Eötvös Loránd University

Department of Mathematics

Márton Hablicsek

Sum-free sets

Master's Thesis

advisor
László Pyber, Research Fellow
Alfréd Rényi Institute of Mathematics
Research Divison: Combinatorics

Budapest, 2009.

Contents

Introduction

A famous theorem of Schur states that for any k there exists an integer N such that for every $n > N$ and for every partition of $\{1, 2, \ldots, n\}$ into k sets there exists x, y, z in the same subset such that $x + y = z$ holds. He applied this theorem to prove that the Fermat-theorem does not hold in $\mathbf{F}_p$, namely for every positive integer k if p is a sufficiently large prime then $x^k + y^k = z^k$ has a non-trivial solution in $\mathbf{F}_p$.

A subset of integers S is a sum-free set if there do not exist $x, y, z \in S$ such that $x + y = z$. Schur's theorem motivated many investigations of sum-free sets. The definition was extended to any group. In an arbitrary group we call these sets product-free sets.

We deal with two main problems of the theory of sum-free sets: how large a sum-free set can be and how many sum-free sets are needed in a partition of a set. In Chapter 1 we discuss the results of the theory of sum-free subsets of integers and that of abelian groups. We show that there exists a sum-free subset of size cn of a set of size n and we can partition this set into $c \log n$ sum-free sets. In Chapter 2 we show that the abelian case is much simpler than the non-abelian case. As an illustration Tim Gowers proved that the size of the largest product-free set of $PSL(2, q)$ is at most $|PSL(2, q)|^{\frac{8}{9}}$.

In Chapter 3 we discuss the number of product-free sets needed in a partition of an arbitrary group. We sharpen a result of Zvi Arad, Gideon Ehrlich, Otto H. Kegel, John C. Lennox ([AEKL] Theorem B). Furthermore we provide lower and upper bound for the number of product-free sets needed in a partition which are relatively close to one another.

1 Sum-free subsets of integers and abelian groups

In this chapter we introduce some results in the theory of sum-free sets. We examine how large a sum-free subset of a set can be and how many sets are necessary to partition a set into sum-free sets.
In Section 1 we show an application of the theory of sum-free sets proving that the Fermat theorem does not hold modulo p, that is for every n, if p is sufficiently large there are three non-zero elements of $\mathbf{F}_p$: x, y and z with the following property: $x^n + y^n = z^n$.
In Section 2 we give generalizations of some propositions from Section 1 and estimate the minimal number of sets needed to partition an abelian group into sum-free sets.

The beginnings of the sections contain lemmas and propositions from [AK]. We use several remarks and a proof from [Özg].

1.1 Sum-free sets of the integers

In this section we will show several results from the theory of sum-free sets of the integers. The definition of the sum-free set is the following:

Definition 1.1.1. *S is a classical sum-free set if $S \subseteq \{1, 2, \ldots, n\}$ for an n and there is no solution to $x + y = z$ where x, y and z are three different elements of S.*

But we will work with another more convenient definition:

Definition 1.1.2. *S is a sum-free set if $S \subseteq \{1, 2, \ldots, n\}$ for an n and there is no solution to $x + y = z$ where x, y and z are not necessarily different elements of S.*

Example 1.1.1. *$\{1, 3, \ldots 2n - 1\}$ is clearly a sum-free set, because the sum of two odd numbers is even.*

Our first goal is to find the maximal size of classical sum-free sets and sum-free sets. We will show in Chapter 3 that the two definitions are essentially the same. So we will work with sum-free sets only.

In every set of integers there exist large sum-free sets, the following lemma of Paul Erdős ([Erd]) gives us a lower bound of the size of the largest one, namely:

Lemma 1.1.1. *If B is a set of m non-zero integers then it contains a sum-free set A with cardinality $|A| > \frac{1}{3}m$.*

Proof. Let $B = (b_1, b_2, \dots b_m)$ be a set of m non-zero integers and $p = 3k + 2$ be a prime with the property that $p > 1 + \max b_i$. Therefore all of the b_i have a different residue with respect to p and this residue is never 0. In the cyclic group Z_p defined by the elements $0, 1, \dots 3k + 1$ we can observe that the following set is a sum-free set: $C = \{k + 1, k + 2, ..., 2k + 1\}$, because

$$C + C = \{2k + 2, \dots, 4k + 2\} \equiv \{0, 1, \dots k, 2k + 2, 2k + 3 \dots 3k + 1\} \quad (p).$$

Furthermore C is a large set in Z_p: $|C| = k + 1 > \frac{1}{3}(3k + 2)$. Now choose at random an integer x $(1 \leq x < p)$ according to the uniform distribution on the set $\{1, 2 \dots p - 1\}$ and define d_i by $d_i \equiv xb_i \ \ (p)$. We can see that if x runs from 1 to $p - 1$ then d_i runs from 1 to $p - 1$ too because b_i is relatively prime to p. Therefore the probability that C contains d_i is exactly $\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}$. Moreover the expected number of elements b_i such that d_i is in C is more than $\frac{1}{3}m$. Thus there exists an $1 \leq x < p$ such that $|\{xb_1, xb_2, \dots xb_m\} \cap C| > \frac{1}{3}m$. Let the corresponding b_i's in the intersection be $b_{i_1}, b_{i_2}, \dots, b_{i_k}$ where $k > \frac{1}{3}m$.
C is a sum-free set, therefore $xb_{i_l} + xb_{i_t} \not\equiv xb_{i_s}$ for any $1 \leq l, s, t \leq k$. Thus $b_{i_l} + b_{i_t} \not\equiv b_{i_s}$, so we found a sum-free subset of B with density more than $\frac{1}{3}$. □

Jean Bourgain sharpened this result ([Bou]) refining this approach:

Theorem 1.1.1. *If B is a set of m non-zero integers then it contains a sum-free set A with cardinality $|A| \geq \frac{1}{3}(m + 2)$.*

As a trivial consequence we obtain from Lemma 1.1.1 the following:

Corollary 1.1.1. *We can partition the set $\{1, 2, \dots, n\}$ into $O(\log n)$ sum-free sets. More precisely if k is fixed then we can partition $\{1, 2, \dots m\}$ into k sum-free sets if $m \leq \left\lfloor \left(\frac{3}{2}\right)^{k-1} \right\rfloor$.*

Proof. We prove simultaneously the two parts of the corollary. We choose a large sum-free subset from $\{1, 2, \dots, n\}$ with density more than $\frac{1}{3}$, then we choose a large sum-free set from the remaining elements again with density more than $\frac{1}{3}$, we repeat it until all elements are chosen. So we can partition $\{1\}$ into 1 sum-free set, $\left\{1, \dots, \left\lfloor \frac{3}{2} \right\rfloor\right\}$ into 2 sum-free sets, $\left\{1, \dots, \left\lfloor \left(\frac{3}{2}\right)^2 \right\rfloor\right\}$ into 3 sum-free sets, ..., $\left\{1, \dots, \left\lfloor \left(\frac{3}{2}\right)^{k-1} \right\rfloor\right\}$ into k sum-free sets. Furthermore, trivially if we partition $\{1, \dots, m\}$ into l sum-free sets then we can partition $\{1, \dots, m'\}$ into l sum-free sets if $m' \leq m$, and by this simple observation the proof is complete. □

So we obtained an upper bound for the number of sets used in a partition of $\{1, 2, \dots n\}$ into sum-free sets. Schur obtained the following ([Sch]). This proof can be found in [Özg].

Theorem 1.1.2 (Classical Schur-problem)**.** *Given an integer k there exists an integer $N(k)$ with the property that if $n \geq N(k)$ then the set $\{1, 2, \dots, n\}$ cannot be partitioned into k sum-free sets. Furthermore:*

$$\frac{1}{2}\left(3^k - 1\right) \leq N(k) \leq [k!e] - 1.$$

Proof. From Corollary 1.1.1 we know that $N(k) \geq \left(\frac{3}{2}\right)^{k-1}$. The improved lower bound of the theorem will be proved by induction. First, the case when $k = 1$ is trivial, the lower bound is 1.

