Vilniaus Gedimino technikos universitetas

Aleksandras KRYLOVAS

DISKREČIOJI MATEMATIKA

Mokomoji knyga

Vilnius „Technika“ 2004

UDK 519.1(075.8)
Kr242
A. Krylovas. Diskrečioji matematika. Mokomoji knyga. Vilnius: Technika, 2004. 142 p.: iliustr.

Mokomojoje knygoje pateikiami pagrindiniai diskrečiosios matematikos skyriai: matematinė logika, Bulio funkcijos, aibių teorija, kombinkatorika, grafų teorija, kombinatoriniai algoritmai, informacijos kodavimo pagrindai.

Leidinys skirtas VGTU Elektronikos bei Fundamentinių mokslų fakultetų bakalaurų studijoms.

Leidinį rekomendavo VGTU Fundamentinių mokslų fakulteto studijų komitetas

Recenzavo dr. doc. J. Raulynaiyis ir dr. doc. M. Meilūnas

VGTU leidyklos „Technika“ *** mokomosios literatūros knyga

ISBN 9986-05-***-*

Turinys

Pratarmė

Klasikinė matematika dažniausiai nagrinėja tolydžiai kintančius dydžius, kuriems tirti taiko ribų teoriją, diferencialinį bei integralinį skaičiavimą. Tačiau net ir klasikinėje matematikoje yra sričių, kurioms būdingas *nutrūkstamumas* arba *diskretiškumas*, ir todėl reikalaujančių kitų tyrimo metodų. Visų pirma, paminėsime *kombinatorinę analizę*, nagrinėjančią baigtinių aibių elementų kombinacijas .

Diskrečiąja matematika arba *diskrečiąja analize* vadinama matematikos sritis, tyrinėjanti pačios matematikos diskrečiąsias struktūras ir realiųjų reiškinių diskrečiuosius matematinius modelius. Nagrinėjamos diskrečiosios struktūros gali būti ne tik baigtinės, bet ir begalinės, tačiau *skaičiosios* aibės. Taigi tyrinėjanti baigtines struktūras *baigtinė matematika* yra tik siauresnė diskrečiosios matematikos dalis.

Diskrečiosios matematikos sritys, be paminėtos *kombinatorikos*, yra *grafų teorija* ir *matematinė logika*. Vienas svarbiausių matematinės logikos klausimų yra uždavinių *išsprendžiamumas*, tiriamas *algoritmų teorijos* metodais. Diskrečiosios matematikos ypatumas yra tas, kad baigtinių struktūrų uždavinių išsprendžiamumas dažnai būna akivaizdus, ir sprendinį galima rasti perrinkus visus įmanomus variantus. Tačiau tokių variantų gali būti daug, ir jų pilnas perrinkimas paprastai yra praktiškai neįmanomas. Todėl svarbu žinoti, ar egzistuoja efektyvesni uždavinio sprendimo algoritmai. Šiuos klausimus nagrinėja uždavinių *sunkumo teorija*.

Išvardinkime ir kitus diskrečiosios matematikos skyrius: *informacijos kodavimas, baigtiniai automatai, formaliosios gramatikos* ir kt. Praplėsdami diskrečiosios matematikos objektą, galėtume jai priskirti ir skaičių teorijos, skaičiavimo matematikos, tikimybių teorijos, matematinio programavimo kai kuriuos atskirus klausimus.

Kol moksliniai tyrimai apsiribodavo teoriniais algorimų teorijos klausimais, praktinio uždavinio sprendimo laikas, naudojama kompiuterių atmintis ir kiti panašūs dalykai nebuvo aktualūs. Kompiuterinės technikos vystymas suteikė praktines galimybes realiems diskrečiojo pobūd-

žio uždaviniams spręsti ir paskatino matematikų interesą diskrečiosios matematikos problemoms.

Pastaraisiais metais diskrečiosios matematikos kursai vis dažniau įtraukiami į aukštųjų mokyklų programas, ruošiant ne tik matematikus, bet ir inžinierius. Ši mokomoji knygelė skirta aukštųjų mokyklų studentams, pradedantiems studijuoti diskrečiąją matematiką. Joje dėstomi šie diskrečiosios matematikos skyriai: matematinės logikos ir bulinių funkcijų pradmenys, baigtinių bei skaičiųjų aibių teorija ir kombinatorinės analizės elementai, sąryšių teorija, informacijos kodavimo teorijos pagrindai, grafų teorija, grafų analizės algoritmai bei algoritmų sudėtingumo teorijos sąvokos. Diskrečiosios matematikos kursą, atitinkantį mokymo knygelės turinį, autorius daug metų skaito VGTU inžinerinės informatikos bei elektronikos specialybės studentams.

Autorius dėkoja docentams Juozui Raulynaičiui ir Mečislavui Meilūnui, pateikusiems nemažai vertingų pastabų.

Aleksandras Krylovas

1. Matematinės logikos ir Bulio funkcijų pradmenys

1.1. Matematinės logikos įžanga

Teiginio sąvoka

Logika nagrinėja mąstymo dėsnius, užtikrinančius jo taisyklingumą, t. y. apibrėžtumą, neprieštaringumą, nuoseklumą, pagrįstumą. Viena pagrindinių, bazinių, pirminių logikos sąvokų yra ***teiginys*** – toks sakinys, tvirtinimas, reiškimas, kuris visada yra arba *teisingas*, arba *klaidingas*. Pavyzdžiui, sakinys "2>5" klaidingas ir todėl yra teiginys, o sakinys "$\alpha = \beta$" nėra teiginys, kadangi jis gali būti ir teisingas, ir klaidingas priklausomai nuo α ir β reikšmių. Tokio pavidalo sakiniai vadinami *predikatais* ir bus nagrinėjami vėliau (žr. 1.6.). Nagrinėjamų logikoje samprotavimų turinys nėra svarbus: logika domisi teisingų samprotavimų sudarymo *formomis*. Todėl svarbios yra tik teiginių reikšmės: *tiesingas* arba *klaidingas*, kurios žymimos "TRUE", "FALSE", "T", "F", "t", "f", "1", "0", ... ir vadinamos ***loginėmis konstantomis***. Abstraktieji teiginiai žymimi $A, B, \ldots, c, d, e, \ldots, f_1, h_2, \ldots$ ir vadinami ***loginiais kintamaisiais***.

Loginės operacijos

Matematinė logika nagrinėja matematinių samprotavimų formas ir plačiai naudoja simbolius bei formules. Naujiems teiginiams sudaryti apibrėžiamos ***loginės operacijos***, kurios formalizuoja matematinių teoremų įrodymus.

Tarkime, kad x ir y yra teiginiai. Atliekant su x ir y *logines operacijas* (veiksmus), gaunami nauji teiginiai.

Apibrėžimai

Unarioji[1] loginė operacija ***neigimas*** skaitoma "ne x", "netiesa, kad x" ir žymima $\overline{x}$: x reikšmė keičiama į priešingą: $\overline{0} = 1$, $\overline{1} = 0$.

Binariosios loginės operacijos:

disjunkcija žymima $\vee$ ("x arba y"): teiginys $x \vee y$ yra teisingas, kai teisingas bent vienas iš teiginių x, y;

konjunkcija žymima $\&$ ("x ir y"): teiginys $x \,\&\, y$ yra teisingas, kai teisingi abu teiginiai x, y;

implikacija žymima $\Rightarrow$ ("jei x, tai y" arba "iš x išplaukia y"): teiginys $x \Rightarrow y$ yra klaidingas tik tuo atveju, kai teiginys x yra teisingas, o y – klaidingas;

ekvivalentumas žymima $\Leftrightarrow$ ("x tada ir tik tada, kai y"): teiginys $x \Leftrightarrow y$ yra teisingas, kai abu teiginiai x, y yra teisingi arba abu klaidingi.

Surašykime apibrėžtas logines operacijas į lentelę.

[1] Unariąja vadinama operacija su vienu kintamuoju (operandu), o binariąja – su dviem. Jas dar vadina vienvietėmis bei dvivietėmis operacijomis.

x	y	$\overline{x}$	$\overline{y}$	$x \vee y$	$x \,\&\, y$	$x \Rightarrow y$	$y \Rightarrow x$	$x \Leftrightarrow y$
0	0	1	1	0	0	1	1	1
0	1	1	0	1	0	1	0	0
1	0	0	1	1	0	0	1	0
1	1	0	0	1	1	1	1	1

Pastabos

1. Disjunkcija kartais yra vadinama *logine suma*, o konjunkcija – *logine sandauga*. Jei į 0 ir 1 žiūrėti kaip į skaičius, tai $x\&y = xy$, $x \vee y = x \oplus y \oplus xy$. Operacija $\oplus$ vadinama ***sudėtimi moduliu du***: $0 \oplus 0 = 0,\ 1 \oplus 1 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1$.

2. Implikaciją galima apibrėžti šiomis išvedimų taisyklėmis:

a) iš teisingos prielaidos (*antecedento*) išplaukia tik teisinga išvada (*konsekventas*);

b) klaidinga išvada išplaukia tik iš klaidingos prielaidos.

3. Loginės operacijos literatūroje gali būti pažymėtos ir kitaip:

$\neg$, $'$ (neigimas), $\wedge$ (konjunkcija), $\rightarrow$, $\supset$ (implikacija), $\leftrightarrow$, $\equiv$, $\sim$ (ekvivalentumas).

1.2. Teiginių algebra

Propozicinės formulės

Teisingų loginių formulių sudarymo taisyklės nepriklauso nuo apibrėžtų loginių operacijų turinio[2]. Norėdami pabrėžti, kad nagrinėsime logines formules tik kaip algebrinius (formaliuosius) reiškinius ir šių formulių reikšmių kol kas neskaičiuosime, kintamuosius (loginius) vadinsime ***propoziciniais***, operacijas vadinsime ***propozicinėmis jungtimis***, o pačias formules – ***propozicinėmis***.

[2] Jos gali būti apibrėžtos ir kitaip. Žr. 1.4.

Apibrėžimai
Teiginių algebros ***abėcėle*** vadinama aibė

$$\mathfrak{A} = \{a, b, \ldots, A, B, \ldots, x_1, \cdots, Y_2, \cdots,$$
$$\neg,\ \&,\ \vee, \Rightarrow,\ \Leftrightarrow,$$
$$(\ ,\ )\ \}.$$

Aibės $\mathfrak{A}$ elementai – propoziciniai kintamieji, propozicinės jungtys bei skliaustai vadinami *raidėmis*. Baigtinės abėcėlės $\mathfrak{A}$ raidžių sekos vadinamos ***žodžiais***.
Kai kurie žodžiai vadinami teiginių skaičiavimo virš aibės $\mathfrak{A}$ ***formulėmis***. Formulės apibrėžiamos jų sudarymo taisyklėmis:
(1) $a, b, \ldots, A, B, \ldots, x_1, \cdots, Y_2, \cdots$ yra formulės;
(2) jei A yra formulė, tai $(\neg A)$ – formulė;
(3) jei A ir B yra formulės,
tai $(A\&B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ – formulės;
(4) kitų formulių nėra.

Pavyzdžiai
Žodis $z_1 = A\&\neg B$ nėra formulė, kadangi sudarytas ne pagal ***(1)–(4)*** taisykles.
Žodis $F = ((\neg p)\&((x \vee y) \Rightarrow z))$ yra formulė, kuri sudaryta taip. Kintamasis p yra formulė pagal ***(1)*** taisyklę. Žodis $F_1 = (\neg p)$ yra formulė pagal ***(2)*** taisyklę. Kintamieji x, y ir z pagal ***(1)*** yra formulės. Pagal ***(3)*** gauname dar dvi formules $F_2 = (x \vee y)$ ir $F_3 = (F_2 \Rightarrow z)$. Galutinai pagal ***(3)*** turime $F = (F_1\&F_3)$.

Susitarkime įeinančias į formulę kitas formules vadinti jos ***poformuliais***. Taigi formulės F_1, F_2 ir F_3 yra formulės F poformuliai.

Formulės gylys

Visų formulių aibę $\mathbb{F}$ galima apibrėžti ir taip.
Apibrėžimas (rekursinis)

$\mathbb{F}_0 = a, b, \ldots, A, B, \ldots, x_1, \cdots, Y_2, \cdots;$
$\mathbb{F}_{n+1} = \mathbb{F}_n \cup \{(\neg x) : x \in \mathbb{F}_n\} \cup$
$\{(x\&y) : x, y \in \mathbb{F}_n\} \cup \{(x \vee y) : x, y \in \mathbb{F}_n\} \cup$
$\{(x \Rightarrow y) : x, y \in \mathbb{F}_n\} \cup \{(x \Leftrightarrow y) : x, y \in \mathbb{F}_n\};$
$\mathbb{F} = \bigcup_{n=0,1,\ldots} \mathbb{F}_n.$

Apibrėžimas. Formulės F ***gyliu*** vadinamas skaičius $n_0 = \min_{F \in \mathbb{F}_n} n$.

Taigi propoziciniai kintamieji sudaro aibę $\mathbb{F}_0$ ir yra nulinio gylio formulės. Aibę $\mathbb{F}_1$ sudaro propoziciniai kintamieji ir visos jų kombinacijos su viena propozicine jungtimi. Aibė $\mathbb{F}_2$ sudaryta iš visų aibės $\mathbb{F}_1$ formulių bei formulių, gaunamų iš šių, taikant vieną propozicinę jungtį.

Anksčiau išnagrinėto pavyzdžio $F = ((\neg p)\&((x \vee y) \Rightarrow z))$ poformuliai F_1 ir F_2 turi gylį 1, poformulis F_3 yra gylio 2, o pačios formulės F gylis lygus 3.

Žodis $z_1 = A\&\neg B$, kaip jau buvo minėta, nėra sudarytas pagal ***(1)-(4)*** taisykles ir todėl nėra formulė. Norėdami jį pataisyti, turime rašyti papildomus skliaustus: $z_1\prime = (A\&(\neg B))$. Tačiau šių skliaustų prasmė akivaizdi ir jie yra praktiškai nereikalingi. Galima susitarti ***nerašyti*** *išorinių skliaustų*. Tada $z_1\prime\prime = A\&(\neg B)$ yra formulė.

Dar svarbesnis yra susitarimas dėl ***operacijų prioriteto***. Operacijos $\neg$, $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ surašytos prioriteto mažėjimo tvarka, t. y. *neigimas* ($\neg$) turi aukščiausią prioritetą, o *ekvivalentumas* ($\Leftrightarrow$) – žemiausią. Tada, jei $A\&(\neg B)$ yra formulė, tai ir $A\&\neg B$ yra formulė. Jei $(A\&B) \Rightarrow C$ yra formulė, tai $A\&B \Rightarrow C$ irgi yra formulė.

Pastebėkime, kad operacijų prioritetų nustatymas neleidžia *visai atsisakyti* skliaustų. Pavyzdžiui, formulė $A \vee B\&C$ reiškia tik antrą iš dviejų iš esmės skirtingų formulių: $x = (A \vee B)\&C$ arba $y = A \vee (B\&C)$. Formulių užrašymas be skliaustų pavidalu "$operacija\ operandai$" vadinamas ***prefiksiniu***, o kitas pavidalas – "$operandai\ operacija$" – ***postfiksiniu*** (tradicinis pavidalas su skliaustais – ***infiksinis***). Prefiksinis bei postfiksinis formulių pavidalai leidžia *visai nerašyti* skliaustų. Pavyzdžiui,
$x = \& \vee ABC = ABC \vee \&$,

$y = \vee A\&BC = ABC\&\vee$,
$F = \neg p\&(x \vee y \Rightarrow z) = \&\neg p \Rightarrow \vee xyz$.

1.3. Logikos formulių semantika

Tautologijos

Tarkime, kad $X = (x_1, x_2, \ldots, x_n)$ yra loginių kintamųjų rinkinys, $F(X)$ – loginė formulė.

Apibrėžimai
Loginių kintamųjų x_j reikšmių $\{0, 1\}$ rinkinį $\nu = (\nu_1, \nu_2, \ldots, \nu_n)$ vadiname loginių kintamųjų ***interpretacija***. Pavyzdžiui, $\nu^{(1)} = (0, 1, 0)$ ir $\nu^{(2)} = (1, 0, 1)$ yra dvi kintamųjų (x, y, z) interpretacijos
Formulė F vadinama ***įvykdoma*** su interpretacija ν, jei $F(\nu) = 1$.
Pavyzdžiui, formulė $x\&y$ yra įvykdoma su interpretacija $\nu = (1, 1)$.
Formulė F vadinama ***tautologija*** (***tapačiai teisinga***), jei ji yra įvykdoma su bet kuria interpretacija.
Formulė F vadinama ***prieštara***, jei su bet kuria interpretacija ν:
$F(\nu) = 0$.
Pastebėkime, kad F yra prieštara tada ir tik tada, kai $\neg F$ yra tautologija.
Formulės F ir G yra vadinamos ***ekvivalenčiomis***, jei su bet kuria interpretacija ν: $F(\nu) = G(\nu)$.
Formulės F ir G yra ekvivalenčios tada ir tik tada, kai formulė
$(F) \Leftrightarrow (G)$ yra tautologija.

Teisingumo lentelės

Žinodami įeinančių į loginę formulę loginių kintamųjų reikšmes, atliekame logines operacijas (žr. 1.1.) ir surandame loginių formulių reikšmes, kurias įrašome į ***teisingumo reikšmių lentelę***.

Pavyzdys. Formulės

$$f(x_1, x_2, x_3) = (x_1 \Rightarrow \overline{x}_2) \ \& \ (\overline{x}_1 \Rightarrow x_3)$$

reikšmes bei jų skaičiavimo eigą nusako ši teisingumo reikšmių lentelė.

x_1	x_2	x_3	$\overline{x}_1$	$\overline{x}_2$	$x_1 \Rightarrow \overline{x}_2$	$\overline{x}_1 \Rightarrow x_3$	$f(x_1, x_2, x_3)$
0	0	0	1	1	1	0	0
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	0
0	1	1	1	0	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	0	0	1	0
1	1	1	0	0	0	1	0

Logikos dėsniai

Tautologijos dar yra vadinamos ***logikos dėsniais***. Surašykime svarbiausius iš jų į lentelę[3].

[3]Atkreipkime dėmesį, kad ekvivalentumo ženklas $\Leftrightarrow$ yra loginė operacija. Visų lentelės formulių reikšmė lygi 1.

Pavadinimas	Formulė
konjunkcijos ***komutatyvumas***	$(x \,\&\, y) \;\Leftrightarrow\; (y \,\&\, x)$
disjunkcijos ***komutatyvumas***	$(x \vee y) \;\Leftrightarrow\; (y \vee x)$
konjunkcijos ***asociatyvumas***	$((x \,\&\, y) \,\&\, z) \;\Leftrightarrow\; (x \,\&\, (y \,\&\, z))$
disjunkcijos ***asociatyvumas***	$((x \vee y) \vee z) \;\Leftrightarrow\; (x \vee (y \vee z))$
negalimo trečiojo dėsnis	$x \vee \overline{x}$
dvigubas neigimas	$\overline{\overline{x}} \;\Leftrightarrow\; x$
prieštaravimas	$\overline{x \,\&\, \overline{x}}$
silogizmas	$((x \Rightarrow y) \,\&\, (y \Rightarrow z)) \;\Leftrightarrow\; (x \Rightarrow z)$
distributyvumas	$(x \,\&\, (y \vee z)) \;\Leftrightarrow\; ((x \,\&\, y) \vee (x \,\&\, z))$ $(x \vee (y \,\&\, z)) \;\Leftrightarrow\; ((x \vee y) \,\&\, (x \vee z))$
idempotentumas	$(x \vee x) \;\Leftrightarrow\; x$ $(x \,\&\, x) \;\Leftrightarrow\; x$
kontrapozicija	$(x \Rightarrow y) \Leftrightarrow (\overline{y} \Rightarrow \overline{x})$
de Morgano dėsniai	$\left(\overline{x \,\&\, y}\right) \;\Leftrightarrow\; (\overline{x} \vee \overline{y})$ $(\overline{x \vee y}) \;\Leftrightarrow\; (\overline{x} \,\&\, \overline{y})$

Visas formules galima įrodyti, sudarant jų teisingumo reikšmių lenteles. Įrodykime, pavyzdžiui, pirmąjį de Morgano[4] dėsnį:

[4] Augustus de Morgan (1806 – 1871) – škotų matematikas ir logikas.

x	y	$\overline{x}$	$\overline{y}$	$x \,\&\, y$	$\overline{x \,\&\, y}$	$\overline{x} \vee \overline{y}$	$\left(\overline{x \,\&\, y}\right) \Leftrightarrow (\overline{x} \vee \overline{y})$
0	0	1	1	0	1	1	1
0	1	1	0	0	1	1	1
1	0	0	1	0	1	1	1
1	1	0	0	1	0	0	1

Tautologijų nustatymo metodai

Teisingumo reikšmių lentelės metodas yra universalus, bet reikalauja daug darbo. Kartais įrodyti, kad formulė yra tautologija galima greičiau, taikant *prieštaros* bei *ekvivalenčiųjų pertvarkių* metodus.

Pavyzdžiai

1. Įrodykime prieštaros metodu, kad formulė $F = (A \Rightarrow (B \Rightarrow A))$ yra tautologija. Sprendžiame lygtį $F = 0$. Implikacija $\Rightarrow$ įgyja nulinę reikšmę tik kai $1 \Rightarrow 0$. Taigi turi būti $A = 1$, $(B \Rightarrow A) = 0$. Gauname, kad $(B \Rightarrow 1) = 0$, o tokių reikšmių B nėra. Todėl lygtis $F = 0$ neturi sprendinių ir visais atvejais gauname $F = 1$, t. y. formulė F yra tautologija.

2. Ekvivalenčiųjų pertvarkių metodu įrodykime, kad formulė $(A \,\&\, B) \vee (\overline{A} \vee \overline{B})$ yra tautologija. Taikome dvigubo neigimo dėsnį: $(A \,\&\, B) \Leftrightarrow \overline{\overline{(A \,\&\, B)}}$. Reiškiniui $\overline{(A \,\&\, B)}$ taikome de Morgano dėsnį: $\overline{(A \,\&\, B)} \Leftrightarrow \overline{A} \vee \overline{B}$. Taigi taikydami negalimo trečiojo dėsnį, gauname $(\overline{A} \vee \overline{B}) \vee (\overline{A} \vee \overline{B}) \Leftrightarrow 1$.

1.4. Teiginių skaičiavimas

Loginės išvados

Apibrėžkime kitą logikos dėsnių įrodymo metodą. Pirma suformuluosime taisyklę, pagal kurią galima gauti naujus logikos dėsnius (teoremas). Toliau (žr. 1.4.) nagrinėsime pradinius dėsnius – aksiomas, leidžiančias įrodyti *visus* logikos dėsnius.

Apibrėžimas
Loginė formulė y vadinama ***logine išvada*** iš formulių $x_1, x_2, \ldots, x_n$, jeigu implikacija

$$(x_1 \& x_2 \& \ldots \& x_n) \Rightarrow y$$

yra tautologija.

Žinodami, pavyzdžiui, kad x yra tautologija, gauname, kad $x \vee y$ irgi yra tautologija. Tai dažnai užrašoma kaip ***išvedimo taisyklė***:

$$\frac{x}{\therefore\ x \vee y}.$$

Surašykime pagrindines išvedimo taisykles į lentelę.

(1)	$x \Rightarrow (x \vee y)$	$\dfrac{x}{\therefore\ x \vee y}$
(2)	$(x \,\&\, y) \Rightarrow x$	$\dfrac{x \,\&\, y}{\therefore\ x}$
(3)	$((x \Rightarrow y) \,\&\, x) \Rightarrow y$	$\dfrac{x \Rightarrow y,\ x}{\therefore\ y}$
(4)	$((x \Rightarrow y) \,\&\, \overline{y}) \Rightarrow \overline{x}$	$\dfrac{x \Rightarrow y,\ \overline{y}}{\therefore\ \overline{x}}.$
(5)	$(((x \Rightarrow y) \,\&\, (z \Rightarrow w)) \,\&\, (x \vee z)) \Rightarrow (y \vee w)$	$\dfrac{(x \Rightarrow y) \& (z \Rightarrow w),\ x \vee z}{\therefore\ y \vee w}$
(6)	$(x \Rightarrow y) \Rightarrow (\overline{y} \Rightarrow \overline{x})$	$\dfrac{x \Rightarrow y}{\therefore\ \overline{y} \Rightarrow \overline{x}}$
(7)	$(x \Rightarrow y) \,\&\, (y \Rightarrow z)) \Rightarrow (x \Rightarrow z)$	$\dfrac{x \Rightarrow y\ ,\ y \Rightarrow z}{\therefore\ x \Rightarrow z}$

Šios taisyklės yra vadinamos: (1) – sudėtis; (2) – suprastinimas; (3) – *modus ponens*; (4) – *modus tollens*; (5) – konstrukcinė dilema; (6) – kontrapozicija; (7) – silogizmas.

Aksiominis metodas

Formalioji matematinė teorija T apibrėžiama keliomis taisyklėmis. Mes suformuluosime jas ir iš karto išnagrinėsime *teiginių skaičiavimą* L kaip tokios teorijos pavyzdį.

(F) Apibrėžiami teorijos L simboliai, kurie vadinami jos *abėcėle*. Šių abėcėlės simbolių baigtinės sekos vadinamos *žodžiais*. Teiginių skaičiavimo formaliosios teorijos L simboliai jau buvo apibrėžti 1.2. skyriuje. Priminsime, kad tai buvo raidės su indeksais arba be jų, loginės operacijos bei skliaustai. Pridėkime prie jų dar kablelį $(,)$, kuris naudojamas išvedimo taisyklėse. Po to apibrėžiamos teorijos *formulių* sudarymo taisyklės, leidžiančios išsiaiškinti ar žodis yra formulė. Tokios taisyklės jau buvo išnagrinėtos (žr. 1.2.).

(A) Išskiriamos teorijos formulės, kurios vadinamos jos *aksiomomis*. Teiginių skaičiavimo aksiomos gali būti[5] tokios: (A, B, C – bet kurios formulės)

$$\begin{array}{ll} \text{(A1)} & (A \Rightarrow (B \Rightarrow C)); \\ \text{(A2)} & (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)); \\ \text{(A3)} & (\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)). \end{array}$$

(MP) Nurodytos *išvedimo taisyklės*, leidžiančios iš vienų teorijos formulių gauti kitas. Teiginių skaičiavimo teorija turi tik vieną išvedimo taisyklę *modus ponens*: B yra *tiesioginė išvada* iš A ir $A \Rightarrow B$ arba trumpiau

$$\frac{A,\ A \Rightarrow B}{\therefore\ B}.$$

Visos teiginių skaičiavimo formulės, kurias galima gauti, taikant aksiomas (A1) – (A3) bei (MP) išvedimo taisyklę, yra teiginių skaičiavimo

[5] Pastebėkime, kad čia dėstomas tik vienas galimas teiginių logikos formalizavimas.

teoremos (jos žymimos $\models$ arba $\vdash$).
Teorema. $\vdash A \Rightarrow A$.
Įrodymas. Įstatome į (A2) $B = (A \Rightarrow A)$ ir $C = A$:
$(1) \quad (A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$.
Rašydami (A1) formulėje $A \Rightarrow A$ vietoje B, gauname
$(2) \quad (A \Rightarrow ((A \Rightarrow A) \Rightarrow A))$.
Taikome išvedimo (MP) taisyklę gautoms (1), (2) formulėms:
$(3) \quad (((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$.
Vėl taikome (A1) aksiomą su $B = A$ ir $C = A$:
$(4) \quad (A \Rightarrow (A \Rightarrow A))$.
Galutinai iš (3) ir (4) formulių pagal (MP) taisyklę gauname
$(5) \quad (A \Rightarrow A)$.

Pastabos
Aksiomose (A1) – (A3) panaudotos tik dvi loginės operacijos: neigimas ($\neg$) bei implikacija ($\Rightarrow$). Todėl teiginių algebros formules galima apibrėžti nenaudojant kitų operacijų. Tada konjunkcijos, disjunkcijos bei ekvivalentumo operacijas galima įvesti tokiais apibrėžimais:

(D1) $(A \,\&\, B) \equiv (\neg(A \Rightarrow \neg B))$;
(D2) $(A \vee B) \equiv ((\neg A) \Rightarrow B))$;
(D3) $(A \Leftrightarrow B) \equiv ((A \Rightarrow B) \,\&\, (B \Rightarrow A))$.

Įrodyta teiginių skaičiavimo formaliosios teorijos L teorema $\vdash A \Rightarrow A$ yra tautologija. Tai yra bendrasis rezultatas: *visos* teorijos L *teoremos yra tautologijos*. Galima įrodyti ir atvirkštinį teiginį: jei formulė yra tautologija ji yra ir teorijos L teorema. Tai reiškia, kad teorija yra *pilnoji*. Dar vienas bendrasis matematinės logikos rezultatas yra teorijos L *neprieštaringumas*: neegzistuoja tokia teorijos formulė A, kad ir A, ir $\neg A$ yra teoremos.

1.5. Bulio funkcijos

Bulio funkcijos apibrėžimas

Tarkime, kad kintamieji $x_1, x_2, \ldots, x_n$ ir funkcija $f(x_1, x_2, \ldots, x_n)$ įgyja tik dvi reikšmes, kurias žymėsime $0, 1$. Tokias funkcijas bei kintamuosius vadinsime ***buliniais*** arba Bulio[6] ***kintamaisiais*** ir ***bulinėmis funkcijomis***. Išnagrinėkime dviejų kintamųjų bulinę funkciją $f(x_1, x_2)$. Kadangi kintamieji įgyja tik dvi reikšmes $0, 1$ ir funkcijos reikšmių irgi yra tik dvi, tai egzistuoja lygiai 16 skirtingų dviejų kintamųjų bulinių funkcijų. Surašykime visas jas į lentelę.

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0

x_1	x_2	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1
1	1	1	1	1	1	1	1	1	1

Funkcijų reiškimas formulėmis

Pastebėkime, kad funkcijos f_0 ir f_{15} yra konstantos: $f_0 = 0$, $f_{15} = 1$. Funkcija $f_{10} = x_2$ nepriklauso nuo kintamojo x_1, o funkcija $f_{12} = x_1$ – nuo x_2.

Apibrėžimai

Bulinės funkcijos $f(x_1, x_2, \ldots, x_n)$ kintamasis x_j $(0 \leqslant j \leqslant n)$ vadinamas ***fiktyviuoju***, jei

$$f(\ldots, x_{j-1}, 0, x_{j+1}, \ldots) = f(\ldots, x_{j-1}, 1, x_{j+1}, \ldots).$$

[6] George Boole (1815 – 1864) – anglų matematikas ir logikas.

Kintamieji, kurie nėra fiktyvieji vadinami ***esminiais***.
Taigi funkcijos f_0 ir f_{15} neturi esminių kintamųjų. Funkcijų f_{10} ir f_{12} esminiai kintamieji yra x_2 ir x_1, o fiktyvieji – x_1 ir x_2.

Funkcijos f_3, f_5, f_8, f_9, f_{11}, f_{13}, f_{14} išreiškiamos apibrėžtomis 1.1. skyriuje (pagerefml.li.lopr psl.) operacijomis:

f_3	f_5	f_8	f_9	f_{11}	f_{13}	f_{14}
$\overline{x}_1$	$\overline{x}_2$	$x_1 \& x_2$	$x_1 \Leftrightarrow x_2$	$x_1 \Rightarrow x_2$	$x_2 \Rightarrow x_1$	$x_1 \vee x_2$

Funkcijos f_2, f_4, f_6 išreiškiamos taip:

f_1	f_2	f_4	f_6	f_7
$\overline{x_1 \vee x_2}$	$\overline{x_2 \Rightarrow x_1}$	$\overline{x_1 \Rightarrow x_2}$	$(x_1 \vee x_2)\&(\overline{x}_1 \vee \overline{x}_2)$	$\overline{x_1 \& x_2}$

1.1. skyriuje (žr. 9 psl.) buvo minėta funkcija $\oplus$, kuri yra vadinama ***sudėtimi moduliu du***. Galima įrodyti (pakanka sudaryti teisingumo lentelę), kad

$$(x_1 \oplus x_2) \Leftrightarrow ((x_1 \vee x_2)\&(\overline{x}_1 \vee \overline{x}_2)).$$

Susitarkime rašyti *lygybės ženklą* ($=$), kai tą pačią bulinę funkciją reiškiame skirtingomis formulėmis. Taigi

$$f_6(x_1, x_2) = x_1 \oplus x_2 = (x_1 \vee x_2)\&(\overline{x}_1 \vee \overline{x}_2).$$

Funkcija f_1 yra vadinama ***Pirso***[7] ***rodykle*** ir žymima $\downarrow$:

$$f_1(x_1, x_2) = x_1 \downarrow x_2 = \overline{x_1 \vee x_2} = \overline{x}_1 \& \overline{x}_2.$$

Funkcija f_7 žymima $|$ ir yra vadinama ***Šeferio***[8] ***brūkšneliu***:

$$f_7(x_1, x_2) = x_1 | \, x_2 = \overline{x_1 \& x_2} = \overline{x}_1 \vee \overline{x}_2.$$

[7] Charles Peirce (1839 – 1914) – amerikiečių matematikas, filosofas ir logikas.
[8] Henry Sheffer (1883 – 1964) – amerikiečių logikas.

