VILNIAUS UNIVERSITETAS

GRAŽVYDAS ŠEMETULSKIS

# Erdős-Turán ir Littlewood-Offord problemų variacijos

Daktaro disertacijos santrauka

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** – prod. dr. Paulius Drungilas (Vilniaus universitetas, fiziniai mokslai, matematika – 01P).

**Disertacija ginama viešame disertacijos gynimo tarybos posedyje:**
**Pirmininkas** – prof. habil. dr. Eugenijus Manstavičius (Vilniaus universitetas, fiziniai mokslai, matematika – 01P).
**Nariai:**
doc. dr. Gintautas Bareikis (Vilniaus universitetas, fiziniai mokslai, matematika – 01P),
prof. habil. dr. Ramūnas Garunkštis (Vilniaus universitetas, fiziniai mokslai, matematika – 01P),
prof. habil. dr. Jonas Šiaulys (Vilniaus universitetas, fiziniai mokslai, matematika – 01P),
dr. Matas Šileikis (Čekijos mokslų akademijos informatikos institutas, fiziniai mokslai, matematika – 01P).

Disertacija bus ginama viešame disertacijos gynimo tarybos posėdyje 2018 m. rugsėjo 21 d. 16 val. 15 min. VU Matematikos ir informatikos fakultete, 102 auditorijoje.
Adresas: Naugarduko g. 24, LT-03225 Vilnius, Lietuva.

Disertacijos santrauka išsiuntinėta 2018 m. liepos 23 d.
Su disertacija galima susipažinti Vilniaus universiteto bibliotekoje ir VU interneto svetainėje adresu: https://www.vu.lt/naujienos/ivykiu-kalendorius.

VILNIUS UNIVERSITY

GRAŽVYDAS ŠEMETULSKIS

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

Summary of 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).

**The dissertation will be defended at the public meeting of the council:**
**Chairman** – prof. habil. dr. Eugenijus Manstavičius (Vilnius University, Physical sciences, Mathematics – 01P).
**Members:**
doc. dr. Gintautas Bareikis (Vilnius University, Physical sciences, Mathematics – 01P),
prof. habil. dr. Ramūnas Garunkštis (Vilnius University, Physical sciences, Mathematics – 01P),
prof. habil. dr. Jonas Šiaulys (Vilnius University, Physical sciences, Mathematics – 01P),
dr. Matas Šileikis (Insitute of Computer Science of the Czech Academy of Sciences, Physical sciences, Mathematics – 01P).

The dissertation will be defended at the public meeting of the council on September 21, 2018 in Vilnius University, Faculty of Mathematics and Informatics, lecture room 102, at 16:15 pm.
Address: Naugarduko st. 24, LT-03225 Vilnius, Lithuania.

The summary of the dissertation was distributed on 23 July, 2018.
The dissertation is available at the library of Vilnius University and online at https://www.vu.lt/naujienos/ivykiu-kalendorius.

# 1 Įžanga

Šis darbas susideda iš dviejų pagrindinių dalių, kuriose yra nagrinėjamos dvi garsių matematinių problemų variacijos. Pirmoje dalyje nagrinėjama Erdős-Turán problemos daugianarinė versija. Joje esantys pagrindiniai rezultatai gauti kartu su vadovu Artūru Dubicku. Antroje dalyje sprendžiama Littlewood-Offord problema apie atsitiktinio klaidžiojimo koncentraciją. Visi joje esantys rezultatai atlikti kartu su Tomu Juškevičiumi.

