Designs, Codes and Cryptography (2020) 88:2133–2170
https://doi.org/10.1007/s10623-020-00769-0

Caps and progression-free sets in $\mathbb{Z}_m^n$

Christian Elsholtz[1] · **Péter Pál Pach**[2]

Received: 21 July 2019 / Revised: 5 March 2020 / Accepted: 29 May 2020 / Published online: 16 June 2020

Abstract
We study progression-free sets in the abelian groups $G = (\mathbb{Z}_m^n, +)$. Let $r_k(\mathbb{Z}_m^n)$ denote the maximal size of a set $S \subset \mathbb{Z}_m^n$ that does not contain a proper arithmetic progression of length k. We give lower bound constructions, which e.g. include that $r_3(\mathbb{Z}_m^n) \geq C_m \frac{((m+2)/2)^n}{\sqrt{n}}$, when m is even. When $m = 4$ this is of order at least $3^n/\sqrt{n} \gg |G|^{0.7924}$. Moreover, if the progression-free set $S \subset \mathbb{Z}_4^n$ satisfies a technical condition, which dominates the problem at least in low dimension, then $|S| \leq 3^n$ holds. We present a number of new methods which cover lower bounds for several infinite families of parameters m, k, n, which includes for example: $r_6(\mathbb{Z}_{125}^n) \geq (85 - o(1))^n$. For $r_3(\mathbb{Z}_4^n)$ we determine the exact values, when $n \leq 5$, e.g. $r_3(\mathbb{Z}_4^5) = 124$, and for $r_4(\mathbb{Z}_4^n)$ we determine the exact values, when $n \leq 4$, e.g. $r_4(\mathbb{Z}_4^4) = 128$. With regard to affine caps, i.e. sets without 3 points on a line, the new methods asymptotically improve the known lower bounds, when $m = 4$ and $m = 5$: in $\mathbb{Z}_4^n$ from 2.519^n to $(3 - o(1))^n$, and when $m = 5$ from 2.942^n to $(3 - o(1))^n$. This last improvement modulo 5 appears to be the first asymptotic improvement of any cap in $AG(n, m)$, when $m \geq 5$ over a tensor lifting from dimension 6 (see Edel, in Des Codes Crytogr 31:5–14, 2004).

Keywords Permutation polynomial · Triple-cycle permutation · Finite field; Block cipher

Mathematics Subject Classification 06E30 · 14G50 · 94A60

Communicated by J. Bierbrauer.

✉ Christian Elsholtz
elsholtz@math.tugraz.at

Péter Pál Pach
ppp@cs.bme.hu

[1] Institute of Analysis and Number Theory, Graz University of Technology, Kopernikusgasse 24/II, 8010 Graz, Austria

[2] MTA-BME Lendület Arithmetic Combinatorics Research Group, Department of Computer Science and Information Theory, Budapest University of Technology and Economics, Magyar tudósok körútja 2, Budapest 1117, Hungary

1 Introduction

There has been great interest in finding progression-free sets in $\mathbb{Z}_m^n := (\mathbb{Z}/(m\mathbb{Z}))^n$, especially when $m = 3$ or 4. 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 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, and hardly any explicit values of the maximal size of such sets is known.[1]

This paper intends to fill this gap and provides several new techniques to find lower bounds, and even to find exact values in the case $m = 4$, which are comparable in size to the known values for $m = 3$.

However, before we come to this, we briefly summarize a number of related questions. The problem of finding sets $S \subset \mathbb{Z}_m^n$ with, or without, a given property has been investigated frequently. Often one is actually interested in the maximal size of $|S|$. Also, often 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 [28] 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, Roth, Salem and Spencer, Sanders, Szemerédi, Tao [5,7,31,33,50,51,53,55]. In particular, the proof of $r_k(N) = o(N)$, as N tends to infinity, and quantitative versions thereof, proved 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 [14,58].
The question of arithmetic progressions has also been studied modulo m, see e.g. Croot [15]. 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 paper, however, we study "proper arithmetic progressions" meaning that all elements in the progression are *distinct*, unless otherwise stated.

(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 [29], 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 [48]. The multidimensional case with $n \geq 3$ is widely open, even though there are lower bounds by Edel, Elsholtz et al. [19,22,25], and upper bounds by Alon and Dubiner [2], Naslund [42] and Hegedüs [35].

(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 $|S| \leq \lfloor \frac{m}{2} \rfloor + 1$, if all x_i are distinct, or $|S| \leq \lfloor \frac{m+1}{2} \rfloor$ if $x_1 = x_2$ is allowed. In the case modulo

[1] There is certainly an extensive literature in the related area of finite geometry over finite fields, but in literature from an additive combinatorics 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.

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 results by Cameron [10], Elsholtz and Rackham [26].

(3) The case of no geometric line (of m points) in the integer grid $\{1, \ldots, m\}^n$ is known as Moser's cube problem, see [41,45]. Closely related is the question of finding the maximal number of lattice points in the same cube $\{1, \ldots, m\}^n$, but without any combinatorial line. The famous upper bound by Hales-Jewett [34] of $o(m^n)$ points, when m is fixed and n tends to infinity, became very influential.

In this paper we concentrate on sets $S \subset \mathbb{Z}_m^n$ 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 $x_i - 2x_{i+1} + x_{i+2} = 0$, $i = 1, \ldots, k-2$.

The multidimensional case of no 3 points in arithmetic progression has frequently been studied, especially modulo $m = 3$. 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 $1 \equiv -2 \bmod 3$. The problem is known as the "cap set problem". There were important contributions by Brown and Buhler [8], Frankl, Graham and Rödl [30], Meshulam [40], Lev [38], Bateman and Katz [4], Croot et al. [16], Ellenberg and Gijswijt [24].

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 [1,2,18,32,36,56]) until the solution by Croot et al. [16] (when $m = 4$), and finally Ellenberg and Gijswijt [24].

Meshulam's [40] 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 [38] to even values $m \geq 4$. Improving this, Sanders [52] 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 [33] write that $c = 2^{-22}$ is admissible. Introducing an entirely new approach, based on the polynomial method rather than Fourier techniques, Croot et al. [16] proved that

$$r_3(\mathbb{Z}_4^n) \leq 4^{\gamma n} = 3.61\ldots^n,$$

where $\gamma \approx 0.926$. The new methods introduced in [16] also led to the result in the case $r_3(\mathbb{Z}_3^n) \leq 2.756^n$ by Ellenberg and Gijswijt [24]. Again, the case of cap sets has applications to the complexity of matrix multiplication, see [3,6].

