AVOIDING ARITHMETIC PROGRESSIONS IN CYCLIC GROUPS

Lorenz & Stephanie Halbeisen

Keywords: arithmetic progressions, cyclic groups, hypergraphs, independent sets, independence number

2000 Mathematics Subject Classification: 05C35 05C65 05D99 90C27 05D15

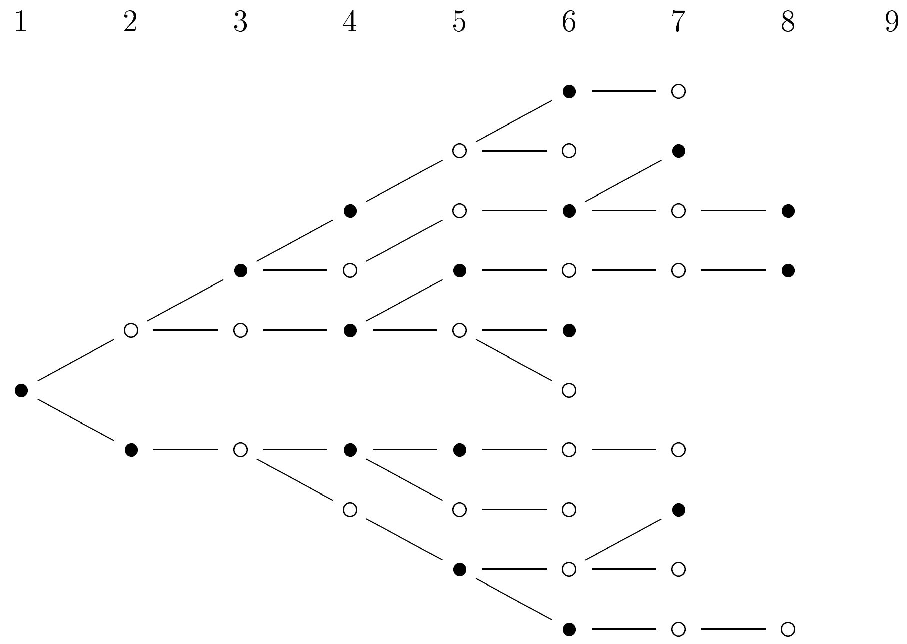
Abstract

For given natural numbers n and r, $\alpha(n,r)$ denotes the maximum cardinality of a subset of $\mathbb{Z}_n$ which does not contain any non-constant arithmetic progression (modulo n) of length r. The function $\alpha(n,r)$ is investigated for several values of n and r. In particular, it is shown that $\alpha(n,n) = n\big(1-\frac{1}{p}\big)$, where p is the smallest prime dividing n, and that for any prime number p we have $\alpha(p^2,p) = (p-1)^2$.

0. Introduction

Van der Waerden's Theorem tells us that for any colouring of the positive integers with two colours, there are arbitrarily long non-constant arithmetic progressions in one colour, *i.e.*, for every length ℓ there are positive integers a and d such that all the numbers a, $a+d$, $a+2d$, $\ldots$, $a+\ell d$ have the same colour. Such arithmetic progressions are called monochromatic. As a consequence, for any positive integer r there exists a positive integer n such that each colouring of the numbers $1,2,\ldots,n$ with two colours contains a monochromatic non-constant arithmetic progression of length r. In other words, we cannot avoid arithmetic progressions of length r in both colours simultaneously.

Let us try to colour the numbers $1,2,\ldots,9$ with two colours in such a way that neither colour contains an arithmetic progression of length 3. Let $\circ$ and $\bullet$ denote the two colours respectively. Without loss of generality we may assume that 1 is coloured $\bullet$. We now proceed by colouring successively the numbers $2,3,\ldots$ such that neither colour contains an arithmetic progression of length 3. This leads to the following graph:



Firstly this graph shows that it is possible to colour the numbers $1, 2, \ldots, 8$ with two colours such that neither colour contains a non-constant arithmetic progression of length 3. Secondly we see that no matter how we colour the numbers $1, 2, \ldots, 9$ with two colours, there is always a monochromatic non-constant arithmetic progression of length 3.

