Vilniaus universitetas
Matematikos ir informatikos fakultetas
Informatikos katedra

Gintaras Skersys

DISKREČIOJI MATEMATIKA

Mokymo priemonė

Vilnius
2011

Įvadas

Kas yra diskrečioji matematika? Diskrečioji matematika yra matematikos šaka, nagrinėjanti diskrečius objektus, diskrečias struktūras, realiųjų reiškinių diskrečiuosius matematinius modelius. Ką reiškia „diskretus“? Atsiverskime tarptautinių žodžių žodyną[1]. Matome, kad žodis „diskretus“ kilęs iš lotynų kalbos žodžio „discretus“, reiškiančio „atskiras“. Žodis „diskretus“ apibrėžiamas taip: „1. netolydus, nutrūkstamas, kintantis, šuoliškas, atskiras visumos atžvilgiu; 2. *komp.* sveikaisiais skaičiais aproksimuojamas objektas“. Taigi, intuityviai „diskretų objektą“ suprasime kaip objektą, kuris gali būti stebimas atskirai, nėra sujungtas su kitais objektais. Pavyzdžiui, sveikieji skaičiai yra diskretieji objektai, tuo tarpu realieji skaičiai – nėra. Dažnai diskretumo sąvoka priešpastatoma tolydumo ir ribos sąvokoms – viskas, kas nesusiję su tolydumu ir riba, gali būti pavadinta diskrečiu. Mes naudojamės diskrečiąja matematika, kai skaičiuojame kokius nors objektus, kai tiriame ryšius tarp baigtinių ar skaičiųjų aibių, kai analizuojame procesus, sudarytus iš baigtinio skaičiaus žingsnių. Pagrindinė diskrečiosios matematikos reikšmės augimo priežastis yra ta, kad kompiuteriuose informacija yra saugoma ir apdirbama diskrečiuoju būdu.

Diskrečioji matematika yra daugelio matematikos ir teorinės informatikos sričių pagrindas. Jei norite suprasti šiuolaikinių kompiuterių architektūrą, programinę įrangą, komunikacijos sistemas, skaitmeninį signalų apdorojimą, informacijos teoriją, neuroninius tinklus, valdymo sistemas ir t. t., jūs turite naudotis bent trupučiu, o gal ir daug, diskrečiosios matematikos.

Diskrečioji matematika yra labai plati sritis. Į ją įeina, pavyzdžiui, tokios matematikos sritys kaip matematinė logika, aibių teorija, kombinatorika, grafų teorija, kodavimas, kriptografija, algoritmų teorija, baigtinių automatų teorija, formalių gramatikų teorija ir kitos.

Šis diskrečiosios matematikos kursas suteiks jums matematinės logikos, aibių teorijos, algoritmų teorijos ir kodavimo pagrindus.

Pastabos

1. Smulkiu šriftu surinktas tekstas nėra būtinas. Jisai skirtas tiems, kurie nori labiau pagilinti diskrečiosios matematikos žinias. Bet nesuklyskite: išnašų tekstas puslapių apačioje, nors ir mažesniu šriftu, yra būtinas.
2. Ženklu ‘□’ paprastai žymime įrodymo ar ilgesnio pavyzdžio pabaigą.

Šių paskaitų konspektų turėtų visiškai užtekti ruošiantis egzaminui. Tiems, kurie visgi norėtų labiau pasigilinti į diskrečiosios matematikos įvairias sritis, galiu rekomenduoti tokią literatūrą.

Papildoma literatūra

S. Norgėla. Logika ir dirbtinis intelektas. TEV, Vilnius, 2007

– norintiems įsigilinti į matematinę logiką.

R. Grigutis. Baigtinės algebrinės struktūros. VU leidykla, Vilnius, 1998

– norintiems įsigilinti į aibių teoriją ir algebrą.

V. Stakėnas. Informacijos kodavimas. VU leidykla, Vilnius, 1996

– norintiems įsigilinti į kodavimą.

K.H. Rosen, Discrete Mathematics and Its Applications, 5-as leid., McGraw-Hill, Boston, 2003

– literatūra anglų kalba, apimanti daugelį diskrečiosios matematikos sričių.

[1] V. Vaitkevičiūtė. Tarptautinių žodžių žodynas, II pataisytas ir papildytas leid. Žodynas, Vilnius, 2001.

С. В. Яблонский. Введение в дискретную математику. „Наука“, Москва, 1979
– kuriems rusiškai skaityti lengviau, nei lietuviškai.

I dalis Matematinės logikos pradmenys

Kaip žmonija gauna žinių apie ją dominančius objektus? Visų pirma, duomenys renkami atliekant bandymus ir stebėjimus, o antra, mąstant ir samprotaujant. Samprotaudami susiduriame su dvejopo pobūdžio žiniomis: vienas jau turime, o kitas išvedame iš jų samprotavimais. Kaip sužinoti, ar teisingai išvedėme? Dar senovėje žymiausi mąstytojai, ypač Aristotelis IV a. pr. m. e., stengėsi nustatyti tokias samprotavimo taisykles, dėsnius, schemas, kad būtų samprotaujama tik teisingai. Taip atsirado logikos mokslas. XIX amžiuje jisai buvo formalizuotas, buvo pradėti taikyti matematikos metodai, sudaryti logikos nagrinėjamų objektų matematiniai modeliai, ir taip atsirado matematinė logika.

1 Teiginiai

Apibrėžimas
Teiginys – *tai sakinys, kuris išreiškia tiesą arba netiesą.*

Pavyzdžiui:

1. Kolumbas atrado Ameriką.
2. Drambliai moka skraidyti.
3. Koks rytoj oras?
4. Penki daugiau už tris (trumpiau: 5>3).
5. 23+(-48) >0
6. Kitose planetose gyvena protingos būtybės.

