Using the slice rank for finding upper bounds on the size of cap sets

by

Sander J. Borst

to obtain the degree of Bachelor of Science
at the Delft University of Technology,
to be defended publicly on Monday January 15, 2018 at 13:30.

Project duration:	September 1, 2017 – January 15, 2018	
Thesis committee:	Dr. D.C. Gijswijt,	TU Delft, supervisor
	Dr. M.C. Veraar ,	TU Delft
	Drs. E.M. van Elderen,	TU Delft

TU Delft

Abstract

The cap set problem consists of finding the maximum size cap sets, i.e. sets without a 3-term arithmetic progression in $\mathbf{F}_3^n$. In this thesis several known results on the behavior of this number as $n \to \infty$ are presented. In particular we discuss a reformulation by Terence Tao and Will Sawin of a proof found by Dion Gijswijt and Jordan Ellenberg [5, 9]. It uses the slice rank, a rank that is defined for elements of tensor products, to give upper bounds on the size of the cap sets. In this report we will explain the slice rank and how it is related to the size of cap sets. We will also explore whether the slice rank might be used for bounding the size of arithmetic progression-free sets in $\mathbf{F}_q^n$ for $q \neq 3$. We show that we can not use the slice rank to give a non-trivial upper bound on the size of n-term progression-free sets for $n \geq 7$. This was already known for $n \geq 8$.

Preface

The first time I heard of the *cap set problem*, I immediately found it very interesting. I really liked that there was so much complex mathematics involved in answering a rather simple question about a simple game. When I got the chance to choose it as the subject of my bachelor's thesis, I did not have to think long about it. And here is the result: my bachelor's thesis.

I want to thank my thesis committee and in particular my supervisor Dion Gijswijt, who helped me a lot during the project. I also want to thank my family for proofreading my thesis.

Sander Borst
Delft, January 2018

Contents

1 Introduction

The card game SET is an interesting game to play. The deck consists of 81 cards, each having a color, shape, fill and number. For all of those properties there are three possible values. All combinations of values are on exactly one card.

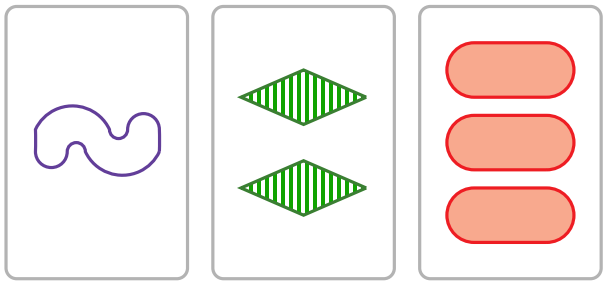
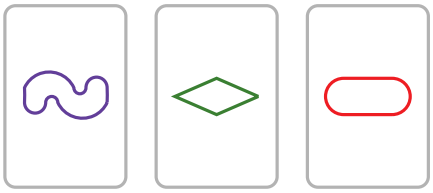
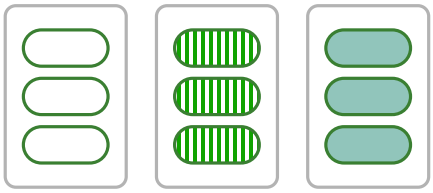


Figure 1.1: Three cards from SET. These three cards all have different color, shape, fill and number. Therefore they form a set.

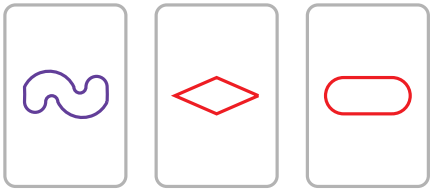
In the game, twelve cards are lying on the table. Players are searching for so-called SET's, combinations of three cards where for each of the four properties either all values are different or all the same.



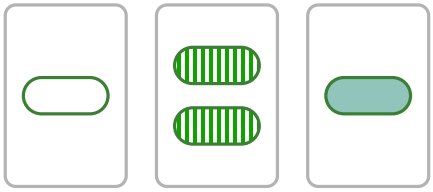
(a) These three cards form a SET



(b) These three cards form a SET



(c) This is not a SET because there are two red cards and one blue card



(d) This is not a SET because there are two cards with just one sybmol and one card with two symbols

Figure 1.2: Example of two SET's and two non-SET's

If no player sees a SET after looking for some time, three more cards are added to the table. However it could happen that there is still no SET among these cards. It is an interesting question to

ask how many times this could happen, i.e. how many cards can be on the table without containing a SET.

1.1. The cap set problem

We can view the problem of finding a maximal combination of cards without a SET mathematically by associating each card in the deck with a unique vector in $\mathbf{F}_3^4$, such that the four properties of a card are encoded by the four components of $v \in \mathbf{F}_3^4$, where each value for a given property corresponds with a value in $\mathbf{F}_3$[3]. It does not really matter which value in $\mathbf{F}_3$ is chosen, but an example is given below.

Count	Value	Color	Value	Shape	Value	Fill	Value
1	0	Red	0	Diamond	0	Solid	0
2	1	Green	1	Oval	1	Striped	1
3	2	Blue	2	Squiggle	2	None	2

Lemma 1. *The three cards corresponding to $a, b, c \in \mathbf{F}_3^4$ form a SET if and only if a, b and c are on the same line, i.e. $a - 2b + c = \mathbf{0}$.*

Proof. Let $a, b, c \in \mathbf{F}_3^4$. Observe that we have that they correspond to three cards that form a SET if and only if in each component the values of a, b and c are all different or all the same, i.e. for $i = 1, \dots, 4$, we have either $a_i = b_i = c_i$ or $a_i \neq b_i \wedge a_i \neq c_i \wedge b_i \neq c_i$. This means that if a, b and c form a set then either $a_i + b_i + c_i = 0 + 1 + 2 = 0$ or $a_i + b_i + c_i = 3 \cdot a_i = 0 \cdot a_i = 0$. So in both cases $a_i + b_i + c_i = 0$. This means $a + b + c = \mathbf{0}$.

We will show that $a+b+c = \mathbf{0}$ exactly when the three corresponding cards form a SET: If $a+b+c = \mathbf{0}$, but a, b and c do not form a SET, then for a certain component i, two of the values of a_i, b_i and c_i have to be the same and one has to be different. Without loss of generality we can assume that $a_i = b_i \neq c_i$. But then $-a_i + c_i \equiv 2a_i + c_i = a_i + b_i + c_i = 0$, so $a_i = b_i = c_i$ contradicting the assumption that a, b and c do not form a set. Now because $a - 2b + c \equiv a + b + c$ in $\mathbf{F}_3^4$, it follows that a, b and c form a set if and only if $a - 2b + c = 0$, i.e. when a, b and c are on the same line in $\mathbf{F}_3^4$. □

We will now introduce the notion of a *cap set* that corresponds to a collection of cards with no SET.

Definition 1. *A* cap set *is a subset $A \subseteq \mathbf{F}_3^n$ containing no three distinct elements $a, b, c \in A$ for which $a - 2b + c = \mathbf{0}$.*

Notice that while cards in the game SET correspond to vectors in $\mathbf{F}_3^4$, the notion of a cap set is defined for all $\mathbf{F}_3^n$ with $n \in \mathbf{N}$. We can view $\mathbf{F}_3^n$ as a SET game with n properties that each have 3 values. As we stated before, we are particularly interested in how many cards there can be with no SET in it, or in other words, what the maximum size of a cap set in $\mathbf{F}_3^n$ is.

Definition 2. *Let a_n be the maximum size of a cap set $A \subseteq \mathbf{F}_3^n$.*

To find the maximum number of cards without a SET we want to know the value of a_4. We point out that it is trivial that $a_0 = 1$ and $a_1 = 2$. Using a few smart tricks it can be proven that $a_2 = 4$, $a_3 = 9$ and $a_4 = 20$ [3]. It has been proven that $a_5 = 45$ [4] and $a_6 = 112$ [7].

In this report we will not look into the value of a_n for specific n, but instead we will look into what happens when $n \to \infty$. First let us give a quite trivial upper and lower bound:

Lemma 2. $2^n \leq a_n \leq 3^n$.

Proof. Let $A \subseteq \mathbf{F}_3^n$ a cap set. Then $|A| \leq |\mathbf{F}_3^n| = 3^n$. This implies our upper bound.

For the lower bound let $A \subseteq \mathbf{F}_3^n$ be the subset of all vector with coordinates in $\{0, 1\}$. All three distinct elements in this set will have at most two different values in each coordinate, so it is a cap set. Therefore $a_n \geq |A| = 2^n$. □

1.2. Generalizing to abelian groups

From the definition we can conclude that a cap set is a subset of $\mathbf{F}_3^n$ without a 3-term arithmetic progression. In general we can look for subsets of G^n without an m-term arithmetic progression, for every abelian group G when $m \leq |G|$.

