VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
MATEMATIKOS MAGISTRANTŪROS STUDIJŲ PROGRAMA

Multiplikatyvusis nepriklausomumas

Multiplicative independence

Baigiamasis magistro darbas

Atliko: Leonardas Mačiulis
VU el. p.: leonardas.maciulis@mif.stud.vu.lt

Vadovas: prof. dr. Paulius Drungilas

Vilnius
2023

Santrauka

Šiame darbe tiriamas multiplikatyviai priklausomų ir nepriklausomų skaičių dažnis aprašant galimus algoritmus jam skaičiuoti, pateikiamas multiplikatyviojo nepriklausomumo taikymas tirti aritmetikos teiginių įrodomumą Cobham teorema, bei apžvelgiamas skaičiavimo sistemos $\mathbb{Z}[\zeta_k]$ bazių multiplikatyviojo nepriklausomumo įrodymas.

Raktiniai žodžiai: multiplikatyvusis nepriklausomumas, algebriniai skaičiai, Büchi aritmetika, Cobham teorema, kanoninės skaičiavimo sistemos

Summary

In this work, the frequency of multiplicatively dependent and independent algebraic numbers is investigated by providing possible algorithms for its calculation. One application of multiplicative independence, namely its use for proving the algorithmic decidability of logical sentences in formal arithmetic using Cobham's theorem, is presented, along with an overview of a proof of multiplicative independence for bases of a number system in $\mathbb{Z}[\zeta_k]$.

Keywords: multiplicative independence, algebraic numbers, Büchi arithmetic, Cobham's theorem, canonical number systems

Turinys

Įvadas

Nenuliniai kompleksiniai skaičiai $z_1, z_2, \ldots z_k$ vadinami multiplikatyviai priklausomais, jei egzistuoja tokie sveikieji skaičiai $x_1, x_2, \ldots x_k$, kurių nors vienas nelygus nuliui, kad

$$z_1^{x_1} z_2^{x_2} \ldots z_k^{x_k} = 1.$$

Jei tokių $x_1, x_2, \ldots x_k$ neegzistuoja, $z_1, z_2, \ldots z_k$ vadinami multiplikatyviai nepriklausomais. Pavyzdžiui, natūralieji skaičiai $2, 3, 12$ yra priklausomi, nes $2^{-2} \cdot 3^{-1} \cdot 12^1 = 1$, tačiau $2, 12$ yra nepriklausomi. Kompleksiniai skaičiai $\exp(2\pi i/3), \exp(2\pi i/5)$ priklausomi, nes $(\exp(2\pi i/3))^{-3} \cdot (\exp(2\pi i/5))^5 = 1$, tuo tarpu $\exp\left(\sqrt{3} \cdot 2\pi i/3\right), \exp\left(\sqrt{5} \cdot 2\pi i/5\right)$ — nepriklausomi.

Baronėnas [1] magistro baigiamajame darbe apžvelgė kompleksinių skaičių bazių multiplikatyviojo nepriklausomumo įrodymą, įrodė, kad skaičiai $m-\alpha, n-\alpha$ yra multiplikatyviai nepriklausomi, jei $m, n \in \mathbb{Z}$, $m \neq n$, α — realusis algebrinis, bet ne sveikasis algebrinis skaičius ir $2\alpha \notin \mathbb{Z}$, bei tyrė sveikųjų algebrinių skaičių atvejį. Šiame baigiamajame darbe pristatomos multiplikatyviojo nepriklausomumo savybės ir pritaikymo būdai. Baigiamajame darbe aptariama, kokiu dažniu natūralieji ir algebriniai skaičiai būna multiplikatyviai priklausomi ir nepriklausomi, apibrėžiamas formalus algoritmas natūraliųjų skaičių aibių nepriklausomumui tikrinti bei multiplikatyviai nepriklausomų skaičių derinių intervale skaičiui skaičiuoti, galimas algoritmas algebrinių skaičių nepriklausomumui tikrinti. Pateikiamas multiplikatyviojo nepriklausomumo taikymas tirti teiginių aritmetikose įrodomumą Cobham teorema bei apžvelgiamas skaičiavimo sistemos $\mathbb{Z}[\zeta_k]$ bazių multiplikatyviojo nepriklausomumo įrodymas.

1. Multiplikatyviai nepriklausomų natūraliųjų skaičių derinių skaičiavimas

Multiplikatyviojo priklausomumo apibrėžimas nerodo, kiek skaičių sekų yra multiplikatyviai priklausomos palyginus su multiplikatyviai nepriklausomomis. Norint palyginti šias aibes galima nagrinėti paprastą pavyzdį, kai skaičiai yra natūralieji intervale $[a, b]$. Kadangi apibrėžime naudojama daugyba komutatyvi, galima skaičiuoti multiplikatyviai nepriklausomų k ilgio derinių iš intervalo skaičių. Iš viso yra C^k_{b-a+1} k ilgio derinių, kurie yra arba priklausomi, arba nepriklausomi, todėl pažymėjus multiplikatyviai nepriklausomų k ilgio derinių skaičių S_k, multiplikatyviai priklausomų to paties ilgio derinių skaičių D_k gaunama, kad

$$C^k_{b-a+1} = S_k + D_k.$$

Vienas iš būdų skaičiuoti nepriklausomus derinius yra perrinkimas kompiuteriu, tačiau derinių skaičius net mažiems intervalams yra didelis. Perrinkimui taip pat reikia algoritmo, gebančio patikrinti skaičių multiplikatyvųjį nepriklausomumą. Algoritmo veikimą galima šiek tiek pagreitinti pasinaudojant šakojimo ir ribojimo (*Branch and Bound*) technika (žr. [14]), tuo tarpu natūraliųjų skaičių nepriklausomumą galima tikrinti pasinaudojant pirminiais dauginamaisiais.

Bet kokiam pirminiam skaičiui p lygybė $p^x p^y = 1$ tada ir tik tada, kai $x = -y$, tuo tarpu skirtingiems pirminiams p_1, p_2 lygybė $p_1^x p_2^y = 1$ tada ir tik tada, kai $x = y = 0$. Taigi, bet koks skirtingų pirminių skaičių derinys yra multiplikatyviai nepriklausomas, o sudėtiniai skaičiai lygybėje $z_1^{x_1} z_2^{x_2} \dots z_m^{x_m} = 1$ turi pirminius dauginamuosius, kurių laipsnių suma lygi nuliui. Remiantis šia idėja, derinys

$$z_1^{x_1} z_2^{x_2} \dots z_m^{x_m} = 1$$

išskaidomas pirminiais dauginamaisiais

$$\begin{array}{lcccccc} z_1 & = & p_1^{y_{11}} & p_2^{y_{12}} & \dots & p_n^{y_{1n}}, \\ z_2 & = & p_1^{y_{21}} & p_2^{y_{22}} & \dots & p_n^{y_{2n}}, \\ \dots & \dots & \dots & \dots & \dots & \dots \\ z_m & = & p_1^{y_{m1}} & p_2^{y_{m2}} & \dots & p_n^{y_{mn}}, \end{array}$$

kur kiekvienam $j = 1, 2, \dots n$ bent vienas iš $y_{1j}, y_{2j}, \dots y_{mj}$ nelygus nuliui. Derinys multiplikatyviai nepriklausomas tada ir tik tada, kai tiesinė homogeninė lygčių sistema

$$\begin{array}{ccccccccccc} y_{11}x_1 & + & y_{21}x_2 & + & \dots & + & y_{m1}x_m & = & 0, \\ y_{12}x_1 & + & y_{22}x_2 & + & \dots & + & y_{m2}x_m & = & 0, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ y_{1n}x_1 & + & y_{2n}x_2 & + & \dots & + & y_{mn}x_m & = & 0 \end{array}$$

neturi netrivialių sveikųjų sprendinių $x_1, x_2, \dots x_m$. Visi koeficientai sveikieji, todėl lygčių sistemos sprendiniai yra racionalūs, tad subendravardiklinus ir padauginus iš bendrojo vardiklio gaunamas sveikasis sprendinys. Jei egzistuoja netrivialus sprendinys, egzistuoja ir sveikasis netrivialus sprendinys, todėl užtenka patikrinti, ar lygčių sistemą atitinkančios koeficientų matricos rangas mažesnis už m. Multiplikatyviojo nepriklausomumo tikrinimą įgyvendina 1 algoritmas.

Paprasčiausiu būdu perrenkant visus k ilgio derinius ir skaičiuojant multiplikatyviai nepriklausomus tektų perrinkti visus C^k_{b-a+1} derinių. Pastebint, kad jei

$$z_1^{x_1} z_2^{x_2} \dots z_k^{x_k} = 1$$

1 algoritmas. Multiplikatyviojo nepriklausomumo tikrinimas.