For given positive integers n and r we can always ask how large a subset of $\{1, 2, \ldots, n\}$ may be such that it does not contain any arithmetic progression of length r. To find optimal upper bounds for the cardinality (*i.e.*, size) of such a set is still an open problem, even in the case of $r = 3$. In order to make the problem more symmetric and to avoid "boundary effects", we shall consider the *cyclic* set $\big(\mathbb{Z}/n\mathbb{Z}\big) = \mathbb{Z}_n$, instead of the *linear* set $1, 2, \ldots, n$, and ask for the maximum cardinality of a subset in $\mathbb{Z}_n$ which does not contain any non-constant arithmetic progression of a given length. More precisely, a non-constant arithmetic progression with respect to $\mathbb{Z}_n$ of length r is a non-constant sequence in the cyclic group $(\mathbb{Z}_n, +)$ (*i.e.*, modulo n) of the form a, $a + d$, $a + 2d$, $\ldots$, $a + (r - 1)d$, where $a \in \mathbb{Z}_n$ and $1 \leq d < n$. Notice that we do not require all elements of the sequence to be different. Seeking for large sets in cyclic groups which do not contain arithmetic progressions of a given length leads to the following question:

> *Given a cyclic group $\mathbb{Z}_n$ and a positive integer r. What is the maximum cardinality of a set $A \subseteq \mathbb{Z}_n$ such that A does not contain any non-constant arithmetic progression with respect to $\mathbb{Z}_n$ of length r?*

In order to give partial answers to this question we shall use finite affine planes, a result in finite geometry, hypergraphs (a general form of graphs), a result for the linear case, as well as some combinatorics.

First we like to reformulate our question above in terms of hypergraphs, but before we can do so, we have to introduce some terminology.

A **hypergraph** $H = (V, E)$ is a finite set V of "vertices" together with a finite set E of "edges" (sometimes called "hyperedges"), which are arbitrary non-empty subsets of V (for a systematic study of hypergraphs we refer the reader to [Be89]). If all edges of a hypergraph H have the same cardinality r, then the hypergraph H is called ***r*-uniform**. In particular, a graph without loops is a 2-uniform hypergraph. A hypergraph is called **regular** if all vertices belong to the same number of edges. A set of vertices of a hypergraph H which does not (completely) contain any edge of H is called an **independent set**. The complement of an independent set is a set of vertices which meets each edge of the hypergraph. Such a set is called a **transversal**. For a hypergraph H, the **independence number** $\alpha(H)$ (in the literature also called *stability number*) is the maximum cardinality of an independent set of H (see [Be89]). The **transversal number** $\tau(H)$ of a hypergraph H is the smallest cardinality of a transversal of H. If each vertex of H is contained in at least one edge of H, then the complement of a maximal independent set (*i.e.*, an independent set which is not properly contained in another independent set) is a minimal transversal (*i.e.*, does not properly contain another transversal) and vice versa. In particular we get that $\alpha(H) + \tau(H)$ is equal to the number of vertices of H.

Let us now turn back to our question:

For a positive integer n, we identify the elements of the cyclic group $\mathbb{Z}_n$ with the set $\{0, 1, \ldots, n-1\}$. For a positive integer r with $r \leq n$, let $H_{n,r} = (V_n, E_r)$ be the hypergraph defined as follows: $V_n := \mathbb{Z}_n$ and a finite set $e \subseteq V_n$ belongs to E_r if and only if there is a non-constant arithmetic progression P in $\mathbb{Z}_n$ of length r, so that the elements appearing in P are exactly the elements of e. Since $\mathbb{Z}_n$ is completely symmetric, $H_{n,r}$ is always a regular hypergraph, but in general $H_{n,r}$ is not r-uniform, *e.g.*, $H_{4,3} = \big\{\{0,1,2\}, \{1,2,3\}, \{2,3,0\}, \{3,0,1\}, \{0,2\}, \{1,3\}\big\}$. On the other hand, $H_{n,r}$ is always r-uniform for $n \geq r$ and n prime. To see this, let $(a_1, a_2, \ldots, a_r)$ be an arithmetic progression with respect to $\mathbb{Z}_n$, where $n \geq r$ and n prime. Let $d = a_2 - a_1$ and assume that $a_k = a_\ell$ for some $1 \leq k < \ell \leq r$. Then $(k-\ell)d \equiv 0 \mod n$, and since n is prime, this implies that $d = 0$ or $d = n$, and therefore, the sequence $(a_1, a_2, \ldots, a_r)$ is constant in $\mathbb{Z}_n$.

Since the set of edges of $H_{n,r}$ correspond to the set of all non-constant arithmetic progressions in $\mathbb{Z}_n$ of length r, it is easy to see that $\alpha\big(H_{n,r}\big)$ is equal to the maximum cardinality of a set $A \subseteq \mathbb{Z}_n$ such that A does not contain any non-constant arithmetic progression of length r. So, to keep the notation short, let $\alpha(n,r) := \alpha\big(H_{n,r}\big)$.

