UDK 510(075.8)
No-66

Aukštųjų mokyklų bendrųjų vadovėlių leidybos komisijos rekomenduota
2003 12 19 Nr. A-177

Redaktorė *Zita Manstavičienė*
Programinė įranga: *Tadeuš Šeibak*
Kompiuterinė grafika: *Inga Paukštienė*
Tekstą rinko ir maketavo: *Aldona Žalienė, Nijolė Drazdauskienė*
Korektorė *Birutė Laurinskienė*
Konsultantas *Elmundas Žalys*

Leidyklos TEV interneto svetainė http://www.tev.lt

ISBN 9955-491-60-4

Turinys

Pratarmė ... 5
Įvadas ... 6

1. Aibės ir grafai ... 10
1.1. Skaičiosios aibės ... 10
1.2. Pagrindinės grafų sąvokos ... 15
1.3. Pratimai ... 17
2. Teiginių logika ... 18
2.1. Loginės operacijos ... 18
2.2. Ekvivalenčiosios formulės ... 22
2.3. Loginės išvados ... 27
2.4. Normaliosios formos ... 29
2.5. Logikos algebros funkcijos ... 34
2.6. Kai kurios neklasikinės logikos ... 36
2.7. Dvejetainis sumavimas ... 38
2.8. Pratimai ... 41
3. Rekursyviosios funkcijos ... 43
3.1. Intuityvioji algoritmo samprata ... 43
3.2. Primityviai rekursyvios funkcijos ... 45
3.3. Minimizavimo operatorius ... 48
3.4. Porų numeravimas ... 49
3.5. Baigtinumo problema ... 51
3.6. Rekursyviai skaičios aibės ... 54
3.7. Ackermanno funkcijos ... 57
3.8. Universaliosios funkcijos ... 60
3.9. Kanoninis Posto skaičiavimas ... 64
3.10. Pratimai ... 67
4. Teiginių skaičiavimai ... 69
4.1. Hilberto tipo skaičiavimas ... 69
4.2. Dedukcijos teorema ... 74
4.3. Teiginių skaičiavimo pilnumas ... 77
4.4. Gentzeno skaičiavimas ... 83
4.5. Natūralioji dedukcija ... 89
4.6. Disjunktų dedukcinė sistema ... 91
4.7. Skaičiavimų ryšys ... 97
4.8. Pratimai ... 99
5. Predikatų logika ... 101
5.1. Predikatų logikos formulės ... 101

5.2. Semantika ... 104
5.3. Pavyzdys formulės, įvykdomos begalinėje ir neįvykdomos jokioje baigtinėje aibėje ... 107
5.4. Normaliosios priešdėlinės formos ... 110
5.5. Formulės, į kurias įeina tik vienviečiai predikatiniai kintamieji ... 111
5.6. Aristotelio logika ... 115
5.7. Pratimai ... 118

6. Predikatų skaičiavimai ... 121
6.1. Formulės, kuriose yra funkciniai simboliai ... 121
6.2. Hilberto tipo predikatų skaičiavimas ... 125
6.3. Sekvencinis skaičiavimas ... 127
6.4. Intuicionistinė logika ... 133
6.5. Kompaktiškumas ... 136
6.6. Semantiniai medžiai ... 138
6.7. Rezoliucijų metodas ... 140
6.8. Pratimai ... 145

7. Modalumo logikos ... 148
7.1. Modalumo logikų formulių semantika ... 148
7.2. Modalumo logikų skaičiavimai ... 151
7.3. Ekvivalenčiosios formulės ... 154
7.4. Rezoliucijų metodas modalumo logikai S4 ... 158
7.5. Kvantorinė modalumo logika S4 ... 160
7.6. Laiko logikos ... 163
7.7. Pratimai ... 168

8. Loginės teorijos ... 169
8.1. Pirmosios eilės teorijos ... 169
8.2. Formalioji aritmetika ... 172
8.3. Peano aritmetikos nepilnumas ... 174
8.4. Aksiominė aibių teorija ... 178
8.5. Antrosios eilės logika ... 180
8.6. Tautologijos baigtinėse struktūrose ... 182
8.7. Pratimai ... 185

Pavardžių rodyklė ... 186

Dalykinė rodyklė ... 187

Lietuvių–anglų kalbų žodynėlis ... 189

Literatūra ... 192

Pratarmė

Tai pirmasis matematinės logikos vadovėlis lietuvių kalba. Jame nuosekliai išdėstytos pagrindinės matematinės logikos temos ir aprašyti kai kurie dirbtinio intelekto metodai. Nagrinėjama pirmosios eilės logika, rekursyviosios funkcijos bei modalumo logikos. Pateikiamos pagrindinės sąvokos, daug rezultatų aiškinama konkrečiais pavyzdžiais.

Šis vadovėlis skirtas informatikos, programų sistemų bei matematikos specialybių studentams. Rašantiems kursinius, bakalauro bei magistro darbus studentams labai pravers vadovėlio pabaigoje pateikiamas kai kurių matematinės logikos terminų lietuvių–anglų kalbų žodynėlis.

Nuoširdžiai dėkoju Romui Alonderiui, Valdui Dičiūnui, Aidai ir Regimantui Pliuškevičiams, Jūratei Sakalauskaitei bei Baliui Šulmanui, daug prisidėjusiems tobulinant šį vadovėlį.

Autorius

Įvadas

Per ilgą savo gyvavimo istoriją matematika pergyveno tris gilias krizes.

Kaip deduktyvus mokslas matematika susiformavo VI a. pr. Kr. Žymiausi to meto matematikai buvo Pitagoras, Tallis bei jų mokiniai. Pitagoro darbai rėmėsi *intuityviai aiškiu* tvirtinimu, kad bet kurie vienarūšiai dydžiai turi bendrą matą. Pavyzdžiui, bet kurioms dviem atkarpoms atsiras trečioji, telpanti sveikąjį skaičių kartų į kiekvieną turimą atkarpą. Buvo manoma, kad visi ilgiai ir plotai tarpusavyje gali būti bendramačiai. Nebendramačių atkarpų atradimas buvo didelis smūgis matematiko Pitagoro mokymui. Netikėtas V a. pr. Kr. atradimas, kad kvadrato įstrižainė neturi bendro mato su kraštine, sukėlė matematikos pagrindų krizę. Pasirodo, kvadrato įstrižainės ir kraštinės santykio negalima išreikšti jokiu tuo metu vartojamu skaičiumi.

Vėliau buvo atrasta ir daugiau nebendramačių dydžių. Tai apskritimo ilgis ir jo skersmuo, kvadrato ir apie jį apibrėžto skritulio plotai bei kiti dydžiai. Krizė tęsėsi ilgai. Jos pabaiga apie 370 m. pr. Kr. siejama su žymaus graikų matematiko Eudoxos darbais. Jis sukūrė bendrąją proporcijų teoriją. Ši krizė suvaidino ypatingą vaidmenį matematinio metodo kūrimui. Be to, buvo įvesti nauji skaičiai. Jie nebuvo nei sveikieji, nei trupmeniniai. Tai *iracionalūs skaičiai* ($\sqrt{2}$, $\pi, \ldots$). Daugelis to meto mokslininkų į juos žiūrėjo su nepasitikėjimu. Šie skaičiai buvo laikomi nesuprantamais, beprasmiais, netikrais, protu nesuvokiamais, t.y. iracionaliais (lot. *irrationalis* – neprotingas.

Antroji krizė siejama su matematine analize ir sukrėtė matematiką XVII amžiaus pabaigoje. Newtono ir Leibnitzo mokiniai, kiti jų teorijos šalininkai mažai rūpinosi analizės pagrindais, žavėjosi tik didele galimybe taikyti analizę praktikoje. Teoremų įrodymai nebuvo griežti. Rezultatai rėmėsi neaiškiu be galo mažų dydžių supratimu. Krizė ir kilo dėl šios sąvokos neaiškumo. Be galo mažas dydis kartais būdavo prilyginamas nuliui ir skaičiavimuose atmetamas, kitais kartais jam būdavo suteikiama nelygi nuliui reikšmė. XIX amžiaus pradžioje Cauchy atsisakė neaiškios be galo mažų dydžių teorijos ir pakeitė ją griežta ribų teorija. Antrosios krizės pabaiga kaip tik ir siejama su šia teorija.

Įdomu, kad ir XX amžiuje matematikai grįžo prie be galo mažų dydžių sąvokos ir ją patikslino. Amerikiečių matematikas A. Robinson 1960 m. pasiūlė kitą būdą, kaip galima griežtai pagrįsti XVII ir XVIII amžių matematinę analizę. Be galo mažus dydžius jis siūlė laikyti ne kintamaisiais, o pastoviais dydžiais. Juk taip buvo elgiamasi ir tada, kai kūrėsi matematinė analizė. Matyt, ir Leibnitz, įvesdamas simbolius dx, dy, laikė juos pastoviais ypatingos rūšies dydžiais. Taigi A. Robinson įvedė be galo mažų ir be galo didelių skaičių sąvokas. Remiantis jomis galima kurti kitokią matematinę analizę (tiksliau, pagrįsti ją kitu būdu). Ji vadinama nestandartine analize.

Trečioji matematikos pagrindų krizė prasidėjo 1897 m., kai spaudoje pasirodė italų matematiko C. Burali-Forti atrasta aibių teorijos antinomija. Kai kalbama apie kurią nors teorijos antinomiją, suprantama, kad toje teorijoje įrodomi du vienas kitam prieštaraujantys teiginiai, nors teorijos aksiomos bei išvedimo taisyklės atrodo teisingos.

Pateiksime porą antinomijų pavyzdžių.

Vienas žmogus pasakė: „*Viskas, ką aš kalbu – melas.*" Vadinasi, melas ir šitas jo posakis. O tai reiškia, kad ne viskas, ką pasako tas žmogus, yra melas. Bet tai prieštarauja pirmajam teiginiui.

Tarkime, a yra mažiausias teigiamas skaičius, kurį apibrėžti reikia daugiau kaip 15 lietuviškų žodžių. Kadangi pastarąjį sakinį sudaro mažiau kaip 15 žodžių, tai a nėra taip apibrėžtas skaičius. Taigi tas sakinys prieštaringas.

Deja, panašių paradoksų, pasirodo, galima rasti ir griežtoje tikslioje matematikoje (žr. skyrelį *Aksiominė aibių teorija*). Taigi aibių teorijoje buvo aptikta paradoksų. Vadinasi, ne viskas joje gerai. Kadangi aibių teorija remiasi ir kitos matematikos šakos, tai susvyravo matematikos pagrindai. Daugelis tyrinėtojų manė, kad paradoksų priežastis slypi logikoje. Reikėjo visapusiškos logikos pagrindų analizės.

Logika nagrinėja žmogaus mąstymą, tiksliau – mąstymo formą. Žodis *logika* kilęs iš senosios graikų kalbos (gr. *logos* – žodis, kalba, protas, samprotavimas). Logika atsirado ir vystėsi kaip filosofijos mokslo šaka. Dar VI–IV a. pr. Kr. ji buvo savarankiškai kuriama Graikijoje, Kinijoje ir Indijoje. Žymiausias tų laikų logikas buvo graikų filosofas *Aristotelis* (384–322 m. pr. Kr.), kurio sukurta teorija (žr. skyrelį *Aristotelio logika*), ypač didelės įtakos turėjusi logikai. Po to prasidėjo stagnacijos periodas, kuris truko daugiau kaip du tūkstančius metų.

Matematinė logika, remdamasi matematika, pirmiausia tiria matematinius samprotavimus. Matematinės logikos pradininkais vieni autoriai vadina vokiečių matematiką G. Leibnitzą (1646–1716), kiti – airių matematiką D. Boole (1646–1716) ar vokietį G. Frege (1848–1925). Ir vieniems, ir kitiems didelę įtaką darė Aristotelis.

Matematikas A. de Morgan iš Londono (1806–1878) kai kurias algebroje nagrinėjamų objektų savybes perkėlė logikos dėsniams. D. Boole stengėsi įgyvendinti idėją, kad logika taptų tiksliuoju mokslu. Vokiečių matematikas E. Schräder (1841–1902) bei Kazanės universiteto (Rusija) profesorius P. S. Poreckij (1846–1907) pagrindė teiginių ir predikatų logiką, dažniausiai siedami ją su algebra. Per šimtmečius susikaupė daug atrastų logikos dėsnių. Pavyzdžiui, vienas jų $((p\&q) \to r)\&(p\&\neg r)) \to \neg q$. Loginių operacijų ženklų dar nebuvo. Dėsnis buvo užrašomas taip:

Jei pirmasis ir antrasis, tai trečiasis. Dabar nėra trečiojo, bet yra pirmasis. Vadinasi, nėra antrojo.

Kaip dėsniai būdavo atrandami? Dažniausiai būdavo iškeliama hipotezė apie dėsnį ir stengiamasi ją paneigti, t.y. ieškoma pavyzdžio, kada hipotezė klaidinga. Jei to padaryti nepavyksta, hipotezė pripažįstama dėsniu. Įrodymo (matematine prasme) nebūdavo. Logikos dėsnių aibę pirmasis susistemino vokiečių matematikas G. Frege. Jis 1879 m. pirmasis sukūrė formaliąją – teiginių skaičiavimo teoriją ir parodė, kad visi žinomi bei daugelis naujų teiginių išvedami joje (dėl paprastumo aksiomos parašytos šių laikų formalia kalba):

(1) $A \to (B \to A)$,
(2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
(3) $(A \to (B \to C)) \to (B \to (A \to C))$,
(4) $(A \to B) \to (\neg B \to \neg A)$,
(5) $\neg\neg A \to A$,
(6) $A \to \neg\neg A$.

Skaičiavime yra formulių keitimo lygiavertėmis ir *modus ponens* taisyklės. Vėliau buvo įrodyta, kad (3) aksioma nereikalinga. Ji išvedama iš likusiųjų. Įdomu tai, kad G. Frege aprašė skaičiavimą anksčiau, negu kad buvo pastebėta, jog logikos dėsnius galima nustatyti ir naudojantis teisingumo lentelėmis. Tik praėjus šešeriems metams – 1885 m. Ch.S. Peirce (amerikiečių matematikas ir filosofas) sukūrė teisingumo lentelių metodą.

Pagrindiniai vadovėlyje aprašyti rezultatai ir prasideda G. Frege skaičiavimu bei vėlesniais logikų darbais.

Logika tolydžio tampa tiksliuoju mokslu, kurio rezultatams suprasti jau reikia matematinio išsilavinimo. Patį mokslą pradėta vadinti tai *simboline logika*, tai *formaliąja* ar *matematine logika*. Kaip savarankiška matematikos šaka su savo problematika ir metodais logika galutinai susiformavo praeito šimtmečio ketvirtajame dešimtmetyje. Ypač daug prie to prisidėjo austrų logiko K. Gödelio (1906–1977) darbai. Net susiformavus matematinei logikai, daugelyje universitetų dar ilgai logikos pavadinimu buvo dėstoma tik Aristotelio sistema. B. Russell knygoje *History of Western Philosophy* 1945 m. apie tai rašė:

> Netgi dabar visi filosofijos katalikai bei daugelis kitų dėstytojų vis dar neigia šiuolaikinės logikos atradimus ir keistai užsispyrę laikosi aiškiai pasenusios, kaip kad Ptolomėjaus sistema astronomijoje, Aristotelio logikos.

Skirtingai negu kiti mokslai, matematika pagrindiniu tyrinėjimo metodu laiko įrodymą, o ne eksperimentą. Pavyzdžiui, išmatavus daugelio trikampių vidaus kampų sumas, galima prieiti išvadą, kad trikampio vidaus kampų suma lygi 180 laipsnių. Bet matematikas tai pripažins matematikos dėsniu (teorema) tik tada, kai bus įrodyta, pagrįsta logiškai.

Pažvelgę į bet kurios teoremos įrodymą, pamatysime, kad tai yra seka formulių, tarp kurių įterpti samprotavimai, paaiškinantys, iš kur gauname prieš ar po einančią formulę. Formulės turi vieną reikšmę, o samprotavimai dažnai būna įvairių netikslumų šaltinis. Ar galima rasti tokias samprotavimų (logikos) taisykles, užrašomas formulėmis, kuriomis naudojasi matematikas, įrodinėdamas teoremas? Jei pasisektų tai padaryti, teoremos įrodymas taptų seka formulių, tarp kurių stovi skaičiai, nurodantys, pagal kurią taisyklę ir iš kokių jau turimų formulių gauta sekančioji. Tuomet, turint samprotavimų grandinę, galima patikrinti, ar tai įrodymas. Dar G. Leibnitz buvo iškėlęs idėją sukurti universalią visai matematikai kalbą ir ta kalba formalizuoti matematinius įrodymus. Ginčus, ar koks nors tvirtinimas teisingas,, ar klaidingas, reikėtų suvesti į skaičiavimus. Paėmę pieštuką bei popieriaus ir atlikę matematinius skaičiavimus, galėtume nustatyti, kas teisus. Formalizavimo entuziazmą kiek prislopino rezultatai apie formaliąją aritmetiką (žr. skyrelį *Aritmetikos nepilnumas*). Bet tai truko neilgai. Atsiradus kompiuteriams, atsivėrė labai didelės logikos taikymų perspektyvos.

Pirmasis vadovėlis *Principia Mathematika*, skirtas matematinei logikai ir jos taikymui matematikoje, pasirodė 1910 metais. Jo autoriai buvo B. Russel ir A. Whitehead. Jame yra ir toks sakinys: *Tas faktas, jog visa matematika yra ne kas kita kaip simbolinė logika – didžiausias mūsų amžiaus atradimas.* Su knygos pasirodymu siejamas naujas matematinės logikos vystymosi etapas. Kito vadovėlio teko laukti pakankamai ilgai. D. Hilberto ir P. Bernayso knygos *Grundlagen der Mathematik* pasirodymas 1939 m. užbaigė logikos, kaip matematinės disciplinos, formavimosi etapą. Atsiradus kompiuteriams ir informatikos mokslui, palaipsniui *matematinė logika* tampa jau *informatikos mokslo* šaka.

Lietuvoje *matematinė logika* pradėta dėstyti Vilniaus universitete 1960 metais. Tų metų pavasario bei rudens semestrus J. Kubilius skaitė *Matematinės logikos* specialųjį kursą matematikos specialybės studentams. V. Kabaila 1962 m. skaitė skaičiavimo matematikos specializacijos trečiakursiams *Loginio konstravimo pagrindų* specialųjį kursą. Nuo 1964 m. Vilniaus universitete matematinė logika dėstoma kaip privaloma disciplina – iš pradžių tik matematikos specialybės, o vėliau ir informatikos bei programų sistemų specialybių studentams. Matematinės logikos tyrimų Lietuvoje pradžia siejama su pirmąja 1963 m. V. Matulio apginta daktaro (tuo metu fizikos–matematikos mokslų kandidato) disertacija tema *Apie kai kuriuos klasikinio predikatų skaičiavimo su vieninteliu išvedimo medžiu sekvencinius variantus.* Po to 1967 m. R. Pliuškevičius apgynė daktaro disertaciją tema *Konstruktyviosios logikos be struktūrinių taisyklių variantai bei sekvencijų su normalinėmis formulėmis išvedimai*, o 2002 m. – ir habilituoto daktaro disertaciją tema *Prisotinimo metodas tiesinei laiko logikai.* Pamažu ir Lietuvoje formavosi matematinės logikos mokykla. Matematikos (dabar Matematikos ir informatikos) institute 1964 m. buvo įkurtas *Matematinės logikos ir programavimo* sektorius (1967 m. jis pervardytas į *Matematinės logikos ir algoritmų teorijos*, o 1993 m. – į *Matematinės logikos* skyrių).

1 skyrius
Aibės ir grafai

1.1 Skaičiosios aibės

Tarkime, yra dvi baigtinės aibės A, B ir norime sužinoti, kurioje jų yra daugiau elementų. Galime tai atlikti skaičiuodami elementus abiejose aibėse. Tarkime, pirmojoje aibėje jų yra m, o antrojoje – n. Jei $m > n$, tai aibėje A elementų yra daugiau negu aibėje B. Jei $m < n$, tai daugiau elementų yra aibėje B. Na, o jei $m = n$, tai abiejose aibėse yra po vienodą skaičių elementų.

Galima tai atlikti ir kitu būdu. Paaiškinsime pavyzdžiu. Norime žinoti, ar pakanka studentams vadovėlių. Išdalijame juos (suprantama, kiekvienam po vieną) ir žiūrime, ar liko vadovėlių. Jei taip, tai vadovėlių yra daugiau negu studentų. Jei ne ir liko studentų, neturinčių vadovėlių, tai studentų yra daugiau. Jei vadovėlių neliko ir visi studentai turi po vadovėlį, tai studentų ir vadovėlių yra vienodas skaičius. Šiuo atveju sakome, kad tarp studentų ir vadovėlių aibių egzistuoja ***abipusiškai vienareikšmė atitiktis*** (bijekcija). Antrasis dviejų aibių lyginimo būdas geresnis tuo, kad jį galima taikyti ir begalinėms aibėms (kaip matysime vėliau, toks palyginimas nesutampa su baigtines aibes atitinkančia sąvoka *vienodas elementų skaičius*).

1.1 apibrėžimas. *Dvi aibės A, B vadinamos* ***ekvivalenčiosiomis****, jei tarp jų elementų egzistuoja abipusiškai vienareikšmė atitiktis* (*žymima $A \sim B$*).

Keletas ekvivalenčių aibių savybių, išplaukiančių iš apibrėžimo:

1. $A \sim A$,

2. Jei $A \sim B$, tai $B \sim A$,

3. Jei $A \sim B$ ir $B \sim C$, tai $A \sim C$.

Raide R žymėsime realiųjų skaičių aibę, Q – racionaliųjų, Z – sveikųjų, $N = \{0, 1, 2, \ldots\}$ – natūraliųjų bei $N_- = \{1, 2, 3, \ldots\}$ – natūraliųjų skaičių aibę be 0.

1.2 apibrėžimas. *Aibė vadinama* ***skaičiąja****, jei ji ekvivalenti natūraliųjų skaičių aibei.*

Iš apibrėžimo išplaukia, kad skaičioji aibė yra begalinė.

Pavyzdys. Parodysime, kad sveikųjų skaičių aibė Z yra skaiti.

Nurodysime abipusiškai vienareikšmę atitiktį tarp aibių Z ir N elementų. Ją žymėsime $\updownarrow$.

$$\begin{array}{cccccccc} 0, & 1, & -1, & 2, & -2, & 3, & -3, & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0, & 1, & 2, & 3, & 4, & 5, & 6, & \ldots \end{array}$$

Atitiktis gali būti užrašyta kuria nors funkcija ar taisykle. Norint įrodyti, kad kuri nors aibė A yra skaiti, pakanka nurodyti taisyklę, pagal kurią būtų gaunama seka visų aibės A elementų (kiekvienas elementas joje aptinkamas tik po vieną kartą). Todėl norint įrodyti, kad aibė Z skaičioji, pakanka parodyti, kad ją galima parašyti sekos pavidalu: $0, 1, -1, 2, -2, 3, -3, \ldots$. Iš tokio užrašymo matyti, kad sekoje yra visi Z elementai po vieną kartą. Pasirinkus kurį nors elementą, galima apskaičiuoti, kelintas jis yra sekoje.

1.3 apibrėžimas. *Aibė vadinama* ***numeruojamąja****, jei ji yra baigtinė arba skaičioji.*

1.1 teorema. *Kiekvienas skaičiosios aibės poaibis yra numeruojamoji aibė.*

Įrodymas. Tarkime, kad $A = \{a_0, a_1, a_2, \ldots\}$ yra kuri nors skaičioji aibė ir $B \subset A$. Išbraukiame sekos $a_0, a_1, a_2, \ldots$ visus tuos narius, kurie nepriklauso aibei B. Gauname seką, kuri yra begalinė ir kartu skaičioji, arba baigtinė. Teorema įrodyta.

Išvada. Jei $A = \{a_0, a_1, a_2, \ldots\}$ yra skaičioji aibė, tai $B = \{a_i, a_{i+1}, a_{i+2}, \ldots\}$ $(i > 0)$ – taip pat skaičioji.

Taigi $N \sim N_-$. Jei A skaičioji, tai $A \sim N$. Iš 3 savybės išplaukia, kad A skaičioji tada ir tiktai tada, kai $A \sim N_-$. Sekos narius dažniausiai pradedama numeruoti nuo vieneto. Tai siejama su nario sekoje eiliškumu: pirmasis narys, antrasis narys ir t.t. Mes taip pat kai kada skaičiosios aibės narius rašysime pradėdami indeksu 1: $a_1, a_2, a_3, \ldots$.

Tarkime, $A = \{A_0, A_1, A_2, \ldots\}$ skaičioji ir jos elementais yra skaičiosios aibės $A_i = \{a_0^i, a_1^i, a_2^i, \ldots\}$. Tuomet aibė $A_0 \cup A_1 \cup A_2 \ldots$ vadinama skaičiosios sistemos skaičiųjų aibių sąjunga.

1.2 teorema. *Skaičiosios sistemos skaičiųjų aibių sąjunga yra skaičioji aibė.*

Įrodymas. Tarkime, $A = \{A_0, A_1, A_2, \ldots\}$ bei A_i $(i = 0, 1, 2, \ldots)$ yra skaičiosios aibės, $A_i = \{a_0^i, a_1^i, a_2^i, \ldots\}$. Nurodysime taisyklę, kaip galima visus aibės A elementus parašyti sekos pavidalu.

$$\begin{array}{cccccccccccc}
a_0^0 & \rightarrow & a_1^0 & & a_2^0 & \rightarrow & a_3^0 & & a_4^0 & \rightarrow & a_5^0 & \cdots \\
& \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
a_0^1 & & a_1^1 & & a_2^1 & & a_3^1 & & a_4^1 & & \cdots & \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & & & & & \\
a_0^2 & & a_1^2 & & a_2^2 & & a_3^2 & & a_4^2 & & \cdots & \\
& \swarrow & & \nearrow & & & & & & & & \\
a_0^3 & & a_1^3 & & a_2^3 & & a_3^3 & & a_4^3 & & \cdots & \\
\downarrow & \nearrow & & & & & & & & & & \\
a_0^4 & & a_1^4 & & a_2^4 & & a_3^4 & & a_4^4 & & \cdots & \\
\cdots & & & & & & & & & & &
\end{array}$$

Rodyklėmis nurodome tvarką, kuria rašomi elementai: $a_0^0, a_1^0, a_0^1, a_0^2, \ldots$. Tik prieš rašydami kurį nors elementą a_j^i, tikriname, ar nėra jam lygaus jau gautoje sekoje. Jei taip, tai a_j^i praleidžiame. Teorema įrodyta.

1.3 teorema. *Dviejų skaičiųjų aibių Dekarto sandauga yra skaičioji aibė.*

Įrodymas. Tarkime, yra dvi skaičios aibės $A = \{a_0, a_1, a_2, \ldots\}$ ir $B = \{b_0, b_1, b_2, \ldots\}$. Raide C_i $(i = 0, 1, 2, \ldots)$ pažymėkime aibę $\{(a_i, b_0), (a_i, b_1), (a_i, b_2), \ldots\}$. Tuomet $A \times B$ lygi sąjungai skaičiųjų aibių $C_0, C_1, C_2, \ldots$. Pagal 1.2 teoremą $C_0 \cup C_1 \cup C_2 \cup \ldots$ yra skaičioji, kartu ir $A \times B$ yra skaičioji aibė. Teorema įrodyta.

Išvada. Baigtinio skaičiaus skaičiųjų aibių Dekarto sandauga yra skaičioji aibė.

1.4 teorema. *Racionaliųjų skaičių aibė Q yra skaičioji.*

Įrodymas. Racionaliuosius skaičius galime parašyti trupmenomis $\frac{m}{n}$ (čia $m \in Z, n \in N_-$), o pastarąsias – poromis (m, n). Kadangi Z bei N_- yra skaičios aibės, tai ir visų porų (m, n) aibė bus skaiti, nes pagal 1.3 teoremą $Z \times N_-$ yra skaiti aibė. Kai kuriomis poromis nusakome vieną ir tą patį racionalųjį skaičių, pavyzdžiui, $(2, 4)$ ir $(1, 2)$. Todėl $Q \subset Z \times N_-$. Begalinė racionaliųjų skaičių aibė Q yra skaičiosios aibės poaibis, todėl pagal 1.1 teoremą ji pati taip pat yra skaiti aibė. Teorema įrodyta.

1.4 apibrėžimas. *Tarkime, yra kuri nors aibė A.*

1. *Bet kuris aibės A elementas vadinamas aibės A žodžiu. Jo ilgis lygus* 1.

2. *Jei u, v yra aibės A žodžiai ir jų ilgiai atitinkamai lygūs m ir n, tai ir uv – taip pat aibės A žodis, o jo ilgis lygus $m + n$.*

Pavyzdys. $A = \{a, b, c\}$. Tuomet a, bba, $cabbaccac$ yra aibės A žodžiai. Jų ilgiai atitinkamai lygūs 1, 3, 9.

Kai kalbama apie kurios nors aibės žodžius, tai A dar vadinama ***abėcėle***, o jos elementai – raidėmis. Žodyje ta pati raidė gali pasitaikyti ne vieną kartą. Pavyzdžiui, žodyje $cabbaccac$ tris kartus kartojasi raidė a, du kartus – b ir keturis kartus – c.

1.5 apibrėžimas. *Raidės x **įeitimi** žodyje u vadiname porą (x, i); čia i – natūralusis skaičius ($i \geqslant 1$), nurodantis kelintą kartą (perbėgant žodį u iš kairės į dešinę) pasitaiko raidė x.*

Pavyzdžiui, paryškintos žodyje $cabbaccac$ raidės c įeitis yra $(c, 3)$. Užrašą (x, i) skaitome: *i-oji x įeitis žodyje u*. Raidės įeitis apibendrinama ir žodžių atveju. Pavyzdžiui, žodyje $cabbaabab$ yra trys žodžio ab įeitys.

1.6 apibrėžimas. *Žodis u vadinamas žodžio uv pradžia, o v – jo pabaiga.*

Tarkime, kad abėcėlė A yra baigtinė aibė. Visų galimų abėcėlės A žodžių aibę žymėsime A^*. Pavyzdžiui, jei $A = \{a\}$, tai $A^* = \{a, aa, aaa, \ldots\}$.

1.5 teorema. *Baigtinės abėcėlės $A = \{a_1, \ldots, a_m\}$ visų žodžių aibė A^* yra skaičioji.*

Įrodymas. Abėcėlėje A fiksuojame kurią nors visišką tvarką. Po to kiekvienai raidei priskiriame po vieną skirtingą skaičių nuo 1 iki m. Tarkime, tas skaičius sutampa su raidės indeksu: $a_1, a_2, a_3, \ldots, a_m$. Nurodysime taisyklę, pagal kurią rašysime seka visus aibės A^* elementus. Visų pirma, laikydamiesi įvestos tvarkos, surašome visus vienetinio ilgio žodžius, po to visus skirtingus žodžius, kurių ilgis lygus 2, dar po to visus skirtingus žodžius, kurių ilgis lygus 3, ir t.t. Jei du žodžiai $b = a_{i_1}, \ldots, a_{i_n}$ ir $c = a_{j_1}, \ldots, a_{j_n}$ yra vienodo ilgio ir $i_1 < j_1$, tai b sekoje aptinkamas anksčiau negu c, o jei $i_1 > j_1$, tai anksčiau aptinkamas c. Jei $a_{i_1} = a_{j_1}, \ldots, a_{i_s} = a_{j_s}, a_{i_{s+1}} \neq a_{j_{s+1}}$ ir $i_{s+1} < j_{s+1}$, tai b sekoje pasitaiko anksčiau negu c, o jei $i_{s+1} > j_{s+1}$, tai anksčiau pasitaiko c.

Seka atrodo šitaip:

$a_1, \dots, a_m, a_1a_1, \dots, a_1a_m, a_2a_1, a_2a_2, \dots, a_2a_m, \dots, a_ma_1, a_ma_2, \dots,$
$a_ma_m, a_1a_1a_1, a_1a_1a_2, \dots, a_1a_1a_m, \dots .$

Toks žodžių išdėstymas dar vadinamas ***leksikografine tvarka***. Teorema įrodyta.

1.6 teorema. *Atvirojo intervalo* (0,1) *visų realiųjų skaičių aibė nėra skaičioji.*

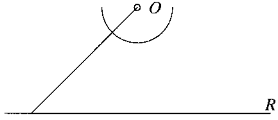
Įrodymas. Tarkime, kad aibė yra skaičioji. Tuomet jos elementus galima užrašyti sekos pavidalu:

$$\begin{array}{c} 0, a_1^1a_2^1a_3^1\dots \\ 0, a_1^2a_2^2a_3^2\dots \\ 0, a_1^3a_2^3a_3^3\dots \\ \dots \end{array}$$

čia $0 \leqslant a_j^i \leqslant 9$ $(i, j \geqslant 1)$ – skaitmenys, i-ajam sekos skaičiui (iš viršaus į apačią) priskiriame natūralųjį i.

Nagrinėjame skaičių $0, b_1b_2b_3\dots$, kurio skaitmuo b_i tenkina sąlygas: $0 < b_i < 9$ ir $b_i \neq a_i^i$. Skaičius priklauso intervalui $(0, 1)$, bet jo aprašytoje sekoje nėra. Taigi neegzistuoja abipusiškai vienareikšmės atitikties tarp natūraliųjų skaičių aibės ir atvirojo intervalo $(0, 1)$ visų realiųjų skaičių aibės. Teorema įrodyta.

Atvirojo intervalo $(0, 1)$ visų realiųjų skaičių aibė ekvivalenti realiųjų skaičių aibei. Abipusiškai vienareikšmę atitiktį gauname transformavę atkarpą į pusapskritimį:



1.7 apibrėžimas. *Aibė, ekvivalenti realiųjų skaičių aibei, vadinama* ***kontinuumo galios aibe***.

Tarkime, duota kuri nors aibė A. Aibę, kurios elementai yra visi galimi A poaibiai, vadiname aibės A poaibių aibe ir žymime $P(A)$.

Pavyzdžiai:

1. $A = \{2, 3\}$. Tuomet $P(A) = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\}$.
2. $A = \emptyset$. Tuomet $P(A) = \{\emptyset\}$.

Jei baigtinėje aibėje yra n elementų, tai aibėje $P(A)$ bus 2^n elementų, t.y. daugiau negu aibėje A. Įdomu, kad analogiškas tvirtinimas teisingas ir begalinėms aibėms. Aibė $P(A)$ yra gausesnė už aibę A.

1.7 teorema. *Bet kurios aibės A poaibių aibė $P(A)$ nėra ekvivalenti jokiai $A_0 \subset A$.*

Įrodymas. Tai akivaizdu turint baigtines aibes. Tarkime, A yra kuri nors begalinė aibė. Tada atsiras toks A poaibis A_0, kad $P(A) \sim A_0$. Taigi tarp aibės A_0 elementų ir $P(A)$ elementų (A poaibių) egzistuoja abipusiškai vienareikšmė atitiktis. Aibę B formuojame atsižvelgdami į reikalavimą, kad elementas a iš A_0 priklauso aibei B tada ir tiktai tada, kai jis nėra jį atitinkančios (pagal nurodytą abipusiškai vienareikšmę atitiktį) aibės iš $P(A)$ elementas.

B tenkina sąlygą $B \subset A_0 \subset A$ ir todėl $B \in P(A)$. Remiantis prielaida, aibėje A_0 atsiras jį atitinkantis elementas (pažymėkime jį raide b). Klausiama, ar $b \in B$. Pagal aibės B konstravimą, $b \in B$ tada ir tiktai tada, kai $b \notin B$. Gavome prieštarą. Teorema įrodyta.

Dvi aibės lygios, jei jas sudaro tie patys elementai. Kai kada mums svarbu ir vienodų elementų skaičius. Pavyzdžiui, aibes $A = \{a, b\}$ ir $B = \{a, a, b\}$ norime laikyti skirtingomis. Tuo atveju jas vadiname ***multiaibėmis***.

1.2 Pagrindinės grafų sąvokos

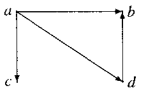
Grafu vadiname aibių porą (V, L). Čia V yra kuri nors netuščia aibė, vadinama *viršūnių* aibe, o L – multiaibė, vadinama grafo *lankų* aibe. Jos elementai yra poros (v, u), $v, u \in V$. Jei aibės V, L baigtinės, tai ir grafas vadinamas baigtiniu. Priešingu atveju – jis begalinis.

Sakoma, kad lankas $l = (v, u)$ jungia viršūnes v, u. Viršūnė v vadinama lanko *pradžia*, o u – *pabaiga*. Jos vadinamos *gretimomis*. Sakoma, kad viršūnė v ir lankas l, taip pat u ir l yra *incidentiniai*. Kadangi L yra multiaibė, tai joje gali būti ne viena pora (u, v). Tuomet lankas l vadinamas *kartotiniu*. Jei $v \in V$ ir aibėje L nėra lanko pavidalo (u, v) ar (v, u), tai viršūnė v vadinama *izoliuotąja*. Lankas pavidalo (v, v) vadinamas *kilpa*.

Grafo realizacija plokštumoje vadiname kurią nors geometrinę schemą (brėžinį), kurioje viršūnės pažymėtos taškais (vienintelis reikalavimas, kad skirtingas viršūnes atitiktų skirtingi taškai). Lankas (v, u) žymimas kuria nors kreive, jungiančia viršūnes v, u. Lankas negali eiti per kitas viršūnes. Kad galėtumėme brėžinyje atskirti, kuri viršūnė yra grafo pradžia, o kuri pabaiga, būtina nurodyti kryptį. Nagrinėjamieji grafai vadinami *orientuotaisiais grafais*. Grafas turi daug skirtingų realizacijų. Schemos, kurios yra to paties grafo realizacijos, vadinamos *izomorfinėmis*.

Pavyzdys

$$V = \{a, b, c, d\}, \qquad L = \{(a, b), (a, c), (a, d), (d, b)\}.$$



Keliu iš viršūnės v_{i_1} į v_{i_n} vadiname baigtinę lankų seką

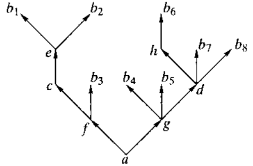
$$(v_{i_1}, v_{i_2}), (v_{i_2}, v_{i_3}), \ldots, (v_{i_{n-2}}, v_{i_{n-1}}), (v_{i_{n-1}}, v_{i_n}).$$

Jei $v_{i_1} = v_{i_n}$, tai toks kelias vadinamas *ciklu*. Kelias gali būti nurodomas ir viršūnių seka $v_{i_1}, v_{i_2}, \ldots, v_{i_n}$. Jis gali būti ir begalinis.

Nagrinėsime ir neorientuotus grafus $G = (V, B)$. Nenurodysime lanko krypties. Toks lankas be krypties vadinamas *briauna*. Taigi neorientuotas grafas yra dviejų aibių viršūnių ir briaunų pora. Jei $(u, v) \in B$, tai galima tiek iš viršūnės u patekti į v, tiek iš v patekti į u.

Neorientuotas be kilpų ir be kartotinių briaunų grafas vadinamas *medžiu*, arba *medžio pavidalo grafu*, jei jame nėra ciklų.

Medžio sąvoka taikoma ir orientuotiesiems grafams. Panaikinus kryptį, grafas tampa neorientuotu medžio pavidalo grafu. Pavyzdžiui,



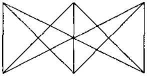
Viršūnė a vadinama *šaknimi*, o viršūnės $b_1, \ldots, b_8$ — *galinėmis viršūnėmis*, arba *lapais*.

Toliau vadovėlyje nagrinėjami medžiai, kurių viršūnės žymimos sudėtingesniais reiškiniais — formulėmis. Tuomet lanką patogiau žymėti horizontaliu brūkšniu. Aprašytasis medis (kai grafas orientuotas, kryptis – iš apačios į viršų) atrodo šitaip:

$$\dfrac{\dfrac{\dfrac{\dfrac{b_1 \quad b_2}{e}}{c} \quad b_3}{f} \qquad \dfrac{b_4 \quad b_5 \quad \dfrac{\dfrac{b_6}{h} \quad b_7 \quad b_8}{d}}{g}}{a}.$$

Jei dvimatėje erdvėje (plokštumoje) galima rasti tokią grafo realizaciją, kurioje briaunos (lankai), išskyrus viršūnes, neturi bendrų taškų, tai grafas vadinamas *plokščiuoju*.

Neplokščias grafas (jis vadinamas $K_{3,3}$) atrodo šitaip:



1.3 Pratimai

1. Raskite visų galimų aibės A poaibių aibę, kai:

   a) $A = \{a, b, c\}$,

   b) $A = \{\emptyset, \{\emptyset\}\}$.

2. Ar $A \times B = B \times A$?

3. Įrodykite, kad aibės $(A \cup B) \cap A$, $(A \cap B) \cup A$ yra lygios.

4. Įrodykite: jei A yra baigtinė aibė, B – skaičioji, tai $A \cup B$ yra skaičioji aibė.

5. Įrodykite, kad pirminių skaičių aibė yra skaičioji.

6. Įrodykite, kad visų sveikųjų dvejetainių skaičių aibė yra skaičioji.

7. Įrodykite, kad binariojo medžio visų baigtinių kelių, prasidedančių šaknyje, aibė yra skaičioji.

2 skyrius
Teiginių kalba

2.1 Loginės operacijos

Kai kurios sąvokos (*aibė, taškas,* ...) matematikoje yra *pirminės*. Jos neapibrėžiamos, o paaiškinamos. Tokia sąvoka logikoje yra *teiginys*.

Teiginiu vadiname sakinį, kurio atžvilgiu prasmingas klausimas, teisingas jis ar klaidingas.

Pavyzdžiui: *Jonukas gerai mokosi, Vilnius yra Lietuvos sostinė, Sausis – šalčiausias metų mėnuo.*

Teiginius žymime raidėmis p, q, r, s, taip pat su indeksais: $p_0, q_0, r_0, s_0, p_1, q_1, r_1, s_1, \ldots$. Ne visi sakiniai yra teiginiai. Pavyzdžiui: *Kelinta valanda*? *Šlovė mokslui*! Ne visada galima pasakyti, ar teiginys teisingas, ar klaidingas. Tai gali būti neišspręstų problemų formulavimai arba, pavyzdžiui, nežinomi tvirtinimai apie praeitį bei ateitį.

Jei teiginys p teisingas, sakome, kad teiginio p ***vertė*** lygi t ir žymime $p = t$. Jei teiginys klaidingas, sakome, kad teiginio ***vertė*** lygi k ir žymime $p = k$.

Apibrėšime šias logines operacijas: neigimą, konjunkciją, disjunkciją, griežtąją disjunkciją, implikaciją, ekvivalentumą, o vėliau ir Shefferio funkciją.

Logines operacijas pritaikę teiginiams, gauname sudėtinius teiginius.

Neigimas žymimas simboliu $\neg$ (pvz., $\neg p$, $\neg q$). Literatūroje dar vartojami simboliai $\bar{}$ (pvz., $\bar{p}, \bar{q}, \ldots$) bei $\sim$ (pvz., $\sim p, \sim q, \ldots$). Užrašą $\neg p$ skaitome: „ne p“, „netiesa, kad p“. Sudėtinio teiginio $\neg p$ vertė priešinga teiginio p vertei: jei teiginio p vertė lygi k, tai teiginio $\neg p$ vertė lygi t, o jei teiginio p vertė yra k, tai teiginio $\neg p$ vertė yra t. Visa tai patogu užrašyti lentele:

p	$\neg p$
t	k
k	t

Konjunkcija žymima simboliu & (dar vartojami simboliai $\wedge$, $\cdot$). Užrašą $p\&q$ skaitome „p ir q“. Konjunkcija nusakoma lentele:

p	q	$p\&q$
t	t	t
t	k	k
k	t	k
k	k	k

Sudėtinis teiginys $p\&q$ teisingas tada ir tiktai tada, kai abu teiginiai p, q teisingi.

Disjunkcija žymima simboliu $\vee$. Užrašą $p \vee q$ skaitome „p arba q“. Disjunkcija nusakoma lentele:

p	q	$p \vee q$
t	t	t
t	k	t
k	t	t
k	k	k

Sudėtinis teiginys $p \vee q$ klaidingas tada ir tiktai tada, kai abu teiginiai p, q klaidingi.

Griežtoji disjunkcija žymima simboliu $\dot{\vee}$ (taip pat $+$, $\oplus$). Užrašą $p\dot{\vee}q$ skaitome „arba p, arba q“. Griežtoji disjunkcija nusakoma lentele:

p	q	$\dot{\vee}$
t	t	k
t	k	t
k	t	t
k	k	k

Sudėtinis teiginys $p\dot{\vee}q$ teisingas tada ir tiktai tada, kai teisingas tik vienas iš teiginių p ir q.

Implikacija žymima $\to$ ($\supset$, $\Rightarrow$). Užrašą $p \to q$ skaitome „jei p, tai q“ arba „iš p išplaukia q“. Terminas „iš p seka q“ (autoriaus nuomone) taip pat vartotinas, nes, kaip matysime vėliau, logikoje tokio sakinio teisingumas dažnai siejamas su ***seka*** formulių, tenkinančių tam tikras sąlygas.

Implikacija nusakoma lentele:

p	q	$p \to q$
t	t	t
t	k	k
k	t	t
k	k	t

Sudėtinis teiginys $p \rightarrow q$ klaidingas tada ir tiktai tada, kai teiginys p teisingas, o teiginys q klaidingas. Pasistengsime pateisinti tokią teisingumo lentelę. Matematikoje aptinkami sakiniai pavidalo „ jei p, tai q" laikomi teisingais, jei kiekvieną kartą, kai p teisingas, q taip pat yra teisingas. Kai p klaidingas, q gali įgyti bet kurią vertę. Pavyzdžiui, sakinys „jei $x < y$ ir $y < z$, tai $x < z$" laikomas teisingu bet kurioms x, y, z reikšmėms. Galima parinkti tokius natūraliuosius x, y, z, kad tvirtinimas „$x < y$ ir $y < z$" (t.y. p) būtų klaidingas, o „$x < z$" (t.y. q) vienu atveju būtų teisingas, kitu klaidingas, bet nėra tokių x, y, z, kad p būtų teisingas, o q klaidingas.

Ekvivalentumas žymimas $\leftrightarrow$ ($\Leftrightarrow$). Užrašą $p \leftrightarrow q$ skaitome „p ekvivalentus q", arba „p ir q ekvivalentūs".

Ekvivalentumas nusakomas lentele:

p	q	$p \leftrightarrow q$
t	t	t
t	k	k
k	t	k
k	k	t

Kaip matome, į teiginius žiūrime kaip į kintamuosius, kurių kitimo sritis yra aibė $\{t, k\}$. Tokie kintamieji dažniausiai vadinami *teigininiais kintamaisiais*. Mes juos vadinsime taip, kaip tokio tipo kintamuosius įprasta vadinti informatikoje – ***loginiais kintamaisiais***. Sudėtinių teiginių sąvoką pakeisime tikslesne – formulės sąvoka, o užuot vartoję terminą *vertė*, kaip ir įprasta kintamųjų atveju, vartosime terminą *reikšmė*. Kai kada bus patogu loginių kintamųjų kitimo sritimi laikyti aibę $\{1, 0\}$, t.y. t keisime 1, o k keisime 0. Dažniausiai mums net nesvarbu, kokia yra aibė, o naudojamės tik tuo, kad ją sudaro du elementai.

Formules žymėsime didžiosiomis lotyniškomis raidėmis A, B, C, ..., F, ..., kai kada su indeksais ar brūkšneliais.

2.1 apibrėžimas:

1. *Loginis kintamasis yra formulė.*
2. *Jei F yra formulė, tai $\neg F$ – taip pat formulė.*
3. *Jei F, G yra formulės, tai $(F \& G)$, $(F \vee G)$, $(F \dot{\vee} G)$, $(F \rightarrow G)$, $(F \leftrightarrow G)$ – taip pat formulės.*

Formulių pavyzdžiai:

$$((p \dot{\vee} q) \rightarrow \neg(\neg p \vee q)), \quad \neg p, \quad ((p_1 \leftrightarrow p_2) \vee \neg\neg(p_1 \& (p_3 \vee \neg p_1))).$$

Kad būtų paprasčiau, išorinių skliaustų formulėse nerašysime. Iš apibrėžimo išplaukia, kad kiekvienai formulei, jei ji nėra loginis kintamasis, arba atsiras tokia formulė G, kad F bus pavidalo $\neg G$ (tuo atveju rašysime $F = \neg G$ arba F: $\neg G$), arba atsiras dvi tokios formulės G, H, kad $F = G\alpha H$ ($\alpha \in \{\&, \vee, \dot{\vee}, \rightarrow, \leftrightarrow\}$). Pirmuoju atveju ***pagrindine formulės F logine operacija*** vadiname $\neg$, o antruoju – α.

Pavyzdžiai:

1. Formulės $(p \rightarrow q)\&(q \vee \neg(q \rightarrow p))$ pagrindinė loginė operacija yra &.
2. Formulės $\neg((p \rightarrow q) \vee (\neg q \rightarrow \neg p))$ pagrindinė loginė operacija yra $\neg$.

2.2 apibrėžimas:

1. *Formulė F yra F poformulis.*
2. *Jei $F = \neg G$, tai formulė G ir visi G poformuliai yra ir F poformuliai.*
3. *Jei $F = G\alpha H$ ($\alpha \in \{\&, \vee, \dot{\vee}, \rightarrow, \leftrightarrow\}$), tai formulės G, H bei jų poformuliai yra ir F poformuliai.*

Kai kada formulės žymimos $F(p_1, \ldots, p_n)$. Tuo atveju $p_1, \ldots, p_n$ yra pilnas sąrašas skirtingų loginių kintamųjų, kurie yra formulės F poformuliai.

Pavyzdžiai:

1. Jei F yra $(p \rightarrow \neg p) \vee \neg\neg p$, tai $F = F(p)$.
2. Jei F yra $(p \vee q) \rightarrow (\neg r \vee p)$, tai $F = F(p, q, r)$.

Skirsime poformulio ir ***poformulio įeities*** sąvokas. Formulė yra tam tikros abėcėlės žodis. Todėl nagrinėdami poformulį, užuot sakę *žodžio įeitis*, vartosime sąvoką *poformulio įeitis*.

Pavyzdžiai:

- Formulėje

$$F = (\mathbf{p\&\neg q}) \rightarrow (\neg(\mathbf{p\&\neg q}) \vee ((q \rightarrow (\mathbf{p\&\neg q}))\dot{\vee}(\neg p\&(\mathbf{p\&\neg q}))))$$

yra 4 poformulio $p\&\neg q$ įeitys (jos paryškintos) – pirmoji, antroji, trečioji ir ketvirtoji (iš kairės į dešinę). Šioje formulėje yra 5 poformulio q įeitys.

- Formulės $(p \to \neg q)\&\neg(q \vee (p \vee \neg r))$ poformuliai yra:

$$(p \to \neg q)\&\neg(q \vee (p \vee \neg r)), \quad p \to \neg q, \quad \neg(q \vee (p \vee \neg r)),$$

$$p, \quad \neg q, \quad q, \quad q \vee (p \vee \neg r), \quad (p \vee \neg r), \quad \neg r, \quad r.$$

Panašiai suprantamos ir loginių operacijų ar skliaustų įeitys.

2.2 Ekvivalenčiosios formulės

2.3 apibrėžimas. *Loginių kintamųjų aibės* $\{p_1, \ldots, p_n\}$ ***interpretacija*** *vadiname kurią nors funkciją* v *su apibrėžimo sritimi* $\{p_1, \ldots, p_n\}$ *ir reikšmėmis iš* $\{t, k\}$.

Turėdami aibės $\{p_1, \ldots, p_n\}$ $(v(p_i) = \beta_i$ $(\beta_i \in \{t, k\}))$ interpretaciją v, galime apskaičiuoti formulės $F(p_1, \ldots, p_n)$ reikšmę. Skaičiuodami naudojamės loginių operacijų apibrėžimo lentelėmis. Skliaustai nurodo operacijų atlikimo tvarką. Jei formulės reikšmė lygi β $(\beta \in \{t, k\})$, tai rašome $v(F) = \beta$, arba tiesiog $F = \beta$. Jei formulę sudaro n skirtingų loginių kintamųjų, tai yra 2^n skirtingų interpretacijų.

Sudarysime formulės $\neg p \to (p\&(q \vee \neg r))$ ***teisingumo lentelę*** (apskaičiuosime formulės reikšmes esant visoms galimoms interpretacijoms).

p	q	r	$\neg p$	$\neg r$	$q \vee \neg r$	$p\&(q \vee \neg r)$	$\neg p \to (p\&(q \vee \neg r))$
t	t	t	k	k	t	t	t
t	t	k	k	t	t	t	t
t	k	t	k	k	k	k	t
t	k	k	k	t	t	t	t
k	t	t	t	k	t	k	k
k	t	k	t	t	t	k	k
k	k	t	t	k	k	k	k
k	k	k	t	t	t	k	k

2.4 apibrėžimas. *Dvi formules* $F(p_1, \ldots, p_n)$, $G(p_1, \ldots, p_n)$ *vadiname* ***ekvivalenčiosiomis*** *(rašome* $F(p_1, \ldots, p_n) \equiv G(p_1, \ldots, p_n)$*), jei su bet kuria interpretacija* v *galioja lygybė* $v(F) = v(G)$.

Atkreipiame dėmesį, kad ekvivalentumas $\equiv$ nėra loginė operacija. Ekvivalenčių formulių pavyzdžiai:

$$p\&q \equiv q\&p,$$
$$p\&(q\&r) \equiv (p\&q)\&r,$$
$$p \vee q \equiv q \vee p,$$
$$p \vee (q \vee r) \equiv (p \vee q) \vee r,$$
$$\neg\neg p \equiv p,$$
$$p \vee q \equiv \neg p \to q,$$
$$p \dot{\vee} q \equiv (p \vee q)\&\neg(p\&q).$$

Naudodamiesi antrąja ir ketvirtąja poromis ekvivalenčių formulių, kai jos yra pavidalo $F_1\&\ldots\&F_n$ arba $F_1 \vee \ldots \vee F_n$, skliaustus praleidžiame, nes tokių formulių reikšmės nuo suskliaudimo tvarkos nepriklauso. Aprašytųjų formulių ekvivalentumas tikrinamas sudarant jų teisingumo lenteles. Pavyzdžiui, parodysime, kad $p \vee q \equiv \neg p \to q$.

p	q	$\neg p$	$p \vee q$	$\neg p \to q$
t	t	k	t	t
t	k	k	t	t
k	t	t	t	t
k	k	t	k	k

Kaip matome, stulpelių, atitinkančių $p \vee q$ ir $\neg p \to q$, reikšmės sutampa. Kai kuriomis ekvivalenčių formulių poromis mes dažnai naudosimės. Išvardysime jas ir sunumeruosime:

$$p \to q \equiv \neg p \vee q, \tag{2.1}$$

$$\neg(p\&q) \equiv \neg p \vee \neg q, \tag{2.2}$$

$$\neg(p \vee q) \equiv \neg p\&\neg q, \tag{2.3}$$

$$p \leftrightarrow q \equiv (p \to q)\&(q \to p), \tag{2.4}$$

$$(p\&q) \vee r \equiv (p \vee r)\&(q \vee r), \tag{2.5}$$

$$(p \vee q)\&r \equiv (p\&r) \vee (q\&r). \tag{2.6}$$

Ekvivalenčių formulių savybės:

1. Jei $A \equiv B$, tai ir $B \equiv A$.

2. Jei $A \equiv B$ ir $B \equiv C$, tai ir $A \equiv C$.

3. $A \equiv B$ tada ir tiktai tada, kai $\neg A \equiv \neg B$.

Ekvivalentumo sąvoką apibendrinsime tuo atveju, kai formulėse yra ne tik vienodi loginiai kintamieji.

2.5 apibrėžimas. *Dvi formulės* $A(p_1, \ldots, p_n, q_1, \ldots, q_s)$ *ir* $B(p_1, \ldots, p_n, r_1, \ldots, r_u)$ *vadinamos* ***ekvivalenčiosiomis****, jei su bet kuria aibės* $\{p_1, \ldots, p_n, q_1, \ldots, q_s, r_1, \ldots, r_u\}$ *interpretacija* ν *galioja lygybė* $\nu(A) = \nu(B)$.

Pavyzdžiai:

1. $p \vee (q \& \neg q) \equiv \neg\neg p \vee (r \& \neg r)$.
2. $(p \& q) \to (\neg p \vee q) \equiv p \to p$.

Jei formulės $A(p_1, \ldots, p_n, q_1, \ldots, q_s)$ ir $B(p_1, \ldots, p_n)$ yra ekvivalenčios, tai loginiai kintamieji $q_1, \ldots, q_s$ formulėje A vadinami *fiktyviaisiais*. Pateiksime dar vieną fiktyviojo loginio kintamojo apibrėžimą.

2.6 apibrėžimas. *Kintamasis* p_i *formulėje* $A(p_1, \ldots, p_{i-1}, p_i, p_{i+1}, \ldots, p_n)$ *vadinamas* ***fiktyviuoju****, jei su bet kuria aibės* $\{p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n\}$ $(\nu(p_j) = \beta_j)$ *interpretacija* ν *galioja lygybė*

$$\nu(A(\beta_1, \ldots, \beta_{i-1}, t, \beta_{i+1}, \ldots, \beta_n)) = \nu(A(\beta_1, \ldots, \beta_{i-1}, k, \beta_{i+1}, \ldots, \beta_n)).$$

Priešingu atveju p_i *vadinamas* ***esminiu****.*

Tarkime, A yra formulės F poformulis. Pažymėkime $F(B/A)$ formulę, gautą formulėje F visas A įeitis pakeitus formule B.

2.1 teorema. *Jei* $A(p_1, \ldots, p_n)$ *yra formulės* F *poformulis ir* $A(p_1, \ldots, p_n) \equiv B(p_1, \ldots, p_n)$, *tai* $F \equiv F(B/A)$.

Įrodymas. Sudarykime F teisingumo lentelę taip, kad iš pradžių joje būtų apskaičiuojamos A reikšmės (prieš tai apskaičiuojant A poformulių reikšmes, t.y. formulių, reikalingų nustatyti A reikšmę). Analogiškai sudarykime $F(B/A)$ teisingumo lentelę taip, kad iš pradžių būtų apskaičiuojamos B reikšmės. Tada F ir $F(B/A)$ teisingumo reikšmės gali skirtis tik iki stulpelių A, B, o visos reikšmės, esančios tų stulpelių dešinėje, sutampa. Tuo pačiu sutampa ir formulių F bei $F(B/A)$ reikšmės. Teorema įrodyta.

Išvados:

1. Jei $A(p_1, \ldots, p_n, q_1, \ldots, q_s)$ yra formulės F poformulis ir $A(p_1, \ldots, p_n, q_1, \ldots, q_s) \equiv B(p_1, \ldots, p_n, r_1, \ldots, r_u)$, tai $F \equiv F(B/A)$.

2. Tarkime, A yra F poformulis ir $A \equiv B$. Kai kurias A įeitis pakeitę formule B, gauname formulę, ekvivalenčią F.

3. Jei $F(p_1, \dots, p_n) \equiv G(p_1, \dots, p_n)$ ir $A_1, \dots, A_n$ yra bet kokios formulės, tai ir $F(A_1/p_1, \dots, A_n/p_n) \equiv G(A_1/p_1, \dots, A_n/p_n)$.

Panašiai kaip ir 2.1 teorema, visos išvados įrodomos nagrinėjant atitinkamų formulių teisingumo lenteles.

2.7 apibrėžimas. *Loginių operacijų aibė E vadinama* ***pilnąja****, jei kiekvienai formulei galima rasti ekvivalenčią, kurioje yra tik loginės operacijos iš aibės E.*

2.2 teorema. *Aibės* $\{\neg, \&\}$, $\{\neg, \vee\}$, $\{\neg, \rightarrow\}$ *yra pilnosios.*

Įrodymas. 1. Nagrinėkime $\{\neg, \&\}$. Įrodysime, kad ji pilna. Remiantis 2.1 teorema bei išvadomis, pakanka parodyti, kad formulėms $p \vee q$, $p \dot{\vee} q$, $p \rightarrow q$, $p \leftrightarrow q$ galima rasti ekvivalenčias, kuriose yra tik loginės operacijos iš $\{\neg, \&\}$. Jas randame naudodamiesi tik aprašytomis ekvivalenčių formulių poromis bei jų savybėmis:

$$p \vee q \equiv \neg(\neg p \& \neg q),$$

$$p \dot{\vee} q \equiv (p \vee q) \& \neg(p \& q) \equiv \neg(\neg p \& \neg q) \& \neg(p \& q),$$

$$p \rightarrow q \equiv \neg p \vee q \equiv \neg(p \& \neg q),$$

$$p \leftrightarrow q \equiv (p \rightarrow q) \& (q \rightarrow p) \equiv \neg(p \& \neg q) \& \neg(q \& \neg p).$$

2. Nagrinėkime $\{\neg, \vee\}$:

$$p \& q \equiv \neg(\neg p \vee \neg q),$$

$$p \dot{\vee} q \equiv (p \vee q) \& \neg(p \& q) \equiv \neg(\neg(p \vee q) \vee \neg(\neg p \vee \neg q)),$$

$$p \rightarrow q \equiv \neg p \vee q,$$

$$\begin{aligned} p \leftrightarrow q &\equiv (p \rightarrow q) \& (q \rightarrow p) \equiv (\neg p \vee q) \& (\neg q \vee p) \\ &\equiv \neg(\neg(\neg p \vee q) \vee \neg(\neg q \vee p)). \end{aligned}$$

3. Nagrinėkime $\{\neg, \rightarrow\}$:

$$p \vee q \equiv \neg p \rightarrow q,$$

$$p \& q \equiv \neg(\neg p \vee \neg q) \equiv \neg(p \rightarrow \neg q),$$

$$\begin{aligned} p \dot{\vee} q &\equiv (p \vee q) \& \neg(p \& q) \equiv (\neg p \rightarrow q) \& (p \rightarrow \neg q) \\ &\equiv \neg((\neg p \rightarrow q) \rightarrow \neg(p \rightarrow \neg q)), \end{aligned}$$

$$p \leftrightarrow q \equiv (p \to q)\&(q \to p) \equiv \neg((p \to q) \to \neg(q \to p)).$$

Teorema įrodyta.

Yra ir kiti pilni loginių operacijų poaibiai, pavyzdžiui, $\{\dot{\vee}, \to\}$. Bet visuose juose yra ne mažiau kaip du elementai. Galima rasti ir vieną tokią loginę operaciją, kuri sudarytų pilną aibę. Pirmasis tokią operaciją 1880 m. sugalvojo Ch. Peirce, bet jis neskyrė tam didelio dėmesio. Jo darbas nebuvo publikuotas, o pati operacija užmiršta. Daug vėliau, 1913 m., kitą tokią operaciją aprašė H. M. Sheffer (mes ją vadiname Shefferio funkcija). Tiesa, visoms mūsų nagrinėjamoms *loginėms operacijoms yra loginių jungčių, vartojamų šnekamojoje kalboje, atitikmenys* *ir*, *arba* ir kt. (iš čia jos ir kilusios). Atitikmenų Peirce bei Shefferio opercijoms šnekamojoje kalboje nėra.

Peirce operaciją žymėsime $\uparrow$, o Shefferio funkciją – $|$. Jos nusakomos tokiomis lentelėmis:

p	q	$p \uparrow q$
t	t	k
t	k	k
k	t	k
k	k	t

p	q	$p \mid q$
t	t	k
t	k	t
k	t	t
k	k	t

Jos sudaro pilnąsias aibes (išplaukia iš 2.2 teoremos), nes $\neg p \equiv p \uparrow q$ ir $p \vee q \equiv (p \uparrow q) \uparrow (p \uparrow q)$ bei $\neg p \equiv p \mid p$ ir $p\&q \equiv (p \mid q)|(p \mid q)$.

Logikoje yra dvi konstantos – ***tiesa*** (t) ir ***melas*** (k). Formulėse jų išreikštiniu pavidalu nepasitaiko, nes jas galima eliminuoti, t.y. rasti kitą, ekvivalenčią formulę be loginių konstantų įeičių. Remiamasi 2.1 teorema, jos išvadomis bei loginių operacijų apibrėžimais.

Pavyzdys. Eliminuokime konstantas $(p \to t)\&((t \to q) \vee (r \leftrightarrow k))$.

Kadangi $p \to t \equiv t$, $t \to q \equiv q$, $r \leftrightarrow k \equiv \neg r$, gauname ekvivalenčią formulę

$$t\&(q \vee \neg r)$$

$t\&F \equiv F$. Todėl pradinė formulė ekvivalenti $q \vee \neg r$.

Suprantama, kad neišreikštiniu pavidalu konstantos vis dėlto formulėse aptinkamos, pavyzdžiui: formulė $p \vee \neg p$ yra konstanta t, o formulė $p\&\neg p$ yra konstanta k.

Atrodytų, kad yra tam tikras loginių operacijų perteklius. Pakaktų ir mažesnio jų kiekio. Tačiau turint daugiau operacijų papraščiau formalizuoti užduotis. Dažniausiai klasikinėje matematinėje logikoje nagrinėjamos formulės, kuriose yra tik keturios loginės operacijos $\neg$, $\&$, $\vee$, $\to$. Prisilaikysime ir mes tos tradicijos, išskyrus keletą skyrelių.