Teorema
Bet kuri loginė formulė gali būti užrašyta, taikant tik vieną loginę operaciją ($\downarrow$) arba ($|$).
Įrodymas. Užtenka įsitikinti, kad neigimas išreiškiamas taip: $\overline{x} \Leftrightarrow (x|x)$. Tada $(x\&y) \Leftrightarrow ((x|y)\,|\,(x|y))$. Disjunkciją išreiškiame, taikant šias formules ir de Morgano dėsnį (arba žr. formules (D1) – (D3), 18 psl.) Pastebėję, kad $(x \downarrow y) \Leftrightarrow (\overline{x}\&\overline{y})$, gauname įrodymą Pirso rodyklei.

Dualumo principas

Apibrėžimas
Funkcija $f_1(x_1, x_2, \ldots, x_n)$ yra vadinama ***dualiąja*** funkcijai $f_2(x_1, x_2, \ldots, x_n)$, jei

$$f_1(x_1, x_2, \ldots, x_n) = \overline{f}_2(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n).$$

Pastebėkime, kad

$$f_2(x_1, x_2, \ldots, x_n) = \overline{\overline{f}}_2(\overline{\overline{x}}_1, \overline{\overline{x}}_2, \ldots, \overline{\overline{x}}_n) = \overline{f}_1(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n).$$

Taigi jei funkcija f_1 yra dualioji funkcijai f_2, tai ir funkcija f_2 yra dualioji funkcijai f_1. Pavyzdžiui, kai $f_1(x, y) = x \vee y$ ir $f_2(x, y) = x\&y$ turime

$$\overline{f}_1(\overline{x}, \overline{y}) = \overline{\overline{x} \vee \overline{y}} = \overline{\overline{x}}\&\overline{\overline{y}} = x \;\&\; y = f_2(x, y),$$
$$\overline{f}_2(\overline{x}, \overline{y}) = \overline{\overline{x}\&\overline{y}} = \overline{\overline{x}} \vee \overline{\overline{y}} = x \;\vee\; y = f_1(x, y).$$

Funkcijos $f(x_1, x_2, \ldots, x_n)$ ***dualiąją*** funkciją $\overline{f}(\overline{x}_1, \ldots, \overline{x}_n)$ žymėsime $f^*(x_1, \ldots, x_n)$. Tada $f_1^*(x, y) = f_2(x, y)$ ir $f_2^*(x, y) = f_1(x, y)$.

Apibrėžimas
Funkcija $f(x_1, \ldots, x_n)$ vadinama ***savidualiąja***, kai

$$f^*(x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

Pavyzdžiui, funkcija $f(x, y, z) = x\&y \vee x\&z \vee y\&z$ yra savidualioji.

Normaliosios formos

Loginę funkciją galima išskleisti jos kintamaisiais:

$$f(x_1, x_2) = x_1 \& f(1, x_2) \vee \overline{x}_1 \& f(0, x_2).$$

Taikant šią formulę dar kartą, gaunama fukcijos $f(x_1, x_2)$ disjunkcinė forma:

$$x_1 \& x_2 \& f(1,1) \vee x_1 \& \overline{x}_2 \& f(1,0) \vee \overline{x}_1 \& x_2 \& f(0,1) \vee \overline{x}_1 \& \overline{x}_2 \& f(0,0).$$

Susitarkime praleisti formulėse konjunkcijos ženklą ($\&$) ir paliksime tik tuos narius, kur $f(\cdots) = 1$.

Pavyzdys
Užrašykime funkcijos, apibrėžtos jos teisingumo reikšmių lentele, disjunkcinę normaliąją formą.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Matome, kad nelygios nuliui tik trys funkcijos reikšmės: $f(0,0,1)$, $f(1,0,0)$ ir $f(1,0,1)$. Todėl funkcijos disjunkcinė normalioji forma yra tokia:

$$f(x_1, x_2, x_3) = \overline{x}_1 \overline{x}_2 x_3 \vee x_1 \overline{x}_2 \overline{x}_3 \vee x_1 \overline{x}_2 x_3.$$

Pažymėkime

$$x^\sigma = \begin{cases} \overline{x}, & \sigma = 0 \\ x, & \sigma = 1. \end{cases}$$

T. y. $x^x = 1$ ir kai $x \neq y : x^y = 0$.
Pastebėkime dar, kad $\overline{x^\sigma} = \overline{x}^\sigma = x^{\overline{\sigma}}$.
Kiekviena (išskyrus $const = 0$) loginė funkcija užrašoma ***disjunkcine normaliąja forma***:

$$f(x_1, x_2, \ldots, x_n) = \bigvee_{f(\sigma_1,\sigma_2,\ldots,\sigma_n)=1} x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n}.$$

Pastebėkime, kad formulėje yra visi kintamieji $x_1, x_2, \ldots, x_n$. Ši disjunkcinė forma yra vadinama ***tobulaja***. Taikydami ekvivalenčiuosius loginius pertvarkius

$$x \vee xy = x(x \vee y) = x,\ xy \vee x\overline{y} = x,\ x \vee x\overline{y} = x \vee y,$$

bet kurią disjunkcinę normaliąją formą, galima suvesti į tobuląją.

Pavyzdys

$$xy \vee \overline{x}\,\overline{z} = xyz \vee xy\overline{z} \vee \overline{x}y\overline{z} \vee \overline{x}\,\overline{y}\,\overline{z}.$$

Panašiai disjunkcinei normaliąjai formai apibrėžiama ***tobuloji konjunkcinė normalioji forma***:

$$f(x_1, x_2, \ldots, x_n) = \bigwedge_{f^*(\sigma_1,\sigma_2,\ldots,\sigma_n)=1} \left(x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee \cdots \vee x_n^{\sigma_n}\right).$$

Įrodykime, kad kiekvieną bulinę funkciją $f(x_1, x_2, \ldots, x_n)$ (išskyrus $const = 1$) galima išreikšti tobulaja *konjunkcine* normaliaja forma. Pagal dualiosios funkcijos $f^*(x_1, x_2, \ldots, x_n)$ apibrėžimą, taikydami šios

funkcijos tobuląją *disjunkcinę* normaliąją formą, turime

$$f(x_1,x_2,\dots,x_n)=\overline{f}^*(\overline{x}_1,\overline{x}_2,\dots,\overline{x}_n)=$$
$$\overline{\bigvee_{f^*(\sigma_1,\sigma_2,\dots,\sigma_n)=1}\overline{x}_1^{\sigma_1}\&\overline{x}_2^{\sigma_2}\&\dots\&\overline{x}_n^{\sigma_n}}=$$
$$\bigwedge_{f^*(\sigma_1,\sigma_2,\dots,\sigma_n)=1}(x_1^{\sigma_1}\vee x_2^{\sigma_2}\vee\dots\vee x_n^{\sigma_n})=$$
$$\bigwedge_{f(\sigma_1,\sigma_2,\dots,\sigma_n)=0}\left(x_1^{\overline{\sigma}_1}\vee x_2^{\overline{\sigma}_2}\vee\dots\vee x_n^{\overline{\sigma}_n}\right).$$

Taigi (22 p.) lentelėje apibrėžtos funkcijos $f(x_1,x_2,x_3)$ tobuloji konjunkcinė normalioji forma yra

$$(x_1\vee x_2\vee x_3)\&(x_1\vee\overline{x}_2\vee x_3)\&(x_1\vee\overline{x}_2\vee\overline{x}_3)\&(\overline{x}_1\vee\overline{x}_2\vee x_3)\&(\overline{x}_1\vee\overline{x}_2\vee\overline{x}_3).$$

Pilnosios funkcijų sistemos

Apibrėžimai

(T_0) Bulio funkciją $f(x_1,x_2,\dots,x_n)$ vadiname ***nekeičiančia nulio***, jei

$$f(0,0,\dots,0)=0.$$

Visų tokių funkcijų klasę (aibę) žymėsime T_0.

(T_1) Panašiai apibrėžiama ***nekeičiančių vieneto*** bulinių funkcijų klasė:

$$T_1=\{f: f(1,1,\dots,1)=1\}.$$

Pavyzdžiui, funkcijos $f(x)=x$, $g(x,y)=x\vee y$, $h(x,y)=x\&y$ priklauso abiems klasėms, o funkcija $w(x)=\overline{x}$ – nė vienai.

(T_*) ***Savidualiųjų*** funkcijų klasę pažymėkime T_*:

$$T_* = \{f : f(x_1, x_2, \ldots, x_n) = f^*(x_1, x_2, \ldots, x_n)\}.$$

Šiai klasei priklauso, pavyzdžiui, funkcijos $f(x) = x$ bei $w(x) = \overline{x}$.

($T_\leqslant$) Tarkime, kad $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ ir $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ yra du bulinių kintamųjų rinkiniai. Susitarkime rašyti $\alpha \preccurlyeq \beta$ (arba $\beta \succcurlyeq \alpha$), kai $\alpha_j \leqslant \beta_j$ su visais $j = 1, 2, \ldots, n$. Pastebėkime, kad ne visi bulinių kintamųjų rinkiniai α ir β tenkina kurią nors iš sąlygų $\alpha \preccurlyeq \beta$ arba $\beta \succcurlyeq \alpha$. Pavyzdžiui, $(0,0) \preccurlyeq (0,1) \preccurlyeq (1,1)$, tačiau ***negalima rašyti*** $(0,1) \preccurlyeq (1,0)$ arba $(0,1) \succcurlyeq (1,0)$. Apibrėžkime ***monotoninių*** funkcijų klasę

$$T_\leqslant = \{f : \alpha \preccurlyeq \beta \Rightarrow f(\alpha) \leqslant f(\beta)\}.$$

Pavyzdžiui, funkcijos $g(x, y) = x \vee y$, $h(x, y) = x\&y$ yra monotoninės.

(T_L) ***Tiesinių*** funkcijų klasė apibrėžiama taip [9]:

$$T_L = \{f : f(x_1, x_2, \ldots, x_n) = c_0 \oplus c_1\&x_1 \oplus c_2\&x_2 \oplus \cdots \oplus c_n\&x_n\}.$$

Čia $c_j \in \{0, 1\}$ yra tiesinio darinio koeficientai. Funkcijos $f(x) = x$ ir $w(x) = \overline{x}$ yra tiesinės:
$f(x) = x = 0 \oplus 1\&x$, $w(x) = \overline{x} = x \oplus 1 = 1 \oplus 1\&x$.
Parodysime, kad funkcija $g(x, y) = x \vee y$ ***nėra*** tiesinė. Užrašykime bendrą teisinio darinio pavidalą su neapibrėžtais koeficientais c_0, c_1, c_2:

$$g(x, y) = x \vee y = c_0 \oplus c_1\&x \oplus c_2\&y.$$

[9] Skliaustų nerašome, kadangi operacijos & prioritetas yra didesnis, negu operacijos $\oplus$.

Imdami bulinių kintamųjų x ir y reikšmes, gauname:

$$g(0,0) = 0 \vee 0 = 0 = c_0 \oplus c_1\&0 \oplus c_2\&0 = c_0,$$
$$g(0,1) = 0 \vee 1 = 1 = 0 \oplus c_1\&0 \oplus c_2\&1 = c_2,$$
$$g(1,0) = 1 \vee 0 = 1 = 0 \oplus c_1\&1 \oplus 1\&0 = c_1.$$

Taigi visi koeficientai rasti: $c_0 = 0$, $c_1 = 1$, $c_2 = 1$ ir turime $g(x,y) = x \oplus y$. Tačiau, $g(1,1) = 1 \vee 1 = 1 \neq 1 \oplus 1 = 0$ ir todėl $x \vee y \neq x \oplus y$.

Tarkime, kad bulinės funkcijos

$$f(x_1, x_2, \ldots, x_n),\ f_1(x_1, x_2, \ldots, x_n),$$
$$f_2(x_1, x_2, \ldots, x_n), \ldots,\ f_n(x_1, x_2, \ldots, x_n)$$

priklauso kuriai nors vienai funkcijų klasei T_0, T_1, T_*, $T_\leqslant$ arba T_L.
Tada sudėtinė funkcija

$$f(f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$$

priklauso tai pačiai funkcijų klasei. Taigi bulinių funkcijų klasės T_0, T_1, T_*, $T_\leqslant$, T_L yra ***uždarosios***.

Apibrėžimas
Funkcijų sistema $F = \{f_1, f_2, \ldots, f_m\}$ yra vadinama ***pilnąja***, jei bet kurią bulinę funkciją galima išreikšti šios sistemos funkcijomis.
Bet kuri bulinė funkcija išreiškiama disjunkcine arba konjunkcine normaliąja forma. Todėl funkcijų (rašome atitinkančias operecijas) sistema $\{\neg, \&, \vee\}$ yra pilnoji. Taikant de Morgano dėsnius, konjunkciją galima išreikšti neigimu bei disjunkcija ir atvirkščiai. Taigi pilnosios yra ir šios sistemos: $\{\neg, \vee\}$, $\{\neg, \&\}$. Prisiminkime, kad mes žinome dar tris pilnąsias funkcijų sistemas: $\{\neg, \Rightarrow\}$ (žr. 1.4.), $\{|\}$, $\{\downarrow\}$ (žr. 1.5.).

Bendruoju atveju nustatyti funkcijų sistemos pilnumą leidžia Posto[10] teorema.

[10] Emil Leon Post (1897 – 1954) – amerikiečių matematikas ir logikas.

Teorema
Bulio funkcijų sistema F yra pilnoji tada ir tik tada, kai ji turi bent po vieną funkciją, ***nepriklausančią*** kiekvienai klasei T_0, T_1, T_*, $T_\leqslant$, T_L, t. y. galima nurodyti bent vieną funkciją kuri ***nėra*** nekeičianti nulio, nėra nekeičianti vieneto ir t. t.

Parodykime, kad sistema $\{0, 1, \&, \oplus\}$ yra pilnoji. Konstantos 0 ir 1 nepriklauso atitinkamai klasėms T_1 ir T_0. Taip pat, šios funkcijos nėra savidualiosios. Funkcija $\oplus$ nėra monotoninė. Funkcija $\&$ nėra tiesinė. Taigi visos teoremos sąlygos yra tenkinamos ir sistema yra pilnoji.

1.6. Predikatų logika

Kvantoriai ir predikatai

Įveskime dar dvi logines operacijas, kurios vadinamos ***egzistavimo*** (žymimas $\exists$) ir ***bendrumo*** ($\forall$) ***kvantoriais***. Egzistavimo kvantorius nurodo, kad yra, galima rasti, egzistuoja tam tikras objektas: $\exists\alpha\ p(\alpha)$ skaitoma "yra tokia (tokios) α, kurios turi savybę p". Bendrumo kvantorius nurodo, kad savybę p turi visi objektai α: $\forall\alpha\ p(\alpha)$ skaitoma "su visomis (kokia bebūtų) α, yra tenkinama salyga p".

Mes jau minėjome (žr. **??**), kad sakinys "$\alpha = \beta$" nėra teiginys, kadangi jis gali būti ir teisingas, ir klaidingas priklausomai nuo α ir β reikšmių. Norėdami nagrinėti tokius sakinius, turime pasitikslinti kintamųjų α, β prigimtį: tai gali būti skaičiai, matricos, funkcijos ir t. t. Tokius kintamuosius vadiname ***dalykiniais*** kintamaisiais arba tiesiog ***kintamaisiais*** ir žymime $x, y, z, \ldots, x_1, y_2, \ldots$ Dalykinių kintamųjų reikšmes vadiname ***konstantomis*** ir žymime $\alpha, \beta, \ldots, \alpha_1, \beta_2, \ldots$

Apibrėžimas
Funkcija $P(x_1, x_2, \ldots, x_n)$ vadinama ***predikatu***, jei su bet kuria dalykinių kintamųjų $x_1, x_2, \ldots, x_n$ realizacija $\alpha_1, \alpha_2, \ldots, \alpha_n$
$P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ yra teiginys. Pavyzdžiui, kai x ir y yra realieji skai-

čiai, galime nagrinėti tokius predikatus: $P(x,y) =$ "$x^2 > y$", $G(x) =$ " $\sin x > \cos x$", $R(y) =$ "$y^2 = e^{-y}$". Tada $P(1,0)$ yra teisingas teiginys, $G(0)$ – klaidingas. Teiginys $R(\alpha)$ įgyja teisingą reikšmę, kai α tenkina lygtį $y^2 e^y = 1$.

Taikydami kvantorius ir predikatus irgi galime sudaryti teiginius: $\forall x \exists y P(x,y)$, $\exists x G(x)$ – teisingi teiginiai; $\forall y R(y)$ – klaidingas teiginys.

Termai ir formulės

Predikatų logika formalizuojama pagal tą pačią schemą kaip ir teiginių logika: apibrėžiama abėcėlė, formulių sudarymo taisyklės, aksiomos bei išvedimo taisyklės. Mes apsiribosime tik pirmuoju bei antruoju klausimais.

Atliekant veiksmus su dalykiniais kintamaisiais turime formalizuoti gaunamų reiškinių nagrinėjimą. Žymėkime visus leistinus dalykinių kintamųjų bei konstantų reiškinius $f, g, \ldots, f_1, g_2, \ldots$ ir vadinsime juos ***funkcinėmis*** raidėmis. Tai gali būti, pavyzdžiui, aritmetinės operacijos arba trigonometrinės funkcijos. Toliau nagrinėjame visus reiškinius, kuriuos galima sudaryti, taikant tas operacijas arba funkcijas.

Apibrėžimas

Termais vadiname reiškinius, kuriuos galima gauti pagal šias taisykles:
(a) kiekviena konstanta arba kintamasis yra termas;
(b) jei f yra funkcinė raidė ir $t_1, t_2, \ldots, t_n$ – termai, tai $f(t_1, t_2, \ldots, t_n)$ yra termas;
(c) nėra termų, gautų ne pagal (a), (b) taisykles;

Predikatų kalbos abėcėlė apibrėžiama kaip aibė, sudaryta iš šių elementų:
1) loginių operacijų: $\neg$, $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$;
2) pagalbinių simbolių: skliaustų () bei kablelio (,);
3) kvantorių: $\forall$, $\exists$;
4) kintamųjų;
5) konstantų;

6) funkcinių raidžių;
7) predikatinių raidžių (predikatų).

Apibrėžimai
Jei $t_1, t_2, \ldots, t_n$ yra termai, o P yra predikatas, tai $P(t_1, t_2, \ldots, t_n)$ vadiname ***elementariąja formule***.
Predikatų skaičiavimo formulės apibrėžiamos šiomis taisyklėmis:
(a) elementariosios formulės yra formulės;
(b) jei A ir B yra formulės, x – kintamasis, tai
$(\neg A)$, $(A \& B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, $(\forall x A)$, $(\exists x A)$
yra formulės;
(c) nėra formulių, gautų ne pagal (a), (b) taisykles.

Suvaržytieji ir laisvieji kintamieji

Apibrėžimas
Kintamojo ***įeitis*** į formulę nusakoma kintamuoju *simboliu* bei jo vietos formulėje *numeriu*. Vietos, kur prieš kintamąjį yra kvantorius, ***neskaičiuojamos***.

Pavyzdys
Formulėje $P(x, z) \Rightarrow \forall z(Q(y, z) \vee y = z)$ yra
viena kintamojo x įeitis;
dvi kintamojo y įeitys;
trys kintamojo z įeitys.

Kaip ir teiginių algebros formulėse (žr. 1.2.) galima išskirti predikatų skaičiavimo formulių *poformulius*. Išnagrinėto pavyzdžio formulėje turime poformulius $y = z$, $Q(y, z)$, $Q(y, z) \vee y = z$ ir t. t.

Apibrėžimai
Kintamojo x *įeitis* į formulę F vadinama ***laisvąja***, jei ji nepriklauso jokiai formulės F daliai (poformuliui), prasidedančiai $\forall x$ arba $\exists x$. Prie-

šingu atveju kintamojo x įeitis vadinama ***suvaržytaja*** formulėje F. *Kintamasis* vadinamas ***laisvuoju*** formulėje F, jei jis turi *bent vieną* laisvąją įeitį. Formulė vadinama ***uždaraja***, jei ji neturi laisvųjų kintamųjų.

Kai visi formulės F kintamieji $x_1, x_2, \ldots, x_n$ yra laisvieji, rašome $F(x_1, x_2, \ldots, x_n)$. Suvaržytųjų kintamųjų kartais nerašome. Susitarkime, kad tokiu atveju formulės F, $\forall x F$ ir $\exists x F$ yra ekvivalenčios.

Predikatų skaičiavimo dėsniai

Surašykime predikatų logikos pagrindinius dėsnius.

$$\overline{\exists x P(x)} \Leftrightarrow \forall x \overline{P(x)}$$

$$\overline{\forall x P(x)} \Leftrightarrow \exists x \overline{P(x)}$$

$$\forall x P(x) \Leftrightarrow \overline{\exists x}\ \overline{P(x)}$$

$$\exists x P(x) \Leftrightarrow \overline{\forall x}\ \overline{P(x)}$$

$$\forall x (P_1(x) \& P_2(x)) \Leftrightarrow \forall x P_1(x) \& \forall x P_2(x)$$

$$\exists x (P_1(x) \vee P_2(x)) \Leftrightarrow \exists x P_1(x) \vee \exists x P_2(x)$$

$$\forall x \forall y P(x, y) \Leftrightarrow \forall y \forall x P(x, y)$$

$$\exists x \exists y P(x, y) \Leftrightarrow \exists y \exists x P(x, y)$$

$$\forall x (P(x) \& Y) \Leftrightarrow \forall x P(x) \& Y$$

$$\forall x (P(x) \vee Y) \Leftrightarrow \forall x P(x) \vee Y$$

$$\exists x (P(x) \& Y) \Leftrightarrow \exists x P(x) \& Y$$

$$\exists x (P(x) \vee Y) \Leftrightarrow \exists x P(x) \vee Y$$

$$(\forall x P_1(x) \vee \forall x P_2(x)) \Rightarrow \forall x (P_1(x) \vee P_2(x))$$

$$(\exists x P_1(x) \& \exists x P_2(x)) \Rightarrow \exists x (P_1(x) \& P_2(x))$$

2. Aibių teorija ir kombinatorika

2.1. Aibės

Aibės sąvoka

Vieną pagrindinių šiuolaikinės matematikos sąvokų yra ***aibė***. Aibių teorijos kūrėjas Kantoras[11] manė šią sąvoką *intuityviai* aiškia. Taip suprantama aibė yra jos ***elementų*** visuma. Kai a yra aibės A elementas, rašome $a \in A$. Jei y nėra šios aibės elementas rašome $y \notin A$ arba $y \overline{\in} A$.

Pavyzdžiai
$A = \{a_1, a_2, \ldots, a_n\}$;
$\mathbb{N} = \{1, 2, 3, \ldots\}$ – natūraliųjų skaičių aibė;
$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$ – pirminių skaičių aibė;
$L = \{n \in \mathbb{N} : n = 2k,\ k = 1, 2, \ldots\}$ – lyginių natūraliųjų skaičių aibė;
$C = \{\{1, 2\}, \{1\}, \{2\}\}$;
$D = \{\mathbb{N}\}$.

Aibių reiškimas predikatais

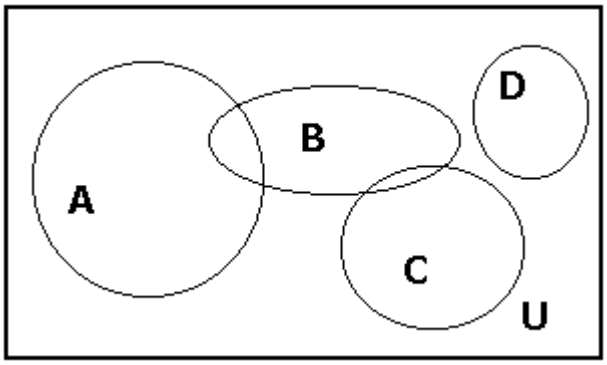
Iš pateiktų pavyzdžių matome, kad aibės gali būti baigtinės (A, C, D) ir begalinės ($\mathbb{N}$, $\mathbb{P}$, L). Aibės elementai gali būti irgi aibės (C, D). Aibės gali būti apibrėžtos surašant visus jų elementus (A, C, D) arba nurodant tam tikrą jų savybę ($\mathbb{N}$, $\mathbb{P}$, L).

Raselo[12] ***paradoksas*** rodo, kad aibės apibrėžimas, nurodant tam tikrą visų aibės elementų savybę, gali būti nekorektiškas. Apibrėžkime aibę Y, kurios elementai yra tokios aibės X, kad aibė X nėra savo elementas: $X \notin X$:

$$Y = \{X : X \notin X\}.$$

[11] Georg Cantor (1845 – 1918) – vokiečių matematikas.

[12] Bertrand Arthur William Rassel (1872 – 1970) – anglų matematikas, logikas ir filosofas.



1: Universalioji aibė U ir aibės A, B, C, D

Ar aibė $Y \in Y$? Jei $Y \in Y$, tai pagal aibės apibrėžimą $Y \notin Y$. Jei $Y \notin Y$, tai $Y \in Y$. Taigi gavome loginį prieštaravimą.

Tam kad išvengti panašių problemų galima įvesti ***universaliosios***[13] aibės U sąvoką ir nagrinėti tuos jos elementus x, kurie tenkina tam tikrą sąlygą $p(x)$. Taigi aibę P galima apibrėžti *predikatu* $p(x)$:

$$P = \{x \in U : p(x)\}.$$

Jei nė vienas elementas $x \in U$ netenkina sąlygos $p(x)$, tai aibė P neturi elementų. Tokia aibė yra vadinama ***tuščiąja*** ir žymima $\emptyset$.
Paveiksle pavaizduota universalioji aibė U ir aibės A, B, C, D. Tokios figūros vadinamos Oilerio[14] ir Veno[15] ***diagramomis***.

[13]Universalioji aibė visada priklauso nuo konkretaus uždavinio. Pavyzdžiui, nagrinėjant natūraliųjų skaičių savybes, U gali būti racionalieji, realieji arba net ir kompleksiniai skaičiai.

[14]Leonhard Euler (1707 – 1783) – šveicarų matematikas, mechanikas ir fizikas.

[15]Jonh Venn (1834 – 1923) – anglų logikas.

Kėliniai

Aibės A *elementų skaičių* žymėsime $|A|$:
$|\emptyset| = 0$, $|\{a_1, a_2, \ldots, a_n\}| = n$.

Kai $|A| = n$ yra nedidelis skaičius, visus aibės A elementus galima išvardinti. Pastebėkime, kad aibės elementų užrašymo eilės tvarka neturi reikšmės. Pavyzdžiui, aibė $\{1, 2, 3\}$ išreiškiama šešiais būdais:

$$\{1, 2, 3\} = \{1, 3, 2\} = \{2, 1, 3\} = \{2, 3, 1\} = \{3, 1, 2\} = \{3, 2, 1\}.$$

Tokie skirtingi elementų užrašymai yra vadinami ***kėliniais***. Bendru atveju n skirtingų elementų galima sukeisti vietomis

$$n! = 1 \cdot 2 \cdots (n-1) \cdot n$$

(skaitome "n – faktorialas") būdais. Taigi ir baigtinė aibė A gali būti išreikšta $|A|!$ būdais.

Aibės poaibiai

Apibrėžimas

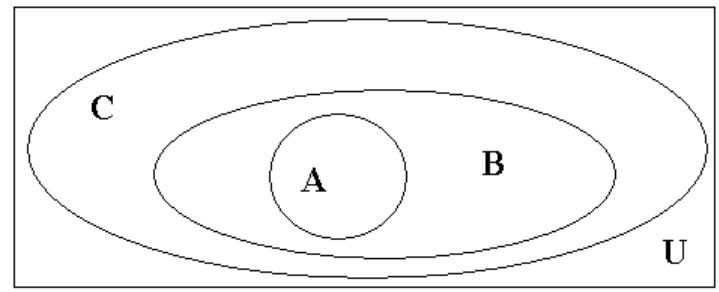
Aibė A yra vadinama aibės B ***poaibiu***, jei visi aibės A elementai yra ir aibės B elementai. Rašome $A \subset B$ arba $B \supset A$.

Kai aibės yra reiškiamos predikatais $A = \{x \in U : a(x)\}$ ir $B = \{x \in U : b(x)\}$, poaibio apibrėžimą galima užrašyti taip:

$$(A \subset B) \Leftrightarrow (\forall x\ a(x) \Rightarrow b(x)).$$

Pastebėkime, kad iš čia išplaukia, kad bet kuriai aibei B gauname $\emptyset \subset B$: kadangi $\emptyset$ neturi elementų, formulėje $\forall x\ a(x) \Rightarrow b(x)$ turi būti $a(x) = const = 0$ ir implikacija $0 \Rightarrow b(x)$ yra teisinga su bet kuriuo predikatu $b(x)$.
Iš šio apibrėžimo dar išplaukia, kad $A \subset A$, kadangi $a(x) \Rightarrow a(x)$ visada yra teisingas teiginys.[16]

[16] Literatūroje kartais taikomi žymėjimai $X \subseteq Y$, $Y \supseteq X$. Tokiu atveju žymėjimas $X \subset Y$ reiškia: $X \subset Y \& X \neq Y$. Netuščiasis poaibis $X \subset Y \& X \neq Y$ vadinamas ***tikriniu***.



2: Aibės poaibiai

Susitarkime, kad $(A = B) \Leftrightarrow (a(x) \Leftrightarrow b(x))$. Šį teiginį galima užrašyti ir taip:

$$(A = B) \Leftrightarrow (A \subset B)\ \&\ (B \subset A).$$

Pavyzdys
Aibė $A = \{0, 1, \{0, 1\}\}$ turi tris elementus: $0 \in A$, $1 \in A$, $\{0, 1\} \in A$ bei aštuonis poaibius:
$\emptyset$, $\{0\}$, $\{1\}$, $\{\{0, 1\}\}$, $\{0, 1\}$, $\{0, \{0, 1\}\}$, $\{1, \{0, 1\}\}$, $\{0, 1, \{0, 1\}\}$.

Pavaizduotos 2 paveiksle aibės A, B, C tenkina sąlygas: $A \subset B$, $B \subset C$, $A \subset C$ arba trumpiau $A \subset B \subset C$.

Deriniai ir gretiniai

Suskaičiuokime, kiek poaibių turi baigtinė aibė $A = \{a_1, a_2, \ldots, a_n\}$.
Yra vienas poaibis, neturintis elementų – tuščioji aibė $\emptyset$.
Poaibių, turinčių po vieną elementą, yra n:

$$\{a_1\},\ \{a_2\},\ \ldots,\ \{a_n\}.$$

Poaibių, sudarytų iš dviejų elementų, yra $\dfrac{n(n-1)}{2}$:

$$\{a_1, a_2\}, \{a_1, a_3\}, \ldots, \{a_1, a_n\}, \ldots, \{a_{n-1}, a_n\}.$$

Poaibių, turinčių po k elementų, yra

$$C_n^k = \frac{n!}{(n-k)!\,k!} = \frac{(n-k+1)\cdot(n-k+2)\cdot\ \cdots\ \cdot(n-1)\cdot n}{k!}.$$

Kitas derinių skaičiaus iš n po k elementų žymėjimas yra $\binom{n}{k}$. Pastebėkime, kad

$$C_n^0 = \binom{n}{0} = C_n^n = \binom{n}{n} = 1.$$

Taigi baigtinė aibė A turi $C_n^0+C_n^1+C_n^2+\cdots+C_n^n$ poaibių. Šiam skaičiui rasti taikome gerai matematikoje žinomą Niutono[17] binomo formulę:

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^{n-k} y^k.$$

Kai $x = y = 1$, iš čia gauname ieškomą skaičių $\sum\limits_{k=0}^{n} C_n^k = 2^n$.

Aibės $A = \{a_1, a_2, \ldots, a_n\}$ visų poaibių aibė vadinama ***buleanu*** ir žymima

$$2^A = \{\emptyset, \{a_1\}, \{a_2\}, \ldots, \{a_1, a_2\}, \ldots, \{a_1, a_2, a_3\}, \cdots, A\}.$$

Turime formulę $|2^A| = 2^{|A|}$.

