Diskrečiosios matematikos konspektai

Marius Gedminas

2003 m. pavasaris
(VU informatikos magistrantūros studijų 2 semestras)

1 Formulės

Apibrėžimas: n-*viečiu predikatu* aibėje M vadiname funkciją $P : M^n \to \{\mathbf{t}, \mathbf{f}\}$. Aibė M vadinama *individinių konstantų aibe*.

Predikatinis kintamasis yra predikatas (ne koks nors konkrečiai, o apskritai).

Formulė apibrėžiama taip:

1. P – formulė, jei P yra predikatinis kintamasis.

2. $\neg F$ – formulė, jei F – formulė.

3. $(F \mathbin{\&} G)$, $(F \vee G)$, $(F \to G)$ yra formulės, jei F ir G yra formulės.

4. $\forall x F$, $\exists x F$ (skaitoma „visiems x“, „egzistuoja x“) yra formulės, jei F yra formulė.

5. $\Box F$, $\Diamond F$ (skaitoma „būtinai F“, „galbūt F“) yra formulės, jei F yra formulė.

Punktai 1–4 apibrėžia predikatų logiką, 1–5 — modalumo logiką.

$\Box F$, $\Diamond F$ galima interpretuoti įvairiai, pvz., „visada“/„kartais“, „visur“/„kai kur“. Semantika nusakoma aksiomomis, pvz., $\Box F \to F$, $F \to \Diamond F$.

Ateityje dar bus laiko logika: $\odot F$ („kitas F“).

$\forall$, $\exists$ vadinami *kvantoriais*, $\Box$, $\Diamond$ – *operatoriais*.

Sąvokos:

- kvantorių bei operatorių *veikimo sritis*

- operatoriaus *įeitis* (angl. occurrence)

- įeities veikimo sritis

- *laisvoji* ir *suvaržytoji* individinio kintamojo įeitis (suvaržytoji – jei patenka į atitinkamo kvantoriaus veikimo sritį). Kad būtų papraščiau, tarkime, jog reiškiniai a la $\forall x(P(x) \mathbin{\&} \exists x Q(x))$ nelegalūs.

Formulė vadinama *uždaraja*, jei ji neturi laisvų kintamųjų įeičių.

2 Semantika

Struktūra (arba *interpretacija*) yra rinkinys

$$S = \langle M; Q_1, \ldots, Q_n; x_1, \ldots, x_m \rangle$$

kur M – individinių konstantų aibė, Q_i – predikatai, x_j – konkretūs M elementai.

Formulė F yra *įvykdoma struktūroje* S, jei pakeitę formulėje predikatus į Q_i, o laisvus kintamuosius į x_j turime teisingą formulę.

Pvz.: $\forall x \forall y \forall z((P(x,y) \,\&\, P(y,z)) \to P(x,z)))$ yra įvykdoma struktūroje $S = \langle R; x < y \rangle$.

Pvz.: $\forall x \exists y(P(x,y) \,\&\, \neg \forall z P(z,z))$ yra įvykdoma struktūroje $S = \langle N; x < y \rangle$.

Pvz.: $Q(x,x,x)$ yra įvykdoma struktūroje $S = \langle Z; x = y = z; 0 \rangle$ arba $S = \langle R; x^2 + y^2 = z^2; 0 \rangle$.

Pvz.: $\forall x P(x,y) \to \exists z R(y,z,z)$ yra įvykdoma struktūroje $S = \langle R; x > y, x = y = z; 0 \rangle$.

Formulė F yra *įvykdoma*, jei egzistuoja struktūra, kurioje ji yra įvykdoma.

(Bendru atveju neįmanoma algoritmiškai nustatyti, ar formulė įvykdoma.)

Formulė F yra *tapačiai teisinga*, jei ji įvykdoma visose struktūrose.

Formulės F ir G yra *ekvivalenčios* ($F \equiv G$), jei su kiekviena struktūra jos yra kartu teisingos arba kartu klaidingos.

(Beje, ne visose logikose $\neg\neg F \equiv F$).

3 Modalumo logikos semantika

S. Kripke *semantika*:

$$S = \langle M, R, \mathcal{V} \rangle$$

kur M – galimų pasaulių aibė, R – dvivietis predikatas (sąryšis) aibėje M (rodo iš kurių pasaulių į kuriuos galima patekti), $\mathcal{V}$ – interpretacijų aibė (priklauso nuo pasaulio).

Fiksuojame pasaulį $\alpha \in M$. $\mathcal{V}$ suteikia reikšmes visiem loginiams kintamiesiems šiame pasaulyje.

1. Jei F – loginis kintamasis, formulė teisinga tada, kai ji teisinga pasaulyje α.
2. Jei $F = \neg G$, formulė teisinga tada, kai G klaidinga pasaulyje α.
3. Jei $F = G \,\&\, H$, formulė teisinga tada, kai ir G ir H teisingos pasaulyje α.
4. Jei $F = G \vee H$, formulė teisinga tada, kai bent viena iš G, H teisinga pasaulyje α.
5. Jei $F = G \to H$, formulė teisinga tada, kai G teisinga arba H klaidinga pasaulyje α.
6. Jei $F = \Box G$, formulė teisinga tada, kai G teisinga visuose pasauliuose α', kuriems $R(\alpha, \alpha') = \mathbf{t}$.
7. Jei $F = \Diamond G$, formulė teisinga tada, kai atsiras bent vienas pasaulis α', toks, kad $R(\alpha, \alpha') = \mathbf{t}$ ir G teisinga pasaulyje α'.

Formulė F yra *įvykdoma*, jei egzistuoja tokia struktūra $\langle M, R, \mathcal{V}\rangle$ ir pasaulis $\alpha \in M$, kad F įvykdoma pasaulyje α.

