הסקה אוטומטית ושימושיה -- דף נוסחאות

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 $sub\left(A\right)$ היא קבוצת תתי הנוסחאות של A ו- $E(C)$ מוגדרת כך:

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

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

2 שיטוח קוביות בסיגנטורות פונקציונאליות

1. $\dfrac{s = t \in \varphi}{X \setminus \{s = t\} \cup \{x_s = t, x_s = s\}}$ אם s אינו משתנה
2. $\dfrac{s \neq t \in \varphi}{X \setminus \{s \neq t\} \cup \{x_s \neq t, x_s = s\}}$ אם s אינו משתנה
3. $\dfrac{x \neq t \in \varphi}{X \setminus \{x \neq t\} \cup \{x \neq x_t, x_t = t\}}$ אם t אינו משתנה
4. $\dfrac{x = f\left(s_1, \ldots, s_n\right) \in \varphi}{X \setminus \{x = f\left(s_1, \ldots, s_n\right)\} \cup \{x = f\left(s_1, \ldots, x_{s_i}, \ldots, s_n\right), x_{s_i} = s_i\}}$ אם יש s_i שאינו משתנה

3 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 $Fail$: $\frac{(M,F,D)}{Fail}$ כאשר $D=\emptyset$ ויש פסוקית C ב-F כך ש-$v_M \models \neg C$.

(ג) כלל BT : $\frac{(M::\ell::N,F,D)}{(M::\overline{\ell},F,D\setminus\{\ell\})}$ 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: $\frac{(M,F,D)}{(M::\ell,F,D)}$ 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. תחשיב $CDCL$:

(א) כלל $Decide$: $\frac{(M,F,D,K)}{(M::\ell,F,D\cup\{\ell\},K)}$ כאשר $var(\ell)$ מופיע ב-F אך $var(\ell)$ לא מוגדר ב-v_M.

(ב) כלל $Fail$: $\frac{(M,F,D,K)}{Fail}$ כאשר $D=\emptyset$, $K\neq no$, ויש פסוקית C ב-F כך ש-$v_M\models\neg C$.

(ג) כלל $UP\ UnitPropagate$: $\frac{(M,F,D,K)}{(M::\ell,F,D,K)}$ כאשר יש C כך ש-$C\vee\ell$ היא פסוקית ב-F, $var(\ell)$ לא מוגדר ב-v_M ו-$v_M\models\neg C$.

(ד) כלל $Conflict$: $\frac{(M,F,D,no)}{(M,F,D,C)}$ כאשר יש $C\in F$ כך שלכל $\ell\in C$, $\overline{\ell}\in M$.

(ה) כלל $Explain$: $\frac{(M\overline{\ell}N,F,D,K)}{(M\overline{\ell}N,F,D,(K\setminus\{\ell\})\cup C)}$ כאשר $\ell\in K$ כך ש-$C\vee\overline{\ell}\in F$ ולכל $c\in C$, $\overline{c}\in M$.

(ו) כלל $Backjump$: $\frac{(M\ell_0N,F,D,K)}{(M\ell,F,D\setminus(N\cup\{\ell_0\}),no)}$ כאשר $\ell_0\in D$, $\ell\in K$, $\overline{\ell}\in N\cup\{\ell_0\}$ ולכל $c\in K\setminus\{\ell\}$, $\overline{c}\in M$.

(ז) כלל $Learn$: $\frac{(M,F,D,K)}{(M,F\cup\{K\},D,K)}$ $K\notin F$.

(ח) כלל $Forget$: $\frac{(M,F\cup\{C\},D,K)}{(M,F,D,K)}$ אם $K=no$ וכל השמה שמספקת את F מספקת את C.

