VILNIUS UNIVERSITY

GRAŽVYDAS ŠEMETULSKIS

# Variations on the problems of Erdős-Turán and Littlewood-Offord

Doctoral dissertation

Physical sciences, mathematics (01P)

Vilnius, 2018

Doctoral dissertation was written in 2013–2018 at Vilnius University

**Scientific supervisor:**

prof. habil. dr. Artūras Dubickas
Vilnius University, Physical sciences, Mathematics – 01P

**Scientific adviser:**

prof. dr. Paulius Drungilas
Vilnius University, Physical sciences, Mathematics – 01P

VILNIAUS UNIVERSITETAS

GRAŽVYDAS ŠEMETULSKIS

# Erdős-Turán ir Littlewood-Offord problemų variacijos

Daktaro disertacija

Fiziniai mokslai, matematika (01P)

Vilnius, 2018

Disertacija rengta 2013–2018 metais Vilniaus universitete.

**Mokslinis vadovas:**

prof. habil. dr. Artūras Dubickas
Vilniaus universitetas, fiziniai mokslai, matematika – 01P

**Mokslinis konsultantas:**

prof. dr. Paulius Drungilas
Vilniaus universitetas, fiziniai mokslai, matematika – 01P

# Contents

# Notation

| | |
|---|---|
| $\mathbb{N}$ | the set of positive integers |
| $\mathbb{Z}$ | the set of integers |
| $\mathbb{R}$ | the set of real numbers |
| $\mathbb{C}$ | the set of complex numbers |
| $\mathbb{Z}_m$ | the ring of residue classes modulo $m$, $\mathbb{Z}/m\mathbb{Z}$ |
| $\mathbb{R}^n$ | Cartesian product of $n$ copies of $\mathbb{R}$ |
| $C^1(\mathbb{R}^k, \mathbb{R}^m)$ | the set of all continuously differentiable functions from $\mathbb{R}^k$ to $\mathbb{R}^m$ |
| $GL_d(K)$ | the group of $d \times d$ invertible matrices with entries from a field $K$ and matrix multiplication as the group operation |
| $GL_d(p)$ | the same as $GL_d(\mathbb{F}_p)$ |
| $C^1(\mathbb{R}^k)$ | the same as $C^1(\mathbb{R}^k, \mathbb{R})$ |
| $\lfloor x \rfloor$, $[x]$ | the largest integer not larger than $x$ (floor) |
| $\lceil x \rceil$ | the smallest integer not smaller than $x$ (ceiling) |
| $\lvert g \rvert$ | the order of an element $g$ in the underlying group |
| $\lvert A \rvert$ | the number of elements in the set $A$ |
| $f \ll g$ | the same as $f = O(g)$ |
| $f \sim g$ | the same as $f = (1 + o(1))g$ |
| $Ag$ | the set $\{ag, a \in A\}$ |

# 1 Introduction

The thesis consists of two parts. In the first part we are interested in a polynomial version of the Erdős-Turán conjecture. In the second part we will study the Littlewood-Offord problem. Let us concisely introduce these parts and the main notions related to the topics therein.

## Polynomial version of the Erdős-Turán conjecture

We consider polynomials

$$P(z) = a_n z^d + \cdots + a_1 z + a_0$$

in one variable $z$ with real coefficients. Polynomials with all coefficients in $\{0, 1\}$ are called *Newman* polynomials. The research will be focused on an open question that can be stated as follows:

*Question.* Is it true that there is an absolute constant $C$ such that, for each positive integer $d \geqslant 1$, the square of some Newman polynomial of degree $d$ has all of its coefficients in $[1, C]$?

This question was asked by Dubickas in 2008 and is motivated by the famous Erdős-Turán conjecture. We will give details on the conjecture in Chapter 2.1.

## Littlewood-Offord problem

Let $V_n = \{v_1, \ldots, v_n\}$ be a multiset in $\mathbb{R}$. Consider a random walk

$$S_n = X_1 + \cdots + X_n,$$

where $X_1, \ldots, X_n$ are independent random variables each uniformly distributed on a two point set $\{-v_i, v_i\}$, i.e., $\mathbb{P}(X_i = v_i) = \mathbb{P}(X_i = -v_i) = 1/2$. The *concentration probability* $\rho(V_n)$ of this random walk is defined to be the quantity

$$\rho(V_n) = \sup_{v \in \mathbb{R}} \mathbb{P}(S_n = v).$$

The concentration probability is a central notion in probability theory and has been studied extensively. The problem of bounding the concentration probability subject to various hypotheses on $v_1, \ldots, v_n$ is often referred to as the Littlewood-Offord problem. Our object of interest will be the concentration probability of a random walk in more general domain when $V_n$ is a multiset in an arbitrary group $G$ that is not necessarily abelian.

## 1.1 Problems and results

We give a short summary of the problems and results considered in this work.

In Chapter 3 we search for the smallest positive number $\kappa(d)$ for which there exists a polynomial $p(z)$ of degree $d$ with nonnegative real coefficients such that the coefficients of the square $p(z)^2$ all lie in the interval $[1, \kappa(d)]$. Under additional assumption of $p(z)$ being a *reciprocal* polynomial (i.e. satisfying $p(z) = z^d p(1/z)$) we prove that if the coefficients of $p(z)^2$ are all at least 1 then the largest coefficient of $p(z)^2$ must be at least $\kappa_{\mathrm{rec}}(d)$ where $\kappa_{\mathrm{rec}}(d) \sim \frac{2}{\pi} \log d$. We show that $\kappa(d) = \kappa_{rec}(d)$ for all $d = 1, \ldots, 7$. For each $d \geqslant 1$, both the number $\kappa_{\mathrm{rec}}(d)$ and the extremal polynomial will be given explicitly in terms of a sum involving central binomial coefficients.

In Chapter 4 we investigate a version of the Littlewood-Offord problem in an arbitrary group $G = (G, *)$. To be more precise, let $V_n = \{g_1, \ldots, g_n\}$ be a multiset of elements in $G$, each of which has order at least $m \geqslant 2$. We give an optimal upper bound for the concentration probability $\rho(V_n) = \sup_{g \in G} \mathbb{P}(X_1 * \cdots * X_n = g)$ by showing that a random walk in a group cannot concentrate to a greater extent than the simple random walk on a certain cyclic subgroup. We also establish an analogous result for a random walk $X_1 * \cdots * X_n$ in groups with elements having odd or infinite order and without the requirement for independent random variables to be two-valued. Both our results are optimal. The results strengthen and generalize some very recent results by Tiep and Vu and provide the following sharp inequalities

$$\rho(V_n) \leqslant \frac{2}{m} + \sqrt{\frac{2}{\pi}} \frac{1}{\sqrt{n}} \leqslant 3 \max\left\{\frac{1}{m}, \frac{1}{\sqrt{n}}\right\}.$$

## 1.2 Methods

Throughout the thesis we use a variety of methods which are quite common in number theory, combinatorics and probability theory.

The results in Chapter 3 are obtained by combining ideas from several sources: combinatorics, some geometric ideas based on convexity, several classical inequalities and the method of Lagrange multipliers. Determining the exact values $\kappa_{\mathrm{rec}}(d)$ and $\kappa(d)$ reduces to a quadratic variational problem. To obtain the exact values of the coefficients of the extremal polynomial we used the method of generating functions.

The proofs of the main results is Chapter 4 relies on a few ideas from convex optimization, graph theory, group theory and the use of a certain recursive relation that the worst-case random walk satisfies. To be more precise, in the proof of Theorem 4.5 we used an idea from convex optimization, namely that the maximum of a linear function is achieved on an extremal point of the parameter space (an extremal probability measure in our case). To obtain these extremal points we use Dirac's theorem from graph theory. The proofs of Theorems 4.1 and 4.5 relied on a certain recursive relation of the worst-case random walk. This idea comes from the work in [10], but in order to transfer the argument to the group theoretic setting we needed to prove an elementary result in group theory (Lemma 4.9). In order to establish an analytic form of the bound in Theorem 4.1 to compare it to result of Tiep and Vu in this context, we used a combinatorial identity on sums evenly spared binomial coefficients from [1] together with some standard techniques to bound integrals of powers of trigonometric functions from harmonic analysis. And finally, we used some basic facts about the mixing times of Markov chains to analyze the asymptotic behavior of the worst-case random walks in Theorem 4.1-4.5 from [25] and [5].

## 1.3 Actuality

Many connections have been found between Littlewood-Offord-type problems and various areas of mathematics. In particular, Littlewood-Offord-type inequalities were essential tools in some of the landmark results in random matrix theory

(see [35]). Most straightforwardly, the Littlewood-Offord inequality gives an upper bound on the probability that a particular row of a random sign matrix is orthogonal to a given vector, and can thus be used to bound the probability that a random matrix is singular.

## 1.4 Novelty and approbation

All results presented in this thesis are original. The main results are either published in or accepted at refereed journals. They were presented at the international conference *"27th Journées Arithmétiques"* (Vilnius, Lithuania, 2011) and at the Conference of Lithuanian Mathematical Society. Some of the results will be presented at *"12th International Vilnius Conference on Probability Theory and Mathematical Statistics"*. Results also were presented at the seminar of the Department of Probability Theory and Number Theory of the Faculty of Mathematics and Informatics of Vilnius University and Department of Theoretical Computer Science of the Institute of Computer Science of the Czech Academy of Sciences.

### Principal publications

The results of this thesis can be found in the following three papers, two of which are already published.

- Artūras Dubickas and Gražvydas Šemetulskis, *On polynomials with flat squares*, Acta Arith. **146** (2011), 247–255.

- Tomas Juškevičius and Gražvydas Šemetulskis, *Optimal Littlewood-Offord inequalities in groups*, Combinatorica, (accepted) (2018).

- Gražvydas Šemetulskis, *On polynomials of degree at most 7 with flat squares*, Šiauliai Math. Semin. **11** (2016), no. 19, 111–123.

## 1.5 Acknowledgments

I would like to express my sincere gratitude to my supervisor Prof. Artūras Dubickas for continuous support of my PhD studies and related research, and most importantly, for patience introducing me to professional mathematics.

I thank Eugenijus Manstavičius and Matas Šileikis for careful reading of the thesis, valuable remarks and corrections.

I am extremely grateful to my advisor Paulius Drungilas who always took care of me and often helped me with good advice.

I am highly indebted to Tomas Juškevičius, who exposed me to beautiful mathematics that brought me new joy in this field of science. The results of Chapter 4 were obtained together with him.

I am grateful to my faculty colleagues Hamletas Markšaitis, Ramūnas Garunkštis, Justas Kalpokas, Valentas Kurauskas, Jonas Šiurys, Jonas Jankauskas, Albertas Zinevičius, Romualdas Kašuba, Aivaras Novikas for creating a great academic atmosphere and to my fellow PhD students Vytautė Pilipauskaitė, Ieva Grublytė, Julius Damarackas for their constant support.

I would like to especially thank Paulius Šarka for all of his guidance and long hours he spent sharing his knowledge with me. He helped me immensely to develop as a mathematician and I am forever in his dept for that.

Special thanks to a friend Audrius Feigelovičius for introducing me to a certain kind of mathematics.

Finally, I wish to thank my family for their neverending care and support.

# 2 Literature overview

## 2.1 Erdős-Turán conjecture

The polynomial version of the Erdős-Turán conjecture was introduced by Dubickas [8] in 2008. This question is motivated by and is strongly related to an old and famous conjecture of Erdős and Turán.

Let $A$ be an infinite set of non-negative integers. By squaring the infinite series $f(z) := \sum_{i \in A} z^i$ with 0-1 coefficients, we obtain

$$f(z)^2 = \sum_{n=0}^{\infty} r_A(n) z^n,$$

where $r_A(n)$ is the number of representations of $n$ in the form $n = a_1 + a_2$ with $a_1, a_2 \in A$, namely

$$r_A(n) = |\{(a_1, a_2) \in A \times A : a_1 + a_2 = n\}|.$$

We call a set $A$ an *additive basis* of $\mathbb{N} \cup \{0\}$ if $r_A(n) \geqslant 1$ for all $n \geqslant 0$. A famous conjecture of Erdős and Turán [16] from 1941 asserts that for any such infinite set $A$ the coefficients $r_A(n)$ cannot all lie in the interval $[1, C]$ with some constant $C$. This deep USD 500 problem [14] remains wide open, although some progress has been made. Grekos, Haddad, Helou and Pihko [17] showed that the numbers $r_A(n)$, $n \geqslant 0$, cannot all lie in the interval $[1, 5]$. In 2006, Borwein, Choi and Chu [2], using an exhaustive computer search, improved 5 to 7. An interesting result was obtained by Sándor [30] who showed that the values $r_A(n)$, when $n$ runs through all sufficiently large integers, cannot all lie in an interval $[u, v]$, where $u > (\sqrt{v} - 1)^2$. Dirac [6] proved that the representation function $r_A(n)$ cannot be a constant for sufficiently large $n$.

It appears that proving that the numbers $r_A(n)$, $n \geqslant 0$, cannot all lie in the interval $[1, C]$ with $C > 7$ is a difficult problem. The opposite direction would be to construct an additive basis with small representation function values. In 1932 Sidon raised the question whether there exist an additive basis $A$ satisfying

$r_A(n) = o(n^\varepsilon)$ for every $\varepsilon > 0$. Erdős answered this question in [12] and showed that there exists an additive basis $A$ such that

$$r_A(n) \leqslant c_1 \log n.$$

Some years later he proved [13] that there exist an additive basis $A$ satisfying:

$$c_1 \log n \leqslant r_A(n) \leqslant c_2 \log n \tag{2.1}$$

and

$$|A \cap [1, n]| \sim c(n \log n)^{1/2}.$$

Moreover, he conjectured that if $A$ is an additive basis then

$$\limsup_{n\to\infty} \frac{r_A(n)}{\log n} > 0.$$

Recently, Dubickas [9] gave explicit values of $c_1$ and $c_2$ in (2.1). All of these proofs use the probabilistic method and establish only the existence of such bases. Kolountzakis [23] derandomized the probabilistic proof and gave an effective algorithm (polynomial time in terms of $n$) to find such an additive basis.

