if $r_k(\mathbb{F}_p^{n+1}) < (p-1)r_k(\mathbb{F}_p^n)$, as in this case the number of point pairs is clearly less than

$$(p-1)\binom{r_k(\mathbb{F}_p^n)}{2}$$

and

$$\binom{r_k(\mathbb{F}_p^{n+1}) - (p-1)r_k(\mathbb{F}_p^n)}{2} \geq 0.$$

On the other hand, every point pair defines a line that is included in exactly $\frac{p^n-1}{p-1}$ n-dimensional affine hyperplanes, so

$$s = \frac{p^n-1}{p-1}\binom{r_k(\mathbb{F}_p^{n+1})}{2}.$$

We get the quadratic inequality

$$p^n\left(r_k(\mathbb{F}_p^{n+1})\right)^2 - \left(p^n + 2(p^{n+1}-1)r_k(\mathbb{F}_p^n)\right)r_k(\mathbb{F}_p^{n+1}) + (p^{n+2}-p)\left(r_k(\mathbb{F}_p^n)\right)^2 \geq 0$$

with roots

$$\frac{2(p^{n+1}-1)r_k(\mathbb{F}_p^n) + p^n \pm \sqrt{4(p^{n+1}-1)r_k(\mathbb{F}_p^n)(p^n - r_k(\mathbb{F}_p^n)) + p^{2n}}}{2p^n}.$$

As

$$r_k(\mathbb{F}_p^{n+1}) \leq p(r_k(\mathbb{F}_p^n)),$$

but

$$\frac{2(p^{n+1}-1)r_k(\mathbb{F}_p^n)+p^n+\sqrt{4(p^{n+1}-1)r_k(\mathbb{F}_p^n)(p^n-r_k(\mathbb{F}_p^n))+p^{2n}}}{2p^n}$$
$$> p(r_k(\mathbb{F}_p^n))+\frac{1}{2}-\frac{r_k(\mathbb{F}_p^n)}{p^n}+\frac{\sqrt{p^{2n}}}{2p^n} \geq p(r_k(\mathbb{F}_p^n))+\frac{1}{2}-1+\frac{1}{2}=p(r_k(\mathbb{F}_p^n)),$$

the theorem follows. □

Proof of Corollary 2.28. The first statement follows immediately from Theorem 2.27 using $r_p(\mathbb{F}_p^2)=(p-1)^2$. For the second statement we are using that

$$8p^6-20p^5+17p^4-12p^3+20p^2-16p+4$$

can be bounded by $(2\sqrt{2}p^3-5/\sqrt{2}p^2)^2$ from below for $p\geq 3$ and we get

$$\begin{aligned} r_p(\mathbb{F}_p^3) &\leq p^3-2p^2+p-\frac{1}{2}+\frac{2}{p}-\frac{1}{p^2}-\sqrt{2}p+\frac{5}{2\sqrt{2}} \\ &\leq p^3-2p^2-(\sqrt{2}-1)p-\frac{1}{2}+\frac{2}{3}+\frac{5}{2\sqrt{2}} \\ &\leq p^3-2p^2-(\sqrt{2}-1)p+2. \end{aligned}$$

□

Proof of Theorem 2.29. Assume that $S\subseteq\mathbb{F}_5^3$ is a 5-progression-free set of size 74. We will compute a weighted sum over all lines containing 4 points to reach a contradiction.

Let us call a line containing exactly r points an r-line. Let ℓ be a 4-line in S and let $H_1,H_2,\ldots,H_6$ be the planes containing ℓ. Then

$$\sum_{i=1}^{6}|H_i\cap S|=(74-4)+6\cdot 4=94.$$

Note that $r_5(\mathbb{F}_5^2)=16$ and $r_4(\mathbb{F}_5^2)=11$, which can be easily checked by computer search. Therefore, $|H_i\cap A|\geq 94-5\cdot 16=14$ for all i and there is no plane in $\mathbb{F}_5^3$ containing 12 or 13 points. Hence, there are five different distributions for the number of points in five parallel planes:

(a) $\{10,16,16,16,16\}$,

(b) $\{11,15,16,16,16\}$,

(c) $\{14,14,14,16,16\}$,

(d) $\{14,14,15,15,16\}$,

(e) $\{14, 15, 15, 15, 15\}$.

Denote by a, b, c, d, e the number of classes of parallel planes having these distributions. Note that

$$a + b + c + d + e = 31. \tag{15}$$

If we compare the number of pairs of points in each plane with the total number of pairs we get $(\binom{10}{2} + 4\binom{16}{2})a + (\binom{11}{2} + \binom{15}{2} + 3\binom{16}{2})b + (3\binom{14}{2} + 2\binom{16}{2})c + (2\binom{14}{2} + 2\binom{15}{2} + \binom{16}{2})d + (\binom{14}{2} + 4\binom{15}{2})e = 6\binom{74}{2}$

$$\Leftrightarrow 525a + 520b + 513c + 512d + 511e = 16206, \tag{16}$$

since each pair lies in exactly six planes.

Now denote by A, B, and C the number of pairs (ℓ, H) where H is a hyperplane containing 16, 15 and 14 points, respectively and $\ell \subseteq H$ is a 4-line. Again, let ℓ be a 4-line and let $H_1, H_2, \ldots, H_6$ be the planes containing ℓ. Then

$$\{|H_i \cap S| : i \in [1, 6]\} \in \{\{14, 16, 16, 16, 16, 16\}, \{15, 15, 16, 16, 16, 16\}\}$$

as multisets, therefore

$$A - 2B - 5C = 0. \tag{17}$$

To bound the size of A, B and C we need the following claims.

Claim 6.1. *Every plane containing* 16 *points contains at least twelve* 4*-lines.*

Proof of Claim 6.1. Consider a plane H containing 16 points and let x_i be the number of i-lines in H for $i \in \{1, 2, 3, 4\}$. By double counting the points in H we get

$$x_1 + 2x_2 + 3x_3 + 4x_4 = 6 \cdot 16 = 96$$

and by double counting the pairs of points in H we get

$$x_2 + 3x_3 + 6x_4 = \binom{16}{2} = 120.$$

By taking the difference of the two equations we get

$$-x_1 - x_2 + 2x_4 = 24,$$

implying that $2x_4 \geq 24$. ∎

Claim 6.2. *For $m \in \{14, 15\}$, every plane containing m points contains at most m 4-lines.*

Proof of Claim 6.2. As $5 \cdot 3 + 1 = 16 > m$, every point in S can be contained in at most four 4-lines and therefore the number of 4-lines in the plane is bounded from above by $\frac{4m}{4} = m$. ∎

Finally combining (15), (16) and (17) we obtain the following system of linear equations and inequalities.

$$\begin{aligned}
&a+b+c+d+e = 31\\
&525a+520b+513c+512d+511e = 16206\\
&A-2B-5C = 0\\
&A \geq 48a+36b+24c+12d\\
&B \leq 15b+30d+60e\\
&C \leq 42c+28d+14e\\
&a,b,c,d,e,A,B,C \geq 0,
\end{aligned}$$

which does not have any integral solution, which is a contradiction. Hence, $|S| \neq 74$.

□

Proof of Theorem 2.30. Assume that $S \subseteq \mathbb{F}_7^3$ is a 7-progression-free set of size 243. Note that we have the following bounds.

Claim 6.3. *Every plane containing* 36 *points contains at least* 18 6*-lines and every plane containing* 35*,* 34 *or* 33 *points contains at most* 33*,* 30*,* 28 6*-lines, respectively. Moreover,* $r_7(\mathbb{F}_7^2) = 36$ *and* $r_6(\mathbb{F}_7^2) = 29$*.*

Proof of Claim 6.3. Consider a plane H containing m points and let x_i be the number of i-lines in H for $i \in [0,6]$. There are 56 lines in the plane, thus

$$x_0+x_1+x_2+x_3+x_4+x_5+x_6 = 56. \tag{18}$$

By double counting the points in H we get

$$x_1+2x_2+3x_3+4x_4+5x_5+6x_6 = 8m, \tag{19}$$

and by double counting the pairs of points in H we get

$$x_2+3x_3+6x_4+10x_5+15x_6 = \binom{m}{2}. \tag{20}$$

If $m = 36$ we take the difference of (20) and two times (19) and get

$$-2x_1-3x_2-3x_3-2x_4+3x_6 = 54,$$

implying that $x_6 \geq 18$. If $m \in \{33,34,35\}$, then by taking three times (18) minus two times (19) plus (20) we get

$$3x_0+x_1+x_4+3x_5+6x_6 = 168-16m+\binom{m}{2},$$

hence, $6x_6 \leq 168-16m+\binom{m}{2}$ which gives the desired bounds.

The last two claims can be easily checked by computer search. ■

If we now proceed analogously to the proof of Theorem 2.29, we again arrive at a contradiction. □

6.2 Proofs of the lower bounds

Proof of Theorem 2.31. We consider three different types of 2-dimensional layers:

- $A \coloneqq [0, p-2]^2$,
- $B \coloneqq [0,p-1]^2 \setminus \{(i,i) \mid i \in [0,p-1]\} \setminus \big(\{p-1\} \times [0, \frac{p-3}{2}]\big) \setminus \big([0, \frac{p-3}{2}] \times \{p-1\}\big)$,
- $C \coloneqq \{(i,i) \mid i \in [0, \frac{p-3}{2}]\}$,

and three disjoint subsets of $\mathbb{F}_p^{n-2}$:

- $\mathcal{A} \coloneqq [0, p-3]^{n-2}$,
- $\mathcal{B} \coloneqq [0, p-2]^{n-2} \setminus [0, p-3]^{n-2}$,
- $\mathcal{C} \coloneqq \bigcup_{j \in [1,n-2]} \{x \in \mathbb{F}_p^{n-2} \mid (x_j = p-1) \wedge (x_i \in [0, p-3] \ \forall i \neq j)\}$.

We show that $S \coloneqq (\mathcal{A} \times A) \cup (\mathcal{B} \times B) \cup (\mathcal{C} \times C)$ is p-progression-free.

First consider the case $n = 3$. Let

$$L \coloneqq \{(a_1, a_2, a_3) + (b_1, b_2, b_3)i \mid i \in [0, p-1]\}$$

be a p-progression in $\mathbb{F}_p^3$ with $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_p$.

- Case 1: $b_1 = 0$ and $a_1 \neq p-2$:

  $[0, p-2]^2$ is p-progression-free and $|\{(i,i) \mid i \in [0, \frac{p-3}{2}]\}| < p$, therefore L is not contained in S.

- Case 2: $b_1 = 0$ and $a_1 = p-2$:

  $L' \coloneqq \{(a_2, a_3) + (b_2, b_3)i \mid i \in [0, p-1]\}$ and $\{(i,i) \mid i \in [0, p-1]\}$ are both lines in $\mathbb{F}_p^2$. If they are not parallel or they are equal, they do intersect, and L is not contained in S. Otherwise we can rewrite $L' = \{(i, c+i) \mid i \in [0, p-1]\}$ with $c \in [1, p-1]$.

  If $c \in [1, \frac{p-1}{2}]$, then $c + (p-1) \in [0, \frac{p-3}{2}]$ (choose $i = p-1$) and

  $$(p-2, p-1, c + (p-1)) \in L \setminus S.$$

  Similarly, if $c \in [\frac{p+1}{2}, p-1]$, then $p-1-c \in [0, \frac{p-3}{2}]$ (choose $i = p-1-c$) and

  $$(p-2, p-1-c, p-1) \in L \setminus S.$$

  Therefore, L is not contained in S.

- Case 3: $b_1 \neq 0$:

  Without the loss of generality let $b_1 = 1$ and $a_1 = p-2$. If $b_2 = b_3 = 0$, then L is not contained in S because the $(p-2)$-layer and $(p-1)$-layer of S have no common point. Otherwise, without the loss of generality, let $b_2 \neq 0$ and therefore $\{a_2 + b_2 i \mid i \in [0, p-1]\} = [0, p-1]$. Assume that $L \subseteq S$. Then $a_2 = p-1$ and $a_3 \in [\frac{p-1}{2}, p-2]$ because the $(p-2)$-layer is the only layer containing points with the coordinate $p-1$. Since the $(p-1)$-layer does not have coordinates in $[\frac{p-1}{2}, p-2]$, also $b_3 \neq 0$, and consequently

  $$\{a_3 + b_3 i \mid i \in [0, p-1]\} = [0, p-1].$$

  As before, it follows that $a_3 = p-1$ contradicting that $L \subseteq S$. Thus, L is not contained in S and S is p-progression-free.

Now, consider $n > 3$. We have already seen that every layer is p-progression-free, so we only consider progressions $L := \{a+bi \mid i \in [0, p-1]\}$ visiting p non-empty layers. Let m be the number of non-zero entries in the first $n-2$ coordinates of b. Since only layers of type C are placed where one of the first $n-2$ coordinates is $p-1$, and all layers where two of the first $n-2$ coordinates are $p-1$ are empty, m is also the number of type C layers visited by L and $m \leq p$.