# 2 Disertacijos mokslinė problema ir tyrimo objektai

## 2.1 Daugianarinė Erdős-Turán problemos versija

1941 m. suformuluota Erdős-Turán hipotezė teigia, kad bet kokiai adityviai bazei $A$ (aibės $A$ porų sumos padengia neneigiamus sveikuosius skaičius, t. y. $\mathbb{N}\cup\{0\} \subset A+A$) reprezentacijų skaičiaus funkcija

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

nėra aprėžta iš viršaus. Kitaip tariant, jei begalinės eilutės

$$f(z) := \sum_{i\in A} z^i, \quad f(z)^2 = \sum_{n=0}^{\infty} r_A(n) z^n$$

tenkina sąlygą $r_A(n) \geqslant 1$ su kiekvienu $n \geqslant 0$, tai $r_A(n)$ negali būti sukoncentruota baigtiniame intervale. Ši garsi hipotezė vis dar lieka atvira. A. Dubickas 2008 m. iškėlė daugianarinę šios problemos versiją. Vietoj eilutės buvo pasiūlyta nagrinėti daugianarį su koeficientais iš aibės $\{0, 1\}$:

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

Toks daugianaris vadinamas *Newman* daugianariu. Tokiu atveju daugianarinė hipotezės versija klausia: ar egzistuoja tokia absoliuti konstanta $C$, kad kiekvienam $d \geqslant 1$ egzistuoja toks $d$-ojo laipsnio Newman daugianaris $p$, kad visi daugianario $p^2$ koeficientai sutelpa į intervalą $[1, C]$? Šis klausimas, kuris taip pat yra atviras, yra viena šios disertacijos mokslinių problemų.

## 2.2 Littlewood-Offord problema

Tegu $V_n = \{g_1, \ldots, g_n\}$ yra multiaibė, sudaryta iš nenulinių realiųjų skaičių. Nagrinėkime atsitiktinį klaidžiojimą

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

čia $X_i$ yra nepriklausomi atsitiktiniai dydžiai, tolygiai pasiskirstę aibėje $\{-v_i, v_i\}$, t. y. $\mathbb{P}(X_i = v_i) = \mathbb{P}(X_i = -v_i) = 1/2$. Koncentracijos tikimybe vadiname dydį

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

Koncentracijos tikimybė yra viena iš centrinių tikimybių teorijos objektų, plačiai tyrinėta daugelio matematikų. J. E. Littlewood ir A. C. Offord, 1949 m. skaičiuodami atsitiktinio daugianario realiųjų šaknų skaičių, įrodė, kad

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

Kiek vėliau, po dvejų metų, P. Erdős pagerino šį rezultatą ir įrodė tikslią nelygybę

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

Šie Littlewood-Offord ir Erdős rezultatai atliko itin reikšmingą vaidmenį tyrinėjant atsitiktinio klaidžiojimo koncentraciją ir padėjo pagrindą daugumai naujų rezultatų. Problema, kai ieškoma koncentracijos tikimybės įverčių, darant skirtingas prielaidas apie elementus $v_1, \ldots, v_n$, dažnai vadinama Littlewood-Offord problema. Tai viena šios disertacijos mokslinių problemų.

# 3 Pagrindiniai uždaviniai

Disertacijoje nagrinėjami šie uždaviniai:

1. **Mažiausias daugianario kvadrato aukštis.** Erdős-Turán problemos versija nagrinėjama platesnei daugianarių klasei. Ieškomi dydžiai $\kappa(d)$ ir $\kappa_{rec}(d)$, čia $\kappa(d)$ – toks mažiausias realusis skaičius, kuriam egzistuoja $d$-ojo laipsnio daugianaris $p(z)$ su neneigiamais realiaisiais koeficientais, kad visi daugianario kvadrato $p(z)^2$ koeficientai priklauso intervalui $[1, \kappa(d)]$. Analogiškai $\kappa_{rec}(d)$ – toks mažiausias realusis skaičius, kad $d$-ojo laipsnio daugianario su neneigiamais realiaisiais koeficientais ir tenkinančio sąlygą $p(z) = z^d p(1/z)$ kvadrato koeficientai priklausytų intervalui $[1, \kappa_{rec}(d)]$. Pagrindinis uždavinys yra atsakyti, ar dydžiai $\kappa_{rec}(d)$ ir $\kappa(d)$ aprėžti iš viršaus. Tiriamas dydžio $\kappa_{rec}(d)$ asimptotinis elgesys. Taip pat siekiama įrodyti, jog dydžiai $\kappa_{rec}(d)$ ir $\kappa(d)$ yra lygūs.

