Boolova algebra

Resničnostne tabele

Vsaka izjava ima **resničnostno vrednost**. Resničnostni vrednosti sta $\bot$ (resnica) in $\top$ (neresnica).

Primer: $\bot \lor (\top \Rightarrow \top)$ je resnična, njena resničnostna vrednost je $\top$.

Primer: $2 + 2 = 5$ je neresnična, njena resničnostna vrednost je $\bot$.

Kadar izjava vsebuje spremenljivke (pravimo jim tudi *parametri*), je njena resničnostna vrednost *odvisna* od parametrov.

Primer: Naj bosta $x, y \in \mathbb{N}$. Resničnstna vrednost izjave $x + y < 3$ je odvisna od x in y, kar lahko prikažemo z **resničnostno tabelo**:

```
x | y | x + 2 * y < 3
---------------------
0 | 0 |     ⊤
0 | 1 |     ⊤
1 | 0 |     ⊤
2 | 0 |     ⊤
1 | 1 |     ⊥
0 | 2 |     ⊥
...
```

Kot vidimo, je lahko takšna tabela neskončna, kar ni praktično.

V izjavi lahko nastopajo tudi **izjavne spremenljivke** ali **zijavni simboli**, to se spremenljivke, ki zavzamejo vrednosti $\bot$ in $\top$.

Primer: Naj bosta $p, q \in 2$. Tedaj je $\neg p \lor q$ izjava, katere resničnostna tabela je

```
p | q | ¬ p ∨ q
---------------
⊥ | ⊥ |     ⊤
⊥ | ⊤ |     ⊤
⊤ | ⊥ |     ⊥
⊤ | ⊤ |     ⊤
```

Izjava $\varphi(p_1, \ldots, p_n)$, v kateri nastopajo izjavne spremenljivke p_1, ..., p_n (in nobeni drugi parametri) določa preslikavo

$$2 \times \cdots \times 2 \to 2$$

s predpisom

$$(p_1, \ldots, p_n) \mapsto \varphi(p_1, \ldots, p_n)$$

Preslikavi, ki slika iz produkta $2 \times \cdots \times 2$ v 2 pravimo **Boolova preslikava**. Prikažemo jo lahko z resničnostno tabelo. Če ima preslikava n argumentov, ima tabela 2^n vrstic.

Tavtologije

Izjava je **tavtologija**, če je njena resničnostna vrednost ⊤ ne glede na vrednosti parametrov. Premisli: kako iz resničnostne tabele razberemo, ali je izjava tavtologija?

> **Izrek:** Naj bo φ izjava, v kateri nastopajo le izjavni simboli `p_1,…,p_n`. Tedaj velja:
>
> 1. Če je φ tavtologija, potem ima dokaz.
> 2. Če ima φ dokaz, je tavtologija.

Dokaz. Dokaz najdete v N. Prijatelj: *Osnove matematične logike* (1. del).

Izrek je pomemben, ker nam pove, da lahko dokazovanje izjav v nekaterih primerih nadomestimo s preverjanjem resničnostnih tabel.

*Opomba:** Izrek velja samo za izjave, ki jih sestavimo iz izjavnih simbolov, ⊥, ⊤ in logičnih veznikov ¬, ∧, ∨, ⇒, ⇔. Za splošne izjave, ki vsebujejo tudi ∀ in ∃ izrek *ne* velja.

Polni nabori

Vsaka formula v izjavnem računu ima resničnostno tabelo. Ali lahko vsako tabelo dobimo kot resničnostno tabelo neke formule? Na primer, ali obstaja formula, katere resničnostna tabela se glasi

```
p | q | ?
----------
⊥ | ⊥ | ⊥
⊥ | ⊤ | ⊤
⊤ | ⊥ | ⊤
⊥ | ⊥ | ⊥
```

Odgovor je pritrdilen. Na kratko povejmo, kako dobimo tako izjavo. Imamo dve množnosti.