Visi šie sakiniai, išskyrus trečią, yra teiginiai. Jie yra arba teisingi, arba ne (bet ne abu iš karto!), nors mes galbūt ir negalim to nustatyti (pavyzdžiui, šeštas sakinys).

Jeigu teiginys išreiškia tiesą, jis vadinamas *teisingu*, jei netiesą – *klaidingu* arba *neteisingu*. Jei teiginys teisingas, sakome, kad jis *įgyja reikšmę t* (arba 1). Jei klaidingas – *įgyja reikšmę k* (arba 0). Taigi teiginiai įgyja reikšmes iš aibės $\{t, k\}$ (arba $\{1,0\}$). Reikšmes t ir k (arba 1 ir 0) vadiname *loginėmis konstantomis*. Teiginius paprastai žymėsime mažosiomis raidėmis, pavyzdžiui, $p, q, r, s, \dots$

Matematinė logika nagrinėja, kaip nustatyti teiginio teisingumo reikšmę, kai teiginys yra *sudėtinis*, tai yra sudarytas iš kelių kitų teiginių.

2 Loginės operacijos

Iš paprastų teiginių galime sudaryti sudėtinius, naudodami *logines jungtis,* pavyzdžiui, „netiesa, kad…“, „ir“, „arba“ ir t. t. Sudėtinio teiginio sudarymas pasinaudojus logine jungtimi vadinamas *logine operacija*.

Išskirsime tokias logines operacijas.

1) Neigimas

Jei p yra teiginys, tai teiginys „netiesa, kad p“ („ne p“) vadinamas teiginio p *neiginiu* ir žymimas $\neg p$ (randamas ir pažymėjimas $\overline{p}$). Pavyzdžiui, teiginio „Petriukas eina į mokyklą“ neiginys yra „Netiesa, kad Petriukas eina į mokyklą“ arba „Petriukas neina į mokyklą“.

Teiginio p neiginys $\neg p$ yra teisingas tada ir tik tada, kai teiginys p yra neteisingas. Galime sudaryti lentelę, vadinamą *teisingumo reikšmių lentele* (arba tiesiog *teisingumo lentele*, žr. dešinėje).

p	$\neg p$
t	k
k	t

2) Konjunkcija (loginė daugyba)

Jei p ir q yra teiginiai, tai teiginys „p ir q“ vadinamas teiginių p ir q *konjunkcija* (arba *logine sandauga*) ir žymimas $p \wedge q$ arba $p\&q$. Pavyzdžiui, teiginių „Petriukas eina į mokyklą“ ir „Petriukas lanko krepšinio treniruotes“ konjunkcija yra teiginys „Petriukas eina į mokyklą ir lanko krepšinio treniruotes“.

Teiginių p ir q konjunkcija yra teisingas teiginys tada ir tik tada, kai abu teiginiai p ir q yra teisingi. Teisingumo reikšmių lentelę žr. dešinėje.

p	q	$p \wedge q$
t	t	t
t	k	k
k	t	k
k	k	k

3) Disjunkcija (loginė sudėtis)

Jei p ir q yra teiginiai, tai teiginys „p arba q“ vadinamas teiginių p ir q *disjunkcija* (arba *logine suma*) ir žymimas $p \vee q$. Pavyzdžiui, teiginių „Knyga yra ant stalo“ ir „Knyga yra ant lentynos“ disjunkcija yra teiginys „Knyga yra ant stalo arba ant lentynos“.

Teiginių p ir q disjunkcija yra neteisingas teiginys tada ir tik tada, kai p ir q abu neteisingi. Kitaip sakant, disjunkcija teisinga tada ir tik tada, kai bent vienas iš p ir q yra teisingas. Teisingumo reikšmių lentelę žr. dešinėje.

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

4) Implikacija

Jei p ir q yra teiginiai, tai teiginys „jei p, tai q“ (arba „iš p išplaukia q“) vadinamas teiginių p ir q *implikacija* ir žymimas $p \rightarrow q$ arba $p \Rightarrow q$. Pavyzdžiui, jei p yra „Petriukui septyneri metai“, o q „Petriukas eina į mokyklą“, tai $p \rightarrow q$ yra „Jei Petriukui septyneri metai, tai jis eina į mokyklą“.

Implikacija $p \rightarrow q$ yra neteisingas teiginys tada ir tik tada, kai p yra teisingas, o q – neteisingas. Teisingumo reikšmių lentelę žr. dešinėje.

p	q	$p \rightarrow q$
t	t	t
t	k	k
k	t	t
k	k	t

Pastebėkime, kad teiginių $p \rightarrow q$ ir $q \rightarrow p$ reikšmės gali skirtis, pavyzdžiui, „jei dabar saulėta, tai dabar diena“ yra teisingas teiginys, o „jei dabar diena, tai dabar saulėta“ yra nebūtinai teisingas (gali būti ir apsiniaukę). Tuo tarpu kitoms loginėms operacijoms, kurias jau apibrėžėme ar dar apibrėšime, tai nebūdinga, pavyzdžiui, $p \wedge q$ ir $q \wedge p$ reikšmės visada sutampa.

5) Ekvivalencija

Jei p ir q – teiginiai, tai teiginys „p tada ir tik tada, kai q“ vadinamas teiginių p ir q *ekvivalencija* (arba *ekvivalentumu*) ir žymimas $p \leftrightarrow q$ arba $p \Leftrightarrow q$. Pavyzdžiui, teiginių „Diskrečiosios matematikos egzamine gausiu 10“ ir „Būsiu viską išmokęs“ ekvivalencija yra teiginys „Diskrečiosios matematikos egzamine gausiu 10 tada ir tik tada, kai būsiu viską išmokęs“.