Kartais išrinktų iš aibės $A = \{a_1, a_2, \ldots, a_n\}$ k elementų eilės tvarka yra svarbi. Kiekvieną tokį poabį galima užrašyti $k!$ būdais. Elementų junginius, kurie vienas nuo kito skiriasi arba pačiais elementais, arba jų

[17] Isaak Newton (1643 – 1727) – anglų fizikas ir matematikas.

eile vadinami ***gretiniais***. Gretinių iš n po k elementų skaičių žymime A_n^k. Turime

$$A_n^k = k!C_n^k = \frac{n!}{(n-k)!} = (n-k+1)\cdot(n-k+2)\cdots(n-1)\cdot n.$$

Pastebėkime, kad $A_n^n = n!$ t. y. kėlinių skaičius.

Pavyzdžiai

1. Surašykime visus gretinius po du elementus iš $\{a, b, c\}$: (a, b), (b, a), (a, c), (c, a), (b, c), (c, b). Taigi $A_3^2 = \frac{3!}{(3-2)!} = 2 \cdot 3 = 6$.

2. Suskaičiuokime, kiek skirtingų vėliavų galima sudaryti iš septynių spalvų vienodo dydžio juostų, jei kiekviena vėliava turi lygiai tris horizontaliąsias juostas. Turime iš septynių juostų išsirinkti tris ir yra svarbi šių trijų juostų eilės tvarka. Tai yra gretinių skaičius

$$A_7^3 = \frac{7!}{(7-3)!} = \frac{7!}{4!} = 5 \cdot 6 \cdot 7 = 210.$$

2.2. Veiksmai su aibėmis

Operacijų su aibėmis apibrėžimai

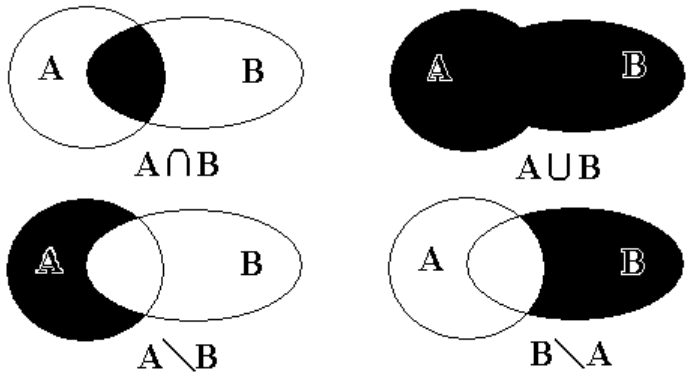
Tarkime, kad aibės A ir B apibrėžtos predikatais $a(x)$, $b(x)$:

$$A = \{x \in U :\ a(x)\},\ B = \{x \in U :\ b(x)\}.$$

Apibrėžimai

Aibių A ir B ***sąjunga*** vadinama aibė, kurios elementai priklauso *bent vienai* aibei A arba B. Sąjungą žymime $A \cup B$. Taikydami predikatus, apibrėžimą galime užrašyti taip:

$$A \cup B \ = \ \{x \in U :\ a(x) \ \vee \ b(x)\}.$$



3: Veiksmai su aibėmis

Aibių A ir B ***sankirta*** vadinama aibė, kurios elementai priklauso *ir aibei* A*, ir aibei* B. Sankirta žymima $A \cap B$ ir taip reiškiama predikatais:

$$A \cap B \;=\; \{x \in U :\; a(x)\ \&\ b(x)\}.$$

Pavyzdžiai
$A = \{1, \{1\}, \{1, 2\}, 3\}$, $B = \{1, \{2\}, \{3, 4\}\}$,
$A \cup B = \{1, \{1\}, \{1, 2\}, \{2\}, 3, \{3, 4\}\}$,
$A \cap B = \{1\}$.

Apibrėžimas
Aibių A ir B ***skirtumas*** $A \setminus B$ – aibė, sudaryta iš tų aibės A elementų, kurie *nėra aibės* B *elementai*:

$$A \setminus B \;=\; \{x \in U :\; x \in A\ \&\ x \notin B\}.$$

Pavyzdžiai
$A = \{1, \{1\}, 2, \{2, 3\}\}$, $B = \{1, \{2\}, \{2, 3\}, 4\}$,
$A \setminus B = \{\{1\}, 2\}$,
$B \setminus A = \{\{2\}, 4\}$.
Pastebėkime, kad $A \setminus B \neq B \setminus A$.

Dar vienos *unariosios* operacijos rezultatas – aibės A ***papildinys*** yra aibė $\overline{A}$, sudaryta iš tų (universaliosios aibės U) elementų, kurie *nėra aibės A elementai*:

$$\overline{A} = U \setminus A = \{x \in U : \ x \notin A\}$$

Operacijų su aibėmis savybės

1	$A \cup B = B \cup A$	komutatyvumo
2	$A \cap B = B \cap A$	dėsniai
3	$(A \cup B) \cup C = A \cup (B \cup C)$	asociatyvumo
4	$(A \cap B) \cap C = A \cap (B \cap C)$	dėsniai
5	$A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$	distributyvumo
6	$A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$	dėsniai
7	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	de Morgano
8	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	dėsniai
9	$A \cup A = A$	idempotentumo
10	$A \cap A = A$	dėsniai
11	$A \cup \emptyset = A$	
12	$A \cap U = A$	U – universalioji aibė
13	$A \cup \overline{A} = U$	
14	$A \cap \overline{A} = \emptyset$	
15	$\overline{(\overline{A})} = A$	dvigubo neigimo dėsnis

Visas formules galima įrodyti, taikant predikatus.
Įrodykime, pavyzdžiui, 10 formulę:

$$A \cap A = \{x \in U : a(x) \& a(x)\} = \{x \in U : a(x)\} = A.$$

2.3. Kombinatoriniai skaičiai

Skaidiniai

Apibrėžimai

Tarkime, kad aibės A poaibiai B_1, B_2, ..., B_k ($B_j \subset A$) tenkina šias sąlygas:

1) $B_j \neq \emptyset$;

2) $B_i \cap B_j = \emptyset \; \forall i \neq j$;

3) $\bigcup\limits_{j=1}^{k} B_j = A$.

Tada sakome, kad poaibių $B_1, B_2, \ldots, B_k$ rinkinys yra aibės A ***skaidinys***. Poaibiai B_j vadinami skaidinio ***blokais***. Tokių skaidinių skaičiai, kai $|A| = n$ vadinami ***antrosios rūšies Stirlingo***[18] ***skaičiais*** ir žymimi $S(n,k)$. Pagal apibrėžimą $S(n,k) = 0$, kai $k > n$, $S(n,n) = 1$. Susitarkime, kad $S(0,0) = 1$.

Pavyzdžiai

1. Tarkime $A = \{1,2,3\}$. Aibės A du poabiai $B_1 = \{1,2\}$, $B_2 = \{3\}$ yra jos skaidinys į du blokus.
2. Aibės $B_1 = \{1,2\}$, $B_2 = \{2,3\}$ nėra aibės $A = \{1,2,3\}$ skaidinys, kadangi netenkina skaidinio 2) apibrėžimo sąlygos.
3. Aibės $B_1 = \{1\}$, $B_2 = \{2\}$ nėra aibės $A = \{1,2,3\}$ skaidinys, kadangi netenkina 3) apibrėžimo sąlygos.
4. Aibės $B_1 = \{1\}$, $B_2 = \{2\}$, $B_3 = \{3,4\}$ nėra aibės $A = \{1,2,3\}$ skaidinys, kadangi B_3 nėra aibės A poaibis. Pastebėkime, kad B_1, B_2, B_3 sudaro aibės $\{1,2,3,4\}$ skaidinį.
5. Aibė $\{1,2,3,4\}$ turi lygiai 7 skaidinius į du blokus:

$$\{\{1,2,3\},\{4\}\},\ \{\{1,2,4\},\{3\}\},\ \{\{1,3,4\},\{2\}\},$$

[18] James Stirling (1692 – 1770) – škotų matematikas.

$$\{\{2,3,4\},\{1\}\},\ \{\{1,2\},\{3,4\}\},\ \{\{1,3\},\{2,4\}\},\ \{\{1,4\},\{2,3\}\}.$$

Teorema. Antrosios rūšies Stirlingo skaičiams galioja lygybė[19]

$$S(n,k) = S(n-1,k-1) + kS(n-1,k).$$

Įrodymas. Tarkime, kad S yra visų aibės $\{1,2,\ldots,n\}$ skaidinių į k blokus aibė. Pažymėkime S_1 tuos skaidinius, į kuriuos įeina blokas $\{n\}$, ir S_2 – visi kiti skaidiniai. Tada $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = S$. Turime $|S_1| = S(n-1,k-1)$, $|S_2| = kS(n-1,k)$, kadangi visi skaidiniai S_2 gaunami taip: imame visus aibės $\{1,2,\ldots,n-1\}$ skaidinius į k blokus ir kiekvieną bloką papildome elementu n. Taigi

$$S(n,k) = |S| = |S_1| + |S_2| = S(n-1,k-1) + kS(n-1,k).$$

Pavyzdys
Keliais būdais galima paskirti 8 budėtojus į 4 postus, su sąlyga, kad kiekviename poste būtų bent vienas budėtojas ir visi 8 žmonės budėtų.
Sprendimas. Reikia suskaidyti aibę $|A| = 8$ į 4 blokus. Tai galima padaryti $S(8,4) = 1701$ būdu.

[19] Tokio pavidalo lygtys vadinamos rekurenčiosiomis (žr. 52 p.).

Antrosios rūšies Stirlingo skaičiai $S(n,k)$

n \ k	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	1	1								
3	0	1	3	1							
4	0	1	7	6	1						
5	0	1	15	25	10	1					
6	0	1	31	90	65	15	1				
7	0	1	63	301	350	140	21	1			
8	0	1	127	966	1701	1050	266	28	1		
9	0	1	255	3025	7770	6951	2646	462	36	1	
10	0	1	511	9330	34105	42525	22827	5880	750	45	1

Visų aibės A ($|A| = n$) skaidinių skaičius vadinamas ***Belo***[20] ***skaičiumi***: $B(n) = \sum_{k=0}^{n} S(n,k),\ B(0) = 1.$

Pavyzdys

Keliais būdais galima sudėti 10 skirtingų pieštukų į 10 vienodų dėžučių, jei kai kurios dėžutės gali būti tuščios.

Sprendimas. Į vieną dėžutę 10 pieštukų galima sudėti $S(10,1) = 1$ būdu, į dvi dėžutes $S(10,2) = 511$ būdais ir t. t. Taigi turime $S(10,1) + S(10,2) + \cdots + S(10,10) = B_{10} = 115975$.

[20] Eric Temple Bell (1893 – 1960) – amerikiečių matematikas.

Belo skaičiai B_n

n		n	
0	1	8	4140
1	1	9	21147
2	2	10	115975
3	5	11	678570
4	15	12	4213597
5	52	13	27644437
6	203	14	190899322
7	877	15	1382958545

Ciklai

Tarkime, kad A, B, C yra taisyklingo trikampio viršūnės. Tada jos gali būti išdėstytos dviem būdais (A, B, C) arba (A, C, B). Kitus trikampius (C, A, B), (B, C, A) galima gauti, sukant trikampį (A, B, C) aplink apibrėžto (ir įbrėžto) apskritimo centrą. Taigi aibės $\{A, B, C\}$ elementų išdėstymus

$$(A, B, C) = (C, A, B) = (B, C, A)$$

vadiname ***ciklu***. Kitas šios aibės ciklas yra

$$(A, C, B) = (C, B, A) = (B, A, C).$$

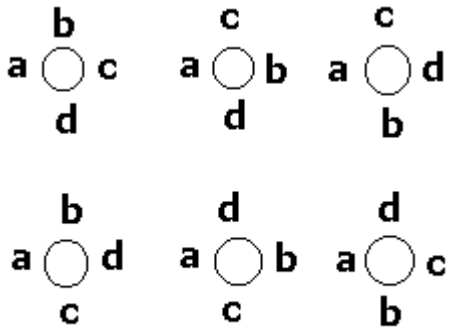
Aibės $\{a, b, c, d\}$ skirtingais ciklais pavadinsime tokius ekvivalenčius reiškinius:

$$(a, b, c, d) = (d, a, b, c) = (c, d, a, b) = (b, c, d, a),$$

arba

$$(a, b, d, c) = (b, d, c, a) = (d, c, a, b) = (c, a, b, d).$$

Visi skirtingi aibės $\{a, b, c, d\}$ ciklai parodyti paveiksle.



4: Visi aibės $\{a, b, c, d\}$ skirtingi ciklai

Pavyzdys
Iš aibės $\{a, b, c, d\}$ elementų galima sudaryti vienuolika skirtingų ciklų porų:
$\{(a, b, c), (d)\}$, $\{(a, c, b), (d)\}$, $\{(a, b, d), (c)\}$, $\{(a, d, b), (c)\}$,
$\{(a, c, d), (b)\}$, $\{(a, d, c), (b)\}$, $\{(b, c, d), (a)\}$, $\{(b, d, c), (a)\}$,
$\{(a, b), (c, d)\}$, $\{(a, c), (b, d)\}$, $\{(a, d), (b, c)\}$.

Apibrėžimas
Pirmosios rūšies Stirlingo skaičiai žymimi $s(n, k)$ ir apibrėžiami taip:

$$s(n, k) = s(n - 1, k - 1) - (n - 1)s(n - 1, k),\ k \leqslant n,\ s(0, 0) = 1.$$

Iš n skirtingų elementų k ciklų galima sudaryti $|s(n, k)|$ būdais.

Pirmosios rūšies Stirlingo skaičiai $s(n,k)$

n \ k	0	1	2	3	4	5	6	7	8
0	1								
1	0	1							
2	0	−1	1						
3	0	2	−3	1					
4	0	−6	11	−6	1				
5	0	24	−50	35	−10	1			
6	0	−120	274	−225	85	−15	1		
7	0	720	−1764	1624	−735	175	−21	1	
8	0	−5040	13068	−13132	6769	−1960	322	−28	1

2.4. Kombinatoriniai principai

Kombinacijų daugybos taisyklė

Tarkime, kad turime dvi aibes $A = \{a_1, a_2, \ldots, a_n\}$ ir $B = \{b_1, b_2, \ldots, b_m\}$. Aibė

$$A \times B = \{(a_i, b_j),\ i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m\}$$

yra vadinama aibių A ir B ***Dekarto***[21] ***sandauga***. Turime $|A \times B| = n \cdot m = |A| \cdot |B|$.

Pavyzdys
Tarkime, kad aibės $A = \{a, b, c\}$ elementams reikia priskirti žymes $Z = \{1, 7, 11, 13\}$. Visus įmanomus variantus užrašome kaip aibių Dekarto sandauga: $A \times B = \{(a,1), (a,7), (a,11), (a,13), (b,1), (b,7), (b,11), (b,13), (c,1), (c,7), (c,11), (c,13)\}$.

Taigi galime suformuluoti ***kombinacijų daugybos taisyklę***: jei elementą $a \in A$ galima išrinkti n būdais, o elementą $b \in B$ – m būdais, tai elementų poras (a, b) galima išrinkti $n \cdot m$ būdais.

[21] René Descartes (1596 – 1650) – prancūzų filosofas ir matematikas

Pavyzdys
Apskaičiuokime, kiek skirtingų triženklių lyginių skaičių galima sudaryti iš skaitmenų $0, 1, 2, 3, 7$. Pirmas skaitmuo neturi būti 0, todėl jį galima rinkti iš keturių skaitmenų $1, 2, 3, 7$. Antras skaitmuo – bet kuris iš penkių duotų. Kadangi ieškomas skaitmuo yra lyginis, paskutinis skaitmuo turi būti išrinktas iš dviejų skaitmenų $0, 2$. Taigi turime $4 \cdot 5 \cdot 2 = 40$ variantų.

Susitarkime žymėti $A^1 = A$, $A^2 = A \times A$, $A^3 = A \times A \times A = A \times A^2 = A^2 \times A$, $A^k = A^{k-1} \times A = A \times A^{k-1}$. Pastebėkime, $|A^k| = |A|^k$.

Pavyzdys
Kiekvieną natūralųjį skaičių x galima užrašyti dvejetainėje sistemoje:

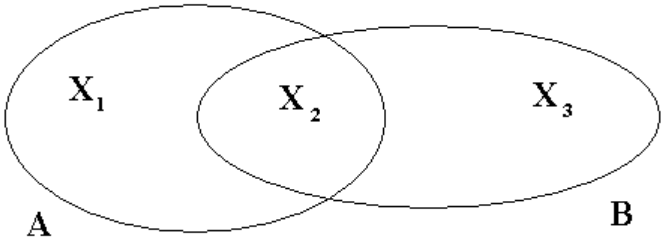
$$x = a_{k-1} \cdot 2^{k-1} + a_{k-2} 2^{k-2} + \cdots + a_2 \cdot 2^2 + a_1 \cdot 2^1 + a_0 \cdot 2^0, \;\; a_j \in \{0, 1\}.$$

Suskaičiuokime kiek skirtingų skaičių galima išreikšti, kai $k = 8$, t. y. taikydami sekas iš aštuonių nulių ir vienetų. Turime $|\{0, 1\}|^8 = 2^8 = 256$:
$0 = (0, 0, 0, 0, 0, 0, 0, 0) = 0 \cdot 128 + 0 \cdot 64 + \cdots + 0 \cdot 2 + 0 \cdot 1,$
$1 = (0, 0, 0, 0, 0, 0, 0, 1) = 0 \cdot 128 + 0 \cdot 64 + \cdots + 0 \cdot 2 + 1 \cdot 1,$
$255 = (1, 1, 1, 1, 1, 1, 1, 1) = 1 \cdot 128 + 1 \cdot 64 + \cdots + 1 \cdot 4 + 1 \cdot 2 + 1 \cdot 1.$

Tarkime, kad iš abėcėlės $A = \{a_1, a_2, \ldots, a_n\}$ raidžių sudaryti ilgio k žodžiai, taip kad raidė a_j pasikartoja lygiai $p_j \geqslant 0$ kartų: $p_1 + p_2 + \cdots + p_n = k$. Tokie žodžiai vadinami ***kartotiniais gretiniais***. Jų yra

$$\binom{k}{p_1 p_2 \ldots p_n} = \frac{k!}{p_1! p_2! \cdots p_n!}.$$

Pavyzdys
Kiek skirtingų kombinacijų galima sudaryti iš visų žodžio MATEMATIKA raidžių?
Sprendimas. Turime iš viso $k = 10$ raidžių, tarp jų skirtingų yra $n = 6$.



5: Įdėties pašalinimo principas

Raidės kartojasi taip: $p_M = 2$, $p_A = 3$, $p_T = 2$, $p_E = 1$, $p_I = 1$, $p_K = 1$. Patikrinkime: $2 + 3 + 2 + 1 + 1 + 1 = 10$. Taigi

$$\frac{10!}{2!3!2!1!1!1!} = \frac{5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10}{1} = 151200.$$

Sudėties taisyklė

Tarkime, kad aibės A ir B nesusikerta, t. y. $A \cap B = \emptyset$. Tada bet kuris aibių sąjungos elementas $x \in A \ \& \ x \notin B$ arba $x \in B \ \& \ x \notin A$. Todėl aibė $A \cup B$ turi $|A| + |B|$ elementų:

$$A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|.$$

Šią formulę galima apibendrinti:

$$\forall i \neq j \ A_i \cap A_j = \emptyset \Rightarrow \left| \bigcup_{k=1}^{n} A_k \right| = \sum_{k=1}^{n} |A_k|$$

Įdėties pašalinimo principas

Pažymėkime $A \setminus B = X_1$, $B \setminus A = X_3$, $A \cap B = X_2$.

Turime $X_i \cap X_j = \emptyset \; \forall i \neq j$ ir $|X| = |A \cup B| = |X_1| + |X_2| + |X_3|$. Pastebėję, kad $A = (A \setminus B) \cup (A \cap B) = X_1 \cup X_2$ ir $B = (B \setminus A) \cup (A \cap B) = X_3 \cup X_2$, turime $|X_1| = |A| - |X_2| = |A| - |A \cap B|$, $|X_3| = |B| - |X_2| = |B| - |A \cap B|$. Taigi

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Formulę galima apibendrinti:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|;$$

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{j=1}^{n} |A_j| - \sum_{1 \leqslant j < i \leqslant n} |A_j \cap A_i| +$$

$$\sum_{1 \leqslant j < i < k \leqslant n} |A_j \cap A_i \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Pavyzdys

Mokykloje mokosi 1000 mokinių. Iš jų 800 studijuoja anglų kalbą, 500 – vokiečių, o 100 nestudijuoja nė vienos iš šių kalbų. Apskaičiuokime, kiek mokinių studijuoja ir anglų, ir vokiečių kalbą.

Sprendimas. Pažymėkime visų mokinių aibę Ω, studijuojančių anglų kalbą mokinių aibę – A, vokiečių V. Turime $|\Omega| = 1000$, $|A| = 800$, $|V| = 500$. Dar mes žinome, kad nė vienos iš šių kalbų nestudijuoja $|\overline{A} \cap \overline{V}| = 100$. Taikome de Morgano dėsnį (žr. 2.2.): $\overline{A} \cap \overline{V} = \overline{A \cup V} = \Omega \setminus (A \cup V)$. Taigi $|A \cup V| = |\Omega| - |\overline{A} \cap \overline{V}| = 1000 - 100 = 900$. Mums reikia rasti $|A \cap V|$. Turime $|A \cap V| = |A| + |V| - |A \cup V| = 800 + 500 - 900 = 400$. Taigi 400 mokinių studijuoja ir anglų, ir vokiečių kalbą.

2.5. Generuojančiosios funkcijos

Generuojančiųjų funkcijų pavyzdžiai

Tarkime, kad $\{a_0, a_1, \ldots\}$ yra skaičių seka. Sudarome laipsninę eilutę $\sum\limits_{n=0}^{\infty} a_n x^n$, kurią vadiname sekos $\{a_n\}$ ***generuojančiaja funkcija***. Kai seka yra baigtinė ($\{a_0, a_1, \ldots, a_n\}$, $a_k = 0$, kai $k > n$), generuojančioji funkcija yra polinomas.

Pavyzdžiai

$$\{a_n\} = \{1, 1, \ldots, 1, 0, 0, \ldots\} \qquad \sum_{k=0}^{n} x^k = \frac{1 - x^{n+1}}{1 - x};$$

$$\{a_n\} = \{1, 4, 6, 4, 1, 0, 0, \ldots\} \qquad \sum_{k=0}^{4} C_4^k x^k = (1 + x)^4;$$

$$\{a_n\} = \{C_n^0, C_n^1, \ldots, C_n^{n-1}, C_n^n, 0, 0, \ldots\} \qquad \sum_{k=0}^{n} C_n^k x^k = (1 + x)^n.$$

Kai kurių begalinių skaičių sekų generuojančiosios funkcijos yra gerai žinomos[22]:

$$\{a_n\} = \{1, 1, \ldots, 1, 1, 1, \ldots\} \qquad \sum_{k=0}^{\infty} x^k = \frac{1}{1 - x};$$

$$\{a_n\} = \{1, -1, 1, -1, 1, -1, \ldots\} \qquad \sum_{k=0}^{\infty} (-1)^k x^k = \frac{1}{1 + x};$$

$$\{a_n\} = \{1, a, a^2, a^3, a^4, a^5, \ldots\} \qquad \sum_{k=0}^{\infty} a^k x^k = \frac{1}{1 - ax};$$

$$\{a_n\} = \{1, 2, 3, 4, 5, 6, \ldots\} \qquad \sum_{k=0}^{\infty} (k + 1) x^k = \frac{1}{(1 - x)^2};$$

$$\{a_n\} = \{0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots\} \qquad \sum_{k=1}^{\infty} \frac{x^k}{k} = \ln \frac{1}{1 - x};$$

[22] Pastebėkime, kad eilutės sumavimo indekso k pradinė reikšmė gali būti nenulinė.

$$\{a_n\} = \{0, 1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \ldots\} \quad \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k = \ln(1+x);$$
$$\{a_n\} = \{1, 1, \frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \frac{1}{120}, \ldots\} \quad \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x;$$

$$\{a_n\} = \{0, 1, 0, -\frac{1}{6}, 0, \frac{1}{120}, 0, \ldots\} \quad \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} x^{2k+1} = \sin x;$$
$$\{a_n\} = \{1, 0, -\frac{1}{2}, 0, \frac{1}{24}, 0, \ldots\} \quad \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} x^{2k} = \cos x.$$

Apibrėžkime n – ojo laipsnio polinomą

$$(x)_n = x(x-1)(x-2)\cdots(x-n+1),$$

kurį vadinsime ***apatiniu faktorialu***. Pastebėkime, kad $(n)_n = n!$. Galima įrodyti, kad pirmosios bei antrosios rūšies Stirlingo skaičiai (žr. 2.3.) tenkina formules ($n > 0$):

$$(x)_n = \sum_{k=0}^{n} s(n,k) x^k,$$
$$x^n = \sum_{k=0}^{n} S(n,k) (x)_k.$$

Generuojančiųjų funkcijų savybės

Tarkime kad $F_a(x)$ ir $F_b(x)$ yra skaičių sekų $\{a_n\}$ ir $\{b_n\}$ generuojančiosios funkcijos. Tada su bet kuriais skaičiais α ir β funkcija $\alpha F_a(x) + \beta F_b(x)$ generuoja skaičių seką $\{\alpha a_n + \beta b_n\}$.

Įrodykime, kad skaičių seką $a_n = b_n - b_{n-1},\ n \geqslant 1$ generuoja funkcija $F_a(x) = F_b(x)(1-x)$.

Turime $F_a(x) = \sum\limits_{k=1}^{\infty} (b_k - b_{k-1}) x^k = \sum\limits_{k=0}^{\infty} b_k x^k - \sum\limits_{k=1}^{\infty} b_{k-1} x^{k-1} x.$

Todėl $F_a(x) = F_b(x) - \left(\sum\limits_{k'=k-1=0}^{\infty} b_{k'} x^{k'} \right) = F_b(x) - x F_b(x).$

Panašiai galima įrodyti, kad skaičių seką $a_n = b_{n+1} - b_n$ generuoja funkcija $F_a(x) = F_b(x)\dfrac{1-x}{x} - \dfrac{b_0}{x}$, o seką $a_n = nb_n$ – funkcija $F_a(x) = x\dfrac{d}{dx}F_b(x)$.

Apibrėžkime dviejų generuojančiųjų funkcijų ***sandaugą***:

$$F_a(x)F_b(x) = \sum_{n=0}^{\infty} c_n x^n,$$

$$c_n = a_0b_n + C_n^1 a_1 b_{n-1} + C_n^2 a_2 b_{n-2} + \cdots + C_n^k a_k b_{n-k} + \cdots + a_n b_0.$$

Taikydami šią formulę funkcijoms $(1+x)^m$ ir $(1+x)^k$, gauname

$$(1+x)^m \cdot (1+x)^k = \sum_{i=0}^{m} C_m^i x^i \cdot \sum_{j=0}^{k} C_k^j x^j =$$

$$(1+x)^{m+k} = \sum_{l=0}^{m+k} C_{m+k}^l x^l$$

Taigi gauname Koši[23] tapatybę:

$$C_{m+k}^l = \sum_{s=0}^{l} C_m^s C_k^{l-s}.$$

Pastebėję binominių koeficientų simetriškumą $C_{2n}^i = C_{2n}^{2n-i}$, turime dar vieną formulę:

$$\sum_{s=0}^{n} C_{2n}^s = C_{2n}^n.$$

[23] Augustin Louis Cauchy (1789 – 1857) – pranc¯uzų matematikas.

Fibonačio skaičiai

Fibonačio[24] skaičiai F_n apibrėžiami *rekurentine* lygtimi:

$$F_0 = F_1 = 1,\ F_n = F_{n-1} + F_{n-2},\ n \geq 1.$$

Pažymėkime skaičių sekos $\{F_n\} = \{1, 1, 2, 3, 5, 8, 13, 21, \ldots\}$ generuojančiąją funkciją $F(x)$:

$$F(x) = \sum_{n=0}^{\infty} F_n x^n = 1 + x + \sum_{n=2}^{\infty} (F_{n-2} + F_{n-1}) x^n =$$

$$1 + x + x^2 \sum_{n=2}^{\infty} F_{n-2} x^{n-2} + x \left(\sum_{n=2}^{\infty} F_{n-1} x^{n-1} + 1 - 1 \right) =$$

$$1 + x + x^2 F(x) + x(F(x) - 1) = 1 + (x + x^2) F(x).$$

Turime $F(x) = \dfrac{1}{1 - x - x^2} = \dfrac{1}{(1 - ax)(1 - bx)}$.

Čia $a = \dfrac{1 + \sqrt{5}}{2}$, $b = \dfrac{1 - \sqrt{5}}{2}$. Pažymėję $A = \dfrac{a}{a - b}$ ir $B = -\dfrac{a}{a - b}$, turime[25]

$$F(x) = \frac{A}{1 - ax} + \frac{B}{1 - bx} = A \sum_{n=0}^{\infty} a^n x^n + B \sum_{n=0}^{\infty} b^n x^n =$$

$$\sum_{n=0}^{\infty} \frac{a^{n+1} - b^{n+1}}{a - b} x^n$$

šaknis. Taigi gavome n – ojo Fibonačio skaičiaus formulę:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right).$$

[24] Fibonacci (Leonardo Pisano, 1180 – 1240) – italų matematikas.

[25] Šias reikšmes galima gauti neapibrėžtųjų koefi cientų metodu, skleidžiant racionaliąją trupmeną elementariųjų trupmenų suma.

2.6. Rekurenčiosios lygtys

Homogeninės lygtys

Apibrėžimas

Tarkime, kad p_1, p_2, …, p_k yra žinomi skaičiai ir $p_k \neq 0$. Lygtis

$$(HL) \quad a_{n+k} + p_1 a_{n+k-1} + p_2 a_{n+k-2} + \cdots + p_k a_n = 0$$

yra vadinama ***tiesine homogenine rekurenčiąja lygtimi***. Jos sprendinys yra skaičių seka $\{a_0, a_1, \ldots, a_n, \ldots\}$. Pastebėkime, kad jei dvi skaičių sekos $\{a_n^{(1)}\}$ ir $\{a_n^{(2)}\}$ tenkina (HL) lygtį, tai ją tenkina ir bet kuris jų tiesinis darinys $\alpha_1 a_n^{(1)} + \alpha_2 a_n^{(2)}$.

Tarkime, kad $a_n = \lambda^n$ tenkina (HL) lygtį. Tada $a_{n+k} = \lambda^{n+k} = \lambda^n \lambda^k$ ir įstatant a_n į (HL), gauname, kad λ yra ***charakteristinės lygties***

$$(CH) \quad \lambda^n + p_1 \lambda^{n-1} + p_2 \lambda^{n-2} + \cdots + p_{k-1}\lambda + p_k = 0$$

šaknis. Taigi kai charakteristinė lygtis turi k skirtingų šaknų λ_1, λ_2, …, λ_k turime (HL) lygties ***bendrąjį sprendinį***

$$a_n = C_1 \lambda_1^n + C_2 \lambda_2^n + \cdots + C_k \lambda_k^n.$$

Pavyzdys

Išspręskime lygtį $a_{n+2} - 4a_{n+1} + 3a_n = 0$ su pradinėmis sąlygomis $a_0 = 2$, $a_1 = 4$.

Sudarome charakteristinę lygtį $\lambda^2 - 4\lambda + 3 = 0$, kurios šaknys yra $\lambda_1 = 1$ ir $\lambda_2 = 3$. Bendrasis sprendinys: $a_n = C_1 + C_2 3^n$. Įstatę į jį pradines sąlygas, gauname $a_0 = 2 = C_1 + C_2$, $a_1 = 4 = C_1 + C_2 3$. Taigi $C_1 = C_2 = 1$ ir $a_n = 1 + 3^n$.

Tarkime, kad charakteristinės lygties šaknis λ_0 yra kartotinė kartotinumo r. Tada ją atitinka r (HL) lygties sprendinių:

$$\lambda_0^n,\ n\lambda_0^n,\ n^2\lambda_0^n, \ldots, n^{r-1}\lambda_0^n.$$

Pavyzdys
Rekurenčiosios lygties $a_{n+2} - 4a_{n+1} + 4a_n = 0$ charakteristinė lygtis

$$\lambda^2 - 4\lambda + 4 = (\lambda - 2)^2 = 0$$

turi kartotinę šaknį $\lambda_0 = 2$. Bendrasis sprendinys yra $a_n = 2^n(C_1 + nC_2)$.

Nehomogeninė lygtis

Tiesine nehomogenine rekurenčiaja lygtimi vadiname lygtį

$$(NH) \quad a_{n+k} + p_1 a_{n+k-1} + p_2 a_{n+k-2} + \cdots + p_k a_n = \varphi(n).$$

Čia $\varphi(n)$ – žinoma funkcija.