Įvestis: s — natūraliųjų skaičių aibė
Išvestis: loginis kintamasis, reiškiantis aibės multiplikatyvųjį nepriklausomumą

```
funkcija NEPRIKLAUSOMAS(s)
    dauginamieji — sekų seka
    rodikliai — sekų seka
    kiekvienam i = 1, 2, ... |s| atlikti
        dauginamieji_i ← s_i pirminių dauginamųjų seka
        rodikliai_i ← s_i pirminių dauginamųjų rodiklių seka
    baigti ciklą
    dauginamųjų aibė ← ∅
    kiekvienam d ∈ dauginamieji atlikti
        dauginamųjų aibė ← dauginamųjų aibė ∪ d
    baigti ciklą
    M — |dauginamųjų aibė| × |s| matmenų nulių matrica
    kiekvienam i = 1, 2, ... |dauginamųjų aibė| atlikti
        kiekvienam j = 1, 2, ... |dauginamieji| atlikti
            jei dauginamųjų aibė_i ∈ dauginamieji_j tuomet
                M_ij ← rodikliai_ji
            baigti sąlygą
        baigti ciklą
    baigti ciklą
    grąžinti ¬(rang(M) < |dauginamųjų aibė|)
baigti funkciją
```

turi netrivialų sveikąjį sprendinį $x_1, x_2, \dots x_k$ ir k ilgio derinys yra multiplikatyviai priklausomas, tai visiems $m > k$

$$z_1^{x_1} z_2^{x_2} \dots z_k^{x_k} z_{k+1}^{x_{k+1}} z_{k+2}^{x_{k+2}} \dots z_m^{x_m} = 1$$

turi netrivialų sprendinį $x_1, x_2, \dots x_k, x_{k+1} = x_{k+2} = \dots = x_m = 0$, todėl deriniai, kurių poaibis yra priklausomas derinys, yra priklausomi. Be to, visi deriniai, kuriuose yra 1, turi netrivialų sprendinį ir yra priklausomi. Taigi, perrenkant nebūtina perrinkti derinių, kuriuose yra jau patikrinti priklausomi deriniai. Šakojimo ir ribojimo (*Branch and Bound*) technika pagrįsti algoritmai perrenka dalinius uždavinius, ir nebeperrenka dalies padidintų dalinių uždavinių. Šiuo atveju galima perrinkti $k = 2$ ilgio derinius, suskaičiuoti nepriklausomus, atmesti priklausomus, tuomet perrinkti $k + 1$ ilgio derinius, sudarytus iš nepriklausomų k ilgio derinių ir skaičių $[a, b] \setminus \{1\}$. Kartojant gaunamas multiplikatyviai nepriklausomų derinių skaičius visiems $1 \leq k \leq b - a + 1$. Ši mintis įgyvendinta 2 algoritmu.

Nors 2 algoritmas yra greitesnis nei paprastas perrinkimas, jo laiko sudėtingumas išlieka didelis, o atminties sudėtingumas padidėja. Žinant, kiek užtruks k ilgio derinių perrinkimas būtų galima išspręsti multiplikatyviai nepriklausomų derinių skaičiavimo uždavinį laiką lyginant su visų k ilgio derinių perrinkimo laiku, todėl nelengva įvertinti tikslų algoritmo sudėtingumą.

Negalint greitai rasti tikslaus multiplikatyviai nepriklausomų derinių skaičiaus galima bandyti jį įvertinti iš viršaus ir iš apačios. Vieną viršutinę ribą nusako multiplikatyviai priklausomi deriniai, kuriuose yra 1 arba du to paties skaičiaus laipsniai. Apatinę ribą nurodo multiplikatyviai nepriklausomi deriniai, kuriuose kiekvienas skaičius turi bent vieną pirminį dauginamąjį, kurio neturi kiti skaičiai derinyje.

Kiekvienas $k - 1$ ilgio derinys gali būti paverstas priklausomu k ilgio deriniu pridėjus 1,

2 algoritmas. Multiplikatyviai nepriklausomų derinių skaičiavimo algoritmas.

Įvestis: $[a, b]$ — natūraliųjų skaičių intervalas
Išvestis: y_k — k ilgio multiplikatyviai nepriklausomų derinių skaičius

```
funkcija SKAIČIUOTI([a, b])
    y ← (0, ... 0)
    deriniai ← {{a}, {a + 1}, ... {b}}
    kol |deriniai| > 0 atlikti
        nepriklausomi deriniai ← ∅
        kiekvienam s ∈ deriniai atlikti
            jei NEPRIKLAUSOMAS(s) tuomet
                y_|s| ← y_|s| + 1
                nepriklausomi deriniai ← nepriklausomi deriniai ∪ s
            baigti sąlygą
        baigti ciklą
        deriniai ← ∅
        kiekvienam s ∈ deriniai atlikti
            kiekvienam x ∈ [a, b] \ {1} atlikti
                jei |s ∪ {x}| > |s| tuomet
                    deriniai ← deriniai ∪ s
                baigti sąlygą
            baigti ciklą
        baigti ciklą
    baigti ciklą
    grąžinti y
baigti funkciją
```

į šį skaičių įeina ir priklausomas derinys $\{1\}$. Suskaičiavus skirtingų laipsnių sekas ir jų elementų skaičių intervale $[a, b]$ gaunami visi multiplikatyviai priklausomi deriniai, sudaryti iš i tam tikro laipsnio sekos elementų ir $k - i$ kitų skaičių, neskaitant jau įskaičiuotų derinių su ankstesniais laipsniais. Formaliai priklausomų derinių skaičiaus apatinis įvertis $\underline{D_k} \leq D_k$ užrašomas kaip

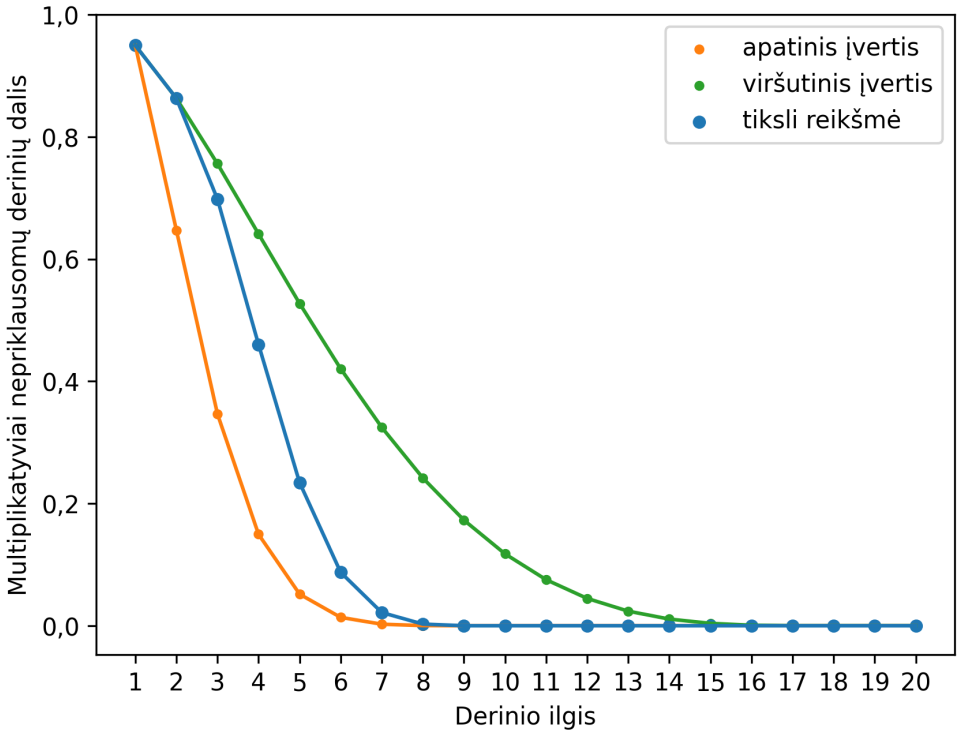
$$Y = \left(y = \left(i^j : j = 1, 2, \dots \lceil \log_i b \rceil\right) \cap [a, b] : y \neq \varnothing, i = 2, 3, \dots b\right),$$
$$\underline{D_k} = \sum_{y_l \in Y} \sum_{i=2}^{\min(k, |y_l|)} C^i_{|y_l|} C^{k-i}_{b-a+1-|y_l|-\sum_{v=1}^{l-1}|y_l|} + \mathbb{1}_{1 \in [a,b]} C^{k-1}_{b-a+1},$$

tuomet multiplikatyviai nepriklausomų derinių skaičius

$$S_k \leq \overline{S_k} = C^k_{b-a+1} - \underline{D_k}.$$

Kadangi pirminiai skaičiai tarpusavyje multiplikatyviai nepriklausomi, jei kiekvienas skaičius derinyje turi tik jam būdingą pirminį dauginamąjį, derinys yra multiplikatyviai nepriklausomas. Tada nepriklausomų derinių skaičiaus apatinis įvertis $\underline{S_k} \leq S_k$ užrašomas kaip

$$Y = \left(y = \left(pi : i = 1, p, p+1, \dots \left\lceil \frac{b}{p} \right\rceil\right) \cap [a, b] : y \neq \varnothing, p = 2, 3, \dots b, p \text{ — pirminis}\right),$$
$$\underline{S_k} = \sum_{\substack{Y_k \subseteq Y \\ |Y_k| = k}} \prod_{y \in Y_k} |y|.$$



1 pav. Tikimybė, kad natūraliųjų skaičių iš $[1, 20]$ derinys be pasikartojimų bus multiplikatyviai nepriklausomas. Dauguma trumpų derinių nepriklausomi, dauguma ilgų derinių — priklausomi.