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 (see [18] for the history and current record) that there is a set S with $|S| > 2.217389^n = |G|^\beta$ with $\beta = \frac{\log 2.217389}{\log 3} \approx 0.724851$). The currently strongest lower bound example comes from a product construction, based on an example in dimension 480.

For a lower bound when $m = 4$ Sanders [52] proved: there exists $S \subset G = (\mathbb{Z}_4^n, +)$ 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 $\sqrt[3]{16} = 2.519\ldots$.)

The following is known:

$$2.21738\ldots^n \ll r_3(\mathbb{Z}_3^n) \le 2.755\ldots^n, [19, 24]$$
$$2.519\ldots^n \ll r_3(\mathbb{Z}_4^n) \le 3.61\ldots^n, [52, 16],$$

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

$$r_3(\mathbb{Z}_p^n) \le (p - \delta_p)^n, [24].$$

Indeed the argument yields the bound

$$r_3(\mathbb{Z}_p^n) \le (J(p)p)^n, [6]$$

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 [6]).

Remark 1.1 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. [6,44]).

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

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 [16], since $r_3(\mathbb{Z}_m^n) \le (m/4)^n r_3(\mathbb{Z}_4)^n \le (0.91m)^n$.

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

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

The author of the 6-dimensional result (Potechin [46]), and the authors of the *classification* of the unique 5-dimensional maximum cap [21], (required for the 6-dimensional case by Potechin) mentioned they used computer calculations. Y. Edel informed us that for the paper [21] the computation time was a few weeks.

The remaining part of the paper is organized as follows: After some necessary notation and describing the results we first prove the asymptotic lower bounds in Sect. 4, as these proofs are shorter. In Sect. 5 we give a reformulation for the problem of finding $r_3(\mathbb{Z}_4^n)$ and $r_4(\mathbb{Z}_4^n)$. In Sect. 3.1 we give a lower bound for $r_3(\mathbb{Z}_4^n)$, we then prove that this construction gives the exact values up to dimension 5 (Sects. 6 and 7), which require some detailed case studies. Finally, in Sect. 8 we prove the exact values for $r_4(\mathbb{Z}_4^n)$ up to dimension 4.

2 Notation

We use the Landau O and o-notation such as $f(n) = O_t(g(n))$, where the O-constant depends at most on a parameter t. We also use the Vinogradov notation, where $f(n) \ll_t g(n)$ or $g(n) \gg_t f(n)$ has the same meaning as the O-expression above.

We use the standard coding notation $A(n, d)$ on the maximal size of a binary code of words of length n and minimum distance d.

In Sections 6, 7, 8 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 $v_1, \ldots, v_k$ will be denoted by $\langle v_1, \ldots, v_k \rangle$.

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 $v_1, \ldots, v_k$ will be denoted by $\langle v_1, \ldots, v_k \rangle_{aff}$.

Throughout the paper for a subset $A \subseteq \mathbb{F}_2^n$ 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.

3 Results and methods

3.1 Progression-free sets

Theorem 3.1 *For sets without arithmetic progression of length* 3 *we have the following results:*

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

We give quite uniform proofs for all these dimensions. The value $r_3(\mathbb{Z}_4^3) = 16$ was stated before by Sanders [52] (and was indeed a computer calculation by O. Sisask), and the value $r_3(\mathbb{Z}_4^4) = 42$ was determined in a Masters' Thesis by Lawrence Newcombe [43] (a student of the first author). From that proof it was already apparent that $r_3(\mathbb{Z}_4^n)$ could be much smaller than 4^n, due to a $\mathbb{Z}_2^n$-substructure of $\mathbb{Z}_4^n$, but proceeding to higher dimension might have been very tedious.

Next we give a 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 are 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/

Theorem 3.2 *For* $n > 1$ *we have* $r_3(\mathbb{Z}_4^n) \geq \max_{0 \leq t \leq n} \sum_{i=t+1}^{n} \binom{n}{i} A(i, i-t)$.

Proof of Theorem 3.2 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 $i \in [1, n]$ 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 $d(a, c) \leq |T(a) \backslash T(b)| = |T(a)| - |T(b)| \leq |T(a)| - t$, 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 $S = \cup_{|T| \geq t} A_T$ gives the stated lower bound. □

As a consequence of this result one can prove a quite good lower bound.

Corollary 3.3

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

which implies that there exists a progression-free set $S \subset \mathbb{Z}_4^n$ *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 0.724851 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 we find 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 3.2.

Proof of Corollary (Proof 1) Calculations show that the optimal choice for t in Theorem 3.2 satisfies $t \sim 2n/3$. In particular, for $2 \le n \le 10$ 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 [12]). □

The proof of Theorem 3.2 and Corollary 3.3 above may appear a bit formal. In Section 4 we explain in detail the geometric motivation of a direct proof of Corollary 3.3, 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.

Corollary 3.4

$$2 \le r_3(\mathbb{Z}_4^1), \quad 6 \le r_3(\mathbb{Z}_4^2), \quad 16 \le r_3(\mathbb{Z}_4^3), \quad 42 \le r_3(\mathbb{Z}_4^4), \quad 124 \le r_3(\mathbb{Z}_4^5),$$
$$344 \le r_3(\mathbb{Z}_4^6), \quad 960 \le r_3(\mathbb{Z}_4^7), \quad 2832 \le r_3(\mathbb{Z}_4^8), \quad 7880 \le r_3(\mathbb{Z}_4^9), \quad 22232 \le r_3(\mathbb{Z}_4^{10}).$$

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 3.1. When $n = 8$, choose $t = 4$.

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

Theorem 3.5 *For sets without arithmetic progression of length* 4 *we have the following results:*

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

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 [22] in the similar setting of zero-sum free sets.

Lemma 3.6 *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.*

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

(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 3.7

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

The first result is considerably weaker than Corollary 3.3, 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 $\frac{3^n}{\sqrt{n}}$. But 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 make use of "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 [18].