Ekvivalencija $p \leftrightarrow q$ yra teisingas teiginys tada ir tik tada, kai teiginių p ir q teisingumo reikšmės sutampa, t. y., arba jie abu teisingi, arba jie abu klaidingi. Teisingumo reikšmių lentelę žr. dešinėje.

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

6) *Šeferio funkcija*

Jei p ir q – teiginiai, tai teiginys „p ir q nesutaikomi“ vadinamas teiginių p ir q *Šeferio funkcija* ir žymimas $p|q$ arba p/q (skaitome „p Šeferio funkcija q“). Pavyzdžiui, teiginių „Šis pieštukas yra Jono“ ir „Šis pieštukas yra Petro“ Šeferio funkcijos reikšmė yra teiginys „Teiginiai „Šis pieštukas yra Jono“ ir „Šis pieštukas yra Petro“ yra nesutaikomi“.

Šeferio funkcija $p|q$ yra neteisingas teiginys tada ir tik tada, kai abu teiginiai p ir q yra teisingi. Teisingumo reikšmių lentelę žr. dešinėje.

p	q	p/q
t	t	k
t	k	t
k	t	t
k	k	t

7) *Griežta disjunkcija (sudėtis moduliu 2)*

Jei p ir q yra teiginiai, tai teiginys „arba p, arba q“ vadinamas teiginių p ir q *griežta disjunkcija* (arba *suma moduliu* 2) ir žymimas $p\oplus q$ arba $p+q$. Pavyzdžiui, teiginių „Knyga yra ant stalo“ ir „Knyga yra ant lentynos“ griežta disjunkcija yra teiginys „Knyga yra arba ant stalo, arba ant lentynos“.

Griežta disjunkcija yra teisingas teiginys tada ir tik tada, kai lygiai vienas iš teiginių p ir q yra teisingas. Teisingumo reikšmių lentelę žr. dešinėje.

p	q	$p\oplus q$
t	t	k
t	k	t
k	t	t
k	k	k

Vadinama „suma moduliu 2“, nes jei pažymėtume t vienetu, o k nuliu, tai teisingumo reikšmių lentelė būtų tokia, kokia pavaizduota dešinėje. Tas pačias reikšmes gautume ir sudėję p ir q moduliu 2 (t. y. sudėję p ir q, ir paėmę dalybos iš dviejų liekaną).

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

8) *Kitos loginės operacijos*

Galime apibrėžti ir kitas logines jungtis, kurios galbūt neturi pavadinimų, žymėjimų ir atitikmenų šnekamojoje kalboje. Pavyzdžiui, tokią, kurios teisingumo reikšmių lentelė yra kaip dešinėje.

Iš viso jų galime apibrėžti tiek, kiek yra skirtingų teisingumo reikšmių lentelių, pavyzdžiui, dvinarėms[1] loginėms jungtims jų yra 2^4=16.

p	q	
t	t	t
t	k	t
k	t	k
k	k	t

3 Loginės formulės

Kaip jau minėjau, teiginius žymime mažosiomis raidėmis *p,q,r,s,…,* ir jungiame juos loginėmis jungtimis. Matematinėje logikoje mums teiginio turinys yra visiškai nesvarbus. Mums svarbu tik tai, ar jis teisingas, ar ne. Todėl nuo šiol nebesigilinsime į teiginių turinį, o nagrinėsime juos kaip kažkokius kintamuosius (vadinsime juos *loginiais kintamaisiais)*, galinčius įgyti reikšmes t arba k, ir iš jų sudarinėsime sudėtinius teiginius, naudodami logines jungtis.

Apibrėžimas

Logine formule *vadinamas reiškinys, gautas baigtinį skaičių kartų pavartojus loginių operacijų ženklus bei skliaustus loginiams kintamiesiems jungti. Formaliai tai galima apibrėžti taip:*

a) *loginės konstantos k ir t yra loginės formulės;*
b) *loginiai kintamieji (p,q,r,s,…) yra loginės formulės;*
c) *jei Q yra loginė formulė, tai (¬Q) taip pat yra loginė formulė;*

[1] Loginė jungtis yra dvinarė, jei ji susieja du kintamuosius. Visos mūsų nagrinėtos jungtys, išskyrus neigimą, yra dvinarės.

d) *jei P ir Q yra loginės formulės, tai (P∆Q) yra loginė formulė, kur ∆ žymi bet kurią dvinarę loginę jungtį (pavyzdžiui,* $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, / , $\oplus$*,...).*

Pastaba

Kad supaprastintume formulių užrašymą, mes įvedame kai kurių loginių operacijų atlikimo tvarką ir daug kur skliaustus praleidžiame. Loginės operacijos bus atliekamos tokia tvarka: $\neg$, $\wedge$, $\vee$, kitos. Taip pat nerašome išorinių skliaustų, pavyzdžiui, rašome ne $(p\rightarrow q)$, o $p\rightarrow q$.

Pavyzdys

Reiškiniai t, r, $p\rightarrow q$, $\neg q$, $\neg q\rightarrow r$, $(p\wedge q)\vee r$, $\neg(p\leftrightarrow q)$, $((p\rightarrow q)\wedge(\neg q\rightarrow r))\rightarrow(q\vee\neg q)$ yra loginės formulės. Pagal loginės formulės apibrėžimą, turėtume rašyti $((\neg q)\rightarrow r)$, bet rašome tiesiog $\neg q\rightarrow r$, nes susitarėme, kad bet kuriuo atveju neigimas bus skaičiuojamas prieš implikaciją. Taigi $\neg q\rightarrow r$ reiškia $(\neg q)\rightarrow r$, o ne $\neg(q\rightarrow r)$. Taip pat galime rašyti $p\wedge q\vee r$ vietoj $(p\wedge q)\vee r$, nes vis tiek pirma atliekame konjunkciją, o tik paskui disjunkciją. Bet, nors šiuo atveju skliaustus apie konjunkciją galime pašalinti, to daryti jums nerekomenduoju, nes, mano nuomone, $(p\wedge q)\vee r$ yra aiškesnis užrašas, nei $p\wedge q\vee r$.