2.3 Loginės išvados

Įvesime formulių klasifikaciją. Bet kuri formulė gali būti tapačiai teisinga, tapačiai klaidinga ar įvykdoma.

Kai kalbama apie kurios nors formulės interpretaciją, tai suprantama, kad jos apibrėžimo aibė yra visi įeinantys į nagrinėjamąją formulę loginiai kintamieji, ir nebūtina jos nurodyti. Poformulį A formulėje F pakeitę B, žymime $F(B/A)$. Tuo atveju, kai formulėje $F(p_1, \ldots, p_n)$ visas loginių kintamųjų įeitis keičiame kuriomis nors formulėmis $A_1, \ldots, A_n$, tai, užuot rašę $F(A_1/p_1, \ldots, A_n/p_n)$, dažniausiai žymėsime $F(A_1, \ldots, A_n)$.

2.8 apibrėžimas. *Formulė F vadinama **tapačiai teisinga**, jei su bet kuria interpretacija ν teisinga lygybė $\nu(F) = t$.*

Tapačiai teisingos formulės dar vadinamos ***tautologijomis***, arba ***logikos dėsniais***. Jų vaidmuo logikoje ypač svarbus, nes daugumos uždavinių sprendimą pavyksta suvesti į kurios nors formulės tapataus teisingumo nustatymą. Tapačiai teisingų formulių pavyzdžiai:

$$\begin{gathered}
\neg\neg p \to p, \\
(p \& q) \to p, \\
(p \to q) \to (\neg q \to \neg p), \\
p \to (p \vee q).
\end{gathered}$$

Norint patikrinti, ar formulė $A(p_1, \ldots, p_n)$ yra tapačiai teisinga, pakanka sudaryti jos teisingumo lentelę ir pažiūrėti, ar paskutiniame stulpelyje yra vien tik reikšmės t. Bet sudarant teisingumo lentelę reikia apskaičiuoti formulės A reikšmes, esant 2^n interpretacijų. Tai labai greitai auganti funkcija, todėl praktiškai galima naudotis teisingumo lentele ir formulės tapatų teisingumą nustatyti tik nedideliems n.

2.3 teorema. *Tarkime, $F(p_1, \ldots, p_n)$ yra tapačiai teisinga formulė, $A_1, \ldots, A_n$ – bet kurios formulės. Tuomet $F(A_1, \ldots, A_n)$ yra tapačiai teisinga formulė.*

Įrodymas. Visiems loginiams kintamiesiems, įeinantiems į $A_1, \ldots, A_n$, priskirkime bet kurias reikšmes. Tarkime, kad esant toms reikšmėms $A_1 = \alpha_1, \ldots, A_n = \alpha_n$; čia $\alpha_i \in \{t, k\}$ $(1 \leqslant i \leqslant n)$. Tada formulės $F(A_1, \ldots, A_n)$ reikšmė, esant toms pačioms loginių kintamųjų reikšmėms, sutampa su $F(\alpha_1, \ldots, \alpha_n)$. Kadangi $F(p_1, \ldots, p_n)$ reikšmė su bet kokiomis loginių kintamųjų $p_1, \ldots, p_n$ reikšmėmis lygi t, tai ji lygi t ir kai $p_1 = \alpha_1, \ldots, p_n = \alpha_n$. Teorema įrodyta.

2.9 apibrėžimas. *Formulė F vadinama **tapačiai klaidinga**, jei su bet kuria interpretacija v teisinga lygybė $v(F) = k$.*

Tapačiai klaidingų formulių pavyzdžiai:

$$p\&\neg p,$$
$$\neg((p\&q) \to p),$$
$$(p \to q)\&\neg((q \to r) \to (p \to r)).$$

Tapačiai klaidingų formulių savybės:

1. F tapačiai klaidinga tada ir tiktai tada, kai $\neg F$ tapačiai teisinga formulė.
2. Jei F tapačiai klaidinga formulė, o G – bet kuri formulė, tai $F \to G$ yra tapačiai teisinga formulė.
3. Tapačiai klaidingų bei tapačiai teisingų formulių visi loginiai kintamieji yra fiktyvūs.

2.10 apibrėžimas. *Formulė F vadinama **įvykdomąja**, jei yra tokia interpretacija v, su kuria $v(F) = t$.*

Iš apibrėžimo išplaukia, kad kiekviena tapačiai teisinga formulė kartu yra ir įvykdoma. Suprantama, yra įvykdomų formulių, kurios nėra tapačiai teisingos. Pavyzdžiui: $p \to q$, $p \to (p\&q)$, $p \leftrightarrow \neg q$.

2.11 apibrėžimas. *Sakome, kad formulė F yra formulių aibės $A = \{F_1, \ldots, F_n\}$ **loginė išvada**, jei su bet kuria interpretacija v, su kuria visos aibės A formulės teisingos, teisinga yra ir F, t.y. $v(F) = t$.*

Dažniausiai aibės A formulės vadinamos *prielaidomis*, arba *tai, kas duota*. Formulė F vadinama *išvada, tikslu*, arba *tai, ką reikia įrodyti*. Kai kada priklausomai nuo užduoties A vadinama *žinių baze*, o F – *užklausa*. Taip pat, užuot vartojus terminą *loginė išvada*, sakoma, kad *samprotavimas teisingas*, arba *samprotavimas pagrįstas*. Žymima ir taip:

$$\frac{\begin{array}{c}F_1\\ \vdots\\ F_n\end{array}}{F}.$$

Iš apibrėžimo išplaukia, kad F yra $\{F_1, \ldots, F_n\}$ loginė išvada tada ir tiktai tada, kai $(F_1\& \ldots \&F_n) \to F$ yra tapačiai teisinga formulė.

Pavyzdžiai:

1. Jei vaikas netvarkingas, tai jis blogai mokosi. Vadinasi, jei vaikas blogai mokosi, tai jis netvarkingas.

Formalizacija. Raide n pažymėkime teiginį „Vaikas netvarkingas", o raide b – „Vaikas blogai mokosi". Tuomet

$$\frac{n \to b}{b \to n}.$$

Formulė $(n \to b) \to (b \to n)$ nėra tapačiai teisinga, nes su interpretacija $n = k$, $b = t$ ji klaidinga. Taigi iš prielaidos $n \to b$ neišplaukia $b \to n$.

2. Kiekvienas aibės A elementas nepriklauso aibei D. Jei x (bet kuris) nepriklauso aibei B, tai jis nepriklauso ir aibei C. Jei x priklauso aibei B, tai jis priklauso ir A, C sankirtai. Vadinasi, jei e yra aibės C elementas, tai jis nėra D elementas.

Formalizacija. Raide a pažymėkime teiginį „$e \in A$", raide b – „$e \in B$", raide c – „$e \in C$" ir raide d – „$e \in D$". Tuomet

$$\frac{\begin{array}{c} a \to \neg d \\ \neg b \to \neg c \\ b \to (a \& c) \end{array}}{c \to \neg d}.$$

Formulė $((a \to \neg d) \& (\neg b \to \neg c) \& (b \to (a \& c))) \to (c \to \neg d)$ yra tapačiai teisinga. Tuo galime įsitikinti sudarę teisingumo lentelę. Vadinasi, formulė $c \to \neg d$ yra duotųjų (virš brūkšnio) išvada, o samprotavimas, aprašytas užduotyje, teisingas.

2.4 Normaliosios formos

Dažniausiai nagrinėjamos ne bet kurio, o tam tikro pavidalo formulės, vadinamosios *normaliosios formos.* Skirsime dvi normaliąsias formas: *normaliąją disjunkcinę formą* (sutrumpintai žymėsime NDF) ir *normaliąją konjunkcinę formą* (žymėsime NKF). Parodysime, kad kiekvienai formulei galima rasti ekvivalenčią tiek normaliosios disjunkcinės, tiek ir normaliosios konjunkcinės formos.

2.12 apibrėžimas. *Loginį kintamąjį bei loginio kintamojo neigimą vadiname litera.*

2.13 apibrėžimas. *Literų disjunkciją $l_1 \vee l_2 \vee \ldots \vee l_v$ vadiname **disjunktu**, o skaičių v – jo ilgiu.*

2.14 apibrėžimas. *Literų konjunkciją* $l_1 \& l_2 \& \ldots \& l_v$ *vadiname* ***konjunktu****, o skaičių* v *– jo ilgiu.*

Disjunkto (konjunkto) D ilgį žymime $i(D)$.

Pavyzdžiai:

- Formulės

$$p \vee \neg q \vee \neg r, \quad \neg p_1 \vee p_2 \vee \neg p_3 \vee p_4, \quad p, \quad \neg p, \quad \neg p \vee q$$

yra disjunktai.

- Formulės

$$p \& \neg q, \quad p, \quad \neg q, \quad \neg p \& q \& \neg p \& \neg r$$

yra konjunktai.

Tarkime, kad tiek disjunktuose, tiek ir konjunktuose yra tik po vieną skirtingų literų įeitį. Naudosimės tuo, kad $l \vee l \equiv l$, $l \& l \equiv l$ (l – kuri nors litera). Pavyzdžiui, užuot nagrinėję disjunktą $p \vee p \vee \neg r \vee \neg q \vee \neg q \vee \neg r$, nagrinėsime jam ekvivalentų $p \vee \neg q \vee \neg r$.

2.15 apibrėžimas. *Formulės* ***normaliąja disjunkcine forma*** *vadiname jai ekvivalenčią formulę pavidalo* $\vee_{i=1}^{s} K_i$; *čia* K_i $(i = 1, \ldots, s)$ *– konjunktai.*

Pavyzdžiai:

- $(p \& q) \vee (p \& \neg q \& r) \vee \neg p \vee (q \& \neg p)$,
- $p \& q \& \neg r$ (šiuo atveju $s = 1$),
- $p \vee \neg q \vee \neg r$.

2.4 teorema. *Kad ir kokia būtų formulė, galima rasti jai ekvivalenčią normaliąją disjunkcinę formą.*

Įrodymas. Aprašysime du transformavimo į NDF būdus.

1. *Transformavimas į NDF naudojantis teisingumo lentele.* Tarkime, yra formulė $F(p_1, \ldots, p_n)$. Sudarome jos teisingumo lentelę. Tarkime, F nėra tapačiai klaidinga. Kiekvienai interpretacijai ν, su kuria F teisinga, priskiriame po konjunktą $l_1 \& l_2 \& \ldots \& l_n$:

$$l_i = \begin{cases} p_i, & \text{jei } \nu(p_i) = t, \\ \neg p_i, & \text{jei } \nu(p_i) = k. \end{cases}$$

Iš jos matyti, kad konjunktas, atitinkantis ν, teisingas tik su vienintele interpretacija ν. Disjunkcija tokių konjuktų ir yra NDF, ekvivalenti formulei $F(p_1, \ldots, p_n)$. Jei F tapačiai klaidinga, tai jos NDF laikysime $p_1 \& \neg p_1$.

Pavyzdys

p	q	r	$F(p,q,r)$
t	t	t	k
t	t	k	t
t	k	t	t
t	k	k	k
k	t	t	k
k	t	k	t
k	k	t	k
k	k	k	k

Ji teisinga su trimis interpretacijomis:

1) $p = q = t, r = k$,

2) $p = r = t, q = k$,

3) $p = r = k, q = t$.

Pirmajai interpretacijai priskiriame $p \& q \& \neg r$, antrajai – $p \& \neg q \& r$, trečiajai – $\neg p \& q \& \neg r$. Formulės NDF yra $(p \& q \& \neg r) \vee (p \& \neg q \& r) \vee (\neg p \& q \& \neg r)$.

2. *Transformavimas į NDF naudojantis ekvivalenčiomis formulėmis.* Transformavimo algoritmo žingsniai yra tokie:

- *Eliminavimas.* Visus poformulius pavidalo $G \to H$ (primename, kad nagrinėjame formules, kuriose yra tik loginės operacijos $\neg$, $\&$, $\vee$, $\to$) keičiame jiems ekvivalenčiais, kuriuose yra tik $\neg$, $\&$, $\vee$. Naudojamės (2.1) ekvivalentumu.

- *Neigimo įkėlimas į skliaustus.* Naudojantis (2.2), (2.3) ekvivalentumais bei $\neg\neg G \equiv G$, galima pasiekti, kad neigimas formulėje būtų tik prieš loginius kintamuosius.

- *Distributyvumo dėsnio taikymas.* Taikant (2.6) ekvivalentumą, gaunama formulė, kuri ir yra NDF.

- *Prastinimas.* Taikome ekvivalentumus $G \vee G \equiv G$, $G \& G \equiv G$, $\neg\neg G \equiv G$. Poformulius $G \& \neg G$, $G \vee \neg G$ keičiame atitinkamai konstantomis k, t ir jas eliminuojame. Prastinti galima ir po pirmojo bei antrojo žingsnių.

Teorema įrodyta.

Pavyzdys. Transformuokime $\neg(p \to q) \lor (q\&r)$ į NDF:

- eliminuojame $\to$: $\neg(\neg p \lor q) \lor (q\&r)$;
- įkeliame neigimą į skliaustus: $(p\&\neg q) \lor (q\&r)$;
- taikome distributyvumo dėsnį: $(p\&q) \lor (p\&r) \lor (\neg q\&q) \lor (\neg q\&r)$;
- prastiname ir gauname NDF: $(p\&q) \lor (p\&r) \lor (\neg q\&r)$.

2.16 apibrėžimas. *Formulės* ***normaliąja konjunkcine forma*** *vadiname jai ekvivalenčią formulę pavidalo* $\&_{i=1}^{s} D_i$; *čia* D_i $(i = 1, \ldots, s)$ *– disjunktai.*

Pavyzdžiai:

- $(p \lor \neg q)\&(p \lor \neg q \lor r)\&\neg p\&(p \lor q)$,
- $p \lor \neg q \lor \neg r$ (šiuo atveju $s = 1$),
- $p\&q\&\neg r$.

Kaip matome, pastarosios dvi formulės yra tiek normaliosios konjunkcinės, tiek ir normaliosios disjunkcinės formos.

2.5 teorema. *Kad ir kokia būtų formulė, galima rasti jai ekvivalenčią normaliąją konjunkcinę formą.*

Įrodymas. Kaip ir įrodydami 2.4 teoremą, aprašysime du transformavimo į NKF būdus.

1. *Transformavimas į NKF naudojantis teisingumo lentelėmis.* Tarkime, yra formulė $F(p_1, \ldots, p_n)$. Sudarome jos teisingumo lentelę. Be to, tarkime, kad F nėra tapačiai teisinga. Kiekvienai interpretacijai ν, su kuria F klaidinga, priskiriame po disjunktą $l_1 \lor l_2 \lor \ldots \lor l_s$:

$$l_i = \begin{cases} \neg p_i, & \text{jei} \quad \nu(p_i) = t, \\ p_i, & \text{jei} \quad \nu(p_i) = k. \end{cases}$$

Matome, kad disjunktas, atitinkantis ν, klaidingas tik su vienintele interpretacija ν. Konjunkcija tokių disjunktų ir yra NKF, ekvivalenti formulei $F(p_1, \ldots, p_n)$. Jei F tapačiai teisinga, tai jos NKF laikysime $p_1 \lor \neg p_1$.

Pavyzdys

p	q	r	$F(p,q,r)$
t	t	t	t
t	t	k	t
t	k	t	k
t	k	k	t
k	t	t	t
k	t	k	k
k	k	t	k
k	k	k	t

Formulė klaidinga su trimis interpretacijomis:

1) $p = r = t,\ q = k$,

2) $p = r = k,\ q = t$,

3) $p = q = k,\ r = t$.

Pirmajai interpretacijai priskiriame disjunktą $\neg p \vee q \vee \neg r$, antrajai – $p \vee \neg q \vee r$, trečiajai – $p \vee q \vee \neg r$. Formulės NKF yra $(\neg p \vee q \vee \neg r)\&(p \vee \neg q \vee r)\&(p \vee q \vee \neg r)$.

2. *Transformavimas į NKF naudojantis ekvivalenčiomis formulėmis.* Transformavimo algoritmo *eliminavimo, neigimo įkėlimo į skliaustus* bei *prastinimo* žingsniai yra tokie pat, kaip įrodant 2.4 teoremą, kai transformuojant formulę į NDF naudojamasi ekvivalenčiomis formulėmis. Skiriasi tik trečiasis žingsnis, t.y. kitaip taikomas distributyvumo dėsnis. Šiuo atveju naudojamės (2.5) ekvivalentumu. Teorema įrodyta.

Iš loginių kintamųjų $p_1, \ldots, p_n$ galima sudaryti 3^n skirtingų konjunktų (įskaitant ir tuščią konjunktą). Todėl skirtingų NDF yra 2^{3^n}. Formulės turi ne vienintelės normaliąsias disjunkcines bei konjunkcines formas. Pavyzdžiui, formulės $F(p,q,r)$, aprašytos pavyzdyje po 2.4 teoremos įrodymo, NDF yra $(p\&q\&\neg r) \vee (p\&\neg q\&r) \vee (\neg p\&q\&\neg r)$, taip pat ir $(q\&\neg r) \vee (p\&\neg q\&r)$. Todėl NDF bei NKF dar skirstomos į *tobuląsias, trumpiausiąsias* ir *minimaliąsias.*

2.17 apibrėžimas. *Formulės $F(p_1, \ldots, p_n)$* ***normalioji disjunkcinė forma*** *$\vee_{i=1}^{s} K_i$ vadinama* ***tobuląja****, jei kiekviename konjunkte K_i ($i = 1, \ldots, s$) yra arba p_j, arba $\neg p_j$ ($j = 1, \ldots, n$).*

2.18 apibrėžimas. *Formulės $F(p_1, \ldots, p_n)$* ***NDF*** *$\vee_{i=1}^{s} K_i$ vadinama* ***trumpiausiąja****, jei bet kuri kita jos NDF $\vee_{i=1}^{m} K'_i$ tenkina sąlygą $m \geqslant s$.*

2.19 apibrėžimas. *Formulės $F(p_1, \ldots, p_n)$ NDF $\vee_{i=1}^{s} K_i$ vadinama* ***minimaliąja****, jei bet kuri kita jos NDF $\vee_{i=1}^{m} K_i'$ tenkina sąlygą*

$$i(K_1) + \cdots + i(K_s) \leqslant i(K_1') + \cdots + i(K_m').$$

Panašiai apibrėžiamos ir *tobulos, trumpiausios* bei *minimalios* NKF.

2.5 Logikos algebros funkcijos

Aprašysime dar vieną formulių pavidalą, į kurį galima transformuoti bet kurią formulę. Šiame skyrelyje konstantą t prilyginsime 1, o k – 0 ir, kaip įprasta logikos algebros funkcijoms, griežtąją disjunkciją (sudėtį moduliu 2) žymėsime $\oplus$, o konjunkciją – $\cdot$ (sandauga).

p	q	$p \oplus q$
1	1	0
1	0	1
0	1	1
0	0	0

p	q	$p \cdot q$
1	1	1
1	0	0
0	1	0
0	0	0

2.20 apibrėžimas. *Funkcijos, kurių apibrėžimo ir kitimo sritys yra aibė $\{0, 1\}$, vadinamos* ***logikos algebros funkcijomis****, arba Boole funkcijomis.*

Formulės yra taip pat ir logikos algebros funkcijos. Logikos algebros funkcijas galima nusakyti lentelėmis:

p_1	$\cdots$	p_{n-1}	p_n	$f(p_1, \ldots, p_{n-1}, p_n)$
0	$\cdots$	0	0	$f(0, \ldots, 0, 0)$
0	$\cdots$	0	1	$f(0, \ldots, 0, 1)$
0	$\cdots$	1	0	$f(0, \ldots, 1, 0)$
	$\cdots$	$\cdots$		$\cdots$
1	$\cdots$	1	1	$f(1, \ldots, 1, 1)$

Dvi logikos algebros funkcijos vadinamos lygiomis, jeigu jas atitinkančios lentelės yra lygios. Kiekvieną logikos algebros funkciją galima išreikšti formule, t.y. rasti tokią formulę, kad jų lentelės būtų vienodos. Tai išplaukia iš praeito skyrelio. Juk kiekvieną logikos algebros funkciją galima transformuoti į normaliąją disjunkcinę (konjunkcinę) formą. Taigi logikos algebros funkciją užrašyti formule pakanka loginių operacijų $\neg$, &, $\vee$. Dėl paprastumo vietoje *logikos algebros funkcija* šiame skyrelyje rašysime *funkcija.*

Aibė $\{0, 1, p \cdot q, p \oplus q\}$ yra pilna, t.y. kad ir kokia būtų funkcija (kartu ir formulė), galima rasti jai lygią, kurioje yra tik sandauga, sudėtis (moduliu 2) bei konstanta 1. Tai išplaukia iš to, kad $\{\neg, \&\}$ yra pilna aibė ir $p\&q = p \cdot q$ (rašysime paprasčiau – pq), o $\neg p = p \oplus 1$. Formulėje $F(p_1, \ldots, p_s)$, į kurią įeina tik konstanta 1, sandauga bei sudėtis moduliu 2, atlikę algebrinius pertvarkius, gauname polinomą

$$\sum_{i_1 \ldots i_s} a_{i_1 \ldots i_s} p_1^{i_1} \cdot p_2^{i_2} \cdot \cdots \cdot p_s^{i_s} \quad (a_{i_1 \ldots i_s} \in \{0, 1\}); \tag{2.7}$$

čia $p^1 = p$, o p^0 reiškia, kad naryje nėra p.

Tokios formulės vadinamos ***Žegalkino polinomais***. Keletas savybių:

$$p^2 = pp = p\&p = p,$$

$$p^n = p,$$

$$p \oplus p = 0,$$

$$1 \oplus 1 = 0.$$

Aprašysime du būdus, kaip bet kurią formulę $F(p_1, \ldots, p_n)$ transformuoti į Žegalkino polinomą.

1. Formulei $F(p_1, \ldots, p_n)$ randame ekvivalenčią, kurioje iš loginių operacijų tėra $\neg$, $\&$ (tokia aibė yra pilna). Konjunkciją keičiame sandauga, o neigimą – $\oplus 1$ (t.y. $\neg G = 1 \oplus G$). Atliekame algebrinius pertvarkius ir gauname Žegalkino polinomą.

Pavyzdys. Transformuokime $\neg(p\&q) \to r$ į Žegalkino polinomą.

Sprendimas. $\neg(p\&q) \to r \equiv (p\&q) \vee r \equiv \neg(\neg(p\&q)\&\neg r) \equiv 1 \oplus (1 \oplus pq)(1 \oplus r) \equiv 1 \oplus 1 \oplus pq \oplus r \oplus pqr$. Taigi formulės $\neg(p\&q) \to r$ Žegalkino polinomas yra $pqr \oplus pq \oplus r$.

---

2. *Neišreikštinių koeficientų metodas.* Jei formulėje yra s loginių kintamųjų, tai užrašome bendrąjį (2.7) Žegalkino polinomo su s kintamaisiais pavidalą. Pagal formulės teisingumo lentelę sudarome 2^s lygčių sistemą, kurią išsprendę ir randame polinomo koeficientus.

Pavyzdys. Raskime formulę $p \to (q\&r)$ atitinkantį Žegalkino polinomą neišreikštinių koeficientų metodu.

Sprendimas. Formulėje yra trys loginiai kintamieji, todėl bendrasis Žegalkino polinomo su 3 kintamaisiais pavidalas yra

$$a_1 pqr \oplus a_2 pq \oplus a_3 qr \oplus a_4 pr \oplus a_5 p \oplus a_6 q \oplus a_7 r \oplus a_8.$$

Sudarome teisingumo lentelę:

p	q	r	$q\&r$	$p \to (q\&r)$
1	1	1	1	1
1	1	0	0	0
1	0	1	0	0
1	0	0	0	0
0	1	1	1	1
0	1	0	0	1
0	0	1	0	1
0	0	0	0	1

Tada $2^3 = 8$ lygčių sistema yra tokia:

$$\begin{cases} a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8 = 1, \\ a_2 \oplus a_5 \oplus a_6 \oplus a_8 = 0, \\ a_4 \oplus a_5 \oplus a_7 \oplus a_8 = 0, \\ a_5 \oplus a_8 = 0, \\ a_3 \oplus a_6 \oplus a_7 \oplus a_8 = 1, \\ a_6 \oplus a_8 = 1, \\ a_7 \oplus a_8 = 1, \\ a_8 = 1. \end{cases}$$

Ją išsprendę, gauname $a_8 = 1$, $a_7 = 0$, $a_6 = 0$, $a_3 = 0$, $a_5 = 1$, $a_4 = 0$, $a_2 = 0$, $a_1 = 1$. Taigi formulę $p \to (q\&r)$ atitinkantis Žegalkino polinomas yra $pqr \oplus p \oplus 1$.

Atkreipiame dėmesį, kad kiekvienai formulei egzistuoja daug jos normaliųjų disjunkcinių (konjunkcinių) formų. Tuo tarpu kiekvienai formulei egzistuoja jai lygus tik vienas vienintelis Žegalkino polinomas. Tai išplaukia iš atitinkamos lygčių sistemos sprendinio vienatinumo.

2.6 Kai kurios neklasikinės logikos

Trumpai apžvelgsime dvi neklasikines logikas, o dar su dviem (intuicionistine bei modalumo) logikomis plačiau susipažinsime kituose skyriuose.

1. *Daugiareikšmė logika.* Nagrinėsime loginius kintamuosius, kurių kitimo sritis yra natūraliųjų skaičių aibė $\{0, 1, \ldots, k-1\}$. Apibendrinsime kai kurias nagrinėtąsias logines operacijas. Kai $k = 2$, jų teisingumo lentelės sutampa su anksčiau aprašytomis.

a) *Neigimas.* Pateikiame tris skirtingus neigimo apibrėžimus k-reikšmės logikos atveju:

p	$\sim p$
0	1
1	2
2	3
$\vdots$	$\vdots$
$k-2$	$k-1$
$k-1$	0

p	Np
0	$k-1$
1	$k-2$
2	$k-3$
$\vdots$	$\vdots$
$k-2$	1
$k-1$	0

$$I_i(p) = \begin{cases} k-1, & \text{jei } p = i, \\ 0, & \text{jei } p \neq i, \end{cases}$$

$$i = 0, \ldots, k-1.$$

b) *Konjunkcija.* $\min(p, q)$ bei antras apibrėžimas $pq \pmod{k}$.

c) *Disjunkcija.* $\max(p, q)$.

Nagrinėsime funkcijas, kurių ir apibrėžimo, ir reikšmių kitimo sritis yra ta pati – $\{0, 1, \ldots, k-1\}$. Jas vadiname k-reikšmėmis funkcijomis.

Loginių operacijų aibė vadinama *pilnąja*, jei kiekvieną k-reikšmę funkciją galima užrašyti formule, kurioje yra tik operacijos iš nagrinėjamosios aibės.

Aibė $\{0, 1, \ldots, k-1, I_0(p), \ldots, I_{k-1}(p), \min(p, q), \max(p, q)\}$ yra pilna. Pažymėkime $\min(p, q)$ konjunkcijos simboliu, o $\max(p, q)$ – disjunkcijos. Tuomet bet kuri k-reikšmė funkcija užrašoma formule

$$f(p_1, \ldots, p_n) = \vee_{(\alpha_1 \ldots \alpha_n)} I_{\alpha_1}(p_1) \& \ldots \& I_{\alpha_n}(p_n) \& f(\alpha_1, \ldots, \alpha_n),$$

$$\alpha_i \in \{0, 1, \ldots, k-1\}.$$

2. *Netiksli logika.* Loginiai kintamieji įgyja kurią nors reikšmę (realųjį skaičių) iš intervalo $[0, 1]$. Neigimas, konjunkcija bei disjunkcija apibrėžiami tokiu būdu:

$$\neg p = 1 - p,$$

$$p \& q = \min(p, q),$$

$$p \vee q = \max(p, q).$$

Iš apibrėžimo išplaukia, kad ne su visomis p reikšmėmis $p \vee \neg p$ lygi 1, o $p \& \neg p$ lygi 0, t.y. pirmoji nėra tapačiai teisinga, o antroji – tapačiai klaidinga įprastine prasme.

2.21 apibrėžimas. *Formulė $F(p_1, \ldots, p_n)$ tapačiai teisinga, jei su bet kuriomis reikšmėmis $\alpha_1, \ldots, \alpha_n \in [0, 1]$ galioja nelygybė $F(\alpha_1, \ldots, \alpha_n) \geqslant 0{,}5$.*

2.22 apibrėžimas. *Formulė $F(p_1, \ldots, p_n)$ tapačiai klaidinga, jei su bet kuriomis reikšmėmis $\alpha_1, \ldots, \alpha_n \in [0, 1]$ galioja nelygybė $F(\alpha_1, \ldots, \alpha_n) \leqslant 0{,}5$.*

Pavyzdžiui: formulė $p \vee \neg p$ yra tapačiai teisinga, nes $\max(p, \neg p) \geqslant 0{,}5$; formulė $p\&\neg p$ yra tapačiai klaidinga, nes $\min(p, \neg p) \leqslant 0{,}5$.

Implikacija $p \to q$ apibrėžiama tokiu būdu: $\max(1 - p, q)$.

Įrodyta, kad *tapačiai teisingų formulių aibė sutampa su klasikinės logikos tapačiai teisingų formulių aibe.*

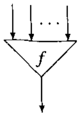
Formulės F, G vadinamos ekvivalenčiosiomis, jei $(F \to G)\&(G \to F)$ yra tapačiai teisinga formulė.

Formulės $\neg(p\&q)$ ir $\neg p \vee \neg q$ ekvivalenčios, nes $1 - \min(p, q) = \max(1 - p, 1 - q)$.

Formulės gali būti ekvivalenčios, bet su kai kuriomis kintamųjų reikšmėmis jos gali nesutapti. Pavyzdžiui, $p\&q$ bei $(p\&q\&r) \vee (p\&q\&\neg r)$ yra ekvivalenčios, bet su $p = q = 0{,}9$, $r = 0{,}3$ jų reikšmės skiriasi: $\min(p, q) = 0{,}9$, t.y. $p\&q$ reikšmė lygi 0,9, o $\min(p, q, r) = 0{,}3$, $\min(p, q, \neg r) = 0{,}7$, t.y. $(p\&q\&r) \vee (p\&q\&\neg r)$ reikšmė šiuo atveju lygi 0,7.

2.7 Dvejetainis sumavimas

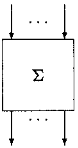
Nagrinėsime signalus transformuojančius elementus, turinčius n įėjimų ($n \geqslant 1$) ir vieną išėjimą. Žymėsime juos schema



Signalai gali būti dviejų rūšių (žymėsime juos 0, 1). Tarsime, kad elementai dirba diskrečiu režimu, t.y. signalai įėjime paduodami laikas nuo laiko vienu metu į visus įėjimo kanalus. Akimirksniu jie apdorojami elementu, t.y. elemento darbo laikas artimas nuliui, ir išėjime gauname rezultatą (0 arba 1). Be to, jei elemento darbas nepriklauso nuo praeities (elementas yra be atminties), tai jis vadinamas *loginiu*. Loginių elementų darbą galima aprašyti lentele:

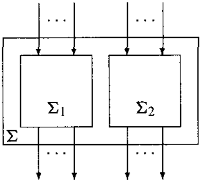
p_1	p_2	...	p_n	$f(p_1, p_2, \ldots, p_n)$
1	1	...	1	$f(1, 1, \ldots, 1)$
0	1	...	1	$f(0, 1, \ldots, 1)$
	...	...		...
0	0	...	0	$f(0, 0, \ldots, 0)$

Čia $p_1, \ldots, p_n$ žymi informaciją, gaunamą n kanalais (iš kairės į dešinę), o $f(p_1, \ldots, p_n)$ – elemento darbo rezultatą. Sakysime, kad loginis elementas realizuoja logikos algebros funkciją $f(p_1, \ldots, p_n)$. Naudodami loginius elementus, konstruosime schemas. Schemoje yra m įėjimų ($m \geqslant 1$) ir n išėjimų ($n \geqslant 1$).



Loginis elementas yra schema. Galimi trys schemų jungimo būdai.

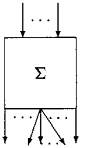
1. *Sujungimas.* Tarkime, yra dvi schemos Σ_1, Σ_2 su m_1 bei m_2 įėjimų ir n_1 bei n_2 išėjimų. Naujoje schemoje, gautoje sujungus duotąsias, bus $(m_1 + m_2)$ įėjimų ir $(n_1 + n_2)$ išėjimų.



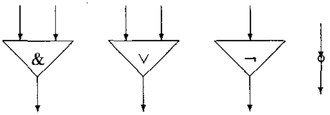
Schemos Σ_1, Σ_2 dirba lygiagrečiai ir informacija (signalai) įėjime į abi siunčiama vienu metu, t.y. dirba sinchroniškai.

2. *Elemento prijungimas.* Tarkime, turime schemą su m įėjimų, n išėjimų ir kurį nors elementą su k įėjimų ($k \leqslant n$) ir 1 išėjimu. Tuomet, prie duotosios schemos išėjimų prijungus elementą, galima gauti naują schemą. Joje bus m įėjimų ir $(n - k + 1)$ išėjimų.

3. *Išėjimų skaidymas.* Yra schema su m įėjimų ir n išėjimų. Išskaidžius kurį *nors vieną išėjimą į k išėjimų, galima gauti naują schemą.*



Nagrinėsime schemas, kuriose yra tik keturių tipų loginiai elementai:



Paskutinis elementas vadinamas trivialiu. Norime rasti schemą, kuri turėtų $2n$ *įėjimų bei* $(n+1)$ *išėjimų ir realizuotų dvejetainį sumavimą, t.y. schemos įėji*me būtų pateikiami du dvejetainiai skaičiai $x_n x_{n-1} \dots x_1$, $y_n y_{n-1} \dots y_1$ (x_i, $y_i \in \{0, 1\}$), o išėjime, apdorojus informaciją, būtų gaunama jų suma $z_{n+1} z_n \dots z_1$:

$$\begin{array}{r} + \begin{array}{r} x_n x_{n-1} \dots x_1 \\ y_n y_{n-1} \dots y_1 \end{array} \\ \hline z_{n+1} z_n z_{n-1} \dots z_1 \end{array}.$$

Įvedame dar schemos vidinius kintamuosius $q_i \in \{0, 1\}$, kurių prasmė tokia: $q_1 = 0$ ir $q_{i+1} = 1$ tada ir tiktai tada, kai $x_i + y_i + q_i > 1$. Sudedame tokius skaičius:

$$\begin{array}{r} \oplus \begin{array}{r} q_{n+1} q_n \dots q_1 \\ x_n \dots x_1 \\ y_n \dots y_1 \end{array} \\ \hline z_{n+1} z_n \dots z_1 \end{array}.$$

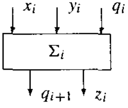
Nesunku apskaičiuoti z_i bei q_i reikšmes, kai x_i ir y_i yra žinomi:

$$\begin{cases} z_i = x_i \oplus y_i \oplus q_i, \\ q_{i+1} = (x_i \& y_i) \vee (x_i \& q_i) \vee (y_i \& q_i). \end{cases}$$

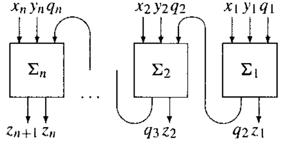
Pas mus nėra loginių elementų, realizuojančių $\oplus$, todėl pirmosios lygties formulę tenka išreikšti per $\neg$, $\&$, $\vee$:

$$\begin{cases} z_i = (\neg((x_i \& y_i) \vee (x_i \& q_i) \vee (y_i \& q_i)) \& (x_i \vee y_i \vee q_i)) \vee (x_i \& y_i \& q_i), \\ q_{i+1} = (x_i \& y_i) \vee (x_i \& q_i) \vee (y_i \& q_i). \end{cases}$$

Schemą, realizuojančią aprašytąją lygčių sistemą, kurioje yra trys įėjimai x_i, y_i, q_i ir du išėjimai z_i, q_{i+1}, pažymėkime simboliu Σ_i.



Dvejetainis sumavimas atrodo šitaip:



2.8 Pratimai

1. Sudarykite teisingumo lenteles:

a) $(p \to q)\&(\neg(\neg p \vee r) \to (q\&\neg r))$,

b) $((p\&q) \to (\neg p\&r))\&((q \to r) \vee (\neg p \to q))$,

c) $(p \to q) \to (q \to p)$.

2. Eliminuokite konstantas:

a) $((p \to t)\&(q \to k)) \vee (r\&t)$,

b) $((t \to p)\&(q\&k)) \to (r \to t)$,

c) $(p \vee k)\&((q \vee k) \to (p \to k))$.

3. Išreikškite disjunkcija ir neiginiu šias formules:

a) $p \to (q \to p)$,

b) $(p \to q) \vee (q \vee p)$,

c) $p \to (q \to (p\&q))$,

d) $(\neg p \to \neg q) \to (q \to p)$.

Patikrinkite, ar jos tapačiai teisingos.

4. Naudodamiesi teisingumo lentelėmis, raskite tobuląsias normaliąsias disjunkcines formas:

a) $(p \to q)\&(q \to r)$,

b) $(p\&q) \to (q\&(\neg p \to r))$.

5. Naudodamiesi ekvivalenčiomis formulėmis, transformuokite į NDF:

a) $(p \vee q)\&\neg(p \to r)$,

b) $((p\&q) \to r)\&(\neg(p\&q) \to r)$.

6. Naudodamiesi ekvivalenčiomis formulėmis, transformuokite į NKF:

a) $(p \to q)\&(q \to (\neg p \to r))$,

b) $(p \vee r)\&(p \to (q \to \neg r))$.

7. Raskite Žegalkino polinomus, atitinkančius formules:

a) $(p \vee q) \to (p\&q)$,

b) $p \to (q \to r)$,

c) $(p\&q) \to ((r\&\neg p) \to \neg q)$.

3 skyrius
Rekursyviosios funkcijos

Šiame skyriuje nagrinėsime vieną *algoritmiškai apskaičiuojamų funkcijų* formalizmą – rekursyviąsias funkcijas. Visų šiame skyriuje nagrinėjamųjų funkcijų apibrėžimų bei reikšmių aibė yra viena ir ta pati *natūraliųjų skaičių aibė* $N = \{0, 1, 2, \ldots\}$. Rekursyviųjų funkcijų aibė sutampa su Turingo mašinomis apskaičiuojamų funkcijų aibe. D. Hilbert suformulavo reikalavimus, kuriuos turi tenkinti algoritmiškai apskaičiuojamos funkcijos. Remdamasis jo darbais, K. Gödel 1931 m. pirmasis aprašė rekursyviųjų funkcijų klasę. Vėliau, 1936 m., A. Church, pritaikęs kitas idėjas, aprašė tą pačią rekursyviųjų funkcijų klasę.

3.1 Intuityvioji algoritmo samprata

XX amžiaus pradžioje atsirado poreikis tiksliai apibrėžti sąvoką *efektyvi procedūra* (*algoritmas*). Pradėta manyti, kad kai kurios problemos nėra išsprendžiamos. Bet kaip tai įrodyti? Kaip išsiaiškinti, kad tam tikrai problemai spręsti nėra algoritmo? Tam nepakanka plačiai vartojamos intuityvios algoritmo sampratos:

> *Seka griežtų komandų (instrukcijų), pagal kurias atliekamos operacijos, leidžiančios spręsti matematikos ar logikos uždavinius.*

Reikia turėti matematiškai tikslią algoritmo sąvoką. Ji turėtų apibendrinti intuityviai suprantamų algoritmų savybes.

Pateiksime plačiai žinomą Euklido algoritmo pavyzdį. Tarkime, yra du natūralieji skaičiai $a_1 \geqslant a_2 > 0$. Raskime didžiausiąjį bendrąjį jų daliklį. Algoritmas toks:

- *Dalijame* a_1 *iš* a_2. Jei liekana $a_3 = 0$, tai a_2 yra didžiausias bendrasis daliklis. Jei $a_3 \neq 0$, tai atliekame kitą veiksmą.

- *Dalijame* a_2 *iš* a_3. Jei liekana $a_4 = 0$, tai a_3 ir yra didžiausias bendrasis daliklis. Jei $a_4 \neq 0$, tai atliekame kitą veiksmą.
- *Dalijame* a_3 *iš* a_4 ir t.t.

Kadangi $a_1 \geqslant a_2 > a_3 > \cdots$, tai po baigtinio skaičiaus žingsnių rasime didžiausiąjį bendrąjį a_1 ir a_2 daliklį.

Pagrindinės savybės, kurias tenkina žinomų algoritmų pavyzdžiai, yra tokios:

1. *Diskretumas.* Veiksmai išdėstyti tam tikra seka. Vieną jų atlikę, pereiname prie kito. Veiksmai dar vadinami algoritmo žingsniais.
2. *Determinuotumas.* Atlikę veiksmą, žinome (nurodyta), ką daryti toliau.
3. *Žingsnių elementarumas.* Algoritmo veiksmų seką galima suskaidyti į labai paprastus, elementarius, paprastai aprašomus ir lengvai įvykdomus žingsnius.
4. *Masiškumas.* Algoritmai taikomi tam tikrai aibei. Pavyzdžiui, aprašytasis Euklido algoritmas taikomas *bet kuriems* natūraliesiems skaičiams $a_1 \geqslant a_2 > 0$.

Iš kur kilo žodis algoritmas? Tai sulotynintas arabų (kai kurie šaltiniai nurodo, kad persų) matematiko Al Chorezmi (*ca* 783–850) vardas. Jis išgarsėjo savo knyga, kurioje aprašė veiksmus su skaičiais, perimtais iš Indijos. Naujoji pozicinė skaičiavimo sistema greitai paplito pasaulyje, o jo knyga tapo daugelio žmonių parankine knyga. Joje buvo daug taisyklių rinkinių, kuriuos taikant po baigtinio žingsnių skaičiaus gaunamas rezultatas.

Algoritmo sąvoka buvo tikslinama dviem būdais:

1) kuriama idealizuota (matematinė) skaičiavimo mašina,

2) aprašoma algoritmiškai apskaičiuojamų funkcijų aibė.

Po daugelio metų – 1934–1936 m. ir viena, ir kita kryptimi dirbančių mokslininkų gauta daug formalizmu bei idėjomis skirtingų algoritmo sąvokos patikslinimų. Pirmosios krypties žinomiausiais darbais tapo A. Turingo ir E. Posto aprašytosios mašinos. A. Turing laikomas *informatikos mokslo tėvu*. Sukurtąją mašiną jis pasiūlė vadinti *elektroniniu kompiuteriu*. Antrojo pasaulinio karo metu tokia mašina jis pasinaudojo iššifruodamas vokiečių naudotą povandeniniuose laivuose kodą *Enigma*. Savo gyvenimą 1954 m. A. Turing baigė nusinuodydamas kalio cianidu. Paskutiniais gyvenimo metais jis dirbo Mančesterio universitete.

Intuityviai *algoritmiškai apskaičiuojama funkcija* suprantama taip: žinodamas funkcijos $y = f(x)$ argumento reikšmę *moku apskaičiuoti* funkcijos reikšmę. Buvo sukurta daug metodų *algoritmiškai apskaičiuojamų funkcijų* klasei nusakyti. Žinomiausios yra K. Gödelio, A. Churcho bei S. Kleene aprašytosios funkcijų klasės. A. Church jas pavadino rekursyviosiomis funkcijomis.

Churcho tezė. *Algoritmiškai apskaičiuojamų funkcijų aibė sutampa su rekursyviųjų funkcijų aibe.*

Ši tezė buvo paskelbta 1936 metais. Teze vadinama todėl, kad tai tvirtinimas, kuriuo, A. Churcho nuomone, reikėtų tikėti, bet įrodyti negalima. Negalima įrodyti dviejų aibių lygybės, nes, viena vertus, tai matematiškai tiksli rekursyviųjų funkcijų klasė, kita vertus – intuityvi, netiksli, skirtingų žmonių skirtingai suprantama algoritmiškai apskaičiuojamų funkcijų klasė.

Kodėl tikima Churcho teze? Pagrindiniai argumentai yra du:

1. Visų pasiūlytų, skirtingomis idėjomis aprašytų algoritmiškai apskaičiuojamų funkcijų klasės sutampa ne tik tarpusavyje, bet ir su idealizuotų skaičiavimo mašinų apskaičiuojamomis funkcijų klasėmis.

2. Nėra žinomas joks intuityviai apskaičiuojamos funkcijos pavyzdys, kuris nebūtų rekursyvioji funkcija.

3.2 Primityviai rekursyvios funkcijos

Aprašysime formaliąją sistemą. Funkcijas, kurias galima gauti toje sistemoje, vadinsime rekursyviosiomis. Formaliąją sistemą sudaro bazinės funkcijos ir operatoriai, kurie taikomi turimoms funkcijoms, o rezultatas – naujosios funkcijos. Visų pirma aprašysime vieną rekursyviųjų funkcijų poaibį, vadinamąsias primityviai rekursyvias funkcijas.

Bazinės funkcijos – tai konstanta 0, paskesniojo nario funkcija $s(x) = x + 1$ ir projekcijų funkcijos $\mathrm{pr}_p^i(x_1, \ldots, x_p) = x_i$ $(p \geqslant 1;\ 1 \leqslant i \leqslant p)$.

Iš bazinių funkcijų gaunamos naujos naudojantis dviem operatoriais: kompozicijos ir primityviosios rekursijos.

1. *Kompozicijos operatorius.* Tarkime, yra $(n + 1)$ funkcijų:

$$f(x_1, \ldots, x_n), g_1(x_1^1, \ldots, x_{m_1}^1), \ldots, g_n(x_1^n, \ldots, x_{m_n}^n). \qquad (3.1)$$

Sakome, kad funkcija $f(g_1(x_1^1, \ldots, x_{m_1}^1), \ldots, g_n(x_1^n, \ldots, x_{m_n}^n))$ gauta iš (3.1) funkcijų panaudojus kompozicijos operatorių.

2. *Primityviosios rekursijos operatorius.* Tarkime, yra dvi funkcijos $g(x_1, \dots, x_{n-1})$, $h(x_1, \dots, x_{n+1})$. Viena jų yra $(n-1)$ argumento, o antroji – $(n+1)$ argumento. Apibrėžiame naują n argumentų funkciją $f(x_1, \dots, x_n)$ pagal tokią schemą:

$$f(x_1, \dots, x_{n-1}, 0) = g(x_1, \dots, x_{n-1}),$$

$$f(x_1, \dots, x_{n-1}, y+1) = h(x_1, \dots, x_{n-1}, y, f(x_1, \dots, x_{n-1}, y)).$$

Kai $n = 1$, funkcija g yra konstanta. Sakome, kad funkcija f gauta iš funkcijų g, h, panaudojus primityviosios rekursijos operatorių. Pabrėždami, kad paskutinio argumento reikšmė nelygi nuliui, rašome $(y+1)$. Kaip matome, funkcija apibrėžta rekursyviai. Norint apskaičiuoti funkcijos $f(x_1, \dots, x_{n-1}, y+1)$ reikšmę, iš pradžių reikia rasti funkcijos reikšmę, kai paskutinio argumento reikšmė vienetu mažesnė. Rekursija (grįžimas) primityvi. Argumento reikšmė sumažinama vienetu.

3.1 apibrėžimas. *Pati mažiausia aibė, kuriai priklauso bazinės funkcijos ir kuri uždara kompozicijos bei primityviosios rekursijos atžvilgiu, vadinama **primityviai rekursyvių funkcijų aibe** (klase).*

Primityviai rekursyvių funkcijų aibę žymėsime PR. Primityviai rekursyvios funkcijos apibrėžtos su bet kuriomis argumentų reikšmėmis. Tokias funkcijas vadiname *visur apibrėžtomis funkcijomis.*

Aibės A charakteringoji funkcija κ apibrėžiama tokiu būdu:

$$\kappa_A(x) = \begin{cases} 1, & \text{jei } x \in A, \\ 0, & \text{jei } x \notin A. \end{cases}$$

3.2 apibrėžimas. *Natūraliųjų skaičių poaibis vadinamas **primityviai rekursyviu**, jei jo charakteringoji funkcija yra **primityviai rekursyvi**.*

Pavyzdžiai:

1. Konstanta 1 priklauso klasei PR, nes $s(0) = 1$ galima gauti iš bazinių funkcijų $s(x)$, 0, naudojantis kompozicijos operatoriumi.

2. Bet kuri konstanta n priklauso klasei PR, nes $s(s(\dots s(0))\dots) \in$ PR. Čia $(n-1)$ kartų taikėme kompoziciją.

3. $x + n \in$ PR, nes $s(s(\dots s(x))\dots) = x + n$. Kompoziciją taikėme taip pat $(n-1)$ kartų.

4. $s(\mathrm{pr}_3^3(x, y, z)) \in$ PR. Gauta iš bazinių funkcijų $s(x)$, $\mathrm{pr}_3^3(x, y, z)$, pritaikius kompozicijos operatorių.

5. Parodysime, kad $(x+y) \in$ PR. Funkcija $(x+y)$ gaunama iš pr_1^1 bei $s(\mathrm{pr}_3^3(x, y, z))$ naudojantis primityviosios rekursijos operatoriumi:

$$x + 0 = \mathrm{pr}_1^1(x) = x,$$

$$x + (y + 1) = (x + y) + 1 = s(\mathrm{pr}_3^3(x, y, x + y)) = s(x + y).$$

Apibrėžiame funkcijas $\mathrm{sg}(x)$, $\overline{\mathrm{sg}}(x)$ bei $x \dot{-} y$:

$$\mathrm{sg}(x) = \begin{cases} 1, & \text{jei } x > 0, \\ 0, & \text{jei } x = 0, \end{cases}$$

$$\overline{\mathrm{sg}}(x) = \begin{cases} 1, & \text{jei } x = 0, \\ 0, & \text{jei } x > 0, \end{cases}$$

$$x \dot{-} y = \begin{cases} x - y, & \text{jei } x > y, \\ 0, & \text{jei } x \leqslant y. \end{cases}$$

Įrodymą, kad $\mathrm{sg}(x)$, $\overline{\mathrm{sg}}(x)$ bei $x \dot{-} y$ yra primityviai rekursyvios, paliekame pratyboms.

Funkcija $|x - y|$ taip pat primityviai rekursyvi, nes $|x - y| = (x \dot{-} y) + (y \dot{-} x)$.

3.1 lema. *Jei $g(x_1, \ldots, x_n)$ primityviai rekursyvi, tai*

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{x_n} g(x_1, \ldots, x_{n-1}, i)$$

taip pat yra primityviai rekursyvi.

Įrodymas.

$$f(x_1, \ldots, x_{n-1}, 0) = g(x_1, \ldots, x_{n-1}, 0),$$

$$f(x_1, \ldots, x_{n-1}, y + 1) = f(x_1, \ldots, x_{n-1}, y) + g(x_1, \ldots, x_{n-1}, y + 1).$$

Todėl $f(x_1, \ldots, x_n)$ gaunama pritaikius primityviosios rekursijos operatorių funkcijoms $g(x_1, \ldots, x_{n-1}, 0)$ bei $h(x_1, \ldots, x_{n+1}) = g(x_1, \ldots, x_{n-1}, s(x_n)) + x_{n+1}$, kurios yra primityviai rekursyvios. Lema įrodyta.

Dalijame x iš y. Sveikąją dalį žymime $[x/y]$, o liekaną – $\mathrm{rest}(x, y)$. Tarkime, kad $[x/0] = x$, bei $\mathrm{rest}(x, 0) = x$. Remiantis 3.1 lema, nesunku įrodyti, kad $[x/y]$ yra primityviai rekursyvi. Tuo tikslu nagrinėjame skaičių seką

$$1 \cdot y \dot{-} x, 2 \cdot y \dot{-} x, \ldots, n \cdot y \dot{-} x, \ldots, x \cdot y \dot{-} x.$$

Sveikoji dalis lygi nulių sekoje skaičiui. Todėl:

$$[x/y] = \sum_{i=0}^{x} \overline{\mathrm{sg}}(iy \dot{-} x) \dot{-} 1,$$

$$\mathrm{rest}(x, y) = x \dot{-} (y \cdot [x/y]).$$

Algoritmų teorijoje dažnai aptinkamas funkcijos *apibrėžimas dalimis.*

$$f(x_1, \ldots, x_n) = \begin{cases} f_1(x_1, \ldots, x_n), & \text{jei } \alpha_1(x_1, \ldots, x_n) = 0, \\ \ldots & \\ f_s(x_1, \ldots, x_n), & \text{jei } \alpha_s(x_1, \ldots, x_n) = 0, \\ f_{s+1}(x_1, \ldots, x_n) & \text{likusiais atvejais.} \end{cases}$$

Be to, su bet kuriuo reikšmių $(x_1, \ldots, x_n)$ rinkiniu, tik viena iš α_i gali būti lygi nuliui.

Jei funkcijos f_i $(i = 1, \ldots, s+1)$ bei α_i $(i = 1, \ldots, s)$ primityviai rekursyvios, tai ir f primityviai rekursyvi, nes teisinga lygybė

$$\begin{aligned} f(x_1, \ldots, x_n) = {} & f_1(x_1, \ldots, x_n) \cdot \overline{\mathrm{sg}}\alpha_1(x_1, \ldots, x_n) + \cdots \\ & + f_s(x_1, \ldots, x_n) \cdot \overline{\mathrm{sg}}\alpha_s(x_1, \ldots, x_n) \\ & + f_{s+1}(x_1, \ldots, x_n) \cdot \mathrm{sg}(\alpha_1(x_1, \ldots, x_n) \cdots \alpha_s(x_1, \ldots, x_n)). \end{aligned}$$

Sąlygas α_i galima pakeisti

$$\alpha_i = \beta_i, \quad \alpha_i \leqslant \beta_i, \quad \alpha_i < \beta_i,$$

(suprantama α_i, β_i primityviai rekursyvios), nes jos redukuojamos į lygtis

$$|\alpha_i - \beta_i| = 0, \qquad \alpha_i \dot{-} \beta_i = 0, \qquad \overline{\mathrm{sg}}(\beta_i \dot{-} \alpha_i) = 0.$$

3.3 Minimizavimo operatorius

Tarkime, yra n argumentų funkcija f. Apibrėžiame naują, taip pat n argumentų funkciją $g(x_1, \ldots, x_n)$, kurios reikšmė lygi mažiausiam y, su kuriuo $f(x_1, \ldots, x_{n-1}, y) = x_n$. Įrodyta: jeigu f yra net primityviai rekursyvi, g gali ir nebūti algoritmiškai apskaičiuojama funkcija. Todėl, nusakydami naują funkciją g, privalome nurodyti ir metodą, kaip ieškoti mažiausio y:

- Jei $f(x_1, \ldots, x_{n-1}, 0) = x_n$, tai funkcijos g reikšmė lygi 0; jei ne, tai tikriname, ar $f(x_1, \ldots, x_{n-1}, 1) = x_n$.

- Jei $f(x_1, \ldots, x_{n-1}, 1) = x_n$, tai funkcijos g reikšmė lygi 1; jei ne, tai tikriname, ar $f(x_1, \ldots, x_{n-1}, 2) = x_n$ ir t.t.

Funkcija g gali būti dalinė, t.y. su kai kuriomis argumentų reikšmėmis ji gali būti neapibrėžta, nes, pavyzdžiui, tokio y, tenkinančio aprašytąją lygybę, gali ir nebūti. Tačiau gali ir būti toks m, kad $f(x_1, \ldots, x_{n-1}, m) = x_n$, bet, jei su kuriuo nors $i < m$ funkcija $f(x_1, \ldots, x_{n-1}, i)$ neapibrėžta, tai ir g bus neapibrėžta.

Sakome, kad funkcija g gauta pritaikius minimizavimo operatorių funkcijai f, ir žymime

$$g(x_1, \ldots, x_n) = \mu_y(f(x_1, \ldots, x_{n-1}, y) = x_n).$$

Naudojantis minimizavimo operatoriumi, gaunama dalinė skirtumo funkcija $x - y = \mu_z(y + z = x)$.

Funkcija $f(x) = \mu_y(y - (x + 1) = 0)$ neapibrėžta su jokiu $x \in N$, nors kiekvienam x atsiras mažiausias y. Jis lygus $x + 1$.

3.3 apibrėžimas. *Pati mažiausia aibė, kuriai priklauso bazinės funkcijos ir kuri uždara kompozicijos, primityviosios rekursijos bei minimizavimo atžvilgiu, vadinama **dalinių rekursyviųjų funkcijų aibe** (klase).*

Funkcija $(x - y)$ yra dalinė rekursyvioji, bet ji nėra primityviai rekursyvi. Iš 3.1 ir 3.3 apibrėžimų išplaukia, kad kiekviena primityviai rekursyvi funkcija yra ir dalinė rekursyvioji.

3.4 apibrėžimas. *Visur apibrėžta dalinė rekursyvioji funkcija vadinama **bendrąja rekursyviąja funkcija**.*

Dalinių rekursyviųjų funkcijų aibę žymėsime DR, o bendrųjų rekursyviųjų – BR. Iš apibrėžimų išplaukia, kad PR $\subseteq$ BR $\subset$ DR. Vėliau parodysime, kad egzistuoja bendrosios rekursyviosios funkcijos, kurios nėra primityviai rekursyvios. Taigi PR $\subset$ DR $\subset$ BR.

3.4 Porų numeravimas

Bet kurių dviejų skaičiųjų aibių Dekarto sandauga yra skaiti, todėl aibė $A = \{(x, y): x, y \in N\}$ taip pat yra skaiti. Visas poras išrašysime tam tikra tvarka. Jei $x + y < u + v$, tai (x, y) sekoje pasitaikys anksčiau negu (u, v). Jei $x + y = u + v$ ir $x < u$, tai pora (x, y) taip pat bus randama anksčiau. Turime tokią porų seką:

$$(0, 0),\ (0, 1),\ (1, 0),\ (0, 2),\ (1, 1),\ (2, 0),\ (0, 3), \ldots .$$

Kiekvienai porai priskirkime po numerį. Numeruoti pradedame nuo nulio. Jei pora yra i-oje vietoje, tai jos numeris yra $(i-1)$. Poros (x, y) numerį žymėsime $\alpha_2(x, y)$. Tada $\alpha_2(0,0) = 0$, $\alpha_2(0,1) = 1$, $\alpha_2(1,0) = 2, \dots$. Taip numeruoti poras pasiūlė G. Cantor.

3.2 lema. *Poros (x, y) numeris apskaičiuojamas naudojantis funkcija*

$$\alpha_2(x, y) = \frac{(x+y)^2 + 3x + y}{2}.$$

Įrodymas. Pora (x, y) yra atkarpoje

$$(0, x+y), (1, x+y-1), \dots, (x, y), \dots, (x+y, 0).$$

Prieš atkarpą yra viena tokia pora (u, v), kad $u + v = 0$, dvi poros (u, v), kuriose $u + v = 1$ ir t.t. Iš viso yra $1 + 2 + \cdots + (x+y)$ porų, t.y.

$$\frac{(x+y)(x+y+1)}{2}.$$

Pora (x, y) yra nagrinėjamosios atkarpos $(x+1)$-oje pozicijoje. Kadangi numeravimas prasideda nuo nulio, tai

$$\alpha_2(x, y) = \frac{(x+y)(x+y+1)}{2} + x = \frac{(x+y)^2 + 3x + y}{2}.$$

Lema įrodyta.

Poros (x, y) kairiuoju nariu vadiname x, o dešiniuoju – y. Kairiojo nario funkciją žymime π_2^1, o dešiniojo – π_2^2. Jos abi yra vieno argumento funkcijos. Jei poros (x, y) numeris yra n, tai $\pi_2^1(n) = x$, o $\pi_2^2(n) = y$. Jos tenkina tokias savybes:

$$\alpha_2(\pi_2^1(n), \pi_2^2(n)) = n,$$

$$\pi_2^1(\alpha_2(x, y)) = x,$$

$$\pi_2^2(\alpha_2(x, y)) = y.$$

Toliau nesinaudosime šiuo konkrečiu Cantoro numeravimu. Svarbu tik faktas, kad toks porų numeravimas galimas, kai $\alpha_2(x, y)$, $\pi_2^1(n)$, $\pi_2^2(n)$ yra primityviai rekursyvios funkcijos.

$\pi_2^1(n)$ apskaičiuojama tokiu būdu:

$$\pi_2^1(n) = x = n \dot{-} \frac{1}{2}\left[\frac{[\sqrt{8n+1}]+1}{2}\right]\left[\frac{[\sqrt{8n+1}] \dot{-} 1}{2}\right].$$

Naudojantis porų numeravimo funkcija, aprašomas trejetų, ketvertų ir t.t. numeravimas. Pavyzdžiui,

$$\alpha_3(x_1, x_2, x_3) = \alpha_2(x_1, \alpha_2(x_2, x_3)).$$

Taip numeruojant pirmieji penki sekos nariai yra trejetai

$$(0, 0, 0), (0, 0, 1), (1, 0, 0), (0, 1, 0), (1, 0, 1), \ldots .$$

Bet kurio n dedamųjų vektoriaus numeris apibrėžiamas rekursija

$$\alpha_n(x_1, \ldots, x_n) = \alpha_2(x_1, \alpha_{n-1}(x_2, \ldots, x_n)).$$

Jei $\alpha_n(x_1, \ldots, x_n) = x$, tai $\pi_n^i(x) = x_i$. Gauname, kad:

$$\begin{aligned}
x_1 &= \pi_2^1(x), \\
x_2 &= \pi_2^1(\pi_2^2(x)), \\
x_3 &= \pi_2^1(\pi_2^2(\pi_2^2(x))), \\
&\ldots\ldots\ldots\ldots\ldots \\
x_{n-1} &= \pi_2^1(\pi_2^2(\pi_2^2(\ldots(\pi_2^2(x)))\ldots), \quad \text{čia } \pi_2^2 \text{ įeina } (n-2) \text{ kartų}, \\
x_n &= \pi_2^2(\pi_2^2(\pi_2^2(\ldots(\pi_2^2(x)))\ldots), \quad \text{čia } \pi_2^2 \text{ įeina } (n-1) \text{ kartų}.
\end{aligned}$$

Kadangi funkcijos α_n, π_n^i (jos vadinamos Cantoro funkcijomis) gaunamos pritaikius kompozicijos operatorių primityviai rekursyvioms funkcijoms, tai ir jos pačios yra primityviai rekursyvios.

3.5 Baigtinumo problema

Nagrinėkime vienajuostes determinuotąsias Turingo mašinas. Be to, tarkime, kad jos tenkina sąlygas (tokias mašinas vadiname standartinėmis):

a) kai mašina po baigtinio skaičiaus žingsnių baigia darbą, t.y. patenka į galutinę būseną, jos skaitymo galvutė turi būti ties pirmąja (iš kairės) netuščia ląstele,

b) be tuščios ląstelės simbolio b, abėcėlėje yra dar du (0, 1). Be to, pradiniai duomenys bei rezultatai yra dvejetainiai skaičiai.

Būsenas, kaip ir įprasta, žymime raidėmis q su indeksais, perėjimų funkciją – raide δ, o perėjimų komandas – $\delta(q_i, x) = (q_j, x', Y)$; čia Y žymime vieną iš raidžių K, D, N.

Yra žinoma, kad ir kokia būtų Turingo mašina, galima rasti jai ekvivalenčią, t.y. apskaičiuojančią tą pačią funkciją, standartinę. Taigi Turingo mašinos abėcėlė yra tokia:

$$A = \{0, 1, b, q, 2, \dots, 9, \delta, =, (,), K, D, N\} \cup \{, \}.$$

3.3 lema. *Standartinių Turingo mašinų aibė yra skaičioji.*

Įrodymas. Remiantis 1.5 teorema, visų galimų žodžių aibė A^* yra skaiti. Tie žodžiai, kurie yra kurios nors standartinės Turingo mašinos perėjimų funkcija, sudaro begalinį A^* poaibį, kuris yra skaitus, nes bet kuris skaičiosios aibės poaibis yra baigtinis arba skaitus. Lema įrodyta.

Tarkime, kad $T_0, T_1, T_2, \dots$ yra pilnas sąrašas standartinių Turingo mašinų, o $\varphi_0, \varphi_1, \varphi_2, \dots$ – vieno argumento dalinės rekursyvios funkcijos, kurias apskaičiuoja atitinkamos Turingo mašinos, t.y. φ_i žymi funkciją, kurią apskaičiuoja mašina T_i.

Baigtinumo problema. *Ar egzistuoja algoritmas, kuriuo naudojantis, pagal bet kurią natūraliųjų skaičių porą (m, n) galima pasakyti, ar Turingo mašina T_m su pradiniais duomenimis n (t.y. juostoje pradiniu laiko momentu yra natūralųjį n atitinkantis dvejetainis skaičius) baigia darbą (t.y. po baigtinio skaičiaus žingsnių pereina į galutinę būseną), ar ne?*

Jei dalinė funkcija $f(x)$ apibrėžta su $x = k$, tai žymime $f(k) < \infty$, jei ne, $f(k) = \infty$.

Baigtinumo problemą galima apibrėžti ir tokiu būdu:

Ar egzistuoja algoritmas, kuriuo galima nustatyti, ar $\varphi_m(n) < \infty$, ar $\varphi_m = \infty$ (m, n – bet kurie natūralieji skaičiai)?

Aibė vadinama *rekursyviąja*, jei jos charakteringoji funkcija yra kuri nors visur apibrėžta rekursyvioji funkcija. Kai kalbama apie aibes, kurias sudaro ne skaičiai, o kitokie elementai (formulės, funkcijos, Turingo mašinos ir kt.), tai dažniausiai, užuot sakę *(ne)rekursyvi aibė*, sakome *(ne)išsprendžiama aibė (klasė, problema)*.