These proofs describe a set explicitly in terms of its coordinate entries, similar to the constructions by Salem and Spencer [51], and Behrend [5]. Salem and Spencer constructed progression-free sets in the integers by representing integers in an m-ary digit system, m odd, and using the digits $0 \leq a_i \leq (m-1)/2$ 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 $0 \leq a_i \leq (m-1)/2$, 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 3.8 *Let $q \geq k \geq 3$ 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 3.11 and 3.12 that $\lceil \frac{m+1}{2} \rceil \le \alpha_{k,m} \le m$. For $k = 3$ more is known, see Sect. 1: $\alpha_{3,p} \le J(p)p$, when $m = p$ is an odd prime, and where $J(p)$ was defined by (1). We state a more general conjecture:

Conjecture 3.9 *By the proposition above and the theorems below we know: for each $k \ge 3$ and each prime $p \ge k$ there exists a constant $\alpha_{k,p}$, which is certainly in $(\frac{p}{2}, p]$, such that $r_k(\mathbb{Z}_p^n) = (\alpha_{k,p} + o(1))^n$ holds, as n tends to infinity.*

We conjecture that the following limit $\alpha_k := \lim_{p\to\infty} \frac{\alpha_{k,p}}{p}$ exists, and thus is in $[\frac{1}{2}, 1]$. (If $k \ge 4$ the bound $\alpha_k < 1$ would mean that an exponential saving for the upper bound holds, as is the case with $k = 3$.)

In view of the above results, and also in view of an upper bound in a relevant case, see Theorem 3.18, we state the following conjecture:

Conjecture 3.10

$$r_3(\mathbb{Z}_4^n) = (3 - o(1))^n, \text{ i.e. } \alpha_{3,4} = 3.$$

Tao and Vu [57, exercise 10.1.3] observe that there is a construction in $\mathbb{Z}_m^n$ with at least $\frac{\lfloor m/2 \rfloor^n}{m^2 n^2}$ points without 3-progression (based on Behrend's construction).[2]

Lin and Wolf [39] proved the following: If m is a prime and $k \le m$

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

Their proof makes use of a product construction, as explained in Lemma 3.6. 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 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 $\lfloor \frac{m+2}{2} \rfloor$ here.

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

Theorem 3.11 *Let $m \ge 5$ be odd. There exists some $C_m > 0$ such that*

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

Moreover, with $\sigma_m = \sqrt{\frac{1}{2880}\left(m^4 + 4m^3 - 14m^2 - 36m + 45\right)}$ the value $C_m = \frac{1}{3\sqrt{3}\,\sigma_m}$ is admissible. For increasing odd m asymptotically $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}\,m^2}$ holds.

The case $m = 5$ also improves the asymptotic lower bound of affine caps, for details see Sect. 3.2 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 $r_k(\mathbb{Z}_m^n) \ge r_3(\mathbb{Z}_m^n)$ the theorem trivially induces lower bounds for any $k \ge 3$ (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 [57, 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.

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

Theorem 3.12 *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 that $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}\,m^2}$.

(A version of this result, in the special case $m = 8$ has also been observed in [44], having seen a precursor of this manuscript. 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 3.13 *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 [39] 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 3.14 *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 3.15 *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 3.16 *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 3.12 for $m = 8, k = 3$ one can use 5 digits, rather than 4.

Corollary 3.17 *There exist positive constants C_m and $c_m \leq m/2$ such that the following holds:*

$$r_{p+1}(\mathbb{Z}_{p^3}^n) \geq C_{p+1} \frac{(p^3 - 2p^2 + 2p)^n}{n^{c_{p+1}}}.$$

$$r_4(\mathbb{Z}_{27}^n) \geq C_{27} \frac{15^n}{n^{c_{27}}}.$$

$$r_{82}(\mathbb{Z}_{729}^n) \geq C_{729} \frac{717^n}{n^{c_{729}}}.$$

$$r_6(\mathbb{Z}_{125}^n) \geq C_{125} \frac{85^n}{n^{c_{125}}}$$

$$r_{26}(\mathbb{Z}_{625}^n) \geq C_{625} \frac{585^n}{n^{c_{625}}}.$$

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 estimations of $r_3(\mathbb{Z}_4^n)$ we shall need a reformulation of the problem which is presented in Section 5. 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:

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

(Note that for $A(x) = \emptyset$ we define $x + A(x) \hat{+} A(x) := \emptyset$.) In Lemma 5.1 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 $r_3(\mathbb{Z}_4^n) \gg 3^n/\sqrt{n}$. This is the heuristic reason why we state Conjecture 3.10.

Theorem 3.18 *If the system of subsets $A(x)$ satisfies $(*)$ and all non-empty subsets $A(x)$ are subspaces, then $\sum_{x \in \mathbb{F}_2^n} |A(x)| \leq 3^n$.*

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 3.19 *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 $x \in \mathbb{Z}_2^n$.*

3.2 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 we 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 [20].
$n = 5, m = 5$ one has at least 195 points.[3]
$n = 6$: one has at least $m^4 + m^2 - 1$ points, see Edel [18].

For large dimensions, the best lower bound constructions are due to Edel [18] 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 [39]), 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 ([18]) 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 0.724851 (see [18]). The progress over the previous record 0.7218 (see [9]) 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 3.11 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 the construction modulo 5, similar to the case $m = 4$ in Theorem 3.2. 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, and 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 dimension.

[3] 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

4 Proofs of the asymptotic lower bounds

We will use several times that the central multinomial coefficients can be approximated by Stirling's formula:

Lemma 4.1 *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 3.3.

Proof of Corollary 3.3 (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 Moser [41]. 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 [13]), $f(4) = 43$ (see [11]), $f(5) = 124$, $f(6) = 353$ [45]. 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 [37] shows that $f(n) \gg \frac{3^n}{\sqrt{n}}$, and the implicit constant was refined again by Chvátal [12]. The construction by Chvátal relates the problem to coding theory and gives $f(5) \geq 124$, for example.

Let us adapt Komlós' [37] 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.