1 paveiksle pavaizduoti multiplikatyviai nepriklausomų derinių iš $[1, 20]$ dalies įverčiai ir tiksli reikšmė. Nors viršutinis įvertis kokybiškai atitinka tikslaus skaičiaus kreivę, yra daug

trejetais ir didesniais poaibiais priklausomų derinių, todėl viršutinis įvertis nėra tikslus. Apatinis įvertis taip pat kokybiškai atitinka tikslaus skaičiaus kreivę ir turi mažesnę paklaidą nei viršutinis.

2. Multiplikatyviai nepriklausomų algebrinių skaičių derinių skaičiavimas

Kompleksinis skaičius α vadinamas algebriniu skaičiumi, jei jis yra kokio nors nenulinio daugianario su racionaliaisiais koeficientais

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_0, a_1, \ldots a_{n-1} \in \mathbb{Q}$$

šaknis, t. y. $p(\alpha) = 0$. Toks mažiausio įmanomo laipsnio daugianaris vadinamas algebrinio skaičiaus α minimaliuoju daugianariu, o jo laipsnis — algebrinio skaičiaus α laipsniu. Pavyzdžiui, laipsnio 1 algebrinio skaičiaus 5/9 minimalus daugianaris lygus $x - 5/9$, laipsnio 2 algebrinio skaičiaus $-1 + i$ minimalus daugianaris lygus $x^2 + 2x + 2$, ir laipsnio 6 algebrinio skaičiaus $\exp(2\pi i/7)$ minimalus daugianaris lygus $\sum_{j=0}^{6} x^j$. Kadangi daugianario koeficientai racionalūs, tokie algebriniai skaičiai dar vadinami algebriniais skaičiais virš $\mathbb{Q}$. Algebrinių skaičių aibė yra skaiti. Algebrinio skaičiaus α aukščiu vadinamas skaičius

$$H(\alpha) = \left(a_d \prod_{i=1}^{d} \max(1, |\alpha_i|) \right)^{1/d}$$

kur d yra minimalaus α daugianario laipsnis, α_i — minimalaus daugianario šaknys, a_d — mažiausias natūralusis skaičius, iš kurio reikia padauginti algebrinio skaičiaus α minimalųjį daugianarį, kad visi jo koeficientai būtų sveikieji skaičiai. Algebrinio skaičiaus logaritminis aukštis apibrėžiamas kaip

$$h(\alpha) = \ln H(\alpha).$$

Norint 2 algoritmą pritaikyti algebriniams skaičiams reikalingas baigtinės algebrinių skaičių aibės multiplikatyviojo nepriklausomumo patikrinimo algoritmas. Vieną galimą tikrinimo algoritmą galima gauti remiantis 3 teorema straipsnyje [16].

1 teorema ([11], 2.1 lema). *Tegul $n \geq 2$, $\alpha_1, \alpha_2, \ldots \alpha_n$ — multiplikatyviai priklausomi nenuliniai algebriniai skaičiai D laipsnio skaičių kūne K virš $\mathbb{Q}$, kurių kiekvieno aukštis ne didesnis už $H \geq 2$. Tuomet egzistuoja $k_1, k_2, \ldots k_n \in \mathbb{Z}$, bent vienas nenulinis, ir tik nuo n priklausantis teigiamas skaičius c_1, kad*

$$\alpha_1^{k_1} \alpha_2^{k_2} \ldots \alpha_n^{k_n} = 1$$

ir

$$\max_{1 \leq i \leq n} |k_i| \leq c_1 D^n (\log(D+1))^{3(n-1)} (\log H)^{n-1}.$$

Be to, jei K totaliai realus, t.y. $K = \mathbb{Q}(\alpha)$, kur visi algebrinio skaičiaus α algebriniai jungtiniai yra realieji skaičiai, tuomet egzistuoja $k_1, k_2, \ldots k_n \in \mathbb{Z}$, bent vienas nenulinis, ir tik nuo n priklausantis teigiamas skaičius c_2, kad

$$\max_{1 \leq i \leq n} |k_i| \leq c_2 (\log H)^{n-1}.$$

1 teoremoje galimos k_i reikšmės apribotos ir sveikosios, todėl perrinkus visas $k_1, k_2, \ldots k_n$ reikšmes galima nuspręsti, ar $\alpha_1, \alpha_2, \ldots \alpha_n$ yra multiplikatyviai nepriklausomi. Pirmojo įverčio dešinioji pusė gali būti perrašyta pagal [16] 3 teoremą kaip

$$\max_{1 \leq i \leq n} |k_i| \leq \max_{1 \leq i \leq n} \left((n-1)! w(K) \prod_{j \neq i} (D h(\alpha_j) \lambda(D)) \right),$$

kur $w(K)$ žymi vieneto šaknų skaičių kūne K, $\lambda(D) = (2-\varepsilon)(\ln\ln D/\ln D)^3$ bet kuriam $\varepsilon > 0$, jei D pakankamai didesnis už ε. Kadangi egzistuoja algoritmas algebrinių skaičių aukščiui nustatyti, šis įvertis yra suskaičiuojamas ir gali būti algoritmo pagrindu. Šio algoritmo sudėtingumas lygus $\mathcal{O}\left(\left(2\cdot c_1(n)D^n(\log(D+1))^{3(n-1)}(\log H)^{n-1}\right)^n\right) = \mathcal{O}\left((c_1(n))^n\,(2^n)^n\right)$ pasirinktam kūnui. Apibūdintas algoritmas veiktų pernelyg lėtai skaičiavimams praktikoje, nebent $c_1(n)$ greitai mažėja.

Multiplikatyviai nepriklausomų algebrinių skaičių derinių skaičiavimą gali pagreitinti 2 teorema.

2 teorema ([11], 3.4 išvada). *Jei algebriniai skaičiai $\alpha_1, \alpha_2, \dots \alpha_n$ poromis skirtingi, tai $\alpha_1 + t, \alpha_2 + t, \dots \alpha_n + t$ multiplikatyviai priklausomi tik su baigtiniu skaičiumi skaičių $t \in \mathbb{Z}$.*

Žinant mažiausią ir didžiausią t reikšmę būtų galima netikrinti visų paslinktų skaičių $\alpha_1, \alpha_2, \dots \alpha_n$ derinių, nes visi deriniai už intervalo ribos yra multiplikatyviai nepriklausomi.

Algebrinių skaičių bet kuriame nenulinio ilgio intervale be galo daug, todėl reikia apibrėžti prasmingą intervalo skaičių aibę perrinkimui. Algebrinių skaičių vektorius $\nu = (\nu_1, \nu_2, \dots \nu_n)$ yra multiplikatyviai nepriklausomas, jei neegzistuoja nenulinio vektoriaus $k = (k_1, k_2, \dots k_n)$, kad $\nu^k = \nu_1^{k_1}\nu_2^{k_2}\dots\nu_n^{k_n} = 1$. Straipsnyje [22] įrodoma, kad multiplikatyviai priklausomų n matmenų laipsnio d ir aukščio neviršijančio H algebrinių skaičių vektorių skaičius auga kaip

$$M^*_{n,d}(H) = C(n,d)H^{d(d+1)(n-1)} + O(H^{d(d+1)(n-1)-d/2}\log H),$$

kur

$$C(n,d) = (nw_0(d) + 2n(n-1))C_1(d)^{n-1},$$

$w_0(d)$ yra laipsnio d vieneto šaknų skaičius,

$$C_1(d) = \frac{d2^d}{\zeta(d+1)}\prod_{j=1}^{\lfloor(d-1)/2\rfloor}\frac{(d+1)(2j)^{d-2j}}{(2j+1)^{d-2j+1}},$$

$\zeta(s)$ yra Rymano dzeta funkcija. Kadangi egzistuoja algoritmas apriboto aukščio algebriniams skaičiams skaičiuoti, pavyzdžiui [8], galima sudaryti šių skaičių derinius. Perrenkant algebrinių skaičių derinius algoritmu būtų galima naudoti tas pačias aukščio ir laipsnio ribas bei intervalo kraštus prasmingai perrinkimo aibei gauti, taip patikslinant šį įvertį pasirinktame intervale.

