Jakob Führer, BSc

Maximal m-progression-free sets in $\mathbb{Z}_m^n$

MASTER'S THESIS

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Mathematics

submitted to

Graz University of Technology

Supervisor

Assoc.Prof. Dipl.-Math. Dr.rer.nat.habil.
Christian Elsholtz

Institute of Analysis and Number Theory

Graz, April 2021

Affidavit

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitely indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis.

Date	Signature

Abstract

In this master thesis we study subsets of $\mathbb{Z}_m^n := (\mathbb{Z}/m\mathbb{Z})^n$ that do not contain progressions of length m. We denote by $r_m(\mathbb{Z}_m^n)$ the cardinality of such subsets containing a maximal number of elements and try to give upper and lower bounds on $r_m(\mathbb{Z}_m^n)$.

For odd prime numbers $m = p$, $r_p(\mathbb{Z}_p^n) = (p-1)^n$ was already known for $n = 1$ and $n = 2$, we however prove that $r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + \frac{p-1}{2}$ holds. We establish a new method to find upper bounds, in particular we get $r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + 1$.

For composite m we provide the biggest side length of a hypercube in $\mathbb{Z}_m^n$ that does not contain progressions of length m and use the probabilistic method to show that the corresponding lower bound for $r_m(\mathbb{Z}_m^n)$ is asymptotically not optimal in general.

For $m = 6$ we present constructions of progression-free sets showing $r_6(\mathbb{Z}_6^n) \geq \max\{3^n + 2n3^{n-1} + n(n-1)3^{n-2}, 4^n + n3^{n-1}\}$.

Finally we use integer programming to find exact values and lower bounds for individual m and n, in particular $r_5(\mathbb{Z}_5^3) \geq 69$ which can be used to give the asymptotic lower bound 4.041^n for $r_5(\mathbb{Z}_5^n)$.

Kurzfassung

In dieser Masterarbeit untersuchen wir Teilmengen von $\mathbb{Z}_m^n := (\mathbb{Z}/m\mathbb{Z})^n$ die keine Progressionen der Länge m enthalten. Wir bezeichnen mit $r_m(\mathbb{Z}_m^n)$ die Kardinaltät einer solchen Teilmenge mit einer maximalen Anzahl an enthaltenen Elementen und versuchen obere und untere Schranken für $r_m(\mathbb{Z}_m^n)$ zu finden.

Für ungerade Primzahlen $m = p$ wurde $r_p(\mathbb{Z}_p^n) = (p-1)^n$ bereits für $n = 1$ und $n = 2$ gezeigt, wir aber beweisen, dass $r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + \frac{p-1}{2}$ gilt. Wir ermitteln eine neue Methode um obere Schranken zu finden und bekommen so $r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + 1$.

Für zusammengesetzte m stellen wir die längste Seitenlänge eines Hyperwürfels in $\mathbb{Z}_m^n$ bereit, der keine Progressionen der Länge m enthält und benutzen probabilistische Methoden um zu zeigen, dass die dazugehörige untere Schranke für $r_m(\mathbb{Z}_m^n)$ im Allgemeinen asymptotisch nicht optimal ist.

Für $m = 6$ stellen wir Konstruktionen von progressionsfreien Mengen vor, die zeigen dass $r_6(\mathbb{Z}_6^n) \geq \max\{3^n + 2n3^{n-1} + n(n-1)3^{n-2}, 4^n + n3^{n-1}\}$ gilt.

Schlussendlichen verwenden wir ganzzahlige lineare Optimierung um exakte Werte und untere Schranken für bestimmte m und n zu finden, im Besonderen $r_5(\mathbb{Z}_5^3) \geq 69$ welche verwendet werden kann um die asymptotische untere Schranke 4.041^n für $r_5(\mathbb{Z}_5^n)$ zu zeigen.

Acknowledgement

First of all, I would like to thank Prof. Christian Elsholtz for supervising this thesis, for giving me a lot of ideas I could work on and most importantly, for introducing me to the very interesting topic of progression-free-sets.

Another big thanks goes to my parents and my sister, who prepared me well for life as a student and making it possible for me to study.

Finally, I would like to thank my girlfriend and all of my friends for their support and giving me a wonderful time here in Graz.

Contents

List of Figures

1 Introduction

Arithmetic progressions may be one of the oldest concepts in mathematics. The idea of starting at a fixed point a and getting to every other desired point by recursively adding a constant b is on the one hand very easy to understand and on the other hand essential to a whole field of mathematics, as induction, which is probably the foundation of all of discrete mathematics, relies on the simplest progression $\{1 + 1i | i \in \mathbb{N}\}$.

One is however not restricted to natural numbers or points in space when using progressions. One particular beautiful example are the progressions in $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ for a prime number p, where a progression reaches every possible value for every starting point a and every non-zero step length b. The progression also repeats itself which leads us to stop looking at an infinite series but at sets with p elements now called p-progressions. When we go up into the multidimensional case $\mathbb{Z}_p^n$ we can also change our perspective and see p-progressions as lines or 1-dimensional affine subspaces.

Now the problem arises how to avoid p-progressions, or more precisely: Can we find subsets of $\mathbb{Z}_p^n$ that do not contain p-progression, and can we make these subsets as large as possible? As soon as we look at these p-progression-free sets, which try to avoid structure, we do not have any simple rules to apply and finding maximal ones is far from trivial. There is however one property we can use: We can project any p-progression down to one dimension and it will there again visit every possible value. Therefore, a n-dimensional hypercube with side length $p - 1$ will not contain any p-progression and we have our first trivial p-progression-free sets.

It was already shown that these hypercubes are indeed maximal p-progression-free sets for dimension one and two and one could guess now that that the same is true for any dimension. However, we could show that as soon as dimension three there are larger p-progression-free sets for any odd prime p. There are also some techniques to lift progression-free sets into higher dimensions, which means using these sets to construct higher dimensional sets that have similar structure. Consequently, the hypercubes are also not maximal in every higher dimension.

When giving up on the restricting that p is a prime number and looking at m-progression-free sets in $\mathbb{Z}_m^n$ for arbitrary natural numbers m the problem changes considerably. We can no longer guarantee that a non-zero step length b gives us an m-progression, as the progression could end up on the starting point after an amount of steps that is a proper divisor of m. We can no longer use facts about vector spaces

and there is very little previous work by other authors. It will be a common theme in this thesis that theorems either only hold for prime numbers or that the corresponding consequences are very weak for composite numbers m.

After formally introducing the problem and discuss fundamental properties in Chapter 2 we will present some lower bounds for the number of elements in a maximal m-progression-free sets in Chapters 3 and 4. While Chapter 3 only covers the n-dimensional hypercube, Chapter 4 deals with other techniques that lead to better lower bounds in certain cases.

In Chapter 5 we accordingly provide some upper bounds for m-progression-free sets and get the first exact results. This is followed by Chapter 6, where we discuss techniques to lift progression-free sets into higher dimensions and look at the asymptotic behaviour as the dimension n tends to infinity.

We finally continue to try to beat lower bounds, first in Chapter 7 with manually constructing m-progression-free sets and then in Chapter 8 by computer calculations.

2 Principles

In this section we provide a clear definition of what we understand by progressions and discuss how basic number theoretic properties apply to them. We also want to formalize our optimisation problem and lay the foundation for the following chapters by presenting some auxiliary results.

2.1 Problem Definition

Definition 1. Let $(A, +)$ be an abelian group and $k \in \mathbb{N}$. A subset $L \subseteq A$ with $|L| = k$ is called k-progression if there exist $a, b \in A$ such that

$$L = \{a + bi | i \in [0, k-1]\}.$$

A subset $S \subseteq A$ is called k-progression-free if it does not contain any k-progression.

Note that in our case of the groups of type $\mathbb{Z}_m^n := (\mathbb{Z}/m\mathbb{Z})^n$ not every set of the form

$$\{a + bi | i \in [0, k-1]\}$$

is a k-progression, not even if we assume $b \neq 0$. Some authors are skipping the condition $|L| = k$ but we will stick with it which could result in some bigger k-progression-free sets.

Now we get to the goal of this work, to maximize progression-free sets.

Definition 2. Let $(A, +)$ be an abelian group and $k \in \mathbb{N}$. Let $\mathcal{S} := \{S \subseteq A | S \text{ is } k\text{-progression-free}\}$. We define

$$r_k(A) := \max_{S \in \mathcal{S}} |S|.$$

Definition 3. Let $m, k \in \mathbb{N}$. We define

$$\alpha_{k,m} := \lim_{n \to \infty} (r_k(\mathbb{Z}_m^n))^{1/n}$$

if the limit exists.

We will see that for m as a prime power the limit in Definition 3 always exists. It is natural to measure progression-free sets in this way, as $|\mathbb{Z}_m^n|$ grows exponentially as n tends to infinity.

2.2 Number theoretic foundation

We now take a look at how progressions in $\mathbb{Z}_m^n$ behave in only one coordinate. This will also help us determining if a set of the form

$$\{a + bi | i \in [0, m-1]\}$$

is an m-progression.

Lemma 1. *Let $m \in \mathbb{N}$, $n \in \mathbb{N}$, $j \in [1, n]$ and $L := \{a + bi | i \in [0, m-1]\}$ be an m-progression in $\mathbb{Z}_m^n$ with $a := (a_1, a_2, ..., a_n) \in \mathbb{Z}_m^n$ and $b := (b_1, b_2, ..., b_n) \in \mathbb{Z}_m^n$. If $\gcd(b_j, m) = 1$ then*

$$\{a_j + b_j i | i \in [0, m-1]\} = [0, m-1].$$

Proof. b_j is a unit of $(\mathbb{Z}_m, *)$, therefore

$$\{a_j + b_j i | i \in [0, m-1]\} = a_j + b_j\mathbb{Z}_m = a_j + \mathbb{Z}_m = \mathbb{Z}_m = [0, m-1].$$

□

Lemma 2. *Let $m \in \mathbb{N}$, $n \in \mathbb{N}$, $j \in [1, n]$ and $L := \{a + bi | i \in [0, m-1]\}$ be an m-progression in $\mathbb{Z}_m^n$ with $a := (a_1, a_2, ..., a_n) \in \mathbb{Z}_m^n$ and $b := (b_1, b_2, ..., b_n) \in \mathbb{Z}_m^n$. Let $d := \gcd(b_j, m)$ then*

$$\{a_j + b_j i | i \in [0, m-1]\} = \{a_j + di | i \in [0, \frac{m}{d} - 1]\}$$

Proof. Let $k, l \in \mathbb{Z}$ be such that $1 = km + l\frac{b_j}{d}$ and therefore $d = dkm + lb_j$. Obviously $\gcd(m, l) = 1$ and thus l is a unit of $(\mathbb{Z}_m, *)$. It follows that

$$d\mathbb{Z}_m = dkm\mathbb{Z}_m + b_j l\mathbb{Z}_m = 0 + b_j\mathbb{Z}_m = b_j\mathbb{Z}_m$$

and consequently

$$\{a_j + b_j i | i \in [0, m-1]\} = a_j + b_j\mathbb{Z}_m = a_j + d\mathbb{Z}_m = \{a_j + di | i \in [0, \frac{m}{d} - 1]\}$$

□

Here we can already see how the divisors of m will play a huge role in the analysis of progressions of $\mathbb{Z}_m^n$. Consequently, if m is a prime, we are only left with the cases that $a_j + b_j i$ runs through all possible values or the coordinate does not change at all.

In most cases a notation of the form

$$\{a + bi | i \in [0, m-1]\}$$

will not be unique to describe a certain m-progression. The next result will show that for prime m we can even pick an arbitrary element of the progression as a and an arbitrary distance between two elements in the progression as b to get a correct description.

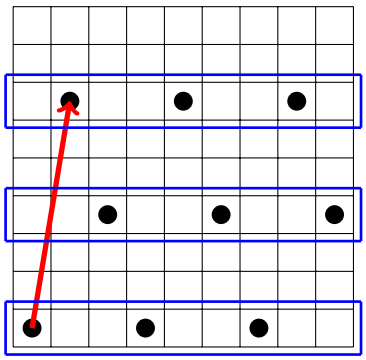


Figure 2.1: Example in $\mathbb{Z}_9^2$:
As the vector $b = (1, 6)$ and $\gcd(9, 6) = 3$, the progression has only points in every third row.

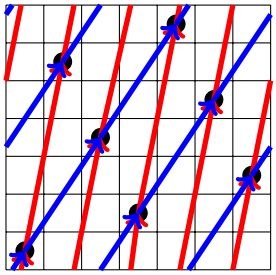


Figure 2.2: Example in $\mathbb{Z}_7^2$:
Different vectors can generate the same progression.

