Gintaras Skersys

DISKREČIOJI MATEMATIKA

Paskaitų kursas

2003

Įvadas

Diskrečioji matematika – tai daugelio šiandienos progresyvių technologijų pagrindas. Jei norite suprasti šiuolaikinių kompiuterių architektūrą, programinę įrangą, komunikacijos sistemas, skaitmeninį signalų apdorojimą, informacijos teoriją, neuroninius tinklus, valdymo sistemas ir t. t., jūs turėsite išmokti bent truputį, o gal ir daug, diskrečiosios matematikos. Tuo pačiu diskrečioji matematika yra daugelio matematikos ir teorinės informatikos sričių pagrindas.

Matematikos mokslą galima sąlyginai padalinti į diskrečiąją matematiką ir tolydžiąją matematiką. Tolydžiajai matematikai priskiriama viskas, kas susiję su ribos ir tolydumo sąvoka. Viską kitką galima priskirti diskrečiajai matematikai. 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 pasigilinti į diskrečiąją matematiką.
2. Ženklu ‘□’ paprastai žymime įrodymo ar ilgesnio pavyzdžio pabaigą.

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

Papildoma literatūra

S. Norgėla. Matematinės logikos įvadas. VU leidykla, Vilnius, 1985
– 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.

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*. Teiginius paprastai žymėsime mažosiomis raidėmis, pavyzdžiui, *p, q, r, s*, … Jei teiginys teisingas, sakome, kad jis įgyja reikšmę *t* (arba 1). Jei neteisingas – reikšmę *k* (arba 0). Taigi, teiginiai įgyja reikšmes iš aibės {*t*, *k*} (arba {1,0}). Reikšmes *t* ir *k* vadiname *loginėmis konstantomis*.

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 $\neg p$. 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 “$p\&q$” arba “$p \wedge q$”. 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	$p\&q$
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 “$p \vee q$”. 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 $p \to q$ arba $p \Rightarrow q$.

Pavyzdžiui, jei p yra “5>3”, o q “5>0”, tai $p \to q$ yra “jei 5>3, tai 5>0”.

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

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

Pastebėkime, kad teiginių $p \to q$ ir $q \to p$ 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).

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 $p \Leftrightarrow q$. 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”). 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 (suma 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 $p+q$. 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 ir atitikmenų šnekamojoje kalboje. Pavyzdžiui, tokią, kurios teisingumo reikšmių lentelė yra kaip dešinėje.

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

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

3. 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 sudėtingesnius teiginius, naudodami logines jungtis.

Apibrėžimas

Loginėmis formulėmis *vadinami reiškiniai, gauti baigtinį skaičių kartų pavartojus loginių operacijų ženklus bei skliaustus raidžių jungimui. 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;

d) jei P ir Q yra loginės formulės, tai (P∆Q) yra loginė formulė, kur ∆ žymi bet kurią dvinarę loginę jungtį (pavyzdžiui, ∨, &, →, ↔, / , ⊕ *,…).*

Pastaba

Kad supaprastintume formulių užrašymą, mes įvedame kai kurių loginių jungčių atlikimo tvarką (┐,&,∨, kitos), ir daug kur skliaustus praleidžiame.

Pavyzdys

Reiškiniai $p \to q$, $\neg q$, $\neg q \to r$, $(p\&q) \vee r$, $\neg(p \leftrightarrow q)$, $((p \to q)\&(\neg q \to r)) \to (q \vee \neg q)$ yra loginės formulės. Pagal loginės formulės apibrėžimą turėtume rašyti $((\neg q) \to r)$, bet rašome tiesiog $\neg q \to r$, nes susitarėme, kad bet kuriuo atveju neigimas bus skaičiuojamas prieš implikaciją. Taip pat galime rašyti $p\&q \vee r$ vietoj $(p\&q) \vee r$, nes vis tiek pirma atliekame konjunkciją, o tik paskui disjunkciją.

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.

Pavyzdys

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

p	q	$\neg p$	$q\vee p$	$\neg(q\vee p)$	$q\&\neg(q\vee p)$	$Q(p,q)$
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 $p_1, p_2, \ldots, p_n$, tai ją žymėsime $A(p_1, p_2, \ldots, p_n)$.

Apibrėžimas

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

Pavyzdys

$p = t$, $q = k$ yra formulės Q 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.

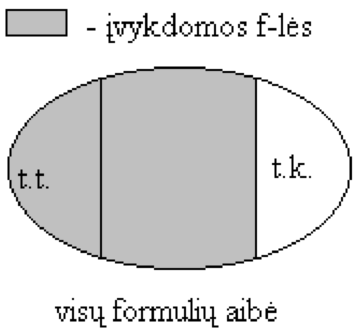
Apibrėžimas

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 (t.t.), $p\&\neg p$ yra tapačiai klaidinga (t.k.), o formulė $p\to\neg p$ yra įvykdoma (jinai yra teisinga, kai $p=k$).

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 $A(p_1, p_2, \ldots, p_n)$ 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 tapataus teisingumo nustatymui 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 kurią formulę 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 $p\&q \sim q\&p$, $p\&(q\&r) \sim (p\&q)\&r$, $p\vee(q\&\neg q) \sim \neg\neg p\vee(r\&\neg r)$, $p\rightarrow p \sim q\rightarrow q$. Žr., pavyzdžiui, dešinėje.

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

Taigi, formulė A yra tapačiai teisinga, jei ji ekvivalenti loginei konstantai t, t.y. $A \sim t$. Iš tikro, loginė konstanta t yra loginė formulė, kuri su bet kuria interpretacija įgyja reikšmę t, pavyzdžiui, kaip kairėje.