- If $m = 1$, L is not contained in S, analogously to the 3-dimensional case.
- If $m \geq 2$ the last two coordinates of every point in L are equal, since the projection of L in the last two coordinates is a line containing two points on the main diagonal, or it is a single point on the main diagonal. Now since only layers of type B are placed where one of the first $n-2$ coordinates is $p-2$, L also visits a layer of type B. Therefore, L is not contained in B because layers of type B contain no points on the main diagonal.

Finally, note that layers of type A and B contain $(p-1)^2$ points, and layers of type C contain $(p-1)/2$ points, thus

$$|S| = (p-1)^2(p-1)^{n-2} + \frac{p-1}{2}(n-2)(p-2)^{n-3} = (p-1)^n + \frac{n-2}{2}(p-1)(p-2)^{n-3}.$$

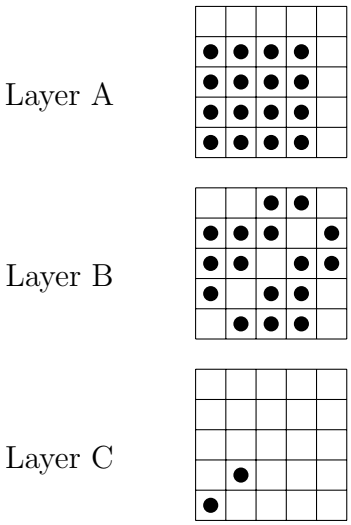
□

Proof of Theorem 2.25. Let $k = \lfloor \sqrt{p} \rfloor$, $t = \lfloor p/k \rfloor$, $K := [0, k-1]$ and $T := \{jk-1 \mid j \in [1, t]\}$. Consider the set

$$\begin{aligned} S :=& [0, p-3] \times [0, p-2]^2 \\ &\cup \{p-2\} \times ([0, p-1]^2 \setminus \{(j, j) \mid j \in [0, p-1]\} \setminus ((K \cup \{p-1\}) \times (T \cup \{p-1\}))) \\ &\cup \{p-1\} \times K \times T. \end{aligned}$$

We will show that $S \subseteq \mathbb{F}_p^3$ is p-progression-free.

Let $L := \{(a_1, a_2, a_3) + (b_1, b_2, b_3)i \mid i \in [0, p-1]\}$ be a p-progression in $\mathbb{F}_p^3$ with $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}_p$.



C	C	C		
B	B	B	B	
A	A	A	B	C
A	A	A	B	C
A	A	A	B	C

Figure 2: A description of the line-free set in Theorem 2.31 for $p = 5$ and $n = 4$.

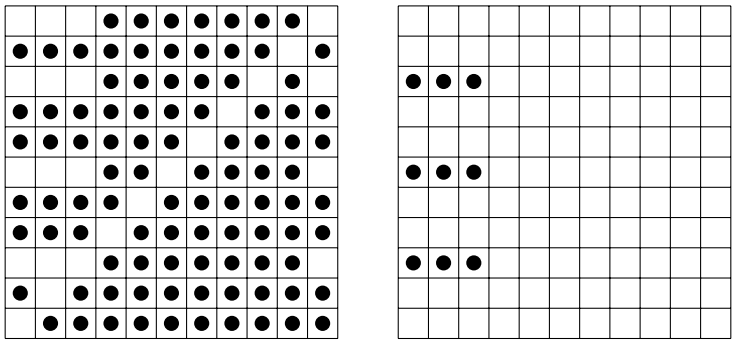


Figure 3: The last two layers of the line-free set in Theorem 2.25 for $p = 11$.

- Case 1: $b_1 = 0$ and $a_1 \neq p-2$:

  $[0, p-2]^2$ is p-progression-free and $|K \times T| = kt < p$, therefore L is not contained in S.

- Case 2: $b_1 = 0$ and $a_1 = p-2$:

  $L' := \{(a_2, a_3) + (b_2, b_3)i \mid i \in [0, p-1]\}$ and $\{(i, i) \mid i \in [0, p-1]\}$ are both lines in $\mathbb{F}_p^2$. If they are not parallel or they are equal, then they do intersect, and L is not contained in S. Otherwise, we can rewrite $L' = \{(i, c+i) \mid i \in [0, p-1]\}$ with $c \in [1, p-1]$. Observe that $\{(i, c+i) \mid i \in [0, k-1]\} \cap (K \times (T \cup \{p-1\})) \neq \varnothing$, and therefore L is not contained in S.

- Case 3: $b_1 \neq 0$:

  Without the loss of generality, let $b_1 = 1$ and $a_1 = p-2$. If $b_2 = b_3 = 0$, then L is not contained in S because the $(p-2)$-layer and $(p-1)$-layer of S have no common point. Else, if $b_2 \neq 0$ and $b_3 \neq 0$, then

  $$\{a_2 + b_2 i \mid i \in [0, p-1]\} = \{a_3 + b_3 j \mid j \in [0, p-1]\} = [0, p-1].$$

  Since the $(p-2)$-layer is the only layer with $p-1$ entries but

  $$(p-2, p-1, p-1) \notin S,$$

  L is not contained in S. Finally, if either $b_2 = 0$ or $b_3 = 0$ but not both, one of the last two coordinates is constant, and the other one attains every possible value. Now again the $(p-2)$-layer is the only layer with $p-1$ entries but the $(p-1)$-layer has empty rows and columns wherever the $(p-2)$-layer has $p-1$ entries, therefore, L is not contained in S.

Note that since p is a prime, $k \geq 2$, $t \leq \frac{p-1}{k}$, from the definition of k it follows that

$$\begin{aligned} & k \in [\sqrt{p} - 1, \sqrt{p} + 1] \\ \Leftrightarrow\ & k^2 - 2\sqrt{p}k + p - 1 \leq 0 \\ \Leftrightarrow\ & k + \frac{p-1}{k} \leq 2\sqrt{p}. \end{aligned}$$

and therefore $k + t \leq 2\sqrt{p}$. Hence,

$$\begin{aligned} |S| =& (p-2)(p-1)^2 + (p^2 - p - (kt-1) - k - t) + kt \\ =& (p-2)(p-1)^2 + p^2 - p + 1 - k - t \\ \geq& (p-2)(p-1)^2 + p^2 - p + 1 - 2\sqrt{p} \\ =& (p-1)^3 + p - 2\sqrt{p} \end{aligned}$$

□

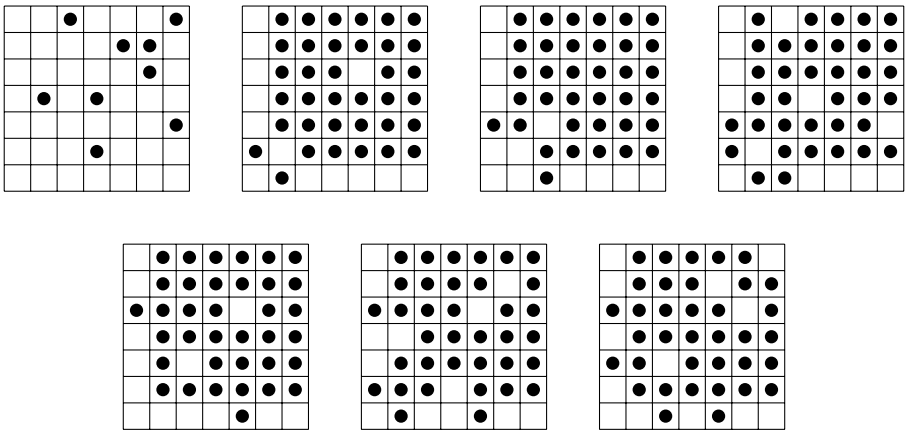


Figure 4: The line-free set in Theorem 2.26 for $p = 7$.

Proof of Theorem 2.26. Let $p = 7 + 24\ell$ for $\ell \in \mathbb{Z}_{\geq 0}$, let A be the set of quadratic residues, that is, $A = \{a^2 \mid a \in \mathbb{F}_p^\times\}$ and $B \coloneqq \mathbb{F}_p^\times \setminus A$. Note that $|A| = |B| = \frac{p-1}{2}$ and the law of quadratic reciprocity yields

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{3+12\ell} = -1,$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{6+42\ell+72\ell^2} = 1,$$

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{3+12\ell}\left(\frac{1}{3}\right) = -1,$$

and therefore $2 \in A$ and $\{-1, 3\} \subseteq B$. Note here that A is a subgroup of $\mathbb{F}_p^\times$ and this means that multiplication by 2 or $\frac{1}{2}$ leaves elements of A or B in the same set, while multiplication by -1, 3 or $\frac{1}{3}$ changes the set. For instance, $3a \in B$ for all $a \in A$ and

$$-\frac{3b}{2} = (-1) \cdot 3 \cdot \frac{1}{2} \cdot b \in B$$

for all $b \in B$. Let

$$\begin{aligned}
S \coloneqq & [1, p-1]^3 \cup \big(\{(a,0,a) | a \in A\} \cup \{(0,a,a) | a \in A\}\big) \\
& \setminus \big(\{(a,a,a) | a \in A\} \cup \{(a/2, a/2, a) | a \in A\}\big) \\
& \cup \big(\{(3b/2, 0, b) | b \in B\} \cup \{(0, 3b/2, b) | b \in B\} \cup (3b, 0, b) | b \in B\} \cup \{(0, 3b, b) | b \in B\}\big) \\
& \setminus \big(\{(b,b,b) | b \in B\} \cup \{(3b/2, 3b/2, b) | b \in B\} \cup \{(b/3, b/3, b) | b \in B\}\big) \\
& \setminus \big(\{(3b, -3b/2, b) | b \in B\} \cup \{(-3b/2, 3b, b) | b \in B\}\big) \\
& \cup \big(\{(b,b,0) | b \in B\} \cup \{(2a, -a, 0) | a \in A\} \cup (-a, 2a, 0) | a \in A\}\big).
\end{aligned}$$

We will show that S is p-progression-free.

Note that S is symmetric in the first two coordinates. We will therefore, in this proof, skip one of the two symmetric cases, whenever possible.

Let $L \coloneqq \{(c_1, c_2, c_3) + (d_1, d_2, d_3)i \mid i \in [0, p-1]\}$ be a p-progression in $\mathbb{F}_p^3$ with $c_1, c_2, c_3, d_1, d_2, d_3 \in \mathbb{F}_p$, and assume that $L \subseteq S$.

First, assume that $d_3 = 0$.

- Case 1: $c_3 = 0$:

  Since S contains no points where the third and one of the first two coordinates is 0, L is not contained in S.

- Case 2: $c_3 \in A$:

  Let $a \coloneqq c_3$. Since $(a, 0, a)$ and $(0, a, a)$ are the only points where the third coordinate is a and one of the first two coordinates is 0, we can assume $(a, 0, a) \in L$. If $d_1 = 0$, then $(a, a, a) \in L$, a contradiction. If $d_1 \neq 0$, then also $(0, a, a) \in L$ and consequently

  $$\left(\frac{a}{2}, \frac{a}{2}, a\right) = \frac{1}{2}(a, 0, a) + \frac{1}{2}(0, a, a) \in L,$$

  again a contradiction.

- Case 3: $c_3 \in B$:

  Let $b \coloneqq c_3$. First, assume $d_1 \neq 0$ and $d_2 \neq 0$. Since $(\frac{3b}{2}, 0, b)$, $(0, \frac{3b}{2}, b)$, $(3b, 0, b)$ and $(0, 3b, b)$ are the only points where the third coordinate is b and one of the first two coordinates is 0, we only have to consider the following cases:

  If $(\frac{3b}{2}, 0, b) \in L$ and $(0, \frac{3b}{2}, b) \in L$, then also

  $$\left(-\frac{3b}{2}, 3b, b\right) = (-1)\left(\frac{3b}{2}, 0, b\right) + 2\left(0, \frac{3b}{2}, b\right) \in L,$$

  if $(\frac{3b}{2}, 0, b) \in L$ and $(0, 3b, b) \in L$, then also

  $$(b, b, b) = \frac{2}{3}\left(\frac{3b}{2}, 0, b\right) + \frac{1}{3}(0, 3b, b) \in L,$$

  and if $(3b, 0, b) \in L$ and $(0, 3b, b) \in L$, then also

  $$\left(\frac{3b}{2}, \frac{3b}{2}, b\right) = \frac{1}{2}(3b, 0, b) + \frac{1}{2}(0, 3b, b) \in L.$$

  Consequently, we arrived at a contradiction. Now, if $d_1 = 0$ or $d_2 = 0$, again L has to contain one of the points

  $$\left(\frac{3b}{2}, 0, b\right),\ \left(0, \frac{3b}{2}, b\right),\ (3b, 0, b),\ (0, 3b, b),$$

and therefore L also contains one of the points

$$\left(\frac{3b}{2}, \frac{3b}{2}, b\right),\ \left(3b, \frac{-3b}{2}, b\right),\ \left(\frac{-3b}{2}, 3b, b\right),$$

again a contradiction.