For small numbers n and r, the value $\alpha(n,r)$ can be easily calculated by computer, using for example a fast Prolog program. However, for general statements like $\alpha(p^2, p) = (p-1)^2$ (for p prime) we have to seek combinatorial proofs. The following result for hypergraphs gives us a lower bound on $\alpha(n,r)$ for $n > r$ and n prime.

If $n > r$ and $H_{n,r}$ is r-uniform, e.g., if n is prime, a lower bound for $\alpha(n,r)$ is given by the formula

$$\alpha(n,r) \geq \frac{n}{m\big(H_{n,r}\big)^{1/r}}\,,$$

where $m\big(H_{n,r}\big)$ denotes the number of edges of $H_{n,r}$ (see [Be 89, p. 136]). Let us give some examples: For $n = 7$ and $r = 3$ we get $\alpha(7,3) \geq \frac{7}{21^{1/3}} \approx 2.54$, therefore, $\alpha(7,3) \geq 3$, and indeed, $\alpha(7,3) = 3$. However, for $n = 25$ and $r = 5$ we get $\alpha(25,5) \geq \frac{25}{255^{1/5}} \approx 8.25$ and therefore $\alpha(25,5) \geq 9$, but we will see later that $\alpha(25,5) = 16$.

In the next section we will give some other lower bounds for $\alpha(n,r)$ and in the last section we will compute exact values of $\alpha(n,r)$ for certain numbers n and r. As a matter of fact we like to mention that $\alpha(n,r)$ is increasing in r, *i.e.*, if $r \geq r' \geq 1$, then $\alpha(n,r) \geq \alpha(n,r')$. But on the other hand, $\alpha(n,r)$ is *not* increasing in n. For example, $\alpha(19,3) = 6$ but $\alpha(20,3) = 5$.

1. Lower Bounds

For positive integers n, a, r let (n,a,r) be the following statement: There is a set $A \subseteq \mathbb{Z}_n$ of cardinality a which does not contain any non-constant arithmetic progression of length r. As mentioned above, $\alpha(n,r)$ denotes the largest integer a with (n,a,r).

A set $A \subseteq \mathbb{Z}_n$ of cardinality a **witnesses** (n,a,r) if it does not contain any non-constant arithmetic progression of length r.

Remark. If $B \subseteq \mathbb{Z}_n$ witnesses (n,b,r) and $\alpha(n,r) \geq a > b$, then in general it is not true that there exists a set $A \supseteq B$ which witnesses (n,a,r); or in terms of hypergraphs, not every maximal independent set of $H_{n,r}$ must have cardinality $\alpha(H_{n,r})$. For example, $B = \{0,1,3,4,11,20\}$ witnesses $(27,6,3)$, $\alpha(27,3) = 8$, but there is no $A \supseteq B$ which witnesses $(27,7,3)$. A witness for $(27,8,3)$ is for example the set $\{0,1,3,4,9,10,12,13\}$.

Theorem 1.1. For all positive integers n, m, a, b and r we have:

$$(n,a,r) \ \textit{and}\ (m,b,r) \ \textit{implies}\ (nm,ab,r)\,.$$

Proof. For a sequence $\bar{z} = (z_0, \ldots, z_{n-1})$ of 0's and 1's, let $\chi_{\bar{z}} := \{i : z_i = 1\} \subseteq \mathbb{Z}_n$. Further, let $\mathbf{0}_n = \underbrace{(0,\ldots,0)}_{n-times}$. Suppose that $\bar{x} = (x_0 \ldots, x_{n-1})$ and $\bar{y} = (y_0, \ldots, y_{m-1})$ are such that $\chi_{\bar{x}}$ and $\chi_{\bar{y}}$ witness (n,a,r) and (m,b,r) respectively, then $\chi_{\bar{B}}$, where

$$\bar{B} = (B_{y_0}, \ldots, B_{y_{m-1}}) \text{ with } B_{y_i} = \begin{cases} \bar{x} & \text{if } y_i = 1, \\ \mathbf{0}_n & \text{otherwise,} \end{cases}$$

witnesses (nm,ab,r). Indeed, if $\chi_{\bar{B}}$ contains an arithmetic progression $(a_1, \ldots, a_r)$ of length r, then, since $\chi_{\bar{x}}$ witnesses (n,a,r), the sequence $(a_1 \bmod n, \ldots, a_r \bmod n)$ is constant. Thus, for every $1 \leq i \leq r$ we have $a_i = k_i \cdot n + c$, where $0 \leq k_i < m$ and $0 \leq c < n$. By construction, the k_i's belong to $\chi_{\bar{y}}$ and since $\chi_{\bar{y}}$ witnesses (m,b,r), all the k_i's must be equal, and therefore, the sequence $(a_1, \dots, a_r)$ is constant. Hence, $\chi_{\bar{B}}$ witnesses (nm, ab, r), which completes the proof. $\dashv$

