Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2016/2017

4. prednáška

CNF, kalkuly

13. marca 2017

Obsah 4. prednášky

Splniteľnosť a výrokovologické vyplývanie

Definícia 3.39 (Výrokovologické vyplývanie)

Z teórie T *výrokovologicky vyplýva* formula X (X je *výrokovologickým dôsledkom* T, skrátene $T \models X$) vtt každé ohodnotenie výrokových premenných, ktoré spĺňa T, spĺňa aj X.

Tvrdenie 3.40

Formula X výrokovologicky vyplýva z množiny formúl $S = \{X_1, X_2, \ldots, X_n\}$ vtt keď je množina $S_1 = \{X_1, X_2, \ldots, X_n, \neg X\}$ nesplniteľná.

Definícia 3.41

Formula X je *nezávislá* od množiny formúl S, ak existuje dvojica ohodnotení v_1, v_2 spĺňajúcich S, pričom v_1 spĺňa X, ale v_2 nespĺňa X.

Ekvivalentné úpravy

Definícia 3.43

Dve formuly X a Y sú *(výrokovologicky) ekvivalentné* vtt pre každé ohodnotenie v výrokových premenných platí, že v spĺňa X vtt v spĺňa Y.

Definícia 3.46

Zobrazenie $u\colon \mathcal{E} \to \mathcal{E}$ nazveme *ekvivalentnou úpravou* vtt, keď pre každú formulu A platí, že formuly A a $u(A)$ sú ekvivalentné.

Definícia 3.47 (Substitúcia)

Nech X, A, B sú formuly.
Substitúciou B za A v X (skrátene $X[A|B]$)) nazývame formulu, ktorá vznikne nahradením každého výskytu A v X formulou B.

Ekvivalentné úpravy

Veta 3.48 (Ekvivalentné úpravy)

Nech X je formula, A a B sú ekvivalentné formuly.
Potom X a $X[A|B]$ sú tiež ekvivalentné.

Tvrdenie 3.49

Nech X je tautológia, a výroková premenná a Y ľubovoľná formula.
Potom $X[a|Y]$ je tiež tautológia.

Ekvivalencie pre ekvivalentné úpravy

Veta 3.52

Nech A, B a C sú ľubovoľné formuly, $\top$ je ľubovoľná tautológia a $\bot$ je ľubovoľná nesplniteľná formula. Nasledujúce dvojice formúl sú ekvivalentné:

$(A \land (B \land C))$ *a* $((A \land B) \land C)$ $(A \lor (B \lor C))$ *a* $((A \lor B) \lor C)$	*asociatívnosť*
$(A \land (B \lor C))$ *a* $((A \land B) \lor (A \land C))$ $(A \lor (B \land C))$ *a* $((A \lor B) \land (A \lor C))$	*distributívnosť*
$(A \land B)$ *a* $(B \land A)$ $(A \lor B)$ *a* $(B \lor A)$	*komutatívnosť*
$\neg(A \land B)$ *a* $(\neg A \lor \neg B)$ $\neg(A \lor B)$ *a* $(\neg A \land \neg B)$	*de Morganove pravidlá*
$\neg\neg A$ *a* A	*dvojitá negácia*

Ekvivalencie pre ekvivalentné úpravy

Veta 3.52 (Pokračovanie)

$(A \land A)$ a A	*idempotencia*
$(A \lor A)$ a A	
$(A \land \top)$ a A	*identita*
$(A \lor \bot)$ a A	
$(A \lor (A \land B))$ a A	*absorpcia*
$(A \land (A \lor B))$ a A	
$(A \lor \neg A)$ a $\top$	*vylúčenie tretieho*
$(A \land \neg A)$ a $\bot$	*spor*
$(A \to B)$ a $(\neg A \lor B)$	*nahradenie* $\to$

Zápis ekvivalentnosti formúl

Definícia 3.55

Formuly A a B sú v relácii $\Leftrightarrow$ vtt
pre každé ohodnotenie v platí $v \models A$ vtt $v \models B$,
teda keď formuly A a B sú ekvivalentné.

Veta 3.56

Relácia $\Leftrightarrow$ na formulách je reláciou ekvivalencie,
teda je reflexívna, symetrická a tranzitívna.