Žinodami, kokias reikšmes įgyja formules sudarantys teiginiai (t. y., loginiai kintamieji), galime apskaičiuoti formulės reikšmę. Apskaičiuodami naudojamės loginių operacijų teisingumo reikšmių lentelėmis. Taigi į formulę galime žiūrėti kaip į funkciją, kurios argumentai įgyja reikšmes iš aibės $\{k, t\}$ (arba $\{0, 1\}$), ir kuri įgyja reikšmes iš tos pačios aibės. Tokios funkcijos vadinamos *loginėmis funkcijomis*.

Pavyzdys

Sudarysime formulės $Q(p, q) := \neg p\rightarrow(q\wedge\neg(q\vee p))$ teisingumo reikšmių lentelę (čia ir toliau ':=' yra pažymėjimo ženklas: dešinėje jo pusėje esantį reiškinį pažymime kairėje pusėje esančiu simboliu):

p	q	$\neg p$	$q\vee p$	$\neg(q\vee p)$	$q\wedge\neg(q\vee p)$	$Q(p,q)$
t	t	k	t	k	k	t
t	k	k	t	k	k	t
k	t	t	t	k	k	k
k	k	t	k	t	k	k

Jei į formulę įeina n loginių kintamųjų, tai teisingumo lentelė turės 2^n eilučių.
Jei formulė A priklauso nuo kintamųjų $p_1, p_2, ..., p_n$, tai ją žymėsime $A(p_1, p_2, ..., p_n)$.

Apibrėžimas

Tegu $A(p_1, p_2, ..., p_n)$ *yra loginė formulė. Tada konkretus kintamųjų* $p_1, p_2, ..., p_n$ *reikšmių rinkinys vadinamas formulės A* interpretacija.

Pavyzdys

$p = t$, $q = k$ yra formulės Q iš pereito pavyzdžio interpretacija. Formulė Q su šia interpretacija įgyja reikšmę t.

Matome, kad kiekvieną interpretaciją atitinka viena teisingumo reikšmių lentelės eilutė, ir atvirkščiai. Todėl, jeigu formulė priklauso nuo n kintamųjų, tai yra 2^n skirtingų jos interpretacijų.

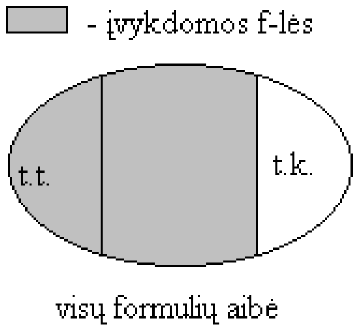
Apibrėžimas

Formulė vadinama tapačiai teisinga *(arba* tautologija*), jei ji teisinga su bet kuria interpretacija.*

Formulė vadinama tapačiai klaidinga *(arba* prieštara, *arba* neįvykdoma*), jeigu ji klaidinga su bet kuria interpretacija.*

Formulė vadinama įvykdoma, *jei atsiras interpretacija, su kuria jinai teisinga.*

Tapačiai teisingų (t. t.), tapačiai klaidingų (t. k.) ir įvykdomų formulių santykį galima pavaizduoti tokia diagrama:



Pavyzdys

Sudarę teisingumo reikšmių lenteles, įsitikinsite, kad formulės $p \to (q \to p)$ ir $\neg\neg p \leftrightarrow p$ yra tapačiai teisingos, kartu ir įvykdomos, $p \wedge \neg p$ yra tapačiai klaidinga, o formulė $p \to \neg p$ yra įvykdoma (jinai yra teisinga, kai $p=k$), bet ne tapačiai teisinga (ji klaidinga, kai $p=t$).

Akivaizdu, kad jei formulė A yra tapačiai teisinga, tai $\neg A$ yra tapačiai klaidinga, ir atvirkščiai. Pavyzdžiui, jei A priklauso nuo kintamųjų p ir q, žr. lentelę dešinėje.

p	q	A	$\neg A$
t	t	t	k
t	k	t	k
k	t	t	k
k	k	t	k

Pavyzdys

Nesunkiai įsitikinsite, kad $\neg(p \to (q \to p))$ yra tapačiai klaidinga.

Norint patikrinti, ar formulė $A(p_1, p_2, ..., p_n)$ yra tapačiai teisinga, pakanka sudaryti jos teisingumo reikšmių lentelę ir pažiūrėti, ar paskutiniame stulpelyje yra vien tik reikšmės t. Bet, sudarant teisingumo reikšmių lentelę, reikia apskaičiuoti formulės A reikšmę 2^n interpretacijų. Tai labai greitai auganti funkcija, todėl praktikoje naudoti teisingumo reikšmių lentelę formulės tapačiam teisingumui nustatyti galima tik nedideliems n.

Atrodytų, kad patikrinti, ar formulė yra įvykdoma, yra daug lengviau negu patikrinti jos tapatų teisingumą, nes užtenka surasti vieną reikšmę t. Bet taip nėra. Iš tikro, tarkime, kad turime algoritmą, kuris bet kuriai formulei A patikrina, ar jinai įvykdoma, ar ne. Bet žinome, kad formulė A yra tapačiai teisinga tada ir tik tada, kai $\neg A$ yra tapačiai klaidinga, t. y. kai $\neg A$ neįvykdoma. Taigi pritaikome tą algoritmą formulei $\neg A$. Jei atsakymas, kad $\neg A$ įvykdoma, tai A nėra tapačiai teisinga, o jei ne, tai A yra tapačiai teisinga.

