הסקה אוטומטית ושימושיה -- דף נוסחאות

- המחלקה למדעי המחשב
- מרצה: ד"ר יוני זוהר

1 שיטת צייטין

תהי נוסחה A. ניצור נוסחה B כדלהלן:
עבור כל תת נוסחה C של A נגדיר משתנה חדש p_C. נגדיר את B להיות הנוסחה $p_A \wedge \bigwedge_{C \in sub(A)} E(C)$, כאשר $sub\,(A)$ היא קבוצת תתי הנוסחאות של A ו- $E(C)$ מוגדרת כך:

$$E(C) = \begin{cases} CNF(p_C \leftrightarrow C) & C \text{ } is \text{ } variable \\ CNF(p_C \leftrightarrow true) & C \text{ } is \text{ } true \\ CNF(p_C \leftrightarrow false) & C \text{ } is \text{ } false \\ CNF(p_C \leftrightarrow \neg p_D) & C = \neg D \\ CNF(p_C \leftrightarrow (p_{C_1} \wedge p_{C_2})) & C = C_1 \wedge C_2 \\ CNF(p_C \leftrightarrow (p_{C_1} \vee p_{C_2})) & C = C_1 \vee C_2 \\ CNF(p_C \leftrightarrow (p_{C_1} \rightarrow p_{C_2})) & C = C_1 \rightarrow C_2 \\ CNF(p_C \leftrightarrow (p_{C_1} \leftrightarrow p_{C_2})) & C = C_1 \leftrightarrow C_2 \end{cases}$$

$$CNF(p \leftrightarrow C) = \begin{cases} (\neg p_C \vee C) \wedge (\neg C \vee p_C) & C \text{ } is \text{ } variable \\ (\neg p_C \vee true) \wedge (false \vee p_C) & C \text{ } is \text{ } true \\ (\neg p_C \vee false) \wedge (true \vee p_C) & C \text{ } is \text{ } false \\ (\neg p_C \vee \neg P_D) \wedge (p_D \vee p_C) & C \text{ } is \text{ } \neg D \\ (\neg p_C \vee p_{C_1}) \wedge (\neg p_C \vee p_{C_2}) \wedge (\neg p_{C_1} \vee \neg p_{C_2} \vee p_C) & C \text{ } is \text{ } C_1 \wedge C_2 \\ (\neg p_C \vee p_{C_1} \vee p_{C_2}) \wedge (\neg p_{C_1} \vee p_C) \wedge (\neg p_{C_2} \vee p_C) & C \text{ } is \text{ } C_1 \vee C_2 \\ (\neg p_C \vee \neg p_{C_1} \vee p_{C_2}) \wedge (p_{C_1} \vee p_C) \wedge (\neg p_{C_2} \vee p_C) & C \text{ } is \text{ } C_1 \rightarrow C_2 \\ (\neg p_C \vee \neg p_{C_1} \vee p_{C_2}) \wedge (\neg p_C \vee p_{C_1} \vee \neg p_{C_2}) \wedge & C \text{ } is \text{ } C_1 \leftrightarrow C_2 \\ (p_C \vee \neg p_{C_1} \vee \neg p_{C_2}) \wedge (p_C \vee p_{C_1} \vee p_{C_2}) & \end{cases}$$

2 תחשיבים

1. תחשיב $DPLL$:
   (א) כלל $Decide$: $\dfrac{(M,F,D)}{(M :: \ell, F, D \cup \{\ell\})}$ כאשר $var(\ell)$ מופיע ב-F אך $var(\ell)$ לא מוגדר ב-v_M.
   (ב) כלל $Fail$: $\dfrac{(M,F,D)}{Fail}$ כאשר $D = \emptyset$ ויש פסוקית C ב-F כך ש- $v_M \models \neg C$.
   (ג) כלל BT : $\dfrac{(M :: \ell :: N, F, D)}{(M :: \bar{\ell}, F, D \setminus \{\ell\})}$ כאשר $\ell \in D$, ויש פסוקית C ב-F כך ש- $v_{M::\ell::N} \models \neg C$ ו-$N \cap D = \emptyset$.
   (ד) כלל UP: $\dfrac{(M,F,D)}{(M :: \ell, F, D)}$ כאשר יש C כך ש-$C \vee \ell$ היא פסוקית ב-F, $var(\ell)$ לא מוגדר ב-v_M ו-$v_M \models \neg C$.
2. כלל BJ: $\dfrac{\langle M\ell N, F, D\rangle}{\langle M\ell', F, D \cap M\rangle}$ כאשר:

(א) $\ell \in D$
(ב) יש פסוקית C ב-F כך ש- $v_{M\ell N} \models \neg C$
(ג) יש פסוקית C' וליטרל ℓ' כך ש:
i. $F \vdash C' \vee \ell'$ (כלומר: כל השמה שמספקת את F מספקת גם את $C' \vee \ell'$)
ii. $v_M \models \neg C'$
iii. $var\left(\ell'\right)$ לא מופיע ב-M אך כן מופיע ב-F

3. תחשיב CC:

(א) כלל $Top-Level$: $\dfrac{(M,F)}{(M \setminus \{X,Y\} \cup \{X \cup Y\}, F)}$ אם $X, Y \in M$ ויש שמות עצם $t \in X$, $s \in Y$ כך ש-$t = s \in F$.

(ב) כלל $Congruence$: $\dfrac{(M,F)}{(M \setminus \{X,Y\} \cup \{X \cup Y\}, F)}$ אם $X, Y \in M$ וקיימים סימן פונקציה f, קבוצה $Z \in M$, ומשתנים $z, z' \in Z$ כך ש- $f(z) \in X$ ו-$f(z') \in Y$.

(ג) כלל $Fail$: $\dfrac{(M,F)}{Fail}$ אם יש $X \in M$ ו-$t_1, t_2 \in X$ כך ש-$t_1 \neq t_2 \in F$.

4. תחשיב $DPLL(UF)$ מתקבל מ-$DPLL$ על ידי הוספת כלל ההיסק הבא:

(א) כלל UF: $\dfrac{(M,F,D)}{([], F \wedge \overline{\varphi_M}, \emptyset)}$ כאשר:
i. (M,F,D) רוויה ביחס $DPLL$
ii. $tr^{-1}(\varphi_M)$ אינה ספיקה על ידי אף Σ-מבנה
iii. tr היא פונקציה חח"ע ועל מנוסחאות בלוגיקה מסדר ראשון לנוסחאות פסוקיות.
iv. אם $M = [\ell_1 \ldots \ell_n]$ אז $\varphi_M = \ell_1 \wedge \ldots \wedge \ell_n$ ו-$\overline{\varphi_M} = \overline{\ell_1} \vee \ldots \vee \overline{\ell_n}$.

5. תחשיב A (כשמפעילים את כלל $reduce$ בתוך גזירה, יש לבחור את אחד משני הצדדים של $||$):

(א) sat: $\dfrac{X}{sat}$ אם הסימן w לא מופיע ב-X ו-X ספיקה.

(ב) $unsat$: $\dfrac{X}{unsat}$ אם הסימן w לא מופיע ב-X ו-X ספיקה.

(ג) $reduce$: $\dfrac{X}{Y \cup \{i=j\} \| Z \cup \{i \neq j\}}$ אם יש ש"ע מהצורה $r(w(a,i,e),j)$ ב-X, Y מתקבל מ-X על ידי החלפת כל המופעים של $r(w(a,i,e),j)$ ב-e ו- Z מתקבל מ-X על ידי החלפת כל המופעים של $r(w(a,i,e),j)$ ב-$r(a,j)$.

3 סיגנטורות

1. Σ_{LA} היא הסיגנטורה $\left(F_{\Sigma_{LA}}, P_{\Sigma_{LA}}, a_{\Sigma_{LA}}\right)$ כך ש:

(א) $F_{\Sigma_{LA}} = \{+, -, 0, 1\}$
(ב) $P_{\Sigma_{LA}} = \{\geq\}$
(ג) $a_{\Sigma_{LA}}(+) = 2, a_{\Sigma_{LA}}(-) = 1, a_{\Sigma_{LA}}(0) = 0, a_{\Sigma_{LA}}(1) = 0, a_{\Sigma_{LA}}(\geq) = 2$

2. $\Sigma_{BV} = (S_{BV}, P_{BV}, F_{BV}, a_{BV})$ כך ש:

(א) $S_{BV} = \{BV_n \mid n \in \mathbb{N}^+\}$
(ב) $P_{BV} = \{<_n \mid n \in \mathbb{N}^+\}$
(ג) לכל $n \in \mathbb{N}^+$ הסימנים הבאים מופיעים ב-F_{BV}: $\sim_n, +_n, \cdot_n, <<_n, >>_n, \&_n, |_n, \oplus_n$
(ד) לכל n ולכל מחרוזת ביטים s באורך n, $s \in F_{BV}$.
(ה) אין עוד סימנים ב-F_{BV}.
(ו) לכל n: $a_{\Sigma_{BV}}(\sim_n) = (BV_n, BV_n)$. $a_{\Sigma_{BV}}(s) = BV_n$ לכל s באורך n.
(ז) $a_{\Sigma_{BV}}(<_n) = (BV_n, BV_n)$, $a_{\Sigma_{BV}}(op_n) = (BV_n, BV_n, BV_n)$ לכל $op_n \in F_{BV}$ חוץ מ-$\sim_n$ והקבועים.

3. Σ_A היא הסיגנטורה $\left(S_{\Sigma_A}, F_{\Sigma_A}, P_{\Sigma_A}, a_{\Sigma_A}\right)$ בה $S_{\Sigma_A} = \{A, I, E\}$, $F_{\Sigma_A} = \{r, w\}$, $P_{\Sigma_A} = \emptyset$ ו-$a_{\Sigma_A}(r) = (A, I, E)$, $a_{\Sigma_A}(w) = (A, I, E, A)$.

4 ספיקות

1. מבנה Σ_{LA} v נקרא מבנה LRA אם:
   (א) $D_v = \mathbb{R}$
   (ב) כל הסימנים מפורשים כצפוי
2. מבנה Σ_{LA} v נקרא מבנה LIA אם:
   (א) $D_v = \mathbb{Z}$
   (ב) כל הסימנים מפורשים כצפוי
3. מבנה Σ_{BV} $v = (D_v, I_v)$ נקרא מבנה BV אם לכל לכל $n \in \mathbb{N}^+$:
   (א) $D_v\left(BV_n\right)$ היא קבוצת כל רשימות הביטים באורך n.
   (ב) לכל שני ביט-וקטורים a, b בגודל n: $(a, b) \in I_v\left(<_n\right)$ אם ורק אם $N\left(a\right) < N\left(b\right)$, כאשר N ממפה כל ביט-וקטור למספר הטבעי המתאים לו בייצוג בינארי.
   (ג) לכל ביט-וקטור a, $I_v\left(a\right) = a$
   (ד) לכל ביט-וקטור a, $I_v\left(\sim_n\right)\left(a\right)$ מתקבל מ-a על ידי החלפת כל האפסים ב-1 וכל ה-1ים באפסים.
   (ה) לכל ביט-וקטורים a, b באורך n:
   (ו) $+_n$ מפורש כחיבור מודולו 2^n, ובאופן דומה $-_n$ ו-$\cdot_n$.
   (ז) $I_v\left(<<_n\right)\left(a, b\right)$ מתקבל מ-a על ידי מחיקת $N\left(b\right)$ איבריו השמאליים והוספת $N\left(b\right)$ אפסים מצד ימין.
   (ח) $I_v\left(>>_n\right)\left(a, b\right)$ מתקבל מ-a על ידי מחיקת $N\left(b\right)$ איבריו הימניים והוספת $N\left(b\right)$ אפסים מצד שמאל.
   (ט) $I_v\left(\&_n\right)\left(a, b\right)$ הוא ביט-וקטור כך שבמקום ה-i יש 1 אם ורק אם במקום ה-i של a יש 1 וגם במקום ה-i של b. אחרת, 0. באופן דומה $\oplus_n$, $|_n$.
4. Σ_A-מבנה v נקרא מבנה A אם v מספק את הנוסחאות הבאות:

$$\begin{aligned} &row1 && \forall a \forall e \forall i. r\left(w\left(a, i, e\right), i\right) = e \\ &row2 && \forall a \forall e \forall i \forall j. i \neq j \rightarrow r\left(w\left(a, i, e\right), j\right) = r\left(a, j\right) \\ &ext && \forall a \forall a'. a \neq a' \rightarrow \exists i. r\left(a, i\right) \neq r\left(a', i\right) \end{aligned}$$

   כאשר a, a' הם משתנים מסוג A, i, j משתנים מסוג I ו-e משתנה מסוג E.
5. נוסחה נקראת "ספיקה" אם היא יש מבנה כלשהו שמספק אותה. עבור $X \in \{LIA, LRA, BV, A\}$: נוסחה נקראת "$X$-ספיקה" אם יש "מבנה X" שמספק אותה.