Iš bendros tiesinių lygčių teorijos yra žinoma, kad (NH) lygties bendrasis sprendinys yra (HL) bendrojo sprendinio ir kokio nors (NH) lygties atskirojo sprendinio suma. Kai $\varphi(n)$ yra polinomas, (NH) atskirojo sprendinio galima ieškoti polinomo su neapibrėžtaisiais koeficientais pavidalu. Jei $\varphi(n)$ yra laipsninė funkcija, lygtis turi atskirąjį sprendinį — laipsninę funkciją.

Pavyzdžiai
1. Rekurenčioji nehomogeninė lygtis $a_{n+2} + pa_{n+1} + qa_n = \alpha n + \beta$ turi atskirąjį sprendinį a_n^* vieno iš šių trijų pavidalų:
1) $a_n^* = An + B$, kai $1 + p + q \neq 0$;
2) $a_n^* = n(An + B)$, kai $1 + p + q = 0$ ir $p \neq -2$;
3) $a_n^* = n^2(An + B)$, kai $p = -2$, $q = 1$.

2. Lygtis $a_{n+2} + pa_{n+1} + qa_n = \gamma\, \mu^n$ turi atskirąjį sprendinį a_n^* vieno iš šių trijų pavidalų:
1) $a_n^* = A\mu^n$, kai $\mu^2 + p\mu + q \neq 0$;
2) $a_n^* = nA\mu^n$, kai $\mu^2 + p\mu + q = 0$ ir $2\mu + p \neq 0$;
3) $a_n^* = An^2$, kai $p = -2$, $q = 1$, $\mu = 1$.

2.7. Asimptotikos

Eilės simboliai

Apibrėžimai

Tarkime, kad $f(n)$ ir $g(n)$ yra neaprėžtai didėjančiosios funkcijos ($n \in \mathbb{N}$). Sakome, kad funkcijos $g(n)$ *augimas yra greitesnis* ir rašome $f(n) \prec g(n)$ (arba $g(n) \succ f(n)$), jei $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 0$.

Galima apibendrinti apibrėžimą ir nagrinėti, pavyzdžiui, nykstamąsias funkcijas:

$f(n) \prec g(n) \Leftrightarrow \dfrac{1}{g(n)} \prec \dfrac{1}{f(n)}$.

Surašykime kai kurių funkcijų *augimo hierarchiją*:

$$1 \prec \ln\ln n \prec \ln n \prec \sqrt{n} \prec n \prec n^2 \prec n^{\ln n} \prec e^n \prec n^n \prec n^{n^n}.$$

Tarkime, kad neaprėžtai didėjančios funkcijos $f(n)$ ir $g(n)$ tenkina sąlygą $\exists C > 0 : |f(n)| \leqslant C|g(n)|$ (su visais n). Tada sakome, kad funkcijos $f(n)$ augimo greitis yra *nedidesnės eilės* negu funkcijos $g(n)$ ir rašome $f(n) = O(g(n))$.

Pavyzdžiui, $n^2 + 5n - 3 = O(n^2)$, $2^n + n^2 = O(2^n)$.

Sakome, kad funkcijos $f(n)$ ir $g(n)$ turi ***tą pačią augimo eilę***, kai $\exists C > 0 : |f(n)| \leqslant C|g(n)|$ & $|g(n)| \leqslant C|f(n)|$ (su visais n). Rašome $f(n) \asymp g(n)$.

Tarkime, kad $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 1$. Tada rašome $f(n) \sim g(n)$ ir sakome, kad $g(n)$ yra funkcijos $f(n)$ *asimptotika*.

Pastabos

1. Visi apibrėžimai galioja ir realaus kintamojo x funkcijoms $f(x)$, $g(x)$, kai $x \to x_0$.

Pavyzdziui, $\sin x \sim x$, kai $x \to 0$, $x^5 \prec e^x$, kai $x \to +\infty$.

2. Simbolis O kartais apibrėžiamas griežtesniais reikalavimais: $f(x) = O(g(x))$ $(x \to x_0) \Leftrightarrow \exists \lim\limits_{x\to x_0} \dfrac{f(x)}{g(x)} = C > 0$. Tai atitinka

mūsų žymėjimą $f(x) \asymp g(x)$.
3. Kitas gerai žinomas matematikoje simbolis *o* (O ir *o* vadinami Landau[26]simboliais) apibrėžiamas taip:
$f(x) = o(g(x))$, kai $x \to x_0 \Leftrightarrow \exists \lim\limits_{x \to x_0} \dfrac{f(x)}{g(x)} = 0$.
Taigi simboliai *o* ir $\prec$ turi panašią prasmę.

Asimptotikų pavyzdžiai

Tarkime, kad n yra natūralusis skaičius. Pažymėkime $\pi(n)$, kiek yra pirminių skaičių, nedidesnių už n. Yra žinoma, kad $\pi(n) \sim \dfrac{n}{\ln n}$ kai $n \to \infty$. Su visais $0 < \varepsilon < 1$ turime $\dfrac{1}{n^\varepsilon} \prec \dfrac{1}{\ln n} \prec 1$. Todėl

$$n^{1-\varepsilon} \prec \pi(n) \prec n.$$

Kai $n \to \infty$, galioja Stirlingo formulė:

$$n! \sim \sqrt{2\pi n} n^n e^{-n}.$$

Apibrėžimai

Sakome, kad asimptotinė aproksimacija $F(n) \approx f(n)$ turi *absoliučią paklaidą* $O(g(n))$, kai $F(n) = f(n) + O(g(n))$.
Jei $F(n) = f(n)(1 + O(g(n)))$, sakome, kad formulė turi *santykinę paklaidą* $O(g(n))$.

Pavyzdžiai

$$\pi(n) = \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + O\left(\frac{n}{(\ln n)^2}\right);$$
$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + \frac{1}{12n} + \frac{1}{288n^2} + O\left(\frac{1}{n^3}\right)\right).$$

Lentelėje surašyti $n!$ ir jo apytikslių reikšmių, apskaičiuotų pagal pateiktą asimptotinę formulę, rezultatai.

[26]Edmund Georg Hermann Landau (1877 – 1938) – vokiečių matematikas

n	$n!$	$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\left(1+\frac{1}{12n}+\frac{1}{288n^2}\right)$
1	1	1.002184
2	2	2.000629
3	6	6.000578
4	24	24.00099
5	120	120.0025
10	3628800	3628810.
11	$3.991660 \cdot 10^7$	$3.991688 \cdot 10^7$
13	$6.227021 \cdot 10^9$	$6.227028 \cdot 10^9$
15	$1.307674 \cdot 10^{12}$	$1.307675 \cdot 10^{12}$
20	$2.432902 \cdot 10^{18}$	$2.432903 \cdot 10^{18}$
30	$2.652529 \cdot 10^{32}$	$2.652529 \cdot 10^{32}$
50	$3.041409 \cdot 10^{64}$	$3.041409 \cdot 10^{64}$
100	$9.332622 \cdot 10^{157}$	$9.332622 \cdot 10^{157}$

3. Sąryšių teorija

3.1. Pagrindiniai apibrėžimai

Sąryšių pavyzdžiai

Apibrėžimai
Sąryšiu R tarp aibių A ir B elementų vadinamas bet kuris jų Dekarto sandaugos poaibis: $R \subset A \times B$. ***Sąryšiu*** *aibėje* A vadinamas bet kuris poaibis $R \subset A^n$. *Unarusis* sąryšis ($n = 1$) reiškia, kad elementas $a \in R \subset A$ turi savybę R.

Pavyzdžiai
1. *Tapatumo* sąryšis $I_A = \{(a, \cdots, a) : a \in A\} \subset A^n$.
2. *Universalusis* sąryšis $U_{A\times B} = \{(a, b) : a \in A \ \& \ b \in B\} = A \times B$.
3. *Tuščiasis* sąryšis $\emptyset \subset A^n$.
4. Sveikųjų skaičių aibėje apibrėžkime sąryšius
$R_1 = \{(x, y) : x$ dalus iš $y\}$, $R_2 = \{(x, y) : x \leqslant y\}$,
$R_3 = \{(x, y) : x = 2y\}$.
5. Tarkime, kad K – studentų kodų aibė, P – studentų pavardžių sąrašas (aibė), V – vardų sąrašas, G – grupių aibė, M – gimimo metai. Sąryšis
$R \subset K \times P \times V \times G \times M$
sudaro tam tikrą *duomenų bazę*.

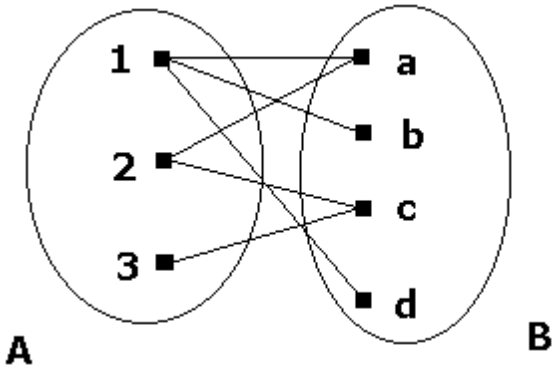
Binarieji sąryšiai

Apibrėžimai
Sąryšio $R \subset A \times B$ ***apibrėžimo sritimi*** vadinama aibė

$$\mathcal{D}(R) = \{x : \exists y \ (x, y) \in R\} \subset A.$$

Sąryšio $R \subset A \times B$ ***reikšmių sritimi*** vadinama aibė

$$\mathcal{R}(R) = \{y : \exists x \ (x, y) \in R\} \subset B.$$



6: Binarusis sąryšis

Pavyzdys

$R = \{(1,1),(2,1),(6,1),(6,2)\},\ \mathcal{D}(R) = \{1,2,6\},\ \mathcal{R}(R) = \{1,2\}.$

Pastaba
Binarusis sąryšis $R \subset A^2$ dažnai užrašomas pavidalu aRb:
$a > b$, $x = y$, $\alpha \leqslant \beta$.

Binarieji sąryšiai gali būti pavaizduoti grafiškai. 6 paveiksle pavaizduotas sąryšis $R \subset A \times B$, $A = \{1,2,3\}$, $B = \{a,b,c,d\}$,
$R = \{(1,a),(1,b),(1,d),(2,a),(2,c),(3,c)\}$.

Pavyzdžiai

1. $R_1 = \{(a_1,b_1),(a_1,b_2),(a_2,b_3)\}$,
$\mathcal{D}(R_1) = \{a_1,a_2\},\ \mathcal{R}(R_1) = \{b_1,b_2,b_3\}$.

2. $R_2 = \{(a,a),(a,b),(a,c),(b,c),(d,c)\}$,
$\mathcal{D}(R_2) = \{a,b,d\},\ \mathcal{R}(R_2) = \{a,b,c\}$.

Apibrėžimas
Matrica $M_R = \|m_{ij}\|_{n\times m}$ su elementais

$$m_{ij} = \begin{cases} 1, & \text{kai } (a_i,b_j) \in R, \\ 0, & \text{kai } (a_i,b_j) \notin R \end{cases}$$

vadinama ***binariojo sąryšio*** $R \subset A \times B$ ***matrica***.
Čia $n = |A|$, $m = |B|$.
Pavyzdžiai
Sąryšių R_1 ir R_2 matricos

$$M_{R_1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},\ M_{R_2} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

6 paveiksle pavaizduoto sąryšio R matrica yra:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Binariųjų sąryšių savybės

Apibrėžimai
Sąryšis R aibėje A vadinamas ***refleksyviuoju***, jei $\forall a \in A\ (a,a) \in R$. Kai $\forall a \in A\ (a,a) \notin R$, sąryšis vadinamas ***antirefleksyviuoju***. Kai $(a,b) \in R \Rightarrow (b,a) \in R$, sąryšis R vadinamas ***simetriniu***. Jei $(a,b) \in R\ \&\ (b,a) \in R \Rightarrow a = b$ — ***antisimetriniu***. ***Tranzityvusis*** sąryšis tenkina sąlygą $(a,b) \in R\ \&\ (b,c) \in R \Rightarrow (a,c) \in R$. ***Pilnasis*** sąryšis apibrėžiamas taip: $\forall a,b \in A\ \&\ a \neq b \Rightarrow (a,b) \in R \vee (b,a) \in R$.

Apibrėžimas
Sąryšis $R^{-1} = \{(a,b) : (b,a) \in R\}$, t. y. $aR^{-1}b \Leftrightarrow bRa$ vadinamas ***atvirkštiniu*** sąryšiui R. Pastebėkime, kad $\left(R^{-1}\right)^{-1} = R$.

Pavyzdžiai
1. $(>)^{-1} = (<)$;
2. $(\leqslant)^{-1} = (\geqslant)$;
3. $(=)^{-1} = (=)$.

Teoremos
Sąryšis $R \subset A^2$ yra
1) refleksyvusis $\Leftrightarrow I_A \subset R$;
2) antirefleksyvusis $\Leftrightarrow R \cap I_A = \emptyset$;
3) simetrinis $\Leftrightarrow R = R^{-1}$;
4) antisimetrinis $\Leftrightarrow R \cap R^{-1} \subset I_A$;
5) pilnasis $\Leftrightarrow R \cup I_A \cup R^{-1} = U_A$.

Operacijos su sąryšiais

Sąryšių *sankirta*, *sąjunga*, *skirtumas* ir *papildinys* apibrėžiami kaip atitinkamos operacijos su aibėmis.

Pavyzdžiai
Tarkime, kad sveikųjų skaičių aibėje apibrėžti sąryšiai

$$\varphi_1 = \{(m,n) : m \geqslant n\},$$
$$\varphi_2 = \{(m,n) : m > n\},$$
$$\varphi_3 = \{(m,n) : m < n\}.$$

Tada

$$\varphi_2 \subset \varphi_1,\ \varphi_1 \cup \varphi_2 = \varphi_1,$$
$$\varphi_1 \cap \varphi_2 = \varphi_2,\ \varphi_1 \setminus \varphi_2 = \{(m,n) : m = n\},$$
$$\overline{\varphi}_3 = \varphi_1.$$

Apibrėžimas
Apibrėžtų aibėje A sąryšių φ ir ψ ***kompozicija*** vadinamas sąryšis

$$\varphi \circ \psi = \{(a,b) : \exists c \in A (a,c) \in \varphi \ \&\ (c,b) \in \psi\}.$$

Pastebėkime, kad bendru atveju $\varphi \circ \psi \neq \psi \circ \varphi$.

Pavyzdžiai

$$\varphi_1 \circ \varphi_2 = \varphi_2 \circ \varphi_1 = \varphi_2,$$
$$\varphi_1 \circ \varphi_3 = \varphi_3 \circ \varphi_1 = \varphi_2 \circ \varphi_3 = \varphi_3 \circ \varphi_2 = U_Z = Z^2.$$

Teoremos
$\forall \varphi, \psi, \rho \subset A^2$:
1) $\varphi \circ I_A = I_A \circ \varphi = \varphi$;
2) $\varphi \circ \emptyset = \emptyset \circ \varphi = \emptyset$;
3) $(\varphi \circ \psi) \circ \rho = \varphi \circ (\psi \circ \rho)$;
4) $(\varphi \circ \psi)^{-1} = \psi^{-1} \circ \varphi^{-1}$.

Apibrėžimas
Sąryšio $R \subset A^2$ *laipsniu* vadinama jo kompozicija su savimi:

$$R^n = \underbrace{R \circ \cdots \circ R}_{n \text{ kartų}},\ R^0 = I_A,\ R^1 = R,\ R^2 = R \circ R, \ldots,$$
$$R^n = R^{n-1} \circ R.$$

Teorema
Saryšis R yra tranzityvusis tada ir tik tada, kai $R \circ R \subset R$.

3.2. Ekvivalentumo sąryšiai

Apibrėžimai ir pavyzdžiai

Apibrėžimas
Sąryšis $R \subset A^2$ vadinamas ***ekvivalentumo sąryšiu***, jei jis yra
1) refleksyvusis;
2) simetrinis;
3) tranzityvusis.

Pavyzdžiai
1. Tapatumo sąryšis I_A yra ekvivalentumo sąryšis.
2. Skaičių lygybė yra tapatumo sąryšis.
3. $\tau = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}$ yra ekvivalentumo sąryšis aibėje $\{1,2,3\}$.

Ekvivalentumo klasės

Apibrėžimas
Tarkime, kad $R \subset A^2$ yra ekvivalentumo sąryšis. Aibės A poaibis

$$[a]_R = \{b \in A : (a,b) \in R\}$$

vadinamas elemento $a \in A$ ***ekvivalentumo klase***.

Lemos
1) $\forall a \in A : [a]_R \neq \emptyset$;
2) $(a,b) \in R \Rightarrow [a]_R = [b]_R$;
3) $\forall (a,b) \notin R \Rightarrow [a]_R \cap [b]_R = \emptyset$.

Teorema

$$\exists \mathcal{B} = \{B_1, B_2, \ldots\} : \; B_j \neq \emptyset, \; \forall i \neq j \, B_i \cap B_j = \emptyset, \; \bigcup_i B_i = A.$$

Taigi bet kuris ekvivalentumo sąryšis apibrėžia aibės A *skaidinį*, kurio blokai yra ekvivalentumo klasės.

Apibrėžimas
Aibė $A/R = \{[a]_R\}_{a \in A}$ vadinama ***faktoraibe***.

3.3. Tvarkos sąryšiai

Apibrėžimai ir pavyzdžiai

Apibrėžimai
Antisimetrinis ir tranzityvusis sąryšis vadinamas ***tvarkos sąryšiu***. Jei sąryšis dar tenkina refleksyvumo arba antirefleksyvumo sąlygas, jis vadinamas ***negriežtosios*** arba ***griežtosios*** tvarkos sąryšiu.

Sąryšio savybės	Sąryšio pavadinimas
antisimetrinis ir tranzityvusis	***tvarkos*** sąryšis
refleksyvusis	***negriežtosios*** tvarkos
antirefleksyvusis	***griežtosios*** tvarkos
pilnasis	***visiškosios*** tvarkos
nėra pilnasis	***dalinės*** tvarkos

Tvarkos sąryšiai žymimi $\prec$, $\preccurlyeq$, $\npreccurlyeq$, $\succ$, $\succcurlyeq$, $\nsucccurlyeq$.

Pavyzdžiai
1. Sąryšiai $\leqslant$, $\geqslant$ yra negriežtosios visiškosios tvarkos sąryšiai skaičių aibėse.
2. Sąryšiai $\subset$, $\supset$ yra negriežtosios dalinės tvarkos sąryšiai buleane $\mathcal{B}(A) = 2^A$.

Sutvarkytosios aibės

Apibrėžimas
Aibės elementas $m \in A$ vadinamas ***minimaliuoju***, jei

$$\overline{\exists} a \in A : a \prec m \;\&\; a \neq m.$$

Teorema
Bet kuri netuščioji iš dalies sutvarkyta aibė turi minimalųjį elementą.

Apibrėžimas
Aibė, kurioje apibrėžtas visiškosios tvarkos sąryšis, vadinama *visiškai sutvarkyta*.

Teorema
Visiškai sutvarkyta aibė turi vienintelį minimalųjį elementą.

3.4. Sąryšių uždaviniai

Sąryšio tranzityvusis uždarinys

Apibrėžimas
Sąryšis

$$R^+ = \{(a,b) \in R : \exists c_1, c_2, \ldots, c_k \in A\ (a,c_1) \in R \& \\ (c_1,c_2) \in R \& \cdots \& (c_k,b) \in R\}$$

vadinamas sąryšio R ***tranzityviuoju uždariniu***.

Jei R yra tranzityvusis, tai $R^+ = R$.

Teoremos
$\forall R \subset A^2$ & $|A| = n$
1) $R^+ = \bigcup\limits_{i=1}^{\infty} R^i = \bigcup\limits_{i=1}^{n-1} R^i$;
2) $M_{R^+} = \bigvee\limits_{i=1}^{n} M_{R^i} = \bigvee\limits_{i=1}^{n} (M_R)^i$.

Pavyzdžiai
1. $R = \{(x,y) : y = x+1\} \subset N^2 \Rightarrow R^+ = \{(x,y) : x < y\}$;
2. $R = \{(x,y) : x < y\} \subset Q^2 \Rightarrow R^+ = R$.

Sąryšio refleksyvusis uždarinys

Apibrėžimas
Sąryšio refleksyvusis uždarinys apibrėžiamas taip:

$$A^* = A^+ \cup I_A.$$

Pavyzdys
$R = \{(x, y) : x < y\},\ R^* = \{(x, y) : x \leq y\}.$

3.5. Funkcijos

Injekcija. Siurjekcija. Bijekcija

Apibrėžimas
Sąryšis $f \subset A \times B$ vadinamas ***funkcija***, kai

$$\forall (a, b) \in f \ \& \ (a, c) \in f \Rightarrow b = c.$$

Funkcija $(a, b) \in f$ paprastai užrašoma $b = f(a)$. Kintamasis $a \in A$ vadinamas jos *argumentu*, o kintamasis $b \in B$ – *reikšme*.
Funkcijos $f \subset A \times B$ ***apibrėžimo sritis*** f_A ir ***reikšmių sritis*** f_B yra šios aibės:

$$f_A = \{a \in A : \exists b \in B\ b = f(a)\},\ f_B = \{b \in B : \ \exists a \in A\ b = f(a)\}.$$

Funkcija vadinama	Sąlygos
injekcija	$b = f(a_1)\ \&\ b = f(a_2) \Rightarrow a_1 = a_2$
siurjekcija	$\forall b \in B\ \exists a \in A\ b = f(a)$
bijekcija	yra injekcija ir siurjekcija

Teorema
Jei $f \subset A \times B$ yra bijekcija ir $f_A = A$, tai atvirkštinė funkcija $f^{-1} \subset B \times A$ irgi yra bijekcija.

Perstatos

Apibrėžimas

Tarkime, kad $|A| = n$. Bijekcija $A \to A$ vadinama ***perstata***.
Perstatą

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}$$

galima užrašyti ir taip:

$$\sigma(1) = 5,\ \sigma(2) = 6,\ \ldots,\ \sigma(6) = 2.$$

Perstata

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix} = \begin{pmatrix} a_n & a_2 & \cdots & a_{n-1} & a_1 \\ a_1 & a_3 & \cdots & a_{n-2} & a_n \end{pmatrix}$$

vadinama ***ciklu***. Šio ciklo ilgis lygus n.
Perstatos $\begin{pmatrix} 1 & 4 & 5 \\ 5 & 1 & 4 \end{pmatrix}$, $\begin{pmatrix} 2 & 6 \\ 6 & 2 \end{pmatrix}$ ir $\begin{pmatrix} 3 \\ 3 \end{pmatrix}$ yra ciklai, kurie gali būti užrašyti taip: $(1, 5, 4)$, $(2, 6)$, (3).

Apibrėžkime perstatų *sandaugą* kaip funkcijų kompoziciją. Pavyzdžiui, kai

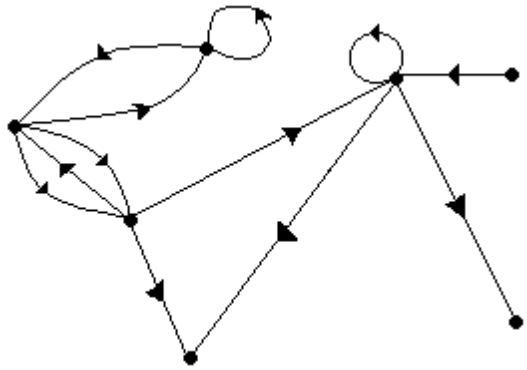
$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 6 & 3 & 1 & 4 & 2 \\ 4 & 5 & 6 & 3 & 1 & 2 \end{pmatrix},$$

turime

$$\rho \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 1 & 2 \end{pmatrix}.$$

Kiekvieną perstatą galima užrašyti kaip nesikertančiųjų ciklų sandaugą. Pavyzdžiui,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix} = (1, 5, 4) \circ (3) \circ (2, 6).$$



7: Multigrafo pavyzdys

4. Grafų teorija

4.1. Pagrindiniai apibrėžimai

Multigrafas

7-ame paveiksle pavaizduotas objektas yra vadinamas ***multigrafu***. Pastebėję, kad multigrafą sudaro jo ***viršūnės*** bei ***lankai***, aprašykime jį matematiškai. Tarkime, $V = \{v_1, v_2, \ldots, v_n\}$ – multigrafo *viršūnių aibė*. Tada jo lankus galime apibrėžti taip:

$$l = (v_i, v_j, z_k) \in V \times V \times N.$$

Čia v_i – lanko pradžia, v_j – jo galas, z_k – lanko numeris (žymė), N – natūraliųjų skaičių aibė. Lankai su tomis pačiomis pradžiomis ir su tais pačiais galais vadinami ***lygiagrečiaisiais***. Taigi lankai $l_1 = (v_i, v_j, 1)$ ir $l_2 = (v_i, v_j, 2)$ yra lygiagretieji. Pastebėkime, kad nelygiagrečiųjų lankų *galima nenumeruoti*. Lankas, kurio pradžia ir galas sutampa (t. y. $l = (v, v, z)$), vadinamas ***kilpa***.

Paprastasis grafas

Apibrėžimas
Multigrafas be kilpų ir lygiagrečiųjų lankų vadinamas ***paprastuoju*** *orientuotuoju* grafu.

Kadangi paprastuojo grafo lankų numeruoti nėra būtina, jie sudaro aibės $V \times V$ poaibį, kurį vadiname ***binariuoju sąryšiu***. Priminsime, kad sąryšis $L \subset V \times V$ vadinamas *antirefleksyviuoju*, kai $(v, v) \notin L \; \forall v \in V$. Taigi kilpų nebuvimą galima išreikšti antirefleksyvumu. Apibrėžkime paprastąjį orientuotąjį grafą G kaip aibių porą $G = (V, L)$, kai $L \subset V \times V$ yra antirefleksyvusis sąryšis.

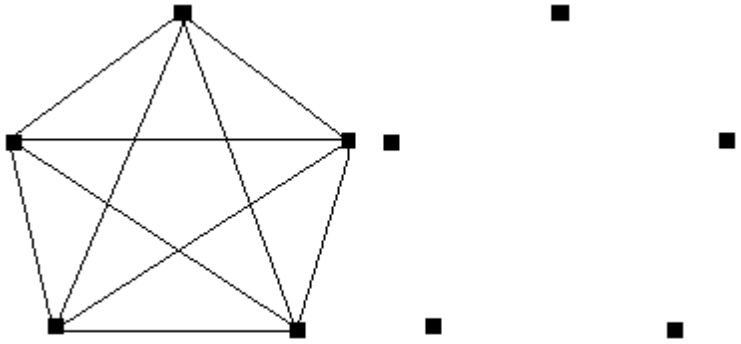
Neorientuotasis grafas

Tarkime, kad paprastas orientuotasis grafas $G = (V, L)$ yra *simetrinis*, t. y. saryšis L turi *simetriškumo* savybę: $(v_i, v_j) \in L \Rightarrow (v_j, v_i) \in L$. Tada dviejų lankų porą $\{(v_i, v_j), (v_j, v_i)\}$ pakeiskime viršūnių v_i ir v_j ***pora*** $\{v_i, v_j\}$ ir vadinsime ją grafo ***briauna***. Šiuo atveju viršūnių eilės tvarka neturi reikšmės ir visų briaunų aibė yra

$$B = \{\{v_i, v_j\}, v_i, v_j \in V\} \subset V^{(2)},$$
$$V^{(2)} = \{\{v_1, v_2\}, \{v_1, v_3\}, \ldots, \{v_{n-1}, v_n\}\}.$$

Apibrėžimas
Grafą $G = (V, B)$ vadiname paprastuoju ***neorientuotuoju*** grafu.

Toliau nagrinėdami paprastuosius neorientuotus grafus, juos vadinsime tiesiog grafais. Kai kalbėsime apie orientuotuosius grafus, tai bus papildomai pabrėžta. Pastebėkime, kad toliau formuluojami neorientuotiems grafams apibrėžimai nesunkiai taikomi ir orientuotiems grafams.
Apibrėžimai
Grafo $G = (V, B)$ ***eile*** vadinamas skaičius $|V| = n$.
Grafas $G = (V, \emptyset)$ vadinamas ***tuščiuoju***. Jis žymimas O_n, čia $n = |V|$



8: Penktosios eilės pilnasis ir tuščiasis grafas

– grafo eilė.
Grafas $G = (\emptyset, \emptyset)$ vadinamas ***nuliniu***.
Grafas, turintis visas $\frac{n(n-1)}{2}$ briaunas ($n = |V|$), vadinamas ***pilnuoju*** ir žymimas K_n.
Grafo $G = (V, B)$ viršūnės v_i ir v_j vadinamos ***gretimomis***, kai $\{v_i, v_j\} \in B$.
Viršūnės v_i ir v_j vadinamos ***incidenčiosiomis*** briaunai $\{v_i, v_j\}$.
Briaunos, turinčios bendrą incidenčiąją viršūnę, vadinamos ***gretimomis***.

Pastebėkime, kad *gretimumas* yra tos pačios (viršūnių arba briaunų) aibės elementų savybė, o *incidentumas* – skirtingų.

Grafo viršūnių laipsniai

Grafo $G = (V, B)$ viršūnės $v \in V$ ***aplinka*** yra vadinama visų jai gretimų viršūnių aibė:

$$\Gamma(v) = \{w \in V : \{v, w\} \in B\}.$$

Orientuoto grafo atveju aibę $\Gamma(v)$ suskaldome i dvi:

$$\Gamma(v) = \Gamma^-(v) \cup \Gamma^+(v),$$

kurios atitinka išeinančius bei įeinančius lankus.

Apibrėžimas. Skaičius $p(v) = |\Gamma(v)|$ yra vadinamas viršūnės v ***laipsniu***. Orientuoto grafo atveju turime $p(v) = p(v)^- + p(v)^+ \equiv |\Gamma^-(v)| + |\Gamma^+(v)|$. Skaičiai $p(v)^-$ ir $p(v)^+$ yra vadinami išėjimo ir įėjimo ***puslaipsniais***. Orientuoto grafo viršūnė v yra vadinama jo ***įėjimu (išėjimu)***, kai $p^+(v) = 0,\ p^-(v) > 0$ ($p^+(v) > 0,\ p^-(v) = 0$).

Skaičiuojant grafo briaunas, incidentiškas kiekvienai jo viršūnei, gausime grafo briaunų skaičių, padauginta iš dviejų. Taigi yra įrodyta Oilerio[27] teorema.

Teorema
Grafo briaunų (lankų) skaičius yra lygus $|B| = \frac{1}{2}\sum_{i=1}^{n} p(v_i)$, n – grafo eilė.

Pastabos
1. Grafo viršūnių laipsnių suma yra lyginis skaičius.
2. Viršūnių su nelyginiais laipsniais skaičius yra lyginis.
3. Pilnojo neorientuotojo grafo K_n visų viršūnių laipsniai yra $n-1$, pilnojo orientuotojo — $2(n-1)$.

Apibrėžimai
Grafo viršūnė v yra vadinama ***izoliuotąja***, kai $p(v) = 0$.
Viršūnę vadiname ***nusvirusiąja***, jei $p(v) = 1$.

[27] Leonhard Euler (1707 – 1783) – šveicarų matematikas.

Grafas vadinamas ***homogeniniu***, kai visų jo viršūnių laipsniai yra lygūs: $p(v) = p(w)\ \forall v, w \in V$. Grafas, kurio visų viršūnių laipsniai yra lygūs dviem: $p(v) = 2\ \forall v \in V$, vadinamas ***ciklu***[28] ir žymimas C_n ($n = |V|$).

4.2. Grafų izomorfizmas

Iizomorfizmo apibrėžimas

Kadangi grafo viršūnes galima pažymėti (sunumeruoti) įvairiais būdais, tą patį grafą užrašome (V_1, B_1) ir (V_2, B_2) ($|V_1| = |V_2|$). Kai turime du grafus $G_1 = (V_1, B_1)$, $G_2 = (V_2, B_2)$, atsakyti į klausimą ar jie yra vieno grafo du skirtingi žymėjimai gali būti sunku. Akivaizdu, kad atsakymas yra neigiamas, kai $|V_1| \neq |V_2|$ arba $|B_1| \neq |B_2|$. Suformuluokime šį uždavinį matematiškai.