Zápis ekvivalentnosti formúl

Dohoda

- Ak formuly A a B sú ekvivalentné a B vznikne substitúciou podľa viet 3.48 a 3.52, názov/skratku substituovaného páru ekvivalentných podformúl zapíšeme nad symbol $\Leftrightarrow$, napríklad:

$$(A \land \neg\neg B) \overset{\text{dvoj.neg.}}{\Leftrightarrow} (A \land B)$$

- Zápisom $A_1 \Leftrightarrow A_2 \Leftrightarrow \cdots \Leftrightarrow A_n$ vyjadrujeme, že $A_i \Leftrightarrow A_{i+1}$ pre každé $1 \leq i < n$.

Dohoda

Nech A_1, A_2, ..., A_n je konečná postupnosť formúl.

- Formulu $(((A_1 \land A_2) \land A_3) \land \cdots \land A_n)$ budeme skrátene zapisovať $(A_1 \land A_2 \land A_3 \land \cdots \land A_n)$, prípadne $\bigwedge_{i=1}^{n} A_i$ a nazývať *konjunkcia postupnosti formúl* $A_1, \ldots, A_n$.
- Formulu $(((A_1 \lor A_2) \lor A_3) \lor \cdots \lor A_n)$ budeme skrátene zapisovať $(A_1 \lor A_2 \lor A_3 \lor \cdots \lor A_n)$, prípadne $\bigvee_{i=1}^{n} A_i$ a nazývať *disjunkcia postupnosti formúl* $A_1, \ldots, A_n$.
- Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1.
- Konjunkciu prázdnej postupnosti formúl $(n = 0)$ chápeme ako ľubovoľnú tautológiu (napríklad $(p_1 \lor \neg p_1)$) a označujeme ju $\top$.
- Disjunkciu prázdnej postupnosti formúl chápeme ako ľubovoľnú nesplniteľnú formulu (napríklad $(p_1 \land \neg p_1)$) a označujeme ju $\bot$ alebo $\square$.

Konjunktívna a disjunktívna normálna forma

Definícia 3.53

- Výrokovú premennú alebo negáciou premennej nazývame *literál*.
- Disjunkciu literálov nazývame *klauzula* (tiež „klauza“).
- Hovoríme, že formula X je v *disjunktívnom normálnom tvare* (DNF), ak X je disjunkciou formúl, z ktorých každá je konjunkciou literálov.
- Hovoríme, že formula X je v *konjunktívnom normálnom tvare* (CNF), ak X je konjunkciou klauzúl (formúl, z ktorých každá je disjunkciou literálov).

Otázka

Ako vyjadríme, že formula je v CNF pomocou $\bigwedge_{i=1}^{n}$ a $\bigvee_{j=1}^{n}$?

Formula X je v CNF vtt, keď existujú postupnosti literálov $\ell_{1,1}, \dots, \ell_{1,n_1}, \ell_{2,1}, \dots, \ell_{2,n_2}, \dots, \ell_{k,1}, \dots, \ell_{k,n_k}$ také, že $X = \bigwedge_{i=1}^{k} \bigvee_{j=1}^{n_i} \ell_{i,j}$.

Existencia DNF, CNF

Veta 3.57

1. *Ku každej formule X existuje ekvivalentná formula A v disjunktívnom normálnom tvare.*
2. *Ku každej formule X existuje ekvivalentná formula B v konjunktívnom normálnom tvare.*

Dôkaz.

1. Zoberme všetky ohodnotenia v_i také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné q nevyskytujúce sa v X. Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu p, ak $v_i(p) = t$, alebo $\neg p$, ak $v_i(p) = f$, pre každú premennú p z X. Očividne formula $A = \bigvee_i C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).
2. K $\neg X$ teda existuje ekvivalentná formula A_1 v DNF. Znegovaním A_1 a aplikáciou de Morganových pravidiel dostaneme formulu B v CNF, ktorá je ekvivalentná s X. □

CNF – trochu lepší prístup

- Skúmanie všetkých ohodnotení nie je ideálny spôsob ako upraviť formulu do CNF — najmä keď má veľa premenných a jej splniteľnosť chceme rozhodnúť SAT solverom.
- Je nejaký lepší *systematický* postup?
- Všimnime si:
  CNF je konjunkcia disjunkcií literálov — výrokových premenných alebo ich negácií
  Teda:
  - CNF neobsahuje implikácie — ako sa ich zbavíme?
  - Negácia sa vyskytuje iba pri výrokových premenných — ako ju tam dostaneme, ak to tak nie je (napr. $\neg(A \vee B)$)?
  - Disjunkcie sa nachádzajú iba vnútri konjunkcií — ako presunieme „vonkajšie“ disjunkcie „dovnútra“ konjunkcií (napr. $(A \vee (B \wedge C))$)?