As an immediate consequence of Theorem 1.1 we get the following:

Corollary 1.2. For all positive integers n, m, and r we have

$$\alpha(nm, r) \geq \alpha(n, r) \cdot \alpha(m, r)\,.$$

Remark. In general, the lower bound for $\alpha(nm, r)$ given in Corollary 1.2 is not sharp. For example, $\alpha(4, 4) = 2$, but $\alpha(16, 4) = 6$, witnessed by $\{0, 1, 2, 4, 5, 7\}$; and $\alpha(6, 3) = 2$, but $\alpha(36, 3) = 8$, witnessed by $\{0, 1, 3, 4, 9, 10, 12, 13\}$. Moreover, this lower bound is not even sharp if n and m are two distinct prime numbers. For example, $\alpha(5, 3) = 2$ and $\alpha(7, 3) = 3$, but $\alpha(35, 3) = 9$, witnessed by $\{0, 1, 3, 4, 10, 12, 22, 26, 28\}$.

For any positive integers n and $r \geq 3$, another lower bound for $\alpha(n, r)$ is given by the following:

Proposition 1.3. For any positive integers n and r, where $r \geq 3$, we have

$$\alpha(n, r) > \frac{\lfloor n/2 \rfloor}{\lfloor n/2 \rfloor^{c(s)/(\ln \lfloor n/2 \rfloor)^{s/s+1}}}\,,$$

where $\lfloor n/2 \rfloor$ is the greatest integer which is less than or equal to $n/2$, s is a positive integer such that $2^s < r \leq 2^{s+1}$ and $c(s) > 0$ is a constant depending only on s.

Proof. Let $m = \lfloor n/2 \rfloor$, $[m] = \{0, 1, \dots, m-1\}$ and let $\nu_r(m)$ be the cardinality of a largest set $A \subseteq [m]$, so that A does not contain any non-constant arithmetic progression with respect to $[m]$ of length r. Now, Robert Rankin proved in [Ra61] that $\nu_r(m) > m^{1-c(s)/(\ln m)^{s/s+1}}$, where s is such that $2^s < r \leq 2^{s+1}$ and $c(s)$ is a constant depending only on s. Hence, if $A \subseteq [m]$ is such that A does not contain any non-constant arithmetic progression with respect to $[m]$ of length r, then, since $n \geq 2m$, A does not contain any non-constant arithmetic progression with respect to $\mathbb{Z}_n$ of length r, which completes the proof. $\dashv$

2. Exact Values

The following table shows some exact value of $\alpha(n, r)$ for some small numbers n and for $r = 3$ and $r = 5$, respectively. The values of $\alpha(n, r)$ as well as the witnesses we found with the help of the programming language Prolog.

n	r	$\alpha(n, r)$	witness
9	3	4	{0, 1, 3, 4}
10	3	4	{0, 1, 3, 4}
11	3	4	{0, 1, 3, 4}
12	3	4	{0, 1, 3, 4}
17	3	5	{0, 1, 3, 7, 8}
18	3	5	{0, 1, 3, 7, 8}
19	3	6	{0, 1, 3, 12, 14, 15}
20	3	5	{0, 1, 3, 4, 9}
24	3	6	{0, 1, 3, 4, 9, 10}
25	3	7	{0, 1, 3, 4, 9, 10, 12}
27	3	8	{0, 1, 3, 4, 9, 10, 12, 13}
9	5	5	{0, 1, 2, 3, 5}
10	5	5	{0, 1, 2, 4, 8}
11	5	6	{0, 1, 2, 3, 5, 6}
12	5	6	{0, 1, 2, 3, 5, 10}
17	5	9	{0, 1, 2, 3, 5, 6, 7, 8, 10}
18	5	8	{0, 1, 2, 3, 5, 6, 7, 8}
19	5	10	{0, 1, 2, 3, 5, 6, 7, 8, 10, 12}
20	5	10	{0, 1, 2, 4, 5, 7, 8, 9, 13, 16}
24	5	11	{0, 1, 2, 3, 5, 6, 7, 8, 10, 11, 21}
25	5	16	{0, 1, 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 15, 16, 17, 18}
27	5	15	{0, 1, 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 15, 17, 25}

In the following we compute the exact value of $\alpha(n, r)$ for certain positive integers n and r. Let us begin with the case $n = r$.