Ruzsa [29] proved that there is an additive basis $A$ of $\mathbb{N} \cup \{0\}$ whose representation function $r_A(n)$ has a bounded square mean, namely,

$$\frac{1}{n} \sum_{k=0}^{n-1} r_A(k)^2 \leqslant c_3$$

for each $n \geqslant 1$. Recently, Chen and Yang [4] (see also [33]) gave a different proof of this claim with the explicit value of $c_3 = 1.4 \cdot 10^7$. Moreover, they noted that following the same proof the constant can be improved to $c_3 = 2920$.

An interesting result was proved by Chen [3]. He showed that there exists an additive basis $A$ such that the set of values $k$ with $r_A(k) = 2$ has density one, i.e.,

$$\limsup_{n\to\infty} \frac{|\{k \in [1, n] : r_A(k) = 2\}|}{n} = 1.$$

Later, Tang [34] and Yang [38] established similar results assuming $r_A(n) = t$ for $t \geqslant 2$.

## 2.2 Littlewood-Offord inequalities

In 1943, while studying the number of real zeros of random polynomials, Littlewood and Offord [26] proved a bound for the probability that a sum of random

signs with non-zero weights hits a point which is asymptotically optimal up to a logarithmic factor. To be more precise, using harmonic analysis they proved that if all of the $v_i$'s are non-zero real numbers, then

$$\rho(V_n) = O(n^{-1/2} \log n).$$

Two years later, Erdős [11] , using Sperner's theorem from finite set combinatorics, showed that, actually,

$$\rho(V_n) \leqslant \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O(n^{-1/2}). \tag{2.2}$$

This bound is optimal as can be seen by taking $g_i = 1$ in $V_n$. In this case we have

$$\rho(V_n) = \mathbb{P}(X_1 + \cdots + X_n \in \{0, 1\}) = \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n}.$$

The results of Littlewood-Offord and Erdős started a long line of research. One of the main directions of the research is to generalize Erdős' result to other groups (instead of real numbers). First such results were obtained by Kleitman [21] and Katona [20]. Using an appropriate extension of Sperner's theorem, they proved that the bound for $\rho(V_n)$ as in (2.2) still holds for $v_i \in \mathbb{C}$. In fact, Kleitman [22] used an ingenious induction to show that instead of complex numbers we may even take vectors in an arbitrary normed space and the latter bound still holds. Griggs used a similar approach in [18] as in Erdős's seminal paper [11] to obtain the best possible result in $\mathbb{Z}_m$. In the latter work the natural assumption that $(v_i, m) = 1$ for all $v_i$'s was used.

Recently, Tiep and Vu [37] investigated the same question for certain matrix groups and obtained results that are sharp up to a constant factor. To be more precise, let $m, d, n \geqslant 2$ be integers and $G = GL_d(\mathbb{C})$. Let $V_n = \{g_1, \ldots, g_n\}$ be a multiset of elements in $G$, each of which has order at least $m$. In this case they have obtained the bound

$$\rho(V_n) \leqslant 141 \max\Big\{\frac{1}{m}, \frac{1}{\sqrt{n}}\Big\}.$$

Furthermore, they have also established an analogous bound for $G = GL_d(p)$. In Chapter 4 we shall extend the result of Tiep and Vu to an arbitrary group $G$ and provide an optimal inequality for $\rho(V_n)$.

Another interesting direction of research started with an observation that the bound can be improved significantly by making addition assumptions on the structure of set $V$. Erdős and Moser [15] showed that if the $v_i$'s all are distinct real numbers, then

$$\rho(V_n) = O(n^{-3/2} \log n).$$

They conjectured that the log term is not necessary and this was confirmed by Sárközy and Szemerédi [31]. The optimal result was obtained by Stanley [32] and later by Proctor [28]. Using algebraic methods they gave very explicit bound for the concentration probability and showed that

$$\rho(V_n) \leqslant \rho(\tilde{V}_n),$$

where $n$ is odd number and $\tilde{V}_n = \{-\frac{n-1}{2}, \ldots, \frac{n-1}{2}\}$.

A generalization of the latter result of Sárközy and Szemerédi [31] was obtained by Halász [19]. Using analytical methods (especially harmonic analysis) he proved that if $R_k$ is the number of solutions of the equation

$$\epsilon_{i_1} v_{i_1} + \cdots + \epsilon_{i_{2k}} v_{i_{2k}} = 0$$

where $\epsilon_i \in \{-1, 1\}$ and $i_1, \ldots, i_{2k}$ are (not necessarily different) elements of $\{1, \ldots, n\}$, then

$$\rho(V_n) = O(n^{-2k-\frac{1}{2}} R_k).$$

The latter bound is asymptotically sharp in all of the aforementioned cases.

In 2009 Tao and Vu [35] developed an inverse Littlewood-Offord theory. To be more precise, instead of trying to improve the bound further by imposing new assumptions on $V$, they tried to provide the complete picture by finding the underlying reason as to why the concentration probability is large (polynomial in $n$). The underlying principle is that if $\rho(V_n)$ is large then $V$ has a strong additive structure. Tao and Vu [35, 36] and Nguyen and Vu [27] showed that if the concentration probability is large then almost all of the $v_1, \ldots, v_n$ can be covered by few arithmetic progressions.

# 3 Polynomials with flat squares

## 3.1 Introduction

Recall that in the polynomial version of the Erdős-Turán problem we are interested in the question whether or not there exists an absolute positive number $C$ such that for each positive integer $d \geqslant 1$ there is a Newman polynomial (polynomial with coefficients 0, 1) $p(z)$ of degree $d$ with coefficients of $p(z)^2$ all lying in $[1, C]$. In attempt to answer this question we will consider a wider class of polynomials.

Let $\mathcal{P}_d$ be the set of real polynomials of degree $d$ having nonnegative coefficients, and let $\mathcal{R}_d$ be the subset of $\mathcal{P}_d$ consisting of *reciprocal* polynomials, i.e. polynomials $p(z)$ satisfying $p(z) = z^d p(1/z)$. Put $\kappa(d)$ for the smallest positive number for which exists a polynomial $p(z) \in \mathcal{P}_d$ such that all coefficients of the polynomial $p(z)^2$ lie in the interval $[1, \kappa(d)]$. Similarly, let $\kappa_{\text{rec}}(d)$ be the smallest positive number such that all coefficients of the its square $p(z)^2$ of a reciprocal polynomial $p(z) \in \mathcal{R}_d$ all lie in the interval $[1, \kappa_{\text{rec}}(d)]$. We clearly have $C \geqslant \sup_d\{\kappa(d)\}$ provided that such constant $C$ exists.

For a polynomial $p(z) = \sum_{j=0}^{d} a_j z^j \in \mathcal{P}_d$ let us denote the largest quotient between pairs of its coefficients by

$$q(p) = \max_{0 \leqslant i,j \leqslant d} \frac{a_i}{a_j}.$$

If a non-zero polynomial $p$ has at least one of its coefficients equal to zero we set $q(p) = +\infty$. Using this definition, the infimum $\inf q(p^2)$, where $p$ runs through polynomials with nonnegative coefficients of degree $d$, is equal to $\kappa(d)$, i.e.

$$\kappa(d) = \inf\{q(p^2) : p \in \mathcal{P}_d\}.$$

Similarly,

$$\kappa_{\text{rec}}(d) = \inf\{q(p^2) : p \in \mathcal{R}_d\}.$$

We will say that the polynomial $p$ is "flat" if quotient $q(p)$ is "small".

Dubickas suggested in [8] that the reciprocal polynomial

$$p_d(z) := y_0 + y_1 z + y_2 z^2 + \cdots + y_2 z^{d-2} + y_1 z^{d-1} + y_0 z^d, \tag{3.1}$$

could be a reasonable candidate to have the "flattest" square among all polynomials in $\mathcal{P}_d$. Here the coefficients $y_n$ were defined by the recurrence formula

$$2y_{2k}y_0 + 2y_{2k-1}y_1 + \cdots + 2y_{k+1}y_{k-1} + y_k^2 = 1 \tag{3.2}$$

for $n = 2k$, $k \geqslant 0$, and

$$2y_{2k+1}y_0 + 2y_{2k}y_1 + \cdots + 2y_{k+2}y_{k-1} + 2y_{k+1}y_k = 1 \tag{3.3}$$

for $n = 2k+1$, $k \geqslant 0$.

The following theorems suggest what the "flattest" polynomial in $\mathcal{P}_d$ could be.

**Theorem 3.1.** *We have $\kappa_{rec}(d) = q(p_d^2)$ for each $d \geqslant 1$.*

This shows that the polynomial (3.1) is optimal among all reciprocal polynomials in the sense that it has the "flattest" square. Note that Theorem 3.3 below ensures that this polynomial has positive coefficients.

**Theorem 3.2.** *We have $\kappa(d) = q(p_d^2)$ for each $d \in \{1, \ldots, 7\}$.*

This theorem suggests that the polynomial $p_d(z)$ indeed has the "flattest" square among all polynomials of degree $d$ with nonnegative real coefficients.

The sequence of rational numbers $y_n$ defined by (3.2) and (3.3), can be given explicitly in terms of the central binomial coefficients:

**Theorem 3.3.** *We have $y_n = 2^{-2n}\binom{2n}{n}$ for each $n \geqslant 0$.*

The next theorem shows that $q(p_d^2)$ is unbounded.

**Theorem 3.4.** *We have*

$$q(p_d^2) = 2(y_0^2 + y_1^2 + \cdots + y_{(d-1)/2}^2)$$

*for each odd positive integer $d$ and*

$$q(p_d^2) = 2(y_0^2 + y_1^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2$$

*for each even positive integer $d$. Here, $y_n = 2^{-2n}\binom{2n}{n}$ and $q(p_d^2) \sim \frac{2}{\pi}\log d$ as $d \to \infty$.*

Theorem 3.2 suggests that $\kappa(d) = \kappa_{\rm rec}(d)$ for all $d \geqslant 1$. This may seem slightly surprising because the situation when we consider Newman polynomials is different. Dubickas [9] proved that for reciprocal Newman polynomials $p$ of degree $d$ we have

$$q(p^2) \geqslant 2\sqrt{d} - 3.$$

On the other hand, in [9] using the probabilistic method it was proved that for each $\varepsilon > 0$ and $d > d_0(\varepsilon)$ there is a Newman polynomial $p$ of degree $d$ such that

$$q(p^2) \leqslant (1+\varepsilon)\frac{4}{\pi}(\log d)^2.$$

The remainder of the chapter is organized as follows. In the next section we prove Theorems 3.3 and 3.4. Then (in Section 3.3) we give several auxiliary lemmas which will be used in the proofs of Theorems 3.1 and 3.2. And finally the proofs of these two theorems are given in the Section 3.4.

## 3.2 Proof of Theorems 3.3 and 3.4

*Proof of Theorem 3.3.* Consider the function

$$g(z) := y_0 + y_1 z + y_2 z^2 + \dots.$$

From (3.2) and (3.3), we deduce that

$$g(z)^2 = 1 + z + z^2 + z^3 + \cdots = \frac{1}{1-z}.$$

On the other hand, let

$$g_2(z) := (1-z)^{-1/2} = \sum_{n=0}^{\infty} (-z)^n \binom{-1/2}{n}.$$

Note that

$$(-1)^n \binom{-1/2}{n} = \frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{2^n n!} = \frac{(2n)!}{2^{2n} n!^2} = 2^{-2n}\binom{2n}{n}.$$

Setting $t_n := 2^{-2n}\binom{2n}{n}$, we obtain

$$g_2(z) = t_0 + t_1 z + t_2 z^2 + \dots.$$

But $g_2(z)^2 = g(z)^2 = 1/(1-z)$, so the sequence $t_n$, $n = 0, 1, 2, \dots$, satisfies the same recurrence formulas (3.2), (3.3). Since each $y_n$ is uniquely determined by $y_0, \dots, y_{n-1}$ and $y_0 = t_0 = 1$, this implies $y_n = t_n = 2^{-2n}\binom{2n}{n}$ for each $n \geqslant 0$, as claimed. □

Similarly, for each integer $k \geqslant 2$, the $k$th power of the series

$$g_k(z) := \sum_{n=0}^{\infty} (-1)^n \binom{-1/k}{n} z^n = (1-z)^{-1/k}$$

with positive coefficients $(-1)^n \binom{-1/k}{n}$ is equal to the series

$$g_k(z)^k = 1/(1-z) = \sum_{n=0}^{\infty} z^n$$

with coefficients $1, 1, 1, \ldots$. This shows the Erdős-Turán problem for the $k$th power of the series with nonnegative real (instead of $0, 1$) coefficients has a trivial answer: such power can have all equal coefficients.

