Topici speciale în logică și securitate I

Domenii abstracte

Paul Irofti

Master anul II, Sem. I, 2019-2020

Variabile multiple

Ce se întâmplă dacă am variabile multiple?

```
int A[4][8] = {...};
int i, j;
int sum = 0;

for (i = 0; i < 4; i++)
    for (j = 0; j < 8; j++)
        sum += A[i][j];

printf("sum = %d\n", sum);
```

Inegalități

Scop: constrângeri numerice asupra domeniului variabilelor $\mathcal{X}$.

Fie $\boldsymbol{x}$ vectorul ce conține toate variabilele din $\mathcal{X}$.

Lin: Fie $Lin^{\mathbb{R}}$ setul expresilor liniare de forma $\boldsymbol{ax}$, unde $\boldsymbol{a} \in \mathbb{R}^n$ sunt coeficienții variabilelor.

Ineq: Fie $Ineq^{\mathbb{R}}$ setul inegalităților liniare de forma $\boldsymbol{ax} \leq c$, unde $c \in \mathbb{R}$ este o constantă.

Exemple:

- $6x_3 \leq x_1 + 5 \iff \begin{bmatrix} -1 & 0 & 6 & 0 & \dots & 0 \end{bmatrix} \boldsymbol{x} \leq 5$
- $x_2 = 7 \iff x_2 \leq 7 \wedge x_2 \geq 7$
- $x_2 \geq 7 \iff -x_2 \leq -7$
- Expresii cu întregi: $e_1 < e_2 \iff e_1 \leq e_2 - 1$

Proprietăți geometrice ale inegalităților

Fiecare inegalitate $\boldsymbol{ax} \leq c \in \mathit{Ineq}^{\mathbb{R}}$ crează semiplanul $[\![\boldsymbol{ax} \leq c]\!] = \{x \in \mathbb{R}^{|\mathcal{X}|} \mid \boldsymbol{ax} \leq c\}$.

Un set de inegalități $I \subseteq \mathit{Ineq}^{\mathbb{R}}$ produce un spațiu convex închis $[\![I]\!] = \bigcap_{\iota \in I} [\![\iota]\!]$.

Fie $\mathcal{S} = \{[\![I]\!] \mid I \subseteq \mathit{Ineq}^{\mathbb{R}}\}$ setul tuturor spațiilor convexe.

Definim $\overline{\curlyvee}$, similar ca la intervale, operația asupra lui $S_1, S_2 \in \mathcal{S}$ ce produce spațiul $S = S_1 \overline{\curlyvee} S_2$ a.î. $S_1 \subseteq S$ și $S_2 \subseteq S$.

Teoremă: $\left(\mathcal{S}, \subseteq, \overline{\curlyvee}, \cap\right)$ formează o latice.

Demonstrație: Exercițiu.

Concluzie: Soluția unui set de ecuații precum cea dată ca exemplu la intervale data trecută există și poate fi rezolvată cu *teorema de punct fix*: cum am rezolvat pentru `i` putem rezolva pentru mai multe variabile deodată.

Probleme de ordin computațional

Numar infinit de inegalități. Poliedere.

- există seturi convexe $S \in \mathcal{S}$ a.î. $|I| \notin \mathbb{N} \forall I \subseteq Ineq$ și $[\![I]\!] = S$.
- implementăriile pot stoca spații convexe generate de către un set finit de inegalități denumite *poliedre*

Exemplu:

- secvența poliedrelor regulate (triunghi echilateral, pătrat, hexagon, dodecagon, ...) converge către disc;
- putem formula lanțul crescător $S_1 \subseteq S_2 \subseteq S_3 \ldots$
- S_i este un poliedru; $\bigcup_i S_i$ nu este pentru că un disc nu poate fi reprezentat de un set finit de inegalități

Concluzii: Laticea poliedrelor este incompletă. Teorema de punct fix poate converge într-un spațiu convex care nu este un poliedru!

