Large Subsets of $\mathbb{Z}_m^n$ without Arithmetic Progressions

Christian Elsholtz, Benjamin Klahn and Gabriel F. Lipnik

Abstract. For integers m and n, we study the problem of finding good lower bounds for the size of progression-free sets in $(\mathbb{Z}_m^n, +)$. Let $r_k(\mathbb{Z}_m^n)$ denote the maximal size of a subset of $\mathbb{Z}_m^n$ without arithmetic progressions of length k and let $P^-(m)$ denote the least prime factor of m. We construct explicit progression-free sets and give an exponential improvement on the best previous lower bound

$$r_k(\mathbb{Z}_p^n) \gg_{p,k} \left(p^{2(k-1)} + p^{k-1} - 1\right)^{\frac{n}{2k}}$$

as follows:

1. If $k \geq 5$ is odd and $P^-(m) \geq k$, then

$$r_k(\mathbb{Z}_m^n) \gg_{m,k} \frac{\left\lfloor \frac{k-1}{k+1} m + 1 \right\rfloor^n}{n^{\lfloor \frac{k-1}{k+1} m \rfloor /2}}.$$

2. If $k \geq 4$ is even, $P^-(m) \geq k$ and $m \equiv -1 \bmod k$, then

$$r_k(\mathbb{Z}_m^n) \gg_{m,k} \frac{\left\lfloor \frac{k-2}{k} m + 2 \right\rfloor^n}{n^{\lfloor \frac{k-2}{k} m + 1 \rfloor /2}}.$$

Moreover, based on a computational method, we give some further improved lower bounds on $r_k(\mathbb{Z}_p^n)$ for primes $p \leq 31$ and progression lengths $4 \leq k \leq 8$.

Christian Elsholtz elsholtz@math.tugraz.at, https://www.math.tugraz.at/~elsholtz, Graz University of Technology, Austria

Benjamin Klahn klahn@math.tugraz.at, Graz University of Technology, Austria

Gabriel F. Lipnik math@gabriellipnik.at, https://www.gabriellipnik.at, Graz University of Technology, Austria

Support The authors acknowledge the support of the Austrian Science Fund (FWF): W 1230 and I 4945-N.

2020 Mathematics Subject Classification 11B25, 05D05, 20K01

Key words and phrases arithmetic progressions, progression-free sets, Behrend-type construction

1. Introduction and Main Result

In additive combinatorics, it has been of great interest to find large subsets of $\mathbb{Z}_m^n := (\mathbb{Z}/m\mathbb{Z})^n$ without arithmetic progressions of a given length k. The case $n = 1$ and $k = 3$ is closely related to progression-free sets in the integers; see the results by Behrend [1], Roth [17] and Szemerédi [19]. The case $k = 3$ and m prime is strongly connected to the well-studied case of capsets [3, 4, 5]. Nevertheless, there is not much literature on lower bounds on these progression-free sets, not even for prime m and for general progression length k, besides a paper by Lin and Wolf [11] and a paper by Elsholtz and Pach [6].

Our Approach. In this work, we present new results in this direction: We extend the combinatorial method of Elsholtz and Pach [6] and hereby obtain good results on lower bounds for the maximal size of a subset without arithmetic progressions of length $k \geq 4$. In particular, we use a digit-based "global" construction (in contrast to a product construction, being based on a "local" low-dimensional solution) in the sense that the progression-free sets are described explicitly in terms of its coordinate entries. This approach has similarities to the constructions by Salem and Spencer [18] and Behrend [1] in the integer case, and the method was used for the construction of capsets in $\mathbb{Z}_p^n$ by Elsholtz and Lipnik [5].

Related Work. Before we come to the description of our method and the outcoming results, let us briefly summarize related previous work. Major results in this field regarding the upper bounds are the following:

1. Szemerédi's theorem [19] states that the size $r_k(N)$ of the largest subset of $\{1, \ldots, N\}$ with no arithmetic progression of length k satisfies $r_k(N) = o(N)$ as $N \to \infty$. A stronger upper bound is due to Gowers [8].

2. Croot, Lev and Pach [2] studied the problem for $(\mathbb{Z}_4^n, +)$ and, by adapting the polynomial method, showed that $r_3(\mathbb{Z}_4^n) \leq 3.611^n$.

3. Ellenberg and Gijswijt [4] eventually showed that for a general prime power $q = p^r$, the inequality $r_3(\mathbb{F}_q^n) \ll_q c_q^n$ holds for some $c_q < q$.

4. In two individual cases, there has been improvement on the upper bound, in $\mathbb{Z}_8^n$ in [16] and in $\mathbb{Z}_6^n$ in [14].

5. When $k = 4$, Green and Tao [9] proved the bound $r_4(\mathbb{Z}_p^n) \ll_p \frac{p^n}{n^{(2^{-22})}}$.

6. When $k = p$ and n tends to infinity, the bound $r_p(\mathbb{Z}_p^n) = o(p^n)$ already follows from the Hales-Jewett theorem [10].