3.1 teorema. *Baigtinumo problema neišsprendžiama.*

Įrodymas. Parodysime, kad tarp visų galimų algoritmų nėra tokio, kuris išsprendžia baigtinumo problemą. Nagrinėkime funkciją

$$g(\alpha_2(x, y)) = \begin{cases} 1, & \text{jei } \varphi_x(y) < \infty, \\ 0, & \text{jei } \varphi_x(y) = \infty. \end{cases}$$

Tarkime, kad algoritmas, apie kurį kalbama baigtinumo problemoje, egzistuoja. Taigi atsiras tokia standartinė Turingo mašina, kad su pradiniais duomenimis $\alpha_2(x, y)$ po baigtinio skaičiaus žingsnių mašina pereis į galutinę būseną ir juostoje bus tik viena netuščia ląstelė. Joje bus 1 arba 0 ir ties ja bus skaitymo galvutė. Tuomet $g(\alpha_2(x, y))$ yra bendroji rekursyvioji funkcija ir atsiras Turingo mašina, apskaičiuojanti funkciją $\psi(x)$:

$$\psi(x) = \begin{cases} 1, & \text{jei } g(\alpha_2(x,x)) = 0, \\ \infty, & \text{jei } g(\alpha_2(x,x)) = 1. \end{cases}$$

Ją gauname tokiu būdu. Kiekvieną galutinę būseną q_i išbraukiame iš galutinių būsenų sąrašo, o perėjimų funkciją papildome:

$$\delta(q_i, 1) = (q_i, 1, D),$$
$$\delta(q_i, b) = (q_i, b, D),$$
$$\delta(q_i, 0) = (q_{k_i}, 1, N);$$

čia q_{k_i} — kurios nors naujos būsenos. Jas priskiriame galutinių būsenų aibei. Tarkime, l yra Turingo mašinos, apskaičiuojančios ψ, kuris nors numeris. Tuomet l bus ir ψ numeris, t.y. $\psi = \varphi_l$. Aiškinamės, ar $\psi(l) < \infty$. Iš prielaidos, kad egzistuoja algoritmas, apie kurį kalbama baigtinumo problemoje, gauname prieštarą:

1) jei $\psi(l) < \infty$, tai $g(\alpha_2(l, l)) = 0$ ir $\varphi_l(l) = \infty$, t.y. $\psi(l) = \infty$;

2) jei $\psi(l) = \infty$, tai $g(\alpha_2(l, l)) = 1$ ir $\varphi_l(l) < \infty$, t.y. $\psi(l) < \infty$.

Teorema įrodyta.

Bendresnę teoremą 1953 m. įrodė H. G. Rice:

Rice teorema. *Tarkime, kad X yra dalinė rekursyvioji vieno argumento funkcijų aibė. Jei X netuščia ir nesutampa su visų dalinių rekursyviųjų vieno argumento funkcijų aibe, tai*

$$A = \{x\colon x \in N \;\; ir \;\; \varphi_x \in X\}$$

yra nerekursyvi.

Remiantis Rice teorema, galima gauti daug nerekursyvių aibių. Pavyzdžiui:

a) X sudaro visos vieno argumento tapačiai lygios nuliui primityviai rekursyvios funkcijos,

b) X sudaro visos bendrosios rekursyviosios vieno argumento funkcijos.

Neišsprendžiama ir tokia problema:

Ar bet kurios dvi Turingo mašinos apskaičiuoja vieną ir tą pačią dalinę rekursyviąją funkciją?

3.6 Rekursyviai skaičios aibės

Pateikiame tris skirtingus rekursyviai skaičios aibės apibrėžimus.

3.5 apibrėžimas. *Sakome, kad aibė yra rekursyviai skaiti, jei ji sutampa su kurios nors dalinės rekursyviosios funkcijos apibrėžimo sritimi.*

3.6 apibrėžimas. *Netuščia aibė yra rekursyviai skaiti, jei ji sutampa su kurios nors primityviai rekursyvios funkcijos reikšmių aibe.*

3.7 apibrėžimas. *Aibė A yra rekursyviai skaiti, jei egzistuoja tokia primityviai rekursyvi funkcija $f(a, x)$, kad lygtis $f(a, x) = 0$ turi sprendinį x tada ir tiktai tada, kai $a \in A$.*

Visi trys apibrėžimai netuščios aibės atveju ekvivalentūs. Įrodysime tai tik keliems atvejams.

1. Tarkime, aibė A rekursyviai skaiti pagal 3.6 apibrėžimą, t.y. ji netuščia ir yra tokia primityviai rekursyvi funkcija $h(x)$, kad $A = \{h(0), h(1), h(2), \ldots\}$. Parodysime, kad egzistuoja tokia dalinė rekursyvi funkcija, kurios apibrėžimo sritis sutampa su A (3.5 apibrėžimas).

Tokia funkcija yra

$$f(x) = \mu_z(h(z) = x).$$

Funkcija $f(x)$ yra dalinė rekursyvi, nes gauta pritaikius minimizavimo operatorių primityviai rekursyviai funkcijai. Be to, jei $x \in A$, t.y. $x = h(i)$, tai atsiras toks $j \leqslant i$, kad $h(j) = x$. Vadinasi, $f(x)$ apibrėžta. Jei $x \notin A$, tai su bet kuriuo i funkcija $h(i) \neq x$ ir $f(x)$ neapibrėžta.

2. Tarkime, aibė A rekursyviai skaiti pagal 3.6 apibrėžimą. Tada A sutampa su primityviai rekursyvios funkcijos $h(x)$ reikšmių aibe, t.y. $A = \{h(0), h(1), h(2), \ldots\}$. Tuomet $|h(x) - a| = 0$ primityviai rekursyvi (žr. skyrelį *Primityviai rekursyvios funkcijos*) ir ji turi sprendinį tada ir tiktai tada, kai $a \in A$. Taigi A rekursyviai skaiti pagal 3.7 apibrėžimą. $f(a, x) = |h(x) - a|$.

3. Tarkime, kad egzistuoja tokia primityviai rekursyvi funkcija $f(a, x)$, kad lygtis $f(a, x) = 0$ turi sprendinį tada ir tiktai tada, kai $a \in A$, t.y. A rekusyviai skaiti pagal 3.7 apibrėžimą. A netuščia ir, tarkime, d yra kuris nors jos

elementas. Nagrinėjame funkciją

$$h(t) = \pi_2^1(t)\overline{\mathrm{sg}}f(\pi_2^1(t), \pi_2^2(t)) + d \cdot \mathrm{sg}f(\pi_2^1(t), \pi_2^2(t)).$$

Ji yra primityviai rekursyvi, nes gauta pritaikius kompozicijos operatorių primityviai rekursyvioms funkcijoms. Tarkime, $a \in A$, x_0 yra lygties $f(a, x_0) = 0$ sprendinys ir $t_0 = \alpha_2(a, x_0)$. Tuomet $\overline{\mathrm{sg}}f(\pi_2^1(t_0), \pi_2^2(t_0)) = \overline{\mathrm{sg}}f(a, x_0) = 1$, $\mathrm{sg}f(\pi_2^1(t_0), \pi_2^2(t_0)) = 0$ ir $h(t_0) = \pi_2^1(t_0) = a$, t.y. $h(t_0) \in A$.

Tarkime, kad $a \notin A$. Tuomet su bet kuriuo x_0 funkcija $f(a, x_0) \neq 0$. Kad ir koks būtų $t_0 = \alpha_2(a, x_0)$, $\overline{\mathrm{sg}}f(\pi_2^1(t_0), \pi_2^2(t_0)) = 0$. Tuo tarpu $\mathrm{sg}f(\pi_2^1(t_0), \pi_2^2(t_0)) = 1$ su bet kuriuo $t_0 = \alpha_2(a, x_0)$ ir $h(t_0) = d$, t.y. $h(t_0) \in A$. Taigi A rekursyviai skaiti pagal 3.6 apibrėžimą.

Norėdami atkreipti dėmesį į rekursyvių ir rekursyviai skaičių aibių skirtumą, pateikiame dar tokį apibrėžimą (palyginkite jį su 3.2 apibrėžimu).

Apibrėžimas. *Tarkime, $\kappa_A(x)$ yra dalinė rekursyvioji funkcija, tenkinanti sąlygą*

$$\kappa_A(x) = \begin{cases} 1, & \text{jei } x \in A, \\ \infty, & \text{jei } x \notin A. \end{cases}$$

Tuomet A yra rekursyviai skaiti.

Kuo skiriasi skaičiosios nuo rekursyviai skaičių aibių? Tai paaiškės vėliau. Kol kas tik pastebėkime, kad jei A yra skaiti ir abipusiškai vienareikšmę N ir A atitiktį galime nusakyti kuria nors primityviai rekursyvia funkcija $h(x)$ ($A = \{h(0), h(1), \ldots\}$), tai A taip pat yra rekursyviai skaiti (pagal 3.6 apibrėžimą). Kiekvienas natūraliųjų skaičių aibės poaibis yra baigtinis arba skaitusis. Vėliau matysime, kad egzistuoja begaliniai natūraliųjų skaičių poaibiai, kurie nėra rekursyviai skaitūs.

Pateikiame keletą rekursyviai skaičių aibių pavyzdžių.

Pavyzdžiai:

1. Tuščia aibė yra rekursyviai skaiti, nes ji sutampa su dalinės rekursyviosios funkcijos $\mu_z(z + (x+1) = 0)$ (ji su jokia reikšme neapibrėžta) apibrėžimo sritimi (naudojamės 3.5 apibrėžimu).

2. $N_- = \{1, 2, 3, \ldots\}$ yra rekursyviai skaiti, nes sutampa su primityviai rekursyviosios funkcijos $s(x)$ reikšmių aibe.

3. Baigtinio skaičiaus rekursyviai skaičių aibių sąjunga ir sankirta yra rekursyviai skaičios aibės.

Tarkime $A_1, A_2, \ldots, A_n$ yra rekursyviai skaičios aibės. Egzistuoja (pagal 3.7 apibrėžimą) tokios primityviai rekursyvios funkcijos $f_i(a, x)$, kad $f_i(a, x) = 0$ turi sprendinį tada ir tiktai tada, kai $a \in A_i$.

a) Sankirtos atveju konstruojame tokią primityviai rekursyvią funkciją:

$$f(a,x) = f_1(a,\pi_n^1(x)) + \cdots + f_n(a,\pi_n^n(x)).$$

Su reikšmėmis $x_1^0,\ldots,x_n^0$ lygybės $f(a,x_i^0) = 0$ $(i = 1,\ldots,n)$ galioja tada ir tiktai tada, kai egzistuoja $a \in A_1 \cap A_2 \cap \cdots \cap A_n$. Tarkime, $x^0 = \alpha_n(x_1^0,\ldots,x_n^0)$. Tuomet $f(a,x^0) = 0$.

b) Sąjungos atveju

$$f(a,x) = f_1(a,\pi_n^1(x)) \cdot \cdots \cdot f_n(a,\pi_n^n(x)).$$

Kai kurios rekursyviai skaičių aibių savybės:

1. Kiekviena rekursyvi aibė yra rekursyviai skaiti.

Tarkime, $\kappa_A(x)$ yra bendroji rekursyvioji charakteringoji aibės A funkcija. Tuomet A sutampa su dalinės rekursyvios funkcijos $f(x) = \kappa_A(x) - 1$ apibrėžimo sritimi.

2. Baigtinės aibės yra rekursyvios, kartu ir rekursyviai skaičios.

Tarkime, $A = \{a_1,\ldots,a_m\}$. Tuomet primityviai rekursyvi $\kappa_A(x) = \overline{sg}(|x - a_1| \cdot |x - a_2| \cdot \cdots \cdot |x - a_m|)$ yra aibės A charakteringoji funkcija.

3. Jei kuri nors aibė A ir jos papildinys $\bar{A}$ (iki natūraliųjų skaičių aibės) yra rekursyviai skaičios aibės, tai A, kaip ir $\bar{A}$, yra rekursyvi.

Tarkime, A sutampa su primityviai rekursyvios funkcijos $f(x)$ reikšmių aibe, o $\bar{A}$ — su $g(x)$ reikšmių aibe (remiamės 3.6 apibrėžimu). Funkcija

$$h(x) = \mu_z(|f(z) - x| \cdot |g(z) - x| = 0)$$

apibrėžta su bet kuriuo natūraliuoju x, nes $A \cup \bar{A} = N$ ir todėl ji yra bendroji rekursyvioji funkcija. Funkcijų A ir $\bar{A}$ charakteringosios yra šios bendrosios rekursyviosios funkcijos:

$$\kappa_A(x) = \overline{sg}|f(h(x)) - x|,$$

$$\kappa_{\bar{A}}(x) = \overline{sg}|g(h(x)) - x|.$$

Iš trečiosios savybės išplaukia teorema.

3.2 teorema. *Jei kuri nors rekursyviai skaiti aibė nėra rekursyvi, tai jos papildinys nėra nei rekursyvi, nei rekursyviai skaiti aibė.*

Ši teorema matematinėje logikoje labai svarbi. Formulėms priskiriami numeriai ir aprašytosios sąvokos bei rezultatai taikomi formulių aibėms. Vėliau matysime, kad rekursyviai skaičios, bet nerekursyvios aibės yra *tapačiai teisingų* bei *tapačiai klaidingų predikatų logikos formulių aibės.* Iš 3.2 teoremos išplaukia, kad įvykdomų predikatų logikos formulių aibė nėra nei rekursyvi, nei rekursyviai skaiti. Tas pats galioja ir formulių, kurios nėra tapačiai teisingos, aibei.

3.7 Ackermanno funkcijos

3.8 apibrėžimas. *Sakome, kad sąryšiu $R(x, y)$, apibrėžtu aibėje A, nusakome dalinę tvarką joje, jei sąryšis refleksyvus, tranzityvus ir antisimetrinis, t.y. kad ir kokie būtų $x, y \in A$, $(R(x, y)\&R(y, x)) \to x = y$.*

Sąryšius, kuriais įvedama dalinė tvarka, žymime $\leqslant$. Kai kada, patikslindami, apie kurios aibės tvarką kalbama, žymėsime $\leqslant$ su indeksu, pavyzdžiui, $\leqslant_A$. Tvarka, kai bet kurie du elementai palyginami, t.y. $R(x, y)$ apibrėžtas su bet kuriais x, y iš nagrinėjamosios aibės, vadinama *tiesine.*

3.9 apibrėžimas. *Tarkime, aibėse A, B įvesta tiesinė tvarka. Aibės vadinamos panašiosiomis (žymime $A \simeq B$), jei jos yra izomorfinės kaip sutvarkytos aibės. Jos dar vadinamos to paties tipo aibėmis.*

Taigi, jei $A \simeq B$, tai egzistuoja tokia abipusiškai vienareikšmė A, B elementų atitiktis, kad nesvarbu, kokie būtų $a_1, a_2 \in A$, jie ir juos atitinkantys $b_1, b_2 \in B$ tenkina sąlygas: $a_1 \leqslant_A a_2$ ir $b_1 \leqslant_B b_2$. Fiksuodami kurią nors netuščią aibę, galime rasti daug jai panašių aibių. Iš visų galimų aibių išskirsime kai kurias, dažniausiai matematikoje bei informatikoje naudojamas skaitines aibes ir suteiksime joms, kartu ir visoms į jas panašioms, vardus. Tie vardai vadinami *tipais*, arba *ordinalais.*

Pagrindinių aibių tipai:

1) tuščiosios – 0,
2) baigtinės $N_n = \{0, 1, \ldots, n - 1\}$ – n,
3) natūraliųjų skaičių – ω,
4) sveikųjų skaičių – π,
5) racionaliųjų skaičių – η,
6) realiųjų skaičių – λ.

Pakeitę $\leqslant$ į $\geqslant$, įvedame jau kitą, vadinamąją *dualiąja tvarką*. Jei aibės A tipas yra α, tai simboliu α^* žymimas dualiosios tvarkos tipas.

Apibrėšime veiksmus su tipais. Tarkime, aibės A tipas yra α (tvarka $\leqslant_A$), o B tipas – β (tvarka $\leqslant_B$).

3.10 apibrėžimas. *Tipų α, β suma (žymime $\alpha + \beta$) yra tiesinė tvarka $\leqslant$ aibėje $A \cup B$, nusakyta tokiu būdu:*

a) *jei $x \in A$, $y \in B$, tai $x < y$,*

b) *jei $x, y \in A$ ir $x \leqslant_A y$, tai $x \leqslant y$,*

c) *jei $x, y \in B$ ir $x \leqslant_B y$, tai $x \leqslant y$.*

3.11 apibrėžimas. *Tipų α, β sandauga (žymime $\alpha \cdot \beta$) yra tiesinė tvarka $\leqslant$ aibėje $A \times B$, nusakyta tokiu būdu:*

a) *jei $y_1 \leqslant_B y_2$, tai $(x_1, y_1) \leqslant (x_2, y_2)$,*

b) *jei $y_1 = y_2$ ir $x_1 \leqslant_A x_2$, tai $(x_1, y_1) \leqslant (x_2, y_2)$.*

Tarkime, aibėje $A = \{x_0, x_1, x_2, \ldots\}$ tvarka yra $x_0 < x_1 < x_2 < \cdots$, o aibėje $B = \{y_0, y_1, y_2, \ldots\}$ – $y_0 < y_1 < y_2 < \cdots$. Tuomet aibėje $A \times B$ yra tokia tvarka:

$$(x_0, y_0) < (x_1, y_0) < (x_2, y_0) < \cdots < (x_0, y_1) < (x_1, y_1) < (x_2, y_1) < \cdots.$$

Nesunku matyti, kad: a) $\alpha + 0 = 0 + \alpha = \alpha$, b) $1 + \omega = \omega$, bet $\omega + 1 \neq \omega$, c) $\omega^* \neq \omega$. Įprasta $\alpha \times \alpha$ žymėti α^2.

Apibrėžiame funkcijas $B_n(a, x)$, kai $a \geqslant 2$:

$$B_0(a, x) = a + x, \qquad B_1(a, x) = a \cdot x, \qquad B_2(a, x) = a^x.$$

Tai didėjančios funkcijos. $B_i(a, x) < B_j(a, x)$, kai $i < j$, pradedant kuriuo nors x_0. Jos tenkina tokias lygybes:

$$B_1(a, 1) = a, \qquad B_1(a, x + 1) = B_0(a, B_1(a, x)),$$

$$B_2(a, 1) = a, \qquad B_2(a, x + 1) = B_1(a, B_2(a, x)).$$

Pratęskime jas (kai $n \geqslant 2$):

$$B_{n+1}(a, 1) = a, \qquad B_{n+1}(a, x + 1) = B_n(a, B_{n+1}(a, x)).$$

Tarkime, kad $B_{n+1}(a, 0) = 1$, kai $n \geqslant 1$. Ackermanno funkcijos variantu, kai $a = 2$, vadiname $A(n, x) = B_n(2, x)$. Įvedame tiesinę tvarką tarp porų:

$$(0, 0) < (0, 1) < (0, 2) < \cdots < (1, 0) < (1, 1) < (1, 2) < \cdots$$
$$< (n, 0) < (n, 1) < (n, 2) < \cdots.$$

Jos tipas yra ω^2. Funkcija $A(n,x)$ aprašoma rekursija pagal tipą ω^2. Pastebėkime, kad reikšmės $A(n+1,0)$ ankstesnė yra $A(n_1,x)$ su $n_1 \leqslant n$ ir bet kuriuo x. Ackermanno funkcija nusakoma tokiomis lygybėmis:

$$A(0,x) = x+2,$$

$$A(1,0) = 0,$$

$$A(y,0) = 1 \quad \text{su } y \geqslant 2,$$

$$A(y+1,x+1) = A(y, A(y+1,x)) \quad \text{visiems } x, y.$$

Funkcija turi tokias savybes:

a) $A(n,x) \geqslant 2^x$ $(n \geqslant 2; x = 1,2,\ldots)$,

b) $A(n+1,x) \geqslant A(n,x)+1$,

c) $A(n,x+1) > A(n,x)$ $(n,x = 1,2,\ldots)$,

d) $A(n+1,x) \geqslant A(n,x+2)$.

Funkcija $h(x) = A(x,x)$ apibrėžta su bet kuriomis x reikšmėmis, todėl ji yra bendroji rekursyvioji. Įrodysime, kad $h(x)$ nėra primityviai rekursyvi. Naudosimės rezultatu, kad vieno argumento primityviai rekursyvių funkcijų aibė gali būti apibrėžta naudojantis tik vieno argumento primityviai rekursyviomis funkcijomis.

Įvedame naujus sudėties bei iteracijos operatorius. Juos taikysime vieno argumento primityviai rekursyvioms funkcijoms. Rezultatas – vieno argumento primityviai rekursyvi funkcija. Pritaikę sudėties operatorių funkcijoms $f(x)$, $g(x)$, gauname $f(x)+g(x)$. Tarkime, $g(x) \in$ PR. Apibrėžiame naują funkciją $f(x)$ tokiu būdu: $f(0) = 0$, $f(x+1) = g(f(x))$. Sakome, kad $f(x)$ gauta iš $g(x)$ pritaikius iteracijos operatorių ir žymime $I(g(x))$.

3.3 teorema. *Vieno argumento primityviai rekursyvių funkcijų aibė sutampa su aibe, kuriai priklauso bazinės funkcijos $s(x)$, $q(x) = x \dot{-} [\sqrt{x}]^2$ ir kuri uždara sudėties, kompozicijos bei iteracijos atžvilgiu.*

Sakome, kad $f(x)$ mažoruojama funkcija $h(x)$, jei $f(x) < h(x)$ pradedant kuriuo nors x_0, t.y., kai $x \geqslant x_0$. Parodysime, kad kiekviena vieno argumento primityviai rekursyvi funkcija mažoruojama funkcija $h(x)$ ir todėl $h(x)$ nėra primityviai rekursyvi. Visų pirma įrodysime, kad ir kokia būtų vieno argumento $f(x) \in$ PR, galima rasti tokį n, kad $f(x)$ būtų mažoruojama funkcija $A(n,x)$.

Remiamės 3.3 teorema, t.y. tariame, kad nagrinėjamosios funkcijos gautos iš $s(x)$, $q(x)$ pritaikius sudėties, kompozicijos bei iteracijos operatorius.

$$s(x) < 2^x = A(2, x) \quad (x = 2, 3, \ldots),$$

$$q(x) < s(x) < 2^x = A(2, x).$$

Tarkime, $f(x) < A(n_1, x)$, $g(x) < A(n_2, x)$ ir $n = n_1 + n_2$. Tuomet $f(x) < A(n, x)$ ir $g(x) < A(n, x)$.

$$\begin{aligned} f(x) + g(x) &< 2 \cdot A(n, x) < 2 \cdot 2^{A(n,x)} \leqslant 2^{A(n+1,x)} \\ &\leqslant A(n, A(n+1, x)) = A(n+1, x+1) \leqslant A(n+2, x). \end{aligned}$$

$$\begin{aligned} f(g(n)) &< A(n, g(x)) < A(n, A(n+1, x)) \\ &= A(n+1, x+1) \leqslant A(n+2, x). \end{aligned}$$

Panašiai gaunamas įvertis ir iteracijos atveju. Jei $f(x) < A(n, x)$, tai

$$f(n + x) < A(n, n + x) < A(n + x, n + x) = h(n + x).$$

Taigi gavome, kad ir kokia būtų vieno argumento $f(x) \in$ PR, ji mažoruojama visur apibrėžta funkcija $h(x)$ ir todėl $h(x)$ nėra primityviai rekursyvi. Tuo pačiu įrodėme, kad aibė PR yra griežtas aibės BR poaibis.

3.8 Universaliosios funkcijos

3.12 apibrėžimas. *Tarkime, A yra kuri nors n argumentų funkcijų aibė. Funkcija* $F(x_0, x_1, \ldots, x_n)$ *vadinama aibės A universaliąja, jei* $A = \{F(0, x_1, \ldots, x_n), F(1, x_1, \ldots, x_n), \ldots\}$, *t.y.* $F(i, x_1, \ldots, x_n) \in A$ $(i = 0, 1, 2, \ldots)$ *ir nesvarbu, kokia būtų* $f(x_1, \ldots, x_n) \in A$, *atsiras bent vienas toks natūralusis i, kad* $f(x_1, \ldots, x_n) = F(i, x_1, \ldots, x_n)$.

Tarkime, kad A yra kuri nors visur apibrėžta n argumentų funkcijų aibė, o $F(x_0, x_1, \ldots, x_n)$ – jos universalioji. Pastebėkime, jei $g(x_1, \ldots, x_n) = F(x_1, x_1, x_2, \ldots, x_n) + 1$ priklauso aibei A, tai universaliajai F atsiras toks i, su kuriuo galios lygybės:

$$F(i, x_1, x_2, \ldots, x_n) = F(x_1, x_1, x_2, \ldots, x_n) + 1,$$

$$F(i, i, x_2, \ldots, x_n) = F(i, i, x_2, \ldots, x_n) + 1.$$

Matome: jei $F \in$ PR, tai ir $g \in$ PR; jei $F \in$ BR, tai ir $g \in$ BR. Iš čia išplaukia du teiginiai:

a) visų n argumentų primityviai rekursyvių funkcijų aibės universali negali būti primityviai rekursyvi funkcija,

b) visų n argumentų bendrųjų rekursyviųjų funkcijų aibės universali negali būti bendroji rekursyvioji funkcija.

3.4 teorema. *Visų vieno argumento primityviai rekursyvių funkcijų aibei egzistuoja universalioji bendroji rekursyvioji funkcija.*

Įrodymas. Remiantis 3.3 teorema, visas vieno argumento primityviai rekursyvias funkcijas galima gauti iš bazinių $s(x)$, $q(x)$ taikant sudėties, kompozicijos bei iteracijos operacijas. Funkcijoms priskirsime natūraliuosius skaičius, t.y. apibrėžiame funkcijų numeraciją. Funkcijos $f(x)$ numerį žymėsime $n(f(x))$ arba rašysime $f_n(x)$, kai jos numeris yra n.

Funkcijoms $s(x)$, $q(x)$ priskiriame numerius: $n(s(x)) = 1$, $n(q(x)) = 3$.

Tarkime, $n(f(x)) = a$, o $n(g(x)) = b$. Tuomet funkcijoms, gautoms pritaikius sudėties, kompozicijos ar iteracijos operatorius, priskiriame tokius numerius:

$$n(f(x) + g(x)) = 2 \cdot 3^a \cdot 5^b,$$
$$n(f(g(x))) = 4 \cdot 3^a \cdot 5^b,$$
$$n(I(f(x))) = 8 \cdot 3^a.$$

Pavyzdžiui, $n(I(2 \cdot s)) = n(I(s + s)) = 8 \cdot 3^{2 \cdot 3 \cdot 5}$, $n(s + I(q)) = 2 \cdot 3 \cdot 5^{8 \cdot 3^3}$.

Apibrėžiame dviejų argumentų funkciją $F(n, x) = f_n(x)$, t.y. $F(n, x)$ lygi vieno argumento funkcijai, kurios numeris yra n.

$$F(n, x) = \begin{cases} f_a(x) + f_b(x), & \text{jei} \quad n = 2 \cdot 3^a \cdot 5^b, \\ f_a(f_b(x)), & \text{jei} \quad n = 4 \cdot 3^a \cdot 5^b, \\ f_a(f_n(x-1)), & \text{jei} \quad n = 8 \cdot 3^a,\ x > 0, \\ 0, & \text{jei} \quad n = 8 \cdot 3^a,\ x = 0, \\ q(x), & \text{jei} \quad n = 3, \\ s(x), & \text{jei} \quad n = 1. \end{cases}$$

Iš apibrėžimo matome, kad kiekviena funkcija turi numerį, bet ne vienintelį. Pavyzdžiui, nors $f(x) + g(x) = g(x) + f(x)$, bet jų numeriai bendruoju atveju skirtingi. Ne kiekvieną natūralųjį skaičių atitinka kuri nors funkcija. Pavyzdžiui, nėra tokios funkcijos, kurios numeris lygus 7, 13 ar 17. Dabar galime apibrėžti vieno argumento primityviai rekursyvių funkcijų universaliąją

$$D(n,x) = \begin{cases} F(n,x), & \text{jei } n \text{ yra kurios nors funkcijos numeris,} \\ 0 & \text{priešingu atveju.} \end{cases}$$

Funkcija $D(n, x)$ yra bendroji rekursyvioji funkcija. Teorema įrodyta.

3.5 teorema. *$D(x_0, \alpha_n(x_1, \ldots, x_n))$ yra visų n argumentų primityviai rekursyvių funkcijų aibės universalioji funkcija.*

Įrodymas. Universaliąją funkciją pažymėkime $D^{n+1}(x_0, x_1, \ldots, x_n)$. Parodysime, kad ji lygi $D(x_0, \alpha_n(x_1, \ldots, x_n))$. Viena vertus, su kiekvienu fiksuotu x_0 funkcija $D(x_0, \alpha_n(x_1, \ldots, x_n))$ yra primityviai rekursyvi. Antra vertus, jei $g(x_1, \ldots, x_n)$ yra kuri nors n argumentų primityviai rekursyvi funkcija, tai tokia yra ir $f(x) = g(\pi_n^1(x), \ldots, \pi_n^n(x))$. Ji yra vieno argumento. Todėl atsiras toks natūralusis x_0, kad $f(x) = D(x_0, x)$. Skaičius x_0 ir yra $g(x_1, \ldots, x_n)$ numeris, nes

$$\begin{aligned} f(\alpha_n(x_1, \ldots, x_n)) &= g(\pi_n^1(\alpha_n(x_1, \ldots, x_n)), \ldots, \pi_n^n(\alpha_n(x_1, \ldots, x_n))) \\ &= g(x_1, \ldots, x_n). \end{aligned}$$

Teorema įrodyta.

Dabar aprašysime dalinių rekursyviųjų funkcijų universaliąsias. Jos taip pat yra dalinės funkcijos.

3.13 apibrėžimas. *Dalinės rekursyviosios funkcijos $f(x_1, \ldots, x_n)$ grafiku vadiname aibę $A = \{(x_1, \ldots, x_n, y) \colon f(x_1, \ldots, x_n) = y\}$. Niekur neapibrėžtos funkcijos grafikas yra tuščia aibė.*

Pavyzdžiui, funkcijos $y = x^2$ grafikas yra aibė $\{(0,0), (1,1), (2,4), (3,9), (4,16), \ldots\}$.

3.6 teorema. *Dalinių rekursyvių n argumentų funkcijų aibei egzistuoja universalioji funkcija.*

Įrodymas. Bet kurios dalinės rekursyvios funkcijos grafikas yra rekursyviai skaiti aibė, nes sutampa su $\overline{\mathrm{sg}}|f(x_1, \ldots, x_n) - y| - 1$ apibrėžimo sritimi. Taigi, kad ir kokia būtų dalinė rekursyvi funkcija $f(x_1, \ldots, x_n)$, remiantis 3.7 apibrėžimu, galima tvirtinti, kad egzistuoja tokia primityviai rekursyvi funkcija $g(x_1, \ldots, x_n, y, z)$, kad $(x_1, \ldots, x_n, y) \in A$ tada ir tiktai tada, kai egzistuoja toks z, kad $g(x_1, \ldots, x_n, y, z) = 0$.

Tarkime, kad $t = \alpha_2(y, z)$. Tuomet $(x_1, \ldots, x_n, y) \in A$ tada ir tiktai tada, kai yra toks t, kad $g(x_1, \ldots, x_n, \pi_2^1(t), \pi_n^2(t)) = 0$. Pažymėkime $g(x_1, \ldots, x_n,$

$\pi_2^1(t), \pi_2^2(t))$ nauja funkcija $F(x_1, \ldots, x_n, t)$. Kad ir kokia būtų dalinė rekursyvioji funkcija $f(x_1, \ldots, x_n)$, atsiras tokia primityviai rekursyvi $F(x_1, \ldots, x_n, t)$, kad

$$f(x_1, \ldots, x_n) = \pi_2^1(\mu_t(F(x_1, \ldots, x_n, t) = 0)). \qquad (3.2)$$

Dalinių rekursyvių n argumentų funkcijų universalioji $\widetilde{D}^{n+1}$ gaunama tokiu būdu:

$$\widetilde{D}^{n+1}(x_0, x_1, \ldots, x_n) = \pi_2^1(\mu_t(D^{n+2}(x_0, x_1, \ldots, x_n, t) = 0)).$$

Iš tikrųjų ši funkcija su kiekvienu fiksuotu x_0 yra dalinė rekursyvioji. Tačiau, jei $f(x_1, \ldots, x_n)$ yra kuri nors dalinė rekursyvioji funkcija, tai egzistuoja tokia primityviai rekursyvi $F(x_1, \ldots, x_n, t)$, kuriai galioja (3.2) lygybė. Tarkime, jos numeris i. Tuomet

$$\widetilde{D}^{n+1}(i, x_1, \ldots, x_n) = \pi_2^1(\mu_t(D^{n+2}(i, x_1, \ldots, x_n, t) = 0)).$$

Teorema įrodyta.

3.14 apibrėžimas. *Sakome, kad visur apibrėžta funkcija $g(x_1, \ldots, x_s)$ yra* ***dalinės funkcijos*** *$f(x_1, \ldots, x_s)$* ***pratęsimas****, jei bet kuriems $x_1^0, \ldots, x_s^0$, su kuriais f apibrėžta, galioja lygybė $g(x_1^0, \ldots, x_s^0) = f(x_1^0, \ldots, x_s^0)$.*

Ar galima kiekvieną dalinę rekursyviąją funkciją pratęsti, t.y. ar atsiras iš bendrųjų rekursyviųjų funkcijų tokia, kuri bus jos pratęsimas? Pasirodo, kad ne visas dalines rekursyviąsias funkcijas galima pratęsti.

3.7 teorema. *Dalinių rekursyviųjų s argumentų funkcijų universalioji funkcija $\widetilde{D}^{s+1}(x_0, x_1, \ldots, x_s)$ neturi pratęsimo.*

Įrodymas. Nagrinėjame $V(x) = \overline{\mathrm{sg}}\widetilde{D}^{s+1}(x, x, \ldots, x)$. Jei $V(x)$ apibrėžta su kuriuo nors x_0, tai jos reikšmė lygi 1 arba 0. Tarkime $V(x)$ turi pratęsimą $W(x)$. Į ją (vieno argumento) galima žiūrėti kaip į s argumentų funkciją

$$W(x_1) = \mathrm{pr}_s^1(W(x_1), x_2, \ldots, x_s).$$

Atsiras toks a, kad $\widetilde{D}^{s+1}(a, x_1, \ldots, x_s) = W(x_1)$. Ji visur apibrėžta. Imame $x_1 = \cdots = x_s = a$. $W(x)$ yra ir $\overline{\mathrm{sg}}\widetilde{D}^{s+1}(x, x, \ldots, x)$ pratęsimas. Gauname prieštarą $W(a) = \overline{\mathrm{sg}}W(a)$. Taigi $V(x)$ neturi pratęsimo.

Tarkime, kad $\widetilde{D}^{s+1}(x_0, x_1, \ldots, x_s)$ turi pratęsimą $P(x_0, x_1, \ldots, x_s)$. Tuomet $\overline{\mathrm{sg}}P(x, x, \ldots, x)$ būtų $V(x)$ pratęsimas, o tokios tarp bendrųjų rekursyviųjų funkcijų nėra. Teorema įrodyta.

3.8 teorema. *Egzistuoja rekursyviai skaičios, bet nerekursyviosios aibės.*

Įrodymas. Nagrinėjame universaliąją vieno argumento funkcijoms $\widetilde{D}^2(x_1, x_2)$. Funkcija $V(x) = \overline{\mathrm{sg}}\widetilde{D}^2(x, x)$ turi savybes:

1) $V(x)$ yra dalinė rekursyvi,

2) $V(x)$ neturi pratęsimo,

3) $V(x)$ reikšmių aibė yra $\{0, 1\}$.

Lygties $V(x) = 0$ sprendinių aibė rekursyviai skaiti, nes sutampa su dalinės rekursyvios funkcijos $\mu_z(V(x) + z = 0)$ apibrėžimo sritimi. Jei ji būtų rekursyvi, t.y. atsirastų tokia bendroji rekursyvioji $\kappa(x)$, kad

$$\kappa(x) = \begin{cases} 1, & \text{jei } V(x) = 0, \\ 0 & \text{priešingu atveju,} \end{cases}$$

tai $\overline{\mathrm{sg}}\,\kappa(x)$ būtų $V(x)$ pratęsimas. O tai prieštarauja antrai funkcijos $V(x)$ savybei. Teorema įrodyta.

3.9 Kanoninis Posto skaičiavimas

Šiame skyrelyje trumpai susipažinsime su amerikiečių logiko E.L. Posto 1943 m. aprašytu *algoritmiškai apskaičiuojamųjų funkcijų* formalizmu – *kanoniniu skaičiavimu.*

3.15 apibrėžimas. *Kanoniniu skaičiavimu vadiname ketvertą* (A, P, Ak, T); *čia* A, Ak, P, T *– baigtinės aibės,* A *vadinama skaičiavimo abėcėle,* P *yra skaičiavimo kintamųjų aibė* ($A \cap P = \emptyset$), Ak *– abėcėlės* A *žodžių aibė, vadinama skaičiavimo aksiomų aibe,* T *– taisyklių aibė pavidalo*

$$\frac{\begin{array}{c} G_{1,1}p_{1,1}G_{1,2}p_{1,2}\ldots G_{1,n_1}p_{1,n_1}G_{1,n_1+1} \\ G_{2,1}p_{2,1}G_{2,2}p_{2,2}\ldots G_{2,n_2}p_{2,n_2}G_{2,n_2+1} \\ \ldots \\ G_{m,1}p_{m,1}G_{m,2}p_{m,2}\ldots G_{m,n_m}p_{m,n_m}G_{m,n_m+1} \end{array}}{G_1p_1G_2p_2\ldots G_np_nG_{n+1}};$$

čia $G_{i,j}$ *– abėcėlės* A *žodžiai,* $p_{i,j}$ *– kintamieji.*

Žodžiai virš brūkšnio vadinami taisyklės prielaidomis, o brūkšnio apačioje – išvada. Tariama, kad kintamieji, įeinantys į išvadą, aptinkami bent vienoje prielaidoje.

Taisyklę *realizuojančiu rinkiniu* vadiname reiškinį pavidalo

$$\begin{pmatrix} p^1, & p^2, & \ldots, & p^s \\ B_1, & B_2, & \ldots, & B_s \end{pmatrix};$$

čia $p^1, \ldots, p^s$ – pilnas sąrašas kintamųjų, įeinančių į taisyklę, o $B_1, \ldots, B_s$ – kurie nors abėcėlės A žodžiai. Pakeitę taisyklėje visas įeitis p^i žodžiais A_i $(i = 1, \ldots, s)$, gauname taisyklės taikymą

$$\frac{\begin{array}{c} Q_1 \\ \vdots \\ Q_m \end{array}}{Q};$$

čia Q, Q_i $(i = 1, \ldots, m)$ – abėcėlės A žodžiai. Žodžių abėcėlėje A seka vadinama išvedimu, jei kiekvienas jos narys yra aksioma arba gautas iš kairėje esančių formulių pritaikius kurią nors skaičiavimo taisyklę. Sakoma, kad žodis B išvedamas skaičiavime, jei galima rasti išvedimą, kuris baigiasi žodžiu B.

Kanoninis skaičiavimas įdomus tuo, kad apima tiek Turingo mašinas, tiek ir loginius skaičiavimus. Į Turingo mašinas ir loginius skaičiavimus galime žiūrėti kaip į atskirus kanoninių skaičiavimų atvejus. Gauname ir kitokį bendresnį formalų aparatą rekursyviai skaičioms aibėms aprašyti. Generuojami objektai nebūtinai yra skaičiai.

Pavyzdžiai:

1. $A = \{|\}$, $P = \{p\}$, $Ak = \{||\}$, $T = \frac{p}{pp}$.

Išvedamų skaičiavime žodžių aibė lygi $\{||, ||||, \ldots, |^{2^n}, \}$.

2. $A = \{1, 0, *\}$, $P = \{p, q\}$, $Ak = \{B\}$; čia B – kuris nors abėcėlės $\{1, 0\}$ žodis. T susideda iš taisyklių:

$$\frac{p}{p*}, \quad \frac{p1*q}{p*0q}, \quad \frac{p0*q}{p*1q}, \quad \frac{*p}{p}.$$

Kai kada domina ne visi išvedami abėcėlės A žodžiai, o išvedami žodžiai abėcėlės A', t.y. kurio nors aibės A poaibio. Tuo atveju sakoma, kad A' yra pagrindinė skaičiavimo abėcėlė. Jei antrajame pavyzdyje pagrindine abėcėle laikysime $\{1, 0\}$, tai skaičiavime išvedamas tik vienas (neskaitant aksiomos) žodis, kuris gaunamas iš B, pakeitus jame visas nuliukų įeitis vienetukais bei vienetukų įeitis nuliukais.

3.16 apibrėžimas. *Sakome, kad du skaičiavimai yra ekvivalentūs atžvilgiu pagrindinės abėcėlės A, jei išvedamų abiejuose skaičiavimuose abėcėlės A žodžių aibės sutampa.*

3.17 apibrėžimas. *Taisyklę, kurioje bent vieno kintamojo, įeinančio į prielaidą, išvadoje nėra, vadiname c-taisykle.*

3.4 lema. *Kad ir koks būtų kanoninis skaičiavimas* $\Pi = (A, P, Ak, T)$, *galima rasti jam ekvivalentų atžvilgiu pagrindinės abėcėlės A, kuriame nėra c-taisyklių.*

Įrodymas. Tarkime, kad $A = \{a_1, a_2, \dots, a_n\}$ ir skaičiavimo Π taisyklėje $G_1, \dots, G_m/G$ kintamųjų $p_1, \dots, p_s$, įeinančių į prielaidas, išvadoje G nėra. Naujasis skaičiavimas, kuriame eliminuota nagrinėjamo skaičiavimo c-taisyklė ir kuris ekvivalentus skaičiavimui Π atžvilgiu pagrindinės abėcėlės A, gaunamas tokiu būdu. Abėcėlė papildoma nauju simboliu, pavyzdžiui, $*$. O taisyklė keičiama tokiomis:

$$\frac{\begin{matrix} G_1 \\ \vdots \\ G_m \end{matrix}}{p_1 \dots p_s * G}, \qquad \frac{pa_i * q}{p * q} \quad (i = 1, \dots, n), \qquad \frac{*q}{q}.$$

Taigi generuodami tam tikrus „tarpinius" žodžius, kuriuose yra $*$, gauname skaičiavimą, kuriame eliminuota c-taisyklė ir jis ekvivalentus skaičiavimui Π atžvilgiu pagrindinės abėcėlės A. Lema įrodyta.

3.18 apibrėžimas. *Kanoninis skaičiavimas* $\Pi = (A, P, Ak, T)$ *vadinamas normaliuoju, jei aibėje Ak tėra vienas elementas, o visos taisyklės yra pavidalo*

$$\frac{Gq}{qG'};$$

čia G, G' – *abėcėlės A žodžiai.*

Parodysime, kaip galima modeliuoti Turingo mašinos darbą esant fiksuotiems pradiniams duomenims. Tuo tikslu nagrinėkime determinuotą standartinę Turingo mašiną su vienpuse viena juosta. Tarkime, Turingo mašinos abėcėlė $A \cup \{b\}$, $A = \{a_1, \dots, a_m\}$. Būsenų aibė $Q = \{q_0, q_1, \dots, q_s\}$; čia q_0 – pradinė būsena. Pradiniai duomenys $e_1 e_2 \dots e_v$ yra abėcėlės A žodžiai. Jie užrašomi pirmose (iš kairės į dešinę) v ląstelėse. Po baigtinio skaičiaus žingsnių Turingo mašina pereina į galutinę būseną (pažymėkime ją q_s) arba dirba be galo ilgai. Jei ji darbą baigia, tai pereina į galutinę būseną q_s ir skaitymo galvutė yra ties pirmąja ląstele. Tuščios ląstelės gali būti tik galutinio rezultato dešinėje, t.y. tuščios ląstelės prirašomos tik iš dešinės. Skaičiavimo eigoje jų negali būti tarp abėcėlės A žodžių.

Nors iš pirmo žvilgsnio ir atrodo, kad Turingo mašina turi tenkinti daug apribojimų, bet yra žinoma, kad ir kokia būtų Turingo mašina, galima rasti jai ekvivalenčią, tenkinančią išvardytus apribojimus.

Pastarosios darbą modeliuojantis normalusis kanoninis skaičiavimas gaunamas tokiu būdu. Abėcėlė $B = \{a_1, \dots, a_m, q_0, q_1, \dots, q_s, b, *\}$, pagrindinė abėcėlė $A \subset B$, $P = \{p\}$, $Ak = \{*q_0 e_1 e_2 \dots e_v\}$. Taisyklės:

$$\frac{xp}{px} \quad (x \in B), \qquad \frac{*q_s p}{p**}, \qquad \frac{b**p}{p**}, \qquad \frac{x**p}{p} \quad (x \in A).$$

Kiekvieną mašinos komandą atitinka po taisyklę. Komandoms pavidalo $\delta(q_i, a_j) = (q_u, a_v, D)$, $\delta(q_i, b) = (q_u, y, D)$ $(y \in A \cup \{b\})$, $\delta(q_i, a_j) = (q_u, a_v, K)$, $\delta(q_i, y) = (q_u, z, N)$ $(y, z \in A \cup \{b\})$ priskiriame taisykles:

$$\frac{q_i a_j p}{p a_v q_u}, \qquad \frac{q_i * p}{p y q_u *}, \qquad \frac{x q_i a_j p}{p q_j x a_v} \quad (x \in A), \qquad \frac{q_i y p}{p q_u z}.$$

Kita teorema priklauso logikui E.L. Postui.

3.9 teorema. *Kad ir koks būtų kanoninis skaičiavimas su pagrindine abėcėle A, galima rasti jam ekvivalentų normalųjį atžvilgiu A.*

3.10 Pratimai

1. Įrodykite, kad funkcijos yra primityviai rekursyvios:

   a) $x \cdot y$, b) x^y, c) $x \dot{-} 1$, d) $n!$, kai $0! = 1$.

2. Funkcija $g(x_1, \dots, x_n)$ yra primityviai rekursyvi. Įrodykite, kad funkcija f taip pat primityviai rekursyvi, kai:

   a)
   $$f(x_1, \dots, x_n) = \prod_{i=0}^{x_n} g(x_1, \dots, x_{n-1}, i),$$

   b)
   $$f(x_1, \dots, x_{n-1}, y, z) = \begin{cases} \sum_{i=y}^{z} g(x_1, \dots, x_{n-1}, i), & \text{jei } y \leqslant z, \\ 0, & \text{jei } y > z. \end{cases}$$

3. Žinoma, kad n argumentų funkcijos f, k, h yra primityviai rekursyvios. Įrodykite, kad primityviai rekursyvi yra

$$f(x_1, \ldots, x_n) = \sum_{i=h(x_1,\ldots,x_n)}^{k(x_1,\ldots,x_n)} g(x_1, \ldots, x_{n-1}, i).$$

4. Įrodykite, kad primityviai rekursyvi yra funkcija

$$\operatorname{div}(x, y) = \begin{cases} 1, & \text{jei } x \text{ dalijasi iš } y, \\ 0 & \text{priešingu atveju.} \end{cases}$$

5. Įrodykite, kad funkcija $nd(x)$, kurios reikšmė lygi x daliklių (įskaitant ir vienetą) skaičiui, yra primityviai rekursyvi.

6. Parašykite pirmuosius tris ketvertus naudodamiesi Cantoro numeravimu.

7. Aibė A yra rekursyvi. Įrodykite, kad jos papildinys taip pat rekursyvi aibė.

8. Aibės $A_1, \ldots, A_n$ yra rekursyvios. Įrodykite, kad jų sąjunga bei sankirta taip pat rekursyvios aibės.

9. Įrodykite: jei $f(x) \in \mathrm{PR}$, tai lygties $f(x) = 0$ sprendinių aibė yra rekursyvi.

10. Ar $\pi^* = \pi$?

11. Kam lygus $\omega^* + \omega$ tipas?

12. Nustatykite, kokio tipo yra aibė

$$(0,0) < (0,1) < (0,2) < \cdots < (1,0) < (1,1) < (1,2) < \cdots.$$

13. Kokią funkciją apibrėžia $B_3(a, n)$?

14. Įrodykite, kad iš bazinių funkcijų $s(x)$, $q(x)$, naudojantis sudėties, kompozicijos bei iteracijos operatoriais, galima gauti funkciją:

a) $\mathrm{pr}_1^1(x)$, b) $f(x) \equiv 0$, c) $\mathrm{sg}\, x$.

15. Kam lygi funkcija:

a) $I(x + 2 \cdot \sqrt{x} + 1)$, b) $I(\overline{\mathrm{sg}}\, x)$?

16. Raskite funkcijų, aprašytų 14-oje užduotyje, numerius.

4 skyrius
Teiginių skaičiavimai

Skaičiavimu nusakome įrodomų jame formulių aibę. Dažniausiai tai tapačiai teisingų ar tapačiai klaidingų formulių aibės. Skaičiavimu nusakoma aibė yra rekursyviai skaiti. Skaičiavimas – tai metodas, kuriuo įrodome, kad aibė rekursyviai skaiti. Jei ji nėra išsprendžiama, tai jos papildinys nėra rekursyviai skaitus ir neegzistuoja skaičiavimo, kuriame išvedamų formulių aibė būtų lygi papildiniui.

4.1 Hilberto tipo skaičiavimas

Nagrinėsime pataisytą ir papildytą konjunkcijos bei disjunkcijos aksiomomis G. Frege 1879 m. aprašytą skaičiavimą. Vėliau buvo sukurta skaičiavimų ir su kitokiomis aksiomomis tai pačiai išvedamų formulių aibei. Vokiečių matematikas D. Hilbert taip pat nagrinėjo skaičiavimus ir gavo kai kurių svarbių rezultatų. Tokius skaičiavimus įprasta vadinti ***Hilberto tipo skaičiavimais***.

Skaičiavimas (toliau jį vadinsime *teiginių skaičiavimu*) nusakomas aksiomomis ir taisykle.

Aksiomos (A, B, C – bet kurios formulės):

1.1. $A \to (B \to A)$,

1.2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,

2.1. $(A\&B) \to A$,

2.2. $(A\&B) \to B$,

2.3. $(A \to B) \to ((A \to C) \to (A \to (B\&C)))$,

3.1. $A \to (A \vee B)$,

3.2. $B \to (A \vee B)$,

3.3. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$,

4.1. $(A \to B) \to (\neg B \to \neg A)$,

4.2. $A \to \neg\neg A$,

4.3. $\neg\neg A \to A$.

Šios 1.1–4.3 aksiomos vadinamos aksiomų schemomis. Skaičiavime yra be galo daug aksiomų. Jos gaunamos iš aksiomų schemų A, B, C keičiant bet kokiomis formulėmis.

Vienintelė teiginių skaičiavimo taisyklė yra *modus ponens* (MP):

$$\frac{A, \quad A \to B}{B};$$

čia A ir B — bet kurios formulės.

4.1 apibrėžimas. *Įrodymu teiginių skaičiavime vadiname baigtinę formulių seką, kurioje kiekviena formulė yra arba aksioma, arba gauta iš prieš ją esančių formulių pagal modus ponens taisyklę.*

4.2 apibrėžimas. *Sakome, kad formulė A įrodoma teiginių skaičiavime (žymime $\vdash A$), jei galime rasti įrodymą, kurio paskutinis narys yra A.*

Pavyzdys. Kad ir kokia būtų formulė A, teiginių skaičiavime įrodoma formulė $A \to A$. Jos įrodymas yra seka. Aksiomą

$$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) \qquad (4.1)$$

gauname iš 1.2 aksiomų schemos, vietoje A įrašę A, vietoje B – $(A \to A)$, vietoje C – A.

$$A \to ((A \to A) \to A) \qquad (4.2)$$

gauname iš 1.1 aksiomų schemos vietoje A įrašę A, vietoje B — $(A \to A)$.

$$(A \to (A \to A)) \to (A \to A) \qquad (4.3)$$

išplaukia iš (4.1) ir (4.2) formulių pagal MP taisyklę.

$$A \to (A \to A) \qquad (4.4)$$

gauname iš 1.1 aksiomų schemos vietoje A įrašę A, vietoje B – A.

$$A \to A$$

išplaukia iš (4.3) ir (4.4) formulių pagal MP taisyklę.

4.1 teorema. *Jei formulė įrodoma teiginių skaičiavime, tai ji tapačiai teisinga.*

Įrodymas. Formulės

1.1. $p \to (q \to p)$,

1.2. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$,

...

4.3. $\neg\neg p \to p$

yra tapačiai teisingos (tuo galime įsitikinti sudarę teisingumo lenteles). Bet kuri aksioma gaunama iš minėtų tapačiai teisingų formulių pakeitus p, q, r konkrečiomis formulėmis ir todėl yra tapačiai teisinga (žr. 2 skyrių). Jei formulės A ir $A \to B$ tapačiai teisingos, tai ir B tapačiai teisinga. Iš tikrųjų, jei su kuria nors interpretacija B klaidinga, tai su ta pačia interpretacija turėtų ir A būti klaidinga, nes pagal prielaidą $A \to B$ yra tapačiai teisinga, o tai prieštarauja formulės A tapačiam teisingumui. Todėl, jei kuri nors seka yra įrodymas, tai kiekvienas sekos narys (iš jų ir paskutinis) yra tapačiai teisinga formulė. Teorema įrodyta.

Dėl paprastumo aksiomų schemas vadiname *aksiomomis.*

4.3 apibrėžimas. *Sakome, kad teiginių skaičiavimo aksioma yra nepriklausoma, jei išbraukę ją iš sąrašo gauname skaičiavimą, kuriame ji neįrodoma.*

4.2 teorema. *Visos teiginių skaičiavimo aksiomos yra nepriklausomos.*

Įrodymas. Iš pradžių įrodysime, kad 2.1 aksioma yra nepriklausoma. Šia aksioma nusakoma konjunkcijos savybė. Vietoje loginių kintamųjų reikšmių aibės $\{t, k\}$ nagrinėkime $\{\alpha, \beta\}$, o logines operacijas šiuo 2.1 aksiomos atveju aprašykime tokiomis lentelėmis:

p	q	$p\&q$
α	α	α
α	β	β
β	α	α
β	β	β

p	q	$p \vee q$
α	α	α
α	β	α
β	α	α
β	β	β

p	q	$p \to q$
α	α	α
α	β	β
β	α	α
β	β	α

p	$\neg p$
α	β
β	α

Kaip matome, $\vee$, $\to$, $\neg$ lentelės gautos iš įprastų, pervardijus t, k atitinkamai į α, β, o $A\&B \equiv B$.

Sakome, kad formulė F *tapačiai teisinga naująja prasme,* jei F lygi α su bet kuriomis loginių kintamųjų reikšmėmis. Panašiai apibrėžiama sąvoka, kad F *įvykdoma naująja prasme.* Kadangi 1.1, 1.2, 3.1–4.3 aksiomose nėra konjunkcijos įeičių, tai jos tapačiai teisingos naująja prasme. Konjunkcija įeina tik į 2.1–2.3 aksiomas. Aksioma 2.1 nėra tapačiai teisinga naująja prasme, nes $(A\&B) \to A \equiv B \to A$, ir ji klaidinga, kai $B = \alpha$, o $A = \beta$. Aksioma 2.2 išlieka tapačiai teisinga ir naująja prasme, nes

$$(A\&B) \to B \equiv B \to B.$$

Taip pat tapačiai teisinga naująja prasme ir 2.3 *aksioma, nes*

$$\begin{aligned}&(A \to B) \to ((A \to C) \to (A \to (B\&C))) \\ &\equiv (A \to B) \to ((A \to C) \to (A \to C)).\end{aligned}$$

Jei A, $A \to B$ yra tapačiai teisingos naująja prasme, tai tokia yra ir B. Išbraukiame 2.1 iš aksiomų sąrašo. Tuomet visos išvedamos formulės naujajame skaičiavime yra tapačiai teisingos naująja prasme. Bet 2.1 tokia nėra. Taigi ji neišvedama iš likusiųjų, o kartu yra nepriklausoma.

Panašiai įrodoma, kad 2.2–4.3 aksiomos yra nepriklausomos. Kiekvieną kartą tik viena loginė operacija apibrėžiama kitokiu būdu (lentelės antrame stulpelyje yra jos apibrėžimas), likusios gaunamos pervardijus reikšmes. Atsiras bent viena interpretacija (ji nurodoma lentelės trečiame stulpelyje), su kuria nagrinėjamoji aksioma klaidinga.

Aksioma	Operacijų apibrėžimas	Interpretacija
2.2	$A\&B = A$	$A = \alpha,\ B = \beta$
2.3	$A\&B = \beta$	$A = B = C = \alpha$
3.1	$A \vee B = B$	$A = \alpha,\ B = \beta$
3.2	$A \vee B = A$	$A = \beta,\ B = \alpha$
3.3	$A \vee B = \alpha$	$A = B = C = \beta$
4.1	$\neg A = A$	$A = \beta,\ B = \alpha$
4.2	$\neg A = \beta$	$A = \alpha$
4.3	$\neg A = \alpha$	$A = \beta$

Sudėtingiau įrodyti, kad pirmosios dvi aksiomos nepriklausomos, nes implikacija įeina ne tik į visas aksiomas, bet ji yra ir taisyklėje. *Klaidingą* teiginį, 1.1 aksiomos atveju dabar atitinka ne tik β, bet ir γ, δ. Prie *klaidingų* reikšmių 1.2 aksiomos atveju priskiriama ir γ. Aksiomos 1.1 atveju loginės operacijos apibrėžiamos lentele:

p	q	$p\&q$	$p \to q$	$p \vee q$	$\neg p$
α	α	α	α	α	β
α	β	β	β	α	β
α	γ	γ	β	α	β
α	δ	δ	β	α	β
β	α	β	α	α	α
β	β	β	α	β	α
β	γ	β	α	γ	α
β	δ	β	α	δ	α
γ	α	γ	α	α	δ
γ	β	β	β	γ	δ
γ	γ	γ	α	γ	δ
γ	δ	δ	β	γ	δ
δ	α	δ	α	α	γ
δ	β	β	β	δ	γ
δ	γ	δ	α	γ	γ
δ	δ	δ	α	δ	γ

Jei A, $A \to B$ yra tapačiai teisingos naująja prasme, tai ir B tokia pat. Be to, jei $F(p_1, \ldots, p_n)$ tapačiai teisinga naująja prasme, $A_1, \ldots, A_n$ – bet kurios formulės, tai ir $F(A_1, \ldots, A_n)$ yra tapačiai teisinga naująja prasme. Aksioma 1.1 nėra tapačiai teisinga naująja prasme, nes su interpretacija $A = \delta$, $B = \alpha$ ji lygi β. Visos likusios aksiomos lieka tapačiai teisingomis naująja prasme. Taigi 1.1 aksioma yra nepriklausoma.

Aksiomos 1.2 atveju loginės operacijos nusakomos lentele:

p	q	$p\&q$	$p \to q$	$p \vee q$	$\neg p$
α	α	α	α	α	β
α	β	β	β	α	β
α	γ	γ	γ	α	β
β	α	β	α	α	α
β	β	β	α	β	α
β	γ	β	α	γ	α
γ	α	γ	α	α	γ
γ	β	β	γ	γ	γ
γ	γ	γ	α	γ	γ

Ir šiuo atveju visos aksiomos, išskyrus 1.2, tapačiai teisingos naująja prasme. Aksioma 1.2 su interpretacija $A = B = \gamma$, $C = \beta$ lygi γ. Iš tapačiai teisingų naująja prasme, pritaikę MP, gauname taip pat tapačiai teisingas naująja prasme. Iš čia išplaukia, kad 1.2 aksioma nepriklausoma. Teorema įrodyta.

4.2 Dedukcijos teorema

Raide Γ žymėsime baigtinę formulių seką, kuri gali būti ir tuščia.

4.4 apibrėžimas. *Formulės B **išvedimu iš prielaidų** Γ vadiname baigtinę formulių seką $B_1, B_2, \ldots, B_m$, kurioje B_i $(1 \leqslant i \leqslant m)$ yra arba aksioma, arba viena iš prielaidų, arba gauta iš prieš ją esančių formulių B_l, B_k $(l, k < i)$ pagal* MP *taisyklę, ir $B_m = B$ (žymima $\Gamma \vdash B$).*

Ženklas $\vdash B$ reiškia, kad B išvedama iš tuščio prielaidų sąrašo, t.y. įrodoma duotame skaičiavime. Sąvoka *įrodymas* vartojama tada, kai prielaidų sąrašas tuščias. Sąvoka *išvedimas* yra bendresnė (prielaidų sąrašas juk gali būti ir tuščias) todėl sąvoka *įrodymas* vartojama tik tada, kai norima *pabrėžti*, jog prielaidų sąrašas tuščias.

Pateikiame kai kurias išvedimų iš prielaidų savybes:

1. $\Gamma, B \vdash B$.

2. Jeigu $\Gamma \vdash B$, tai $\Gamma, A \vdash B$.

3. Jeigu $\Gamma, A, C \vdash B$, tai $\Gamma, C, A \vdash B$.

4. Jeigu $\Gamma, A, A \vdash B$, tai $\Gamma, A \vdash B$.

5. Jeigu $\Gamma, A \vdash B$ ir $\Gamma \vdash A$, tai $\Gamma \vdash B$. Atskiru atveju, jei $\Gamma, A \vdash B$ ir $\vdash A$, tai $\Gamma \vdash B$.

Įrodymas. Tarkime, kad

$$B_1, B_2, \ldots, B_{m-1}, B \tag{4.5}$$

yra B išvedimas iš prielaidų Γ, A ir seka

$$A_1, A_2, \ldots, A_{k-1}, A \tag{4.6}$$

yra A išvedimas iš prielaidų Γ (atskiru atveju A įrodoma teiginių skaičiavime). Tada formulės B išvedimas iš prielaidų Γ gaunamas (4.5) sekoje formules A pakeitus (4.6) seka.

6. Jeigu $\Gamma \vdash A_1$, $\Gamma \vdash A_2, \ldots, \Gamma \vdash A_n$ ir $A_1, \ldots, A_n \vdash B$, tai $\Gamma \vdash B$.

Įrodymas. Jeigu $A_1, \ldots, A_n \vdash B$, tai pagal 2 savybę gauname $\Gamma, A_1, \ldots, A_n \vdash B$. Pasinaudoje $\Gamma \vdash A_n$ ir 5 savybe, gauname $\Gamma, A_1, \ldots, A_{n-1} \vdash B$. Panašiai eliminuojame ir kitas A_i. Lieka $\Gamma \vdash B$. Savybė įrodyta.

7. Jeigu $\Gamma \vdash A \to B$, tai $\Gamma, A \vdash B$.

Įrodymas. Tarkime, kad $B_1, \ldots, B_{m-1}, A \to B$ yra formulės $A \to B$ išvedimas iš prielaidų Γ. Prirašę prie sekos A (kaip prielaidą) bei B (pagal MP taisyklę iš $A \to B$ ir A), gauname išvedimą

$$B_1, B_2, \ldots, B_{m-1}, A \to B, A, B.$$

Savybė įrodyta.

4.3 teorema (dedukcijos). *$\Gamma, A \vdash B$ tada ir tiktai tada, kai $\Gamma \vdash A \to B$.*

Įrodymas. Jei $\Gamma \vdash A \to B$, tai $\Gamma, A \vdash B$ (7 savybė). Reikia įrodyti: jei $\Gamma, A \vdash B$, tai $\Gamma \vdash A \to B$.

Tarkime, kad

$$B_1, B_2, \ldots, B_{m-1}, B_m \tag{4.7}$$

(čia $B_m = B$) yra formulės B išvedimas iš prielaidų Γ, A. Juo remdamiesi pasistengsime gauti formulės $A \to B$ išvedimą iš prielaidų Γ. Šios sekos narį B_i $(1 \leqslant i \leqslant m)$ pakeitę į $A \to B_i$, sudarome seką

$$A \to B_1, \ldots, A \to B_i, \ldots, A \to B_m. \tag{4.8}$$

Be abejo, taip gauta seka nebūtinai yra išvedimas, t.y. kiekvienas sekos narys nebūtinai yra aksioma arba prielaida iš Γ, arba gauta iš kairėje stovinčių formulių pagal MP taisyklę. Kiekvieną (4.8) sekos narį pakeiskime tokia formulių seka, kad po pakeitimų gautoji seka taptų formulės $A \to B$ išvedimu iš prielaidų Γ.

Nagrinėkime formulę $A \to B_i$. Galimi tokie atvejai:

1) B_i yra aksioma,

2) B_i yra prielaida iš sąrašo Γ,

3) $B_i = A$,

4) B_i gaunama pagal MP taisyklę iš formulių B_j, B_k $(j, k < i)$.

Kiekvieną šių atvejų panagrinėkime atskirai.

1) $A \to B_i$ pakeiskime $A \to B_i$ įrodymu: B_i (aksioma), $B_i \to (A \to B_i)$ (1.1 aksioma), $A \to B_i$ (pagal MP taisyklę).

2) $A \to B_i$ keiskime analogiška seka (tik šiuo atveju B_i – prielaida).

3) $A \to A$ keiskime jos įrodymu, kuris anksčiau buvo pateiktas pavyzdyje.