Lemma 3. *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$ and $L := \{a + bi | i \in [0, p-1]\}$ be a p-progression in $\mathbb{Z}_p^n$ with $a, b \in \mathbb{Z}_p^n$. Choose $j, k \in [0, p-1]$ arbitrarily with $j \neq k$, then we can rewrite*

$$L = \{a' + b'i | i \in [0, p-1]\}$$

with $a' := a + bj$ and $b' := b(k - j) = (a + bk) - (a + bj)$.

Proof. Since $j \neq k$, $k - j$ is a unit in $\mathbb{Z}_p$. Therefore

$$\{a' + b'i | i \in [0, p-1]\} = a' + b'\mathbb{Z}_p = a' + b(k-j)\mathbb{Z}_p = a' + b\mathbb{Z}_p$$

and since $bj \in b\mathbb{Z}_p$,

$$a' + b\mathbb{Z}_p = a + bj + b\mathbb{Z}_p = a + b\mathbb{Z}_p = L.$$

□

As an immediate conclusion we get that in the prime case two progressions meet at most in one common point.

Corollary 1. *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$ and L, L' be different p-progressions in $\mathbb{Z}_p$ and $L \cap L' \neq \emptyset$. Then*

$$|L \cap L'| = 1.$$

Proof. Assume to the contrary that a, a' are different elements of $L \cap L'$. From Lemma 3 we know that

$$L = a + (a' - a)\mathbb{Z}_p = L',$$

which contradicts the definition of L and L'. □

The final Lemma in this subsection describes an easy way to check if a set is an m-progression.

Lemma 4. *Let $m \in \mathbb{N}$, $n \in \mathbb{N}$, $j \in [1, n]$ and $L := \{a + bi | i \in [0, m-1]\}$ with $a \in \mathbb{Z}_m^n$ and $b := (b_1, b_2, ..., b_n) \in \mathbb{Z}_m^n$. Then L is an m-progression in $\mathbb{Z}_m^n$ if and only if*

$$\gcd(b_1, b_2, ..., b_n, m) = 1.$$

Proof. Let $d := \gcd(b_1, b_2, ..., b_n, m)$. Our goal is to count the elements of L in relation to d. It holds that

$$a + b\frac{m}{d} = a + (\frac{b_1}{d}m, \frac{b_2}{d}m, ..., \frac{b_n}{d}m) = a + (0, 0, ..., 0) = a.$$

If we can show that

$$bj \neq 0, \quad \forall j \in [1, \frac{m}{d} - 1]$$

then

$$a, a + b1, a + b2, ..., a + b(\frac{m}{d} - 2), a + b(\frac{m}{d} - 2), a + b(\frac{m}{d} - 1)$$

are pairwise different. It follows that $|L| = \frac{m}{d}$, which proves the lemma. Assume to the contrary that there exists $j \in [1, \frac{m}{d} - 1]$ with $bj = 0$. Define $\tilde{b}_i := \frac{b_i}{d}$ for $i \in [1, n]$. It holds that $m | jd\tilde{b}_i$ for all $i \in [1, n]$ and thus also

$$m | jd \gcd(\tilde{b}_1, \tilde{b}_2, ..., \tilde{b}_n).$$

Since $\frac{m}{d}$ and $\gcd(\tilde{b}_1, \tilde{b}_2, ..., \tilde{b}_n)$ are coprime, it follows that $m | jd$. Now $jd < \frac{m}{d}d = m$, so $jd = 0$ contradicting the definition of d and j. □

Remark 1. Note that even in the case $\gcd(b_1, b_2, ..., b_n, m) = d \neq 1$, the proof also shows that L is an $\frac{m}{d}$-progression.

2.3 Counting progressions

Now we want to focus on counting the number of m-progressions in $\mathbb{Z}_m^n$ and therefore possible m-progressions in subsets of $\mathbb{Z}_m^n$ which we try to avoid. Apart from being an interesting topic on its own, this will also help us determine upper and lower bounds for our maximization problem.

We start with the related topic of counting subspaces of final vector spaces over finite fields. As one can easily see from the description of p-progressions in $\mathbb{Z}_p^n$ where p and $b \neq 0$is prime as

$$a + b\mathbb{Z}_p$$

, the p-progressions are exactly the affine 1-dimensional subspaces of $\mathbb{Z}_p^n$.

Lemma 5 ([18])**.** *Let $q = p^n$ with $p \in \mathbb{P}$ and $n \in \mathbb{N}$. Furthermore, let $k, t \in \mathbb{N}$ satisfying $t \leq k \leq n$. Then the number of k-dimensional subspaces of $\mathbb{F}_q$ is*

$$\frac{(q^n-1)(q^n-q)...(q^n-q^{k-1})}{(q^k-1)(q^k-q)...(q^k-q^{k-1})}$$

and more generally, the number of k-dimensional subspaces of $\mathbb{F}_q$ containing a fixed t-dimensional subspace is

$$\frac{(q^{n-t}-1)(q^{n-t}-q)...(q^{n-t}-q^{k-t-1})}{(q^{k-t}-1)(q^{k-t}-q)...(q^{k-t}-q^{k-t-1})}.$$

Lemma 6. *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$ and $x \in \mathbb{Z}_p^n$. Then there are $\frac{p^n-1}{p-1}$ pairwise different p-progressions in $\mathbb{Z}_p^n$ containing x.*

Proof. W.l.o.g let $x = 0$. Then the p-progressions containing x are exactly the 1-dimensional subspaces of $\mathbb{Z}_p^n$ and by Lemma 5 there are

$$\frac{p^n-1}{p-1}$$

of these. □

Lemma 7. *Let $p \in \mathbb{P}$ and $n \in \mathbb{N}$ then there are*

$$\frac{\binom{p^n}{2}}{\binom{p}{2}} = \frac{p^{n-1}(p^n-1)}{p-1}$$

pairwise different p-progressions in $\mathbb{Z}_p^n$.

Proof. We prove this by double counting the set of pairs

$$D = \{(x, L) | x \in \mathbb{Z}_p^n, L \text{ is a } p\text{-progression in } \mathbb{Z}_p^n \text{ with } x \in L\}.$$

Let N be the number of p-progressions in $\mathbb{Z}_p^n$. By the previous lemma, we know that

$$|D| = p^n \frac{p^n - 1}{p - 1}$$

and since every p-progressions contains p-elements, we know that

$$|D| = pN.$$

In conclusion

$$\begin{aligned} pN &= p^n \frac{p^n - 1}{p - 1} \\ \Leftrightarrow \qquad N &= p^{n-1} \frac{p^n - 1}{p - 1} \end{aligned}$$

□

For non-prime m it is far more challenging to count the exact number of m-progressions but as we only need the result for an asymptotic bound, we are satisfied with the following rough estimate.

Lemma 8. *Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$ then there are at most*

$$\frac{\binom{m^n}{2}}{m} = \frac{m^{n-1}(m^n - 1)}{2}$$

pairwise different m-progressions in $\mathbb{Z}_m^n$.

Proof. Again, we prove this by double counting. Consider the set

$$D = \{(a, a + b, L) | L = \{a + bi | i \in \mathbb{Z}_m\} \text{is an } m\text{-progression in } \mathbb{Z}_m \text{ with } a, b \in \mathbb{Z}_m^n\}.$$

It holds that for fixed $(a, a + b, L) \in D$,

$$\{(a + ib, a + (i + 1)b, L) | i \in [0, m - 1]\} \subseteq D$$

and

$$\{(a + ib, a + (i - 1)b, L) | i \in [0, m - 1]\} \subseteq D,$$

which means that for every m-progression there are at least $2m$ elements in D. In other words

$$|D| \geq 2mN.$$

On the other hand, we consider the set

$$D' := \{(a, a + b, L) | a \in \mathbb{Z}_m^n, b \in \mathbb{Z}_m^n \setminus \{0\}, L = \{a + bi | i \in \mathbb{Z}_m\}\} \supseteq D,$$

which contains $m^n(m^n - 1)$ elements.

To sum things up

$$N \leq \frac{|D|}{2m} \leq \frac{|D'|}{2m} = \frac{m^n(m^n - 1)}{2m} = \frac{\binom{m^n}{2}}{m}.$$

□

3 Trivial Lower Bounds

The first idea that comes to mind when constructing a progression-free set is to take an n-dimensional cube

$$[0, l-1]^n$$

in $\mathbb{Z}_m^n$ for which we can assure that it contains no m-progression. We can then immediately conclude

$$r_m(\mathbb{Z}_m^n) \geq l^n$$

and therefore

$$\alpha_{m,m} \geq l$$

if it exists.

In this chapter we will present the best lower bounds one can achieve with this idea and for the rest of the work it will be our objective to beat these bounds.

Theorem 1. *Let $m = p^k$ with $p \in \mathbb{P}$, $k \in \mathbb{N}$ and $n \in \mathbb{N}$. Then*

$$r_m(\mathbb{Z}_m^n) \geq (m-1)^n.$$

Proof. Consider the set $S := [0, m-2]^n$. We show that S is m-progression-free. Let $L := \{a + bi | i \in [0, m-1]\}$ be an m-progression in $\mathbb{Z}_m^n$ with $a, b \in \mathbb{Z}_m^n$. Since L is an m-progression, there is a $j \in [0, m-1]$ with $\gcd(p, b_j) = 1$. Therefore $\{a_j + b_j i | i \in [0, m-1]\} = [0, m-1]$ and thus $L \not\subseteq S$. □

Theorem 2. *Let $m = \prod_{i=1}^{s} p_i^{\lambda_i}$ with $s \geq 2$, $n \in \mathbb{N}$, $p_i \in \mathbb{P}$ and $\lambda_i \in \mathbb{N}$ $\forall i \in [1, s]$ such that $p_1^{\lambda_1} < p_2^{\lambda_2} < ... < p_s^{\lambda_s}$. Then*

$$r_m(\mathbb{Z}_m^n) \geq (m - \frac{m}{p_s^{\lambda_s}})^n.$$

Proof. Consider the set $S := [0, m - \frac{m}{p_s^{\lambda_s}} - 1]^n$. We show that S is m-progression-free. Let $L := \{a + bi | i \in [0, m-1]\}$ be an m-progression in $\mathbb{Z}_m^n$ with $a, b \in \mathbb{Z}_m^n$. Since L is an m-progression there is a $j \in [0, m-1]$ with $\gcd(p_s, b_j) = 1$. We can write $\{a_j + b_j i | i \in [0, m-1]\} = \{c + di | i \in [0, k-1]\}$ with d a proper divisor of m, $k := \frac{m}{d}$ and $c < d$. Since $\gcd(p_s, b_j) = 1$ it also follows that $\gcd(p_s, d) = 1$ and therefore $d \leq \frac{m}{p_s^{\lambda_s}}$. It follows

$$c + d(k-1) = c + m - d \geq m - d > m - \frac{m}{p_s^{\lambda_s}} - 1$$

and thus $L \not\subseteq S$. □

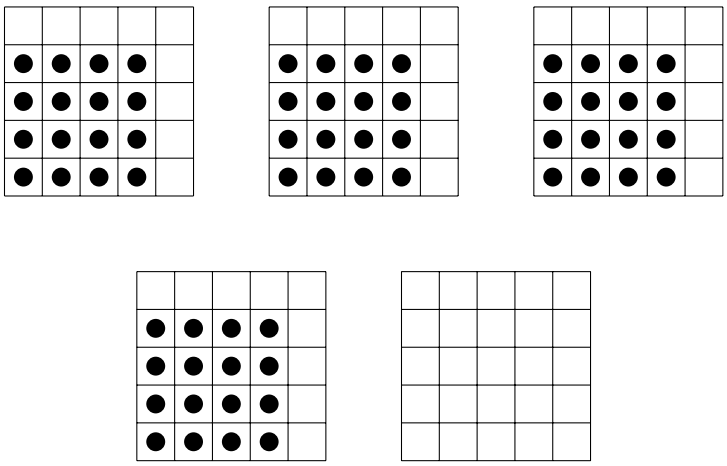


Figure 3.1: the construction of the trivial lower bound in $\mathbb{Z}_5^3$:
For prime numbers and prime powers, the cube is only one step smaller than the whole space.

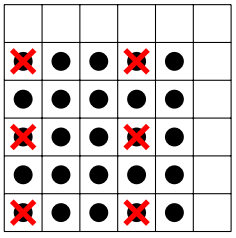


Figure 3.2: $[0,4]^2$ is not 6-progression-free in $\mathbb{Z}_6^2$.
For composite numbers m m-progressions are not necessarily compatible with our understanding of a line.