Now assume that $d_3 \neq 0$. If $d_1 = d_2 = 0$, L contains a point with a zero last coordinate. We get that either $(b, b, 0)$, thus also (b, b, b) is in L for some $b \in B$ or $(2a, -a, 0) \in L$ for some $a \in A$ and therefore also $(3b, \frac{-3b}{2}, b) \in L$ for the unique $b \in B$ such that $3b = 2a$, both a contradiction.

In the remaining case $d_3 \neq 0$ and at least one of d_1 and d_2 is non-zero. Since there is no point in S where both the third and one of first two coordinates is zero, L has to include a point with third coordinate being zero and a different point where one of the other two coordinates is zero. We are therefore left with checking the following cases, where L is given by a pair of two points in S. For some of these cases it is important to note that S contains no points where one of the first two coordinates is 0 and the other is in B.

- $(b, b, 0) \in L$ and $(0, a, a) \in L$:

$$L = \left\{ \begin{pmatrix} b \\ b \\ 0 \end{pmatrix} + k \begin{pmatrix} -b \\ a - b \\ a \end{pmatrix} \middle|\ k \in \mathbb{F}_p \right\}.$$

  Since $a \neq b$, setting $k := \frac{b}{b-a}$, we get

$$(x, y, z) := \left(-\frac{ab}{b-a}, 0, \frac{ab}{b-a}\right) \in L.$$

  Now $x = -z$, so $z \in B$ and $x \in A$, so $-1 = \frac{3}{2}$ or $-1 = 3$, a contradiction.

- $(b, b, 0) \in L$ and $(0, \frac{3b'}{2}, b') \in L$:

$$L = \left\{ \begin{pmatrix} b \\ b \\ 0 \end{pmatrix} + k \begin{pmatrix} -b \\ \frac{3b'}{2} - b \\ b' \end{pmatrix} \middle|\ k \in \mathbb{F}_p \right\}.$$

  Since $\frac{3b'}{2} \neq b$, setting $k := \frac{b}{b - \frac{3b'}{2}}$, we get

$$(x, y, z) := \left(-\frac{3bb'}{2(b - \frac{3b'}{2})}, 0, \frac{bb'}{b - \frac{3b'}{2}}\right) \in L.$$

  Now $x = -\frac{3}{2}z$, thus $x, z \in A$, so $-\frac{3}{2} = 1$, a contradiction.

- $(b, b, 0) \in L$ and $(0, 3b', b') \in L$:

$$L = \left\{ \begin{pmatrix} b \\ b \\ 0 \end{pmatrix} + k \begin{pmatrix} -b \\ 3b' - b \\ b' \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}.$$

  Since $3b' \neq b$, setting $k := \frac{b}{b-3b'}$, we get

$$(x, y, z) := \left(-\frac{3bb'}{b-3b'}, 0, \frac{bb'}{b-3b'} \right) \in L.$$

  Now $x = -3z$, thus $x, z \in A$, so $-3 = 1$, a contradiction.

- $(2a, -a, 0) \in L$ and $(0, a', a') \in L$:

$$L = \left\{ \begin{pmatrix} 2a \\ -a \\ 0 \end{pmatrix} + k \begin{pmatrix} -2a \\ a' + a \\ a' \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}.$$

  Since $a' \neq -a$, setting $k := \frac{a}{a+a'}$, we get

$$(x, y, z) := \left(\frac{2aa'}{a+a'}, 0, \frac{aa'}{a+a'} \right) \in L.$$

  Now $x = 2z$, thus $x, z \in A$, so $2 = 1$, a contradiction.

- $(2a, -a, 0) \in L$ and $(a', 0, a') \in L$:

$$L = \left\{ \begin{pmatrix} 2a \\ -a \\ 0 \end{pmatrix} + k \begin{pmatrix} a' - 2a \\ a \\ a' \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}.$$

  Assume $a' \neq 2a$, then setting $k := \frac{2a}{2a-a'}$, we get

$$(x, y, z) := \left(0, \frac{aa'}{2a-a'}, \frac{2aa'}{2a-a'} \right) \in L.$$

  Now $2y = z$, thus $y, z \in A$, so $1 = 2$, a contradiction.

  If $a' = 2a$, then setting $k := 3$, we get $(x, y, z) := (2a, 2a, 6a) \in L$, a contradiction since $6a \in B$.

- $(2a, -a, 0) \in L$ and $(\frac{3b}{2}, 0, b) \in L$:

$$L = \left\{ \begin{pmatrix} 2a \\ -a \\ 0 \end{pmatrix} + k \begin{pmatrix} \frac{3b}{2} - 2a \\ a \\ b \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}.$$

Assume $\frac{3b}{2} \neq 2a$, then setting $k := \frac{2a}{2a-\frac{3b}{2}}$, we get

$$(x,y,z) := \left(0, \frac{3ab}{2(2a-\frac{3b}{2})}, \frac{2ab}{2a-\frac{3b}{2}}\right) \in L.$$

Now $y = \frac{3z}{4}$, thus $z \in B$ and $x \in A$, so $\frac{3}{4} = \frac{3}{2}$ or $\frac{3}{4} = 3$, a contradiction.

If $\frac{3b}{2} = 2a$, then setting $k := 3$, we get $(x,y,z) := (2a, 2a, 4a) \in L$, a contradiction since $4a \in A$.

- $(2a, -a, 0) \in L$ and $(0, \frac{3b}{2}, b) \in L$:

$$L = \left\{ \begin{pmatrix} 2a \\ -a \\ 0 \end{pmatrix} + k \begin{pmatrix} -2a \\ \frac{3b}{2} + a \\ b \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}.$$

Assume $\frac{3b}{2} \neq -3a$, then setting $k := \frac{3a}{\frac{3b}{2}+3a}$, we get

$$(x,y,z) := \left(\frac{3ab}{\frac{3b}{2}+3a}, \frac{3ab}{\frac{3b}{2}+3a}, \frac{3ab}{\frac{3b}{2}+3a}\right) \in L.$$

Now $x = y = z$, a contradiction. If $\frac{3b}{2} = -3a$, then setting $k := -\frac{1}{2}$, we get $(x,y,z) := (3a, 0, a) \in L$, so $1 = 3$, a contradiction.

- $(2a, -a, 0) \in L$ and $(3b, 0, b) \in L$:

$$L = \left\{ \begin{pmatrix} 2a \\ -a \\ 0 \end{pmatrix} + k \begin{pmatrix} 3b-2a \\ a \\ b \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}.$$

Since $b \neq a$, then setting $k := \frac{a}{a-b}$, we get

$$(x,y,z) := \left(\frac{ab}{a-b}, \frac{ab}{a-b}, \frac{ab}{a-b}\right) \in L.$$

Now $x = y = z$, a contradiction.

- $(2a, -a, 0) \in L$ and $(0, 3b, b) \in L$:

$$L = \left\{ \begin{pmatrix} 2a \\ -a \\ 0 \end{pmatrix} + k \begin{pmatrix} -2a \\ a+3b \\ b \end{pmatrix} \middle| \; k \in \mathbb{F}_p \right\}$$

since $3b \neq -a$, setting $k := \frac{a}{a+3b}$, we get

$$(x,y,z) := \left(\frac{6ab}{a+3b}, 0, \frac{ab}{a+3b}\right) \in L.$$

Now $x = 6z$, thus $z \in B$ and $x \in A$, so $6 = \frac{3}{2}$ or $6 = 3$, a contradiction.

Finally, note that the layer with third coordinate 0 contains

$$|B| + 2|A| = \frac{3}{2}(p-1)$$

points, layers with the third coordinate in A contain $(p-1)^2$ points, and layers with the third coordinate in B contain $(p-1)^2 - 1$ points, thus

$$|S| = \frac{p-1}{2}(p-1)^2 + \frac{p-1}{2}((p-1)^2 - 1) + \frac{3}{2}(p-1) = (p-1)^3 + (p-1).$$

In the special case of $p = 7$, the layers with third coordinate in B actually contain $(p-1)^2 = 36$ points, since $\frac{3}{2} = \frac{1}{3}$, thus giving the lower bound of 225.

□

7 Applications of the Slice rank method

In this section first we present the so-called *slice rank method*. This is the symmetrized version given by Tao of the polynomial method developed by Croot, Lev and the author [31] to show that 3AP-free sets in $\mathbb{Z}_4^n$ are exponentially small which was subsequently adapted by Ellenberg and Gijswijt [41] to the case of $\mathbb{F}_3^n$. For an exposition of the slice rank method we refer to [119, 112]. Here, let us briefly summarize the technique.

7.1 Slice rank method

For finite sets $A_1, \dots, A_k$ and a field $\mathbb{F}$ we say that

$$h : A_1 \times \cdots \times A_k \to \mathbb{F}$$

has slice-rank 1 and called a *slice*, if

$$h(x_1, \dots, x_k) = f(x_i)g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_k)$$

for some $1 \le i \le k$. The slice rank of $F : A_1 \times \cdots \times A_k \to \mathbb{F}$, denoted slice-rank$(F)$, is the smallest r such that $F = \sum_{i=1}^{r} h_i$, where the functions h_i are slices. Note that for $k = 2$ the slice rank coincides with the usual matrix rank.

The following lemma from [119] will be applied several times:

Lemma 7.1. *Let A be a finite set and let $F : \underbrace{A \times \cdots \times A}_{k} \to \mathbb{F}$ be a diagonal tensor attaining only nonzero entries on its diagonal, that is,*

$$F(x_1, \dots, x_k) = \sum_{a \in A} c_a \delta_a(x_1) \dots \delta_a(x_k),$$

where $c_a \neq 0$ $(a \in A)$ and $\delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$.

Then

$$\text{slice-rank}(F) = |A|.$$

In the applications for bounding the size of a set A satisfying certain criteria, a diagonal tensor F is going to be presented, then it will suffice to bound the slice-rank of F.

For bounding the slice-rank the tensor F is going to be represented as a multivariate polynomial, and in certain cases we will have to calculate with the dimension of certain subspaces of polynomials. Namely, we will use multiple times that the number of monomials in $\mathbb{F}[x_1, \dots, x_n]$ with total degree at most d is $\binom{n+d}{d}$. Indeed, the number of n-variable monomials with total degree exactly i is $\binom{n+i-1}{i}$, and $\sum_{i=0}^{d} \binom{n+i-1}{i} = \binom{n+d}{d}$.

For a prime power q let $f_q(n,d)$ denote the number of those monomials in n variables whose total degree is at most d and each individual degree is at most $q-1$, that is:

$$f_q(n,d) = |\{(i_1,\dots,i_n) \in \{0,1,\dots,q-1\}^n : i_1+\dots+i_n \le d\}|.$$

As an illustration of the technique we briefly outline the proof of the cap set bound in Tao's slice rank formulation and the bound of Naslund and Sawin [88] for 3-sunflower-free sets.

The proof is essentially the same for $q=3$ and for other odd prime powers, so we present it in the general case. Let q be an odd prime power and assume that $A \subseteq \mathbb{F}_q^n$ is 3AP-free. Let $F : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be the function

$$F(x,y,z) = \delta_{x-2y+z=0} = \prod_{i=1}^{n}(1-(x_i-2y_i+z_i)^{q-1}),$$

that is, $F(x,y,z)=1$ if and only if x,y,z (in this order) form a 3AP, otherwise $F(x,y,z)=0$. According to Lemma 7.1 we have $|A| = \text{slice-rank}(F\big|_{A\times A\times A})$, since A is 3AP-free, but $F(a,a,a)=1$ for every $a \in A$. Clearly,

$$\text{slice-rank}(F\big|_{A\times A\times A}) \le \text{slice-rank}\, F,$$

so it suffices to bound the slice rank of F. Observe that

$$F(x,y,z) = \prod_{i=1}^{n}(1-(x_i-2y_i+z_i)^{q-1})$$

is a polynomial in $x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n$ of degree $(q-1)n$. Consequently, in each monomial

$$x_1^{\alpha_1}\dots x_n^{\alpha_n}y_1^{\beta_1}\dots y_n^{\beta_n}z_1^{\gamma_1}\dots z_n^{\gamma_n}$$

we have

$$\min(\alpha_1+\dots+\alpha_n, \beta_1+\dots+\beta_n, \gamma_1+\dots+\gamma_n) \le (q-1)n/3).$$

For each n-tuple $(\alpha_1,\dots,\alpha_n)$ satisfying $0 \le \alpha_i \le q-1$ and $\alpha_1+\dots+\alpha_n \le (q-1)n/3$ we can group the monomials of the form $x_1^{\alpha_1}\dots x_n^{\alpha_n}y_1^{\beta_1}\dots y_n^{\beta_n}z_1^{\gamma_1}\dots z_n^{\gamma_n}$ obtaining a slice of the form $x_1^{\alpha_1}\dots x_n^{\alpha_n}g(y,z)$.
After this, we do so for the remaining terms with $y_1^{\beta_1}\dots y_n^{\beta_n}$ (satisfying $\beta_1+\dots+\beta_n \le (q-1)n/3$) and finally, also with $z_1^{\gamma_1}\dots z_n^{\gamma_n}$ (satisfying $\gamma_1+\dots+\gamma_n \le (q-1)n/3$). This yields a slice rank decomposition with at most $3f_q(n,(q-1)n/3)$ slices. Therefore, $|A| \le 3f_q(n,(q-1)n/3)$. Numerically, this implies the bound $r_3(\mathbb{F}_q^n) \le (J(q)q)^n$ with $J(q) = \frac{1}{q}\min_{0<t<1}\frac{1-t^q}{(1-t)\,t^{(q-1)/3}} < 1$.