Formulė F yra *tapačiai teisinga*, jei ji teisinga bet kurios struktūros kiekviename pasaulyje.

Formulė F yra *tapačiai klaidinga*, jei ji klaidinga bet kurios struktūros kiekviename pasaulyje.

Pvz.: $F = \Box p$. M – pasaulio šalys. $R(x, y) = \mathbf{t}$ tada ir tik tada, kai valstybės x ir y turi bendrą sieną. p – teiginys „sausis yra šalčiausias mėnuo“. Pasaulyje $\alpha =$ Lietuva F prasmė yra „visose Lietuvos kaimynėse sausis – šalčiausias mėnuo“. Šiame pasaulyje F yra teisinga, o pvz., pasaulyje „Kongas“ ji yra klaidinga.

Pvz.: $F = p \to \Box\Box p$, M – sveikųjų skaičių aibė, $R(x, y) = \mathbf{t}$ tada ir tik tada, kai $y = x + 1$, p – „pasaulis nusakomas neigiamu skaičiumi“. Kai $\alpha = -1$, $p = \mathbf{t}$, $\Box\Box p = \mathbf{f}$, o formulė F klaidinga. ($\Box\Box p$ prasmė yra daugmaž ar $\alpha + 2 < 0$, ar ne.)

Formulės F *projekcija* $pr(F)$ gaunama išbraukus iš F visas modalumo logikos operatorių įeitis.

Pvz.: $F = p \to \Box\Diamond(q \vee \Box r)$, tada $pr(F) = p \to (q \vee r)$.

Jei $pr(F)$ nėra tapačiai teisinga, tai F taip pat nėra tapačiai teisinga (bet ne atvirkščiai).

$pr(F)$ ekvivalenti F kai $M = \{\alpha\}$ ir $R(\alpha, \alpha) = \mathbf{t}$.

Pvz.: $M = Z$, $R(x, y) = (y = x + 1) \vee (y = x + 2)$, p – „pasaulis – lyginis skaičius“, $q = \neg p$. Pasaulyje 2 $\Box(p \vee q) = \mathbf{t}$, $\Box p = \mathbf{f}$, $\Box q = \mathbf{f}$.

Formulės F transformacija į teiginių logiką žymima $[F]_\tau$ ir skaičiuojama pagal šias taisykles:

$$\begin{aligned}
[\Box F]_\tau &= \forall v(R(\tau, v) \to [F]_v)\\
[\Diamond F]_\tau &= \exists v(R(\tau, v) \,\&[F]_v)\\
[\neg F]_\tau &= \neg[F]_\tau\\
[F \,\&\, G]_\tau &= [F]_\tau \,\&[G]_\tau\\
[F \vee G]_\tau &= [F]_\tau \vee [G]_\tau\\
[F \to G]_\tau &= [F]_\tau \to [G]_\tau\\
[p]_\tau &= P(\tau)
\end{aligned}$$

Pvz.:

$$\begin{aligned}
[\Box\Diamond p]_\tau &= \forall v(R(\tau, v) \to \exists u(R(v, u) \,\&\, P(u))),\\
[\Box p \to \Diamond(q \vee \Diamond r)]_\tau &= \forall v\big(R(\tau, v) \to P(\tau)\big) \to\\
&\qquad \exists v\big(R(\tau, v) \,\&\, \big(Q(v) \vee \exists u(R(v, u) \,\&\, Z(u))\big)\big).
\end{aligned}$$

NB norint, kad formulė būtų teisinga ir pačiame pasaulyje, reikia, kad R būtų refleksyvus, t.y. $R(x, x) = \mathbf{t}$. Tai galima nusakyti aksioma $\Box p \to p$.

Jei norime R tranzityvumo, t.y. $\forall x\forall y\forall z((R(x, y) \,\&\, R(y, z)) \to R(x, z))$, galime tai užrašyti aksioma $\Box p \to \Box\Box p$.

4 Hilberto tipo skaičivimas

Nagrinėsime modalumo logikas, kuriose perėjimo funkcija $R(x, y)$ tenkina tam tikrus apribojimus. Du baziniai apribojimai, tinkantys visiems taikymams:

- refleksyvumas, t.y. $\forall x R(x,x)$
- tranzityvumas, t.y. $\forall x \forall y \forall z((R(x,y) \,\&\, R(y,z)) \to R(x,z))$

Kaip patikrinti formulės F tapatų teisingumą? Vien tik struktūros apibrėžimo nepakanka – visų struktūrų neišrašysim, ten jau nebeskaiti aibė. Vienas (vienintėlis iš žinomų) būdų – įvairūs formalūs skaičiavimai, kuriose įrodomos tik ir tik tapačiai teisingos formulės. Tuomet galime ieškoti įrodymo kuriame nors skaičiavime.

Yra sugalvoti trys skaičiavimai: Hilberto tipo, sekvenciniai ir rezoliucijų. Juos galima pritaikyti įvairioms logikoms (klasikinei, predikatų, modalumo, laiko).

Hilberto tipo skaičiavime naudojama tokia aksiomų sistema (A, B, C – 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 $\neg\neg A \to A$

5.1 $\Box(A \to B) \to (\Box A \to \Box B)$

5.2 $\Box A \to A$ (refleksyvumas)

5.3 $\Box A \to \Box\Box A$ (tranzityvumas).

Aksiomos 1.1–4.3 aprašo teiginių logiką, 5.1–5.3 prideda modalumo logiką Kadangi $\Diamond A \equiv \neg\Box\neg A$, o $\Box A \equiv \neg\Diamond\neg A$, tad aksiomų pakanka.