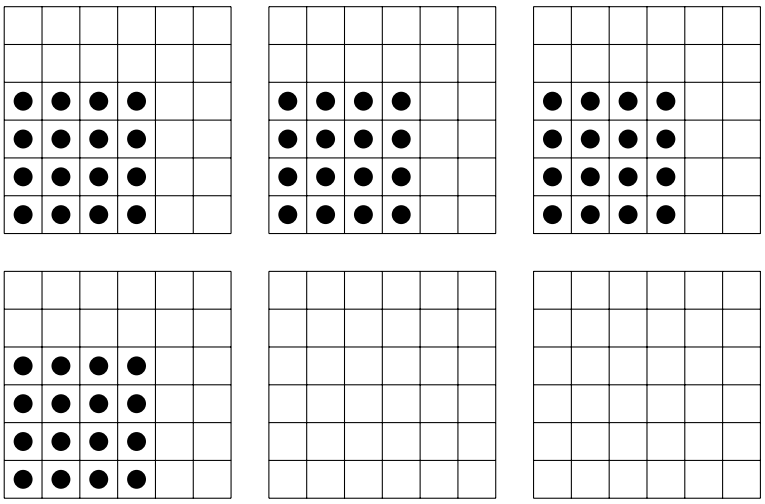


Figure 3.3: the construction of the trivial lower bound in $\mathbb{Z}_6^3$:
For composite numbers the trivial lower bound is often very disappointing (e.g. the bound for 6 is not even larger than for 5) and one can expect much larger progression-free sets.

Remark 2. Note that the constraint $s \geq 2$ is not necessary and Theorem 1 is actually a special case of Theorem 2.

Remark 3. This theorem is best possible, in the sense that $S := [0, m - \frac{m}{p_s^{\lambda_s}}]^n$ is not m-progression-free for $n \geq s$ since

$$\{(\frac{m}{p_1^{\lambda_1}}i, \frac{m}{p_2^{\lambda_2}}i, ..., \frac{m}{p_s^{\lambda_s}}i, 0, ...0) | i \in [0, m-1]\}$$

is an m-progression in S.

4 Other Lower Bounds

The next result will not only be based on combinatorial and number theoretic arguments but will use a strong tool from probability theory: Lovász Local Lemma [6]. It is used to show the existence of certain objects in a random set for many combinatorial problems.

Lemma 9. *Lovász Local Lemma*
Let $l \in \mathbb{N}$ and $A_1, A_2, ..., A_l$ be random events and $p \in (0,1)$, $d \in \mathbb{N}$ such that

- $P(A_i) \leq p \quad \forall i \in [1,l]$,
- *every event A_i is mutually independent of all but d other events,*
- $4pd \leq 1$.

Then

$$P(\bigwedge_{i=1}^{k} \bar{A}_i) > 0.$$

In our case we look at all subsets of $\mathbb{Z}_n^m$ with a elements. Now the argument is very intuitive: If a is small enough we can guarantee that one of our subsets is m-progression-free . The downside of Lovász Local Lemma is that it is not constructive and therefore we can only use the results as a theoretical lower bound but it will not help us to construct progression-free sets.

Theorem 3. *Consider $r_k(\mathbb{Z}_m^n)$ as a function in n, then*

$$r_k(\mathbb{Z}_m^n) = \Omega((m^{\frac{k-2}{k}})^n)$$

as $n \to \infty$.

Proof. Let $l \in \mathbb{N}$ be the number of k-progressions in $\mathbb{Z}_m^n$. Note that $l \leq m^{2n}$. Let $a = \lfloor (\frac{1}{4})^{\frac{1}{k}} (m^{\frac{k-2}{k}})^n \rfloor$, $\mathcal{S}$ the set of subsets of $\mathbb{Z}_m^n$ with a elements and S be chosen uniformly at random from $\mathcal{S}$. Let $B_1, B_2, ..., B_l$ be the distinct k-progressions in $\mathbb{Z}_m^n$ and A_i the event that $B_i \in S$ for all $i \in [1,l]$. Then

$$P(A_i) \leq (\frac{a}{m^n})^k \quad \forall i \in [1,l]$$

and

$$4(\frac{a}{m^n})^k m^{2n} \leq 1.$$

From Lemma 9 it follows that

$$P(\bigwedge_{i=1}^{k} \bar{A}_i) > 0,$$

which means there exists $S \subset \mathbb{Z}_m^n$ with a elements that is k-progression-free. □

Corollary 2.

$$r_m(\mathbb{Z}_m^n) = \Omega((m^{\frac{m-2}{m}})^n).$$

Remark 4. This might seem like a very weak lower bound, but for composite m with many or high prime divisors this is actually much better than the trivial lower bound. The smallest m where this would apply is 60. It holds that $60^{58/69} \approx 52.35$, while the trivial lower bound for $r_{60}(\mathbb{Z}_{60}^n)$ is 48^n.

Another strong lower bound was given by Frankl, Graham and Rödl [8]. It was originally intended for the related problem of line free subspaces of vector spaces and uses a concept called sunflowers. Its main disadvantage is that its only applicable in high dimensions.

Theorem 4. *[8] Let $p \in \mathbb{P}$. Then*

$$r_p(\mathbb{Z}_p^{2p}) \geq p(p-1)^{2p-1}.$$

5 Upper Bounds

In this chapter we now try to also find upper bounds for our problem, which is of course harder than finding lower bounds for which we could simply take the number of elements in any m-progression-free set. A common tool for finding upper bounds is linear optimization, so consider the following reformulation as a linear program:

$$\begin{aligned} &\max \sum_{y \in \mathbb{Z}_m^n} X_y \\ &\text{s. t. } X_{x_1} + X_{x_2} + ... + X_{x_m} \leq m-1, \quad \forall\, m\text{-progressions } \{x_1, x_2, ..., x_m\} \\ &\quad X_y \in \{0,1\}, \quad \forall\, y \in \mathbb{Z}_m^n. \end{aligned} \tag{5.1}$$

It has the following linear relaxation:

$$\begin{aligned} &\max \sum_{y \in \mathbb{Z}_m^n} X_y \\ &\text{s. t. } X_{x_1} + X_{x_2} + ... + X_{x_m} \leq m-1, \quad \forall\, m\text{-progressions } \{x_1, x_2, ..., x_m\} \\ &\quad 0 \leq X_y \leq 1, \quad \forall\, y \in \mathbb{Z}_m^n. \end{aligned} \tag{5.2}$$

Since the restrictions in 5.1 are more strict than in 5.2 we know that the solution of 5.2 is an upper bound for 5.1. Unfortunately, $X_y = \frac{m-1}{m}\ \forall y \in \mathbb{Z}_m^n$ is an optimal solution for 5.2, which leaves us with the following upper bounds:

$$r_m(\mathbb{Z}_m^n) \leq (m-1)m^{m-1}$$

and the trivial bound

$$\alpha_{m,m} \leq m$$

if $\alpha_{m,m}$ exists.

Again, the case where m is a prime gives us some more structure to find a better upper bound, which is due to Aleksanyan and Papikian [1].

Theorem 5. *Let $p \in \mathbb{P}$ and $n \in \mathbb{N}$. Then*

$$r_p(\mathbb{Z}_p^n) \leq p^n - \frac{p^n - 1}{p-1}.$$

Proof. Let $S \subseteq \mathbb{Z}_p^n$ be a p-progression-free set and $x \in S$. Then there are $\frac{p^n-1}{p-1}$ m-progressions containing x (see Lemma 5). From Corollary 1 we know that each pair of these progressions intersect only in x. Therefore, each of these progression contains a different point not contained in S which proves the theorem. □

Remark 5. This again does not give us a non-trivial upper bound for $\alpha_{m,m}$.

One can use the idea from Theorem 5 to generalize the result in a way that uses already known upper bounds in lower dimensions. For this we must first observe that any l-dimensional subspace of $\mathbb{Z}_p^n$ is isomorphic to $\mathbb{Z}_p^l$.

Lemma 10. *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$ and $l \in \mathbb{N}$ with $l \leq n$. Let U be a l-dimensional subspace of $\mathbb{Z}_p^n$. Then*

$$r_p(\mathbb{Z}_p^l) = r_p(U).$$

Proof. Let $d_1, d_2, ..., d_l$ be a basis of U and let $e_1, e_2, ..., e_l$ be the canonical basis of $\mathbb{Z}_p^l$. Then

$$\begin{aligned} \phi\colon \mathbb{Z}_p^l &\to U \\ e_i &\mapsto d_i \quad \forall i \in [1, l] \end{aligned}$$

defines a vector space isomorphism between $\mathbb{Z}_p^l$ and U that maps p-progressions

$$\{(a_1, a_2, ..., a_l) + (b_1, b_2, ..., b_l)i | i \in \mathbb{Z}_m\}$$

in $\mathbb{Z}_p^l$ to p-progressions

$$\{a_1d_1 + a_2d_2 + ... + a_kd_k + (b_1d_1 + b_2d_2 + ... + b_ld_l)i | i \in \mathbb{Z}_m\}$$

in U. Therefore, for every p-progression-free subset $S \subseteq \mathbb{Z}_p^l$, $\phi(S)$ is p-progression-free in U with the same number of elements. The same holds for every p-progression-free set $S' \subseteq U$ and $\phi^{-1}(S')$. □

Now we modify the proof of Theorem 5 by using $(n-1)$- and $(n-2)$-dimensional subspaces instead of p-progressions and points. Note that the intersection between two $(n-1)$-dimensional subspaces is either a $(n-2)$-dimensional subspace or a $(n-1)$-dimensional subspace and the subspaces are equal.

Method 1. *Let $p \in \mathbb{P}$ and $n \in \mathbb{N}$. There is a $k(p, n) \geq 1$ such that*

$$r_p(\mathbb{Z}_p^n) \leq (p+1)r_p(\mathbb{Z}_p^{n-1}) - pk(p, n)$$

Proof. Let $S \subseteq \mathbb{Z}_p^n$ be a p-progression-free set and let L be a $(n-2)$-dimensional affine subspace of $\mathbb{Z}_p^n$ that shares the most points with S. Through shifting the problem we can assume that L is a proper subspace. Let $k(p, n) := |S \cap L|$. It is clear that $k(p, n) \geq 1$.

Now from Lemma 5 we know that there are $\frac{p^2-1}{p-1} = p+1$ $(n-1)$-dimensional subspaces containing L. These subspaces pairwise only intersect in L. Each of these subspaces contains at most $r_p(\mathbb{Z}_p^{n-1})$ different point contained in S, which means they contain at least

$$p^{n-1} - r_p(\mathbb{Z}_p^{n-1})$$

different point not contained in S. Now at least

$$p^{n-1} - r_p(\mathbb{Z}_p^{n-1}) - p^{n-2} + k(p,n) = p^{n-2}(p-1) - r_p(\mathbb{Z}_p^{n-1}) + k(p,n)$$

of those are not contained in L and therefore unique for each subspace. Considering also the $p^{n-2} - k(p,n)$ points in $L \setminus S$ the theorem follows from

$$\begin{aligned} r_p(\mathbb{Z}_p^n) &\leq p^n - (p^{n-2}(p-1) - r_p(\mathbb{Z}_p^{n-1}) + k(p,n))(p+1) - (p^{n-2} - k(p,n)) \\ &= p^n - (p^{n-2}((p-1)(p+1)+1) - r_p(\mathbb{Z}_p^{n-1})(p+1) + pk(p,n)) \\ &= p^n - (p^{n-2}p^2 - (p+1)r_p(\mathbb{Z}_p^{n-1}) + pk(p,n)) \\ &= (p+1)r_p(\mathbb{Z}_p^{n-1}) - pk(p,n) \end{aligned}$$

□

Remark 6. Naively applying this method with $k(p,n) = 1$ for $n > 2$ will achieve little as then already the trivial bound $r_p(\mathbb{Z}_p^n) \leq r_p(\mathbb{Z}_p^{n-1})p$ will be more strict. The goal will be to find a good lower bound for the number of elements in the biggest $n-2$-dimensional subset and then apply the method with this $k(p,n)$.

The first exact result in this thesis was first discovered by Jamison [10] and deals with the case of prime numbers in two dimensions. The above presented proof from Alon [2] needs the Theorem of Chevalley (see [3]), which deals with the existence of roots of polynomials over finite fields.