*Proof of Theorem 3.4.* Write

$$p_d(z)^2 = (y_0 + y_1 z + \cdots + y_1 z^{d-1} + y_0 z^d)^2 = s_0 + s_1 z + \cdots + s_d z^d + \cdots + s_0 z^{2d}.$$

By (3.2), (3.3), we have $s_0 = s_1 = \cdots = s_{[d/2]} = 1$. Set

$$y_i^* := y_{\min\{i,d-i\}} = \begin{cases} y_i \text{ for } 0 \leqslant i \leqslant [d/2], \\ y_{d-i} \text{ for } [d/2]+1 \leqslant i \leqslant d, \end{cases}$$

and $y_i^* = y_i := 0$ for $i \notin \mathbb{Z}$. Then $p_d(z) = \sum_{i=0}^{d} y_i^* z^i$, so

$$s_\ell = \sum_{i=0}^{\ell} y_i^* y_{\ell-i}^* = 2 \sum_{i=0}^{[\ell/2]} y_i^* y_{\ell-i}^* - (y_{\ell/2}^*)^2 \tag{3.4}$$

for each integer $\ell$ satisfying $0 \leqslant \ell \leqslant d$. Also, as $p_d(z)$ is reciprocal, $s_\ell = s_{2d-\ell}$ for $d+1 \leqslant \ell \leqslant 2d$. We claim that

$$1 < s_\ell < s_d \tag{3.5}$$

for each $\ell$ in the range $[d/2]+1 \leqslant \ell \leqslant d-1$.

Note that $y_i^* = y_i$ for $i \leqslant \ell/2 \leqslant [d/2]$. Similarly, $y_{\ell-i}^* = y_{d-\ell+i}$ for $i \leqslant \ell - [d/2] - 1$ and $y_{\ell-i}^* = y_{\ell-i}$ for $i \geqslant \ell - [d/2]$. Hence, by (3.4),

$$s_\ell = 2 \sum_{i=0}^{[\ell/2]} y_i y_{\ell-i}^* - y_{\ell/2}^2 = 2 \sum_{i=0}^{\ell-[d/2]-1} y_i y_{d-\ell+i} + 2 \sum_{i=\ell-[d/2]}^{[\ell/2]} y_i y_{\ell-i} - y_{\ell/2}^2. \tag{3.6}$$

Inserting $\ell = d$ into (3.4) we find that

$$s_d = 2 \sum_{i=0}^{[d/2]} y_i^2 - y_{d/2}^2 = 2 \sum_{i=0}^{d-[d/2]-1} y_i^2 + y_{d/2}^2. \tag{3.7}$$

By Theorem 3.3,

$$\frac{y_{s-1}}{y_s} = \frac{2^{2s}(s!)^2(2s-2)!}{2^{2s-2}(s-1)!^2(2s)!} = \frac{4s^2}{2s(2s-1)} = \frac{2s}{2s-1} > 1 \tag{3.8}$$

for each $s \in \mathbb{N}$. Thus $y_i > y_{d-\ell+i}$, because $i < d - \ell + i$. Similarly, $y_i \geqslant y_{\ell-i}$, because $i \leqslant \ell/2$. Thus, using

$$[\ell/2] \leqslant [(d-1)/2] = d - [d/2] - 1,$$

from (3.6) and (3.7) we obtain

$$s_d - y_{d/2}^2 = 2 \sum_{i=0}^{d-[d/2]-1} y_i^2 > 2 \sum_{i=0}^{\ell-[d/2]-1} y_i y_{d-\ell+i} + 2 \sum_{i=\ell-[d/2]}^{[\ell/2]} y_i y_{\ell-i} = s_\ell + y_{\ell/2}^2.$$

Hence $s_d > s_\ell + y_{d/2}^2 + y_{\ell/2}^2 \geqslant s_\ell$, giving the second inequality in (3.5).

The proof of the first inequality in (3.5) is simpler. Fix an integer $\ell$ in the range $[d/2] + 1 \leqslant \ell \leqslant d$. Observe that, by (3.2), (3.3), $\sum_{i=0}^{\ell} y_i y_{\ell-i} = 1$. By (3.8), we find that $y_i \leqslant y_i^* = y_{\min\{i,d-i\}}$ and $y_{\ell-i} \leqslant y_{\ell-i}^*$ for $i \leqslant \ell \leqslant d$. So $y_i y_{\ell-i} \leqslant y_i^* y_{\ell-i}^*$ for each $i = 0, 1, \ldots, \ell$. Moreover, at least one inequality is strict, because $\ell > [d/2]$. So (3.4) yields that

$$1 = \sum_{i=0}^{\ell} y_i y_{\ell-i} < \sum_{i=0}^{\ell} y_i^* y_{\ell-i}^* = s_\ell.$$

This completes the proof of (3.5).

Now, from (3.5) it follows that all $s_j$, where $j = 0, 1, \ldots, 2d$, belong to the interval $[s_0, s_d]$. Here $s_0 = 1$. It is easily seen that

$$s_d = 2(y_0^2 + y_1^2 + \cdots + y_{(d-1)/2}^2)$$

for odd positive integer $d$ and

$$s_d = 2(y_0^2 + y_1^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2$$

for even positive integer $d$. This proves the formulas for $q(p_d^2) = s_d$ as stated in the theorem.

We next find an asymptotic formula for $q(p_d^2)$. Fix $\varepsilon > 0$. By Theorem 3.3 and Stirling's formula,

$$y_n = \frac{(2n)!}{2^{2n} n!^2} \sim \frac{(2n/e)^{2n}\sqrt{2\pi \cdot 2n}}{2^{2n}(n/e)^{2n} 2\pi n} = \frac{1}{\sqrt{\pi n}}$$

as $n \to \infty$. So there is a positive integer $d_0(\varepsilon)$ such that

$$\frac{1-\varepsilon}{\pi n} < y_n^2 < \frac{1+\varepsilon}{\pi n} \tag{3.9}$$

for each $n \geqslant d_0(\varepsilon)$. Thus, in both cases (even and odd $d$), we have

$$|q(p_d^2) - 2\sum_{n=d_0(\varepsilon)}^{[d/2]} y_n^2| \leqslant 2d_0(\varepsilon) + 1. \tag{3.10}$$

Using $\sum_{n=d_0(\varepsilon)}^{[d/2]} \frac{1}{n} \sim \log d$ as $d \to \infty$ and (3.9), we deduce that the sum $\sum_{n=d_0(\varepsilon)}^{[d/2]} y_n^2$ belongs to the interval

$$\left[\frac{(1-\varepsilon)^2}{\pi}\log d, \frac{(1+\varepsilon)^2}{\pi}\log d\right]$$

for $d \geqslant d_1(\varepsilon)$. Thus, by (3.10),

$$\frac{2(1-\varepsilon)^3}{\pi}\log d < q(p_d)^2 < \frac{2(1+\varepsilon)^3}{\pi}\log d$$

for $d \geqslant d_2(\varepsilon)$. It follows that $q(p_d^2) \sim \frac{2}{\pi}\log d$ as $d \to \infty$. □

## 3.3 Auxiliary lemmas

**Lemma 3.5.** *Let $f \in C^1(\mathbb{R}^k)$, $g \in C^1(\mathbb{R}^k, \mathbb{R}^m)$, $m < k$, where $C^1$ is the space of continuously differentiable functions. Suppose $\mathbf{x}^*$ is a conditional extremum point with the condition $g(\mathbf{x}^*) = (g_1(\mathbf{x}^*), \ldots, g_m(\mathbf{x}^*)) = \mathbf{0}$ and the rank of $g'(\mathbf{x}^*)$ is equal to $m$. Then there exist unique real numbers $\lambda_1, \ldots, \lambda_m$, such that*

$$f'(\mathbf{x}^*) = \sum_{j=1}^{m} \lambda_j g_j'(\mathbf{x}^*).$$

The proof for this lemma can be found in any multivariable calculus book that includes the Lagrange multipliers method.

Let us introduce a notation which will be used in the rest of this chapter.

Let $V_n(L)$ be a subset of vectors $(x_0, \ldots, x_{n-1})$ in $\mathbb{R}^n$ determined by the inequalities

$$L \geqslant x_0, x_1, \ldots, x_{n-1} \geqslant 0,$$

$$h_0(\mathbf{x}) := x_0^2 \geqslant 1,$$

$$h_1(\mathbf{x}) := 2x_0x_1 \geqslant 1,$$

$$h_2(\mathbf{x}) := 2x_0x_2 + x_1^2 \geqslant 1,$$

$$h_3(\mathbf{x}) := 2x_0x_3 + 2x_1x_2 \geqslant 1,$$

$$\vdots$$

$$h_{n-1}(\mathbf{x}) := \sum_{i=0}^{n-1} x_i x_{n-1-i} = 2x_0x_{n-1} + 2x_1x_{n-2} + \ldots \geqslant 1.$$

We will denote by $V_n$ the case when $L$ equals infinity (i.e. when there are no restrictions $L \geqslant x_i$).

The following lemma will be the key result in the proof of the Theorem 3.1.

**Lemma 3.6.** *Let* $\mathbf{v} \in V_n$. *Then* $|\mathbf{v}|^2 \geqslant y_0^2 + \cdots + y_{n-1}^2$, *where equality holds if and only if* $\mathbf{v} = (y_0, \ldots, y_{n-1})$.

*Proof.* Suppose that $\mathbf{v} = (x_0, \ldots, x_{n-1}) \in V_n$. By Theorem 3.3, $y_n > 0$ for each $n \geqslant 0$. So, for every pair $i, j$ satisfying $0 \leqslant i < j \leqslant n-1$, we have

$$\frac{x_i^2 y_j}{y_i} + \frac{x_j^2 y_i}{y_j} \geqslant 2x_i x_j,$$

where equality holds if and only if $\frac{x_j}{y_j} = \frac{x_i}{y_i}$. Fix an integer $\ell$ in $[0, n-1]$. Replacing each double product $2x_ix_{\ell-i}$ in this way and leaving $x_{\ell/2}^2$ as it is (if $\ell$ is even), we obtain

$$1 \leqslant \sum_{i=0}^{\ell} x_i x_{\ell-i} = 2x_0x_\ell + 2x_1x_{\ell-1} + \ldots$$

$$\leqslant \frac{x_0^2 y_\ell}{y_0} + \frac{x_\ell^2 y_0}{y_\ell} + \frac{x_1^2 y_{\ell-1}}{y_1} + \frac{x_{\ell-1}^2 y_1}{y_{\ell-1}} + \cdots = \sum_{i=0}^{\ell} \frac{x_i^2 y_{\ell-i}}{y_i}.$$

Here, the second inequality becomes equality if and only if

$$(x_0, \ldots, x_\ell) = \lambda_\ell (y_0, \ldots, y_\ell)$$

with a scalar multiple $\lambda_\ell > 0$. For such a vector $(x_0, \ldots, x_\ell)$, the first inequality,

$$1 \leqslant \sum_{i=0}^{\ell} x_i x_{\ell-i} = \lambda_\ell^2 \sum_{i=0}^{\ell} y_i y_{\ell-i} = \lambda_\ell^2$$

(see (3.2), (3.3)), is equality if only if $\lambda_\ell = 1$. Hence

$$1 = \sum_{i=0}^{\ell} \frac{x_i^2 y_{\ell-i}}{y_i}$$

for $\ell = 0, 1, \ldots, n-1$ if and only if $\mathbf{v} = (x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1}) \in V_n$.

Let $\mu_0, \dots, \mu_{n-1}$ be some positive constants to be chosen later. Multiplying $\ell$th inequality

$$1 \leqslant \sum_{i=0}^{\ell} x_i x_{\ell-i}$$

by $\mu_\ell$ and adding them for $\ell = 0, 1, \dots, n-1$, we find that

$$\sum_{\ell=0}^{n-1} \mu_\ell \leqslant \sum_{\ell=0}^{n-1} \mu_\ell \sum_{i=0}^{\ell} x_i x_{\ell-i} \leqslant \sum_{\ell=0}^{n-1} \mu_\ell \sum_{i=0}^{\ell} \frac{x_i^2 y_{\ell-i}}{y_i} = \sum_{i=0}^{n-1} \frac{x_i^2}{y_i} \sum_{\ell=i}^{n-1} \mu_\ell y_{\ell-i}. \tag{3.11}$$

We next show that positive numbers $\mu_0, \dots, \mu_{n-1}$ can be chosen so that all coefficients $a_i := y_i^{-1} \sum_{\ell=i}^{n-1} \mu_\ell y_{\ell-i}$ for $x_i^2$ in the inequality (3.11), i.e.

$$\sum_{\ell=0}^{n-1} \mu_\ell \leqslant \sum_{i=0}^{n-1} a_i x_i^2,$$

are equal $a_{n-1} = \dots = a_0$, namely,

$$\frac{\mu_{n-1} y_0}{y_{n-1}} = \frac{\mu_{n-1} y_1}{y_{n-2}} + \frac{\mu_{n-2} y_0}{y_{n-2}} = \frac{\mu_{n-1} y_2}{y_{n-3}} + \frac{\mu_{n-2} y_1}{y_{n-3}} + \frac{\mu_{n-3} y_0}{y_{n-3}} = \dots$$

$$= \frac{\mu_{n-1} y_{n-1}}{y_0} + \dots + \frac{\mu_1 y_1}{y_0} + \mu_0.$$

Indeed, set $\mu_{n-1} := 1$ and then, step by step left to right, determine $\mu_{n-2}$, $\mu_{n-3}$, $\dots$, $\mu_0$. We claim that $\mu_{n-1}, \dots, \mu_0$ are all positive. For a contradiction assume that $\mu_{n-1} = 1 > 0, \dots, \mu_{n-i+1} > 0$, but $\mu_{n-i} \leqslant 0$ for some $i$ satisfying $2 \leqslant i \leqslant n$. Since

$$\frac{\mu_{n-i} y_0}{y_{n-i}} = \sum_{j=1}^{i-1} \mu_{n-j} \Big( \frac{y_{i-j-1}}{y_{n-i+1}} - \frac{y_{i-j}}{y_{n-i}} \Big)$$

and $\mu_{n-1}, \dots, \mu_{n-i+1} > 0$, this can happen only if some difference

$$\frac{y_{i-j-1}}{y_{n-i+1}} - \frac{y_{i-j}}{y_{n-i}}$$

is at most 0. Hence

$$y_{i-j-1} y_{n-i} \leqslant y_{n-i+1} y_{i-j}$$

for some $i, j$ satisfying $1 \leqslant j \leqslant i-1 \leqslant n-1$. However, by (3.8), $y_{i-j-1} > y_{i-j}$ and $y_{n-i} > y_{n-i+1}$, giving

$$y_{i-j-1} y_{n-i} > y_{n-i+1} y_{i-j},$$

a contradiction.