7. There are numerous upper bounds on different point set configurations, see for example [13, 12, 15].

Lower bounds have been studied before:

1. Using a geometrically motivated construction, Behrend showed in [1] that there is a subset $S \subseteq \{1, \ldots, N\}$ of size $|S| \geq N\exp(-c\sqrt{\log N})$ without any arithmetic progression of length three.

2. Lin and Wolf [11] proved that if p is a prime and $k \leq p$, then
$$r_k(\mathbb{Z}_p^n) \geq \left(p^{2(k-1)} + p^{k-1} - 1\right)^{\frac{n}{2k}}$$
holds, which one can approximately simplify to $p^{\frac{(k-1)n}{k}}$. Their result works more generally in finite fields and is an application of corresponding bounds on caps by Edel [3].

3. Elsholtz and Pach [6] adapted Behrend's method to higher dimensions, showing that there is a positive constant C_m such that
$$r_3(\mathbb{Z}_m^n) \geq \begin{cases} \frac{C_m}{\sqrt{n}}\left(\frac{m+1}{2}\right)^n & \text{if } m \text{ is odd,} \\ \frac{C_m}{\sqrt{n}}\left(\frac{m+2}{2}\right)^n & \text{if } m \text{ is even.} \end{cases}$$
Using a combinatorial construction, they also showed $r_4(\mathbb{Z}_{11}^n) \gg \frac{7^n}{n^3}$, and $r_{p+1}(\mathbb{Z}_{p^2}) \geq C'_m \frac{(m-p+1)^n}{n^{c_m}}$ holds for primes p and positive constants c_m and C'_m.
Moreover, Elsholtz and Pach were also able to find the exact values of $r_3(\mathbb{Z}_4^n)$ for $n \leq 5$ and the values of $r_4(\mathbb{Z}_4^n)$ for $n \leq 4$.

Main Results. The following main results of this paper provide good asymptotic lower bounds for $r_k(\mathbb{Z}_m^n)$ for odd progression length k and for even k when $m \equiv -1 \bmod k$. We note that the results are a direct consequence of the outcome of our construction method, i.e., a consequence of Theorem 2.2 and Theorem 2.3.

While for $k \geq 4$ an improvement over the results in [11] was only known in very special cases (see [6]), we present in this paper a further considerable improvement for $k \geq 5$, indeed an exponential improvement in the terminology of [2].

Theorem 1.1. *Let m be an integer and let $k \geq 5$ be an odd integer. Let $P^-(m)$ denote the least prime factor of m. If $P^-(m) \geq k$, then the following estimate holds:*
$$r_k(\mathbb{Z}_m^n) \gg_{m,k} \frac{\lfloor \frac{k-1}{k+1}m + 1 \rfloor^n}{n^{\lfloor \frac{k-1}{k+1}m \rfloor/2}}.$$

Note that, in particular, when $m = p > k$ is a prime, then the base $\lfloor (1 - \frac{2}{k+1})p \rfloor + 1$ considerably improves on the previous base of about $p^{(k-1)/k}$ in [11].

In the case of even k it seems more difficult to find any general pattern. At least for certain m we have been able to increase the base of the numerator by one.

Theorem 1.2. *Let $k \geq 4$ be an even integer. Let $m \equiv -1 \bmod k$ and assume that $P^-(m) \geq k$, then we have*
$$r_k(\mathbb{Z}_m^n) \gg_{m,k} \frac{\lfloor \frac{k-2}{k}m + 2 \rfloor^n}{n^{\lfloor \frac{k-2}{k}m+1 \rfloor/2}}.$$

A result of this strength was only known in the special case $k = 4$ and $m = 11$; see [6]. Here we can give an explicit construction of sets for all even $k \geq 4$ and integers $m \equiv -1 \bmod k$ where the least prime factor of m is at least k.

Structure. The remaining part of this paper is organized as follows: We present further results and the key idea of the corresponding method in Section 2. Section 3 contains a description of the explicit construction of large progression-free sets in $\mathbb{Z}_m^n$ for fixed integers m and fixed progression length. We finally conclude the paper by giving the proofs for our results in Section 4, and some additional helpful data can be found in Appendix A.

2. Method and Further Results

The work of Elsholtz and Pach [6] suggests that for the construction of large subsets of $\mathbb{Z}_m^n$ without arithmetic progressions of length k, it is a good idea to consider vectors whose entries only take values from a prescribed set of digits. To be more precise, we consider the following sets.