Theorem 6. *Theorem of Chevalley*
Let $f \in \mathbb{F}_q[X_1, X_2..., X_\lambda]$ be a polynomial of degree $d < \lambda$, satisfying $f(0,0,...,0) = 0$. Then f has a non-trivial root in $\mathbb{F}_q$.

Theorem 7. *[10]*
Let $p \in \mathbb{P}$. Then

$$r_p(\mathbb{Z}_p^2) = (p-1)^2.$$

Proof. Let $B \subseteq \mathbb{Z}_p^2$ be such that $\mathbb{Z}_p^2 \setminus B$ is p-progression-free. Obviously, B is not empty, so we can assume that $(0,0) \in B$. Otherwise we can use $-b + B$ instead of B for any $b \in B$. Now let $B' := B \setminus (0,0)$. By definition B' intersects every p-progression in $\mathbb{Z}_p^2$ that does not intersect $(0,0)$. Now we change our perspective and look at the p-progressions as lines in $\mathbb{Z}_p^2$. Every line can be described as the solutions of the form $(b_1, b_2) \in \mathbb{Z}_p^2$ of a linear equation $xb_1 + yb_2 = c$ with $x, y, c \in \mathbb{Z}_p$. If $c = 0$ the equation

describes a p-progression containing $(0,0)$, otherwise $xb_1 + yb_2 = c$ can be transformed to $x'b_1 + y'b_2 = 1$ by multiplying with the multiplicative inverse of c. Consequently, for every $(x,y) \in \mathbb{Z}_p^2$ there is $(b_1,b_2) \in B'$ such that $xb_1 + yb_2 = 1$. Now consider

$$f := \prod_{b \in B'} (1 - b_1 X - b_2 Y) \in \mathbb{Z}_p[X,Y].$$

It holds that $f(0,0) = 1$ and $f(x,y) = 0$ for all $x, y \in \mathbb{Z}_p$. Thus the following polynomial

$$g := (\sum_{i=1}^{p-1} f(X_1, Y_1)) - (p-1) \in \mathbb{Z}_p[X_1, X_2, ...X_{p-1}, Y_1, Y_2, ..., Y_{p-1}]$$

has only $(0,0,...,0)$ as a root. Now the logical negation of Theorem 6 tells us that g has degree smaller than $2(p-1)$ and therefore,

$$|B| = |B'| + 1 = deg(f) + 1 = deg(g) + 1 \geq 2(p-1) + 1 = 2p - 1.$$

Hence an p-progression-free set in $\mathbb{Z}_p^2$ can contain at most $p^2 - (2p-1) = (p-1)^2$ points which is also the lower bound from Theorem 1. □

Remark 7. The idea of this proof is not restricted to the 2-dimensional case. Since the intersection of any $n-1$ $(n-1)$-dimensional planes of $\mathbb{Z}_p^n$ contains a p-progression, we can find for every $\{a_{i,j}\}_{i \in [1,n], j \in [1,n-1]} \in \mathbb{Z}_p^{n(n-1)}$ a point $(b_1, b_2, ..., b_n)$ in the set B' (defined analogously as in the above proof) such that

$$\sum_{i=0}^{n} b_i a_{i,j} = 1 \qquad \forall j \in [1,n].$$

One could now try to construct a polynomial as in the proof, but the problem is that the resulting lower bound for $|B|$ will still be linear in p, which is not sufficient for dimensions higher than 2.

We finish this chapter with a theorem which uses all the previous results and gives us a reasonable upper bound for the three-dimensional case.

Theorem 8. *Let $p \in \mathbb{P}$. Then*

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

Proof. Let $S \subseteq \mathbb{Z}_p^3$ be such that $|S|$ is maximized. Let L be a p-progression in $S \subseteq \mathbb{Z}_p^3$ that shares the most point with L and let $k := |S \cup L|$. We can distinguish two cases:

- Case 1: $k \leq p-2$
  Since we can decompose $S \subseteq \mathbb{Z}_p^3$ into disjoint p-progressions S contains at most

$$(p-2)|\mathbb{Z}_p^3| = (p-2)p^2 < p^3 - 2p^2 + 1$$

  elements.

- Case 2: $k = p-1$
  Since the p-progressions are exactly the 1-dimensional affine subspaces, we can use Method 1 with $k(p,3) = k = p-1$ and get

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

  Using Theorem 7 we get

$$\begin{aligned} & r_p(\mathbb{Z}_p^3) \leq (p+1)(p-1)^2 - p(p-1) = (p-1)((p^2-1)-p) \\ \Leftrightarrow \quad & r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + 1. \end{aligned}$$

□

6 Lifting To Higher Dimensions

Now we take a deeper dive into the asymptotic behaviour of $r_m(\mathbb{Z}_m^n)$. The question arises if we can use m-progression-free sets in low dimensions to construct m-progression-free sets in one or more dimensions higher. The first idea is to just duplicate the set and add them in as many layers in the next dimension as possible.

Theorem 9. *Let* $m = \prod_{i=1}^{s} p_i^{\lambda_i}$, $n \in \mathbb{N}$, $p_i \in \mathbb{P}$ *and* $\lambda_i \in \mathbb{N}$ $\forall i \in [1, s]$ *such that* $p_1^{\lambda_1} < p_2^{\lambda_2} < ... < p_s^{\lambda_s}$. *Then*

$$r_m(\mathbb{Z}_m^{n+1}) \geq r_m(\mathbb{Z}_m^n)(m - \frac{m}{p_1^{\lambda_1}}).$$

Proof. Let $c := r_m(\mathbb{Z}_m^n)$ and let $S \subseteq \mathbb{Z}_m^n$ be an m-progression-free set with cardinality c. Consider the set $S' := [0, m - \frac{m}{p_1^{\lambda_1}} - 1] \times S \subseteq \mathbb{Z}_m^{n+1}$. Now

$$|S'| = c(m - \frac{m}{p_1^{\lambda_1}})$$

and we will show that S' is m-progression-free. Assume to the contrary that $L := \{a + bj | j \in [0, m-1]\}$ is an m-progression in S with $a, b \in \mathbb{Z}_m^{n+1}$, where $a := (a_1, a_2, ..., a_{n+1})$ and $b := (b_1, b_2, ..., b_{n+1})$. Since

$$\{a_1 + b_1 j | j \in [0, m-1]\} \subseteq [0, m - \frac{m}{p_1^{\lambda_1}} - 1],$$

Lemma 2 tells us that

$$\gcd(b_1, m) > \frac{m}{p_1^{\lambda_1}}.$$

Therefore $p_i \mid \gcd(b_1, m)$ and thus also $p_i \mid b_1$ for all $i \in [1, s]$. Because $|L| = m$, $\gcd(b_1, b_2, ..., b_{n+1}, m) = 1$ and since every prime in m divides b_1, $\gcd(b_2, ..., b_{n+1}, m) = 1$ from which follows that

$$L' := \{(a_2, ..., a_{n+1}) + (b_2, ..., b_{n+1})j | j \in [0, m-1]\}$$

is a progression in S with cardinality m, contradicting the definition of S. Therefore, S' is m-progression-free and

$$r_m(\mathbb{Z}_m^{n+1}) \geq c(m - \frac{m}{p_1^{\lambda_1}})$$

. □

Remark 8. Note that for prime powers $m = p^k$, $r_m(\mathbb{Z}_m^n)$ grows at least by a factor of $m-1$ for every dimension, meaning that every solution that beats the trivial lower bound will give us a construction of a solution that beats the trivial lower bound in every higher dimension. For numbers composed of two or more primes however this theorem is not really practical.

Another idea is to take the tensor product of two solutions. However, this again only works for prime powers $m = p^k$.

Theorem 10. *Let $m = p^k$ with $p \in \mathbb{P}$, $k \in \mathbb{N}$ and $n_1, n_2 \in \mathbb{N}$. Then*

$$r_m(\mathbb{Z}_m^{n_1+n_2}) \geq r_m(\mathbb{Z}_m^{n_1}) r_m(\mathbb{Z}_m^{n_2}).$$

Proof. Let $c_1 := r_m(\mathbb{Z}_m^{n_1})$, $c_2 := r_m(\mathbb{Z}_m^{n_2})$ and let $S_1 \subseteq \mathbb{Z}_m^{n_1}, S_2 \subseteq \mathbb{Z}_m^{n_2}$ be m-progression-free sets with cardinality c_1 and c_2, respectively. Consider the set $S := S_1 \times S_2 \subseteq \mathbb{Z}_m^{n_1+n_2}$. Clearly, $|S| = c_1 c_2$ and we will show that S is m-progression-free. Assume to the contrary that $L := \{a + bi | i \in [0, m-1]\}$ is an m-progression in S with $a, b \in \mathbb{Z}_m^{n_1+n_2}$, where

$$a := (a_1, a_2, ..., a_{n_1}, a_{n_1+1}, ..., a_{n_1+n_2})$$

and

$$b := (b_1, b_2, ..., b_{n_1}, b_{n_1+1}, ..., b_{n_1+n_2}).$$

Since $|L| = m$, there is a $i \in [1, n_1 + n_2]$ with $p \nmid b_i$. W.l.o.g. let $j \leq n_1$, then

$$L' := \{(a_1, a_2, ..., a_{n_1}) + (b_1, b_2, ..., b_{n_1}) i | i \in [0, m-1]\}$$

is an m-progression in S_1, contradicting the definition of S_1. Therefore, S is m-progression-free and $r_m(\mathbb{Z}_m^{n_1+n_2}) \geq c_1 c_2$. □

We have now seen that we can lift an m-progression-free set S from dimension n to any dimension that is a multiple of n, such that $|S|^{1/n}$ keeps unchanged. This assures that $|S|^{1/n}$ is a lower bound for a possibly existing $\alpha_{m,m}$. However, together with Fekete's Lemma about superadditive sequences [7] the above Lemma as well gives as the existence of $\alpha_{m,m}$ where m is a prime power.

Lemma 11. *Fekete's Lemma*
Let $\{a_n\}_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ be a superadditive sequence, i.e.

$$a(n_1 + n_2) \geq a(n_1) + a(n_2) \qquad \forall n_1, n_2 \in \mathbb{N},$$

then the limit

$$\lim_{n\to\infty} \frac{a_n}{n}$$

exists and is equal to

$$\sup_{n\in\mathbb{N}} \frac{a_n}{n}.$$

Without change $((r_m(\mathbb{Z}_m^n))^{1/n})_{n\in\mathbb{N}}$ is not a superadditive sequence, but with a simple transformation that was already used by Davis and Maclagan [4] Fekete's Lemma can be applied.

Theorem 11. *Let $m = p^k$ with $p \in \mathbb{P}$. Then the limit*

$$\alpha_{m,m} := \lim_{n\to\infty} (r_m(\mathbb{Z}_m^n))^{1/n}$$

exists and it holds that

$$m - 1 \leq \alpha_{m,m} \leq m.$$

Moreover, if S is an m-progression-free set in $\mathbb{Z}_m^{n'}$ then

$$\alpha_{m,m} \geq |S|^{1/n'}.$$

Proof. Let $n_1, n_2 \in \mathbb{N}$. From Theorem 10 we know that

$$\begin{aligned} & r_m(\mathbb{Z}_m^{n_1+n_2}) \geq r_m(\mathbb{Z}_m^{n_1}) r_m(\mathbb{Z}_m^{n_2}) \\ \Leftrightarrow \quad & (r_m(\mathbb{Z}_m^{n_1+n_2})^{\frac{1}{n_1+n_2}})^{n_1+n_2} \geq (r_m(\mathbb{Z}_m^{n_1})^{\frac{1}{n_1}})^{n_1} (r_m(\mathbb{Z}_m^{n_2})^{\frac{1}{n_2}})^{n_2} \\ \Leftrightarrow \quad & (n_1+n_2) \log(r_m(\mathbb{Z}_m^{n_1+n_2})^{\frac{1}{n_1+n_2}}) \geq n_1 \log(r_m(\mathbb{Z}_m^{n_1})^{\frac{1}{n_1}}) + n_2 \log(r_m(\mathbb{Z}_m^{n_2})^{\frac{1}{n_2}}), \end{aligned}$$

which means that $\{n \log(r_m(\mathbb{Z}_m^n)^{\frac{1}{n}})\}_{n\in\mathbb{N}}$ is a superadditive sequence. Fekete's Lemma now tells us that

$$\lim_{n\to\infty} \log((r_m(\mathbb{Z}_m^n))^{1/n})$$

and therefore

$$\lim_{n\to\infty} (r_m(\mathbb{Z}_m^n))^{1/n}$$

exists. From Theorem 1 we know that $(m-1)^n \leq r_m(\mathbb{Z}_m^n) \leq m^n$ and therefore the second claim follows.