4) Šis atvejis galimas tik tada, kai $i \geqslant 3$. Kadangi B_i gauta pagal MP taisyklę iš B_j ir B_k, tai $B_k = B_j \to B_i$ (arba $B_j = B_k \to B_i$; šiuo atveju įrodoma panašiai). $A \to B_j$ keiskime tokia seka:

- $(A \to (B_j \to B_i)) \to ((A \to B_j) \to (A \to B_i))$ (1.2 aksioma);
- $(A \to B_j) \to (A \to B_i)$ (pagal MP taisyklę iš prieš stovinčios formulės ir formulės $A \to B_k$, kuri (4.8) sekoje yra kairiau formulės $A \to B_i$, nes $k < i$; primename, kad $A \to B_k = A \to (B_j \to B_i)$);
- $A \to B_i$ (pagal MP taisyklę iš prieš stovinčios formulės ir $A \to B_j$).

Atlikę tokius keitimus, vietoje kiekvienos formulės $A \to B_i$ $(i = 1, \ldots, m)$ gauname formulės $A \to B_m = A \to B$ išvedimą.

Pastebėkime, kad darydami keitimus (4.8) sekoje, naudojomės 1.1 ir 1.2 aksiomomis. Teorema įrodyta.

Išvada. Jei $A_1, \ldots, A_n \vdash B$, tai $\vdash A_1 \to (A_2 \to \cdots \to (A_n \to B) \cdots))$.

Ją įrodyti galima taikant dedukcijos teoremą n kartų.

Pavyzdys. Naudodamiesi dedukcijos teorema, įrodykime, kad formulė $(A \to B) \to ((B \to C) \to (A \to C))$ išvedama teiginių skaičiavime.

Įrodymas. Formulė išvedama teiginių skaičiavime tada ir tiktai tada, kai $A \to B \vdash (B \to C) \to (A \to C)$. Dar du kartus pasinaudoję dedukcijos teorema, gauname, kad pradinė formulė išvedama teiginių skaičiavime tada ir tiktai tada, kai C išvedama iš prielaidų $A \to B$, $B \to C$, A. Pastarosios išvedimą nesunku rasti:

A (prielaida),

$A \to B$ (prielaida),

B (pagal MP taisyklę),

$B \to C$ (prielaida),

C (pagal MP taisyklę).

Išvedimas nesinaudojant dedukcijos teorema ilgesnis ir sudėtingesnis. Tiesa, neradome išvedimo pradinės formulės. Dedukcijos teorema vienos formulės išvedimą suvedame į kitos formulės su kitokiomis prielaidomis išvedimą. Mes tik įrodėme, kad pradinė formulė išvedama teiginių skaičiavime, kai egzistuoja C išvedimas, ir jį (pradinės formulės išvedimą), naudojantis dedukcijos teoremos įrodymu bei gautuoju C išvedimu, galima rasti.

Formalioji teorija vadinama absoliučiai neprieštaringa, jeigu ne visos teorijos formulės jame yra įrodomos. Formalių teorijų, tarp kurių taisyklių yra ir *modus ponens* ir kuriose įrodoma formulė $\neg A \to (A \to B)$ (t.y. loginėms formaliosioms teorijoms), neprieštaringumas apibrėžiamas taip:

4.5 apibrėžimas. *Teorija vadinama **neprieštaringąja**, jei neegzistuoja joje tokios formulės, kad ji bei jos neigimas, t.y. jos abi, būtų įrodomos teorijoje.*

Parodysime, kad teiginių skaičiavime įrodoma formulė $\neg A \rightarrow (A \rightarrow B)$. Ši formulė įrodoma tada ir tiktai tada, kai $\neg A, A \vdash B$ (tai išplaukia iš dedukcijos teoremos). Pateikiame pastarosios išvedimą.

1. $(\neg B \rightarrow A) \rightarrow (\neg A \rightarrow \neg\neg B)$ (4.1 aksioma, A pakeitėme $\neg B$, B pakeitėme A),
2. $A \rightarrow (\neg B \rightarrow A)$ (1.1 aksioma, B pakeitėme $\neg B$),
3. A (prielaida),
4. $\neg B \rightarrow A$ (pagal MP taisyklę iš 2 ir 3 formulių),
5. $\neg A \rightarrow \neg\neg B$ (pagal MP taisyklę iš 1 ir 4 formulių),
6. $\neg A$ (prielaida),
7. $\neg\neg B$ (pagal MP taisyklę iš 5 ir 6 formulių),
8. $\neg\neg B \rightarrow B$ (4.3 aksioma, A pakeitėme B),
9. B (pagal MP taisyklę iš 7 ir 8 formulių).

Prieštaringa teorija bloga tuo, kad joje įrodoma bet kuri formulė, ir kartu toji teorija tampa nereikalinga.

Taigi, jei teiginių skaičiavime yra tokia formulė, kuri ir kurios neigimas įrodomi, tai teiginių skaičiavime įrodoma ir bet kuri jo formulė.

4.4 teorema. *Teiginių skaičiavimas yra neprieštaringas.*

Įrodymas. Iš 4.1 teoremos išplaukia: jei kuri nors formulė įrodoma teiginių skaičiavime, tai ji tapačiai teisinga. Kadangi bet kurios tapačiai teisingos formulės neigimas yra tapačiai klaidinga formulė, tai neatsiras tokios formulės, kad ji bei jos neigimas būtų įrodomi teiginių skaičiavime. Teorema įrodyta.

4.3 Teiginių skaičiavimo pilnumas

Norime įrodyti, kad bet kuri formulė F įrodoma teiginių skaičiavime tada ir tiktai tada, kai F tapačiai teisinga. Pagal 4.1 teoremą, jeigu F įrodoma, tai ji tapačiai teisinga. Šiame skyrelyje įrodysime, kad kiekviena tapačiai teisinga formulė įrodoma teiginių skaičiavime. Tada sakome, kad teiginių skaičiavimas yra pilnas tapačiai teisingų formulių atžvilgiu.

4.1 lema. *Teiginių skaičiavime įrodoma formulė* $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$.

Įrodymas. Pakanka įrodyti, kad $\neg B \to \neg A, A \vdash B$ (tai išplaukia iš dedukcijos teoremos).

1. $(\neg B \to \neg A) \to (\neg\neg A \to \neg\neg B)$ (4.1 aksioma),
2. $\neg B \to \neg A$ (prielaida),
3. $\neg\neg A \to \neg\neg B$ (pagal MP taisyklę iš 1 ir 2 formulių),
4. $A \to \neg\neg A$ (4.2 aksioma),
5. A (prielaida),
6. $\neg\neg A$ (pagal MP taisyklę iš 4 ir 5 formulių),
7. $\neg\neg B$ (pagal MP taisyklę iš 3 ir 6 formulių),
8. $\neg\neg B \to B$ (4.3 aksioma),
9. B (pagal MP taisyklę iš 7 ir 8 formulių).

Lema įrodyta.

4.2 lema (kontrapozicijos taisyklė). *$\Gamma, A \vdash B$ tada ir tiktai tada, kai $\Gamma, \neg B \vdash \neg A$.*

Įrodymas. Pakanka parodyti, kad $\vdash A \to B$ tada ir tiktai tada, kai $\vdash \neg B \to \neg A$.

Tarkime, kad $\vdash A \to B$. Įrodysime, kad tuo atveju $\vdash \neg B \to \neg A$:

$(A \to B) \to (\neg B \to \neg A)$ (4.1 aksioma),

$\neg B \to \neg A$ (pagal MP taisyklę).

Tarkime, kad $\vdash \neg B \to \neg A$. Parodysime, kad $\vdash A \to B$:

$(\neg B \to \neg A) \to (A \to B)$ (4.1 lema),

$A \to B$ (pagal MP taisyklę).

Lema įrodyta.

Tarkime, A yra kuri nors formulė, $p_1, \ldots, p_n$ – pilnas sąrašas loginių kintamųjų, sudarančių A. Pažymėkime:

$$p^v = \begin{cases} p, & \text{jei } v = t, \\ \neg p, & \text{jei } v = k, \end{cases} \qquad A^v = \begin{cases} A, & \text{jei } v = t, \\ \neg A, & \text{jei } v = k. \end{cases}$$

Loginių operacijų įeičių skaičių formulėje A vadiname formulės A laipsniu ir žymime $g(A)$. Pavyzdžiui, $A = \neg(\neg p \to p)$, $B = (p_1 \to (\neg p_1 \to \neg\neg p_1))$. Tuomet $g(A) = 3$, $g(B) = 5$.

4.5 teorema. *Tarkime, kad* $v_1, \ldots, v_n$ *yra kuri nors reikšmių* t, k *seka ir* $A(v_1, \ldots, v_n) = v$. *Tada*

$$p_1^{v_1}, \ldots, p_n^{v_n} \vdash A^v.$$

Įrodymas. Įrodysime matematinės indukcijos metodu pagal formulės A laipsnį.

Tarkime, $g(A) = 0$, $A = p$. Tuomet teoremos tvirtinimas $p^v \vdash p^v$ teisingas remiantis išvedimų iš prielaidų pirmąja savybe.

Tarkime, kad teorema teisinga visoms formulėms, kurių laipsnis $g(A) < m$. Įrodysime, kad teorema teisinga ir tada, kai $g(A) = m$. Galimi tokie atvejai:

1) $A = \neg B$, 2) $A = B \to C$,

3) $A = B\&C$, 4) $A = B \vee C$.

Panagrinėkime juos atskirai.

1) Tarkime, $B(v_1, \ldots, v_n) = w$, $g(B) = m - 1$. Pagal indukcijos prielaidą

$$p_1^{v_1}, p_2^{v_2}, \ldots, p_n^{v_n} \vdash B^w. \tag{4.9}$$

Šį prielaidų sąrašą pažymėkime raide Γ. Galimi du atvejai: $w = t$, $w = k$.

Jei $w = k$, tai (4.9) yra pavidalo $\Gamma \vdash \neg B$. Šiuo atveju $v = t$, todėl $A^v = A$, t.y. $A^v = \neg B$. Iš čia išplaukia $\Gamma \vdash A^v$.

Jei $w = t$, tai (4.9) yra pavidalo $\Gamma \vdash B$. Šiuo atveju $v = k$, todėl $A^v = \neg A$, t.y. $\neg\neg B$.

$B \to \neg\neg B$ (4.2 aksioma),

B (indukcijos prielaida),

$\neg\neg B$ (pagal MP taisyklę).

Taigi $\Gamma \vdash \neg\neg B$, t.y. $\Gamma \vdash A^v$.

2) Kadangi $g(A) = m$, tai $g(B) < m$ ir $g(C) < m$, t.y. formulėms B ir C galioja indukcijos prielaida:

$$\Gamma \vdash B^{w_1}, \qquad \Gamma \vdash C^{w_2} \qquad (B(v_1, \ldots, v_n) = w_1, C(v_1, \ldots, v_n) = w_2).$$

Pastebėkime, kad B ir C sudaro nebūtinai visi loginiai kintamieji $p_1, \ldots, p_n$, t.y. nuo kai kurių loginių kintamųjų jos gali priklausyti fiktyviai.

Nagrinėkime keturis galimus atvejus:

a) $w_1 = k,\ w_2 = k$; b) $w_1 = k,\ w_2 = t$;

c) $w_1 = t,\ w_2 = t$; d) $w_1 = t,\ w_2 = k$.

Abiem a) ir b) atvejais $B^{w_1} = \neg B$, o $A^v = A$, t.y. $A^v = B \to C$. Žinoma, kad $\Gamma \vdash \neg B$. Reikia įrodyti, kad $\Gamma \vdash B \to C$ arba (dedukcijos teorema) $\Gamma, B \vdash C$.

Tarkime, kad $E_1, E_2, \ldots, E_s, \neg B$ yra $\neg B$ išvedimas iš prielaidų Γ, o $D_1, D_2, \ldots, D_r, \neg B \to (B \to C)$ yra $\neg B \to (B \to C)$ įrodymas (žr. 4.2 skyrelį). Tuomet ši formulių seka yra C išvedimas iš prielaidų Γ, B:

$$E_1, E_2, \ldots, E_s, \neg B, D_1, D_2, \ldots, D_r, \neg B \to (B \to C), B \to C, B, C.$$

Atveju c) $A^v = A$, t.y. $A^v = B \to C$, $B^{w_1} = B$, $C^{w_2} = C$. Pagal indukcijos prielaidą žinoma, kad $\Gamma \vdash B$, $\Gamma \vdash C$. Reikia įrodyti, kad $\Gamma \vdash B \to C$ arba $\Gamma, B \vdash C$. Bet tai išplaukia iš antrosios išvedimo iš prielaidų savybės (žr. 4.2 skyrelį).

Atveju d) $A^v = \neg A$, t.y. $A^v = \neg(B \to C)$. Be to, $B^{w_1} = B$, o $C^{w_2} = \neg C$. Pagal indukcijos prielaidą žinoma, kad $\Gamma \vdash B$ ir $\Gamma \vdash \neg C$. Reikia įrodyti, kad $\Gamma \vdash \neg(B \to C)$. Visų pirma įrodykime, kad $B, \neg C \vdash \neg(B \to C)$:

$B, B \to C \vdash C$ (pagal MP taisyklę),
$B, \neg C \vdash \neg(B \to C)$ (pagal kontrapozicijos taisyklę).

Pasinaudoję išvedimų iš prielaidų 6 savybe, gauname $\Gamma \vdash \neg(B \to C)$.

Panašiai įrodomi 3) ir 4) atvejai. Teorema įrodyta.

4.6 teorema. *Jei formulė A tapačiai teisinga, tai ji įrodoma teiginių skaičiavime.*

Įrodymas. Tarkime, $p_1, p_2, \ldots, p_n$ – pilnas sąrašas loginių kintamųjų, įeinančių į A. Iš 4.5 teoremos išplaukia, kad ir kokia būtų reikšmių seka $v_1, \ldots, v_n$ $(v_i \in \{t, k\})$,

$$p_1^{v_1}, \ldots, p_n^{v_n} \vdash A, \quad \text{nes } A(v_1, \ldots, v_n) = t.$$

Visus galimus ilgio n reikšmių rinkinius (iš viso 2^n) suskirstome į poras $(v_1, \ldots, v_{n-1}, t)$, $(v_1, \ldots, v_{n-1}, k)$, kuriose pirmosios $(n-1)$ reikšmės sutampa. Tokių porų iš viso yra 2^{n-1}. Iš 4.5 teoremos išplaukia, kad:

$$p_1^{v_1}, \ldots, p_{n-1}^{v_{n-1}}, p_n \vdash A, \qquad p_1^{v_1}, \ldots, p_{n-1}^{v_{n-1}}, \neg p \vdash A.$$

Iš čia, remdamiesi dedukcijos teorema, gauname:

$$p_1^{v_1}, \dots, p_{n-1}^{v_{n-1}} \vdash p_n \to A, \tag{4.10}$$

$$p_1^{v_1}, \dots, p_{n-1}^{v_{n-1}} \vdash \neg p_n \to A. \tag{4.11}$$

Norime įrodyti, kad $p_1^{v_1}, \dots, p_{n-1}^{v_{n-1}} \vdash A$. Tam pakanka parodyti, kad $\vdash (p_n \to A) \to ((\neg p_n \to A) \to A)$, nes, pasinaudojus MP taisykle, iš formulės dešinėje išvedimo simbolio ir (4.10), (4.11) nesunku gauti norimą rezultatą. Visų pirma įrodysime, kad:

a) $\vdash (A \to (B \to C)) \to ((A \& B) \to C)$,

b) $\vdash (A \to (B \to C)) \to ((B \& A) \to C)$,

c) $\vdash (A \& \neg A) \to \neg(B \to B)$,

d) $\vdash A \vee \neg A$.

Atveju a) pakanka įrodyti (taikome dedukcijos teoremą), kad $A \to (B \to C)$, $A \& B \vdash C$:

$(A \& B) \to A$ (2.1 aksioma),
$A \& B$ (prielaida),
A (pagal MP taisyklę),
$A \to (B \to C)$ (prielaida),
$B \to C$ (pagal MP taisyklę),
$(A \& B) \to B$ (2.2 aksioma),
B (pagal MP taisyklę),
C (pagal MP taisyklę).

Atveju b) formulė įrodoma analogiškai, atveju c) įrodoma taip:

$A \to ((B \to B) \to A)$ (1.1 aksioma),
$((B \to B) \to A) \to (\neg A \to \neg(B \to B))$ (4.1 aksioma),
$A \to (\neg A \to \neg(B \to B))$ (iš aksiomų schemos 1.2, pakeitę B į $(B \to B) \to A$, o C į $\neg A \to \neg(B \to B)$, ir pritaikę du kartus MP taisyklę),
$(\neg A \& A) \to \neg(B \to B)$ (remiamės formule *b*).

Atveju d) įrodymas toks:

$A \to (A \vee \neg A)$ (3.1 aksioma),
$\neg A \to (A \vee \neg A)$ (3.2 aksioma).

Iš šių dviejų formulių ir 4.1 aksiomos, pritaikę MP taisyklę, gauname kitas:

$\neg(A \vee \neg A) \to \neg A$,
$\neg(A \vee \neg A) \to \neg\neg A$,
$(\neg(A \vee \neg A) \to \neg\neg A) \to ((\neg(A \vee \neg A) \to \neg A) \to (\neg(A \vee \neg A) \to (\neg\neg A \& \neg A)))$ (2.3 aksioma).

Iš paskutinių trijų formulių, pritaikę du kartus MP taisyklę, gauname:

$\neg(A \vee \neg A) \to (\neg\neg A \& \neg A)$,
$\neg(A \vee \neg A) \to \neg(A \to A)$ (iš formulių a), c), 1.2 aksiomos, pritaikę du kartus MP taisyklę),
$(\neg(A \vee \neg A) \to \neg(A \to A)) \to (\neg\neg(A \to A) \to \neg\neg(A \vee \neg A))$ (4.1 aksioma),
$\neg\neg(A \to A) \to \neg\neg(A \vee \neg A)$ (pagal MP taisyklę),
$\neg\neg(A \to A)$ (kadangi $\vdash A \to A$ (žr. 4.1 skyrelio pavyzdį), tai $\vdash \neg\neg(A \to A)$, remiantis 4.2 aksioma),
$\neg\neg(A \vee \neg A)$ (pagal MP taisyklę),
$A \vee \neg A$ (iš aksiomos 4.3, pritaikę MP taisyklę).

Dabar įrodysime, kad $\vdash (A \to B) \to ((\neg A \to B) \to B)$, t.y. $A \to B, \neg A \to B \vdash B$:

$(A \to B) \to ((\neg A \to B) \to ((A \vee \neg A) \to B))$ (iš aksiomos 3.3, pakeitę B į $\neg A$, ir C į B),
$A \to B$ (prielaida),
$(\neg A \to B) \to ((A \vee \neg A) \to B)$ (pagal MP taisyklę),
$\neg A \to B$ (prielaida),
$(A \vee \neg A) \to B$ (pagal MP taisyklę),
$A \vee \neg A$ (įrodėme šiame skyrelyje),
B (pagal MP taisyklę).

Taigi, remdamiesi tuo, kad formulė $(A \to B) \to ((\neg A \to B) \to B)$ įrodoma, gauname

$$p_1^{v_1}, \ldots, p_{n-1}^{v_{n-1}} \vdash A.$$

Analogiškai gaunamas tvirtinimas ir $(n-1)$ ilgio rinkiniams nagrinėjant poras $(v_1, \ldots, v_{n-2}, t)$, $(v_1, \ldots, v_{n-2}, k)$, t.y. galima gauti $p_1^{v_1}, \ldots, p_{n-2}^{v_{n-2}} \vdash A$.
Pakartoję analogiškus samprotavimus $(n-2)$ kartus, gauname $\vdash A$. Teorema įrodyta.

Kiti Hilberto tipo teiginių skaičiavimai. Yra sukurta daug pilnų ir neprieštaringų Hilberto tipo teiginių skaičiavimų. Visų juose išvedamų formulių aibė yra ta pati – tapačiai teisingų formulių aibė. Pateiksime du skaičiavimus. Abu teturi tik po vieną *modus ponens* taisyklę. Nuo jau nagrinėtojo šie skaičiavimai skiriasi tik aksiomų schemomis. Antrojo formulėse yra tik neigimo ir implikacijos loginės operacijos.

Pirmojo skaičiavimo *aksiomos*:

1.1. $A \to (B \to A)$,

1.2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,

2.1. $(A \& B) \to A$,

2.2. $(A \& B) \to B$,

2.3. $A \to (B \to (A \& B))$,

3.1. $A \to (A \vee B)$,

3.2. $B \to (A \vee B)$,

3.3. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$,

4.1. $(A \to B) \to ((A \to \neg B) \to \neg A)$,

4.2. $\neg\neg A \to A$.

Antrojo skaičiavimo *aksiomos*:

1. $A \to (B \to A)$,

2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,

3. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$.

4.4 Gentzeno skaičiavimas

Hilberto teiginių skaičiavimuose sunku rasti formulių įrodymus. Nedaug padeda ir išvedimų iš prielaidų savybės (pavyzdžiui, dedukcijos teorema). Net gana paprastų (pavyzdžiui, $A \vee \neg A$; žr. 4.2 skyrelį) formulių įrodymai gan ilgi. O kaip įsitikinti, kad teiginių skaičiavime kuri nors formulė neįrodoma? Tik praėjus daugiau kaip penkiems dešimtmečiams po G. Frege darbų apie teiginių skaičiavimus, vokiečių logikas G. Gentzen 1930 m. aprašė kitokio tipo loginį skaičiavimą, kuris padarė perversmą logikoje. Išvedimo paieška, bent jau teiginių logikos atveju, tapo *mechaninė* (paaiškinsime tai vėliau). Yra daug G. Gentzeno skaičiavimo variantų. Be nagrinėjamojo, kurį vadiname ***sekvenciniu skaičiavimu G***, šiame skyrelyje aprašytas skaičiavimas G' ir dar vienas skaičiavimas 6 skyriuje.

4.6 apibrėžimas. *Sekvencija vadiname reiškinį* $A_1, \ldots, A_n \vdash B_1, \ldots, B_m$; *čia* A_i $(i = 1, \ldots, n)$ *bei* B_i $(i = 1, \ldots, m)$ *yra formulės ir* $n + m \neq 0$.

Raidėmis $\Gamma, \Gamma', \Gamma'', \Delta, \Delta', \Delta''$ žymime baigtines formulių sekas. Jos gali būti ir tuščios. Sekvencijoje $\Gamma \vdash \Delta$ seka Γ vadinama ***antecedentu***, o Δ – ***sukcedentu***.

Aksiomos: $\Gamma', A, \Gamma'' \vdash \Delta', A, \Delta''$.

Taisyklės:

$$(\to\vdash)\ \frac{\Gamma', \Gamma'' \vdash \Delta', A, \Delta'' \qquad \Gamma', B, \Gamma'' \vdash \Delta', \Delta''}{\Gamma', A \to B, \Gamma'' \vdash \Delta', \Delta''},$$

$$(\vdash\to)\ \frac{\Gamma', A, \Gamma'' \vdash \Delta', B, \Delta''}{\Gamma', \Gamma'' \vdash \Delta', A \to B, \Delta''},$$

$$(\&\vdash)\ \frac{\Gamma', A, B, \Gamma'' \vdash \Delta}{\Gamma', A\&B, \Gamma'' \vdash \Delta}, \qquad (\vdash\&)\ \frac{\Gamma \vdash \Delta', A, \Delta'' \qquad \Gamma \vdash \Delta', B, \Delta''}{\Gamma \vdash \Delta', A\&B, \Delta''},$$

$$(\vee\vdash)\ \frac{\Gamma', A, \Gamma'' \vdash \Delta \qquad \Gamma', B, \Gamma'' \vdash \Delta}{\Gamma', A \vee B, \Gamma'' \vdash \Delta}, \qquad (\vdash\vee)\ \frac{\Gamma \vdash \Delta', A, B, \Delta''}{\Gamma \vdash \Delta', A \vee B, \Delta''},$$

$$(\neg\vdash)\ \frac{\Gamma', \Gamma'' \vdash \Delta', A, \Delta''}{\Gamma', \neg A, \Gamma'' \vdash \Delta', \Delta''}, \qquad (\vdash\neg)\ \frac{\Gamma', A, \Gamma'' \vdash \Delta', \Delta''}{\Gamma', \Gamma'' \vdash \Delta', \neg A, \Delta''}.$$

Pakeitę kurioje nors taisyklėje $\Gamma, \Gamma', \Gamma'', \Delta, \Delta', \Delta'', A, B$ konkrečiomis formulėmis, gauname ***taisyklės taikymą***.

Sekvencijos, esančios taisyklėje virš brūkšnio arba jos taikyme virš brūkšnio, vadinamos ***prielaidomis*** (jų gali būti ne daugiau kaip dvi), o esančios žemiau brūkšnio – ***išvada*** (ji visada viena).

Pavyzdžiui, taisyklės $(\vee\vdash)$ išvada yra $\Gamma', A \vee B, \Gamma'' \vdash \Delta$, o prielaidos yra $\Gamma', A, \Gamma'' \vdash \Delta$ ir $\Gamma', B, \Gamma'' \vdash \Delta$.

Jei $\Gamma \vdash \Delta$ yra kurios nors taisyklės α taikymo išvada, o $\Gamma' \vdash \Delta'$, $\Gamma'' \vdash \Delta''$ (jų gali būti ir viena) yra prielaidos, tai sakoma, kad $\Gamma \vdash \Delta$ gauta iš $\Gamma' \vdash \Delta'$ ir $\Gamma'' \vdash \Delta''$, pritaikius taisyklę α.

4.7 apibrėžimas. *Sekvencijos išvedimu sekvenciniame skaičiavime G vadiname medį, kurio visose galinėse viršūnėse (lapuose) yra aksiomos, likusiose viršūnėse – formulės, gautos pagal kurią nors sekvencinio skaičiavimo taisyklę iš tiesiogiai virš jų medyje esančių formulių, ir šaknyje esanti sekvencija lygi pradinei.*

Pavyzdžiai:

1. $\vdash A \vee \neg A$.

$$\cfrac{\cfrac{A \vdash A}{\vdash A, \neg A}}{\vdash A \vee \neg A}.$$

2. $(A\&B) \to C, A\&\neg C \vdash \neg B$.

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{A, B \vdash C, A \qquad A, B \vdash C, B}{A, B \vdash C, A\&B} \qquad C, A, B \vdash C}{(A\&B) \to C, A, B \vdash C}}{(A\&B) \to C, A, \neg C, B \vdash}}{(A\&B) \to C, A\&\neg C, B \vdash}}{(A\&B) \to C, A\&\neg C \vdash \neg B}.$$

Primename, kad išvedimuose brūkšniai atitinka grafo lankus (kryptis – iš apačios į viršų), o sekvencijos – viršūnes. Ilgiausiame kelyje nuo šaknies iki viršūnės aptinkamų sekvencijų skaičius vadinamas išvedimo aukščiu.

Taisyklių (jų taikymų) $(\to\vdash)$, $(\vdash\to)$ *centrine formule* vadinama $(A \to B)$, taisyklių $(\& \vdash)$, $(\vdash \&)$ – $A\&B$, taisyklių $(\vee \vdash)$, $(\vdash \vee)$ – $A \vee B$, taisyklių $(\neg \vdash)$, $(\vdash \neg)$ – $\neg A$.

G. Gentzen įrodė, kad formulė A tapačiai teisinga tada ir tiktai tada, kai sekvencija $\vdash A$ išvedama skaičiavime G.

Iš čia išplaukia, kad formulė A tapačiai klaidinga tada ir tiktai tada, kai $A \vdash$ išvedama skaičiavime G.

4.8 apibrėžimas. *Sakome, kad taisyklė α apverčiama, jei jos prielaidos išvedamos sekvenciniame skaičiavime tada ir tiktai tada, kai išvedama išvada.*

4.7 teorema. *Visos sekvencinio skaičiavimo G taisyklės apverčiamos.*

Įrodymas. Nagrinėjame taisyklę $(\vdash \&)$ ir sekvenciją

$$\Gamma \vdash \Delta', A\&B, \Delta''. \tag{4.12}$$

Įrodysime, kad $\Gamma \vdash \Delta', A\&B, \Delta''$ išvedama sekvenciniame skaičiavime G tada ir tiktai tada, kai išvedamos abi sekvencijos $\Gamma \vdash \Delta', A, \Delta''$ ir $\Gamma \vdash \Delta', B, \Delta''$. Jei jos išvedamos, tai ir (4.12) išvedama. Išvedimo medis yra

$$\cfrac{\cfrac{D_1}{\Gamma \vdash \Delta', A, \Delta''} \qquad \cfrac{D_2}{\Gamma \vdash \Delta', B, \delta''}}{\Gamma, \vdash \Delta', A\&B, \Delta''};$$

čia

$$\frac{D_1}{\Gamma \vdash \Delta', A, \Delta''}, \quad \frac{D_2}{\Gamma \vdash \Delta', B, \Delta''}$$

yra sekvencijų $\Gamma \vdash \Delta', A, \Delta''$ ir $\Gamma \vdash \Delta', B, \Delta''$ išvedimų medžiai.

Tarkime, (4.12) išvedama. Įrodykime, kad sekvencijos $\Gamma \vdash \Delta', A, \Delta''$ ir $\Gamma \vdash \Delta', B, \Delta''$ išvedamos sekvenciniame skaičiavime G. Taikysime indukciją pagal (4.12) sekvencijos išvedimo aukštį l.

Indukcijos prielaida. Tarkime, $l = 0$, t.y. (4.12) yra aksioma. Tuomet (4.12) *sekvencijos antecedente ir sukcedente yra viena ir ta pati formulė F. Jei* $F \neq A\&B$, tai $\Gamma \vdash \Delta', A, \Delta''$ ir $\Gamma \vdash \Delta', B, \Delta''$ yra taip pat aksiomos ir kartu išvedamos skaičiavime. Jei $F = A\&B$, t.y. $\Gamma = \Gamma', A\&B, \Gamma''$, tai jų išvedimai yra tokie:

$$\frac{\Gamma', A, B, \Gamma'' \vdash \Delta', A, \Delta''}{\Gamma', A\&B, \Gamma'' \vdash \Delta', A, \Delta''}, \quad \frac{\Gamma', A, B, \Gamma'' \vdash \Delta', B, \Delta''}{\Gamma', A\&B, \Gamma'' \vdash \Delta', B, \Delta''}.$$

Tarkime, tvirtinimas teisingas, kai $l < m$. Parodysime, kad jis teisingas ir kai $l = m$.

1 *atvejis.* Pirmasis, iš apačios į viršų, (4.12) išvedime taisyklės taikymas yra $(\vdash \&)$ su centrine formule $A\&B$, t.y. išvedimo medis yra pavidalo (D_1, D_2 – išvedimų medžiai)

$$\frac{\dfrac{D_1}{\Gamma \vdash \Delta', A, \Delta''} \quad \dfrac{D_2}{\Gamma \vdash \Delta', B, \Delta''}}{\Gamma \vdash \Delta', A\&B, \Delta''}.$$

Tuomet nagrinėjamųjų sekvencijų išvedimų medžiai yra

$$\frac{D_1}{\Gamma \vdash \Delta', A, \Delta''}, \quad \frac{D_2}{\Gamma \vdash \Delta', B, \Delta''}.$$

2 *atvejis.* Pirmojo taisyklės taikymo centrinė formulė nėra $A\&B$ ir (4.12) sekvencijos išvedimo medžio aukštis lygus m.

Tarkime, išvedimo medis yra pavidalo

$$\frac{\dfrac{D_1}{\Gamma' \vdash \Delta_1', A\&B, \Delta_1''} \quad \dfrac{D_2}{\Gamma'' \vdash \Delta_2', A\&B, \Delta_2''}}{\Gamma \vdash \Delta', A\&B, \Delta''}.$$

Panašiai būtų įrodoma, jei (4.12) sekvencijos išvedime prielaidos būtų ne dvi, *o viena sekvencija. Abiejų išvedimų medžių*

$$\frac{D_1}{\Gamma' \vdash \Delta_1', A\&B, \Delta_1''}, \quad \frac{D_2}{\Gamma'' \vdash \Delta_2', A\&B, \Delta_2''}$$

aukščiai neviršija $(m-1)$. Todėl jiems galioja indukcijos prielaida:

a) $\Gamma' \vdash \Delta_1', A\&B, \Delta_1''$ išvedama tada ir tiktai tada, kai išvedamos abi sekvencijos $\Gamma' \vdash \Delta_1', A, \Delta_1''$ ir $\Gamma' \vdash \Delta_1', B, \Delta_1''$. Taigi atsiras pastarųjų dviejų išvedimų medžiai:

$$\frac{D_1'}{\Gamma' \vdash \Delta_1', A, \Delta_1''}, \qquad \frac{D_2'}{\Gamma' \vdash \Delta_1', B, \Delta_1''}.$$

b) $\Gamma'' \vdash \Delta_2', A\&B, \Delta_2''$ išvedama tada ir tiktai tada, kai išvedamos abi sekvencijos $\Gamma'' \vdash \Delta_2', A, \Delta_2''$ ir $\Gamma'' \vdash \Delta_2', B, \Delta_2''$. Taigi atsiras pastarųjų dviejų išvedimų medžiai:

$$\frac{D_3'}{\Gamma'' \vdash \Delta_2', A, \Delta_2''}, \qquad \frac{D_4'}{\Gamma'' \vdash \Delta_2', B, \Delta_2''}.$$

Tuomet $\Gamma \vdash \Delta', A, \Delta''$ bei $\Gamma \vdash \Delta', B, \Delta''$ išvedimų medžiai yra:

$$\frac{\dfrac{D_1'}{\Gamma' \vdash \Delta_1', A, \Delta_1''} \quad \dfrac{D_3'}{\Gamma'' \vdash \Delta_2', A, \Delta_2''}}{\Gamma \vdash \Delta', A, \Delta''}, \qquad \frac{\dfrac{D_2'}{\Gamma' \vdash \Delta_1', B, \Delta_1''} \quad \dfrac{D_4'}{\Gamma'' \vdash \Delta_2', B, \Delta_2''}}{\Gamma \vdash \Delta', B, \Delta''}.$$

Panašiai įrodomas ir likusiųjų taisyklių apverčiamumas. Teorema įrodyta.

Praktiškai išvedimo medis konstruojamas iš apačios į viršų, o taisyklės – apverčiamos, todėl patogu naudotis kitu išvedimo apibrėžimu.

4.9 apibrėžimas. *Sekvencijos išvedimu vadiname medžio pavidalo orientuotą grafą, kurio visos viršūnės pažymėtos sekvencijomis (šaknis – pradinė sekvencija) ir virš kiekvienos viršūnės visos tiesiogiai esančios sekvencijos gautos iš nagrinėjamąją viršūnę atitinkančios sekvencijos, pritaikius kurią nors sekvencinio skaičiavimo taisyklę. Visas medžio galines viršūnes, t.y. lapus, atitinkančios sekvencijos yra aksiomos.*

Išvedimas sekvenciniame skaičiavime G yra *mechaninis* ta prasme, kad, jei galima rinktis, kurią taisyklę taikyti, tai galima taikyti bet kurią iš jų (išplaukia iš 4.7 teoremos). Sekvencija yra išvedama tada ir tiktai tada, kai išvedamos visos gautosios. Sekvencinio skaičiavimo taisyklėms būdinga tai, kad pritaikius kurią nors jų gaunamos sekvencijos yra paprastenės, t.y. loginių operacijų skaičius vienetu mažesnis. Todėl, jei pradinėje sekvencijoje yra n operacijų įeičių, tai skaičiavimo taisykles pritaikius ne daugiau kaip n kartų arba visose medžio viršūnėse bus aksiomos, arba vienoje jų bus sekvencija, kuri nėra aksioma ir kurioje nėra loginių operacijų įeičių. Taigi *mechanine procedūra* patikrinama, ar sekvencija išvedama. Vadinasi, išvedamų sekvencijų aibė yra rekursyvi. Rekursyvi aibė yra ir jos papildinys.

4.10 apibrėžimas. *Antisekvencija vadiname reiškinį* $A_1, \ldots, A_n \dashv B_1, \ldots, B_m$; *čia* A_i $(i = 1, \ldots, n)$, B_i $(i = 1, \ldots, m)$ *yra formulės ir* $n + m \neq 0$.

Panagrinėkime skaičiavimą $\overline{G}$.

Aksiomos: $\Gamma \dashv \Delta$. Sekos Γ, Δ yra tik iš loginių kintamųjų. Be to, nėra to paties loginio kintamojo, įeinančio ir į antecedentą, ir į sukcedentą.

Taisyklės:

$$(\to\dashv_1)\ \frac{\Gamma', \Gamma'' \dashv \Delta', A, \Delta''}{\Gamma', A \to B, \Gamma'' \dashv \Delta', \Delta''}, \qquad (\to\dashv_2)\ \frac{\Gamma', B, \Gamma'' \dashv \Delta', \Delta''}{\Gamma', A \to B, \Gamma'' \dashv \Delta', \Delta''},$$

$$(\dashv\to)\ \frac{\Gamma', A, \Gamma'' \dashv \Delta', B, \Delta''}{\Gamma', \Gamma'' \dashv \Delta', A \to B, \Delta''},$$

$$(\&\dashv)\ \frac{\Gamma', A, B, \Gamma'' \dashv \Delta}{\Gamma', A\&B, \Gamma'' \dashv \Delta}, \qquad (\dashv\&)\ \frac{\Gamma \dashv \Delta', A_i, \Delta''}{\Gamma \dashv \Delta', A_1\&A_2, \Delta''}\ (i \in \{1,2\}),$$

$$(\vee\dashv)\ \frac{\Gamma', A_i, \Gamma'' \dashv \Delta}{\Gamma', A_1 \vee A_2, \Gamma'' \dashv \Delta}\ (i \in \{1,2\}), \qquad (\dashv\vee)\ \frac{\Gamma \dashv \Delta', A, B, \Delta''}{\Gamma \dashv \Delta', A \vee B, \Delta''},$$

$$(\neg\dashv)\frac{\Gamma', \Gamma'' \dashv \Delta', A, \Delta''}{\Gamma', \neg A, \Gamma'' \dashv \Delta', \Delta''}, \qquad (\dashv\neg)\ \frac{\Gamma', A, \Gamma'' \dashv \Delta', \Delta''}{\Gamma', \Gamma'' \dashv \Delta', \neg A, \Delta''}.$$

Pavyzdys. $p \vee q \dashv p\&q$.

$$\cfrac{\cfrac{\cfrac{\text{aksioma}}{q \dashv p}}{p \vee q \dashv p}}{p \vee q \dashv p\&q}.$$

Skaičiavimą, kuris skiriasi nuo G tik tuo, kad aksiomomis yra sekvencijos pavidalo $\Gamma', p, \Gamma'' \vdash \Delta', p, \Delta''$, t.y. aksiomos antecedente ir sukcedente turi būti to paties *loginio kintamojo* įeitys, pažymėkime G'.

4.8 teorema. *Sekvencija išvedama skaičiavime* G *tada ir tiktai tada, kai ji išvedama skaičiavime* G'.

Įrodymas. Jei kuri nors sekvencija išvedama skaičiavime G', tai kartu ji išvedama ir skaičiavime G. Parodysime, jei kuri nors sekvenija išvedama skaičiavime G, tai galima rasti ir jos išvedimą skaičiavime G'. Pakanka parodyti, kad kiekviena sekvencija pavidalo $\Gamma', A, \Gamma'' \vdash \Delta', A, \Delta''$ išvedama skaičiavime G'. Taikysime indukciją pagal loginių operacijų įeičių formulėje A skaičių (žymime $l(A)$).

Tarkime, kad $l(A) = 0$. Tuomet A yra loginis kintamasis ir sekvencija išvedama skaičiavime G', nes tai yra to skaičiavimo aksioma. Tarkime, teorema teisinga su $l(A) < m$. Parodysime, kad ji teisinga, kai $l(A) = m$. A gali būti vieno iš pavidalų: a) $B \to C$, b) $B\&C$, c) $B \vee C$, d) $\neg B$.

Sekvencija yra pavidalo $\Gamma', B \to C, \Gamma'' \vdash \Delta', B \to C, \Delta''$. Nagrinėjame medį

$$\cfrac{\cfrac{\Gamma', B, \Gamma'' \vdash \Delta', B, C, \Delta'' \quad \Gamma', C, B, \Gamma'' \vdash \Delta', C, \Delta''}{\Gamma', B \to C, B, \Gamma'' \vdash \Delta', C, \Delta''}}{\Gamma', B \to C, \Gamma'' \vdash \Delta', B \to C, \Delta''}.$$

Kadangi $l(B) < m$ ir $l(C) < m$, tai galioja indukcijos prielaida ir sekvencijas $\Gamma', B, \Gamma'' \vdash \Delta', B, C, \Delta''$ bei $\Gamma', C, B, \Gamma'' \vdash \Delta', C, \Delta''$, jei jos dar nėra G' aksiomos, galima pratęsti iki aksiomų.

Panašiai įrodomi ir likusieji atvejai. Teorema įrodyta.

4.5 Natūralioji dedukcija

Lenkas S. Jaskowski ir vokietis G. Gentzen 1934 m. nepriklausomai vienas nuo kito aprašė vadinamąsias ***natūraliosios dedukcijos*** sistemas. Skaičiavimai vadinami ***natūraliosiomis*** sistemomis, nes perėjimai nuo prielaidų prie išvadų geriausiai (iš visų žinomų skaičiavimų) modeliuoja tiek šnekamosios kalbos, tiek ir mokslininkų vartojamus išvedimuose (įrodymuose) samprotavimus.

Nagrinėjamasis skaičiavimas apibendrina natūraliųjų skaičiavimų variantus ir skiriasi nuo pradinių tokio tipo skaičiavimų. Kaip ir sekvenciniame skaičiavime, sekvencija $\vdash F$ išvedama tada ir tiktai tada, kai F tapačiai teisinga. Atkreipiame dėmesį, kad sekvencijų sukcedentuose yra ne daugiau kaip viena formulė.

Aksioma: $A \vdash A$

Loginių operacijų taisyklės:

- $\to$ įvedimas

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B},$$

- $\to$ eliminavimas

$$\frac{\Gamma \vdash A \qquad \Delta \vdash A \to B}{\Gamma, \Delta \vdash B},$$

- $\&$ įvedimas

$$\frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A\&B},$$

- $\&_1$ eliminavimas

$$\frac{\Gamma \vdash A\&B}{\Gamma \vdash A},$$

- $\&_2$ eliminavimas

$$\frac{\Gamma \vdash A\&B}{\Gamma \vdash B},$$

- $\vee_1$ įvedimas

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B},$$

- $\vee_2$ įvedimas

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B},$$

- $\vee$ eliminavimas

$$\frac{\Gamma \vdash A \vee B \qquad \Delta, A \vdash C \qquad \Delta', B \vdash C}{\Gamma, \Delta, \Delta' \vdash C},$$

- $\neg$ įvedimas

$$\frac{\Gamma, A \vdash}{\Gamma \vdash \neg A},$$

- $\neg_1$ eliminavimas

$$\frac{\Gamma \vdash A \qquad \Delta \vdash \neg A}{\Gamma, \Delta \vdash},$$

- $\neg_2$ eliminavimas

$$\frac{\Gamma, \neg A \vdash}{\Gamma \vdash A}.$$

Struktūrinės taisyklės:

- silpninimas

$$\frac{\Gamma \vdash}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A},$$

- perstatymas

$$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, B, A, \Delta \vdash C},$$

- kartojimas

$$\frac{\Gamma, A, A, \Delta \vdash C}{\Gamma, A, \Delta \vdash C}.$$

Čia Γ, Δ, Δ' yra baigtinės formulių sekos (gali būti ir tuščios), A, B, C – formulės. Taisyklių prielaidose esančių sekvencijų tvarka nesvarbi.

Dėl patogumo išvedimo medyje aptiktą sekvenciją $\Gamma,\ A,\ \Delta \vdash A$ taip pat laikysime aksioma, nes, naudojantis tik struktūrinėmis taisyklėmis, nesunku ją pratęsti iki norimos sekvencijos $A \vdash A$. Be to, naudojantis tik struktūrinėmis taisyklėmis, iš $\Gamma,\ \Delta \vdash A$ galima gauti $\Delta, \Gamma \vdash A$, todėl taikant taisykles galima nekreipti dėmesio į išvados antecedente esančių formulių tvarką.

Pateikiame išvedimų natūraliosios dedukcijos sistemoje porą pavyzdžių.

Pavyzdžiai:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A \vee B} \quad \neg(A \vee B) \vdash \neg(A \vee B)}{\neg(A \vee B), A \vdash}}{\neg(A \vee B) \vdash \neg A} \quad \dfrac{\dfrac{\dfrac{B \vdash B}{B \vdash A \vee B} \quad \neg(A \vee B) \vdash \neg(A \vee B)}{\neg(A \vee B), B \vdash}}{\neg(A \vee B) \vdash \neg B}}{\neg(A \vee B) \vdash \neg A \& \neg B}}{\vdash \neg(A \vee B) \to (\neg A \& \neg B)},$$

$$\dfrac{A \to B, B \to C, A \vdash B \to C \quad \dfrac{A \to B, A \vdash A \to B \quad B \to C, A \vdash A}{A \to B, B \to C, A \vdash B}}{A \to B, B \to C, A \vdash C}.$$

4.6 Disjunktų dedukcinė sistema

Priminsime, kad *disjunktu* vadiname literų disjunkciją, t.y formulę pavidalo $l_1 \vee \ldots \vee l_s$; čia l_i $(i = 1, \ldots, s)$ yra literos. Disjunktus žymime $C, C_0, C_1, \ldots$. Tuščias disjunktas žymimas simboliu $\square$. Šio skyrelio nagrinėjimo objektas – aibės, kurių elementai yra disjunktai bei iš jų išvedami disjunktai. *Deductio* (lotyniškai) – išvedimas.

Yra tik viena išvedimo taisyklė – ***atkirtos taisyklė***. Ji taikoma dviem disjunktams, rezultatas – vienas disjunktas. Taisyklė yra labai paprasta:

$$\frac{C_1 \vee p \vee C_2, \qquad C_3 \vee \neg p \vee C_4}{C_1 \vee C_2 \vee C_3 \vee C_4}.$$

Paaiškinsime ją. Taisyklę (sutrumpintai žymėsime AT) galima taikyti tik tuo atveju, kai viename disjunktų yra kurio nors loginio kintamojo (taisyklėje jis pažymėtas raide p) įeitis, o antrajame – jo neigimas. Kadangi $A \vee B \equiv B \vee A$ ir literų tvarka disjunktuose nesvarbi, tai atkirtos taisyklę galima nusakyti ir taip:

$$\frac{p \vee C_1, \qquad \neg p \vee C_2}{C_1 \vee C_2}.$$

Kai kada atkertamą literą patiksliname ir sakome, kad *taikome atkirtos taisyklę atžvilgiu kintamojo p*. Be to, tarsime, kad bet kurio loginio kintamojo įeitis bet kuriame disjunkte yra tik viena. Pavyzdžiui, $p \vee p \vee \neg q \vee \neg q$ laikysime lygiu $p \vee \neg q$ ir nagrinėsime pastarąjį.

4.11 apibrėžimas. *Sakome, kad disjunktas C išvedamas iš disjunktų aibės S (žymime $S \vdash C$), jei yra tokia baigtinė disjunktų seka $C_1, \ldots, C_u$, kurioje kiekvienas C_i $(i = 1, \ldots, u)$ arba priklauso aibei S, arba gautas iš kairėje jo stovinčių disjunktų pagal atkirtos taisyklę. Be to, $C_u = C$.*

Nagrinėjamoji išvedimo sistema dažniausiai vadinama *teiginių logikos rezoliucijų metodu.*

Pavyzdžiai. Skliaustuose nurodome, kaip gautas disjunktas, t.y. ar jis priklauso pradinei aibei S, ar gautas pagal atkirtos taisyklę.

1. $S = \{\neg p \vee q, \neg q \vee r, p \vee q \vee r, \neg r\}$. Parodysime, kad $S \vdash q$:
   $\neg p \vee q(S), \neg q \vee r(S), \neg p \vee r(AT), \neg r(S), \neg p(AT), p \vee q \vee r(S), q \vee r(AT), q(AT)$.
2. $S = \{\neg p \vee q \vee r, \neg p \vee \neg r, \neg q, p\}$. Parodysime, kad $S \vdash \Box$:
   $\neg p \vee q \vee r(S), p(S), q \vee r(AT), \neg q(S), r(AT), \neg p \vee \neg r(S), \neg p(AT), \Box(AT)$.

Disjunktų išvedimai aprašomi ir kitokiais būdais. Paaiškinsime tai remdamiesi antruoju pavyzdžiu.

a) Išvedimas kaip taisyklių taikymų seka:

$$\frac{\neg p \vee q \vee r, \quad p}{q \vee r}, \quad \frac{q \vee r, \quad \neg q}{r}, \quad \frac{\neg p \vee \neg r, \quad r}{\neg p}, \quad \frac{p, \quad \neg p}{\Box}.$$

b) Išvedimas kaip orientuotas grafas:

$$\cfrac{\cfrac{\cfrac{\cfrac{\neg p \vee q \vee r \quad p}{q \vee r} \quad \neg q}{r} \quad \neg p \vee \neg r}{\neg p} \quad p}{\Box}.$$

4.12 apibrėžimas. *Formulių aibė vadinama prieštaringąja, jei nesvarbu, kokia būtų interpretacija, aibėje yra bent viena klaidinga formulė.*

Pagal apibrėžimą aibė $S = \{C_1, \ldots, C_s\}$ prieštaringa tada ir tiktai tada, kai formulė $C_1 \& C_2 \& \ldots \& C_s$ yra tapačiai klaidinga. Atkreipiame dėmesį, kad tuščias disjunktas neįvykdomas.

4.9 teorema. *Jei $S \vdash C$ ir C nėra įvykdomas, tai aibė S prieštaringa.*

Įrodymas. Tarkime, $C_1, C_2, \dots, C_s = C$ yra disjunkto C išvedimas iš aibės S ir aibė S įvykdoma. Atsiras interpretacija ν, su kuria visi aibės S disjunktai teisingi.

Išvedimo ilgiu vadiname formulių, esančių išvedimo sekoje, skaičių. Taikydami indukciją pagal išvedimo ilgį s, parodysime, kad su ta pačia interpretacija ν ir C yra teisingas.

Jei $s = 1$, tai $C_1 \in S$ ir todėl $\nu(C_1) = t$. Tarkime, kad visi disjunktai C_i $(i < m)$ tenkina sąlygą $\nu(C_i) = t$. Parodysime, kad ir $\nu(C_m) = t$. C_m yra arba aibės S elementas (tuomet žinoma, kad $\nu(C_m = t)$), arba gautas iš kairėje jo esančių disjunktų (pažymėkime juos C_j, C_k) pagal atkirtos taisyklę.

Tarkime, kad $C_j = p \vee C'_j$, $C_k = \neg p \vee C'_k$ ir $C_m = C'_j \vee C'_k$. Pagal indukcijos prielaidą abu C_j, C_k teisingi su interpretacija ν. Galimi atvejai: a) $\nu(p) = t$, b) $\nu(p) = k$. Atveju a) $\nu(C'_k) = t$ ir todėl $\nu(C_m) = t$, o atveju b) – $\nu(C'_j) = t$ ir todėl $\nu(C_m) = t$, t.y. C_m įvykdomas su ta pačia interpretacija.

Taigi gavome: jei S įvykdoma, tai ir C įvykdomas. Jei $S \vdash C$ ir C nėra įvykdomas, tai aibė S prieštaringa. Teorema įrodyta.

Išvada. Jei iš disjunktų aibės S išvedamas tuščias disjunktas, tai aibė S prieštaringa.

Tarkime, aibės $S = \{C_1, \dots, C_m, C_{m+1}, \dots, C_s\}$ disjunktai tenkina savybes:

a) kuris nors loginis kintamasis p įeina į C_i $(i = m+1, \dots, s)$ ir neįeina į C_j $(j = 1, \dots, m)$,

b) litera $\neg p$ neįeina į jokį aibės S disjunktą.

Tuomet S prieštaringa tada ir tiktai tada, kai prieštaringa aibė $S' = \{C_1, \dots, C_m\}$. Iš tikrųjų, jei atsirastų interpretacija ν, su kuria $\nu(C_i) = t$ $(i = 1, \dots, m)$, tai pratęsus ją $(p = t)$, gautume, kad S įvykdoma. Jei nėra interpretacijos, su kuria S' įvykdoma, t.y. S' prieštaringa, tai tokia bus ir S.

Gavome tam tikrą tuščio disjunkto išvedimo paieškos taktiką: *išbraukti visus tuos disjunktus, kuriuose yra loginis kintamasis, tenkinantis sąlygas* a) ir b). Jei gauta aibė tuščia, tai ji įvykdoma (su $p = t$).

Panašiai galima elgtis ir tuo atveju, kai aibė $S = \{C_1, \dots, C_m, C_{m+1}, \dots, C_s\}$ tenkina salygas:

a) atsiras toks loginis kintamasis p, kad prieš kiekvieną jo įeitį būtų neigimas (yra tik įeitys $\neg p$),

b) litera $\neg p$ įeina į visas C_i $(i = m + 1, \ldots, s)$ ir neįeina į C_j $(j = 1, \ldots, m)$.

4.10 teorema. *Jei disjunktų aibė prieštaringa, tai iš S išvedamas tuščias disjunktas.*

Įrodymas. Taikome indukciją pagal skirtingų loginių kintamųjų, aptinkamų aibėje S, skaičių (žymime l). Pavyzdžiui, jei $S = \{\neg p \vee q, \neg p \vee \neg q, p\}$, tai $l = 2$; jei $S = \{p, \neg p, p \vee q, p \vee q \vee r\}$, tai $l = 3$.

Indukcijos bazė ($l = 1$). Tuomet S yra vieno iš pavidalų: a) $\{p\}$, b) $\{\neg p\}$, c) $\{p, \neg p\}$. Tik atveju c) aibė prieštaringa ir tik šiuo atveju išvedamas tuščias disjunktas.

Nesunku matyti, jei aibėje S yra disjunktas pavidalo $p \vee \neg p \vee C$, tai išbraukę jį iš S, gauname aibę, kuri prieštaringa tada ir tiktai tada, kai prieštaringa S. Tariame, kad tokių disjunktų nagrinėjamoje aibėje nėra.

Tarkime: jei aibėje S yra $l < m$ skirtingų loginių kintamųjų ir ji prieštaringa, tai iš jos išvedamas tuščias disjunktas. Parodysime: jei aibėje S yra $l = m$ skirtingų loginių kintamųjų ir ji prieštaringa, tai iš jos išvedamas tuščias disjunktas.

Tegul p yra kuris nors loginis kintamasis, tenkinantis sąlygas: yra aibėje S disjunktas, kuriame yra įeitis $\neg p$, ir yra kitas disjunktas, kuriame yra įeitis p ir nėra įeities $\neg p$. Jei tokio loginio kintamojo neatsirastų, tai aibė būtų įvykdoma.

Pažymėkime S_p aibę visų tų disjunktų, kuriuose yra įeitis p (kartu jai priklauso ir visi tie disjunktai, kuriuose yra įeitys $\neg p$). Suskaidome S_p į du poaibius. Aibei S_p^- priklauso visi tie disjunktai, kuriuose pasitaiko įeitys $\neg p$, likusieji disjunktai priklauso aibei S_p^+.

$$S_p = S_p^- \cup S_p^+ \quad \text{ir} \quad S_p^- \cap S_p^+ = \emptyset.$$

Taikome atžvilgiu p atkirtos taisyklę, imdami vieną disjunktą iš S_p^-, o kitą iš S_p^+. Visų gautų tokiu būdu disjunktų aibę pažymėkime $\mathrm{at}(S_p)$. Aibės $\mathrm{at}(S_p)$ disjunktuose nėra įeičių p (kartu ir $\neg p$). Parodysime, kad aibė S įvykdoma tada ir tiktai tada, kai įvykdoma

$$(S - S_p) \cup \mathrm{at}(S_p). \tag{4.13}$$

1. Tarkime, S įvykdoma. Tuomet visi disjunktai iš $\mathrm{at}(S_p)$ taip pat įvykdomi, nes gauti iš įvykdomų disjunktų, pritaikius atkirtos taisyklę (žr. 4.9 teoremos įrodymą). $S - S_p$ įvykdoma, kadangi yra įvykdomos aibės poaibis. Be to, abi aibės įvykdomos su viena ir ta pačia interpretacija. Taigi (4.13) įvykdoma.

2. Tarkime, aibė (4.13) įvykdoma. Vadinasi, yra interpretacija ν, su kuria visi disjunktai iš (4.13) teisingi. Parodysime, kad ν galima pratęsti taip, t.y priskirti kintamajam p tokią reikšmę, kad būtų įvykdoma S_p. Kartu su ta pačia interpretacija bus įvykdoma ir S.

Tegul $S_p^+ = \{C_1' \vee p, C_2' \vee p, \ldots, C_v' \vee p\}$, $S_p^- = \{C_1'' \vee \neg p, C_2'' \vee \neg p, \ldots, C_r'' \vee \neg p\}$. Tuomet

$$\text{at}(S_p) = \left\{ \begin{array}{llll} C_1' \vee C_1'', & C_1' \vee C_2'', & \ldots, & C_1' \vee C_r'' \\ \ldots & & & \\ C_v' \vee C_1'', & C_v' \vee C_2'', & \ldots, & C_v' \vee C_r'' \end{array} \right\}.$$

a) Tegul egzistuoja toks i $(1 \leqslant i \leqslant v)$, kad $\nu(C_i') = k$. Tuomet $\nu(C_j'') = t$ $(j = 1, \ldots, r)$ ir kintamajam p galime priskirti reikšmę t.

b) Sakykime, kad su visais i $(1 \leqslant i \leqslant v)$ $\nu(C_i') = t$. Tuomet kintamajam p priskiriame reikšmę k.

Gavome, kad aibė S įvykdoma tada ir tiktai tada, kai įvykdoma (4.13), t.y. aibė S prieštaringa tada ir tiktai tada, kai prieštaringa (4.13). Aibė (4.13) gauta iš S taikant atkirtos taisyklę ir jos disjunktuose aptinkamas ne daugiau kaip $(m-1)$ loginis kintamasis. Jai galioja indukcijos prielaida. Ji prieštaringa tada ir tiktai tada, kai iš jos išvedamas tuščias disjunktas. Teorema įrodyta.

Atkreipiame dėmesį, kad aibės $\{p \vee C_1, \neg p \vee C_2\}$ ir $\{C_1 \vee C_2\}$ yra vienu metu arba abi prieštaringos, arba ne, bet $(p \vee C_1)\&(\neg p \vee C_2)$ ir $C_1 \vee C_2$ nėra ekvivalenčios formulės. Pavyzdžiui, $S' = \{p \vee q, \neg p \vee r\}$, $S'' = \{q \vee r\}$. $(p \vee q)\&(\neg p \vee r)$ nėra ekvivalenti formulei $q \vee r$, nes su $p = q = k$, $r = t$ jų reikšmės skiriasi.

Paaiškinsime, kaip aprašytasis metodas taikomas loginėms išvadoms nustatyti. Klausiama, ar formulė F yra formulių aibės $\{F_1, \ldots, F_n\}$ loginė išvada. Tai, kas duota, įprasta rašyti virš brūkšnio, o išvadą (tikslą, tai, ką reikia įrodyti) – žemiau brūkšnio:

$$\begin{array}{c} F_1 \\ \vdots \\ F_n \\ \hline F \end{array}.$$

F yra loginė išvada tada ir tiktai tada, kai

$$(F_1\&\ldots\&F_n) \to F \tag{4.14}$$

yra tapačiai teisinga formulė. Norime patikrinti, ar (4.14) yra tapačiai teisinga formulė. Tuo tikslu taikysime *paneigimo metodą*, t.y. tikrinsime, ar (4.14) neigimas yra tapačiai klaidinga formulė:

$$\neg((F_1\&\ldots\&F_n)\rightarrow F)\equiv$$
$$\neg(\neg(F_1\&\ldots\&F_n)\vee F)\equiv$$
$$F_1\&\ldots\&F_n\&\neg F.$$

Gavome, kad F yra $\{F_1,\ldots,F_n\}$ loginė išvada tada ir tiktai tada, kai $\{F_1,\ldots, F_n,\neg F\}$ yra prieštaringa aibė, t.y. prie prielaidų aibės reikia prijungti tikslą su neigimu. Transformuojame $F_1,\ldots,F_n,\neg F$ į normaliąsias konjunkcines formas, pakeičiame konjunkcijos operacijas kableliais ir gauname disjunktų aibę S, kuri prieštaringa tada ir tiktai tada, kai F yra $\{F_1,\ldots,F_n\}$ loginė išvada. Savo ruožtu S prieštaringa tada ir tiktai tada, kai iš S išvedamas tuščias disjunktas.

Taigi norime nustatyti, ar F yra $\{F_1,\ldots,F_n\}$ loginė išvada. Šią problemą redukuojame į tuščio disjunkto išvedimo iš tam tikros disjunktų aibės uždavinį. Tokį uždavinio sprendimą vadiname *loginės išvados nustatymu naudojantis rezoliucijų metodu.*

Pavyzdžiai:

1. Sekmadieniais nedirbama. Šiandien darbo diena. Vadinasi, šiandien nėra sekmadienis.

Pažymėkime: s – *šiandien sekmadienis*, n – *šiandien nedarbo diena.*

Klausiama, ar samprotavimas

$$\frac{\begin{array}{c}s\rightarrow n\\ \neg n\end{array}}{\neg s}$$

teisingas (pagrįstas), t.y. ar $\neg s$ yra $\{s\rightarrow n,\neg n\}$ loginė išvada. Transformuojame pastarąją aibę į disjunktų aibę $S=\{\neg s\vee n,\neg n, s\}$. Tikriname, ar $S\vdash\Box$:

$$\frac{\neg s\vee n,\quad s}{n},\qquad \frac{n,\quad \neg n}{\Box}.$$

Taigi samprotavimas teisingas.

2. Algis, Jonas ir Petras susitarė dėl paskaitos lankymo tvarkos: a) jei į paskaitą neateina Jonas, tai neateina ir Algis, b) jei į paskaitą ateina Jonas, tai turi ateiti ir Algis su Petru. Klausiama, ar šiomis sąlygomis privalo paskaitoje dalyvauti Petras, kai žinoma, kad joje yra Algis?

Pažymėkime: a – *paskaitoje yra Algis*, j – *paskaitoje yra Jonas*, p – *paskaitoje yra Petras.*

Tuomet užduotis užrašoma taip:

$$\frac{\begin{array}{c}\neg j\rightarrow\neg a\\ j\rightarrow(a\&p)\end{array}}{a\rightarrow p}.$$

Tikriname, ar aibė $\{\neg j \to \neg a, j \to (a\&p), \neg(a \to p)\}$ prieštaringa. Transformuojame į disjunktų aibę $S = \{j \vee \neg a, \neg j \vee a, \neg j \vee p, a, \neg p\}$.

Iš S išvedamas tuščias disjunktas:

$$\frac{j \vee \neg a, \quad a}{j}, \quad \frac{j, \quad \neg j \vee p}{p}, \quad \frac{p, \quad \neg p}{\square}.$$

Taigi, laikantis paskaitos lankymo susitarimo, Petras privalo būti paskaitoje. QED (lot. *quod erat demonstrandum*) – ką ir reikėjo įrodyti.

Tam tikras privalumas tuščio disjunkto išvedimo paieškai gaunamas, kai nagrinėjamųjų disjunktų aibė susideda tiktai iš *Horno disjunktų*.

4.13 apibrėžimas. *Disjunktas* $l_1 \vee \ldots \vee l_s$ *vadinamas Horno, jei jame yra ne daugiau kaip viena neigimo įeitis.*

Pavyzdžiui, $\neg p \vee q \vee r$, $p \vee q \vee r$, $p \vee \neg q \vee s \vee r$ yra Horno disjunktai, bet $\neg p \vee \neg q \vee r$ nėra Horno disjunktas.

4.7 Skaičiavimų ryšys

Egzistuoja glaudus visų aprašytųjų formaliųjų sistemų ryšys. Šiame skyrelyje paaiškinsime tiktai sekvencinio skaičiavimo ir rezoliucijų metodo ryšį. Naudosimės amerikiečių logiko G. Mintso idėjomis, aprašytomis 1988 metais.

Nagrinėjame disjunktų aibę $S = \{C'_1, \ldots, C'_s\}$. Užduotis – patikrinti, ar S prieštaringa. Tikriname dviem skirtingais būdais: a) ar $C'_1, \ldots, C'_s \vdash$ išvedama sekvenciniame skaičiavime; b) ar iš S išvedamas tuščias disjunktas. Patikslinsime sekvencinį skaičiavimą bei rezoliucijų metodą, kuriais naudosimės šiame skyrelyje, ir parodysime, kaip pagal išvedimą sekvenciniame skaičiavime randamas pradinę sekvenciją atitinkančio disjunkto išvedimas.

Tarkime, $S = \{C'_1, \ldots, C'_s\}$ yra pradinė disjunktų aibė ir $p_1, \ldots, p_v$ – pilnas sąrašas loginių kintamųjų, įeinančių į S.

Sekvencinis skaičiavimas. *Aksiomos*: $\Gamma', l, \Gamma', \neg l, \Gamma'' \vdash$.

Išvedimo taisyklė:

$$(\vee)\quad \frac{\Gamma', l_1, \Gamma'' \vdash \quad \Gamma', l_2, \Gamma'' \vdash \quad \ldots \quad \Gamma', l_n, \Gamma'' \vdash}{\Gamma', l_1 \vee \ldots \vee l_n, \Gamma'' \vdash}; \tag{4.15}$$

čia l_i – literos. Be to, tariama, kad $\neg\neg p$ lygus p (p – loginis kintamasis).