Apibrėžimas

Dvi loginės formulės A ir B vadinamos logiškai ekvivalenčiomis *(arba tiesiog* ekvivalenčiomis*), jei su bet kuria interpretacija jos įgyja tą pačią reikšmę. Žymime $A \sim B$ (arba $A \equiv B$).*

Pavyzdys

Nesunkiai patikrinsite, kad $p \wedge q \sim q \wedge p$, $p \wedge (q \wedge r) \sim (p \wedge q) \wedge r$, $p \vee (q \wedge \neg q) \sim \neg\neg p \vee (r \wedge \neg r)$, $p \to p \sim q \to q$, $p \to q \sim \neg p \vee q$, $p \leftrightarrow q \sim (p \to q) \wedge (q \to p)$. Pavyzdžiui, dešinėje parodyta, kad paskutinės dvi tapatybės iš tikrųjų yra teisingos (paryškintuose stulpeliuose visos reikšmės sutampa). □

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

p	q	$p \leftrightarrow q$	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$
t	t	t	t	t	t
t	k	k	k	t	k
k	t	k	t	k	k
k	k	t	t	t	t

Jei žiūrėtume į loginę formulę kaip į loginę funkciją, tai pastebėtume, kad ekvivalenčios loginės formulės atitinka lygias logines funkcijas, nes jų reikšmės su kiekviena argumento reikšme sutampa. Kitaip tariant, visos ekvivalenčios loginės formulės atitinka tą pačią loginę funkciją.

Aišku, kad loginė konstanta t yra loginė formulė, kuri su bet kuria interpretacija įgyja reikšmę t, pavyzdžiui, kaip dešinėje.

p	q	t
t	t	t
t	k	t
k	t	t
k	k	t

Teorema

Formulė A yra tapačiai teisinga tada ir tik tada, kai ji ekvivalenti loginei konstantai t, t. y. $A \sim t$.

Įrodymas.[1] *Būtinumas*. Tarkime, kad formulė A yra tapačiai teisinga. Pagal apibrėžimą, ji yra teisinga su bet kuria interpretacija. Formulė t taip pat yra teisinga su bet kuria interpretacija, taigi formulės A ir t įgyja tą pačią reikšmę su kiekviena interpretacija. Todėl jos ekvivalenčios.

Pakankamumas. Iš kitos pusės, tegu formulė A yra ekvivalenti loginei konstantai t. Pagal ekvivalenčių formulių apibrėžimą, jos įgyja tą pačią reikšmę su kiekviena interpretacija. Bet formulė t įgyja reikšmę t su kiekviena interpretacija. Taigi formulė A taip pat įgyja reikšmę t su kiekviena interpretacija, todėl ji yra tapačiai teisinga. □

Analogiškai galime įrodyti, kad formulė A yra tapačiai klaidinga tada ir tik tada, kai jinai ekvivalenti loginei konstantai k. Be to, nesunku pastebėti, kad bet kurios dvi tapačiai teisingos formulės yra ekvivalenčios, ir bet kurios dvi tapačiai klaidingos formulės taip pat yra ekvivalenčios.

Atkreipsiu jūsų dėmesį į skirtumą tarp žymėjimų „↔“ ir „~“. Atminkite, kad „↔“ – tai loginė operacija, kuri sujungia formules A ir B į sudėtinę formulę $A \leftrightarrow B$, o „$A \sim B$“ tiesiog reiškia, kad formulės A ir B ekvivalenčios, t. y. jų reikšmės vienodos su bet kuria interpretacija. Bet tarp šių sąvokų yra aiškus ryšys: „$A \sim B$“ reiškia, kad formulių A ir B reikšmės vienodos su bet kuria interpretacija, o formulė $A \leftrightarrow B$ yra teisinga tada ir tik tada, kai formulių A ir B reikšmės yra vienodos. Todėl turime tokį teiginį.

Teorema

Loginės formulės A ir B yra logiškai ekvivalenčios tada ir tik tada, kai loginė formulė A↔B yra tapačiai teisinga.

Įrodymas. Prisiminkime, kad formulės $A \leftrightarrow B$ teisingumo reikšmių lentelė yra tokia, kaip parodyta dešinėje.

A	B	$A \leftrightarrow B$
t	t	t
t	k	k
k	t	k
k	k	t

Būtinumas. Tarkime, kad formulės A ir B yra logiškai ekvivalenčios. Pagal ekvivalenčių formulių apibrėžimą, jos įgyja tą pačią reikšmę su kiekviena jų kintamųjų interpretacija. Taigi arba abi jos teisingos, arba klaidingos. Abiem atvejais formulė A↔B yra teisinga. Taigi formulė A↔B yra tapačiai teisinga.

[1] Ši teorema, kurią norime įrodyti, yra pavidalo $p \leftrightarrow q$, kur p yra teiginys „formulė A yra tapačiai teisinga“, q yra „formulė A ekvivalenti loginei konstantai t“, o ↔ yra ekvivalencijos loginė jungtis („tada ir tik tada“). Norėdami parodyti, kad tokio pavidalo teorema yra teisinga, galime pasinaudoti tuo, kad $p \leftrightarrow q \sim (p \rightarrow q) \wedge (q \rightarrow p)$ (žr. pavyzdį aukščiau). Taigi turime parodyti, kad teiginiai $p \rightarrow q$ ir $q \rightarrow p$ yra teisingi. Jei tai įrodysime, tada ir jų konjunkcija bus teisinga. O kaip parodyti, kad $p \rightarrow q$ yra teisingas? Turime du atvejus: p yra klaidingas arba teisingas. Jei p yra klaidingas, tai pagal implikacijos teisingumo reikšmių lentelę teiginys $p \rightarrow q$ yra teisingas, ką ir reikėjo įrodyti. Jei p teisingas, tai turime parodyti, kad q irgi teisingas, nes tik tokiu atveju $p \rightarrow q$ bus teisingas. Taigi norėdami parodyti, kad $p \rightarrow q$ yra teisingas teiginys, padarome prielaidą, kad p yra teisingas, ir parodome, kad q irgi yra teisingas. Tą patį darome ir teiginiui $q \rightarrow p$. Reziumuokime. $p \leftrightarrow q$ pavidalo teoremą galime įrodyti dviem etapais: 1) padarome prielaidą, kad teiginys p yra teisingas, ir parodome, kad tada q irgi yra teisingas (sakome, kad įrodome sąlygos q *būtinumą*), 2) padarome prielaidą, kad teiginys q yra teisingas, ir parodome, kad tada p irgi yra teisingas (sakome, kad įrodome sąlygos q *pakankamumą*).