Apibrėžimas
Grafai $G_1 = (V_1, B_1)$ ir $G_2 = (V_2, B_2)$ yra vadinami ***izomorfiniais*** (rašome $G_1 \cong G_2$), jei egzistuoja tokia *bijekcija* $f : V_1 \to V_2$, kad

$$\forall\{v_i^1, v_j^1\} \in B_1 \ \Rightarrow\ \{f(v_i^1), f(v_j^1)\} \in B_2,$$
$$\forall\{v_i^2, v_j^2\} \in B_2 \ \Rightarrow\ \{f^{-1}(v_i^2), f^{-1}(v_j^2)\} \in B_1.$$

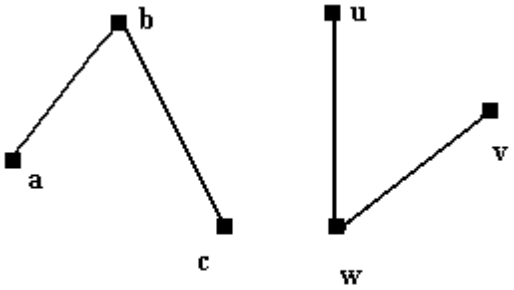
Pavyzdys. Pavaizduoti 9 paveiksle grafai užrašomi taip:

$$V_1 = \{a, b, c\}, B_1 = \{\{a, b\}, \{b, c\}\},$$
$$V_2 = \{u, v, w\}, B_2 = \{\{u, w\}, \{v, w\}.$$

Taigi apibrėžimo sąlygas tenkina ši bijekcija:

$$f(a) = u,\ f(b) = w,\ f(c) = v.$$

[28] Čia kalbama apie jungųjį grafą, kai grafas nėra sudarytas iš kelių atskirų komponenčių. Priešingu atveju gausime kelis ciklus.



9: Izomorfinių grafų pavyzdys

Žymėtieji ir nežymėtieji grafai

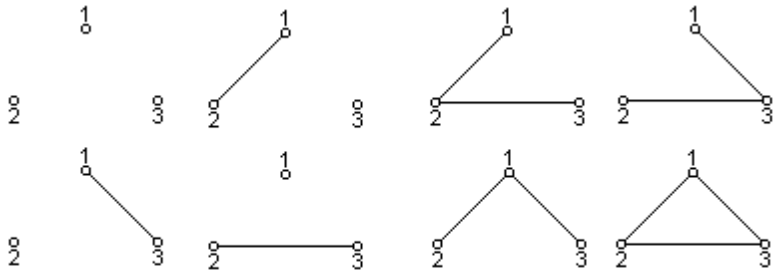
Pastebėkime, kad grafų izomorfizmas yra *ekvivalentumo sąryšis*. Prisminsime, kad toks sąryšis turi tris savybes.
1) Refleksyvumas: $G \cong G$. Šiuo atveju bijekcija $f(v_i) = v_i$.
2) Simetriškumas: $f : G_1 \to G_2 \ \Rightarrow \ f^{-1} : G_2 \to G_1$.
3) Tranzityvumas: $f : G_1 \to G_2 \& h : G_2 \to G_3 \Rightarrow (f \circ h) : G_1 \to G_3$.
Visų izomorfinių grafų klasė vadinama ***nežymėtuoju*** grafu, atskiri šios klasės elementai – ***žymėtieji*** grafai.

Invariantai

Visi *izomorfiniai* vienas kitam grafai (t. y. visa ekvivalentumo klasė arba *nežymėtasis* grafas) turi tam tikras bendrąsias savybes, kurios nepriklauso nuo grafo viršūnių žymėjimo būdo (galioja kiekvienam pasirinktam žymėtajam grafui). Grafo funkcijos[29], įgyjančios tas pačias reikšmes su visais izomorfiniais grafais, vadinamos grafų teorijos ***invariantais***.

Pavyzdžiui, grafo $G = (V, B)$ eilė (viršūnių skaičius: $n(G) = |V|$)

[29]T. y. priklausantys nuo grafo kintamieji dydžiai (funkcijos apibrėžtos grafų aibėje).



10: Visi trečiosios eilės žymėtieji grafai

arba briaunų skaičius $m(G) = |B|$ yra invariantai. Kitas invariantas yra aibė, sudaryta iš grafo viršūnių laipsnių: $\{p_1, p_2, \ldots, p_k\}$. Mes išnagrinėsime daug kitų grafo charakteristikų, kurios irgi yra invariantai.

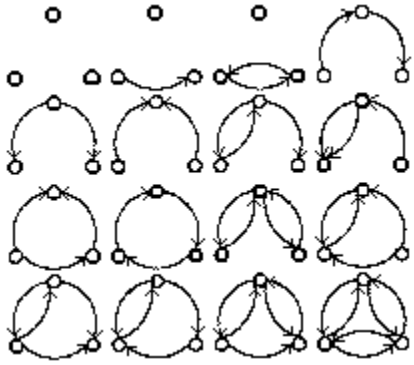
Grafų skaičius

Matome (žr. 10 pav.), kad iš viso yra 8 skirtingi trečiosios eilės žymėtieji grafai. Suskaičiuokime, kiek tokių grafų yra bendruoju atveju. Tarkime, kad $|V| = n$. Tada skirtingų grafo viršūnių porų yra $m = C_n^2 = \binom{n}{2} = \dfrac{n(n-1)}{2}$. Jei grafas turi k briaunų, tai reikia išrinkti k iš m tokių viršūnių porų. Tai galima padaryti $C_m^k = \binom{\binom{n}{2}}{k}$ būdais.

Taigi n-osios eilės žymėtųjų grafų skaičių *generuojančioji* funkcija yra

$$G_n(x) = \sum_{k=0}^{m} \binom{m}{k} x^k = (1+x)^m,\ m = \binom{n}{2}.$$

Todėl visų žymėtųjų grafų skaičius lygus $G_n(1) = (1+1)^m = 2^{\binom{n}{2}}$. Kai $n = 3$ (žr. 10 pav.), turime



11: Trečiosios eilės nežymėtieji orientuotieji grafai

$m = C_3^2 = 3$, $G_3(1) = 2^3 = 8$.

Panašiai galime suskaičiuoti *orientuotuosius* grafus. Orientuotųjų n–osios eilės žymėtųjų grafų, turinčių k lankų yra $C^k_{n(n-1)}$. Generuojančioji funkcija šiuo atveju yra

$$\tilde{G}_n(x) = \sum_{k=0}^{n(n-1)} C^k_{n(n-1)} x^k = (1+x)^{n(n-1)}.$$

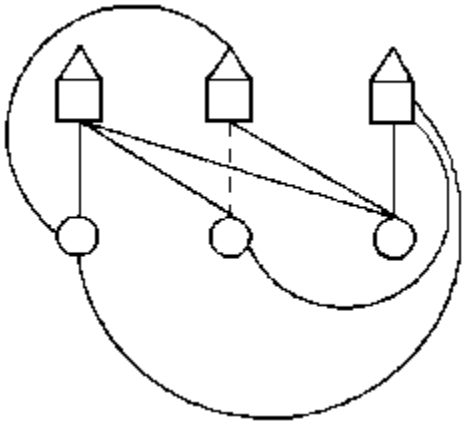
Taigi turime $\tilde{G}_n(x) = (G(x))^2$ ir $\tilde{G}_n(1) = 2^{n(n-1)}$.

Nežymėtųjų grafų skaičių formulės yra gremėzdiškos. Pažymėkime g_n visų nežymėtųjų neorientuotųjų n-tosios eilės grafų skaičių. Kai n yra didelis skaičius galioja *asimptotinė* formulė

$$g_n \sim \frac{2^{\binom{n}{2}}}{n!},\ n \to \infty.$$

Planarieji grafai

Izomorfinius grafus galima ne tik pažymėti įvairiais būdais, bet ir pavaizduoti skirtingomis diagramomis. Pasirinkime tokį grafo viršūnių



12: Trijų namų ir trijų šulinių uždavinys

išdėstymą plokštumoje, kad visi briaunų susikirtimo taškai sutaptu su grafo viršūnėmis. Taip pavaizduotą grafą vadiname ***plokščiuoju***. Plokščiajam grafui izomorfinių grafų klasė yra vadinama ***planariaisiais*** grafais. Trijų šulinių galvosūkis (reikia sujungti kiekvieną iš trijų namų su kiekvienu iš trijų šulinių taip, kad takeliai nesusikirstų), kaip 1930 m. įrodė Kuratovskis[30] neturi sprendinio. Taigi ne visi grafai yra planarieji.

4.3. Grafų jungumas

Maršrutai ir grandinės

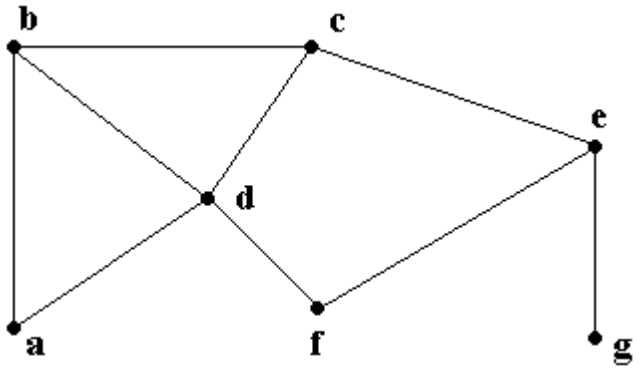
Baigtinė seka, sudaryta iš grafo $G = (V, B)$ viršūnių ir briaunų

$$v_{i_0},\ b_{i_1},\ v_{i_1},\ b_{i_2},\ \ldots,\ v_{i_k},\ b_{i_k},\ v_{i_k},$$

taip, kad kiekviena briauna $b_{i_j} = \{v_{i_{j-1}}, v_{i_j}\}$, vadinama ***maršrutu***.

Pavaizduotas 13-ame paveiksle grafas turi maršrutą M:

[30] Kazimierz Kuratowski (1896 – 1980) – lenkų matematikas.



13: Maršrutai ir grandinės

$$a, \{a,b\}, b, \{b,c\}, c, \{c,e\}, e, \{e,f\}, f,$$
$$\{d,f\}, d, \{c,d\}, c, \{b,c\}, b, \{b,d\}, d.$$

Maršrutą M galima užrašyti ir trumpiau:

$$M = (a,b,c,e,f,d,c,b,d).$$

Panašiai galime išnagrinėti kitus maršrutus:

$$M_1 = (a,b,c,d,f),$$
$$M_2 = (c,e,g),$$
$$M_3 = (b,c,e,f,d,b),$$
$$M_4 = (a,b,d,c,e,f,d,a).$$

Apibrėžimai

Maršruto viršūnės v_{i_0} ir v_{i_k} vadinamos *galinėmis* (*terminalinėmis*), kitos viršūnės v_{i_j} – *vidinės*.

Maršrutas vadinamas ***atviruoju***, jei jo galinės viršūnės yra skirtingos. Priešingu atveju maršrutą vadiname ***uždaruoju***.

Maršrutas, kurio visos briaunos yra skirtingos, vadinamas ***grandine***.
Atviroji grandinė yra vadinama ***keliu***.
Uždarąją grandinę vadiname ***ciklu***.
Grandinę, kurios visos vidinės viršūnės yra skirtingos, vadiname ***paprastąja***.

Maršrutas M nėra grandinė, maršrutai M_1 – M_2 yra grandinės. Grandinės M_1 ir M_2 yra keliai, M_3, M_4 – ciklai. Ciklas M_3 yra paprastasis, o M_4 – nėra.

Grafo jungosios komponentės

Apibrėžimas
Grafas vadinamas ***jungiuoju***, jei bet kurias jo viršūnes galima sujungti keliu.

Tarkime, kad grafas $G = (V, B)$ nėra jungusis. Tada jo viršūnių aibę V galima suskaidyti į *blokus* V_1, V_2 ($V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$) taip, kad

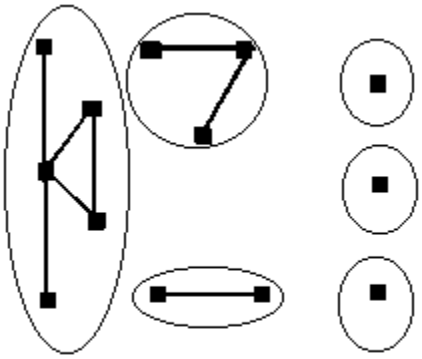
$$\forall v_1, v_2 \in V : v_1 \in V_1 \;\&\; v_2 \in V_2 \;\Rightarrow\; \overline{\exists}\, \{v_1, v_2\} \in B.$$

Jei kurių nors dviejų aibės V_1 arba V_2 viršūnių negalima sujungti keliu, šią aibę vėl skaidome į blokus: $V_1 = V_3 \cup V_4$ ir bet kurių viršūnių $v_3 \in V_3$, $v_4 \in V_4$ negalima sujungti keliu. Taigi, atlikus baigtinį žingsnių skaičių, gausime tokį viršūnių aibės V skaidinį

$$V = V_1 \cup V_2 \cup \cdots \cup V_k,\; V_i \cap V_j = \emptyset \; \forall i \neq j,$$

kad bet kurio poaibio $V_s \subset V$ viršūnės gali būti sujungti keliu. Pažymėkime $B_j \subset B$ grafo $G = (V, B)$ briaunų aibės poaibį, sudarytą iš visų briaunų, incidenčiųjų bent vienai viršūnei $v \in V_j$.

Apibrėžimas



14: Grafas su išskirtomis jungiosiomis komponentėmis

Grafą $G_j = (V_j, B_j)$ vadiname grafo $G = (V, B)$ ***jungiąja komponente***.

Pastabos
1. Bet kuris n-ojo laipsnio grafas turi ne daugiau kaip n jungiųjų komponenčių.
2. Jei n-ojo laipsnio grafas turi n jungiųjų komponenčių, tai jos yra izoliuotosios grafo viršūnės. Taigi šiuo atveju turime tuščiąjį grafą.
3. Antrosios eilės jungusis grafas turi vieną briauną.
4. Trečiosios eilės jungusis grafas turi dvi arba tris briaunas.

Jungumo sąryšys

Tarkime, kad $G = (V, B)$ bet kuris grafas. Jo viršūnių aibėje apibrėžkime grafo *jungumo* sąryšį $\rho \subset V^2$:

$$(u, w) \in \rho \Leftrightarrow u = w \ \vee \ \exists(u, v_{i_1}, \ldots, v_{i_k}, w),$$

t.y (u, w) priklauso sąryšiui, kai u ir w galima sujungti grandine.

Šis saryšis yra ekvivalentumas:
1) $\forall v \in V : v\rho v$ – refleksyvumas;
2) $v\rho w \Rightarrow w\rho v$ – simetriškumas;
3) $v\rho w \ \& \ w\rho u \Rightarrow v\rho u$ – tranzityvumas.

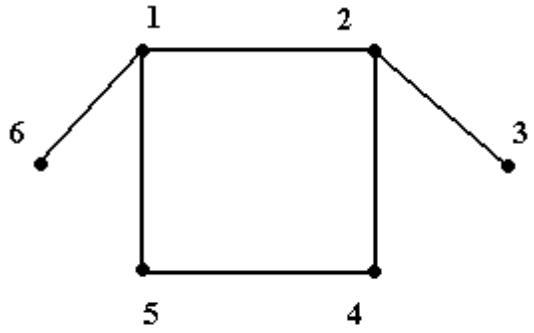
Taigi viršūnių aibę V galima suskaidyti į ekvivalentumo klases, kurios ir yra grafo jungiosios komponentės.

Ilgiausias kelias

Kelio ***ilgiu*** vadinamas įeinančių į jį briaunų skaičius.

Teorema
Du maksimalaus ilgio jungiojo grafo keliai turi bendrą viršūnę.
Įrodymas. Tarkime, kad $P_1 = (v_0, v_1, \ldots, v_k)$, $P_2 = (v'_0, v'_1, \ldots, v'_k)$ yra du grafo $G = (V, B)$ maksimalaus ilgio keliai. Kadangi grafas G yra jungusis, bet kurias dvi jo viršūnes galima sujungti keliu. Paimkime tokias dvi grafo viršūnes $v_i \in P_1$ ir $v'_j \in P_2$, kad jas būtų galima sujungti keliu $P_a = (v_i, \ldots, v'_j)$, taip kad visos vidinės kelio P_a viršūnės nepriklausytų nė vienam iš kelių P_1 ir P_2. Jei to negalima padaryti – keliai P_1 ir P_2 turi bent vieną bendrą viršūnę, ir teorema būtų įrodyta. Pažymėkime $t_1 = (v_0, v_1, \ldots, v_i)$, $t_2 = (v_i, \ldots, v_k)$, $t'_1 = (v'_0, v'_1, \ldots, v'_j)$, $t'_2 = (v'_j, \ldots, v'_k)$. Neprarandant bendrumo, galime laikyti, kad $|t_1| \geqslant |t_2|$ ir $|t'_1| \geqslant |t'_2|$. Tada kelio t_1, P_a, t'_1 ilgis $|t_1| + |P_a| + |t'_1| > |t_1| + |t_2| = k$. Taigi gavome prieštaravimą teoremos prielaidai, kad P_1 ir P_2 yra maksimalaus ilgio keliai.

Pavyzdys
Pavaizduotas 15 paveiksle grafas $G = (V, G)$, $V = \{1, 2, 3, 4, 5, 6\}$, $B = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{1, 5\}, \{1, 6\}, \{4, 5\}\}$ turi maksimalaus il-



15: Ilgiausi grafo keliai

gio kelius:

$$P_1 = (3, 2, 4, 5, 1, 6),\ |P_1| = 5,$$
$$P_2 = (6, 1, 2, 4, 5, 1),\ |P_2| = 5.$$

Taigi šiuo atveju bendrosios viršūnės yra: $1, 2, 4, 5, 6$.

Grafo metrinės charakteristikos

Tarkime, kad $G = (V, B)$ yra *jungusis* grafas, $u, w \in V$ – dvi kurios nors jo viršūnės. Sunumeruokime visus jungiančius šias viršūnes kelius:

$$P_k = (u, v_{i_1}, v_{i_2}, \ldots, v_{i_{l_k}}, w).$$

Apibrėžimas
Atstumu tarp grafo viršūnių vadinamas trumpiausio jas jungiančio kelio ilgis:

$$\rho(u, w) = \min_k |P_k(u, \ldots, w)|.$$

Pastebėkime, kad taip apibrėžtas atstumas turi *metrikos* savybes:
1) $\rho(u,w) \geqslant 0$ & $\rho(u,w) = 0 \Leftrightarrow u = w$;
2) $\rho(u,w) = \rho(w,u)\ \forall u, w \in V$;
3) $\rho(v,u) + \rho(u,w) \geqslant \rho(v,w)\ \forall v, u, w \in V$.

Atstumai tarp 15 paveiksle pavaizduoto grafo viršūnių yra: $\rho(1,2) = 1$, $\rho(3,6) = 3$, $\rho(5,3) = 2$.

Atstumo sąvoką galima apibendrinti ir tam atvejui, kai grafas *nėra jungusis*. Tada galima susitarti kad *atstumas* tarp viršūnių v ir w, priklausančių skirtingoms grafo jungiosioms komponėntėms, lygus $\rho(v,w) = \infty$.

Apibrėžimai

1. Grafo ***skersmeniu*** vadinamas maksimalus atstumas tarp grafo viršūnių:

$$d(G) = \max_{v,w \in V} \rho(v,w).$$

2. Viršūnės ***ekscentricitetu*** vadinamas jos atstumų nuo kitų grafo viršūnių maksimumas:

$$e(u) = \max_{v \in V} \rho(v,u).$$

3. Viršūnė $c \in V$ vadinama grafo ***centru***, jei jos ekscentricitetas yra minimalus:

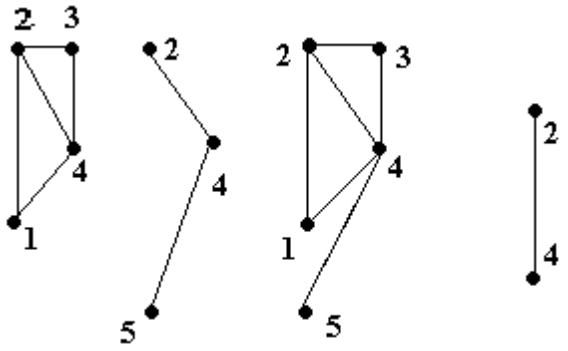
$$e(c) = \min_{v \in V} e(v).$$

4. Centro ekscentricitetas vadinamas grafo ***spinduliu***:

$$r(G) = \min_{v \in V} e(v).$$

5. Paprastąją grandinę vadiname ***skersmenine***, jei jos ilgis lygus grafo skersmeniui bei nėra trumpesnio, jungiančio jos galus, kelio.

Pavaizduoto 15 paveiksle grafo skersmuo $d(G) = 3$, spindulys $r(G) = 3$. Viršūnių ekscentricitetai: $e(1) = e(2) = 2$, $e(3) = e(4) = e(5) = e(6) = 3$. Grafo centrai yra viršūnės 1 ir 2. Grandinės (v_3, v_2, v_1, v_6) ir (v_4, v_5, v_1, v_6) yra skersmeninės.



16: Dviejų grafų sąjunga ir sankirta

4.4. Operacijos su grafais

GRAFŲ SĄJUNGA IR SANKIRTA

Tarkime, kad turime du grafus $G_1 = (V_1, B_1)$ ir $G_2 = (V_2, B_2)$. Kadangi V_i ir B_i $(i = 1, 2)$ yra aibės, galime apibrėžti grafų ***sąjungą*** ir ***sankirtą***:

$$G_1 \cup G_2 = (V_1 \cup V_2,\ B_1 \cup B_2),\ G_1 \cap G_2 = (V_1 \cap V_2,\ B_1 \cap B_2).$$

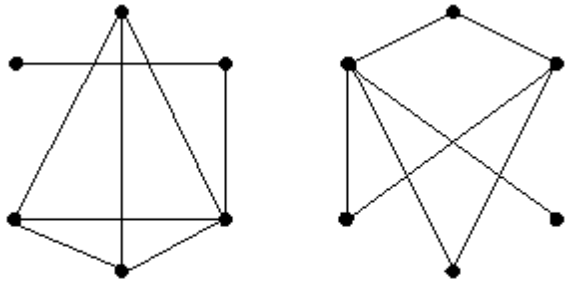
Pografis ir papildinys

Grafas $G' = (V', B')$ vadinamas grafo $G = (V, B)$ ***pografiu***, jei $V' \subset V$ ir $B' \subset B$. Rašome $G' \subset G$.

Pastebėkime, kad visos grafo jungiosios komponėntės yra jo pografiai. Dar pastebėkime, kad $G_1 \subset G_1 \cup G_2$ ir $G_1 \cap G_2 \subset G_2$.

Grafo $G = (V, B)$ ***papildinys*** $\overline{G}$ apibrėžiamas taip: $\overline{G} = (V, \overline{B})$.

Pastabos



17: Grafas ir jo papildinys

1. $G \cup \overline{G} = K_n$ – pilnasis grafas.
2. $G \cap \overline{G} = \emptyset$ – tuščiasis grafas.

Grafų ciklinė suma

Grafų $G_1 = (V_1, B_1)$ ir $G_2 = (V_2, B_2)$ ***cikline suma*** vadinsime grafą $G_1 \oplus G_2 = (\tilde{V}, \tilde{B})$, apibrėžtą taip:

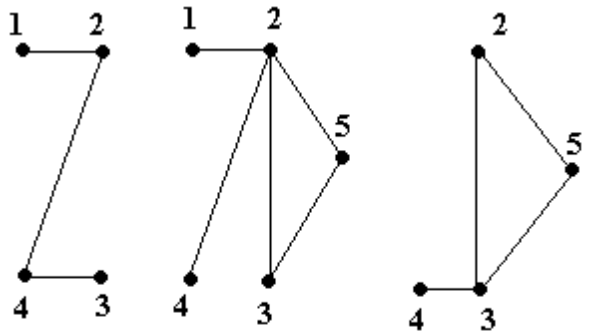
$$\tilde{B} = \{\{v,w\} : \{v,w\} \in B_1 \& \{v,w\} \notin B_2 \ \vee \ \{v,w\} \in B_2 \& \{v,w\} \notin B_1\},$$
$$\tilde{V} = \{v \in V_1 \cup V_2 : \exists \{v,w\} \in \tilde{B}\}.$$

Pastebėkime, kad grafas $G_1 \oplus G_2$ neturi izoliuotų viršūnių.

Grafo viršūnės pašalinimas

Grafo $G = (V, B)$ ***viršūnės pašalinimo operacija*** $G - v = (V', B')$ apibrėžiama taip:

$$V' = V \setminus \{v\}, \ B' = B \setminus \bigcup_{w \in V : \{w,v\} \in B} \{w, v\},$$



18: Grafų ciklinė suma

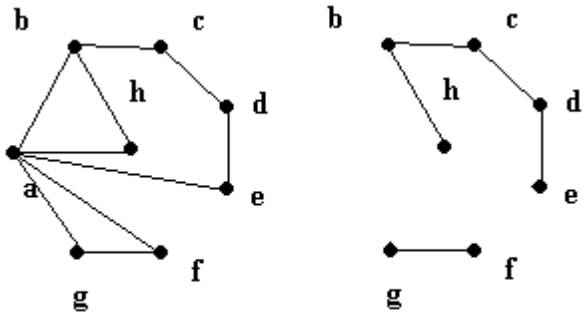
t. y. iš grafo pašalinama viršūnė $v \in V$ ir visos jai incidenčiosios briaunos.

Grafo briaunos pašalinimas

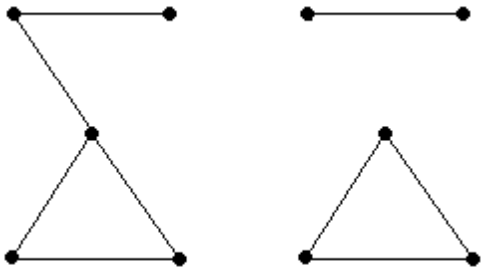
Apibrėžkime grafo $G = (V, B)$ ***briaunos pašalinimo operaciją***: $G - \{v, w\} = (V, B \setminus \{\{v, w\}\})$, t. y. pašalinama tik pati briauna, o jai incidenčiosios viršūnės paliekamos (žr. 20 pav.).

Grafo viršūnių sutapatinimas

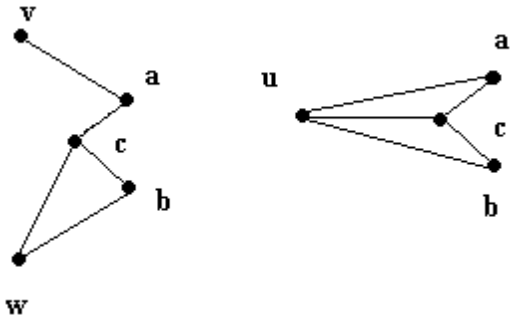
Grafo $G = (V, B)$ dvi viršūnės v ir w keičiamos nauja viršūne u, o briaunų aibė papildoma briaunomis taip, kad visos grafo viršūnes, kurios buvo gretimos bent vienai viršūnei v arba w, yra gretimos ir viršūnei u (žr. 21 pav.).



19: Grafo viršūnės a pašalinimas



20: Grafo briaunos pašalinimas



21: Grafo viršūnių v ir w sutapatinimas

4.5. Grafų skaidumas

Grafo sujungimo taškai

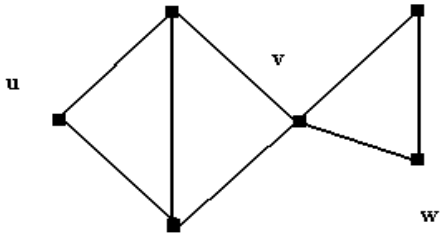
Apibrėžimas
Grafo $G = (V, B)$ viršūnė $v \in G$ yra vadinama jo ***sujungimo tašku***, jei grafas $G - v$ turi daugiau jungiųjų komponenčių negu grafas G.

Trivialusis grafas $G = (\{v\}, \emptyset)$ neturi sujungimo taškų.

Grafas, neturintis sujungimo taškų, vadinamas ***neskaidžiuoju***.

Visi kiti (nebūtinai jungieji) grafai yra *skaidieji*. Pavyzdžiui, grafas $(\{u, v, w\},\ \{\{u, v\}, \{u, w\}, \{v, w\}\})$ yra neskaidusis, o grafas $(\{u, v, w\},\ \{\{u, v\}, \{u, w\}\})$ – skaidusis. Jo viršūnė u yra sujungimo taškas.

Teorema
Viršūnė $v \in V$ yra grafo $G = (V, B)$ sujungimo taškas tada ir tik tada, kai egzistuoja tokios dvi kitos grafo G viršūnės $u, w \in V$, kad viršūnė



22: Grafo sujungimo taškas v

v priklauso bet kuriai, jungiančiai viršūnes u ir w grandinei P:

$$\exists u, w \in V \& u \neq v \& w \neq w : v \in P \; \forall P = (u, v_{i_1}, \ldots, v_{i_k}, w).$$

Teorema
Bet kuris *netrivialusis* grafas turi mažiausiai dvi viršūnes, kurios nėra jo sujungimo taškai.

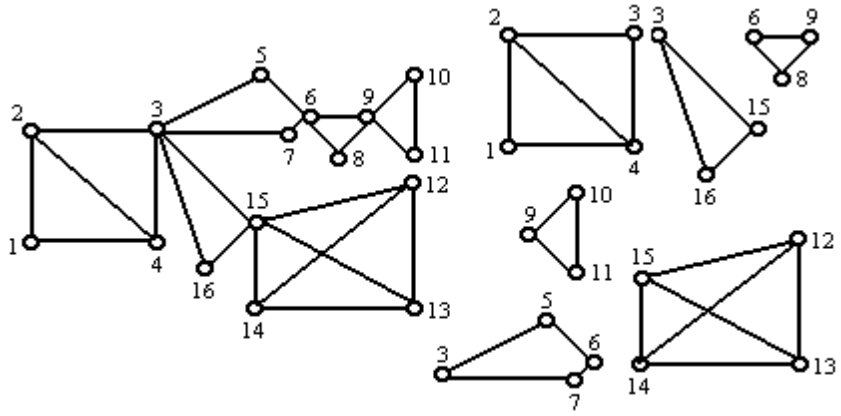
Grafo blokai

Tarkime, kad $G' = (V', B')$ yra tokie grafo $G = (V, B)$ *pografiai*, kad

$$\forall u, v \in V' \subset V : \; \{u, v\} \in B \Rightarrow \{u, v\} \in B'.$$

T. y. grafas G' turi kai kurias grafo G viršūnes ir *visas* jas atitinkančias grafo G briaunas.

Apibrėžimas
Grafo G *maksimalus* neskaidusis pografis G' vadinamas jo ***bloku***. 23-



23: Grafas ir jo blokai

ame paveiksle pavaizduotas grafas turi 6 pografius. Jie visi yra maksimalūs: jei prie bet kurio iš jų pridėti bent vieną viršūnę su atitinkančiomis briaunomis, naujas grafas jau nebus neskaidusis. Pavyzdžiui, blokas

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

negali būti papildytas briauna $\{3,5\}$ arba $\{3,7\}$, kadangi toks grafas nėra neskaidusis. Jei iš šio bloko pašalinti kurią nors briauną, jis nebus maksimalus.

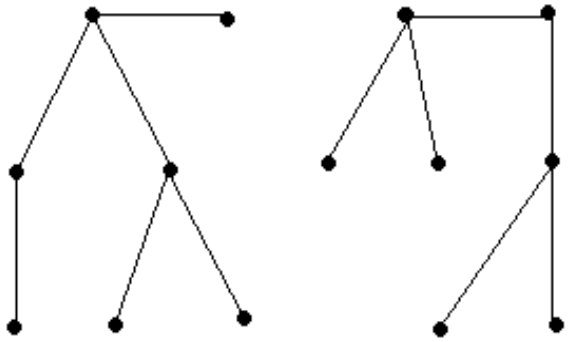
Medžiai ir miškai

Apibrėžimas

Jungusis ir neturintis ciklų (*aciklinis*) grafas vadinamas ***medžiu***.

Grafas yra medis tada ir tik tada, kai bet kurias dvi jo viršūnes galima sujungti *vienintele* grandine.

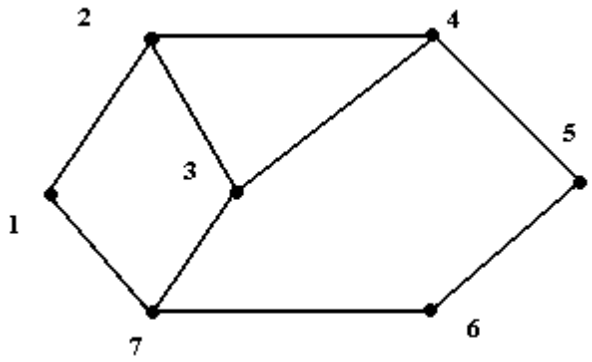
Teorema



24: Dviejų medžių miškas

Bet kuris n-osios eilės medis ($|V| = n$) turi lygiai $n-1$ briauną ($|B| = n-1$).

Apibrėžimas
Aciklinis grafas, turintis k jungiųjų komponenčių, vadinamas k-medžių ***mišku***.



25: Skiriančioji aibė ir kirpis

Teorema
Miškas iš k-medžių turi lygiai $n - k$ briaunų.