Disjunktivna oblika: za vsako vrstico v tabeli, ki ima vrednost ⊤ zapišemo konjunkcijo simbolov in njihovih negacij, pri čemer negiramo tiste simbole, ki imajo v dani vrstici vrednost ⊥. Na primer, v zgornji tabeli imata druga in tretja vrstica vrednost ⊤, zanju zapišemo konjukciji:

- 1. vrstica: `¬ p ∧ q`
- 1. vrstica: `p ∧ ¬ q`

Nato tvorimo disjunkcijo tako dobljenih konjukcij:

```
(¬ p ∧ q) ∧ (p ∧ ¬ q)
```

Dobljena formula ima želeno resničnostno tabelo.

Konjunktivna oblika: za vsako vrstico v tabeli, ki ima vrednost ⊥ zapišemo disjunkcijo simbolov in njihovih negacij, pri čemer negiramo tiste simbole, ki imajo v dani vrstici vrednost ⊤. Na primer, v zgornji tabeli imata prva in čertrta vrstica vednost ⊥, zanju zapišemo disjukciji:

- 1. vrstica: `p ∨ q`
- 1. vrstica: `¬ p ∨ ¬ q`

Nato tvorimo konjunkcijo tako dobljenih disjunkcij:

```
(p ∨ q) ∧ (¬p ∨ ¬q)
```

Zgornjo tabelo bi lahko dobili tudi kot resničnostno tabelo formule

$p \Leftrightarrow q$

Vidimo, da lahko vsako resničnostno tabelo dobimo z uporabo veznikov ¬, ∨ in ∧. **Polni nabor** je tak izbor veznikov, k katerim lahko dobimo vsako resničnostno tabelo.

Torej je ¬, ∨, ∧ poln nabor. Lahko bi ga še zmanjšali na ¬, ∧, saj lahko

$p \vee q$

izrazimo kot

$\neg p \wedge \neg q$.

Boolova algebra

Ekvivalentni izjavi imata enake resničnostne vrednosti, torej lahko ekvivalenco ⇔ obravnavamo kar kot enakost, saj to tudi je, kar se tiče resničnostnih vrednosti. Zato lahko namesto $p \Leftrightarrow q$ pišemo tudi $p = q$, če imamo v mislih le resničnostne vrednosti.

(*Opomba:* izjavi sta lahko ekvivalentni, a nimata enakega *pomena*. Na primer, izjavi $\forall\ x, y \in R\ .\ x + y = y + x$ in $\forall\ \alpha \in R\ .\ \sin(2\ \alpha) = 2 \cdot \cos\alpha \cdot \sin\alpha$ sta ekvivalentni, saj sta obe resnični, a ne moremo reči, da je njun pomen enak.)

Za logične veznike veljajo *algebrajska pravila*. Ta pravila lahko uporabljamo kot računska pravila, s katerimi lahko izjavo poenostavmi v ekvivalentno obliko. Pogosto je tako računanje bolj prikladno kot dokazovanje. Spodaj naštete pravila lahko preverimo tako, da zapišemo resničnostne tabele izjav in jih primerjamo.

Pravilom, ki veljajo za logične veznike, pravimo **Boolova algebra**.

Pravila za ⊤ in ⊥

- $\top \vee p = \top$ (⊤ absorbira ∨)
- $\top \wedge p = p$ (⊤ je nevtralni element za ∧)
- $\neg\ \top = \bot$
- $\bot \wedge p = \bot$ (⊥ absorbira ∧)
- $\bot \vee p = p$ (⊥ je nevtralni element za ∧)
- $\neg\bot = \top$

Pravila za negacijo ¬

- $\neg\neg p = p$ (negacija je involucija)
- de Morganovi pravili:
  - $\neg(p \wedge q) = \neg p \vee \neg q$
  - $\neg(p \vee q) = \neg p \wedge \neg q$

Pravila za konjukcijo in disjunkcijo

- $p \wedge q = q \wedge p$ (konjunkcija je komutativna)
- $p \wedge p = p$ (konjunkcija je idempotentna)

- $(p \land q) \land r = p \land (q \land r)$ (konjunkcija je asociativna)