Now, since all $\mu_i$ are positive and all $a_i$, $i = 0, 1, \ldots, n-1$, are equal, we must have

$$\sum_{\ell=0}^{n-1} \mu_\ell \leqslant \sum_{i=0}^{n-1} a_i x_i^2 = a_{n-1} \sum_{i=0}^{n-1} x_i^2 = \frac{\mu_{n-1} y_0}{y_{n-1}} \sum_{i=0}^{n-1} x_i^2. \tag{3.12}$$

As we already observed, for $(x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1})$ (and only for this vector), we have equality in (3.11) and so in (3.12). Thus

$$\sum_{\ell=0}^{n-1} \mu_\ell = \frac{\mu_{n-1} y_0}{y_{n-1}} \sum_{i=0}^{n-1} y_i^2.$$

Hence, by (3.12), we find that

$$|\mathbf{v}|^2 = \sum_{i=0}^{n-1} x_i^2 \geqslant \frac{y_{n-1}}{\mu_{n-1} y_0} \sum_{\ell=0}^{n-1} \mu_\ell = \sum_{i=0}^{n-1} y_i^2.$$

This proves the lemma. □

**Lemma 3.7.** *Let* $\mathbf{x}$, $\mathbf{z} \in V_n(L)$ *and* $n \in \{1, 2, 3, 4\}$. *Then, for sufficiently large* $L$, *we have* $\mathbf{x}\mathbf{z}^t \geqslant y_0^2 + \cdots + y_{n-1}^2$, *where equality holds if and only if* $\mathbf{x} = \mathbf{z} = (y_0, \ldots, y_{n-1})$.

*Proof.* The case $n = 1$ is trivial. Let $2 \leqslant n \leqslant 4$. Consider the function

$$G(\mathbf{x}, \mathbf{z}) := 2\mathbf{x}\mathbf{z}^t = 2x_0 z_0 + 2x_1 z_1 + \cdots + 2x_{n-1} z_{n-1}.$$

It is not hard to see that $G$ is a continuous real-valued function of $2n$ variables. Since for all $L \geqslant 1$ the set $V_n(L)$ is a compact set in $\mathbb{R}^n$, the function $G$ attains its minimum at some vectors $\mathbf{x}, \mathbf{z} \in V_n(L)$. Denote this minimum by

$$G_m(n) := \inf_{\substack{\mathbf{x} \in V_n(L) \\ \mathbf{z} \in V_n(L)}} G(\mathbf{x}, \mathbf{z}).$$

Our main focus will be the investigation of the quantity $G_m(n)$. Clearly, we have $G_m(n) \leqslant 2(y_0^2 + \cdots + y_{n-1}^2)$, hence $G_m(n) < 2.97$ for $n \in \{1, 2, 3, 4\}$. Since $\frac{\partial}{\partial x_i} G(\mathbf{x}, \mathbf{z}) = 0$ and $\frac{\partial}{\partial z_i} G(\mathbf{x}, \mathbf{z}) = 0$ for $i = 0, \ldots, n-1$ leads to $\mathbf{x} = \mathbf{z} = (0, \ldots, 0)$, it follows that the function $G$ has no local minimum in the interior the set of $\mathbf{x}, \mathbf{z} \in V_n(L)$. Hence the minimum of $G$ is attained at some vectors on the boundary. To describe the location of the vector $\mathbf{x}$ on the boundary we define three type of sets:

$$S_0(\mathbf{x}) := \{i \in \{0, \ldots, n-1\} : x_i = 0\}, \tag{3.13a}$$

$$S_1(\mathbf{x}) := \{i \in \{0, \ldots, n-1\} : h_i(\mathbf{x}) = 1\}, \tag{3.13b}$$

$$S_L(\mathbf{x}) := \{i \in \{0, \ldots, n-1\} : x_i = L\}. \tag{3.13c}$$

Suppose $\mathbf{u} = (u_0, \ldots, u_{n-1})$, $\mathbf{v} = (v_0, \ldots, v_{n-1}) \in V_n(L)$ are the vectors at which the function $G$ attains its minimum value $G_m(n)$. Since $v_{n-1}$ is restricted only on $0 \leqslant v_{n-1} \leqslant L$ and $1 \leqslant h_{n-1}(\mathbf{v}) = 2v_{n-1}v_0 + 2v_{n-2}v_1 + \ldots$, we can assume that $n-1 \in S_0(\mathbf{v}) \cup S_1(\mathbf{v})$. By the same argument, $n-1 \in S_0(\mathbf{u}) \cup S_1(\mathbf{u})$. Notice that if $S_1(\mathbf{v}) = S_1(\mathbf{u}) = \{0, \ldots, n-1\}$, then $\mathbf{u} = \mathbf{v} = (y_0, \ldots, y_{n-1})$. We will consider this case trivial.

To find $G_m(n)$, we will check on what kind of boundary (described by the sets (3.13)) the function $G$ can attain the minimum. By examining all possible nontrivial cases, we will see that the function $G$ fails to achieve the minimum value. Hence, the minimum must be obtained when $S_1(\mathbf{v}) = S_1(\mathbf{u}) = \{0, \ldots, n-1\}$. We consider each case $n = 2, 3, 4$ separately.

*Case $n = 2$:*

If $\mathbf{u}$, $\mathbf{v} \in V_2(L)$, then $(\sqrt{u_0v_0}, \sqrt{v_1u_1}) \in V_2(L)$. Indeed, since $2u_0u_1 \geqslant 1$, $2v_0v_1 \geqslant 1$, $v_0^2 \geqslant 1$, $u_0^2 \geqslant 1$, $v_0 \geqslant 0$, $u_0 \geqslant 0$, we deduce that $\sqrt{u_0v_0} \geqslant 1$ and $2\sqrt{u_0v_0u_1v_1} \geqslant \min\{2u_0u_1, 2v_0v_1\} \geqslant 1$. But then $G_m(2)$ is equal to $2|\mathbf{w}|^2$ for some $\mathbf{w} \in V_2(L)$. Thus, by Lemma 3.6, we obtain that $G_m(2) \geqslant 2y_0^2 + 2y_1^2$ and inequality becomes equality if and only if $\mathbf{u} = \mathbf{v} = (y_0, y_1)$.

*Case $n = 3$:*

First we prove that $S_L(\mathbf{v}) = \emptyset$. Since $u_0 \geqslant 1$ and

$$G_m(3) = 2(u_0v_0 + u_1v_1 + u_2v_2) < 3,$$

we have $v_0 < 2$, so $0 \notin S_L(\mathbf{v})$ for $L > 3$. Also, $2 \notin S_L(\mathbf{v})$, as $2 \in S_1(\mathbf{v}) \cup S_0(\mathbf{v})$. If $1 \in S_L(\mathbf{v})$, then using $2u_1u_0 \geqslant 1$ we get

$$G_m(3) = 2(v_0u_0 + v_1u_1 + v_2u_2) \geqslant 2(u_0 + L\frac{1}{2u_0}) \geqslant \sqrt{2L},$$

which is a contradiction for $L > 9$, thus $S_L(\mathbf{v}) = \emptyset$. Also, by the same argument we have $S_L(\mathbf{u}) = \emptyset$. Next we show that $S_0(\mathbf{v}) = \emptyset$. Obviously $0, 1 \notin S_0(\mathbf{v})$. If $2 \in S_0(\mathbf{v})$, then from $h_2(\mathbf{v}) \geqslant 1$ and $v_2 = 0$ we get that $v_1 \geqslant 1$. This immediately gives a contradiction, since then

$$G_m(3) = 2(v_0u_0 + v_1u_1 + v_2u_2) \geqslant 2u_0 + \frac{1}{u_0} \geqslant 3.$$

Here, the last inequality comes from the fact that the function $2x + \frac{1}{x}$ is increasing when $x \geqslant 1$. So, $S_0(\mathbf{v}) = \emptyset$ and also, by the same argument, $S_0(\mathbf{u}) = \emptyset$. Thus $S_0(\mathbf{v}) = S_0(\mathbf{u}) = S_L(\mathbf{v}) = S_L(\mathbf{u}) = \emptyset$.

Next we will see that $G_m(3)$ cannot be obtained in the case when at least one of the sets $S_1(\mathbf{v}), S_1(\mathbf{u})$ is not equal to $\{0,1,2\}$ (nontrivial case).

If $G_m(3) = G(\mathbf{v},\mathbf{u})$ and at least one of the sets $S_1(\mathbf{v})$, $S_1(\mathbf{u})$ is not equal to $\{0,1,2\}$, then the pair $(\mathbf{x},\mathbf{z}) = (\mathbf{u},\mathbf{v})$ is a conditional extremum point of function $G(\mathbf{x},\mathbf{z})$, where the condition is

$$\begin{aligned} h_i(\mathbf{x}) &= 1 \qquad i \in S_1(\mathbf{u}), \\ h_j(\mathbf{z}) &= 1 \qquad j \in S_1(\mathbf{v}). \end{aligned}$$

Let $S_1(\mathbf{u}) = \{t_1,\dots,t_{s_1}\}$, $S_1(\mathbf{v}) = \{l_1,\dots,l_{s_2}\}$, where $t_1 < \cdots < t_{s_1} = 2$ and $l_1 < \cdots < l_{s_2} = 2$. Define a conditional function

$$g(\mathbf{x},\mathbf{z}) := (g_1(\mathbf{x}),\dots,g_{s_1}(\mathbf{x}), g_{s_1+1}(\mathbf{z}),\dots,g_{s_1+s_2}(\mathbf{z})), \tag{3.14}$$

where

$$\begin{aligned} g_i(\mathbf{x}) &:= h_{t_i}(\mathbf{x}) - 1 \qquad i = 1,\dots,s_1, \\ g_{s_1+j}(\mathbf{z}) &:= h_{l_j}(\mathbf{z}) - 1 \qquad j = 1,\dots,s_2. \end{aligned}$$

Using this definition $(\mathbf{x},\mathbf{y}) = (\mathbf{v},\mathbf{u})$ is a conditional extremum point with the condition $g(\mathbf{x},\mathbf{z}) = \mathbf{0}$. Notice that for any sets $S_1(\mathbf{u})$, $S_1(\mathbf{v})$, the rank of matrix $g'(\mathbf{u},\mathbf{v})$ is equal to $s_1 + s_2$. For example when $S_1(\mathbf{u}) = S_1(\mathbf{v}) = \{1,2\}$ we have

$$g'(\mathbf{u},\mathbf{v}) = \begin{pmatrix} 2u_1 & 2u_0 & 0 & 0 & 0 & 0 \\ 2u_2 & 2u_1 & 2u_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2v_1 & 2v_0 & 0 \\ 0 & 0 & 0 & 2v_2 & 2v_1 & 2v_0 \end{pmatrix},$$

and the rank of this matrix is 4. Now, by Lemma 3.5, there exist real numbers $\lambda_1,\dots,\lambda_{s_1}$, $\beta_1,\dots,\beta_{s_2}$ such that

$$G'(\mathbf{u},\mathbf{v}) = \lambda_1 g_1'(\mathbf{u}) + \cdots + \lambda_{s_1} g_{s_1}'(\mathbf{u}) + \beta_1 g_{s_1+1}'(\mathbf{v}) + \cdots + \beta_{s_2} g_{s_1+s_2}'(\mathbf{v}).$$

This is equivalent to

$$\frac{\partial G}{\partial x_i}(\mathbf{u},\mathbf{v}) = \lambda_1 \frac{\partial h_{t_1}}{\partial x_i}(\mathbf{u}) + \cdots + \lambda_{s_1} \frac{\partial h_{t_{s_1}}}{\partial x_i}(\mathbf{u}), \qquad i = 0,1,2, \tag{3.15a}$$

$$\frac{\partial G}{\partial z_j}(\mathbf{u},\mathbf{v}) = \beta_1 \frac{\partial h_{l_1}}{\partial z_i}(\mathbf{v}) + \cdots + \beta_{s_2} \frac{\partial h_{l_{s_2}}}{\partial z_i}(\mathbf{v}), \qquad j = 0,1,2. \tag{3.15b}$$

By solving this system of equations, together with $g(\mathbf{u}, \mathbf{v}) = \mathbf{0}$, we will get that either the system of equation has no solution or the solution does not give the minimum value. We need to check 15 cases. We will work out one case here and check the remaining ones using a computer.

If $S_1(\mathbf{u}) = S_1(\mathbf{v}) = \{2\}$, equations (3.15) are

$$v_0 = \lambda_2 u_2, \quad v_1 = \lambda_2 u_1, \quad v_2 = \lambda_2 u_0,$$
$$u_0 = \beta_2 v_2, \quad u_1 = \beta_2 v_1, \quad u_2 = \beta_2 v_0.$$

Using equalities and $h_2(\mathbf{u}) = 1$, $h_2(\mathbf{v}) = 1$, we get

$$1 = 2u_2u_0 + u_1^2 = \beta_2^2(2v_2v_0 + v_1^2) = \beta_2^2,$$

hence $\beta_2 = 1$. But this immediately gives contradiction, since then

$$2u_0u_2 + u_1^2 > 2\beta_2 v_0 u_0 \geqslant 2.$$

Using the *Maple* we get that for all remaining cases, the system of equations (3.15), together with $g(\mathbf{u}, \mathbf{v}) = \mathbf{0}$, has no solution (see for code in Section 3.5). Therefore, $G$ attains the minimum only when $\mathbf{u} = \mathbf{v} = (y_0, y_1, y_2) = (1, \frac{1}{2}, \frac{3}{8})$ and $G_m(3) = \frac{89}{32}$. This proves the lemma for $n = 3$.