As we have seen before, Theorem 10 gives us

$$r_m(\mathbb{Z}_m^n) \geq |S|^k$$

for all $k \in \mathbb{N}$ such that $n = kn'$. Now as $\{r_m(\mathbb{Z}_m^{kn'})\}_{k\in\mathbb{N}}$ is a subsequence of $\{r_m(\mathbb{Z}_m^n)\}_{n\in\mathbb{N}}$

$$\lim_{n\to\infty} (r_m(\mathbb{Z}_m^n))^{1/n} = \lim_{k\to\infty} (r_m(\mathbb{Z}_m^{kn'}))^{1/kn'} \geq |S|^{1/n'}$$

which proves the last statement.

□

We end this chapter with a purely theoretical result. The Density Hales-Jewett Theorem was first proven by Furstenberg and Katznelson [9] and was originally used to show the existence of combinatorial lines. However, as every combinatorial line in $[0, m-1]^n$ corresponds to an m-progression in $\mathbb{Z}_m^n$ we can use the following Version.

Theorem 12. *Density Hales-Jewett Theorem*
Consider $r_k(\mathbb{Z}_m^n)$ as a function in n, then

$$r_m(\mathbb{Z}_m^n) = o(m^n)$$

as $n \to \infty$.

Remark 9. Note that this does not give us a non-trivial upper bound for $\alpha_{m,m}$.

7 Constructions

In this chapter we present some constructions of progression-free sets that beat the trivial lower bound. As the first construction is set in 3-dimensional spaces it is useful to define layers of a space and describe which points are included in each layer.

Definition 4. Let $m \in \mathbb{N}$, $S \subseteq \mathbb{Z}_m^3$ and $j \in [0, m-1]$. Let ϕ be the following projection

$$\begin{aligned} \phi \colon \mathbb{Z}_m^3 &\longrightarrow \mathbb{Z}_m^2 \\ (a,b,c) &\mapsto (b,c)\,, \end{aligned}$$

then

$$\phi(S \cap (\{j\} \times \mathbb{Z}_m^2)) \subseteq \mathbb{Z}_m^2$$

is called the j-layer of S.

The first construction deals with the 3-dimensional case where $m = p$ is a prime number. It differs from the trivial solution only in one layer, although in that layer the number of points stay unchanged, and $\frac{p-1}{2}$ new points in the previously empty layer.

Theorem 13. *Let $p \in \mathbb{P} \setminus \{2\}$. Then*

$$r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + \frac{p-1}{2}.$$

Proof. Consider the set

$$S := [0, p-3] \times [0, p-2]^2$$

$$\cup \{p-2\} \times ([0,p-1]^2 \setminus \{(i,i) | i \in [0,p-1]\} \setminus (\{p-1\} \times [0, \frac{p-3}{2}]) \setminus ([0, \frac{p-3}{2}] \times \{p-1\}))$$

$$\cup \{p-1\} \times \{(i,i) | i \in [0, \frac{p-3}{2}]\}.$$

We show that S is p-progression-free. Let $L := \{(a_1,a_2,a_3) + (b_1,b_2,b_3)i | i \in [0,p-1]\}$ be a p-progression in $\mathbb{Z}_p^3$ with $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}_p$.

- Case 1: $b_1 = 0$ and $a_1 \neq p-2$:
  $[0, p-2]^2$ is p-progression-free and $|\{(i,i) | i \in [0, \frac{p-3}{2}]\}| < m$, therefore L is not contained ion S.

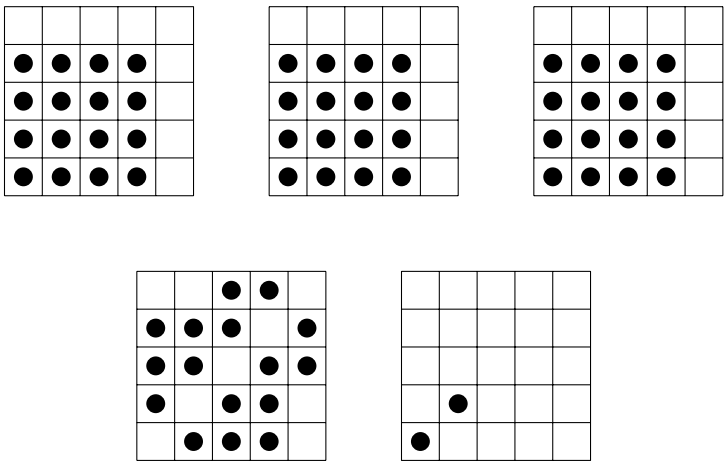


Figure 7.1: the first construction in $\mathbb{Z}_5^3$ consisting of 66 points

- Case 2: $b_1 = 0$ and $a_1 = p - 2$:
  $L' := \{(a_2, a_3) + (b_2, b_3)i | i \in [0, p-1]\}$ and $\{(i, i) | i \in [0, p-1]\}$ are both lines in $\mathbb{Z}_p^2$. If they are not parallel or they are equal, they do intersect, and L is not in S. Else we can rewrite $L = \{(i, c+i) | i \in [0, p-1]\}$ with $c \in [1, p-1]$. If $c \in [1, \frac{p-1}{2}]$ then $c + (p-1) \in [0, \frac{p-3}{2}]$ (choose $i = p-1$) and $(p-2, p-1, c+(p-1)) \in L \setminus S$. Similarly if $c \in [\frac{p+1}{2}, p-1]$ then $p-1-c \in [0, \frac{p-3}{2}]$ (choose $i = p-1-c$) and $(p-2, p-1-c, p-1) \in L \setminus S$. Therefore, L is not contained in S.
- Case 3: $b_1 \neq 0$:
  W.l.o.g. $b_1 = 1$ and $a_1 = p-2$. If $b_2 = b_3 = 0$ then L is not contained in S because the $(p-2)$-layer and $(p-1)$-layer of S have no common point. Else, w.l.o.g $b_2 \neq 0$ and $\{a_2 + b_2 i | i \in [0, p-1]\} = [0, p-1]$. Assume that $L \subseteq S$. Then $a_2 = p-1$ and $a_3 \in [\frac{p-1}{2}, p-2]$ because the $(p-2)$-layer is the only layer containing points with the coordinate $p-1$. Since the $(p-1)$-layer does not have coordinates in $[\frac{p-1}{2}, p-2]$, also $b_3 \neq 0$ and consequently $\{a_3 + b_3 i | i \in [0, p-1]\} = [0, p-1]$. Like before it follows that $a_3 = p-1$ contradicting that $L \subseteq S$. Thus, L is not contained in S and S is p-progression-free, concluding the proof.

□

Remark 10. It seems at first reasonable to assume that this is the best we can get for $p-2$ layers with filled with a $(p-1) \times (p-1)$ square and one layer that is also filled with a maximal number of points, however as early as $p = 7$ there are better examples (see Figure 8.12).

The second construction deals with the case where m is composed of exactly two prime numbers $p > q$. In Theorem 2 we established that a n-dimensional cube with side length $q(p-1)$ is m-progression-free and it is the biggest cube with that property. However, the only types of progressions that prevent us from taking a bigger cube are

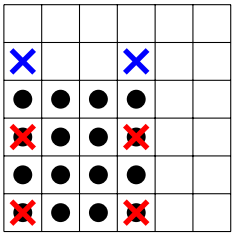


Figure 7.2: Example in $\mathbb{Z}_6^3$
Exactly two point of a progression with step length 2 and 3 are not contained in the 4×4 square. Any shift or rotation to the progression can only lead to at least the same number of points outside.

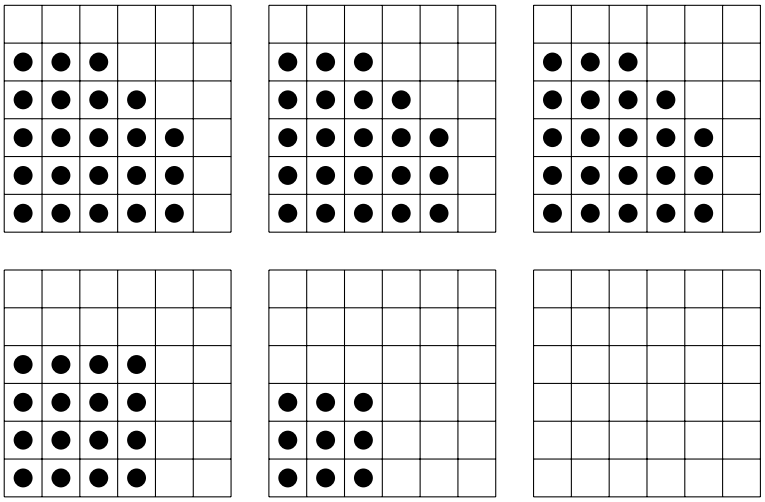


Figure 7.3: the second construction in $\mathbb{Z}_6^3$ consisting of 91 points

those that have a step length of a multiple of p in one dimension and a multiple of q in another dimension. The structure of these progressions assures that at least q points of each progression do not lie in the $q(p-1)$ side length cube (see Figure 7.2).

If we can now add points to our original cube in a way that at most $q-1$ points of each of our critical progressions are added we get a bigger set, which is still m-progression-free. In this construction we add in every dimension a hyperrectangle with side length $p(q-1)$ for all sides except one with length $q-1$, therefore these hyperrectangles do not contain q points on a line with distance p each.

Theorem 14. *Let $m = pq$ with $p, q \in \mathbb{P}$, $p > q$ and $n \in \mathbb{N}$. Then*

$$r_m(\mathbb{Z}_m^n) \geq ((p-1)q)^n + np^{n-1}(q-1)^n.$$

Proof. Consider the set

$$S := [0, (p-1)q - 1]^n$$

$$\cup\bigcup_{i=1}^{n}([0,p(q-1)-1]^{i-1}\times[(p-1)q,pq-2]\times[0,p(q-1)-1]^{n-i}).$$

We show that S is m-progression-free. Let $L := \{(a_1,a_2,...,a_n)+(b_1,b_2,...,b_n)i|i\in[0,m-1]\}$ be an m-progression in $\mathbb{Z}_m^n$ with $a_1,a_2,...,a_n,b_1,b_2,...,b_n\in\mathbb{Z}_m$.

- Case 1: There exists $j\in[1,n]$ with $\gcd(b_j,m)=1$:
  It holds that
  $$\{a_j+b_ji|i\in[0,m-1]\}=[0,m-1],$$
  but there is no point in S with a $m-1$ coordinate, so L is not contained in S.
- Case 2: $\gcd(b_j,m)\in\{0,q,p\}$ for all $j\in[1,n]$:
  Since L is an m-progression, there exist $k,l\in[1,n]$ with $\gcd(b_k,m)=q$ and $\gcd(b_l,m)=p$. Therefore

  $$\{(a_k,a_l)+(b_k,b_l)i|i\in[0,m-1]\}=\{a_k+qi_1|i_1\in[0,p-1]\}\times\{a_l+pi_2|i_2\in[0,q-1]\},$$

  and there exist $i_1\in[0,p-1]$ and $i_2\in[0,q-1]$ with

  $$a_k+qi_1\in[(p-1)q,m-1]\subseteq[p(q-1),m-1]$$

  and
  $$a_l+qi_2\in[p(q-1),m-1].$$

  For all points in S the construction allows only one coordinate to be in $[p(q-1),m-1]$ so L is not contained in S.

As a consequence, S is m-progression-free. □

Corollary 3. *Let $n\in\mathbb{N}$. Then*

$$r_6(\mathbb{Z}_6^n)\geq 4^n+n3^{n-1}.$$

The next construction only works for $m=6$. We take the opposite approach of the last construction and start with a cube of side length 5 and try to delete some points. Again, only progressions with length of a multiple of 2 in one dimension a multiple of 3 in another dimension can cause trouble. As one can see in Figure 3.2 it is sufficient to remove two corners. In higher dimensions this translates into removing all points which have either two 0 coordinates or two 4 coordinates.