Now we will prove that if we can partition $\{1, 2, \dots, n\}$ into k sum-free sets then we can partition $\{1, 2, \dots, 3n + 1\}$ into $k + 1$ sum-free sets. Let the k sum-free sets in the partition of $\{1, 2, \dots, n\}$ be:

$$S_1 = \{x_{11}, x_{12}, \dots, x_{1t_1}\}, \dots, S_k = \{x_{k1}, \dots, x_{kt_k}\}.$$

Now we define the $k + 1$ sum-free sets in the partition of $\{1, 2, \dots, 3n + 1\}$. First we construct the first k sum-free set from $S_1, S_2, \dots S_k$ in the following way:

$$S'_j = \left\{3x_{j1}, 3x_{j1} - 1, 3x_{j2}, 3x_{j2} - 1, \dots, 3x_{jt_j}, 3x_{jt_j} - 1\right\}.$$

Furthermore let the $k + 1$-th sum-free set be the set of the remaining elements which are the elements congruent to 1 modulo 3. Clearly it is a sum-free set because the sum of two such elements is congruent to 2 modulo 3.

Now consider the set S'_j and suppose that it is not a sum-free set. Then there exist $a, b, c \in S'_j$ such that $a + b = c$ holds. There are two kinds of elements in S'_j those which are congruent to 2 modulo 3 and those which are divisible by 3. There are three possible cases: $a \equiv c \equiv 2 \pmod 3$ and $3|b$ or $b \equiv c \equiv 2 \pmod 3$ and $3|a$ or $a \equiv b \equiv c \equiv 0 \pmod 3$. In the first case let $a = 3x_{ju} - 1$, $b = 3x_{jv}$ and $c = 3x_{jw} - 1$. Then from the equation $3x_{ju} - 1 + 3x_{jv} = 3x_{jw} - 1$ we obtain that $x_{ju} + x_{jv} = x_{jw}$ which is a contradiction because S_j is a sum-free set. We can exclude the second case after exchanging a and b. So the only possible case is the third one.

But in this case let $a = 3x_{ju}$, $b = 3x_{jv}$ and $c = 3x_{jw}$, then the equation $x_{ju} + x_{jv} = x_{jw}$

is a trivial consequence of the equation $3x_{ju} + 3x_{jv} = 3x_{jw}$, which is a contradiction again.
Therefore $N(k+1) \geq 3N(k)+1$. Since $N(1) \geq 1$ by recursion we obtain that $N(k) \geq 1+3+\ldots+3^{k-1} = \frac{3^k-1}{2}$.
We will not prove the second part of this theorem, a more general statement will be proved with a constant 3 instead of e. □

An interesting consequence of the theorem is:

Corollary 1.1.2. *The Fermat-theorem does not hold in $\boldsymbol{F}_p$, namely for every positive integer n there exist three non-zero elements in $\boldsymbol{F}_p$ for every prime p large enough: x, y and z such that $x^n + y^n = z^n$ holds.*

Proof. First suppose that $n|p-1$, namely $nr = p-1$. We know that there is a primitive root in $\mathbf{F}_p$, let us denote it by g. Let s_m be the residue of g^m with respect to p. Since g is a primitive root s_m runs from 1 to $p-1$ and attains all values once.
Then we partition $\{1, 2, \ldots, p-1\}$ into n disjoint sets: $X_i = \left\{s_i, s_{i+n}, \ldots, s_{i+n(r-1)}\right\}$ where i runs from 0 to $n-1$. From Theorem 1.1.2 we obtain that if p is large enough $(p-1 \geq n!e)$ then at least one of the sets X_i is not sum-free set.
Suppose that X_i is not a sum-free set. Then there exist a_1, a_2 and a_3 such that $s_{i+a_1 n} + s_{i+a_2 n} = s_{i+a_3 n}$. Therefore $g^{i+a_1 n} + g^{i+a_2 n} = g^{i+a_3 n}$ in $\mathbf{F}_p$, hence $(g^{a_1})^n + (g^{a_2})^n = (g^{a_3})^n$. We can see that $g^{a_1}, g^{a_2}, g^{a_3}$ are non-zero elements of $\mathbf{F}_p$ so we have proved the statement.
In the other case when $p-1$ is not divisible by n let $d = (n, p-1)$. From the first case we know that there exist three non-zero elements of $\mathbf{F}_p$: a, b and c such that $a^d + b^d = c^d$ if p is large enough $(p-1 \geq d!e)$. The existence of a primitive root and $d = (n, p-1)$ imply that there exist $u, v, w \in \mathbf{F}_p$ with the property that $u^n = a^d$, $v^n = b^d$ and $w^n = c^d$ and we can easily see that u, v and w are non-zero elements.
Summing up we obtain that if $p-1 \geq n!e \geq d!e$ then there is a solution of $x^n + y^n = z^n$ where x, y and z are non-zero elements. Thus we have proved the statement. □

Remark 1.1.1. *The smallest such $N(k)$ in Theorem 1.1.2 for an integer k is called the Schur-number. Only the first four Schur-numbers are exactly calculated. Let us compare it with the lower bounds and upper bounds given in Theorem 1.1.2:*

k	$N(k)$	*lower bound*	*upper bound*
1	1	1	1
2	4	4	4
3	13	13	15
4	44	40	64

1.2 Sum-free sets in finite abelian groups

In this section we will discuss results for sum-free sets in finite abelian groups that are similar to those proved in the previous section for sum-free sets of the integers. We have to redefine sum-free sets. Again we can define two types of sum-free sets as in Section 1:

Definition 1.2.1. *S is a classical sum-free set of an abelian group G if $S \subseteq G$ and there is no solution for $x+y=z$ such that x, y and z are three different elements of S.*

Definition 1.2.2. *S is a sum-free set of an abelian group G if $S \subseteq G$ and there is no solution for $x+y=z$ such that x, y and z are not necessarily different elements of S.*

We will use the more convenient definition but we will show in Chapter 3 that the two definitions are essentially equivalent. Note that if we use the second definition then 0 cannot be an element of a sum-free set because $0+0=0$.
Moreover we can see that if S is a sum-free set in a finite group G then $|S| \leq \frac{|G|}{2}$, because clearly $S+S$ is disjoint from S. This upper bound for the density is sharp, since there are sum-free sets with density $\frac{1}{2}$. As an example consider the non-trivial coset of $H \leq G$ where $|G:H|=2$.

Now we want to find a lower bound for the density of the largest sum-free set in a finite abelian group G.
Remember that in the proof of Lemma 1.1.1 the existence of a large sum-free set of Z_p was a crucial point. Now, we will use two large sum-free sets in Z_n to prove a sharp result. The two sum-free sets are:

$$I_1 = \left\{ x \in Z_n : \frac{1}{3}n < x \leq \frac{2}{3}n \right\},$$

$$I_2 = \left\{ x \in Z_n : \frac{1}{6}n < x \leq \frac{1}{3}n \text{ or } \frac{2}{3}n < x \leq \frac{5}{6}n \right\}.$$

In the proof of Lemma 1.1.1 another important observation that we used was the following: if $ax + bx \equiv cx \quad (p)$ and $x \neq 0$ then $a + b \equiv c \quad (p)$. Clearly, if we replace p with n then these two equations are not equivalent.
Still if $a, b, c \in Z_n$ and for an $x \in Z_n$ we know that $ax + bx \neq cx$ then $a + b = c$ cannot hold. So instead of proving that $A \subseteq Z_n$ is a sum-free set it is sufficient to prove that $xA \subseteq Z_n$ is a sum-free set for an $x \in Z_n$. Moreover we can see the following:

Lemma 1.2.1. *If $\varphi : G_1 \to G_2$ is a homomorphism and $S \subseteq G_2$ is a sum-free set then $\varphi^{-1}(S)$ is also a sum-free set.*

Proof. Suppose that $\varphi^{-1}(S)$ is not a sum-free set. Then there exist three elements in $\varphi^{-1}(S)$: $\varphi^{-1}(a)$, $\varphi^{-1}(b)$ and $\varphi^{-1}(c)$ $(a, b, c \in S)$ such that $\varphi^{-1}(a) + \varphi^{-1}(b) = \varphi^{-1}(c)$. Applying φ to both sides we obtain that $a + b = c$ which is a contradiction because S is a sum-free set. □

In the next step suppose that d is a divisor of n and look at dZ_n. We are interested in the density of I_1 and I_2 in dZ_n, namely in $\frac{|dZ_n \cap I_j|}{|dZ_n|}$ $(j = 1, 2)$.