Let us continue with showing how the technique applies to the so-called Erdős-Szemerédi sunflower problem. A family $\mathcal{F}$ of subsets is called a k-sunflower, if it is not possible to choose distinct $A_1,A_2,\dots,A_k \in \mathcal{F}$ such that all the pairwise

intersections $A_i \cap A_j$ coincide. Erdős and Szemerédi conjectured that for $k \geq 3$ the largest k-sunflower-free family of subsets of $[n]$ has size at most $(2 - c_k)^n$ with some positive c_k. Here we discuss the case $k = 3$. Alon, Shpilka and Umans [5] showed that an exponential saving for $r_3(\mathbb{F}_3^n)$ also yields an exponential saving for the size a 3-sunflower-free family of subsets of $[n]$. Quantitatively, the bound $r_3(\mathbb{F}_3^n) \leq c^n$ yields the constant $\sqrt{1+c}$, thus the cap set bound provides the constant $\sqrt{1+2.756} \approx 1.938$. However, Naslund and Sawin – in fact only a few hours after Terry Tao's blog post on the slice rank method – gave a better bound using the technique itself, not just the cap set bound as a black box. Here we briefly present their proof.

Let $\mathcal{F}$ be a 3-sunflower-free family of subsets of $[n]$. Let us consider their characteristic vectors. That is, to each $F \in \mathcal{F}$ we assign a vector $v_F \in \mathbb{R}^n$ such that $v_i = 1$, if $i \in F$ and $v_i = 0$ otherwise. Let $S \subseteq \{0,1\}^n$ be the set of characteristic vectors assigned to elements of $\mathcal{F}$, note that $|S| = |\mathcal{F}|$. The condition that $\mathcal{F}$ is 3-sunflower-free implies that for distinct $x, y, z \in S$ we have at least one coordinate such that $x_i + y_i + z_i = 2$, since having $x_i + y_i + z_i \in \{0, 1, 3\}$ for every i would mean that the three sets to which x, y, z are assigned form a 3-sunflower.

Let $T : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \mathbb{R}$ be defined as

$$T(x, y, z) := \prod_{i=1}^{n} (2 - (x_i + y_i + z_i)).$$

We have already observed that $T(x, y, z) = 0$ if $x, y, z \in S$ are *distinct* and clearly, $T(x, x, x) \neq 0$. However, it may happen that $T(x, y, z) \neq 0$ for some $x, y, z \in S$, if two of the variables x, y, z coincide: $|\{x, y, z\}| = 2$.

By symmetry, assume that $x = y$. If $x_i + y_i + z_i$ is never equal to 2, then for every index i such that $x_i (= y_i) = 1$, we also have $z_i = 1$. This means, that the set to which z is assigned is a superset of the set to which $x (= y)$ is assigned. To overcome this difficulty, let us define S_ℓ to be the set of those elements of S that contain exactly ℓ ones. Observe that S_ℓ is inclusion-free, thus $T\big|_{S_\ell \times S_\ell \times S_\ell}$ is diagonal.

Now, Lemma 7.1 yields that $|S_\ell| = \text{slice-rank}\, T\big|_{S_\ell \times S_\ell \times S_\ell}$, so it suffices to bound the slice-rank of T. As

$$T(x, y, z) = \prod_{i=1}^{n} (2 - (x_i + y_i + z_i)),$$

each monomial appearing in T is multilinear in $x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n$ and of degree at most n. Consequently, in each monomial

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} y_1^{\beta_1} \ldots y_n^{\beta_n} z_1^{\gamma_1} \ldots z_n^{\gamma_n}$$

we have

$$\min(\alpha_1 + \cdots + \alpha_n, \beta_1 + \cdots + \beta_n, \gamma_1 + \cdots + \gamma_n) \leq n/3.$$

For each n-tuple $(\alpha_1, \dots, \alpha_n)$ satisfying $0 \le \alpha_i \le 1$ and $\alpha_1 + \cdots + \alpha_n \le n/3$ we can group the monomials of the form $x_1^{\alpha_1} \dots x_n^{\alpha_n} y_1^{\beta_1} \dots y_n^{\beta_n} z_1^{\gamma_1} \dots z_n^{\gamma_n}$ into a slice of the form $x_1^{\alpha_1} \dots x_n^{\alpha_n} g(y,z)$. After this, we do so for the remaining terms with $y_1^{\beta_1} \dots y_n^{\beta_n}$ (satisfying $\beta_1 + \cdots + \beta_n \le n/3$) and finally, with $z_1^{\gamma_1} \dots z_n^{\gamma_n}$ (satisfying $\gamma_1 + \cdots + \gamma_n \le n/3$). This yields a slice rank decomposition with at most $3 \sum_{k \le n/3} \binom{n}{k}$ slices. Therefore,

$$|S| = \sum_{\ell=0}^{n} |S_\ell| \le 3(n+1) \sum_{k \le n/3} \binom{n}{k},$$

leading to the bound $|\mathcal{F}| \le 1.89^n$.

7.2 Right angle free sets

We consider problems about determining the largest possible size of sets avoiding certain geometric configurations. Some of our questions are related to coding theoretic problems.

Let q be an odd prime power and n a positive integer. A *right angle* in $\mathbb{F}_q^n$ is a triple $x, y, z \in \mathbb{F}_q^n$ of distinct elements satisfying

$$\langle x - z, y - z \rangle = 0,$$

where $\langle \cdot, \cdot \rangle$ denotes the standard dot product.

Let $R(n,q)$ denote the largest possible size of a subset of $\mathbb{F}_q^n$ which contains no right angle.

Bennett [11] proved that

$$R(n,q) \ll q^{\frac{n+2}{3}}.$$

Ge and Shangguan [57] used the slice rank method to improve this bound for fixed q and large n, namely, they showed that

$$R(n,q) \le \binom{n+q}{q-1} + 3,$$

that is, for fixed q the quantity $R(n,q)$ is only polynomial in n. They mentioned that the standard orthonormal basis yields the lower bound $R(n,q) \ge n$ and conjectured that their upper bound is asymptotically tight (for fixed q):

Conjecture 7.2 (Ge-Shangguan, [57])**.** *For any fixed prime power q, $R(n,q) = \Theta(n^{q-1})$.*

Naslund [86] further improved on the upper bound for $R(n,q)$ by showing that

$$R(n,q) \le \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}.$$

We show that for every odd prime power q, in fact, $R(n,q) \ll n^{q-2}$, which refutes Conjecture 7.2:

Theorem 7.3 (Bursics-Matolcsi-Pach-Schrettner [22]). *Let q be an odd prime power. If a set $A \subseteq \mathbb{F}_q^n$ does not contain a right angle, i.e. three distinct vectors with $\langle x-z, y-z\rangle = 0$, then*

$$|A| \le 2(q-1)q\binom{n+q-2}{q-2} + 2q.$$

The above problem may be considered as a finite field version of the Erdős-Falconer problem, which was originally defined in the setting of Euclidean spaces [50, 53, 67] and asked for the smallest d for which any compact set in $\mathbb{R}^n$ with Hausdorff dimension larger than d contains three points forming an angle α (for given n and α). While in the real setting the question is interesting for any α, in the case of the finite field version it is crucial that the dot product 0 is the forbidden one: If A is an isotropic subspace of $\mathbb{F}_q^n$ of maximum dimension, then $\langle x-z, y-z\rangle = 0$ for any $x, y, z \in A$, thus a set A for which $\langle x-y, x-z\rangle \neq \alpha$ for some $\alpha \neq 0$ can be as large as $q^{\frac{n}{2}-1}$.

Naslund also considered a generalized version of right angles. Namely, we say that the vectors $x_0, x_1, \dots, x_k$ form a *k-right corner* if they are distinct, and the k vectors $x_1 - x_0, \dots, x_k - x_0$ form a mutually orthogonal k-tuple, that is, $\langle x_i - x_0, x_j - x_0\rangle = 0$ for all $1 \le i < j \le k$. (Specially, a 2-right corner is a right angle.) Naslund proved that for an integer k, an odd prime power $q = p^r$ with $p > k$ if a subset $A \subseteq \mathbb{F}_q^n$ satisfies

$$|A| > \binom{n+(k-1)q}{(k-1)(q-1)}, \tag{21}$$

then A contains a k-right corner.

We give the following lower bound for this problem:

Theorem 7.4 (Bursics-Matolcsi-Pach-Schrettner [22]). *Let q be an odd prime and $2 \le k$ an integer. There exists a subset $A \subset \mathbb{F}_q^n$ of size*

$$|A| \ge (1-o(1)) \cdot \binom{n}{\left\lceil \frac{k-1}{k}\left\lfloor \frac{k}{2k-1}q\right\rfloor\right\rceil} \Big/ \binom{\left\lfloor \frac{k}{2k-1}q\right\rfloor}{\left\lceil \frac{k-1}{k}\left\lfloor \frac{k}{2k-1}q\right\rfloor\right\rceil}$$

which does not contain any k-right corner, i.e. vectors $x_0, x_1, \dots, x_k$ such that

$$\langle x_i - x_0, x_j - x_0\rangle = 0$$

for all $1 \le i < j \le k$.

Note that for fixed q and k the upper bound for k-right corner free sets is of order $\Theta(n^{(k-1)(q-1)})$, while our lower bound is of order $\Theta\left(n^{\left\lceil \frac{(k-1)(q-1)}{2k-1}\right\rceil}\right)$, where the exponent is the closest integer to $\frac{k-1}{2k-1} \cdot q$.

In the special case $k = 2$ Theorem 7.4 yields the following lower bound for $R(n, q)$:

Corollary 7.5 (Bursics-Matolcsi-Pach-Schrettner [22]). *Let q be an odd prime. There exists a subset $A \subset \mathbb{F}_q^n$ of size*

$$|A| \geq (1 - o(1)) \cdot \binom{n}{\left\lceil \frac{1}{2} \left\lfloor \frac{2}{3} q \right\rfloor \right\rceil} \Big/ \binom{\left\lfloor \frac{2}{3} q \right\rfloor}{\left\lceil \frac{1}{2} \left\lfloor \frac{2}{3} q \right\rfloor \right\rceil}$$

which does not contain a right angle, that is, it is not possible to choose distinct $x, y, z \in A$ such that $\langle y - x, z - x \rangle = 0$.

That is, $R(n, q) \gg n^{\left\lceil \frac{q-1}{3} \right\rceil}$. Note that the exponent in this bound is the closest integer to $q/3$.