Definition 3. *For G an abelian group, $V \subseteq G$ and $m \in \mathbf{N}$, let $r_m(V)$ be the maximum size of subset $A \subseteq V$ that has no non-constant m-term arithmetic progression, meaning there are no $a, b \in G$ with $b \neq 0$ such that for all $i \in \{1, \dots, m\}$ it holds that $a + i \cdot b \in A$.*

Now $a_n = r_3(\mathbf{F}_3^n)$.

Lemma 3. *It holds that $r_m(V \times W) \geq r_m(V) \cdot r_m(W)$.*

Proof. Let $A \subset V, B \subset W$ be m-term progression-free sets with $|A| = r_m(V)$ and $|B| = r_m(W)$. Now the set $A \times B$ does not contain m-term arithmetic progressions: Suppose there exists a non-constant m-term progression $(a_1, b_1), \dots, (a_m, b_m)$ in $A \times B$. This implies that $a_1, \dots, a_m$ and $b_1, \dots, b_m$ also must be arithmetic progressions, but because they are m-term arithmetic progression-free, they must be constant progressions. This contradicts our assumption that $(a_1, b_1), \dots, (a_m, b_m)$ is a non-constant progression. □

We can also use the values of $r_m(V^n)$ for individual n's to say something about the asymptotic behavior.

Lemma 4 (Fekete's lemma)**.** *Let $(u_n)_{n\geq 1}$ be a nonnegative subadditive sequence of real numbers (i.e. $u_{n+m} \leq u_n + u_m$). Then the $\frac{u_n}{n}$ converge as $n \to \infty$ and*

$$\lim_{n\to\infty} \frac{u_n}{n} = \inf_{n\geq 1} \frac{u_n}{n}$$

Proof. The proof can be found in [1]. □

Lemma 5. *The value of $\sqrt[n]{r_m(V^n)}$ converges as $n \to \infty$ and $\lim_{n\to\infty} \sqrt[n]{r_m(V^n)} = \sup_{n\geq 1} \sqrt[n]{r_m(V^n)}$.*

Proof. In Lemma 3 we have seen that the sequence $(a_n)_{n\geq 1}$ with $a_n = -\log(r_m(V^n))$ is subadditive. Fekete's lemma now tells us that $\lim_{n\to\infty} \frac{a_n}{n}$ exists and that it is equal to $\inf_{n\geq 1} \frac{a_n}{n}$. This implies that

$$\lim_{n\to\infty} \sqrt[n]{r_m(V^n)} = \sup_{n\geq 1} \sqrt[n]{r_m(V^n)}$$

□

With this lemma we can find asymptotic upper bounds for a_m, using values for individual m's. For example $a_6 = 112$ gives us that $r_3(\mathbf{F}_3^n) = \Omega(112^{n/6}) = \Omega(2.1955^n)$.

1.3. Polynomial method and slice rank

In recent years, mathematicians have successfully used the so-called *polynomial method* in optimization problems. The method works by finding polynomials that vanish on a certain set. This method has been used to find that $r_3((\mathbf{Z}/4\mathbf{Z})^n) < 0.926^n$ [2]. The argument was modified by Jordan Ellenberg and Dion Gijswijt to show that if $p \geq 3$ is a prime then $r_3(\mathbf{F}_p^n) < p^{(1-\epsilon)n}$ for some small $\epsilon > 0$ and in particular $r_3(\mathbf{F}_3^n) = o(2.756^n)$ [5].

This argument was later reformulated in a symmetric way by Terence Tao and Will Sawin [8, 9]. In this report we will describe their proof and explain some of the concepts they use.

In their proof Tao and Sawin use the notion of the slice rank. The slice rank of a function is something that is comparable to the matrix rank. It determines how many 'rank-one' functions are needed to sum up to the function. Those 'rank-one' functions are functions that can be written as the product of a function of one of the variables and a function that does not depend on this variable. In Chapter 2 we will define this rank and show how it is related to the problem of determining the size of progression-free sets. In Chapter 3 we will then introduce ways of finding upper bounds for the slice rank. In Chapter 4 we will also provide a way for finding lower bounds for the slice rank. In Chapter 5 we will apply these results to our initial problem of finding bounds for $r_m(V^n)$ as $n \to \infty$ again.

2

The slice rank

In the polynomial argument, the space of functions that vanish on a particular set is used. In this report we will also use them, but we will think of them as subsets of tensor products of smaller vector spaces. First we will define what we mean by that. Note that we will only define the tensor product of finite-dimensional vector spaces.

Definition 4 (The tensor product)**.** *Let $V_1, \dots, V_n$ be finite-dimensional vector spaces over $\mathbf{F}$. Then*

$$V_1 \otimes \cdots \otimes V_n$$

is the vector space $\mathrm{Mul}(V_1^*, \dots, V_n^*)$, which is the space of multilinear maps from $V_1^* \times \cdots \times V_n^*$ to $\mathbf{F}$. We will call it the tensor product of $V_1, \dots, V_n$.

For all $v_1 \in V_1, \dots, v_n \in V_n$ we will write $v_1 \otimes \cdots \otimes v_n$ to refer to the map in $V_1 \otimes \cdots \otimes V_n$ with $v_1^*, \dots, v_n^* \mapsto v_1^*(v_1) \cdots v_n^*(v_n)$.

From [6, Proposition 8.4] we see that this definition is consistent with other defintions of the tensor product. We will use only a few properties of the tensor product that we will list below.

Lemma 6. *Let $V_1, \dots, V_n$ be vector spaces over $\mathbf{F}$. Let $W = V_1 \otimes \cdots \otimes V_n$. Then the following holds:*

1. *If for each $i \in [n]$ $v_{i,1}, \dots, v_{i,k_i}$ is a basis for V_i, then*

$$\{v_{1,c_1} \otimes \cdots \otimes v_{n,c_n} : c_j \in [k_j]\}$$

   is a basis for W.

2. *If the V_i's are finite dimensional vector spaces then we can identify $V_1^* \otimes \cdots \otimes V_n^*$ with $(V_1 \otimes \cdots \otimes V_n)^*$.*

3. *If each V_i is the space of functions from $X_i \to \mathbf{F}$ with X_i an finite set, then we can view W as the space of functions from $X_1 \times \cdots \times X_n$ to $\mathbf{F}$ with $v_1 \in V_1, \dots, v_n \in V_n$ that*

$$(v_1 \otimes \cdots \otimes v_n)(x_1, \dots, x_n) = v_1(x_1) \cdots v_n(x_n)$$

4. *Taking the tensor product is associative i.e. $(V_1 \otimes V_2) \otimes V_3 = V_1 \otimes (V_2 \otimes V_3)$ which allows us to omit writing parentheses.*

Proof. The proof of (1) and (4) can be found in [6, Proposition 8.4] and (2) follows by the fact that for finite dimensional spaces V is isomorphic to V^{**}. □

Example 1. *If we take $V_1 = \mathbf{R}^n$ and $V_2 = \mathbf{R}^m$. Note that $V_1^* = \mathbf{R}^n$ and $V_2^* = \mathbf{R}^m$. This means $V_1 \otimes V_2$ is the space of bilinear functions $\mathbf{R}^n \times \mathbf{R}^m \to \mathbf{R}$, which we can view as the space of $n \times m$ matrices.*

We will write $v^{\otimes n}$ for $\bigotimes_{i=1}^n v$.

Definition 5. *For a $W_j = \otimes_{1\le i\le n\wedge i\neq j} V_i$, $v_j \in V_j$ and $0 \le j \le n$ define $\otimes_j : V_j \times W_j \to V_1 \times \cdots \times V_n$ with*

$$v_j \otimes_j (v_1 \otimes \cdots \otimes v_{j-1} \otimes v_{j+1} \otimes \cdots \otimes v_n) = v_1 \otimes \cdots \otimes v_n$$

for the simple elements and extend it linearly. In other words $\otimes_j$ inserts its first argument into the j'th position of the tensor product in the second argument.

In Example 1 we showed that we can view spaces of real matrices as tensor products. In linear algebra the matrix rank is defined for matrices. The slice rank is a similar notion, but is also defined for elements of a tensor product in general.

Definition 6 (The slice rank)**.** *For vector spaces $V_1, \ldots, V_n$ we define the rank-one elements to be the non-zero elements of the form $v \otimes_j w$ with $v \in V_i$ and $w \in \otimes_{0\le j\le n\wedge i\neq j} V_j$.*

Now we define the rank of a $w \in V_1 \otimes \cdots \otimes V_n$ as the minimum number m for which it can be written as the sum of m rank-one elements. Note that this implies that all rank-one elements do in fact have a rank of 1.