Probleme de ordin computațional

Creșterea nelimitată a coeficienților.

- $Lin^{\mathbb{R}}$ și $Ineq^{\mathbb{R}}$ sunt definite pe $\mathbb{R}$
- numerele reprezentate în virgulă mobilă reprezintă elemente finite din $\mathbb{R}$; mai exact numerele pe calculator fac parte din $\mathbb{Q}$

Exemplu:

- fie secvența $x_i \in \mathbb{Q}$ definită de $x_0 = 1$ și $x_{n+1} = (x_n + 2/x_n)/2$
- $S_j = [\![\{1 \leq x \leq x_j\}]\!]$ cuprinde $x_0, \ldots, x_j$
- putem formula lanțul crescător $S_0 \subseteq S_1 \subseteq \ldots$
- lanțul converge la $[\![\{1 \leq x \leq \sqrt{2}\}]\!]$

Concluzii: Teorema de punct fix poate crea inegalități ce conțin coeficienți și constante de dimensiune infinită. Restrângerea coeficienților și constantelor la mulțimea numerelor raționale duce la un domeniu incomplet!

Operatorul de *widening*

Widening este o tehnică de accelerare ce permite încheierea execuției iterațiilor de punct fix în timp finit prin eliminarea anumitor inegalități.

Când se aplică *widening* unui lanț crescător, se obține un set de inegalități ce poate fi finit descris.

Redefinim: Fie *Lin* setul cu coeficienții $\boldsymbol{a} \in \mathbb{Z}^n$ și *Ineq* inegalitățiile construite cu *Lin* și constante $c \in \mathbb{Z}$.

Semiplanul definit de o inegalitate devine $[\![\boldsymbol{ax} \leq c]\!] = \{\boldsymbol{x} \in \mathbb{Q}^{|\mathcal{X}|} \mid \boldsymbol{ax} \leq c\}$.

Spațiile convexe obținute prin *widening* sunt $Poly = \{[\![I]\!] \mid I \in Ineq \wedge |I| \in \mathbb{N}\}$ sau setul poliedrelor convexe generate în timp finit.

Astfel operatorul de *widening* este $\nabla : Poly \times Poly \to Poly$ cu propiretățiile

1. $P \subseteq P \nabla Q, \forall P, Q$
2. $Q \subseteq P \nabla Q, \forall P, Q$
3. Pentru toate lanțurile $P_0 \subseteq P_1 \subseteq \ldots$, lanțul $R_0 = P_0$ și $R_{i+1} = R_i \nabla P_{i+1}$ este stabil ($\exists i$ a.î. $\bigcup_{j \in \mathbb{N}} R_j \subseteq R_i$)

Proprietăți. Dezavantaje.

Laticea $(\mathit{Poly}, \leq_P, \vee_P, \wedge_P)$:

- $\leq_P$ este operatorul de incluziune $\subseteq$
- $\vee_P = \overline{\Upsilon}$ este operația de *join* pentru poliedre
- $\wedge_P$ este operația de *meet* pentru seturi

Laticea este incompletă pentru că operațiile de *join* sau *meet* aplicate unui număr arbitrar de poliedre nu rezultă neapărat într-un poliedru.

Operatorul de widening împreună cu laticea incompletă restrâng numărul de puncte fixe ce pot fi atinse.

Un poliedru stabil obținut la convergență este în general un *post-fixpoint*: un poliedru ce cuprinde poliedrul punctului fix. O aproximare.

Exemplu:

- fie secvența $x_i \in \mathbb{Q}$ definită de $x_0 = 1$ și $x_{n+1} = (x_n + 2/x_n)/2$
- lanțul converge la $[\![\{1 \leq x \leq \sqrt{2}\}]\!] \notin \mathit{Poly}$
- *post-fixpoint*: $[\![\{1 \leq x \leq 2\}]\!]$ sau chiar $[\![\{1 \leq x\}]\!]$

Operații

Asignarea unei valori unei variabile.