FACT 2.1. If p is prime, then $\alpha(p, p) = p - 1$.

Proof. Obviously we have $\alpha(p, p) < p$. On the other hand, since p is prime, the set $\{0, 1, \ldots, p - 2\}$ witnesses $(p, p - 1, p)$. ⊣

THEOREM 2.2. If $n = m \cdot p$, where p is the smallest prime number dividing n, then $\alpha(n, n) = m(p - 1) = n(1 - 1/p)$.

Proof. For each h with $0 \leq h < m$, let $e_h := \{h + mi : 0 \leq i < p\}$. Notice that each e_h is equal to the set $h + m\mathbb{Z}_p = \{h + mi : i \in \mathbb{Z}_p\}$, which gives us an arithmetic preserving bijection between $\mathbb{Z}_p$ and e_h, and thus, each e_h is an arithmetic progressions preserving copy of $\mathbb{Z}_p$. Therefore, each e_h is an infinite non-constant arithmetic progression in $\mathbb{Z}_n$ with common difference $d = m$. Consider the hypergraph $H_{n,n} = (\mathbb{Z}_n, E_n)$, where E_n is the set of all arithmetic progressions of length n in $\mathbb{Z}_n$. Since each e_h has p elements and $p \leq n$, $e_h \in E_n$. Further, since p is prime, by Fact 2.1 we have $\alpha(p,p) = p-1$, which implies that for any j with $0 \leq j \leq p-1$, $e_h \setminus \{h + mj\} \notin E_n$. Finally, since there are m edges e_h and the e_h's are pairwise disjoint, we get $\alpha(n,n) \leq m(p-1)$.

On the other hand, the set $A = \{0, 1, \dots, m(p-1)-1\}$ witnesses $(n, m(p-1), n)$. Indeed, assume that $(a_1, \dots, a_n)$ is a non-constant arithmetic progression with common difference $d < n$, built with elements of A. Since $|A| = m(p-1)$, the arithmetic progression uses at least one element of A twice. Let $1 < k_0 \leq n$ be the least number such that $a_1 = a_{k_0} = a_1 + (k_0 - 1)d$. Then $(k_0 - 1)d = \ell n$, which implies that $\{a_1 + k\frac{d}{\ell} : 0 \leq k < k_0\} = \{a_i : 1 \leq i \leq k_0\}$. Because of the gap of length m in A, $\frac{d}{\ell} > m$, but since m is the greatest proper divisor of n, this is a contradiction.

Therefore we have $\alpha(n,n) = m(p-1)$, which completes the proof. $\dashv$

As an immediate consequence of Theorem 2.2 we get the following:

Corollary 2.3. For any positive integer m we have $\alpha(2m, 2m) = m$.

Moreover, combining Fact 2.1 and Corollary 1.2 we get the following:

Corollary 2.4. For any prime number p and any non-negative integer k, $\alpha(p^k, p) \geq (p-1)^k$.

Moreover, by Proposition 1.3, for large numbers k and for prime numbers $p > 2$ we have $\alpha(p^k, p) > (p-1)^k$. To see this, let $\varepsilon(k) = \frac{c(s)}{(\ln \lfloor \frac{p^k}{2} \rfloor)^{s/s+1}}$ and note that since $\lim_{k\to\infty} \ln \lfloor \frac{p^k}{2} \rfloor^{s/s+1} \to \infty$ we get $\lim_{k\to\infty} \varepsilon(k) \to 0$. Therefore, by taking the logarithm on both sides of the following expression, one verifies that for k large enough we have

$$\left(\lfloor \frac{p^k}{2} \rfloor \right)^{1-\varepsilon(k)} > (p-1)^k \,,$$

and since $\alpha(p^k, p) > \left(\lfloor \frac{p^k}{2} \rfloor \right)^{1-\varepsilon(k)}$ (by Proposition 1.3), it follows that for k large enough we have $\alpha(p^k, p) > (p-1)^k$. Thus, the lower bound for $\alpha(p^k, p)$ given in Corollary 2.4 is in general not sharp. On the other hand, this lower bound is sharp for $k = 2$. Before we can prove this result we have to introduce some terminology.