Example 2. *Let $f : \mathbf{F}_3^3 \to \mathbf{F}_3$ with $f(x,y,z) = xy + xz + yx$. Then the slice rank of $f \in (\mathbf{F}_3^{\mathbf{F}_3})^{\otimes 3}$ is equal to 2. The slice rank is smaller or equal to 2 because $f(x,y,z) = x(y+z) + yx$, so the sum of two rank-one functions. The slice rank of f is not equal to zero because f is not the zero function. Now suppose the slice rank of f is 1. Then it can be written as the product of a function that depends on one of the variables and a function that does not depend on this variable. Because of the symmetry it does not matter which variable we choose, so we can write $f(x,y,z) = g(x)h(y,z)$. Because $g(0)h(1,0) = 0$, but $g(1)h(1,0) = 1$ we see that $g(0) = 0$, which contradicts $g(0)h(1,1) = 1$.*

Example 3 (The slice rank is an extension of the matrix rank)**.** *Let A be an $n \times m$ matrix A over $\mathbf{F}$. We can see this matrix as an $A \in \mathrm{Mul}(\mathbf{F}^n, \mathbf{F}^m) = (\mathbf{F}^n)^* \otimes (\mathbf{F}^m)^* = \mathbf{F}^n \otimes \mathbf{F}^m$. Then the rank r of B is the smallest value r for which there exist $v_i \in \mathbf{F}^n, w_i \in \mathbf{F}^m$ with:*

$$A = \sum_{i=1}^{r} v_i \otimes w_i$$

Because $v_i \otimes w_i = v_i w_i^\intercal$ we see that r is the smallest number for which:

$$A = \sum_{i=1}^{r} v_i w_i^\intercal$$

This is exactly the definition of the matrix rank, so the matrix rank of a matrix A is always equal to the slice rank of its corresponding bilinear map.

Because for a tensor product of two vector spaces the slice rank is equal to the rank of the corresponding matrix, we will write $\mathrm{rk}\, w$ for the slice rank of w.

Lemma 7. *For $i = 1, \ldots, k$ let V_i be a vector space. Let $v \in V_1 \otimes \cdots \otimes V_k$. Then the following holds:*

1. *There exist subspaces $U_i \subseteq V_i$ with*

$$v \in \bigoplus_{i=1}^{k} V_1 \otimes \cdots \otimes V_{i-1} \otimes U_i \otimes V_{i+1} \otimes \cdots \otimes V_k$$

   and $\sum_{i=1}^{k} \dim U_i \le \mathrm{rk}\, v$.

2. *There exist subspaces $W_i \subseteq V_i^*$ with $w(v) = 0$ for all $w \in \otimes_{i=1}^{k} W_i$ and $\mathrm{rk}\, v + \sum_{i=1}^{k} \dim W_i \ge \sum_{i=1}^{k} \dim V_i$.*

Proof. We can see that (1) holds for rank-one functions by their definition. A function f of rank r can be written as the sum of r function of rank one. So we can find each U_i that satisfy our requirements by taking the span of the corresponding elements for all these rank one functions.

Now take the U_i's as in (1). Let $W_i = \mathrm{Ann}_{V_i^*}(U_i) = \{v \in V_i^* : v(u) = 0 \forall u \in U_i\}$. Then $\sum_{i=1}^k (\dim V_i - \dim W_i) = \sum_{i=1}^k \dim(U_i) \leq \mathrm{rk}\, v$ and for all $w_1 \in W_1, \dots, w_k \in W_k$ we have

$$(w_1 \otimes \cdots \otimes w_k)(v) \in \bigoplus_{i=1}^{k} w_1(V_1) \otimes \cdots \otimes w_{i-1}(V_{i-1}) \otimes w_i(U_i) \otimes w_{i+1}(V_{i+1}) \otimes \cdots \otimes w_k(V_k) = \{0\}.$$

This implies that $w(v) = 0$ for all $w \in \bigotimes_{i=1}^k W_i$. So this proves (2). □

Lemma 8. *Let $f : S^k \to \mathbf{F}$ where $f(x_1, \dots, x_k)$ is non-zero if and only if $x_1 = \cdots = x_k$ for all i. Then $\mathrm{rk}\, f = |S|$.*

Proof. We will show $\mathrm{rk}\, f = |S|$. First we will show that $\mathrm{rk}\, f \leq |S|$ by observing that

$$f(x_1, \dots, x_k) = \sum_{a \in S} c_a \delta_a(x_1) \cdots \delta_a(x_k)$$

and that because for every a the function $\mathbf{x} \mapsto c_a \delta_a(x_1) \cdots \delta_a(x_k)$ is a rank-one function this means that f is the sum of $|S|$ rank-one functions. In Chapter 4 we will finish the proof by showing that $\mathrm{rk}\, f \geq |S|$. □

2.1. Slice rank as upper bound for the size of progression-free sets

Theorem 1. *Let $f : V^m \to \mathbf{F}$ such that $f(v_1, \dots, v_m) \neq 0$ only if $v_1, \dots, v_m$ is an arithmetic progression and $f(v, \dots, v) \neq 0$ for all $v \in V$. Let $A \subseteq V$ be a set without an m-term arithmetic progression. Then $|A| \leq \mathrm{rk}\, f$.*

Proof. Let $g = f|_{A^m}$. We can still write g as the sum of the same rank-one functions as f if we restrict them to A^m, so $\mathrm{rk}\, g \leq \mathrm{rk}\, f$. Now observe that $g(x_1, \dots, x_m) = \sum_{a \in A} g(a, \dots, a) \delta_a(x_1) \cdots \delta_a(x_m)$. Using our result from Lemma 8 we know this means that $\mathrm{rk}\, g = |A|$. Now we have our inequality $|A| \leq \mathrm{rk}\, f$. □

We can use the above theorem to give an upper bound on the size of progression-free sets by finding an f that satisfies the conditions of the theorem and has a low slice rank.

3

Upper bounds for the slice rank

We have shown in Theorem 1 that the size of progression-free sets is bounded from above by the slice rank of certain functions. Because we want to find an upper bound for the size of the cap sets, we need a way to bound the slice rank for a function f. In this chapter we will explain techniques that allow us to give upper bounds for the slice rank.

The following theorem was developed by Terence Tao [9]. We will give a more extensive proof. In the theorem we will use the word covering. We say that the sets $\Gamma_1, \dots, \Gamma_k$ are a *covering* of Γ when $\bigcup_{i=1}^{k} \Gamma_i = \Gamma$.

Theorem 2. *Let $V_1, \dots, V_k$ be finite-dimensional vector spaces over a field $\mathbf{F}$ and let $(v_{j,s})_{s \in S_j}$ be an independent set in V_j for all $1 \leq j \leq k$, where S_j is some finite set. Now let $\Gamma \subseteq S_1 \times \cdots \times S_k$. Then for every*

$$v = \sum_{(s_1,\dots,s_k) \in \Gamma} c_{(s_1,\dots,s_k)} v_{1,s_1} \otimes \cdots \otimes v_{k,s_k} \tag{3.1}$$

it holds that

$$\operatorname{rk} v \leq \min_{\Gamma = \Gamma_1 \cup \dots \cup \Gamma_k} |\pi_1(\Gamma_1)| + \cdots + |\pi_k(\Gamma_k)| \tag{3.2}$$

where π_j is the projection map that maps an input to its j'th coordinate.

Proof. We will show $\operatorname{rk} v \leq |\pi_1(\Gamma_1)| + \cdots + |\pi_k(\Gamma_k)|$ holds for every partition $\Gamma_1, \dots, \Gamma_k$ of Γ. It is then trivial that the inequality also holds for all coverings $\Gamma_1, \dots, \Gamma_k$ of Γ, which implies that Eq. (3.2) holds.

We may assume that each V_j is spanned by the v_{j,s_j}, because otherwise we can simply extend them to a basis.

Let $\Gamma_1, \dots, \Gamma_n$ be a partition of Γ. Then for all j it is true that

$$\sum_{(s_1,\dots,s_k) \in \Gamma_j} c_{s_1,\dots,s_k} v_{s_1} \otimes \cdots \otimes v_{s_k} = \sum_{s \in \pi_j(\Gamma_j)} v_s \otimes w_s$$

for some $w_s \in \bigotimes_{i \neq j} V_i$. By summing these we get that:

$$\operatorname{rk} v \leq |\pi_1(\Gamma_1)| + \cdots + |\pi_1(\Gamma_k)| \tag{3.3}$$

□

3.1. Bounding the rank of function products

We are not just interested in finding $r_m(G^n)$ (the maximum size of a subset of G^n without m-term arithmetic progression) for some n, but we also want to know what happens when $n \to \infty$. Therefore we will now use Theorem 2 to find an asymptotic upper bound for $f^{\otimes n}$ as $n \to \infty$, using a method shown in [9].