Motivated by these problems we also consider the following question:
How large can a set $A \subseteq \mathbb{F}_q^n$ be, if it contains no triangle with *all* right angles, that is, there are no distinct vectors $x, y, z \in A$ with

$$\langle x - y, y - z \rangle = \langle y - z, z - x \rangle = \langle z - x, x - y \rangle = 0?$$

Using the slice rank method, we obtain the following upper bound:

Theorem 7.6 (Bursics-Matolcsi-Pach-Schrettner [22]). *Let q be an odd prime power. If $A \subseteq \mathbb{F}_q^n$ contains no triangle with* all *right angles, i.e. vectors x, y, z with*

$$\langle x - y, y - z \rangle = \langle y - z, z - x \rangle = \langle z - x, x - y \rangle = 0,$$

then

$$|A| \leq \binom{n + 2q - 2}{2q - 2} + \binom{n + 2q - 3}{2q - 3} + 2\left(\binom{n + q - 1}{q - 1} + \binom{n + q - 2}{q - 2}\right).$$

The problem of avoiding triangles with all right angles is equivalent (cf. the proof of Theorem 7.6) to avoiding triples $\{x, y, z\}$, where

$$\langle x - y, x - y \rangle = \langle y - z, y - z \rangle = \langle z - x, z - x \rangle = 0.$$

We consider the following related problem: How large can a set $A \subseteq \mathbb{F}_q^n$ be if $\langle x - y, x - y \rangle \neq 0$ for any two distinct $x, y \in A$? For the maximal size of such a set in $\mathbb{F}_q^n$, we give the following bounds:

Theorem 7.7 (Bursics-Matolcsi-Pach-Schrettner [22]). *Let q be an odd prime. Let $S(n, q)$ be the maximal size of a set in $\mathbb{F}_q^n$ which does not contain distinct vectors x, y such that $\langle x - y, x - y \rangle = 0$. We have the following bounds:*

$$\binom{n}{q - 1} \leq S(n, q) \leq \binom{n + q}{q - 1} - \binom{n + q - 2}{q - 3}.$$

Moreover, whenever $n \not\equiv -2 \pmod{q}$ or $q \equiv 1 \pmod{4}$, then

$$S(n, q) \geq \binom{n}{q - 1} + \binom{n}{q - 2}.$$

In the special case $q = 3$ we can further improve on the lower bound of Theorem 7.7 assuming that n has residue 2 mod 3. Namely, we can construct a suitable set of size $\binom{n+3}{2}-1$ which is our general upper bound. Therefore, in infinitely many cases the exact answer is determined:

Theorem 7.8 (Bursics-Matolcsi-Pach-Schrettner [22]). *For $n \equiv 2 \pmod 3$ we have*

$$S(n,3) = \binom{n+3}{2} - 1.$$

For $n \equiv 0 \pmod 3$, resp. $n \equiv 1 \pmod 3$, we can achieve the lower bounds $\binom{n+2}{2}-1$, resp. $\binom{n+1}{2}-1$, by choosing the last 1, resp. 2, digits to be constant and taking the construction from Theorem 7.8 on the remaining entries. For $n = 3, 4$ these turn out to be sharp, however, for infinitely many values of n there is a better construction. Namely, whenever $q \equiv 2 \pmod 3$ is a prime power, and $n = q^2 + q + 1$, we have a construction of size $\binom{n+1}{2}$, which is bigger (by one!) than the construction given above.

We can also think of the problem of determining $S(n,3)$ from a coding theoretic point of view. Since in $\mathbb{F}_3$ the square of every nonzero element is 1, the value of $\langle x-y, x-y\rangle$ is the same as the Hamming distance of x and y (modulo 3). Therefore, $S(n,3)$ is the largest possible size of a ternary code where none of the Hamming distances between the codewords is divisible by 3.

In the construction from the proof of Theorem 7.8 we use the following observation: there are $\binom{n}{2}+1$ vectors in $\{0,1\}^n (\subseteq \mathbb{F}_3^n)$ with no two of them having Hamming distance divisible by 3. We investigate this question more generally: What is the largest possible size of a binary code of length n, if the Hamming distance of two different codewords is never divisible by a fixed prime q?

We provide the following bounds:

Theorem 7.9 (Bursics-Matolcsi-Pach-Schrettner [22]). *Let q be an odd prime. Let $T(n,q)$ be the maximal size of a subset of $\{a,b\}^n$ with no two vectors having Hamming distance divisible by a fixed prime q. Then the following bounds hold:*

$$T(n,q) \le \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0} \qquad \textit{in general,}$$

$$T(n,q) \le \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0} \qquad \textit{for } n \equiv 0 \pmod q,$$

$$T(n,q) \ge \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0} \qquad \textit{in general,}$$

$$T(n,q) \ge \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0} \qquad \textit{for } n \equiv -1 \pmod q.$$

Hence, by Theorem 7.9 the exact values are determined for $n \equiv 0$ or $-1 \pmod q$.

For the particular case $q = 3$, Theorem 7.9 leaves open only the case $n \equiv 1 \pmod 3$. In this case, for $n = 4$ the exact value is 8, which is 1 larger than the

general lower bound, but we do not know the exact values for any larger n which has residue 1 mod 3.

Note that the general upper bound from Theorem 7.9 is a classical result of Delsarte [34]. Different proofs were given by Frankl [55, Theorem 1.6] and Babai et al [6]. Note that Delsarte's bound is related to the celebrated Ray-Chaudhuri-Wilson [102] theorem stating that maximum number of k-subsets of an n-element set that can be chosen in such a way that there are at most s possible intersection sizes is $\binom{n}{s}$. In fact this result was part of Delsarte's motivation to investigate the problem.

In this thesis the prime case is considered, we give yet another proof of the statement, and provide a general lower bound. Furthermore, we show that both the lower and upper bounds are tight in infinitely many cases.

One application of the slice rank method is going to be through the following lemma:

Lemma 7.10. *Let q be a prime power. Let $\alpha \in \mathbb{F}_q$ and $R \subseteq \mathbb{F}_q \setminus \{\alpha\}$. Let us assume that for a set $A \subseteq \mathbb{F}_q^n$ we have $\langle a, a\rangle = \alpha$ for every $a \in A$ and $\langle x, y\rangle \in R$ for any two distinct $x, y \in A$. Then $|A| \leq \binom{n+|R|}{|R|}$.*

Proof. Let us consider $T : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ defined as

$$T(x, y) = \prod_{r \in R} (\langle x, y\rangle - r).$$

Note that $T(x, x) \neq 0$ and $T(x, y) = 0$ for any $x \neq y$, $x, y \in R$. By Lemma 7.1 we have

$$|A| = \text{slice-rank}\, T\big|_{A \times A} \leq \text{slice-rank}\, T.$$

(Note that since T is a 2-tensor, the slice-rank coincides with the usual matrix rank. We still decided to use the slice-rank notation here, to illustrate the method and show the common flavour with our latter proofs.)

Observe that the slice-rank of T is at most the number of those monomials with n variables that have degree at most $|R|$. Indeed, in each monomial arising in the expansion of T the total degree of the x's is at most $|R|$. Thus T may be expressed as a sum of products fg, where f is a monomial of total degree at most $|R|$ from $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and $g \in \mathbb{F}_q[y_1, y_2, \ldots, y_n]$.

As the number of n-variable monomials of total degree at most $|R|$ is $\binom{n+|R|}{|R|}$, we obtain that

$$|A| \leq \text{slice-rank}\, T \leq \binom{n + |R|}{|R|}.$$

□

For our lower bound constructions we shall use the following lemma about t-uniform families of sets with bounded intersection size:

Lemma 7.11. *Let $\ell \le t$ be positive integers. There exists a t-uniform family $\mathcal{A}$ of subsets of $[n]$ such that for any two distinct $F, G \in \mathcal{A}$ we have $|F \cap G| < \ell$ and*

$$|\mathcal{A}| \ge (1 - o_{n\to\infty}(1)) \cdot \frac{\binom{n}{\ell}}{\binom{t}{\ell}}.$$

Proof. The statement was proved by Rödl in [107]. □

Note that to achieve a lower bound that is valid for every n one can generalize [51, Proposition 1] to get a construction of size $|\mathcal{A}| \ge \frac{\binom{n}{\ell}}{\binom{t}{\ell}^2}$.

7.3 Proofs

Proof of Theorem 7.3. Let $A \subseteq \mathbb{F}_q^n$ be a set such that $\langle x-z, y-z\rangle \neq 0$ for distinct $x, y, z \in A$. For some $\alpha \in \mathbb{F}_q$ for at least $|A|/q$ elements of A we have $\langle x, x\rangle = \alpha$. Let $A^\alpha := \{x \in A : \langle x, x\rangle = \alpha\}$.

Let us pick an element $u \in A^\alpha$. For $\beta \in \mathbb{F}_q$ let

$$A^\alpha_\beta = \{x \in A^\alpha \setminus \{u\} : \langle u, x\rangle = \beta\}.$$

For any two distinct $x, y \in A^\alpha_\beta$ we have $\langle x, y\rangle \in \mathbb{F}_q \setminus \{\alpha, 2\beta - \alpha\}$. Indeed, $\langle x, y\rangle = \alpha$ would imply that

$$\langle x-y, u-y\rangle = \langle x, u\rangle - \langle x, y\rangle - \langle y, u\rangle + \langle y, y\rangle = \beta - \alpha - \beta + \alpha = 0.$$

Similarly, $\langle x, y\rangle = 2\beta - \alpha$ would imply $\langle x-u, y-u\rangle = 0$.

For $\beta \neq \alpha$ Lemma 7.10 applied with the choice $R := \mathbb{F}_q \setminus \{\alpha, 2\beta - \alpha\}$ readily implies that

$$|A^\alpha_\beta| \le \binom{n+q-2}{q-2}.$$

To also bound A^α_α, let us pick an element $v \in A^\alpha_\alpha$. (Note that $v \neq u$.) For $\beta \in \mathbb{F}_q$ let

$$A^\alpha_{\alpha,\beta} = \{x \in A^\alpha_\alpha \setminus \{v\} : \langle v, x\rangle = \beta\}.$$

Note that $A^\alpha_{\alpha,\alpha} = \varnothing$, since for any $x \in A^\alpha_{\alpha,\alpha}$ we would get

$$\langle u-x, v-x\rangle = \alpha - \alpha - \alpha + \alpha = 0.$$

Now, again by Lemma 7.10,

$$|A^\alpha_{\alpha,\beta}| \le \binom{n+q-2}{q-2}$$

for every $\beta \neq \alpha$.

Therefore,

$$|A^\alpha| = 1 + |A^\alpha_\alpha| + \sum_{\beta\in\mathbb{F}_q\setminus\{\alpha\}} |A^\alpha_\beta| \le 2 + \sum_{\beta\in\mathbb{F}_q\setminus\{\alpha\}} |A^\alpha_{\alpha,\beta}| + \sum_{\beta\in\mathbb{F}_q\setminus\{\alpha\}} |A^\alpha_\beta| \le 2(q-1)\binom{n+q-2}{q-2} + 2.$$

Hence, $|A| \le q|A^\alpha| \le 2(q-1)q\binom{n+q-2}{q-2} + 2q$. □

Remark 7.12. *Note that we did not optimize in the proof the arising constant factor $2(q-1)q$. Also, in case q is a power of 2 we would get a bound weaker by a factor n, since in this case R is a $(q-1)$-element set.*

Proof of Theorem 7.4. Let $t = \lfloor \frac{k}{2k-1} q \rfloor$. Let $\mathcal{A}$ be a t-uniform family of subsets of $[n]$ such that for any two distinct $F, G \in \mathcal{A}$ we have $|F \cap G| < \frac{k-1}{k} t$. According to Lemma 7.11 we may take a system of size

$$|\mathcal{A}| \geq (1 - o(1)) \cdot \frac{\binom{n}{\lceil (k-1)t/k \rceil}}{\binom{t}{\lceil (k-1)t/k \rceil}}.$$

Now, let A consist of the characteristic vectors of the elements of $\mathcal{A}$, considered as elements of $\mathbb{F}_q^n$. That is, $a = (a_1, \ldots, a_n) \in \{0,1\}^n$ is contained in A if and only if $\{i : \ a_i = 1\} \in \mathcal{A}$.

We claim that A avoids k-right corners, that is, for any $k+1$ distinct elements $x_0, x_1, \ldots, x_k \in A$ the dot products $\langle x_i - x_0, x_j - x_0 \rangle$ $(1 \leq i < j \leq k)$ can not be simultaneously 0 (in $\mathbb{F}_q$).

To show this, let us take arbitrarily $k+1$ distinct elements, $x_0, x_1, \ldots, x_k \in A$, and denote by $X_0, X_1, \ldots, X_k$ the corresponding subsets of $[n]$. First, let us show that for some indices $1 \leq i < j \leq k$ we have $X_0 \setminus (X_i \cup X_j) \neq \varnothing$. Since $X_0 \in \mathcal{A}$, we have $|X_0| = t$, and we also know that $|X_0 \setminus X_i| > \frac{t}{k}$ for every $1 \leq i \leq k$. Thus, by the pigeonhole principle we obtain that for two different indices i and j we have

$$\varnothing \neq (X_0 \setminus X_i) \cap (X_0 \setminus X_j) = X_0 \setminus (X_i \cup X_j),$$

as it was claimed.

Observe that

$$\begin{aligned} &\langle x_i - x_0, x_j - x_0 \rangle = \langle x_i, x_j \rangle + \langle x_0, x_0 \rangle - \langle x_i, x_0 \rangle - \langle x_0, x_j \rangle = \\ &= |X_i \cap X_j| + |X_0| - |X_i \cap X_0| - |X_0 \cap X_j| = |(X_i \cap X_j) \setminus X_0| + |X_0 \setminus (X_i \cup X_j)|. \end{aligned}$$

As

$$0 \leq |(X_i \cap X_j) \setminus X_0| < \frac{k-1}{k} t \text{ and } 0 < |X_0 \setminus (X_i \cup X_j)| \leq t$$

we have

$$0 < |(X_i \cap X_j) \setminus X_0| + |X_0 \setminus (X_i \cup X_j)| < \frac{k-1}{k} t + t = \frac{2k-1}{k} t \leq q,$$

hence $\langle x_i - x_0, x_j - x_0 \rangle \neq 0$.