Rezoliucijų skaičiavimas. *Aksiomos*: $C'_1, \ldots, C'_s$ ir $p_i \vee \neg p_i \vee C$ ($i = 1, \ldots, v$); čia C – kuris nors disjunktas, kuriame gali būti tik literos iš sąrašo $p_1, \neg p_1, \ldots, p_v, \neg p_v$.

Išvedimo taisyklė:

$$\frac{l_1 \vee \ldots \vee l_n, \quad \neg l_1 \vee C_1, \ldots, \neg l_n \vee C_n}{C_1 \vee \ldots \vee C_n};$$

čia $l_1 \vee \ldots \vee l_n$ priklauso pradinei disjunktų aibei S, t.y. aksioma.

Pastaba. Jei būtų įprasta atkirtos taisyklė

$$\frac{p \vee C', \quad \neg p \vee C''}{C' \vee C''},$$

tai reikalavimu, kad viena prielaidų ($p \vee C', \neg p \vee C''$) priklausytų pradinei disjunktų aibei, apibrėžtumėme nepilną skaičiavimą. Pavyzdžiui, iš $S = \{p \vee q, \neg p \vee q, p \vee \neg q, \neg p \vee \neg q\}$ nebūtų išvedamas tuščias disjunktas, nors ji ir yra prieštaringa.

Tarkime, turime $\Gamma \vdash$ išvedimą sekvenciniame skaičiavime. Parodysime, kaip jį galime transformuoti į išvedimą rezoliucijų skaičiavime. Γ yra sąrašas formulių, tarp kurių gali būti ir literų. Visų jų aibę pažymėkime raide P. Tada $P' = \{p_{i_1}, \ldots, p_{i_u}\}$ – pilnas sąrašas skirtingų loginių kintamųjų iš P, o $P'' = \{\neg p_{j_1}, \ldots, \neg p_{j_v}\}$ – likusios literos. $P = P' \cup P''$ ir $P' \cap P'' = \emptyset$. Sekvencijai $\Gamma \vdash$ priskiriame disjunktą $\neg p_{i_1} \vee \ldots \vee \neg p_{i_u} \vee p_{j_1} \vee \ldots \vee p_{j_v}$ (žymime $\neg P' \vee \neg P''$). Jį vadiname *sekvenciją atitinkančiu disjunktu*. Taisyklę (4.15) transformuojame į rezoliucijos taisyklę

$$\frac{l_1 \vee \ldots \vee l_n, \quad \neg l_1 \vee \neg P' \vee \neg P'', \ldots, \neg l_n \vee \neg P' \vee \neg P''}{\neg P' \vee \neg P''};$$

čia $\neg P' \vee \neg P''$ yra sekvenciją $\Gamma', \Gamma'' \vdash$ iš (4.15) atitinkantis disjunktas.

Pavyzdys. $p \vee q, \neg p \vee q, p \vee \neg q, \neg p \vee q \vdash$. Nagrinėsime tik vieną išvedimo šaką. Panašiai nagrinėjama ir antroji (pažymėta išvedime skaičiumi 2).

$$\cfrac{\cfrac{p, \neg p, p \vee \neg q, \neg p \vee \neg q \vdash \qquad \cfrac{\cfrac{p, q, p, \neg p \vdash \quad p, q, p, \neg q \vdash}{p, q, p, \neg p \vee \neg q \vdash} \quad p, q, \neg q, \neg p \vee \neg q \vdash}{p, q, p \vee \neg q, \neg p \vee \neg q \vdash}}{p, \neg p \vee q, p \vee \neg q, \neg p \vee \neg q \vdash}\ 2}{p \vee q, \neg p \vee q, p \vee \neg q, \neg p \vee \neg q \vdash}.$$

Pagal išvedimo medį konstruojame rezoliucijų metodu pradinę sekvenciją atitinkančio *disjunkto išvedimą*:

$$
\dfrac{p\vee q,\quad \dfrac{\neg p\vee q,\quad \dfrac{\text{aksioma}}{p\vee\neg p},\quad \dfrac{p\vee\neg q,\quad \dfrac{\text{aksioma}}{\neg p\vee\neg p\vee\neg q},\quad \dfrac{\text{aksioma}}{q\vee\neg p\vee\neg q}}{\neg q\vee\neg p}}{\neg p}\qquad \dfrac{2}{\neg q}}{\Box}.
$$

4.8 Pratimai

1. Raskite sekvencijų išvedimus natūraliosios dedukcijos sistemoje:

a) $\vdash (\neg A\vee\neg B)\to\neg(A\&B)$,

b) $\vdash (\neg A\&\neg B)\to\neg(A\vee B)$,

c) $\vdash \neg(A\&B)\to(\neg A\vee\neg B)$,

d) $A\&(B\vee C)\vdash (A\&B)\vee(A\&C)$,

e) $\vdash (A\vee B)\to(B\vee A)$,

f) $B\&(C\to D), (A\to B)\to(B\to C)\vdash D$,

g) $(A\to B)\to C, \neg(C\vee D), B\vdash$,

h) $(A\&B)\to C, A\&\neg C\vdash\neg B$,

i) $A\to(B\to C), A\to B, A\vdash C$,

j) $A\to B, B\to C, A\vdash C$,

k) $\vdash (\neg A\to B)\to(\neg B\to A)$.

2. Raskite formulių išvedimus teiginių skaičiavime:

a) $(A\&B)\to(B\&A)$, b) $(A\&B)\to(B\vee C)$,

c) $\neg\neg\neg\neg A\to A$.

3. Taikydami dedukcijos teoremą, raskite formulių išvedimus teiginių skaičiavime:

a) $(A\to B)\to((C\vee A)\to(C\vee B))$,

b) $(A\to(B\to C))\to((A\&B)\to C))$,

c) $(A\to B)\to((C\&A)\to(D\vee B))$,

d) $(A\to B)\to((A\&C)\to(B\&C))$.

4. Raskite 1 uždavinio sekvencijų išvedimus sekvenciniame skaičiavime G.

5. Raskite antisekvencijų išvedimus skaičiavime $\overline{G}$:

a) $p \to q, \neg q \vee r \dashv r \to p$,

b) $(p\&q) \to r, (p \vee r) \to q \dashv (q \vee r) \to p$,

c) $p \vee q, \neg p \vee r, r \vee \neg q \dashv p\&\neg r$.

6. Ar išvedamas tuščias disjunktas iš aibės:

a) $\{p \vee q, \neg p \vee \neg q\}$,

b) $\{r \vee \neg s \vee \neg u, \neg p \vee q \vee \neg u, p \vee \neg u \vee \neg s, \neg q \vee \neg r \vee p \vee \neg s, s, \neg s \vee u, \neg s \vee q, \neg p\}$?

7. Rezoliucijų metodu patikrinkite, ar formulė tapačiai klaidinga:

a) $(\neg p \vee q)\&\neg((q \to r) \to (\neg p \vee r))$,

b) $((p \to q) \to r)\&(\neg(r \vee s)\&q)$.

5 skyrius

Predikatų logika

5.1 Predikatų logikos formulės

Teiginių požymiai dar kitaip vadinami predikatais (lot. *praedicatum* – kas pasakyta, tarinys), t.y. tai, kas tvirtinama arba neigiama teiginyje. Pavyzdžiui, *Penki – natūralusis skaičius*. Čia objekto požymis yra natūralusis skaičius. Bendresne prasme predikatai suprantami kaip teiginiai su parametrais, t.y. tvirtinamojo pobūdžio sakiniai, kuriuose konkretizuoti požymiai, o objektai ne. Nurodyta tik objektų kitimo aibė. Pavyzdžiui, $3/4$ *ir* $4/5$ – *racionalieji skaičiai* yra teiginys, o pasakymas, kad *x ir y yra racionalieji skaičiai* – predikatas, jei greta nurodyta, kad, pavyzdžiui, realiųjų skaičių aibė yra parametrų kitimo aibė. Pakeitę sakinyje x, y konkrečiais realiaisiais skaičiais, gauname teisingą arba klaidingą teiginį. Taigi teiginys, kurio *kai kuriose vietose* objektai pakeisti parametrais, virsta predikatu. Todėl ir predikatai yra vadinami *vienviečiais, dviviečiais, n-viečiais*, o parametrai – ***individiniais kintamaisiais***.

Pateiksime tikslesnį predikato apibrėžimą.

5.1 apibrėžimas. *n-viečiu predikatu aibėje A vadiname vienareikšmę n argumentų funkciją, kurios apibrėžimo sritis yra aibė A ir reikšmių aibė –* $\{t, k\}$.

Pavyzdžiai:

- *x ir y kaimynai.* Vilniaus miesto gyventojų aibė.
- *x ūgis didesnis kaip* 200 cm. Lietuvos piliečių aibė.
- *x ir y statmenos.* Tiesių plokštumoje aibė.
- *x dalijasi iš* 5. Sveikųjų skaičių aibė.
- $x + y = z$. Natūraliųjų skaičių aibė.

Predikatus bei predikatinius kintamuosius (kai funkcija nėra konkretizuota) žymime didžiosiomis lotyniškomis raidėmis (kartais su indeksais). Skliaustuose dažniausiai nurodome ir vietų (argumentų) skaičių:

$$P(x, y, z),\ Q(x_1, x_2, \ldots, x_n),\ R(x), \ldots .$$

Taigi nagrinėjame trijų rūšių kintamuosius:

- *loginius* $p, q, r, \ldots, p_1, p_2, p_3, \ldots,$
- *predikatinius* $P_i(x_1, x_2, \ldots, x_n), \ldots,$
- *individinius* $x, y, z, \ldots, x_1, x_2, x_3, \ldots .$

Teiginių logikos abėcėlę praplečiame predikatiniais ir individiniais kintamaisiais bei dviem ***kvantoriais*** (lot. *quantum* – kiek). Tai ***bendrumo kvantorius*** (žymime $\forall$) bei ***egzistavimo kvantorius*** (žymėsime $\exists$). Tai loginis veiksmas, kiekybiškai apibūdinantis objektų sritį. Ženklas $\exists$ yra angliško žodžio *Exist*, vokiškojo *Existieren* apversta pirmoji raidė, kurios vidurinis brūkšnelis prailgintas. ženklas $\forall$ yra angliškojo žodžio *All*, vokiškojo *Alle* apversta pirmoji raidė. Kvantorius naudojame tik kartu su individiniais kintamaisiais (aukštesnės eilės logikose ir su kitais objektais) ir vadiname ***kvantoriniais kompleksais***. Užrašą $\forall x, \forall y, \forall z, \forall x_1, \ldots, \exists x, \exists y, \exists z, \exists x_1, \ldots$ iki daugtaškio skaitome „kiekvienam x“, „kiekvienam x teisinga“, „kad ir koks būtų x“, o po daugtaškio – „egzistuoja x“, „egzistuoja x, su kuriuo teisinga“, „yra toks x“.

5.2 apibrėžimas. *Predikatų logikos formulių aibė $\mathcal{F}$ yra tokia pati mažiausia aibė, kad:*

- *predikatiniai kintamieji priklauso aibei $\mathcal{F}$,*
- *jei F yra formulė, tai $\neg F$ – taip pat formulė,*
- *jei F, G yra formulės, tai $(F \& G)$, $(F \vee G)$, $(F \to G)$ – taip pat formulės,*
- *jei F yra formulė, x – individinis kintamasis, tai $\forall x F$, $\exists x F$ – taip pat formulės.*

Pavyzdžiai:

$$\forall x \exists y ((P(x, y) \& Q(y, x, z)) \to \exists z R(z, x, y)), \tag{5.1}$$

$$(P(x, y, z) \vee \forall x \forall z (Q(y, z, x) \vee \neg Q(x, y, z))). \tag{5.2}$$

Dėl paprastumo formules rašome be išorinių skliaustų.

Kaip matome iš apibrėžimo, konstruojant formulę naudojamės kitomis, jau turimomis formulėmis, kurias, taip pat ir galutinę, vadiname gautosios ***poformuliais***.

Pavyzdys. Šios formulės yra (5.1) ***poformuliai***:

$$P(x, y), \quad Q(x, y, z), \quad P(x, y)\&Q(x, y, z), \quad R(z, x, y), \quad \exists z R(z, x, y),$$

$$(P(x, y)\&Q(x, y, z)) \to \exists z R(z, x, y), \quad \exists y((P(x, y)\&Q(x, y, z)) \to \exists z R(z, x, y)),$$

$$\forall x \exists y((P(x, y)\&Q(x, y, z)) \to \exists z R(z, x, y)).$$

Kaip matome, formulė yra tam tikros abėcėlės žodis. Kuris nors žodis (atskiru atveju raidė), pavyzdžiui, individinis kintamasis x, gali būti aptinkamas (tai vadinsime ***įeitimi***) formulėje F (peržiūrint ją iš kairės į dešinę) ne vieną kartą. Priklausymą kvantoriniam kompleksui nelaikysime individinio kintamojo įeitimi. Pavyzdžiui: (5.1) formulėje yra trys x įeitys, trys y įeitys, dvi z įeitys ir nė vienos x_1 įeities; (5.2) formulėje yra po tris x, y, z įeitis. Panašiai apibrėžiamos ir *poformulio įeities* bei *kvantorinio komplekso įeities* sąvokos.

Atkreipiame dėmesį, kad, pavyzdžiui, $P(x, x, y, z, y, y)$ taip pat yra predikatinis kintamasis, t.y. kai kurios (atskiru atveju visos) individinių kintamųjų įeitys tame pačiame predikatiniame kintamajame gali būti vienodos.

5.3 apibrėžimas. *Tarkime, įeitis QxG ($Q \in \{\forall, \exists\}$) yra F poformulis. Tuomet nagrinėjamąją formulės G įeitį vadiname **kvantoriaus Q bei kvantorinio komplekso Qx įeities veikimo sritimi**.*

Kai iš konteksto aišku, apie kurią kvantoriaus įeitį kalbama, tai, užuot vartojus terminą *kvantoriaus įeities veikimo sritis*, sakoma *kvantoriaus veikimo sritis*.

5.4 apibrėžimas. *Individinio kintamojo x įeitis formulėje F vadinama **suvaržytąja**, jei ji patenka į kvantorinio komplekso $\forall x$ arba $\exists x$ veikimo sritį. Priešingu atveju nagrinėjamoji individinio kintamojo įeitis vadinama **laisvąja**.*

Pavyzdys. Visos x bei y įeitys (5.1) formulėje yra suvaržytos, o z – pirmoji įeitis laisva, antroji – suvaržyta. Kitoje (5.2) formulėje visos y įeitys yra laisvos, o pirmosios x, z įeitys – laisvos, antrosios bei trečiosios – suvaržytos.

Užuot vartoję terminą *individinis kintamasis*, dažniausiai sakysime tiesiog *kintamasis*. Jei formulėje F yra bent viena laisva x įeitis, kintamasis x toje formulėje yra laisvasis.

5.5 apibrėžimas. *Formulė vadinama **uždarąja**, jei joje nėra laisvųjų kintamųjų įeičių.*

Nenagrinėsime formulių, kuriose yra tokie poformuliai QxG, WxF (Q, $W \in \{\forall, \exists\}$), kad WxF yra G poformulis. Tokias formules laikysime netaisyklingomis. Pavyzdžiui, $\forall x \exists x P(x)$.

5.2 Semantika

Norint nustatyti tam tikros formulės vertę, reikia konkretizuoti *individinių kintamųjų apibrėžimo aibę, predikatinius kintamuosius ir laisvuosius kintamuosius.* Nuo jų parinkimo dažniausiai priklauso ir formulės vertė. Pavyzdžiui, ar tvirtinimas *Visi studentai gauna stipendiją* teisingas, ar ne, priklauso nuo pasirinktos studentų aibės.

Formulė $\forall x F(x)$ teisinga aibėje A, jei, nesvarbu, koks būtų aibės A elementas a, $F(a)$ ($F(a)$ gauta iš $F(x)$, pakeitus joje visas x laisvąsias įeitis į a) yra teisinga. Formulė $\forall x F(x)$ klaidinga, jei yra bent vienas aibės A elementas a, su kuriuo $F(a)$ klaidinga.

Kai A baigtinė (tarkime, $A = \{a_1, \ldots, a_n\}$), bendrumo kvantorių galima eliminuoti:

$$\forall x F(x) \equiv F(a_1) \& F(a_2) \& \ldots \& F(a_n).$$

Formulė $\exists x F(x)$ teisinga aibėje A, jei *galima rasti bent vieną* aibės A elementą (pažymėkime jį a), su kuriuo $F(a)$ teisinga. Formulė $\exists x F(x)$ klaidinga, jei nesvarbu, koks būtų aibės A elementas a, $F(a)$ klaidinga.

Kai A baigtinė, egzistavimo kvantorių galima eliminuoti:

$$\exists x F(x) \equiv F(a_1) \vee F(a_2) \vee \ldots \vee F(a_n).$$

Taigi predikatų logikos formulę, kurioje individinių kintamųjų kitimo aibė baigtinė, galima transformuoti į teiginių logikos formulę.

5.6 apibrėžimas. *Tarkime, kad $P_1^{k_1}, \ldots, P_n^{k_n}$ yra pilnas sąrašas predikatinių kintamųjų (viršutinis indeksas nurodo predikatinio kintamojo vietų skaičių), o $x_1, \ldots, x_m$ – pilnas sąrašas laisvųjų individinių kintamųjų, aptinkamų formulėje F. Sąrašą $< M; R_1^{k_1}, \ldots, R_n^{k_n}; a_1, \ldots, a_m >$ vadiname formulę F atitinkančia **struktūra** S; čia M – kuri nors netuščia aibė, $R_i^{k_i}$ ($i = 1, 2, \ldots, n$) – kurie nors predikatai (juos vadiname atitinkančiais predikatinius kintamuosius $P_i^{k_i}$), kurių apibrėžimo aibė yra M, a_i ($i = 1, 2, \ldots, m$) – kurie nors aibės M elementai (juos vadiname atitinkančiais laisvuosius individinius kintamuosius x_i).*

5.7 apibrėžimas. *Sakome, kad* ***formulė F teisinga*** *(klaidinga) ją atitinkančioje* ***struktūroje S****, jei pakeitę formulėje F predikatinius kintamuosius juos atitinkančiais predikatais, o laisvuosius kintamuosius – juos atitinkančiais elementais iš struktūros S, gauname teisingą (klaidingą) formulę.*

Kalbėdami apie formules bei struktūras, nagrinėjame tik formules *atitinkančias* struktūras, todėl žodį „atitinkanti" praleisime.

5.8 apibrėžimas. *Formulė vadinama* ***įvykdomąja****, jei yra struktūra, kurioje ji teisinga.*

5.9 apibrėžimas. *Formulė vadinama* ***tapačiai teisinga*** *(tautologija), jei ji teisinga bet kurioje struktūroje.*

5.10 apibrėžimas. *Formulė vadinama* ***tapačiai klaidinga****, jei ji klaidinga bet kurioje struktūroje.*

Pavyzdžiai:

1. Formulė $\forall x\forall y\forall z((P(x,y)\&P(y,z)) \rightarrow P(x,z))$ įvykdoma struktūroje $< R; =>$, kadangi $\forall x\forall y\forall z((x=y\&y=z) \rightarrow x=z)$ yra teisinga.

2. $(P(x,y)\&\neg P(x,x))\&\forall x\exists y P(x,y)$. Parašysime jos laisvuosius kintamuosius tokia tvarka: x, y. Formulė įvykdoma struktūroje $< N; <; 3, 5 >$, kadangi $(3 < 5\&\neg(3 < 3))\&\forall x\exists y(x < y)$ yra teisinga.

3. Formulė $\forall x P(x) \rightarrow \exists x P(x)$ tapačiai teisinga, nes nesvarbu, kokia būtų struktūra $< M; R >$, kiekvieną kartą, kai toje struktūroje teisinga $\forall x R(x)$, joje teisinga ir $\exists x R(x)$. Šiuo atveju yra toks x, su kuriuo $R(x)$ teisingas – tai bet kuris aibės M elementas. O jei struktūroje $\forall x P(x)$ klaidinga, tai nagrinėjamoji formulė taip pat teisinga.

4. Formulė $\exists x\forall y(P(x,x)\&\neg P(x,y))$ tapačiai klaidinga. Tarkime, formulė teisinga struktūroje $< M; R >$. Tuomet kad ir koks būtų aibės M elementas y, atsiras toks aibės M elementas (pažymėkime jį raide a), su kuriuo $R(a,y)$ klaidingas. Tuo pačiu klaidingas ir $R(a,a)$. Taigi su šiuo pasirinktuoju elementu a pradinė formulė klaidinga. Tas pats ir su bet kuriuo kitu elementu, su kuriuo $\exists x\forall y\neg R(x,y)$ teisinga. Vadinasi, nėra tokios struktūros, kurioje nagrinėjamoji formulė būtų teisinga.

Pateiktieji pavyzdžiai nesudėtingi, ir todėl nesunku nustatyti, ar formulės įvykdomos, tapačiai teisingos, ar tapačiai klaidingos. O kaip bendru atveju? Ar egzistuoja algoritmas, kuriuo naudojantis galima būtų pasakyti, ar tam tikra formulė įvykdoma, tapačiai teisinga, ar tapačiai klaidinga? Deja, tokio algoritmo nėra. Visos tos klasės neišsprendžiamos. Pirmasis 1936 m. tai įrodė A. Church. Tą faktą suformuluosime kaip teoremą be įrodymo.

5.1 teorema. *Įvykdomų, tapačiai teisingų bei tapačiai klaidingų predikatų logikos formulių aibės yra nerekursyviosios.*

Pastebėsime, kad skirtingi sakiniai

Kiekvienas grybas, kuris nėra nuodingas, yra valgomas,
Kiekvienas grybas, kuris nėra valgomas, yra nuodingas,
Viskas, kas nėra nei valgomas grybas, nei nuodingas grybas, nėra grybas

gali būti užrašyti viena ir ta pačia formule

$$\forall x(\text{grybas}(x) \to (\neg\text{nuodingas.grybas}(x) \to \text{valgomas.grybas}(x)).$$

5.11 apibrėžimas. *Dvi formulės F, G vadinamos* ***ekvivalenčiosiomis*** *(žymime $F \equiv G$), jei bet kurioje struktūroje jos arba abi teisingos, arba abi klaidingos.*

5.2 teorema. *Predikatų logikoje šios poros formulių ekvivalenčios:*

$$\forall x \forall y H \equiv \forall y \forall x H, \tag{5.3}$$

$$\exists x \exists y H \equiv \exists y \exists x H, \tag{5.4}$$

$$\forall x H(x) \equiv \forall y H(y), \tag{5.5}$$

$$\exists x H(x) \equiv \exists y H(y), \tag{5.6}$$

(čia y – naujas kintamasis, neįeinantis į formulę $H(x)$)

$$\neg\forall x H \equiv \exists x \neg H, \tag{5.7}$$

$$\neg\exists x H \equiv \forall x \neg H. \tag{5.8}$$

Įrodymas. Įrodysime tik (5.7) ekvivalentumą. Tarkime, $\neg\forall x H$ teisinga struktūroje S. Tuomet $\forall x H$ joje klaidinga. Vadinasi, atsiras toks struktūros aibės elementas a, su kuriuo $H'(a)$ klaidinga. Čia H' gauta iš H, pakeitus pastarojoje, atsižvelgiant į jos struktūrą, predikatinius ir laisvuosius kintamuosius. $H'(a)$ gauta iš H' visas laisvąsias x įeitis joje pakeitus į a. Tuomet $\neg H'(a)$ teisinga, kartu teisinga ir $\exists x \neg H$.

Tarkime, kad $\neg\forall x H$ struktūroje S klaidinga. Tuomet joje $\forall x H$ teisinga. Vadinasi, kad ir koks būtų struktūros aibės elementas a, $H'(a)$ teisinga, t.y. *su bet kuriuo* struktūros aibės elementu a, $\neg H'(a)$ klaidinga ir kartu klaidinga $\exists x \neg H$.

Taigi įrodėme, kad nesvarbu, kokia būtų struktūra, kairėje ir dešinėje ekvivalentumo ženklo esančios formulės yra arba abi teisingos, arba abi klaidingos, t.y. jos ekvivalenčios.

Kitus ekvivalentumus paliekame įrodyti per pratybas. Teorema įrodyta.

Formulės $\forall x \exists y H$, $\exists y \forall x H$ nėra ekvivalenčios.

Nesunku rasti struktūrą, kurioje viena iš formulių būtų teisinga, o antroji – klaidinga. Pavyzdžiui, $S =< N; >>$. Pirmoji formulė $\forall x \exists y(y > x)$ natūraliųjų skaičių aibėje teisinga, o $\exists y \forall x(y > x)$ – klaidinga.

Dažnai neigimo įkėlimo (5.7), (5.8) taisyklės naudojamos norint patikslinti įvairias sąvokas (*funkcija nėra tolydi, seka nekonverguoja* ir pan.). Predikatas $P(x, y)$ vadinamas *refleksyviuoju*, jei $\forall x P(x, x)$ teisinga. Pavyzdžiui, $x = y$ realiųjų skaičių aibėje, $x \geqslant y$ natūraliųjų skaičių aibėje, $x \parallel y$ plokštumos tiesių aibėje. Predikatas $P(x, y)$ vadinamas *irefleksyviuoju*, jei teisinga $\forall x \neg P(x, x)$. Pavyzdžiui, $x > y$ natūraliųjų skaičių aibėje, $x \perp y$ plokštumos tiesių aibėje. O ką reiškia teiginys, kad *predikatas $P(x, y)$ nėra refleksyvusis*? Gal tai tolygu sąvokai *irefleksyvusis predikatas*? *Nėra refleksyvusis*, arba *netiesa, kad refleksyvusis*, užrašomas formule $\neg \forall x P(x, x)$. Ji ekvivalenti $\exists x \neg P(x, x)$. Kaip matome, tai skirtingos sąvokos. Pavyzdžiui, $5x = y$ sveikųjų skaičių aibėje nėra refleksyvusis ir nėra irefleksyvusis.

5.3 Pavyzdys formulės, įvykdomos begalinėje ir neįvykdomos jokioje baigtinėje aibėje

Norime nustatyti, ar tam tikra formulė įvykdoma. Naudojamės tokiu algoritmu.

Imame struktūras, kurių aibėse yra tik po vieną elementą (nesvarbu, koks tas elementas, o svarbu, kiek jų yra struktūros aibėje). Tokių struktūrų skaičius baigtinis. Tikriname, ar pasirinkta formulė teisinga bent vienoje iš jų. Jei taip, tai darbą baigiame ir atsakymas – *formulė įvykdoma*. Jei ne, tai darbą tęsiame struktūrų aibių galią padidinę vienetu, t.y. nagrinėjame struktūras, kurių aibės yra iš dviejų elementų. Ir vėl tokių struktūrų yra baigtinis skaičius. Tikriname, ar mūsų formulė teisinga bent vienoje iš jų. Jei taip, tai darbą baigiame ir atsakymas – *formulė įvykdoma*. Jei ne, tai darbą tęsiame struktūrų aibių galią padidinę vienetu.

Ar galime tikėtis, kad tuo atveju, kai formulė įvykdoma, naudodamiesi aprašytuoju algoritmu, rasime struktūrą, kurioje ji teisinga? Suprantama, jei ji neįvykdoma, tai aprašytasis procesas niekada nesibaigs. Deja, ne.

5.3 teorema. *Formulė*

$$\forall x \exists y P(x, y) \& \forall x \neg P(x, x) \& \forall x \forall y \forall z ((P(x, y) \& P(y, z)) \to P(x, z))$$

įvykdoma begalinėje ir neįvykdoma jokioje baigtinėje aibėje.

Įrodymas. Formulė įvykdoma begalinėje aibėje (t.y. atsiras struktūra su begaline aibe, kurioje ji bus teisinga). Imkime $S =< N; <>$. Formulė yra konjunkcija trijų poformulių:

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

$$\forall x \neg P(x, x),$$

$$\forall x \forall y \forall z ((P(x, y) \& P(y, z)) \to P(x, z)).$$

Struktūroje S jos visos teisingos:

$$\forall x \exists y (x < y),$$

$$\forall x \neg (x < x),$$

$$\forall x \forall y \forall z ((x < y) \& (y < z)) \to (x < z)).$$

Parodysime, kad ir kokia būtų struktūra su baigtine aibe, formulė toje struktūroje klaidinga. Įrodysime prieštaros metodu. Tarkime, formulė teisinga struktūroje $S =< M; Q(x, y) >$ ir M yra baigtinė aibė. Jos elementus pažymėkime $a_1, a_2, \ldots, a_m$. Predikatas $Q(x, y)$ ir apibrėžimo aibė M tokie, kad visos trys formulės yra teisingos:

(1) $\forall x \exists y Q(x, y)$,

(2) $\forall x \neg Q(x, x)$,

(3) $\forall x \forall y \forall z ((Q(x, y) \& Q(y, z)) \to Q(x, z))$.

Iš aibės M elementų konstruojame begalinę seką $a_{i_1}, a_{i_2}, a_{i_3}, \ldots$ tokiu būdu. Pirmąjį narį a_{i_1} imame kurį nors iš aibės M elementų. Antrąjį narį parenkame taip, kad $Q(a_{i_1}, a_{i_2})$ būtų teisinga. Toks bent vienas elementas yra, nes pagal prielaidą (1) formulė teisinga. Trečiąjį narį parenkame taip, kad $Q(a_{i_2}, a_{i_3})$ būtų teisinga. Vėl iš pirmosios formulės teisingumo išplaukia, kad atsiras bent vienas toks elementas. Taigi seką konstruojame taip, kad $Q(a_{i_j}, a_{i_{j+1}}) = t$ ($j = 1, 2, 3, \ldots$). Imame jos pirmuosius $(m + 1)$ narių:

$$a_{i_1}, a_{i_2}, \ldots, a_{i_{m+1}}.$$

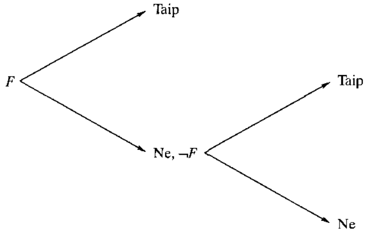
Kadangi aibėje iš viso yra m elementų, tai sekoje yra bent du vienodi nariai.

Tarkime, $a_{i_k} = a_{i_{k+s}}$. Iš to, kad (3) formulė teisinga, išplaukia, jog $Q(x, y)$ tranzityvus. Todėl $Q(a_{i_k}, a_{i_{k+2}}) = t$, $Q(a_{i_k}, a_{i_{k+3}}) = t, \ldots, Q(a_{i_k}, a_{i_{k+s}}) = t$. Bet $a_{i_k} = a_{i_{k+s}}$. Iš čia išplaukia, kad $Q(a_{i_k}, a_{i_k}) = t$. Bet tai prieštarauja (2) formulei, kuri tvirtina, kad ir koks būtų aibės M elementas a_i, $Q(a_i, a_i) = k$. Teorema įrodyta.

Vadovėlyje nagrinėjami įvairūs metodai, kuriais nustatoma, ar formulės yra *tapačiai teisingos*, ar *tapačiai klaidingos*, ar *įvykdomos*. Pastebėsime, kad iš efektyvios procedūros egzistavimo vienai iš išvardintųjų problemų spręsti, išplaukia tokios procedūros egzistavimas ir likusioms dviem, t.y. tos problemos tarpusavyje tampriai susijusios.

Tarkime, egzistuoja procedūra, kuria naudojantis galima patikrinti, ar bet kuri formulė F yra tapačiai teisinga. Tada egzistuoja ir procedūra, nustatanti, ar bet kuri formulė tapačiai klaidinga, bei ar ji įvykdoma.

Iš tikrųjų norėdami patikrinti, ar formulė F tapačiai klaidinga, tereikia nustatyti, ar $\neg F$ tapačiai teisinga. Norėdami patikrinti, ar formulė F įvykdoma, iš pradžių tikriname, ar F tapačiai teisinga. Jei *taip*, tai ji įvykdoma, jei *ne* – tikriname, ar $\neg F$ tapačiai teisinga. Jei *taip*, tai formulė *neįvykdoma*, jei *ne* – *įvykdoma*.



Pagal apibrėžimą struktūrų aibe gali būti bet kurios galios aibė. Iš 5.3 teoremos išplaukia, kad negalime apsiriboti vien tik baigtinėmis aibėmis. Tačiau kita teorema tvirtina, jog nebūtina nagrinėti individų aibių, kurių galia didesnė kaip skaičioji.

5.4 teorema (Löwenheimo–Skolemo). *Jei predikatų logikos formulė įvykdoma, tai ji įvykdoma ir kurioje nors numeruojamoje aibėje.*

5.4 Normaliosios priešdėlinės formos

Šiame skyrelyje parodysime, kad kiekvieną formulę galime transformuoti į tam tikrą specialų pavidalą, vadinamą *priešdėline normaliąja forma.*

5.12 apibrėžimas. *Formulės F* ***normaliąja priešdėline forma*** *vadiname jai ekvivalenčią formulę pavidalo* $Q_1x_1Q_2x_2\cdots Q_nx_nG$; *čia G – formulė, kurioje nėra kvantorių (bekvantorė formulė, dar vadinama* ***matrica****), o* $Q_1x_1Q_2x_2\cdots Q_nx_n$ *vadiname formulės F* ***prefiksu*** $(Q_i \in \{\forall, \exists\}(i = 1, \ldots, n))$.

5.5 teorema. *Kad ir kokia būtų predikatų logikos formulė F, atsiras jai ekvivalenti normaliosios priešdėlinės formos.*

Įrodymas. Nesvarbu, kokia yra formulė F, ją galima transformuoti į priešdėlinę normaliąją, t.y. visus kvantorius iškelti į formulės priekį, naudojantis ekvivalenčių formulių poromis.

$$\exists xA(x) \equiv \exists yA(y),$$

$$\forall xA(x) \equiv \forall yA(y);$$

čia y – naujasis kintamasis, neįeinantis į $A(x)$. Toks veiksmas vadinamas kintamojo pervardijimu.

$$\forall x(A(x)\&B) \equiv \forall xA(x)\&B, \tag{5.9}$$

$$\forall x(A(x) \vee B) \equiv \forall xA(x) \vee B, \tag{5.10}$$

$$\exists x(A(x)\&B) \equiv \exists xA(x)\&B, \tag{5.11}$$

$$\exists x(A(x) \vee B) \equiv \exists xA(x) \vee B; \tag{5.12}$$

čia formulėje B nėra x.

$$\neg\forall xA(x) \equiv \exists x\neg A(x),$$

$$\neg\exists xA(x) \equiv \forall x\neg A(x).$$

Be to, galima naudotis ir kitomis poromis ekvivalenčių formulių. Kartu suprastinsime priešdėlinę normaliąją formą. Prefikse bus mažiau kvantorinių kompleksų:

$$\forall x(A(x)\&B(x)) \equiv \forall xA(x)\&\forall xB(x),$$

$$\exists x(A(x) \vee B(x)) \equiv \exists xA(x) \vee \exists xB(x).$$

Bet

$$\forall x(A(x) \vee B(x)) \not\equiv \forall xA(x) \vee \forall xB(x).$$

Struktūroje, kurios aibe yra N, $A(x) - x < 5$, $B(x) - x \geqslant 5$, kairioji formulė teisinga, o dešinioji – klaidinga.

$$\exists x(A(x)\&B(x)) \not\equiv \exists xA(x)\&\exists xB(x).$$

Struktūroje, kurios aibe yra N, $A(x) - x < 3$, $B(x) - x > 10$, kairioji formulė klaidinga, o dešinioji – teisinga.

Naudodamiesi aprašytomis ekvivalenčių formulių poromis, bet kurią formulę galime transformuoti į priešdėlinę normaliąją formą. Jei formulėje yra ir kitos loginės operacijos, tai jas išreiškiame per $\neg$, $\&$, $\vee$. Teorema įrodyta.

Pavyzdys. Transformuokime

$$\forall x\exists yA(x,y) \to \forall y(B(y,y)\&\exists xA(y,x))$$

į priešdėlinę normaliąją formą.

Sprendimas:

$$\neg\forall x\exists yA(x,y) \vee \forall y(B(y,y)\&\exists xA(y,x)),$$

$$\exists x\forall y\neg A(x,y) \vee \forall y(B(y,y)\&\exists xA(y,x)),$$

$$\exists u\forall v\neg A(u,v) \vee \forall y(B(y,y)\&\exists xA(y,x)),$$

$$\exists u\forall v\forall y\exists x(\neg A(u,v) \vee (B(y,y)\&A(y,x))).$$

5.5 Formulės, į kurias įeina tik vienviečiai predikatiniai kintamieji

Nėra algoritmo, pagal kurį galėtumėme patikrinti, ar predikatų logikos formulė įvykdoma, ar ne. Kai kuriems formulių poaibiams, iš jų ir formulėms, į kurias įeina tik vienviečiai predikatiniai kintamieji, toks algoritmas egzistuoja.

Tarkime, $x_1, x_2, \ldots, x_n$ yra pilnas formulės F laisvųjų kintamųjų sąrašas. Iš struktūros apibrėžimo išplaukia, kad F tapačiai teisinga (tapačiai klaidinga) tada ir tiktai tada, kai $\forall x_1\forall x_2 \ldots \forall x_n F$ tapačiai teisinga (tapačiai klaidinga). Formulė F įvykdoma tada ir tiktai tada, kai $\exists x_1\exists x_2 \ldots \exists x_n F$ įvykdoma. Taigi, norėdami nustatyti, ar formulės tapačiai teisingos, ar tapačiai klaidingos, ar įvykdomos, galime nagrinėti tik formules be laisvųjų kintamųjų.

5.6 teorema. *Aibė formulių, į kurias įeina tik vienviečiai predikatiniai kintamieji, išsprendžiama įvykdomumo atžvilgiu.*

Įrodymas. Galime apsiriboti tik uždaromis formulėmis. Tarkime, formulėje F iš viso yra n skirtingų predikatinių kintamųjų (žymėkime juos $P_1, P_2, \ldots, P_n$) ir ji yra normaliosios priešdėlinės formos $Q_1x_1\ Q_2x_2\ Q_mx_mG$. Parodysime, kad, jei F įvykdoma kurioje nors aibėje, tai ji įvykdoma ir aibėje, kurioje ne daugiau kaip 2^n elementų. Tarkime, ji teisinga struktūroje $< M;\ P_1^0, \ldots, P_n^0 >$. Atliekame tokią transformaciją:

1. Jei $Q_m = \forall$, tai transformuojame G į normaliąją konjunkcinę formą. Po to, naudodamiesi (5.9), (5.10) ekvivalentumais, keliame $\forall x_m$ į skliaustus tol, kol tai įmanoma. Poformuliai, prasidedantys $\forall x_m$, yra pavidalo $\forall x_m(k_1P_{i_1} \vee \cdots \vee k_sP_{i_s})$ ($k_j = \neg$ arba tuščias žodis, $j = 1, \ldots, s$).

2. Jei $Q_m = \exists$, tai transformuojame G į normaliąją disjunkcinę formą. Po to, naudodamiesi (5.11), (5.12) ekvivalentumais, keliame $\exists x_m$ į skliaustus tol, kol tai įmanoma. Poformuliai, prasidedantys $\exists x_m$, yra pavidalo $\exists x_m(k_1P_{i_1}\& \ldots \& k_uP_{i_u})$ ($k_j = \neg$ arba tuščias žodis, $j = 1, \ldots, u$).

Panašiai įkeliame $Q_{m-1}, Q_{m-2}, \ldots, Q_1$. Gautoji formulė yra pavidalo

$$\&_{j=1}^{r}(H_1^j \vee \ldots \vee H_{v_j}^j) \tag{5.13}$$

arba

$$\vee_{j=1}^{u}(H_1^j \& \ldots \& H_{l_j}^j). \tag{5.14}$$

Čia H_i^j – formulės, kurių visi poformuliai, prasidedantys kvantoriais, yra pavidalo

$$\forall x_v(k_1P_{i_1} \vee \ldots \vee k_sP_{i_s}) \tag{5.15}$$

($k_j = \neg$ arba tuščias žodis ($j = 1, \ldots, s$)) arba

$$\exists x_v(k_1P_{i_1}\& \ldots \& k_uP_{i_u}) \tag{5.16}$$

($k_j = \neg$ arba tuščias žodis ($j = 1, \ldots, u$)).

Parodysime, kad galima rasti kitą struktūrą, kurios aibėje yra ne daugiau kaip 2^n elementų, ir nagrinėjamoji formulė toje struktūroje teisinga. Tuo tikslu pakanka įrodyti, kad visos (5.15), (5.16) formulės, kurios teisingos (klaidingos) pradinėje struktūroje, yra teisingos (klaidingos) ir naujoje struktūroje.

Aibę M skaidome į poaibius $A_{k_1,\ldots,k_n}$ ($k_j \in \{t, k\}$; $j = 1, 2, \ldots, n$) laikydamiesi nuostatos: kad ir koks būtų aibės M elementas b, jis priklauso poaibiui $A_{k_1,\ldots,k_n}$ tada ir tiktai tada, kai $P_1^0(b) = k_1, \ldots, P_n^0(b) = k_n$. Gautieji poaibiai neturi bendrų elementų. Kai kurie iš jų gali būti tušti. Visų tokių poaibių atstovų aibę pažymėkime M'. Joje yra ne daugiau kaip 2^n elementų. Parodysime, kad visos (5.15), (5.16) formulės, kurios teisingos (klaidingos) pradinėje struktūroje, yra teisingos (klaidingos) ir struktūroje $< M'; P_1^0, \dots, P_n^0 >$.

Tarkime, kuri nors formulė pavidalo (5.15) teisinga pradinėje struktūroje. Tuomet ji teisinga ir naujoje struktūroje, nes M' yra M poaibis. Tarkime, kuri nors formulė pavidalo (5.15) yra klaidinga pradinėje struktūroje. Vadinasi, atsiras toks aibės M elementas c, kad visi $k_1 P_{i_1}(c), \dots, k_s P_{i_s}(c)$ bus klaidingi. Tarkime, $P_i^0(c) = d_i (i = 1, \dots, n)$. Tuomet c priklauso poaibiui $A_{d_1 \dots d_n}$. Taigi tas poaibis netuščias. Tuo atveju, kai c nepriklauso M', aibėje M' yra poaibio $A_{d_1 \dots d_n}$ atstovas. Tarkime, tai e. Tuomet $P_i^0(e) = d_i (i = 1, \dots, n)$, t.y. visi $k_1 P_{i_1}(e), \dots, k_s P_{i_s}(e)$ yra klaidingi, kartu klaidingas ir nagrinėjamasis poformulis. Panašiai nagrinėjamas ir atvejis, kai formulė yra pavidalo (5.16). Teorema įrodyta.

Parodysime, kaip normaliosios priešdėlinės formos formulių aibės klasifikuojamos į išsprendžiamas ir neišsprendžiamas klases pagal prefiksą ir predikatinius kintamuosius. Aprašomose formulėse nėra laisvųjų kintamųjų. Raide P^i žymime i-vietį predikatinį kintamąjį. Klases žymime poromis (Π, σ); čia Π – žodis abėcėlėje $C = \{\forall, \exists, \forall^\infty, \exists^\infty, \forall^n, \exists^n\} (n = 2, 3, \dots)$, σ – predikatinių kintamųjų aibė.

Tarkime, yra du abėcėlės C žodžiai A ir B. Sakykime, kad A yra B dalis, jei A gali būti gauta iš B pritaikius baigtinį skaičių operacijų:

1) išbraukus žodyje B simbolį $\forall$ arba $\exists$,

2) pakeitus žodyje B simbolį $\forall^\infty$ į $\forall^n$ arba $\exists^\infty$ į $\exists^n$ $(n = 1, 2, \dots)$,

3) pakeitus žodyje B simbolį $\forall^n$ į $\forall^m$ arba $\exists^n$ į $\exists^m$ $(m < n)$.

5.13 apibrėžimas. *Pora* (Π, σ) *žymime klasę* $Q_1 x_1 \dots Q_n x_n G$ *normaliosios priešdėlinės formos formulių, tenkinančių sąlygas:*

1) $Q_1 Q_2 \dots Q_n = \Pi$,

2) *egzistuoja predikatinių kintamųjų formulėje* G *ir* σ *abipusiškai vienareikšmė atitiktis (atsižvelgiant į vietų skaičių).*

Pavyzdžiui, formulė $\forall x \exists y ((P(x) \vee P(y)) \& (Q(x, y) \vee R(y)))$ priklauso klasei $(\forall\exists, \{P^2, P_0^1, P_1^1\})$, nes joje yra vienas dvivietis predikatinis kintamasis ir du vienviečiai predikatiniai kintamieji, be to, $\forall\exists$ yra formulės prefiksas.

5.14 apibrėžimas. *Sakome, kad klasė* $(\Pi, \sigma) \leqslant (\Pi_1, \sigma_1)$, *jei:*

1) Π *lygus* Π_1 *arba yra jo dalis,*

2) σ *izomorfinis* σ_1 *poaibiui.*

Nesunku matyti, jei kuri nors klasė neišsprendžiama, tai bet kuri didesnė klasė tuo labiau neišsprendžiama. Kalbame apie neišsprendžiamumą *pagal išvedamumą*, t.y. nėra algoritmo, kuriuo galima nustatyti, ar predikatų skaičiavime formulė išvedama.

Šios klasės yra minimalios neišsprendžiamos:

1. $\Pi = \exists\forall\exists$, $\sigma = \{P^2, P_0^1, P_1^1, P_2^1, \ldots\}$.

Šiai klasei priklauso formulės, kurių prefiksai lygus $\exists\forall\exists$ arba $\exists\forall\exists$ yra jų dalis, be to, formulėse gali būti ne mažiau kaip vienas dvivietis predikatinis kintamasis ir bet kuris skaičius vienviečių predikatinių kintamųjų.

2. $\Pi = \exists^3\forall$, $\sigma = \{P^2, P_0^1, P_1^1, P_2^1, \ldots\}$.

3. $\Pi = \forall^\infty\exists^3\forall$, $\sigma = \{P^2\}$.

4. $\Pi = \exists^\infty\forall$, $\sigma = \{P^2\}$.

5. $\Pi = \exists\forall\exists^\infty$, $\sigma = \{P^2\}$.

6. $\Pi = \exists^3\forall^\infty$, $\sigma = \{P^2\}$.

7. $\Pi = \forall^\infty\exists\forall\exists$, $\sigma = \{P^2\}$.

8. $\Pi = \exists\forall^\infty\exists$, $\sigma = \{P^2\}$.

9. $\Pi = \exists\forall\exists\forall^\infty$, $\sigma = \{P^2\}$.

Klasė (Π, σ) išsprendžiama pagal išvedamumą, jei:

a) σ sudaro tik vienviečiai predikatiniai kintamieji,

b) $\Pi = \forall^\infty\exists^\infty$,

c) $\Pi = \forall^\infty\exists^2\forall^\infty$.

Taip pat klasė (Π', σ') išsprendžiama, jei $(\Pi', \sigma') \leqslant (\Pi, \sigma)$; čia (Π, σ) yra viena iš išvardytųjų *a, b, c*.

5.6 Aristotelio logika

Naudodamiesi kai kuriais predikatų logikos rezultatais, paaiškinsime graikų mokslininko Aristotelio (384–322 m. pr. Kr.) išplėtotos tradicinės (senosios) logikos teoriją – silogistiką. Tradicinėje logikoje teiginiai buvo vadinami *sprendimais*. Sprendimo objektas vadinamas *subjektu* (S), jo savybė – *predikatu* (P). Buvo nagrinėjami tik tokio pavidalo teiginiai (kategoriški silogizmai):

S yra P,

S nėra P.

Abu jie – subjektas ir predikatas vadinami *sprendimo terminais*. Šiuolaikinės logikos požiūriu sprendimo terminai yra *vienviečiai predikatai*, nes elementų savybės matematinėje logikoje nusakomos vienviečiais predikatais. Sprendimai skirstomi į *teigiamus*

Visi S yra P, (a)

Kai kurie S yra P (i)

ir *neigiamus*

Nė vienas S nėra P, (e)

Kai kurie S nėra P. (o)

Subjektas gali būti ir vienintelis. Tuomet teigiamajame sprendime jam priskiriamas (a) tipo sprendimas, o neigiamajame – (e) tipo.

Teigiamieji sprendimai žymimi raidėmis a, i. Tai lotyniškojo žodžio *affirmo* (teigiu) pirmosios dvi balsės. Neigiamieji sprendimai žymimi raidėmis e, o. Tai lotyniškojo žodžio *nego* (neigiu) balsės.

Taigi iš viso nagrinėjami keturių rūšių – (a), (i), (e), (o) sprendimai. Juos atitinka tokios matematinės logikos formulės:

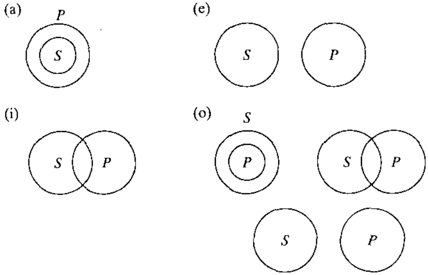
$$\forall x(S(x) \to P(x)) \qquad \text{(a)}$$

$$\exists x(S(x) \& P(x)), \qquad \text{(i)}$$

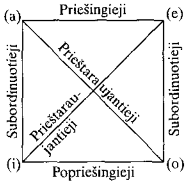
$$\forall x(S(x) \to \neg P(x)), \qquad \text{(e)}$$

$$\exists x(S(x) \& \neg P(x)). \qquad \text{(o)}$$

Sprendimų rūšys vaizduojamos diagramomis:



Teisingumo požiūriu sprendimų (a), (e), (i), (o) ryšys aprašomas loginiu kvadratu.



Sprendimų ryšys įrodomas naudojantis diagrama arba predikatų logikos dėsniais. Pavyzdžiui, parodysime, kad (a) ir (o) yra prieštaraujantys, t.y.

$$\neg\forall x(S(x) \to P(x)) \equiv \exists x(S(x)\&\neg P(x)).$$

Ekvivalentumas gaunamas naudojantis neigimo įkėlimo į skliaustus dėsniais bei savybe $\to$:

$$\neg\forall x(S(x) \to P(x)) \equiv$$

$$\equiv \exists x\neg(S(x) \to P(x)) \equiv$$

$$\equiv \exists x\neg(\neg S(x) \vee P(x)) \equiv$$

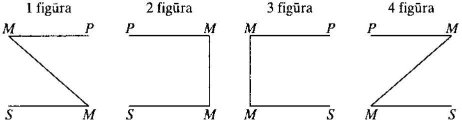
$$\equiv \exists x(S(x)\&\neg P(x)).$$

Tarp sprendimų (a) ir (i), (e) ir (o) yra *subordinacijos* ryšys. Jei (a) teisingas, tai ir (i) teisingas. Jei (e) teisingas, tai ir (o) teisingas.

Tarp sprendimų (a) ir (e) yra *priešingumo* ryšys. Jei vienas jų teisingas, tai antrasis klaidingas. Jei vienas jų klaidingas, tai antrasis neapibrėžtas.

Tarp sprendimų (i) ir (o) yra *popriešingumo* ryšys. Jei vienas jų klaidingas, tai antrasis teisingas. Jei vienas jų teisingas, tai antrasis neapibrėžtas.

Glaustai aprašysime vienviečių predikatų logikos fragmentą – Aristotelio sukurtą dedukcinę sistemą *silogistiką* (gr. *syllogistikos* – išvedantis samprotavimą). *Silogizmas* yra deduktyvus samprotavimas. Jį sudaro dvi prielaidos, viena išvada ir logikos taisyklė. Tiek prielaidomis, tiek ir išvada tegali būti (a), (i), (e), (o) tipo formulės. Iš viso galima gauti $4^3 = 64$ kombinacijas aaa, aea, aia, aoa, ... Jas vadiname *modusais* (lot. *modus* – saikas, rūšis, kiekis, matas). Be to, formulėse yra tiktai trys predikatai. Jie žymimi P, M, S. Į pirmąją prielaidą įeina predikatai P, M, į antrąją – M, S, o išvadoje yra S, P. Atkreipiame dėmesį, kad išvadoje jie yra būtent tokia tvarka, t.y. negali būti P, S. Priklausomai nuo predikatų išsidėstymo formulėse gaunamos keturios silogizmo figūros:



Iš viso gaunamos $64 \times 4 = 256$ kombinacijos. Yra 64 galimi modusai ir 4 galimos figūros. Logikos dėsniais gaunama tik 19 kombinacijų. Norėdami geriau jas įsiminti, senovės scholastai sukūrė joms pavadinimus:

1 figūra: aaa – *Barbara*, eae – *Celarent*, aii – *Darii*, eio – *Ferio*.

2 figūra: eae – *Cesare*, aee – *Camestres*, eio – *Festino*, aoo – *Baroco*.

3 figūra: aai – *Darapti*, iai – *Disamis*, aii – *Datisi*, eao – *Felapton*, oao – *Bocardo*, eio – *Ferison*.

4 figūra: aai – *Bramantip*, aee – *Camenes*, iai – *Dimaris*, eao – *Fesapo*, eio – *Fresison*.

Pavyzdys. Nustatykime silogizmo modusą ir figūrą:

Kiekvienas nelyginis skaičius yra natūralusis
Pirminiai skaičiai yra nelyginiai

Vadinasi, pirminiai skaičiai yra natūralieji

Raide M pažymėkime tvirtinimą, kad *skaičius yra nelyginis*, P – *skaičius yra natūralusis*, S – *skaičius yra pirminis*. Tuomet matome, kad silogizmo modusas yra aaa, o figūra – pirmoji (*Barbara*). Vadinasi, samprotavimas pagrįstas.

Tuščios aibės sąvoka tais laikais nebuvo žinoma. Todėl šiuolaikinėje logikoje *Darapti, Felapton, Bramantip* bei *Fesapo* nėra logikos dėsniai. Kad tai būtų taisyklingi silogizmai, pridedama dar po vieną prielaidą, nurodančia, kad egzistuoja individai, tenkinantys predikatus.

Aristotelio logika įdomi istoriniu požiūriu. Logikos taikymams informatikoje bei matematikoje ja nesinaudojama, nes sukurtos bendresnės loginėms išvadoms nustatyti sistemos, kai prielaidų sąrašas yra bet kuris baigtinis skaičius formulių (o ne dvi kaip Aristotelio logikoje), kuriose vietų skaičius predikatuose nėra ribojamas (Aristotelio logikoje nagrinėjami tik vienviečiai predikatai). Be to, lygybės predikatas, be kurio negalima apsieiti formalizuojant matematikos uždavinius, neišreiškiamas formulėmis, nagrinėjamomis Aristotelio sistemoje.

5.7 Pratimai

1. Struktūros $S =< \mathbf{N}; Q, P >$, predikatai Q, P yra triviečiai ir tenkina sąlygas: $Q(x, y, z) = t$ tada ir tiktai tada, kai $x + y = z$, o $P(x, y, z) = t$ tada ir tiktai tada, kai $xy = z$. Parašykite formulę, kurioje yra vienas laisvasis kintamasis x ir kuri teisinga struktūroje S tada ir tiktai tada, kai:

a) $x = 0$,

b) $x = 1$,

c) $x = 2$,

d) x yra lyginis skaičius,

e) x yra nelyginis skaičius,

f) x yra pirminis skaičius.

2. Parašykite formulę, kurioje yra du laisvieji kintamieji x, y ir kuri teisinga struktūroje S tada ir tiktai tada, kai:

a) $x = y$,

b) $x \leqslant y$,

c) $x < y$,

d) x dalijasi iš y.

3. Struktūroje S parašykite formulę, kuria nusakomas:

a) sudėties asociatyvumas, b) sudėties komutatyvumas.

4. Tarkime, M yra taškų ir tiesių kurioje nors plokštumoje aibė. Joje apibrėžti predikatai:

$T(x) = t$ tada ir tiktai tada, kai x yra taškas,

$T_i(x) = t$ tada ir tikta tada, kai x yra tiesė,

$P(x, y) = t$ tada ir tiktai tada, kai x priklauso y.

Parašykite nurodytoje struktūroje formulę, kuria tvirtinama:

a) per bet kuriuos du taškus galima nubrėžti tiesę; jei taškai skirtingi, tai *tiesė vienintelė*,

b) egzistuoja dvi lygiagrečios tiesės.

5. Tarkime, M yra kurios nors aibės A visų poaibių aibė, o predikatas $Q(x, y)$ teisingas tada ir tiktai tada, kai $x \subset y$.

Parašykite formulę, kurioje yra trys laisvieji kintamieji x, y, z ir kuri teisinga tada ir tiktai tada, kai:

a) x yra y ir z sankirta,

b) x yra y ir z sąjunga.

Parašykite formulę, kurioje yra vienas laisvasis kintamasis ir kuri teisinga tada ir tiktai tada, kai:

a) x yra tuščia aibė,

b) $x = A$.

Parašykite formulę, kurioje yra du laisvieji kintamieji ir kuri teisinga tada ir tiktai tada, kai x yra y papildinys.

6. Ar įvykdomos formulės:

a) $\exists x \forall y \exists z P(x, y, z)$,

b) $\exists x \exists y (P(x) \& \neg P(y))$,

c) $\exists x \forall y (Q(x, y) \to \forall z R(x, y, z))$,

d) $\forall x \exists y P(x, y) \to \exists y \forall x P(x, y)$,

e) $P(x) \to \forall y P(y)$?

7. Ar tapačiai teisingos formulės:

a) $\exists x P(x) \rightarrow \forall x P(x)$,

b) $\neg(\exists x P(x) \rightarrow \forall x P(x))$,

c) $\forall y \exists x P(x, y) \rightarrow \exists x \forall y P(x, y)$?

8. Parašykite formulę, kurioje yra vienviečiai predikatiniai kintamieji ir kuri teisinga tik struktūroje, turinčioje ne mažiau kaip 3 elementus.

9. Įrodykite, kad formulė $\neg\exists x A(x) \rightarrow \neg\forall x A(x)$ tapačiai teisinga.

10. Įrodykite, kad formulė $\exists x \forall y(P(x, y) \rightarrow (\neg P(y, x) \rightarrow (P(x, x) \leftrightarrow P(x, y))))$ teisinga struktūroje su dviem elementais.

11. Žinoma struktūra $S =< M; P, Q >$; čia $M = \{a, b, c\}$ predikatai $P(x, y)$, $Q(x, y)$ apibrėžti tokia lentele:

x	y	$P(x, y)$	$Q(x, y)$
a	a	t	k
a	b	k	k
a	c	k	k
b	a	k	t
b	b	k	k
b	c	k	k
c	a	k	k
c	b	t	t
c	c	k	t

Nustatykite, ar struktūroje S formulė $\exists x \forall y \exists z((P(x, y) \& \neg Q(x, z)) \rightarrow (\neg P(x, z) \& Q(y, x)))$ teisinga.

12. Raskite normaliąją priešdėlinę formą:

a) $\forall x \exists y \forall z(P(x, y, z) \rightarrow \exists u P(u, y, u)) \& \exists x \forall y \forall z(P(y, y, z) \& \exists P(u, x, z))$,

b) $\exists x \forall y \exists u \forall v P(x, y, u, v) \vee (\exists x \forall y \exists u Q(x, y, u) \& \exists x \forall u \exists y R(x, u, y))$.

13. Raskite normaliąją priešdėlinę formą, kurios prefiksas būtų pavidalo $\exists \ldots \exists \forall \ldots \forall$ $\forall x \exists y \forall z((P(x) \& \neg Q(z)) \vee (P(z) \& \neg P(y)))$.

6 skyrius

Predikatų skaičiavimai

Šiame skyriuje praplėsime formulių kalbą įvesdami termo sąvoką. Remdamiesi tuo, kad predikatų logikos tapačiai teisingų formulių aibė yra rekursyviai skaiti, aprašysime keletą skaičiavimų, kuriuose formulė išvedama tada ir tiktai tada, kai ji tapačiai teisinga.

6.1 Formulės, kuriose yra funkciniai simboliai

Tarkime, M yra kuri nors individinių konstantų aibė. Nagrinėsime funkcijas, kurių apibrėžimo ir reikšmių aibė yra M. Kurią nors n argumentų funkciją vadiname n-viečiu funkciniu simboliu. Kai kada nurodome ir vietų skaičių, rašydami, *pavyzdžiui*, $f(x_1, \ldots, x_n)$ *arba* f^n. Atskiru *atveju, jei funkciniame simbolyje* vietų skaičius lygus nuliui, tai jis yra konstanta.

6.1 apibrėžimas (termo).

1. *Individinė konstanta yra termas.*

2. *Individinis kintamasis yra termas.*

3. *Jei f yra n-vietis funkcinis simbolis ir $t_1, \ldots, t_n$ — termai, tai $f(t_1, \ldots, t_n)$ taip pat yra termas.*

Pavyzdys. $M = \{a, b, c\}$, $f(x)$ yra vienvietis funkcinis simbolis. Termų pavydžiai: $a, b, c, x, y, z, f(x), f(a), f(c), f(f(x)), f(f(a)), f(f(f(y)))$.

Apibrėšime formules, kuriose yra funkciniai simboliai.

6.2 apibrėžimas:

1. *Jei P yra n-vietis predikatinis simbolis, $t_1, \ldots, t_n$ — termai, tai $P(t_1, \ldots, t_n)$ yra formulė. Ji dar vadinama atomine formule.*

2. *Jei* F yra formulė, *tai* $\neg F$ *— taip pat formulė.*

3. *Jei* F, G yra *formulės, tai* $(F\&G)$, $(F \vee G)$, $(F \to G)$ *— taip pat formulės.*

4. *Jei* F yra *formulė,* x *— formulės* F *laisvasis kintamasis, tai* $\forall x F$, $\exists x F$ *— taip pat formulės.*

Kaip ir anksčiau, išorinius skliaustus praleisime.

6.3 apibrėžimas. *Atominę formulę arba jos neigimą vadiname* ***litera.***

Įvykdomų, tapačiai teisingų bei tapačiai klaidingų formulių apibrėžimai tokie pat kaip ir praeitame skyriuje. Skiriasi tiktai struktūros sąvoka.

6.4 apibrėžimas. *Tarkime, formulė* F *ir* $P_1^{m_1}, \ldots, P_n^{m_n}$ *yra pilnas sąrašas predikatinių kintamųjų, įeinančių į* F, $x_1, \ldots, x_u$ *— pilnas sąrašas laisvųjų kintamųjų, o* $f_1^{k_1}, \ldots, f_v^{k_v}$ *— funkcinių simbolių. Tuomet* ***formulę F atitinkančia struktūra*** *vadiname reiškinį*

$$S = < M;\ Q_1^{m_1}, \ldots, Q_n^{m_n};\ a_1, \ldots, a_u;\ g_1^{k_1}, \ldots, g_v^{k_v} >;$$

čia M *— kuri nors aibė,* $Q_i^{m_i}$ *—* m_i*-viečiai* $(i = 1, \ldots, n)$ *predikatai, apibrėžti aibėje* M, $a_i (i = 1, \ldots, u)$ *— kurie nors aibės* M *elementai,* $g_i^{k_i}$ *—* k_i*-vietės* $(i = 1, \ldots, v)$ *funkcijos, kurių apibrėžimo ir reikšmių aibė yra* M.

Sakome, kad ***formulė F įvykdoma struktūroje S****, jei* $P_i^{m_i}$, x_i, $f_i^{k_i}$ *pakeitę atitinkamai* $Q_i^{m_i} (i = 1, \ldots, n)$, a_i $(i = 1, \ldots, u)$, $g_i^{k_i}$ $(i = 1, \ldots, v)$ *gauname teisingą teiginį.*

6.5 apibrėžimas. *Sakome, kad formulė tapačiai teisinga, jei ji teisinga bet kurioje struktūroje. Formulė tapačiai klaidinga, jei ji klaidinga bet kurioje struktūroje.*

Pavyzdžiai:

1. $\forall x \exists y (Q(x, y, f(x)) \& P(y, y, y))$.

Išrašome predikatinius kintamuosius tokia tvarka: Q^3, P^3. Be to, formulėje yra ir funkcinis simbolis f. Formulė įvykdoma, nes ji teisinga struktūroje $< N; x+y = z, xy = z; x+1 >$, t.y. teisinga formulė $\forall x \exists y (x + y = x + 1 \& yy = y)$.

2. $\forall x \neg P(x, x) \& \forall x P(y, f(x)) \& \forall x \exists y (P(f(x), y) \& P(y, f(f(x))))$.

Formulė teisinga struktūroje $< N; x < y; 1; x + 2 >$, t.y. teisinga formulė $\forall x \neg (x < x) \& \forall x (1 < x + 2) \& \forall x \exists y (x + 2 < y \& y < x + 4)$.

6.6 apibrėžimas. *Dvi formules F, G vadiname* ***deduktyviai ekvivalenčiomis****, jei F tapačiai klaidinga tada ir tiktai tada, kai G tapačiai klaidinga.*

Nagrinėjame uždaras formules normaliosios priešdėlinės formos, t.y. pavidalo $Q_1x_1 \dots Q_mx_mM(x_1, \dots, x_m)$; čia $M(x_1, \dots, x_m)$ – bekvantorė formulė, $Q_i \in \{\forall, \exists\}, x_1, \dots, x_m$ – pilnas sąrašas laisvųjų kintamųjų formulėje M. Parodysime, kaip remiantis bet kuria tokio pavidalo formule F galima rasti jai deduktyviai ekvivalenčią G, kurioje nėra egzistavimo kvantorių. Jų eliminavimą 1920 m. aprašė norvegų logikas Th. Skolem. Formulės F transformaciją į G vadiname ***skulemizacija***.