Definition 2.1. Let n be a positive integer, let $D = \{d_1, \ldots, d_{|D|}\} \subseteq \mathbb{Z}_m$ be a set of digits and let $\mathbf{f} = (f_1, f_2, \ldots, f_{|D|}) \in [0, n]^{|D|}$ be an integral vector whose entries sum to n. Then we define

$$S(D, n, \mathbf{f}) \coloneqq \{(a_1, \ldots, a_n) \in \mathbb{Z}_m^n \mid \forall i \leq |D| \colon a_j = d_i \text{ for } f_i \text{ values of } j\}.$$

Thus, $S(D, n, \mathbf{f})$ is the set of n-dimensional vectors where every digit of D occurs with a fixed frequency given by $\mathbf{f}$. The task is then to construct “good ” sets $D \subseteq \mathbb{Z}_m$ such that for some frequency distribution the set $S(D, n, \mathbf{f})$ does not contain an arithmetic progression of a given length. For a fixed size $|D|$ of the digit set we maximize the size of $|S(D, n, \mathbf{f})|$ by making the distribution $\mathbf{f}$ as uniform as possible. We will therefore mainly consider sets $S(D, n, \mathbf{f})$ where the distribution of digits is uniform. Given a digit set D and an integer n such that $|D| \mid n$, we set

$$S(D, n) \coloneqq S(D, n, \mathbf{f}) \quad \text{with } \mathbf{f} = \Big(\frac{n}{|D|}, \ldots, \frac{n}{|D|}\Big).$$

If $S(D, n)$ does not contain an arithmetic progression, then we say that the set D does not yield an arithmetic progression in $S(D, n)$, or that D is *admissible.*

Let us next determine the size of $S(D, n)$. For a vector in this set, we have to choose $n/|D|$ coordinates out of n for each digit in D. Thus, the size of $S(D, n)$ is given by a multinomial coefficient. By Stirling’s formula, one can give the asymptotic lower bound

$$|S(D, n)| = \binom{n}{\frac{n}{|D|}, \ldots, \frac{n}{|D|}} \gg_{m,k} \frac{|D|^n}{n^{(|D|-1)/2}} \tag{2.1}$$

as $n \to \infty$, where k is the progression length and m is the modulus.

It remains to find large digit sets D such that $S(D, n)$ is progression-free. In [6] it has been shown that one can take $D = \{0, \ldots, (p-1)/2\}$ of size $|D| = (p+1)/2$, without having an arithmetic progression of length $k = 3$ in $S(D, n)$. For odd $k \geq 5$ we shall see that we can extend the interval D found for $k = 3$ without having arithmetic progressions in $S(D, n)$ of length k.

Theorem 2.2. *Let m be an integer and let the progression length $k \geq 5$ be odd. If $P^-(m) \geq k$ and n is an integer divisible by $\delta = \lfloor \frac{k-1}{k+1} m \rfloor + 1$, then the set*

$$D = \Big\{0, 1, \ldots, \Big\lfloor \frac{k-1}{k+1} m \Big\rfloor\Big\}$$

of size $|D| = \delta$ does not yield any arithmetic progression of length k in $S(D, n)$.

For $k = 2\ell \geq 4$ even and $m \equiv -1 \bmod k$ with $P^-(m) \geq k$, we can extend the set D found in the case $k = 2\ell - 1$ by one element.

Theorem 2.3. *Let $k \geq 4$ be an even integer and let m be an integer with $m \equiv -1 \bmod k$. If $P^-(m) \geq k$ and n is an integer divisible by $\delta = \lfloor \frac{k-2}{k} m \rfloor + 2$, then the set*

$$D = \Big\{0, 1, \dots, \Big\lfloor \frac{k-2}{k} m \Big\rfloor, \frac{(k-1)m-1}{k} \Big\}$$

of size $|D| = \delta$ does not yield any arithmetic progression of length k in $S(D, n)$.

From our computations (see Appendix A) it seems likely that it should also be possible to extend the construction from Theorem 2.2 to integers with $m \not\equiv -1 \bmod k$. In particular, based on experiments with small primes we have the following conjecture.

Conjecture 2.4. Let $p \geq 13$ be a prime with $p \equiv 1 \bmod 4$ and let $n \in \mathbb{N}$ be a multiple of $\frac{p+3}{2}$. Then the set

$$D = \Big\{0, 1, \dots, \frac{p-1}{2}, \frac{p+3}{2} \Big\}$$

does not yield any arithmetic progression of length 4 in $S(D, n)$.

Finally, Table 1 provides explicit results for some values of p respectively k. As the computational effort of finding large admissible digit sets grows for increasing p and k (see Section 3), the values of p and k given here are rather small. In particular, we list the size of the largest admissible digit set for each pair (p, k), or a lower bound for it if the existence of larger digit sets cannot be excluded.

As an example we give a detailed discussion of the case $p = 17$ and $k = 3$ at the end of Section 3; all the other cases can be dealt with analogously. A corresponding admissible digit set of maximal cardinality as well as the number of maximal admissible digit sets for each pair (p, k) can be found in Appendix A.

$p \backslash k$	3	4	5	6	7	8
5	3	3	4 (4)	5	5	5
7	4	5 (5)	5 (5)	5	6 (6)	7
11	6	7 (7)	8 (8)	9 (9)	9 (9)	9
13	7	8	10 (9)	11	11 (10)	11
17	9	10	13 (12)	13 (13)	15 (13)	15
19	10	11 (11)	14 (13)	15	16 (15)	17
23	≥ 12	≥ 13 (13)	≥ 17 (16)	18 (17)	≥ 19 (18)	≥ 20 (19)
29	≥ 15	≥ 17	≥ 21 (20)	≥ 22 (21)	≥ 24 (22)	≥ 25
31	≥ 16	≥ 18 (17)	≥ 22 (21)	≥ 23	≥ 26 (24)	≥ 26 (25)

Table 1: Maximal size of digit sets D modulo p such that $S(D, n)$ does not contain an arithmetic progression of length k. The numbers given in parentheses are the bounds that we obtain from the general Theorems 2.3 and 2.2.