Pakankamumas. Tarkime, kad formulė A↔B yra tapačiai teisinga, t. y. su kiekviena interpretacija įgyja reikšmę *t*. Pagal formulės *A*↔*B* teisingumo reikšmių lentelę tai reiškia, kad formulės *A* ir *B* negali įgyti skirtingų reikšmių su jokia interpretacija, t. y. formulės *A* ir *B* įgyja tą pačią reikšmę su kiekviena jų kintamųjų interpretacija. Pagal ekvivalenčių formulių apibrėžimą, jos yra logiškai ekvivalenčios. □

Šitą teiginį sutrumpintai galime užrašyti taip: $A \sim B$ tada ir tik tada, kai $A \leftrightarrow B \sim t$.

Pavyzdys

$p \wedge q \sim q \wedge p$, todėl $(p \wedge q) \leftrightarrow (q \wedge p)$ yra tapačiai teisinga formulė, t. y. $(p \wedge q) \leftrightarrow (q \wedge p) \sim t$. Ir atvirkščiai, pavyzdžiui, žinome, kad $\neg\neg p \leftrightarrow p \sim t$, todėl $\neg\neg p \sim p$.

4 Logikos dėsniai

Apibrėžimas

Logikos dėsniu *vadiname tapačiai teisingą formulę*.

Logikos dėsniai naudojami pertvarkant loginius reiškinius ir samprotaujant. Su keliais logikos dėsniais (t. y., tapačiai teisingomis formulėmis) jau susidūrėme, pavyzdžiui, $p \rightarrow (q \rightarrow p)$. Be to, kaip matėme ką tik įrodytame teiginyje, logikos dėsnį gauname iš kiekvienos ekvivalenčių formulių poros: jei $A \sim B$, tai formulė $A \leftrightarrow B$ yra logikos dėsnis. Pavyzdžiui, matėme, kad $p \wedge q \sim q \wedge p$. Taigi $(p \wedge q) \leftrightarrow (q \wedge p)$ yra logikos dėsnis. Kadangi tai tokios artimos sąvokos, tai ekvivalenčių formulių porą irgi vadinsime *logikos dėsniu*, pavyzdžiui, $p \wedge q \sim q \wedge p$ vadinsime logikos dėsniu.

Kai kurie logikos dėsniai vartojami dažniau, kiti – rečiau. Dabar susipažinsime su svarbesniais dėsniais. Visų jų įrodymas labai paprastas. Tiesiog sudarome jų teisingumo reikšmių lenteles ir patikriname, kad tai tikrai ekvivalenčios formulės.

	Neigimo savybė:		
1.	$\neg\neg p \sim p$		dvigubo neigimo dėsnis
	Konjunkcijos savybės:	Disjunkcijos savybės:	
2.	*a)* $p \wedge p \sim p$	*b)* $p \vee p \sim p$	idempotencijos dėsniai
3.	*a)* $p \wedge \neg p \sim k$	*b)* $p \vee \neg p \sim t$	
	(prieštaravimo dėsnis)	(negalimo trečiojo dėsnis)	
4.	*a)* $p \wedge q \sim q \wedge p$	*b)* $p \vee q \sim q \vee p$	komutatyvumo dėsniai
5.	*a)* $(p \wedge q) \wedge r \sim p \wedge (q \wedge r)$	*b)* $(p \vee q) \vee r \sim p \vee (q \vee r)$	asociatyvumo dėsniai
	Kiti dėsniai:		
6.	*a)* $(p \vee q) \wedge r \sim (p \wedge r) \vee (q \wedge r)$	*b)* $(p \wedge q) \vee r \sim (p \vee r) \wedge (q \vee r)$	distributyvumo dėsniai
7.	*a)* $\neg(p \wedge q) \sim \neg p \vee \neg q$	*b)* $\neg(p \vee q) \sim \neg p \wedge \neg q$	De Morgano dėsniai
8.	*a)* $(p \wedge q) \vee p \sim p$	*b)* $(p \vee q) \wedge p \sim p$	absorbavimo dėsniai
9.	$p \rightarrow q \sim \neg p \vee q$		implikacijos pašalinimo dėsnis
10.	$p \leftrightarrow q \sim (p \rightarrow q) \wedge (q \rightarrow p)$		ekvivalencijos pašal. d.
11.	$p / q \sim \neg(p \wedge q)$		Šeferio f-jos pašal. d.
12.	$p \oplus q \sim \neg(p \leftrightarrow q)$		griežtos disj. pašal. d.
13.	$p \rightarrow q \sim \neg q \rightarrow \neg p$		kontrapozicijos dėsnis

Pavyzdys

Sudarykime 8a) dėsnio teisingumo reikšmių lentelę ir įsitikinkime, kad iš tikrųjų tai yra logikos dėsnis, t. y. ekvivalenčių formulių pora (žr. dešinėje).

p	*q*	$p \wedge q$	$(p \wedge q) \vee p$
t	*t*	*t*	*t*
t	*k*	*k*	*t*
k	*t*	*k*	*k*
k	*k*	*k*	*k*

Iš komutatyvumo ir asociatyvumo dėsnių (ketvirtas ir penktas logikos dėsniai) matome, kad formulėje, į kurią įeina vien kintamieji, skliaustai ir, pavyzdžiui, disjunkcijos ženklai, galima kintamuosius keisti vietomis, bet kaip juos suskliausti arba ir visai neskliausti – visos taip gautos formulės bus ekvivalenčios. Pavyzdžiui, $(p\vee q)\vee r \sim q\vee(p\vee r) \sim p\vee(q\vee r) \sim \ldots \sim p\vee q\vee r$ (jei skliaustų nėra, operacijas atliekame jų užrašymo tvarka). Tas pats galioja ir konjunkcijai, t. y. veiksmų atlikimo tvarka neturi reikšmės, vis tiek gausime tą patį rezultatą.