*Case $n = 4$:*

The proof for this case is the same as that in the case $n = 3$. The difference is that there are more possibilities for the sets $S_1(\mathbf{v})$, $S_1(\mathbf{u})$, $S_0(\mathbf{v})$, $S_0(\mathbf{u})$, $S_L(\mathbf{v})$, $S_L(\mathbf{u})$. As in the case $n = 3$ we have that $0, 1, 3 \notin S_L(\mathbf{u})$ and $0, 1, 2 \notin S_0(\mathbf{u})$. If $2 \in S_L(\mathbf{u})$ then from $2.97 > G_m(4) \geqslant 2u_2v_2 + 2v_0u_0$ and $2v_2v_0 + v_1^2 \geqslant 1$ we have $v_0 < 3$ and $v_2 \leqslant \frac{3}{2L}$, so $v_1 \geqslant \sqrt{1 - \frac{9}{L}}$, for large $L$. But this leads to the contradiction, since for sufficiently large $L$ we get

$$G_m(4) \geqslant 2u_0v_0 + 2v_1u_1 \geqslant 2u_0 + \frac{\sqrt{1 - \frac{9}{L}}}{u_0} \geqslant 2 + \sqrt{1 - \frac{9}{L}} > 2.97.$$

Therefore, we have one of the following two cases:

$$S_L(\mathbf{u}) = \emptyset, S_0(\mathbf{u}) = \{3\}.$$
$$S_L(\mathbf{u}) = S_0(\mathbf{u}) = \emptyset.$$

The same is true for the sets $S_L(\mathbf{v})$, $S_0(\mathbf{v})$.

The rest of the investigation is divided in two cases. The case when at least one of the sets $S_0(\mathbf{v})$, $S_0(\mathbf{u})$ is equal to $\{3\}$ and the case $S_0(\mathbf{v}) = S_0(\mathbf{u}) = \emptyset$.

For the first one, without loss of generality we can assume that $S_0(\mathbf{u}) = \{3\}$, i.e. $u_3 = 0$. From the conditions $2u_2u_1 = 2u_3u_0 + 2u_2u_1 \geqslant 1$ and $2u_1u_0 \geqslant 1$ we have

$$2u_2u_0 + u_1^2 \geqslant \frac{u_0}{u_1} + u_1^2 \geqslant 2\sqrt{\frac{u_0}{u_1}}u_1 \geqslant \sqrt{2}.$$

Hence, the condition $2u_2u_0 + u_1^2 \geqslant 1$ is irrelevant. Notice that $v_3$ is also irrelevant, and so is the condition $h_3(\mathbf{v}) \geqslant 1$. Also, since $u_2$ is restricted only on $0 \leqslant u_2 \leqslant L$ and $1 \leqslant 2u_0u_2$, we can clearly assume that $2u_1u_2 = 1$. By a similar argument, at least one of $u_0^2$, $2u_0u_1$ is equal to 1 and $2 \in S_1(\mathbf{v})$. Therefore there are 3 possible cases for the set $S_1(\mathbf{u})$: $\{0,1,3\}$, $\{0,3\}$, $\{1,3\}$. And 4 possible cases for the set $S_1(\mathbf{v})$: $\{0,1,2\}$, $\{0,2\}$, $\{1,2\}$, $\{2\}$. Next we show that for any of those cases, such $\mathbf{u}$, $\mathbf{v}$ do not exist.

Suppose $S_1(\mathbf{u}) = \{t_1, \ldots, t_{s_1}\}$, $S_1(\mathbf{v}) = \{l_1, \ldots, l_{s_2}\}$, where $t_1 < \cdots < t_{s_1} = 3$ and $l_1 < \cdots < l_{s_2} = 2$. Define a conditional function

$$g(\mathbf{x}, \mathbf{z}) := (g_1(\mathbf{x}), \ldots, g_{s_1}(\mathbf{x}), g_{s_1+1}(\mathbf{z}), \ldots, g_{s_1+s_2}(\mathbf{z})),$$

where

$$\begin{aligned} g_i(\mathbf{x}) &:= h_{t_i}(\mathbf{x}) - 1, \qquad i = 1, \ldots, s_1 - 1, \\ g_{s_1}(\mathbf{x}) &:= 2x_2x_1 - 1, \\ g_{s_1+j}(\mathbf{z}) &:= h_{l_j}(\mathbf{z}) - 1 \qquad j = 1, \ldots, s_2. \end{aligned}$$

Then $(\mathbf{x}, \mathbf{z}) = (\mathbf{u}, \mathbf{v})$ is a conditional extremum point of function $\widetilde{G}(\mathbf{x}, \mathbf{z}) = 2x_0z_0 + 2x_1z_1 + 2x_2z_2$ with the condition $g(\mathbf{x}, \mathbf{z}) = \mathbf{0}$. As in the case $n = 3$, the rank of matrix $g'(\mathbf{u}, \mathbf{v})$ is equal to $s_1 + s_2$. Hence, by Lemma 3.5, there exist real numbers $\lambda_1, \ldots, \lambda_{s_1}$, $\beta_1, \ldots, \beta_{s_2}$ satisfying the system of equations

$$\begin{aligned} \frac{\partial \widetilde{G}}{\partial x_i}(\mathbf{u}, \mathbf{v}) &= \lambda_1 \frac{\partial h_{t_1}}{\partial x_i}(\mathbf{u}) + \cdots + \lambda_{s_1} \frac{\partial h_{t_{s_1}}}{\partial x_i}(\mathbf{u}), \qquad i = 0, 1, 2, \\ \frac{\partial \widetilde{G}}{\partial z_j}(\mathbf{u}, \mathbf{v}) &= \beta_1 \frac{\partial h_{l_1}}{\partial z_i}(\mathbf{v}) + \cdots + \beta_{s_2} \frac{\partial h_{l_{s_2}}}{\partial z_i}(\mathbf{v}), \qquad j = 0, 1, 2. \end{aligned}$$

Using the *Maple*, we get that this system of equations, together with $g(\mathbf{u}, \mathbf{v}) = 0$, has a solution only when $S_1(\mathbf{u}) = \{3, 1, 0\}$ and $S_1(\mathbf{v}) = \{0, 1, 2\}$, $\{0, 2\}$. For

both of these solutions the value $G(\mathbf{u}, \mathbf{v}) = \frac{13}{4} > 3$ is not the minimum, a contradiction. Therefore, the case when at least one of the sets $S_0(\mathbf{v})$, $S_0(\mathbf{u})$ is equal to $\{3\}$ is not possible.

Let us now turn to the second case, namely, $S_0(\mathbf{v}) = S_0(\mathbf{u}) = \emptyset$. If at least one of the sets $S_1(\mathbf{u})$, $S_1(\mathbf{v})$ is not equal to $\{0, 1, 2, 3\}$, then again, viewing $(\mathbf{x}, \mathbf{z}) = (\mathbf{u}, \mathbf{v})$ as a conditional extremum point of function $G(\mathbf{x}, \mathbf{z})$ with the corresponding condition

$$\begin{aligned} h_i(\mathbf{x}) &= 1 \qquad i \in S_1(\mathbf{u}), \\ h_j(\mathbf{z}) &= 1 \qquad j \in S_1(\mathbf{v}), \end{aligned}$$

we will get a contradiction. The way we get a contradiction is completely the same as for case $n = 3$. Using the program *Maple*, we find that the systems of equations (3.15), together with the corresponding condition $g(\mathbf{u}, \mathbf{v}) = \mathbf{0}$, has a solution only for the sets $S_1(\mathbf{u}) = \{0, 1, 3\}$, $S_1(\mathbf{v}) = \{0, 2, 3\}$ and $S_1(\mathbf{v}) = \{0, 1, 3\}$, $S_1(\mathbf{u}) = \{0, 2, 3\}$. For these solutions the value $G(\mathbf{u}, \mathbf{v}) \approx 3.158833604$ (the same for both solutions) is greater then $G_m(4)$, a contradiction.

Hence, the minimum must be obtained when $S_1(\mathbf{v}) = S_1(\mathbf{u}) = \{0, \ldots, n-1\}$, which proofs the lemma for the case $n = 4$. □

## 3.4 Proof of Theorems 3.1 and 3.2

*Proof of Theorem 3.1.* Let fix $d \in \mathbb{N}$ and assume that $p(z) = x_0 + x_1 z + \cdots + x_1 z^{d-1} + x_0 z^d$ is a reciprocal polynomial of degree $d$ with nonnegative coefficients such that the coefficients of its square $p(z)^2 = r_0 + r_1 z + \cdots + r_1 z^{2d-1} + r_0 z^{2d}$ are all greater than or equal to 1. Then

$$r_0 = x_0^2 \geqslant 1, \;\; r_1 = 2x_0 x_1 \geqslant 1, \;\; \ldots, \;\; r_{[d/2]} = \sum_{i=0}^{[d/2]} x_i x_{[d/2]-i} \geqslant 1,$$

and so $(x_0, \ldots, x_{[d/2]}) \in V_{[d/2]+1}$. The coefficient $r_d$ for $z^d$ in $p(z)^2$ is equal to

$$2(x_0^2 + \cdots + x_{(d-1)/2}^2)$$

for $d$ odd and to

$$2(x_0^2 + \cdots + x_{d/2-1}^2) + x_{d/2}^2$$

for $d$ even.

For $d$ odd, by Lemma 3.6, we have

$$r_d = 2(x_0^2 + \cdots + x_{(d-1)/2}^2) \geqslant 2(y_0^2 + \cdots + y_{(d-1)/2}^2).$$

Moreover, if $x_i \neq y_i$ for at least one $i \in \{0, \ldots, (d-1)/2\}$, then this inequality is strict. This implies that the polynomial $p(z)^2$ has at least one coefficient greater than $2(y_0^2 + \cdots + y_{(d-1)/2}^2)$, unless $x_0 = y_0, \ldots, x_{(d-1)/2} = y_{(d-1)/2}$. So

$$q(p^2) \geqslant q(p_d^2) = 2(y_0^2 + \cdots + y_{(d-1)/2}^2)$$

for every reciprocal polynomial $p$ with nonnegative coefficients. On the other hand, the example $p(z) = p_d(z)$ shows that all coefficients of $p_d(z)^2$ range from 1 to $2(y_0^2 + \cdots + y_{(d-1)/2}^2)$ (see Theorem 3.4 and, more precisely, inequality (3.5)).

For $d$ even, applying Lemma 3.6 to $n = d/2$ and to $n = d/2 + 1$, we find that

$$r_d = 2(x_0^2 + \cdots + x_{d/2-1}^2) + x_{d/2}^2 = \sum_{i=0}^{d/2-1} x_i^2 + \sum_{i=0}^{d/2} x_i^2$$

$$\geqslant \sum_{i=0}^{d/2-1} y_i^2 + \sum_{i=0}^{d/2} y_i^2 = 2(y_0^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2.$$

Consequently, $q(p^2) \geqslant q(p_d^2) = 2(y_0^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2$ for every reciprocal polynomial $p$ with nonnegative coefficients. The proof of Theorem 3.1 can now be concluded as above with the same example $p(z) = p_d(z)$. □

*Proof of Theorem 3.2.* In the proof there is a difference between the cases when $d$ is odd and $d$ is even. Although this is a small difference, to be clear, we will prove these two cases separately.

Let $d \in \{2, 4, 6\}$ be even and suppose that

$$p(z) = x_0 + x_1 z + \cdots x_{d/2} z^{d/2} + z_{d/2-1} z^{d/2+1} + \cdots + z_1 z^{d-1} + z_0 z^d$$

is a polynomial with nonnegative coefficients such that the coefficients of its square $p(z)^2 = r_0 + r_1 z + \cdots + r_{2d-1} z^{2d-1} + r_{2d} z^{2d}$ are all greater than or equal to 1. Then

$$r_0 = x_0^2 \geqslant 1, \;\; r_1 = 2x_0 x_1 \geqslant 1, \;\; \ldots \;\; , r_{d/2} = 2x_{d/2} x_0 + 2x_{d/2-1} x_1 + \ldots \geqslant 1,$$

$$r_{2d} = z_0^2 \geqslant 1, \;\; r_{2d-1} = 2z_0 z_1 \geqslant 1, \;\; \ldots, \;\; r_{3d/2} = 2x_{d/2} z_0 + 2z_{d/2-1} z_1 + \ldots \geqslant 1,$$

so $(x_0, \ldots, x_{d/2-1}, x_{d/2}), (z_0, \ldots, z_{d/2-1}, x_{d/2}) \in V_{d/2+1}(L)$, for sufficiently large $L$. The coefficient $r_d$ of $z^d$ in $p(z)^2$ is equal to

$$2z_0x_0 + \cdots + 2z_{d/2-1}x_{d/2-1} + x_{d/2}^2.$$

By Lemma 3.7, we have

$$z_0x_0 + \cdots + z_{d/2-1}x_{d/2-1} + x_{d/2}^2 \geqslant y_0^2 + \cdots + y_{d/2}^2,$$
$$z_0x_0 + \cdots + z_{d/2-1}x_{d/2-1} \geqslant y_0^2 + \cdots + y_{d/2-1}^2,$$

and so $r_d \geqslant 2(y_0^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2$. Moreover, if $(x_0, \ldots, x_{d/2}) \neq (y_0, \ldots, y_{d/2})$ or $(z_0, \ldots, z_{d/2-1}, x_{d/2}) \neq (y_0, \ldots, y_{d/2})$, then this inequality is strict. This implies that the polynomial $p(z)^2$ has at least one coefficient greater then

$$2(y_0^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2,$$

unless $(x_0, \ldots, x_{d/2}) = (z_0, \ldots, z_{d/2-1}, x_{d/2}) = (y_0, \ldots, y_{d/2})$. Since all coefficients of $p_d(z)^2$ range from 1 to $2(y_0^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2$, we have

$$q(p^2) \geqslant q(p_d^2) = 2(y_0^2 + \cdots + y_{d/2-1}^2) + y_{d/2}^2$$

with equality if and only if $p(z) = p_d(z)$.