Theorem 15. *Let $n\in\mathbb{N}$. Then*

$$r_6(\mathbb{Z}_6^n)\geq 3^n+2n3^{n-1}+n(n-1)3^{n-2}.$$

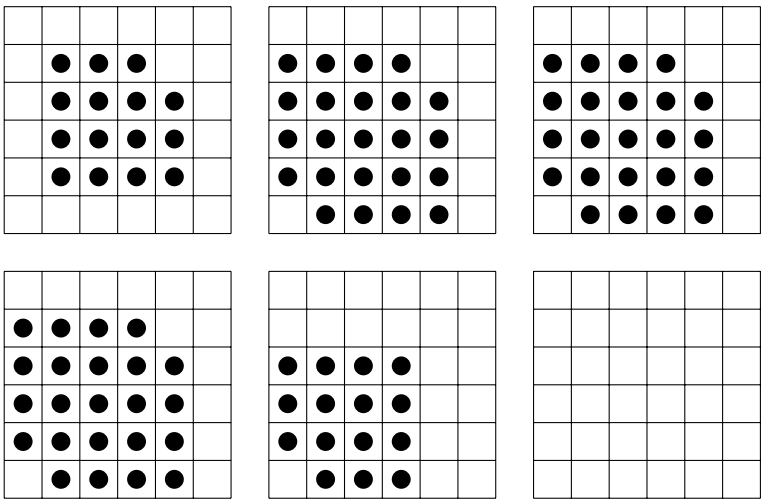


Figure 7.4: the third construction in $\mathbb{Z}_6^3$ consisting of 99 points

Proof. Consider the set

$$S := \{(x_1, x_2, ..., x_n) | (x_i \in [0,4], \forall i \in [1,n]) \wedge (\nexists j \neq k \in [1,n] : x_j = x_k = 0 \vee x_j = x_k = 4)\}.$$

Let $L := \{(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n)i | i \in [0,5]\}$ be a 6-progression in $\mathbb{Z}_6^n$ with $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in \mathbb{Z}_6$.

- Case 1: There exists $j \in [1,n]$ with $\gcd(b_j, 6) = 1$:
  It holds that
  $$\{a_j + b_j i | i \in [0,5]\} = [0,5],$$
  but there is no point in S with a 5 coordinate, so L is not contained in S.
- Case 2: $\gcd(b_j, m) \in \{0,2,3\}$ for all $j \in [1,n]$:
  Since L is a 6-progression, there exist $k, l \in [1,n]$ with $\gcd(b_k, m) = 2$ and $\gcd(b_l, m) = 3$. Therefore

  $$\{(a_k, a_l) + (b_k, b_l)i | i \in [0,5]\} = (a'_k, a'_l) + \{(0,0), (0,3), (2,0), (2,3), (4,0), (4,3)\},$$

  with $a'_k \in [0,1]$ and $a'_l \in [0,2]$.
  If $a'_k = 1$ or $a'_l = 2$, then L has a point with a 5 coordinate, so it is not contained in S.
  Otherwise $a'_k = 0$ and $a'_l \in [0,1]$, therefore L has a point with two 0 or two 4 coordinates, so it is not contained in S.

As a consequence, S is m-progression-free.
It remains to count the elements of S.

$$|S| = |\{(x_1, x_2, ..., x_n) | (x_i \in [0,4], \forall i \in [1,n]) \wedge (\nexists j \neq k \in [1,n] : x_j = x_k = 0 \vee x_j = x_k = 4)\}|$$

$$= |\{(x_1, x_2, ..., x_n)|x_i \in [1,3], \forall i \in [1,n]\}|$$
$$+|\{(x_1, x_2, ..., x_n)|(\exists j \in [1,n] : x_j = 0 \vee x_j = 4) \wedge (x_i \in [1,3], \forall i \in [1,n] \setminus \{j\})\}|$$
$$+|\{(x_1, x_2, ..., x_n)|(\exists j,k \in [1,n] : \{x_j, x_j\} = \{0,4\}) \wedge (x_i \in [1,3], \forall i \in [1,n] \setminus \{j,k\})\}|$$
$$= 3^n + 2\binom{n}{1}3^{n-1} + 2\binom{n}{2}3^{n-2}$$
$$= 3^n + 2n3^{n-1} + n(n-1)3^{n-2}$$

□

Remark 11. This theorem is an improvement to Corollary 3 up to Dimension 7.

8 Computational Approach

Another approach is to use the computer to find maximal progression-free sets in $\mathbb{Z}_m^n$ for small m and n. We use the optimization software package by Laurent Perron and Vincent Furnon called OR-tools [16]. From the package we use their mixed integer solver which is based on a branch-and-cut approach. In this chapter we will show how branch-and-bound work, provide a way to describe our optimization problem as an integer program and present optimal solutions for some instances and other not necessarily optimal solution, which however are better than any lower bounds presented before for other instances.

8.1 Branch and Cut

Consider the following optimization problem, where we want to find an optimal solution $(X_1, X_2, ..., X_n)$:

$$\begin{aligned} &\max \sum_{i=1}^{n} c_i X_i \\ &\text{s. t. } a_{j,1}X_1 + a_{j,2}X_2 + ... + a_{j,n}X_n \leq b_j \quad \forall\, j \in [1, m] \\ &\quad X_i \geq 0, \quad \forall\, i \in [1, n] \end{aligned} \tag{8.1}$$

This kind of problem is called a linear program and if it has one or more optimal solutions, one of these can be found, most commonly by the simplex algorithm [12]. It gets more involved if we want our variables to be integers.

$$\begin{aligned} &\max \sum_{i=1}^{n} c_i X_i \\ &\text{s. t. } a_{j,1}X_1 + a_{j,2}X_2 + ... + a_{j,n}X_n \leq b_j \quad \forall\, j \in [1, m] \\ &\quad X_i \in \mathbb{N}_0, \quad \forall\, i \in [1, n] \end{aligned} \tag{8.2}$$

This modified problem is called an integer program and we call 8.1 the linear relaxation of 8.2. Integer programs are NP-hard in general (see [11]) so we cannot expect solutions for large instances.

A linear program can be divided into three categories: they can have an optimal solution, no solution at all or they are unbounded. In this chapter we will assume

that all linear programs are bounded, which is not a restriction since our optimization problem is bounded and therefore all subproblems remain bounded.

Branch-and-cut is a method to deal with integer programs and is considered one of the most promising ways to do so. We will present the branch-and-cut approach as described by John E. Mitchell in "Integer programming: branch and cut algorithms" [13].

At first, note that the optimal solution of the linear relaxation will always provide us with an upper bound for an integer program. In the case that the solution is an integer solution it is furthermore also the solution of the integer program.

As the name suggests branch-and-bound consists of two vital steps, branching and cutting which are alternatingly used in the algorithm.

8.1.1 Branching

The idea of branching is to divide the set of all feasible solutions into two disjoint subsets. For that we choose $i \in [1, n]$ and $B \in \mathbb{N}_0$ and add the constraints

$$X_i \leq B$$

and accordingly

$$X_i \geq B + 1$$

to two copies of our original problem. We know that the better of the two solutions of the subproblems is the optimal solution of the original solution. Now the idea is to divide every problem, where the solution of the related linear relaxation is not an integer solution, into two subproblems and solve iteratively until an integer solution is found.

It is now important to note, that we do not need to investigate every subproblem. In the algorithm we store the currently best solution and every time the solution of a linear relaxation is worse than our stored solution, we do not need to find a solution for that subproblem nor divide it any further.

There are some choices how to divide the problem, but the most commonly used is to to choose $i \in [1, n]$ such that x_i is not an integer in the current solution $(x_1, x_2, ..., x_n)$ of the linear relaxation and add the inequalities

$$X_i \leq \lfloor x_i \rfloor$$

and accordingly

$$X_i \geq \lceil x_i \rceil.$$

Following these steps would result in a so-called branch-and-bound method. To get to branch-and-cut we sometimes need to choose to cut instead of branching.

8.1.2 Cutting

To get to branch-and-cut we sometimes need to choose to cut instead of branching which basically means reducing the set of feasible solutions of the linear relaxation but not of the integer program. For that purpose, cutting planes are introduced.

When our algorithm finds a non-integer solution for a subproblem we modify the subproblem by adding an additional linear restriction, called cutting plane. This cutting plane must have the property that all feasible integer solutions have to fulfil the restricting, while the optimal non-integer solution does not fulfil it. After cutting we again compute an optimal solution for the linear relaxation and continue like before.

Choosing a cutting plane can be done in various ways but it will not be discussed here. For further information see [14]. One can choose to cut once in every subproblem, but Mitchell suggests doing it after every eight branching steps.

8.1.3 Combining both approaches

In our algorithm we will always store the best-known integer solution and its cost and build up a set of subproblems we need to investigate with an additional number l for each subproblem that keeps track of the times the problem has been modified. When we investigate a subproblem, we solve its linear relaxation, check if it has a solution and if that solution is better than our current best integer solution. If so, we check if the solution is an integer solution.

If it is an integer solution, we update our best known integer solution and its cost and continue with another subproblem.

If the solution is non-integer, we either branch the problem, or if l is divisible by some previously fixed number we cut away the optimal non-integer solution. All resulting new instances will be added to our set of investigated problems.

Once every subproblem was investigated the algorithm stops with the optimal solution.

Note that we do not specify which subproblem should be investigated first. There are several ways to do this, but it will not discussed here.

We assume that every integer linear program is given in the form of 8.2 and every linear program in the form of 8.1 and for a feasible solution $x = (x_1, x_2, ..., x_n)$ we call

$$c(x) := c_1x_1 + c_2x_2 + ... + c_nx_n$$

the cost of x.

Algorithm Branch-and-Cut

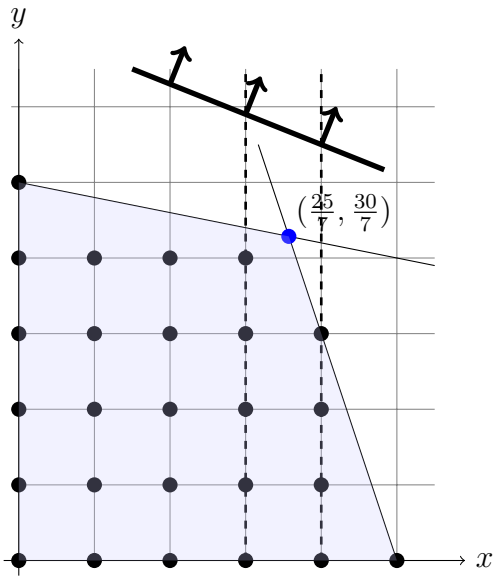
Input: an integer program S and $k \in \mathbb{N}_0$
Output: a optimal solution $y \in \mathbb{R}^n$ with cost $C \in \mathbb{R}$ if a solution exists

set $\mathcal{S} := \{(S, 1)\}$, $C := -\infty$.
while $\mathcal{S} \neq \emptyset$ **do**
    choose $(S', l) \in \mathcal{S}$ and remove it from $\mathcal{S}$
    solve the linear relaxation of S'
    if we get an optimal solution $x \in \mathbb{R}^n$ of the relaxation **then**
        if $c(x) > C$ **then**
            if $x \in \mathbb{N}_0^n$ **then**
                set $L := c(x)$, $y := x$
            else
                if $k|l$ **then**
                    add a cutting plane at x to S' to get S''
                    add $(S'', l + 1)$ to $\mathcal{S}$
                else
                    choose $i \in [1, n]$ such that x_i is not integer
                    branch S' at X_i to get S'_1 and S'_2
                    add $(S'_1, l + 1)$ and $(S'_2, l + 1)$ to $\mathcal{S}$
return y and C

8.1.4 An example

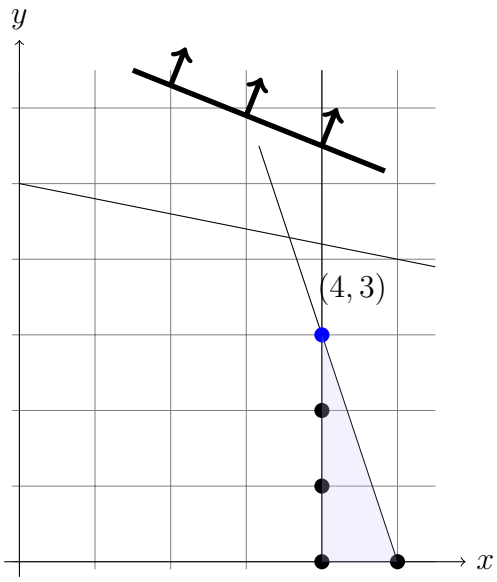
Consider the following integer program in two variables.

$$\begin{aligned} \max\ & 2x + 5y \\ \text{s. t. } & 3x + y \leq 15 \\ & x + 5y \leq 25 \\ & x, y \in \mathbb{N}_0 \end{aligned}$$