Remark 2.5. It may be possible to obtain slightly better denominators in the bounds given in Theorem 1.1 and Theorem 1.2, for example by fixing the frequency of only *some* digits in the vectors of $S(D, n)$ instead of fixing the frequencies of all digits. A description of some successful approaches in this direction can be found in [5] and [6, Proof of Theorem 3.11].

3. Approaches for Finding Admissible Digit Sets

In this section, we present approaches to find admissible digit sets—the most important part of our method for obtaining large progression-free sets. Most of the ideas given in this section can also found in [5], where the authors use similar techniques for capset constructions.

Modelling the Problem. As already seen in the previous section, the described construction relies on finding large digit sets $D \subseteq \mathbb{Z}_p$ such that $S(D, n)$ does not contain arithmetic progressions for all dimensions $n \in \mathbb{N}$ with $|D| \mid n$. For this purpose, let $k \geq 3$ be the progression length and let p be a prime. Moreover, let

$$P_k(D) \coloneqq \{v \in D^k \,|\, v \text{ is a non-trivial arithmetic progression modulo } p\}$$

be the set of k-term arithmetic progressions in D. Assume that there are k points in $S(D, n)$ which form an arithmetic progression for some $n \in \mathbb{N}$. For each progression $v = (v_1, \ldots, v_k) \in P_k(D)$, let x_v be a variable which counts the occurrences of v in the components of these k points. Due to the fact that each digit $d \in D$ has to occur the same number of time in each of the k points, the equation

$$\sum_{\substack{v \in P_k(D) \\ v_i = d}} x_v = \sum_{\substack{v \in P_k(D) \\ v_j = d}} x_v \tag{3.1}$$

has to hold for each digit $d \in D$ and for any pair (i, j) with $1 \leq i < j \leq k$.

It is easy to check that the non-existence of a non-negative non-trivial integral solution $(x_v \mid v \in P_k(D))$ of the system of equations given in (3.1) is equivalent to the non-existence of a k-term arithmetic progression in $S(D, n)$. Hence, if we want to prove admissibility of some digit set D, we have to ensure that the set

$$\mathcal{P}(D) = \{x \in \mathbb{Z}^{\ell}_{\geq 0} \,|\, Ax = 0\}$$

only contains the zero vector, where the system of linear equations $Ax = 0$ describes the equations stated in (3.1). If we want to show that a digit set is not admissible, on the other hand, then we have to find a non-negative non-trivial solution of $Ax = 0$. This solution directly corresponds to a k-term arithmetic progression in $S(D, n)$ (for infinitely many dimensions n).

Both can be achieved by methods of integer linear programming. Unfortunately, the problem of deciding if a polyhedron contains an integral point is computationally hard and in general NP-complete [7]. This indicates that checking this condition for all possible digit sets modulo p can only be done for small p—and has been done for primes $5 \leq p \leq 31$ and progression length $3 \leq k \leq 8$, as Table 1 indicates.

Reducibility as a Sufficient Condition. Next, we describe a technique which allows to show admissibility in a computationally simple and comprehensible way. For some fixed digit set D and the corresponding constraint matrix A, let B be a fixed matrix which is equivalent to A in the sense that there exists an invertible matrix T such that $TA = B$. This certainly implies

$$\{x \in \mathbb{Z}^{\ell}_{\geq 0} \,|\, Ax = 0\} = \mathcal{P}(D) = \{x \in \mathbb{Z}^{\ell}_{\geq 0} \,|\, Bx = 0\}.$$

This matrix B is the starting point of the procedure.

Remember that we want to show the emptiness of $\mathcal{P}(D)$. Therefore, if some non-zero row i of B only contains non-negative or non-positive entries, then it clearly follows that the variables corresponding to non-zero entries of this row have to be zero. This is because we are looking for non-negative solutions x of $Bx = 0$, and if the said variables were non-zero, then the equation corresponding to row i of B would not have such a solution.

Consequently, we remove those columns of B which belong to these variables, i.e., columns of B with non-zero entry in row i, and then proceed with the remaining matrix and the next non-negative or non-positive row. We want to emphasize that the deletion of columns possibly brings out new non-negative or non-positive rows. Naturally, the process determines if no non-negative or non-positive non-zero row is left in the matrix. If at the end all columns of B are deleted—which means that all variables x_i have to be zero and that this is the only non-negative integral solution—, then the digit set D is admissible.

Furthermore, we say that D is *reducible with initial matrix B* if B is equivalent to A and all columns of B can be deleted by the process above.