3. Nepriklausomumo svarba Büchi aritmetikoje

Įvairių aritmetikų raiška ir teiginių jose įrodomumas apžvelgiamas [2].

Žinoma, kad natūraliųjų skaičių aritmetika su sudėties ir daugybos operacijomis $\langle \mathbb{N}, =, +, \times \rangle$ turi teiginių, kurie negali būti įrodyti per baigtinį laiką. Norint apibrėžti aritmetiką, kurios visi teiginiai įrodomi algoritmais, reikia susilpninti įprastinės aritmetikos operacijas išsaugant kuo daugiau aritmetikoje išreiškiamų teiginių.

Presburger aritmetika $\langle \mathbb{N}, =, + \rangle$ neturi daugybos operacijos. Šioje aritmetikoje kiekvienas teiginys gali būti įrodytas algoritmu, veikiančiu per baigtinį laiką. Vienas toks algoritmas, paremtas teiginio kintamųjų sprendinių aibę atpažįstančio baigtinio automato konstravimu pateiktas [4]. Aritmetikoje apibrėžiamas sąryšis apibrėžia aibę vektorių, kuriuos priskyrus sąryšio kintamiesiems sąryšis yra teisingas.

3 teorema ([2], 3 išvada). *Poaibis $X \subseteq \mathbb{N}$ gali būti apibrėžtas $\langle \mathbb{N}, =, + \rangle$ tada ir tik tada, kai X yra galiausiai periodinė aibė, kitaip tariant, egzistuoja $M, p \geq 1$, kad kiekvienam $x \geq M$, $x \in X \iff x + p \in X$.*

4 teorema ([2], 4 teorema; [12]). *Kai $n \geq 1$, poaibis $X \subseteq \mathbb{N}^n$ gali būti apibrėžtas $\langle \mathbb{N}, =, + \rangle$ tada ir tik tada, kai X yra pusiau tiesinė aibė, kitaip tariant, X yra apibrėžiama baigtine pavidalo*

$$\exists y_1 \dots \exists y_m (x = a_0 + a_1 \cdot y_1 + \dots + a_m \cdot y_m)$$

formulių disjunkcija, kur $x = (x_1, x_2, \dots x_n)$, $a_0, a_1, \dots a_m \in \mathbb{N}^n$, $a_j \cdot y_j = (a_{j1} y_j, a_{j2} y_j, \dots a_{jn} y_j)$, $j = 1, 2, \dots m$.

Atsisakius daugybos, aritmetikos $\langle \mathbb{N}, =, + \rangle$ teiginiai gali būti įrodyti per baigtinį laiką, bet neįmanoma išreikšti daugelio teiginių, pavyzdžiui, teiginių apie daugianarius. Prie Presburger aritmetikos operacijų pridėjus skaičiaus kėlimą kvadratu gaunama aritmetika $\langle \mathbb{N}, =, +, x \mapsto x^2 \rangle$, tačiau joje daugyba $x \times y = z$ gali būti išreikšta kaip lygties $(x + y)^2 = x^2 + z + z + y^2$ sprendinys. Taigi, aritmetika su skaičiaus kėlimu kvadratu turi per baigtinį laiką neįrodomų teiginių, kaip ir $\langle \mathbb{N}, =, +, \times \rangle$, tad papildomos funkcijos turi būti atidžiai parinktos.

Büchi aritmetika yra aritmetika $\langle \mathbb{N}, =, +, V_k \rangle$, kur V_k yra funkcija, randanti didžiausią nenulinį skaičių dalinantį k laipsnį:

$$\begin{aligned} V_k(0) &= 1, \\ V_k(x) &= \max_{0 \leq j \leq \lfloor \log_k x \rfloor} k^j \cdot \mathbb{1}_{x \bmod k^j = 0}, \quad x \in \mathbb{N} \setminus \{0\}. \end{aligned}$$

Šios aritmetikos įrodomumas susijęs su k simbolių abėcėlės baigtiniais automatais.

Apibrėžiant baigtinį automatą, abėcėlė Σ yra baigtinė simbolių aibė. Σ^* žymima galimų baigtinių žodžių aibė iš abėcėlės Σ, įskaitant tuščią žodį λ. Baigtinis automatas su abėcėle Σ — tai ketvertas (Q, q_0, δ, Q'), kur Q yra baigtinė būsenų aibė, q_0 yra pradinė būsena, $Q' \subseteq Q$ yra galutinių būsenų aibė, $\delta : Q \times \Sigma \to Q$ yra perėjimo funkcija. Ši perėjimo funkcija nurodo, kaip baigtinio automato būsena keičiasi apdorojant vieną įvesties simbolį. Perėjimo funkcija pratęsiama visai baigtinių žodžių aibei Σ^* apdorojant kiekvieną žodžio simbolį paeiliui:

$$\begin{aligned} \delta^*(q, a) &= \delta(q, a), & q \in Q, a \in \Sigma, \\ \delta^*(q, aw) &= \delta(\delta^*(q, w), a), & q \in Q, a \in \Sigma, w \in \Sigma^*. \end{aligned}$$

Jei $\delta^*(q_0, w) \in Q'$, žodis $w \in \Sigma^*$ yra atpažįstamas baigtinio automato. Visų tam tikro baigtinio automato atpažįstamų žodžių aibė vadinama jo kalba.

Büchi aritmetikoje skaičiai apibrėžiami k-tainėje sistemoje. Jei aibė k-tainių skaičių vektorių $x \in \mathbb{N}^n$ yra kurio nors baigtinio automato su abėcėle $\{0, 1, ... k-1\}^n$ kalba, ši aibė vadinama k-atpažįstama. Teiginys aritmetikoje užrašomas naudojant aritmetinius simbolius $=, +, V_k$ bei pirmosios eilės logiką su visuotinumo ir egzistavimo kvantoriais.

5 teorema ([2], 20 teorema; [6]). *Tegul $k \geq 2$, $n \geq 1$. Poaibis $X \subseteq \mathbb{N}^n$ yra k-atpažįstamas tada ir tik tada, kai jį galima apibrėžti $\langle \mathbb{N}, =, +, V_k \rangle$.*

Büchi aritmetikoje apibrėžiami teiginiai $\mathrm{Th}(\mathbb{N}, =, +, V_k)$ gali būti įrodyti per baigtinį laiką, nes šioje aritmetikoje kiekvienam teiginiui iš aritmetinės formulės, suvaržytos egzistavimo kvantoriais galima rasti atitinkamą k-atpažįstamą baigtinio automato kalbą, kuri būtų tuščia tada ir tik tada, kai teiginys klaidingas. Büchi taip pat įrodė, kad multiplikatyviai priklausomiems k ir l, $k \neq l$, k ir l-tainių aritmetikų teiginiai yra k-atpažįstami ir l-atpažįstami vienu metu. Kyla klausimas, ar yra teiginių, kurie gali būti k-atpažįstami ir l-atpažįstami multiplikatyviai nepriklausomiems k ir l. Į šį klausimą atsako Cobham teorema, kuri rodo, kad multiplikatyviai nepriklausomiems k ir l visos k ir l-atpažįstamos aibės yra galiausiai periodinės ir negali išreikšti sudėtingesnių teiginių nei aritmetika $\langle \mathbb{N}, =, + \rangle$.

6 teorema (Cobham, [2], 24 teorema; [7]). *Tegul $k, l \geq 2$ yra multiplikatyviai nepriklausomi natūralieji skaičiai. Kiekvienas poaibis $X \subseteq \mathbb{N}$, kuris yra k ir l-atpažįstamas, yra galiausiai periodinis.*

Cobham teoremą Semionov išplėtė daugiaviečiams sąryšiams.