Tarkime, $Q_r = \exists$ ir tai yra pirmasis (iš kairės į dešinę) egzistavimo kvantorius prefikse. Tuomet $Q_1 = Q_2 = \dots = Q_{r-1} = \forall$. Pažymėkime raide G formulę

$$\begin{aligned} &\forall x_1 \dots \forall x_{r-1} Q_{r+1} x_{r+1} \dots Q_m x_m \\ &\quad \times M(x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_m); \end{aligned}$$

čia f – naujas, nepriklausantis formulei F funkcinis simbolis.

6.1 teorema. *Formulės F ir G yra deduktyviai ekvivalenčios.*

Įrodymas. Parodysime, jei F nėra tapačiai klaidinga, tai ir G tokia nėra, bei atvirkščiai. Tarkime, S yra struktūra, kurioje F teisinga. Tuomet, kad ir kokie būtų struktūros aibės elementai $x_1^0, \dots, x_{r-1}^0$, atsiras toks x_r^0 iš tos pačios aibės, kad F bus teisinga struktūroje S (pažymėkime tą funkciją $f_0(x_1, \dots, x_{r-1})$). Formulė G teisinga struktūroje S', kuri skiriasi nuo S tiktai tuo, kad formulę G atitinkančioje struktūroje $f(x_1, \dots, x_{r-1})$ pakeista į $f_0(x_1, \dots, x_{r-1})$. Tarkime, kad yra struktūra S', kurioje G teisinga. Tuomet formulė teisinga struktūroje, kuri gauta iš S', išbraukus joje funkciją, atitinkančią $f(x_1, \dots, x_{r-1})$. Samprotavimai teisingi ir tuo atveju, kai $r = 1$, t.y. $f(x_1, \dots, x_{r-1})$ yra nauja konstanta, nepriklausanti formulei F. Teorema įrodyta.

Išvada. Kad ir kokia būtų uždara normaliosios priešdėlinės formos formulė, galima rasti jai deduktyviai ekvivalenčią, kurioje nėra egzistavimo kvantoriaus įeičių.

Įrodymas. Tarkime, uždara formulė yra normaliosios formos ir joje yra k egzistavimo kvantoriaus įeičių. Taikome k kartų teoremoje aprašytą procedūrą ir gauname deduktyviai ekvivalenčią formulę be egzistavimo kvantoriaus įeičių. Išvada įrodyta.

Pavyzdys. Skulemizuokime (eliminuokime visas egzistavimo kvantoriaus įeitis) formulę

$$\exists x_1 \exists x_2 \forall y_1 \forall y_2 \exists x_3 \forall y_3 \exists x_4 M(x_1, x_2, y_1, y_2, x_3, y_3, x_4).$$

Tarkime, a, b yra naujos konstantos, t.y. kurių nėra nurodytoje formulėje, $f(y_1, y_2)$, $g(y_1, y_2, y_3)$ – nauji funkciniai simboliai. Tuomet skulemizuotoji formulė yra pavidalo

$$\forall y_1 \forall y_2 \forall y_3 M(a, b, y_1, y_2, f(y_1, y_2), y_3, g(y_1, y_2, y_3)).$$

Tarkime, F yra kuri nors uždara formulė. Atliekame su ja tokius veiksmus:

a) *transformuojame į normaliąją priešdėlinę formą,*

b) skulemizuojame,

c) išbraukiame kvantorinius kompleksus, prasidedančius bendrumo kvantoriumi,

d) transformuojame į normaliąją konjunkcinę formą.

Gautoji formulė vadinama formulės F ***standartine forma***. Nors formulėje ir nėra kvantorių, visi joje esantys laisvieji kintamieji laikomi suvaržytais bendrumo kvantoriais.

Pavyzdys. Raskime formulės

$$\forall x((P(x)\&Q(x)) \rightarrow \exists y(R(x, y)\&C(y)))$$

standartinę formą.

Sprendimas. Jos normalioji priešdėlinė forma yra

$$\forall x \exists y((P(x)\&Q(x)) \rightarrow (R(x, y)\&C(y))).$$

Ją skulemizuojame, o kvantorinį kompleksą, prasidedantį bendrumo kvantoriumi, išbraukiame. Tada

$$(P(x)\&Q(x)) \rightarrow (R(x, f(x))\&C(f(x))).$$

Transformuojame į NKF ir gauname standartinę formą:

$$(\neg P(x) \vee \neg Q(x) \vee R(x, f(x)))\&(\neg P(x) \vee \neg Q(x) \vee C(f(x))).$$

6.2 Hilberto tipo predikatų skaičiavimas

Tarkime, formulės $A(x)$ laisvasis kintamasis yra x ir termas — t. Formulę, gautą iš $A(x)$, pakeitus joje visas x laisvąsias įeitis termu t, žymime $A(t)$.

6.7 apibrėžimas. *Sakome, kad termas t yra laisvas kintamojo x atžvilgiu formulėje $A(x)$, jei nesvarbu, koks yra į termą t įeinantis individinis kintamasis y, jokia jo įeitis nepatenka nei į $\forall y$, nei į $\exists y$ veikimo sritį formulėje $A(t)$.*

Hilberto tipo predikatų skaičiavimas nusakomas aksiomų schemomis bei taisyklėmis. Aksiomų schemas sudaro teiginių logikos Hilberto tipo skaičiavimo aksiomų 1.1–4.3 schemos ir:

5.1. $\forall x A(x) \to A(t)$,

5.2. $A(t) \to \exists x A(x)$.

Schemoje pakeitę A kuria nors konkrečia formule, gauname aksiomą.
Taisyklės:

$$(\mathrm{MP})\ \frac{A,\quad A \to B}{B}, \qquad (\forall)\ \frac{B \to A(y)}{B \to \forall x A(x)}, \qquad (\exists)\ \frac{A(y) \to B}{\exists x A(x) \to B}.$$

Aksiomose 5.1, 5.2 reikalaujama, kad termas t būtų laisvas kintamojo x atžvilgiu formulėje $A(x)$. Jei šio reikalavimo nebūtų, tai iš teisingų teiginių galėtume išvesti klaidingus. Pavyzdžiui, natūraliųjų skaičių aibėje $\forall x \exists y (x \neq y)$ yra teisingas tvirtinimas, bet $\forall x \exists y (x \neq y) \to \exists y (y \neq y)$ būtų klaidingas.

Taisyklėse ($\forall$), ($\exists$) kintamasis y negali laisvai įeiti į apatinę formulę ir turi būti laisvas kintamojo x atžvilgiu formulėje $A(x)$. Kad tas reikalavimas būtinas, matome iš tokio pavyzdžio:

$$\frac{x > 7 \to x > 3}{x > 7 \to \forall x (x > 3)}.$$

Pastebėkime, kad y gali būti ir lygus x. Taisyklė ($\forall$) atskiru atveju, kai nėra formulės B, užrašoma taip:

$$(\forall)\quad \frac{A(y)}{\forall x A(x)}.$$

6.8 apibrėžimas. *Formulės F išvedimu iš formulių aibės Γ vadiname baigtinę seką $F_1, \ldots, F_n$, kuri baigiasi formule $F_n = F$, o kiekvienas sekos narys yra aksioma, prielaida (t.y. priklauso Γ) arba gaunama iš kairėje nuo jo esančių formulių pagal kurią nors* (MP), ($\forall$) *ar* ($\exists$) *taisyklę.*

Įrodyta, kad *formulė F tapačiai teisinga tada ir tiktai tada, kai ji išvedama Hilberto tipo predikatų skaičiavime.*

Pavyzdys. Įrodykime, kad nagrinėjamajame predikatų skaičiavime iš $\forall x\forall y A(x, y)$ išvedama formulė $\forall y\forall x A(x, y)$:

$\forall x\forall y A(x, y)$ (prielaida),
$\forall x\forall y A(x, y) \to \forall y A(x, y)$ (5.1 aksioma),
$\forall y A(x, y)$ (pagal (MP) taisyklę),
$\forall y A(x, y) \to A(x, y)$ (5.1 aksioma),
$A(x, y)$ (pagal (MP) taisyklę),
$\forall x A(x, y)$ (pagal ($\forall$) taisyklę),
$\forall y\forall x A(x, y)$ (pagal ($\forall$) taisyklę).

6.2 teorema. *Hilberto tipo predikatų skaičiavimas nėra prieštaringas.*

Įrodymas. Kiekvieną predikatų logikos formulę transformuokime į teiginių logikos, naudodamiesi operatoriumi $\mathrm{Tr}(P(t_1, \ldots, t_n)) = P$, t.y. atominei formulei priskiriamas loginis kintamasis vardu P:

$$\begin{aligned}
&\mathrm{Tr}(\neg A) = \neg\mathrm{Tr}(A),\\
&\mathrm{Tr}(A\&B) = \mathrm{Tr}(A)\&\mathrm{Tr}(B),\\
&\mathrm{Tr}(A \vee B) = \mathrm{Tr}(A) \vee \mathrm{Tr}(B),\\
&\mathrm{Tr}(A \to B) = \mathrm{Tr}(A) \to \mathrm{Tr}(B),\\
&\mathrm{Tr}(\forall x A(x)) = \mathrm{Tr}(A(x)),\\
&\mathrm{Tr}(\exists x A(x)) = \mathrm{Tr}(A(x)).
\end{aligned}$$

Jei F yra aksioma, tai transformavus ją į teiginių logiką, gaunama tapačiai teisinga formulė.

Jei transformacija F yra tapačiai teisinga formulė ir G gauta iš F pagal taisyklę ($\forall$) ar ($\exists$), tai transformavus G į teiginių logiką, gaunama taip pat tapačiai teisinga formulė, nes jų abiejų transformacijos sutampa.

Jei transformacijos A ir $A \to B$ yra tapačiai teisingos formulės, tai tokia yra ir transformacija B.

Taigi jei kuri nors formulė F išvedama Hilberto tipo predikatų skaičiavime, tai jos transformacija yra tapačiai teisinga formulė. Todėl $\neg F$ negali būti išvedama, nes jos transformacija nėra tapačiai teisinga (ji lygi $\neg\mathrm{Tr}(F)$). Teorema įrodyta.

Pastebėkime, kad dedukcijos teorema predikatų skaičiavimo atveju negalioja. Iš prielaidos $A(x)$ išvedama formulė $\forall x A(x)$ tokiu būdu:

$A(x)$ (prielaida),
$\forall x A(x)$ (pagal taisyklę ($\forall$)).

Predikatų skaičiavime $A(x) \to \forall x A(x)$ neišvedama, nes tai nėra tapačiai teisinga formulė. Struktūroje, kurios aibė yra $\{a, b\}$, $A(x)$ keičiamas predikatu $A_0(a) = t$, $A_0(b) = k$, o laisvasis kintamasis – elementu a, gaunamas klaidingas tvirtinimas $A_0(a) \to \forall x A_0(x)$. Dedukcijos teorema teisinga formulėms su tam tikrais apribojimais, pavyzdžiui, kai jos yra uždaros.

6.3 Sekvencinis skaičiavimas

6.9 apibrėžimas. *Sekvencija vadiname reiškinį pavidalo* $F_1, \ldots, F_n \vdash G_1, \ldots, G_m$; *čia* F_i $(i = 1, \ldots, n)$ *ir* G_i $(i = 1, \ldots, m)$ *yra formulės.*

Sekvencijos apibrėžimas toks pat kaip ir 4.4 skyrelyje. Tik šiuo atveju formulės yra bendresnio pavidalo – jos yra predikatų logikos formulės.

Kaip ir anksčiau, raidėmis Γ, Γ_1, Γ_2, Δ, Δ_1, Δ_2 žymime baigtines formulių sekas. Jos gali būti ir tuščios. Nagrinėsime tik sekvencijas, kuriose yra bent viena formulė.

Vokiečių logikas G. Gentzen 1930 m. aprašė vadinamąjį sekvencinį skaičiavimą, kuriame išvedimo paieška daugeliu atvejų paprastesnė negu Hilberto tipo skaičiavime.

Aksiomos: $F \vdash F$.

Struktūrinės taisyklės:

(silpninimas) $$\frac{\Gamma \vdash \Delta}{F, \Gamma \vdash \Delta}, \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, F},$$

(prastinimas) $$\frac{F, F, \Gamma \vdash \Delta}{F, \Gamma \vdash \Delta}, \qquad \frac{\Gamma \vdash \Delta, F, F}{\Gamma \vdash \Delta, F},$$

(perstatymas) $$\frac{\Gamma_1, F, G, \Gamma_2 \vdash \Delta}{\Gamma_1, G, F, \Gamma_2 \vdash \Delta}, \qquad \frac{\Gamma \vdash \Delta_1, F, G, \Delta_2}{\Gamma \vdash \Delta_1, G, F, \Delta_2}.$$

Loginių operacijų taisyklės:

$(\neg \vdash)$ $$\frac{\Gamma \vdash \Delta, F}{\neg F, \Gamma \vdash \Delta},$$ $(\vdash \neg)$ $$\frac{F, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg F},$$

$(\& \vdash)$ $$\frac{F, G, \Gamma \vdash \Delta}{F\&G, \Gamma \vdash \Delta},$$ $(\vdash \&)$ $$\frac{\Gamma \vdash \Delta, F \quad \Gamma \vdash \Delta, G}{\Gamma \vdash \Delta, F\&G},$$

$$(\vee\vdash)\ \frac{F,\Gamma\vdash\Delta \quad G,\Gamma\vdash\Delta}{F\vee G,\Gamma\vdash\Delta},\qquad (\vdash\vee)\ \frac{\Gamma\vdash\Delta,F,G}{\Gamma\vdash,\Delta,F\vee G},$$

$$(\rightarrow\vdash)\ \frac{\Gamma\vdash\Delta,F \quad G,\Gamma\vdash\Delta}{F\rightarrow G,\Gamma\vdash\Delta},\qquad (\vdash\rightarrow)\ \frac{F,\Gamma\vdash\Delta,G}{\Gamma\vdash\Delta,F\rightarrow G}.$$

Pjūvio taisyklė:

$$\frac{\Gamma_1\vdash\Delta_1,F \quad F,\Gamma_2\vdash\Delta_2}{\Gamma_1,\Gamma_2\vdash\Delta_1,\Delta_2}.$$

Kvantorinės taisyklės:

$$(\exists\vdash)\ \frac{F(z),\Gamma\vdash\Delta}{\exists xF(x),\Gamma\vdash\Delta},\qquad (\vdash\exists)\ \frac{\Gamma\vdash\Delta,F(t),\exists xF(x)}{\Gamma\vdash\Delta\exists xF(x)},$$

$$(\forall\vdash)\ \frac{F(t),\forall xF(x),\Gamma\vdash\Delta}{\forall xF(x),\Gamma\vdash\Delta},\qquad (\vdash\forall)\ \frac{\Gamma\vdash\Delta,F(z)}{\Gamma\vdash\Delta\forall xF(x)}.$$

Čia z yra naujas kintamasis, neįeinantis į Γ, $\Delta, \exists xF(x)$ arba $\forall xF(x)$, t – termas, laisvas kintamojo x atžvilgiu formulėje $F(x)$.

Primename, kad sekvencijoje $\Gamma\vdash\Delta$ seka Γ vadinama ***antecedentu***, o Δ – ***sukcedentu***. Sakoma: formulė F priklauso sekvencijos antecedentui, jei ji yra sekoje Γ; formulė priklauso sukcedentui, jei ji yra sekoje Δ.

6.10 apibrėžimas. *Medžio pavidalo orientuotą grafą, kurio visos viršūnės pažymėtos sekvencijomis (šaknis – pradinė sekvencija) ir kiekviena viršūnė (išskyrus lapus) gauta iš tiesiogiai virš jos esančių (gretimų) sekvencijų, pritaikius kurią nors sekvencinio skaičiavimo taisyklę, vadiname* ***išvedimo paieškos medžiu.***

Jei visos medžio galinės viršūnės, t.y. lapai, yra aksiomos, tai medis vadinamas ***sekvencijos****, kuria pažymėta šaknis,* ***išvedimu****.*

Visose loginių operacijų ir kvantorinėse taisyklėse formulių įeitys skirstomos į *centrines, šonines* bei *parametrines*. Pavyzdžiui, taisyklėje ($\vdash$ &), kurioje $F\&G$ yra centrinės formulės įeitis, F, G – šoninės, formulės, priklausančios Γ, Δ, vadinamos parametrinėmis. Taisyklėje ($\vdash\exists$), kurioje $\exists xF(x)$ yra centrinės formulės įeitis, $F(t)$ – šoninės, formulės, priklausančios Γ, Δ, vadinamos parametrinėmis.

Kaip ir anksčiau, išvedimo medyje žymime tik medžio viršūnes. Lanką atitinka brūkšnys. Primename, kad grafas orientuotas, kryptis – iš apačios į viršų.

Pavyzdžiai:

1. Parodykime, kad sekvencija $F\&G, \neg H \vdash (\neg F \vee \neg G) \to H$ išvedama nagrinėjamajame skaičiavime:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{F \vdash F}{F \vdash F, H}}{F \vdash H, F}}{\neg H, F \vdash H, F}}{F, \neg H \vdash H, F}}{G, F, \neg H \vdash H, F}}{F, G, \neg H \vdash H, F}}{\neg F, F, G, \neg H \vdash H} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{G \vdash G}{G \vdash G, H}}{G \vdash H, G}}{\neg H, G \vdash H, G}}{G, \neg H \vdash H, G}}{F, G, \neg H \vdash H, G}}{\neg G, F, G, \neg H \vdash H}}{\neg F \vee \neg G, F, G, \neg H \vdash H}}{F, G, \neg H \vdash (\neg F \vee \neg G) \to H}}{F\&G, \neg H \vdash (\neg F \vee \neg G) \to H}.$$

2. Sekvencija $\vdash \exists x \forall y A(x, y) \to \forall y \exists x A(x, y)$ taip pat išvedama:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A(a, b) \vdash A(a, b)}{A(a, b) \vdash A(a, b), \exists x A(x, b)}}{\forall y A(a, y), A(a, b) \vdash A(a, b), \exists x A(x, b)}}{A(a, b), \forall y A(a, y) \vdash A(a, b), \exists x A(x, b)}}{A(a, b), \forall y A(a, y) \vdash \exists x A(x, b)}}{\forall y A(a, y) \vdash \exists x A(x, b)}}{\forall y A(a, y) \vdash \forall y \exists x A(x, y)}}{\exists x \forall y A(x, y) \vdash \forall y \exists x A(x, y)}}{\vdash \exists x \forall y A(x, y) \to \forall y \exists x A(x, y)}.$$

Vokiečių logikas G. Gentzen įrodė Hilberto ir sekvencinio skaičiavimų ekvivalentumą. Iš įrodymo išplaukia teorema:

6.3 teorema. *Predikatų logikos formulė F tapačiai teisinga tada ir tiktai tada, kai $\vdash F$ išvedama sekvenciniame skaičiavime.*

Loginių operacijų taisyklių prielaidos gaunamos skaidant kurią nors išvados formulę į poformulius, t.y. prielaidos formulės yra tik išvados formulės ar jų poformuliai. Kiekvienoje prielaidoje loginių operacijų skaičius vienetu mažesnis negu išvadoje. Todėl po baigtinio skaičiaus taisyklių taikymo sekvencijai, kurioje yra tik teiginių logikos formulės, gaunama sekvencija, kurioje yra tik loginiai kintamieji. Be to, tos taisyklės tenkina vadinamąją *apverčiamumo savybę*, t.y. visos loginių operacijų bet kurios taisyklės prielaidos išvedamos tada ir tiktai tada, kai išvedama išvada. Daugelio formulių išvedimo paieška gaunama *eksponentinio sprogimo* pavidalu. Išvedant vieną sekvenciją pagal kai kurias taisykles reikia tikrinti dviejų sekvencijų išvedimą. Daugelio sekvencijų išvedimą sunku praktiškai realizuoti, nes tam reikalingų išvesti sekvencijų skaičius sparčiai auga. Be to, atliekama daug nereikalingų žingsnių.

Pjūvio taisyklės prielaidose atsiranda formulės, kurių išvadoje gali ir nebūti. Pasirodo, be tos taisyklės galima apsieiti, t.y. teisingas tvirtinimas (jis dar vadinamas *pagrindine Gentzeno teorema*).

Gentzeno teorema. *Kad ir kokia būtų sekvencija $\Gamma \vdash \Delta$, kurioje laisvieji ir suvaržytieji individiniai kintamieji pažymėti skirtingais simboliais, ji sekvenciniame skaičiavime išvedama tada ir tiktai tada, kai išvedama skaičiavime be pjūvio taisyklės.*

Vienas dažniausiai logikos taikymuose pasitaikantis predikatas yra *lygybės*. *Sekvencinis skaičiavimas su lygybės predikatu* (žymimas $G^=$) nuo aprašytojo skiriasi tuo, kad aksiomų sąrašas papildomas *aksiomomis* $\vdash t = t$.

Taisyklių sąrašas papildomas naujomis taisyklėmis:

$$\frac{t_1 = t_2, [\Gamma]^{t_1}_{t_2} \vdash [\Delta]^{t_1}_{t_2}}{t_1 = t_2, \Gamma \vdash \Delta}, \qquad \frac{t_1 = t_2, [\Gamma]^{t_2}_{t_1} \vdash [\Delta]^{t_2}_{t_1}}{t_1 = t_2, \Gamma \vdash \Delta};$$

čia $[\Gamma]^{t_1}_{t_2}$ žymime formulių seką, kurioje visų termų t_1 įeitys pakeistos termu t_2 (analogiškai $[\Delta]^{t_1}_{t_2}$, $[\Gamma]^{t_2}_{t_1}$, $[\Delta]^{t_2}_{t_1}$).

Raide G žymime sekvencinį skaičiavimą (žr. 4.4 skyrelį), kuris nuo aukščiau aprašytojo skiriasi tuo, kad jame nėra pjūvio bei struktūrinių taisyklių, o aksiomos atrodo šitaip:

$$\Gamma_1, F, \Gamma_2 \vdash \Delta_1, F, \Delta_2.$$

Taisyklės panašios į ankstesniąsias, tik centrinė formulė nebūtinai pirmoji iš kairės yra antecedente arba paskutinė – sukcedente. Pavyzdžiui, taisyklė ($\vdash \&$) skaičiavime G yra tokia:

$$\frac{\Gamma \vdash \Delta_1, F, \Delta_2 \qquad \Gamma \vdash \Delta_1, G, \Delta_2}{\Gamma \vdash \Delta_1, F\&G, \Delta_2}.$$

Nesunku matyti, kad abu skaičiavimai ekvivalentūs, t.y. kad ir kokia būtų sekvencija, ji ankstesniame skaičiavime išvedama tada ir tiktai tada, kai išvedama skaičiavime G.

Kintamuosius, kurių reikšmės yra kurios nors individinės konstantos, žymime raidėmis $a, b, c, a_1, b_1, c_1, \ldots$. Tik tokie laisvieji kintamieji aptinkami nagrinėjamuose sekvencijų išvedimuose. Suvaržytuosius kintamuosius žymime $x, y, z, x_1, y_1, z_1, \ldots$, t.y. laisvieji ir suvaržytieji kintamieji žymimi skirtingomis raidėmis. Termo įeitis vadinama *pagrindine*, jei jame nėra suvaržytųjų kintamųjų įeičių.

6.11 apibrėžimas. *Sekvencinis skaičiavimas vadinamas* ***minus-normaliuoju****, jei termas t taisyklėse* ($\vdash \exists$), ($\forall \vdash$) *yra pagrindinis, įeinantis į kurią nors išvados formulę; jei išvadoje nėra pagrindinių termų, tai t yra kuri nors nauja konstanta a.*

Sekvencinių skaičiavimų ekvivalentumą 1963 m. įrodė švedų logikas S. Kanger. Mes ekvivalentumą įrodysime tik tuo atveju, kai formulėse nėra funkcinių simbolių. Kai kalbama apie formules be funkcinių simbolių, suprantama, kad į jas neįeina i-viečiai funkciniai simboliai su $i \geqslant 1$.

6.4 teorema. *Tarkime,* Γ, Δ *yra baigtinės formulių be funkcinių simbolių sekos.* $\Gamma \vdash \Delta$ *išvedama skaičiavime G tada ir tiktai tada, kai ji išvedama minus-normaliajame G.*

Įrodymas. Jei $\Gamma \vdash \Delta$ išvedama minus-normaliajame G, tai ji išvedama ir skaičiavime G. Tereikia parodyti, kad jei $\Gamma \vdash \Delta$ išvedama skaičiavime G, tai galime rasti jos išvedimą ir minus-normaliajame G. Šiuo atveju į išvedimo medį žiūrėsime kaip į neorientuotą medžio pavidalo grafą. Pervardijant galima pasiekti, kad taikant kiekvieną taisyklę ($\vdash \forall$), ($\exists \vdash$) laisvųjų kintamųjų neatsirastų ne tik taikymo išvadoje, bet ir išvedimo medyje, esančiame nuo nagrinėjamojo taikymo iki šaknies.

Leidžiamės kuria nors šaka žemyn nuo aksiomų link šaknies. Tarkime, radome pirmą taisyklės ($\vdash \exists$) taikymą, kuris netenkina minus-normalumo sąlygos (arba $\forall \vdash$, šiuo atveju samprotavimai būtų analogiški):

$$\frac{\dfrac{M}{\Gamma \vdash \Delta_1, A(a_i), \exists x_j A(x_j), \Delta_2}}{\Gamma \vdash \Delta_1, \exists x_j A(x_j), \Delta_2}$$

$$\ldots$$

Virš sekvencijos $\Gamma \vdash \Delta_1, A(a_i), \exists x_j A(x_j), \Delta_2$ esantį išvedimo medį pažymėkime raide M. Viršutinėje sekvencijoje ir visur medyje M pakeiskime a_i kuria nors konstanta (pažymėkime ją a), įeinančia į taisyklės taikymo apatinę sekvenciją. Jei apatinėje sekvencijoje konstantų nėra, tai a yra kuri nors naujoji konstanta, neaptinkama medyje M.

Parodysime, kad po pakeitimo gautasis medis išlieka išvedimo medžiu, t.y.:

a) kvantorinių taisyklių taikymai tenkina jiems keliamus reikalavimus,

b) aksiomos ir po pakeitimo išlieka aksiomomis.

Visi taisyklių ($\vdash \forall$), ($\exists \vdash$) taikymai tenkina tuos pačius apribojimus ir medyje M, nes individiniai kintamieji, taikant tas taisykles, pakeisti kintamaisiais, skirtingais nuo esamų nagrinėjamoje sekvencijoje. Visi taisyklių ($\vdash \exists$), ($\forall \vdash$) taikymai taip pat tenkina tuos pačius apribojimus, nes laisvųjų ir suvaržytųjų kintamųjų vardai skirtingi, todėl a yra laisvas atžvilgiu individinio kintamojo, kurį pakeitėme nagrinėjamose formulėse. Jei kuri nors sekvencija buvo aksioma, tai ji liks ir po pakeitimo, nes keitėme visas a_i įeitis.

Gautajame išvedimo medyje taisyklės ($\vdash \exists$) (arba ($\forall \vdash$)) taikymų, netenkinančių minus-normalumo, yra vienu mažiau. Tarkime, kad pradiniame medyje tokių taikymų yra n. Pritaikę n kartų aprašytąją vienų kintamųjų keitimo kitais procedūrą, gauname minus-normalųjį pradinės sekvencijos išvedimą skaičiavime G. Teorema įrodyta.

6.5 teorema. *Formulių klasė be funkcinių simbolių su prefiksu $\forall^\infty \exists^\infty$ yra išsprendžiama pagal išvedamumą.*

Įrodymas. Tarkime, F yra kuri nors formulė be funkcinių simbolių pavidalo

$$\forall y_1 \dots \forall y_m \exists x_1 \dots \exists x_n M(y_1, \dots, y_m, x_1, \dots, x_n);$$

čia $M(y_1, \dots, y_m, x_1, \dots, x_n)$ – bekvantorė formulė ir $b_1, b_2, \dots, b_s$ – pilnas formulėje F sąrašas laisvųjų kintamųjų. Iš 6.4 teoremos išplaukia, jei $\vdash F$ išvedama, tai galima rasti jos išvedimą ir minus-normaliajame G. Pritaikę taisyklę ($\vdash \forall$) (tik ją ir tegalime taikyti nagrinėjamosios formulės atžvilgiu) m kartų, gauname sekvenciją pavidalo $\vdash \exists x_1 \dots \exists x_n M(a_1, \dots, a_m, x_1, \dots, x_n)$; čia a_i $(i = 1, \dots, m)$ yra tarpusavyje skirtingi ir nelygūs b_i $(i = 1, \dots, s)$ laisvieji kintamieji, kuriais pakeitėme y_i. Aukščiau medyje tegalėsime taikyti taisyklę ($\vdash \exists$) ir loginių operacijų taisykles. Kadangi taikant ($\vdash \exists$) kintamuosius x_i galima pakeisti tik kuriais nors iš $\{a_1, \dots, a_m, b_1, \dots, b_s\}$, tai skirtingų išvedimo paieškos medžių tėra baigtinis skaičius. Jei tarp jų bus bent vienas išvedimo medis, tai $\vdash F$ išvedama, jei ne, tai $\vdash F$ nėra išvedama. Teorema įrodyta.

Pateikiame vieną išsprendžiamą ir dvi neišsprendžiamas klases formulių su funkciniais simboliais.

Maksimalios išsprendžiamos klasės	Minimalios neišsprendžiamos klasės
$\Pi(pred\colon \infty; funkc\colon \infty)$	$\exists\exists(pred\colon 0, 1; funkc\colon 1)$
	$\exists\exists(pred\colon 1; funkc\colon 0, 1)$

Klasės išsprendžiamumą 1969 m. įrodė amerikiečių logikas Y. Gurevich. Formulės yra normaliosios priešdėlinės formos. Reiškiniu $pred\colon \infty$; $funkc\colon \infty$

žymime formules, kurių matricose gali būti bet koks skaičius vienviečių predikatinių ir vienviečių funkcinių kintamųjų. Reiškiniu *pred*: a, b žymime formules, kuriose yra a vienviečių predikatinių kintamųjų ir b – dviviečių predikatinių kintamųjų. Panašiai suprantame ir žymėjimą *funkc*: a, b. Raide Π žymime bet kurį prefiksą.

Pateikiame normaliosios priešdėlinės formos su lygybės predikatu formulių klasifikaciją (nurodomi reikalavimai prefiksui ir matricai) pagal įrodomumą.

Maksimalios išsprendžiamos klasės su lygybės predikatu	Minimalios neišsprendžiamos klasės su lygybės predikatu
$\Pi(=;\ pred\colon\ \infty;\ funkc\colon\ 1)$	$\exists\exists\forall(=,\ pred\colon\ \infty,\ 1)$
$\forall^*(=;\ pred\colon\ bet\ kurie;\ funkc\colon\ bet\ kurie)$	$\exists\exists\forall(=;\ pred\colon\ 0, 1;\ konstantos\colon\ \infty)$
$\forall^*\exists\forall^*(=;\ pred\colon\ bet\ kurie;\ funkc\colon\ 1)$	$\exists\exists\forall^*(=;\ pred\colon\ 0, 1)$
$\forall^*\exists^*(=;\ pred\colon\ bet\ kurie;\ konstantos\colon\ \infty)$	$\forall^*\exists\exists\forall(=;\ pred\colon\ 0, 1)$
	$\exists(=;\ funkc\colon\ 2)$
	$\exists(=;\ funkc\colon\ 0, 1)$

Pavyzdžiui, reiškiniu $\Pi(=;\ pred\colon\ \infty;\ funkc\colon\ 1)$ pažymėta klasė formulių normaliosios priešdėlinės formos su bet kokiu prefiksu, o matricoje gali būti lygybės predikatas, bet kuris skaičius vienviečių predikatinių kintamųjų ir vienas vienvietis funkcinis simbolis.

6.4 Intuicionistinė logika

6.6 teorema. *Egzistuoja du tokie iracionalieji a, b, kad a^b yra racionalusis skaičius.*

Įrodymas. Tarkime, $\sqrt{2}^{\sqrt{2}}$ yra racionalusis skaičius. Tuomet pasirinkę $a = b = \sqrt{2}$, gauname, kad $a^b = \sqrt{2}^{\sqrt{2}}$ yra racionalusis skaičius, o a, b – iracionalieji. Priešingu atveju, jei $\sqrt{2}^{\sqrt{2}}$ yra iracionalus, imkime $a = \sqrt{2}^{\sqrt{2}}$, o $b = \sqrt{2}$. Tada $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$, t.y. a^b yra racionalusis skaičius. Teorema įrodyta.

Tai kam vis dėlto lygūs a ir b? Nors ir įrodėme egzistavimą tokių skaičių, bet kam jie lygūs, nežinome. Toks įrodymas vadinamas *nekonstruktyviuoju įrodymu.* Įrodoma, kad egzistuoja koks nors objektas, bet iš įrodymo neišplaukia algoritmas, kaip jį rasti. Teoremos 6.6 atveju galima rasti kitą, konstruktyvų jos įrodymą. Jis yra daug ilgesnis ir kur kas sudėtingesnis. Įrodyta, kad $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$.

Bet, pasirodo, ne visoms žinomoms matematikoje teoremoms galima rasti kitus, konstruktyvius įrodymus. Palyginkime dvi teoremas. Viena jų gerai žinoma matematikams.

Teorema. *Iš kiekvienos aprėžtos skaičių sekos galima išrinkti konverguojantį posekį.*

Teorema. *Nėra algoritmo, kuriuo iš bet kurios aprėžtos skaičių sekos galėtume išrinkti konverguojantį posekį.*

Norint turėti kitą, *konstruktyvią matematiką*, t.y. tokią, kurioje įrodžius, kad egzistuoja kurie nors objektai, galima būtų remiantis įrodymu juos rasti, reikalinga *kita logika*. Ji vadinama ***intuicionistine logika***. Ją 1930 m. sukūrė olandų logikas A. Heyting. Joje teisingi tik tokie logikos dėsniai, kuriais naudojantis galimi tik konstruktyvūs matematiniai įrodymai.

Hilberto intuicionistinis skaičiavimas nuo klasikinio skiriasi tiktai tuo, kad 4.3 aksioma $\neg\neg A \to A$ pakeista nauja – $\neg A \to (A \to B)$.

Intuicionistinė natūralioji dedukcija nuo klasikinės skiriasi tik tuo, kad iš taisyklių sąrašo išbraukta

$$\frac{\Gamma, \neg A \vdash}{\Gamma \vdash A}.$$

Yra keletas intuicionistinio sekvencijų skaičiavimo variantų. Pateiksime vieną jų, kai sukcedente gali būti ne daugiau kaip viena formulė.

Intuicionistinis sekvencinis skaičiavimas. *Aksiomos*: $F \vdash F$.

Struktūrinės taisyklės:

$$\text{(silpninimas)} \quad \frac{\Gamma \vdash \Delta}{F, \Gamma \vdash \Delta}, \qquad \frac{\Gamma \vdash}{\Gamma \vdash F},$$

$$\text{(prastinimas)} \quad \frac{F, F, \Gamma \vdash \Delta}{F, \Gamma \vdash \Delta},$$

$$\text{(perstatymas)} \quad \frac{\Gamma_1, F, G, \Gamma_2 \vdash \Delta}{\Gamma_1, G, F, \Gamma_2 \vdash \Delta}.$$

Taisyklės loginėms operacijoms:

$$(\neg\vdash)\quad \frac{\Gamma\vdash F}{\neg F,\Gamma\vdash\Delta},\qquad (\vdash\neg)\quad \frac{F,\Gamma\vdash}{\Gamma\vdash\neg F},$$

$$(\&\vdash)\quad \frac{F,G,\Gamma\vdash\Delta}{F\&G,\Gamma\vdash\Delta},\qquad (\vdash\&)\quad \frac{\Gamma\vdash F\quad \Gamma\vdash G}{\Gamma\vdash F\&G},$$

$$(\vee\vdash)\quad \frac{F,\Gamma\vdash\Delta\quad G,\Gamma\vdash\Delta}{F\vee G,\Gamma\vdash\Delta},\qquad (\vdash\vee)\quad \frac{\Gamma\vdash F}{\Gamma\vdash F\vee G}\ \text{arba}\ \frac{\Gamma\vdash G}{\Gamma\vdash F\vee G},$$

$$(\to\vdash)\quad \frac{\Gamma\vdash F\quad G,\Gamma\vdash\Delta}{F\to G,\Gamma\vdash\Delta},\qquad (\vdash\to)\quad \frac{F,\Gamma\vdash G}{\Gamma\vdash F\to G}.$$

Kvantorinės taisyklės:

$$(\exists\vdash)\quad \frac{F(z),\Gamma\vdash\Delta}{\exists xF(x),\Gamma\vdash\Delta},\qquad (\vdash\exists)\quad \frac{\Gamma\vdash F(t)}{\Gamma\vdash\exists xF(x)},$$

$$(\forall\vdash)\quad \frac{F(t),\Gamma\vdash\Delta}{\forall xF(x),\Gamma\vdash\Delta},\qquad (\vdash\forall)\quad \frac{\Gamma\vdash F(z)}{\Gamma\vdash\forall xF(x)}.$$

Kintamasis z bei termas t tenkina tuos pačius reikalavimus kaip ir klasikinio sekvencinio skaičiavimo atveju.

Pjūvio taisyklė:

$$\frac{\Gamma_1\vdash F\quad F,\Gamma_2\vdash\Delta}{\Gamma_1,\Gamma_2\vdash\Delta}.$$

Sekvencija $\vdash F\vee\neg F$ intuicionistiniame skaičiavime neišvedama (jei neišvedamos $\vdash F$ ir $\vdash\neg F$), nes jos prielaidomis gali būti tik viena sekvencijų $\vdash F$, $\vdash\neg F$.

Pavyzdžiai. Sekvencijų $\vdash\neg(F\&\neg F)$ ir $\vdash\neg\neg\neg F\to\neg F$ išvedimai:

$$\cfrac{\cfrac{\cfrac{F\vdash F}{F,\neg F\vdash}}{F\&\neg F\vdash}}{\vdash\neg(F\&\neg F)},\qquad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{F\vdash F}{\neg F,F\vdash}}{F\vdash\neg\neg F}}{\neg\neg\neg F,F\vdash}}{\neg\neg\neg F\vdash\neg F}}{\vdash\neg\neg\neg F\to\neg F}.$$

Intuicionistiniame skaičiavime sekvencija $\vdash \neg\neg F \to F$ neišvedama, o $\vdash F \to \neg\neg F$ išvedama.

Intuicionistinėje logikoje teisingi teiginiai:

1. Jei kuri nors sekvencija $\Gamma \vdash \Delta$ išvedama intuicionistiniame skaičiavime, tai ji išvedama ir klasikiniame skaičiavime.

2. Kiekviena sekvencija išvedama intuicionistiniame skaičiavime tada ir tiktai tada, kai ji išvedama intuicionistiniame skaičiavime be pjūvio taisyklės.

Kaip matyti iš kito pavyzdžio, prastinimo taisyklė būtina intuicionistiniame skaičiavime. Be jos sekvencija $\vdash \neg\neg(F \vee \neg F)$ neišvedama. Nes skaičiavime be pjūvio ir prastinimo taisyklių tėra tik tokie galimi išvedimo paieškos medžiai:

$$\cfrac{\cfrac{\cfrac{\vdash F \quad \text{arba} \quad \cfrac{F \vdash}{\vdash \neg F}}{\vdash F \vee \neg F}}{\neg(F \vee \neg F) \vdash}}{\vdash \neg\neg(F \vee \neg F)}.$$

Turint prastinimo taisyklę, ji išvedama:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{F \vdash F}{F \vdash F \vee \neg F}}{\neg(F \vee \neg F), F \vdash}}{F, \neg(F \vee \neg F) \vdash}}{\neg(F \vee \neg F) \vdash \neg F}}{\neg(F \vee \neg F) \vdash F \vee \neg F}}{\neg(F \vee \neg F), \neg(F \vee \neg F) \vdash}}{\neg(F \vee \neg F) \vdash}}{\vdash \neg\neg(F \vee \neg F)}.$$

Matematikoje dažnai konstruktyvumas prarandamas įrodant prieštaros būdu. Tariame, kad $\neg F$ (norėdami įrodyti F), įrodome $\neg\neg F$ ir darome išvadą, kad įrodėme F. Intuicionistinėje logikoje teiginiai F, $\neg\neg F$ turi skirtingą prasmę.

6.5 Kompaktiškumas

Šiame skyrelyje nagrinėsime tik teiginių logikos formulių aibes. Sakysime, kad formulėse loginiai kintamieji yra tik iš sąrašo $P = \{p_1, p_2, \ldots\}$, o loginės operacijos — $\neg$, &, $\vee$, $\to$. Tarkime, $h(x)$ yra kuri nors interpretacija, t.y. funkcija, kurios apibrėžimo aibė yra P, o reikšmių aibė — $\{t, k\}$. Turėdami h, vienareikšmiškai galime nustatyti bet kurios formulės F reikšmę. Ją žymime $h(F)$.

6.12 apibrėžimas. *Formulių aibė vadinama* ***baigiai įvykdoma****, jei įvykdomas kiekvienas jos baigtinis poaibis.*

6.13 apibrėžimas. *Baigiai įvykdomų formulių* ***aibė*** *T yra* ***maksimali****, nesvarbu, kokia būtų formulė F, arba $F \in T$, arba $\neg F \in T$.*

6.7 teorema. *Egzistuoja interpretacijų ir maksimalių aibių abipusiškai vienareikšmė atitiktis.*

Įrodymas. Kiekvienai interpretacijai h priskiriame formulių aibę $\Sigma_h = \{F : h(F) = t\}$. Aišku, kad ji maksimali, nes kad ir kokia būtų formulė F, arba $h(F) = t$, arba $h(\neg F) = \neg h(F) = t$.

Kiekvienai maksimaliai (pagal apibrėžimą ji ir baigiai įvykdoma) aibei Σ priskiriame tokią interpretaciją: nors ir koks būtų p_i, $h(p_i) = t$ tada ir tiktai tada, kai $p_i \in \Sigma$.

Taikydami indukciją pagal loginių operacijų skaičių (žymėsime jį l) įrodysime, kad $\Sigma = \Sigma_h$, t.y. nesvarbu, kokia yra formulė F, $F \in \Sigma$ tada ir tiktai tada, kai $h(F) = t$.

Kai $l = 0$, teorema teisinga, nes taip jau apibrėžėme h. Tarkime, teorema teisinga, kai $l \leqslant m$. Parodysime, kad ji teisinga ir kai $l = m + 1$. Taigi formulėje F yra $(m + 1)$ loginių operacijų ir norime parodyti, kad $F \in \Sigma$ tada ir tiktai tada, kai $h(F) = t$. Formulės F pagrindine logine operacija gali būti $\neg$, $\&$, $\vee$, $\rightarrow$.

Tarkime, $F = \neg G$. Jei $\neg G \in \Sigma$, tai $G \notin \Sigma$, nes aibė yra maksimali. Formulėje G yra m loginių operacijų, todėl pagal indukcijos prielaidą $h(G) = k$, o iš čia $h(\neg G) = \neg h(G) = t$.

Jei $\neg G \notin \Sigma$, tai $G \in \Sigma$ (aibė juk maksimali). Pagal indukcijos prielaidą $h(G) = t$ ir todėl $h(\neg G) = \neg h(G) = k$.

Tarkime, $F = G \& H$. Jei $G \& H \in \Sigma$, tai $G \in \Sigma$ ir $H \in \Sigma$, nes jei kuri nors viena (pavyzdžiui, G) nepriklausytų, tai $\neg G$ priklausytų ir $\{G \& H, \neg G\}$ turėtų būti įvykdoma kaip baigtinis aibės poaibis. Tai yra neįmanoma. Pagal indukcijos prielaidą $h(G) = h(H) = t$ ir kartu $h(G \& H) = t$.

Jei $G \& H \notin \Sigma$, tai bent viena iš G, H taip pat nepriklauso Σ, nes jei abi priklausytų Σ, tai turėtų būti interpretacija, su kuria $\{G, H, \neg(G \& H)\}$ įvykdoma. Pagal indukcijos prielaidą bent viena iš G, H yra klaidinga su interpretacija h, o todėl ir $G \& H$ klaidinga su ta pačia interpretacija.

Panašiai nagrinėjami ir atvejai, kai formulės pagrindinė operacija yra $\vee$ arba $\rightarrow$. Teorema įrodyta.

6.8 teorema (kompaktiškumo). *Formulių aibė T įvykdoma tada ir tiktai tada, kai ji baigiai įvykdoma.*

Įrodymas. Jei formulių aibė T įvykdoma, tai, aišku, ji ir baigiai įvykdoma. Tarkime, kad T baigiai įvykdoma. Parodysime, kad ji įvykdoma. Pastebėsime, kad T nebūtinai sutampa su kuria nors Σ_h, nors ir yra begalinė. Pavyzdžiui, aibė $\{p_1, p_1\&p_2, p_1\&p_2\&p_3, \ldots\}$.

Teoremą įrodyti pakanka rasti tokią maksimalią aibę Σ, kad $T \subset \Sigma$, nes tuomet, remiantis 6.7 teorema, atsiras tokia interpretacija h, kad $\Sigma = \Sigma_h$. Su ta pačia interpretacija h bus teisingos ir visos T formulės, t.y. T įvykdoma. Visų formulių aibė yra skaičioji. Tarkime, sekoje $F_1, F_2, F_3, \ldots$ aptinkama bet kuri nagrinėjamojo pavidalo formulė ir tiktai vieną kartą. Aibes apibrėžiame tokiu būdu:

$$T_0 = T,$$

$$T_{n+1} = \begin{cases} T_n \cup \{F_n\}, & \text{jei ji baigiai įvykdoma,} \\ T_n \cup \{\neg F_n\} & \text{priešingu atveju.} \end{cases}$$

Parodysime, kad bent viena iš aibių $T_n \cup \{F_n\}$, $T_n \cup \{\neg F_n\}$ baigiai įvykdoma, jei tokia yra T_n. Jei jos abi nebūtų baigiai įvykdomos, tai atsirastų jų baigtiniai neįvykdomi poaibiai:

$$A = \{G_1, \ldots, G_r, F_n\}, \qquad B = \{H_1, \ldots, H_s, \neg F_n\}.$$

Tai reikštų, kad jau T_n nebuvo baigiai įvykdoma, nes $\{G_1, \ldots, G_r, H_1, \ldots, H_s\}$ yra T_n poaibis ir nėra įvykdomas. Iš tikrųjų, jei jis įvykdomas, t.y. yra tokia interpretacija g, kad

$$g(G_1) = \cdots = g(G_n) = g(H_1) = \cdots = g(H_s) = t,$$

tai su ta pačia interpretacija įvykdoma ir bent viena iš aibių A, B. Ieškomoji Σ ir yra $\bigcup_{n=0}^{\infty} T_n$. Aibė $T \subset \Sigma$ ir, be to, Σ yra maksimali. Teorema įrodyta.

Išvada. Jei begalinė formulių aibė prieštaringa, tai egzistuoja jos baigtinis prieštaringas poaibis.

6.6 Semantiniai medžiai

Nagrinėjame formules su funkciniais simboliais, bet be laisvųjų kintamųjų. Transformuojame į normaliąją priešdėlinę formą bei skulemizuojame.

Formulės F ***Herbrando universumas*** (sritis) nusakomas tokiu būdu:

1. Visos konstantos, priklausančios formulei F, priklauso ir universumui H. Jei formulėje F nėra konstantų, tai jai priklauso konstanta a.

2. Jei f^n yra n-vietis funkcinis simbolis, priklausantis F, ir $t_1, \ldots, t_n$ yra H elementai, tai $f(t_1, \ldots, t_n)$ taip pat priklauso universumui H.

Taigi kad ir kokia būtų formulė F, jos universumas H nėra tuščias. Jis gali būti baigtinis arba skaitusis.

Formulės F ***Herbrando bazę*** B sudaro visos tokios atominės formulės $P(t_1, \ldots, t_n)$, kuriose P^n yra n-vietis predikatinis kintamasis, priklausantis F, o $t_1, \ldots, t_n$ – kurie nors universumo H elementai.

Formulės F ***H-interpretacija*** vadiname aibę $\{\alpha_1 P_1, \alpha_2 P_2, \ldots\}$, kurioje $\alpha_i \in \{\neg, \emptyset\}$, o P_i $(i = 1, 2, \ldots)$ yra visi aibės B elementai. Jei $\alpha_i = \neg$, tai laikome $P_i = k$, o jei $\alpha_i = \emptyset$, tai $P_i = t$.

Prancūzų logikas J. Herbrand 1930 m. įrodė teoremą.

Teorema. *Formulė F įvykdoma tada ir tiktai tada, kai ji įvykdoma aibėje H.*

Formulės F H-interpretacija vadinama ***modeliu***, jei F teisinga su ja.

Primename, kad nagrinėjame skulemizuotas formules, kurios prieš tai buvo transformuotos į normaliąją priešdėlinę formą. Tik tokioms formulėms galioja Herbrando teorema. Pavyzdžiui, formulė $P(a) \& \exists x \neg P(x)$ įvykdoma. Imkime individinių konstantų aibę $M = \{a, b\}$, o P apibrėžkime taip: $P(a) = t$, $P(b) = k$. Bet ji neturi H-modelio. $H = \{a\}$, $P(a) = t$ arba $P(a) = k$. Abiem atvejais formulė klaidinga.

Taigi nagrinėjame formules pavidalo $\forall x_1 \forall x_2 \ldots \forall x_n G(x_1, x_2, \ldots, x_n)$; čia G – bekvantorė formulė. Remiantis Herbrando teorema, galima sakyti, kad individinių kintamųjų kitimo sritis yra aibė H. Nagrinėjame pagrindinių formulių aibę $T = \{G(t_1, \ldots, t_n)\text{: } t_1, \ldots, t_n \in H\}$. Ji baigtinė tik tuo atveju, kai formulėje nėra funkcinių simbolių. Pagal kompaktiškumo teoremos išvadą, aibė T nėra įvykdoma, t.y. prieštaringa tada ir tiktai tada, kai egzistuoja jos baigtinis neįvykdomas poaibis.

Visas galimas H-interpretacijas (jų ne daugiau kaip kontinuumas) vaizduosime medžiu. Tuo tikslu išrašome kokia nors tvarka nagrinėjamosios formulės bazės H elementus. Tarkime, tai $P_1, P_2, \ldots$. Medžio pavidalo grafą

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{P_3}\quad\dfrac{\vdots}{\neg P_3}}{P_2}\qquad\dfrac{\dfrac{\vdots}{P_3}\quad\dfrac{\vdots}{\neg P_3}}{\neg P_2}}{P_1}\qquad\dfrac{\dfrac{\dfrac{\vdots}{P_3}\quad\dfrac{\vdots}{\neg P_3}}{P_2}\qquad\dfrac{\dfrac{\vdots}{P_3}\quad\dfrac{\vdots}{\neg P_3}}{\neg P_2}}{\neg P_1}}{F}$$

vadiname ***semantiniu medžiu***.

Kiekvienas kelias (jis begalinis, kai H begalinė) atitinka kurią nors H-interpretaciją. Semantinis medis yra teisingumo lentelių teiginių logikos formulėms analogas. Jei formulė tapačiai klaidinga, tai remiantis kompaktiškumo teoremos išvada kiekviename kelyje, prasidedančiame formule F, yra toks k (jis priklauso nuo pasirinkto kelio), kad su interpretacija $\{\alpha_1 P_1, \alpha_2 P_2, \ldots, \alpha_k P_k\}$ formulė klaidinga. Tuomet medyje nuvalome $\alpha_{k+1} P_{k+1}, \alpha_{k+2} P_{k+2}, \ldots$, o virš viršūnės $\alpha_k P_k$ pažymime $\oplus$.

Semantinis medis transformuojamas į baigtinį tada ir tiktai tada, kai formulė tapačiai klaidinga.

Pavyzdžiai:

1. Raskime baigtinį semantinį formulės $\forall x(P(x, f(a))\&\neg P(x, x))$ medį.

Sprendimas. $H = \{a, f(a), f(f(a)), \ldots\}$, $B = \{P(a, a), P(a, f(a)), P(f(a), f(a)), \ldots\}$.

$$\dfrac{\dfrac{\oplus}{P(a,a)} \qquad \dfrac{\dfrac{\dfrac{\oplus}{P(f(a),f(a))} \quad \dfrac{\oplus}{\neg P(f(a),f(a))}}{P(a,f(a))} \qquad \dfrac{\oplus}{\neg P(a,f(a))}}{\neg P(a,a)}}{F}.$$

2. Raskime formulės $\forall x(P(x)\&(\neg P(x) \vee Q(f(x)))\&\neg Q(f(a)))$ baigtinį semantinį medį.

Sprendimas. Čia $H = \{a, f(a), f(f(a)), \ldots\}$, $B = \{Q(a), P(a), Q(f(a)), P(f(a)), \ldots\}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\oplus}{Q(f(a))} \quad \dfrac{\oplus}{\neg Q(f(a))}}{P(a)} \quad \dfrac{\oplus}{\neg P(a)}}{Q(a)} \qquad \dfrac{\dfrac{\dfrac{\oplus}{Q(f(a))} \quad \dfrac{\oplus}{\neg Q(f(a))}}{P(a)} \quad \dfrac{\oplus}{\neg P(a)}}{\neg Q(a)}}{F}.$$

6.7 Rezoliucijų metodas

Nagrinėjame normaliosios priešdėlinės formos skulemizuotas formules F pavidalo $\forall x_1 \forall x_2 \ldots \forall x_n G(x_1, x_2, \ldots, x_n)$. Iš Herbrando teoremos išplaukia, kad F tapačiai klaidinga tada ir tiktai tada, kai aibė $A = \{G(t_1, \ldots, t_n)\colon t_1, \ldots, t_n \in H\}$ yra prieštaringa. Aibė A yra teiginių logikos formulių numeruojamoji aibė. Transformuojame $G(x_1, \ldots, x_n)$ į normaliąją konjunkcinę formą. Tarkime,

$G(x_1, \dots, x_n) = \&_{i=1}^{s} D_i(x_1, \dots, x_n)$. Nagrinėjame teiginių logikos formulių aibę

$$K = \{D_i(t_1, \dots, t_n)\colon t_1, \dots, t_n \in H;\ i \in \{1, \dots, s\}\}. \qquad (6.1)$$

Ji prieštaringa tada ir tiktai tada, kai prieštaringa A. Remiantis kompaktiškumo teoremos išvada, aibė prieštaringa tada ir tiktai tada, kai egzistuoja jos baigtinis prieštaringas poaibis. Savo ruožtu baigtinė teiginių logikos formulių aibė prieštaringa tada ir tiktai tada, kai iš jos išvedamas tuščias disjunktas.

Taigi norėdami nustatyti, ar kuri nors uždara predikatų logikos formulė tapačiai klaidinga, atliekame tokius veiksmus:

1) transformuojame į normaliąją priešdėlinę formą,

2) skulemizuojame, išbraukiame bendrumo kvantorius,

3) randame Herbrando universumą H,

4) sudarome disjunktų aibę.

Tarkime, gautoji aibė $S = \{D_1(x_1^1, \dots, x_{n_1}^1), \dots, D_u(x_1^u, \dots, x_{n_u}^u)\}$. Prieštaringojo baigtinio poaibio ieškome taip.

Visus aibės $\{D_i(t_1^i, \dots, t_{n_i}^i)\colon t_1^i, \dots, t_{n_i}^i \in H;\ i \in \{1, \dots, u\}\}$ elementus (teiginių logikos formules) išrašome kuria nors tvarka (ji baigtinė arba skaičioji): $G_1, G_2, G_3, \dots$. Tikriname, ar iš $\{G_1, G_2\}$ išvedamas tuščias disjunktas. Jei taip, tai nagrinėjamoji formulė yra tapačiai klaidinga, jei ne, tai tikriname, ar iš $\{G_1, G_2, G_3\}$ išvedamas tuščias disjunktas. Formulė tapačiai klaidinga tada ir tiktai tada, kai yra toks i, kad iš $\{G_1, G_2, \dots, G_i\}$ išvedamas tuščias disjunktas. Taigi, jei ji klaidinga, turi būti tas poaibis, o jei ne, tai aprašytoji procedūra tęsis be galo ilgai.

Tokia procedūra nėra patogi ieškant prieštaringo poaibio. Aprašysime kitokią. Toks paieškos būdas vadinamas ***rezoliucijų metodu***. Jį 1965 m. aprašė amerikiečių logikas J.A. Robinson. Tarkime, norime nustatyti, ar uždara formulė F tapačiai klaidinga. Kaip ir anksčiau, pagal F randame disjunktų aibę S. Aprašysime metodą, kuriuo ieškoma tuščio disjunkto išvedimo iš S.

Reiškinį (termą, formulę, ...) vadiname *pagrindiniu*, jei jame nėra individinių kintamųjų įeičių.

6.14 apibrėžimas. ***Keitiniu*** *vadiname reiškinį pavidalo* $(t_1/x_1, t_2/x_2, \dots, t_n/x_n)$; *čia* t_i *— termai (nebūtinai pagrindiniai).*

Keitinius žymime raidėmis $\alpha, \beta, \sigma, \gamma$. Reiškinį (termą, formulę), kuriame visos kintamojo x_i $(i = i, \dots, n)$ įeitys pakeistos termu t_i, žymime $R\alpha$.

6.15 apibrėžimas. *Keitinys α vadinamas reiškinių R, R'* ***unifikatoriumi****, jei $R\alpha = R'\alpha$.*

6.16 apibrėžimas. *Unifikatorius σ vadinamas* ***bendriausiuoju*** *reiškiniams R, R', jei bet kuriam reiškinių R, R' unifikatoriui α, egzistuoja toks β, kad α yra lygus β ir σ kompozicijai.*

Keitinys σ yra baigtinės atominių formulių aibės $\{A_1, \ldots, A_m\}$ bendriausias unifikatorius, jei $A_1\sigma = \cdots = A_m\sigma$ ir bet kuriam šios aibės unifikatoriui α yra toks β, kad α lygus β ir σ kompozicijai.

Pavyzdžiai:

1. Keitinys $\sigma = (c/x, d/y, f(d)/z)$ yra atominių formulių poros $P(g(y, c), z)$, $P(g(d, x), f(d))$ unifikatorius.

2. Atominių formulių pora $P(x, f(f(y)))$, $P(f(z), f(f(g(a))))$ unifikuojama. Jos unifikatoriai yra:

$$\sigma = (f(a)/x, g(a)/y, a/z), \qquad \beta = (f(f(a))/x, g(a)/y, f(a)/z).$$

Bendriausias unifikatorius yra keitinys $\alpha = (f(z)/x, g(a)/y, /z)$. Žymėjimas $/z$ reiškia, kad z gali būti bet koks iš nagrinėjamosios termų aibės. Keitiniuose tokius praleisime, t.y. bendriausiąjį unifikatorių šiuo atveju užrašysime $\alpha = (f(z)/x, g(a)/y)$.

Suprantama, ne visi reiškiniai unifikuojami. Formulės $P(t)$, $P(t')$ nėra unifikuojamos, jei, pavyzdžiui, termai t, t' yra:

a) dvi skirtingos konstantos,

b) kintamasis x ir termas (aukštis ne mažesnis kaip 1), kuriame aptinkamas x,

c) konstanta ir funkcinis simbolis,

d) prasidedantys skirtingais funkciniais simboliais termai.

Rezoliucijos taisyklė yra tokia:

$$\frac{C_1 \quad C_2}{C};$$

čia C, C_1, C_2 yra disjunktai, C_1, C_2 vadinami prielaidomis, o C – išvada. Rezoliucijos taisyklę taikysime disjunktų aibei S. Keitinių termuose pasitaikančios konstantos bei funkciniai simboliai priklauso aibės S formulėms. Kablelis aibėje

S atitinka konjunkciją, o visi laisvieji kintamieji suvaržyti tik bendrumo kvantoriais, todėl, jei tai tikslinga, skirtingus disjunktus galima laikyti neturinčiais bendrų laisvųjų kintamųjų.

Rezoliucijos taisyklė:
$$\frac{D_i\sigma \quad D_j\sigma}{D\sigma}.$$

Taisyklė taikoma prielaidoms, kuriose galima rasti tokias dvi literas $P(t_1', \ldots, t_n')$, $\neg P(t_1'', \ldots, t_n'')$ (jos yra skirtingose prielaidose), kad σ yra $P(t_1', \ldots, t_n')$, $P(t_1'', \ldots, t_n'')$ unifikatorius. $D\sigma$ gaunama išbraukus $P(t_1', \ldots, t_n')\sigma$, $\neg P(t_1'', \ldots, t_n'')\sigma$ iš prielaidų ir apjungus gautąsias formules disjunkcija. Jei išvadoje yra dvi vienodos literos ar daugiau, tai paliekama tik viena.

6.17 apibrėžimas. *Sakoma, kad iš S išvedamas tuščias disjunktas, jei egzistuoja baigtinė disjunktų seka $E_1, \ldots, E_r$, tenkinanti sąlygas*:

1) $E_r = \Box$,

2) *kiekviena E_i priklauso aibei S arba gauta iš kairėje jos esančių disjunktų pagal rezoliucijos taisyklę.*

Kaip matome, keitiniuose naudojami ne tik pagrindiniai termai. Turint tuščio disjunkto išvedimą, kintamuosius jame galime pakeisti kuriais nors (skirtingus galbūt skirtingais) termais iš H ir gauti tuščio disjunkto išvedimą iš formulių aibės (6.1). Vadinasi, pradinė formulė yra tapačiai klaidinga.

Pavyzdys. Įrodykime rezoliucijų metodu, kad teisingas toks samprotavimas:

Nė vienas žmogus nėra vabzdys. Yra musės ir nė viena jų nėra ne vabzdys. Vadinasi, kai kurios musės nėra žmonės.

Pažymėkime $Z(x)$ predikatą „*x yra žmogus*", $M(x)$ – „*x yra musė*", $V(x)$ – „*x yra vabzdys*". Tuomet reikia nustatyti, ar iš $\forall x(Z(x) \to \neg V(x))$, $\exists x M(x)$, $\forall x(M(x) \to V(x))$ išplaukia $\exists x(M(x) \& \neg Z(x))$, t.y. ar prieštaringa aibė

$$\{\forall x(Z(x) \to \neg V(x)), \exists x M(x), \forall x(M(x) \to V(x)), \neg\exists x(M(x) \& \neg Z(x))\}.$$

Transformuojame ją į disjunktų aibę:

$$S = \{\neg Z(x) \vee \neg V(x), M(a), \neg M(x) \vee V(x), \neg M(x) \vee Z(x)\}.$$

Tuomet tuščio disjunkto išvedimas yra toks (kad būtų vaizdžiau, pateiksime jį ne sekos pavidalu):

$$\frac{M(a) \quad \neg M(x) \vee V(x)}{V(a)}, \quad \sigma = \{a/x\},$$

$$\frac{V(a) \quad \neg Z(x) \vee \neg V(x)}{\neg Z(a)}, \quad \sigma = \{a/x\},$$

$$\frac{\neg Z(a) \quad \neg M(x) \vee Z(x)}{\neg M(a)}, \quad \sigma = \{a/x\},$$

$$\frac{M(a) \quad \neg M(a)}{\square}, \quad \sigma = \emptyset.$$

Rezoliucijų metodo taktikos. Taikant rezoliucijos taisyklę, galima reikalauti ir papildomų sąlygų tiek taisyklės prielaidoms, tiek ir išvadai. Tie reikalavimai vadinami ***išvedimų taktikomis***. Taktika vadinama *pilnąja*, jei tuščias disjunktas išvedamas rezoliucijų metodu tada ir tiktai tada, kai jis išvedamas ir prisilaikant taktikos. Naudojantis taktikomis, išvedamų disjunktų aibės dažniausiai yra siauresnės. Aprašysime keletą pilnųjų taktikų.

1. *Tiesinė taktika.* Tarkime, disjunktas C išvedamas iš aibės S ir $T_1, T_2, \ldots, T_k$ yra rezoliucijos taisyklės taikymų seka, tenkinanti sąlygas:

a) T_k išvada yra disjunktas C,

b) kiekvieno taikymo T_i $(i > 1)$ viena iš prielaidų yra T_{i-1} išvada.

Toks disjunkto išvedimas vadinamas tiesiniu.

2. *Podisjunkčio taktika.* Disjunktas C yra D podisjunktis (D vadinamas C viršdisjunkčiu), jei egzistuoja toks keitinys σ, kad $D = C\sigma \vee D'$. Pavyzdžiui, $C = P(x)$, $D = P(a) \vee Q(a)$. Tuomet C yra D podisjunktis, nes $D = C\sigma \vee Q(a)$, kai $\sigma = \{a/x\}$. Apribojimai rezoliucijos taisyklei tokie: išvada negali būti jau turimų disjunktų viršdisjunkčiu.

Naudojantis šia taktika, peržiūrimi visi jau turimi disjunktai. Jei, pritaikius taisyklę, tarp turimų disjunktų yra išvados viršdisjunkčių, tai jie išbraukiami.

3. *Semantinės rezoliucijos taktika.* Tarkime, S yra disjunktų aibė ir I – kuri nors interpretacija, suskaidanti S į du poaibius: S_+ ir S_-. Poaibiui S_+ priklauso visi tie disjunktai, kurie teisingi su interpretacija I, o poaibiui S_- – tie, kurie klaidingi. Pagal semantinės rezoliucijos taktiką rezoliucijos taisyklės taikymo prielaidos gali būti tik disjunktai, priklausantys skirtingiems poaibiams. Gautąją išvadą, jei ji teisinga su interpretacija I, priskiriame aibei S_+, jei ne – aibei S_-.