For odd $d \in \{3, 5, 7\}$, let

$$p(z) = x_0 + x_1z + \cdots x_{\frac{d-1}{2}} z^{\frac{d-1}{2}} + z_{\frac{d-1}{2}} z^{\frac{d+1}{2}} + \cdots + z_1z^{d-1} + z_0z^d$$

be a polynomial with nonnegative coefficients such that the coefficients of its square $p(z)^2 = r_0 + r_1z + \cdots + r_{2d-1}z^{2d-1} + r_{2d}z^{2d}$ are all greater than or equal to 1. Then

$$r_0 = x_0^2 \geqslant 1, \;\; r_1 = 2x_0x_1 \geqslant 1, \;\; \ldots \;\; , r_{\frac{d-1}{2}} = 2x_{\frac{d-1}{2}}x_0 + 2x_{\frac{d-1}{2}-1}x_1 + \ldots \geqslant 1,$$
$$r_{2d} = z_0^2 \geqslant 1, \;\; r_{2d-1} = 2z_0z_1 \geqslant 1, \;\; \ldots, \;\; r_{\frac{3d+1}{2}} = 2z_{\frac{d-1}{2}}z_0 + 2z_{\frac{d-1}{2}-1}z_1 + \ldots \geqslant 1,$$

and so $(x_0, \ldots, x_{\frac{d-1}{2}}), (z_0, \ldots, z_{\frac{d-1}{2}}) \in V_{\frac{d+1}{2}}(L)$, for sufficiently large $L$. Applying Lemma 3.7, we find that

$$r_d = 2z_0x_0 + \cdots + 2z_{\frac{d-1}{2}}x_{\frac{d-1}{2}} \geqslant 2y_0^2 + \cdots + 2y_{\frac{d-1}{2}}^2,$$

with equality if and only if $(x_0, \ldots, x_{\frac{d-1}{2}}) = (z_0, \ldots, z_{\frac{d-1}{2}}) = (y_0, \ldots, y_{\frac{d-1}{2}})$. Therefore, by the same argument as in the case for even $d$, we obtain

$$q(p^2) \geqslant q(p_d^2) = 2(y_0^2 + \cdots + y_{\frac{d-1}{2}}^2)$$

with equality if and only if $p(z) = p_d(z)$. This finishes the proof of the theorem. □

## A remark on the proof

Theorem 3.2 cannot be proved for all $d > 7$ with the same idea, since there are counterexamples to the Lemma 3.7. For instance, when $n = 6$, we take $\mathbf{x} = (y_0, y_1, y_2, 2, 0, 0, 0)$, $\mathbf{z} = (y_0, y_1, 1, 0, 1, 1, 1)$, which leads to a contradiction as

$$\mathbf{x}\mathbf{z}^t = y_0^2 + y_1^2 + y_2 = 1.625 < y_0^2 + \cdots + y_6^2 \approx 1.6745.$$

## 3.5 Example of a code for computation with *Maple*

The following code is used for computations in the proof of Lemma 3.7, case $n = 3$. In the code, we first generate all possible cases of the boundary. Here, $a_i = 1$ corresponds to the case when $i \in S_1(\mathbf{u})$, and respectively, $b_i = 1$ corresponds to the case when $i \in S_1(\mathbf{v})$. Next we define the system of equation (3.15) together with the corresponding equation $g(\mathbf{x}, \mathbf{z}) = \mathbf{0}$ from (3.14) and the conditions from definition of $V_3(L)$. Finally, we check all those cases by solving system of equation.

---

*Boundary* := *solve*($\{a_0(a_0-1)=0,\ a_1(a_1-1)=0,\ b_0(b_0-1)=0,\ b_1(b_1-1)=0\}$)*:*

$$
\begin{aligned}
\textit{Equations} := \{&a_0(u_0-1)=0, a_1(2u_0u_1-1)=0, 2u_2u_1+u_1^2-1=0,\\
&b_0(v_0-1)=0, b_1(2v_0v_1-1)=0, 2v_2v_1+v_1^2-1=0,\\
&u_0=\lambda_0b_0v_0+\lambda_1b_1v_1+\lambda_2v_2,\\
&u_1=\lambda_1b_1v_0+\lambda_2v_1,\\
&u_2=\lambda_2v_0,\\
&v_0=\beta_0a_0u_0+\beta_1a_1u_1+\beta_2u_2,\\
&v_1=\beta_1a_1u_0+\beta_2u_1,\\
&v_2=\beta_2u_0,\\
&u_0\geqslant 1, u_1\geqslant 0, u_2\geqslant 0, v_0\geqslant 1, v_1\geqslant 0, v_2\geqslant 0,\\
&2u_1u_0\geqslant 1, 2v_1v_0\geqslant 1\} :
\end{aligned}
$$

**for** *i* **from** 1 **to** *nops({Boundary})* - 1 **do**
  **use** *RealDomain* **in** *Solution:=solve(subs(Boundary[i],Equations))* **end use**;
  **if** *Solution != NULL* **then**
    **for** *j* **from** 1 **to** *nops({Solution})* **do**
      **if** *subs({Solution}[j],* $2v_0u_0+2v_1u_1+2v_2u_2$*)* <= 89/32 **then**
        *print({Solution}[j])*;
      **end if**;
    **od**;
**od**;

---

# 4 Littlewood-Offord inequalities in groups

## 4.1 Introduction

In this Chapter we will investigate the concentration probability of a random walk in an arbitrary group that is not necessarily abelian.

Let $V_n = \{g_1, \ldots, g_n\}$ be a multiset of non-identity elements of an arbitrary group $G = (G, *)$. Consider a collection of independent random variables $X_i$ that are each uniformly distributed on a two point set $\{g_i^{-1}, g_i\}$. The concentration probability in this case is defined as

$$\rho(V_n) = \sup_{g \in G} \mathbb{P}(X_1 * \cdots * X_n = g).$$

Recently Tiep and Vu [37] initiated the study of the Littlewood-Offord problem in the non-abelian setting. They investigated the problem for matrix groups and obtained results that are sharp. They showed that if $V_n = \{g_1, \ldots, g_n\}$ is a multiset of elements in $GL_d(\mathbb{C})$, each of which has order at least $m \geqslant 2$, then the following bound holds

$$\rho(V_n) \leqslant 141 \max\left\{\frac{1}{m}, \frac{1}{\sqrt{n}}\right\}. \tag{4.1}$$

Furthermore, they have also established an analogous bound for $GL_d(p)$. The proof of the inequality (4.1) in [37] makes use of results in representation theory, additive combinatorics, linear algebra and analytic number theory.

Before explaining the meaning of the two terms in the upper bound given in (4.1) let us introduce some definitions and state some facts regarding the convergence of Markov chains to their stationary distributions. It is well known (see [5], page 120) that if the group $G$ is a finite group and $V_n$ is not contained in a coset of a subgroup then the random walk $S_n = X_1 * \cdots * X_n$ converges to the uniform

distribution, that is,

$$\mathbb{P}(S_n = g) \to \frac{1}{|G|} \quad \text{as } n \to \infty.$$

The speed of convergence is usually measured by the total variation distance

$$||\mathbb{P}_n - u||_{TV} = \max_{A \subset G} \left| \mathbb{P}(S_n \in A) - \frac{|A|}{|G|} \right|,$$

where $u$ stands for the uniform distribution on $G$. The number of steps after which the distribution of a Markov chain $S_n$ becomes close to uniform is called the *mixing time*. To be more precise, it is defined to be the quantity

$$t_{mix}(\varepsilon) = \min \{n : ||\mathbb{P}_n - u||_{TV} < \varepsilon\}.$$

Let us now return to the explanation of the two terms appearing in (4.1). Take some element $g$ in $G$ of order $m$ and consider the multiset $V_n = \{g, \dots, g\}$. Let us for the simplicity assume that $m$ is odd. In this setup the random variable $S_n = X_1 * \cdots * X_n$ is just the simple random walk on a subgroup of $G$ that is isomorphic to $\mathbb{Z}_m$. The distribution of $S_n$ is asymptotically uniform, which accounts for the $\frac{1}{m}$ term in (4.1). It is also very natural that the term $\frac{1}{m}$ is dominant for $n \geqslant m^2$, exactly above the mixing time of $S_n$, which satisfies the inequality

$$c_1(\varepsilon)m^2 \leqslant t_{mix}(\varepsilon) \leqslant c_2(\varepsilon)m^2,$$

where $c_1(\varepsilon)$, $c_2(\varepsilon)$ are positive constants depending on $\varepsilon$ only (see [25], page 96).

On the other hand, for $n < m/2$ the point masses of $S_n$ are just the usual binomial probabilities $\binom{n}{\lfloor k/2 \rfloor}/2^n$, $k = 0, \dots, n$. Therefore in this regime

$$\mathbb{P}(S_n = g) \leqslant \binom{n}{\lfloor n/2 \rfloor}/2^n \sim c\frac{1}{\sqrt{n}}.$$

This shows that the inequality (4.1) cannot be improved apart from the constant factor.

In this chapter we will prove an optimal upper bound for $\rho(V_n)$. It turns out that a bound as in (4.1) holds for arbitrary groups. Furthermore, for groups with elements having odd or infinite order we shall establish an optimal inequality for $\mathbb{P}(X_1 * \cdots * X_n = g)$ where $X_1, \dots, X_n$ are independent random variables without the requirement for them to be two-valued.

Throughout this chapter we shall denote by $\varepsilon$ (usually supplied with a subscript) a uniform random variable on $\{-1, 1\}$. Sometimes it will be important to

stress that these random variables are defined on $\mathbb{Z}_m$ instead of $\mathbb{R}$ and we shall do so on each occasion. We denote by $(a,b]_m$ and $[a,b]_m$ the set of integers in the intervals $(a,b]$ and $[a,b]$ modulo $m$. Given a natural number $m$, we shall write $\tilde{m}$ for the smallest even number such that $\tilde{m} \geqslant m$. That is, we have $\tilde{m} = 2\lceil \frac{m}{2} \rceil$. We shall denote by $|g|$ the order of an element $g$ of underlying group $G$.

**Theorem 4.1.** *Let $g_1, \dots, g_n$ be elements of some group $G$ such that $|g_i| \geqslant m \geqslant 2$. Let $X_1, \dots, X_n$ be independent random variables so that each $X_i$ has the uniform distribution on the two point set $\{g_i^{-1}, g_i\}$. Then for any $A \subset G$ with $|A| = k$ we have*

$$\mathbb{P}\left(X_1 * \cdots * X_n \in A\right) \leqslant \mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in (-k,k]_{\tilde{m}}\right), \tag{4.2}$$

*where $\varepsilon_i$ are independent uniform random variables on the set $\{-1,1\} \subset \mathbb{Z}_{\tilde{m}}$.*

*Remark* 4.2. Theorem 4.1 is optimal in the sense that if $G$ contains an element of order $\tilde{m}$, the bound in (4.2) can be atteined. For instance, in the case $G = GL_d(\mathbb{C})$ the upper bound in the inequality is achieved by taking two point distributions concentrated on the diagonal matrix $\mathrm{e}^{\frac{2\pi i}{\tilde{m}}}\,\mathbb{I}_d$ and its inverse - this way we get exactly the distribution of $\varepsilon_1 + \cdots + \varepsilon_n$ and its $k$ largest probabilities coincide with the upper bound in (4.2).

Theorem 4.1 implies an inequality of the same type as the one by Tiep and Vu, but with a much better constant.

**Corollary 4.3.** *Let $V_n = \{g_1, \dots, g_n\}$ be elements in some group $G$ satisfying $|g_i| \geqslant m \geqslant 2$. Then*

$$\rho(V_n) \leqslant \frac{2}{m} + \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}} \leqslant 3\max\{\frac{1}{m}, \frac{1}{\sqrt{n}}\}. \tag{4.3}$$

The sequence of sums appearing on the right hand side of (4.2) is a periodic Markov chain and so does not converge to a limit as $n \to \infty$. Nonetheless, it is well known that it does converge to a limit if we restrict the parity of $n$. Let us now express the quantity in the right hand side of (4.2) in the case $|A| = 1$ in asymptotic terms.

**Proposition 4.4.** *Let $m \in \mathbb{N}$ and assume that $n \to \infty$. Then for any $l \in \mathbb{Z}_{\tilde{m}}$ of the same parity as $n$ we have*

$$\mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n = l\right) = \frac{2}{\tilde{m}} + o(1),$$

*where $\varepsilon_i$ are independent uniform random variables on the set $\{-1, 1\} \subset \mathbb{Z}_{\tilde{m}}$.*

The $o(1)$ term is actually exponentially small in terms of $n$. For such sharp quantitative estimates see [5] pages 124-125. Note that Proposition 4.4 implies that in (4.3) the constant after the last inequality cannot be smaller than 2. Let us also note that both constants in the expression $\frac{2}{\tilde{m}} + \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}$ are sharp. The term $\frac{2}{\tilde{m}}$ is dominant in the case $m, n \to \infty$ and $n \gg m^2$ and so Proposition 4.4 shows that the constant 2 cannot be reduced. In the case $m, n \to \infty$ and $n < m$ the term $\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}$ is dominating. For $V_n = \{g, \ldots, g\}$ for some element $g$ of order $\tilde{m}$ we have

$$\rho(V_n) = \mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in (-1, 1]_{\tilde{m}}\right) = \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = (1 + o(1))\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}. \tag{4.4}$$

The sharp asymptotic relation in (4.4) follows ether from Stirling's formula or the local limit theorem (see [24]).