CNF – trochu lepší prístup

Algoritmus CNF_1

1. Prepíšeme implikácie:
   - $(A \to B) \quad \Leftrightarrow \quad (\neg A \lor B)$.
2. Presunieme $\neg$ dovnútra pomocou de Morganových pravidiel a dvojitej negácie.
3. „Roznásobíme“ $\land$ s $\lor$ podľa distributívnosti a komutatívnosti:
   - $(A \lor (B \land C)) \quad \Leftrightarrow \quad ((A \lor B) \land (A \lor C))$
   - $((B \land C) \lor A) \quad \Leftrightarrow (A \lor (B \land C)) \Leftrightarrow ((A \lor B) \land (A \lor C)) \Leftrightarrow ((B \lor A) \land (A \lor C)) \Leftrightarrow \quad ((B \lor A) \land (C \lor A))$
4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

Tvrdenie 3.58

Výsledná formula alg. CNF_1 je ekvivalentná s pôvodnou a je v CNF.

CNF – trochu lepší prístup

Príklad 3.59

$$((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$$
$$\overset{1}{\Leftrightarrow} (\neg(a \lor \neg b) \lor \neg(c \lor (d \land \neg e)))$$
$$\overset{2}{\Leftrightarrow} ((\neg a \land \neg\neg b) \lor \neg(c \lor (d \land \neg e)))$$
$$\overset{2}{\Leftrightarrow} ((\neg a \land b) \lor \neg(c \lor (d \land \neg e)))$$
$$\overset{2}{\Leftrightarrow} ((\neg a \land b) \lor (\neg c \land \neg(d \land \neg e)))$$
$$\overset{2}{\Leftrightarrow} ((\neg a \land b) \lor (\neg c \land (\neg d \lor \neg\neg e)))$$
$$\overset{2}{\Leftrightarrow} ((\neg a \land b) \lor (\neg c \land (\neg d \lor e)))$$
$$\overset{3}{\Leftrightarrow} (((\neg a \land b) \lor \neg c) \land ((\neg a \land b) \lor (\neg d \lor e)))$$
$$\overset{2\times 3}{\Leftrightarrow} ((((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e))))$$
$$\overset{4}{\Leftrightarrow} ((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e)))$$
$$\overset{2\times 4}{\Leftrightarrow} ((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$$

CNF – trochu lepší prístup

- Algoritmus CNF_1 je jednoduchý, ale nie vždy výhodný
- Všimnite si:
  - Z formuly $((p_1 \land q_1) \lor (p_2 \land q_2))$ s 2 konjunkciami dostaneme $((p_1 \lor p_2) \land (p_1 \lor q_2) \land (q_1 \lor p_1) \land (q_1 \lor q_2))$ so 4 klauzulami
  - Z formuly $((p_1 \land q_1) \lor (p_2 \land q_2) \lor (p_3 \land q_3))$ s 3 konjunkciami dostaneme $((p_1 \lor p_2 \lor p_3) \land (p_1 \lor p_2 \lor q_3) \land (p_1 \lor q_2 \lor p_3) \land (p_1 \lor q_2 \lor q_3) \land (q_1 \lor p_2 \lor p_3) \land (q_1 \lor p_2 \lor q_3) \land (q_1 \lor q_2 \lor p_3) \land (q_1 \lor q_2 \lor q_3))$ s 8 klauzulami
  - Z $((p_1 \land q_1) \lor (p_2 \land q_2) \lor \cdots \lor (p_n \land q_n))$ s n konjunkciami dostaneme $\bigwedge_{x_1 \in \{p_1, q_1\}} \cdots \bigwedge_{x_n \in \{p_n, q_n\}} \bigvee_{i=1}^{n} x_i$ s 2^n klauzulami
- Distribuovanie disjunkcií dovnútra konjunkcií teda môže formulu zväčšiť exponenciálne

