TIN – cvičení 6 – Logika 24. 11. 2023

- Převod formule ve výr. logice do NNF ($\neg, \vee, \wedge$ + $\neg$ jen v literálech)
  - postup:
    1. odstraníme "nežádoucí" spojky
    2. De Morgan: $\neg(a \overset{\vee}{\wedge} b) \Leftrightarrow \neg a \overset{\wedge}{\vee} \neg b$

- $\neg(x \Leftrightarrow \neg(x \wedge y)) \Leftrightarrow$

$\neg((x \rightarrow \neg(x \wedge y)) \wedge (\neg(x \wedge y) \rightarrow x)) \Leftrightarrow$ fáze 1

$\neg((\neg x \vee \neg(x \wedge y)) \wedge ((x \wedge y) \vee x)) \Leftrightarrow$

$\neg(\neg x \vee \neg(x \wedge y)) \vee \neg((x \wedge y) \vee x) \Leftrightarrow$

$(x \wedge (x \wedge y)) \vee (\neg(x \wedge y) \wedge \neg x) \Leftrightarrow$ fáze 2

$(x \wedge (x \wedge y)) \vee ((\neg x \vee \neg y) \wedge \neg x) \Leftrightarrow$

$(x \wedge y) \vee \neg x$ zjednodušení nad rámec převodu

- Jaká je velikost NNF(φ) vůči velikosti φ
  - exponenciálně větší kvůli rozepsání zanořených "$\Leftrightarrow$"

- velikost roste exponenciálně kvůli zdvojnásobení u "$\Leftrightarrow$", které mohou být zanořeny.
- Jaká je velikost NNF(φ) vůči φ v nejhorším případě, pokud φ neobsahuje "$\Leftrightarrow$" (ani xor...)
  - nárůst je lineární.
- Dokážeme pomocí indukce, že nárůst velikosti NNF(φ) vůči φ obsahujícím jen spojky $\vee, \wedge, \neg$ je lineární:
  - Definujeme přesně proceduru NNF(φ) rekurzivně takto:

    if φ je v NNF, return φ.
    else if φ je $(\varphi_1 \overset{\wedge}{\vee} \varphi_2)$, return $(NNF(\varphi_1) \overset{\wedge}{\vee} NNF(\varphi_2))$
    else if φ je $\neg(\varphi_1 \overset{\wedge}{\vee} \varphi_2)$, return $(NNF(\neg\varphi_1) \overset{\vee}{\wedge} NNF(\neg\varphi_2))$
  - Dokážeme indukcí, že $|NNF(\varphi)| \leq 2|\varphi|$ pro φ v dané podobě (tedy pouze spojky $\wedge, \vee, \neg$), a to indukcí podle počtu $\vee/\wedge$, označeného $\underline{n}$:
    - bázový případ $n=0$:
      - pak φ je literál a $NNF(\varphi) = \varphi$.

- <u>indukční předpoklad</u>
  - předpokládejme, že tvrzení platí pro všechny formule s max $n = k$, $k \geq 0$, $\wedge / \vee$.
- <u>indukční krok</u>: ukážeme, že pak tvrzení platí pro formule φ s $n = k+1$ $\wedge / \vee$:
  - Protože $n = k+1$, je $n \geq 1$. Nastávají 4 případy:

    a) $\varphi = (\varphi_1 \wedge \varphi_2)$ pro nějaké φ_1, φ_2.
    - $|NNF(\varphi)| = |NNF(\varphi_1)| + |NNF(\varphi_2)| + 3$
    - dle ind. předp.:
      $|NNF(\varphi)| \leq 2 \cdot |\varphi_1| + 2 \cdot |\varphi_2| + 3$
    - $|\varphi| = |(\varphi_1 \wedge \varphi_2)| = |\varphi_1| + |\varphi_2| + 3$
    - Tedy $|NNF(\varphi)| < 2 \cdot |\varphi|$

    b) $\varphi = (\varphi_1 \vee \varphi_2)$ — analogie

    c) $\varphi = \neg(\varphi_1 \wedge \varphi_2)$ pro nějaké φ_1, φ_2.
    - $|NN\varphi(\varphi)| = |NNF(\neg\varphi_1)| + |NNF(\neg\varphi_2)| + 3$

- dle ind. předp.:

$$|NNF(\varphi)| \leq 2\cdot|\neg\varphi_1| + 2\cdot|\neg\varphi_2| + 3 =$$
$$= 2\cdot(1+|\varphi_1|) + 2\cdot(1+|\varphi_2|) + 3 =$$
$$= 2\cdot|\varphi_1| + 2\cdot|\varphi_2| + 7$$

- $|\neg(\varphi_1 \wedge \varphi_2)| = |\varphi_1| + |\varphi_2| + 4$
- tedy $|NNF(\varphi)| < 2\cdot|\varphi|$.

d) $\varphi = \neg(\varphi_1 \vee \varphi_2)$ – analogie $\square$

- Chybí pokrytí případu $NNF(\varphi_1 \to \varphi_2)$.
  Ale $NNF(\varphi_1 \to \varphi_2) = NNF(\neg(\varphi_1) \vee \varphi_2) = (NNF(\neg\varphi_1) \vee NNF(\varphi_2))$
  Pak $|NNF(\varphi_1 \to \varphi_2)| = 3 + |NNF(\neg\varphi_1)| + |NNF(\varphi_2)|$
  - stále lineární.