Definition 7 (Shannon entropy)**.** *Let X be a discrete random variable that takes values in V. Then $h(X) := -\sum_{v\in V} \mathbf{P}(X = v)\ln(\mathbf{P}(X = v))$. This is called the Shannon entropy of X.*

When (X, Y) is a discrete random variable that takes values in $V \times W$, we define

$$h(X|Y) := \frac{1}{|W|}\sum_{w\in W} h(X|Y = w)\mathbf{P}(Y = w)$$

where $h(X|Y = w) = -\sum_{v\in V} \mathbf{P}(X = v|Y = w)\ln(\mathbf{P}(X = v|Y = w))$.

Definition 8 (Strongly typical sequences)**.** *Let X be a random variable taking values in Γ. Then $\mathbf{x} \in \Gamma^n$ is called an ε* strongly typical sequence *with respect to X if and only if:*

$$\sum_{a\in\Gamma}\left|\frac{|\{1 \le i \le n : x_i = a\}|}{n} - \mathbf{P}(X = a)\right| \le \epsilon$$

The set of all ϵ strongly typical sequences with respect to X of length n in Γ is called $T^n_{[X]\epsilon}$.

We will say that $(\mathbf{x}, \mathbf{y}) \in T^n_{[X,Y]\epsilon}$ if the sequence $(x_i, y_i)_{1\le i\le n}$ is ϵ strongly typical with respect to the random variable (X, Y).

Lemma 9. *If $(\mathbf{x}, \mathbf{y}) \in T^n_{[X,Y]\epsilon}$, then $\mathbf{x} \in T^n_{[X]\epsilon}$ and $\mathbf{y} \in T^n_{[Y]\epsilon}$.*

Proof. The proof of this lemma can be found in [10, Theorem 6.7] □

Lemma 10 (Strong asymptotic equipartition property)**.** *Let X be a random variable. Let $\delta : \mathbf{R}_{>0} \to \mathbf{R}_{>0}$ with $\lim_{n\to\infty}\delta(n) = 0$. Then we have:*

$$|T^n_{[X]\delta(n)}| \le \exp(n(h(X) + o(1))) \qquad \text{as } n \to \infty \tag{3.4}$$

There is a function δ' with $\lim_{n\to\infty}\delta'(n) = 0$ such that $\delta \ge \delta'$ implies that:

$$|T^n_{[X]\delta(n)}| = \exp(n(h(X) + o(1))) \qquad \text{as } n \to \infty \tag{3.5}$$

Proof. A proof of this property can be found in [10, Theorem 6.2]. Note that in this proof we can see that the upper bound (Eq. (3.4)) holds for all δ, while the lower bound only holds if $\delta \to 0$ sufficiently slowly. □

Definition 9 (Conditional strongly typical sequences)**.** *We define*

$$T^n_{[X|Y]\epsilon}(\mathbf{y}) = \{\mathbf{x} \in T^n_{[X]\epsilon} : (\mathbf{x}, \mathbf{y}) \in T^n_{[X,Y]\epsilon}\}.$$

Lemma 11 (Conditional strong equipartition partition property)**.** *Let $\delta : \mathbf{R}_{>0} \to \mathbf{R}_{>0}$ with $\lim_{n\to\infty}\delta(n) = 0$. For all $\mathbf{y} \in T^n_{[Y]\delta(n)}$ with $|T^n_{[X|Y]\delta(n)}| \ge 1$ we have*

$$|T^n_{[X|Y]\delta(n)}(\mathbf{y})| = \exp(n(h(X|Y) + o(1))) \qquad \text{as } n \to \infty. \tag{3.6}$$

Proof. A proof of this theorem can be found in [10, Theorem 6.10]. □

Lemma 12. *Let B be the set of all probability distributions on a finite set Γ, represented by a random variable with this distribution. Now the the function $\delta : B \times B \to [0, 1]$ with $\delta(A, B) = \sum_{\gamma\in\Gamma}|\mathbf{P}(A = \gamma) - \mathbf{P}(B = \gamma)|$ defines a metric on B. Also if $(R_i)_{1\le i\le n}$ is a sequence in Γ and X is a random Γ-valued variable with probabilities equal to the relative frequence in $(R_i)_{1\le i\le n}$ (i.e. $\mathbf{P}(A = \gamma) = \frac{|\{1\le i\le n:R_n=a\}|}{n}$), then $(R_i)_{1\le i\le n} \in T^n_{[Y]\epsilon}$ if and only if $\delta(X, Y) \le \epsilon$.*

Proof. We can view each probability distribution as an element of $\mathbf{R}^{|\Gamma|}$ with the values in the vector corresponding to the probabilities. Then δ is equal to the metric induced by the ℓ_1-norm on $\mathbf{R}^{|\Gamma|}$. Now the following inequality gives us that $(R_i)_{1\le i\le n} \in T^n_{[Y]\epsilon}$ if and only if $\delta(X, Y) \le \epsilon$:

$$\delta(X, Y) = \sum_{\gamma\in\Gamma}|\mathbf{P}(A = \gamma) - \mathbf{P}(B = \gamma)| \le \sum_{\gamma\in\Gamma}\left|\frac{|\{1 \le i \le n : R_n = a\}|}{n} - \mathbf{P}(B = \gamma)\right|$$

□

Theorem 3. *Let $V_1, \dots, V_k$ be finite-dimensional vector spaces over a field $\mathbf{F}$ and let $(v_{j,s})_{s \in S_j}$ be an independent set in V_j for all $1 \le j \le k$, where S_j is some finite set. Now let $\Gamma \subseteq S_1 \times \cdots \times S_k$. Then for every*

$$v = \sum_{(s_1,\dots,s_k)\in\Gamma} c_{(s_1,\dots,s_k)} v_{1,s_1} \otimes \cdots \otimes v_{k,s_k} \tag{3.7}$$

it holds that

$$\operatorname{rk} v^{\otimes n} \le \exp((H + o(1))n) \tag{3.8}$$

with

$$H = \sup_{X=(X_1,\dots,X_k)} \min_{j=1,\dots,k} h(X_j) \tag{3.9}$$

as $n \to \infty$ where the supremum ranges over all random variables with values in Γ.

Proof. We will prove that

$$\min_{\Gamma^n = \Gamma_1 \cup \dots \cup \Gamma_k} |\pi_1(\Gamma_1)| + \dots + |\pi_k(\Gamma_k)| \le \exp((H + o(1))n).$$

Then Eq. (3.8) follows from Theorem 2.

Let $\epsilon(n) := \frac{1}{n}$. Let $N \ge \frac{|\Gamma|}{\epsilon(n)}$. Let $W = \left\{\frac{i}{N} : i = 0, \dots, N\right\}$. Now let P be the set of all random variables on Γ with all probability values in W. Note that $|P| \le |W|^{|\Gamma|} = (N+1)^{|\Gamma|} \le \exp(o(n))$. Now for each Γ-valued random variable X there is an $Y \in P$ with $\delta(X, Y) \le \frac{1}{n}$. So for each $\gamma \in \Gamma^n$ there is an $Y \in P$ with $\gamma \in T^n_{[Y]\epsilon(n)}$

Let $\Gamma_i := \bigcup_{Y \in P \wedge h(Y_i) \le H} T^n_{[Y]\epsilon(n)}$. For each $Y \in P$ we have $|T^n_{[Y]\epsilon(n)}| \le \exp(n(h(Y) + o(1)))$. Note that for each $Y = (Y_1, \dots, Y_k) \in P$ we can find a $1 \le i \le k$ with $h(Y_i) \le H$, so $\Gamma_1 \cup \dots \cup \Gamma_k = \Gamma^n$. Note that by Lemma 10 we now have for all i that

$$|\Gamma_i| \le |P| \cdot \exp(n(H + o(1))) \le \exp(o(n)) \cdot \exp(n(H + o(1))) \le \exp(n(H + o(1)))$$

□

4

Lower bounds for the slice rank

In the previous chapters we have seen that the slice rank of certain functions is an upper bound for the size of progression-free sets. We have also shown how to give upper bounds for the slice rank. It is also interesting to see if we can find lower bounds for the slice rank. We will use them to show that for certain instances of the problem our method will only provide trivial upper bounds.