Atkreipkite dėmesį, kad distributyvumo dėsnis $(p\vee q)\wedge r \sim (p\wedge r)\vee(q\wedge r)$ labai primena gerai jums žinomą aritmetikos taisyklę $(p+q)\cdot r = (p\cdot r) + (q\cdot r)$ (dauginamojo įkėlimą į skliaustus), užtenka pakeisti disjunkciją „$\vee$“ į sudėtį „+“, ir konjunkciją „$\wedge$“ į daugybą „$\cdot$“. Bet logikoje galima dar daugiau! Logikoje galioja dar vienas distributyvumo dėsnis: $(p\wedge q)\vee r \sim (p\vee r) \wedge(q\vee r)$, kurio atitikmuo $(p\cdot q)+r = (p+r)\cdot(q+r)$ negalioja aritmetikoje!

Distributyvumo dėsnius galima apibendrinti didesniam narių skaičiui, t. y.

$$(p_1\vee p_2\vee\ldots\vee p_n)\wedge q \sim (p_1\wedge q)\vee(p_2\wedge q)\vee \ldots\vee(p_n\wedge q),$$

$$(p_1\wedge p_2\wedge\ldots\wedge p_n)\vee q \sim (p_1\vee q)\wedge(p_2\vee q)\wedge \ldots\wedge(p_n\vee q).$$

De Morgano dėsnius taip pat galime apibendrinti:

$$\neg(p_1\vee p_2\vee \ldots\vee p_n) \sim \neg p_1\wedge\neg p_2\wedge\ldots\wedge\neg p_n,$$

$$\neg(p_1\wedge p_2\wedge\ldots\wedge p_n) \sim \neg p_1\vee\neg p_2\vee\ldots\vee\neg p_n.$$

Logikos dėsniai naudojami formulėms pertvarkyti ir prastinti. Pateiksime dvi pastabas, kurios paaiškina, kaip tai galima padaryti.

1 pastaba

Logikos dėsniai tebegalios, jei pakeisime kintamuosius bet kokiomis formulėmis.

Iš tikro, turime tokį teiginį:

1 teiginys

Tarkime, $A(p_1,\ldots,p_n)$ yra tapačiai teisinga formulė, o $B_1,\ldots,B_n$ yra bet kokios formulės. Tada $A(B_1,\ldots,B_n)$ yra tapačiai teisinga.

Įrodymas. Imkime bet kurias formulių $B_1,\ldots,B_n$ interpretacijas. Tarkime, kad su tomis interpretacijomis B_1 įgyja reikšmę α_1, B_2 įgyja reikšmę $\alpha_2,\ldots,$ B_n – reikšmę α_n, kur $\alpha_i\in\{t, k\}$ $(1\le i\le n)$. Tada formulės $A(B_1,\ldots,B_n)$ reikšmė su tomis formulių $B_1,\ldots,B_n$ interpretacijomis bus lygi reikšmei $A(\alpha_1,\ldots,\alpha_n)$. Tačiau formulė $A(p_1,\ldots,p_n)$ yra tapačiai teisinga, todėl $A(\alpha_1,\ldots, \alpha_n)$ yra t. Parodėme, kad su bet kokia interpretacija formulė $A(B_1,\ldots,B_n)$ yra teisinga, o tai reiškia, kad $A(B_1,\ldots,B_n)$ yra tapačiai teisinga formulė. □

Išvada

Jei $A(p_1,\ldots,p_n) \sim B(p_1,\ldots,p_n)$, o $C_1,\ldots,C_n$ yra bet kokios formulės, tai $A(C_1,\ldots,C_n) \sim B(C_1,\ldots,C_n)$.

Įrodymas. Jei $A(p_1,\ldots,p_n) \sim B(p_1,\ldots,p_n)$, tai $A(p_1,\ldots,p_n) \leftrightarrow B(p_1,\ldots,p_n)$ yra tapačiai teisinga formulė, todėl pagal pirmą teiginį $A(C_1,\ldots,C_n) \leftrightarrow B(C_1,\ldots,C_n)$ yra tapačiai teisinga formulė, ir $A(C_1,\ldots,C_n) \sim B(C_1,\ldots,C_n)$. □

Ši išvada leidžia naudotis išvardintais logikos dėsniais ne tik tokia forma, kokia jie užrašyti, bet ir įstačius sudėtingesnes formules vietoj kintamųjų.

Pavyzdys

Absorbavimo dėsnis ne tik parodo, kad formulės $(p\vee q)\wedge p$ ir p yra ekvivalenčios, bet kad ekvivalenčios ir formulės $(P\vee Q)\wedge P$ bei P, kur P ir Q – bet kokios formulės. Todėl, pavyzdžiui, $((p\to q)\vee(r/s))\wedge(p\to q) \sim p\to q$ (čia įstatėme $p\to q$ vietoj P ir r/s vietoj Q).