The simple random walk on $\mathbb{Z}_m$ for $m$ odd converges to the uniform distribution on $\mathbb{Z}_m$ and so all probabilities converge to $\frac{1}{m}$. It should now be unsurprising that the simple random walk on $\mathbb{Z}_{\tilde{m}} = \mathbb{Z}_{m+1}$ rather than $\mathbb{Z}_m$ is a much better "candidate" for a maximizer of the left hand side in (4.2), as by Proposition 4.4 we gain an extra factor of 2 asymptotically.

From this point on our prime focus will be on groups only having elements of odd order. The reader could think of particular group $G = \mathbb{Z}_m^l$ for $m$ odd as a prime example. For these groups Theorem 4.1 does not provide the optimal bound, since the worst case scenario there is provided by the simple walk on a cyclic subgroup of even order and in all latter case such a subgroup does not exist. For $k \geqslant 1$ we define

$$I_{n,k}^m = \left[\left\lceil \frac{n-k+1}{2} \right\rceil, \left\lceil \frac{n+k-1}{2} \right\rceil\right]_m.$$

The latter set is an interval of $k$ points in $\mathbb{Z}_m$ for $k < m$ and $I_{n,k}^m = \mathbb{Z}_m$ for $k > m$. We shall use the convention that $I_{n,0}^m = \emptyset$.

**Theorem 4.5.** *Let $X_1, \dots, X_n$ be independent discrete random variables taking values in some group $G$ such that for each $i$ we have*

$$\sup_{g \in G} \mathbb{P}(X_i = g) \leqslant \frac{1}{2}. \tag{4.5}$$

*Furthermore, assume that all non-identity elements in $G$ have odd or infinite order and that the minimal such order is at least some odd number $m \geqslant 3$. Then for any set $A \subset G$ of cardinality $k$ we have*

$$\mathbb{P}(X_1 * \cdots * X_n \in A) \leqslant \mathbb{P}\left(\tau_1 + \cdots + \tau_n \in I^m_{n,k}\right),$$

*where $\tau_i$ are independent uniform random variables on the set $\{0,1\} \subset \mathbb{Z}_m$.*

It is well known that the distribution of $\tau_1 + \cdots + \tau_n$ is asymptotically uniform in $\mathbb{Z}_m$ and thus we have $\mathbb{P}(X_1 * \cdots * X_n = g) \leqslant \frac{1}{m} + o(1)$.

*Remark* 4.6. Note that

$$\mathbb{P}\left(\tau_1 + \cdots + \tau_n \in I^m_{n,k}\right) = \mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in 2I^m_{n,k} - n\right).$$

We formulated the result in terms of $\{0,1\}$-valued random variables $\tau_i$ for the sake of convenience only - in this formulation the set of maximum probability is an interval. As one notices, it is not so if one formulates it in terms of $\{-1,1\}$-valued random variables $\varepsilon_i$.

*Remark* 4.7. The reason we restrict the elements to have odd order in Theorem 4.5 is as follows. If there is an element of even order in the underlying group, then the group contains an element of order 2, say $h$. Then by taking independent uniform random variables $X_i$ on the set $\{1, h\}$ we obtain $\sup_{g \in G} \mathbb{P}(X_1 * \cdots * X_n = g) = \frac{1}{2}$.

In the case when $G$ is torsion-free (a group whose only element of finite order is the identity) we can actually prove that Erdős's bound (2.2) still holds even in this general setting.

**Theorem 4.8.** *Under the notation of Theorem 4.5 and assuming that $G$ is torsion-free for any set $A \subset G$ of cardinality $k$ we have*

$$\mathbb{P}(X_1 * \cdots * X_n \in A) \leqslant \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_n \in (-k, k]),$$

*where $\varepsilon_i$ are independent. In particular, for any $g \in G$ we have*

$$\mathbb{P}\left(X_1 * \cdots * X_n = g\right) \leqslant \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n}.$$

The latter proposition immediately follows by taking $m$ large enough in Theorem 4.5 so that $\tau_1 + \cdots + \tau_n$ is concentrated in a proper subset of $\mathbb{Z}_m$. For instance, assume that $m = n + 2$. In this case the latter sum is strictly contained in $\mathbb{Z}_m$ and its probabilities are exactly the largest $k$ probabilities of $\varepsilon_1 + \cdots + \varepsilon_n$ and we are done.

## 4.2 An open problem

Theorem 4.1 gives an optimal inequality if an element with of order $\tilde{m}$ exists. To be more precise, if an element of order $\tilde{m}$ exists. For groups in which all elements have odd or infinite order, Theorem 4.5 gives the best possible result. It is thus natural to ask what happens if we have full knowledge of the orders of the elements of the underlying group $G$ and we are not in the aforementioned cases. The asymptotics of the cases when we do know the exact answer suggest the following guess.

*Conjecture.* Let $G$ be any group and fix an odd integer $m \geqslant 3$. Suppose that all possible even orders of elements in $G$ greater than $m$ are given by the sequence $S = \{m_1, m_2, \ldots\}$ in the increasing order. Consider a collection of independent random variables $X_1, \ldots, X_n$ in $G$ such that each $X_i$ is concentrated on a two point set $\{g_i, g_i^{-1}\}$ and $|g_i| \geqslant m$. Then in the case $m_1 < 2m$ for any $A \subset G$ with $|A| = k$ we have

$$\mathbb{P}\left(X_1 * \cdots * X_n \in A\right) \leqslant \mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in (-k, k]_{m_1}\right),$$

where $\varepsilon_i$ are independent uniform random variables on the set $\{-1, 1\} \subset \mathbb{Z}_{m_1}$. On the other hand, if $m_1 \geqslant 2m$ we have

$$\mathbb{P}\left(X_1 * \cdots * X_n \in A\right) \leqslant \mathbb{P}\left(\tau_1 + \cdots + \tau_n \in I_{n,k}^m\right),$$

where $\tau_i$ are independent uniform random variables on the set $\{0, 1\} \subset \mathbb{Z}_m$. If true, the latter conjecture would settle the remaining cases.

## 4.3 Structure of the proofs

The remainder of the chapter is organized as follows. In the next two sections we prove Theorems 4.1 and 4.5. Then we will finish the chapter with the proof of Corollary 4.3.

In order to prove Theorems 4.1 and 4.5, we shall require a simple group theoretic statement contained in the following lemma.

**Lemma 4.9.** *Let $G$ be a group and $g \in G$ be an element of order greater then or equal to $m \geqslant 2$. Then for any finite set $A \subset G$ and a positive integer $s$ such that $s < \frac{m}{|A|}$ we have $A \neq Ag^s$.*

*Proof.* Suppose there is a nonempty set $A \subset G$ and a positive integer $s$ such that $|A| = k < \frac{m}{s}$ and $A = Ag^s$. Take some $a \in A$ and consider elements $ag^{si}$, $i = 0 \dots k$. All these $k+1$ elements are in the set $A$, hence at least two of them must be equal. Let us say $ag^{si} = ag^{sj}$ for some integers $0 \leqslant i < j \leqslant k$. But this immediately contradict that $g$ has order at least $m$, since then $g^{s(j-i)}$ is equal to the group identity element and $s(j-i) \leqslant sk < m$. □

The proofs of Theorems 4.1 and 4.5 are similar in spirit to Kleitman's approach in his solution of the Littlewood-Offord problem in all dimensions. Actually, it is closer to a simplification of Kleitman's proof in dimension 1 obtained in [10]. The proofs thus proceed by induction on the number of random variables, taking into account a certain recurrence relation satisfied by the worst-case random walk.

## 4.4 Proof of Theorem 4.1

*Proof.* The proof is by induction on $n$. If $n = 1$ the inequality (4.2) is trivial. For $k \geqslant \frac{m}{2}$ and all $n$ the right hand side of (4.2) becomes 1 since in this case $(-k, k]_{\tilde{m}}$ is the whole $\mathbb{Z}_m$ and so there is nothing to prove. We shall henceforth assume that $n > 1$ and $k < \frac{m}{2}$.

By Lemma 4.9 we have that $Ag_n \neq Ag_n^{-1}$. Take some $h \in Ag_n \backslash Ag_n^{-1}$ and define

$B = Ag_n \backslash \{h\}$ and $C = Ag_n^{-1} \cup \{h\}$. We then have

$$\begin{aligned} & 2\mathbb{P}(X_1 * \cdots * X_n \in A) \\ = \; & \mathbb{P}(X_1 * \cdots * X_{n-1} \in Ag_n) + \mathbb{P}(X_1 * \cdots * X_{n-1} \in Ag_n^{-1}) \\ = \; & \mathbb{P}(X_1 * \cdots * X_{n-1} \in B) + \mathbb{P}(X_1 * \cdots * X_{n-1} \in C) \\ \leqslant \; & \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_{n-1} \in (-k-1, k+1]_{\tilde{m}}) \\ & + \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_{n-1} \in (-k+1, k-1]_{\tilde{m}}). \end{aligned}$$

Since for $k < \frac{m}{2}$ (this implies that $k \leq \frac{\tilde{m}}{2} - 1$) the sets $(-k+1, k-1]_{\tilde{m}}$ and $(k-1, k+1]_{\tilde{m}}$ are disjoint in $\mathbb{Z}_{\tilde{m}}$ we have

$$\begin{aligned} & \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_{n-1} \in (-k-1, k+1]_{\tilde{m}}) \\ & + \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_{n-1} \in (-k+1, k-1]_{\tilde{m}}) \\ = \; & \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_{n-1} \in (-k+1, k+1]_{\tilde{m}}) \\ & + \mathbb{P}(\varepsilon_1 + \cdots + \varepsilon_{n-1} \in (-k-1, k-1]_{\tilde{m}}) \\ = \; & 2\mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in (-k, k]_{\tilde{m}}\right). \end{aligned}$$

□

## 4.5 Proof of Theorem 4.5

In the proof of Theorem 4.5 we shall make use of the following simple lemma which will allow us to switch from general distributions satisfying the condition (4.5) to two-point distributions.

**Lemma 4.10.** *Let $X$ be a random variable on some group $G$ that takes only finitely many values, say $x_1, \ldots, x_n$. Suppose that $p_i = \mathbb{P}(X = x_i)$ are rational numbers and that $p_i \leqslant \frac{1}{2}$. Then we can express the distribution of $X$ as a convex combination of distributions that are uniform on some two point set.*

In the proof of lemma 4.10 we shall use Dirac's theorem from graph theory. Let us therefore introduce the relevant terminology. We shall only consider finite simple graphs $G = (V, E)$, where $V$ is the (finite) set of vertices and $E$ - the set of edges of $G$. A graph $G$ is called *Hamiltonian* if it contains a cycle that visits every vertex of $V$. A *perfect matching* in $G$ is a set of $\lfloor |V|/2 \rfloor$ edges in $E$ that do

not share any endpoints (vertices). And finally, the number of edges coming out of a certain vertex $v \in V$ is called the degree of that vertex and denoted by $d(v)$.

**Theorem 4.11** (Dirac, [7]). *Let $G = (V, E)$ be a finite simple graph with $|V| \geqslant 3$ such that for each $v \in V$ we have $d(v) \geqslant |V|/2$. Then $G$ is Hamiltonian.*

*Proof of Lemma 4.10.* Denote by $\mu$ the distribution of $X$. Since the $p_i$'s are all rational, we have $p_i = \frac{k_i}{K_i}$ for some $k_i, K_i \in \mathbb{Z}$. We shall now view $\mu$ as a distribution on a multiset $M$ made from the elements $x_i$ in the following way - take $x_i$ exactly $2k_i \prod_{j \neq i} K_j$ times into $M$. This way $\mu$ has the uniform distribution on $M$. We thus have that $M = \{y_1, \ldots, y_{2N}\}$ for an appropriate $N$. Construct a graph on the elements of $M$ by joining two of them by an edge if and only if they corresponding to distinct $x_i$'s. Since we had $p_i \leqslant \frac{1}{2}$, each vertex of this graph has degree at least $N$. Thus by Dirac's Theorem, our graph contains a Hamiltonian cycle, and, consequently - a perfect matching. Let $\mu_i$ be the uniform distribution on two vertices of the latter matching ($i = 1, 2, \ldots, N$). We have

$$\mu = \frac{1}{N} \sum_{i=1}^{N} \mu_i.$$

□

*Proof of Theorem 4.5.* We shall argue by induction on $n$. First notice that the claim of the Theorem is true for $n = 1$. Furthermore, it is also true for $k \geqslant m$ since in that case the bound for the probability in question becomes 1. We therefore shall from now on assume that $n > 1$ and $1 \leqslant k \leqslant m - 1$. Denote by $\mu_i$ the distribution of the random variable $X_i$. We can without loss of generality assume that each $X_i$ is concentrated on finitely many points and that for each $g \in G$ we have $\mathbb{P}(X_i = g) \in \mathbb{Q}$. By Lemma 4.10, each $\mu_i$ can be written as a convex combination of distributions that are uniform on some two-point set. Define a random variable $f_i(X_i) = \mathbb{E}_i 1\{X_1 * \cdots * X_n \in A\}$, where $\mathbb{E}_i$ stands for integration with respect to all underlying random variables except $X_i$. Then for each $i$ we have

$$\mathbb{P}\left(X_1 * \cdots * X_n \in A\right) = \mathbb{E} f_i(X_i). \tag{4.6}$$

The latter expectation is linear with respect to the distribution of $X_i$. Therefore we can assume that it will be maximized by some choice of two-point distributions

coming from the decomposition of $\mu_i$. We shall therefore from this point assume that $X_n$ takes only two values, say $h_1$ and $h_2$, with equal probabilities.