Theorem 4. *Let $V_1, \dots, V_k$ be finite-dimensional vector spaces over a field $\mathbf{F}$ and let $(v_{j,s})_{s \in S_j}$ be an independent set in V_j for all $1 \leq j \leq k$, where S_j is some finite set. Now let $\Gamma \subseteq S_1 \times \cdots \times S_k$. Then for every*

$$v = \sum_{(s_1,\dots,s_k) \in \Gamma} c_{(s_1,\dots,s_k)} v_{1,s_1} \otimes \cdots \otimes v_{k,s_k} \tag{4.1}$$

where all $c_{(s_1,\dots,s_k)} \neq 0$. If each of the S_j has a total ordering and Γ' is the set of maximal elements in Γ then

$$\operatorname{rk} v \geq \min_{\Gamma' = \Gamma_1 \cup \dots \cup \Gamma_k} |\pi_1(\Gamma_1)| + \dots + |\pi_k(\Gamma_k)| \tag{4.2}$$

where π_j is the projection map that maps an input to its j'th coordinate. In particular if $\Gamma' = \Gamma$, equality holds in Eq. (4.2)

Proof. Choose the W_i as in Lemma 7. Now for $1 \leq j \leq k$ we can find a basis $w_{j,1}, \dots, w_{j,d_j}$ of W_j using Gaussian elimination that is in row-echelon form with respect to the standard dual basis $e_1^*, \dots, e_{|X_j|}^*$ of $\mathbf{F}^{|X_j|}$. In other words, there are $s_{j,i}$ with $1 \leq s_{j,1} < \dots < s_{j,d_j} \leq |X_j|$ such that $w_{j,t}$ is a linear combination of $e_{s_{j,t}}^*, \dots, e_{|X_j|}^*$ with the coëfficient for $e_{s_{j,t}}^*$ being one.

We will show that $P := \prod_{j=1}^k \{s_{j,t} : 1 \leq t \leq d_j\}$ is disjoint from Γ'. Otherwise there would be t_j with $1 \leq t_j \leq d_j$ for all j such that

$$(s_{1,t_1}, \dots, s_{k,t_k}) \in \Gamma'.$$

Because Γ' only contains maximal elements of Γ this means that $(s_1, \dots, s_k) \notin \Gamma$ for any tuple $(s_1, \dots, s_k) \in \prod_{j=1}^k \{s_{j,t_j}, \dots, |S_j|\}$ except $(s_{1,t_1}, \dots, s_{k,t_k})$. Because w_{j,t_j} is a linear combination of $e_{s_{j,t}}^*, \dots, e_{|X_j|}^*$ with the coëfficient for $e_{s_{j,t}}^*$ being one, we know that $w_{1,t_1} \otimes \cdots \otimes w_{k,t_k}$ is equal to $e_{1,t_1}^* \otimes \cdots \otimes e_{k,t_k}^*$ plus a linear combination of $e_{1,p_1}^* \otimes \cdots \otimes e_{k,p_k}^*$ for tuples $(p_1, \dots, p_k) \notin \Gamma$. Now it follows that

$$\left\langle \otimes_{i=1}^k w_{i,t_i}, v \right\rangle = \left\langle \otimes_{i=1}^k e_{i,t_i}^*, v \right\rangle + \sum_{(s_1,\dots,s_k) \notin \Gamma} \left\langle k_{s_1,\dots,s_k} \otimes_{i=1}^k e_{i,t_{s_i}}^*, v \right\rangle = c_{s_{1,t_1},\dots,c_{s_{k,t_k}}}$$

where $c_{s_{1,t_1},\dots,c_{s_{k,t_k}}}$ is as in Eq. (4.1), which is not zero because we assumed that $(s_{1,t_1}, \dots, s_{k,t_k}) \in \Gamma'$. This is in contradiction with our choice of the W_i which imposes that $\left\langle \otimes_{i=1}^k w_{i,t_i}, v \right\rangle = 0$, so we can conclude that P is indeed disjoint with from Γ'.

Now for each $1 \leq j \leq k$ we define Γ_j to be the set of all tuples $(s_1, \ldots, s_k)$ where $s_j \notin \{s_{j,t} : 1 \leq t \leq d_j\}$. Now $\pi_j(\Gamma_j) \leq |S_j| - d_j$.

By the choice of the W_j's we have that:

$$\operatorname{rk} v \geq \sum_{i=1}^{k} (|S_i| - d_i) \geq \sum_{i=1}^{k} |\pi_i(\Gamma_i)|$$

We also know that $\bigcup_{j=1}^{k} \Gamma_j = \Gamma$. So this proves our inequality. □

Now we can use this theorem to finish the proof of Lemma 8.

Continuation of proof of Lemma 8. We will use Theorem 4 to show that for the function f with

$$f = \sum_{a \in S} c_a \delta_a \otimes \cdots \otimes \delta_a$$

where all c_a are non-zero we have that $\operatorname{rk} f \geq |S|$. For each $V_i = \mathbf{F}^S$ we choose the basis $(v_{i,a})_{a \in S}$ with $v_{i,a} = \delta_a$. Then $\Gamma' = \{(a, \ldots, a) : (a, \ldots, a) \in S^k\}$. Now by Theorem 4 we have that $\operatorname{rk} f \geq \min_{\Gamma' = \Gamma_1 \cup \ldots \cup \Gamma_k} |\pi_1(\Gamma_1)| + \ldots + |\pi_k(\Gamma_k)| = \min_{\Gamma' = \Gamma_1 \cup \ldots \cup \Gamma_k} |\Gamma_1| + \ldots + |\Gamma_k| = |\Gamma'| = |S|$. □

Lemma 13. *If π_1 is the projection on the first coordinate that maps $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}$, then if $\delta \to 0$ slowly enough as $n \to \infty$ it holds that*

$$|\pi_1(T^n_{[X,Y]\delta(n)})| = \exp(n(H(X) + o(1))$$

for X ranging over S_X and Y ranging over S_Y.

Proof. From Lemma 9 it follows that $\pi_1(T^n_{[X,Y]\delta(n)}) \subseteq T^n_{[X]\delta(n)}$. Combining this with Lemma 10 gives that

$$|\pi_1(T^n_{[X,Y]\delta(n)+\frac{1}{n}})| \leq |T^n_{[X]\delta(n)+\frac{1}{n}}| \leq \exp(n(H(X) + o(1))).$$

Now we will prove a lower bound for the size of the set. We may assume that $\delta(n) > \frac{1}{n}$. We will show that if $\delta \to 0$ slowly enough then $T^n_{[X](\delta(n)-\frac{1}{n})/|S_Y|} \subseteq \pi_1(T^n_{[X,Y]\delta(n)})$.

Let $\mathbf{x} \in T^n_{[X]\delta(n)}$. Let X' be the random variable with all probabilities corresponding to the frequencies of $\mathbf{x}$. Let Y' be the random variable such that $P(Y' = y \wedge X' = x) = P(Y = y | X = x)P(X' = x)$. We know that $\sum_{x \in S_X} |P(X' = x) - P(X = x)| \leq \delta(n)$. Now we can find a random variable Y'' such that $P(Y'' = y \wedge X = x) \cdot n \in \mathbf{N}_{\geq 0}$ and $|P(Y'' = y \wedge X' = x) - P(Y' = y \wedge X' = x)| \leq \frac{1}{n}$ for all x and y. Now

$$\sum_{(x,y) \in S_X \times S_Y} |P((X', Y'') = (x, y)) - P((X, Y) = (x, y))| \leq \delta(n)$$

□

Theorem 5. *Let $V_1, \ldots, V_k$ be finite-dimensional vector spaces over a field $\mathbf{F}$ and let $(v_{j,s})_{s \in S_j}$ be an independent set in V_j for all $1 \leq j \leq k$, where S_j is some finite set. Now let $\Gamma \subseteq S_1 \times \ldots \times S_k$. If each of the S_j has a total ordering and Γ' is the set of maximal elements in Γ then for every*

$$v = \sum_{(s_1, \ldots, s_k) \in \Gamma} c_{(s_1, \ldots, s_k)} v_{1,s_1} \otimes \cdots \otimes v_{k,s_k} \tag{4.3}$$

with all $c_{(s_1, \ldots, s_k)}$ non-zero it holds that

$$\operatorname{rk} v^{\otimes n} \geq \exp((H + o(1))n) \tag{4.4}$$

with

$$H = \sup_{X = (X_1, \ldots, X_k)} \min_{j=1,\ldots,k} h(X_j) \tag{4.5}$$

as $n \to \infty$ where the supremum ranges over all random variables with values in Γ'

Proof. We will prove that

$$\min_{\Gamma'^n=\Gamma'_1\cup\ldots\cup\Gamma'_k} |\pi_1(\Gamma'_1)| + \ldots + |\pi_k(\Gamma'_k)| \geq \exp((H+o(1))n). \tag{4.6}$$

Then Eq. (4.4) follows from Theorem 4.

Let X be a random variable taking values in Γ'. Let $\delta : \mathbf{R}_{>0} \to \mathbf{R}_{>0}$ with $\delta(n) \to 0$ as $n \to \infty$ slow enough such that by Lemma 11

$$|T^n_{[X]\delta(n)}| = \exp((h(X_1,\ldots,X_k)+o(1))n) \tag{4.7}$$

and by Lemma 13

$$|\pi_{n,j}(T^n_{[X]\delta(n)})| = \exp((h(X_j)+o(1))n) \tag{4.8}$$

where $\pi_{n,j}$ is the projection projecting sequences in $(S_1\times\cdots\times S_k)^n$ to $(S_j)^n$.