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

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

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), one would need, in each coordinate, that
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 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 ones, unless all three entries are identically 1. This means that all three points have their ones 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, a contradiction to the definition of a proper progression. □

Proof of Proposition 3.8 The idea of this proof might go back to Shannon [54], see also Davis and Maclagan [17]. Let $\alpha_{k,m}(n) = \left(r_k(\mathbb{Z}_m^n)\right)^{1/n}$, so that we have the following properties: By the product construction (Lemma 3.6) we have

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

i.e. $\alpha_{k,m}(n_1)^{n_1} \alpha_{k,m}(n_2)^{n_2} \leq \alpha_{k,m}(n_1+n_2)^{n_1+n_2}$ and therefore

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

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 3.11: We first prove a slightly weaker result based on the Salem-Spencer construction [51] for sets of integers without arithmetic 3-progression. 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 $n_i = \frac{n}{\frac{m+1}{2}}$ 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, c_m. If n is not a multiple of $(m+1)/2$ one can fill the remaining coordinates with entries $0 \leq a_i < k$, 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. One then continues: 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 3 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, 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 that 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 larger by a factor n^c only.

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

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

Here S_R can be thought of as a sphere about centre $((m-1)/4, \ldots, (m-1)/4))$ 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 $\sum_{i=1}^{n}(a_i - d_i - \frac{m-1}{4})^2 = \sum_{i=1}^{n}(a_i - \frac{m-1}{4})^2 = \sum_{i=1}^{n}(a_i + d_i - \frac{m-1}{4})^2$. 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 gives $\sum_{i=1}^{n} 2d_i^2 = 0$. 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 $(a_1, \ldots, a_n) \in [0, \frac{m-1}{2}]^n$ 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 [23] and consider $a_i - \frac{m-1}{4}$ as independent random variables $Y_1, \ldots, Y_n$, distributed uniformly in $\{-(m-1)/4, \ldots, (m-1)/4\}$, and $Z_i = Y_i^2$, $Z = \sum_{i=1}^{n} Z_i$, $i \in \{1, \ldots, n\}$. 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

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

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

and $Var(Z) = nVar(Z_i)$. The standard deviation is $\sigma_m = \sqrt{Var(Z_i)}$ and $\sigma_Z = \sqrt{Var(Z)} = \sigma_m\sqrt{n}$, 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 $[0, \frac{m-1}{2}]^n$ 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 $m \geq 5$ 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 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 slowly, as one would need to search for a good value R. However, a result of Rankin [47] 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 [23], 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 3.12: 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 $n_i = \frac{n}{\frac{m+2}{2}}$ for every i. This gives at least $(\frac{m+2}{2})^n \frac{C'_m}{n^{cm}}$ 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 the same number of progressions of type $0\frac{m}{2}0$ and $\frac{m}{2}0\frac{m}{2}$. Hence other nontrivial progressions using 0, or $\frac{m}{2}$, 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 concludes 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 non-constant 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 let 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 $n_1\frac{m^2}{16} + n_2\frac{m^2}{16} + \sum_i n_i(p_i - d_i - \frac{m}{4})^2 = n_1\frac{m^2}{16} + n_2\frac{m^2}{16} + \sum_i n_i(p_i - \frac{m}{4})^2 = n_1\frac{m^2}{16} + n_2\frac{m^2}{16} + \sum_i n_i(p_i + d_i - \frac{m}{4})^2$. 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 gives $\sum_{i=3}^{s} n_i 2d_i^2 = 0$. Hence for all non-constant 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 $Z_i = Y_i^2$, $Z = \sum_{i=1}^{n} Z_i$, $i \in \{1, \ldots, n\}$. 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

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

and $Var(Z) = nVar(Z_i)$. The standard deviation is $\sigma_m = \sqrt{Var(Z_i)}$ and $\sigma_Z = \sqrt{Var(Z)} = \sigma_m\sqrt{n}$, 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 3.13 Let n be a multiple of 7 and let $D = \{0, 1, 2, 3, 4, 5, 6\}$. 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:

$$\begin{cases} 0000, 1111, 2222, 3333, 4444, 5555, 6666 \\ 01\underline{2}3, 0246, 12\underline{3}4, 16\underline{0}5, \underline{2}345, 3456, 32\underline{1}0, \underline{4}321, 50\underline{6}1, 543\underline{2}, 6420, 6543 \end{cases}$$

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. As the digit 0 occurs in all 4 positions with the same frequency, and applying it 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:

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

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

$$\begin{aligned} d(0246) &= d(1234) = d(2345) = d(3456) = d(4321) \\ &= d(5432) = d(6420) = d(6543) = 0. \end{aligned}$$

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 weakens the overall lower bound by a small factor. □

Proof of Theorem 3.14 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 element 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 $-1 \bmod p^{s-1}$. We observe that no such k-progression can

start with $p^{s-1}-1$, as it would have to end at *another* element -1 mod 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

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

The number $|S|$ of elements is the multinomial coefficient $\binom{n}{n/|D|,\dots,n/|D|} \sim C_m \frac{|D|^n}{n^{(|D|-1)/2}}$ according to Lemma 4.1. 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 3.16 Recall that $m = p^s, s \geq 3, k = p^{s-2}+1$. Let $D_1 = \left\{p^{s-2}i : i = 0, \dots, p^2-1\right\}$,

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

and $D_3 = \{0, 1, 2, , \dots, p-1\}$. 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 mod 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

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

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. □

5 Subset reformulation

In this section we give a "subset formulation" for the question of determining $r_3(\mathbb{Z}_4^n)$ and $r_4(\mathbb{Z}_4^n)$. As an application of the former one, we give another proof for Corollary 3.3, then we prove Theorem 3.18.

5.1 Reformulation for 3AP-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:

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

(Note that for $A(x) = \emptyset$ we define $x + A(x)\hat{+}A(x) := \emptyset$.) 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 5.1 (below) shows that property $(*)$ nicely captures the condition that the "corresponding" $A \subseteq \mathbb{Z}_4^n$ is 3AP-free.

Lemma 5.1 *For every $n \geq 1$ we have $r_3(\mathbb{Z}_4^n) = r_3'(n)$.*

Proof Let $F = \{0, 2\}^n \leq \mathbb{Z}_4^n$ 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 $A(y) \neq \emptyset$. 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 $(*)$. □

5.2 3AP-free sets: lower bound and subspace version

In this subsection, first, as an illustration, we give an alternative – different from the proof presented in Section 4 – proof (using the subset reformulation) for Corollary 3.3, then we prove Theorem 3.18.