Lemma 1.2.2. *For every n and for every divisor d of n:*

$$\frac{4}{7}\frac{|dZ_n \cap I_1|}{|dZ_n|} + \frac{3}{7}\frac{|dZ_n \cap I_2|}{|dZ_n|} \geq \frac{2}{7}.$$

Proof. We prove the statement by computing the densities with respect to the residue of $\frac{n}{d}$ modulo 6. The results are contained in the following table :

$\frac{n}{d}$	$\frac{\lvert dZ_n \cap I_1\rvert}{\lvert dZ_n\rvert}$	$\frac{\lvert dZ_n \cap I_2\rvert}{\lvert dZ_n\rvert}$
$6k$	$\frac{1}{3}$	$\frac{1}{3}$
$6k+1$	$\frac{2k}{6k+1}$	$\frac{2k}{6k+1}$
$6k+2$	$\frac{2k+1}{6k+2}$	$\frac{2k}{6k+2}$
$6k+3$	$\frac{2k+1}{6k+3}$	$\frac{2k+1}{6k+3}$
$6k+4$	$\frac{2k+1}{6k+4}$	$\frac{2k+2}{6k+4}$
$6k+5$	$\frac{2k+2}{6k+5}$	$\frac{2k+2}{6k+5}$

Now with simple calculations we obtain the statement. □

After these preparations we can prove the following theorem due to Alon and Kleitman [AK]:

Theorem 1.2.1. *Let B be a set of m non-zero elements of a finite abelian group G. Let us denote the maximal cardinality of a sum-free set in B by $s(B)$. Then $s(B) > \frac{2}{7}m$.*

Proof. First of all we know that a finite abelian group can be written as a direct sum of cyclic groups. Therefore we can assume that G is a subgroup of a direct sum of s copies of Z_n hence $B \subseteq Z_n \oplus \ldots \oplus Z_n$. Thus we can write the elements $b_i \in B$ into the following form: $b_i = (b_{i1}, \ldots, b_{is})$ where each b_{ij} corresponds to a positive integer less than n. Let us denote the greatest common divisor of the integers corresponding to $b_{i1}, \ldots, b_{is}$ and n by d_i.
As in the proof of Lemma 1.1.1 we choose at random an element of Z_n^s according to the unifom distribution, denote it by $x = (x_1, \ldots, x_s)$.
We can see that:

$$f_i(x) = \sum_{j=1}^{s} b_{ij}x_j \quad (n)$$

is a homomorphism from Z_n^s to Z_n. We can see that the image of this homomorphism is precisely d_iZ_n. Moreover as $x = (x_1, \ldots, x_s)$ ranges over all the elements of Z_n^s, $f_i(x)$ ranges over all of the elements of d_iZ_n and takes each element of d_iZ_n the same number of times. Therefore the probability that $f_i(x)$ is in I_j $(j = 1, 2)$ is $\frac{|d_iZ_n \cap I_j|}{|d_iZ_n|}$.
Now we want to calculate the expected number of elements b_i such that $f_i(x) \in I_j$. For every divisor d of n we denote the number of elements $b_i \in B$ such that $d_i = d$ by m_d. We can see that $\sum_{d|n} m_d = m$ (all elements of B are calculated once) and the expected number is $M_j = \sum_{d|n} m_d \frac{|dZ_n \cap I_j|}{|dZ_n|}$ $(j = 1, 2)$.
Since $x = (0, \ldots, 0)$ maps every b_i into $f_i = 0 \notin I_j$ there is an $x = (x_1, \ldots, x_s)$ such that it maps more than M_1 elements of B to I_1. Thus there is a set $A \subseteq B$ with strictly more than M_1 elements such that for every $a = (a_1, \ldots, a_s) \in A$: $\sum_{j=1}^{s} a_jx_j \in I_1$. Since f_i was a homomorphism and I_1 is a sum-free set we obtain that A is a sum-free set too from Lemma 1.2.1.
Therefore we have $s(B) > M_1$ $(j = 1, 2)$. Similarly we can see that $s(B) > M_2$. Thus we obtain:

$$s(B) = \frac{4}{7}s(B) + \frac{3}{7}s(B) > \frac{4}{7}M_1 + \frac{3}{7}M_2 =$$

$$= \frac{4}{7}\sum_{d|n} m_d \frac{|dZ_n \cap I_1|}{|dZ_n|} + \frac{3}{7}\sum_{d|n} m_d \frac{|dZ_n \cap I_2|}{|dZ_n|} \geq \sum_{d|n} m_d \frac{2}{7} = \frac{2}{7}m$$

from Lemma 1.2.2. □

Again as a corollary we obtain an upper bound for the number of sets needed in a partition of G into sum-free sets. This corollary is stated in the following theorem first observed by Abbott and Hanson ([AH]). Note again that 0 cannot be an element of a sum-free set thus we can partition only $G \setminus \{0\}$.

Theorem 1.2.2. *Let G be a finite abelian group. Then we can partition G into $O(\log |G|)$ sum-free sets.*

Furthermore we remark that the constant $\frac{2}{7}$ in Theorem 1.2.1 is best possible. In fact we have the following deep theorem of Ben Green and Imre Z. Ruzsa ([GR]):

Theorem 1.2.3. *Let us denote the density of the largest sum-free set in a finite abelian group, G by $\mu(G)$. Then:*

1. *if n is divisible by a prime $p \equiv 2$ (mod 3) then $\mu(G) = \frac{1}{3} + \frac{1}{3p}$ where p is the smallest such prime,*
2. *if n is not divisible by any prime $p \equiv 2$ (mod 3) but $3|n$ then $\mu(G) = \frac{1}{3}$,*
3. *if n is divisible only by primes $p \equiv 1$ (mod 3) then $\mu(G) = \frac{1}{3} - \frac{1}{3m}$ where m is the exponent of G.*

In particular we obtain that if $G = Z_7^s$ then $\mu(G) = \frac{1}{3} - \frac{1}{21} = \frac{2}{7}$. From this we see that if $B = G \setminus \{0\}$ then $s(B) = 2 \cdot 7^{s-1}$ which shows that $\frac{2}{7}$ cannot be improved. This example was first found by Rhemtulla and Street ([RS]).

Returning to partitions, there exists a lower bound for the number of the partitioning sum-free sets similar to the one in Theorem 1.1.2.

Theorem 1.2.4 (Abelian Schur-problem)**.** *Given an integer k there exists a least integer $N(k)$ with the property that if $n \geq N(k)$ and G is an abelian group with order n then G cannot be partitioned into k sum-free sets. Furthermore:*

$$\left(\frac{7}{5}\right)^k \leq N(k) \leq 3k!.$$

Proof. We can prove the lower bound by applying Theorem 1.2.1 until only $\{0\}$ remains. For the upper bound a stronger statement will be proved in Chapter 3. □

2 Product-free sets in finite groups

In the previous chapter we considered sum-free sets in the integers and in finite abelian groups. We will continue by presenting results on sum-free sets in finite groups. In this case we talk about product-free sets instead of sum-free sets.
First let us define product-free sets. Again we have two possibilities. We will use only the more convenient definition and in Chapter 3 we will prove that the two definitions are essentially the same.

Definition 2.0.3. *S is a product-free set in an arbitrary group G if $S \subseteq G$ and there is no solution to $xy = z$ where x, y and z are not necessarily different elements of S.*

We saw that the cardinality of the largest sum-free set in a finite abelian group G is at least $c\,|G|$ and we can partition G into $c \log |G|$ sum-free sets. The situation for an arbitrary group is much more complicated.
In 1985, László Babai and Vera T. Sós [BS] asked whether there exists a product-free set in every G with cardinality at least $c\,|G|$ where c is an absolute constant. They proved that there is such a set in every finite solvable group. Furthermore they noted that if H is a non-trivial subgroup of G then a non-trivial coset of H is a product-free set. Kiran S. Kedlaya improved this result in [Ke1] (see further in [Ke2] and [Ke3]) by showing that if H is a non-trivial subgroup of G with index k then we can find a product-free set in G with density $\frac{c}{k^{\frac{1}{2}}}$ where c is an absolute constant. Kedlaya repeated the question also asking whether for every $\varepsilon > 0$ there exists a product-free set in every G with cardinality $c_\varepsilon\,|G|^{1-\varepsilon}$.
Tim Gowers ([Gow]) showed that the answers to these question are negative. He proved that if S is a product-free set of G then the cardinality of S is at most $\frac{|G|}{k_G^{\frac{1}{3}}}$ where k_G is the minimal degree of a non-trivial complex linear representation of G. For example if we consider $G = PSL(2, q)$ then the cardinality of a product-free set is at most $c\,|G|^{\frac{8}{9}}$. The notation k_G will be used in the rest of the Thesis.

László Pyber and Nikolai Nikolov ([NP]) gave a simpler proof of this theorem but only for symmetric product-free sets. Following Gowers we prove a more general statement.