Let $\Gamma'^n = \Gamma'_1 \cup \cdots \cup \Gamma'_k$ be an arbitrary covering of Γ^n. By the pigeon hole-principle, there is an $j \in \{1,\ldots,k\}$ with

$$|\Gamma'_j \cap T^n_{[X]\delta(n)}| \geq \frac{1}{k}\left|T^n_{[X]\delta(n)}\right|.$$

By the definition of conditional strongly typical sequences we see that

$$\bigcup_{a\in\pi_{n,j}(T^n_{[X]\delta(n)})} T^n_{[X|X_j]\delta(n)}(a) = T^n_{[X]\delta(n)}.$$

This implies that

$$\bigcup_{a\in\pi_{n,j}(T^n_{[X]\delta(n)}\cap\Gamma'_j)} T^n_{[X|X_j]\delta(n)}(a) \supseteq T^n_{[X]\delta(n)} \cap \Gamma'_j.$$

Using Lemma 11 and the fact that $T^n_{[X|X_j]\delta(n)}(a)$ is not empty for all $a \in \pi_{n,j}(T^n_{[X]\delta(n)})$ we see that

$$\sum_{a\in\pi_{n,j}(T^n_{[X]\delta(n)}\cap\Gamma'_j)} \exp((h(X|X_j)+o(1))n) = \sum_{a\in\pi_{n,j}(T^n_{[X]\delta(n)}\cap\Gamma'_j)} |T^n_{[X|X_j]\delta(n)}(a)| \geq |T^n_{[X]\delta(n)}\cap\Gamma'_j|.$$

This implies

$$|\pi_{n,j}(T^n_{[X]\delta(n)}\cap\Gamma_{n,j})|\exp((h(X|X_j)+o(1))n) \geq |T^n_{[X]\delta(n)}\cap\Gamma_{n,j}|.$$

So we also have

$$\begin{aligned}|\pi_{n,j}(T^n_{[X]\delta(n)}\cap\Gamma_{n,j})| &\geq \frac{|T^n_{[X]\delta(n)}\cap\Gamma_{n,j}|}{k\exp((h(X|X_j)+o(1))n)}\\ &= \frac{1}{k}\exp((h(X)-h(X|X_j)+o(1))n) = \frac{1}{k}\exp((h(X_j)+o(1))n).\end{aligned}$$

when we use the property of the entropy that $h(X) = h(X,Y) - h(Y|X)$. Now we absorb the factor $\frac{1}{k}$ into the $o(1)$ term and we use $h(X_j) \geq H$, resulting in

$$|\pi_1(\Gamma'_1)| + \ldots + |\pi_k(\Gamma'_k)| \geq \exp((H+o(1))n).$$

Because this holds for all coverings of Γ'^n we have proven Eq. (4.6). □

4.1. Using lower bounds to show limitations of our method

We will now use this lemma to show that in some cases our method will only provide a trivial upper bound for $r_m(\mathbf{F}^n)$.

Theorem 6. *Let G be an finite abelian group. Suppose there exist k total orderings on G such that their product order on G^k has all constant tuples as maximal elements of the set of k-term arithmetic progressions in G. Let $f : G^k \to \mathbf{F}$ be a function with $f(\mathbf{x}) = 0$ for all $\mathbf{x} = (x_1, \dots, x_k) \in G^k$ that do not form an arithmetic progression and $f(\mathbf{y}) \neq 0$ for all $\mathbf{y} = (y, \dots, y) \in G^k$. Then $\mathrm{rk}\, f \geq |G|$.*

Proof. We apply Theorem 4 with the following basis: for all $i \in \{1, \dots, k\}$ and all $a \in G$, $v_{i,a} = \delta_a$. Now Γ is subset of only k-term arithmetic progressions in G and all k-term constant progressions in G. We know there is an ordering for each of the coordinates such that all constant terms are maximal in Γ, and therefore are all in Γ'. This means that there exist $\Gamma_1, \dots, \Gamma_k$ with $\Gamma' = \Gamma_1 \cup \cdots \cup \Gamma_k$ such that $\mathrm{rk}\, f \geq |\pi_1(\Gamma_1)| + \cdots + |\pi_k(\Gamma_k)|$. This number will now be bigger than $|G|$, which is the number of constant progressions. So $\mathrm{rk}\, f \geq |G|$. □

It has been proven that there exist orderings per coordinate, such that in the product order the constant sequences are maximal in the set of arithmetic progressions in C_n^8, where C_n is the cyclic group of order n. [9]. Note that because every finite abelian group G can be written as the product of cyclic groups, this holds for the arithmetic progressions in G^8. It also holds in G^n for $n > 8$, because we choose an arbitrary order for the remaining coordinates. Then from Theorem 6 it follows that our method will only yield trivial upper bounds for the asymptotic size of $r_m(G^n)$ with $m \geq 8$.

A slight modification of the proof allows us to prove the same for C_n^7, implying our method will only yield trivial upper bounds for the asymptotic size of $r_m(G^n)$ with $m \geq 7$.

Theorem 7 (Order of C_n^7 with constant progressions maximal)**.** *Let $P = \{(a, a+b, a+2b, a+3b, a+4b, a+5b, a+6b) : a, b \in C_n\}$ Define a partial order on C_n^7 by taking the standard order for the third, fifth, sixth and seventh coordinate and the reverse order for the first, second and fourth coordinate. Then the constant tuples (c, c, c, c, c, c, c) are maximal in P.*

Proof. Suppose that $(a, a+b, a+2b, a+3b, a+4b, a+5b, a+6b) > (c, c, c, c, c, c, c)$ for some $a, b, c \in C_n$ with. If $b = 0$, then the first coordinate gives us $a \leq c$ and the third coordinate gives us $a \geq c$, so the two tuples are the same, so it can not be true that the first is greater than the second.

Suppose now that $b \neq 0$. We will now choose a representative for b in $[-\frac{n}{2}, \frac{n}{2}]$ and call this b.

If $c \in [0, \frac{n-1}{2} - 1]$, choose a representative of a in s_0 (we can do this because $(a \mod n) \leq c$). For $m \in \mathbf{N}_{\geq 0}$ we define $s_m = [0 - mn, c - mn] \cup [0 + mn, c + mn]$ and $g_m = [c - n - mn, -1 - mn] \cup [c + mn, n - 1 + mn]$. Note that we can say now that if $a + k_1 b \in s_{n_1}$ and $a + k_2 b \in g_{n_2}$ for $k_1 \geq 0$ and $k_2 \geq 0$ then $n_1 < n_2$ if and only if $k_1 \leq k_2$. The distance between s_m and $s_{m'}$ for $m \neq m'$ is now at least $n - c$, so at least $\frac{n-1}{2} + 1 > \frac{n}{2} \geq |b|$. Because of this $a + b \in s_0$.

Because $(a + 2b \mod n) \geq c$ we know for an $m \in \mathbb{N}_{\geq 0}$ that $a + 2b \in g_m$. Because this interval has to be within a distance of $|b| \leq \frac{n}{2}$ of $a + b$ which is in s_0, we know $a + 2b \in g_0$. We know $a + 3b \in s_m$ for an $m > 0$, but because it has to be within a distance of $\frac{n}{2}$ of $a + 2b \in g_0$ it has to be in s_1. Using the same argument as before we now know that $a + 4b \in g_1$. Because $a \in s_0$ and $a + b \in s_0$, we know that $|b| \leq c$. Because the distance between different g_m intervals is at least $c + 1$, we know that $a + 5b \in g_1$ and therefore also $a + 6b \in g_1$. So $[a + 4b, a + 6b] \subseteq g_1$, which means that

$$|2b| \leq n - 1 - c \tag{4.9}$$

But we also know that $a + b \in s_0$ and $a + 3b \in s_1$. The distance between these intervals is $n - c$, so $|2b| > n - c$. This is in contradiction with 4.9.