CNF – iný prístup

Rovnaká splniteľnosť

- Pri úprave formuly do CNF pre SAT solver *nepotrebujeme*, aby bola výsledná formula s pôvodnou *ekvivalentná*
- Stačí nám oveľa slabšia vlastnosť:

Definícia 3.60

Formuly X a Y sú *rovnako splniteľné* (ekvisplniteľné, equisatisfiable) práve vtedy, keď X je splniteľná vtt Y je splniteľná.

Tvrdenie 3.61

Ak X a Y sú ekvivalentné, sú aj rovnako splniteľné.

Príklad 3.62 (Ekvivalentnosť vs. ekvisplniteľnosť)

Sú $(p \to q)$ a $(p \wedge r)$ rovnako splniteľné? Sú ekvivalentné?

CNF – iný prístup

- Ako by sa dá vyhnúť exponenciálnemu nárastu $X = ((p_1 \land q_1) \lor (p_2 \land q_2) \lor \cdots \lor (p_n \land q_n))$, keď nám stačí nájsť rovnako splniteľnú formulu?
- Označme $X_i = (p_i \land q_i)$.
  - Aký je vzťah medzi X a X_i?
    X je splnená vtt jedna z X_i je splnená.
  - Akými klauzulami to vieme vyjadriť?
    $(X_i \to X)$ pre každé $i \in \{1, \ldots, n\}$ $\quad (\neg X_i \lor X)$
    $(X \to (X_1 \lor \cdots \lor X_n))$ $\quad (\neg X \lor X_1 \lor \cdots \lor X_n)$
  - Aký je vzťah medzi X_i, p_i a q_i?
    X_i je splnená vtt p_i je splnená a q_i je splnená.
  - Akými klauzulami to vieme vyjadriť?
    Pre každé $i \in \{1, \ldots, n\}$:
    $(X_i \to p_i)$ $\quad (\neg X_i \lor p_i)$
    $(X_i \to q_i)$ $\quad (\neg X_i \lor q_i)$
    $((p \land q) \to X_i)$ $\quad (\neg p \lor \neg q \lor X_i)$
  - Koľko klauzúl potrebujeme? $4n + 1$, celkový stupeň CNF $11n + 1$

CNF – iný prístup

Algoritmus CNF_2

1. Zostrojíme vytvárajúci strom pre formulu X a označíme formuly v ňom $X_0, X_1, X_2, \dots$ tak, aby $X_0 = X$.
2. Pre každú formulu X_i, ak $X_i = p$ pre nejakú $p \in \mathcal{V}$, označíme $x_i = p$, inak označíme ako x_i novú výrokovú premennú, ktorá bude „reprezentovať" formulu X_i.
3. Vytvoríme formuly, ktoré popisujú vzťah medzi X_i a jej priamymi podformulami prostredníctvom „reprezentačných" premenných:
   - ak X_i je tvaru $\neg X_j$ pre nejaké X_j, pridáme $(x_i \leftrightarrow \neg x_j)$,
   - ak X_i je tvaru $(X_j \wedge X_k)$, pridáme $(x_i \leftrightarrow (x_j \wedge x_k))$,
   - ak X_i je tvaru $(X_j \vee X_k)$, pridáme $(x_i \leftrightarrow (x_j \vee x_k))$,
   - ak X_i je tvaru $(X_j \rightarrow X_k)$ pridáme $(x_i \leftrightarrow (x_j \rightarrow x_k))$,
4. Pridáme formulu x_0 (chceme aby formula X bola pravdivá).
5. Všetky nové formuly z krokov 3 a 4 prevedieme do CNF (je to jednoduché) a spojíme konjunkciou.

CNF – iný prístup

Korektnosť

Tvrdenie 3.63

Výsledná formula Y algoritmu CNF_2 je v CNF, jej dĺžka je lineárna voči veľkosti X a Y je ekvisplniteľná s X.