(ט) כלל $restart$: $\frac{(M,F,D,K)}{([],F,\{\},no)}$

3. תחשיב CC:

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

(ב) כלל $Congruence$: $\frac{(M,F)}{(M\setminus\{X,Y\}\cup\{X\cup Y\},F)}$ 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 $Fail$: $\frac{(M,F)}{Fail}$ 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: $\frac{(M,F,D)}{([],F\wedge\overline{\varphi_M},\emptyset)}$ 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 $M=[\ell_1\dots\ell_n]$ אז $\varphi_M=\ell_1\wedge\dots\wedge\ell_n$ ו-$\overline{\varphi_M}=\overline{\ell_1}\vee\dots\vee\overline{\ell_n}$.

5. תחשיב A:

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

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

(ג) $reduce$: $\frac{X}{Y\cup\{i=j\}\,\|\,Z\cup\{i\neq j\}}$ 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-$r(a,j)$.

4 סיגנטורות

1. $\Sigma_{BV} = (S_{BV}, P_{BV}, F_{BV}, a_{BV})$ 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 $n \in \mathbb{N}^+$ ולכל מחרוזת ביטים s באורך n, $s \in F_{BV}$.
   (ה) אין עוד סימנים ב-F_{BV}.
   (ו) לכל $n \in \mathbb{N}^+$: $a_{\Sigma_{BV}}(\sim_n) = (BV_n, BV_n)$. $a_{\Sigma_{BV}}(s) = BV_n$ לכל s באורך n, $a_{\Sigma_{BV}}(<_n) = (BV_n, BV_n)$, ו-$a_{\Sigma_{BV}}(op_n) = (BV_n, BV_n, BV_n)$ לכל $op_n \in F_{BV}$ חוץ מ-$\sim_n$ והקבועים.

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

5 ספיקות

1. מבנה Σ_{BV} $v = (D_v, I_v)$ נקרא מבנה BV אם לכל $n \in \mathbb{N}^+$:
   (א) $D_v(BV_n)$ היא קבוצת כל הביט-וקטורים באורך n.
   (ב) לכל שני ביט-וקטורים a, b בגודל n: $(a, b) \in I_v(<_n)$ אם ורק אם $N(a) < N(b)$, כאשר N ממפה כל ביט-וקטור למספר הטבעי המתאים לו בייצוג בינארי.
   (ג) לכל ביט-וקטור a, $I_v(a) = a$
   (ד) לכל ביט-וקטור a, $I_v(\sim_n)(a)$ 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 $\cdot_n$.
   (ז) $I_v(<<_n)(a, b)$ מתקבל מ-a על ידי מחיקת $N(b)$ איבריו השמאליים והוספת $N(b)$ אפסים מצד ימין.
   (ח) $I_v(>>_n)(a, b)$ מתקבל מ-a על ידי מחיקת $N(b)$ איבריו הימניים והוספת $N(b)$ אפסים מצד שמאל.
   (ט) $I_v(\&_n)(a, b)$ 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 $|_n, \oplus_n$.

2. Σ_A-מבנה v נקרא מבנה A אם v מספק את הנוסחאות הבאות:

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

   כאשר a, a' הם משתנים מסוג A, i, j משתנים מסוג I ו-e משתנה מסוג E.

3. נוסחה נקראת "ספיקה" אם יש מבנה כלשהו שמספק אותה. עבור $X \in \{BV, A\}$: נוסחה נקראת "X-ספיקה" אם יש "מבנה X" שמספק אותה.

6 $Bit - blasting$

תהי נוסחה φ ב-Σ_{BV} ונניח שהיא קוביה שטוחה.

1. לכל אטום של φ נתאים אטום בוליאני p_φ.

2. לכל ש"ע t ב-Σ_{BV} מסוג BV_n נתאים n אטומים בוליאנים $p_{t,1}, \ldots, p_{t,n}$.