Now suppose that $c \in [\frac{n-1}{2}, n-1]$. For $m \in \mathbf{N}_{\geq 0}$ we define $\hat{s}_m = [0 - mn, c - mn] \cup [n + mn, n + c + mn]$ and $\hat{g}_m = [c - mn, n - 1 - mn] \cup [c + mn, n - 1 + mn]$. Choose a such that $a + 6b \in \hat{g}_0$. Note that we can say now that if $a + 6b - k_1 b \in \hat{s}_{n_1}$ and $a + 6b - k_2 b \in \hat{g}_{n_2}$ for $k_1 \geq 0$ and $k_2 \geq 0$ then $n_1 < n_2$ if and only if $k_1 \leq k_2$. Because the distance between the intervals $\hat{g}_m$ is at least $c + 1 \geq \frac{n-1}{2} + 1 > \frac{n}{2} > |b|$, we know that $a + 5b \in \hat{g}_0$ and therefore also $a + 4b \in \hat{g}_0$. This yields the following:

$$|2b| \leq n - 1 - c \leq \frac{n-1}{2} \tag{4.10}$$

Because $a+3b$ has to be within $\frac{n-1}{2}$ of this interval and $(a+3b \mod n) \leq c$ we know that $a+3b \in \hat{s}_0$. Now $a+2b$ has to be within $\frac{n-1}{2}$ of this, so $a+2b \in \hat{g}_1$, and using the same reasoning $a+b \in \hat{s}_1$ and $a \in \hat{s}_1$. This means that $|2b| \geq \frac{n-1}{2}+1$, which is in contradiction with 4.10.

We have now derived a contradiction for all cases where there is an arithmetic progression 'bigger' than the constant tuple. So this means all constant tuples are maximal elements of P. □

Now that we have shown that our result also holds for $r_m(G^n)$ with $m \geq 7$ it would be natural to ask whether we can do the same for $m = 6$. For some individual C_n there is a suitable ordering: For C_7 the sequence of orderings s, s, r, s, r, r where s is the standard order and r the reverse standard order suffices, implying we won't find non-trivial upper bounds for $r_5(\mathbf{F}_7^n)$. However, this ordering does not work for C_8 or C_9. It could be interesting to find out for which C_n there exist suitable orderings for the 6-term arithmetic progressions.

5

Applications

Now we will apply the techniques that we developed to our initial problem. We use them to give an asymptotic upper bound for $r_3(\mathbf{F}_3^n)$. To calculate our upper bound we have to find the supremum in Eq. (3.9). The following theorem makes finding the supremum easier.

Theorem 8. *If $X = (X_1, \dots, X_k)$ is a random variable taking values only in the finite set $\Gamma \subseteq S^k$ for some set S. Now $\sigma \in S_k$ be a permutation, such that for each $a = (a_1, \dots, a_k) \in \Gamma$ also $\sigma(a) = (a_{\sigma(1)}, \dots, a_{\sigma(k)}) \in \Gamma$. Then there is a random variable Y taking values only in Γ such that for all $\gamma \in \Gamma$: $\mathbf{P}(Y = \gamma) = \mathbf{P}(Y = \sigma(\gamma))$ and*

$$\min_{j=1,\dots,k} h(Y_j) = \sup_{X=(X_1,\dots,X_k)} \min_{j=1,\dots,k} h(X_j)$$

where the supremum ranges over all random variables taking values in Γ.

Proof. If we view probability distributions as vectors in $[0,1]^{|\Gamma|}$ for which the sum of all components is 1, then the entropy function is convex, because it is the sum of the convex functions $-x \ln x$. Note that the supremum in Eq. (5.1) is really a maximum because the space of probability distributions is compact. The maximum exists because the entropy function is bounded. Now we define $\sigma(X)$ of a random variable X taking values in Γ such that $\mathbb{P}(\sigma(X) = \sigma(\gamma)) = \mathbb{P}(X = \gamma)$.

We will show that there is an Y that takes a maximum in Eq. (5.1) with $\sigma(Y) = Y$. Let X be an X that takes a maximum in Eq. (5.1) and let f_X be it's probability distribution. Note that $\sigma(X)_i = X_{\sigma(i)}$. Because of that

$$\min_{j=1,\dots,k} h(X_j) = \min_{j=1,\dots,k} h(\sigma(X)_j)$$

Let n be the order or σ. Now let Y be a random variable with distribution $f_Y = \frac{\sum_{i=0}^{n-1} f_{\sigma^i(X)}}{n}$. Note that $h(Y_j) \geq \frac{\sum_{i=0}^{n-1} h(\sigma^i(X))}{n}$, because of the convexity of h. This implies that:

$$\min_{j=1,\dots,k} h(Y_j) \geq \frac{\sum_{i=0}^{n-1} \min_{j=1,\dots,k} h(\sigma^i(X)_j)}{n} = \min_{j=1,\dots,k} h(X_j).$$

So then Y also takes the maximum in Eq. (5.2) and $Y = \sigma(Y)$. □

Theorem 9. *It is true that $r_3(\mathbf{F}_3^n) \leq \exp((H + o(1))n)$ with $H = g(\beta + 2\gamma) + g(2\beta) + g(\gamma) \approx 1.013445$ for $g(x) = -x \ln x$, $\beta = \sqrt{\frac{2}{3}} - \frac{2}{3}$ and $\gamma = 1 - \sqrt{\frac{2}{3}}$.*

Proof. We define $f_n : \mathbf{F}_3^n \times \mathbf{F}_3^n \times \mathbf{F}_3^n \to \mathbf{F_3}$ with $f_n(x,y,z) = \prod_{i=1}^{n}(1 - (x_i - 2y_i + z_i)^2)$. Note that $f_n(x,y,z) = 0$ when distinct x, y and z do not form a arithmetic progression and $f_n(x,x,x) = 1$ for all x. From Theorem 1 it follows that $r_3(\mathbf{F}_3^n) \leq \operatorname{rk} f_n$.

Let $g : \mathbf{F}_3 \times \mathbf{F}_3 \times \mathbf{F}_3 \to \mathbf{F}$ with $g(x,y,z) = 1-(x-2y+z)^2$. Then $f_n = g^{\otimes n}$. We take $v_i = x^i$ for $i \in \{0,1,2\}$.

Now g is a linear combination of $v_{t_1} \otimes v_{t_2} \otimes v_{t_3}$ for $t \in \Gamma$, with

$$\Gamma = \{(0,0,0),(2,0,0),(0,2,0),(0,0,2),(1,1,0),(1,0,1),(0,1,1)\}.$$

Now by Theorem 1 and Theorem 3

$$r_3(\mathbf{F}_3^n) \leq \operatorname{rk} f^{\otimes n} \leq \exp((H+o(1))n) \tag{5.1}$$

with

$$H = \sup_{X=(X_1,\ldots,X_k)} \min_{j=1,\ldots,k} h(X_j) \tag{5.2}$$

where X takes values in Γ.

Γ is fully symmetric (i.e. for all $\sigma \in S_3, \gamma \in \Gamma$ we have $\sigma(\gamma) \in \Gamma$. Theorem 8 implies that there is an X that takes maximum in Eq. (5.2) with the same probability for all $\gamma \in \Gamma$ that are permutations of each other. The probability distribution of such a variable is defined by its values $\alpha = f_X((0,0,0))$, $\beta = f_X((1,1,0))$ and $\gamma = f_X((2,0,0))$ with the condition that $\alpha,\beta,\gamma \in [0,1]$ and $\alpha+3\beta+3\gamma = 1$.

Then the entropy of X_i is now given by:

$$\begin{aligned} h(X_i) &= g(f_{X_i}(0)) + g(f_{X_i}(1)) + g(f_{X_i}(2)) \\ &= g(\alpha+\beta+2\gamma) + g(2\beta) + g(\gamma) \end{aligned}$$

with $g(x) = -x\ln x$.

Using calculus it is now easy to verify that this function is maximal when

$$\begin{aligned} \alpha &= 0 \\ \beta &= \sqrt{\frac{2}{3}} - \frac{2}{3} \\ \gamma &= 1 - \sqrt{\frac{2}{3}}. \end{aligned}$$

The proof can be found in Appendix A. □

When applying the standard order on the set $\{0,1,2\}$ in this proof, we see that $\Gamma := \Gamma \setminus \{(0,0,0)\}$ is the set of maximal elements in Γ. Then by Theorem 5 we see that for f in the proof we also have $\operatorname{rk} f = \exp((H+o(1))n)$. This means that we can not find a better upper bound for $r_3(\mathbf{F}_3^n)$ using this function by using another basis.

There are, however, bases that give a worse upper bound. For example using the basis $\{\delta_0,\delta_1,\delta_2\}$ we can write $f(a,b,c) = \sum_{i=0}^{2} \delta_i(a)\delta_i(b)\delta_i(c) + \sum_{\sigma\in \mathrm{Sym}(\{0,1,2\})} \delta_{\sigma(0)}(a)\delta_{\sigma(1)}(b)\delta_{\sigma(2)}(c)$. Then $\{(0,0,0),(1,1,1),(2,2,2)\} \subseteq \Gamma$. Now we see that the random variable X that takes each of these values with probability $\frac{1}{3}$ we have $h(X_i) = \log(3)$ for all i, so this gives the upper bound $\operatorname{rk} f \leq 3^{(1+o(1))n}$, which is a trivial upper bound.