An **affine plane of order *p***, where p is prime, is a set P containing p^2 points, together with $p+1$ so-called **parallel classes** consisting of subsets of P which are called **lines**, such that the following hold:

(i) Each parallel class contains p pairwise disjoint lines.
(ii) Each line contains p points of P.
(iii) For any two distinct points of P, there is exactly one line in some parallel class which contains these two points.

THEOREM 2.5. For any prime number p we have $\alpha(p^2, p) = (p-1)^2$.

Proof. By Corollary 2.4 we get $\alpha(p^2, p) \geq (p-1)^2$. Now, Robert Jamison in [Ja77] and Andries Brouwer and Alexander Schrijver in [BS78] have shown that a set which intersects each line of the affine plane of order p, *i.e.*, a transversal, must contain at least $2p-1$ points. Notice that the complement of a set which intersects each line of an affine plane cannot contain a line. Thus, in order to prove Theorem 2.5 it is enough to prove that there exists an affine plane of order p such that each line forms an arithmetic progression with respect to $\mathbb{Z}_{p^2}$, since we then can conclude that $\alpha(p^2, p) \leq p^2 - (2p-1) = (p-1)^2$.

So, let us show that there is an affine plane of order p such that every line forms an arithmetic progression of length p. Let $\{a_{i,j} : 0 \leq i, j < p\}$ be the set of points, where $a_{i,j} := i + jp$ (for all $0 \leq i, j < p$). The $p^2 + p$ lines ℓ are defined as follows: For $0 \leq j < p$ and $0 \leq s < p$ let $\ell_{j,s} := \{a_{i,(si+j) \bmod p} : 0 \leq i < p\}$ and let $\ell_{j,p} := \{a_{j,i} : 0 \leq i < p\}$. By construction, for fixed j, $\{\ell_{j,s} : 0 \leq s \leq p\}$ is the set containing the $p+1$ lines going through $a_{0,j}$, and for any s with $0 \leq s \leq p$, the set $C_s = \{\ell_{j,s} : 0 \leq j < p\}$ consists of p parallel lines, *i.e.*, is a parallel class. Now, for every $0 \leq j < p$ and every $0 \leq s \leq p$, $\ell_{j,s}$ forms an arithmetic progression with respect to $\mathbb{Z}_{p^2}$. Indeed, for $0 \leq s < p$, $\ell_{j,s}$ forms an arithmetic progression with common difference $sp+1$ and $\ell_{j,p}$ forms an arithmetic progression with common difference p. Further, for any two distinct points, there is exactly one line (in some parallel class C_s) which contains these two points.

Thus, for every prime number p there exists an affine plane of order p such that each line forms an arithmetic progression with respect to $\mathbb{Z}_{p^2}$, which completes the proof. $\dashv$

The proof of the Jamison-Brouwer-Schrijver result is algebraic, using polynomial equations over a finite field, and no combinatorial proof is known (*cf.* [Ju01, Problem 3.13$^+$]). In the case of $p = 3$ or $p = 5$, we were able to prove the equation $\alpha(p^2, p) = (p-1)^2$ in a purely combinatorial way. However, since the proof is already awkward for $p = 5$, it is difficult to see how it could be extended to larger primes. In the following we like to present a combinatorial proof just for the case of $p = 3$:

PROPOSITION 2.6. $\alpha(9, 3) = 4$.

Proof. By Corollary 2.4 we get $\alpha(9, 3) \geq 4$. So, assume towards a contradiction that there is a set $\tilde{A} \subseteq \mathbb{Z}_9$ which witnesses $(9, 5, 3)$, or in other words, assume that $\tilde{A} \subseteq \mathbb{Z}_9$ is a set with five elements which does not contain any non-constant arithmetic progression of length 3. Let M_9 be the 3×3-matrix

$$M_9 = \begin{pmatrix} 0 & 3 & 6 \\ 1 & 4 & 7 \\ 2 & 5 & 8 \end{pmatrix}$$

and let R_1, R_2 and R_3 be the rows of M_9. Since each row R_i is equal to the set $i+3\mathbb{Z}_3$, each row is an arithmetic progressions preserving copy of $\mathbb{Z}_3$, and since $\alpha(3,3)=2$ for each $1 \le i \le 3$, we have $|\tilde{A} \cap R_i| \le 2$ (where $|\tilde{A} \cap R_i|$ denotes the cardinality of the set $\tilde{A} \cap R_i$). Further, since $|\tilde{A}| = 5$, there must be two rows, say R_1 and R_2, such that $|\tilde{A} \cap R_1| = |\tilde{A} \cap R_2| = 2$, which—by checking the 9 possible cases—implies that $\tilde{A} \cap R_3 = \emptyset$, and hence, $\tilde{A}$ does not witness $(9,5,3)$, which completes the proof. $\dashv$

As we have seen above, for any prime number $p > 2$ and sufficiently large k we have $\alpha(p^k, p) > (p-1)^k$. On the other hand, we also have seen that $\alpha(p^2, p) = (p-1)^2$ holds for any prime number p. Thus, it still might be the case that the equation $\alpha(p^3, p) = (p-1)^3$ holds for all prime numbers p. A first step towards this conjecture is the following:

PROPOSITION 2.7. $\alpha(27,3) = 8$.