Two very natural choices[1] for the initial matrix B are $B = A$ and $B = A_{\mathrm{ech}}$, where A_{ech} denotes the reduced row echelon form of A. It turns out that these choices are not only intuitive, but also very successful and good enough for our purpose: We were able to verify 50 of the 54 bounds given in Table 1 using them; see Appendix A. One comprehensible example with a different choice of B can be found at the end of this section.

Illustration of the Method in the Case $k = 3$ and $p = 11$. In the following, we exemplarily illustrate the concept of reducibility. For this purpose, let us have a look at the modulus $p = 11$ and the progression length $k = 3$.

First, we show that the digit set $D_1 = \{0, 1, 2, 3, 4, 5\}$ is admissible (even though this is already known from [6]) by deducing its reducibility with reduced row echelon form as initial matrix. The set $P_3(D_1)$ of non-trivial 3-term arithmetic progressions in D_1 is given by

$$\begin{aligned} P_3(D_1) = \{&(0,1,2),(0,2,4),(1,2,3),(1,3,5),(2,3,4),(2,1,0),\\ &(3,4,5),(3,2,1),(4,2,0),(4,3,2),(5,3,1),(5,4,3)\}, \end{aligned}$$

and thus, the constraint matrix A is given by

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

where the first six rows represent equations which arise from the first and second position in the vectors of $P_3(D_1)$ (i.e., $i = 1$ and $j = 2$ in (3.1)), and the latter six rows represent the constraints for the positions one and three in the vectors of $P_3(D_1)$ (i.e., $i = 1$ and

[1] Note the approach of reducing the set $P_k(D)$ due to certain conditions on the occurring digits which is used in [5, 6] is a special case of the reducibility presented here, namely with initial matrix $B = A$. For further details we refer to the mentioned papers.

$j = 3$ in (3.1)). Moreover, its reduced row echelon form is given by

$$A_{\text{ech}} = \begin{pmatrix} 1&0&0&0&0&0&0&-1&-1&0&0&1\\ 0&1&0&0&0&0&0&1&1&0&0&-1\\ 0&0&1&0&0&0&0&-1&-1&-1&0&2\\ 0&0&0&1&0&0&0&0&1&1&0&-1\\ 0&0&0&0&1&0&0&-1&-2&-1&0&1\\ 0&0&0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0&-1&-1&0&1\\ 0&0&0&0&0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix}.$$

The described matrix reduction is given as follows, where the non-negative respectively non-positive rows as well as the columns which have to be deleted in the next step are marked:

$$\begin{pmatrix} 1&0&0&0&0&0&0&-1&-1&0&0&1\\ 0&1&0&0&0&0&0&1&1&0&0&-1\\ 0&0&1&0&0&0&0&-1&-1&-1&0&2\\ 0&0&0&1&0&0&0&0&1&1&0&-1\\ 0&0&0&0&1&0&0&-1&-2&-1&0&1\\ 0&0&0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0&-1&-1&0&1\\ 0&0&0&0&0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&0&0&0&0&0&-1&0\\ 0&1&0&0&0&0&1&0\\ 0&0&1&0&0&0&-1&-1\\ 0&0&0&1&0&0&0&1\\ 0&0&0&0&1&0&-1&-1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&-1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&0&0&0\\ 0&0&0&0\\ 0&1&0&0\\ 0&0&0&0\\ 0&0&1&0\\ 0&0&0&0\\ 0&0&0&1\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0 \end{pmatrix} \rightsquigarrow \left(\quad \right).$$

The last step trivially follows. As a consequence, the only non-negative vector x that solves $Ax = 0$ is the zero vector. This implies that D_1 is reducible and thus, also admissible. So the largest admissible digit for $k = 3$ and $p = 11$ contains at least $|D_1| = 6$ elements. In order to show that no larger digit set is admissible, one can find a non-negative non-trivial integral solution to $Ax = 0$ by solving the integer linear program

$$\begin{aligned} \max \quad & 0 \\ \text{s.t.} \quad & x \in \mathcal{P}(D) \\ & (1 \;\; \cdots \;\; 1) \cdot x \geq 1 \end{aligned}$$

for all digit sets D with $|D| = 7$, with appropriate software. As a consequence, the largest admissible digit set for $p = 11$ and $k = 3$ has indeed cardinality 6, as stated in Table 1.

Finally, let us have a look at a second digit set of size 6: Consider the digit set $D_2 = \{0, 1, 4, 6, 8, 10\}$. The set of non-trivial progressions in D_2 of length 3 is given by

$$\begin{aligned} P_3(D_2) = \{&(0,4,8), (0,6,1), (1,6,0), (1,8,4), (1,10,8), (1,0,10), (4,6,8), \\ &(4,8,1), (6,8,10), (8,10,1), (8,4,0), (8,6,4), (10,0,1), (10,8,6)\}. \end{aligned}$$