7 teorema (Cobham-Semionov, [2], 25 teorema; [23]). *Tegul $n \geq 1$, $k, l \geq 2$ yra multiplikatyviai nepriklausomi natūralieji skaičiai. Kiekvienas poaibis $X \subseteq \mathbb{N}^n$, kuris yra k ir l-atpažįstamas, yra apibrėžiamas $\langle \mathbb{N}, =, + \rangle$.*

Kita vertus, multiplikatyviai nepriklausomų k ir l atveju aritmetika $\langle \mathbb{N}, =, +, V_k, V_l \rangle$ atitinka $\langle \mathbb{N}, =, +, \times \rangle$.

4. Multiplikatyviai nepriklausomos bazės

q-tainę skaičių sistemą sudaro bazė $q \leq -2$ ir skaitmenys $0, 1, |q|-1$. Kiekvienas sveikasis skaičius turi vienintelę išraišką q-tainėje sistemoje. Gauso sveikieji skaičiai — kompleksiniai skaičiai $z = a + bi, a, b \in \mathbb{Z}$, arba $Z[i]$ — gali būti išreiškiami vieninteliu būdu skaičių sistemose su baze $-1 + i$ ir skaitmenimis $\{0, 1\}$ bei baze $-1 - i$ ir skaitmenimis $\{0, 1\}$ pagal [15]. Madritsch ir Ziegler straipsnyje [18] įrodoma, kad bazės $-m + \zeta_k$, kur ζ_k yra primityvioji k-toji vieneto šaknis, $m \geq \varphi(k)+1$ sudaro $\mathbb{Z}[\zeta_k]$ skaičių sistemą. Cobham teorema susieja atpažįstamas skaičiavimo sistemas pagal multiplikatyvųjį bazių priklausomumą ar nepriklausomumą, todėl straipsnyje tirtas bazių nepriklausomumas. Įrodyta, kad $-m + \zeta_k$ ir $-n + \zeta_k$ nepriklausomos, kai $m > n > C(k)$. Vėlesniame straipsnyje [19] Madritsch ir Ziegler iškėlė hipotezę, kad $-m + \zeta_k$ ir $-n + \zeta_k$ nepriklausomos, kai $m > n > 1, k > 2$.

Pastaroji hipotezė buvo įrodyta Drungilo ir Dubicko [10]. Taip pat įrodytas apibendrintas hipotezės atvejis daugiau nei dviejoms nepriklausomoms bazėms.

8 teorema ([10], 1.1 teorema). *Kiekvienam $k \geq 3$ ir visiems teigiamiems sveikiesiems skaičiams $m > n$, skaičiai $m - \zeta_k, n - \zeta_k$ multiplikatyviai nepriklausomi, išskyrus kai $(n, k) = (1, 6)$.*

8 teorema įrodoma taikant 9 teoremą.

9 teorema ([10], 1.2 teorema). *Tegul α yra toks laipsnio $d \geq 4$ sangrąžinis algebrinis skaičius, kad skaičius $\beta = 1 + 1/\alpha$ turi bent du jungtinius skaičius intervale $(-\infty, 2]$. Tuomet bet kokiems sveikiesiems skaičiams $m > n > 0$ skaičiai $m - \alpha, n - \alpha$ yra multiplikatyviai nepriklausomi.*

Čia algebrinis skaičius $\alpha \neq 0$ yra sangrąžinis, jei $1/\alpha$ lygus α jungtiniam skaičiui virš $\mathbb{Q}$. Jungtiniai skaičiai kūno išplėtime yra to paties minimalaus daugianario šaknys, kitaip, egzistuoja izomorfizmas $\sigma : F(\alpha) \to F(\beta)$, kuris lygus tapatybei kūne F. Kiekvienas sangrąžinis $\alpha \neq \pm 1$ turi lyginį laipsnį d, tuomet $\beta = \alpha + 1/\alpha$ turi laipsnį $d/2$.

Įrodymas. Teorema įrodoma prieštara. Tarkime, kad egzistuoja sveikieji skaičiai a, b, bent vienas nenulinis, kad

$$(m - \alpha)^a = (n - \alpha)^b.$$

Neprarandant bendrumo galima teigti, kad $a \geq 0$.

Tegul G yra normaliojo uždarinio $\mathbb{Q}(\alpha)$ Galua grupė virš $\mathbb{Q}$. Pasirinkus bet kurį automorfizmą iš G $\alpha \mapsto 1/\alpha$ ir pritaikius lygybei gauname

$$(m - 1/\alpha)^a = (n - 1/\alpha)^b$$

Sudauginus abi lygybes gauname

$$\begin{aligned}(m - 1/\alpha)^a(m - \alpha)^a &= (n - 1/\alpha)^b(n - \alpha)^b,\\ ((m - 1/\alpha)(m - \alpha))^a &= ((n - 1/\alpha)(n - \alpha))^b,\\ (m^2 - m\alpha - m/\alpha + 1)^a &= (n^2 - n\alpha - n/\alpha + 1)^b.\end{aligned}$$

Tuomet pagal $\beta = \alpha + 1/\alpha$

$$(m^2 + 1 - m\beta)^a = (n^2 + 1 - n\beta)^b$$

Tegul $\beta_1 < \beta_2 < 2$ būna bet kurie realūs β jungtiniai skaičiai virš $\mathbb{Q}$. Kadangi $\deg(\beta_2) = \deg(\beta) = d/2 \geq 2$, $\beta \neq 2$. $\mathbb{Q}(\beta)$ yra $\mathbb{Q}(\alpha)$ pokūnis, todėl G egzistuoja automorfizmai $\beta \mapsto \beta_1$ ir $\beta \mapsto \beta_2$. Pritaikius automorfizmus lygybei gauname

$$\begin{aligned}(m^2 + 1 - m\beta_1)^a &= (n^2 + 1 - n\beta_1)^b\\ (m^2 + 1 - m\beta_2)^a &= (n^2 + 1 - n\beta_2)^b\end{aligned}$$

Reikia parodyti, kad $a > 0$. Jei $a = 0$ ir $b \neq 0$, tai $n^2 + 1 - n\beta_1$, $n^2 + 1 - n\beta_2$ yra vieneto šaknys. $n^2 + 1 - n\beta_j \geq 2n - n\beta_j > 0$, todėl vieneto šaknys realios ir teigiamos, taigi, lygios vienintelei realiai teigiamai vieneto šakniai 1. Tuomet $\beta_1 = \beta_2 = n$, tačiau tai prieštarauja prielaidai $\beta_1 < \beta_2$.

Reikia parodyti, kad $b \neq 0$. $m \geq 2 > \beta_j$, todėl $m^2 + 1 - m\beta_j > 1$. Kadangi $a \geq 1$, kairioji lygybės

$$(m^2 + 1 - m\beta_j)^a = (n^2 + 1 - n\beta_j)^b$$

pusė didesnė nei 1, todėl laipsnio rodiklis $b \neq 0$, kitaip dešinioji pusė būtų lygi vienam. Pastebima, kad $m^2 + 1 - mx > n^2 + 1 - nx > 0$, jei $x \in (-\infty, 2)$, todėl

$$f(x) = a \log(m^2 + 1 - mx) - b \log(n^2 + 1 - nx)$$

intervale $x \in (-\infty, 2)$ lygi 0 bent du kartus: kai $x = \beta_1$ ir $x = \beta_2$. Pagal Rolio teoremą, išvestinė

$$f'(x) = -\frac{am}{m^2 + 1 - mx} + \frac{bn}{n^2 + 1 - nx}$$

lygi 0 bent vieną kartą tarp $x = \beta_1$ ir $x = \beta_2$ kai $x = \gamma$. Įstačius $f'(\gamma) = 0$ gauname

$$0 = -\frac{am}{m^2 + 1 - m\gamma} + \frac{bn}{n^2 + 1 - n\gamma}$$
$$a(n + 1/n - \gamma) = b(m + 1/m - \gamma)$$