Hilberto tipo skaičiavime yra dvi taisyklės:

1. *MP – modus ponens*: $\dfrac{A, A \to B}{B}$
2. *AT*: $\dfrac{A}{\Box A}$

Teiginių logikai pakanka vienos modus ponens taisyklės. Modalumo logikai reikia ir antros.

Formulės F *išvedimas* $\vdash F$ – baigtinė formulių seka $F_1, \ldots, F_n$, kad

1. $F_n = F$ ir
2. $\forall i$ arba F_i – aksioma, arba ji gauta pagal kurią nors taisykle iš kairiau esančių formulių.

Hilberto skaičiavimas – bazinis, patogus teoriniams samprotavimams, o ne praktiniam naudojimui.

Pvz.: Įrodykime, kad $\vdash A \to \Diamond A$, kitaip tariant, kad $\vdash A \to \neg\Box\neg A$.

1. $\Box\neg A \to \neg A$ (aksioma 5.2)
2. $(\Box\neg A \to \neg A) \to (\neg\neg A \to \neg\Box\neg A)$ (aksioma 4.1)
3. $\neg\neg A \to \neg\Box\neg A$ arba $\neg\neg A \to \Diamond A$ (MP iš 1 ir 2)
4. $A \to \neg\neg A$ (aksioma 4.2)
5. $A \to \Diamond A$ (implikacijos tranzityvumas, kurį reiktų sunkiai ir ilgai įrodinėti remiantis aksioma 1.2)

5 Sekvencinis skaičiavimas

Sekvencija yra reiškinys $\Gamma \vdash \Delta$, kur Γ, Δ – (galbūt tuščios) baigtinės formulių aibės (formulių tvarka nesvarbi).

Aksioma:

$$\Gamma_1, A, \Gamma_2 \vdash \Delta_1, A, \Delta_2$$

Taisyklės:

1. $\dfrac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}$
2. $\dfrac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}$
3. $\dfrac{A, B, \Gamma \vdash \Delta}{A \,\&\, B, \Gamma \vdash \Delta}$
4. $\dfrac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \,\&\, B}$
5. $\dfrac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}$
6. $\dfrac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$
7. $\dfrac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}$
8. $\dfrac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{A \to B, \Gamma \vdash \Delta}$

Išvedimas turi medžio pavidalą: pradedam iš apačios (nuo šaknies) $\Gamma \vdash \Delta$ ir keliaujam aukštyn. Sekvencija yra *išvedama*, jei visos šakos baigiasi aksiomomis.

Bet kokiai tapačiai teisingai formulei F atsiras išvedimas $\vdash F$.

Kiekviena taisyklė panaikina vieną loginę operaciją, tad medžio gylis ribotas.

Pvz.: $\vdash (A \,\&\, B) \to (A \vee B)$

$$\dfrac{\dfrac{\dfrac{A, B \vdash A, B}{A \,\&\, B \vdash A, B}}{A \,\&\, B \vdash A \vee B}}{\vdash (A \,\&\, B) \to (A \vee B)}$$

Kitas pvz:

$$\dfrac{\dfrac{\dfrac{B \to C, \underline{A} \vdash \underline{A}, C \qquad \dfrac{\underline{B}, A \vdash \underline{B}, C \quad B, \underline{C}, A \vdash \underline{C}}{B, B \to C, A \vdash C}}{A \to B, B \to C, A \vdash C}}{\dfrac{A \to B, B \to C \vdash A \to C}{A \to B \vdash (B \to C) \to (A \to C)}}}{\vdash (A \to B) \to ((B \to C) \to (A \to C))}$$

Dar vienas pvz:

$$\dfrac{\dfrac{(B \mathbin{\&} C)\to D,\underline{A},B\vdash C \mathbin{\&} D,\underline{A} \qquad \dfrac{\cdots}{B\to C,(B \mathbin{\&} C)\to D,A,B\vdash C \mathbin{\&} D}}{A\to(B\to C),(B \mathbin{\&} C)\to D,A,B\vdash C \mathbin{\&} D}}{A\to(B\to C),(B \mathbin{\&} C)\to D,A \mathbin{\&} B\vdash C \mathbin{\&} D}$$

kur

$$\dfrac{(B \mathbin{\&} C)\to D,A,\underline{B}\vdash C \mathbin{\&} D,\underline{B} \qquad \dfrac{A,B,\underline{C},(B \mathbin{\&} C)\to D\vdash \underline{C} \qquad \dfrac{\cdots}{A,B,C,(B \mathbin{\&} C)\to D\vdash D}}{C,(B \mathbin{\&} C)\to D,A,B\vdash C \mathbin{\&} D}}{B\to C,(B \mathbin{\&} C)\to D,A,B\vdash C \mathbin{\&} D}$$

kur

$$\dfrac{\dfrac{A,\underline{B},C\vdash \underline{B} \qquad A,B,\underline{C}\vdash \underline{C}}{A,B,C\vdash B \mathbin{\&} C} \qquad A,B,C,\underline{D}\vdash \underline{D}}{A,B,C,(B \mathbin{\&} C)\to D\vdash D}$$

Ir dar vienas

$$\dfrac{\dfrac{\dfrac{\dfrac{\underline{B},A\vdash C,D,\underline{B}}{B\vdash C,D,A\to B} \qquad \underline{C},B\vdash \underline{C},D}{(A\to B)\to C,B\vdash C,D}}{(A\to B)\to C,B\vdash C\vee D}}{(A\to B)\to C,\neg(C\vee D),B\vdash}$$

Ilgą laiką nebuvo sekvencinio skaičiavimo pritaikymo modalumo logikai. Štai papildomos taisyklės:

9. $\dfrac{F,\Box F,\Gamma\vdash\Delta}{\Box F,\Gamma\vdash\Delta}$

10. $\dfrac{\Box\Gamma\vdash F}{\Sigma,\Box\Gamma\vdash\Delta,\Box F}$

kur $\Box\Gamma$ – visos formulės, kurios prasideda operatoriumi $\Box$; Σ – visos kitos formulės. Taisykles operatoriui $\Diamond$ galima išsivesti.