- $p \lor q = q \lor p$ (disjunkcija je komutativna)

- $p \lor p = p$ (disjunkcija je idempotentna)
- $(p \lor q) \lor r = p \lor (q \lor r)$ (disjunkcija je asociativna)

Absorbcijski pravili:

- $p \land (p \lor q) = p$
- $p \lor (p \land q) = p$

Distributivnostni pravili:

- $p \land (q \lor r) = (p \land q) \lor (p \land r)$
- $p \lor (q \land r) = (p \lor q) \land (p \lor r)$

Ostala pravila

- $p \lor \lnot p = \top$ (izključena tretja možnost)
- $p \land \lnot p = \bot$
- $(p \Rightarrow q) = (\lnot q \Rightarrow \lnot p)$
- $(p \Rightarrow q) = \lnot q \lor p$

Ekvivalence za kvantifikatorje

Zapišimo še uporabna logična pravila za kvantifikatorje. Tokrat uporabimo $\Leftrightarrow$ namesto =, ker je to bolj običajno.

- $(\forall x \in \emptyset \,.\, \varphi(x)) \Leftrightarrow \top$
- $(\exists x \in \emptyset \,.\, \varphi(x)) \Leftrightarrow \bot$
- $(\forall x \in \{a\} \,.\, \varphi(x)) \Leftrightarrow \varphi(a)$
- $(\exists x \in \{a\} \,.\, \varphi(x)) \Leftrightarrow \varphi(a)$
- $(\lnot \forall x \in A \,.\, \varphi(x)) \Leftrightarrow \exists x \in A \,.\, \lnot \varphi(x)$
- $(\lnot \exists x \in A \,.\, \varphi(x)) \Leftrightarrow \forall x \in A \,.\, \lnot \varphi(x)$
- $(\psi \Rightarrow \forall x \in A \,.\, \varphi(x)) \Leftrightarrow \forall x \in A \,.\, \psi \Rightarrow \varphi(x)$
- $(\psi \lor \forall x \in A \,.\, \varphi(x)) \Leftrightarrow \forall x \in A \,.\, \psi \lor \varphi(x)$
- $(\psi \land \exists x \in A \,.\, \varphi(x)) \Leftrightarrow \exists x \in A \,.\, \psi \land \varphi(x)$
- $(\forall u \in A \times B \,.\, \varphi(u)) \Leftrightarrow \forall x \in A \,.\, \forall y \in B \,.\, \varphi(x, y)$
- $(\exists u \in A \times B \,.\, \varphi(u)) \Leftrightarrow \exists x \in A \,.\, \exists y \in B \,.\, \varphi(x, y)$
- $(\forall u \in A + B \,.\, \varphi(u)) \Leftrightarrow (\forall x \in A \,.\, \varphi(\iota_1(x))) \land (\forall y \in B \,.\, \varphi(\iota_2(y)))$
- $(\forall u \in A \cup B \,.\, \varphi(u)) \Leftrightarrow (\forall x \in A \,.\, \varphi(x)) \land (\forall y \in B \,.\, \varphi(y))$
- $(\exists u \in A + B \,.\, \varphi(u)) \Leftrightarrow (\exists x \in A \,.\, \varphi(\iota_1(x))) \lor (\exists y \in B \,.\, \varphi(\iota_2(y)))$
- $(\exists u \in A \cup B \,.\, \varphi(u)) \Leftrightarrow (\exists x \in A \,.\, \varphi(x)) \lor (\exists y \in B \,.\, \varphi(y))$
- $(\forall u \in \{x \in A \mid \psi(x)\} \,.\, \varphi(u)) \Leftrightarrow \forall x \in A \,.\, \psi(x) \Rightarrow \varphi(x)$
- $(\exists u \in \{x \in A \mid \psi(x)\} \,.\, \varphi(u)) \Leftrightarrow \exists x \in A \,.\, \psi(x) \land \varphi(x)$

Te ekvivalence je treba preveriti tako, da jih dokažemo.