2. **Littlewood-Offord problemos analogas grupėse.** Disertacijoje siekiama išnagrinėti Littlewood-Offord problemos analogą grupėse. Tiksliau, nagrinėti atsitiktinio klaidžiojimo bet kokioje, nebūtinai Abelio, grupėje $G = (G, *)$ koncentracijos tikimybę

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

kai $V_n = \{g_1, \ldots, g_n\}$ yra multiaibė, sudaryta iš grupės $G$ elementų, kurių kiekvieno eilė bent $m \geqslant 2$. Norima įrodyti, jog atsitiktinis klaidžiojimas $X_1 * \cdots * X_n$ grupėje $G$ negali būti labiau koncentruotas negu paprastas atsitiktinis klaidžiojimas tam tikrame cikliniame grupės $G$ pogrupyje. Taip pat siekiama išnagrinėti atvejį, kai nepriklausomi dydžiai $X_i$ gali įgyti daugiau nei dvi reikšmes, ir gauti analogišką Erdős rezultatui įvertį.

# 4 Tyrimų metodika

Trečio skyriaus rezultatai gauti naudojantis idėjomis ir metodais iš šaltinių priklausančių kombinatorikos ir optimizavimo iškilose aibėse sritims. Taikomos klasikinės nelygybės ir Lagranžo daugiklių metodas. Tikslių $\kappa_{rec}(d)$ ir $\kappa(d)$ reikšmių radimas suvedamas į kvadratinės eilės variacinę problemą. Ekstremalaus daugianario koeficientams rasti taikomas generuojančių funkcijų metodas.

Ketvirtojo skyriaus pagrindinių rezultatų įrodymai remiasi idėjomis iš grupių teorijos, grafų teorijos, optimizavimo iškilose aibėse metodų. Tiksliau, 5.2.3 teoremos įrodyme naudojamasi idėja, jog tiesinės funkcijos maksimali reikšmė įgyjama ekstremaliame parametrų aibės taške (šiuo atveju ekstremaliame tikimybiniame mate). Ekstremalių taškų ieškoma remiantis klasikine Dirac teorema apie Hamiltono ciklą grafe. Teoremoms 5.2.1 ir 5.2.3 įrodyti taikomas rekursinis sąryšis, kurį tenkina tam tikras blogiausia atvejį atitinkantis atsitiktinis klaidžiojimas. Įrodant 5.2.1 teoremą naudojama klasikinė Ramus formulė vienodai nutolusių binominių koeficietų sumai rasti. Trigonometrinių funkcijų integralams įvertinti taikomi standartiniai harmoninės analizės metodai.

# 5 Moksliniai rezultatai

## 5.1 Mažiausias daugianario kvadrato aukštis

Pirmiausia apibrėžkime (prisiminkime) keletą pažymėjimų, kurie mums padės aiškiau perteikti rezultatus.

Tegu $\mathcal{P}_d$ yra $d$ laipsnio daugianarių su neneigiamais realiaisiais koeficientais klasė, o $\mathcal{R}_d$ – apgręžiamųjų (angl. *reciprocal*) daugianarių poklasis. Čia daugianaris vadinamas apgręžiamuoju, jei jis tenkiną sąlygą $p(z) = z^d p(1/z)$. Be to, $\kappa(d)$ yra mažiausias realusis skaičius, kuriam egzistuoja toks daugianaris $p(z) \in \mathcal{P}_d$, kad visi daugianario $p(z)^2$ koeficientai priklauso intervalui $[1, \kappa(d)]$. Analogiškai $\kappa_{\mathrm{rec}}(d)$ – mažiausias realusis skaičius, kuriam egzistuoja toks daugianaris $p(z) \in \mathcal{R}_d$, kad visi daugianario $p(z)^2$ koeficientai priklauso intervalui $[1, \kappa_{\mathrm{rec}}(d)]$.

Apibrėžkime daugianario $p(z) = \sum_{j=0}^{d} a_j z^j \in \mathcal{P}_d$ aukštį kaip didžiausio ir mažiausio koeficientų santykį:

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

Jei nenulinio daugianario $p$ bent vienas iš koeficientų yra nulis, tuomet tarsime, jog $q(p) = +\infty$. Nesunku įsitikinti, kad

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

ir

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

Sakysime, jog daugianaris yra plokščias, jei jo aukštis $q(p)$ yra mažas.