□

Proof of Theorem 7.6. First of all, we show that the condition that the three sides of a triangle are pairwise orthogonal is equivalent to the condition that all the three sides are self-orthogonal. Assume first that

$$\langle x-y, y-z\rangle = \langle y-z, z-x\rangle = \langle z-x, x-y\rangle = 0.$$

Now,

$$\langle x-y, x-y\rangle = \langle x-y, (x-z)+(z-y)\rangle = \langle x-y, x-z\rangle + \langle x-y, z-y\rangle = 0+0=0,$$

and $\langle y-z, y-z\rangle = \langle z-x, z-x\rangle = 0$ can be proved analogously.

For the reverse direction assume that

$$\langle x-y, x-y\rangle = \langle y-z, y-z\rangle = \langle z-x, z-x\rangle = 0.$$

Then

$$\langle x-y, y-z\rangle = \frac{\langle (x-y)+(y-z), (x-y)+(y-z)\rangle - \langle x-y, x-y\rangle - \langle y-z, y-z\rangle}{2} = 0,$$

and $\langle x-y, z-x\rangle = \langle y-z, z-x\rangle = 0$ follows similarly.

Hence, if $A \subseteq \mathbb{F}_q^n$ does not contain a triangle with all right angles, then the set A does not contain three distinct vectors x, y, z such that

$$\langle x-y, x-y\rangle = \langle y-z, y-z\rangle = \langle z-x, z-x\rangle = 0.$$

Let us consider $F : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ defined as

$$F(x,y,z) = (1-\langle x-y, x-y\rangle^{q-1})(1-\langle y-z, y-z\rangle^{q-1})(1-\langle z-x, z-x\rangle^{q-1}).$$

Observe that for distinct $x, y, z \in A$ we have $F(x,y,z) = 0$ according to the assumption on A. Also, for $x = y = z$ we have $F(x,y,z) = F(x,x,x) = 1$. However, $F\big|_{A\times A\times A}$ might not be diagonal, as for instance $F(x,x,z)$ may be nonzero for $x \neq z$. Therefore, let us consider

$$G(x,y,z) := F(x,y,z)(1-\delta(x,y)-\delta(y,z)-\delta(z,x)),$$

where δ is the Kronecker delta function.

For $x = y = z$ we have

$$G(x,y,z) = 1\cdot(1-1-1-1) = -2 \neq 0$$

and G vanishes at (x,y,z) when x, y, z are distinct elements of A. Moreover, if two of x, y, z coincide, but the third one is different, then $1-\delta(x,y)-\delta(y,z)-\delta(z,x) = 0$, thus $G(x,y,z) = 0$ also holds.

Hence, $G\big|_{A\times A\times A}$ is diagonal, that is, for $x, y, z \in A$ we have $G(x,y,z) \neq 0$ if and only if $x = y = z$. According to Lemma 7.1 we have $|A| = \text{slice-rank}(G\big|_{A\times A\times A})$. Now, we give an upper bound for the slice-rank of $G\big|_{A\times A\times A}$.

First of all,

$$F(x,y,z) = (1-\langle x-y, x-y\rangle^{q-1})(1-\langle y-z, y-z\rangle^{q-1})(1-\langle z-x, z-x\rangle^{q-1}) =$$
$$= [1-(x_0+y_0-2x_1y_1-2x_2y_2-\cdots-2x_ny_n)^{q-1}]\cdot[1-(y_0+z_0-2y_1z_1-2y_2z_2-\cdots-2y_nz_n)^{q-1}]\cdot$$
$$\cdot[1-(z_0+x_0-2z_1x_1-2z_2x_2-\cdots-2z_nx_n)^{q-1}],$$

where $x_0 = \sum_{i=1}^{n} x_i^2$, $y_0 = \sum_{i=1}^{n} y_i^2$ and $z_0 = \sum_{i=1}^{n} z_i^2$.

Each monomial in $F(x,y,z)$ can be written as a product of a monomial of the form $x_0^{\alpha_0}x_1^{\alpha_1}\dots x_n^{\alpha_n}$ where $\alpha_0+\alpha_1+\cdots+\alpha_n \le 2(q-1)$ and a polynomial of y and z. Therefore, the slice-rank of F is at most the dimension of the subspace spanned by these polynomials of x which, by a lemma of Bannai and Bannai [8, Lemma], is at most $\binom{n+2q-2}{2q-2} + \binom{n+2q-3}{2q-3}$.

Let us consider now $\delta(x,y)F(x,y,z)$. Observe that on $A\times A\times A$ we have

$$\delta(x,y)F(x,y,z) = \delta(x,y)(1-\langle z-x, z-x\rangle^{q-1}).$$

Note that each monomial in

$$1-\langle z-x, z-x\rangle^{q-1} = 1-(z_0+x_0-2z_1x_1-\cdots-2z_nx_n)^{q-1}$$

can be written as a product of a monomial of the form $z_0^{\alpha_0}z_1^{\alpha_1}\dots z_n^{\alpha_n}$ where $\alpha_0+\alpha_1+\cdots+\alpha_n \le q-1$ and a polynomial of x and y. Since $\delta(x,y) = \prod_{i=1}^{n}(1-(x_i-y_i)^{q-1})$ is a polynomial of x and y, the slice-rank of $\delta(x,y)F(x,y,z)\big|_{A\times A\times A}$ is at most $\binom{n+q-1}{q-1} + \binom{n+q-2}{q-2}$ by [8, Lemma].

Analogously, the slice-rank of $\delta(z,x)F(x,y,z)\big|_{A\times A\times A}$ is also at most $\binom{n+q-1}{q-1} + \binom{n+q-2}{q-2}$. Also, each monomial of $\delta(y,z)F(x,y,z)\big|_{A\times A\times A}$ can be written as a product of a monomial of the form $x_0^{\alpha_0}x_1^{\alpha_1}\dots x_n^{\alpha_n}$ where $\alpha_0+\alpha_1+\cdots+\alpha_n \le q-1$ and a polynomial of y and z. However, these types of products already appeared when we considered the slice-rank of F, so in fact

$$\text{slice-rank}(F(x,y,z)(1-\delta(y,z)) \le \binom{n+2q-2}{2q-2} + \binom{n+2q-3}{2q-3}.$$

Hence,

$$|A| = \text{slice-rank}\left(G\big|_{A\times A\times A}\right) \le$$
$$\le \binom{n+2q-2}{2q-2} + \binom{n+2q-3}{2q-3} + 2\left(\binom{n+q-1}{q-1} + \binom{n+q-2}{q-2}\right).$$

□

Proof of Theorem 7.7. Let us start with proving the upper bound.

Let A be a set satisfying the property, that is, for every pair of distinct $x, y \in A$ we have $\langle x-y, x-y\rangle \neq 0$. For every $a \in A$ let p_a be the following polynomial:

$$p_a(x) := 1 - \langle x-a, x-a\rangle^{q-1} = 1 - \left(\sum_{i=1}^{n}(x_i-a_i)^2\right)^{q-1}.$$

Note that $p_a(a) = 1$, and for every $b \in A \setminus \{a\}$ we have $p_a(b) = 0$, since $\langle a-b, a-b\rangle \neq 0$. This readily implies that the system of polynomials $\{p_a \mid a \in A\}$ is linearly independent.

Since

$$p_a(x) = 1 - \left(\sum_{i=1}^{n}(x_i-a_i)^2\right)^{q-1} = \\ = 1 - \left((x_1^2+\cdots+x_n^2) - 2a_1x_1 - \cdots - 2a_nx_n + (a_1^2+\cdots+a_n^2)\right)^{q-1},$$

we have $\{p_a \mid a \in A\} \subseteq \mathrm{span}_{\mathbb{F}_q}(H)$, where

$$H = \left\{(x_1^2+\cdots+x_n^2)^{\alpha_0} \cdot x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \mid \sum_{i=0}^{n}\alpha_i \leq q-1\right\}.$$

By using a lemma of Bannai and Bannai [8, Lemma] we bound the dimension of the subspace spanned by the elements of H and get that

$$|A| \leq \dim\big(\mathrm{span}_{\mathbb{F}_q}(H)\big) \leq \binom{n+q-1}{q-1} + \binom{n+q-2}{q-2} = \binom{n+q}{q-1} - \binom{n+q-2}{q-3},$$

which completes the proof of the upper bound.

Let us continue with the lower bound.

Let A be the set of all vectors having $q-1$ components equal to 1, and all the remaining $n-q+1$ components being equal to 0. Note that $|A| = \binom{n}{q-1}$.

If $x, y \in A$ are distinct, then $\langle x-y, x-y\rangle = 2(q-1)-2\langle x, y\rangle \neq 0$, since $\langle x, y\rangle \neq q-1$.

Finally, in the cases when $n \not\equiv -2 \pmod q$ or $q \equiv 1 \pmod 4$ we can further improve on the previous lower bound. The construction is as follows: let A_1 be the previously defined set of all vectors with $q-1$ components being equal to 1, and $n-q+1$ components being equal to 0. Furthermore, let A_2 be the set of all vectors with $q-2$ entries a and $n-q+2$ entries b, where the elements $a \neq b$ are going to be chosen later. Note that the size of A is $\binom{n}{q-1} + \binom{n}{q-2}$. We claim that for an appropriate choice of a and b the set $A = A_1 \cup A_2$ does not contain two vectors x, y such that $\langle x-y, x-y\rangle = 0$.

We have already seen that $\langle x-y, x-y\rangle \neq 0$, if x, y are distinct elements taken from A_1. Similarly, if x, y are distinct vectors taken from A_2, then

$$\langle x-y, x-y\rangle = 2k(a-b)^2 \neq 0,$$

where k is the number of entries that are a in x and b in y. (As $a \neq b$, we have $0 < k \leq q-2$, and by the definition of A_2 the number of those entries that are b in x and a in y is also k, all the remaining entries are the same in x and y.)

It remains to consider the pairs $x \in A_1,\ y \in A_2$.

Let us assume that there are k indices i with $(x_i, y_i) = (1, a)$. Then $0 \leq k \leq q-2$ and there are

- $q-1-k$ indices i with $(x_i, y_i) = (1, b)$,
- $q-2-k$ indices i with $(x_i, y_i) = (0, a)$,
- $n+k-2q+3$ indices i with $(x_i, y_i) = (0, b)$.

Therefore, (calculating in $\mathbb{F}_q$)

$$\langle x-y, x-y\rangle = k(a-1)^2 + (q-1-k)(b-1)^2 + (q-2-k)a^2 + (n+k-2q+3)b^2 =$$
$$= -2a^2 + (n+2)b^2 - 2ka + (2k+2)b - 1 = (2b-2a)k - 2a^2 + (n+2)b^2 + 2b - 1.$$

Thus we can think of $\langle x-y, x-y\rangle$ as a linear function of k with leading coefficient $-2a+2b = 2(b-a) \neq 0$ (since $a \neq b$). Hence, there is exactly one residue class ($k \bmod q$) which solves this linear equation (and gives $\langle x-y, x-y\rangle = 0$). Note that $k \in [0, q-2]$, so to ensure $\langle x-y, x-y\rangle \neq 0$ for all choices of x, y this (unique) solution must be $k \equiv -1 \pmod q$. That is, we shall choose a and b in such a way that

$$-2a^2 + (n+2)b^2 + 2a - 1 = 0,$$

or equivalently

$$(n+2)b^2 = 2a^2 - 2a + 1. \tag{22}$$

Here we distinguish two cases depending on whether $n \not\equiv -2 \pmod q$ or $n \equiv -2 \pmod q$. Let us assume first that $n \not\equiv -2 \pmod q$.

Observe that both sides of equation (22) can attain exactly $\frac{q+1}{2}$ different values, thus, there must be at least one element which can be expressed as $(n+2)b^2$ and as $2a^2 - 2a + 1$, simultaneously. In other words, the equation has a solution a, b. If $a \neq b$, then we are done, otherwise we may take the solution $a, -b$, which also satisfies $a \neq -b$ (since $a = b = 0$ is not a solution).

Finally, we consider the case $n \equiv -2 \pmod q$. Here, the solvability of (22) reduces to the solvability of $0 = 2a^2 - 2a + 1$. This equation is solvable if its discriminant -4 is a square modulo q, that is, if $q \equiv 1 \pmod 4$. In this case for a solution a we may choose any $b \neq a$. This completes our proof.

□

Proof of Theorem 7.8. The upper bound follows from Theorem 7.7, by presenting a matching lower bound the proof will be complete. The construction for the lower bound is as follows:
Let the set $A \subseteq \mathbb{F}_3^n$ consist of

- all the vectors where exactly two entries are 1's and all other entries are 0's,
- all the vectors where one entry is 0 and all other entries are 2's,
- all the vectors where one entry is 1 and all the other entries are 2's,
- all the vectors where one entry is 0 and all the other entries are 1's,
- the all-zero vector $(0, 0, \ldots, 0)$,
- the all-2 vector $(2, 2, \ldots, 2)$.