The corresponding constraint matrix is

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

and its reduced row echelon form A_{ech} and the reduction steps are given by

$$A_{\mathrm{ech}} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&-1&0&-1&4&1 \\ 0&1&0&0&0&0&0&0&0&1&0&1&5&-1 \\ 0&0&1&0&0&0&0&0&0&0&1&0&9&0 \\ 0&0&0&1&0&0&0&0&0&-1&-1&0&4&1 \\ 0&0&0&0&1&0&0&0&0&1&0&0&10&-1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&10&0 \\ 0&0&0&0&0&0&1&0&0&-1&-1&0&8&0 \\ 0&0&0&0&0&0&0&1&0&0&0&-1&7&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&-1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix} \rightsquigarrow \cdots \rightsquigarrow \begin{pmatrix} 1&0&0&0&0&0&0&-1&-1&1 \\ 0&1&0&0&0&0&0&1&1&-1 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&-1&0&1 \\ 0&0&0&1&0&0&0&1&0&-1 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&-1&0&0 \\ 0&0&0&0&0&1&0&0&-1&1 \\ 0&0&0&0&0&0&1&0&0&-1 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix},$$

where the matrix on the right hand-side is the result of the reduction. This implies that D_2 is not reducible with initial matrix A_{ech}. The reduction stopped because there is neither a non-negative nor a non-positive row left. However, we can add the second to the forth row, which is a valid row transformation at this point in the sense that no solution of the corresponding linear system gets lost. Moreover, this transformation yields a new non-negative row (namely the forth one), and the reduction can be proceeded with this new matrix, which can be fully reduced now:

$$\begin{pmatrix} 1&0&0&0&0&0&0&-1&-1&1 \\ 0&1&0&0&0&0&0&1&1&-1 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&-1 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&-1&0&0 \\ 0&0&0&0&0&1&0&0&-1&1 \\ 0&0&0&0&0&0&1&0&0&-1 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix} \rightsquigarrow \cdots \rightsquigarrow \begin{pmatrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{pmatrix}.$$

Consequently, the digit set D_2 is reducible with initial matrix $B = TA_{\mathrm{ech}}$, where T is chosen in such a way that the multiplication results in an addition of the second row of A_{ech} to its forth row. Hence, also D_2 is admissible.

4. Proofs

The following proofs do not directly make use of approaches presented in the previous section. Nevertheless, reducibility was essential to find admissible sets which can be generalized as stated in the Theorems 2.2 and 2.3.

Proof of Theorem 2.2. This result is proven inductively as follows: We show that if for some $d < t := \lfloor m(k-1)/(k+1) \rfloor$ the set $D_d := \{0, \dots, d\}$ does not yield a k-term arithmetic progression in $S(D_d, n)$ for any $n \in \mathbb{N}$ with $|D| \mid n$, then the digit set $D_{d+1} = D_d \cup \{d+1\}$ does not either.

The base case is obviously fulfilled as $D_0 = \{0\}$ does not yield a non-trivial k-term arithmetic progression in $S(D_0, n) = \{(0, \dots, 0)\}$ for any dimension $n \in \mathbb{N}$.

Next, assume for $d < t$ there does not exist any non-trivial arithmetic progression of length k in $S(D_d, n)$ for all $n \in \mathbb{N}$ with $|D| \mid n$, and consider $S(D_{d+1}, n)$. Assume for the sake of contradiction that there is an arithmetic progression of length k in $S(D_{d+1}, n')$ for some $n' \in \mathbb{N}$. As there is no such progression in $S(D_d, n')$, there has to exist a coordinate such that the progression in D_d formed by the digits in this coordinate is non-constant and makes use of the digit $d+1$. Therefore, the digit $d+1$ occurs in a non-trivial progression in each of the k positions, and, in particular $d+1$ must also occur non-trivially in the centre position, i.e., in the position $(k+1)/2 = \ell + 1$ for $\ell = (k-1)/2$. Let us denote this arithmetic progression in the said coordinate by $v = (v_1, \ldots, v_k) \in (D_{d+1})^k$; then we have $v_{\ell+1} = d + 1$. We show that this leads to a contradiction.

The elements $v_1, v_2, \ldots, v_k$ may be described as $v_i = v_1 + (i-1)c$ for some non-zero element $c \in \mathbb{Z}_m$, and as $P^-(m) \geq k$ we see that all elements $v_1, v_2, \ldots, v_k$ are pairwise different. If any digit v_i with $i \leq \ell$ is contained in the interval $[m(\ell-1)/(\ell+1), d]$, then $v_{i+\ell}$ cannot be in $\{0, \ldots, d\}$. Thus, all digits v_1, …, v_ℓ are contained in the interval $[0, m(\ell-1)/(\ell+1))$. By the pigeon hole principle, there are two of the digits v_i and v_j with $0 \leq i, j \leq \ell$ and $v_i > v_j$ which satisfy $0 < v_i - v_j < m/(\ell+1)$. However, this implies that $v_{\ell+i-j} \in \{d+1, \ldots, m-1\}$, which cannot be true.