A. Dubickas 2008 m. numatė daugianarį

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

kaip turintį mažiausią galimą kvadrato aukštį $q(p^2)$ iš visų klasės $\mathcal{P}_d$ daugianarių. Čia koeficientai $y_n$ apibrėžiami lygtimis:

$$2y_{2k}y_0 + 2y_{2k-1}y_1 + \cdots + 2y_{k+1}y_{k-1} + y_k^2 = 1, \tag{3}$$

kai $n = 2k$, $k \geqslant 0$, ir

$$2y_{2k+1}y_0 + 2y_{2k}y_1 + \cdots + 2y_{k+2}y_{k-1} + 2y_{k+1}y_k = 1, \tag{4}$$

kai $n = 2k+1$, $k \geqslant 0$. Pastebėkime, jog (3) ir (4) lygtys iš pirmo žvilgsnio neužtikrina, jog $y_k \geqslant 0$ visiems $k$, tačiau tuo įsitikinsime iš toliau pateikiamų rezultatų.

**5.1.1 teorema.** *Kiekvienam $d \geqslant 1$ yra teisinga lygybė $\kappa_{rec}(d) = q(p_d^2)$.*

Šis rezultatas parodo, jog (2) daugianaris turi plokščiausią kvadratą tarp apgręžiamų daugianarių, t. y. daugianarių iš klasės $\mathcal{R}_d$. Kita teorema teigia, jog šis daugianaris, kai laipsnis mažas, $p_d$ yra plokščiausias ir klasėje $\mathcal{P}_d$.

**5.1.2 teorema.** *Jei $d \in \{1, \ldots, 7\}$, tai $\kappa(d) = q(p_d^2)$.*

Racionalių skaičių sekos $y_n$, apibrėžtos (3) ir (4) lygtimis, reikšmes galima užrašyti tiksliai, naudojantis centriniais binominiais koeficientais.

**5.1.3 teorema.** *Kiekvienam $n \geqslant 0$ yra teisinga lygybė $y_n = 2^{-2n}\binom{2n}{n}$.*

Pastebėkim, jog tai užtikrina, kad $p_d \in \mathcal{P}_d$. Iš toliau pateiktos teoremos matyti kiek plokščias yra daugianario $p_d$ kvadratas.

**5.1.4 teorema.** *Jei $d$ yra nelyginis natūralusis skaičius, tuomet galioja lygybė*

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

*Jei $d$ yra lyginis natūralusis skaičius, tai*

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

*Čia, $y_n = 2^{-2n}\binom{2n}{n}$ ir $q(p_d^2) \sim \frac{2}{\pi}\log d$, kai $d \to \infty$.*

Taigi nesvarbu, kad nagrinėjami daugianariai turi neneigiamus realius koeficientus, dydis $\kappa_{\mathrm{rec}}(d)$ auga pakankamai greitai ir nėra aprėžtas iš viršaus. Be to, 5.1.2 teorema sufleruoja, jog $\kappa(d) = \kappa_{\mathrm{rec}}(d)$ visiems $d \geqslant 1$. Tai yra truputį netikėta, nes Newman daugianario atveju situacija yra kitokia. A. Dubickas 2012 m. parodė, jog kiekvienam apgręžiamam $d$-ojo laipsnio Newman daugianariui $p$ galioja nelygybė

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

Kita vertus, naudodamasis tikimybiniu metodu A. Dubickas įrodė, kad kiekvienam $\varepsilon > 0$ ir $d > d_0(\varepsilon)$ egzistuoja $d$-ojo laipsnio Newman daugianaris, kuriam teisinga nelygybė

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

Įdomu dar ir tai, jog nagrinėjant platesnę daugianarių klasę, prarandama pakankamai nedaug.