Pavyzdys. $S = \{p \vee q \vee \neg r, \neg p \vee q, \neg q \vee \neg r, r\}$, I: $p = t, q = t, r = k$. Tuomet $S_+ = \{p \vee q \vee \neg r, \neg p \vee q, \neg q \vee \neg r\}$, $S_- = \{r\}$,

$$\frac{p \vee q \vee \neg r \quad r}{p \vee q}, \qquad p \vee q = t.$$

Todėl $S_+ = \{p \vee q \vee \neg r, \neg p \vee q, \neg q \vee \neg r, p \vee q\}$, $S_- = \{r\}$,

$$\frac{\neg q \vee \neg r \quad r}{\neg q}, \qquad \neg q = k.$$

Tada $S_+ = \{p \vee q \vee \neg r, \neg p \vee q, \neg q \vee \neg r, p \vee q\}$, $S_- = \{r, \neg q\}$,

$$\frac{\neg q \quad p \vee q}{p}, \quad p \in S_+, \qquad \frac{\neg p \vee q \quad \neg q}{\neg p}, \quad \neg p \in S_-, \qquad \frac{p \quad \neg p}{\Box}.$$

4. *Tvarkos taktika.* Visus aibės S predikatinius simbolius (loginius kintamuosius) išrašome kuria nors tvarka $P > Q > R > \cdots$. Jei taisyklės taikymo prielaidoje yra ne viena litera, kurios atžvilgiu galima taikyti taisyklę, tai privalome rinktis tą, kurios vardas didžiausias.

5. *Absorbcijos taktika.* Sakysime, kad disjunktas $C' = L \vee D$ absorbuojamas disjunkto C'', jei $C'' = \neg L \vee D \vee D'$; čia L yra litera, laikome $\neg\neg L = L$, D, D' – disjunktai, D' gali būti ir tuščias. Pagal absorbcijos taktiką rezoliucijos taisyklę galima taikyti tik disjunktams, kai vienas jų absorbuojamas antrojo, tiksliau, kai $C'\sigma$ yra absorbuojamas $C''\sigma$ arba atvirkščiai.

6.8 Pratimai

1. Išveskite skaičiavime G sekvencijas:

a) $\exists x M(x), \forall x(M(x) \to P(x)), \forall x(M(x) \to S(x)) \vdash \exists x(S(x) \& P(x))$,

b) $\vdash (\neg\forall x A(x) \to \exists x \neg A(x)) \& (\exists x \neg A(x) \to \neg\forall x A(x))$,

c) $\vdash \exists x \forall y \forall z \exists v((P(x) \vee \neg P(y)) \& (P(z) \vee \neg P(v)))$.

2. Įrodykite, kad sekvencija $\vdash \forall y \exists x A(x, y) \to \exists x \forall y A(x, y)$ neišvedama.

3. Išveskite intuicionistiniame sekvenciniame skaičiavime:

a) $\vdash A \to (\neg A \to B)$,

b) $\vdash (A \to B) \to (\neg B \to \neg A)$,

c) $\vdash \exists x \exists y(\neg\neg(\neg\neg A(x) \to A(y)))$,

d) $\vdash \forall x \exists y((\neg\neg A(x) \to A(y)) \to (\neg\neg(A(x) \to B(y)) \to (A(x) \to B(y))))$,

e) $\neg\neg(A \to B), A \vdash \neg\neg B$,

f) $\neg\neg B \to B, \neg\neg(A \to B) \vdash A \to B$,

g) $\neg(A \vee B) \equiv \neg A \& \neg B$.

4. Ar intuicionistinėje logikoje $\neg A \vee B \equiv A \rightarrow B$?

5. Raskite išvedimus klasikiniame ir intuicionistiniame sekvenciniame skaičiavimuose:

$$p_1 \vee (p_2 \vee (p_3 \vee \ldots (p_{n-1} \vee p_n))) \ldots) \vdash (((\ldots (p_1 \vee p_2) \vee p_3) \vee \ldots \vee p_{n-1}) \vee p_n.$$

6. Ar *unifikuojami* termai:

$$t_1 = g(f(c, g(x_4, x_5)), f(c, g(x_5, x_4)), k(x_5, x_4, x_1)),$$

$$t_2 = g(x_2, x_2, x_6)?$$

7. Transformuokite į tiesinį išvedimą:

$$\dfrac{\dfrac{M}{C_3 \vee p} \qquad \dfrac{C_1 \vee \neg p \vee q \qquad C_2 \vee \neg q}{C_1 \vee C_2 \vee \neg p}}{C_1 \vee C_2 \vee C_3}.$$

Raide M žymime disjunkto $C_3 \vee p$ išvedimą. Žinoma, kad M yra tiesinis.

8. Raskite tiesinį tuščio disjunkto išvedimą iš S:

$$S = \{\neg E(x) \vee V(x) \vee S(x, f(x)), \neg E(x) \vee V(x) \vee C(f(x)), P(a), E(a),$$

$$\neg S(a, y) \vee P(y), \neg P(x) \vee \neg V(x), \neg P(x) \vee \neg C(x)\}.$$

9. Naudodamiesi semantinės rezoliucijos taktika, raskite tuščio disjunkto išvedimą:

a) $S = \{p_1 \vee p_2, p_1 \vee \neg p_2, \neg p_1 \vee p_2, \neg p_1 \vee \neg p_2\}$, I: $p_1 = t$, $p_2 = k$,

b) $S = \{\neg Q(x) \vee \neg Q(a), R(b) \vee S(c), Q(x) \vee Q(a) \vee \neg R(y) \vee \neg R(b), \neg S(c)\}$,
I: $Q(a) = t, Q(b) = t, Q(c) = t,$
$R(a) = k, R(b) = k, R(c) = k,$
$S(a) = k, S(b) = k, S(c) = k.$

10. Naudodamiesi absorbcijos taktika, išveskite tuščią disjunktą:

a) $S = \{\neg C(x) \vee Q(a) \vee P(y), \neg C(x) \vee \neg Q(a) \vee P(b), C(x) \vee \neg Q(x) \vee P(b), C(x) \vee Q(a) \vee \neg P(b), \neg C(a) \vee Q(a) \vee \neg P(x), C(a) \vee \neg Q(a) \vee \neg P(x), \neg C(a) \vee \neg Q(a) \vee \neg P(b), C(x) \vee Q(x) \vee P(b)\}$,

b) $S = \{\neg Q(f(a)) \vee R(f(x)) \vee V(x), Q(f(x)) \vee \neg P(f(x)), \neg V(x) \vee R(f(x)), \neg R(f(x)) \vee \neg Q(f(x)), P(f(a)) \vee W(x), \neg W(x) \vee Q(f(a))\}$.

11. Individidinių konstantų aibė yra realieji skaičiai. $T(x, y, u, v) = t$ tada ir tiktai tada, kai figūra $xyuv$ yra trapecija. $P(x, y, u, v) = t$, kai atkarpa xy lygiagreti su atkarpa uv. $E(x, y, z, u, v, w) = t$, kai kampas xyz lygus kampui uvw.

Žinoma, kad:

$$\forall x \forall y \forall u \forall v (T(x, y, u, v) \to P(x, y, u, v)),$$

$$\forall x \forall y \forall u \forall v (P(x, y, u, v) \to E(x, y, v, u, v, y)),$$

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

Rezoliucijų metodu įrodykite, kad iš šių formulių išplaukia $E(a, b, d, c, d, b)$.

12. Tarkime, kad išvedimo medį mokame transformuoti į išvedimo medį pagal absorbcijos taktiką, kai jame yra ne daugiau kaip n rezoliucijos taisyklių (indukcijos prielaida). Disjunkto $A \vee B$ išvedimo medis, kuriame $(n + 1)$ kartą taikoma rezoliucijos taisyklė:

$$(*)\,\dfrac{\dfrac{\dfrac{M_1}{A \vee p \vee q} \quad \dfrac{M_2}{A \vee p \vee \neg q}}{A \vee p} \qquad \dfrac{M_3}{B \vee \neg p}}{A \vee B}.$$

Ženklu $(*)$ pažymėtas taisyklės taikymas, pažeidžiantis absorbcijos reikalavimą. Įrodykite, kad disjunkto $A \vee B$ išvedimą galima rasti naudojantis absorbcijos taktika.

7 skyrius
Modalumo logikos

Klasikinės logikos kalbą praplėsime vadinamaisiais *modalumo operatoriais*, nusakančiais *būtinimą* ir *galimybę*. Jų dėka galima formalizuoti ir tvirtinimus, kuriais išreiškiame tvirtą įsitikinimą kurio nors teiginio teisingumu ar abejones. Modalumo logikos buvo nagrinėjamos dar antikos laikais. Naujo etapo pradžia siejama su amerikiečių logiko C.I. Lewiso darbais, pasirodžiusiais XX amžiaus antrajame dešimtmetyje. Juose aprašytos modalumo logikų formaliosios sistemos (skaičiavimai). Yra daug priežasčių, pateisinančių logikoje modalumą. Viena jų – išvengti „implikacijos paradokso" (iš klaidingo išvedamas bet koks teiginys). Buvo norima išskirti dvi rūšis *tiesos*: *būtiną* ir *galimą*. Galima tiesa egzistuoja tik tam tikruose pasauliuose.

7.1 Modalumo logikų formulių semantika

Naudosimės dviem modalumo operatoriais. Juos žymime $\Box$ (būtinumas) ir $\Diamond$ (galimybė). Pateikiame modalumo (teiginių) logikų formulių apibrėžimą.

7.1 apibrėžimas:

1. *Loginis kintamasis yra formulė.*
2. *Jei F yra formulė, tai $\neg F$, $\Box F$, $\Diamond F$ – taip pat formulės.*
3. *Jei F, G yra formulės, tai $(F\&G)$, $(F\vee G)$, $(F \to G)$ – taip pat formulės.*

Formulių pavyzdžiai: $\Box\Diamond p$, $\Box(p \to (\Box q\&\Diamond\Diamond p))$, $(\neg p \vee \Box\Box(q \vee p))$.

Toliau išorinius skliaustus praleisime. Užrašą $\Box p$ skaitome „*būtinai p*", o $\Diamond p$ – „*galbūt p*".

Galimos ir kitos modalumo operatorių interpretacijos:

$\Box F$	$\Diamond F$
Vienas asmuo (agentas) žino, kad F teisingas	Vienas asmuo (agentas) nežino, ar $\neg F$ teisingas
Vienas asmuo įsitikinęs, kad F	Vienas asmuo F laiko galimu
Visada F	Kai kada F
F tikrai įvyks	Įvykis F tikėtinas
F įrodoma	F nėra tapačiai klaidinga
Visi nedeterminuotojo skaičiavimo keliai su pradiniais duomenimis F baigiasi galutinėmis būsenomis	Kai kurie nedeterminuotojo skaičiavimo keliai su pradiniais duomenimis F baigiasi galutinėmis būsenomis

Kad būtų papraščiau, kai kada nagrinėjamos formulės, kuriose yra tik vienas modalumo operatorius $\Box$, formulė $\neg\Box\neg F$ žymima $\Diamond F$.

Pateikiame Kripke standartinę modalumo logikų formulių semantiką.

7.2 apibrėžimas. *Modalumo logikų teiginių formulės F Kripke struktūra vadiname trejetą $\Phi = (M, R, V)$; čia M – kuri nors netuščia aibė, vadinama* ***galimų pasaulių aibe****, R – apibrėžtas aibėje M binarusis predikatas, vadinamas* ***pasaulių sąryšiu****, V –* ***aibė interpretacijų*** *pasauliuose (t.y. funkcijų, apibrėžtų formulės F loginių kintamųjų aibėje su reikšmėmis iš $\{t, k\}$ ir priklausančių nuo pasaulių).*

Tarkime, $\Phi = (M, R, V)$ yra tam tikros formulės kuri nors struktūra. Tvirtinimą, kad *formulė teisinga struktūros Φ pasaulyje α*, suprantame, kad *formulė teisinga su pasaulį α atitinkančia interpretacija iš V.*

7.3 apibrėžimas. *Formulės F teisingumas struktūros Φ pasaulyje α nusakomas taikant indukciją pagal formulės pavidalą:*

- *jei F yra loginis kintamasis, tai F yra teisinga tada ir tiktai tada, kai jis (loginis kintamasis) teisingas pasaulyje α,*
- *jei $F = \neg G$, tai F teisinga tada ir tiktai tada, kai G klaidinga pasaulyje α,*
- *jei $F = G \& H$, tai F teisinga tada ir tiktai tada, kai abi F, G teisingos pasaulyje α,*
- *jei $F = G \vee H$, tai F teisinga tada ir tiktai tada, kai bent viena iš G, H teisinga pasaulyje α,*
- *jei $F = G \to H$, tai F teisinga tada ir tiktai tada, kai G klaidinga arba H teisinga pasaulyje α,*

- *jei* $F = \Box G$*, tai* F *teisinga tada ir tiktai tada, kai* G *teisinga visuose tokiuose pasauliuose* α'*, kad* $R(\alpha, \alpha') = t$,
- *jei* $F = \Diamond G$*, tai* F *teisinga tada ir tiktai tada, kai yra bent vienas toks pasaulis* α'*, kad* $R(\alpha, \alpha') = t$ *ir* G *teisinga pasaulyje* α'.

7.4 apibrėžimas. *Sakoma, kad* ***formulė F įvykdoma****, jei egzistuoja tokia struktūra* $\Phi = (M, R, V)$ *ir pasaulis* $\alpha \in M$*, kad* F *teisinga pasaulyje* α.

7.5 apibrėžimas. *Sakoma, kad* ***formulė F tapačiai teisinga****, jei ji teisinga bet kurios struktūros kiekviename pasaulyje.*

7.6 apibrėžimas. *Sakoma, kad* ***formulė F tapačiai klaidinga****, jei ji klaidinga bet kurios struktūros kiekviename pasaulyje.*

Pavyzdžiai:

1. $F = \Box p$. Struktūrą (M, R, V) apibrėžiame taip: M – *pasaulio valstybės*, $R(x, y) = t$ tada ir tiktai tada, kai valstybės x, y turi bendrą sieną, interpretacijos V – *sausis yra šalčiausias valstybėje mėnuo*. Tuomet priklausomai nuo pasirinkto pasaulio formulė F gali būti tiek teisinga, tiek ir klaidinga. Pasirinktos struktūros pasaulyje *Lietuva* formulė teisinga, nes visose Lietuvos kaimyninėse valstybėse iš tikrųjų sausis yra šalčiausias metų mėnuo. Tuo tarpu pasirinkus *Pietų Afrikos Respubliką*, formulė būtų klaidinga. Taigi formulė įvykdoma, bet nėra tapačiai teisinga.

2. $F = p \to \Box\Box p$, M – sveikųjų skaičių aibė, $R(x, y) = t$ tada ir tiktai tada, kai $y = x + 1$. Interpretacijos V – *pasaulis nusakomas neigiamu skaičiumi*. Pasaulyje *minus vienetas* formulė p teisinga, o $\Box\Box p$ klaidinga, nes ji atitinka teiginį *plius vienetas yra neigiamas skaičius*. Kadangi F yra pastarųjų implikacija, tai ji pasaulyje *minus vienas* klaidinga.

7.7 apibrėžimas. *Modalumo logikų formulės* F *projekcija į klasikinę logiką vadiname formulę, gautą iš* F *(žymime* pr(F)*), išbraukus joje visas modalumo operatorių įeitis.*

Pavyzdys. $F = p\&(\Box\Diamond q \vee \neg\Box p)$. Tuomet $\mathrm{pr}(F) = p\&(q \vee \neg p)$.

Pastebėkime, jei klasikinės logikos formulė $\mathrm{pr}(F)$ nėra tapačiai teisinga, tai ir F nėra tapačiai teisinga. Iš tikrųjų yra interpretacija, su kuria $\mathrm{pr}(F)$ klaidinga. Struktūrą apibrėžiame taip: M yra iš vienintelio elemento a, $R(a, a) = t$, aibei V priklauso tik viena interpretacija – būtent ta, su kuria $\mathrm{pr}(F)$ klaidinga. Tuomet abiejų formulių F ir $\mathrm{pr}(F)$ reikšmės sutampa, t.y. F klaidinga.

Tačiau, jei pr(F) tapačiai teisinga, F nebūtinai tapačiai teisinga. Pavyzdžiui, formulė $(p \vee q) \to (p \vee q)$ tapačiai teisinga, o $\Box(p \vee q) \to (\Box p \vee \Box q)$ nėra tapačiai teisinga. Tarkime, M – natūraliųjų skaičių aibė. $R(x, y) = t$ tada ir tiktai tada, kai $y = x + 1$ arba $y = x + 2$. V yra tokių interpretacijų aibė: p – *pasaulis nusakomas lyginiu skaičiumi*, q – *pasaulis nusakomas nelyginiu skaičiumi*. Tuomet bet kuriame nurodytos struktūros pasaulyje formulė $\Box(p \vee q) \to (\Box p \vee \Box q)$ klaidinga.

Kad ir kokia būtų modalumo logikos formulė F, galima rasti tokią klasikinės predikatų logikos formulę $[F]_\tau$, kad F įvykdoma tada ir tiktai tada, kai įvykdoma $[F]_\tau$.

Taikydami indukciją pagal F pavidalą, apibrėžiame $[F]_\tau$: $[p]_\tau = P(\tau)$, čia p – loginis kintamasis, $P(\tau)$ – vienvietis predikatinis kintamasis.

$$
\begin{aligned}
&[\neg G]_\tau = \neg[G]_\tau,\\
&[H \& G]_\tau = [H]_\tau \& [G]_\tau,\\
&[H \vee G]_\tau = [H]_\tau \vee [G]_\tau,\\
&[H \to G]_\tau = [H]_\tau \to [G]_\tau,\\
&[\Box G]_\tau = \forall x(R(\tau, x) \to [G]_x),\\
&[\Diamond G]_\tau = \exists x(R(\tau, x) \& [G]_x).
\end{aligned}
$$

Abiem paskutiniais atvejais x yra naujas individinis kintamasis.

Pavyzdys

$$
\begin{aligned}
&[\Box\Diamond(p \to q)]_\tau = \forall x(R(\tau, x) \to [\Diamond(p \to q)]_x) =\\
&\forall x(R(\tau, x) \to \exists y(R(x, y) \& [p \to q]_y)) =\\
&\forall x(R(\tau, x) \to \exists y(R(x, y) \& ([p]_y \to [q]_y))) =\\
&\forall x(R(\tau, x) \to \exists y(R(x, y) \& (P(y) \to Q(y)))).
\end{aligned}
$$

7.2 Modalumo logikų skaičiavimai

Aprašysime kai kurių dažniausiai literatūroje pasitaikančių modalumo logikų skaičiavimus.

Hilberto tipo skaičiavimai. Nagrinėkime formules, kuriose gali būti tik modalumo operatorius $\Box$. Skaičiavimai gaunami klasikinės teiginių logikos Hilberto skaičiavimą papildžius naujomis aksiomomis bei taisykle.

Aksiomos:

1.1. $A \to (B \to A)$,

...

4.3. $\neg\neg A \to A$,

k. $\Box(A \to B) \to (\Box A \to \Box B)$,

t. $\Box A \to A$,

4. $\Box A \to \Box\Box A$.

Taisyklės:

$$\frac{A, A \to B}{B}, \quad \frac{A}{\Box A}.$$

Pirmoji taisyklė vadinama *modus ponens* (sutrumpintai ją žymime MP), o antroji – *apibendrinimo* (AT). Skaičiavimas, kuriame yra 1.1–4.3 ir k aksiomos, vadinamas modalumo logikos **K** skaičiavimu (arba tiesiog *modalumo logika* K). Modalumo logika **T** nusakoma skaičiavimu, kuris susideda iš 1.1–4.3 ir k, t aksiomų. Logika, kurios aksiomos yra 1.1–4.3 ir k, t, 4, vadinama modalumo logika **S4**. Abi taisyklės yra visų trijų minėtųjų logikų taisyklės.

7.8 apibrėžimas. *Formulės F išvedimu modalumo logikos X skaičiavime vadiname baigtinę formulių seką, kuri baigiasi formule F ir kurios kiekvienas narys yra modalumo logikos X skaičiavimo aksioma arba gautas iš kairėje nuo jo esančių narių pagal taisyklę* MP *ar* AT.

Paminėsime dar porą modalumo logikų, kurių šioje knygoje nenagrinėsime. Formulę $\Box A \to \Diamond A$ pažymėkime raide d, o formulę $\Diamond\Box A \to \Box A$ – skaičiumi 5. Modalumo logikos **D** skaičiavimą sudaro 1.1–4.3, k, d aksiomos, o logikos **S5** – 1.1–4.3, k, t, 4, 5 aksiomos. Taisyklės MP, AT yra vienintelės logikų D, S5 taisyklės.

Modalumo logikos, tarp kurių aksiomų yra k, vadinamos *normaliosiomis*, priešingu atveju – *pusiau normaliomis.*

Kai kuriose aksiomose yra tam tikrų pasaulių sąryšio apribojimų. Aprašysime juos lentele:

Aksioma	Savybė
t	$\forall x R(x, x)$
4	$\forall x \forall y \forall z((R(x, y) \& R(y, z)) \to R(x, z))$
d	$\forall x \exists y R(x, y)$
5	$\forall x \forall y \forall z((R(x, y) \& R(x, z)) \to R(y, z))$

Iš čia išplaukia, kad formulė tapačiai teisinga, pavyzdžiui, logikoje S4, tada ir tiktai tada, kai ji teisinga kiekvienos struktūros, kurios sąryšis *refleksyvus* ir *tranzityvus*, bet kuriame pasaulyje.

7.1 lema. *Jei $F(p_1, \dots, p_n)$ tapačiai teisinga klasikinės teiginių logikos formulė ir $G_1, \dots, G_n$ yra bet kurios modalumo logikų formulės, tai $F(G_1, \dots, G_n)$ išvedama kiekvienos modalumo logikos skaičiavime.*

Įrodymas. Kadangi $F(p_1, \dots, p_n)$ yra tapačiai teisinga formulė, tai egzistuoja tokia baigtinė klasikinės teiginių logikos formulių seka $F_1, \dots, F_s$, kad $F = F_s$ ir kiekvienas narys F_i yra viena iš 1.1–4.3 aksiomų arba gautas iš kairėje jo esančių formulių F_k, F_m $(k, m < i)$ pagal *modus ponens* taisyklę. Visose išvedime naudojamose formulėse loginius kintamuosius p_i $(i = 1, \dots, n)$ pakeiskime formulėmis G_i. Gauname modalumo logikų formulės $F(G_1, \dots, G_n)$ išvedimą, kuriame pasinaudota tik 1.1–4.3 aksiomomis ir taisykle MP. Kadangi šios aksiomos ir taisyklė priklauso visoms nagrinėjamoms modalumo logikoms, tai kartu gavome ir išvedimą modalumo logikose. Lema įrodyta.

Pavyzdys. Formulės $A \to \Diamond A$ išvedimas modalumo logikos T skaičiavime:

$\Box\neg A \to \neg A$ (aksioma t),
$(\Box\neg A \to \neg A) \to (\neg\neg A \to \neg\Box\neg A)$ (4.1 aksioma),
$\neg\neg A \to \neg\Box\neg A$ (pagal taisyklę MP),
$A \to \neg\neg A$ (4.2 aksioma),
$A \to \neg\Box\neg A$ (naudojantis implikacijos tranzityvumu ir 7.1 lema),
$A \to \Diamond A$ (pagal $\Diamond$ apibrėžimą, t.y. $\Diamond = \neg\Box\neg$).

Sekvenciniai skaičiavimai. Aprašysime sekvencinius modalumo logikų K, T, S4 skaičiavimų variantus.

Aksiomos: $F, \Pi \vdash F, \Delta$.

Taisyklės $(\to\vdash)$, $(\vdash\to)$, $(\&\vdash)$, $(\vdash\&)$, $(\vee\vdash)$, $(\vdash\vee)$, $(\neg\vdash)$, $(\vdash\neg)$ visoms modalumo logikoms tos pačios kaip ir sekvencinio skaičiavimo G. Tik į formulių sąrašus antecedente bei sukcedente žiūrime kaip į multiaibes.

Modalumo logikoms K, T, S4 apibrėšime tik taisykles $(\Box\vdash)$ ir $(\vdash\Box)$.

Modalumo logika **K**:

$$(\vdash\Box)\quad \frac{\Gamma^* \vdash F}{\Sigma, \Box\Gamma \vdash \Delta, \Box F}.$$

Modalumo logika **T**:

$$(\Box\vdash)\quad \frac{F, \Box F, \Pi \vdash \Delta}{\Box F, \Pi \vdash \Delta}, \qquad (\vdash\Box)\quad \frac{\Gamma^* \vdash F}{\Sigma, \Box\Gamma \vdash \Delta, \Box F}.$$

Modalumo logika **S4**:

$$(\Box\vdash)\quad \frac{F, \Box F, \Pi \vdash \Delta}{\Box F, \Pi \vdash \Delta}, \qquad (\vdash\Box)\quad \frac{\Box\Gamma \vdash F}{\Sigma, \Box\Gamma \vdash \Delta, \Box F}.$$

Čia Π, Δ yra baigtinės formulių sekos; Σ – baigtinė seka formulių, neprasidedančių operatoriumi $\Box$; $\Box\Gamma$ – baigtinė seka formulių, prasidedančių operatoriumi $\Box$; Γ^* – gauta iš $\Box\Gamma$, išbraukus iš visų $\Box\Gamma$ formulių pirmąsias $\Box$ įeitis (formulių sekos gali būti ir tuščios); F – formulė.

Pateikiame porą išvedamų sekvencijų pavyzdžių.

Pavyzdžiai:

1. Sekvencijos $\vdash \neg\Box\neg(A \vee \Box\neg A)$ išvedimas logikos S4 sekvenciniame skaičiavime:

$$\begin{array}{c}
A, \Box\neg(A \vee \Box\neg A) \vdash A, \Box\neg A \\ \hline
A, \Box\neg(A \vee \Box\neg A) \vdash A \vee \Box\neg A \\ \hline
\neg(A \vee \Box\neg A), \Box\neg(A \vee \Box\neg A), A \vdash \\ \hline
\Box\neg(A \vee \Box\neg A), A \vdash \\ \hline
\Box\neg(A \vee \Box\neg A) \vdash \neg A \\ \hline
\Box\neg(A \vee \Box\neg A) \vdash A, \Box\neg A \\ \hline
\Box\neg(A \vee \Box\neg A) \vdash A \vee \Box\neg A \\ \hline
\neg(A \vee \Box\neg A), \Box\neg(A \vee \Box\neg A) \vdash \\ \hline
\Box\neg(A \vee \Box\neg A) \vdash \\ \hline
\vdash \neg\Box\neg(A \vee \Box\neg A)
\end{array}.$$

Logikos S4 taisyklėje ($\Box \vdash$) kartojama centrinė formulė. Jei to nebūtų, tai nagrinėjamoji sekvencija nebūtų išvedama:

$$\begin{array}{c}
A \vdash \\ \hline
\vdash \neg A \\ \hline
\vdash A, \Box\neg A \\ \hline
\vdash A \vee \Box\neg A \\ \hline
\neg(A \vee \Box\neg A) \vdash \\ \hline
\Box\neg(A \vee \Box\neg A) \vdash \\ \hline
\vdash \neg\Box\neg(A \vee \Box\neg A)
\end{array}.$$

2. Sekvencijos $\Box(p\&q) \vdash \Box p\&\Box q$ išvedimas logikos T sekvenciniame skaičiavime:

$$\dfrac{\dfrac{\dfrac{p, q \vdash p}{p\&q \vdash p}}{\Box(p\&q) \vdash \Box p} \qquad \dfrac{\dfrac{p, q \vdash q}{p\&q \vdash q}}{\Box(p\&q) \vdash \Box q}}{\Box(p\&q) \vdash \Box p\&\Box q}.$$

7.3 Ekvivalenčiosios formulės

7.9 apibrėžimas. *Formulės F, G vadinamos ekvivalenčiosiomis (žymime $F \equiv G$) modalumo logikoje* X, *jei jų reikšmės vienodos bet kurios struktūros kiekviename pasaulyje. Pasaulių sąryšiai tenkina logikos* X *sąryšių apribojimus.*

Formulių F, G ekvivalentumo įrodymas, naudojantis Hilberto tipo skaičiavimu, suvedamas į dviejų formulių $F \to G$, $G \to F$ išvedimų paiešką, o sekvenciniame skaičiavime – į sekvencijų $F \vdash G$, $G \vdash F$ išvedimų paiešką.

Modalumo logikoje S4 galioja tokie ekvivalentumai:

1. $\Diamond\Diamond p \equiv \Diamond p$,
2. $\Box\Box p \equiv \Box p$,
3. $(\Box\Diamond)^2 \equiv \Box\Diamond p$,
4. $(\Diamond\Box)^2 \equiv \Diamond\Box p$,
5. $\neg\Box p \equiv \Diamond\neg p$,
6. $(\Box p \& \Box q) \equiv \Box(p \& q)$,
7. $(\Diamond p \vee \Diamond q) \equiv \Diamond(p \vee q)$.

Bet $\Box p \vee \Box q$ ir $\Box(p \vee q)$ nėra ekvivalenčios kaip ir $\Diamond p \& \Diamond q$, $\Diamond(p \& q)$.

Nagrinėjame formules pavidalo $M_1 \ldots M_n l$; čia M_i $(i \leqslant n$ yra vienas iš modalumo operatorių $\Box$, $\Diamond$, o l – klasikinės logikos litera. Kai kurias tokio pavidalo formules galima redukuoti į ekvivalenčias, kuriose modalumo operatorių mažiau. Pavyzdžiui, formulė $\Box\Box\Box\neg p$ logikoje S4 redukuojama į $\Box\neg p$, bet neredukuojama į $\neg p$. Išvardysime visas neredukuojamas modalumo logikoje S4 formules: l, $\Box l$, $\Diamond l$, $\Box\Diamond l$, $\Diamond\Box l$, $\Box\Diamond\Box l$, $\Diamond\Box\Diamond l$.

Tarkime, A yra kurios nors formulės F poformulis. Jį žymime $F(A)$. Klasikinėje logikoje yra teisingas tvirtinimas: jei $A \equiv B$, tai ir $F(A) \equiv F(B)$. Deja, modalumo logikose jis neteisingas. Pavyzdžiui, modalumo logikoje S4 iš sąlygos $p \equiv q$ neišplaukia $\Box p \equiv \Box q$, nes tokios išvedimo paieškos medžio šakos negalima pratęsti iki aksiomų:

$$\begin{array}{c} q, p, \Box p \vdash \Box q \\ \hline \cdots \\ \hline q, q \to p, \Box p \vdash \Box q \\ \hline \cdots \\ \hline p \to q, q \to p \vdash \Box p \to \Box q \\ \hline \cdots \\ \hline (p \to q)\&(q \to p) \vdash (\Box p \to \Box q)\&(\Box q \to \Box p) \end{array}.$$

Jei formulės A, B yra tokios, kad $\Box(A \equiv B)$ išvedama logikoje S4, tai keitimas formulėje F išlaikant ekvivalentumą galimas. Teisinga tokia teorema, kurią pateikiame be įrodymo.

7.1 teorema (Mintso). *Kad ir kokia būtų formulė F ir jos poformulis A, modalumo logikoje* S4 *iš sąlygos* $\Box(A \equiv B)$ *išplaukia* $F(A) \equiv F(B)$.

Taigi keitimas poformulių ekvivalenčiais ne visada leistinas. Tarkime, formulėse tėra loginės operacijos $\neg$, &, $\vee$. Įrodyta, kad modalumo logikoje S4 formulėms galima rasti ekvivalenčias, kuriose neigimas yra tik prieš loginius kintamuosius. Tai gaunama, kai neigimas keliamas į skliaustus naudojantis žinomomis klasikinės logikos formulėmis ir $\neg\Box A \equiv \Diamond\neg A$, $\neg\Diamond A \equiv \Box\neg A$. Šiuo atveju modalumo operatoriaus $\Box$ nepakanka. Naudojami abu modalumo operatoriai. Skaičiavimus reiktų papildyti aksiomomis ar taisyklėmis modalumo operatoriui $\Diamond$. Gali skirtis ir kai kurios taisyklės, taikomos modalumo operatoriui $\Box$. Sekvencinio skaičiavimo **S4** modalumo operatorių taisyklės:

$$(\Diamond\vdash)\quad \frac{F, \Box\Gamma \vdash \Diamond\Lambda}{\Diamond F, \Box\Gamma, \Sigma \vdash \Delta, \Diamond\Lambda}, \qquad (\vdash\Diamond)\quad \frac{\Pi \vdash \Delta, F, \Diamond F}{\Pi \vdash \Delta, \Diamond F},$$

$$(\Box\vdash)\quad \frac{F, \Box F, \Pi \vdash \Delta}{\Box F, \Pi \vdash \Delta}, \qquad (\vdash\Box)\quad \frac{\Box\Gamma \vdash F, \Diamond\Lambda}{\Sigma, \Box\Gamma \vdash \Omega, \Box F, \Diamond\Lambda}.$$

Čia $\Diamond\Lambda$ žymi baigtinę seką formulių, prasidedančių operatoriumi $\Diamond$; Ω – baigtinę seką formulių, neprasidedančių operatoriumi $\Diamond$; kitos raidės – tuos pačius reiškinius kaip ir anksčiau aprašytame sekvenciniame skaičiavime.

7.10 apibrėžimas. *Modalumo litera vadiname klasikinės logikos literas bei formules pavidalo* $\Box l$, $\Diamond l$; *čia* l – *klasikinės logikos litera.*

7.11 apibrėžimas. *Modalumo disjunktu vadiname modalumo literų disjunkciją.*

7.2 teorema. *Kad ir kokia būtų formulė F, egzistuoja tokie modalumo disjunktai* $D_1, \ldots, D_n$ *ir klasikinės logikos litera l, kad* $\vdash F$ *įrodoma modalumo logikos* S4 *sekvenciniame skaičiavime tada ir tiktai tada, kai įrodoma* $\Box D_1, \ldots, \Box D_n, l \vdash$.

Įrodymas. Aprašysime tik transformavimo algoritmą. Poformulius $\neg p$, $p \vee q$, $p\&q$, $\Box p$, $\Diamond p$ (p, q yra loginiai kintamieji) tolydžio pakeisime naujais loginiais kintamaisiais. Antecedentą papildysime formulėmis $\Box(r \leftrightarrow \neg p)$, $\Box(r \leftrightarrow (p \vee q))$, $\Box(r \leftrightarrow (p\&q))$, $\Box(r \leftrightarrow \Box p)$, $\Box(r \leftrightarrow \Diamond p)$. Jas savo ruožtu redukuosime į seką formulių $\Box D$ (D – modalumo disjunktas):

$\Box(r \leftrightarrow \neg p)$: $\Box(r \to \neg p), \Box(\neg p \to r)$: $\Box(\neg r \vee \neg p), \Box(p \vee r)$,

$\Box(r \leftrightarrow (p \vee q))$: $\Box(r \to (p \vee q)), \Box((p \vee q) \to r)$: $\Box(\neg r \vee p \vee q)$, $\Box(\neg p \vee r), \Box(\neg q \vee r)$,

$\Box(r \leftrightarrow (p\&q))$: $\Box(r \to (p\&q)), \Box((p\&q) \to r)$: $\Box(\neg r \vee p), \Box(\neg r \vee q)$, $\Box(\neg p \vee \neg q \vee r)$,

$\Box(r \leftrightarrow \Box p)$: $\Box(r \rightarrow \Box p), \Box(\Box p \rightarrow r)$: $\Box(\neg r \vee \Box p), \Box(r \vee \Diamond\neg p)$,

$\Box(r \leftrightarrow \Diamond p)$: $\Box(r \rightarrow \Diamond p), \Box(\Diamond p \rightarrow r)$: $\Box(\neg r \vee \Diamond p), \Box(r \vee \Box\neg p)$.

Panašiai aprašomos redukcijos ir kitų loginių operacijų. Taip žingsnis po žingsnio redukuojant formulę, sukcedente liks tik kuris nors, tarkime, v, loginis kintamasis. Parašę antecedente $l = \neg v$, gauname sekvenciją $\Box D_1, \ldots, \Box D_n, l \vdash$. Ji išvedama skaičiavime S4 tada ir tiktai tada (įrodymas priklauso Mintsui), kai išvedama $\vdash F$. Teorema įrodyta.

Pavyzdys. Redukuokime formulę $\neg\Box(p\&q) \vee q$. Tuo tikslu $p\&q$ pažymime nauju kintamuoju r. Gauname, kad $\vdash \neg\Box(p\&q) \vee q$ išvedamas skaičiavime S4 tada ir tiktai tada, kai išvedama

$$\Box(\neg r \vee p), \Box(\neg r \vee q), \Box(\neg p \vee \neg q \vee r) \vdash \neg\Box r \vee q.$$

Pažymėkime $\Box r$ raide v. Tuomet pastaroji sekvencija išvedama tada ir tiktai tada, kai išvedama

$$\Box(\neg r \vee p), \Box(\neg r \vee q), \Box(\neg p \vee \neg q \vee r), \Box(\neg v \vee \Box r), \Box(v \vee \Diamond\neg r) \vdash \neg v \vee q.$$

Pažymime $\neg v$ kintamuoju w. Tada

$$\Box(\neg r \vee p), \Box(\neg r \vee q), \Box(\neg p \vee \neg q \vee r), \Box(\neg v \vee \Box r), \Box(v \vee \Diamond\neg r),$$
$$\Box(\neg w \vee \neg v), \Box(w \vee v) \vdash w \vee q.$$

Pažymime $w \vee q$ kintamuoju u. Tuomet gauname, kad $\vdash \neg\Box(p\&q) \vee q$ išvedama skaičiavime S4 tada ir tiktai tada, kai jame išvedama sekvencija

$$\Box(\neg r \vee p), \Box(\neg r \vee q), \Box(\neg p \vee \neg q \vee r), \Box(\neg v \vee \Box r), \Box(v \vee \Diamond\neg r),$$
$$\Box(\neg w \vee \neg v), \Box(w \vee v), \Box(\neg u \vee w \vee q), \Box(\neg w \vee u), \Box(\neg q \vee u), \neg u \vdash .$$

7.12 apibrėžimas. *Tarkime, formulėje F yra tik loginės operacijos* $\neg$, $\&$, $\vee$. *Sakome, kad poformulio G įeitis formulėje F yra teigiama, jei ji patenka į 2n neigimo įeičių veikimo sritį* ($n = 0, 1, 2, \ldots$). *Priešingu atveju įeitis neigiama.*

Teigiamas ir neigiamas įeičių sąvokas galima apibrėžti ir taip:

a) formulės F įeitis formulėje F yra teigiama,

b) jei $G = \neg H$ ir G įeitis teigiama (neigiama), tai H įeitis neigiama (teigiama),

c) jei $G = H \vee K$ arba $G = H\&K$ ir G įeitis teigiama (neigiama), tai ir H, K įeitys teigiamos (neigiamos).

Atkreipiame dėmesį, kad formulėse, kuriose yra tik loginės operacijos $\neg$, $\&$, $\vee$ ir neigimas gali būti tik prieš loginius kintamuosius, visų poformulių, išskyrus kai kurių loginių kintamųjų, įeitys yra teigiamos. Tuo atveju, kai visų poformulių, išskyrus loginių kintamųjų, įeitys teigiamos, formulės redukuojamos naudojantis paprastesnėmis taisyklėmis:

$\Box(r \leftrightarrow \neg p)$: $\Box(p \vee r)$,

$\Box(r \leftrightarrow (p \vee q))$: $\Box(\neg p \vee r), \Box(\neg q \vee r)$,

$\Box(r \leftrightarrow (p\&q))$: $\Box(\neg p \vee \neg q \vee r)$,

$\Box r \leftrightarrow \Box p)$: $\Box(r \vee \Diamond\neg p)$,

$\Box(r \leftrightarrow \Diamond p)$: $\Box(r \vee \Box\neg p)$.

Kad ir kokia būtų formulė, galima rasti jai ekvivalenčią, kurioje yra tik loginės operacijos $\neg$, $\&$, $\vee$ ir neigimas gali būti tik prieš loginius kintamuosius. Todėl pakanka paprastesnių redukcijos taisyklių.

7.4 Rezoliucijų metodas modalumo logikai S4

Pirmasis rezoliucijų metodą modalumo logikai 1985 m. aprašė prancūzų logikas L. Fariñas. Vėliau buvo pateikta dar keletas skirtingų metodo variantų. Šiame skyrelyje vieną jų aprašysime logikai S4.

Nagrinėkime formulių aibę $S = \{F_1, \ldots, F_n\}$, kurios elementai yra modalumo disjunktai bei formulės pavidalo $\Box D$ (D – modalumo disjunktai). Nustatysime, ar aibė S prieštaringa logikoje S4. Tuščią disjunktą žymime $\perp$. Tvarka disjunktuose nėra fiksuota, t.y. $F \vee G = G \vee F$. Iš praeitame skyrelyje aprašytų rezultatų išplaukia, kad bet kuriai formulei galima rasti tokią nagrinėjamojo pavidalo aibę, kad formulė tapačiai teisinga tada ir tiktai tada, kai ją atitinkanti aibė yra prieštaringa.

Pateikiame apibendrintos formulės apibrėžimą.

7.13 apibrėžimas:

1. *Jei F, G yra formulės, tai* $\mathrm{res}(F,G)$ *– apibendrintoji formulė.*

2. *Jei F yra apibendrintoji formulė, tai $\Box F$, $\Diamond F$ – taip pat apibendrintosios formulės.*

3. *Jei F yra formulė, G – apibendrintoji formulė, tai $(F \vee G)$, $(F\&G)$ taip pat yra apibendrintosios formulės.*

Taigi formulėse negali būti res, o apibendrintose formulėse yra tik viena res įeitis.

Įvedimo taisyklė taikoma tik formulėms

$$\text{(r)} \quad \frac{F,\ G}{\operatorname{res}(F, G)}.$$

Klasikinės taisyklės:

$$\text{(c1)} \quad \frac{\operatorname{res}(l \vee F, \neg l \vee H)}{F \vee H}, \qquad \text{(c2)} \quad \frac{\operatorname{res}(F \vee G, H)}{\operatorname{res}(F, H) \vee G}.$$

Čia raide l žymime klasikinės logikos literą. Visur nagrinėjamose formulėse $\neg\neg F = F$. Formulės F, H taisyklėje (c1) gali būti ir tuščios, t.y. $F \vee H = \perp$.

Modalumo taisyklės:

$$\text{(m1)} \quad \frac{\operatorname{res}(\Box F, \Box G)}{\Box\operatorname{res}(F, G)}, \qquad \text{(m2)} \quad \frac{\operatorname{res}(\Box F, \Diamond G)}{\Diamond\operatorname{res}(F, G)}, \qquad \text{(m3)} \quad \frac{\operatorname{res}(\Box F, G)}{\operatorname{res}(F, G)}.$$

Prastinimo taisyklė yra

$$\frac{F}{G};$$

čia G gauta iš F, pakeitus joje:

a) visas $\Box \perp$ įeitis simboliu $\perp$,

b) visas $\Diamond \perp$ įeitis simboliu $\perp$,

c) visas $H \vee \perp$ įeitis formule H,

d) visas $\Box\Box H$ įeitis formule $\Box H$,

e) visas $\Diamond\Diamond H$ įeitis formule $\Diamond H$.

Faktorizavimo taisyklė yra

$$\frac{F}{G};$$

čia G gauta iš F, pakeitus joje visas poformules $H \vee H \vee D$ formulėmis $H \vee D$.

7.14 apibrėžimas. *Formulės (apibendrintosios formulės) F išvedimu iš formulių aibės S vadiname baigtinę seką $G_1, \ldots, G_n$, tenkinančią sąlygas*:

1) $G_n = F$,

2) G_i $(i = 1, \ldots, n)$ *yra formulė arba apibendrintoji formulė*,

3) *kiekviena* G_i *priklauso aibei S arba tenkina vieną iš sąlygų*:

   a) $G_i = \text{res}(G_j, G_k)$ $(j, k < i)$ *ir* G_j, G_k *yra formulės*,

   b) *egzistuoja sekoje apibendrintoji formulė* G_j $(j < i)$, *kurioje yra* $\text{res}(H, K)$ *ir* G_i *gauta iš* G_j *pagal kurią nors taisyklę* (c1), (c2), (m1), (m2), (m3), *t.y.* $\text{res}(H, K)$ *pakeista atitinkamos taisyklės išvada*,

   c) G_i *gauta iš* G_j *pagal prastinimo ar faktorizavimo taisyklę*.

Pavyzdys. Raskime tuščio disjunkto išvedimą iš aibės $S = \{\Box(\neg p \vee \Diamond q), \Box(p \vee r), \Box\neg q, \Diamond\neg r\}$. Laužtiniuose skliaustuose nurodome taisyklę, kuria remiantis gauta formulė (apibendrintoji formulė). Simboliu [S] žymime faktą, kad nagrinėjamoji formulė priklauso pradinei aibei.

$\Box(\neg p \vee \Diamond q)$ [S], $\Box(p \vee r)$ [S], $\text{res}(\Box(\neg p \vee \Diamond q), \Box(p \vee r))$ [r], $\Box(\text{res}(\neg p \vee \Diamond q, p \vee r))$ [m1], $\Box(\Diamond q \vee r)$ [c1], $\Diamond\neg r$ [S], $\text{res}(\Box(\Diamond q \vee r), \Diamond\neg r))$ [r], $\Diamond\text{res}(\Diamond q \vee r, \neg r)$ [m2], $\Diamond\Diamond q$ [c1], $\Diamond q$ [prast.], $\Box\neg q$ [S], $\text{res}(\Diamond q, \Box\neg q)$ [r], $\Diamond\text{res}(q, \neg q)$ [m2], $\Diamond \perp$ [c1], $\perp$ [prast.].

7.5 Kvantorinė modalumo logika S4

Net tą pačią modalumo logiką, pavyzdžiui, S4, atitinka skirtingos kvantorinės modalumo logikos. Jos skirstomos pagal individinių konstantų aibių, termų žymėjimų bei konstantų egzistavimo reikalavimus.

Individinių konstantų aibė. Ar ji viena ir ta pati visuose pasauliuose? Jei taip, tai sakoma, kad *individinių konstantų aibė pastovi*. Jei ne, tai sakoma, nagrinėjama *kintanti individinių konstantų aibė*. Iš logikų su kintančiomis individinių konstantų aibėmis išskiriama logika su *monotonine individinių konstantų aibe*. Taip vadinamos logikos, tenkinančios sąlygą: jei iš pasaulio v galima patekti į pasaulį w (tiksliau, $R(v, w) = t$, R – pasaulių sąryšis), tai pasaulio v individinių konstantų aibė yra w individinių konstantų poaibis.

Termų žymėjimai. Jei bet kuris simbolis apibrėžiamas vienodai visuose gretimuose pasauliuose v, w, t.y. $R(v, w) = t$, tai logika vadinama *fiksuotąja*, priešingu atveju – *nefiksuotąja*.

Objektų (konstantų) egzistavimas. Jei nesvarbu, koks yra pasaulis w, nagrinėjamosios logikos kalbos n-vietis funkcinis simbolis f ir pasaulio w individinių konstantų aibės elementai $a_1, \ldots, a_n$, $f(a_1, \ldots, a_n)$ taip pat priklauso pasaulio w individinių konstantų aibei, tai logika vadinama *lokaliąja*, priešingu atveju – *nelokaliąja*.

Šiame skyrelyje nagrinėsime tik kvantorinę modalumo logiką S4, gautą iš klasikinės predikatų logikos, papildžius ją atitinkamomis modalumo operatorių aksiomomis bei taisyklėmis. Pavyzdžiui, sekvencinis kvantorinės modalumo logikos S4 skaičiavimas susideda iš klasikinės logikos sekvencinio skaičiavimo G, aprašyto 6.3 skyrelyje, ir modalumo operatorių taisyklių, aprašytų 7.3 skyrelyje. Pateikiame porą išvedamų sekvencijų pavyzdžių.

Pavyzdžiai:

1. Sekvencija $\vdash \Box\forall x A(x) \rightarrow \forall x \Box A(x)$ išvedama taip:

$$\begin{array}{c}
A(a), \forall x A(x), \Box\forall x A(x) \vdash A(a) \\ \hline
\forall x A(x), \Box\forall x A(x) \vdash A(a) \\ \hline
\Box\forall x A(x) \vdash A(a) \\ \hline
\Box\forall x A(x) \vdash \Box A(a) \\ \hline
\Box\forall x A(x) \vdash \forall x \Box A(x) \\ \hline
\vdash \Box\forall x A(x) \rightarrow \forall x \Box A(x)
\end{array}.$$

2. Sekvencijos $\Box\forall x A(x) \& \Box\forall x B(x) \vdash \Box\forall x (A(x) \& B(x))$ išvedimas yra toks:

$$\begin{array}{c}
A(a), \forall x A(x), \Box\forall x A(x), B(a), \forall x B(x), \Box\forall x B(x) \vdash A(a) \qquad M \\ \hline
A(a), \forall x A(x), \Box\forall x A(x), B(a), \forall x B(x), \Box\forall x B(x) \vdash A(a) \& B(a) \\ \hline
A(a), \forall x A(x), \Box\forall x A(x), \forall x B(x), \Box\forall x B(x) \vdash A(a) \& B(a) \\ \hline
A(a), \forall x A(x), \Box\forall x A(x), \Box\forall x B(x) \vdash A(a) \& B(a) \\ \hline
\forall x A(x), \Box\forall x A(x), \Box\forall x B(x) \vdash A(a) \& B(a) \\ \hline
\Box\forall x A(x), \Box\forall x B(x) \vdash A(a) \& B(a) \\ \hline
\Box\forall x A(x), \Box\forall x B(x) \vdash \forall x (A(x) \& B(x)) \\ \hline
\Box\forall x A(x), \Box\forall x B(x) \vdash \Box\forall x (A(x) \& B(x)) \\ \hline
\Box\forall x A(x) \& \Box\forall x B(x) \vdash \Box\forall x (A(x) \& B(x))
\end{array}.$$

Čia M yra sekvencija $A(a), \forall x A(x), \Box\forall x A(x), B(a), \forall x B(x), \Box\forall x B(x) \vdash B(a)$.

Logika, kurioje įrodoma $\Box\forall x A(x) \rightarrow \forall x \Box A(x)$, yra monotoninė. Jei logikoje įrodoma $\forall x A(x) \rightarrow A(t)$, t – bet kuris pagrindinis nagrinėjamoje kalboje termas, tai logika yra fiksuota ir lokali. Taigi, papildę klasikinį skaičiavimą G modalumo operatorių taisyklėmis, gauname monotoninę, fiksuotą ir lokalią logiką. Atkreipiame dėmesį, kad tokiame skaičiavime sekvencija $\forall x \Box A(x) \vdash \Box\forall x A(x)$ neišvedama. Formulė $\forall x \Box A(x) \rightarrow \Box\forall x A(x)$ vadinama *Barcano formule*.

Aprašysime sekvencinį kvantorinės modalumo logikos skaičiavimą, kai nagrinėjamose formulėse yra tik loginės operacijos $\neg$, $\&$, $\vee$ ir neiginys gali būti tik prieš atomines formules. Tokias formules vadiname *teigiamosiomis*. Kaip ir anksčiau, formulių antecedente bei sukcedente tvarka nėra fiksuota. Pavyzdžiui, sekvencijoje $\Gamma, F \vdash \Delta$ išskirtoji formulė yra kuri nors F iš antecedento, bet nebūtinai paskutinė. Aprašysime skaičiavimą, kuriame $G \vdash$ išvedama tada ir tiktai tada, kai G yra tapačiai klaidinga.

Aksiomos: $\Gamma, F, \neg F \vdash$.

Taisyklės:

$$(\&)\quad \frac{\Gamma, F, G \vdash}{\Gamma, F\&G \vdash}, \qquad (\vee)\quad \frac{\Gamma, F \vdash \quad \Gamma, G \vdash}{\Gamma, F \vee G \vdash},$$

$$(\Box)\quad \frac{\Gamma, F, \Box F \vdash}{\Gamma, \Box F \vdash}, \qquad (\Diamond)\quad \frac{\Gamma^*, F \vdash}{\Gamma, \Diamond F \vdash},$$

$$(\forall)\quad \frac{\Gamma, F(t), \forall x F(x) \vdash}{\Gamma, \forall x F(x) \vdash}, \qquad (\exists)\quad \frac{\Gamma, F(a) \vdash}{\Gamma, \exists x F(x) \vdash}.$$

Sąrašas Γ^* susideda iš visų Γ formulių, prasidedančių operatoriumi $\Box$, t – kuris nors termas laisvas kintamojo x atžvilgiu formulėje F, a – naujas laisvasis kintamasis, neįeinantis į apatinę sekvenciją.

Dar 1962 m. S. Kripke įrodė, kad logikų K, T, D, S4, S5 klasė formulių, kuriose yra tik du skirtingi vienviečiai predikatiniai kintamieji, neišsprendžiama. Rusų logikas V.P. Orevkov 1967 m. įrodė neišsprendžiamumą klasės logikos S5 formulių, kuriose yra tik vienas vienintelis predikatinis kintamasis.

Kaip ir klasikinėje logikoje, egzistavimo kvantorius galima eliminuoti įvedus funkcinius simbolius. Pateikiame italų logikės M. Cialdea Mayer aprašytą skulemizavimą. Jis logikų K, D, T, S4 formulėms vienodas. Nagrinėkime tik teigiamas formules, kuriose taikant klasikinės logikos ekvivalentumus jau neįmanoma kvantorių iškelti į kurio nors poformulio pradžią. Pavyzdžiui, prieš skulemizuojant teigiama formulė $\forall x \Box P(x) \vee \Diamond \exists y (Q(y) \& \neg P(y))$ visų pirma turėtų būti transformuojama į $\forall x (\Box P(x) \vee \Diamond \exists y (Q(y) \& \neg P(y)))$, o paskui jau skulemizuojama. Be to, tarsime, kad formulė uždara ir nėra dviejų skirtingų kvantorinių kompleksų įeičių su vienodais kintamaisiais. Taigi, sakykime, kad *formulė F tenkina aprašytąsias sąlygas. Tuomet skulemizuotoji $Sk(F)$ gaunama* žingsnis po žingsnio taikant operatorių Skm tol, kol jį įmanoma taikyti:

$\mathrm{Sk}(F) = \mathrm{Skm}(F, 0)$,

$\mathrm{Skm}(P, n) = P$, jei P yra litera,

$\mathrm{Skm}(A\&B, n) = \mathrm{Skm}(A, n)\&\mathrm{Skm}(B, n)$,

$\mathrm{Skm}(A \vee B, n) = \mathrm{Skm}(A, n) \vee \mathrm{Skm}(B, n)$,

$\mathrm{Skm}(\Box A, n) = \Box\mathrm{Skm}(A, n+1)$,

$\mathrm{Skm}(\Diamond A, n) = \Diamond\mathrm{Skm}(A, n+1)$,

$\mathrm{Skm}(\forall x A(x), n) = \mathrm{Skm}(A(x^n), n)$,

$\mathrm{Skm}(\exists x A(x), n) = \mathrm{Skm}(A(f_x^n(y_1, \ldots, y_m)), n)$.

Čia f_x yra naujasis funkcinis simbolis, o $y_1, \ldots, y_m$ – pilnas formulės $\exists x A(x)$ laisvųjų kintamųjų sąrašas.

Pavyzdys. Skulemizuokime formulę

$$F = \forall x\Box(P(x)\&\Diamond\exists y(Q(x, y) \vee \Box\forall u P(u, y))):$$

$\mathrm{Skm}(F, 0) = \mathrm{Skm}(\forall x\Box(P(x)\&\Diamond\exists y(Q(x, y) \vee \Box\forall u P(u, y))), 0) =$
$\mathrm{Skm}(\Box(P(x^0)\&\Diamond\exists y(Q(x^0, y) \vee \Box\forall u P(u, y))), 0) =$
$\Box\mathrm{Skm}(P(x^0)\&\Diamond\exists y(Q(x^0, y) \vee \Box P(u, y)), 1) =$
$\Box(\mathrm{Skm}(P(x^0), 1)\&\mathrm{Skm}(\Diamond\exists y(Q(x^0, y) \vee \Box\forall u P(u, y)), 1)) =$
$\Box(P(x^0)\&\Diamond(\mathrm{Skm}(\exists y(Q(x^0, y) \vee \Box\forall u P(u, y)), 2))) =$
$\Box(P(x^0)\&\Diamond(\mathrm{Skm}(Q(x^0, f_y^2(x^0)) \vee \Box\forall u P(u, f_y^2(x_0))), 2)) =$
$\Box(P(x^0)\&\Diamond(\mathrm{Skm}(Q(x^0, f_y^2(x^0)), 2) \vee \mathrm{Skm}(\Box\forall u P(u, f_y^2(x^0)), 2))) =$
$\Box(P(x^0)\&\Diamond(Q(x^0, f_y^2(x^0)) \vee \Box\mathrm{Skm}(\forall u P(u, f_y^2(x^0), 3))) =$
$\Box(P(x^0)\&\Diamond(Q(x^0, f_y^2(x^0)) \vee \Box\mathrm{Skm}(P(u^3, f_y^2(x^0)), 3))) =$
$\Box P(x^0)\&\Diamond(Q(x^0, f_y^2(x^0)) \vee \Box P(u^3, f_y^2(x^0))))$.

Kaip ir klasikinėje logikoje, pagrindinės skulemizuotosios formulės gaunamos pakeitus visas kintamųjų įeitis pagrindiniais termais. Tik modalumo logikos atveju, kai kintamojo laipsnis yra i, jį leidžiama pakeisti tik termais, kuriuose bet kurio funkcinio simbolio laipsnis neviršija i. Remdamasi skulemizacija, M. Cialdea Mayer 1991 m. aprašė rezoliucijų metodą kvantorinėms logikoms D, T, S4. G. Mints 1994 m. aprašė rezoliucijų metodą neskulemizuotoms logikos S4 formulėms.

7.6 Laiko logikos

Uždaviniai, formalizuojami klasikinės logikos formulėmis, atskleidžia nagrinėjamų objektų ar reiškinių statinę būseną. Keičiantis laikui, kinta objektų vertės, todėl formalizavimui reikia kitokios logikos, kuri atsižvelgtų į laiko faktorių.

Visų pirma nagrinėkime laiko logiką, kurios modelis yra *baigtiniai orientuoti grafai.* Raide V žymime baigtinę loginių kintamųjų aibę.

7.15 apibrėžimas. *Laiko logikos Kripke struktūra vadiname ketvertą* $M = (S, I, R, L)$; *čia:* S *– kuri nors baigtinė aibė, vadinama būsenų aibe;* $I \subseteq S$ *– netuščia aibė, vadinama pradinių būsenų aibe;* $R \subseteq S \times S$ *– perėjimų sąryšio aibė;* L: $S \times 2^V$ *– loginių kintamųjų interpretacijų aibė.*

Kripke struktūra vaizduojama orientuotu baigtiniu grafu, kurio viršūnės yra būsenos, o lankai atitinka perėjimų sąryšį. Iš viršūnės s eina lankas į s', jei $(s, s') \in R$. Be to, visos viršūnės pažymėtos V poaibiais, t.y. tais V loginiais kintamaisiais, kurie nagrinėjamoje viršūnėje (būsenoje) laikomi teisingais.

Baigtinę viršūnių seką $s_0, s_1, \ldots, s_k$ vadiname keliu iš s_0 į s_k, jei $(s_i, s_{i+1}) \in R$ $(i = 0, 1, \ldots, k-1)$.

Kaip įprasta, raidėmis t, k žymime logines konstantas *tiesa* ir *melas.* Nagrinėjamoje logikoje yra keturi laiko operatoriai:

$\circ$: *kitoje (sekančioje) kelio viršūnėje,*
$\Diamond$: *kurioje nors kelio viršūnėje,*
$\Box$: *visose kelio viršūnėse,*
U: *iki tam tikros viršūnės.*

7.16 apibrėžimas (formulės):

1) *t ir k yra formulės.*

2) *Loginis kintamasis yra formulė (atominė).*

3) *Jei F yra formulė, tai $\neg F$ – taip pat formulė.*

4) *Jei F, G yra formulės, tai $(F \vee G)$, $(F \& G)$, $(F \to G)$, $(F \leftrightarrow G)$ – taip pat formulės.*

5) *Jei F yra formulė, tai $\circ F$, $\Diamond F$, $\Box F$ yra* ***pagalbinės formulės****.*

6) *Jei F, G yra formulės, tai (FUG) yra* ***pagalbinė formulė****.*

7) *Jei F yra pagalbinė formulė, tai $\forall F$, $\exists F$ yra formulės.*

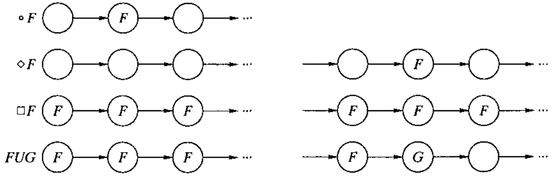
Kaip matome iš apibrėžimo, reiškiniai $\Box\Box F$, $\Diamond\Diamond F$ nėra nei formulės, nei pagalbinės formulės.

Paaiškinsime formulių semantiką. Tarkime, $M = (S, I, R, L)$ yra Kripke struktūra virš loginių kintamųjų aibės, V ir G – struktūrą atitinkantis orientuotas grafas, s – kuri nors viršūnė, $\pi = s_0, s_1, \ldots$ – kuris nors grafo kelias, F –

formulė, Π – pagalbinė formulė. Paaiškinsime, kaip suprantamas tvirtinimas, kad *F yra teisinga struktūros M būsenoje s* (žymime $M, s \models F$) ir Π *yra teisinga kelyje* π (žymime $M, \pi \models \Pi$). Taikysime indukciją pagal F, Π pavidalus.

1. $M, s \models p$, jei loginis kintamasis p teisingas struktūroje M.
2. $M, s \models G \vee H$, jei $M, s \models G$ arba $M, s \models H$. Panašiai apibrėžiama, kai $F = \neg G$, $F = G \& H$, $F = G \to H$, $F = G \leftrightarrow H$.
3. $M, s \models \forall G$, jei visuose keliuose π, prasidedančiouse viršūne s, galioja $M, \pi \models G$.
4. $M, s \models \exists G$, jei kai kuriuose keliuose π, prasidedančiuose viršūne s, galioja $M, \pi \models G$.
5. $M, \pi \models \circ G$, jei $M, s_1 \models G$.
6. $M, \pi \models \Diamond G$, jei egzistuoja toks $i \geqslant 0$, kad $M, s_i \models G$.
7. $M, \pi \models \Box G$, jei su visais $i \geqslant 0$ $M, s_i \models G$.
8. $M, \pi \models G U H$, jei egzistuoja toks $i \geqslant 0$, kad $M, s_i \models H$, ir su visais $j < i$ $M, s_j \models G$.

Taigi kvantoriais $\forall$, $\exists$ nusakome tam tikras kelių savybes, o laiko operatoriais $\circ$, $\Box$, $\Diamond$, U – viršūnių savybes. Laiko operatorių semantiką galima paaiškinti tokiomis schemomis:



7.17 apibrėžimas. *Sakome, kad formulė F teisinga Kripke struktūroje M (žymime $M \models F$), jei, esant bet kuriai pradinei būsenai $s \in I$, $M, s \models F$.*

7.18 apibrėžimas. *Sakome, kad formulės F, G ekvivalenčios, jei bet kurioje Kripke struktūroje $M \models F$ tada ir tiktai tada, kai $M \models G$.*

Kaip matome, teisingumo apibrėžime figūruoja pradinės būsenos. Teisinga tokia lema.

7.2 lema. *Tarkime, F yra kuri nors formulė ir Kripke strutūroje M yra tik viena pradinė būsena s. Tuomet $M \models F$ tada ir tiktai tada, kai $M, s \models F$.*

Nagrinėkime dar vieną laiko logiką – ***tiesinę laiko logiką***. Jos abėcėlėje yra *paskesniojo nario* operatorius $\circ$. Skaitome: *kitu laiko momentu*. Operatorius $\Diamond$, $\Box$, kaip ir $\circ$, vadiname *laiko operatoriais* ir skaitome: *visada* ($\Box$), *kai kada* ($\Diamond$). Nors tikslesnė jų semantika būtų: *pradedant nuo dabar, visada ateityje* ($\Box$) ir *pradedant nuo dabar, kartais ateityje* ($\Diamond$). Tiesinės laiko logikos modelis yra natūraliųjų skaičių aibė. Formulės apibrėžimas gaunamas iš 7.1 (teiginių modalumo logikos formulės) apibrėžimo, pakeitus 2 punktą tokiu:

2. *Jei F yra formulė, tai $\neg F$, $\Box F$, $\Diamond F$, $\circ F$ – taip pat formulės.*

Pateiksime keletą tiesinės laiko logikos skaičiavimų, kurių formulėse nėra operatoriaus $\Diamond$, ir vieną – su laiko operatoriumi U. Kaip ir anksčiau, laikysime $\Diamond F \equiv \neg\Box\neg F$.

Hilberto tipo skaičiavimas. *Aksiomos*:

1.1. $A \to (B \to A)$,

...