- Znamená výše uvedené, že $NNF(.)$ pracuje v lineárním prostoru a čase?
  - prostor: - NNF opravdu pracuje v lineárním prostoru, ale výše uvedený důkaz to neukazuje – jen jen dává do relace velikost in/out. Funkce by mohla alokovat pomocnou paměť.

- ~~času~~ : nelze usuzovat – fce může opakovaně procházet stejnou paměť!

- <u>Převod do DNF</u> (na nejvyšší úrovni „$\vee$“ – disjunkce konjunkcí literálů)
  - postup: 1. převod do NNF
    2. roznásobení / rozsčítání!
       - $(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$
       - $(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$
  - $((x \wedge y) \vee z) \wedge (x \vee \neg y)$ – již v NNF

$\Leftrightarrow ((x \vee z) \wedge (y \vee z)) \wedge (x \vee \neg y)$ [náhodou v CNF]

$\Leftrightarrow (x \wedge y \wedge \cancel{x}) \vee \cancel{(x \wedge y \wedge \neg y)} \vee (x \wedge z \wedge \cancel{x}) \vee \cancel{(x \wedge z \wedge \neg y)}$
$\vee \cancel{(z \wedge y \wedge x)} \vee \cancel{(z \wedge y \wedge \neg y)} \vee \cancel{(z \wedge z \wedge x)} \vee (z \wedge \cancel{z} \wedge \neg y)$ DNF

zjednodušení (volitelné)

červeně: – eliminace redundance („x“)
– eliminace sporných podformulí („—“)
– eliminace pokrytých formulí („~~“)

- DNF umožňuje velmi jednoduše řešit SAT problém (typický NP úplný problém) – stačí najít jednu bezespornou konjunkci? Není P = NP?

  NE: převod do DNF je exponenciální!

- Převod do CNF – tu používají SAT solvery.
  - lze analogicky – ale nepraktické: exp. explose již při předzpracování!
  - alternativa – Tseytinova transformace (lineární)

$$(\underbrace{(\underbrace{x \vee y}_{x_3}) \wedge z}_{x_4}) \vee (\underbrace{x \wedge \underbrace{\neg y}_{x_1}}_{x_2})) \quad \text{— celé: } x_5$$

konst. velikost: $(x_1 \Leftrightarrow \neg y) \wedge$ → $(x_1 \Rightarrow \neg y) \wedge (\neg y \Rightarrow x_1)$ (konst. vel.) → $(\neg x_1 \vee \neg y) \wedge (y \vee x_1)$

$(x_2 \Leftrightarrow x \wedge x_1) \wedge$

$(x_3 \Leftrightarrow x \vee y) \wedge$

$(x_4 \Leftrightarrow x_3 \wedge z) \wedge$

$(x_5 \Leftrightarrow x_4 \vee x_2) \wedge$

x_5

$\wedge \; \vdots$ $\qquad \wedge \; \vdots$

lineární velikost $\qquad$ lineární velikost $\qquad$ lineární velikost.

- <u>Predikátová logika s rovností – jazyk a interpretace</u>

- Mějme formuli φ : $\forall x\,(E(x) \to M(x,a))$
- zapište signaturu jazyka této formule :

konvence:
- x, y … proměnné
- a, b … konstanty.

$$\langle \{ a_{/0} \} , \{ E_{/1} , M_{/2} \} \rangle$$

f-ční symboly — predikátové symboly

- mějme interpretaci $I = (D_I , \alpha_I)$

└ doména, neprázdná

$D_I = \{1, 3, 5, 15\}$

$\alpha_I(a) = 1$ // nulární fce $a() = 1$

$\alpha_I(E) = \emptyset$ // prázdná unární relace – neplatí nikde

$\alpha_I(M) = \{ (1,1), (3,1), (15,5) \dots \}$

// (x,y) je v relaci M, jestliže x je násobek y.

- Platí, že $I \models \varphi$? Je I modelem φ ?

ANO: E nikdy neplatí a tudíž "$\to$" platí vždy.

- Platí také, že $I \models \exists y.\, E(y)$?

$\overline{\text{NE}}$. E nikde neplatí!

- Má formule $\varphi: \exists x\,(P(x) \wedge \forall y\,(\neg(f(x,y) = f(y,x))))$ model?