Išvedimas sudėtingesnis, nes galima vienu keliu patekti į aklavietę, teks grįžti ir bandyti kitaip.

Pvz.:

$$\dfrac{\dfrac{\dfrac{\dfrac{\underline{p},q,\Box(p \mathbin{\&} q)\vdash\underline{p}}{(p \mathbin{\&} q),\Box(p \mathbin{\&} q)\vdash p}}{\Box(p \mathbin{\&} q)\vdash p}}{\Box(p \mathbin{\&} q)\vdash\Box p} \qquad \dfrac{\dfrac{\dfrac{p,\underline{q},\Box(p \mathbin{\&} q)\vdash\underline{q}}{(p \mathbin{\&} q),\Box(p \mathbin{\&} q)\vdash q}}{\Box(p \mathbin{\&} q)\vdash q}}{\Box(p \mathbin{\&} q)\vdash\Box q}}{\Box(p \mathbin{\&} q)\vdash\Box p \mathbin{\&} \Box q}$$

Pvz.:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box\neg(A\vee\Box\neg A),\underline{A}\vdash\underline{A},\Box\neg A}{\Box\neg(A\vee\Box\neg A),A\vdash(A\vee\Box\neg A)}}{\Box\neg(A\vee\Box\neg A),A,\neg(A\vee\Box\neg A)\vdash}}{\Box\neg(A\vee\Box\neg A),A\vdash}}{\Box\neg(A\vee\Box\neg A)\vdash\neg A}}{\Box\neg(A\vee\Box\neg A)\vdash A,\Box\neg A}}{\Box\neg(A\vee\Box\neg A)\vdash(A\vee\Box\neg A)}}{\neg(A\vee\Box\neg A),\Box\neg(A\vee\Box\neg A)\vdash}}{\Box\neg(A\vee\Box\neg A)\vdash}}{\vdash\neg\Box\neg(A\vee\Box\neg A)}$$

NB $\Diamond A\equiv\neg\Box\neg A$.

Pabandykim įrodyti ekvivalentumus:

$$\Box\Box A \equiv \Box A$$
$$\Box\Diamond A \equiv \Diamond A$$
$$\Box\Diamond A \equiv \Box A$$

$$\frac{\Box A, \Box\Box A \vdash \underline{\Box A}}{\Box\Box A \vdash \Box A} \qquad \frac{\underline{\Box A} \vdash \underline{\Box A}}{\Box A \vdash \Box\Box A}$$

$$\frac{\underline{\underline{\neg\Box\neg A}}, \Box\neg\Box\neg A \vdash \underline{\neg\Box\neg A}}{\Box\neg\Box\neg A \vdash \neg\Box\neg A} \qquad \frac{\text{neišeina}}{\neg\Box\neg A \vdash \Box\neg\Box\neg A}$$

$$\frac{\text{neišeina}}{\Box\neg\Box\neg A \vdash \Box A} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\underline{A}, \Box A, \Box\neg A \vdash \underline{A}}{A, \neg A, \Box A, \Box\neg A \vdash}}{\Box A, \Box\neg A \vdash}}{\Box A \vdash \neg\Box\neg A}}{\Box A \vdash \Box\neg\Box\neg A}$$

6 Kvantorinė modalumo logika

Priminisime sekvencinio skaičiavimo taisykles modalumo logikos operatoriams:

9. $\dfrac{F, \Box F, \Gamma \vdash \Delta}{\Box F, \Gamma \vdash \Delta}$ 10. $\dfrac{\Box\Gamma \vdash F}{\Sigma, \Box\Gamma \vdash \Delta, \Box F}$

kvantorinė modalumo logika papildo jas šiomis:

11. $\dfrac{\Gamma \vdash \Delta, F(z)}{\Gamma \vdash \Delta, \forall x F(x)}$ kur z yra naujas kintamasis (nesutinkamas niekur kitur).

12. $\dfrac{\Gamma \vdash \Delta, F(u), \exists x F(x)}{\Gamma \vdash \Delta, \exists x F(x)}$ čia u – bet koks laisvas kintamasis.

13. $\dfrac{F(u), \forall x F(x), \Gamma \vdash \Delta}{\forall x F(x), \Gamma \vdash \Delta}$ čia u – bet koks laisvas kintamasis.

14. $\dfrac{F(z), \Gamma \vdash \Delta}{\exists x F(x), \Gamma \vdash \Delta}$ kur z yra naujas kintamasis (nesutinkamas niekur kitur).

Pvz.:

$$\dfrac{\dfrac{\dfrac{\underline{\underline{A(u)}}, \forall x A(x) \vdash \underline{A(u)}, \exists x A(x)}{A(u), \forall x A(x) \vdash \exists x A(x)}}{\forall x A(x) \vdash \exists x A(x)}}{\vdash \forall x A(x) \rightarrow \exists x A(x)}$$

o

$$\dfrac{\dfrac{\dfrac{A(z_1) \vdash A(z_2)}{A(z_1) \vdash \forall x A(x)}}{\exists x A(x) \vdash \forall x A(x)}}{\vdash \exists x A(x) \rightarrow \forall x A(x)} \quad \text{arba} \quad \dfrac{\dfrac{\dfrac{A(z_1) \vdash A(z_2)}{\exists x A(x) \vdash A(z_2)}}{\exists x A(x) \vdash \forall x A(x)}}{\vdash \exists x A(x) \rightarrow \forall x A(x)}$$

neišvedama.