Žinoma, kad $a > 0$ ir $n + 1/n - \gamma \geq 2 - \gamma > 0$, todėl kairioji lygybės pusė teigiama, ir dešinioji teigiama. $m + 1/m - \gamma > 0$, todėl $b > 0$, arba $b \geq 1$, nes b sveikasis. Lygybėje

$$(m^2 + 1 - m\beta_j)^a = (n^2 + 1 - n\beta_j)^b$$

kairioji pusė didesnė už 1 ir $b \geq 1$, tada $n^2 + 1 - n\beta_j > 1$, nes kitaip būtų keliama trupmena neviršytų 1. Taigi, $m^2 + 1 - m\beta_j > n^2 + 1 - n\beta_j > 1$, $a, b \geq 1$, tuomet $a < b$, nes laipsnio pagrindas kairėje lygybės pusėje didesnis nei dešinėje, ir abu didesni už vienetą. Be to,

$$0 < n^2 + 1 - n\beta_j < m^2 + 1 - m\beta_j,$$

todėl $a(n + 1/n - \gamma) < b(m + 1/m - \gamma)$ lygybėje

$$a(n + 1/n - \gamma) = b(m + 1/m - \gamma)$$

Gauta prieštara įrodo teoremą. □

8 teoremos įrodymas. k-tojo laipsnio primityviąją vieneto šaknį galima apskaičiuoti formule

$$\zeta_k = \exp(2\pi i/k).$$

Jei $k = 5$ arba $k \geq 7$, $\deg(\zeta_k) = \varphi(k) \geq 4$, kur $\varphi(k)$ yra Oilerio funkcija. Tuomet šiems sveikiems k skaičius α_k yra algebrinis ir sangrąžinis, turintis laipsnį $\varphi(k) \geq 4$. Šį α atitinkantis $\beta = \zeta_k + 1/\zeta_k = 2\cos(2\pi/k)$ turi $\varphi(k)/2 \geq 2$ jungtinių skaičių intervale $(-2, 2)$. Pagal 2 teoremą skaičiai $m - \zeta_k$, $n - \zeta_k$ yra multiplikatyviai nepriklausomi bet kuriems sveikiesiems $m > n > 0$.

Lieka įrodyti teoremą, kai $k = 3, 4, 6$. Kai $k = 3$, $\beta = 2\cos(2\pi/k) = -1$. Įstačius β į

$$(m^2 + 1 - \beta m)^a = (n^2 + 1 - \beta n)^a$$
$$(m^2 + 1 + m)^a = (n^2 + 1 + n)^b$$

gauname, kad skaičiai m^2+m+1 ir n^2+n+1 būtų multiplikatyviai priklausomi. Tuomet egzistuoja $0<a<b$ ir $g>1$, kad $m^2+m+1=g^b$, $n^2+n+1=g^a$. Pagal T. Nagell [21] diofantinė lygtis $X^2+X+1=Y^b$ turi vienintelį sprendinį $(X,Y,b)=(18,7,3)$, jei $X,Y,b>1$. Taigi, $m^2+m+1=18^2+18+1=7^3=(n^2+1+n)^3$, ir $2^2+2+1=7$, tai rodo, kad $m=18$, $b=3$, $n=2$. Kadangi $7=n^2+n+1=g^a=7^a$, $a=1$. Šiems vieninteliams m,n skaičiai $18-\zeta_3$, $2-\zeta_3$ yra multiplikatyviai nepriklausomi, nes

$$\begin{gathered}
a\in\mathbb{N}, b\in\mathbb{Z}\\
(18-\zeta_3)^a=(2-\zeta_3)^b \qquad |\cdot(18-\zeta_3^{-1})^a=(2-\zeta_3^{-1})^b\\
((18-\zeta_3)(18-\zeta_3^{-1}))^a=((2-\zeta_3)(2-\zeta_3^{-1}))^b\\
(18^2-18\zeta_3^{-1}-18\zeta_3+1)^a=(2^2-2\zeta_3^{-1}-2\zeta_3+1)^b\\
(18^2-18(\zeta_3+\zeta_3^{-1})+1)^a=(2^2-2(\zeta_3+\zeta_3^{-1})+1)^b\\
\left(18^2-18\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}-\frac{1}{2}-\frac{\sqrt{3}}{2}\right)+1\right)^a=\left(2^2-2\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}-\frac{1}{2}-\frac{\sqrt{3}}{2}\right)+1\right)^b\\
(18^2+18+1)^a=(2^2+2+1)^b\\
343^a=7^b\\
7^{3a}=7^b
\end{gathered}$$

rodo, kad $b=3a$, tačiau trumpena

$$\frac{18-\zeta_3}{(2-\zeta_3)^3}=\frac{360+323\zeta_3}{343}=\frac{397+323\sqrt{3}i}{686}$$

nėra sveikasis algebrinis skaičius, todėl negali būti vieneto šaknis. Tai prieštarauja teiginiui, kad skaičiai $18-\zeta_3$, $2-\zeta_3$ yra multiplikatyviai priklausomi.

Kai $k=4$, $\beta=0$, ir skaičiai m^2+1, n^2+1 būtų multiplikatyviai priklausomi. Tuomet $m^2+1=g^b, m,g,b>1$. Tačiau pagal Catalan konjektūros [20] atvejį diofantinė lygtis $X^2+1=Y^b$ neturi sprendinių, kai $X,Y,b>1$. Todėl skaičiai multiplikatyviai nepriklausomi, kai $k=4$.

Kai $k=6$, $\beta=1$ ir skaičiai m^2-m+1, n^2-n+1 būtų multiplikatyviai priklausomi. Kai $n=1$, tai skaičiai $m-\zeta_6$, $1-\zeta_6$ yra multiplikatyviai priklausomi.

Kitais atvejais, kai $m>n>1$, tarkime, kad skaičiai $m-\zeta_6$, $n-\zeta_6$ yra multiplikatyviai priklausomi. Tuomet $m^2-m+1>n^2-n+1>1$, ir egzistuoja $m,n,g,b>1, a\geq 1$, kad $m^2-m+1=g^b$, $n^2-n+1=g^a$. Lygybė $m^2-m+1=g^b$ ekvivalenti $(2m-1)^2+3=4g^b$. Pagal ypatingą 1.1 teoremos [17] atvejį diofantinė lygtis $X^2+3=4Y^b$, $X,Y,b>1$ turi vienintelį sprendinį $(X,Y,b)=(37,7,3)$. Tuomet $(m,g,b)=(19,7,3)$, tada $a=1$, $n=3$. Taigi, yra vienintelė pora $19-\zeta_6$, $3-\zeta_6$. Šiems vieninteliams m,n skaičiai $19-\zeta_6$, $3-\zeta_6$ yra multiplikatyviai nepriklausomi, nes

$$\begin{gathered}
a\in\mathbb{N}, b\in\mathbb{Z},\\
(19-\zeta_6)^a=(3-\zeta_6)^b \qquad |\cdot(19-\zeta_6^{-1})^a=(3-\zeta_6^{-1})^b
\end{gathered}$$

rodo, kad $b=3a$, tačiau trumpena

$$\frac{19-\zeta_6}{(3-\zeta_6)^3}=\frac{37+323\zeta_6}{343}$$

nėra algebrinis sveikasis skaičius, todėl negali būti vieneto šaknis. Tai prieštarauja teiginiui, kad skaičiai $19-\zeta_6$, $3-\zeta_6$ yra multiplikatyviai priklausomi. □

Nenuliniai skaičiai $z_1, z_2, \dots z_k \in \mathbb{C}$ vadinami multiplikatyviai priklausomais, jei egzistuoja $a_1, a_2, \dots a_k \in \mathbb{Z}$, ne visi nuliniai, kad

$$z_1^{a_1} z_2^{a_2} \dots z_k^{a_k} = 1$$

kitais atvejais $z_1, z_2, \dots z_k \in \mathbb{C}$ vadinami multiplikatyviai nepriklausomais. [9] pastebėta, kad algebriniam skaičiui α, kuris nėra algebrinis sveikasis skaičius, lygybė

$$(m_1 - \alpha)^{a_1}(m_2 - \alpha)^{a_2} \dots (m_k - \alpha)^{a_k} = 1,$$

$a_1, a_2, \dots a_k \in \mathbb{Z}$ galioja tik tada, kai $a_1 + a_2 + \dots + a_k = 0$.

Tuo atveju, kai $k = 2$, α - algebrinis skaičius, bet ne algebrinis sveikasis skaičius (šaknis daugianario, kurio didžiausio laipsnio koeficientas lygus 1, kiti koeficientai tik racionalūs, ne sveikieji), $m_1, m_2 \in \mathbb{Z}$, $m_1 > m_2$, skaičiai $m_1 - \alpha$, $m_2 - \alpha$ multiplikatyviai priklausomi tada ir tik tada, kai trupmena $(m_1 - \alpha)/(m_2 - \alpha)$ yra vieneto šaknis.

10 teorema ([10], 3.1 teorema). *Tegul α - laipsnio $d \geq 6$ sangrąžinis algebrinis skaičius, toks, kad $\beta = \alpha + 1/\alpha$ turi bent $t \geq 3$ jungtinius skaičius intervale $(-\infty, 2]$. Tuomet bet kuriems sveikiesiems skaičiams $m_1 > m_2 > \dots > m_{t-1} > 0$ skaičiai*

$$m_1 - \alpha, m_2 - \alpha, \dots m_{t-1} - \alpha$$

yra multiplikatyviai nepriklausomi.