Note that the intervals $I_{n,k}^m$ have recursive structure. Namely, if $1 \leqslant k \leqslant m-1$ and we regard them as multisets, we have the relation

$$I_{n,k}^m \cup (I_{n,k}^m - 1) = I_{n-1,k-1}^m \cup I_{n-1,k+1}^m.$$

The pairs on intervals appearing on both sides of the latter equality heavily overlap. This means that we can take one endpoint of $I_{n-1,k+1}^m$ that does not belong to $I_{n-1,k-1}^m$ and move it to this shorter interval. The resulting intervals are both of length $k$ and are exactly the intervals $I_{n,k}^m$ and $I_{n,k}^m - 1$. We shall use this after the inductive step.

Take a finite set $A \subset G$ with $k$ elements. Note that the element $h_2^{-1}h_1 \neq 1_G$ and so it has order at least $m$. By Lemma 4.9 we have that $Ah_1^{-1} \neq Ah_2^{-1}$ as $A \neq Ah_2^{-1}h_1$. Take some $h \in Ah_1^{-1} \backslash Ah_2^{-1}$ and define $B = Ah_1^{-1} \backslash \{h\}$ and $C = Ah_2^{-1} \cup \{h\}$. We have

$$\begin{aligned}
& 2\mathbb{P}(X_1 * \cdots * X_n \in A) \\
= \ & \mathbb{P}(X_1 * \cdots * X_{n-1} \in Ah_1^{-1}) + \mathbb{P}(X_1 * \cdots * X_{n-1} \in Ah_2^{-1}) \\
= \ & \mathbb{P}(X_1 * \cdots * X_{n-1} \in B) + \mathbb{P}(X_1 * \cdots * X_{n-1} \in C) \\
\leqslant \ & \mathbb{P}(\tau_1 + \cdots + \tau_{n-1} \in I_{n-1,k-1}^m) + \mathbb{P}(\tau_1 + \cdots + \tau_{n-1} \in I_{n-1,k+1}^m) \\
= \ & \mathbb{P}(\tau_1 + \cdots + \tau_{n-1} \in I_{n,k}^m - 1) + \mathbb{P}(\tau_1 + \cdots + \tau_{n-1} \in I_{n,k}^m) \\
= \ & 2\mathbb{P}(\tau_1 + \cdots + \tau_n \in I_{n,k}^m).
\end{aligned}$$

□

## 4.6 Proof of Corollary 4.3

In the proof we shall make use of Ramus's identity on evenly spaced binomial coefficients (see [1] for the proof):

$$\binom{n}{t} + \binom{n}{t+s} + \binom{n}{t+2s} + \cdots = \frac{1}{s} \sum_{j=0}^{s-1} \left(2\cos\frac{j\pi}{s}\right)^n \cos\frac{\pi(n-2t)j}{s}. \tag{4.7}$$

*Proof.* By Theorem 4.1 we have

$$\rho(V_n) \leqslant \mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in (-1, 1]_{\tilde{m}}\right). \tag{4.8}$$

The right hand of the equation (4.8) is the sum of binomial probabilities $\binom{n}{i}/2^n$, where $i$ is such that $2i-n$ is congruent to $1_{\{n\in 2\mathbb{Z}+1\}}$ modulo $\tilde{m}$. Let $t$ be the residue of $(n-1_{\{n\in 2\mathbb{Z}+1\}})/2$ modulo $\frac{\tilde{m}}{2}$.

Using the identity (4.7) and the elementary inequalities

$$\cos x \leqslant \exp(-x^2/2)$$

for $x \in [0, \frac{\pi}{2}]$ and

$$\int_0^\infty \mathrm{e}^{\frac{-x^2}{2\sigma^2}}\, dx \leqslant \frac{\sigma\sqrt{2\pi}}{2}$$

we obtain

$$\begin{aligned}
\mathbb{P}\left(\varepsilon_1+\cdots+\varepsilon_n \in (-1,1]_{\tilde{m}}\right) &= \frac{\binom{n}{t}+\binom{n}{t+\tilde{m}/2}+\binom{n}{t+2\tilde{m}/2}+\cdots}{2^n} \\
&= \frac{2}{2^n\tilde{m}}\sum_{j=0}^{\frac{\tilde{m}}{2}-1}\Big(2\cos\frac{2i\pi}{\tilde{m}}\Big)^n\cos\frac{2\pi(n-2t)j}{\tilde{m}} \\
&\leqslant \frac{2}{\tilde{m}}+\frac{2}{\tilde{m}}\sum_{j=1}^{\frac{\tilde{m}}{2}-1}\Big|\cos\frac{2j\pi}{\tilde{m}}\Big|^n \qquad (4.9)\\
&\leqslant \frac{2}{\tilde{m}}+\frac{4}{\tilde{m}}\sum_{j=1}^{\lfloor\frac{\tilde{m}}{4}\rfloor}\Big|\cos\frac{2j\pi}{\tilde{m}}\Big|^n \\
&\leqslant \frac{2}{\tilde{m}}+\frac{4}{\tilde{m}}\sum_{j=1}^{\lfloor\frac{\tilde{m}}{4}\rfloor}\mathrm{e}^{-2\pi^2j^2n/\tilde{m}^2} \\
&< \frac{2}{\tilde{m}}+\frac{4}{\tilde{m}}\int_0^\infty \mathrm{e}^{-2\pi^2x^2n/\tilde{m}^2}\,dx \\
&\leqslant \frac{2}{\tilde{m}}+\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}} \leqslant \frac{2}{m}+\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}.
\end{aligned}$$

Note that in (4.9) we replaced $|\cos\frac{2\pi j}{\tilde{m}}|$ by $|\cos\frac{\pi(\tilde{m}-2j)}{\tilde{m}}|$ when $j > \frac{\tilde{m}}{4}$. □

# 5 Conclusions

From the results obtained in Chapter 3 we derive the following conclusions:

- The polynomial $p_d(z)$ is the "flattest" among the reciprocal polynomials, that is $\kappa_{\text{rec}}(d) = q(p_d^2)$ for all $d \geqslant 1$.
- We have shown that $\kappa(d) = \kappa_{rec}(d)$ for $d = 1, \ldots, 7$. This suggests that reciprocal polynomials may be the "flattest" ones for all $d$.
- We have proved that $\kappa_{\text{rec}}(d) \sim \frac{2}{\pi} \log d$ as $d \to \infty$. It is known that there exists a Newman polynomial $p$ of degree $d$ (see [9]) for which $q(p^2) \leqslant \frac{8}{\pi}(\log d)^2$ for sufficiently large $d$. This means that relaxing the condition for the coefficients does not change the answer that much and allows one to use analytic machinery.

From the results obtained in Chapter 4 we derive the following conclusions:

- We have established the following simple principle - for arbitrary groups $\rho(V_n)$ is maximum when $V_n$ is a multiset that consists of $n$ copies of the same element $g$ that has small order in $G$. In other words - simple random walks on small cyclic subgroups of $G$ concentrate the most.
- Combinatorial methods seem to be much more powerful in establishing bounds in the Littlewood-Offord problem in general groups as opposed to the usual Fourier analytic approach (used by Tiep and Vu [37]). These methods allowed us to obtain optimal bounds for arbitrary groups, whereas the usual Fourier analytics methods are applicable for groups with special structure only and also do not yield optimal bounds.
- For torsion-free groups Erdős's bound still holds. That is, random walks maximizing $\rho(V_n)$ are just simple random walks on a subgroup of $G$ isomorphic to $\mathbb{Z}$.

# Bibliography


[1] Arthur Benjamin, Bob Chen, and Kimberly Kindred, *Sums of Evenly Spaced Binomial Coefficients*, Mathematics Magazine **83** (2010), 370–373.

[2] Peter Borwein, Stephen Choi, and Frank Chu, *An old conjecture of Erdős-Turán on additive bases*, Math. Comp. **75** (2006), 475–484.

[3] Yong-Gao Chen, *On the Erdős-Turán conjecture*, C. R. Math. Acad. Sci. Paris **305** (2012), 933–935.

[4] Yong-Gao Chen and Quan-Hui Yang, *Ruzsa's theorem on Erdős-Turán conjecture*, European J. Combin. **34** (2013), 410–413.

[5] Persi Diaconis, *Random walks on groups: characters and geometry*, London Mathematical Society Lecture Note Series, vol. 1, p. 120–142, Cambridge University Press, 2003.

[6] Gabriel A. Dirac, *Note on a problem in additive number theory*, J. London Math. Soc. **26** (1951), 312–313.

[7] ———, *Some theorems on abstract graphs*, Proc. London Math. Soc **2** (1952), 69–81.

[8] Artūras Dubickas, *Additive basis of positive integers and related problems*, Uniform Distribution Theory **3** (2008), no. 2, 81–90.

[9] ———, *A bases of finite and infinite sets with small representation function*, The Electronic Journal of Combinatorics **19** (2012), no. 6, 16p.

[10] Dainius Dzindzalieta, Tomas Juškevičius, and Matas Šileikis, *Optimal probability inequalities for random walks related to problems in extremal combinatorics*, SIAM J. Discrete Math. **26** (2012), no. 2, 828–837.

[11] Paul Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902.

[12] ———, *On a problem of Sidon in additive number theory*, Acta Sci. Math. **15** (1954), 255–259.

[13] ———, *Problems and results in additive number theory*, Colloque sur la Théorie des Nombres (CBRM), Bruxelles (1956), 127–137.

[14] ———, *Some old and new problems on additive and combinatorial number theory*, Combinatorial Mathematics: Proc. of the Third Intern. Conf. (New York, 1985), New York Acad. Sci., New York, 1989, pp. 181–186.

[15] Paul Erdős and Leo Moser, *Elementary Problems and Solutions*, Amer. Math. Monthly **54** (1947), no. 4, 229–230.

[16] Paul Erdős and Pál Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), no. 4, 212–215.

[17] Georges Grekos, Labib Haddad, Charles Helou, and Jukka Pihko, *On the Erdős-Turán conjecture*, J. Number Theory **102** (2003), 339–352.

[18] Jerrold R. Griggs, *On the distribution of sums of residues*, Bull. Amer. Math. Soc. (N.S.) **28** (1993), no. 2, 329–333.

[19] Gábor Halász, *Estimates for the concentration function of combinatorial number theory and probability*, Period. Math. Hungar. **8** (1977), no. 3-4, 197–211.

[20] Gyula O. H. Katona, *On a conjecture of Erdős and a stronger form of Sperner's theorem*, Studia Sci. Math. Hungar. **1** (1966), 59–63.

[21] Daniel J. Kleitman, *On a lemma of Littlewood and Offord on the distributions on certain sums*, Math. Z. **90** (1965), 251–259.

[22] ———, *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors*, Advances in Math. **5** (1970), 155–157.

[23] Mihail N. Kolountzakis, *An effective additive basis for the integers*, Discrete Math. **145** (1995), 307–313.

[24] Emmanuel Lesigne, *Heads or tails: An introduction to limit threoms in probability*, Student Mathematical Library, vol. 28, pp. 53–58, American Mathematical Society, 2005.

[25] David A. Levin, Yuval Peres, and Elizabeth L. Wilmer, *Markov chains and mixing times*, American Mathematical Society, 2006.

[26] John E. Littlewood and Albert C. Offord, *On the number of real roots of a random algebraic equation. III*, Rec. Math. [Mat. Sbornik] N.S. **12** (1943), no. 53, 277–286.

[27] Hoi H. Nguyen and Van H. Vu, *Optimal Littlewood-Offord theorems*, Advances in Math. **226** (2011), no. 6, 5298–5319.

[28] Robert A. Proctor, *Solution of two difficult combinatorical problems with linear algebra*, Amer. Math. Monthly **89** (1982), no. 10, 721–734.

[29] Imre Z. Ruzsa, *A just basis*, Monatsh. Math. **109** (1990), 145–151.

[30] Csaba Sándor, *A note on a conjecture of Erdős-Turán*, Integers **8** (2008), 4p.

[31] András Sárközy and Endre Szemerédi, *Über ein problem von Erdős und Moser*, Acta Arithmetica **11** (1965), 205–208.

[32] Richard P. Stanley, *Weyl groups, the hard Lefschetz theorem, and the Sperner property*, SIAM J. Algebraic Discrete Methods **1** (1980), 168–184.

[33] Min Tang, *A note on a result of Ruzsa, II*, Bull. Australian Math. Soc. **82** (2010), 340–347.

[34] ———, *On the Erdős-Turán conjecture*, J. Number Theory **150** (2015), 74–80.

[35] Terence Tao and Van H. Vu, *Inverse Littlewood-Offord theorems and the condition number of random matrices*, Annals of Mathematics **169** (2009), no. 2, 595–632.

[36] ———, *A sharp inverse Littlewood-Offord theorem*, Random Structures Algorithms **37** (2010), no. 4, 525–539.

[37] Pham H. Tiep and Van H. Vu, *Non-abelian Littlewood-Offord inequalities*, Advances in Mathematics **302** (2016), 1233–1250.

[38] Quan-Hui Yang, *A generalization of Chen's theorem on the Erdős-Turán conjecture*, Int. J. Number Theory **9** (2013), 1683–1686.