Thus, $d+1$ never occurs in the middle of a progression, which is a contradiction. This completes the induction step. □

Proof of Theorem 2.3. By Theorem 2.5 it suffices to show that a non-trivial arithmetic progression in D cannot have $h := \frac{(k-1)m-1}{k}$ in the first position. Assume that there is such a progression $a_1, a_2, \ldots, a_k$ with $a_1 = h$. Again, as $P^-(m) \geq k$ all elements $a_1, a_2, \ldots, a_k$ are pairwise different. Note that the nearest elements in D to h, namely the residue classes of m (which is 0) and $\lfloor\frac{(k-2)m}{k}\rfloor$, both have distance

$$|m - h| = \Big|h - \Big\lfloor\frac{(k-2)m}{k}\Big\rfloor\Big| = \frac{m+1}{k} \tag{4.1}$$

to h.

The elements a_2, a_3, …, a_k are all different from h and must therefore all lie in the interval $[0, \lfloor\frac{(k-2)m}{k}\rfloor]$. Thus, by the pigeon hole principle there are two elements a_i and a_j with $k \geq j > i \geq 2$ and distance $|a_i - a_j| < \frac{m}{k}$. But this would mean that also $|a_1 - a_{j-i+1}| < \frac{m}{k}$, contradicting the minimal distance from h to another element given in (4.1). Thus, there can be no such progression. □

Proof of Theorem 1.1. By Theorem 2.2 we can find a digit set D of size at least $m(k-1)/(k+1)$ such that there is no arithmetic progression of length k in $S(D, n)$ for $n \in \mathbb{N}$ with $|D| \mid n$. By (2.1) we find

$$|S(D, n)| \gg_{m,k} \frac{\lfloor\frac{k-1}{k+1}m + 1\rfloor^n}{n^{\lfloor\frac{k-1}{k+1}m\rfloor/2}}.$$

If $|D| \nmid n$ with $n = |D|m + r$ and $1 \leq r < |D|$, we can embed the set $S(D, n-r)$ into $\mathbb{Z}_m^n$ by simply putting zeroes in the last r coordinates. The image does not contain any arithmetic progressions and is also of size

$$|S(D, n-r)| \gg_{m,k} \frac{\lfloor\frac{k-1}{k+1}m + 1\rfloor^n}{n^{\lfloor\frac{k-1}{k+1}m\rfloor/2}},$$

as claimed. □

Theorem 1.2 can be proven analogously, as a conclusion of Theorem 2.3.

References

[1] Felix A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. USA **32** (1946), 331–332. MR 18694

[2] Ernie Croot, Vsevolod F. Lev, and Péter P. Pach, *Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small*, Ann. of Math. (2) **185** (2017), no. 1, 331–337. MR 3583357

[3] Yves Edel, *Extensions of generalized product caps*, Des. Codes Cryptogr. **31** (2004), no. 1, 5–14. MR 2031694

[4] Jordan S. Ellenberg and Dion Gijswijt, *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math. (2) **185** (2017), no. 1, 339–343. MR 3583358

[5] Christian Elsholtz and Gabriel F. Lipnik, *Exponentially larger affine and projective caps*, submitted, 2020.

[6] Christian Elsholtz and Péter P. Pach, *Caps and progression-free sets in $\mathbb{Z}_m^n$*, Des. Codes Cryptogr. **88** (2020), 2133–2170.

[7] Michael R. Garey and David S. Johnson, *Computers and intractability*, W. H. Freeman and Co., San Francisco, Calif., 1979, A guide to the theory of NP-completeness, A Series of Books in the Mathematical Sciences. MR 519066

[8] William T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588. MR 1844079

[9] Ben Green and Terence Tao, *New bounds for Szemerédi's theorem. I. Progressions of length 4 in finite field geometries*, Proc. Lond. Math. Soc. (3) **98** (2009), no. 2, 365–392. MR 2481952

[10] Alfred W. Hales and Robert I. Jewett, *Regularity and positional games*, Trans. Amer. Math. Soc. **106** (1963), 222–229. MR 143712

[11] Yuncheng Lin and Julia Wolf, *On subsets of $\mathbb{F}_q^n$ containing no k-term progressions*, European J. Combin. **31** (2010), no. 5, 1398–1403. MR 2644427

[12] Neil Lyall, Ákos Magyar, and Hans Parshall, *Spherical configurations over finite fields*, Amer. J. Math. **142** (2020), no. 2, 373–404. MR 4084158

[13] Ákos Magyar, *k-point configurations in sets of positive density of $\mathbb{Z}^n$*, Duke Math. J. **146** (2009), no. 1, 1–34. MR 2475398

[14] Péter P. Pach and Richárd Palincza, *Sets avoiding six-term arithmetic progressions in $\mathbb{Z}_6^n$ are exponentially small*, arXiv e-prints (2020), arXiv:2009.11897.

[15] Hans Parshall, *Simplices over finite fields*, Proc. Amer. Math. Soc. **145** (2017), no. 6, 2323–2334. MR 3626492

[16] Fedor Petrov and Cosmin Pohoata, *Improved bounds for progression-free sets in C_8^n*, Israel J. Math. **236** (2020), no. 1, 345–363. MR 4093890

[17] Klaus F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104–109. MR 51853

[18] Raphaël Salem and Donald C. Spencer, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U.S.A. **28** (1942), 561–563. MR 7405

[19] Endre Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245. MR 369312

Appendix A. Maximal Admissible Digit Sets (Verification of Table 1)

In the following, we list one maximal admissible set for each pair (p, k) with $5 \leq p \leq 31$ and $3 \leq k \leq 8$. Admissibility was checked via reducibility as presented in Section 3; we list the lexicographically first admissible digit set which is reducible with initial matrix A or A_{ech}, where this is possible. We also give the initial matrices with which we have established reducibility of the corresponding digit sets.