## 5.2 Littlewood-Offord nelygybės grupėje

Tegul $V_n = \{g_1, \dots, g_n\}$ yra multiaibė, sudaryta iš netrivialių (ne grupės vienetų) grupės (nebūtinai Abelio) $G = (G, *)$ elementų. Nagrinėkime nepriklausomų atsitiktinių dydžių $X_i$ rinkinį, kurių kiekvienas tolygiai pasiskirstęs dviejų elementų aibėje $\{g_i^{-1}, g_i\}$. Tokiu atveju atsitiktinio klaidžiojimo koncentracijos tikimybė $\rho(V_n)$ yra apibrėžiama lygybe

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

P. H. Tiep ir V. H. Vu pirmieji pradėjo nagrinėti atsitiktinio klaidžiojimo tikimybę grupėse, kurios nėra Abelio. Jiems 2016 m. pavyko parodyti, kad jei $V_n = \{g_1, \dots, g_n\}$ yra multiaibė, sudaryta iš matricų grupės $G = GL_d(\mathbb{C})$ elementų, kurių kiekvieno eilė bent $m \geqslant 2$, tai

$$\rho(V_n) \leqslant 141 \max\left\{\frac{1}{m}, \frac{1}{\sqrt{n}}\right\}. \tag{5}$$

Taip pat analogišką nelygybę jiems pavyko įrodyti, kai $G = GL_d(p)$. Kad įrodytų šią nelygybę, Tiep ir Vu pasinaudojo reprezentacijų teorijos, adityviosios kombonatorikos, tiesinės algebros ir analitinės skaičių teorijos metodais.

Disertacijoje gaunamas optimalus viršutinis įvertis koncentracijos tikimybei $\rho(V_n)$, iš kurios išplaukia, jog net stipresnis už Tiep ir Vu (5) neglybę įvertis yra teisingas bet kokioje grupėje $G$.

Prieš suformuluodami pagrindinę, teoremą apibrėžkime keletą žymėjimų. Pažymėkime $(a, b]_m$ ir $[a, b]_m$ sveikųjų skaičių iš atitinkamų intervalų $(a, b]$ ir $[a, b]$ dalybos iš $m$ liekanų aibes. Tiksliau,

$$(a, b]_m := \{x \mod m \mid x \in (a, b] \cap \mathbb{Z}\}.$$

Tegul $|g|$ yra grupės elemento $g$ eilė ir $\tilde{m}$ – mažiausias lyginis skaičius, didesnis už $m$, t. y. $\tilde{m} = 2\lceil \frac{m}{2} \rceil$.

**5.2.1 teorema.** *Tegu $g_1, \dots, g_n$ yra grupės $G$ elementai, kurių kiekvieno eilė tenkina nelygybę $|g_i| \geqslant m \geqslant 2$. Tegul $X_1, \dots, X_n$ yra nepriklausomi atsitiktiniai dydžiai, tolygiai pasiskirstę aibėje $\{g_i^{-1}, g_i\}$. Tada kiekvienai aibei $A \subset G$, kurios dydis $|A| = k$, galioja nelygybė*

$$\mathbb{P}\left(X_1 * \cdots * X_n \in A\right) \leqslant \mathbb{P}\left(\varepsilon_1 + \cdots + \varepsilon_n \in (-k, k]_{\tilde{m}}\right), \tag{6}$$

*čia $\varepsilon_i$ yra nepriklausomi atsitiktiniai dydžiai, tolygiai pasiskirstę aibėje $\{-1, 1\} \subset \mathbb{Z}_{\tilde{m}}$.*

Jei grupė $G$ turi $\tilde{m}$-osios eilės elementą, tai 5.2.1 teoremos nelygybė yra optimali. Tuo nesunku įsitikinti paėmus grupę $G = GL_d(\mathbb{C})$ ir elementus $g_i = \mathrm{e}^{\frac{2\pi i}{\tilde{m}}}\,\mathbb{I}_d$, $i = 1 \dots n$.