Analogiškai, jei į De Morgano dėsnį $\neg(p\wedge q) \sim \neg p\vee\neg q$ vietoj kintamojo p įstatysime formulę $p/\neg r$, o vietoj q įstatysime $r\to q$, tai gausime logikos dėsnį

$$\neg((p/\neg r)\wedge(r\to q)) \sim \neg(p/\neg r)\vee \neg(r\to q).$$

2 pastaba

Ekvivalenčias formules gausime ir pakeitę dalį formulės jai ekvivalenčia formule.

Iš tikro, tarkime, A, B ir C yra bet kurios formulės, ir formulė B yra formulės A sudėtyje, t. y. B yra formulės A dalis.

Pavyzdys

Formulė $p \vee \neg q$ yra formulės $r \wedge (p \vee \neg q) \to q$ sudėtyje.

Beje, formulė B gali kelis kartus pasikartoti formulėje A. Formulę, kuri gaunama iš formulės A, pakeitus joje kurią nors formulę B formule C, žymėsime $A[B,C]$.

Pavyzdys

Jei A yra $r \wedge (p \vee \neg q) \to q$, B yra $p \vee \neg q$, C yra $\neg p \to \neg q$, tai $A[B,C]$ yra $r \wedge (\neg p \to \neg q) \to q$.

2 teiginys

Tarkime, B ir C yra ekvivalenčios formulės. Tada formulės A[B,C] ir A irgi yra ekvivalenčios.

Įrodymas. Reikia įrodyti, kad formulių $A[B,C]$ ir A reikšmės su visomis interpretacijomis sutampa, t. y. kad jų teisingumo reikšmių lentelių paskutiniai stulpeliai sutampa. Sudarykime formulės A teisingumo reikšmių lentelę taip, kad iš pradžių joje būtų apskaičiuojamos formulės B reikšmės (įskaitant formules, įeinančias į B). Analogiškai sudarykime formulės $A[B,C]$ teisingumo lentelę taip, kad iš pradžių būtų apskaičiuojamos formulės C reikšmės. Tada iki stulpelių B ir C formulių A ir $A[B,C]$ teisingumo lentelių reikšmės gali skirtis, bet stulpeliuose B ir C jos pasidarys lygios, nes B ir C yra ekvivalenčios formulės. Tolesniuose stulpeliuose reikšmės taip pat liks lygios, nes formulės A ir $A[B,C]$ daugiau niekuo nesiskiria, todėl paskutiniai stulpeliai irgi sutaps. □

Pavyzdys

Tegu A yra formulė $[(p \to q) \vee (q \oplus p)] \,/\, (p \to q)$, B yra $p \to q$, ir C yra $\neg p \vee q$. Tada formulė $A[B,C]$ gali būti tokia: $[(\neg p \vee q) \vee (q \oplus p)] \,/\, (p \to q)$. Formulių A ir $A[B,C]$ teisingumo reikšmių lenteles galima skaičiuoti taip:

p	q	B	$q \oplus p$	$B \vee (q \oplus p)$	A
t	t	t	k	t	k
t	k	k	t	t	t
k	t	t	t	t	k
k	k	t	k	t	k

p	q	$\neg p$	C	$q \oplus p$	$C \vee (q \oplus p)$	$p \to q$	$A[B,C]$
t	t	k	t	k	t	t	k
t	k	k	k	t	t	k	t
k	t	t	t	t	t	t	k
k	k	t	t	k	t	t	k

Taigi, skaičiuodami formulės A teisingumo reikšmių lentelę, iš pradžių apskaičiuojame formulę B, o paskui kitas formulės A dalis bet kuria tvarka. Skaičiuodami $A[B,C]$, iš pradžių apskaičiuojame formulę C, o paskui kitas formulės $A[B,C]$ dalis ta pačia tvarka, kaip ir formulei A. Matome, kad, kadangi formulės B ir C ekvivalenčios, tai stulpeliai B ir C, o ir visi toliau einantys stulpeliai, sutampa. Todėl $[(p \to q) \vee (q \oplus p)] \,/\, (p \to q) \sim [(\neg p \vee q) \vee (q \oplus p)] \,/\, (p \to q)$.

Pavyzdys

Kadangi $p \to q \sim \neg p \vee q$, tai formulėje $[(p \to q) \vee (q \oplus p)] \,/\, (p \to q)$ galime pakeisti, pavyzdžiui, pirmąją formulę $p \to q$ formule $\neg p \vee q$, taip gaudami formulę $[(\neg p \vee q) \vee (q \oplus p)] \,/\, (p \to q)$. Todėl $[(p \to q) \vee (q \oplus p)] \,/\, (p \to q) \sim [(\neg p \vee q) \vee (q \oplus p)] \,/\, (p \to q)$.

Naudojantis turimais logikos dėsniais ir ką tik pateiktomis pastabomis, galima išvesti naujus logikos dėsnius. Antra pastaba tvirtina, kad pakeitę bet kurią formulę, įeinančią į formulę A, jai ekvivalenčia formule, gausime formulei A ekvivalenčią formulę. O pirmoji sako, kad galime naudoti logikos dėsnius, įstatę bet kokias formules vietoj kintamųjų.

Pavyzdys

$(p \to q)/r \sim$	implikacijos pašalinimo dėsnis ir 2 pastaba
$(\neg p \vee q)/r \sim$	Šeferio f-jos pašalinimo dėsnis ir 1 pastaba
$\neg[(\neg p \vee q) \wedge r] \sim$	De Morgano dėsnis ir 1 pastaba
$\neg(\neg p \vee q) \vee \neg r \sim$	De Morgano dėsnis ir 1 bei 2 pastabos
$(\neg(\neg p) \wedge \neg q) \vee \neg r \sim$	dvigubo neigimo dėsnis ir 2 pastaba
$(p \wedge \neg q) \vee \neg r$	

Nuo šiol pertvarkydami logines formules minėsime tik naudojamus logikos dėsnius, o tas dvi pastabas laikysime savaime suprantamomis ir jų neminėsime.