Alternative proof of Corollary 3.3 For $x \in \mathbb{F}_2^n$ let $\mathrm{supp}(x) = \{i : x_i \neq 0\}$. Let us fix some $r \in \{0, 1, \ldots, n\}$. Let $A(x) = \{v : \mathrm{supp}(v) \subseteq \mathrm{supp}(x)\}$ if $|\mathrm{supp}(x)| = r$ and $A(x) = \emptyset$ 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 $A(y) = \emptyset$.

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 3.18 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 $x^{(1)}, \ldots, x^{(k)}$ 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 $(x_1, x_2, \ldots, x_t) \in \mathbb{F}_2^{nt}$ let $A((x_1, x_2, \ldots, x_t)) = A(x_1) \times A(x_2) \times \cdots \times A(x_t)$. 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, $S^t \leq 6 \cdot 3^{nt}$, thus $S \leq 6^{1/t}3^n$. This holds for every t, so the statement is proven. □

5.3 Reformulation 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 $A(x) = \emptyset$ we define $A(x) + A(x) := \emptyset$.) Let $r_4'(n)$ 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 $(**)$.

Lemma 5.2 *For every $n \geq 1$ we have $r_4(\mathbb{Z}_4^n) = r_4'(n)$.*

Proof Similarly to the proof of Lemma 5.1 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 progression-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 $(**)$. □

6 3AP-free subsets of $\mathbb{Z}_4^n$, if $n \leq 4$

Now, we are ready to prove Theorem 3.1. In this section we give a proof for $n \leq 4$, the case $n = 5$ is covered in the next section.

Before starting the proof we give a brief outline of the main strategy. 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 sets with a small doubling. 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 $n \leq 5$) 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 both handling the all-subspace problem is getting more difficult. The 5-dimensional case is considerably more difficult than the previous cases, the proof of it is presented in the next section. Now, we continue with the proof of the cases $1 \leq n \leq 4$.

Proof of Theorem 3.1 in the cases $n \leq 4$. According to Lemma 5.1 and Corollary 3.4 it suffices to show that $r_3'(1) \leq 2, r_3'(2) \leq 6, r_3'(3) \leq 16, r_3'(4) \leq 42$.

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 $(x + A(x)) \cap (y + A(x)) \neq \emptyset$, 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 $S = |A(x)| \leq 2^n$. Hence, in this case the statement holds.

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

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 $A(x) = \langle u, v\rangle$ 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, $k \le \binom{l}{3}$. We have $S \le 4k+2(8-k-l) = 16+2k-2l \le 16+2\binom{l}{3}-2l \le 16$, if $l \le 4$, equality holds if and only if $l = 4$. If $5 \le l$, then $S \le 3 \cdot 4 = 12$. Therefore, $S \le 16$ is shown and the maximum occurs when $k = l = 4$.

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 we will also 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 $0 \ne g \in (A(x) \cap A'(x)) \setminus \{f_1, f_2, f_3\}$, 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 $k \leq \binom{l}{3}$.

Hence, $S \leq 4k + 2(16 - k - l) = 32 + 2k - 2l \leq 32 + 2\binom{l}{3} - 2l$. If $l \leq 4$, then this yields $S \leq 32$. Moreover, for $l = 5$ we obtain that $S \leq 42$. If $l \geq 6$, 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 $U \cap V = \emptyset$, then $U \cup V = \mathbb{F}_2^4$ and $A(x) = \emptyset$ 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 3.19 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, $A(x_0) = \emptyset$, then for any $x \neq x_0$ the set $A(x)$ must contain two elements whose difference is x. Two such configurations always can 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 $A(x_1) = A(x_2) = A(x_3) = A(x_4) = \emptyset$. We claim that x_1, x_2, x_3, x_4 are affine independent. Otherwise they form an affin 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 these 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 $k = 10, l = 5$.

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 $A(0) = A(e_1) = A(e_2) = A(e_3) = A(e_4) = \emptyset$, 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 might 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. □

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 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:

(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 $S = \sum |A(y)| \leq 16k + 10(11 - k) = 110 + 6k$. If $k \leq 2$, 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 $K \cap L = \emptyset$, then $K \cup L = \mathbb{F}_2^5$, giving that $A(t) = \emptyset$ for every $t \notin \{y, z\}$, which is a contradiction. So any two of them intersect nontrivially each other, and then any pairwise intersection is a 3-dimensional affine subspace. As $y \notin L \cup M$, we have that $(K \cap L) \cap (K \cap M) \neq \emptyset$, since both of them is an 8-element subset of the 15-element set $K \setminus \{y\}$, hence $K \cap L \cap M \neq \emptyset$. Then $K \cap L \cap M$ has size 4 or 8. By inclusion-exclusion principle, in both cases $|K \cup L \cup M| = |K| + |L| + |M| - |K \cap L| - |K \cap M| - |L \cap M| + |K \cap L \cap M| \geq 28$, therefore, 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 $|K \cap L| \le 4$, we have $|K \cup L| \ge 16 + 8 - 4 = 20$, so there are at least $20 - 2 = 18$ empty subsets, thus at most 14 non-empty ones implying $S \le 16 + 13 \cdot 8 = 120$, 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 $0 < |A(x)| \le 4$, 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 $S \le 8 \cdot 15 = 120$, so it can be assumed that at most 16 subsets are empty.

If there is no subset with size larger than 2, then $S \le 64$. 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 $S \le 29 \cdot 4 = 116$. 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 $A(e_i) = \emptyset$, $A(e_i + e_j) = \emptyset$ for every $i \ne j$. 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 $A(0) \ne \emptyset$, we have $0 \notin K$. We claim that $K \setminus \{x\} \not\subseteq T$.