Pvz.:

$$\begin{array}{c}
\underline{\underline{A(a,b)}}, \forall y A(x,y) \vdash \underline{A(a,b)}, \exists x A(x,b) \\ \hline
A(a,b), \forall y A(x,y) \vdash \exists x A(x,b) \\ \hline
\forall y A(a,y) \vdash \exists x A(x,b) \\ \hline
\forall y A(a,y) \vdash \forall y \exists x A(x,y) \\ \hline
\exists x \forall y A(x,y) \vdash \forall y \exists x A(x,y) \\ \hline
\vdash \exists x \forall y A(x,y) \to \forall y \exists x A(x,y)
\end{array}$$

Pvz.:

$$\begin{array}{c}
A(b,a), \forall y \exists x A(x,y) \vdash A(b,c), \exists x \forall y A(x,y) \\ \hline
A(b,a), \forall y \exists x A(x,y) \vdash \forall y A(b,y), \exists x \forall y A(x,y) \\ \hline
A(b,a), \forall y \exists x A(x,y) \vdash \exists x \forall y A(x,y) \\ \hline
\exists x A(x,a), \forall y \exists x A(x,y) \vdash \exists x \forall y A(x,y) \\ \hline
\forall y \exists x A(x,y) \vdash \exists x \forall y A(x,y)
\end{array}$$

neišvedama.

Ar $\forall x \Box A(x) \equiv \Box \forall x A(x)$?

$$\begin{array}{c}
\text{neįrodoma} \\ \hline
A(a), \Box A(a) \vdash A(b) \\ \hline
\Box A(a) \vdash A(b) \\ \hline
\Box A(a) \vdash \forall x A(x) \\ \hline
\Box A(a), \forall x \Box A(x) \vdash \Box \forall x A(x) \\ \hline
\forall x \Box A(x) \vdash \Box \forall x A(x)
\end{array}
\qquad
\begin{array}{c}
\underline{\underline{A(a)}}, \forall x A(x), \Box \forall x A(x) \vdash \underline{\underline{A(a)}} \\ \hline
\forall x A(x), \Box \forall x A(x) \vdash A(a) \\ \hline
\Box \forall x A(x) \vdash A(a) \\ \hline
\Box \forall x A(x) \vdash \Box A(a) \\ \hline
\Box \forall x A(x) \vdash \forall x \Box A(x)
\end{array}$$

Ar $\Diamond \exists x P(x) \equiv \exists x \Diamond P(x)$?

$$\begin{array}{c}
\text{neįrodoma} \\ \hline
\vdash \neg \exists x P(x) \\ \hline
\vdash \Box \neg \exists x P(x), \exists x \neg \Box \neg P(x) \\ \hline
\neg \Box \neg \exists x P(x) \vdash \exists x \neg \Box \neg P(x)
\end{array}
\qquad
\begin{array}{c}
\underline{\underline{P(z)}}, \Box \neg \exists x P(x) \vdash \underline{\underline{P(z)}}, \exists x P(x) \\ \hline
P(z), \Box \neg \exists x P(x) \vdash \exists x P(x) \\ \hline
P(z), \neg \exists x P(x), \Box \neg \exists x P(x) \vdash \\ \hline
\Box \neg \exists x P(x) \vdash \neg P(z) \\ \hline
\Box \neg \exists x P(x) \vdash \Box \neg P(z) \\ \hline
\neg \Box \neg P(z) \vdash \neg \Box \neg \exists x P(x) \\ \hline
\exists x \neg \Box \neg P(x) \vdash \neg \Box \neg \exists x P(x)
\end{array}$$

7 Reoliucijų tipo metodai

Kaip patikrinti, ar iš formulių $F_1, \ldots, F_n$ seka formulė F? Užrašome reiškinio

$$F_1 \,\&\, \ldots \,\&\, F_n \,\&\, \neg F$$

normalinę konjunkcinę formą $S = \{D_1, \ldots, D_k\}$, kur D_i – disjunktai (literų disjunkcija; litera yra arba loginis kintamasis, arba jo neiginys). Taisyklė

$$\frac{p \vee D', \neg p \vee D''}{D' \vee D''}$$

Jei ją taikydami gauname apačioje tuščią reiškinį (žymima $\perp$), įrodyta.

Pvz.: Įmonėje yra trys cechai: A, B ir C, susitarę dėl projektų tvirtinimo tvarkos. Jei cechas B nedalyvauja, tai nedalyvauja ir A tvirtinant projektą. Jei B dalyvauja, tai kartu dalyvauja ir A, ir C. Klausimas: ar privalo cechas C dalyvauti tvirtinant projektą, kai tvirtina A?