  - $\exists x$ lze splnit – doména je neprázdná!
  - Pak ale lze volit $x = y$ a dostaneme, že $f(x,x) \neq f(x,x)$ – nelze, nemá model!

- Co se stane z hlediska existence modelu, pokud vynecháme "$\neg$"

  - Pak model existuje, např.:

$D_I = \{1\}$

$\alpha_I(P) = \{1\}$

$\alpha_I(f) = \{((1,1),1)\}$

$(1,1) \mapsto 1$

- <u>Teorie</u> : mn-a vět (uzavřených formulí) (speciální axiomy)
- $M \models T$: interpretace M je modelem T : $\forall \varphi \in T : M \models \varphi$
- $T \models \varphi$: φ je důsledkem T : všechny modely T jsou modely φ.
- $T \vdash \varphi$: φ je dokazatelná z T
- <u>bezesporná teorie</u> : neexistuje φ : $T \vdash \varphi \wedge T \vdash \neg\varphi$
    - bezesporná teorie $T \Leftrightarrow T$ má model.
- <u>úplná teorie T</u> : pro každé φ : $T \vdash \varphi \vee T \vdash \neg\varphi$.
    - T je úplná $\Leftrightarrow \neg\exists$ modely M, M' teorie T a formule φ :
      $M \models \varphi \wedge M' \models \neg\varphi$
    - spec. případy: - T má právě 1 model $\Rightarrow T$ je úplná
      - T je sporná $\Rightarrow T$ je úplná (nemá modely).
- Je teorie $T = \{ \forall x \forall y ((f(x) = 0 \wedge f(y) = 0) \Rightarrow x = y), \neg\exists x (f(x) \neq 0) \}$ bezesporná, úplná ?

- 1. axiom: max 1. prvek se mapuje na 0
  2. axiom: všechny se mapují na 0

  $\Big\}$ doména musí být neprázdná a tedy má právě 1 prvek. (*)

- sestavíme interpretaci:

  $M: D_M = \{a\}$

  $\alpha_M(f) = \{a \mapsto a\}$

  $\alpha_M(0) = a$

- $M \models T$ — bezesporná teorie, protože má model.
- Jedná se o jedinou možnou interpretaci vzhledem k (*) — až na pojmenování! — úplná.

- Uvažme teorii $T' = \{ \forall x \forall y \, ((f(x)=0 \wedge f(y)=0) \Rightarrow x=y),$
  $\exists x \, (f(x) \neq 0) \}$.

Je bezesporná, úplná?

- Model M teorie T výše není modelem T'.
- M': $D_{M'} = \{a, b\}$

  $\alpha_{M'}(0) = a$

  $\alpha_{M'}(f) = \{a \mapsto a, b \mapsto b\}$

  M'': $D_{M''} = \{a, b\}$

  $\alpha_{M''}(0) = a$

  $\alpha_{M''}(f) = \{a \mapsto b, b \mapsto b\}$

$M' \models T'$ — T' je bezesporná | $M'' \models T'$

Uvažme formuli φ: $\forall x : f(x) = x$.

Pak $M' \models \varphi$, ale $M'' \models \neg\varphi$. → T' není úplná!

- Uvažme $T'' = \{ \forall x (f(x) = 0 \rightarrow x = 0),$
  $\exists x (f(x) = 0),$
  $f(0) \neq 0 \}$.

<u>Je T'' bezesporná, úplná?</u>

- 1. axiom: Jen 0 se mapuje na 0.
  2. axiom: někdo se mapuje na 0. } tedy 0 se mapuje na 0.
  3. axiom: 0 se ~~...~~ nemapuje na 0 — SPOR!

  → je sporná
  → je úplná.

- <u>Rozhodnutelná teorie</u> T: jazyk $\{ \varphi \mid T \models \varphi \}$ je rozhodnutelný TS

  - <u>platí</u>: je-li T úplná $\Rightarrow$ T je rozhodnutelná?

NE: – TS lze generovat lexikografický sekvence znaků nad jazyky formulí s vhodným oddělovačem a kontrolovat:

- zda jde o sekvenci korektních formulí,
- zda je na konci $\varphi / \neg\varphi$,
- zda je n-tá formule odvozena z předchozích.

– ALE není-li n-tá formule odvozena, TS nemusí být schopen posoudit, zda tato formule je axiom!

– platí ale: T je úplná $\wedge$ T je efektivní $\Rightarrow$ T je rozhodnutelná

jazyk $\{\varphi \mid \varphi$ je axiom $T\}$ je rozhodnutelný.

– pokud je mn-a axiomů konečná — je efektivní.

– Opačná implikace neplatí — $\exists$ rozhodnutelné teorie, které nejsou úplné (např. některé ~~[illegible]~~ teorie s konečným počtem modelů).