Įrodymas. Tegul $\beta_1 < \dots < \beta_t < 2$ yra t realiųjų β jungtinių skaičių. Tarkime priešingai teoremos teiginiui: egzistuoja $a_1, a_2, \dots a_{t-1} \in \mathbb{Z}$, ne visi nuliniai, kad

$$(m_1 - \alpha)^{a_1}(m_2 - \alpha)^{a_2} \dots (m_{t-1} - \alpha)^{a_{t-1}} = 1$$

Kaip ir anksčiau galime gauti

$$(m_1^2 + 1 - m_1\beta_j)^{a_1}(m_2^2 + 1 - m_2\beta_j)^{a_2} \dots (m_{t-1}^2 + 1 - m_{t-1}\beta_j)^{a_{t-1}} = 1,$$

$j = 1, \dots t$. Tuomet funkcija

$$f(x) = \sum_{j=1}^{t-1} a_j \log(m_j^2 + 1 - m_j x)$$

yra lygi nuliui intervale $(-\infty, 2)$ bent t taškų $x = \beta_1, \dots \beta_t$. Pagal Rolio teoremą išvestinė

$$f'(x) = -\sum_{j=1}^{t-1} \frac{a_j m_j}{m_j^2 + 1 - m_j x}$$

turi būti lygi nuliui bent $t - 1$ taškų intervale $(-\infty, 2)$, tačiau taip nėra.

Daugianaris

$$P(x) = f'(x) \prod_{j=1}^{t-1} (m_j^2 + 1 - m_j x)$$

yra ne didesnio nei $t - 2$ laipsnio. Kadangi $m_j^2 + 1 - m_j x > 0$ visiems $j = 1, \dots t - 1$, $P(x)$ turi tiek pat nulinių taškų intervale $(-\infty, 2)$, kiek $f'(x)$. $P(x)$ negali visur būti lygus nuliui, nes tuomet

$$(m_1^2 + 1 - m_1 x)^{a_1}(m_2^2 + 1 - m_2 x)^{a_2} \dots (m_{t-1}^2 + 1 - m_{t-1} x)^{a_{t-1}} - 1$$

būtų lygus nuliui visiems $x \in (-\infty, 2)$. Gaunama lygybė

$$\prod_{j \in N_+} (m_j^2 + 1 - m_j x)^{a_j} = \prod_{j = N_-} (m_j^2 + 1 - m_j x)^{a_j}$$

$$N_+ = \{j \in \{1, \dots t-1\} : a_j \geq 0\}$$

$$N_- = \{j \in \{1, \dots t-1\} : a_j < 0\}$$

visiems $x \in (-\infty, 2)$. Taigi, ši lygybė turėtų galioti visiems $x \in \mathbb{C}$. Tačiau kiekvienam $x = m_j + 1/m_j$, kuriam $a_j \neq 0$, vienas iš sandaugos narių vienoje lygybės pusėje lygus nuliui, tad viena lygybės pusė lygi nuliui, kita - nelygi nuliui. Todėl $P(x)$, ir $f'(x)$ intervale $x \in (-\infty, 2)$ lygūs nuliui ne daugiau nei $t - 2$ taškų. Gauta prieštara išvadai, kad intervale $x \in (-\infty, 2)$ $f'(x)$ lygi nuliui bent $t - 1$ taškų. □

5. Büchi aritmetikos teiginiai bazėse

Büchi aritmetikoje $\langle \mathbb{N}, =, +, V_k \rangle$ galima išreikšti teiginius, ir visi šie teiginiai gali būti patikrinti algoritmu. Pavyzdžiui, teiginys

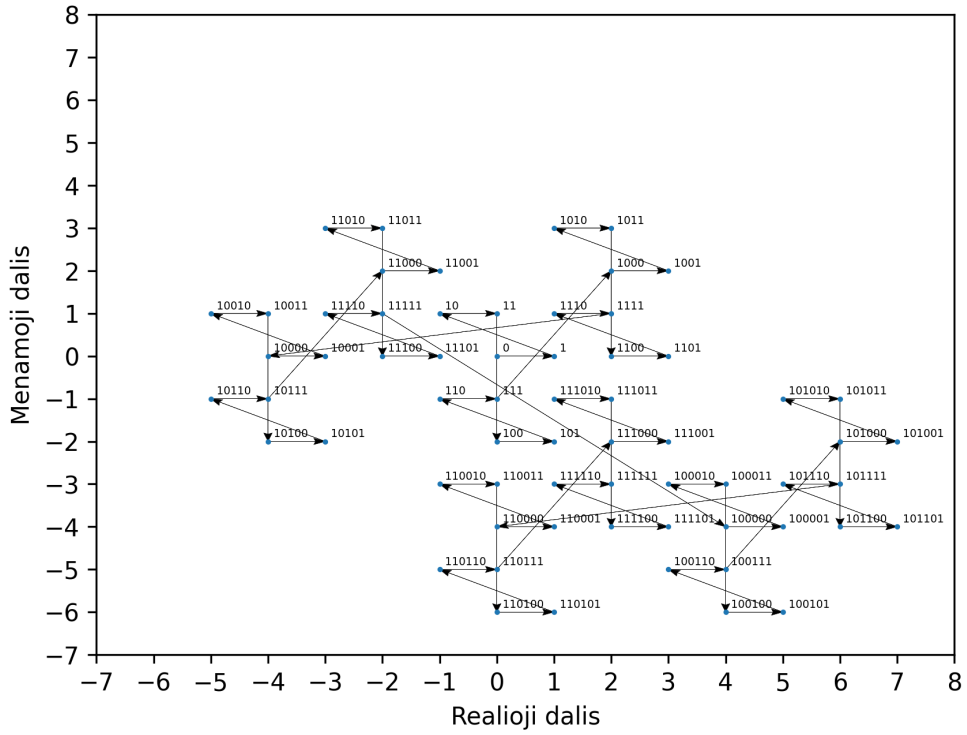
$$\forall x \exists y \, (y + y = x \vee y + y + 1 = x)$$

teigia, kad visi natūralieji skaičiai yra dalūs iš dviejų arba dalūs iš dviejų atėmus vienetą. Tą patį teiginį, kai bazė lygi 2, galima išreikšti ir naudojant Büchi aritmetikos funkciją V_2:

$$\forall x \, (x = 0_2 \vee \exists z V_2(x) = 10_2 + z \vee \exists y \, (y + 1_2 = x \wedge \exists z V_2(y) = 10_2 + z)) \, .$$

Kitas teiginio pavyzdys — sąryšis, reiškiantis, kad x ir y abu dalūs iš to paties didžiausio dvejeto laipsnio $z \geq 2$:

$$\neg(z = 1_2) \wedge V_2(x) = z \wedge V_2(y) = z.$$

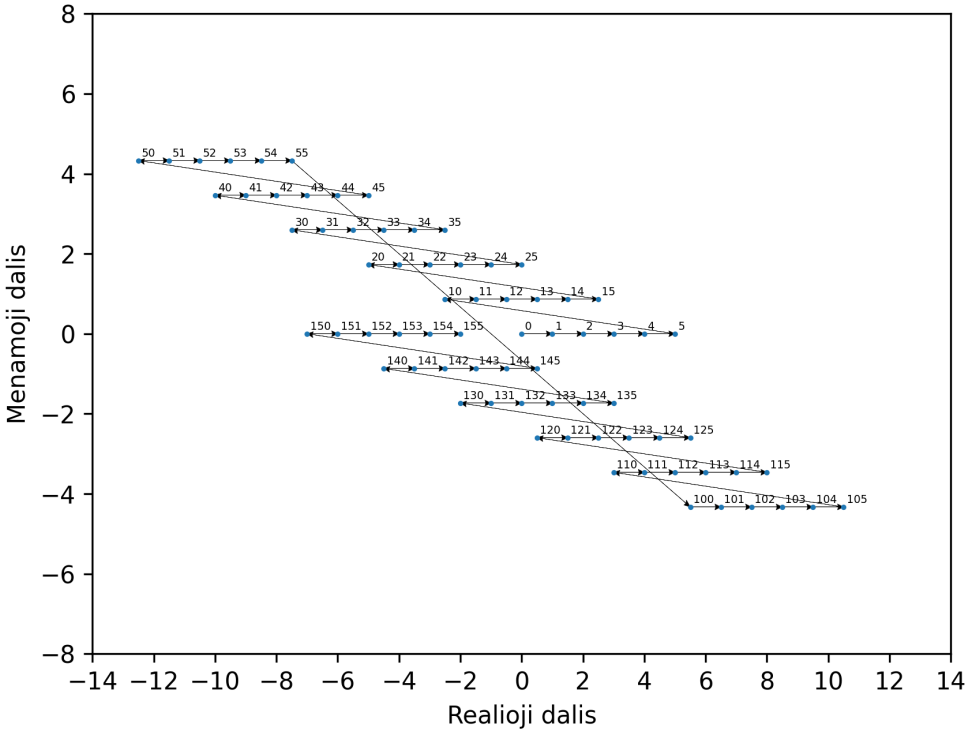


2 pav. Pirmi $2^6 = 64$ skaičiavimo sistemos $(-1 + i, \{0, 1\})$ skaičiai. Skaičiavimo sistema nurodo skaičius $\mathbb{Z}[i]$.