Skiriančioji aibė ir kirpis

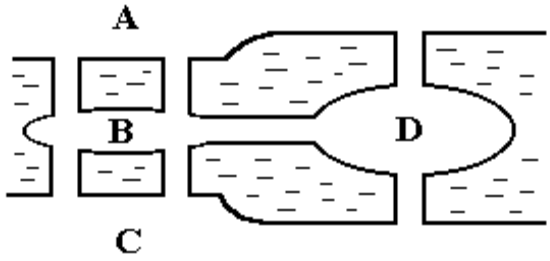
Grafo briauną vadiname ***siejančiaja*** arba *tiltu*, kai pašalinus ją iš grafo, didėja jo jungiųjų komponenčių skaičius.

Apibrėžimas
Jungiojo grafo $G = (V, B)$ briaunų aibės poaibis $S \subset B$ vadinamas ***skiriančiaja aibe***, jei grafas $G' = (V, B \setminus S)$ nėra jungusis.

Minimalioji skiriančioji aibė (iš kurios negalima pašalinti nė vienos briaunos) vadinama ***kirpiu***. Taigi $K \subset B$ yra kirpis, jei K yra skiriančioji aibė, o $\forall P \subset K \ \& \ P \neq K$ – nėra.

Siejančioji briauna yra ne tik skiriančioji aibė, bet ir kirpis. 25-ame paveiksle pavaizduoto grafo briaunų aibės poaibis

$$\{\{2,4\},\{2,3\},\{3,4\},\{3,7\},\{6,7\}\}$$



26: Karaliaučiaus tiltai

yra skiriančioji aibė, bet nėra kirpis. Aibė

$$\{\{2,4\},\{3,4\},\{6,7\}\}$$

yra kirpis. Siejančiųjų briaunų šis grafas neturi.

4.6. Grafo ciklai

Karaliaučiaus tiltų uždavinys

Karaliaučius yra išsidėstęs Priegliaus upės krantuose ir dviejose jos salose (žr. 26 pav.). Krantai ir salos buvo sujungtos septyniais tiltais taip, kaip yra parodyta scheminiame miesto plane. Karaliaučiaus gyventojai mėgdavo pasivaikščioti po tiltus. Ar egzistuoja toks maršrutas, kad išėjus iš namų būtų galima grįžti namo, perėjus per *kiekvieną* tiltą lygiai po *vieną* kartą? Oileris [31] 1736 m. išsprendė šį galvosūkį.

Oilerio grafas

Karaliaučiaus tiltu uždavinį galima pavaizduoti grafu (žr. 28 pav.). Pastebėkime, kad tai iš tikrųjų yra *multigrafas,* tačiau toliau dėstoma teorija

[31] žr. 70 p.

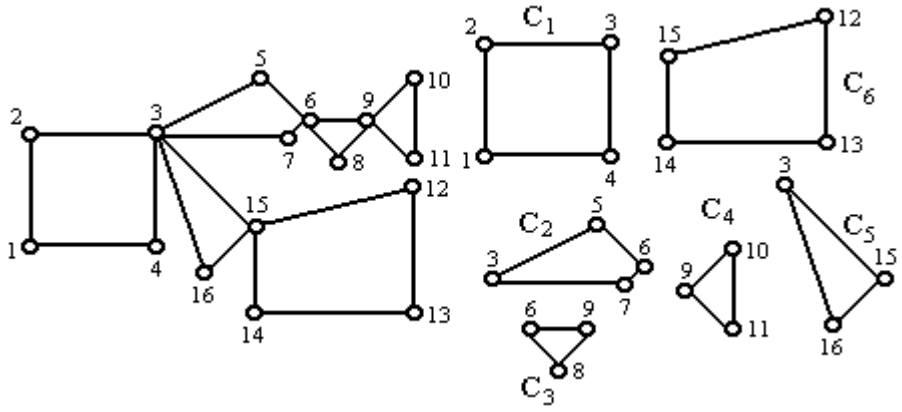
galioja ir jiems. Įrodymui galima paimti ant kurios nors iš pasikartojančių briaunų po vieną papildomą viršūnę (*fiktyviąją* viršūnę) ir turėsime *paprastąjį* grafą.

Apibrėžimas
Grafo ciklas, einantis per *visas* grafo briaunas, yra vadinamas ***Oilerio ciklu***. Grafą, turintį Oilerio ciklą, vadiname *Oilerio grafu*.

Taigi reikia atsakyti į klausimą, ar pavaizduotas 28 pav. (94 psl.) grafas yra Oilerio grafas.

Lema
Jei visų grafo viršūnių laipsniai yra nemažesni už 2, tai egzistuoja ciklas.
Įrodymas. Tarkime v yra bet kuri grafo viršūnė. Kadangi jos laipsnis $p(v) \geqslant 2$, egzistuoja jai gretima viršūnė v_1, kuri irgi turi gretimą v_2. Jei $v_2 = v$ turime ciklą. Jei ne – galime tęsti grandinę tol, kol nesutiksime jau buvusios viršūnės. Tada turėsime ciklą. Kadangi viršūnių skaičius yra $|V| = n$, bus padaryta ne daugiau kaip n žingsnių.

Teorema
Jungusis neorientuotasis grafas turi Oilerio ciklą tada ir tik tada, kai visų grafo viršūnių laipsniai yra lyginiai skaičiai.
Įrodymas. Būtinumas. Grafas turi ciklą, einanti per visas grafo briaunas lygiai po vieną kartą. Nurodykime judėjimo ciklu kryptį ir suskaičiuokime, kiek kartų pereinama per kiekvieną viršūnę. Fiksuojame ciklo pradžią v_0 (tai gali būti bet kuri viršūnė). Į kitą viršūnę v_1 įeiname viena briauna, o išeinama – kita (briaunos negali kartotis). Todėl viršūnės laipsnis $p(v_1) \geqslant 2$. Visų kitų ciklo viršūnių laipsniai irgi tenkina nelygybę $p(v_j) \geqslant 2$. Jei grįžtame į kurią nors jau buvusią viršūnę, tai įeiname į ją trečiąja briauna, o išeiname – ketvirtąja. Taigi $p(v_j) \geqslant 4$. Pereinant per visas ciklo briaunas, gauname, iš visų viršūnių išeita tiek kartų, kiek ir įeita. Kadangi nepereitų briaunų grafas neturi, tai visi laipsniai yra lyginiai.
Pakankamumas. Pagal įrodytą lemą grafas turi ciklą, kurį pažymėkime



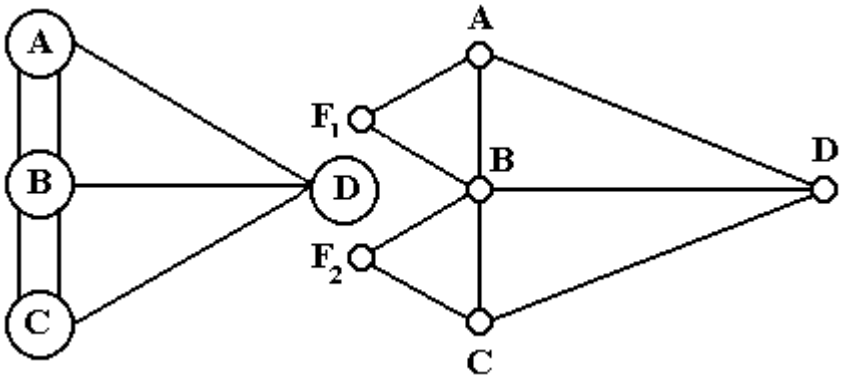
27: Oilerio ciklo egzistavimo įrodymas

C_1 (žr. 27 pav.). Pašaliname iš grafo visas ciklo C_1 briaunas. Jei po to nelieka neizoliuotųjų grafo viršūnių, tai C_1 yra Oilerio ciklas. Tarkime, kad neizoliuotosios viršūnės liko. Tada jų laipsniai yra lyginiai (po briaunų pašalinimo jie galėjo sumažėti 2, 4 ir t. t.). Pašaliname izoliuotasias viršūnes ir vėl konstruojame ciklą C_2. Jei po jo briaunų pašalinimo grafas nebeturi neizoliuotųjų viršūnių, tai $C_1 \cup C_2$ yra Oilerio ciklas. Priešingu atveju procesą galime tęsti ir po baigtinio žingsnių skaičiaus gausime Oilerio ciklą:

$$C = C_1 \cup C_2 \cup \cdots \cup C_k,\ C_i \cap C_j = \emptyset.$$

Suskaičiuokime 28-ojo paveikslo grafo viršūnių laipsnius: $p(A) = 3$, $p(B) = 5$, $p(C) = 3$, $p(D) = 3$. Matome, kad grafas netenkina teoremos reikalavimų ir todėl neturi Oilerio ciklo.

Oilerio keliu vadinama einanti per *visas* grafo briaunas atviroji grandinė. Jei šios grandinės galus sujungti briauna, gausime Oilerio ciklą. Taigi jei dvi grafo viršūnės turi nelyginius laipsnius, o visų kitų laipsniai yra lyginiai, tai grafas turi Oilerio kelią. Iš čia išplaukia, kad

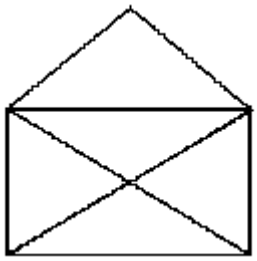


28: Karaliaučiaus tiltų grafas ir grafas su fiktyviosiomis viršūnėmis

voką (29 pav.) galima nupiešti, neatitraukant pieštuko nuo popieriaus bei nepiešiant tų pačių linijų kelis kartus.

Orientuotasis grafas turi Oilerio ciklą tada ir tik tada, kai visos jo viršūnės tenkina sąlygą

$$p^+(v) = p^-(v),\ \forall v \in V.$$



29: Voko galvosūkis

Oilerio ciklo konstravimas

Pateiksime Oilerio ciklo konstravimo algoritmą:
1) imame bet kurią grafo viršūnę $v \in V$;
2) imame gretimą v viršūnę $w \in V$;
jei gretimų viršūnių nėra - procesą baigiame;
3) patikrinama ar briauna $\{v, w\}$
yra siejančioji (tiltas);
4) jei $\{v, w\}$ nėra siejančioji - ji pašalinama;
5) jei $\{v, w\}$ yra siejančioji briauna - ieškome
kitos gretimos viršūnės,
t. y. pereiname prie 2);
6) jei $\{v, w\}$ yra siejančioji briauna
ir kitų gretimų viršūnių nėra -
pašaliname šią briauną ir kartojame
procesą su viršūne w (pereiname prie 2).

Taigi Oilerio ciklą sudarys grandinė iš pašalintų viena po kitos briaunų.

Hamiltono grafas

Apibrėžimas

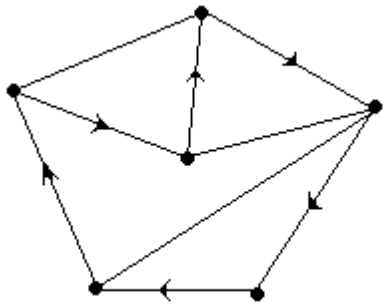
Paprastoji grandinė (ciklas), einanti (-is) per *visas* grafo viršūnes, vadinama (-as) ***Hamiltono***[32] grandine (ciklu).

Grafas, turintis Hamiltono ciklą, yra vadinamas *Hamiltono grafu*.

Pavaizduotame (30 pav.) grafe Hamiltono ciklas nėra Oilerio ciklas, kadangi eina ne per visas grafo briaunas.

Jei briaunų yra pakankamai daug, grafas turi Hamiltono ciklą. Matematiškai tai galima suformuluoti taip: jei $p(v) \geqslant \frac{n}{2}\ \forall v \in V$, tai grafas yra Hamiltono. Iš čia išplaukia, kad pilnasis grafas ($p(v) = n - 1$) turi Hamiltono ciklą. Pastebėkime, kad tai yra pakankama, bet nėra būtina sąlyga: grafas ciklas C_n yra Hamiltono (ir Oilerio) ciklas, nors $p(v) = 2$.

[32] William Rowan Hamilton (1805 – 1865) – airių matematikas ir astronomas.



30: Hamiltono ciklas

Briauninis grafas

Apibrėžimas
Grafo $G = (V, B)$ ***briauniniu*** grafu vadinamas grafas $G_b = (V_b, B_b)$, kurio viršūnių aibė turi tiek elementų, kiek briaunų turi grafas G: $|V_b| = |B|$ ir jo viršūnės yra gretimos, jei buvo gretimos atitinkamos grafo G briaunos:

$$\{v^b, w^b\} \in B_b \Leftrightarrow v^b = \{v_i, v_j\}, w^b = \{w_i, w_j\} \& \\ (v_i = w_i \vee v_i = w_j \vee v_j = w_i \vee v_j = w_j)\,.$$

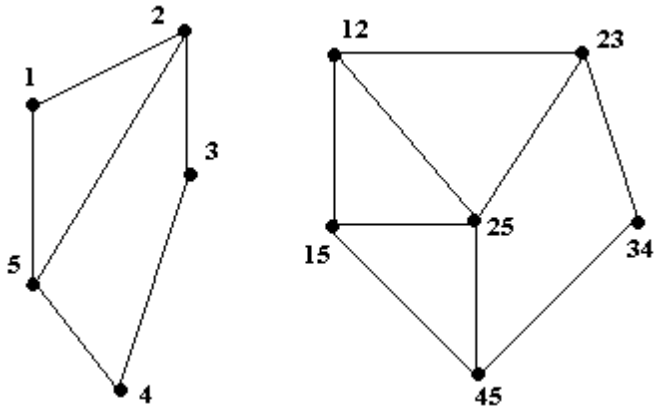
Teorema
Briauninis grafas turi $\frac{1}{2}\sum_{i=1}^{n} p^2(v_i) - m$ briaunų ($m = |B|$).

Pavaizduoto 31 paveiksle grafo viršūnių laipsniai:

$$p(1) = 2, p(2) = 3, p(3) = 2, p(4) = 2, p(5) = 3, m = 6.$$

Taigi

$$\frac{1}{2}\left(2^2 + 3^2 + 2^2 + 2^2 + 3^2\right) - 6 = 9.$$



31: Grafas ir jo briauninis grafas

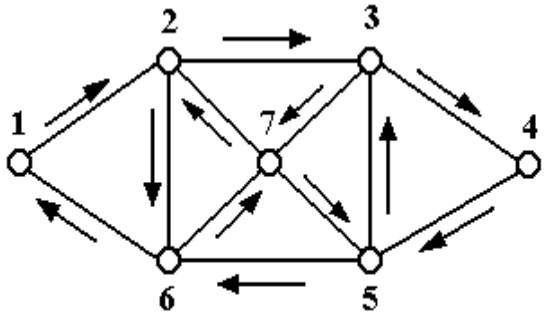
Teorema
Oilerio grafo G briauninis grafas G_b turi ir Oilerio, ir Hamiltono ciklą.

Teorema
Hamiltono grafo briauninis grafas irgi yra Hamiltono grafas.

Grafo nepriklausomi ciklai

Tarkime, kad G yra bet kuris (orientuotasis arba neorientuotasis) grafas (arba multigrafas). Jei jis nėra orientuotasis – suteiksime jo briaunoms orientaciją (bet kurią). Pažymėkime $M = (v_{i_0}, v_{i_1}, \ldots, v_{i_k}, v_{i_0})$ – uždarąjį maršrutą. Uždarojo maršruto M ***vektoriumi ciklu*** $\overrightarrow{M} \in R^m$, $m = |B|$ vadinamas toks vektorius:

$$\overrightarrow{M} = (c_1, c_2, \ldots, c_m),\ c_j = r_j - l_j.$$



32: Nepriklausomi ciklai

Čia r_j yra j-osios briaunos praėjimas teigiama kryptimi skaičius, l_j – šios briaunos praėjimų skaičius neigiama kryptimi.

Visoms 32-ame paveiksle pavaizduoto grafo briaunoms nustatytos kryptys. Raskime uždarojo maršruto $M = (1, 2, 3, 4, 5, 7, 3, 2, 7, 6, 1)$ vektorių ciklą $\overrightarrow{M}$. Sunumeruokime visas grafo briaunas:

$$\{1,2\}-1,\ \{2,3\}-2,\ \{3,4\}-3,\ \{4,5\}-4,$$
$$\{5,6\}-5,\ \{1,6\}-6,\ \{2,6\}-7,\{2,7\}-8,$$
$$\{3,7\}-9,\ \{3,5\}-10,\ \{5,7\}-11,\ \{6,7\}-12$$

ir suskaičiuokime, kiek kartų praeinama kiekviena briauna:

$$\overrightarrow{M} = (1, 1-1, 1, 1, 0, 1, 0, -1, -1, 0, -1, -1) =$$
$$(1, \quad 0, \quad 1, 1, 0, 1, 0, -1, -1, 0, -1, -1).$$

Apibrėžimas
Uždarieji maršrutai M_1, M_2, ..., M_k vadinami ***nepriklausomais***, jei atitinkami vektoriai ciklai $\overrightarrow{M_1}$, $\overrightarrow{M_2}$, ..., $\overrightarrow{M_k}$ yra tiesiškai nepriklausomi.

Pavyzdys

Nustatykime, ar ciklai $m_1 = (1,2,6,1)$, $m_2 = (1,2,7,6,1)$ ir $m_3 = (2,7,6)$ yra nepriklausomi. Surašome vektorius ciklus:

$$\begin{aligned}\overrightarrow{m_1} &= (1,0,0,0,0,1,1,0,0,0,0,0),\\ \overrightarrow{m_2} &= (1,0,0,0,0,1,0,-1,0,0,0,-1),\\ \overrightarrow{m_3} &= (0,0,0,0,0,0,-1,-1,0,0,0,-1).\end{aligned}$$

Sudarome iš šių vektorių koordinačių matricą

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

ir apskaičiuojame jos rangą[33]:

$$A \sim \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & -1 & -1 \\ 0 & 0 & -1 & -1 & -1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1-1 & 0-1 & 0-1 & -1-0 & -1-0 \\ 0 & 0 & -1 & -1 & -1 \end{pmatrix} \sim$$

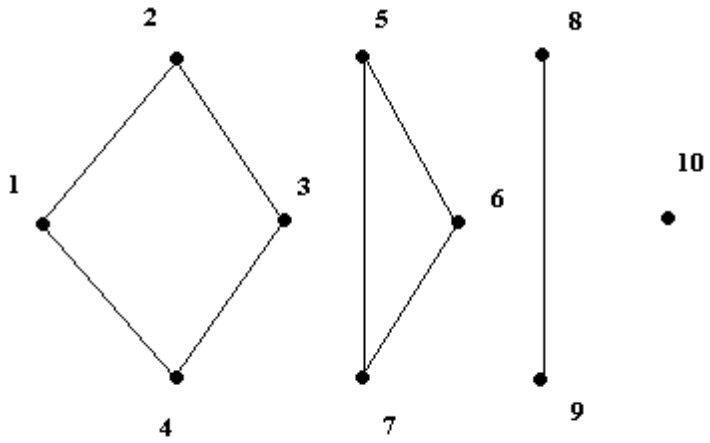
$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & -1 & -1 & -1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

[33] Žr. bet kurį tiesinės algebros vadovėlį.



33: Grafo ciklomatinis skaičius

Gavome $rankA = 2$. Todėl tarp vektorių $\overrightarrow{m_1}$, $\overrightarrow{m_2}$, $\overrightarrow{m_3}$ yra tik du tiesiškai nepriklausomi. Taigi ciklai m_1, m_2 ir m_3 ***nėra*** nepriklausomi.

Grafo ciklomatinis skaičius

Tarkime, kad grafas $G = (V, B)$ turi k jungiųjų komponenčių,
$|V| = n$, $|B| = m$.

Apibrėžimas
Grafo G ***ciklomatiniu skaičiumi*** vadinamas skaičius

$$\nu(G) = m - n + k.$$

Raskime pavaizduoto 33 paveiksle grafo ciklomatinį skaičių:

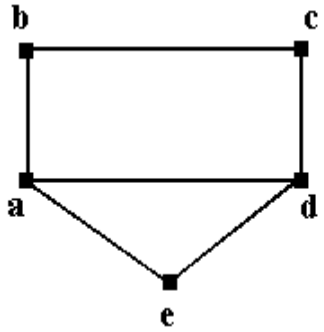
$$k = 4,\ n = 10,\ m = 8,\ \nu(G) = 8 - 10 + 4 = 2.$$

Teorema
Bet kurio grafo ciklomatinis skaičius yra neneigiamas.
Įrodymas. Apskaičiuokime nulinio bei tuščiojo grafų ciklomatinius skaičius: $\nu(\emptyset) = 0 - 0 + 0 = 0$, $\nu(\{v_0\}) = 0 - 1 + 1 = 0$. Parodykime, kad teoremą tenkina bet kuris antrosios eilės grafas. Šiuo atveju gali būti $G_1 = (\{v_1, v_2\}, \emptyset)$ arba $G_2 = (\{v_1, v_2\}, \{\{v_1, v_2\}\})$. Taigi $\nu(G_1) = 0 - 2 + 2 = 0$ ir $\nu(G_2) = 1 - 2 + 1 = 0$. Tarkime, kad teorema yra teisinga bet kuriam n-osios eilės grafui. Prijungiame prie grafo vieną izoliuotą viršūnę ir gauname $(n + 1)$-osios eilės grafą. Jis turės $k + 1$ jungiąją komponentę ir tiek pat (t. y. m) briaunų. Turime $\nu' = m - (n + 1) + (k + 1) = \nu$. Sujungiame šią naują viršūnę su bet kuria kita grafo viršūne. Tada briaunų skaičius bus $m + 1$, o jungiųjų komponenčių skaičius liks arba tas pats, arba sumažės vienetu. Pirmuoju atveju turime $\nu' = m + 1 - n + k = \nu + 1$. Antruoju atveju – $\nu' = m + 1 - n + k - 1 = \nu$. Taigi $(n + 1)$-osios eilės grafas irgi tenkina teoremą, ir pagal matematinę indukciją teorema yra įrodyta.

Teorema
Bet kuris grafas (multigrafas) turi lygiai $\nu(G)$ nepriklausomų ciklų (uždarųjų maršrutų).

Pavyzdys
Pavaizduotas 33 paveiksle grafas turi du nepriklausomus ciklus $(1, 2, 3, 4, 1)$ ir $(5, 6, 7, 5)$.

Pastabos
1. Grafas G neturi ciklų tada ir tik tada, kai $\nu(G) = 0$.
2. Jungusis grafas G yra medis tada ir tik tada, kai $\nu(G) = 0$.
3. Grafas G yra k-miškas tada ir tik tada, kai jis turi k jungiųjų komponenčių ir $\nu(G) = 0$.
4. Grafas G turi vieną ciklą tada ir tik tada, kai $\nu(G) = 1$.



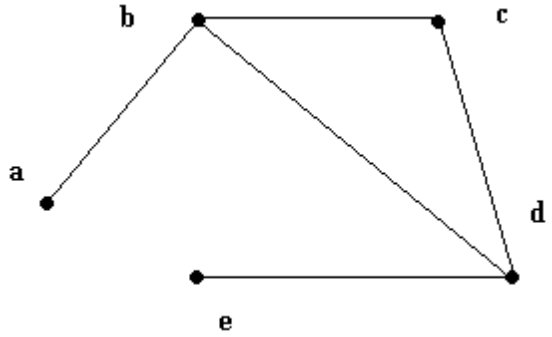
34: Ciklų bazė

Apibrėžimas
$\nu(G)$ nepriklausomų grafo G ciklų rinkinį $\{C_1, C_2, \ldots, C_\nu\}$ vadiname ciklų ***baze***. Ciklai C_j vadinami baziniais.

Teorema
Bet kurį grafo G ciklą $C \subset G$ galima išreikšti baziniais ciklais:

$$C = C_{i_1} \oplus C_{i_2} \oplus \cdots \oplus C_{i_r}.$$

Pavyzdys
Išnagrinėkime 34 pav. grafą. Jo ciklomatinis skaičius $\nu = 6-5+1 = 2$. Ciklai $C_1 = (a, b, c, d, e, a)$ ir $C_2 = (d, e, a, d)$ yra nepriklausomi ir todėl sudaro ciklų bazę. Ciklą $C = (a, b, c, d, a)$ išreiškiame: $C = C_1 \oplus C_2$.



35: Stabilieji iš vidaus poaibiai

4.7. Grafo stabilieji poaibiai

Vidinis stabilumas

Apibrėžimas
Grafo $G = (V, B)$ viršūnių aibės poabis $S \subset V$ vadinamas ***stabiliuoju iš vidaus***[34], jei bet kurios dvi jo viršūnės nėra gretimos grafo viršūnės:

$$\{v, u\} \notin B \; \forall v, u \in S.$$

Pavaizduotas 35 pav. grafas turi stabiliuosius iš vidaus aibės V poaibius $S_1 = \{a, c\}$, $S_2 = \{a, e\}$, $S_3 = \{a, c, e\}$. Akivaizdu, kad bet kuris poabis $\{v_j\} \subset V$ visada yra stabilusis iš vidaus. Poaibiai, turintys dvi viršūnes $\{v_j, v_k\} \subset V$, gali nebūti stabileji iš vidaus. Nagrinėjamas grafas turi vieną stabilųjį iš vidaus poabį, turintį tris viršūnes, ir neturi nė vieno – su keturiomis viršūnėmis.

Bendruoju atveju svarbu rasti stabilųjį iš vidaus poaibį, turintį kuo daugiau viršūnių. Pažymėkime $\mathcal{F}_V$ – visų stabiliųjų iš vidaus poaibių aibę.

[34] Literatūroje tokie poaibiai dar vadinami nepriklausomais.

Apibrėžimas
Grafo ***vidinio stabilumo skaičiumi*** vadiname skaičių

$$\alpha(G) = \max_{S \in \mathcal{F}_V} |S|.$$

Pastebėkime, kad visais atvejais $0 \leqslant \alpha(G) \leqslant n$.

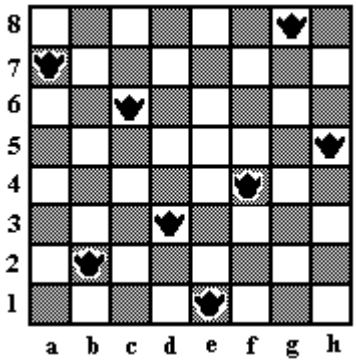
Teorema

$$\alpha(G) \geqslant \sum_{i=1}^{n} \frac{1}{1 + p(v_i)}.$$

Pavaizduotas 35 pav. grafas turi vidinio stabilumo skaičių $\alpha(G) = 3$. Apskaičiuokime teoremos reiškinį šitam grafui:

$$\frac{1}{1+3} + \frac{1}{1+2} + \frac{1}{1+3} + \frac{1}{1+1} + \frac{1}{1+1} = \\ \frac{1}{4} + \frac{1}{3} + \frac{1}{4} + \frac{1}{2} + \frac{1}{2} = \frac{11}{6}.$$

Aštuonių valdovių uždavinys
Reikia išdėstyti šachmatų lentoje kuo daugiau valdovių taip, kad jos nekirstų viena kitos. (Valdovės kerta visus savo horizontalės, vertikalės bei įstrižainių langelius.) Vienas šio galvosūkio sprendinys pateiktas 36 paveiksle. Uždavinio matematinis modelis yra grafas $G = (V, B)$, kurio viršūnes sudaro visi 64 šachmatų lentos langeliai: $V = \{a1, a2, \ldots, h8\}$. Briaunų aibė sudaroma taip, kad dvi viršūnės $v_i, v_j \in V$ yra gretimos, jei esanti langelyje v_i valdovė gali kirsti langelį v_j. Pavyzdžiui, viršūnės $a1$ gretimos viršūnės yra $a2$, $a3$, …, $a8$, $b1$, $c1$, …, $h1$, $b2$, $c3$, …, $h8$. Išspręsti šį uždavinį – reiškia rasti viršūnių aibės V stabilųjį iš vidaus poabį. Vienas toks poaibis pavaizduotas paveiksle $\{a7, b2, c6, d3, e1, f4, g8, h5\}$. Akivaizdu, kad daugiau kaip aštuonias viršūnes toks poaibis turėti negali. Taigi nagrinėjamo grafo vidinio stabilumo skaičius $\alpha(G) = 8$.



36: Aštuonių valdovių uždavinys

Išorinis stabilumas

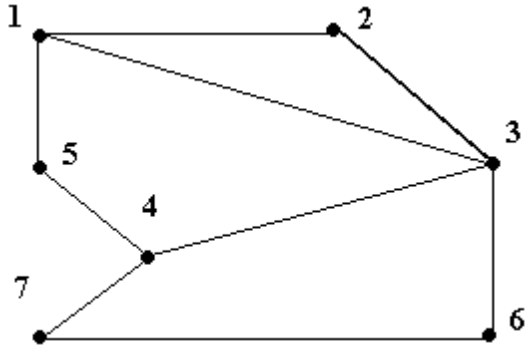
Apibrėžimas
Grafo $G = (V, B)$ viršūnių aibės poabis $S \subset V$ vadinamas ***stabiliuoju iš išorės***[35], jei bet kuri nepriklausanti šiam poaibiui grafo viršūnė u yra gretima kuriai nors poaibio viršūnei $v \in S$:

$$\forall u \in V \setminus S \; \exists v \in S : \{v, u\} \in B.$$

Pavaizduotas 37 pav. grafas turi stabiliuosius iš išorės aibės V poaibius $\{1, 3, 4, 6\}$, $\{1, 4, 6\}$, $\{3, 4\}$. Visų grafo viršūnių aibė V yra stabilioji iš išorės. Todėl reikia rasti stabilųjį jos poaibį, turintį kuo mažiau viršūnių. Nagrinėjame pavyzdyje yra toks poaibis, turintis dvi viršūnes, bet nėra poabių, turinčių vieną viršūnę.

Pažymėkime $\mathcal{F}_I$ – visų stabiliųjų iš išorės poaibių aibę.

[35] Literatūroje tokie poaibiai dar vadinami dominuojančiais.



37: Stabilieji iš išorės poaibiai

Apibrėžimas
Grafo ***išorinio stabilumo skaičiumi*** vadiname

$$\beta(G) = \min_{S \in \mathcal{F}_I} |S|.$$

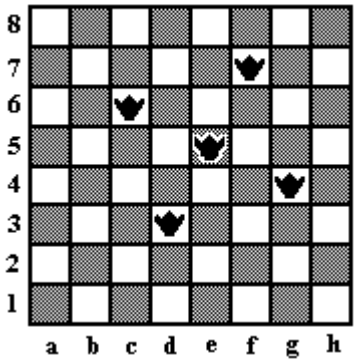
Penkių valdovių uždavinys
Reikia išdėstyti šachmatų lentoje kuo mažiau valdovių taip, kad jos kirstų visus šachmatų lentos langelius. Vienas šio galvosūkio sprendinys pateiktas 38 paveiksle. Matematinis šio uždavinio modelis yra jau išnagrinėtas grafas. Sprendinys $\{c6,\, d3,\, e5,\, f7,\, g4\}$ yra iš išorės stabilusis grafo viršūnių aibės poabis.

4.8. Grafų matricos

Gretimumo matrica

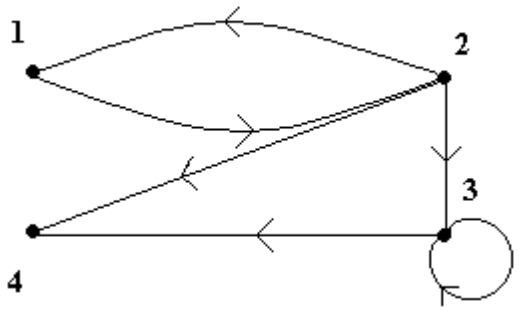
Tarkime, kad $G = (V, L)$ yra orientuotasis grafas. Pažymėkime

$$a_{ij} = \begin{cases} 1 & \exists (v_i, v_j) \in L \\ 0, & \overline{\exists}\,(v_i, v_j) \in L \end{cases}$$



38: Penkių valdovių uždavinys

T. y. a_{ij} yra vienetas, kai grafas turi lanką (v_i, v_j).



39: Šio orientuotojo grafo gretimumo matrica yra 108 psl.

Apibrėžimas
Grafo $G = (V, L)$ ***gretimumo matrica*** vadiname tokią n-osios eilės ($n = |V|$) kvadratinę matricą

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Pavaizduoto 39 pav. grafo gretimumo matrica yra

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Galima pastebėti, kad vienetai eilutėse atitinka išeinančius iš j-osios viršūnės lankus (jos numeris j sutampa su stulpelio numeriu). Vienetas stulpelyje atitinka įeinantį į i-ąją viršūnę lanką. Taigi grafo įėjimo ir

išėjimo puslaipsnius apskaičiuojame taip:

$$p^-(v_i) = \sum_{j=1}^{n} a_{ij}, \;\; p^+(v_j) = \sum_{i=1}^{n} a_{ij}.$$

Visų orientuotojo grafo lankų skaičius $m = |L|$ yra

$$m = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}.$$

Jei grafas turi kilpą $(v_i, v_i) \in L$ turime $a_{ii} = 1$, t. y. atitinkamas matricos įstrižainės elementas lygus vienetui.
Izoliuotąją grafo viršūnę atitinka nulinis gretimumo matricos stulpelis bei nulinė eilutė.
Jei pakeisti orientuotojo grafo lankų orientaciją, gauto grafo gretimumo matrica bus transponuota matrica A: $A^T = ||a_{ji}||_{n\times n}$.