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

Analogiškai, formulė A yra tapačiai klaidinga, kai jinai ekvivalenti loginei konstantai k. Be to, 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 "$\leftrightarrow$" ir "$\sim$". Turėkite omenyje, kad "$\leftrightarrow$" – 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 žymėjimų yra aiškus ryšys, kurį rodo šis teiginys.

Teiginys

Loginės formulės A ir B yra logiškai ekvivalenčios tada ir tik tada, kai loginė formulė $A\leftrightarrow B$ *yra tapačiai teisinga.*

<u>*Įrodymas*</u>. 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

Pagal formulės $A\leftrightarrow B$ teisingumo reikšmių lentelę, $A\leftrightarrow B$ yra teisinga tada ir tik tada, kai formulių A ir B reikšmės sutampa. Todėl $A\leftrightarrow B$ yra tapačiai teisinga tada ir tik tada, kai A ir B reikšmės sutampa su kiekviena kintamųjų interpretacija, t.y. tada ir tik tada, kai $A \sim B$. □

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

Pavyzdys

$p\&q \sim q\&p$, todėl $(p\&q)\leftrightarrow(q\&p)$ yra tapačiai teisinga formulė, t.y. $(p\&q)\leftrightarrow(q\&p) \sim t$. 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 samprotaujant. Kelis logikos dėsnius (t.y., tapačiai teisingas formules) jau sutikome, pavyzdžiui, $p \to (q \to p)$. 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 $p\&q \sim q\&p$. Taigi, $(p\&q) \leftrightarrow (q\&p)$ yra logikos dėsnis. Kadangi tai tokios artimos sąvokos, tai ekvivalenčių formulių porą irgi vadinsime *logikos dėsniu*, pavyzdžiui, $p\&q \sim q\&p$ 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)* $p\&p \sim p$	*b)* $p \vee p \sim p$	idempotencijos dėsniai
3.	*a)* $p\&\neg p \sim k$ (prieštaravimo dėsnis)	*b)* $p \vee \neg p \sim t$ (negalimo trečiojo dėsnis)	
4.	*a)* $p\&q \sim q\&p$	*b)* $p \vee q \sim q \vee p$	komutatyvumo dėsniai
5.	*a)* $(p\&q)\&r \sim p\&(q\&r)$	*b)* $(p \vee q) \vee r \sim p \vee (q \vee r)$	asociatyvumo dėsniai
	Kiti dėsniai:		
6.	*a)* $(p \vee q)\&r \sim (p\&r) \vee (q\&r)$	*b)* $(p\&q) \vee r \sim (p \vee r)\&(q \vee r)$	distributyvumo dėsniai
7.	*a)* $\neg(p\&q) \sim \neg p \vee \neg q$	*b)* $\neg(p \vee q) \sim \neg p\&\neg q$	De Morgano dėsniai
8.	*a)* $(p\&q) \vee p \sim p$	*b)* $(p \vee q)\&p \sim p$	absorbavimo dėsniai
9.	$p \to q \sim \neg p \vee q$		implikacijos pašalinimo dėsnis
10.	$p \leftrightarrow q \sim (p \to q)\&(q \to p)$		ekvivalencijos pašal. d.
11.	$p/q \sim \neg(p\&q)$		Šeferio f-jos pašal. d.
12.	$p \oplus q \sim \neg(p \leftrightarrow q)$		griežtos disj. pašal. d.

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

Iš komutatyvumo ir asociatyvumo dėsnių (ketvirtas ir penktas loginiai 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 $(p \vee q)\&r \sim (p\&r) \vee (q\&r)$ labai primena gerai jums žinomą aritmetikos taisyklę $(p+q)r = pr + qr$, užtenka pakeisti disjunkciją "$\vee$" į sudėtį "+", ir konjunkciją "&" į daugybą "·". Bet logikoje galima dar daugiau! Logikoje galioja dar vienas distributyvumo dėsnis: $(p\&q)\vee r \sim (p\vee r)\&(q\vee r)$, kurio atitikmuo $pq+r = (p+r)(q+r)$ negalioja aritmetikoje!

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

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

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

De Morgano dėsnius taip pat galime apibendrinti:

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

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

1 pastaba

Loginiai 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 $\alpha_i\in\{t, k\}$ $(1\leq i\leq n)$. 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 loginiais dėsniais ne tik tokia forma, kokia jie užrašyti, bet ir įstačius sudėtingesnes formules vietoj kintamųjų.

Pavyzdys

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

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

$$\neg((p/\neg r)\&(r\rightarrow q)) \sim \neg(p/\neg r)\vee\neg(r\rightarrow q).$$

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 $r\&(p\vee\neg q)\rightarrow q$ 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 $r\&(p\vee\neg q)\rightarrow q$, B yra $p\vee\neg q$, C yra $\neg p\rightarrow\neg q$, tai $A[B,C]$ yra $r\&(\neg p\rightarrow\neg q)\rightarrow q$.

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 $[(p\rightarrow q) \vee (q\oplus p)] / (p\rightarrow q)$, B yra $p\rightarrow q$, ir C yra $\neg p\vee q$. Tada formulė $A[B,C]$ gali būti tokia: $[(\neg p\vee q) \vee (q\oplus p)] / (p\rightarrow q)$. 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	$q\oplus p$	$C \vee (q\oplus p)$	$A[B,C]$
t	t	k	t	k	t	k
t	k	k	k	t	t	t
k	t	t	t	t	t	k
k	k	t	t	k	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 $[(p\rightarrow q) \vee (q\oplus p)] / (p\rightarrow q) \sim [(\neg p\vee q) \vee (q\oplus p)] / (p\rightarrow q)$.

Pavyzdys

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

Naudojantis turimais logikos dėsniais ir ką tik gautais rezultatais, 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

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