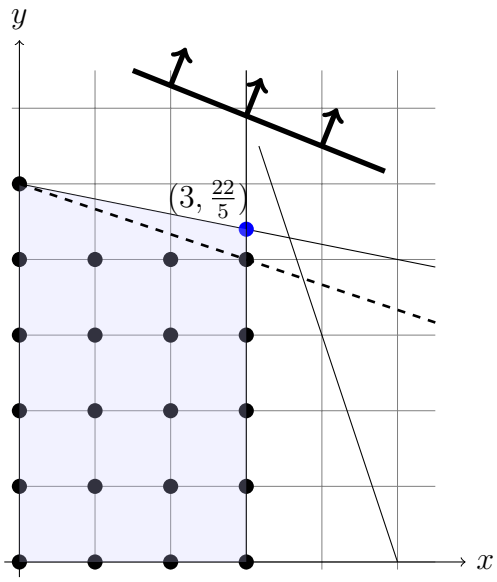
We apply the branch-and-cut algorithm with $k = 2$. The optimal solution of the linear relaxation is $(\frac{25}{7}, \frac{30}{7})$, so in the first round we branch the problem via $x \leq 3$ and $y \geq 4$. Now we first investigate the subproblem

$$\begin{aligned} \max\ & 2x + 5y \\ \text{s. t. } & 3x + y \leq 15 \\ & x + 5y \leq 25 \\ & x \geq 4 \\ & x, y \geq 0 \end{aligned}$$



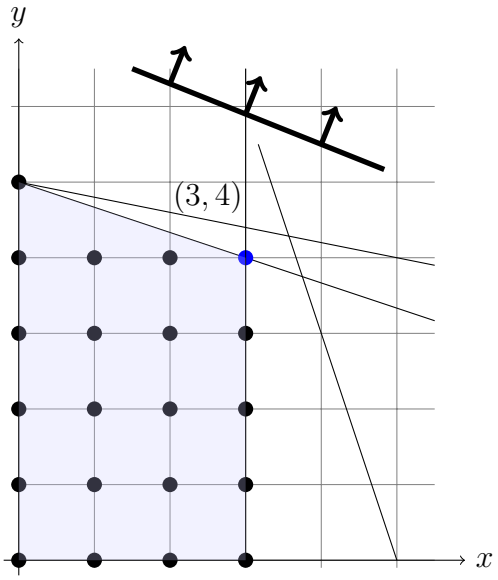
and get its optimal solution $(4, 3)$ with cost 23. Because that solution is an integer solution, we store them in y and C, respectively. The other open subproblem

$$\begin{aligned} \max\ & 2x + 5y \\ \text{s. t. } & 3x + y \leq 15 \\ & x + 5y \leq 25 \\ & x \leq 3 \\ & x, y \geq 0 \end{aligned}$$



has the optimal solution $(3, \frac{22}{5})$ with cost 28 which is greater than C, therefore we have to investigate further. This time we decide to cut by adding the cutting plane $x + 3y \leq 15$.

$$
\begin{aligned}
&\max\ 2x + 5y \\
&\text{s. t. } 3x + y \leq 15 \\
&\qquad x + 5y \leq 25 \\
&\qquad x + 3y \leq 15 \\
&\qquad x \leq 3 \\
&\qquad x, y \geq 0
\end{aligned}
$$



Here we finally get the optimal solution for the whole problem $(3, 4)$ with cost 26.

8.2 Generating all progressions

Now we get back to the integer program formulation of our problem.

$$
\begin{aligned}
&\max \sum_{y \in \mathbb{Z}_m^n} X_y \\
&\text{s. t. } X_{x_1} + X_{x_2} + ... + X_{x_m} \leq m - 1, \quad \forall\ m\text{-progressions } \{x_1, x_2, ..., x_m\} \\
&\qquad X_y \in \{0, 1\}, \quad \forall\ y \in \mathbb{Z}_m^n
\end{aligned}
$$

To solve the problem algorithmically it remains to generate all m-progressions. For $m = p \in \mathbb{P}$ Lemma 3 tells us that all p-progressions are uniquely determined by two of its elements. This allows us to generate all progressions by induction over n:

If $n = 1$ the whole space is a p-progression. Else all p-progressions can be generated in two steps.

- For all $i \in [0, p-1]$ generate all p-progressions in $\{i\} \times \mathbb{Z}_p^{n-1}$, which is equivalent to generate all p-progressions in $\mathbb{Z}_p^n$.
- For each pair (x_1, x_2) with $x_1 \in \{1\} \times \mathbb{Z}_p^{n-1}$ and $x_2 \in \{2\} \times \mathbb{Z}_p^{n-1}$ generate the unique p-progression containing x_1 and x_2.

Lemma 1 assures that this covers all p-progressions.

The case for composite m is more involved and there is no easy way to avoid progressions being generated twice. First we generate all step lengths $b \in [0, \lfloor \frac{m}{2} \rfloor] \times [0, m-1]^{n-1}$ with $\gcd(b_1, b_2, ..., b_n, m) = 1$ as these are the step lengths that assure a

m	3	4	5	6	7	8	9
$r_m(\mathbb{Z}_m^2)$	4	10	16	25	36	52	66
$r_m(\mathbb{Z}_m^3)$	9	36					

Figure 8.1: the optimal values for $r_m(\mathbb{Z}_m^n)$ found via the computational approach

progression to have m elements. It is sufficient to take $b_1 \in [0, \lfloor \frac{m}{2} \rfloor]$ as all other steps are covered by progressions with step length $-b$. Now it remains to find all starting points $a \in \mathbb{Z}_m^n$ to get m-progressions in the form

$$\{a + bi | i \in [0, m-1]\}.$$

We again reduce the case where any $b_i = 0$ to generating all progressions in one dimension lower. Else we compute $d_i = \gcd(b_i, m)$ and choose $i \in [1, n]$ such that d_i is smallest. Lemma 2 assures us that each m-progression with step length b contains a point in $[0, m-1]^{i-1} \times [0, d_i - 1] \times [0, m-1]^{n-i}$, we therefore just use all of these points as our starting points. Note that if $d_i \neq 1$, which can only happen if m is not a prime power, every m-progression with step length b is generated exactly d_i times. If in this case we can find $j \in [1, n]$ such that $d_i d_j = m$, which is in particular possible if m is composed of exactly two prime factors, it is sufficient to take all $a \in [0, m-1]^n$ such that $a_i \in [0, d_i - 1]$ and $a_j \in [0, d_j - 1]\}$ as the starting points and all resulting progressions are generated exactly once. This also follows from Lemma 2 since

$$\{(a_i, a_j) + (b_i, b_j)i | i \in [0, m-1]\}$$

is a set of m elements contained in the set

$$(\{a_i + d_i i | i \in [0, m-1]\} \times [0, m-1]) \cap ([0, m-1] \times \{a_j + d_j i | i \in [0, m-1]\}),$$

which contains also m elements, therefore they are equal.

8.3 Results

In this section we present the computational values. Note that since all variables are either 0 or 1 every branching step is setting one variable to a fixed value. Because the current best solution is always stored in the algorithm is is also possible to stop the algorithm and get a feasible solution that is not necessarily best possible. Those not necessarily optimal solutions presented here are however the best known so far.

m	3	4	5	6	7	8	9	10
$r_m(\mathbb{Z}_m^2)$	(4)	(10)	(16)	(25)	(36)	(52)	(66)	81
$r_m(\mathbb{Z}_m^3)$	(9)	(36)	69	112	220			
$r_m(\mathbb{Z}_m^4)$	20*							

Figure 8.2: some lower bounds for $r_m(\mathbb{Z}_m^n)$ found via the computational approach $r_3(\mathbb{Z}_3^4) = 20$ is already known to be optimal [4]. Values in brackets were already presented in Figure 8.1.

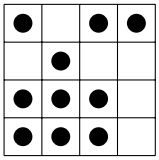


Figure 8.3: optimal solution in $\mathbb{Z}_4^2$: $r_4(\mathbb{Z}_4^2) = 10$

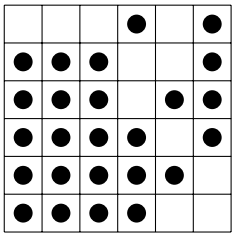


Figure 8.4: optimal solution in $\mathbb{Z}_6^2$: $r_6(\mathbb{Z}_6^2) = 25$

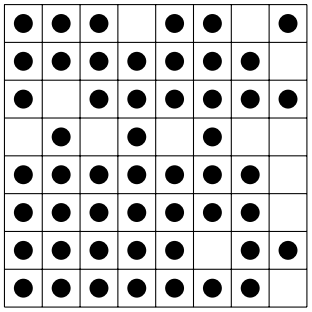


Figure 8.5: optimal solution in $\mathbb{Z}_8^2$: $r_8(\mathbb{Z}_8^2) = 52$

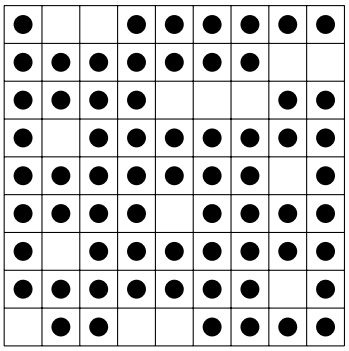


Figure 8.6: optimal solution in $\mathbb{Z}_9^2$: $r_9(\mathbb{Z}_9^2) = 66$

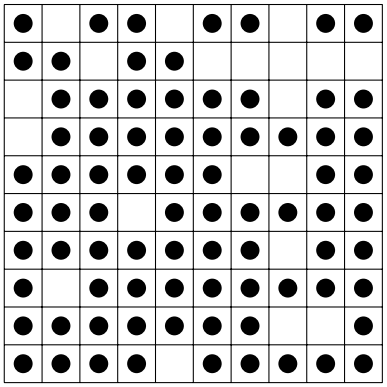


Figure 8.7: feasible solution in $\mathbb{Z}_{10}^2$: $r_{10}(\mathbb{Z}_{10}^2) \geq 81$

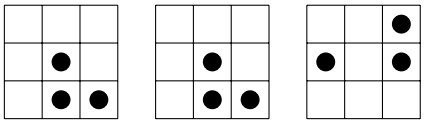


Figure 8.8: optimal solution in $\mathbb{Z}_3^3$: $r_3(\mathbb{Z}_3^3) = 9$

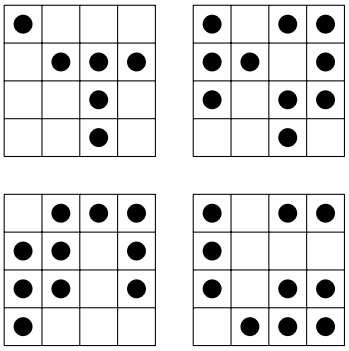


Figure 8.9: optimal solution in $\mathbb{Z}_4^3$: $r_4(\mathbb{Z}_4^3) = 36$

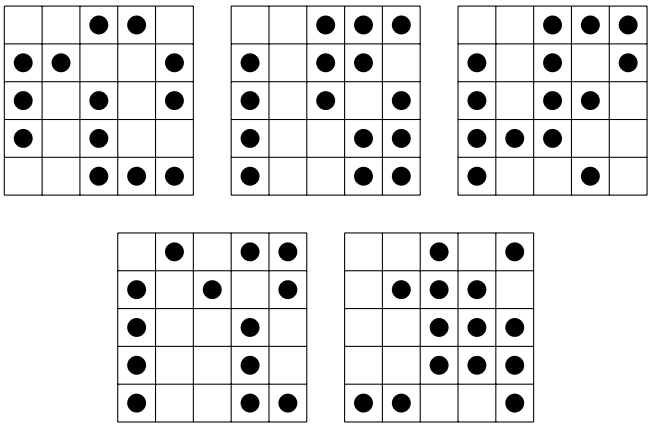


Figure 8.10: feasible solution in $\mathbb{Z}_5^3$: $r_5(\mathbb{Z}_5^3) \geq 69$