Seka sumų, esančių dešiniojoje (6) nelygybės pusėje, yra periodinė Markovo grandinė, todėl nekonverguoja, kai $n \to \infty$. Tačiau yra gerai žinoma, jog atskiru atveju, kai apribojamas $n$ lyginumas, pastaroji seka konverguoja. Tiksliau, jei $m \in \mathbb{N}$ ir $n \to \infty$, tai visiems $l \in \mathbb{Z}_{\tilde{m}}$, kurių lyginumas sutampa su $n$, yra teisinga asimptotika

$$\mathbb{P}\left(\varepsilon_1 + \dots + \varepsilon_n = l\right) = \frac{2}{\tilde{m}} + o(1). \tag{7}$$

Tai parodo (6) nelygybės dešinėje esančios dydžio asimptotinį elgesį, kai $|A| = 1$.

Iš 5.2.1 teoremos gaunamas daug stipresnis Tiep ir Vu nelygybės analogas.

**5.2.2 išvada.** *Tegul $V_n = \{g_1, \dots, g_n\}$ yra grupės $G$ elementai, tenkinantys nelygybę $|g_i| \geqslant m \geqslant 2$. Tada*

$$\rho(V_n) \leqslant \frac{2}{m} + \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}} \leqslant 3\max\{\frac{1}{m}, \frac{1}{\sqrt{n}}\}. \tag{8}$$

Išraiškoje $\frac{2}{\tilde{m}} + \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}$ abi konstantos yra optimalios. Iš tikro, kai $m, n \to \infty$ ir $n \gg m^2$, pastarojoje išraiškoje dominuoja narys $\frac{2}{\tilde{m}}$. Remdamiesi (7) lygybe gauname, jog konstanta 2 negali būti sumažinta. Jei $m, n \to \infty$ ir $n < m$, tuomet dominuoja narys $\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}$. Tuo, kad konstanta prie pastarojo reiškinio taip pat yra optimali galima įsitikinti paėmus $V_n = \{g, \dots, g\}$, čia $g$ yra bet koks $\tilde{m}$-osios eilės elementas. Tokiu atveju

$$\rho(V_n) = \mathbb{P}\left(\varepsilon_1 + \dots + \varepsilon_n \in (-1, 1]_{\tilde{m}}\right) = \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = (1 + o(1))\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}. \tag{9}$$

Čia tiksli asimptotinė (9) išraiška išplaukia iš Stirling formulės arba lokalios ribinės teoremos.

Yra žinoma, jog paprastas atsitiktinis klaidžiojimas grupėje $\mathbb{Z}_m$, kai $m$ yra nelyginis, konverguoja į tolygų pasiskirstymą visoje grupėje $\mathbb{Z}_m$. Iš (7) matome, jog tokiu atveju paprastas atsitiktinis klaidžiojimas grupėje $\mathbb{Z}_{\tilde{m}} = \mathbb{Z}_{m+1}$ gali geriau maksimizuoti reikšmę kairiojoje (6) nelygybės pusėje.

Jei grupėje nėra elemento, kurio eilė $\tilde{m}$, tai iš 5.2.1 teoremos tikslios nelygybės negaunname. Taip atsitinka visose grupėse, kurios neturi lyginės eilės elementų, pavyzdžiui, $G = \mathbb{Z}_m^q$, čia $m$ yra nelyginis skaičius. Iš kitos teoremos gaunamas tikslus įvertis, kai grupėje nėra lyginės eilės elementų.

Pasižymėkime

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

kai $k \geqslant 1$ ir $I_{n,0}^m = \emptyset$.

**5.2.3 teorema.** *Tegul $X_1, \dots, X_n$ yra tokie diskretūs nepriklausomi atsitiktiniai dydžiai, įgyjantys reikšmes grupėje $G$, kad kiekvienam $X_i$ galioja nelygybė*

$$\sup_{g \in G} \mathbb{P}(X_i = g) \leqslant \frac{1}{2}. \tag{10}$$

*Taip pat tarkime, kad grupėje $G$ nėra lyginės eilės elementų, o mažiausia netrivialaus elemento eilė egzistuoja ir yra lygi $m \geqslant 3$. Tada bet kokiai $k$ elementų aibei $A \subset G$ galioja nelygybė*

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

*čia $\tau_i$ yra nepriklausomi atsitiktiniai dydžiai, tolygiai pasiskirstę aibėje $\{0,1\} \subset \mathbb{Z}_m$.*

Sumos $\tau_1 + \cdots + \tau_n$ skirstinys yra asimptotiškai tolygiai pasiskirstęs grupėje $\mathbb{Z}_m$, todėl

$$\mathbb{P}(X_1 * \cdots * X_n = g) \leqslant \frac{1}{m} + o(1).$$

Atveju, kai grupėje $G$ nėra baigtinės eilės elementų, Erdős (1) įvertis vis tiek galioja.