Tarkime, kad $G = (V, B)$ yra paprastasis neorientuotasis grafas. Jei jį apibrėžti *simetriniu antirefleksyviuoju* sąryšiu (žr. 4.1.), gausime, kad jo gretimumo matrica yra simetrinė ir turi nulinę pagrindinę įstrižainę. Kadangi mes susitarėme apibrėžti tokį grafą jo briaunų aibe $B = \{\{v_{i_1}, v_{j_1}\}, \ldots, \{v_{i_m}, v_{j_m}\}\}$, reikia performuluoti gretimumo matricos $A = ||a_{ij}||_{n\times n}$ apibrėžimą:

$$a_{ij} = \begin{cases} 1, & \{v_i, v_j\} \in B, \\ 0, & \{v_i, v_j\} \notin B. \end{cases}$$

Šiuo atveju briaunų skaičius $m = |B|$ lygus

$$m = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}.$$

Teorema
Matricos A^k elementas a'_{ij} yra lygus ilgio k maršrutų iš viršūnės v_i į viršūnę v_j skaičiui.

Pavyzdžiai
1. Raskime 39 pav. pavaizduoto grafo gretimumo matricos kvadratą:

$$A^2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Taigi turime vieną maršrutą ***ilgio*** 2 iš 1 į 1: $(1, 2, 1)$; vieną – iš 1 į 3: $(1, 2, 3)$; vieną – iš 3 į 4: $(3, 3, 4)$. Nėra nė vieno maršruto, prasidedančio viršūnėje 4; nėra ***ilgio*** 2 maršrutų iš 2 į 1 arba iš 3 į 2.
2. Raskime neorientuotojo grafo $G = (\{1, 2, 3\},\ \{\{1, 2\}, \{2, 3\}\})$ gretimumo matricos laipsnius:

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix},\ A^3 = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$

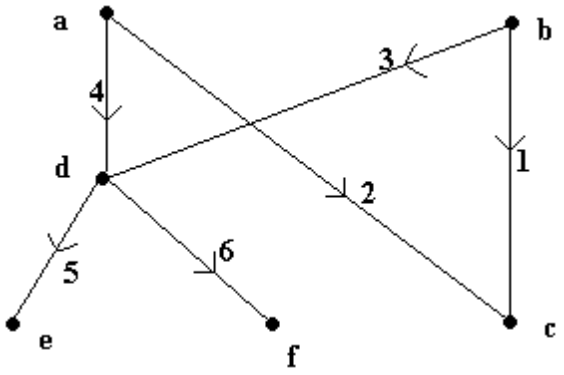
Užrašykime kai kuriuos grafo maršrutus ilgio 2: $(1, 2, 1)$, $(1, 2, 3)$, $(2, 1, 2)$, $(2, 3, 2)$ ir ilgio 3: $(1, 2, 3, 2)$, $(1, 2, 1, 2)$.

Iicidencijų matrica

Sunumeruokime orientuotojo grafo $G = (V, L)$ lankus l_1, l_2, ..., l_m, $m = |L|$.
Apibrėžimas
Grafo G ***incidencijų matrica*** $I = ||e_{ij}||_{n \times m}$ apibrėžiama taip:

$$e_{ij} = \begin{cases} 1, & l_j = (v_i, w) \in L, \\ -1, & l_j = (w, v_i) \in L, \\ 0, & l_j \neq (v_i, w)\ \&\ l_j \neq (w, v_i)\ \forall w \in V. \end{cases}$$

Taigi incidencijų matricos elementai lygūs vienetui atitinka išeinančius lankus, vienetai su minuso ženklu – įeinančius, o nuliai reiškia, kad lankas nėra incidentusis atitinkamai grafo viršūnei.



40: Šio orientuotojo grafo incidencijų matrica yra 111 psl.

Kai $G = (V, B)$ yra neorientuotasis grafas, incidencijų matricoje $I = ||e_{ij}||_{n\times m}$ nerašome neigiamų elementų:

$$e_{ij} = \begin{cases} 1, & l_j = \{v_i, w\} \in B, \\ 0, & l_j \neq \{v_i, w\}\ \forall w \in V. \end{cases}$$

Pavyzdys
Pavaizduoto 40 pav. grafo incidencijų matrica yra

$$I = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Teorema
Tarkime, kad $G = (V, B)$ yra paprastasis neorientuotasis grafas, $|V| = n$, $|B| = m$, G_b – briauninis grafas, I – grafo G incidencijų matrica, A

– grafo G_b gretimumo matrica. Tada

$$A = I^T \cdot I - 2E_n.$$

Čia E_n – vienetinė matrica.

Pavyzdys

Pažymėkime grafo $G = (\{v_1, v_2, v_3\},\ \{\{v_1, v_2\}, \{v_2, v_3\}\})$ briaunas $u_1 = \{v_1, v_2\}$, $u_2 = \{v_2, v_3\}$. Tada grafo G briauninis grafas $G_b = (\{u_1, u_2\},\ \{\{u_1, u_2\}\})$. Jų incidencijų bei gretimumo matricos yra

$$I = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Taigi

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

4.9. Orientuotieji grafai

Pusmaršrutis

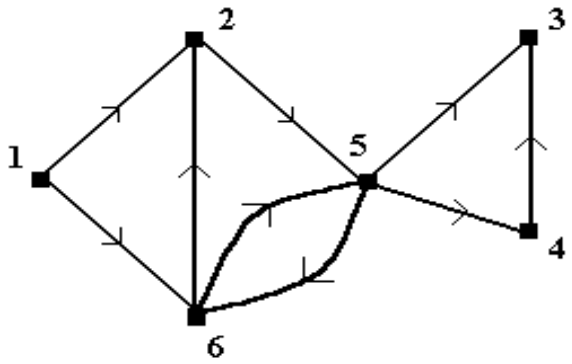
Tarkime, kad $G = (V, L)$ yra orientuotasis grafas ($L \subset V^2$). Žymėsime $M = (u, v_{i_1}, \ldots, v_{i_k}, w)$ jungiantį grafo viršūnes $u, w \in V$ *maršrutą*, jei (u, v_{i_1}), $(v_{i_j}, v_{i_{j+1}})$, $(v_{i_k}, w) \in L$. Pavaizduotas 41 paveiksle grafas turi maršrutus $(1, 2, 5, 3)$, $(1, 6, 5, 4)$, $(2, 5, 4)$, tačiau neturi maršruto $(4, 5, 2)$.

Apibrėžimas

Sakome, kad $M = (u, v_{i_1}, \ldots, v_{i_k}, w)$ yra ***pusmaršrutis***, jungiantis grafo viršūnes $u, w \in V$, jei

$$(u, v_{i_1}) \ \vee (v_{i_1}, u),\ (v_{i_j}, v_{i_{j+1}}) \vee (v_{i_{j+1}}, v_{i_j}),\ (v_{i_k}, w) \vee (w, v_{i_k}) \in L,$$

t. y. bent vienas iš sudarančių grandinę lankų $(v_{j_i}, v_{j_{i+1}})$ arba $(v_{j_{i+1}}, v_{j_i})$ priklauso grafui.



41: Maršrutas ir pusmaršrutis

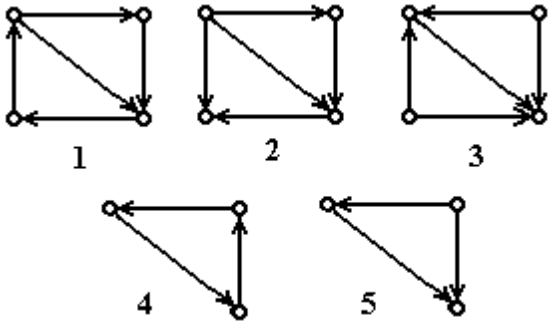
Taigi $(4, 5, 2)$ nėra maršrutas, bet yra pusmaršrutis.

Panašiai orientuotajam grafui apibrėžiama *grandinė, pusgrandinė, kelias, puskelis, ciklas ir pusciklis.*

Apibrėžimas
Grafo viršūnė v yra vadinama ***pasiekiamąja*** iš viršūnės u, jei egzistuoja maršrutas $(u, \ldots, v)$. Susitarkime, kad bet kuri grafo viršūnė yra pasiekiama pati iš saves.

Stiprumas

Apibrėžimas
Sakome, kad orientuotasis grafas $G = (V, L)$ yra ***stiprusis*** (***stipriai jungusis***), jei $\forall u, v \in V\ \exists K_1 = (u, \ldots, v)\ \&\ \exists K_2 = (v, \ldots, u)$, kai K_1 ir K_2 yra keliai. Taigi grafas vadinamas *stipriuoju,* kai bet kurios dvi jo viršūnės yra pasiekiamos viena iš kitos. Kai egzistuoja tik vienas iš kelių K_1 ir K_2, orientuotąjį grafą vadiname ***vienakryptiškai jungiuoju***. Jei bet kurias dvi grafo viršūnes galima sujungti *puskeliu,* grafą vadiname ***silpnuoju*** (***silpnai jungiuoju***).



42: Stiprieji, vienakryptiškai stiprieji ir silpnasis grafai

Taigi bet kuris stiprusis grafas yra ir vienakryptiškai jungusis, o pastarasis grafas – silpnasis. Pavaizduoti 42paveiksle grafai (1), (4) yra stiprieji, (2),(5) – vienakryptiškai stiprieji, grafas (3) yra silpnasis.

Teoremos
Grafas yra stiprusis tada ir tik tada, kai egzistuoja einantis per visas jo viršūnes ciklas.
Grafas yra vienakryptiškai stiprusis tada ir tik tada, kai jis turi einantį per visas viršūnes maršrutą.
Grafas yra silpnasis tada ir tik tada, kai per visas jo viršūnes eina pusmaršrutis.

Branduolys

Apibrėžimas
Grafo $G = (V, L)$ viršūnių aibės poabis $S \subset V$ vadinamas grafo ***branduoliu***, kai aibė S yra stabilioji ir iš vidaus, ir iš išorės.

Pavyzdžiai
1. Grafas $(\{1,2,3\},\ \{(1,2),\ (1,3),\ (2,3)\})$ neturi branduolio.
2. Grafas $(\{1,2,3,4\},\ \{(1,3),(3,4),(4,2),(2,1)\})$ turi du branduolius $B_1 = \{1,4\}$ ir $B_2 = \{2,3\}$.

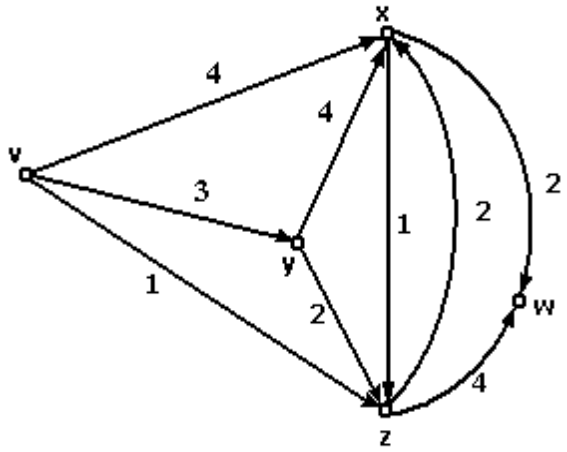
Teorema
Simetrinis grafas be kilpų turi branduolį.

Srautas

Tarkime, kad $G = (V, L)$ yra vienaryptiškai stiprusis grafas, turintis vieną ***šaltinį*** (grafo įėjimas, žr. 4.1.) ir vieną ***sankaupos*** tašką (grafo išėjimas). Jei kiekvienam grafo G lankui $l \in L$ apibrėžta neneigiama funkcija $\psi(l) : L \to R_+$, sakome kad apibrėžtas ***tinklas*** $T = (G, \psi)$. Funkciją $\psi(l)$ vadiname tinklo T ***pralaidumu***.
Apibrėžimas
Funkciją $\varphi(l) : L \to R_+$ vadiname ***srautu per tinklą*** $T = (G, \psi)$, jei ji tenkina sąlygas:
1) $\varphi(l) \leqslant \psi(l)\ \forall l \in L$;
2) $\sum\limits_{i:l_i=(v,v_i)} \varphi(l_i) = \sum\limits_{j:l_j=(v_j,v)} \varphi(l_j)\ \forall v \in V$.

Taigi srautas negali būti didesnis už tinklo pralaidumą, ir išeinantis iš kiekvienos grafo viršūnės srautas lygus įeinančiam. Trivialus srauto funkcijos $\varphi(l)$ pavyzdys yra nulinis srautas. Raskime maksimalų srautą, kurį gali praleisti pavaizduotas 43 pav. tinklas.

Priminsime, kad grafo *kirpiu* vadiname minimalią (iš kurios negalima pašalinti nė vieno elemento, žr.4.5.) lankų aibę, kad pašalinus šiuos lankus, kurių nors dviejų grafo viršūnių negalima sujungti maršrutu. Išvardinkime visus 43 pav. pavaizduoto tinklo kirpius:
$K_1 = \{(v,x),(v,y),(v,z)\}$, $K_2 = \{(x,w),(z,w)\}$,
$K_3 = \{(v,x),(y,x),(z,x),(z,w)\}$, $K_4 = \{(v,z),(y,z),(x,z),(x,w)\}$.



43: Tinklas

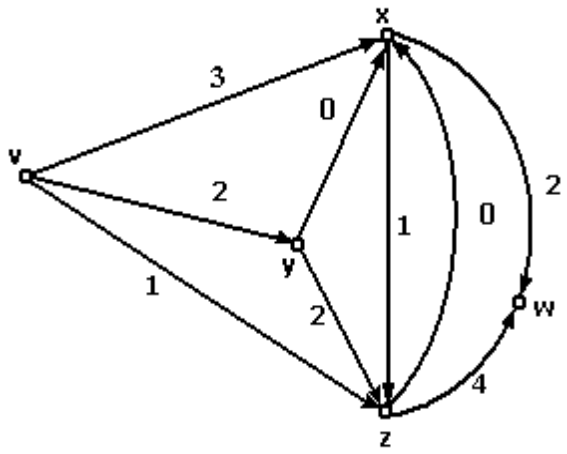
Apskaičiuokime kiekvieno iš šių kirpių pralaidumą:

$$P(K_j) = \sum_{l:\, l \in K_j} \psi(l).$$

Turime $P(K_1) = 4 + 3 + 1 = 8$, $P(K_2) = 2 + 4 = 6$,
$P(K_3) = 4 + 4 + 1 + 4 = 13$, $P(K_4) = 1 + 2 + 1 + 2 = 6$.

Teorema
Maksimalus srauto per tinklą pralaidumas lygus minimaliam tinklo kirpio pralaidumui.

Taigi joks srautas per pavaizduotą 43-ame paveiksle tinklą negali turėti didesnio pralaidumo, negu pavaizduotas 44-ame paveiksle srautas.



44: Srautas per tinklą

5. Kombinatoriniai algoritmai

5.1. Algoritmo sąvoka

Algoritmų pavyzdžiai

Žodis *algoritmas* kyla nuo matematiko pavardės[36] ir pradžioje Europoje reiškė aritmetinių veiksmų taisykles dešimtainėje sistemoje. Vėliau šis žodis įgyjo platesnę prasmę ir pradėjo reikšti tam tikrų veiksmų rinkinį. Kurį laiką šį žodį vartojo tik matematikai, kaip įvairių uždavinių sprendimo taisykles, pavyzdžiui, kvadratinės lygties sprendimo žingsnius arba kampo dalijimo pusiau skriestuvu ir liniuote procedūrą. Dabar *algoritmu* galima pavadinti ir maisto gaminimo aprašymą kulinarinėje knygoje, naudojimosi telefonu automatu instrukciją, tekstinio pranešimo mobiliuoju telefonu siuntimą ir pan.

Euklido algoritmas

Kaip matematinio uždavinio sprendimo proceso aprašymo pavyzdį panagrinėkime Euklido[37] algoritmą: rasti dviejų natūraliųjų skaičių x ir y didžiausiąjį bendrąjį daliklį z. Pavaizduokime veiksmų atlikimo schemą (45 pav.).

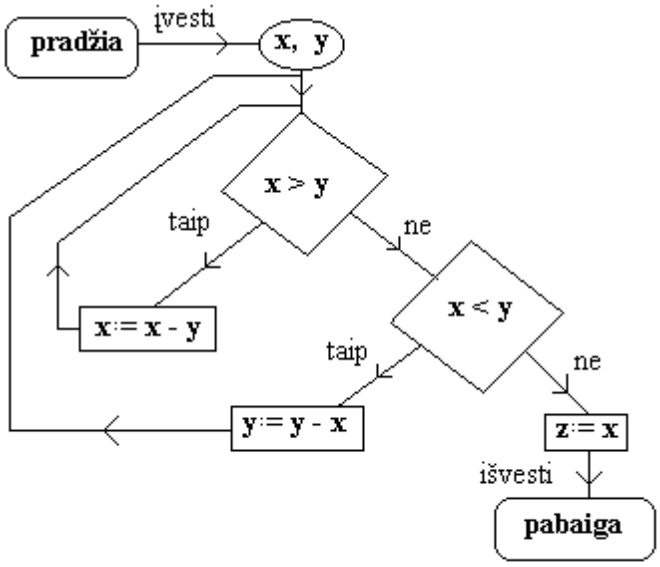
Pavyzdys

Raskime skaičių $x = 9$ ir $y = 12$ didžiausiąjį bendrąjį daliklį z, taikydami Euklido algoritmą. Surašome algoritmo veiksmus:

1) $x := 9,\ y := 12;$
2) $x < y \Rightarrow y := y - x;$
3) $y := 12 - 9 = 3,\ x := 9;$
4) $x > y \Rightarrow x := x - y;$
5) $x := 9 - 3 = 6,\ y := 3;$
6) $x > y \Rightarrow x := x - y;$

[36] al-Chorezmi (Algorithmi) (787 – apie 850) – Vidurinės Azijos matematikas ir astronomas.

[37] $Ευκλειδης$ (apie 3a. p. m. e.) – senovės Graikijos matematikas.



45: Euklido algoritmas

7) $x := 6 - 3 = 3$, $y := 3$;
8) $x = y \Rightarrow z := x$.
Taigi gauname $z = 3$ – didžiausiąjį skaičių 9 ir 12 daliklį.

Analizuojant įvairius algoritmus, galima išskirti bendruosius jų parametrus:
1) pradiniai duomenys (45 pav. atveju du natūralieji skaičiai);
2) galimi galutiniai rezultatai (mūsų pavyzdžio atveju visada surandamas natūralusis skaičius, tačiau yra uždavinių, kurie negali būti išspręsti ir reikia numatyti ką laikyti rezultatu);
3) galimi tarpiniai rezultatai;
4) pradžios taisyklė;
5) pabaigos taisyklė (mūsų atveju algoritmas baigia darbą, kai $x = y$);
6) atliekamos operacijos (čia palyginimas, atimtis ir priskyrimas (:=));
7) rezultato gavimas (čia $z := x$).

Tiuringo mašina

Minėtų parametrų ir taisyklių formalizavimas buvo atliktas 1936 m. kaip ***abstrakčiosios*** *skaičiavimo* Tiuringo[38] *mašinos* aprašymas. Ši mašina turi neribotą atmintį – begalinę padalintą sekcijomis juostą. Visos šios juostos sekcijos yra sunumeruotos; į kiekvieną sekciją galima rašyti ir iš jos galima skaityti po vieną duotosios baigtinės abėcėlės raidę. Skaitymą bei rašymą atlieka Tiuringo mašinos galvutė, kurios veiksmus sudaro baigtinė būvių aibė. Algoritmas apibrėžiamas kaip programa, kurią sudaro judančios išilgai juostos galvutės veiksmai (rašyti arba skaityti esamoje sekcijoje, pereiti juostos atžvilgiu kairėn, dešinėn arba likti toje pačioje pozicijoje, baigti darbą).

Išspendžiamumas

Svarbus algoritmų teorijos klausimas yra uždavinių ***išsprendžiamumo*** (***apskaičiuojamumo***) nustatymas: įrodyti, kad egzistuoja arba neegzistuoja algoritmas, sprendžiantis tam tikrą uždavinį per *baigtinį* žingsnių

[38] Alan Mathison Turing (1912 – 1954) – anglų matematikas.

skaičių. Pavyzdžiui, kampo trisekcijos (kampo dalijimas į tris lygias dalis) arba skritulio kvadratūros (sudaryti kvadratą, kurio plotas lygus duotojo skritulio plotui) uždaviniai nėra išsprendžiami, kai leistini tik veiksmai su skriestuvu ir liniuote. Kitas neišprendžiamo uždavinio pavyzdys yra dešimtoji Hilberto[39] problema: sudaryti algoritmą, per baigtinį žingsnių skaičių nustatantį ar polinomas $P_n(x_1, x_2, \ldots, x_m)$ su sveikaisiais koeficientais turi bent vieną sveikąją šaknį $x^0 = (x_1^0, x_2^0, \ldots, x_m^0)$: $P(x^0) = 0$. Įrodyta (Matijasevič[40], 1970), kad toks algoritmas neegzistuoja.

Perrinkimas
Kombinatoriniai algoritmai skirti baigtinių matematinių struktūrų uždaviniams spręsti. Kadangi tokius uždavinius galima spręsti visų galimų elementų kombinacijų *perrinkimu*, kombinatorinių uždavinių *išsprendžiamumas* yra akivaizdus. Kai perrenkamų variantų nėra daug, toks sprendimo metodas yra natūralus ir kitų uždavinio sprendimo būdų galima neieškoti. Esant dideliam perrenkamų kombinacijų skaičiui tiesioginis jų perrinkimas yra *praktiškai neįmanomas* ir svarbu rasti *efektyvų* uždavinio sprendimo algoritmą.

5.2. Algoritminio uždavinio matmuo

Uždavinių aibė

Kalbant apie tam tikro uždavinio sprendimo algoritmą, turima omenyje ne vienas konkretus uždavinys, o tam tikras panašių uždavinių rinkinys, klasė, aibė. Pavyzdžiui, Euklido algoritmas (žr. 5.1.) taikytinas bet kuriems natūraliesiems skaičiams x ir y. Taigi uždavinių klasę sudaro aibė $N^2 = \{(x, y) : x, y \in N\}$. Euklido algoritmas per baigtinį žingsnių skaičių $k(x, y)$ suras x ir y didžiausiąjį bendrąjį daliklį $z(x, y)$. Taigi algoritmo tyrimas reikalauja gana sudėtingų funkcijų $k(x, y)$ ir $z(x, y)$ nagrinėjimo. Tačiau, nagrinėdami *visas* poras (x, y) galime įvesti

[39] David Hilbert (1862 – 1943) – vokiečių matematikas.
[40] Jurii Vladimirovič Matijasevič (gim. 1947) – tarybinis matematikas.

uždavinių klasės ***matmens*** (***dydžio***) sąvoką. Tai gali būti, pavyzdžiui, $\max\{x, y\}$, $x + y$ arba $\sqrt{x^2 + y^2}$. Kuo didesnis yra šis dydis, tuo daugiau žingsnių turi atlikti algoritmas, spręsdamas *visus* tokio arba mažesnio dydžio uždavinius.

Išnagrinėkime dar vieną pavyzdį. Turime dvi aibes A ir B. Reikia patikrinti ar $A \cap B = \emptyset$? Užrašykime algoritmą kaip kompiuterinę programą (pseudokodą):

```
begin
x[] := A,  n := |A|
i := 1  while (x[i] ∉ B)  if  (i ⩽ n)  i := i + 1
if (i ⩽ n) then "nėra"
else "yra"
end
```

Pastebėkime, kad čia neapibrėžtas patikrinimo $(x[i] \notin B)$ algoritmas ir žingsnių skaičius nagrinėjamam uždaviniui išspręsti formaliai priklauso tik nuo $n = |A|$. Norėdami turėti bendrą *visoms* aibėms A ir B rezultatą, apibūdiname uždavinių klasę ***matmeniu*** n.

Grafų modeliai

Išnagrinėkime grafo $G = (V, B)$ pateikimo kompiuterio atmintyje būdus, arba, kitais žodžiais, jo *informacinius modelius*.

Visą informaciją apie grafą galima gauti iš jo *gretimumo* matricos (žr. 4.8.) $A = ||a_{ij}||_{n\times n}$, $(n = |V|)$:

$$a_{ij} = \begin{cases} 1, & \{v_i, v_j\} \in B, \\ 0, & \{v_i, v_j\} \notin B. \end{cases}$$

Kai G yra paprastasis neorientuotasis grafas, matrica A yra simetrinė ir turi nulinę pagrindinę įstrižainę. Todėl visą informaciją apie grafą suteikia $m = n^2 - \frac{n(n-1)}{2} - n$ matricos elementų. Pastebėkime dar, kad šių elementų reikšmės yra 0 ir 1. Taigi paprastąjį neorientutąjį grafą galima *koduoti* m bitais.

Tarkime, kad $G = (V, L)$ yra orientuotasis nebūtinai paprastasis (gali turėti kilpų) grafas. Tada jo gretimumo matricos elementai yra 0, 1, (-1) ir matrica bendru atveju nėra simetrinė. Kiekvienam tokio grafo lankui galima priskirti teigiamą skaičių ir nagrinėti *svertinį* grafą, pavyzdžiui, *tinklą* (žr. 4.9.). Taigi visą informaciją apie tinklą užrašome n^2 skaičiais.

Grafo $G = (V, B)$ *incidencijų matrica* turi $n \times m = |V| \times |B|$ elementų (žr. 4.8.). Kai grafo briaunų (lankų) skaičius m yra nedidelis, uždavinio *matmuo* $n \cdot m << n^2$. Kai turime artimą pilnajam grafui, $m \cdot n = O(n^3)$ ir grafo modeliavimas gretimumo matrica yra ekonomiškesnis. Dar pastebėkime, kad reikalinga papildoma informacija apie briaunų (lankų) numeraciją.

Pats ekonomiškiausias grafo modelis yra briaunų sąrašas. Sudarome du viršūnių masyvus:
$V_1 = \{v_{11}, v_{12}, \ldots, v_{1m}\}$, $V_2 = \{v_{21}, v_{22}, \ldots, v_{2m}\}$. Čia $\{v_{1j}, v_{2j}\} \in B$. Uždavinio *matmuo* šiuo atveju yra $2m$, tačiau ieškant incidentinių duotajai viršūnei briaunų, reikia peržiūrėti abu masyvus V_1 ir V_2.

Taigi grafo pateikimo kompiuterio atmintyje būdas turi būti pasirinktas atsižvelgiant į sprendžiamą uždavinį. Tarkime, reikia rasti $\max\limits_{i=1,2,\ldots,n} p(v_i)$. Šiam uždaviniui spręsti pasirinksime grafo užrašymą jo gretimumo matrica $A = ||a_{ij}||_{n\times n}$. Pažymėję $m_i = \sum\limits_{j=1}^{n} a_{ij}$, turime algoritmą:

```
begin
i := 1  m0 := 0  n := |A|
while (i ⩽ n) { if (m0 < mi)  m0 = mi
if (i < tn)  i := i + 1 }
end
```

5.3. Algoritmo sudėtingumas

Sudėtingumo sąvoka

Panagrinėkime apibrėžtų algoritmų atliekamų operacijų skaičius. Pradėkime nuo Euklido algoritmo (žr. 5.1.) ir įvertinkime žingsnių skaičių $k(x, y)$. Mums reikia ištirti *visus* galimus atvejus x ir y, kai $x \to \infty$ ir $y \to \infty$, arba kai uždavinio *matmuo* $n = \max\{x, y\} \to \infty$. Jei vienas iš skaičių x ir y lygus 1, Euklido algoritmas turės atlikti operaciją $x := x - 1$ arba $y := y - 1$ bei palyginimo operacijas $x < y$ arba $y < x$ daug kartų ir jo veikimo *laikas* bus daug didesnis, negu, pavyzdžiui, kai $x = y$ ir $z = x$. (Šiuo atveju z bus rastas po kelių palyginimų.) Susitarkime, kad nagrinėjant algoritmo efektyvumą turi būti įvertinimas jo veikimo laikas ***blogiausiu*** atveju[41]. Kadangi realaus uždavinio sprendimo *laikas* priklauso ne tik nuo algoritmo, bet ir nuo kompiuterinės programos bei konkretaus kompiuterio ypatumų, jis netinka teoriniams algoritmų tyrimamas. Todėl algoritmo veikimo *laikas* suprantamas kaip *abstrakčiosios*, pavyzdžiui, Tiuringo (žr. 5.1.) skaičiavimo mašinos žingsnių, reikalingų uždaviniui išspręsti blogiausiu atveju, t. y. maksimalus skaičius $S(n)$. Taigi funkcija $S(n)$ ir vadinama *algoritmo* ***sudėtingumu***.

Rasti tikslų šios funkcijos pavidalą pavyksta tik atskirais atvejais ir neturi didelės vertės dėl jos "jautrumo" neesminiams algoritmo keitimams. Tarkime, papildžius Euklido algoritmą palyginimu

$$\texttt{if } (x = 1 \ \vee \ y = 1 \ ) \ z = 1,$$

galime gerokai sumažinti žingsnių skaičių. Be to nėra esminio skirtumo ar algoritmas atliks $n + 1$ ar $n - 2$ operacijas, kai n – uždavinio matmuo – yra didelis skaičius. Nėra esminio skirtumo ar $S(n) = 10n^3$, ar $S(n) = 9n^3$, kadangi technologijų vystymasis, programinės įrangos tobulinimas ir panašūs veiksniai turi daug didesnę įtaką praktiniam algoritmo taikymui. Pastebėkime dar, kad ir funkcijos $S(n)$ argumentas

[41] Praktikoje gali būti svarbus *vidutinis* atvejis, kurio teorinis tyrinėjimas reikalauja įvairių galimybių tikimybių pasiskirstymo žinojimo ir yra gana sudėtingas.

n gali būti apibrėžtas įvairiai (žr. 5.2.) ir nevisada yra tiksliai išmatuojamas dydis. Išdėstyti samprotavimai paaiškina kodėl algoritmų teorija paprastai apsiriboja funkcijos $S(n)$ *įverčiais*. Pavyzdžiui, Euklido algoritmo sudėtingumą galime įvertinti $S(n) = O(n)$, kai $n \to \infty$. Priminsime žymėjimo $O(S(n)) = O(f(n))$ prasmę: $\exists C : \ S(n) \leqslant C\, f(n)$.

Kitas mūsų nagrinėtas algoritmas maksimaliam grafo viršūnės laipsniui skaičiuoti (žr. 5.2.) atlieka veiksmus su grafo gretimumo matrica. Jo veikimo laikas yra *determinuotas* ir nagrinėti *blogiausio* atvejo čia nereikia. Nors reikalingų operacijų skaičius $S(n)$ šiuo atveju gali būti nustatytas tiksliai, tai neturi didelės prasmės dėl jau minėto funkcijos $S(n)$ jautrumo neesminiams algoritmo keitimams. Todėl ir šiuo atveju apsiribojame įverčiu $S(n) = O(n^2)$.

Polinominis sudėtingumas

Kai funkcija $S(n) = O(n^\alpha)$ $(\alpha > 0)$, sakome kad turime ***polinominio*** *sudėtingumo* algoritmą. Ši savybė yra patogi sudėtingų algoritmų analizei, kai vienas algoritmas taiko kitą (žr. 5.2. dėstomą algoritmą dviejų aibių susikirtimui nustatyti). Jei abudu algoritmai yra polinominio sudėtingumo, jų *superpozicija* irgi bus polinominis algoritmas.

Algoritmas, sprendžiantis uždavinį per laiką $S(n) > n^\alpha \ \forall \alpha > 0$, vadinamas ***eksponentiniu***. Tokie yra, pavyzdžiui, algoritmai su sudėtingumais $O(2^n)$, $O(n!)$ arba $O(n^n)$.

Polinominis algoritmas yra greitesnis už eksponentinį, kai uždavinio matmuo n yra pakankamai didelis. Lentelėje palyginamas polinominio algoritmo algoritmo su sudėtingumu n^{10} augimo greitis su eksponentinio algoritmo n^n augimu.

n	n^{10}	n^n
5	$9.77 \cdot 10^6$	3125
10	10^{10}	10^{10}
15	$5.77 \cdot 10^{11}$	$4.38 \cdot 10^{17}$
20	$1.02 \cdot 10^{13}$	$1.05 \cdot 10^{26}$
25	$9.54 \cdot 10^{13}$	$8.88 \cdot 10^{34}$

Pastebėkime, kad galimas atvejis, kai polinominis algoritmas negali būti pritaikytas dėl labai didelio laiko (pvz., $n^{100}, n = 15$), o eksponentinis algoritmas $2^n = 32768$ taikytinas. Patirtis, tačiau, rodo, kad jei uždaviniui spręsti egzistuoja sudėtingumo $O(n^\alpha)$ polinominis algoritmas, jį, paprastai, pavyksta patobulinti ir sumažinti laipsnį iki $\alpha = 3$ arba $\alpha = 4$.