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 $A(y) = \emptyset$, so the number of the empty subsets is at least 16. If the number of 3-subspaces is at most 14, then $S \le 14 \cdot 8 + 2 \cdot 6 = 124$, 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 $A(i_1 i_2 \dots i_l)$ for $A(e_{i_1} + e_{i_2} + \cdots + e_{i_l})$ if

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

(E.g. $A(1) = A(e_1)$, $A(123) = A(e_1 + e_2 + e_3)$, 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 $8k+5(16-k-l) \geq 88$, and then

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

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,

$$\binom{l}{3} \geq k. \tag{4}$$

By (3) and (4) we obtain that $l(l-1)(l-2)/2 \geq 5l+8$, which yields $l \geq 6$. Then (3) 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 $e_1+e_2+e_3+e_4$. Since, 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, 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: $l \geq 4$. Note that that the sum of the four corresponding vectors is 0. Also, note that in this case (similarly to (3) in the previous case) we shall assume that

$$3k \geq 5l. \tag{5}$$

Now (5) yields that at least 7 such subsets are 3-subspaces: $k \geq 7$. Then (4) implies that the number of empty ones is at least 5. Again, by (5) we get $k \geq 9$. If $l = 5$, 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: $l \geq 6$, and by (5) 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, since 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", 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 $1 \le k$ 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 $A(x) = \emptyset$ 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 $125 \le S$, then $125 \le 8k + (32 - k - l)4$ which yields $l \le k$. Now we are going to show that $l \ge 13$. 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 $l < 13$, 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 $16 - 3 = 13 \le l$, contradiction.

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

$$7l + \frac{28l}{2} \le 7k + \frac{28k}{2} \le \binom{l}{3},$$

thus

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

implying that $l \ge 13$.

Therefore, $k \ge l \ge 13$, 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 $\tilde{A}(x) = L \cup (L + x)$, $\tilde{A}(y) = L \cup (L + y)$, $\tilde{A}(z) = L \cup (L + z)$.

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 has 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 7 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 $k \leq 11$, contradiction. Hence, there is at most one L-translate without any red vector. In particular, this means that $l \geq 16$, since there are 13 red vectors in M and at least 3 red vectors outside of M.

Thus $k = l = 16$. 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, $A(v_1 + v_2 + v_3)$), 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 $13 \leq l \leq k$ 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

$$35k \leq \binom{l}{3} + 4N, \tag{6}$$

since each of the k 3-subspaces contain 35 empty triples. Hence, for $l < 16$ 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 $l = 13$, 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 $32 - 13 - 8 = 11$, contradiction.

Subcase 2. If $l = 14$, 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 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 $k \leq 4 + 6 + 2 = 12$, contradiction.

Subcase 3. Let us assume that $l = 15$. 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 $L_4, \ldots, L_8$ 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, contradiction. So without the loss of generality it can be assumed that either (i) L_4 contains two red vectors and L_5, L_6, L_7 contain one-one red vector: v_i in L_i $(5 \leq i \leq 7)$ or (ii) $L_4, \ldots, L_8$ contain one-one red vector: v_i in L_i $(4 \leq i \leq 8)$.

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 $k \le 2+6+5 = 13$, 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, $k \le 2 + 6 + 3 = 11$, a contradiction.

Subcase 4. Finally, let us assume that $l = k = 16$, 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

$$|S_1 \cup S_2 \cup S_3 \cup S_4| \ge \sum |S_i| - \sum |S_i \cap S_j| \ge 4 \cdot 8 - 6 \cdot 2 = 20, \tag{7}$$

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 (7), 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, $v_5 + v_6 + v_7$), 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 $l_1 = 0, l_2 = e_3, l_3 = e_4, l_4 = e_3 + e_4, l_5 = e_5, l_6 = e_3 + e_5, l_7 = e_4 + e_5, l_8 = e_3 + e_4 + e_5$ and $L = \langle e_1, e_2 \rangle$. For every $1 \leq i \leq 8$ let $L_i = L + l_i$. We can assume that L_1 contains 4 red vectors and L_2, L_3 contains 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, 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 $l_i + t_i$ for $i \in \{4, 6, 7, 8\}$.

Let $i \in \{6, 7, 8\}$. We claim that $\tilde{A}(l_i + t_i + e_2)$ and $\tilde{A}(l_i + t_i + e_1 + e_2)$ must be of type-1. Otherwise, $\tilde{A}(l_i + t_i + e_2)$ or $\tilde{A}(l_i + t_i + e_1 + e_2)$ 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 $l_i + t_i + e_1$ would also lie in the 3-subspace (to get parallel pairs from the different translates), a contradiction. Hence, $\tilde{A}(l_i + t_i + e_2)$ and $\tilde{A}(l_i + t_i + e_1 + e_2)$ are of type-1.

Consider $\tilde{A}(l_6 + t_6 + e_2)$ and $\tilde{A}(l_6 + t_6 + e_1 + e_2)$. Each of these two subspaces contain either e_5 or $e_5 + e_1$ and they contain $l_7 + t_7$ and $l_8 + t_8$. As the intersection of $\tilde{A}(l_6 + t_6 + e_2) \cap \tilde{A}(l_6 + t_6 + e_1 + e_2)$ 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 $\tilde{A}(l_6 + t_6 + e_2)$ contains e_5. Then $e_5 + (l_6 + t_6 + e_2) + (l_7 + t_7) + (l_8 + t_8) = 0$, that is, $t_6 + t_7 + t_8 = e_2$. Now $\tilde{A}(l_6 + t_6 + e_2)$ and $\tilde{A}(l_6 + t_6 + e_2 + e_1)$ are determined, since they must contain $l_4 + t_4$:

$$\begin{aligned}
&\tilde{A}(l_6 + t_6 + e_2)\\
&\quad = \{l_1 + t_4 + t_8, l_2 + t_4 + t_6 + t_8 + e_2, l_3 + t_4 + t_7 + t_8, l_4 + t_4, l_5,\\
&\qquad l_6 + t_6 + e_2, l_7 + t_7, l_8 + t_8\},\\
&\tilde{A}(l_6 + t_6 + e_2 + e_1)\\
&\quad = \{l_1 + t_4 + t_8 + e_1, l_2 + t_4 + t_6 + t_8 + e_2 + e_1, l_3 + t_4 + t_7 + t_8, l_4 + t_4,\\
&\qquad l_5 + e_1, l_6 + t_6 + e_2 + e_1, l_7 + t_7, l_8 + t_8\}.
\end{aligned}$$