Since we are modulo 3, we have $\langle x - y, x - y \rangle = 0$ if and only if the Hamming distance of the vectors x and y is divisible by 3. It is easy to check that assuming $n \equiv 2 \pmod 3$ none of the pairs of vectors from the above defined set have Hamming distance divisible by 3.

The cardinality of the set is

$$|A| = \binom{n}{2} + 3n + 2 = \binom{n+3}{2} - 1.$$

□

Proof of Theorem 7.9. Let us start with proving the lower bound. Let A consist of those elements of $\{a, b\}^n$ in which the number of characters a is even and at most $q - 1$.

Let x and y be two distinct elements of A. Let k, resp. ℓ, denote the number of characters a in x, resp. y, and denote by m the number of those entries where both x and y have a. Then the number of indices i such that $(x_i, y_i) = (a, b)$ is $k - m$ and the number of indices i such that $(x_i, y_i) = (b, a)$ is $\ell - m$. Hence, the total number of those indices where x and y differ from each other is $k + \ell - 2m$:

$$d(x, y) = k + \ell - 2m,$$

where $d(x, y)$ stands for the Hamming distance of x and y. Observe that k and ℓ are even and $k, \ell \leq q - 1$, thus $d(x, y) = k + \ell - 2m \in (0, 2q)$ is even, which implies that $d(x, y)$ is not divisible by q.

As $|A| = \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$, this completes the proof of our general lower bound.

In the special case when $n \equiv -1 \pmod q$, we present a better construction.

Let us add to the previously defined set A those elements of $\{a, b\}^n$ in which the number of characters b is odd and at most $q - 2$. This way the set A' is obtained which has size

$$|A'| = \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}.$$

We have already seen that $q \nmid d(x,y) = k+\ell-2m$, if $x, y \in A$ are distinct.

If x and y are two distinct elements of $A' \setminus A$, then $n-k$ and $n-\ell$ are odd and at most $q-2$. The number of those indices for which $(x_i, y_i) = (b,b)$ is $n-k-\ell+m$, thus

$$0 < d(x,y) = k+\ell-2m = (n-k)+(n-\ell)-2(n+m-k-\ell) \le 2(q-2) < 2q,$$

and $k+\ell-2m$ is even, therefore, $d(x,y) = k+\ell-2m \neq q$, so $q \nmid d(x,y)$.

Finally, let us assume that $x \in A$ and $y \in A' \setminus A$. Then $k \le q-1$ is even and $n-\ell \le q-2$ is odd. Observe that

$$d(x,y) = k+\ell-2m = n+2(k-m)-k-(n-\ell),$$

thus

$$n-2q+3 = n+0-(q-1)-(q-2) \le n+2(k-m)-k-(n-\ell) = d(x,y) \le n.$$

Since $2 \mid k$ and $2 \nmid n-\ell$, the Hamming distance $d(x,y) = k+\ell-2m$ has the same parity as $n+1$. As $q \mid n+1$, in the interval $[n-2q+3, n]$ only one element, $n-q+1$, is divisible by q, however, its parity is different from the parity of $n+1$. Hence, $q \nmid d(x,y)$, as we claimed.

Let us continue with the upper bound. We may assume that the two characters are ± 1, considered as elements of $\mathbb{F}_q$. This way, $A \subseteq \{-1,1\}^n \subset \mathbb{F}_q^n$. Note that for $x, y \in \{-1,1\}^n$ we have

$$\langle x-y, x-y\rangle = \sum_{i=1}^{n} (x_i - y_i)^2 = 4d(x,y),$$

as $(x_i-y_i)^2$ is 4, if x and y differ in the ith coordinate and 0, otherwise. Therefore, the Hamming distance $d(x,y)$ is divisible by q if and only if $\langle x-y, x-y\rangle = 0$.

Let $A = \{a_1, a_2, \ldots, a_r\}$. The assumption on A implies that $\langle a_i - a_j, a_i - a_j\rangle \neq 0$, when $i \neq j$. Let us consider the polynomials $p_i(x) := 1 - \langle x-a_i, x-a_i\rangle^{q-1}$. Let $f_i := p_i\big|_A$, that is, by restricting the domain of p_i to A we obtain the function f_i. Note that for every i, j we have $f_i(a_j) = \delta_{ij}$. This condition implies that $f_1, f_2, \ldots, f_r$ are linearly independent. Now, we show that these functions are contained in a subspace of dimension $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$.

Let $a_{i,j}$ denote the jth entry of a_i. Observe that for every $1 \le i \le r$ and every $x \in A$

$$\langle x-a_i, x-a_i\rangle = \sum_{j=1}^{n} (x_j - a_{i,j})^2 = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} 2a_{i,j}x_j + \sum_{j=1}^{n} a_{i,j}^2 = 2n - \sum_{j=1}^{n} 2a_{i,j}x_j,$$

where the last equality holds, since $a_{i,j} \in \{\pm 1\}$ and $x \in A \subseteq \{-1,1\}^n$.

Therefore, $f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}$ is a polynomial of $x_1, x_2, \ldots, x_n$ of degree $q-1$.

Furthermore, since $x_j^2 = 1$ for every $x_j \in A$ we can reduce the exponent of x_j to 0 or 1, according to the parity of the original exponent. This way each f_i is represented as a polynomial of degree at most $q-1$, where each individual degree is at most 1.

Each such monomial is uniquely determined with the subset of those variables x_i which has exponent 1 (the rest of the variables have exponent 0). The number of these monomials is

$$\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0},$$

hence by the linear independency of $f_1, \ldots, f_r$ this also serves as an upper bound for $r = |A|$, which completes the proof.

If $q \mid n$, then we can improve on this upper bound. Since, in this case $2n = 0$ (in $\mathbb{F}_q$), thus

$$f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1} = 1 - \left(\sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}.$$

Expressing f_i this way, with the exception of the constant term 1, all the monomials have degree $q-1$. After reducing the exponents, we get monomials with even total degree (as $q-1$ is also even). Consequently, the upper bound is improved to the number of those subsets of $x_1, \ldots, x_n$ whose size is even and at most $q-1$. Hence,

$$|A| = r \leq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}.$$

□

Remark 7.13. *In this section we proved that the largest subset of $\mathbb{F}_q^n$ (where q is an odd prime) is between $\Theta(n^{q/3})$ and $\Theta(n^{q-2})$, however, for $q > 3$ this leaves open what the right exponent is between $q/3$ and $q-2$. We shall note that one can transform our lower bound construction to a set A for which $\langle x, x\rangle = 0$ for every $x \in A$ and $\langle x, y\rangle \in B$ for any two distinct $x, y \in A$ with some sum-free subset $B \subseteq \mathbb{F}_q$. Then $\langle x - z, y - z\rangle = \langle x, y\rangle - (\langle x, z\rangle + \langle z, y\rangle) \neq 0$ indeed holds.*

For the analogous problem for k-right corners there is also a gap between our lower bound and Naslund's upper bound (which gets larger as k grows). In the case of triangles with all right angles, there's also a gap in the exponent of n.

For the problem where self-orthogonal differences are to be avoided our bounds are asymptotically tight, though the exact answer is determined only for a specific (infinite) family of parameters q and n.

It would be interesting to further tighten these gaps.

References

[1] A. Aleksanyan and M. Papikian, On Blocking Sets of Affine Spaces, (1999) arXiv: 9910084

[2] N. Alon, Combinatorial Nullstellensatz, Combinatorics, Probability and Computing 8 (1999) 7–29.

[3] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in: "Combinatorics, Paul Erdős is Eighty", Bolyai Society, Mathematical Studies, Keszthely, Hungary (1993) 33–50.

[4] N. Alon and M. Dubiner, A lattice point problem and additive number theory, Combinatorica 15 (1995) 301–309.

[5] N. Alon, A. Shpilka, C. Umans, On sunflowers and matrix multiplication, Comput. Complexity 22 (2013) no. 2, 219–243.

[6] L. Babai, H. Snevily, R. M. Wilson, A new proof of several inequalities on codes and sets, Journal of Combinatorial Theory, Series A 71 (1) (1995) 146–153.

[7] S. Ball, The polynomial method in Galois geometries (2009) https://web.mat.upc.edu/simeon.michael.ball/polynomialmethod.pdf

[8] E. Bannai and E. Bannai, An upper bound for the cardinality of an s-distance subset in real Euclidean space, Combinatorica, 1 (2) (1981) 99–102.

[9] M. Bateman and N. H. Katz, New bounds on cap sets, J. Amer. Math. Soc. 25 (2012) no. 2, 585–613.

[10] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, Proc. Natl. Acad. Sci. USA 32 (1946) 331–332.

[11] M. Bennett, Occurrence of right angles in vector spaces over finite fields, European Journal of Combinatorics 70 (2018) 155–163.

[12] J. Bierbrauer and Y. Edel, Large caps in small spaces, Des. Codes Cryptogr. 23 (2001) no. 2, 197–212.

[13] A. Bishnoi, J. D'haeseleer, D. Gijswijt, A. Potukuchi, Blocking sets, minimal codes and trifferent codes, arXiv:2301.09457

[14] J. Blasiak, T. Church, H. Cohn, J. Grochow, E. Naslund, W. Sawin, C. Umans, On cap sets and the group-theoretic approach to matrix multiplication, Discrete Anal. (2017) Paper No. 3, 27 pp.

[15] T. Bloom and O. Sisask, Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions, arXiv:2007.03528

[16] T. Bloom and O. Sisask, The Kelley–Meka bounds for sets free of three-term arithmetic progressions, arXiv:2302.07211

[17] T. Bloom and O. Sisask, An improvement to the Kelley-Meka bounds on three-term arithmetic progressions, arXiv:2309.02353

[18] J. Bourgain, On triples in arithmetic progression, Geom. Funct. Anal. 9 (5) (1999) 968–984.

[19] J. Bourgain, Roth's theorem on progressions revisited, J. Anal. Math. 104 (2008) 155–192.

[20] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, J. Combinatorial Theory Ser. A 24.2 (1978) 251–253.

[21] T. C. Brown and J. P. Buhler, A density version of a geometric Ramsey theorem, J. Combin. Theory Ser. A 25 (1982) 20–34.

[22] B. Bursics, D. Matolcsi, P.P. Pach, J. Schrettner, Avoiding right angles and certain Hamming distances, Linear Algebra and its Applications 677 (2023) 71–87.

[23] A. R. Calderbank and P. C. Fishburn, Maximal three-independent subsets of $\{0,1,2\}^n$, Des. Codes Cryptogr. 4 (1994) no. 3, 203–211.

[24] P. J. Cameron, Sum-free sets of a square, manuscript, available at `http://www.maths.qmul.ac.uk/~pjc/odds/sfsq.pdf`

[25] A. K. Chandra, On the solution of Moser's problem in four dimensions, Canad. Math. Bull. 16 (1973) 507–511.

[26] V. Chvátal, Remarks on a problem of Moser, Canad. Math. Bull. 15 (1972) 19–21.

[27] V. Chvátal, Edmonds polytopes and a hierarchy of combinatorial problems, Discrete Math. 4 (1973) 305-337. Reprinted: Discrete Math. 306 (2006) 886–904.

[28] D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progressions, STOC '87 (Proceedings of the nineteenth annual ACM symposium on Theory of computing) Pages 1–6, also: Journal of Symbolic Computation 9 no. 3 (1990) 251–280.

[29] E. Croot, The minimal number of three-term arithmetic progressions modulo a prime converges to a limit, Canad. Math. Bull. 51 (2008) no. 1, 47–56.

[30] E. Croot and O. Sisask, A probabilistic technique for finding almost-periods of convolutions, Geom. Funct. Anal. 20 (2010) 1367–1396.

[31] E. Croot, V.F. Lev, P.P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small, Ann. of Math. (2) 185 (2017) no. 1, 331–337.

[32] E. Croot, V.F. Lev, P.P. Pach, Past and future of the cap set problem, submitted (conference paper, International Congress of Basic Science, Beijing) (2024)

[33] B. L. Davis and D. Maclagan, The card game SET, Math. Intelligencer 25 (2003) no. 3, 33–40.

[34] P. Delsarte, Four Fundamental Parameters of a Code and Their Combinatorial Significance, Information and Control 23 (1973) 407–438.

[35] Z. Dvir: On the size of Kakeya sets in finite fields, Journal of the American Mathematical Society 22.4 (2008) pp. 1093–1097.

[36] Y. Edel, Extensions of generalized product caps, Des. Codes Cryptography 31 (2004) 5–14.

[37] Y. Edel, Sequences in abelian groups G of odd order without zero-sum subsequences of length $\exp(G)$, Des. Codes Cryptogr. 47 (2008) no. 1-3, 125–134.