**5.2.4 teorema.** *Tegul galioja 5.2.3 teoremos sąlygos ir grupėje $G$ nėra baigtinės eilės elementų. Tada bet kokiai $k$ elementų aibei $A \subset G$ teisinga nelygybė*

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

*čia $\varepsilon_i$ yra nepriklausomi atsitiktiniai dydžiai, tolygiai pasiskirstę aibėje $\{-1, 1\}$. Atskiru atveju kiekvienam $g \in G$ turime*

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

# 6 Darbo mokslinis naujumas ir aktualumas

Abi disertacijoje nagrinėjamos mokslinės problemos yra aktyviai sprendžiamos ir rutuliojamos daugelio matematikų.

Nagrinėjama Erdős-Turán problemos daugianarinė versija yra susijusi su viena garsiausių adityviosios kombinatorikos hipotezių. Ši hipotezė, paties P. Erdős įvertinta 500 USD, yra rutuliota garsių matematikų, tačiau išlieka neišspręsta iki šiol.

Kita disertacijoje nagrinėjama Littlewood-Offord problema yra fundamentali tikimybių teorijoje. Littlewood-Offord nelygybės yra vienas pagrindinių įrankių tyrinėjant atsitiktinių matricų savybes. Vienas iš tiesioginių jos taikymų leidžia įvertinti tikimybę, jog atsitiktinė nepriklausomų ženklų matrica yra išsigimusi.

Disertacijoje pateikiami rezultatai yra nauji. Jie paskelbti recenzuojamuose žurnaluose (žr. skyrių „Pagrindinės publikacijos”) ir pristatyti konferencijose (žr. skyrių „Rezultatų sklaida”).

# 7 Darbo struktūra ir apimtis

Disertacija parašyta anglų kalba. Disertaciją sudaro 6 skyriai: įvadas, literatūros apžvalga, du skyriai su pagrindinių rezultatų formuluotėmis ir įrodymais, išvados ir literatūros sąrašas. Bendra darbo apimtis yra 54 puslapiai.

# 8 Pagrindinės publikacijos

Disertacijos rezultatai publikuojami 3 moksliniuose straipsniuose:

- 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.

# 9 Rezultatų sklaida

Disertacijoje gauti rezultatai buvo pristatyti šiose mokslinėse konferencijose ir seminaruose:

- *27th Journées Arithmétiques*, Vilnius, 2011 m. birželio 27 d. – liepos 1 d.
- *55-oji Lietuvos matematikų draugijos konferencija*, Kaunas, 2018 m. birželio 18–19 d.
- *12th International Vilnius Conference on Probability Theory and Mathematical Statistics*, Vilnius, 2018 m. liepos 2–6 d.
- *Skaičių teorijos seminaras*, Vilniaus universiteto Matematikos ir informatikos fakultetas, Vilnius, 2018 m. kovo 12 d.
- *Ekstremalių grafų teorijos grupės seminaras*, Čekijos mokslų akademijos informatikos institutas, Praha, 2018 m. gegužės 25 d.

# 10 Išvados

Disertacijoje gautos tokios išvados:

- Daugianaris $p_d(z)$ turi plokščiausią kvadratą tarp apgręžiamų daugianarių su neneigiamais koeficientais, t. y. $\kappa_{\mathrm{rec}}(d) = q(p_d^2)$ visiems $d \geqslant 1$.

- Teisinga lygybė $\kappa(d) = \kappa_{rec}(d)$, kai $d = 1, \ldots, 7$. Tai leidžia manyti, jog nagrinėjant daugianarius su neneigiamais realiaisiais koeficientais plokščiausias daugianaris yra taip pat ir apgręžiamas.