Theorem 2.0.5. *Let A, B and C subsets of a finite group G. If $|A|\,|B|\,|C| > \frac{|G|^3}{k_G}$, then there is a triple $(a, b, c) \in A \times B \times C$ such that $ab = c$.*

Proof. Let $V = \mathbf{C}G$ be the complex group algebra of G with basis G and let us denote $|G|$ by n. We consider V as vectorspace equipped with the standard Hermitian-product

so the elements of the basis form an orthonormal basis. Let X be the following n by n matrix over V: $x_{g,h} = 0$ if $h^{-1}g \notin B$ and $x_{g,h} = 1$ otherwise. If we consider an $u \in G \subseteq V$ then we can see that $Xu = \sum_{b\in B} ub$. Therefore by linearity for every vector $v \in V$ we obtain that $Xv = \sum_{b\in B} vb$.

Consider the eigenspaces of X. First observe that each row of X contains 1 $|B|$ times therefore $e = \sum_{g\in G} g$ is an eigenvector of X with eigenvalue $|B|$. Let $I = e^{\perp}$ namely if $v \in I$ then the sum of its coordinates in the standard basis is 0. We can see that I is X and G-invariant furthermore does not have G invariant vectors.

Now consider the eigenspaces of I. Let λ be an eigenvalue of X. Consider the eigenspaces according to λ: $V_\lambda = \{v \in V : Xv = \lambda v\}$ where λ is a complex number. Then if $v \in V_\lambda$ then $gv \in V_\lambda$ for every $g \in G$ because:

$$X(gv) = \sum_{b\in B}(gv)b = g\sum_{b\in B} vb = gXv = g\lambda v = \lambda gv.$$

Hence V_λ is a non-trivial G-module. Therefore $\dim V_\lambda \geq k_G$.

Now calculate the trace of X^*X. We can see that if we consider X in a new orthonormal basis then the new matrix form of X is $Y = UXU^{-1}$ where U is an unitary matrix. Hence $X^*X = UY^*YU^{-1}$. Therefore we only need to calculate the trace of Y^*Y. Let the new orthonormal basis be the following: we choose an orthonormal basis in V_λ and complete it to an orthonormal basis in V. Hence $\mathrm{tr}(Y^*Y) \geq k_G |\lambda|^2$, because each element of the diagonal is a sum of non-negative numbers.

We can calculate the trace of X^*X in a different way. We know that in each row of X we have 1 $|B|$ times therefore $\mathrm{tr}(X^*X) = |B|\, n$. Hence $k_G |\lambda|^2 \leq |B|\, n$. It follows that we have an upper bound for the eigenvalues $|\lambda| \leq \sqrt{\frac{|B|n}{k_G}}$.

From estimating the eigenvalues we obtain that $|Xu|^2 \leq \frac{|B|n}{k_G} |u|^2$ if $u \in I$. We will use this estimation for proving the theorem. Let $w = n\sum_{a\in A} a$. The sum of its coordinates is $|A|\, n$ moreover this equals the sum of the coordinates of $|A|\, e$. Therefore we can write w in the following form: $w = w_1 + w_2 = |A|\, e + w_2$ where $w_2 \in I$. Furthermore we can see that $|w_2|^2 = |w|^2 - |w_1|^2 \leq n^2 |A|$.

Now assume that $ab = c$ has no solution if $a \in A$, $b \in B$ and $c \in C$. From the definition of X we obtain that Xw has zeros in all coordinates corresponding to C. However $Xw = Xw_1 + Xw_2 = X\,|A|\, e + Xw_2 = |A|\,|B|\, e + Xw_2$ and it follows that the vector Xw_2 has coordinates equal to $-|A|\,|B|$ in at least $|C|$ positions so $|Xw_2|^2 \geq |A|^2\,|B|^2\,|C|$.

Summing up we obtain:

$$|A|^2 |B|^2 |C| \leq |Xw_2|^2 \leq \frac{n|B|}{k_G} |w_2|^2 \leq \frac{n|B|}{k_G} n^2 |A|$$

which implies $|A||B||C| \leq \frac{n^3}{k_G}$. □

If we set $A = B = C = S$ then we obtain the following consequence:

Corollary 2.0.1. *Suppose that S is a product-free set of a finite group G. Then $|S| \leq \frac{|G|}{k^{\frac{1}{3}}}$.*

László Pyber and Nikolai Nikolov proved in [NP] that this result cannot be improved much. Corollary 5 says from [NP] that:

Proposition 2.0.1. *Suppose that G is a finite group which has an irreducible representation of degree $k_G \geq 2$. Then G has a proper subgroup H of index at most ck_G^2 where c is an absolute constant.*

Therefore applying Kedlaya's result we see that G has a product-free set of size at least $\frac{n}{ck_G}$.

After reviewing known results from the theory of sum-free and product-free sets we will estimate how many product-free sets are needed in partitioning a finite group, using the result of Gowers.

3 Partitioning groups into product-free sets

In this chapter we will consider the minimal number of sets needed in a partition of an arbitrary group G into product-free sets. In the first section we will prove that the two definitions for sum-free sets or product-free sets are essentially the same, therefore we need to consider only one of the definitions. In the second section preliminary results will be proved. After these preparations we will give various estimates for the minimal number of such sets. These results are new.

3.1 Partitioning and colorings

In the previous chapters we got familiar with sum-free sets then with product-free sets. In this chapter our goal is to partition the group into product-free sets. Let us consider the classical definition.

Definition 3.1.1. *Let us denote the minimal number of sets needed in the partition into classical product-free sets of the group G by $g(G)$.*

If we would like to estimate $g(G)$ in terms of the structure of G we can see that there is a problem: the condition that a, b and c are different elements may not hold in a homomorphic image.
If we use the second definition of product-free sets this problem does not occur. As we saw in the previous chapters we can only partition of $G \setminus \{1\}$ into product-free subsets.

Definition 3.1.2. *Let us denote the minimal number of sets used in the partition into product-free sets of $G \setminus \{1\}$ by $f(G)$.*

To differentiate between the two definitions we will say colorings instead of partitions and we will say colors instead of product-free sets when we use the second definition.
First we discuss the relation between $g(G)$ and $f(G)$.
We can see that if we consider a partition and forget about $\{1\}$ we cannot be sure that we obtain a coloring of G. Clearly the only possible problem is that $x, y \in S$ where S is a product-free set and $x^2 = y$.
But if we consider a coloring of G then if we put 1 into an arbitrary product-free subset then we obtain a partition of G. Therefore $g(G) \leq f(G)$. We will show that the order of magnitude of $f(G)$ and $g(G)$ are the same.

Theorem 3.1.1. $g(G) \leq f(G) \leq 3g(G)$

Proof. Let us partition the group into $g(G)$ product-free sets, and let S be a product-free set in this partition. First, forget about $\{1\}$. Then we will give a coloring of S by 3 sets, S_1, S_2 and S_3 such that if $a, b, c \in S_i$ for $i = 1, 2, 3$ then $ab \neq c$. If we find these sets then we obtain that $f(G) \leq 3g(G)$.
Our goal is to find sets S_i such that for any two elements a and b in S_i $a^2 = b$ cannot hold. First choose an element x of S. Put x into S_1.
We put the elements of S into S_1, S_2 and S_3 by the following algorithm:

1. We have chosen $x_1, \ldots, x_n$ from S and we put them into three sets such that if $x_i, x_j, x_k \in S_l$ then $x_i x_j \neq x_k$. The last chosen element was x_n. Now we consider the color of x_n^2.

2. If we have chosen x_n^2 already or $x_n^2 \notin S$ then we choose another arbitrary non-chosen element of S, let us denote it by x_{n+1} and put it into S_1. Continue the algorithm from 1.

3. If x_n^2 is a non-chosen element then we have to put it into a set S_i which is different from any set S_l which is a set containing an element y such that $y^2 = x_n^2$. If $y = x_j$ where $j < n$ then we can see from the algorithm that x_n^2 has been chosen already. So there is one y such that $y^2 = x_n^2$: x_n. Therefore only one such set is excluded.

   Moreover if x_n^4 has been chosen already then S_i must be different from the set S_m which is the set that contains x_n^4. It is possible that S_l and S_m are not necessarily different sets. We can see that in any case we can choose a set S_i from S_1, S_2, S_3 because there are at most two sets we cannot choose. Let us denote $x_n^2 = x_{n+1}$ and continue the algorithm from 1.