[38] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, L. Rackham, Zero-sum problems in finite abelian groups and affine caps, Q. J. Math. 58 (2007) no. 2, 159–186.

[39] Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in $AG(5,3)$, J. Combin. Theory Ser. A 99 (2002) 95–110.

[40] M. Elkin, An Improved Construction of Progression-Free Sets, Israeli J. Math. 184 (2011) 93–128.

[41] J. S. Ellenberg and D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, Ann. of Math. (2) 185 (2017) no. 1, 339–343.

[42] C. Elsholtz, Lower bounds for multidimensional zero sums, Combinatorica 24 (2004) no. 3, 351–358.

[43] C. Elsholtz, J. Führer, E. Füredi, B. Kovács, P. P. Pach, D. G. Simon, N. Velich, Maximal line-free sets in $\mathbb{F}_p^n$, Periodica Mathematica Hungarica, to appear

[44] C. Elsholtz, Z. Hunter, L. Proske, L. Sauermann, Improving Behrend's construction: Sets without arithmetic progressions in integers and over finite fields, arXiv:2406.12290

[45] C. Elsholtz and P. P. Pach, Des. Codes Cryptography 88 (2020) 2133-2170.

[46] C. Elsholtz and L. Rackham, Maximal sum-free sets of integer lattice grids, J. Lond. Math. Soc. (2) 95 (2017) no. 2, 353–372.

[47] P. Erdős, Problems in number theory and combinatorics, Proceedings of the Sixth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1976), Congress. Numer., XVIII, pages 35–58. Utilitas Math., Winnipeg, Man. (1977)

[48] P. Erdős, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel F (10) (1961) 41–43.

[49] P. Erdős, Problems and results on combinatorial number theory, in: A survey of Combinatorial Theory, J.N Srivastava et al., eds, North Holland (1973) 117–138.

[50] P. Erdős and Z. Füredi, The greatest angle among n points in the d-dimensional Euclidean space, In Combinatorial mathematics (Marseille-Luminy, 1981), volume 75 of NorthHolland Math. Stud., pages 275–283. North-Holland, Amsterdam (1983)

[51] P. Erdős, P. Frankl, Z. Füredi, Families of finite sets in which no set is covered by the union of two others, Journal of Combinatorial Theory, Series A 33 (2) (1982) 158–166.

[52] P. Erdős and P. Turán, On some sequences of integers, J. London Math. Soc. 11 (1936) 261–264.

[53] K. J. Falconer, On a problem of Erdős on fractal combinatorial geometry, J. Combin. Theory Ser. A, 59(1) (1992) 142–148.

[54] J. Fox and L. M. Lovász, A tight bound for Green's arithmetic triangle removal lemma in vector spaces, Adv. Math. 321 (2017) 287–297.

[55] P. Frankl, Orthogonal vectors in the n-dimensional cube and codes with missing distances, Combinatorica 6 (3) (1986) 279–285.

[56] P. Frankl, R. L. Graham, V. Rödl, On subsets of abelian groups with no 3-term arithmetic progression, J. Comb. Theory, Ser. A 45(1) (1987) 157–161.

[57] G. Ge and C. Shangguan, Maximum subsets of $\mathbb{F}_q^n$ containing no right angles, J. Algebr. Comb. (2019) https://doi.org/10.1007/s10801-019-00908-4

[58] W. T. Gowers, A new proof of Szemerédi's theorem, Geom. Funct. Anal. 11 (3) (2001) 465–588.

[59] W. T. Gowers, Generalizations of Fourier analysis, and how to apply them, Bull. Amer. Math. Soc. 54 (2017) 1-44.

[60] B. J. Green, Finite field models in additive combinatorics, Surveys in Combinatorics 2005, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge University Press (2005) pp. 1–27.

[61] B. Green and T. Tao, New bounds for Szemerédi's theorem. I. Progressions of length 4 in finite field geometries. Proc. Lond. Math. Soc. (3) 98 (2009), no. 2, 365–392.
and correction: New bounds for Szemeredi's theorem, Ia: Progressions of length 4 in finite field geometries revisited, 16 pages, arXiv:1205.1330

[62] B. Green and T. Tao, New bounds for Szemerédi's theorem. II. A new bound for $r_4(N)$, Analytic number theory, Cambridge Univ. Press, Cambridge (2009) pp. 180–204.

[63] B. Green and T. Tao, New bounds for Szemerédi's theorem, III: a polylogarithmic bound for $r_4(N)$, Mathematika 63 (2017) 944–1040.

[64] J. A. Grochow, New applications of the polynomial method: The cap set conjecture and beyond, Bulletin of the American Mathematical Society 56 (2019) no. 1, 29–64.

[65] L. Guth and N. H. Katz, On the Erdős distinct distances problem in the plane, Annals of Mathematics 181 (1) (2015) 155–190.

[66] A. W. Hales and R. I. Jewett, Regularity and positional games, Trans. Amer. Math. Soc. 106 (1963) 222–229.

[67] V. Harangi, T. Keleti, G. Kiss, P. Maga, A. Máthé, P. Mattila, B. Strenner, How large dimension guarantees a given angle?, Monatsh. Math., 171(2):169–187 (2013)

[68] D. R. Heath-Brown, Integer sets containing no arithmetic progressions, J. London Math. Soc. 35 (1987) 385–394.

[69] G. Hegedüs, A new exponential upper bound for the Erdős-Ginzburg-Ziv constant, arXiv:1712.00228

[70] R. E. Jamison, Covering finite fields with cosets of subspaces, J. Combinatorial Theory Ser. A 22.3 (1977) 253–266.

[71] Z. Jiang, Improved explicit upper bounds for the Cap Set Problem, arXiv:2103.06481

[72] G. Kalai, Webblog, 7th February 2009, http://gilkalai.wordpress.com/2009/02/07/frankl-rodls-theorem-and-variations-on-the-cap-set-problem-a-recent-research-project-with-roy-meshulam-a/

[73] Z. Kelley and R. Meka, Strong bounds for 3-Progressions, 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS), 933–973.

[74] J. Kim, H. Liu, P. P. Pach, Optimal polynomial Schur's theorem, submitted arXiv:2404.00794

[75] J. Komlós, solution to problem P.170 by Leo Moser, Canad. Math. Bull. vol. 15 (1972) 312–313.

[76] J. Leng, A. Sah, M. Sawhney, Improved bounds for Szemerédi's theorem, arXiv:2402.17995

[77] V. F. Lev, Progression-free sets in finite abelian groups, J. Number Theory 104 (2004) 162–169.

[78] V. Lev, Character-free approach to progression-free sets, Finite Fields Their Appl. 18 (2012) 378–383.

[79] Y. Lin and J. Wolf, Subsets of $\mathbb{F}_q^n$ containing no k-term progressions, European J. Combin., 31(5) (2010) 1398–1403.

[80] H. Liu, P. P. Pach, C. Sándor, Polynomial Schur's Theorem, Combinatorica (2) (2022) 1357–1384.

[81] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland (1977)

[82] N. McNew, On sets of integers which contain no three terms in geometric progression, Mathematics of Computation 84 (2015) 2893-2910.

[83] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, J. Comb. Theory, Ser. A 71 (1995) 168–172.

[84] L. Moser, Problem P.170 in Canad. Math. Bull. 13 (1970) 268

[85] E. Naslund, Exponential Bounds for the Erdős-Ginzburg-Ziv constant, J. Combin. Theory Ser. A 174 (2020) 105185, 19 pp.

[86] E. Naslund, The partition rank of a tensor and k-right corners in $\mathbb{F}_q^n$, Journal of Combinatorial Theory, Series A 174 (2020) 105190

[87] E. Naslund, Lower bounds for the Shannon Capacity of Hypergraphs, manuscript (2024)

[88] E. Naslund and W. Sawin, Upper bounds for sunflower-free sets, Forum Math. Sigma 5 (2017) e15

[89] L. Newcombe, MSc Thesis, Royal Holloway (2008)

[90] J. Nagy and P. P. Pach, The Alon-Jaeger-Tarsi conjecture via group ring identities, Journal of the Eur. Math. Soc., to appear

[91] J. Nagy, P. P. Pach, I. Tomon, Additive bases, coset covers, and non-vanishing linear maps, arXiv:2111.13658

[92] P. P. Pach, Monochromatic solutions to the equation $x+y=z^2$ in the interval $[N, cN^4]$, Bulletin of the London Mathematical Society 50 (6) (2018) 1113–1116.

[93] P. P. Pach: Bounds on the size of progression-free sets in $\mathbb{Z}_m^n$, Unif. Distrib. Theory 17 (2022) no.1, 1–10.

[94] P. P. Pach and R. Palincza, Sets avoiding six-term arithmetic progressions in $\mathbb{Z}_6^n$ are exponentially small, SIAM Journal on Discrete Mathematics 36 (2) (2022) 1135–1142.

[95] S. Peluse, Finite field models in arithmetic combinatorics – twenty years on, arXiv:2312.08100

[96] F. Petrov, Combinatorial Results Implied by Many Zero Divisors in a Group Ring, Funct. Analy. Appl. 58 (2024) 80–89.

[97] F. Petrov and C. Pohoata, Improved Bounds for Progression-Free Sets in C_8^n, Israel J. Math. 236 (2020) no. 1, 345–363.

[98] D. H. J. Polymath, Density Hales-Jewett and Moser numbers, in: An irregular mind, 689–753, Bolyai Soc. Math. Stud. 21 János Bolyai Math. Soc., Budapest (2010)

[99] C. Pohoata, O. Roche-Newton, Four-term progression free sets with three-term progressions in all large subsets, Random Structure & Algorithms 60 (4) (2022) 749–770.

[100] A. Potechin, Maximal caps in $AG(6,3)$. Des. Codes Cryptogr. 46 (2008) no. 3, 243–259.

[101] R. A. Rankin, Representations of a number as the sum of a large number of squares. Proc. Roy. Soc. Edinburgh Sect. A 65 1960/1961, 318–331.

[102] D. K. Ray-Chaudhuri and R. M. Wilson, On t-designs, Osaka J. Math. 12 (1975) 737–744.

[103] C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, The Ramanujan Journal 13 (2007) 333–337.

[104] J. Riddel, A lattice point problem related to sets containing no ℓ-term arithmetic progression, Canad Math. Bull. 14 (1971) 535–538.

[105] B. Romera-Paredes, M. Barekatain, A. Novikov, M. Balog, M. Kumar, E. Dupont, F. Ruiz, J. Ellenberg, P. Wang, O. Fawzi, P. Kohli, A. Fawzi, Mathematical discoveries from program search with large language models, Nature 625 (2023) 468–475.

[106] K. F. Roth, On certain sets of integers, J. Lond. Math. Soc. (2) 28 (1) (1953) 104–109.

[107] V. Rödl, On a Packing and Covering Problem, European Journal of Combinatorics 6 (1) (1985) 69–78.

[108] R. Salem and D. C. Spencer, On sets of integers which contain no three terms in arithmetical progression, Proc. Nat. Acad. Sci. U. S. A. 28 (1942) 561–563.

[109] T. Sanders, Roth's theorem in $\mathbb{Z}_4^n$. Anal. PDE 2 (2009) no. 2, 211–234.

[110] T. Sanders, On Roth's theorem on progressions, Ann. of Math. (2) 174 (1) (2011) 619–636.

[111] T. Sanders, On certain other sets of integers, J. Anal. Math. 116 (2012) 53–82.

[112] W. Sawin and T. Tao, Notes on the slice rank of tensors, https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors/ (2016)

[113] C. E. Shannon, The zero-Error capacity of a noisy channel, IRE Trans. Inform. Theory. 2. (1956) 8–19.

[114] D. Speyer, https://sbseminar.wordpress.com/2016/07/08/bounds-for-sum-free-sets-inprime-power-cyclic-groups-three-ways/

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

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

[117] P. Sziklai, Nuclei of pointsets in $PG(n, q)$, In: vol. 174. 1-3. Combinatorics (Rome and Montesilvano, 1994) (1997) 323–327.

[118] T. Tao, Webblog, 23rd February 2007
http://terrytao.wordpress.com/2007/02/23/open-question-best-bounds-for-cap-sets/
Open question: best bounds for cap sets

[119] T. Tao, A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound,
https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound (2016)

[120] T. Tao and V. Vu, Additive Combinatorics, Cambridge University Press (2006)

[121] F. Tyrrell, New lower bounds for cap sets, Discrete Anal. (2023) Paper No. 20, 18pp.

[122] V. Vassilevska Williams, Multiplying matrices faster than Coppersmith-Winograd, STOC'12–Proceedings of the 2012 ACM Symposium on Theory of Computing, 887–898, ACM, New York (2012)

[123] J. Wolf, Finite field models in arithmetic combinatorics–ten years on, Finite Fields Appl. 32 (2015) 233–274.

[124] D. Zare, https://mathoverflow.net/q/ 229442