Skaičiai $\mathbb{Z}[i]$ yra kompleksiniai, todėl juos skaičiuojant skaičiavimo sistemoje $(-1 + i, \{0, 1\})$ skaičiai išdėstomi gana sudėtinga tvarka, kuri pavaizduota 2 paveiksle. $\mathbb{Z}[i]$ yra žiedas, kitaip nei $\mathbb{N}$, naudojama Presburger ir Büchi aritmetikų apibrėžime.

Presburger aritmetika $\langle \mathbb{N}, =, + \rangle$ gali būti išplėsta į tiesinę sveikųjų skaičių aritmetiką $\langle \mathbb{Z}, =, + \rangle$. Šios aritmetikos teiginiai irgi gali būti įrodyti per baigtinį laiką, pavyzdžiui, taikant [5] aprašytą algoritmą. Sudėties atveju žiedas $\mathbb{Z}[i]$ yra izomorfiškas žiedui $\mathbb{Z}^2$, kuriame teiginiai taip pat gali būti įrodyti pastaruoju algoritmu.

Nors panašu, kad Büchi aritmetika nebuvo atskirai tirta išplečiant ją $\mathbb{Z}$ ar $\mathbb{Z}[i]$, straipsniuose [13] ir [3] tirti būdai suformuluoti Cobham teoremą žiede $\mathbb{Z}[i]$. [3] keliama Cobham teoremos atvejo $\mathbb{Z}[i]$ hipotezė skaičiavimo sistemos bazėms iš $\mathbb{Z}[i]$.



3 pav. Pirmi $2 \cdot 6^2 = 72$ skaičiavimo sistemos $(-3+\zeta_6, \{0, 1, \ldots 5\})$ skaičiai. Skaičiavimo sistema nurodo skaičius $\mathbb{Z}[\zeta_6]$.

Pagal [18], skaičius iš žiedo $\mathbb{Z}[\zeta_k]$, kurį sudaro aibė $\{a + b\zeta_k : a, b \in \mathbb{Z}\}$ ir visi galimi iš jos daugyba ir sudėtimi gauti skaičiai, gali būti vieninteliu būdu užrašytas skaičiavimo sistemoje su baze $-m + \zeta_k$, $m \geq \varphi(k) + 1$ ir skaitmenimis $\{0, 1, \ldots |\Phi_k(m)| - 1\}$, kur k-tasis ciklotominis daugianaris $\Phi_k(x)$ apibrėžtas kaip

$$\Phi_k(x) = \prod_{\substack{1 \leq j \leq k \\ \gcd(j,k)=1}} \left(x - e^{2\pi i \cdot j/k}\right).$$

Ankstesniame skyrelyje pateiktas įrodymas, kad iš tirtų $\mathbb{Z}[\zeta_k]$ bazių porų multiplikatyviai priklausomos tik $-m + \zeta_6$ ir $-1 + \zeta_6$, $m > 1$. Tačiau bazė $-1 + \zeta_6$ nesudaro kanoninės skaičiavimo sistemos. Šios bazės atveju kiekvienas skaičius $\mathbb{Z}[\zeta_6]$ gali būti užrašytas ne vienu būdu, kaip natūraliuosiuose skaičiuose $\mathbb{N}$ su bazėmis $k \geq 2$, kuriomis apibrėžta Büchi aritmetika. Pavyzdžiui, $(-1+\zeta_6)^7 = (-1+\zeta_6)^1$. Tai gali reikšti, kad Büchi aritmetikos sąlygas tenkinančių multiplikatyviai priklausomų bazių Cobham teoremai taikyti žieduose $\mathbb{Z}[\zeta_k]$ nėra.

Literatūra

[1] Ž. Baronėnas. *Algebrinių skaičių multiplikatyvusis priklausomumas*. Magistrinis darbas, Vilniaus universitetas, 2020.

[2] A. Bès. A Survey of Arithmetical Definability. 2003. URL: https://lacl.univ-paris12.fr/bes/publi/survey.pdf. Tikrinta 2023-03-14.

[3] W. Bosma, R. J. Fokkink ir T. J. P. Krebs. On Cobham's Theorem for Gaussian Integers. English. J. Bernat ir et al, redaktoriai, *Proceedings of the 15th Mons Theoretical Computer Science Days, Nancy, 2014*, p.p. 1–5, 2014.

[4] A. Boudet ir H. Comon. Diophantine equations, Presburger arithmetic and finite automata. H. Kirchner, redaktorius, *Trees in Algebra and Programming — CAAP '96*, p.p. 30–43, Berlin, Heidelberg. Springer Berlin Heidelberg, 1996. ISBN: 978-3-540-49944-2.

[5] M. Bromberger, T. Sturm ir C. Weidenbach. Linear Integer Arithmetic Revisited, 2020. arXiv: 1503.02948 [cs.LO].

[6] V. Bruyère. Entiers et automates finis. Mémoire de fin d'études, 1985.

[7] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Mathematical Systems Theory*, 3:186–192, 1969.

[8] J. R. Doyle ir D. Krumm. Computing algebraic numbers of bounded height, 2013. arXiv: 1111.4963 [math.NT].

[9] P. Drungilas ir A. Dubickas. Multiplicative dependence of shifted algebraic numbers. *Colloquium Mathematicum*, 96:75–81, 2003-01. DOI: 10.4064/cm96-1-7.

[10] P. Drungilas ir A. Dubickas. Multiplicative dependence of two integers shifted by a root of unity. *Proceedings of the American Mathematical Society*, 2018.

[11] A. Dubickas ir M. Sha. Multiplicative dependence of the translations of algebraic numbers, 2018. arXiv: 1608.05458 [math.NT].

[12] S. Ginsburg ir E. H. Spanier. Semigroups, Presburger formulas and languages. *Pacific Journal of Mathematics*, 16:285–296, 1966.

[13] G. Hansel ir T. Safer. Vers un théorème de Cobham pour les entiers de Gauss. *Bulletin of the Belgian Mathematical Society - Simon Stevin*, 10, 2003-12. DOI: 10.36045/bbms/1074791328.

[14] K. Kianfar. *Branch-and-Bound Algorithms*. 2011. DOI: 10.1002/9780470400531.eorms0116.

[15] D. E. Knuth. *The Art of Computer Programming, Vol. 2. Seminumerical Algorithms*. Addison-Wesley, Reading, Massachusetts, 1981.

[16] J. Loxton ir A. van der Poorten. Multiplicative dependence in number-fields. English. *Acta Arithmetica*, 42(3):291–302, 1983. ISSN: 0065-1036.

[17] F. Luca, S. Tengely ir A. Togbé. On the Diophantine Equation $x^2 + C = 4y^n$. *Annales des sciences mathématiques du Québec*, 33:171–184, 2009.

[18] M. Madritsch ir V. Ziegler. An infinite family of multiplicatively independent bases of number systems in cyclotomic number fields, 2014. DOI: 10.48550/ARXIV.1403.1673. URL: https://arxiv.org/abs/1403.1673.

[19] M. G. Madritsch ir V. Ziegler. On multiplicatively independent bases in cyclotomic number fields, 2014. DOI: 10.48550/ARXIV.1408.3991. URL: https://arxiv.org/abs/1408.3991.

[20] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *Journal für die reine und angewandte Mathematik*, 572:167–195, 2004.

[21] T. Nagell. Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. *Norsk matematisk forenings skrifter*, 2:14, 1920.

[22] F. Pappalardi, M. Sha, I. E. Shparlinski ir C. L. Stewart. On multiplicatively dependent vectors of algebraic numbers, 2016. DOI: 10.48550/ARXIV.1606.02874. URL: https://arxiv.org/abs/1606.02874.

[23] A. L. Semenov. Presburgerness of predicates regular in two number systems. *Siberian Mathematical Journal*, 18:403–418, 1977.