We can see that the algorithm runs until we cannot choose another element from S and in any step we prohibit the existence of two elements a and b having the same color such that $a^2 = b$.
Therefore S_1, S_2 and S_3 are colors, hence $f(G) \leq 3g(G)$. □

Now we concentrate on finding some lower and upper bounds on $f(G)$ in terms of the structure of G.

3.2 Preliminaries

In this section we will prove elementary lemmas and propositions.

Lemma 3.2.1. *If H is a subgroup of G, then $f(H) \leq f(G)$. Thus f is a monotone increasing function.*

Proof. If G has a colouring then restricting this to a subgroup H we obtain a colouring of H. □

But f is not a strictly monotonic function, because $f(Z_2^4) \leq 3$ as shown by the following example. The sets are:

$$X_1 = \{(1,0,0,0); (0,1,0,0); (0,0,1,0); (0,0,0,1); (1,1,1,1)\},$$
$$X_2 = \{(1,1,0,0); (0,1,1,0); (0,0,1,1); (0,1,1,1); (1,1,1,0)\},$$
$$X_3 = \{(1,1,0,1); (1,0,1,1); (1,0,0,1); (0,1,0,1); (1,0,1,0)\}.$$

We can check that every four elements in each set are independent vectors in the four dimensional vectorspace over F_2, so these sets must be sum-free sets.

Lemma 3.2.2. *Suppose that H is a subgroup of G, then $f(G) \leq f(H) + |G : H| - 1$.*

Proof. Let us consider the cosets of H. We will color each non-trivial coset with only one color. Let aH be a non-trivial coset. Suppose that there exist three elements in the coset ah_1, ah_2 and ah_3 such that $ah_1ah_2 = ah_3$. From simple calculations we obtain $a = h_1^{-1}h_3h_2^{-1} \in H$ which is a contradiction. So we colored every element except the elements of H, these elements can be colored with $f(H)$ colors. So we used $f(H) + |G : H| - 1$ colors. □

Let us apply this lemma for the symmetric group. With recursion we obtain that

$$f(A_n) \leq f(A_{n-1}) + n - 1 \leq f(A_{n-2}) + n - 1 + n - 2 \leq ... \leq \sum_{j=1}^{n-1} j = \frac{n(n-1)}{2}.$$

Similarly we have an upper bound for the number of colors in permutation groups:

Proposition 3.2.1. *Suppose that G is a permutation group of degree n, then $f(G) \leq n \log |G|$.*

Proof. Let us apply Lemma 3.2.2 to the stabilizer of α. The index of the stabilizer of α is the size of the orbit corresponding to the stabilized point which is less than or equal to n, hence we obtain that $f(G) \leq f(G_\alpha) + n - 1$. G_α is a permutation group of degree at most $n-1$. Next we apply again Lemma 3.2.2 to another stabilizer. Then we obtain $f(G) \leq f((G_\alpha)_\beta) + n - 1 + n - 2 \leq f(G_{\alpha\beta}) + 2n$. We use this method until we obtain the trivial group. We can assume that every stabilizer was a proper subgroup of the previous one. Then in this process we have at most $\log |G|$ steps. In every step the upper bound increased by at most n, so from this two we obtain $f(G) \leq n \log |G|$ which proves the statement. □

We colored the groups by means of subgroups. We can sharpen Lemma 3.2.2 if we consider normal subgroups:

Lemma 3.2.3. *If $N \triangleleft G$, then $f(G) \leq f(N) + f(G/N)$.*

Proof. Let us color G/N with $f(G/N)$ colors and consider the homomorphism $\varphi : G \to G/N$. We know from Lemma 1.2.1 that if we find a product-free set S in G/N then $\varphi^{-1}(S)$ is a product-free subset of G. Since the $f(G/N)$ product-free subset of G/N cover G/N except the identity therefore we can color $G \setminus N$ with $f(G/N)$ colors.
The remaining elements are the elements of $N \setminus \{1\}$ which can be colored with $f(N)$ colors. Summing the two estimations we obtain the statement. □

Corollary 3.2.1. *Suppose that G is a solvable group. Then $f(G) \leq c \log |G|$ where c is an absolute constant.*

Proof. Apply the lemma above and Theorem 1.2.2. □

3.3 Lower bounds

After these preparations we will find a lower bound for the number of colors. We begin with a general estimate then we will prove a lower bound in terms of the structure of the group. First we prove a lemma to obtain the general estimate:

Lemma 3.3.1. *Suppose that Γ is complete graph with n vertices and we colored the edges with r colors such that there is no unicolor triangle. Then $n < 3r!$.*

Proof. We prove this statement by induction with respect to r. The case of $r = 1$ is trivial. Suppose that we proved the statement for r, now we will prove it for $r + 1$. If we have two red edges from one vertex then the edge between the two other endpoints cannot be red because Γ has not got unicolor triangles. Thus by induction the maximal number of unicolor edges from one vertex is less than $3r!$. We have $r+1$ colors therefore the number of vertices cannot be greater than $1 + (3r! - 1) \cdot (r + 1) < 3(r + 1)!$, so the lemma is proved. □

Theorem 3.3.1. *$f(G) \geq c\frac{\log|G|}{\log\log|G|}$, where c is an absolute constant.*

Proof. Suppose that we colored G with r colors. Let us consider the Cayley-graph of G. We will color the edges of the graph using these r colors. First, we enumerate the vertices: $g_1, g_2, \ldots, g_{|G|}$. If $1 \leq i < j \leq |G|$ are two indices we color the edge between g_i and g_j with the color of $g_i^{-1}g_j$. Observe that there is no monochromatic triangle in the graph in this coloring since suppose that there are indices $1 \leq i < j < k \leq |G|$ such that the edges between them are unicolor. Then $g_i^{-1}g_j$, $g_j^{-1}g_k$ and $g_i^{-1}g_k$ are unicolor, but $g_i^{-1}g_j \cdot g_j^{-1}g_k = g_i^{-1}g_k$ which is a contradiction.
Now we use the well-known lemma above and we obtain that $|G| < 3r!$, therefore $f(G) \geq c\frac{\log|G|}{\log\log|G|}$. □

A much weaker lower bound was earlier obtained in [AEKL].

Corollary 3.3.1. *$f(A_n) \geq c_2 n$, where c_2 is a constant.*

We can obtain a sharper lower bound for every group if we can find a better upper bound for Lemma 3.3.1. Now we can see a relation between product-free sets and the Ramsey-numbers, more precisely $R(3,\dots,3)$.
Till now we did not consider the structure of the group, now we will focus on it. By the theorem of Gowers ([Gow]) we know that the cardinality of the greatest product-free subset of a group, G is less than $\frac{|G|}{k_G^{\frac{1}{3}}}$ where k_G is the minimum of the dimensions of non-trivial representations. From this we obtain:

Theorem 3.3.2. *Let G be a group, then $f(G) \geq k_G^{\frac{1}{3}}$.*

Unfortunately if we take the direct product of G with an abelian group, A then the lower bound in the theorem above gives us only that $f(G \times A) \geq 1$. But with Lemma 3.2.1 we obtain that $f(G \times A) \geq f(G)$ which is usually a better lower bound. Now we use this method to obtain an improvement of Theorem 3.3.2.
In the proof we will apply a theorem of Feit and Tits from [FT]:

Theorem 3.3.3. *Let $\gamma : H \to L$ be an epimorphism where L is a non-abelian simple group and $\lambda : H \to PGL(m,F)$ be a minimal non-trivial projective representation. Suppose that H is minimal namely no subgroup of H can be mapped onto L by a homomorphism. Then one of the following two statements must be true:*

1. *$Ker\lambda = Ker\gamma$ or*
2. *$charF \neq 2$, $m = 2^n$ where $n \geq 4$ and there exists a $\mu : L \to PSp(2n,2)$ irreducible representation.*

Furthermore also from [FT] we know that

Proposition 3.3.1. *If G is a non-abelian simple group for which conclusion 2. of the theorem holds, then G is a group of Lie type in characteristic 2.*

Now we will give an improvement of Theorem 3.3.2 where we only consider Lie type composition factors by applying these statements. We will use the minimal degree of complex projective representation. Let us denote this minimal degree of a G group by r_G.
Let $\varphi : G \to GL(n,\mathbf{C})$ be a complex linear representation. We can obtain a projective representation by factorizing with the scalar matrices. If we obtain a trivial projective representation then φ maps the elements of the group into scalar matrices. Therefore if $k_G \geq 2$ then $k_G \geq r_G$. As an illustration we can see that $k_G \geq r_G$ for simple groups.