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

$$\begin{aligned}
&\{l_1 + t_4 + t_8, l_2 + t_4 + t_6 + t_8, l_3 + t_4 + t_7 + t_8 + e_2, l_4 + t_4,\\
&\quad l_5, l_6 + t_6, l_7 + t_7 + e_2, l_8 + t_8\},\\
&\{l_1 + t_4 + t_8, l_2 + t_4 + t_6 + t_8, l_3 + t_4 + t_7 + t_8 + e_2 + e_1, l_4 + t_4,
\end{aligned}$$

$$l_5 + e_1, l_6 + t_6, l_7 + t_7 + e_2 + e_1, l_8 + t_8\},$$
$$\{l_1 + t_4 + t_8 + e_2, l_2 + t_4 + t_6 + t_8 + e_2, l_3 + t_4 + t_7 + t_8 + e_2, l_4 + t_4,$$
$$l_5, l_6 + t_6, l_7 + t_7, l_8 + t_8 + e_2\},$$
$$\{l_1 + t_4 + t_8 + e_2 + e_1, l_2 + t_4 + t_6 + t_8 + e_2 + e_1, l_3 + t_4 + t_7 + t_8 + e_2 + e_1, l_4 + t_4,$$
$$l_5 + e_1, l_6 + t_6, l_7 + t_7, l_8 + t_8 + e_2 + e_1\}.$$

So the set of red vectors in L_2 is $\{l_2+t_4+t_6+t_8, l_2+t_4+t_6+t_8+e_2, l_2+t_4+t_6+t_8+e_2+e_1\}$ and in L_3 is $\{l_3 + t_4 + t_7 + t_8, l_3 + t_4 + t_7 + t_8 + e_2, l_3 + t_4 + t_7 + t_8 + e_2 + e_1\}$.

Now consider $l_8 + t_8 + e_1$ which is a blue vector in L_8. Note that $\tilde{A}(l_8 + t_8 + e_1)$ 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, 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:

$$\{l_2 + t_4 + t_6 + t_8 + e_2, l_2 + t_4 + t_6 + t_8 + e_2 + e_1, l_3 + t_4 + t_7$$
$$+t_8 + e_2, l_3 + t_4 + t_7 + t_8 + e_2 + e_1,$$
$$l_5, l_5 + e_1, l_8 + t_8, l_8 + t_8 + e_1\}.$$

As $\{l_2+t_4+t_6+t_8+e_2, l_2+t_4+t_6+t_8+e_2+e_1\} = \{l_5, l_5+e_1\}+e_5+e_3+t_4+t_6+t_8+e_2$, we get that $\{l_8+t_8, l_8+t_8+e_1\}+e_5+e_3+t_4+t_6+t_8+e_2 = \{l_3+t_4+t_6+e_2, l_3+t_4+t_6+e_2+e_1\}$ has to coincide with $\{l_3 + t_4 + t_7 + t_8 + e_2, l_3 + t_4 + t_7 + t_8 + e_2 + e_1\}$. However, this leads to $t_6 + t_7 + t_8 \in \{0, e_1\}$, contradiction.

8 4AP-free subsets of $\mathbb{Z}_4^n$

Proof of Theorem 3.5 According to Lemma 5.2 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.

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 3.1) 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 $16 \cdot 8 \le r'_4(4)$. □

Acknowledgements Open access funding provided by Graz University of Technology. We would like to thank Yves Edel for useful comments, especially on the case of cap sets and the anonymous referees for their useful comments. In particular, we also thank one referee for the quite compact formulation of the proof of Theorem 3.2. C.E. was partially supported by The Austrian Science Fund (FWF), grant W1230, P.P.P. was supported by the Lendület program of the Hungarian Academy of Sciences (MTA), the National Research, Development and Innovation Office of Hungary (Grant Nr. PD115978 and K129335) and the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

References

1. Alon N., Dubiner M.: Zero-sum sets of prescribed size. In: Combinatorics, Paul Erdős is Eighty. Bolyai Society, Mathematical Studies, Keszthely, Hungary, pp. 33–50 (1993).
2. Alon N., Dubiner M.: A lattice point problem and additive number theory. Combinatorica **15**, 301–309 (1995).
3. Alon N., Shpilka A., Umans C.: On sunflowers and matrix multiplication. Comput. Complexity **22**(2), 219–243 (2013).
4. Bateman M., Katz N.H.: New bounds on cap sets. J. Am. Math. Soc. **25**(2), 585–613 (2012).