Lema 3.64

Ak $X = (A \, c \, B)$ je formula a p, q, $r \in \mathcal{V}$ sa nevyskytujú v X, tak X a $Y = (p \land (p \leftrightarrow (q \, c \, r)) \land (q \leftrightarrow A) \land (r \leftrightarrow B))$ sú ekvisplniteľné.

CNF – iný prístup

Príklad 3.65

$$X_0 = ((a \vee \neg b) \to \neg(c \vee (d \wedge \neg e)))$$

$$X_1 = (a \vee \neg b) \qquad X_2 = \neg(c \vee (d \wedge \neg e))$$

$$a \qquad X_3 = \neg b \qquad X_4 = (c \vee (d \wedge \neg e))$$

$$b \qquad c \qquad X_5 = (d \wedge \neg e)$$

$$d \qquad X_6 = \neg e$$

$$e$$

$$x_0$$

$$(x_0 \leftrightarrow (x_1 \to x_2))$$

$$x_1 \leftrightarrow (a \vee x_3) \quad x_2 \leftrightarrow \neg x_4$$

$$x_3 \leftrightarrow \neg b \quad x_4 \leftrightarrow (c \vee x_5)$$

$$x_5 \leftrightarrow (d \wedge x_6)$$

$$x_6 \leftrightarrow \neg e$$

Dokazovanie ekvivalencie syntakticky vs. sémanticky

- Pomocou substitúcie ekvivalentných formúl vieme dokázať, že dve formuly sú ekvivalentné bez toho, aby sme vyšetrovali všetky ohodnotenia ich výrokových premenných.
- Výhodné pri formulách s veľkým počtom premenných.
- Formulu $X = ((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$ sme upravili do CNF $Y = ((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$ pomocou 12 substitúcií ekvivalentných podformúl.
- Zároveň sme dokázali, že X a Y sú ekvivalentné.
- Na dôkaz ich ekvivalencie tabuľkovou metódou by sme potrebovali vyšetriť 32 prípadov.

Ekvivalencia syntakticky vs. sémanticky

- Tabuľková metóda je **sémantická**
  - využíva ohodnotenia výrokových premenných a spĺňanie formúl ohodnoteniami
- Substitúcie ekvivalentných formúl sú **syntaktickou** metódou
  - pracujú iba s postupnosťami symbolov, nie s ohodnoteniami
- Navyše sú **deduktívnou** metódou
  - odvodíme *iba* ekvivalentné formuly
- Má dve pomerne samozrejmé pravidlá:
  Eulerovské *pravidlo* nahradenia ekvivalentnej formuly ekvivalentnou a tranzitivita ekvivalencie

  $$\frac{A \Leftrightarrow B}{X \Leftrightarrow X[A|B]} \qquad \frac{A \Leftrightarrow B \quad B \Leftrightarrow C}{A \Leftrightarrow C}$$
- Veľa (nevýhoda) *schém axióm* — distributívnosť, de Morgan, ...
  - vytvoríme z nich nekonečne veľa axióm, základných ekvival.
- Postupnosť substitúcií slúži ako **dôkaz**:
  Každý (aj program), kto pozná pravidlo a axiómy ľahko mechanicky overí, že postupnosť je správna

Dokazovanie vyplývania a tautológií syntakticky vs. sémanticky — kalkuly

- Ak začneme nejakou formulou a budeme substituovať ekvivalentné podformuly, dostávame postupne rôzne formuly, ktoré sú ale stále ekvivalentné s pôvodnou formulou.
- Čo keby sme začali s tautológiou?
  Dostávame stále tautológie.
- Tautológie a vyplývanie formúl z množín sme doteraz dokazovali sémanticky — vyšetrovaním všetkých ohodnotení.
- Na tento účel ale existujú aj syntaktické metódy — *kalkuly*.
- Ukážeme si tri kalkuly:
  hilbertovský — klasický, lineárny, pomerne ťažkopádny
  tablový — modernejší, stromový, prirodzenejší
  rezolvenciu — strojový
- Pokračovanie nabudúce. . .

Literatúra

Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994. ISBN 978-0-201-53082-7.

Raymond M. Smullyan. *Logika prvého rádu*. Alfa, 1979. Z angl. orig. *First-Order Logic*, Berlin-Heidelberg: Springer-Verlag, 1968 preložil Svätoslav Mathé.