Proposition 3.3.2. *Suppose that $G_1, G_2, \dots G_s$ are non-abelian simple groups and composition factors of G. Then*

1. *if G_i is a Lie type group in characteristic 2 then $f(G) \geq r_{G_i}^{\frac{1}{6}}$,*
2. *otherwise $f(G) \geq r_{G_i}^{\frac{1}{3}}$.*

Proof. We use induction with respect to the number of composition factors and to the size of the group. If the number of composition factors is 1, then the group is simple, and by using Theorem 3.3.2 we obtain that $f(G) \geq k_G^{\frac{1}{3}} \geq r_G^{\frac{1}{3}}$.
Now suppose that L is a non-abelian simple composition factor of G and consider the minimal subgroup H of G which can be mapped onto L by γ.
We know from Lemma 3.2.1 that $f(H) \leq f(G)$ so it is sufficient to prove that $f(H) \geq r_L^{\frac{1}{6}}$ if L is a Lie type group in characteristic 2 and $f(H) \geq r_L^{\frac{1}{3}}$ otherwise. Let φ be a complex representation of degree k_H of H. This defines a complex projective representation of degree k_H of H. From the minimality of H it follows that H has no abelian quotients hence the above complex projective representation is non-trivial. Let λ be a minimal non-trivial complex projective representation of H. The degree of lambda is at most k_H.
Now we can apply Theorem 3.3.3, first observe that we have complex projective representations so the characteristic of $\mathbf{F}$ is zero. We have two cases namely which conclusion holds:

1. case: If $\mathrm{Ker}\gamma = \mathrm{Ker}\lambda$ then we obtain that λ can be considered as a projective representation of L too. Clearly that representation of L is a non-trivial projective representation of L. Therefore $k_H \geq m = r_H \geq r_L$.
Thus $f(G) \geq f(H) \geq k_H^{\frac{1}{3}} \geq r_H^{\frac{1}{3}} \geq r_L^{\frac{1}{3}}$ as required.

2. case: If $m = 2^n$ where $n \geq 4$ and there exists a $\mu : L \to PSp(2n, 2)$ irreducible representation. We know that $PSp(2n, 2)$ has a complex projective representation of degree 2^{2n} hence L also has such a representation, that is a projective representation of degree at most m^2. Therefore $r_L \leq r_H^2 \leq k_H^2$. It follows that $f(G) \geq f(H) \geq k_H^{\frac{1}{3}} \geq r_L^{\frac{1}{6}}$ as required.
By Proposition 3.3.1 in this case L is a simple group of Lie type simple of characteristic 2.
The proof is complete. □

Observe that we know that $f(A_n) \geq cn$ where c is an absolute constant. However the theorem above states only that if A_n is a composition factor of G then $f(G) \geq n^{\frac{1}{3}}$. We can obtain a better lower bound by using Theorem 3.3.1. It states that $f(G) \geq c\frac{\log|G|}{\log\log|G|}$ therefore if A_n is a composition factor of G then $f(G) \geq c\frac{\log|G|}{\log\log|G|} \geq c'\frac{\log|A_n|}{\log\log|A_n|} = r_{A_n}$ since $\frac{\log x}{\log\log x}$ is an increasing function if x is large enough.
Furthermore since there exist only finitely many sporadic groups then there exists a constant c such that $f(G) \geq c\frac{\log|G|}{\log\log|G|}$ for all sporadic groups G. Therefore we can omit these cases from Proposition 3.3.2. Now we obtain our main result of this section:

Theorem 3.3.4. *Suppose that $G_1, G_2, \ldots G_s$ are the Lie type composition factors of G. Then:*

$$f(G) \geq \max\left(c\frac{\log|G|}{\log\log|G|}; r_{G_i}^{l_i}\right)$$

where $l_i = \frac{1}{3}$ if G_i is a Lie type composition factor in characteristic not 2 and $l_i = \frac{1}{6}$ otherwise.

To complete this section let us list the minimal degrees of non-trivial projective representations of simple groups of Lie type ([LS]):

G	r_G	conditions
$PSL(2,q)$	$\frac{q-1}{(2,q-1)}$	
$PSL(n,q)$	$q^{n-1}-1$	$n>2$
$PSp(2n,q)$	$\frac{q^n-1}{2}$	$2 \not\mid n$
$PSp(2n,q)$	$\frac{1}{2}q^{n-1}\left(q^{n-1}-1\right)(q-1)$	$2\mid n$
$PSU(n,q)$	$\frac{q^n-q}{q+1}$	$2 \not\mid n$
$PSU(n,q)$	$\frac{q^n-1}{q+1}$	$2\mid n$
$PS\Omega^+(2n,q)$	$\left(q^{n-1}-1\right)\left(q^{n-2}+1\right)$	$q\neq 2,3,5$
$PS\Omega^+(2n,q)$	$q^{n-2}\left(q^{n-1}-1\right)$	$q=2,3,5$
$PS\Omega^-(2n,q)$	$\left(q^{n-1}+1\right)\left(q^{n-2}-1\right)$	
$\Omega(2n+1,q)$	$q^{2n-2}-1$	$q>5$
$\Omega(2n+1,q)$	$q^{n-1}\left(q^{n-1}-1\right)$	$q=3,5$
$E_6(q)$	$q^9\left(q^2-1\right)$	
$E_7(q)$	$q^{15}\left(q^2-1\right)$	
$E_8(q)$	$q^{27}\left(q^2-1\right)$	
$F_4(q)$	$q^4\left(q^6-1\right)$	$2 \not\mid q$
$F_4(q)$	$\frac{q^7\left(q^3-1\right)(q-1)}{2}$	$2\mid q$
${}^2E_6(q)$	$q^8\left(q^4+1\right)\left(q^3-1\right)$	
$G_2(q)$	$q\left(q^2-1\right)$	
${}^3D_4(q)$	$q^3\left(q^2-1\right)$	
${}^2F_4(q)$	$q^4(q-1)\sqrt{\frac{q}{2}}$	
${}^2B_2(q)$	$(q-1)\sqrt{\frac{q}{2}}$	
${}^2G_2(q)$	$q(q-1)$	

These bounds hold with only finitely many exceptions.

3.4 Upper bound

After the result in the Lower bound section we give an upper bound which is not much greater than the lower bound. We found that the lower bound depends on the composition factors, we would like an upper bound also depending on the composition factors. First let us consider only one composition factor, suppose that the group G is simple. From Proposition 3.2.1 we have an upper bound for $f(G)$ in terms of the permutation degree. Let us denote the minimal degree of a faithful permutation representation of G by p_G. We need a theorem which gives us a relation between the

permutation degree and the minimal degree of a non-trivial projective representation. Proposition 2.2 from [NP] shows us this relation:

Theorem 3.4.1. *There is an absolute constant $c_0 < 10^{10}$ such that if L is a non-abelian finite simple group then $p_{Aut(L)} \leq c_0 r_L^2$.*

Since $L \cong InnL \leq AutL$ if L is a non-abelian simple group we obtain the following:

Corollary 3.4.1. *There is an absolute constant $c_0 < 10^{10}$ such that if L is a non-abelian finite simple group then $p_L \leq c_0 r_L^2$.*

From this corollary and from Proposition 3.2.1 we can obtain an upper bound for the number of colors in a non-abelian simple group:

Proposition 3.4.1. *Let G be a non-abelian simple group. Then $f(G) \leq p_G \log|G| \leq c_0 r_G^2 \log|G|$.*

Observe that we have a sharper upper bound for the alternating group: $f(A_n) \leq \frac{n^2}{2}$. Taking into consideration this remark we will find an upper bound for an arbitrary group G in terms of its structure. In the proof we apply the following analitical lemma:

Lemma 3.4.1. $\frac{\log x}{\log^2 \log x} + \frac{\log y}{\log^2 \log y} \leq \frac{\log(xy)}{\log^2 \log(xy)}$ *if* $x, y \geq 6$.