Proof. By Corollary 2.4 we get $\alpha(27,3) \ge 8$. So, assume towards a contradiction that there is a set $\tilde{A} \subseteq \mathbb{Z}_{27}$ which witnesses $(27,9,3)$. Let M_{27} be the 3×9-matrix

$$M_{27} = \begin{pmatrix} 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \\ 1 & 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 \\ 2 & 5 & 8 & 11 & 14 & 17 & 20 & 23 & 26 \end{pmatrix}$$

and let R_1, R_2 and R_3 be the rows of M_{27}. Since each row R_i is an arithmetic progressions preserving copy of $\mathbb{Z}_9$ and $\alpha(9,3) = 4$, for each $1 \le i \le 3$, $|\tilde{A} \cap R_i| \le 4$. We partition $\mathbb{Z}_{27}$ into the three pairwise disjoint sets

$$\begin{aligned} T_1 &= \{0,1,2,9,10,11,18,19,20\}, \\ T_2 &= \{3,4,5,12,13,14,21,22,23\}, \\ T_3 &= \{6,7,8,15,16,17,24,25,26\}. \end{aligned}$$

Let $j,k,l \in \{1,2,3\}$ be three distinct numbers. The three sets T_1, T_2 and T_3 are such that for each i with $1 \le i \le 3$ we have

$$R_i \cap \tilde{A} \cap T_j \neq \emptyset \textit{ and } R_i \cap \tilde{A} \cap T_k \neq \emptyset \textit{ implies } R_i \cap \tilde{A} \cap T_l = \emptyset\,. \qquad (\sharp)$$

Indeed, let $a \in R_i \cap T_j$ and $b \in R_i \cap T_k$. Then there are three different arithmetic progression of length 3 through a and b, say $\{a,b,c_1\}$, $\{a,b,c_2\}$ and $\{a,b,c_3\}$, and by construction we have $\{c_1,c_2,c_3\} = R_i \cap T_l$. Since $|\tilde{A}| = 9$, there must be two rows, say R_1 and R_2, such that $|\tilde{A} \cap R_1| \ge 3$ and $|\tilde{A} \cap R_2| \ge 3$. Hence, by $(\sharp)$, there must be $j_1, j_2 \in \{1,2,3\}$ such that $|R_1 \cap \tilde{A} \cap T_{j_1}| = |R_2 \cap \tilde{A} \cap T_{j_2}| = 2$. Consider the hypergraph $H_{27,3} = (\mathbb{Z}_{27}, E)$, where E consists of all instances of arithmetic progressions of length 3 in $\mathbb{Z}_{27}$. For $a \in R_1 \cap \tilde{A} \cap T_{j_1}$ and $b \in R_2 \cap \tilde{A} \cap T_{j_2}$ let $S_{a,b} = \big\{c \in R_3 : \{a,b,c\} \in E\big\}$. Then $|S_{a,b}| = 3$ and it is easy to see that $|S_{a,b} \cap T_1| = |S_{a,b} \cap T_2| = |S_{a,b} \cap T_3| = 1$. Moreover, for $\{a_1,a_2\} = R_1 \cap \tilde{A} \cap T_{j_1}$ and $\{b_1,b_2\} = R_2 \cap \tilde{A} \cap T_{j_2}$ we have

$$S_{a_1,b_1} \cup S_{a_1,b_2} \cup S_{a_2,b_1} \cup S_{a_2,b_2} = R_3\,, \qquad (*)$$

which implies that $\tilde{A} \cap R_3 = \emptyset$, and hence, $\tilde{A}$ does not witness $(27,9,3)$. Let us illustrate $(*)$ with the following example: Let $j_1 = 1$, $a_1 = 0$, $a_2 = 9$, and $j_2 = 3$, and consider the six arithmetic progressions of length 3 going through a_1 or a_2, $R_2 \cap T_3$, and $R_3 \cap T_3$:

a_1	$R_2 \cap T_3$	$R_3 \cap T_3$	a_2	$R_2 \cap T_3$	$R_3 \cap T_3$
0	7	17	9	7	8
0	16	8	9	16	26
0	25	26	9	25	17