Fie $P \in Poly$ și $x \in \mathcal{X}$. Operația $x = 42$ corespunde poliedrului $P \wedge_P [\![\{x = 42\}]\!]$ care este de fapt poliedrul P doar că valoarea lui x este fixată la 42.

Exercițiu: Arătați că operația $P \wedge_P [\![\{x = 42\}]\!]$ implemnetează semantica operației `if (x == 42)`. Dați un exemplu!

Actualizarea valorii unei variabile.

Pentru ca x să primească o nouă valoare, valoarea veche trebuie să dispară: folosim operatorul de proiecție $\exists_x : Poly \to Poly$:

$$\exists_{x_i}(P) = \{\Big[x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n\Big] \mid \boldsymbol{x} \in P, x \in \mathbb{R}\}$$

Operatorul elimină orice informație privind $x \in \mathcal{X}$ din $P \in Poly$.

Exercițiu: Cum implementați semantica operației `x=42`? Dar `x=x+1`?

Operații speciale

Cum implementați operația `x=x+1`?

- $\exists_x(P) \wedge_P [\![\{x = x + 1\}]\!]$ nu este fezabil
- folosim o variabilă intermediară $t \in \mathcal{X}^T$ și apoi asignăm pe t lui x
- $\mathcal{X}^T \subseteq \mathcal{X}$ reprezintă un set abstract al variabilelor temporare ce nu corespund nici unei variabile din program
- deci orice operație `x=e`, unde e este o expresie liniară

Exercițiu: Arătați că `x=e` poate fi implementat ca

$$\exists_t([\![\{x = t\}]\!] \wedge_P \exists_x(P \wedge_P [\![\{t = e\}]\!]))$$

Vom nota cu $P \triangleright x := e$ această operație.

Operații speciale

Notația $P \triangleright x := e$ este suficientă pentru toate operațiile de asignare cu excepția diviziunii și a operației de *shift*.

Fie $P \triangleright x := y \gg n$ cu $n \in \mathbb{N}$ operația de *shift* la dreapta cu n biți.

- rescriem: x este actualizat a.î. P conține soluțiile întregi $x = \lfloor y/2^n \rfloor$
- ecuația liniară echivalentă este: $2^n x = y - d$ cu $d \in \{0, \ldots, 2^n - 1\}$
- rezultă modelul:

$$\exists_t (\llbracket \{x = t\} \rrbracket \wedge_P \exists_x (P \wedge_P \llbracket \{y - (2^n - 1) \leq 2^n t \leq y\} \rrbracket))$$

Exercițiu: Ilustrați geometric poliedrul rezultat din operația $P' = P \triangleright y := x \gg 2$. Ce se întâmplă dacă avem precondiția $x = 8$? ($P' \wedge_P \llbracket \{x = 8\} \rrbracket$.)

Exercițiu: Cum poate fi modelată operația de diviziune?

Tehnici de optimizare

Cum pot găsi valoarea minimă a unei expresii $\boldsymbol{ax} \in Lin$ astfel încât $x \in P$?

Fie setul $C = \{c \in \mathbb{Z} \mid P \wedge_P [\![\{\boldsymbol{ax} \leq c\}]\!] \neq \emptyset\}$ ce conține toate constantele c pentru care semi-planul $\boldsymbol{ax} \leq c$ se intersectează cu poliedrul P.

Definim funcția $minExp : Lin \times Poly \to (\mathbb{Z} \cup \{-\infty\})$

$$minExp(\boldsymbol{ax}, P) = \begin{cases} \min(C), & \text{dacă există } \min(C) \\ -\infty, & \text{altfel} \end{cases}$$

Aceasta este o problemă de programare liniară de tipul

$$\min \boldsymbol{c}^T \boldsymbol{x} \quad \text{a.î.} \quad \boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b}, \quad \boldsymbol{x} \geq 0$$

ce poate fi rezolvată de algoritmi standard precum simplex.