5.4. Sunkieji uždaviniai

NP uždavinių klasė

Uždaviniai, kuriems spręsti ***neegzistuoja*** *polinominis* algoritmas, yra vadinami ***sunkiaisiais***. Aišku, kad kai kurių uždavinių *iš principo* negalima išspręsti per *polinominį laiką*. Pavyzdžiui, sugeneruoti *visus* $2^{|A|}$ aibės A poaibius. Todėl toliau bus kalbama tik apie *atpažinimo* uždavinius: algoritmas $\mathbb{A}lg$ tikrina, ar tam tikras objektas U turi kokią nors savybę

$$\mathbb{A}lg(U) \rightarrow \begin{pmatrix} taip \\ ne \end{pmatrix}.$$

Paminėkime keletą tokių uždavinių.

Sudėtiniai skaičiai. Patikrinti ar natūralusis skačius a yra kurių nors sveikųjų skaičių $x > 1$, $y > 1$ sandauga: $a = x \cdot y$.

Hamiltono ciklas. Patikrinti, ar duotasis grafas turi Hamiltono ciklą.

Aibės skaidymas. Patikrinti, ar duotąją *svertinę*[42] baigtinę aibę galima

[42]Kiekvienam aibės elementui $a \in A$ priskirtas neneigiamas *svoris* $s(a)$. Poaibio $B \subset A$ svoris $s(B) = \sum_{a \in B} s(a)$.

suskaidyti į du vienodo svorio *blokus*.

Šiuos uždavinius galima spręsti pilnu visų variantų *perrinkimu*, t. y. *eksponentiniais* algoritmais. Tačiau priskirti juos prie *sunkiųjų* uždavinių negalima, kadangi ***nėra žinoma*** ar jiems spręsti *egzistuoja* polinominiai algoritmai. Todėl tokiems uždaviniams tirti algoritmų teorija apibrėžia dar vieną klasę – ***NP***[43] ***uždavinius***. Griežtas šios klasės apibrėžimas yra sudėtingas ir galimas *Turingo mašinos* papildymu "spėliojimų" bloku. Mes apsiribosime neformaliu NP klasės sąvokos paaiškinimu.

Tarkime, kad uždavinio sprendimą galima suskaidyti į dvi *stadijas*: *spėjimo* ir *tikrinimo*. Spėjimo rezultatas yra tam tikra *struktūra*, kuri antroje stadijoje *patikrinama* per *polinominį* laiką. Jei patikrinimo rezultatas yra "$taip$", algoritmas baigia darbą. Priešingu atveju grįžtama prie *spėjimo* stadijos. Pavyzdžiui, siūlomi įvairūs grafo ciklai patikrinti, ar jie praeina lygiai po vieną kartą per kiekvieną grafo viršūnę. Atsakymo "$taip$" atveju gauname Hamiltono grafą ir nutraukiame algoritmo darbą. Priešingu atveju tikriname kitą grafo ciklą.

Iš NP uždavinių klasės apibrėžimo išplaukia, kad *polinominių* uždavinių klasė P (t. y. tokių uždavinių, kuriems spręsti *egzistuoja* polinominiai algoritmai) tenkina sąlygą $P \subset NP$. Tačiau ***nėra įrodyta***, kad $P \neq NP$ ir šis klausimas yra ***neišspręsta*** algoritmų teorijos problema.

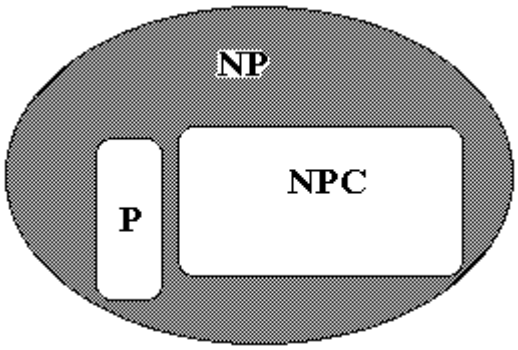
NP klasės tyrimas

NP uždavinių teorijos pamatą sudaro ***hipotezė***, kad

$$NP \setminus P \neq \emptyset$$

(t. y. $P \neq NP$). Svarbus šios teorijos rezultatas yra įrodymas, kad keli šimtai gerai žinomų NP klasės uždavinių gali būti *transformuoti* vienas į kitą per polinominį laiką. Ši uždavinių savybė vadinama jų *transformuojamumu* ir leidžia išskirti dar vieną *NP pilnųjų* (žymime NPC) uždavinių klasę. Ją sudaro *visi* NP klasės uždaviniai, transformuojami į kurį nors vieną *laisvai* pasirinktą NPC klasės uždavinį. Yra ***įrody-***

[43] Nondeterministically Polynomial.



46: Sunkieji uždaviniai

ta, kad jei $P \neq NP$, tai ir $NPC \neq NP$. Taigi šiuo metu vyrauja pavaizduotas 46 paveiksle sunkiųjų uždavinių klasifikavimas. Dar viena neišspręsta NP uždavinių teorijos problema yra uždavinių papildinių tyrimas. Uždavinio U papildinys U^c yra uždavinys su priešingu atsakymu. Pavyzdžiui, uždavinį "**sudėtiniai skaičiai**" (žr. 126 p.) galima pakeisti tokiu uždaviniu.
"**Pirminiai skaičiai**": patikrinti ar duotasis natūralusis skaičius yra pirminis.
Abu šie uždaviniai priklauso klasei NP, tačiau nėra žinoma ar jie priklauso klasei NPC. Bendru atveju nėra įrodyta, kad $U \in NP \Rightarrow U^c \in NP$. Todėl apibrėžiama dar viena uždavinių klasė co-$NP = \{U^c : U \in NP\}$. Yra žinoma, kad jei egzistuoja bent vienas toks uždavinys $U \in NPC$ & $U^c \in NP$, tai $NP =$co-NP. Kadangi abudu (pirminių ir sudėtinių skaičių) uždaviniai yra NP klasės, jei jie būtų ir iš NPC klasės, mes gautume, kad co-$NP = NP$, tačiau, tikriausiai, taip nėra. Todėl, vyrauja hipotezė, kad šie uždaviniai priklauso klasei $NP \setminus NPC$.

NPC klasės uždaviniai

Yra žinomi keli šimtai šios klasės uždavinių, jų tarpe jau minėtas uždavinys **Hamiltono ciklo** uždavinys. Paminėsime dar kelis NPC klasės uždavinius.

Dominuojančioji aibė. (žr. 4.7.) Duotas grafas $G = (V, B)$ ir natūralusis skaičius k. Patikrinti, ar egzistuoja tokia stabilioji iš išorės aibė $V' \subset V$, kad $|V'| \leqslant k$.

Nepriklausomoji aibė. (žr. 4.7.) Duotas grafas $G = (V, B)$ ir natūralusis skaičius k. Patikrinti, ar egzistuoja tokia stabilioji iš vidaus aibė $V' \subset V$, kad $|V'| \geqslant k$.

Klika. Duotas grafas $G = (V, B)$ ir natūralusis skaičius k. Patikrinti, ar jis turi ne mažesnės kaip k-osios eilės pilnąjį pografį (*kliką*).

Sutraukimas. (žr. 4.4.) Duoti du grafai $G_1 = (V_1, B_1)$ ir $G_2 = (V_2, B_2)$. Patikrinti, ar galima taikant grafui G_1 viršūnių sutapatinimo operaciją gauti grafą, izomorfinį grafui G_2.

Branduolys. (žr. 4.9.) Patikrinti, ar orientuotasis grafas turi branduolį.

Kvadratiniai lyginiai. Duoti natūralieji skaičiai x, y ir z. Patikrinti, ar egzistuoja toks natūralusis skaičius $w < x$, kad $w^2 \equiv y \pmod{z}$.

Įvykdymas. Patikrinti ar yra įvykdoma bulinė funkcija.

6. Informacijos kodavimas

6.1. Bendrosios sąvokos

Informacijos šaltinis

Mes nagrinėjame pranešimų šaltinio matematinį modelį. Tarkime, kad šaltinis generuoja simbolius $a_j \in A = \{a_1, a_2, \ldots, a_n\}$. Aibė A yra vadinama informacijos šaltinio ***abėcėle***, jos elementai a_j – ***raidėmis***. Baigtinė raidžių seka $a = a_{i_1} a_{i_2} \cdots a_{i_m}$ vadinama ***žodžiu***. Žodžio a ***ilgį*** žymime $|a| = m$.

Visų abėcėlės A ilgio m žodžių aibę žymime A^m, t. y.

$$A^m = \underbrace{A \times A \times \cdots \times A}_{m-\text{kartų}}$$

yra Dekarto[44] sandauga. Tokių žodžių galima sudaryti $|A|^m = n^m$.

Dažnai nagrinėjami ne visi žodžiai, bet tik tam tikras jų poaibis

$$A^* \subset \bigcup_{m=1,2,\ldots} A^m.$$

Gali būti apibrėžtos tam tikros žodžių sudarymo taisyklės – ***automatas***. Kitas šaltinio modeliavimo būdas – ***statistinis***: apibrėžiamos atskirų raidžių arba jų kombinacijų tikimybės.

Kodo sąvoka

Tarkime, kad $B = \{b_1, b_2, \ldots, b_k\}$ – baigtinė abėcėlė. Nagrinėjamų abėcėlės B žodžių aibę pažymėkime B^*. Atvaizdį $C : A^* \to B^*$ vadiname ***kodu***. Taigi kodas yra funkcija (injekcija), atvaizduojanti žodžius $a \in A^*$ į žodžius $b = C(a) \in B^*$.

Pastebėkime, kad mes nereikalaujame kad atvaizdis C būtų ***bijekcija***, t. y. kad egzistuotų atvirkštinė funkcija C^{-1}. Tarkime, kad[45]

[44] René Descartes (1596 – 1650) – prancūzų filosofas ir matematikas.

[45] $\exists!$ reiškia "egzistuoja vienintelis".

$\tilde{B} \subset B^*$ ir $\forall b \in \tilde{B}\ \exists! a \in A^* : C^{-1}(b) = C^{-1}(C(a)) = a$,
t. y. įmanomas ***dekodavimas*** ir sakome, kad kodas C yra ***dekoduojamas***.

6.2. Kodavimo uždaviniai

Informacijos kodavimo būdas priklauso nuo kodavimo tikslo. Išskirkime tris tokius tikslus ir parodykime galimus jų pasiekimo variantus.

Tikslas – apsaugoti informaciją nuo iškraipymų

Tarkime, kas informacijos šaltinis generuoja raides $\{a, b\}$ ir jos yra koduojamos simboliais $\{0, 1\}$. Dėl tam tikrų[46] priežasčių įmanomi iškraipymai ir vietoje 0 gali būti suprastas 1 ir atvirkščiai. Pažymėkime klaidos tikimybę p. Ši tikimybė turi būti pakankamai maža (rašome $0 < p << 1$). Kai $p \approx 0.5$ patikimai užkoduoti informacijos neįmanoma. Tarkime, kad $p = 0.05$ ir panagrinėkime kodą $a \to 0$, $b \to 1$. Vietoje pranešimo (žodžio) $aabab$ turėsime užkoduotą pranešimą 00101. Raskime tikimybę, kad gautas pranešimas 00101 ištikrųjų atitinka žodį $aabab$. Tikimybė, kad vienas simbolis perskaitytas teisingai $q = 1 - p = 0.95$. Taigi turi būti teisingai perskaityti visi penki simboliai ir šio įvykio tikimybė yra $(0.95)^5 \approx 0.774$. T. y. teisingai bus priimta tik apie 77% tokių pranešimų.

Panagrinėkime kitą kodavimo būdą: $a \to 00$, $b \to 11$. Tada žodžiai 01 ir 10 nepriklauso aibei B^* (žr. 6.1.) ir liudija informacijos iškraipymą. Tarkime, kad gautas pranešimas 0000110011. Apskaičiuokime tikimybę, kad jis atitinka žodį $aabab$. Jei buvo siunčiama raidė b, o gautas pranešimas 00 (t. y. a), tai turėjo įvykti dvi klaidos. Šio įvykio tikimybė $p^2 = 0.0025$. Taigi tikimybė, kad pranešimas nebuvo iškraipytas $(1 - p^2)^5 = 0.9975^5 \approx 0.988$ ir teisingai bus priimta jau apie 99% pranešimų.

[46] Mes nagrinėjame matematinę teoriją ir konkrečios fizikinės, techninės bei kitokios iškraipymų priežastys nėra šios teorijos objektas.

Matome, kad išnagrinėtas kodas ne tik sumažina tikimybę neteisingai dekoduoti pranešimą bet ir ***aptinka klaidas*** (kai pasitaiko kombinacijos 01 ir 10). Tokie kodai vadinami kodais, ***randančiais klaidas*** arba ***klaidų aptikties*** kodais.

Tarkime, kad kodas apibrėžtas taip: $a \to 000$, $b \to 111$. Tada klaidas liudija net šeši žodžiai:

$$\begin{array}{ll} 001 & 011 \\ 010 & 101 \\ 100 & 110 \end{array}$$

Jei priimtas, pavyzdžiui, pranešimas 001, įvyko arba viena klaida (buvo siunčiama raidė a), arba dvi klaidos (raidė b). Pažymėkime šiuos įvykius H_a bei H_b ir manydami, kad $P(H_a) = P(H_b) = 0.5$, apskaičiuokime aposteriorines tikimybes $p_a = P(H_a|001)$ ir $p_b = P(H_b|001)$. Turime

$$P(001) = P(001|H_a)P(H_a) + P(001|H_b)P(H_b) = \\ \left(p(1-p)^2 + p^2(1-p)\right) 0.5$$

ir taikome Bejeso formules:

$$p_a = \frac{P(001|H_a)P(H_a)}{P(001)} = 1 - p = 0.95,$$
$$p_b = \frac{P(001|H_b)P(H_b)}{P(001)} = p = 0.05.$$

Taigi pasirinkdami patikimesnį variantą, galime žodžius iš kairiojo stulpelio dekoduoti kaip raidę a, o iš dešiniojo – kaip b.

Matome, kad pasiūlytas kodas gali ***ištaisyti klaidą***. Tokie kodai vadinami ***koreguojančiais*** arba ***korekcijos*** kodais.

Pastebėkime, kad kiekvieną žodį $a \in A^*$ atitinka ilgio $k = 3|a|$ simbolių $\{0, 1\}$ blokas ir tokie kodai vadinami ***blokiniais***. Vienos raidės $\{a, b\}$ patikimesniam perdavimui turime imti ilgesnius blokus. Parametras $\dfrac{|a|}{k} = \dfrac{1}{3} < 1$ rodo patikimesnio kodavimo "kainą" ir kartais vadinamas blokinio kodo ***greičiu***. Taigi vienas kodavimo teorijos uždavinių yra ne tik patikimų, bet ir pakankamai greitų kodų sudarymas.

Tikslas – sumažinti duomenų kiekį

Tarkime, kad informacijos šaltinis generuoja keturias raides $\{a, b, c, d\}$, tačiau jų pasirodymo tikimybės yra nevienodos: $p_a = \frac{1}{2}$, $p_b = \frac{1}{4}$, $p_c = p_d = \frac{1}{8}$. Išnagrinėkime du skirtingus kodus. Pirmasis – blokinis:

$$a \to 00,\ b \to 01,\ c \to 10,\ d \to 11. \qquad (C_1)$$

Tada pranešimas $\alpha_1\alpha_2\cdots\alpha_n$ ($\alpha_j \in \{a, b, c, d\}$) turi vidutiniškai $\frac{n}{2}$ simbolių a, $\frac{n}{4}$ simbolių b ir po $\frac{n}{8}$ simbolių c bei d. Taip užkoduoto pranešimo vidutinis ilgis yra

$$l_1 = 2 \cdot \frac{n}{2} + 2 \cdot \frac{n}{4} + 2 \cdot \frac{n}{8} + 2 \cdot \frac{n}{8} = 2n$$

arba $\frac{l_1}{n} = 2$. T. y. gauname, kad vienai raidei $\{a, b, c, d\}$ koduoti mes naudojame vidutiniškai[47] du simbolius $\{0, 1\}$. Šiuo atveju mes tai matome iš kodavimo schemos (C_1).

Paimkime kitą kodą:

$$a \to 0,\ b \to 10,\ c \to 110,\ d \to 111. \qquad (C_2)$$

Pastebėkime, kad šis kodas jau nėra blokinis ir jo *dekodavimo algoritmas*[48] gali būti pavaizduotas tokiu *medžiu*:

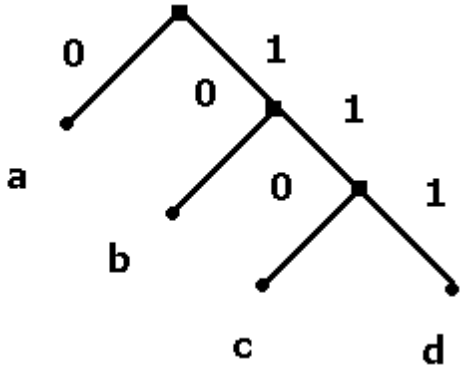
Apskaičiuokime vidutinį pranešimo ilgį:

$$l_2 = 1 \cdot \frac{n}{2} + 2 \cdot \frac{n}{4} + 3 \cdot \frac{n}{8} + 3 \cdot \frac{n}{8} = \frac{7}{4}\,n$$

arba $\frac{l_2}{n} = 1.75$. Taigi koduojant simbolius pagal (C_2) schemą gausime kiek trumpesnius pranešimus.

[47] Šiuo atveju tiksliai, kadangi turime blokinį kodą.

[48] Kiekvienas kodo (C_2) žodis ***n'era*** jokio kito žodžio pradžia. Tokie kodai vadinami ***prefiksiniais*** ir yra lengvai dekoduojami.



47: Kodo (C_2) dekodavimo medis

Tikslas – užtikrinti informacijos slaptumą

Tarkime, kad pranešimas $a = a_{i_1}a_{i_2}\cdots a_{i_m} \in A^*$ yra simbolių $a_j \in \{0,1\}$ seka. Sudarykime tokį kodą: $b_j = a_j \oplus c_j^{(r)}$. Čia

$$c^{(r)} = \begin{pmatrix} c^{(0)} \\ c^{(1)} \\ \vdots \\ c^{(2^m-1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix}.$$

Tada, žinant $c^{(r)}$ randamas $a_j = b_j \oplus c_j^{(r)}$, t. y. skaitomas *slaptas* pranešimas $b = b_{i_1}b_{i_2}\cdots b_{i_m}$. Nežinant $c^{(r)}$, t. y. slaptojo ***rakto*** r, gauti a yra ***sunku***. Galima, pavyzdžiui, *perrinkti* visus 2^m raktus, tačiau kai m yra pakankamai didelis, tai yra praktiškai neįmanoma. Kai $m = 260$ (paprasto natūraliosios kalbos teksto keliasdešimt žodžių) skirtingų raktų r yra $2^m \sim 10^{78}$ – tiek yra elektronų visatoje!

Pastebėkime, kad ne visi raktai $r \in \{0,1,\ldots,2^m-1\}$ užtikrina pranešimo slaptumą. Pavyzdžiui, kai $r = 0$, turime $b = a$. Jei pir-

mieji $c^{(r)}$ yra nuliai, liks *neužšifruota* pirmoji pranešimo dalis. Susitarkime slaptumą užtikrinančius kodus vadinti ***šifrais***. Šifrų sudarymą bei patikimumą[49] nagrinėja ***kriptografija***.

6.3. Kodų pavyzdžiai

Išnagrinėkime kelis gerai žinomus kodus, kurie sudaryti, sprendžiant kurį nors vieną iš trijų kodavimo uždavinių.

Kodas du iš penkių

Šis kodas koduoja dešimtainius skaitmenis penkiais nuliais ir vienetais:

$$\begin{array}{ll} 0 \to 11000 & 5 \to 01010 \\ 1 \to 00011 & 6 \to 01100 \\ 2 \to 00101 & 7 \to 10001 \\ 3 \to 00110 & 8 \to 10001 \\ 4 \to 01001 & 9 \to 10100 \end{array}$$

Penktasis šio kodo simbolis yra kontrolinis. Jis pasirenkamas taip, kad vienetų skaičius kiekviename bloke būtų lygus dviem. Tokie kodai vadinami ***lyginumo kontrolės*** kodais.

Morzės kodas

Raidžių atskyrimui Morzės[50] kode naudojamas trečiasis simbolis – pauzė. Tokie kodai dar vadinami kodais ***su kableliu***. Pastebėkime, kad kitaip būtų neįmanoma atskirti pranešimo EE nuo I, arba IE – nuo EI, nuo S ir t. t.

[49] Dešifravimo galimybės yra ***kriptoanalizės*** nagrinėjimo objektas. Literatūroje kriptoanalizė dažnai atskiriama nuo kriptografijos ir jos abi vadinamos ***kriptologija***

[50] Samuel Finley Breese Morse (1791 – 1872) – amerikiečių išradėjas ir verslininkas.

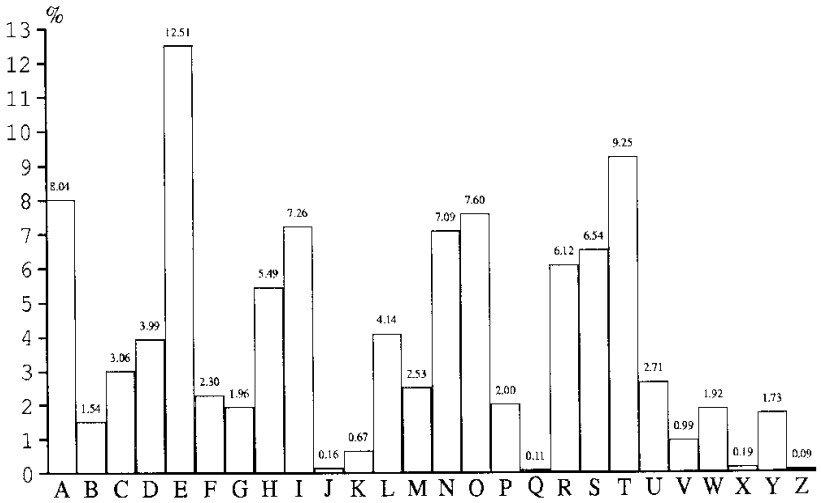
A	· –	J	· – – –	S	· · ·
B	– · · ·	K	– · –	T	–
C	– · – ·	L	· – · ·	U	· · –
D	– · ·	M	– –	V	· · · –
E	·	N	– ·	W	· – –
F	· · – ·	O	– – –	X	– · · –
G	– – ·	P	· – – ·	Y	– · – –

H	· · · ·	Q	– – · –
Z	– – · ·	I	· ·
R	· – ·	1	· – – – –
2	· · – – –	3	· · · – –
4	· · · · –	5	· · · · ·
6	– · · · ·	7	– – · · ·
8	– – – · ·	9	– – – – ·
0	– – – – –		

Kodas sudarytas taip, kad dažniau pasitaikančios raidės būtų koduojamos trumpesnėmis taškų bei brūkšnių sekomis. Pats Moržė gavo informaciją apie santykinius raidžių dažnius spaustuvėje. Įdomu palyginti šią informaciją su anglų kalbos raidžių dažnių statistika.

Pateiksime raidžių pasirodymo dažnius ir lietuvių kalbos tekstuose[51].

[51] Šį tyrimą 2002 m. atliko Juozas Kaunas.



48: Anglų kalbos tekstų atskirų raidžių dažniai

tarpas	0.1495	i	0.1125	a	0.1019
s	0.0696	t	0.0479	e	0.0462
o	0.0450	u	0.0438	r	0.0433
n	0.0417	k	0.0400	m	0.0267
l	0.0259	p	0.0249	d	0.0225
v	0.0221	j	0.0190	ė	0.0168
g	0.0164	š	0.0144	b	0.0127
y	0.0106	ž	0.0096	ų	0.0082
ą	0.0072	į	0.0058	ū	0.0045
č	0.0038	ę	0.0031	z	0.0016
c	0.0011	h	0.0006	f	0.0006

Cezario kodas

Šį kodą Cezaris[52] naudojo kaip slaptąjį šifrą, susirašinėjant su Ciceronu[53].

A	B	C	D	E	F	G	$\cdots$	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	$\cdots$	W	X	Y	Z	A	B	C

Knygų numeracija

Knygų tarptautinė standartinė numeracijos sistema ISBN[54] yra 10 skaitmenų a_j (brūkšniai naudojami tik patogumui[55]) kodas:

$$a_1 - a_2a_3a_4 - a_5a_6a_7a_8a_9 - a_{10}.$$

Pirmieji 9 simboliai a_j yra dešimtainiai skaitmenys $\{0, 1, \ldots, 9\}$. Dešimtasis skaitmuo a_{10} yra kontrolinis ir įgyja reikšmes $\{0, 1, \cdot, 8, 9, X\}$ (Raidė X rašoma, kai $a_{10} = 10$). Kodo kontrolinė suma sudaroma taip:

$$\sum_{j=1}^{9} ja_j \equiv a_{10} \pmod{11}.$$

Priminsime, kad žymėjimas $x \equiv y \pmod{11}$ reiškia, kad skaičius $x-y$ yra dalus iš 11. Skaitome: x *lygsta* y *moduliu* 11. Pastebėkime, kad kontrolinę sumą galima perrašyti taip:

$$\sum_{j=1}^{10} ja_{11-j} \equiv 0 \pmod{11}.$$

[52] Gaius Julius Caesar (100 – 44 pr. m. e.) – Romos diktatorius.

[53] Marcus Tillius Cicero (106 – 43 pr. m. e.) – Romos politikas, oratorius, rašytojas.

[54] International Standard of Book Numeration.

[55] Pirmieji keturi skaitmenys skirti šalies bei leidyklos žymėjimui. Skaitmenys $a_5 \ldots a_9$ skirti leidiniu žymėti.

Kontrolinė suma ***nebegalioja***, įvykus vienai ***paprastajai klaidai*** (pakeistas vienas kodo simbolis) arba vienai ***transpozicinei klaidai*** (sukeisti vietomis du simboliai).

Išnagrinėkime Lietuvoje išleistos knygos ISBN kodo pavyzdį[56]

$$5-430-02548-8.$$

Apskaičiuokime kontrolinę sumą:

$$\begin{aligned}1\cdot 5+2\cdot 4+3\cdot 3+4\cdot 0+5\cdot 0+6\cdot 2+7\cdot 5+8\cdot 4+9\cdot 8 &= \\ 5+8+9+0+0+12+35+32+72 &= \\ 173=15\cdot 11+8\equiv 8 \pmod{11}.&\end{aligned}$$

Taikydami antrą formulę, gauname

$$\begin{aligned}1\cdot 8+2\cdot 8+3\cdot 4+4\cdot 5+5\cdot 2+6\cdot 0+7\cdot 0+8\cdot 3+9\cdot 4+10\cdot 5 &= \\ 8+16+12+20+10+0+0+24+36+50 &= \\ 176=16\cdot 11\equiv 0 \pmod{11}.&\end{aligned}$$

Prekių numeracija

Prekių numeracijos (brūkšninių kodų) sistema EAN–13[57] yra 13 skaitmenų
$\{0,1,\ldots,8,9\}$ kodas

$$a_1a_2a_3-a_4\cdots a_{12}-a_{13}$$

su tokia kontroline suma:

$$a_1+3a_2+a_3+3a_4+\cdots+a_{11}+3a_{12}+a_{13}\equiv 0 \pmod{10}.$$

Patikrinkime Lietuvoje[58] pagamintos prekės kodą $477-008048113-1$:

$$4+3\cdot 7+7+\cdots+3\cdot 1+1+3\cdot 3+1=90=9\cdot 10\equiv 0 \pmod{10}.$$

[56] Kodo pirmieji skaitmenys (prefiksas) $5-430$ reiškia Kauno leidyklą "Šviesa".
[57] European Article Numeration.
[58] Tai nurodo EAN–13 kodo ***prefiksas*** 477.

Literat ̄ura

[1] Bloznelis M. *Kombinatorikos paskaitų ciklas. (Mokomoji priemonė)*. Vilniaus universiteto leidykla, Vilnius, 1996.

[2] Griniuvienė L. *Matematinė logika (mokymo priemonė)*. VPU leidykla, Vilnius, 1997.

[3] Jusas V. *Matematinė logika (Mokomoji knyga)*. Technologija, Kaunas, 2002.

[4] Lassaigne R., de Rougemont M. *Logika ir informatikos pagrindai*. Žodynas, Vilnius, 1996.

[5] Mišeikis F. *Diskretinės matematikos pradmenys (Mokymo priemonė)*. VU, Vilnius, 1989.

[6] Morkeliūnas A. *Binarieji sąryšiai, grafai ir operacijos. (Mokomoji metodikos priemonė)*. Vilniaus universitetas, Vilnius, 1998.

[7] Norgėla S. *Matematinės logikos įvadas*. Vilnius, 1985.

[8] Ore O. *Grafai ir jų pritaikymas*. Mintis, Vilnius, 1973.

[9] Plukas K. , Mačikėnas E., Jarašiūnienė B., Mikuckienė I. *Taikomoji diskrečioji matematika: vadovėlis*. Technologija, Kaunas, 2001.

[10] Stakėnas V. *Informacijos kodavimas. (Mokomoji priemonė)*. Vilniaus universiteto leidykla, Vilnius, 1996.

[11] Vilenkinas N. *Kombinatorika*. Šviesa, Kaunas, 1976. (Vertimas iš rusų kalbos. Maskva, Nauka, 1969).

[12] Žilinskas A., Leonavičius G., Valavičius E. *Informatika (vadovėlis aukštosioms mokykloms)*. Aldorija, Vilnius, 2000.

[13] Althoen S. C. and Bumcrot R. J. *Introduction to Discrete mathematics*. 1988.

[14] Balakrishnan V. K. *Introductory Discrete mathematics*. 1991.

[15] Cooke D. J. and Bez H. E. *Computer Mathematics*. Cambridge University Press, Cambridge, 1984. (Yra šios knygos vertimas į rusų kalbą. Maskva, Nauka, 1990).

[16] Garey M. R. and Johnson D. S. *Computers and Intractability. A Guide to the Theory of NP-Completeness*. Bell Laboratories Murray Hill, New Jersey, 1979. (Yra šios knygos vertimas į rusų kalbą. Maskva, Mir, 1982).

[17] Kolman B. and Busby R. C. *Discrete Structures with Applications*. New Jersey, 1987.

[18] Nicodemi O. *Discrete mathematics*. New York, 1987.

[19] Reingold E. M., Nievergelt J., Deo N. *Combinatorial Algorithms. Theory and Practice*. Prentice–Hall, Inc., Englewood Cliffs, New Jersey, 1977. (Yra šios knygos vertimas į rusų kalbą. Maskva, Mir, 1980).

[20] Roman S. *An introduction to Discrete mathematics*. New York, 1986.

[21] Fudzisava T. and Kasami T. *Matematika dlia radioinženerov: Teorija diskretnych struktur*. Radio i sviaz, Moskva, 1984.

[22] Gavrilov G. P. , Sapoženko A. A. *Sbornik zadač po diskretnoi matematike*. Nauka, Moskva, 1977.

[23] Gorbatov V. A. *Osnovy diskretnoi matematiki*. Vyš. škola, Moskva, 1986.

[24] Emeličev V. A. , Mel'nikov O. I., Sarvanov V. I., Tyškevič R. I. *Lekcii po teorii grafov*. Nauka, Moskva, 1990.

[25] Ivanov B. N. *Diskretnaja matematika: Algoritmy i programmy*. Laboratorija bazovych znanii, Moskva, 2001.

[26] Jablonskii S. V. *Vvedenie v discretnuju matematiku*. Nauka, Moskva, 1986.

[27] Karpov V. G. , Moščenskii V. A. *Matematičeskaja logika i diskretnaja matematika*. Vyš. škola, Minsk, 1977.

[28] Kuznecov O. P. , Adelson – Velskii G. M. *Diskretnaja matematika dlia inženera*. Energoatomizdat, Moskva, 1988.

[29] Novikov F. A. *Diskretnaja matematika dlia programmistov*. Piter, Sankt Peterburg, 2000.

[30] Romanovskii I. V. *Diskretnyi analiz*. Nevskii dialekt, Sankt Peterburg, 2000.

[31] Zykov A. A. *Osnovy teorii grafov*. Nauka, Moskva, 1987.