Hence, no matter which two numbers b_1 and b_2 we take from $R_2 \cap T_3$, we always have

$$(R_3 \cap T_3) = (S_{0,b_1} \cap T_3) \cup (S_{0,b_2} \cap T_3) \cup (S_{9,b_1} \cap T_3) \cup (S_{9,b_2} \cap T_3)\,,$$

which, by symmetry, is true for any choice of a_1 and a_2 from $R_1 \cap T_1$. Thus, we have

$$(R_3 \cap T_3) = (S_{a_1,b_1} \cap T_3) \cup (S_{a_1,b_2} \cap T_3) \cup (S_{a_2,b_1} \cap T_3) \cup (S_{a_2,b_2} \cap T_3)\,.$$

Considering the six arithmetic progressions of length 3 going through a_1 or a_2, $R_2 \cap T_2$, and $R_3 \cap T_2$, we get

$$(R_3 \cap T_2) = (S_{a_1,b_1} \cap T_2) \cup (S_{a_1,b_2} \cap T_2) \cup (S_{a_2,b_1} \cap T_2) \cup (S_{a_2,b_2} \cap T_2)\,.$$

Similarly, by considering the six arithmetic progressions of length 3 going through a_1 or a_2, $R_2 \cap T_1$, and $R_3 \cap T_1$, we get

$$(R_3 \cap T_1) = (S_{a_1,b_1} \cap T_1) \cup (S_{a_1,b_2} \cap T_1) \cup (S_{a_2,b_1} \cap T_1) \cup (S_{a_2,b_2} \cap T_1)\,.$$

Thus, we finally have

$$R_3 = (R_3 \cap T_1) \cup (R_3 \cap T_2) \cup (R_3 \cap T_3) = S_{a_1,b_1} \cup S_{a_1,b_2} \cup S_{a_2,b_1} \cup S_{a_2,b_2}\,.$$

$\dashv$

3. Summary

The function $\alpha(n,r)$ is monotone in r but not monotone in n. However, for any positive integers n, m and r we have $\alpha(nm,r) \geq \alpha(n,r) \cdot \alpha(m,r)$. In particular, for any positive integers n, k, and r we have $\alpha(n^k,r) \geq \alpha(n,r)^k$, which implies that for any prime number p, $\alpha(p^k,p) \geq \alpha(p,p)^k = (p-1)^k$. On the one hand, for each prime number $p > 2$ there are integers k such that $\alpha(p^k,p) > (p-1)^k$, but on the other hand, for every prime number p we have $\alpha(p^2,p) = (p-1)^2$ and $\alpha(p,p) = (p-1)$. In addition we have seen that $\alpha(3^3,3) = 2^3$ (Proposition 2.7) but the authors were not able to prove $\alpha(5^3,5) = 4^3$, since the proof of Proposition 2.7 seems not generalisable. This leads to the open question whether $\alpha(p^3,p) = (p-1)^3$ for all primes p larger than 3 (the authors could not agree what they expect to be the answer). Further, we have seen that for any positive integer n, $\alpha(n,n) = n\bigl(1 - \frac{1}{p}\bigr)$, where p is the smallest prime number dividing n. In particular, for any positive integer m we have $\alpha(2m,2m) = m$.

References

[Be89] Claude Berge: ***Hypergraphs: Combinatorics of Finite Sets***, North-Holland $\{Mathematical Library, vol.\ 45\}$, Amsterdam (1989).

[BS78] Andries E. Brouwer and Alexander Schrijver: *The blocking number of an affine space*, ***Journal of Combinatorial Theory (A)***, vol. 24 (1978), 251–253.

[Ja77] Robert E. Jamison: *Covering finite fields with cosets of subspaces*, ***Journal of Combinatorial Theory (A)***, vol. 22 (1977), 253–266.

[Ju01] Stasys Jukna: ***Extremal Combinatorics: With Applications in Computer Science***, Springer-Verlag, Berlin et al. (2001).

[Ra61] Robert A. Rankin: *Sets of integers containing not more than a given number of terms in arithmetical progression*, ***Proceedings of the Royal Society of Edinburgh (A)***, vol. 65 (1960/61), 332–344.

Department of Pure Mathematics
Queen's University Belfast
Belfast, BT7 1NN (Northern Ireland)

halbeis@qub.ac.uk

s.halbeisen@att.net