5. Behrend F.A.: On sets of integers which contain no three terms in arithmetical progression. Proc. Natl Acad. Sci. U.S.A. **32**, 331–332 (1946).
6. Blasiak J., Church T., Cohn H., Grochow J., Naslund E., Sawin W., Umans C.: On cap sets and the group-theoretic approach to matrix multiplication. Discret. Anal. Paper No. 3, 27 pp. (2017)
7. Bourgain J.: On triples in arithmetic progression. Geom. Funct. Anal. **9**(5), 968–984 (1999).
8. Brown T.C., Buhler J.P.: A density version of a geometric Ramsey theorem. J. Combin. Theory Ser. A **25**, 20–34 (1982).
9. Calderbank A.R., Fishburn P.C.: Maximal three-independent subsets of $\{0, 1, 2\}^n$. Des. Codes Cryptogr. **4**(3), 203–211 (1994).
10. Cameron P.J.: Sum-free sets of a square. Manuscript. http://www.maths.qmul.ac.uk/~pjc/odds/sfsq.pdf.
11. Chandra A.K.: On the solution of Moser's problem in four dimensions. Can. Math. Bull. **16**, 507–511 (1973).
12. Chvátal V.: Remarks on a problem of Moser. Can. Math. Bull. **15**, 19–21 (1972).
13. Chvátal V.: Edmonds polytopes and a hierarchy of combinatorial problems Discret. Math. **4**, 305–337 (1973). Reprinted: Discret. Math. **306**, 886–904 (2006).
14. Coppersmith D., Winograd S.: Matrix multiplication via arithmetic progressions STOC '87 (Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing) Pages 1–6, also: J. Symbol. Comput. **9**(3), 251–280 (1990).
15. Croot E.: The minimal number of three-term arithmetic progressions modulo a prime converges to a limit. Can. Math. Bull. **51**(1), 47–56 (2008).
16. Croot E., Lev V.F., Pach P.P.: Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. Ann. Math. (2) **185**(1), 331–337 (2017).
17. Davis B.L., Maclagan D.: The card game SET. Math. Intell. **25**(3), 33–40 (2003).
18. Edel Y.: Extensions of generalized product caps. Des. Codes Cryptogr. **31**, 5–14 (2004).
19. Edel Y.: Sequences in abelian groups G of odd order without zero-sum subsequences of length $\exp(G)$. Des. Codes Cryptogr. **47**(1–3), 125–134 (2008).
20. Edel Y., Bierbrauer J.: Large caps in small spaces. Des. Codes Cryptogr. **23**(2), 197–212 (2001).
21. Edel Y., Ferret S., Landjev I., Storme L.: The classification of the largest caps in AG(5,3). J. Comb. Theory Ser. A **99**, 95–110 (2002).
22. Edel Y., Elsholtz C., Geroldinger A., Kubertin S., Rackham L.: Zero-sum problems in finite abelian groups and affine caps. Q. J. Math. **58**(2), 159–186 (2007).
23. Elkin M.: An improved construction of progression-free sets. Isr. J. Math. **184**, 93–128 (2011).
24. Ellenberg J.S., Gijswijt D.: On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. Ann. Math. (2) **185**(1), 339–343 (2017).
25. Elsholtz C.: Lower bounds for multidimensional zero sums. Combinatorica **24**(3), 351–358 (2004).
26. Elsholtz C., Rackham L.: Maximal sum-free sets of integer lattice grids. J. Lond. Math. Soc. (2) **95**(2), 353–372 (2017).
27. Erdős P.: Problems and results on combinatorial number theory. In: Srivastava J.N., et al. (eds.) A Survey of Combinatorial Theory, pp. 117–138. North Holland, Amsterdam (1973).
28. Erdős P., Turán P.: On some sequences of integers. J. Lond. Math. Soc. **11**, 261–264 (1936).
29. Erdős P., Ginzburg A., Ziv A.: Theorem in the additive number theory. Bull. Res. Council Israel F (10), 41–43 (1961).
30. Frankl P., Graham R.L., Rödl V.: On subsets of abelian groups with no 3-term arithmetic progression. J. Comb. Theory Ser. A **45**(1), 157–161 (1987).
31. Gowers W.T.: A new proof of Szemerédi's theorem. Geom. Funct. Anal. **11**(3), 465–588 (2001).
32. Green B.J.: Finite field models in additive combinatorics. In: Surveys in Combinatorics 2005. London Mathematical Society. Lecture Note Series, vol. 327, pp. 1–27. Cambridge University Press, Cambridge (2005).
33. Green B., Tao T.: New bounds for Szemerédi's theorem. I. Progressions of length 4 in finite field geometries. Proc. Lond. Math. Soc. (3) **98**(2), 365–392 and correction: New bounds for Szemeredi's theorem, Ia: Progressions of length 4 in finite field geometries revisited. arXiv:1205.1330 (2009).
34. Hales A.W., Jewett R.I.: Regularity and positional games. Trans. Am. Math. Soc. **106**, 222–229 (1963).
35. Hegedüs G.: A new exponential upper bound for the Erdős–Ginzburg–Ziv constant. arXiv:1712.00228.
36. Kalai G.: 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/ (2009).
37. Komlós J.: Solution to problem P.170 by Leo Moser. Can. Math. Bull. **15**, 312–313 (1972).
38. Lev V.F.: Progression-free sets in finite abelian groups. J. Number Theory **104**, 162–169 (2004).
39. Lin Y., Wolf J.: Subsets of $\mathbb{F}_q^n$ containing no k-term progressions. Eur. J. Comb. **31**(5), 1398–1403 (2010).
40. Meshulam R.: On subsets of finite abelian groups with no 3-term arithmetic progressions. J. Comb. Theory Ser. A **71**, 168–172 (1995).

41. Moser L.: Problem P.170. Can. Math. Bull. **13**, 268 (1970).
42. Naslund E.: Exponential bounds for the Erdős-Ginzburg-Ziv constant. J. Combin. Theory Ser. A **174**, 105185 (2020).
43. Newcombe L.: MSc Thesis, Royal Holloway (2008).
44. Petrov F., Pohoata C.: Improved bounds for progression-free sets in C_8^n. Israel J. Math. **236**(1), 345–363 (2020).
45. Polymath D.H.J.: Density Hales-Jewett and Moser numbers. In: An Irregular Mind, pp. 689–753. Bolyai Soc. Math. Stud., vol. 21, János Bolyai Math. Soc., Budapest (2010).
46. Potechin A.: Maximal caps in AG(6,3). Des. Codes Cryptogr. **46**(3), 243–259 (2008).
47. Rankin R.A.: Representations of a number as the sum of a large number of squares. Proc. R. Soc. Edinb. Sect. A **65**, 318–331 (1960/1961).
48. Reiher C.: On Kemnitz' conjecture concerning lattice-points in the plane. Ramanuj. J. **13**, 333–337 (2007).
49. Riddel J.: A lattice point problem related to sets containing no l-term arithmetic progression. Can. Math. Bull. **14**, 535–538 (1971).
50. Roth K.F.: On certain sets of integers. J. Lond. Math. Soc. (2) **28**(1), 104–109 (1953).
51. Salem R., Spencer D.C.: On sets of integers which contain no three terms in arithmetical progression. Proc. Natl Acad. Sci. U.S.A. **28**, 561–563 (1942).
52. Sanders T.: Roth's theorem in $\mathbb{Z}_4^n$. Anal. PDE **2**(2), 211–234 (2009).
53. Sanders T.: On Roth's theorem on progressions. Ann. Math. (2) **174**(1), 619–636 (2011).
54. Shannon C.E.: The zero-error capacity of a noisy channel. IRE Trans. Inf. Theory. **2**, 8–19 (1956).
55. Szemerédi E.: On sets of integers containing no k elements in arithmetic progression. Acta Arith. **27**, 199–245 (1975).
56. Tao T.: Webblog, 23 February 2007. Open question: best bounds for cap sets. http://terrytao.wordpress.com/2007/02/23/open-question-best-bounds-for-cap-sets/ (2007).
57. Tao T., Vu V.: Additive Combinatorics. Cambridge University Press, Cambridge (2006).
58. Williams V.V.: Multiplying matrices faster than Coppersmith–Winograd. In: STOC'12–Proceedings of the 2012 ACM Symposium on Theory of Computing, pp. 887–898. ACM, New York, (2012).
59. Wolf J.: Finite field models in arithmetic combinatorics-ten years on. Finite Fields Appl. **32**, 233–274 (2015).