Kitais žodžiais tariant, ar iš $\neg B \to \neg A$, $B \to (A \,\&\, C)$ išplaukia $A \to C$?

$$(\neg B \to \neg A) \,\&(B \to (A \,\&\, C)) \,\&\, \neg(A \to C)$$
$$S = \{B \vee \neg A, \neg B \vee A, \neg B \vee C, A, \neg C\}$$
$$\frac{B \vee \neg A, A}{B} \quad \frac{\neg B \vee C, B}{C} \quad \frac{C, \neg C}{\perp}$$

Kitas pvz.: jei Biblija yra teisinga ir ją reikia suprasti pažodžiui, tai egzistuoja Dievas, be to Adomo ir Ievos išvarymo istorija yra teisinga. Jei tiesa, kad Dievas ištaip išvsrė iš rojaus Adomą ir Ievą, tai jis yra kerštingas ir nemielaširdingas. Tačiau, jei, kaip teigia Biblija, Dievas yra, tai jis visagalis ir mielaširdingas. Vadinasi Biblija yra tik graži pasaka arba nereikia jos suprasti pažodžiui.

b – Biblija yra teisinga

p – Bibliją reikia suprasti pažodžiui

d – egzistuoja Dievas

a – Adomo ir Ievos išvarymo istorija yra teisinga

e – Dievas yra kerštingas

m – Dievas yra mielaširdingas

v – Dievas yra visagalis

Duota: $(b \,\&\, p) \to (d \,\&\, a)$, $a \to (e \,\&\, \neg m)$, $d \to (v \,\&\, m)$. Įrodyti: $\neg b \vee \neg p$.

$$(b \,\&\, p) \to (d \,\&\, a) = (\neg b \vee \neg p) \vee (d \,\&\, a) = (\neg b \vee \neg p \vee d) \,\&(\neg b \vee \neg p \vee a)$$
$$a \to (e \,\&\, \neg m) = \neg a \vee (e \,\&\, \neg m) = (\neg a \vee e) \,\&(\neg a \vee \neg m)$$
$$d \to (v \,\&\, m) = \neg d \vee (v \,\&\, m) = (\neg d \vee v) \,\&(\neg d \vee m)$$
$$\neg(\neg b \vee \neg p) = b \,\&\, p$$

$$S = \{\neg b \vee \neg p \vee d, \neg b \vee \neg p \vee a, \neg a \vee e, \neg a \vee \neg m, \neg d \vee v, \neg d \vee m, b, p\}$$

$$\frac{\neg b \vee \neg p \vee a, b}{\neg p \vee a} \quad \frac{\neg p \vee a, p}{a} \quad \frac{a, \neg a \vee \neg m}{\neg m} \quad \frac{\neg d \vee m, \neg m}{\neg d}$$
$$\frac{\neg d, \neg b \vee \neg p \vee d}{\neg b \vee \neg p} \quad \frac{\neg b \vee \neg p, p}{\neg b} \quad \frac{\neg b, b}{\perp}$$

Kaip elgtis su modalumo logikos operatoriais? Taisyklės tokios:

$$\frac{\Box p \vee D', \neg p \vee D''}{D \vee D''} \quad \frac{\Box p \vee D', \Diamond\neg p \vee D''}{D \vee D''}$$

Pvz.: Jei šį pavasarį nusipirksiu mašiną arba susitaisysiu senąją, tai važiuosiu į Latviją, o tada būtinai užsuksiu į Biržus. Jei tikrai užsuksiu į Biržus, tai aplankysiu tėvus. Jei užsuksiu pas tėvus, jie galbūt įšnekins mane kartu praleisti vasarą. Tokiu atveju pasiliksiu ten iki rudens. Bet jei užsibūsiu ten iki rudens, tai Latvijos šią vasarą turbūt nepasieksiu. Taigi, galbūt neapsimoka taisyti senosios mašinos.

n – nusipirksiu mašiną

s – susitaisysiu senąją

l – važiuosiu į Latviją

b – užsuksiu į Biržus

a – aplankysiu tėvus

v – kartu praleisiu vasarą

r – pasiliksiu pas tėvus iki rudens

Duota: $(n \vee s) \to (l \,\&\, \Box b)$, $\Box b \to a$, $a \to \Diamond v$, $v \to r$, $r \to \neg l$. Patikrinti, ar $\Diamond\neg s$.

$$
\begin{aligned}
&(n \vee s) \to (l \,\&\, \Box b) = (\neg n \,\&\, \neg s) \vee (l \,\&\, \Box b)\\
&\qquad\qquad\qquad\quad = (\neg n \vee l) \,\&(\neg n \vee \Box b) \,\&(\neg s \vee l) \,\&(\neg s \vee \Box b)\\
&\Box b \to a = \neg\Box b \vee a = \Diamond\neg b \vee a\\
&a \to \Diamond v = \neg a \vee \Diamond v\\
&v \to r = \neg a \vee r\\
&r \to \neg l = \neg r \vee \neg l\\
&\neg\Diamond\neg s = \Box s
\end{aligned}
$$

$$S = \{\neg n \vee l, \neg n \vee \Box b, \neg s \vee l, \neg s \vee \Box b, \Diamond\neg b \vee a, \neg a \vee \Diamond v, \neg a \vee r, \neg r \vee \neg l, \Box s\}$$

$$\frac{\Box s, \neg s \vee \Box b}{\Box b} \quad \frac{\Box s, \neg s \vee l}{l} \quad \frac{l, \neg r \vee \neg l}{\neg r} \quad \frac{\neg r, \neg a \vee r}{\neg a} \quad \frac{\neg a, \Diamond\neg b \vee a}{\Diamond\neg b} \quad \frac{\Box b, \Diamond\neg b}{\bot}$$

Ar $a \equiv b \vdash \Box a \equiv \Box b$?

$$\cfrac{\cfrac{\cfrac{\text{neišeina}}{\Box a \vdash b}}{a \to b, b \to a, \Box a \vdash \Box b}}{a \to b, b \to a \vdash \Box a \to \Box b}$$

Ne.

Jei turime formulę F su kažkokiu poformuliu A ir turime $A \equiv B$, tai nieko, bet jei turime $\Box(A \equiv B)$, tuomet formulėje F galime poformulį A pakeisti į B.