Although we have shown that this particular function f can not provide a better upper bound for $r_3(\mathbf{F}_3^n)$ it is possible that a better upper bound can be obtained using a different function f that is zero on all arithmetic progressions of size 3 and nonzero when $a=b=c$.

While we have seen that using this method we won't be able to find non-trivial asymptotic upper bounds for $r_m(\mathbf{F}^n)$ when $m \geq 7$, it might be possible when $4 \leq m \leq 6$.

5.1. Extending to $\mathbf{F}_5$

We can find an asymptotic upper bound for $r_3(\mathbf{F}_5^n)$ using the function $f(x,y,z) = \prod_{i=1}^{n}(1-(x_i-2y_i+z_i)^4)$. When using the polynomial basis again as in the proof of Theorem 9 we see that the Γ for this function will now consist of all permutations of the tuples in

$$\{(4,0,0),(3,1,0),(2,2,0),(2,1,1),(0,0,0)\}.$$

If we let $x_1 = \mathbf{P}(X = (4,0,0)), \ldots, x_5 = \mathbf{P}(X = (0,0,0))$ this reduces to the problem of maximizing

$$\begin{aligned} & h(X) = g(x_1) + g(2x_2) + g(2x_3 + x_4) + g(2x_2 + 2x_4) + g(2x_1 + 2x_2 + x_3 + x_5) \\ \text{with} \quad & g(x) = -x \log x \\ \text{subject to} \quad & 0 \le x_i \qquad \forall i \in \{1,2,3,4,5\} \\ & 1 \ge 3x_1 + 6x_2 + 3x_3 + 3_4 + x_5 \end{aligned}$$

We used numerical optimization to approximate the maximum. We see that the maximal value for $h(X)$ is approximately 1.49550221. This maximum is obtained when $x \approx (8.81041304 \times 10^{-2}, 6.23655994 \times 10^{-2}, 5.68842581 \times 10^{-2}, 6.36137460 \times 10^{-2}, 0)$.

This results in the upper bound $r_3(\mathbf{F}_5^n) \le 4.46158^{(1+o(1))n}$.

6

Conclusion

We have seen that m-term arithmetic progression-free sets are a generalization of cap sets. We also saw that the slice rank can be used to give an upper bound for the size of these sets. Using this method we obtained the non-trivial asymptotic upper-bound $r_3(\mathbf{F}_3^n) \leq 2.755^{n(1+o(1))}$ on the size of cap sets. We did this by using the polynomial basis for the function space from $\mathbf{F}_3^n \to \mathbf{F}_3$. We have also shown that it is not possible to get a better upper bound by only using another basis. However, it might be possible to get a better upper bound for $r_3(\mathbf{F}_3^n)$ by using a different function f.

We also saw some limitations of our method: It only gives trivial upper bounds on the size of sets without m-term arithmetic progressions for $m \geq 7$. For $4 \leq m \leq 6$ we still don't know whether the method can provide us with a non-trivial asymptotic upper bound for $r_m(\mathbf{F}^n)$ for certain $\mathbf{F}$. This is an interesting question for further research.

Overall, it is clear that we don't know much about the asymptotic behavior of $r_m(G^n)$ for arbitrary groups. Although the slice rank has been helpful for some instances of the problem, it might not work for all instances. Another limitation of the method described in this report is that it only provides asymptotic upper bounds, not lower bounds. In short, there is still a lot left to discover in this area, that is much more complex than simply playing a game of SET.

Appendices

A

Maximizing h

We want to maximize $h(\alpha,\beta,\gamma) = g(\alpha+\beta+2\gamma)+g(2\beta)+g(\gamma)$ with $\alpha,\beta,\gamma \in [0,1]$ and $\alpha+3\beta+3\gamma = 1$, where $g(x) = -x\ln x$.

Using that $\alpha = 1-3\beta-3\gamma$ we see that this is equivalent with maximizing $f(\beta,\gamma) = g(1-2\beta-\gamma)+g(2\beta)+g(\gamma)$ for $a,b \in [0,1]$ and $3\beta+3\gamma \in [0,1]$. Because this function is differentiable on this closed, bounded set, we know that it takes a maximum in either

- a point where $f_\beta(\beta,\gamma) = f_\gamma(\beta,\gamma) = 0$ or
- a point on one of the boundaries (so $\beta = 0$ or $\gamma = 0$ or $3\beta+3\gamma = 1$).

A.1. When derivatives are zero

We find that

$$f_\beta(\beta,\gamma) = -2\ln(2\beta)+2\ln(-2\beta-\gamma+1)$$
$$f_\gamma(\beta,\gamma) = -\ln(\gamma)+\ln(-2\beta-\gamma+1).$$

Now $f_\alpha(\alpha,\beta) = f_\beta(\alpha,\beta) = 0$ implies that $\ln(2b) = \ln(c)$, so $2b = c$. Also $f_\beta(\alpha,\beta) = 0$ gives that $\gamma = 2\beta-\gamma+1$. Substituting that $2\beta = \gamma$ results in $\gamma = \gamma-\gamma+1 = 1$ and $\beta = \gamma/2 = \frac{1}{2}$. Now $3\beta+3\gamma > 1$, so this point is outside of our boundaries. So there is no point where $f' = 0$ inside our boundaries.

A.2. Points on the boundary

When $\beta = 0$, we are left with maximizing $\phi(\gamma) := f(0,\gamma) = g(1-\gamma)+g(\gamma)$. Now $\phi'(\beta) = 0$ if and only if $\beta = \frac{1}{2}$, which is outside our domain because then $3\beta+3\gamma \geq 1$.

When $\beta = \gamma = 0$ we get that $f(\alpha,\beta) = -\ln 1$. When $\beta = 0$ and $3\beta+3\gamma = 1$ we get that $\gamma = \frac{1}{3}$ and $f(0,\gamma) = g(\frac{1}{3})+g(\frac{2}{3}) \approx 0.64$.

When $\gamma = 0$, we are left with maximizing $\phi(\beta) := f(\beta,0) = g(1-2\beta)+g(2\beta)$. Now $\phi'(\beta) = 0$ if and only if $\beta = \frac{1}{4}$, which gives us a value of $\phi(\frac{1}{4}) \approx 0.69$.

When $\gamma = 0$ and $3\beta+3\gamma = 1$ we get that $\beta = \frac{1}{3}$ and $f(\beta,\gamma) = g(\frac{1}{3})+g(\frac{2}{3}) \approx 0.64$.

When $3\beta+3\gamma = 1$ we get that $\beta = \frac{1}{3}-\gamma$. Then we only have to optimize $\phi(\beta) = g(1-\beta-\frac{1}{3})+g(2\beta)+g(\frac{1}{3}-\gamma)$. Now $\phi_\beta(\beta) = -2\ln(2\beta)+\ln(-\beta+2/3)+\ln(-b+1/3)$ which is zero if and only if $4\beta^2 = \left(\frac{2}{3}-\beta\right)\left(\frac{1}{3}-\beta\right)$, which is exactly when $3\beta^2+\beta-\frac{2}{9} = 0$, which implies that $\beta = \frac{\sqrt{11/3}-1}{6}$ (because it has to be within the bounds). Then $\gamma = \frac{3-\sqrt{11/3}}{6}$ and $\alpha = 0$ and $h(\alpha,\beta,\gamma) \approx 1.01345$ which is the maximum.

Bibliography

[1] Michel Coornaert. *Topological Dimension and Dynamical Systems*, chapter 6.2, page 109. Springer, 2015.

[2] Ernie Croot, Vsevolod F Lev, and Péter Pál Pach. Progression-free sets in $\mathbb{Z}_4^n$. *Annals of Mathematics*, 185:331–337, 2017.

[3] Benjamin Lent Davis and Diane Maclagan. The card game set. *The Mathematical Intelligencer*, 25(3):33–40, 2003.

[4] Yves Edel, Sandy Ferret, I Landjev, and Leo Storme. The classification of the largest caps in AG$(5,3)$. *Journal of Combinatorial Theory, Series A*, 99(1):95–110, 2002.

[5] Jordan S Ellenberg and Dion Gijswijt. On large subsets of $\mathbf{F}_q^n$ with no three-term arithmetic progression. *Annals of Mathematics*, 185:339–343, 2017.

[6] John Lee. *Introduction to smooth manifolds*. Springer, New York, 2003.

[7] Aaron Potechin. Maximal caps in AG$(6,3)$. *Designs, Codes and Cryptography*, 46(3):243–259, 2008.

[8] Terence Tao. A symmetric formulation of the croot-lev-pach-ellenberg-gijswijt capset bound. `https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound/`, 2016.

[9] Terence Tao and William F Sawin. Notes on the “slice rank” of tensors. `https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors/`, 2016.

[10] Raymond W Yeung. *Information theory and network coding*. Springer Science & Business Media, 2008.