From these results we obtain:

Theorem 3.4.2. *Suppose that $G_1, G_2, \ldots G_s$ are Lie type simple composition factors of G. Then:*

$$f(G) \leq \sum_{j=1}^{s} p_{G_i} \log|G| + c\frac{\log^2|G|}{\log^2 \log|G|} \leq \log^2|G| \left(\max_{i=1,\ldots s} p_{G_i} + \frac{c}{\log^2 \log|G|} \right).$$

Proof. If G_i is abelian group or a sporadic group then applying Theorem 1.2.2 or using that there exist only finitely many sporadic groups we obtain that $f(G_i) \leq c \log|G_i| \leq c' \frac{\log^2|G_i|}{\log^2 \log|G_i|}$. If G_i is the alternating group then we know that $f(A_n) \leq \frac{n^2}{2} \leq \frac{\log^2|A_n|}{2 \log^2 \log|A_n|}$. By induction and from Lemma 3.2.3 we obtain that if $G_1, G_2, \ldots, G_s$ are the composition factors of G then $f(G) \leq \sum_{j=1}^{s} f(G_i)$. From these estimates above and from Proposition 3.4.1 and by using the lemma above we obtain the desired statement. □

Now our main goal is to obtain a sharper upper bound for Lie type simple groups. We use the method of proving Theorem 3.2 from [Ke2]. During the calculations we will also apply two well-known analitical lemmas:

Lemma 3.4.2. *Suppose that* $0 \leq x \leq \frac{2}{3}$. *Then there exists a constant* c *such that* $1 - x \geq e^{-cx}$.

Lemma 3.4.3. *Suppose that* $0 \leq x \leq q < 1$. *Then there exist a constant only depending on* q *(*c_q*) such that* $\log(1 - x) \geq -c_q x$.

After these preparations let us begin to achieve our goal. Let G be a permutation group on $\{1, 2, \ldots, m\}$ and assume that for every $g \neq 1$ the number of fixpoints of g is at most s. We want to find an upper bound for $f(G)$.

Let S be a subset of $\{1, 2, \ldots m\}$. Consider a set of elements of G with the following properties: 1) they take 1 into S and 2) they take every element s of S outside of S. Then these elements form a product-free set, because if we look at the product $g_1 g_2$ then g_1 takes 1 into S but g_2 takes it out.

Now consider a set X of elements g of G such that 1 is not a fixpoint of them. We intend to find a subset S of $\{1, 2, \ldots m\}$ for which there are a lot of elements in X with the property above. Now fix k and we consider a subsets S of size k. Let us denote the number of possible subsets of $\{1, 2, \ldots m\}$ with cardinality k for $g \in X$ by $h_1(g)$ and the number of possible elements of X for $T \subseteq \{1, 2, \ldots m\}$ by $h_2(T)$ ($|T| = k$). We want to maximize $h_2(T)$. First we estimate $h_1(g)$:

Lemma 3.4.4. $h_1(g) \geq \frac{(m-s-3)(m-s-6)\ldots(m-s-3k+3)}{(k-1)!}$ *for all* $g \in X$ *where* $m-s-3k+3 > 0$.

Proof. Calculate the number of possible T's. First, the image of 1 is in T, let it be t. But the image of t is not in T. Now we want to choose another element of T. We have at least $m - s - 3$ possibilities, we we can choose any element apart from the fixpoints, 1, t and the image of t. Neither the inverse of the chosen element nor the image of it can be in T. This is the only restriction for choosing a third element. Therefore we can choose the next element from at least $m - s - 6$ points. Again neither the inverse of it nor the image of it can be in T. I repeat this method till I choose all the k elements. Finally we have at least $m - s - 3k + 3$ possibilities for the last one.

I could choose the chosen $k - 1$ points in any order, so the number of such subsets is at most $\frac{(m-s-3)(m-s-6)\ldots(m-s-3k+3)}{(k-1)!}$. □

From this lemma we obtain a lower bound for the maximum of $h_2(T)$:

Lemma 3.4.5. *Assume that the following holds:*

1. $3s + 8k - 8 \leq 2m$,

2. $s(k-1) \leq m-k+1$,

3. $k^2 \leq m+1$.

Then $\max_{|T|=k} h_2(T) \geq \frac{k}{m} e^{-2c} |X|$ *where* c *is an absolute constant.*

Proof. First we can see that the condition of Lemma 3.4.4 $m-s-3k+3 > 0$ automatically holds from condition 1 of the lemma: $2(s+3k-3) = 2s+6k-6 < 3s+8k-8 \leq 2m$. Now observe that $\sum_{|T|=k} h_2(T) = \sum_{g \in X} h_1(g)$ because we calculate each (T, g) pair once where g corresponds to T. Therefore:

$$\max_{|T|=k} h_2(T) \cdot \binom{m}{k} \geq \sum_{|T|=k} h_2(T) = \sum_{g \in X} h_1(g) \geq \min_{g \in X} h_1(g) \cdot |X| \geq$$

$$\geq \frac{(m-s-3)(m-s-6)...(m-s-3k+3)}{(k-1)!} \cdot |X| .$$

Hence:

$$\max_{|T|=k} h_2(T) \geq \frac{(m-s-3)(m-s-6)...(m-s-3k+3)}{(k-1)!} \cdot \frac{|X|}{\binom{m}{k}}.$$

Transforming the expression we obtain:

$$|X| \cdot \frac{k}{m} \cdot \frac{m-s-3}{m-1} \cdot \frac{m-s-6}{m-2} \cdot \ldots \cdot \frac{m-s-3k+3}{m-k+1}.$$

Look at the fractions

$$\frac{m-s-3j}{m-j} = 1 - \frac{s+2j}{m-j}.$$

Now we will want to apply Lemma 3.4.2. We need that $\frac{s+2j}{m-j} \leq \frac{2}{3}$ for all j between 1 and k. Rearranging the expression we obtain $3s+8j \leq 2m$, so we need that $3s+8k-8 \leq 2m$. Assume that this holds, then the expression can be estimated in the following way:

$$\max_{|T|=k} h_2(T) \geq |X| \cdot \frac{k}{m} e^{-c(\frac{s+2}{m-1} + \frac{s+4}{m-2} + \ldots + \frac{s+2k-2}{m-k+1})}.$$

Furthermore:

$$\max_{|T|=k} h_2(T) \geq |X| \cdot \frac{k}{m} e^{-c(\frac{s+2}{m-k+1} + \frac{s+4}{m-k+1} + \ldots + \frac{s+2k-2}{m-k+1})} \geq |X| \cdot \frac{k}{m} e^{-c(\frac{s(k-1)+k(k-1)}{m-k+1})}.$$

If $s(k-1) \leq m-k+1$ and $k(k-1) \leq m-k+1$ then $\max_{|T|=k} h_2(T) \geq \frac{k}{m} e^{-2c} |X|$. $\square$

Now we can apply this lemma to color G:

Lemma 3.4.6. *Let G be a permutation group on $1, 2, \ldots, m$, and suppose that every non-identical element has at most s fixpoints. If the following holds:*

1. $3s + 8k - 8 \leq 2m$,
2. $s(k-1) \leq m - k + 1$,
3. $k^2 \leq m + 1$,

then we can color $X = \{g \in G : 1^g \neq 1\}$ with $1 + c_2 \frac{m}{k} \log |X|$ colors, where c_2 is an absolute constant. Furthermore $f(G) \leq (s+1)(1 + c_2 \frac{m}{k} \log |G|)$.

Proof. First we prove the first statement of the Lemma. From the previous lemma we know that there exists a product-free subset in X with cardinality at least $\frac{k}{m} e^{-2c} |X|$. Now let X_1 be the set of remaining group elements of X, we obtain that $|X_1| \leq |X| \left(1 - \frac{k}{m} e^{-2c}\right)$. We use again this method, with this fixed k then the inequalities hold, because m and k is fixed and s cannot be greater. So again we find a large product-free subset in X_1 with density at least $\frac{k}{m} e^{-2c}$. Let X_2 be the set of remaining elements. We obtain that $|X_2| \leq |X_1| \left(1 - \frac{k}{m} e^{-2c}\right) \leq |X| \left(1 - \frac{k}{m} e^{-2c}\right)^2$. Now we continue this algorithm until we color all the elements of X. Using Lemma 3.4.3 we see that the number of sets is:

$$1 + \log_{\left(1 - \frac{k}{m} e^{-2c}\right)^{-1}} |X| = 1 + \frac{\log |X|}{\log \left(1 - \frac{k}{m} e^{-2c}\right)^{-1}} \leq 1 + c_2 \frac{m}{k} \log |X| .$$

Note that the condition of the lemma holds because $\frac{k}{m} e^{-2c} \leq e^{-2c} < 1$. So the proof of the first statement is complete.