Moreover, for small primes we also give the number of maximal admissible digit sets. This result was obtained by the computational integer programming approach. Note that many admissible digit sets are in some sense symmetric to each other. We have refrained from filtering out such patterns because the given number should only convey a sense for its range. To keep the following tables concise, we use the usual notation for discrete intervals, i.e.,

$$[a, b] := \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

for integers a and b with $0 \leq a \leq b < p$, and we consider these sets to be subsets of $\mathbb{Z}_p$.

The admissibility of the four digit sets marked with a star (*) has been checked by using the integer programming approach which is described in Section 3, because no reducible digit set has been found of the same size, neither with initial matrix A nor with initial matrix A_{ech}. (Numerous digit sets with one element less are reducible with initial matrix A respectively A_{ech}, though.)

p	one maximal admissible digit set	initial matrix B	number of maximal admissible digit sets
5	$[0, 2]$	A, A_{ech}	10
7	$[0, 3]$	A, A_{ech}	35
11	$[0, 5]$	A, A_{ech}	275
13	$[0, 6]$	A	546
17	$[0, 8]$	A	1496
19	$[0, 9]$	A	2223
23	$[0, 11]$	A	4301
29	$[0, 14]$	A	–
31	$[0, 15]$	A	–

Table 2: Progression length $k = 3$ (see also [6])

p	one maximal admissible digit set	initial matrix B	number of maximal admissible digit sets
5	$[0,2]$	A, A_{ech}	10
7	$[0,4]$	A, A_{ech}	21
11	$[0,6]$	A_{ech}	220
13	$[0,6] \cup \{8\}$	A_{ech}	468
17	$[0,8] \cup \{10\}$	A_{ech}	5848
19	$[0,10]$	A_{ech}	16416
23	$[0,12]$	A_{ech}	–
29	$[0,12] \cup \{14,25,27,28\}$	A_{ech}	–
31	$[0,12] \cup \{14,16,27,29,30\}$	A_{ech}	–

Table 3: Progression length $k = 4$

p	one maximal admissible digit set	initial matrix B	number of maximal admissible digit sets
5	$[0,3]$	A, A_{ech}	5
7	$[0,4]$	A, A_{ech}	21
11	$[0,7]$	A, A_{ech}	165
13	$[0,9]$	A_{ech}	286
17	$[0,9] \cup [11,13]$	A	1768
19	$[0,13]$	A_{ech}	10089
23	$[0,12] \cup [14,16] \cup \{18\}$	A	–
29	$[0,15] \cup [17,20] \cup \{26\}$	A	–
31	$[0,17] \cup \{19,20,26,29\}$	A	–

Table 4: Progression length $k = 5$

p	one maximal admissible digit set	initial matrix B	number of maximal admissible digit sets
5	$[0,4]$	A, A_{ech}	1
7	$[0,4]$	A, A_{ech}	21
11	$[0,8]$	A, A_{ech}	55
13	$[0,10]$	A_{ech}	78
17	$[0,12]$	A_{ech}	2312
19	$[0,14]$	A_{ech}	2052
23	$[0,13] \cup \{15,19,21,22\}$	A_{ech}	23529
29	$[0,15] \cup \{17,18,23\} \cup [25,17]$	A_{ech}	–
31	$[0,18] \cup \{20,26,29,30\}$	A_{ech}	–

Table 5: Progression length $k = 6$

p	one maximal admissible digit set	initial matrix B	number of maximal admissible digit sets
5	$[0,4]$	A, A_{ech}	1
7	$[0,5]$	A, A_{ech}	7
11	$[0,8]$	A, A_{ech}	55
13	$[0,10]$	A, A_{ech}	78
17	$[0,14]^*$	–	136
19	$[0,15]$	A_{ech}	969
23	$[0,18]$	A_{ech}	–
29	$[0,23]^*$	–	–
31	$[0,25]^*$	–	–

Table 6: Progression length $k = 7$

p	one maximal admissible digit set	initial matrix B	number of maximal admissible digit sets
5	$[0,4]$	A, A_{ech}	1
7	$[0,6]$	A, A_{ech}	1
11	$[0,8]$	A, A_{ech}	55
13	$[0,10]$	A, A_{ech}	78
17	$[0,14]$	A_{ech}	136
19	$[0,14] \cup \{16,17\}$	A_{ech}	171
23	$[0,15] \cup \{18,19,21,22\}$	A_{ech}	1771
29	$[0,24]^*$	–	–
31	$[0,19] \cup \{22,24,25\} \cup [28,30]$	A	–

Table 7: Progression length $k = 8$