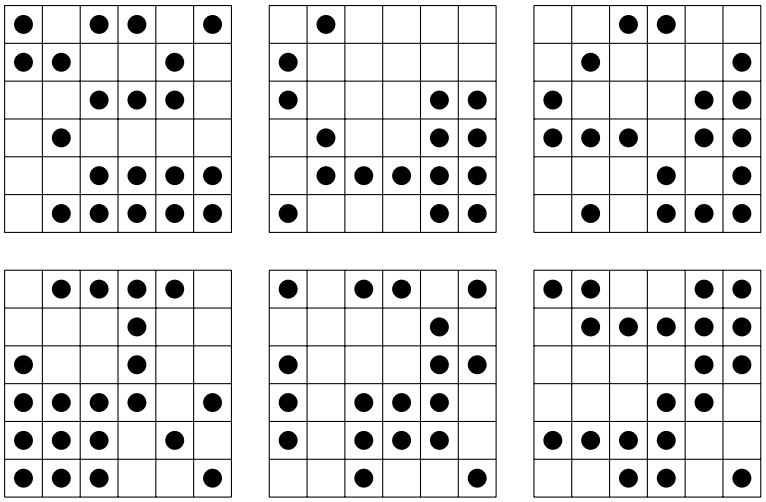


Figure 8.11: feasible solution in $\mathbb{Z}_6^3$: $r_6(\mathbb{Z}_6^3) \geq 112$

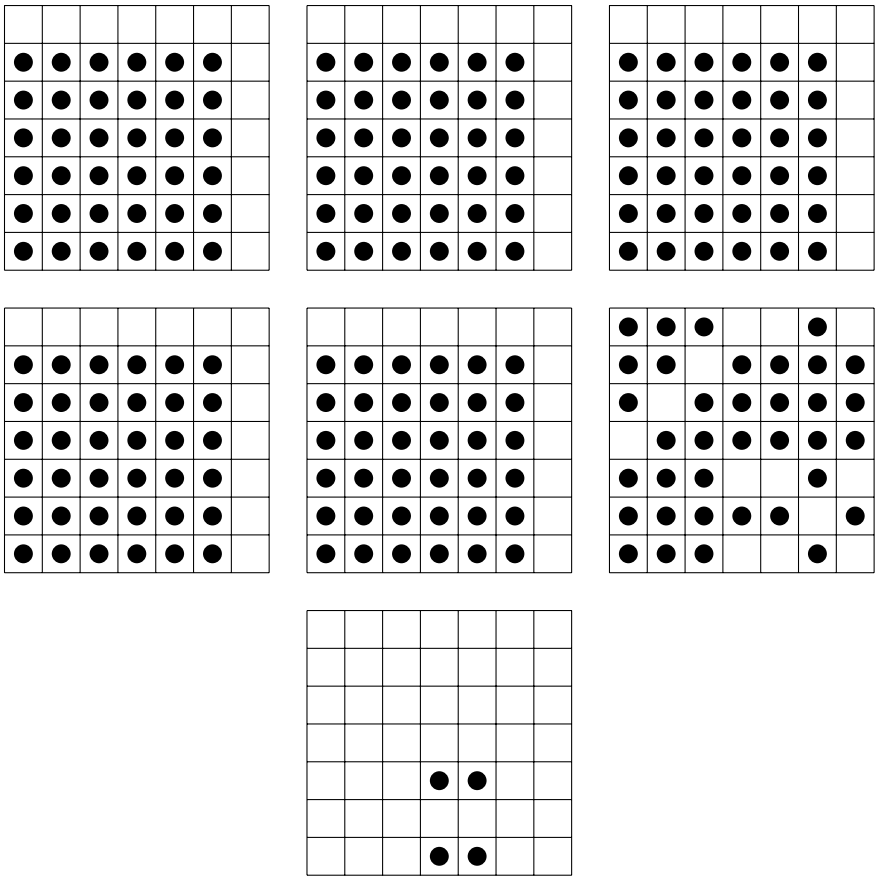


Figure 8.12: feasible solution in $\mathbb{Z}_7^3$: $r_7(\mathbb{Z}_7^3) \geq 220$

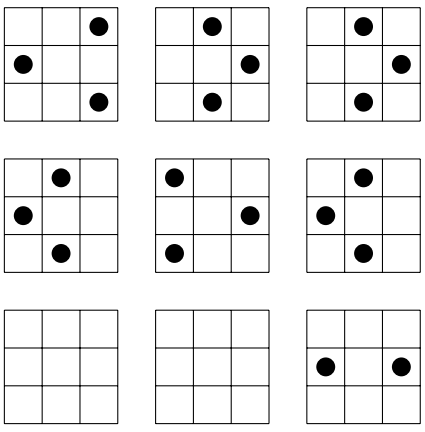


Figure 8.13: optimal solution in $\mathbb{Z}_3^4$: $r_3(\mathbb{Z}_3^4) = 20$

9 Conclusion

Throughout this thesis we brought up the following lower and upper bounds for $r_m(\mathbb{Z}_m^n)$:

- For $m = 3$ and $m = 4$ there is no improvement to the work of Potechin [17] and Elsholtz and Pach [5] who calculated $r_m(\mathbb{Z}_m^n)$ up to $r_3(\mathbb{Z}_3^6) = 112$ and $r_4(\mathbb{Z}_4^4) = 128$, respectively as well as the corresponding lower bounds $\alpha_{3,3} \geq 2.195$ and $\alpha_{4,4} \geq 3.363$.
- We could prove $69 \leq r_5(\mathbb{Z}_5^3) \leq 76$, where the lower bound comes from a computer calculation and the upper bound from Theorem 8 and the corresponding lower bound $\alpha_{5,5} \geq 4.101$.
- We got $r_6(\mathbb{Z}_6^2) = 25$ and $r_6(\mathbb{Z}_6^3) \geq 112$ through computer calculation, however $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$ was shown by Pach and Palincza [15]. We also provided constructions to get $r_6(\mathbb{Z}_6^n) \geq 3^n + 2n3^{n-1} + n(n-1)3^{n-2}$ for $n \in [4, 7]$ as well as $r_6(\mathbb{Z}_6^n) \geq 4^n + n3^{n-1}$ for $n \geq 8$. It is not known if $\alpha_{6,6}$ exists. The same holds for all other m that have more than one prime divisor. There is however the asymptotic upper bound $r_6(\mathbb{Z}_6^n) \leq 5.709^n$ by Pach and Palincza [15].
- We could prove $220 \leq r_7(\mathbb{Z}_7^3) \leq 246$, where, as in the case $m = 5$, the lower bound comes from a computer calculation and the upper bound from Theorem 8. The best asymptotic value comes from the construction by Frankl, Graham and Rödl [8] with $r_7(\mathbb{Z}_7^{14}) \geq 9.142 * 10^{10}$ and $\alpha_{7,7} \geq 6.066$ (see 9.1).
- We found $r_8(\mathbb{Z}_8^2) = 52$, $r_9(\mathbb{Z}_9^2) = 66$ and $r_{10}(\mathbb{Z}_{10}^2) \geq 81$ and the corresponding lower bounds for the asymptotic values $\alpha_{8,8} \geq 7.211$ and $\alpha_{9,9} \geq 8.124$ through computer calculations.
- For $p \in \mathbb{P}$ with $p \geq 11$ we proved $(p-1)^3 + \frac{p-1}{2} \leq r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + 1$ but the the best asymptotic bound again come from from the construction by Frankl, Graham and Rödl with $\alpha_{p,p} \geq (p(p-1)^{2p-1})^{\frac{1}{2p}}$.
- For $m = pq$ where $p, q \in \mathbb{P}$ we came up with a construction to prove $r_m(\mathbb{Z}_m^n) \geq ((p-1)q)^n + np^{n-1}(q-1)^n$.

With Method 1 we established a way to bound $r_p(\mathbb{Z}_p^n)$ from above by $(p+1)r_p(\mathbb{Z}_p^{n-1}) - pk$ where we choose k maximal such that for any p-progression-free subset s there has to be a $(n-1)$-dimensional subspace of $\mathbb{Z}_p^n$ that shares at least k elements with S.

For composite m we found the largest hypercube in $\mathbb{Z}_p^n$ that is m-progression-free and used Lovász Local Lemma to prove $r_m(\mathbb{Z}_m^n) = \Omega((m^{\frac{m-2}{m}})^n)$ which can in some cases beat the hypercube asymptotically.

p	$r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + \frac{p-1}{2}$	$r_p(\mathbb{Z}_p^{2p}) \geq p(p-1)^{2p-1}$	computational values
5	4.041	4.090	4.101
7	6.027	6.066	6.036
11	10.016	10.043	
13	12.013	12.037	
17	16.010	16.028	
19	18.009	18.025	
23	22.007	22.021	
29	28.006	28.016	

Figure 9.1: comparing lower bounds for $\alpha_{p,p}$ for some small prime numbers: Theorem 4 leads to stronger lower bounds for $\alpha_{p,p}$ than Theorem 13. In the case $p = 5$ the computer solution in dimension three could beat this bound.

Bibliography

[1] Ara Aleksanyan and Mihran Papikian. "On Blocking Sets of Affine Spaces". In: *arXiv preprint math/9910084* (1999).

[2] Noga Alon. "Tools from Higher Algebra". In: *Handbook of Combinatorics (Vol. 2)*. Cambridge, MA, USA: MIT Press, 1996, pp. 1749–1783. ISBN: 0262071711.

[3] Zenon Ivanovich Borevich and Igor Rostislavovich Shafarevich. *Number theory*. Academic press, 1986, p. 6.

[4] Benjamin Lent Davis and Diane Maclagan. "The card game SET". In: *The Mathematical Intelligencer* 25.3 (2003), pp. 33–40.

[5] Christian Elsholtz and Péter Pál Pach. "Caps and progression-free sets in $\mathbb{Z}_m^n$". In: *Designs, Codes and Cryptography* 88.10 (2020), pp. 2133–2170.

[6] Paul Erdős and László Lovász. "Problems and results on 3-chromatic hypergraphs and some related questions". In: *Colloquia Mathematica Societatis Janos Bolyai 10. Infinite and Finite Sets, Keszthely (Hungary)*. Citeseer. 1973.

[7] Michael Fekete. "Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten". In: *Mathematische Zeitschrift* 17.1 (1923), pp. 228–249.

[8] P Frankl, R.L Graham, and V Rödl. "On subsets of abelian groups with no 3-term arithmetic progression". In: *Journal of Combinatorial Theory, Series A* 45.1 (1987), pp. 157–161. ISSN: 0097-3165. DOI: https://doi.org/10.1016/0097-3165(87)90053-7. URL: http://www.sciencedirect.com/science/article/pii/0097316587900537.

[9] Hillel Furstenberg and Yitzhak Katznelson. "A density version of the Hales-Jewett theorem". In: *Journal d'Analyse Mathématique* 57.1 (1991), pp. 64–119.

[10] Robert E Jamison. "Covering finite fields with cosets of subspaces". In: *Journal of Combinatorial Theory, Series A* 22.3 (1977), pp. 253–266. ISSN: 0097-3165. DOI: https://doi.org/10.1016/0097-3165(77)90001-2. URL: https://www.sciencedirect.com/science/article/pii/0097316577900012.

[11] Richard M Karp. "Reducibility among combinatorial problems". In: *Complexity of computer computations*. Springer, 1972, pp. 85–103.

[12] Bernhard Korte and Jens Vygen. *Kombinatorische Optimierung: Theorie und Algorithmen*. Springer-Verlag, 2012, pp. 63–66.

[13] John E. Mitchell. “Integer programming: branch and cut algorithmsInteger Programming: Branch and Cut Algorithms”. In: *Encyclopedia of Optimization*. Ed. by Christodoulos A. Floudas and Panos M. Pardalos. Boston, MA: Springer US, 2009, pp. 1643–1650. ISBN: 978-0-387-74759-0. DOI: 10.1007/978-0-387-74759-0_287. URL: https://doi.org/10.1007/978-0-387-74759-0_287.

[14] John E. Mitchell. “Integer programming: cutting plane algorithmsInteger Programming: Cutting Plane Algorithms”. In: *Encyclopedia of Optimization*. Ed. by Christodoulos A. Floudas and Panos M. Pardalos. Boston, MA: Springer US, 2009, pp. 1650–1657. ISBN: 978-0-387-74759-0. DOI: 10.1007/978-0-387-74759-0_288. URL: https://doi.org/10.1007/978-0-387-74759-0_288.

[15] Péter Pál Pach and Richárd Palincza. “Sets avoiding six-term arithmetic progressions in $\mathbb{Z}_6^n$ are exponentially small”. In: *arXiv preprint arXiv:2009.11897* (2020).

[16] Laurent Perron and Vincent Furnon. *OR-Tools*. Version 7.2. Google. URL: https://developers.google.com/optimization/.

[17] Aaron Potechin. “Maximal caps in AG (6, 3)”. In: *Designs, Codes and Cryptography* 46.3 (2008), pp. 243–259.

[18] Amritanshu Prasad. “Counting subspaces of a finite vector space—1”. In: *Resonance* 15.11 (2010), pp. 977–987.