4.3. $\neg\neg A \to A$,

5.1. $\Box A \to (A \& \circ \Box A)$,

5.2. $(A \& \circ \Box A) \to \Box A$,

5.3. $\circ(A \to B) \to (\circ A \to \circ B)$,

5.4. $\Box(A \to B) \to (\Box A \to \Box B)$,

5.5. $\neg \circ A \to \circ\neg A$,

5.6. $\circ\neg A \to \neg \circ A$.

Taisyklės:

$$\frac{A, \quad A \to B}{B}, \qquad \frac{A}{\Box A}, \qquad \frac{A}{\circ A}.$$

Sekvencinis skaičiavimas gaunamas papildžius klasikinį sekvencinį skaičiavimą struktūrinėmis taisyklėmis ir tokiomis:

$$(\circ)\quad \frac{\Gamma \vdash \Delta}{\Sigma, \circ\Gamma \vdash \circ\Delta, \Pi}, \qquad (\circ\Box)\quad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash \circ\Box A, \Delta}{\Gamma \vdash \Box A, \Delta}.$$

Nė viena iš formulių, įeinančių į Σ, Π, neprasideda operatoriumi $\circ$.

$$(\Box\vdash)\quad \frac{A, \circ\Box A, \Gamma\vdash\Delta}{\Box A, \Gamma\vdash\Delta}, \qquad \frac{\Box\Gamma\vdash A}{\Sigma, \Box\Gamma\vdash\Box A, \Pi}.$$

Nė viena iš formulių, įeinančių į Σ, Π, neprasideda operatoriumi $\Box$.

Yra ir kitokių tiesinės laiko logikos variantų.

Tiesinė laiko logika su indukcijos aksioma. Prie aprašytojo Hilberto tipo skaičiavimo pridedama aksioma

5.7. $(A\&\Box(A\to\circ A))\to\Box A$.

Ją atitinkanti taisyklė sekvenciniame skaičiavime yra

$$(\vdash\Box)\quad \frac{\Gamma\vdash\Delta, B \quad B\to\circ B, \quad B\to A}{\Gamma\vdash\Delta, \Box A}.$$

Be jos, išlieka dvi (iš keturių) taisyklės, charakterizuojančios laiko operatorius – $(\circ)$ ir $(\Box\vdash)$.

Tiesinės laiko logikos Hilberto tipo skaičiavimas PLTL su laiko operatoriumi U.

Aksiomos:

1.1–4.3,

5.1. $\Box(A\to B)\to(\Box A\to\Box B)$,

5.2. $\circ\neg A\to\neg\circ A$,

5.3. $\neg\circ A\to\circ\neg A$,

5.4. $\circ(A\to B)\to(\circ A\to\circ B)$,

5.5. $\Box A\to(A\&\circ\Box A)$,

5.6. $\Box(A\to\circ A)\to(A\to\Box A)$,

5.7. $(AUB)\to\Diamond B$,

5.8. $(AUB)\to(B\vee(A\&\circ(AUB)))$,

5.9. $(B\vee(A\&\circ(AUB)))\to(AUB)$.

Taisyklės:

$$\frac{A, \quad A\to B}{B}, \qquad \frac{A}{\Box A}.$$

D. Gabbay 1980 m. įrodė skaičiavimo PLTL pilnumą ir korektiškumą.

7.7 Pratimai

1. Pasaulių aibė yra N_+. Pasaulių sąryšis $R(x, y)$: $R(n, n+2)$, $R(n, n+3)$, $R(n, n+5)$ teisingas su visais n, p pasaulyje α tada ir tiktai tada, kai α yra lyginis skaičius, q – kai α nelyginis skaičius, r – α yra pirminis skaičius. Ar įvykdomos formulės:

   a) $\Box r$, b) $\Box\Diamond q$, c) $\Box(p\vee(q\vee\Box r))$, d) $\Box\Diamond p \to \Diamond\Box p$?

2. Pasaulių aibė yra *visų tiesių plokštumoje aibė*, pasaulių sąryšis $R(x, y)$ teisingas tada ir tiktai tada, kai x ir y statmenos arba lygiagrečios skirtingos tiesės, p teisingas pasaulyje α, jei α kerta Ox ašį. Ar įvykdomos formulės:

   a) $\Box\Diamond p$, b) $\Box\Box p \vee \Diamond\Diamond p$?

3. Raskite sekvencijų išvedimus modalumo logikoje S4:

   a) $\Box(p \vee q) \vdash \Diamond(p \vee q)$, b) $\Diamond(p \vee q) \vdash \Diamond p \vee \Diamond q$,

   c) $\Diamond p \vee \Diamond q \vdash \Diamond(p \vee q)$.

4. Ar išvedamos modalumo logikoje S4 sekvencijos:

   a) $\Box(p \vee \Box p \vee q) \vdash \Box(\Box p \vee q)$, b) $\Box\Diamond p \vdash \Diamond\Box p$?

5. Transformuokite į klasikinės logikos formulę:

   a) $\Diamond(\Box p \to \Box(\neg q \vee r))$, b) $\Box p \& \Box\Diamond(q \to r)$.

6. Redukuokite į disjunktų ir formulių aibę:

   a) $\Box(\Box p \vee \Diamond q) \& \Diamond\Box\neg q$, b) $\Box(\Box p \& (\Box q \vee (\Box r \vee \neg p)))$.

7. Išveskite tuščią disjunktą iš aibės:

   a) $S = \{\Box\Diamond\neg w, \Box\neg r, \Box(\neg q \vee r \vee \Box w), \Box(p \vee \Diamond q), \neg p\}$,

   b) $S = \{\Box(\neg p_4 \vee \neg p_2), \Box(\neg p_3 \vee \Diamond p_4), \Box(\neg p_2 \vee \Box p_3), \Box(p_1 \vee \Box p_2), \neg p_1\}$.

8. Įrodykite, kad sekvenciniame skaičiavime $\forall x \Box A(x) \vdash \Box \forall x A(x)$ neišvedama.

9. Raskite sekvencijų išvedimus:

   a) $\exists x \Box A(x) \vee \exists x \Box B(x) \vdash \Box \exists x (A(x) \vee B(x))$,

   b) $\exists x \Box \forall y A(x, y) \vdash \forall y \exists x \neg\Box\neg A(x, y)$.

10. Skulemizuokite formules:

    a) $\forall x \Box \exists y \Diamond \forall u \Box (P(x, y) \& \neg\Box Q(y, u))$,

    b) $\Box\Diamond\forall x \Box \exists y (P(x, y) \& \Box \forall z R(x, y, z))$,

    c) $\forall x \exists y \forall u (\Box P(x) \vee \Diamond\Box Q(x, y))$.

8 skyrius

Loginės teorijos

8.1 Pirmosios eilės teorijos

Pirmosios eilės teorijos abėcėlę sudaro:

1) loginės operacijos ($\neg$, &, $\vee$, $\rightarrow$) ir kvantoriai ($\forall$, $\exists$),

2) individinių kintamųjų simboliai $x, y, z, x_1, y_1, z_1, \ldots$,

3) skliaustai (,).

Šių simbolių aibę pažymėkime raide A. Loginių operacijų sąrašas gali būti ir kitoks. Tik reikalaujama, kad jis sudarytų pilną aibę. Individinių kintamųjų simboliai gali būti žymimi ir kitaip. Pagrindinis reikalavimas – ta aibė turi būti numeruojamoji. Galime apsieiti ir su baigtine abėcėle. Tuo tikslu pakanka prie abėcėlės pridėti skaitmenis $0, 1, \ldots, 9$, o individinius kintamuosius naujojoje abėcėlėje rašyti žodžiais. Pavyzdžiui, vietoje x_5 rašyti $x5$. Aibė A yra visų pirmosios eilės teorijų abėcėlės dalis. Kiekviena konkreti teorija dar charakterizuojama elementais, būdingais tik tai teorijai. Tai konstantos, funkcijos, predikatai, t.y. teorijos abėcėlė yra $A \cup K$. Kalbėdami apie konkrečią teoriją, nurodome tik K, t.y. tą teoriją charakterizuojančias konstantas, funkcijas bei predikatus, ir vadiname tai *specifine teorijos abėcėle.*

Iš visų galimų formulių aibės išskiriama dalis, kuri vadinama *aksiomomis.* Pirmosios eilės teorijos aksiomas sudaro kurio nors (Hilberto, sekvencinio ir pan.) pirmosios eilės predikatų logikos skaičiavimo aksiomos ir *specifinės teorijos aksiomos,* būdingos tik tai konkrečiai teorijai. Be predikatų logikos taisyklių, kiekviena teorija gali turėti ir *specifines teorijos taisykles.* Nagrinėjame tik pirmosios eilės teorijas, todėl jas vadiname tiesiog teorijomis. Taigi norint apibūdinti teoriją, pakanka nurodyti specifinę abėcėlę, specifines aksiomas bei taisykles. Gauname formaliąją sistemą.

Teorija – tai visų uždarųjų išvedamų formaliojoje sistemoje formulių aibė.

Pateikiame pirmosios eilės Hilberto formaliųjų sistemų porą pavyzdžių. Joms priklauso 1.1–5.2 aksiomos ir taisyklės, aprašytos 6 skyriuje.

Dalinės tvarkos teorija. *Specifinė abėcėlė*: konstantų ir funkcinių simbolių nėra, o iš predikatų tėra vienintelis dvivietis $<$.

Specifinės aksiomos:

1) $\forall x \neg (x < x)$,

2) $\forall x \forall y \forall z ((x < y \& y < z) \rightarrow x < z)$.

Grupių teorija. *Specifinė abėcėlė*: konstanta 0, dvivietė funkcija $+$ ir dvivietis predikatas $=$.

Specifinės aksiomos:

1) $\forall x \forall y \forall z ((x + (y + z)) = ((x + y) + z))$,

2) $\forall x ((0 + x) = x)$,

3) $\forall x \exists y ((y + x) = 0)$,

4) $\forall x (x = x)$,

5) $\forall x \forall y ((x = y) \rightarrow (y = x))$,

6) $\forall x \forall y \forall z ((x = y) \rightarrow ((y = z) \rightarrow (x = z)))$,

7) $\forall x \forall y \forall z ((y = z) \rightarrow (((x + y) = (x + z)) \& ((y + x) = (z + x))))$.

Jei aksiomų sąraše yra ir $\forall x \forall y ((x + y) = (y + x))$, tai tokia grupių teorija vadinama *Abelio*.

8.1 teorema. *Jei $Q(p_1, \ldots, p_n)$ yra kuri nors tapačiai teisinga teiginių logikos formulė, $F_1, \ldots, F_n$ – kurios nors predikatų logikos formulės, tai $Q(F_1, \ldots, F_n)$ išvedama predikatų skaičiavime.*

Įrodymas. Kadangi $Q(p_1, \ldots, p_n)$ tapačiai teisinga, tai ji išvedama teiginių skaičiavime. Tame išvedime visus loginius kintamuosius $p_1, \ldots, p_n$ pakeiskime atitinkamai predikatų logikos formulėmis $F_1, \ldots, F_n$. Gauname išvedimą predikatų logikos formulės $Q(F_1, \ldots, F_n)$. Išvedime taikomos tik teiginių skaičiavimo aksiomos ir taisyklės. Jos priklauso ir predikatų skaičiavimui, todėl gauname nagrinėjamosios formulės išvedimą predikatų skaičiavime. Teorema įrodyta.

8.2 teorema. *Jei F yra uždara formulė ir teorijoje T neišvedama $\neg F$, tai, prijungę F prie teorijos T aksiomų, gauname neprieštaringą teoriją T'.*

Įrodymas. Tarkime, T' yra prieštaringa. Tada egzistuoja tokia formulė G, kad teorijoje T' išvedamos G ir $\neg G$, t.y. $\vdash_{T'} G$ ir $\vdash_{T'} \neg G$.

Remiantis 8.1 teorema, teorijoje T' išvedama formulė

$$G \to (\neg G \to \neg F).$$

Pritaikę du kartus *modus ponens* taisyklę, gauname, kad teorijoje T' išvedama formulė $\neg F$. Vadinasi,

$$F \vdash_T \neg F.$$

Kadangi formulė F uždara, tai pritaikę dedukcijos teoremą, gauname, kad teorijoje T išvedama $F \to \neg F$. Pagal 8.1 teoremą teorijoje išvedama ir $(F \to \neg F) \to \neg F$. Taigi, pritaikę *modus ponens*, gauname, kad teorijoje T išvedama $\neg F$. O tai prieštarauja teoremos sąlygai. Teorema įrodyta.

8.1 apibrėžimas. *Teorija T vadinama pilnąja, jei nesvarbu, kokia yra uždara formulė F, teorijoje T išvedama arba F, arba* $\neg F$.

8.3 teorema. *Jei teorijos T abėcėlė baigtinė ir ji neprieštaringa, tai galima ją papildyti iki pilnosios.*

Įrodymas. Teorijos abėcėlė yra baigtinė aibė, todėl uždarųjų formulių aibė yra skaičioji. Tarkime,

$$F_1, F_2, \dots \tag{8.1}$$

yra pilnas sąrašas skirtingų uždarų teorijos T formulių.

Teorijas $T_0, T_1, T_2, \dots$ konstruojame tokiu būdu:

$T_0 = T$, jei teorijoje T_i $(i = 1, 2, \dots)$ neišvedama $\neg F_{i-1}$, tai T_i gaunama iš T_{i-1} prijungus prie jos aksiomą F_i (pagal 8.2 teoremą gautoji teorija nėra prieštaringa). Priešingu atveju $T_i = T_{i-1}$ (kartu ji nėra prieštaringa).

Simboliu $\widetilde{T}$ pažymėkime teoriją $\cup_{i=0}^{\infty} T_i$. Įrodysime, kad ji neprieštaringa. Tarkime, yra tokia formulė G, kad teorijoje $\widetilde{T}$ išvedama ji bei jos neiginys. Tarkime, kad jų išvedimai yra šios sekos:

$$H_1, H_2, \dots, H_s, G, \qquad L_1, L_2, \dots, L_v, \neg G.$$

Jose gali būti ne daugiau kaip $(s + v + 1)$ (8.1) sekos narių. Tarkime, k yra toks natūralusis skaičius, kad visų aptinkamų formulių iš (8.1) indeksai nagrinėjamose sekose neviršija k. Tuomet abi formulės G ir $\neg G$ išvedamos teorijoje T_k. O tai prieštarauja teiginiui, kad visos T_i neprieštaringos. Teorema įrodyta.

Pirmosios eilės teorijose su baigtiniu predikatų ir funkcinių simbolių abėcėle galima „eliminuoti“ lygybės predikatą. Naują dvivietį predikatą pažymėkime raide A ir teorijos aksiomų sąrašą papildykime aksiomomis:

$\forall x A(x, x)$,

$\forall x \forall y (A(x, y) \to A(y, x))$,

$\forall x \forall y \forall z ((A(x, y) \& A(x, y)) \to A(x, y))$.

Kiekvieną n-vietį predikatą iš specifinės abėcėlės atitinka n naujų aksiomų:

$$\forall x_1 \ldots \forall x_n \forall y ((A(x_1, y) \& P(x_1, x_2, \ldots, x_n)) \to P(y, x_2, \ldots, x_n)),$$
$$\ldots$$
$$\forall x_1 \ldots \forall x_n \forall y ((A(x_n, y) \& P(x_1, \ldots, x_{n-1}, x_n)) \to P(x_1, \ldots, x_{n-1}, y)).$$

Kiekvieną n-vietę funkciją iš specifinės abėcėlės atitinka n naujų aksiomų:

$$\forall x_1 \ldots \forall x_n \forall y (A(x_1, y) \to A(f(x_1, x_2, \ldots, x_n), f(y, x_2, \ldots, x_n))),$$
$$\ldots$$
$$\forall x_1 \ldots \forall x_n \forall y (A(x_n, y) \to A(f(x_1, \ldots, x_{n-1}, x_n), f(x_1, \ldots, x_{n-1}, y))).$$

8.2 Formalioji aritmetika

Italų matematikas G. Peano 1891 m. suformulavo penkias aritmetikos aksiomas:

(P1) Nulis yra natūralusis skaičius.

(P2) Kad ir koks būtų natūralusis x, egzistuoja paskesnis skaičius $s(x)$.

(P3) Kad ir koks būtų natūralusis x, nulis nelygus $s(x)$.

(P4) Jei $s(x) = s(y)$, tai $x = y$.

(P5) Tarkime, Q yra savybė, kurią tenkina nulis. Be to, kad ir koks būtų natūralusis x, tenkinantis savybę Q, $s(x)$ taip pat tenkina Q. Tuomet visi natūralieji skaičiai tenkina savybę Q (indukcijos principas).

R. Dedekind 1901 m. sukūrė pusiau aksiominę aritmetikos teoriją, kurią pavadino *Peano aksiomų sistema*. Ja remiantis, vėliau buvo aprašyta formalioji aritmetika ir kai kurie jos aksiominiai variantai.

Peano aritmetika. *Specifinė abėcėlė*: konstanta 0, vienvietė funkcija s, dvivietės funkcijos $\cdot$, $+$, dviviečiai predikatai $=$, $<$.

Specifinės aksiomos:

1) $\forall x \neg (s(x) = 0)$,

2) $\forall x \forall y (s(x) = s(y) \to x = y)$,

3) $\forall x \forall y (x = y \to s(x) = s(y))$,

4) $\forall x \forall y \forall z (x = y \to (x = z \to y = z))$,

5) $\forall x \neg(x < 0)$,

6) $\forall x \forall y(x < s(y) \rightarrow (x < y \vee x = y))$,

7) $\forall x \forall y((x < y \vee x = y) \rightarrow x < s(y))$,

8) $\forall x(x + 0 = x)$,

9) $\forall x \forall y(x + s(y) = s(x + y))$,

10) $\forall x(x \cdot 0 = 0)$,

11) $\forall x \forall y(x \cdot s(y) = x \cdot y + x)$,

12) $\forall x_1 \ldots \forall x_n((F(x_1, \ldots, x_n, 0) \& \forall y(F(x_1, \ldots, x_n, y) \rightarrow$
$\rightarrow F(x_1, \ldots, x_n, s(y)))) \rightarrow \forall y F(x_1, \ldots, x_n, y))$.

Čia F yra kuri nors nagrinėjamosios teorijos formulė. Pakeitę 12) aksiomą

12) $\forall x \forall y(x < y \vee x = y \vee y < x)$,

gauname formaliąją teoriją, vadinamą ***Robinsono aritmetika***.

Iš specifinės abėcėlės išbraukus daugybą ir 10), 11) bei 12) specifines aksiomas, gaunama formalioji teorija, vadinama ***Presburgerio aritmetika***. Vokiečių matematikas M. Presburger 1929 m. įrodė, kad tokia teorija pilna ir išsprendžiama.

Sekvencinis Peano aritmetikos variantas. Nagrinėjame sekvencinį predikatų logikos skaičiavimą su lygybės predikatu. Skaičiavimui priklauso ir pjūvio taisyklė.

Specifinė abėcėlė: konstanta 0, funkcijos $\cdot$, $+$.
Specifinės aksiomos:

1) $s(t) = 0 \vdash$,

2) $s(t) = s(r) \vdash t = r$,

3) $t = r \vdash s(t) = s(r)$,

4) $\vdash t + 0 = t$,

5) $\vdash t + s(r) = s(t + r)$,

6) $\vdash t \cdot 0 = 0$,

7) $\vdash t \cdot s(r) = t \cdot r + t$.

Čia t, r yra nagrinėjamosios teorijos kurie nors termai.

Specifinė taisyklė (indukcijos schema):

$$\frac{\Gamma_1, F(x), \Gamma_2 \vdash \Delta_1, F(s(x)), \Delta_2}{\Gamma_1, F(0), \Gamma_2 \vdash \Delta_1, F(t), \Delta_2}.$$

Čia x neįeina į $F(0), \Gamma_1, \Gamma_2, \Delta_1, \Delta_2$, t – bet kuris termas, $F(x)$ – kuri nors teorijos formulė.

Pavyzdžiai:

- Išvedamos sekvencijos:

$$\cfrac{\cfrac{\cfrac{t = r, r = s \vdash r = s}{t = r, r = s \vdash t = s}}{t = r \vdash r = s \to t = s}}{\vdash t = r \to (r = s \to t = s)},$$

$$\cfrac{(\text{pjv})\cfrac{\cfrac{4\ \text{aksioma}}{\vdash 0+0=0} \quad \cfrac{0+0=0 \vdash 0=0}{0+0=0 \vdash 0=0+0}}{\vdash 0=0+0} \qquad (\text{ind})\cfrac{M}{0=0+0 \vdash t=0+t}}{\vdash t=0+t}.$$

- Medis M:

$$\cfrac{\cfrac{5\ \text{aksioma}}{\vdash 0+s(x)=s(0+x)} \quad \cfrac{\cfrac{0+s(x)=s(x), x=0+x \vdash s(x)=s(x)}{0+s(x)=s(0+x), x=0+x \vdash s(x)=s(0+x)}}{0+s(x)=s(0+x), x=0+x \vdash s(x)=0+s(x)}}{x=0+x \vdash s(x)=0+s(x)}.$$

Abejuose medžiuose visų pirma taikoma pjūvio taisyklė.

8.3 Peano aritmetikos nepilnumas

Sekvencinį Peano aritmetikos variantą vadiname PA teorija. Termus $0, s(0), s(s(0)), \ldots$ žymime $\bar{0}, \bar{1}, \bar{2}, \ldots$ ir vadinsime juos *skaitmenimis*. PA teorijos pakanka, kad įrodytume viską, kas teisinga elementariojoje aritmetikoje. Pavyzdžiui, įrodomos sekvencijos:

$$\vdash t \cdot (r + s) = (t \cdot r) + (t \cdot s),$$

$$\vdash t \cdot \bar{2} = t + t.$$

Taip pat įrodoma, kad

$$\neg(m = n) \vdash \neg(s(m) = s(n)).$$

Todėl PA teorijos modelis yra begalinis, nes skirtingus skaitmenis atitinka skirtingi modelio srities elementai.

8.2 apibrėžimas. *Funkcija, kurios apibrėžimo ir reikšmių aibės yra natūraliųjų skaičių aibė, vadinama aritmetine.*

8.3 apibrėžimas. *Funkcija, kurios apibrėžimo aibė yra natūraliųjų skaičių aibė, o reikšmių – aibė $\{t, k\}$, vadinama aritmetiniu predikatu.*

8.4 apibrėžimas. *Aritmetinis predikatas $P(x_1, \ldots, x_n)$ apibrėžiamas* PA *teorijoje, jei egzistuoja tokia teorijos formulė su n laisvųjų kintamųjų $F(x_1, \ldots, x_n)$, kad bet kuriems natūraliesiems $m_1, \ldots, m_n$, teorijoje* PA *įrodoma*:

(a) $\vdash F(\bar{m}_1, \ldots, \bar{m}_n)$, *jei* $P(m_1, \ldots, m_n) = t$,
(b) $\vdash \neg F(\bar{m}_1, \ldots, \bar{m}_n)$, *jei* $P(m_1, \ldots, m_n) = k$.

Panašiai vartojama sąvoka *aritmetinė funkcija apibrėžiama* PA *teorijoje.*
PA teorijoje apibrėžiamų predikatų pavyzdžiai:

a) „$x < y$“ apibrėžiamas formule $\exists z(\neg(z = 0)\&(x + z = y))$,
b) „*x dalijasi iš y*“ apibrėžiamas formule $\exists z(x = z \cdot y)$.

PA teorijoje įrodomos ir tokios formulės:

1) $\forall x \forall z((z < x \to F(z)) \to F(x)) \to \forall x F(x)$. Tai yra *pilnosios indukcijos principas.*

Tarkime, kad savybė F yra tokia, kad nesvarbu, koks būtų natūralusis x, iš to, kad savybę tenkina bet kuris natūralusis mažesnis už x, išplaukia, kad ją tenkina ir x. Tuomet savybę F tenkina bet kuris natūralusis skaičius.

2) $F(x) \to \exists y(F(y)\&\forall z(z < y \to \neg F(z)))$. Tai yra *mažiausiojo skaičiaus principas.*

Jei kurią nors savybę tenkina nors vienas natūralusis skaičius, tai tarp natūraliųjų skaičių, tenkinančių F, egzistuoja mažiausias.

Apskritai bet kuriame *skaičių teorijos* vadovėlyje įrodytos teoremos išvedamos ir PA teorijoje. PA teorija turi tokias svarbias savybes:

8.4 teorema. PA *teorija yra neprieštaringa.*

8.5 teorema. *Visos primityviai rekursyvios funkcijos bei predikatai apibrėžiami* PA *teorijoje.*

Kiekvienai PA abėcėlės formulei F priskirkime po natūralųjį skaičių, kurį vadiname *formulės Gödelio numeriu* (žymime $\mathrm{nm}(F)$). Iš pradžių sunumeruojame simbolius, kurie gali pasitaikyti nagrinėjamose formulėse:

$\mathrm{nm}(\neg) = 1$, $\mathrm{nm}(\&) = 2$, $\mathrm{nm}(\vee) = 3$, $\mathrm{nm}(\rightarrow) = 4$, $\mathrm{nm}(() = 5$, $\mathrm{nm}())= 6$, $\mathrm{nm}(\forall) = 7$, $\mathrm{nm}(\exists) = 8$, $\mathrm{nm}(=) = 9$, $\mathrm{nm}(0) = 10$, $\mathrm{nm}(s) = 11$, $\mathrm{nm}(+) = 12$, $\mathrm{nm}(\cdot) = 13$, $\mathrm{nm}(\vdash) = 14$, $\mathrm{nm}(x_n) = 15 + n$.

Kiekviena nagrinėjamojo pavidalo formulė yra sunumeruotos abėcėlės žodis. Žodžio $F = e_1 e_2 \ldots e_s$ numeris $\mathrm{nm}(F)$ yra $\Pi_{i=1}^{s} p_i^{\mathrm{nm}(e_i)}$; čia p_i yra i-asis pirminis skaičius. Pavyzdžiui, formulės $\exists x_1 \forall x_2 (x_1 = x_2)$ numeris yra $2^8 \cdot 3^{16} \cdot 5^7 \cdot 7^{17} \cdot 11^5 \cdot 13^{16} \cdot 17^9 \cdot 19^{17} \cdot 23^6$. Panašiai numeruojamos ir baigtinės formulių bei sekvencijų sekos. Kartu kiekvienam sekvencijos išvedimui galima priskirti po vienintelį natūralųjį skaičių.

Dėl patogumo individinius kintamuosius žymime ir kitomis raidėmis: $x, y, z, x_1, y_1, z_1, \ldots$.

Apibrėžiame predikatą $W(x, y)$ natūraliųjų skaičių aibėje: $W(x, y) = t$ tada ir tiktai tada, kai x yra kurios nors formulės $F(z)$ su vienu laisvuoju kintamuoju z *Gödelio numeris* ir y yra formulės $F(\bar{x})$ (t.y. sekvencijos $\vdash F(\bar{x})$) išvedimo PA teorijoje *Gödelio numeris* (vadinsime tiesiog numeriu).

Įrodyta, kad $W(x, y)$ yra primityviai rekursyvus predikatas. Todėl PA aritmetikoje egzistuoja apibrėžianti formulė $V(x_1, x_2)$, t.y. kad ir kokie būtų natūralieji skaičiai m_1, m_2, PA teorijoje įrodoma:

(a) $\vdash V(\bar{m}_1, \bar{m}_2)$, jei $W(m_1, m_2) = t$,

(b) $\vdash \neg V(\bar{m}_1, \bar{m}_2)$, jei $W(m_1, m_2) = k$.

Nagrinėjame formulę $\forall x_2 \neg V(x_1, x_2)$. Tarkime, m yra jos numeris. Formulė $\forall x_2 \neg V(\bar{m}, x_2)$ yra uždara. Ji tvirtina, kad $W(m, x_2)$ klaidingas su bet kuriuo natūraliuoju x_2, t.y. ji tvirtina, kad ją atitinkanti sekvencija

$$\vdash \forall x_2 \neg V(\bar{m}, x_2) \tag{8.2}$$

neįrodoma PA teorijoje.

8.6 teorema. *Jei* PA *teorija neprieštaringa, tai* (8.2) *sekvencija neįrodoma* PA *teorijoje.*

Įrodymas. Remiantis 8.4 teorema, PA teorija neprieštaringa. Tarkime, (8.2) įrodoma ir l yra kurio nors įrodymo numeris. Tuomet $W(m, l) = t$ ir todėl

$\vdash V(\bar{m},\bar{l})$ įrodoma. Bet juk taip pat įrodoma ir $\vdash \neg V(\bar{m},\bar{l})$:

$$(\text{pjv})\dfrac{\dfrac{\text{prielaida}}{\vdash \forall x_2 \neg V(\bar{m},x_2)} \qquad \dfrac{\dfrac{\text{aksioma}}{\neg V(\bar{m},\bar{l}), \forall x_2 \neg V(\bar{m},x_2) \vdash \neg V(\bar{m},\bar{l})}}{\forall x_2 \neg V(\bar{m},x_2) \vdash \neg V(\bar{m},\bar{l})}}{\vdash \neg V(\bar{m},\bar{l})}.$$

Tai reikštų, kad PA teorija prieštaringa. Taigi

$$\text{su bet kuriuo } n \qquad W(m,n) = k. \tag{8.3}$$

Teorema įrodyta.

8.5 apibrėžimas. *Teorija K vadinama ω-neprieštaringa, jei nesvarbu, kokia yra teorijos formulė $F(x)$, iš to, kad $F(\bar{n})$ įrodoma su bet kuriuo n, išplaukia, kad teorijoje K neįrodoma $\exists x \neg F(x)$.*

Taigi teorija *ω-prieštaringa*, jei yra tokia teorijos formulė $F(x)$, kad nesvarbu, koks būtų natūralusis n, teorijoje įrodoma $F(\bar{n})$, taip pat ir $\exists x \neg F(x)$.

Pastebėsime, kad teorijos neprieštaringumas išplaukia iš ω-neprieštaringumo, nes jei neįrodoma $\exists x \neg F(x)$, tai ne visos teorijos formulės įrodomos.

Standartinis PA modelis yra ω-neprieštaringas.

8.7 teorema. *Jei* PA *teorija ω-neprieštaringa, tai joje neįrodoma*

$$\vdash \neg \forall x_2 \neg V(\bar{m},x_2). \tag{8.4}$$

Įrodymas. Iš ω-neprieštaringumo išplaukia PA teorijos neprieštaringumas. Todėl pagal 8.6 teoremą (8.3) teisinga, t.y. $W(m,n) = k$ su bet kuriuo n. Iš čia išplaukia, kad PA teorijoje $\vdash \neg V(\bar{m},\bar{n})$ įrodoma su bet kuriuo n. O iš PA teorijos ω-neprieštaringumo išplaukia, kad $\vdash \exists x_2 \neg\neg V(\bar{m},x_2)$ neįrodoma, t.y. $\vdash \neg \forall x_2 \neg V(\bar{m},x_2)$. Teorema įrodyta.

Šias 8.6 ir 8.7 teoremas 1931 m. įrodė austrų matematikas *K. Gödel*. Dažniausiai jos abi vadinamos vienu vardu – *Gödelio teorema apie aritmetikos nepilnumą*.

PA teorijos nepilnumą galima įrodyti ir nesinaudojant ω-neprieštaringumu. Pakanka neprieštaringumo, t.y. silpnesnio rezultato, kad PA yra neprieštaringa. Tai 1936 m. įrodė J. B. Rosser, sukonstravęs tokią PA formulę, kad nei ji, nei jos neigimas nėra įrodomi PA teorijoje.

Prijunkime prie PA aksiomų $\neg \forall x_2 \neg V(\bar{m},x_2)$. Pagal 8.2 teoremą gausime neprieštaringą teoriją. Pažymėkime ją PA′. Teorijoje PA′ įrodoma $\vdash \exists x_2 V(\bar{m},x_2)$.

Tačiau iš (8.3) išplaukia, kad teorijoje PA$'$ įrodoma ir $\vdash \neg V(\bar{m}, \bar{n})$. Vadinasi, PA$'$ nėra prieštaringa, bet yra ω-prieštaringa.

8.8 teorema. *Visų teisingų uždarų* PA *teorijos formulių aibė nėra nei rekursyvioji, nei rekursyviai skaiti.*

Įrodymas. Tarkime, $f(x)$ yra primityviai rekursyvi funkcija, kurios reikšmių aibė $A = \{f(0), f(1), f(2), \ldots\}$ nėra rekursyvi. Taigi A yra rekursyviai skaiti, bet nėra rekursyvi. Dvivietis predikatas $y = f(x)$ primityviai rekursyvus. Todėl pagal 8.5 teoremą atsiras jį apibrėžianti PA teorijos formulė $F(x, y)$. $F(m, n) = t$ tada ir tiktai tada, kai $n = f(m)$. Be to, sekvencija $\vdash F(\bar{m}, \bar{n})$ išvedama.

Nagrinėjame formules $\exists x F(x, \bar{n})$. Jos uždaros. Pagal natūralųjį n negalime pasakyti, ar formulė teisinga, nes kartu atpažintumėme, ar $n \in A$. Tarkime, visų uždarųjų teisingų formulių aibė $G_0, G_1, G_2, \ldots$ yra rekursyviai skaiti. Tuomet *rekursyviai skaiti yra ir visų klaidingų formulių aibė* $\neg G_0, \neg G_1, \neg G_2, \ldots$.

Visų uždarųjų formulių aibė rekursyvi. Ji suskaidoma į du bendrų elementų neturinčius poaibius. Todėl abu jie nėra nei rekursyviai skaitūs, nei rekursyvūs. Teorema įrodyta.

8.4 Aksiominė aibių teorija

Bet kurios aibės A atžvilgiu prasmingas klausimas: *Ar A yra aibės A* elementas? Kai kurios aibės turi tokią savybę, o kai kurios – ne. Pavyzdžiui, *visų Vilniaus miesto troleibusų aibė* nėra troleibusas ir, aišku, ji negali būti pačios savęs elementas. Bet jei imame *aibę visų aibių*, tai ji yra pačios savęs elementas.

Tarkime, B yra *aibė visų tų aibių, kurios nėra jų pačių elementai.* Norime išsiaiškinti, ar B yra aibės B elementas.

Tarkime, B yra aibės B elementas. Tuomet B yra pačios savęs elementas ir ji negali priklausyti aibei, t.y. aibei B.

Tarkime, B nėra aibės B elementas. Tuomet B nėra pačios savęs elementas ir ji turi priklausyti aibei B.

Taigi gauname paradoksą, kurį 1903 m. aprašė anglų logikas ir filosofas B. Russel: *B yra aibės B elementas tada ir tiktai tada, kai B nėra aibės B elementas.*

Šį paradoksą galima iliustruoti tokiu pavyzdžiu.

Tarkime, vieno kaimo kirpėjas skuta barzdas tik tiems kaimo gyventojams, kurie patys nesiskuta. Klausiama, ar kirpėjas skutasi. Jei ne, tai jis yra iš tų gyventojų, kurie patys nesiskuta, ir todėl kirpėjas privalo skustis. Jei jis skutasi, tai priklauso tiems gyventojams, kurie patys skutasi, ir todėl privalo nesiskusti. Taigi *kirpėjas skutasi tada ir tiktai tada, kai jis nesiskuta.*

Pasirodžiusios XX amžiaus pradžioje antinomijos sugriovė pasitikėjimą plačiai taikoma intuityviąja aibių teorija. Reikėjo sukurti kitą, formaliąją neprieštaringą aibių teoriją. Yra keletas jos variantų, bet jie skiriasi tik tuo, kad kitaip pateikiami. Aprašysime vieną jų, kurį 1928 m. nagrinėjo von Neumann, o vėliau patikslino ir suprastino R. Robinson, P. Bernays ir K. Gödel. Tai pirmosios eilės teorija su lygybės predikatu.

Specifinė abėcėlė: dvivietis predikatas $\in$.

Individinius kintamuosius žymime $X, Y, Z, x, y, z, x_1, y_1, z_1, \ldots$. Užuot žymėję $\neg(X \in Y)$, rašome $X \notin Y$. Įvedame dar kai kurių formulių žymėjimus:

$\forall Z(Z \in X \leftrightarrow Z \in Y)$ žymime $X = Y$,
$\forall Z(Z \in X \rightarrow Z \in Y)$ žymime $X \subseteq Y$,
$X \subseteq \& X \neq Y$ žymime $X \subset Y$.

Specifinės aksiomos:

1 (ekstensionalumo, arba apimties) aksioma. $\forall X \forall Y(X = Y \rightarrow \forall Z(X \in Z \leftrightarrow Y \in Z))$.

Ne visos intuityviąja prasme aibės yra formaliosios teorijos aibės. Todėl $X, Y, Z, \ldots$ vadiname *klasėmis*. *Aibėmis* vadiname tik tuos kintamuosius X, kurie tenkina sąlygą $\exists Y(X \in Y)$. Žymime $M(X)$ arba mažosiomis raidėmis $x, y, z, x_1, y_1, z_1, \ldots$.

2 (poros) aksioma. $\forall x \forall y \exists z \forall u(u \in z \leftrightarrow (u = x \vee u = y))$.

Ja tvirtinama, kad nesvarbu, kokios yra aibės x, y, egzistuoja tokia aibė z, kad x ir y yra jos vieninteliai elementai.

3 (tuščios aibės) aksioma. $\exists x \forall y(y \notin x)$.

Ji teigia, kad egzistuoja aibė, neturinti elementų. Teorijoje įrodoma, kad egzistuoja vienintelė tuščia aibė, ir ji žymima $\emptyset$.

Dvielementę aibę žymime $\{x, y\}$. Įrodoma, kad $\{x, y\} = \{y, x\}$. Pora $\{\{X\}, \{X, Y\}\}$ vadinama sutvarkytąja ir žymima $< X, Y >$.

4 (klasių egzistavimo) aksioma:

4a) $\exists X \forall u \forall v(< u, v > \in X \leftrightarrow u \in v)$.
4b) $\forall X \forall Y \exists Z \forall u(u \in Z \leftrightarrow (u \in X \& u \in Y))$.
4c) $\forall X \exists Z \forall u(u \in Z \leftrightarrow u \notin X)$.
4d) $\forall X \exists Z \forall u(u \in Z \leftrightarrow \exists v(< u, v > \in X))$.
4e) $\forall X \exists Z \forall u \forall v(< u, v > \in Z \leftrightarrow u \in X)$.
4f) $\forall X \exists Z \forall u \forall v \forall w(< u, v, w > \in Z \leftrightarrow < v, w, u > \in X)$.
4g) $\forall X \exists Z \forall u \forall v \forall w(< u, v, w > \in Z \leftrightarrow < u, w, v > \in X)$.

4b aksioma apibrėžiama sankirta, o 4c yra papildinys.

5 (sąjungos) aksioma. $\forall x \exists y \forall u(u \in y \leftrightarrow \exists v(u \in v \& v \in x))$.

6 (visų poaibių aibės) aksioma. $\forall x \exists y \forall u (u \in y \leftrightarrow u \subseteq x)$.

7 (išskyrimo) aksioma. $\forall x \forall Y \exists z \forall u (u \in z \leftrightarrow (u \in x \& u \in Y))$.

Ja tvirtinama, kad nesvarbu, kokia aibė x ir klasė Y, atsiras aibė, kurios elementai yra bendri x ir Y elementai.

$\mathrm{Un}(X)$ žymime formulę, nusakančią X vienareikšmiškumą $\forall x \forall y \forall z ((< x, y > \in X \& < x, z > \in X) \rightarrow y = z)$.

8 (pakeitimo) aksioma. $\forall x (\mathrm{Un}(X) \rightarrow \exists y \forall u (x \in y \leftrightarrow \exists v (< v, u > \in X \& v \in x)))$.

9 (begalybės) aksioma. $\exists x (\emptyset \in x \& \forall u (u \in x \rightarrow u \cup \{x\} \in x))$.

8.5 Antrosios eilės logika

Antrosios eilės logikos abėcėlė ir predikatų logikos (pirmosios eilės) su funkciniais simboliais abėcėlė sutampa. Termo, atominės formulės ir literos sąvokos taip pat tokios pat, kaip ir pirmosios eilės logikoje. Funkcinių simbolių aibę suskaidykime į dvi: funkcijų (turima omenyje konkrečios funkcijos) bei funkcinių kintamųjų. Analogiškai skaidome ir predikatinių simbolių aibę.

8.6 apibrėžimas. *Antrosios eilės logikos formulių aibė $\mathcal{F}$ yra tokia pati mažiausia aibė, kad:*

- *atominės formulės priklauso aibei $\mathcal{F}$,*
- *jei F yra formulė, tai $\neg F$ – taip pat formulė,*
- *jei F, G yra formulės, tai $(F \& G)$, $(F \vee G)$, $(F \rightarrow G)$, $(F \leftrightarrow G)$ – taip pat formulės,*
- *jei F yra formulė, x – individinis kintamasis, tai $\forall x F$, $\exists x F$ – taip pat formulės,*
- *jei F yra formulė, P – predikatinis kintamasis, tai $\forall P F$, $\exists P F$ – taip pat formulės,*
- *jei F yra formulė, f – funkcinis kintamasis, tai $\forall f F$, $\exists f F$ – taip pat formulės.*

Sakome, kad formulė F yra *taisyklinga*, jei kiekvienas jos poformulis pavidalo $\forall X G$ ar $\exists X G$ (X gali būti individinis, predikatinis ar funkcinis kintamasis) tenkina sąlygą: nėra formulėje G poformulio, prasidedančio kvantoriniu kompleksu $\forall X$ ar $\exists X$. Nagrinėsime tik taisyklingas formules. Formalizuojamų teiginių aibė yra platesnė, palyginti su pirmosios eilės logikos galimybėmis.

Pavyzdžiai:

1. Pirmosios eilės logikos formule $\forall x(f(x) = x)$ tvirtinama, kad f yra projekcijos funkcija. Antrosios eilės logikos formule galima formalizuoti ir teiginį *egzistuoja projekcijos funkcija*: $\exists f \forall x(f(x) = x)$.

2. Pirmosios eilės logikoje galima užrašyti tvirtinimą kad, jei konkrečios dvi individinės konstantos lygios, tai jos arba turi kurią nors savybę P: $a = b \to (P(a) \leftrightarrow P(b))$, arba jos neturi. Antrosios eilės logikoje galima tiesiog apibrėžti dviejų elementų lygybę: $a = b \leftrightarrow \forall P(P(a) \leftrightarrow P(b))$.

Kita teorema tvirtinama, kad antrosios eilės logikoje negalioja Löwenheimo–Skolemo teorema.

8.9 teorema. *Egzistuoja antrosios eilės logikos formulė, kuri įvykdoma kontinuumo galios aibėje ir neįvykdoma jokioje numeruojamoje aibėje.*

Įrodymas. Nagrinėjame formulę

$$F\colon\ \exists z \exists u \forall X((X(z) \& \forall x(X(x) \to X(u(x)))) \to \forall x X(x)). \tag{8.5}$$

Visi šios formulės kintamieji z, u, X, x suvaržyti, todėl bet kurią formulės struktūrą sudaro tik individinių konstantų aibės.

Formulė (8.5) teisinga bet kurioje skaičiojoje aibėje $A = \{a_1, a_2, a_3, \ldots\}$. Imkime $z = a_1$, o funkciją $u(x)$ apibrėžkime tokiu būdu: $u(a_i) = a_{i+1}$. Tuomet su bet kuriuo vienviečiu predikatu X, kurio apibrėžimo aibė yra A, (8.5) formulė teisinga. Ji teisinga ir bet kurioje baigtinėje aibėje. Todėl $\neg F$ klaidinga bet kurioje numeruojamoje aibėje.

Parodykime, kad $\neg F$ teisinga realiųjų skaičių aibėje. Tuo tikslu įrodysime, kad F klaidinga realiųjų skaičių aibėje, t.y. kad ir kokie būtų z, u, egzistuoja toks predikatas X, kad formulė

$$(X(z) \& \forall x(X(x) \to X(u(x)))) \to \forall x X(x)$$

klaidinga. Pagal bet kurį $b \in R$ ir bet kurią vieno argumento funkciją $u(x)$ konstruojame aibę $B = \{b, u(b), u(u(b)), \ldots\}$. Aibė B yra numeruojama. Vienvietį predikatą $X(x)$ realiųjų skaičių aibėje R apibrėžiame tokiu būdu:

$$X(x) = \begin{cases} t, & \text{jei } x \in B, \\ k, & \text{jei } x \in R - B. \end{cases}$$

Formulė (8.5) realiųjų skaičių aibėje su aprašytaisiais b, u, X klaidinga. Teorema įrodyta.

Dar du antrosios eilės logikos teiginiai:

1. Antrosios eilės logikos tapačiai teisingų formulių aibė nėra rekursyviai skaiti.
2. Kompaktiškumo teorema antrosios eilės logikos formulių aibėms negalioja.

8.6 Tautologijos baigtinėse struktūrose

Raide T pažymėkime tapačiai teisingų pirmosios eilės logikos formulių aibę, o Tb — tapačiai teisingų baigtinėse struktūrose pirmosios eilės logikos formulių aibę. Aišku, kad $T \subset Tb$, bet $T \neq Tb$, nes formulė

$$F\colon\ \forall x \exists y P(x, y) \& \forall x \neg P(x, x) \& \forall x \forall y \forall z ((P(x, y) \& P(y, z)) \rightarrow P(x, z))$$

įvykdoma begalinėje aibėje ir neįvykdoma jokioje baigtinėje aibėje (žr. 5.3 skyrelį). Todėl $\neg F \in Tb$, o $\neg F \notin T$. Informatikoje dažniausiai galima apsiriboti baigtinėmis, t.y. paprastesnėmis, struktūromis. Deja, tapačiai teisingų formulių aibė tokiose struktūrose nėra ne tik rekursyvi, bet ir rekursyviai skaiti.

Pažymėkime raide S visų įvykdomų baigtinėse struktūrose formulių aibę. Tuomet, kad ir kokia būtų formulė F, ji priklauso aibei Tb tada ir tiktai tada, kai $\neg F \notin S$. Iš čia išplaukia, kad jei S neišsprendžiama, tai ir Tb neišsprendžiama.

8.10 teorema. *Aibė S nerekursyvi.*

Įrodymas. Tuo tikslu nagrinėjame vienajuostes Turingo mašinas su vienpuse begaline juosta į dešinę. Parodysime formulėmis, kaip galima modeliuoti tokių Turingo mašinų darbą. Kad būtų paprasčiau, modeliuojame pirmosios eilės logikos formulėmis su lygybės predikatu ir funkcija $f(x) = x + 1$. Numeruojame juostos ląsteles. Pačiai pirmajai (iš kairės, juosta juk vienpusė) priskiriame 0, o toliau iš eilės $1, 2, 3, \ldots$.

Tarkime, yra Turingo mašina M, kurios abėcėlė $\Sigma = \{a_0, a_1, \ldots, a_m\}$, būsenų aibė $Q = \{q_0, q_1, \ldots, q_j\}$, o galutinių būsenų aibė yra iš vienos būsenos q_1. Nagrinėkime mašinas, kurios arba po baigtinio žingsnių skaičiaus pereina į galutinę būseną q_1, arba dirba be galo ilgai, t.y. jos nepatenka į poziciją be išeities. Iš algoritmų teorijos žinoma, kad bet kurią rekursyviąją funkciją galima apskaičiuoti tokiomis Turingo mašinomis. Mus domina tik aibių Σ, Q elementų indeksai. Tiksliau, laikysime $\Sigma = \{0, 1, \ldots, m\}$, o $Q = \{0, 1, \ldots, j\}$. Be to, aibei Σ priklauso tuščiosios ląstelės simbolis b ir jo numeris yra m. Pradiniai duomenys yra abėcėlės $\Sigma' = \{0, 1, \ldots, m\}$ žodžiai. Tariame, kad jie užrašomi pirmose ląstelėse, t.y., jei žodžio ilgis yra n, tai ląstelės su numeriais $0, 1, \ldots, n-1$ nėra tuščios, o visose likusiose $n, n+1, \ldots$ įrašytas simbolis b.

Turingo mašinos darbas diskretus. Jo žingsnius numeruojame skaičiais 0, 1, 2, ... ir vadiname juos laiko momentais. Aprašome predikatus, kurių apibrėžimų aibe yra natūraliųjų skaičių aibė:

- $S(l, s, k) = t$ tada ir tiktai tada, kai momentu l ląstelėje s yra simbolis k,
- $B(l, q) = t$ tada ir tiktai tada, kai momentu l mašina yra būsenos q,
- $P(l, s) = t$ tada ir tiktai tada, kai momentu l skaitymo galvutė yra ties ląstele su numeriu s.

Nagrinėjame mašinas be pradinių duomenų, t.y. *kai jos pradeda darbą nulinės* būsenos, jų skaitymo galvutė yra ties nuline ląstele ir visose ląstelėse yra simboliai b. Tokios mašinos iš pradžių užrašo pradinius duomenis, o paskui atlieka skaičiavimus.

Pradinė situacija aprašoma formule

$$\text{Pr: } \forall u S(0, u, b) \& B(0, 0) \& P(0, 0).$$

Egzistavimas ir vienatinumas nusakomi formule

$$\begin{aligned}\text{Ex: } &\forall t \exists x \exists y \exists z \exists u (B(t, x) \& P(t, y) \& S(t, z, u) \& \forall v (B(t, v) \to \\ &(x = v)) \& \forall v (P(t, v) \to (y = v)) \& \forall v (S(t, z, v) \to (u = v))).\end{aligned}$$

Formule Ex tvirtinama, kad kiekvienu laiko momentu t mašina yra kurios nors vienintelės būsenos x, skaitymo galvutė yra ties vienintele ląstele y ir ląstelėje įrašytas vienintelis aibės Σ elementas.

Modeliuojame aprašytosios mašinos perėjimus formulėmis. Tarkime, yra r perėjimų ir j-asis yra pavidalo $\delta(q, m) = (q', m', D)$. Jam priskiriame formulę

$$\begin{aligned}\text{Per}(j)\text{: } &\forall t \forall s ((B(t, q) \& P(t, s) \& S(t, s, m)) \to \\ &(B(t+1, q') \& P(t+1, s+1) \& S(t+1, s, m') \& \\ &\forall u \forall v ((\neg (u = s) \& S(t, u, v)) \to S(t+1, u, v)))).\end{aligned}$$

Panašiai priskiriamos formulės ir likusiems $(r - 1)$ perėjimų.

$$\begin{aligned}\text{St: } &\forall t \forall s ((B(t, 1) \& P(t, s) \& S(t, s, m)) \to \\ &(B(t+1, 1) \& P(t+1, s) \& S(t+1, s, m))).\end{aligned}$$

Nagrinėjame formulę

$$F\text{: } \exists t (B(t, 1) \& Pr \& Ex \&_{j=1}^{r} Per(j) \& St).$$

Tarkime, po τ žingsnių mašina patenka į galutinę būseną, naudodama h ląstelių atminties. Pažymėkime $k = \{\tau, m+1, j+1, h\}$. Tuomet formulė įvykdoma struktūroje, kurios aibė $\{0, 1, \ldots, k\}$. Ir atvirkščiai, jei formulė įvykdoma baigtinėje struktūroje iš k elementų, tai Turingo mašina pereina į galutinę būseną po ne daugiau kaip k žingsnių.

Nėra algoritmo, kuris pagal Turingo mašinos pradinius duomenis pasakytų, ar mašina baigs darbą, t.y. po baigtinio skaičiaus žingsnių pereis į būseną 1, ar dirbs be galo ilgai. Tai *baigtinumo problema*, kuri nėra išsprendžiama.

Teorema įrodyta.

8.11 teorema. *Aibė Tb nėra rekursyviai skaiti.*

Įrodymas. Tarkime, F kuri nors formulė. Tikriname, ar F įvykdoma. Visų pirma tikriname, ar F įvykdoma kurioje nors struktūroje, kurios aibė yra iš vieno elemento. Tokių struktūrų skaičius yra baigtinis. Jei F teisinga kurioje nors iš jų, tai ji įvykdoma. Priešingu atveju nagrinėjame, ar formulė įvykdoma kurioje nors struktūroje iš dviejų elementų. Jei ji teisinga kurioje nors iš jų, tai ji įvykdoma. Priešingu atveju nagrinėjame visas tas struktūras, kurių aibėse yra trys elementai ir t.t. Jei F įvykdoma kurioje nors baigtinėje struktūroje, tai, naudodamiesi aprašytąja struktūra, rasime ją. Jei F neįvykdoma jokioje baigtinėje struktūroje, tai aprašytoji procedūra tęsis be galo ilgai.

Taigi įvykdomų baigtinėse struktūrose formulių aibė yra rekursyviai skaiti. Bet remiantis 8.10 teorema, ji nėra rekursyvi. Todėl jos papildinys, t.y. tapačiai klaidingų baigtinėse struktūrose formulių aibė, nėra rekursyviai skaiti. Kartu ir aibė *Tb* nėra rekursyviai skaiti. Teorema įrodyta.

8.7 apibrėžimas. *Formulių aibė A vadinama baigiai kontroliuojama, kai kiekviena $F \in A$ tenkina sąlygą: jei F įvykdoma, tai ji įvykdoma ir baigtinėje aibėje.*

8.12 teorema. *Jei formulių aibė baigiai kontroliuojama, tai ji išsprendžiama.*

Įrodymas. Aibę A suskaidome į dviejų nepersikertančiųjų aibių A', A'' sąjungą: $A = A' \cup A''$ ir $A' \cap A'' = \emptyset$. Aibei A' priklauso visos įvykdomos baigtinėse aibėse formulės, o aibei A'' – visos likusios. Kadangi A baigiai kontroliuojama, tai aibei A'' priklausančios formulės neįvykdomos ne tik baigtinėse aibėse, bet ir visose begalinėse aibėse. Todėl, jei $F \in A''$, tai sekvencija $F \vdash$ išvedama sekvenciniame predikatų skaičiavime. Taigi abi aibės A', A'' yra rekursyviai skaičios ir todėl A išsprendžiama. Teorema įrodyta.

Išvada. Kad ir kokia būtų neišsprendžiama klasė, egzistuoja joje formulė, įvykdoma begalinėje ir neįvykdoma jokioje baigtinėje aibėje.

Pateikiame porą tokių formulių:

1. $\forall x \forall y \forall z \forall u(\neg G(x, x) \& ((G(x, y) \& G(y, z)) \to G(x, z)) \& G(x, u))$,

2. $\forall x \exists u \forall y(\neg G(x, x) \& G(x, u) \& (G(u, y) \to G(x, y)))$.

Abiejose formulėse raide G pažymėtas dvivietis predikatinis kintamasis.

8.7 Pratimai

1. Raskite sekvencijų išvedimus aksiominėje aibių teorijoje:

a) $\vdash X = Y \leftrightarrow (X \subseteq Y \& Y \subseteq X)$,

b) $\vdash X = Y \to (Z \in X \to Z \in Y)$,

c) $\vdash X = Y \leftrightarrow \forall z(z \in X \leftrightarrow z \in Y)$,

d) $\vdash M(Z) \& Z = Y \to M(Y)$.

2. Raskite formulės $\forall X \forall x \exists y P(X, x, y)$ ekvivalenčiąją, individidiniams kintamiesiems žymėti naudodami tik didžiąsias raides (predikatą M).

Pavardžių rodyklė

W. Ackermann 57, 58
Aristotelis 7, 115, 117
P. Bernays 9, 179
D. Boole 7
C. Burali-Forti 7
G. Cantor 50
O. Cauchy 6
Al Chorezmi 44
A. Church 43, 45
M. Cialdea Mayer 162, 163
R. Dedekind 172
Eudoxos 6
L. Fariñas 158
G. Frege 7, 8, 69, 83
D. Gabbay 167
G. Gentzen 83, 89, 127
K. Gödel 7, 43, 45, 177, 179
Y. Gurevitch 132
A. Heyting 134
J. Herbrand 139
D. Hilbert 8, 43, 69
S. Jaskowski 89
V. Kabaila 9
S. Kleene 45
S. Kripke 149, 162
J. Kubilius 9
G. Leibnitz 6, 9
C. I. Lewis 148
L. Löwenheim 109
V. Matulis 9
G. Mints 97, 156, 157, 163
A. de Morgan 7
J. von Neumann 179
I. Newton 6
V. P. Orevkov 162
G. Peano 172
Ch. S. Peirce 7, 26
Pitagoras 6
R. Pliuškevičius 9
P. S. Poreckij 7
E. L. Post 44, 64, 67
M. Presburger 173
H. G. Rice 53
A. Robinson 6
J. A. Robinson 141
R. Robinson 179
J. B. Rosser 177
B. Russell 8, 9, 178
E. Schräder 7
H. M. Sheffer 18, 26
T. Skolem 109, 123
Tallis 6
A. Turing 44
A. Whitehead 9

Dalykinė rodyklė

abėcėlė 13
aibė
  baigiai įvykdoma — 137
  galimų pasaulių — 149
  kontinumo galios — 14
  maksimali formulių — 137
  numeruojamoji — 11
  prieštaringoji formulių — 93
  skaičioji — 11
  rekursyviai skaičioji — 54
antecedentas 84
antisekvencija 88
apibrėžimas dalimis 48
aritmetika
  Peano — 172
  Robinsono — 173
  Presburgerio — 173
aritmetinis predikatas 175

disjunktas 29
  Horno — 97
  tuščias — 91
dedukcijos teorema 75
disjunkcija 19
  griežtoji — 19

ekvivalenčiosios aibės 10
ekvivalenčiosios formulės 22
ekvivalentumas 20

forma
  normalioji disjunkcinė — 30
  — minimali — 34
  — tobuloji — 33
  — trumpiausioji — 33
  — konjunkcinė — 32
  — priešdėlinė — 110
  standartinė — 124
formulė 20
  antrosios eilės logikos — 180
  apibendrintoji — 158
  Barcano — 161
  įvykdomoji — 28
  modalumo logikos — 148
  pagalbinė — 164
  — su funkciniais simboliais 121
  tapačiai klaidinga — 28, 105
  tapačiai teisinga — 27, 105
  uždaroji — 104
funkcija
  aritmetinė — 175
  bazinė — 45
  bendroji rekursyvioji — 49
  logikos algebros — 34
  primityviai rekursyvi — 46
  universalioji — 60

grafas 15

Herbrando
  — bazė 139
  — universumas 138
H-interpretacija 139

įeitis 13
implikacija 19
interpretacija 22
išvada 84
  loginė — 28
išvedimas iš prielaidų 74
išvedimų taktikos 144

keitinys 141
kintamasis
  esminis — 24
  fiktyvusis — 24
  laisvasis — 103
  loginis — 20
  suvaržytasis — 103
kompaktiškumo teorema 138
konjunkcija 19
konjunktas 30
kvantoriaus veikimo sritis 103
kvantorinis kompleksas 102
kvantorius 102
  bendrumo — 102
  egzistavimo — 102

leksikografinė tvarka 14
litera 29
  modalumo — 156
logika
  intuicionistinė — 134
  modalumo K, T, D, S4, S5 — 152

tiesinė laiko – 166
logikos dėsnis 27
loginės konstantos 26

matrica 110
multiaibė 15

neigimas 18
nepriklausomoji aksioma 71

operatorius
kompozicijos – 45
minimizavimo – 49
primityviosios rekursijos – 46
ordinalas 57

pagrindinė loginė operacija 21
poformulio įeitis 21
poformulis 21
prefiksas 110
predikatas 101
lygybės – 130
prielaida 85

sekvencija 84
sekvencijos išvedimas 84, 128
semantinis medis 139
skaičiavimas
kanoninis – 64
minus-normalusis – 131
rezoliucijų – 97
sekvencinis – 83, 127
– intuicionistinis – 134
teiginių – 69
skulemizacija 123

struktūra 104
struktūrinės taisyklės 91, 127
sukcedentas 84

taisyklė
apverčiamoji – 85
atkirtos – 91
rezoliucijos – 143
taisyklės taikymas 84
taktika
absorbcijos – 145
podisjunkčio – 144
semantinės rezoliucijos – 144
tiesinė – 144
tvarkos – 145
tautologija 27
teiginys 18
teisingumo lentelė 22
teorija
dalinės tvarkos – 170
grupių – 170
pilnoji – 171
termas 121
tipų suma 58
tipų sandauga 58

unifikatorius 142
bendriausiasis – 142

vertė 18

Žegalkino polinomas 35
žodis 13
žodžio ilgis 13

Lietuvių–anglų kalbų žodynėlis

aibė	**set**
baigtinė ~	finite ~
išsprendžiamoji ~	decidable ~
rekursyviai skaiti ~	recursively enumerable ~
algoritmas	**algorithm**
unifikavimo ~	unification ~
antecedentas	**antecedent**
apverčiamumas	**invertibility**
atitiktis	**correspondance**
būsena	**state**
dedukcija	**deduction**
disjunkcija	**disjunction**
griežtoji ~	exclusive ~
disjunktas	**clause**
tuščias ~	empty ~
ekvivalentumas	**equivalence**
forma	**form**
normalioji ~	normal ~
~ disjunkcinė ~	disjunctive ~ ~
~ konjunkcinė ~	conjunctive ~ ~
~ priešdėlinė ~	prenex ~ ~
formulė	**formula**
atominė ~	atomic ~
bekvantorė ~	quantifier-free ~
centrinė ~	main ~
įvykdomoji ~	satisfiable ~
neprieštaringoji ~	consistent ~
pagrindinė ~	ground ~
parametrinė ~	parametric ~
prisotintoji ~	saturated ~
skulemizuotoji ~	skolemized ~
šoninė ~	side ~
uždaroji ~	closed ~
funkcija	**function**
bendroji rekursyvioji ~	general recursive ~
dalinė ~ ~	partial ~ ~
dalinė ~	partial ~
primityviai rekursyvi ~	primitive recursive ~
Skolemo ~	Skolem ~
visur apibrėžta ~	total ~

grafas	**graph**
orientuotasis ~	directed ~
įeitis	**occurrence**
implikacija	**implication**
indukcija	**induction**
interpretacija	**interpretation**
įrodymas	**proof**
išvedimas	**derivation, deduction**
~ nesinaudojant pjūvio taisykle	cut-free ~
išvedimo medis	**deduction tree**
įvykdomumas	**satisfiability**
keitinys	**substitution**
kelias	**path**
kintamasis	**variable**
individinis ~	individual ~
laisvasis ~	free ~
suvaržytasis ~	bound ~
konjunkcija	**conjunction**
konstanta	***constant***
loginė ~	logical ~
kvantorius	**quantifier**
bendrumo ~	universal ~
egzistavimo ~	existential ~
laipsnis	**degree**
modalumo ~	modal ~
lapas	**leaf**
lentelė	**table**
teisingumo ~	truth ~
litera	**literal**
logika	**logic**
antrosios eilės ~	second-order ~
aukštesniosios eilės ~	higher-order ~
intuicionistinė ~	intuitionistic ~
klasikinė ~	classical ~
matematinė ~	*mathematical* ~
modalumo ~	modal ~
netikslioji ~	fuzzy ~
pirmosios eilės ~	first-order ~
predikatų ~	*predicate* ~
teiginių ~	propositional ~
matrica	**matrix**
neišsprendžiamas	**undecidable**
operatorius	**operator**
modalumo ~	modal ~

paieška	**search**
pakankamumas	**sufficiency**
palankus	**favorable**
~ rinkinys	~ disjunct
pasaulis	**world**
galimasis ~	possible ~
pervardyti	**rename**
pilnas	**complete**
poformulis	**subformula**
prieštaringumas	**contradiction**
predikatas	**predicate**
prielaida	**premise**
reikšmė	**value**
rekursija	**recursion**
rezoliucija	**resolution**
semantinė ~	semantic ~
rezolventė	**resolvent**
sutvarkytoji ~	ordered ~
rinkinys	**disjunct**
bendriausiasis ~	general ~
vienetinio ilgio ~	unit ~
pradinis ~	initial ~
tuščias ~	empty ~
sąryšis	**relation**
seka	**sequence**
sekvencija	**sequent**
silpninimas	**weakening**
simbolis	**symbol**
funkcinis ~	function ~
n-vietis ~ ~	n-place ~ ~
n-vietis predikatinis ~	n-place predicate ~
skaičiavimas	**calculus**
sukcedentas	**succedent**
šaka	**branch**
šaknis	**root**
taisyklė	**rule**
apverčiamoji ~	invertible ~
išvedimo ~	inference ~
prastinimo ~	contraction ~
struktūrinė ~	structural ~
tautologija	**tautology**
termas	**term**
unifikatorius	**unifier**
bendriausiasis ~	most general ~
unifikavimas	**unification**
universumas	**universe**
Herbrando ~	Herbrand ~

Literatūra

1. R. Lassaigne, M. de Rougemont. *Logika ir informatikos pagrindai*. Vilnius: Žodynas, 1996.

2. R. Lassaigne, M. de Rougemont. *Logika ir algoritmų sudėtingumas*. Vilnius: Žara, 1999.

3. N. Lomanienė. *Logika. Deduktyvaus samprotavimo analizės pagrindai*. Vilnius: Justitia, 2001.

4. S. Norgėla. *Matematinės logikos įvadas*. Vilnius: VU rotaprintas, 1985.

5. S. Norgėla, R. Vaicekauskas. *Programavimo kalba Prolog*. Vilnius: VU rotaprintas, 1990.

6. R. Plečkaitis. *Logikos įvadas*. Vilnius: Mintis, 1968.

7. R. Pliuškevičius. *Susipažinkime su matematine logika*. Vilnius: Mokslas, 1983.

2004 02 02. 12 sp. l. Užs. Nr. 219
Leidykla TEV, Akademijos g. 4, LT-08412 Vilnius
Spausdino AB „Spauda"
Laisvės pr. 60, LT-05120 Vilnius