נסמן ב-$lit^+(\varphi)$ את כל הליטרלים החיוביים שמופיעים ב-φ וב-$lit^-(\varphi)$ את השליליים. לכל ליטרל שלילי ℓ ב-φ נסמן ב-ℓ^{-1} את האטום שמופיע בו. נסמן ב-$at(\varphi)$ את כל האטומים שמופיעים ב-φ וב-$tr(\varphi)$ את כל שמות העצם שמופיעים ב-φ.

$$B(\varphi) = \left(\bigwedge_{\ell \in lit^+(\varphi)} p_\ell\right) \wedge \left(\bigwedge_{\ell \in lit^-(\varphi)} \neg p_{\ell^{-1}}\right) \wedge \left(\bigwedge_{\psi \in at(\varphi)} C(\psi)\right) \left(\bigwedge_{t \in tr(\varphi)} C(t)\right)$$

כך ש-C מוגדרת כך:

1. $C(x = t) = p_{x=t} \leftrightarrow \bigwedge_{i=1}^{n} p_{x,i} \leftrightarrow p_{t,i}$ כאשר x, t הם מסוג BV_n.

2. $C(x) = true$ כאשר x הוא משתנה
3. $C(s) = \bigwedge_{i=1}^{n} p_{s,i} \leftrightarrow s_i$ כאשר s קבוע באורך n ו-s_i הוא האיבר ה-i שלו (מזהים 0 עם $false$ ו-1 עם $true$)
4. $C(\sim_n x) = \bigwedge_{i=1}^{n} p_{\sim_n x,i} \leftrightarrow \neg p_{x,i}$
5. $C(x \&_n y) = \bigwedge_{i=1}^{n} (p_{x\&_n y,i} \leftrightarrow (p_{x,i} \wedge p_{y,i}))$
6. $C(x|_n y) = \bigwedge_{i=1}^{n} \left(p_{x|_n y,i} \leftrightarrow (p_{x,i} \vee p_{y,i})\right)$
7. $C(x +_n y) = \bigwedge_{i=1}^{n} (p_{x+_n y,i} \leftrightarrow \pi_0 (add(x, y, 000\ldots 0))_i)$ כאשר:
   (א) $\pi_0((a, b)) = a$
   (ב) $add(x, y, cin) = (result, cout)$ כך ש:
      i. $result_i = sum(p_{x,i}, p_{y,i}, c_i)$ לכל $0 \leq i \leq n$
      ii. $cout = c_n$
      iii. $c_0 = cin$ ולכל $0 < i \leq n$, $c_i = carry(p_{x,i-1}, p_{y,i-1}, c_{i-1})$
      iv. $sum(a, b, cin) = (a \oplus b) \oplus cin$
      v. $carry(a, b, cin) = (a \wedge b) \vee ((a \oplus b) \wedge cin)$ כאשר a ו-b ביטים.

7 שקילויות עבור צורת PNF

1. $(A \to B) \leftrightarrow (\neg A \vee B)$
2. $(A \leftrightarrow B) \leftrightarrow ((A \to B) \wedge (B \to A))$
3. $\neg (A \vee B) \leftrightarrow (\neg A \wedge \neg B)$
4. $\neg (A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
5. $(A \wedge Qx.B) \leftrightarrow Qx.(A \wedge B)$ כאשר $Q \in \{\forall, \exists\}$, x לא מופיע ב-A
6. $(A \vee Qx.B) \leftrightarrow Qx.(A \vee B)$ כאשר $Q \in \{\forall, \exists\}$, x לא מופיע ב-A
7. $((Q_1 y.A) \wedge (Q_2 x.B)) \leftrightarrow (Q_1 y Q_2 x.(A \wedge B))$ כאשר $Q, Q_1, Q_2 \in \{\forall, \exists\}$, x לא מופיע ב-A, y לא מופיע ב-B
8. $((Q_1 y.A) \vee (Q_2 x.B)) \leftrightarrow (Q_1 y Q_2 x.(A \vee B))$ כאשר $Q, Q_1, Q_2 \in \{\forall, \exists\}$, x לא מופיע ב-A, y לא מופיע ב-B