Pvz.: $\Box p \vee \Diamond(q \,\&\, r)$. Pasižymėkime $a := (q \,\&\, r)$. Keiskime $\Box(a \equiv (q \,\&\, r) \vdash \Box p \vee \Diamond a$ ir t.t.:

$$
\begin{aligned}
&\vdash \Box p \vee \Diamond \underbrace{q \,\&\, r}_{a}\\
&\Box(a \equiv (q \,\&\, r) \vdash \Box p \vee \underbrace{\Diamond a}_{b}\\
&\Box(a \equiv (q \,\&\, r), \Box(b \equiv \Diamond a) \vdash \underbrace{\Box p}_{c} \vee b\\
&\Box(a \equiv (q \,\&\, r), \Box(b \equiv \Diamond a), \Box(c \equiv \Box p) \vdash \underbrace{c \vee b}_{l}\\
&\Box(a \equiv (q \,\&\, r), \Box(b \equiv \Diamond a), \Box(c \equiv \Box p), \Box(l \equiv c \vee b) \vdash
\end{aligned}
$$

Taisyklės yra šios

$$\Box(a \equiv (b \vee c)) : \Box(a \to (b \vee c)), \Box((b \vee c) \to a) : \Box(\neg a \vee b \vee c), \underline{\Box(a \vee \neg c)}, \underline{\Box(a \vee \neg b)}$$

$$\Box(a \equiv (b \,\&\, c)) : \Box(a \to (b \,\&\, c)), \Box((b \,\&\, c) \to a) : \Box(\neg a \vee b), \Box(a \vee c), \underline{\Box(\neg b \vee \neg c \vee a)}$$

$$\Box(a \equiv \neg b) : \Box(a \to \neg b), \Box(\neg b \to a) : \Box(\neg a \vee \neg b), \underline{\Box(b \vee a)}$$

$$\Box(a \equiv \Box b) : \Box(a \to \Box b), \Box(\Box b \to a) : \Box(\neg a \vee \Box b), \underline{\Box(\Diamond\neg b \vee a)}$$

$$\Box(a \equiv \Diamond b) : \Box(a \to \Diamond b), \Box(\Diamond b \to a) : \Box(\neg a \vee \Diamond b), \underline{\Box(\Box\neg b \vee a)}$$

$\blacksquare$

Išrašę tai gauname disjunktų aibės atitikmenį modalumo logikai.

Jei formulėje neigimas yra tik prieš loginius kintamuosius, pakanka tik pabrauktų disjunktų.

8 Rezoliucijų metodas modalumo teiginių logikoje

Formulė F yra išvedama ($\vdash F$), jei atsiras formulių seka $\Box D_1, \ldots, \Box D_s, l \vdash$, kur D_i – modalumo logikos disjunktai (modalumo logikos literų konjunkcijos, kur modalumo logikos litera yra $\Box l$, $\Diamond l$ arba l, o l yra įprastinė teiginių logikos litera).

Rezoliucijų metodo taisyklės:

$$\frac{F, G}{res(F, G)}$$

$$\frac{res(\Box F, \Box G)}{\Box res(F, G)} \qquad \frac{res(F \vee G, H)}{F \vee res(G, H)}$$

$$\frac{res(\Box F, G)}{res(F, G)}$$

$$\frac{res(\Box F, \Diamond G)}{\Diamond res(F, G)} \qquad \frac{res(l, \neg l)}{\bot}$$

Prastinimas:

$$\frac{F \vee \bot}{\bot} \qquad \frac{\Box\bot}{\bot} \qquad \frac{\Diamond\bot}{\bot}$$

Išvedimo paieška. Turime disjunktų aibę $S = \{D_1, \ldots D_s\}$. Galime imti bet kuriuos du disjunktus ir iš jų išvesti naują:

$$\frac{D_i, D_j}{D'}$$

Tiesinė taktika. Perbėgame disjunktus iš kairės į dešinę. Naujai gautus dedame į eilės galą. Išvedimo medis atrodo labai tiesiškai (kiekviename mazge dešinioji šaka yra lapas).

Absorbcijos taktika. Turime disjunktų aibę

$$S = \{D_1, D_2, \ldots, D_s\}$$

Paimame gautus disjunktus C_1, C_2 Taktika: susiaurinti išvedamų disjunktų aibę. Galime taikyti $\frac{C_1, C_2}{C}$ tik jei

1. arba vienas iš C_1, C_2 priklauso pradinei aibei S
2. nei vienas iš C_1, C_2 nepriklauso S, tada galime taikyti tik jei $C_1 = p \lor D'$, $C_2 = \neg p \lor D''$ ir $D' \subset D''$ arba $D'' \subset D'$ (čia $A \subset B$ reiškia, kad A yra B dalis, pvz, $q \lor \neg r \subset q \lor s \lor \neg r$)

Pvz.:

$$\dfrac{\dfrac{p \lor \Box q \quad \dfrac{D_1}{\neg q \lor r}}{p \lor r} \qquad \dfrac{D_2}{\Box\neg r \lor s}}{p \lor s}$$ – šis taikymas netaisyklingas pagal absorbcijos taktiką

galime perkelti tą netaisyklingą taikymą aukščiau:

$$\dfrac{\dfrac{\dfrac{D_1}{\neg q \lor r} \quad \dfrac{D_2}{\Box\neg r \lor s}}{\neg q \lor s}\text{– pažeidimas dabar čia} \quad p \lor \Box q}{p \lor s}$$

Kitas pvz:

$$(*)\dfrac{\dfrac{\Box(p \lor q) \quad \dfrac{D_1}{\Diamond\neg q \lor r}}{\Box p \lor \Box r} \qquad \dfrac{D_2}{\Box(\neg r \lor s)}}{\Diamond p \lor \Diamond s}$$

perkeliam aukščiau

$$\dfrac{\dfrac{\dfrac{D_1}{\Box\neg q \lor r} \quad \dfrac{D_2}{\Box(\neg r \lor s)}}{\Diamond\neg q \lor \Diamond s} \quad \Box(p \lor q)}{\Diamond p \lor \Diamond s}$$

Rezoliucijų metodas klasikinėje predikatų logikoje Bendra schema: turime $F_1, \ldots, F_n$, norime įrodyti F. $(F_1 \,\&\, \ldots \,\&\, F_n) \to F$ yra tapačiai teisinga tada ir tik tada, kai $F_1 \,\&\, \ldots \,\&\, \neg F$ yra tapačiai klaidinga.