Now let us prove the second one. We can color $X^{(1)} = \{g \in G : 1^g \neq 1\}$ with $1 + c_2 \frac{m}{k} \log \left|X^{(1)}\right| \leq 1 + c_2 \frac{m}{k} \log |G|$ colors. Then 1 is a fixpoint of the un-colored elements of G. Similarly we color $X^{(2)} = \left\{g \in G \setminus X^{(1)} : 2^g \neq 2\right\}$ with $1 + c_2 \frac{m}{k} \log |G|$ colors. Thus the remaining elements have at least two fixpoints: 1 and 2. Then we define $X^{(3)} = \left\{g \in G \setminus (X^{(1)} \cup X^{(2)}) : 3^g \neq 3\right\}$ and again we color this set.

We use this method until $X^{(j)}$ is empty for all remaining $1 \leq j \leq m$. We can easily see that $X^{(1)}, X^{(2)}, \ldots, X^{(s+1)}$ cover all the elements of $G \setminus \{1\}$ because all element have at most s fixpoints. Therefore $f(G) \leq (s+1)(1 + c_2 \frac{m}{k} \log |G|)$. □

Remark 3.4.1. *Suppose that G acts on a linear vectorspace or on a projective vectorspace. Then we can see that if $b_1, \ldots b_n$ is a basis then $X^{(b_1)}, \ldots X^{(b_n)}$ cover $G \setminus \{1\}$.*

Here $s = \mathrm{O}(1)$ is the best case. We have the following:

Corollary 3.4.2. *If* $s = O\left(m^{\frac{1}{2}}\right)$ *then* $f(G) \leq O\left(sm^{\frac{1}{2}}\right)\log|G|$.

Proof. We can see that all the condition holds in Lemma 3.4.6 for sufficiently large m if $k = \left\lfloor cm^{\frac{1}{2}} \right\rfloor$, where $c \leq \max\left(1, \sup \frac{s}{2m^{\frac{1}{2}}}\right)$. Therefore we can apply it and we obtain that $f(G) \leq O\left(sm^{\frac{1}{2}}\right)\log|G|$. □

Remark 3.4.2. *This result improves Proposition 3.2.1 if* $s = o\left(m^{\frac{1}{2}}\right)$. *In particular if* $s = O(1)$ *then we have* $f(G) \leq O\left(m^{\frac{1}{2}}\right)\log|G|$.
Furthermore if we apply this corollary to the regular representation of G *we obtain that* $f(G) \leq |G|^{\frac{1}{2}}\log|G|$.

The sharpest estimate we can obtain from Corollary 3.4.2 is the following:

Proposition 3.4.2. $f(PSL(2,q))) \leq O(k_{PSL(2,q)}^{\frac{1}{2}}\log|PSL(2,q)|)$.

Proof. $PSL(2,q)$ acts on $m = q+1$ points with at most 2 fixpoints. Therefore from Corollary 3.4.2 we obtain that:

$$f(PSL(2,q)) \leq \mathrm{O}\left(q^{\frac{1}{2}}\log|PSL(2,q)|\right) = \mathrm{O}(k_{PSL(2,q)}^{\frac{1}{2}}\log|PSL(2,q)|).$$

□

Moreover we can obtain an upper bound for the other classical simple groups. In these cases G acts on a projective space with $\mathrm{O}(q^l)$ points for a positive integer l and every non-identical element has at most $\mathrm{O}(q^f)$ fixpoints for a positive integer $f < l$. In this case if $2f \geq l$ then we can choose k in Lemma 3.4.6 to be $O(q^{l-f})$. Therefore we can color X with only $\mathrm{O}\left(q^f\log|G|\right)$ colors. In Lemma 3.4.6 we covered G with $s+1$ sets to color G in this case we can color G with only l sets, namely with a set corresponding to an arbitrary basis. Therefore we obtain that in this case $f(G) \leq \mathrm{O}\left(lq^f\log|G|\right)$.

3.5 Summary and open problems

From the results in Lower bound and Upper bound sections we obtain our main result:

Theorem 3.5.1. *Let* $G_1, G_2, \ldots, G_s$ *be the Lie-type composition factors of* G. *Then:*

$$A = \max\left(c_1\frac{\log|G|}{\log\log|G|}; r(G_i)^{l_i}\right) \leq f(G) \leq \log^2|G|\left(\max_{i=1,\ldots s} p_{G_i} + \frac{c_2}{\log^2\log|G|}\right) = c_3A^{14}$$

where c_1, c_2 *and* c_3 *are absolute constants.*

Proof. We have to prove only that the upper bound is a power of the lower bound. From the definition of r_{G_i} and p_{G_i} and from Theorem 3.4.1 we obtain that $r_{G_i}^{l_i} \geq c_4 p_{G_i}^{\frac{1}{12}}$ which implies the statement. □

Naturally we can pose questions about how we can sharpen these lower and upper bounds. In Corollary 3.4.2 we saw that the upper bound depends on $\mathrm{fix}(G)$. If we can color elements of G that have many fixpoints with few colors then we can obtain a better upper bound.

Problem 1. *Is it true that we can color* $Y = \{g \in G \setminus \{1\} : fix(g) = fix(G)\}$ *with* $\log|G|$ *colors where* G *is a classical simple group?*

We saw at the end of the Upper bound section that there exist infinitely many simple groups such that $f(G) \leq ck_G^{\frac{1}{2}} \log|G|$ where c is an absolute constant.

Problem 2. *Is it true that* $f(G) \geq ck_G^{\frac{1}{2}}$ *for any finite simple group* G*?*

Furthermore we also saw a large gap between the lower and upper bounds of A_n.

Problem 3. *Is it true that* $f(A_n) \leq cn \log n$ *where* c *is an absolute constant?*

Or can we find a better lower bound for A_n? Posing this question to arbitrary groups:

Problem 4. *Can we sharpen Theorem 3.3.1? Is it true that* $f(G) \geq O(\log|G|)$*?*

Acknowledgement

I would like to thank Laszlo Pyber for his assistance, patience and guidance in the preparation of my thesis.

References

[AEKL] Zvi Arad, Gideon Ehrlich, Otto H. Kegel and John C. Lennox: An application of Ramsey's theory to partitions in groups - I, Rendiconti del Seminario Matematico della Università di Padova 84 143-157 (1990)

[AH] H.L. Abbott and D. Hanson: A problem of Schur and its generalizations, Acta Arithmetica 20 175-187 (1972)

[AK] Noga Alon and Daniel J. Kleitman: Sum-free sets, A Tribute to Paul Erdős 13-26 (1990)

[Bou] Jean Bourgain: Estimates related to sumfree subsets of sets of integers, Israel Journal of Mathematics 97 (1) 71-92 (1997)

[BS] László Babai and Vera T. Sós: Sidon sets in groups and induced subgraphs of Cayley graphs, European Journal of Combinatorics 6, 101-114 (1985)

[Erd] Paul Erdős: Extremal problems in number theory, Proceedings of the Symposium on Pure Mathematics 8 181-189 (1965)

[FT] Walter Feit and Jacques Tits: Projective representations of minimal degree of group extensions, Canadian Journal of Mathematics Vol.XXX No.5 1092-1102 (1978)

[Gow] Tim Gowers: Quasirandom groups, Combinatorics, Probability and Computing 17 363-387 (2008)

[GR] Ben Green and Imre Z. Ruzsa: Sum-free sets in abelian groups, Israel Journal of Mathematics (2005)

[Ke1] Kiran S. Kedlaya: Product-free subsets of groups, The American Mathematical Monthly 105 (10) 819-824 (Dec., 1998)

[Ke2] Kiran S. Kedlaya: Product-free subsets of groups, then and now, Communicating Mathematics, Contemporary Math. 479 168-178 (2009)

[Ke3] Kiran S. Kedlaya and Xuancheng Shao: Generalizations of product-free subsets,Communicating Mathematics, Contemporary Math. 479 179-188 (2009)

[LS] Vicente Landazuri and Gary M. Seitz: On the minimal degrees of projective representations of the finite Chevalley groups, Journal of Algebra 32 418-443 (1974)

[NP] Nikolai Nikolov and László Pyber: Product decompositions of quasirandom groups and a Jordan type theorem (preprint)

[Özg] Cengiz Altay Özgener: Sum-free sets and sequences, Thesis M.Sc. - Simon Fraser University (1988)

[RS] A.H. Rhemtulla and Anne Penfold Street: Maximal sum-free sets in elementary abelian p-groups, Canadian Mathematical Bulletin 14 73-86 (1971)

[Sch] Issai Schur: Über die Kongruenz $x^m + y^m = z^m \pmod{p}$, Jahresbericht der Deutschen Mathematiker Vereinigunk 25 114-117 (1916)