- Mažiausias apgręžiamo $d$-ojo laipsnio daugianario kvadrato aukštis $\kappa_{rec}(d)$ asimptotikai lygus $\frac{2}{\pi}\log d$, kai $d \to \infty$. A. Dubickas yra parodęs, jog egzistuoja $d$-ojo laipsnio Newman daugianaris $p$, kuriam $q(p^2) \leqslant \frac{8}{\pi}(\log d)^2$, kai $d$ pakankamai didelis. Tai parodo, jog nagrinėjant platesnę klasę daugianarių (su realiais koeficientais) prarandama nedaug. Tai padidina galimų analizės metodų pasirinkimą.

- Koncentracijos tikimybė $\rho(V_n)$ įgyja didžiausią reikšmę, čia $V_n = \{g, \ldots, g\}$, kur $g$ yra mažiausios eilės grupės $G$ elementas. Trumpai tariant – paprastas atsitiktinis klaidžiojimas mažame cikliniame pogrupyje yra labiausiai koncentruotas klaidžiojimas.

- Kombinatoriniais metodais gaunami tikslesni ir bendresni rezultatai sprendžiant Littlewood-Offord problemą grupėse, nei dažniausiai taikoma Furjė analizė.

- Grupėms, neturinčioms baigtinės eilės elementų, Erdős (1) įvertis taip pat galioja. Tiksliau, atsitiktinis klaidžiojimas, kuris maksimizuoja $\rho(V_n)$, yra paprastas atsitiktinis klaidžiojimas pogrupyje, kuris izomorfiškas $(\mathbb{Z}, +)$.

# 11 Summary

This thesis is focused of two problems - one in additive combinatorics and one in combinatorial probability. The first problem is a polynomial version of the famous Erdős-Turán problem concerning the growth of the representation function of additive bases of integers. The second problem is a variation of the Littlewood-Offord problem in arbitrary groups.

The thesis consists of the introduction, 3 chapters, conclusions and bibliography.

In Chapters 1-2 a detailed description of the problems that are dealt with in the thesis is provided and the relevant literature discussed in order to put these problems in the proper context.

In the Chapter 3 we deal with the polynomial version of the Erdős-Turán problem for the reciprocal polynomials with non-negative coefficients. We prove that for reciprocal polynomials of degree $d$ whose squares have all coefficients greater than 1, the quotient of the largest and the smallest coefficients is at least $(\frac{2}{\pi} + o(1)) \log d$. We find the worst case polynomial and an explicit formula for its coefficients. Furthermore, we provide an optimal bound for the aforementioned quotient without the reciprocity condition imposed on the polynomials for $d = 1, \ldots, 7$. It turns out that, perhaps surprisingly, the worst case polynomial is the same reciprocal polynomial as it was in the more restrictive reciprocal setting. This result fact tempts us to the conjecture that the latter phenomenon should also be true for $d \geqslant 8$.

In Chapter 4 we deal with a version of the classical Littlewood-Offod problem in arbitrary groups. Such research was started by Tiep and Vu who gave an asymptotically sharp bound in the case of certain matrix groups. We obtain an optimal bound for this problem in arbitrary groups. It turns out that for arbitrary groups $G$ the worst case random walks are just simple random walks on a certain cyclic subgroups of $G$. Our approach simplifies and extends the results of Tiep and Vu which is mostly due to the fact that instead of using Fourier analysis we used a purely combinatorial argument.

# 12 Trumpos žinios apie autorių

**Išsilavinimas**

**2008 m.** Kelmės Aukuro vidurinės mokyklos absolventas.

**2011 m.** Vilniaus universiteto matematikos bakalauras.

**2013 m.** Vilniaus universiteto matematikos magistras (*Magna cum laude*).

**Mokslinio darbo patirtis**

**2010–2012 m.** Vilniaus universiteto laborantas

**2014–2015 m.** Vilniaus universiteto jaunesnysis mokslinis darbuotojas

**Pedagoginio darbo patirtis**

**2013–2016 m.** Vilniaus universiteto asistentas