1. suvedame į normalinę priešdėlinę formą
2. skulemizacija (egzistavimo kvantoriaus eliminavimas), bendrumo kvantorius $\forall$ praleidžiame
3. suvedame į normalinę konjunkcinę formą.

Rezultatas – turime disjunktų aibę $D = \{D_1 \ldots D_s\}$ ir ieškome išvedimo.

Normalinė priešdėlinė forma yra $Q_1 x_1 Q_2 x_2 \ldots Q_n x_n G$, kur $Q_i \in \{\forall, \exists\}$, o formulėje G kvantorių nėra.

Leidžiamos transformacijos:

$$\forall x A(x) \equiv \forall y A(y) \qquad \forall x A(x) \,\&\, B \equiv \forall x (A(x) \,\&\, B)$$
$$\exists x A(x) \equiv \exists y A(y) \qquad \exists x A(x) \,\&\, B \equiv \exists x (A(x) \,\&\, B)$$
$$\neg \forall x A(x) \equiv \exists x \neg A(x) \qquad \forall x A(x) \vee B \equiv \forall x (A(x) \vee B)$$
$$\neg \exists x A(x) \equiv \forall x \neg A(x) \qquad \exists x A(x) \vee B \equiv \exists x (A(x) \vee B)$$

jei formulėje B nėra kintamojo x (jei jis yra, galima pervadinti).

$$\forall x A(x) \,\&\, \forall x B(x) \equiv \forall x (A(x) \,\&\, B(x))$$
$$\forall x A(x) \vee \forall x B(x) \equiv \forall x \forall y (A(x) \,\&\, B(y))$$
$$\exists x A(x) \,\&\, \exists x B(x) \equiv \exists x \exists y (A(x) \,\&\, B(y))$$
$$\exists x A(x) \vee \exists x B(x) \equiv \exists x (A(x) \vee B(x))$$

Pvz.:

$$\begin{array}{l}
\exists x \forall y A(x,y) \to \forall y \exists x B(x,y) \\
\neg \exists x \forall y A(x,y) \vee \forall y \exists x B(x,y) \\
\forall x \neg \forall y A(x,y) \vee \forall y \exists x B(x,y) \\
\forall x \exists y \neg A(x,y) \vee \forall y \exists x B(x,y) \\
\forall x (\exists y \neg A(x,y) \vee \forall y \exists x B(x,y)) \\
\forall x (\exists y \neg A(x,y) \vee \forall y \exists u B(u,y)) \\
\forall x \exists y (\neg A(x,y) \vee \forall v \exists u B(u,v)) \\
\forall x \exists y \forall v (\neg A(x,y) \vee \exists u B(u,v)) \\
\forall x \exists y \forall v \exists u (\neg A(x,y) \vee B(u,v))
\end{array}$$

Skulemizacija – egzistavimo kvantorių eliminavimas. Kiekvieną kintamąjį $\exists x$ keičiame naujai įvestu funkciniu simboliu, kuris priklauso nuo visų kairiau esančių bendrumo kvantorių.

O bendrumo kvantorius tiesiog praleidžiame. Pvz.:

$$\exists x \forall y \exists z \forall u \forall v \exists s F(x,y,z,u,v,s) \to F(a,y,f(y),u,v,g(y,u,v))$$

Dabar tereikia suvesti F į normalinę konjunkcinę formą ir gausime disjunktų aibę.

Keitinys $\sigma = (t_1/x_1, \ldots, t_n/x_n)$ kur x_i – kintamieji, o t_i – termai.

Jei $F(x_1, \ldots x_n)$ – formulė, tai $F\sigma = F(t_1, \ldots t_n)$ yra ta pati formulė, kurioje kintamieji $x_1 \ldots x_n$ pakeisti termais $t_1 \ldots t_n$.

Keitinys vadinamas *unifikatoriumi* formulėms F ir G, jei $F\sigma = G\sigma$.

Keitinys σ yra bendriausias unifikatorius jei bet koks kitas unifikatorius β yra kompozicija $F\sigma\phi = F\beta$.

Pvz. formulių $P(x, f(a), g(z))$ ir $P(f(y), z, g(f(a))$ unifikatorius yra $\sigma = (f(a)/x, a/y, f(a)/z)$, o bendriausias unifikatorius yra $(f(y)/x, f(a)/z)$ (į ką keičiamas y nefiksuojama, nes tai nesvarbu).

Ne visas formules galima unifikuoti.

Galima taikyti taisyklę

$$\frac{C_1 \quad C_2}{C}, \quad \text{kur } P(t_1, \ldots, t_n) \in C_1, \text{ o } \neg P(g_1, \ldots g_n) \in C_2,$$

jei egzistoja unifikatorius σ, kad $P(t_1, \ldots, t_n)\sigma = P(g_1, \ldots g_n)\sigma$. Tik tuomet keisime visur:

$$\frac{C_1\sigma \quad C_2\sigma}{C\sigma}$$