SS 2024 lecture 12

Constraint Solving

René Thiemann and Fabian Mitterwallner

based on a previous course by Aart Middeldorp

Outline

1. **Quantifier Elimination**
2. **Ferrante and Rackoff's Method**
3. **Cooper's Method**
4. **Further Reading**

Outline

1. **Quantifier Elimination**
2. Ferrante and Rackoff's Method
3. Cooper's Method
4. Further Reading

Remark

since last lecture: consider formulas involving quantifiers

Definition

first-order theory T admits quantifier elimination if there exists algorithm that transforms formulas in T into T-equivalent quantifier-free formulas

Remarks

- first-order theory T is decidable if
  1. it admits quantifier elimination
  2. satisfiability of quantifier-free formulas is decidable
- quantifier elimination algorithm is needed only for formulas $\exists x.\, \varphi$ with quantifier-free φ
  - remove universal quantifiers: replace each $\forall x.\, \varphi$ by $\neg\exists x.\, \neg\varphi$
  - apply quantifier elimination algorithm starting with innermost quantifiers

Lemma

QBF admits quantifier elimination; algorithm: replace $\exists x.\, \varphi$ by $\varphi[x/\bot] \vee \varphi[x/\top]$

Examples

- LRA formula $\exists x.\, 2x = y$ is equivalent to $\top$
- LIA formula $\exists x.\, 2x = y$ has no equivalent quantifier-free formula (over same signature)

Upcoming

- LRA admits quantifier elimination (Ferrante and Rackoff's method)
- augmented version of LIA admits quantifier elimination (Cooper's method)

Remark

real arithmetic admits quantifier elimination (even non-linear)
(Tarski–Seidenberg, Collin's cylindrical algebraic decomposition algorithm)

Outline

1. Quantifier Elimination
2. **Ferrante and Rackoff's Method**
3. Cooper's Method
4. Further Reading

Ferrante and Rackoff's Method

input: QLRA formula $\exists x.\, \varphi(x)$ with φ quantifier-free
output: equivalent quantifier-free formula

1. $\varphi_1(x)$ is NNF of $\varphi(x)$
2. $\varphi_2(x)$ is result of replacing literals in $\varphi_1(x)$ as follows:

$$\begin{aligned} s \leq t &\implies s < t \vee s = t & \qquad \neg(s \leq t) &\implies t < s \\ \neg(s < t) &\implies t < s \vee s = t & \qquad \neg(s = t) &\implies t < s \vee s < t \end{aligned}$$

3. $\varphi_3(x)$ is result of replacing atoms in $\varphi_2(x)$ as follows:

$$t < cx \implies \begin{cases} \frac{t}{c} < x & \text{if } c > 0 \\ x < \frac{t}{c} & \text{if } c < 0 \end{cases} \qquad\qquad t = cx \implies x = \frac{t}{c}$$

such that x does not appear in t

Example

- $\exists x.\, 3x + 1 < 10 \wedge 7x - 6 > 7$
- $\exists x.\, x < 3 \wedge x > \frac{13}{7}$
- left infinite projection: $\top \wedge \bot \equiv \bot$

  right infinite projection: $\bot \wedge \top \equiv \bot$

  $S = \{3, \frac{13}{7}\}$

$$\bigvee_{s,t \in S} \left(\frac{s+t}{2} < 3 \wedge \frac{s+t}{2} > \frac{13}{7} \right) \equiv \frac{\frac{13}{7}+3}{2} < 3 \wedge \frac{\frac{13}{7}+3}{2} > \frac{13}{7} \equiv \top$$

Ferrante and Rackoff's Method (cont'd)

4. $\varphi_3(x)$ is formula without negations and contains three types of atoms involving x:

(A) $x < t$ (B) $t < x$ (C) $x = t$

S is set of terms t in (A), (B) and (C) atoms

idea: finitely many cases for $\exists x.\varphi_3(x)$: x can be some element of S, between two elements of S, smaller than all elements of S or larger than all elements of S

left infinite projection $\varphi_{-\infty}$ is obtained from $\varphi_3(x)$ by replacing all (A) atoms with $\top$ and all (B) and (C) atoms with $\bot$

right infinite projection $\varphi_{+\infty}$ is obtained from $\varphi_3(x)$ by replacing all (A) and (C) atoms with $\bot$ and all (B) atoms with $\top$

$$\varphi_4 = \varphi_{-\infty} \vee \varphi_{+\infty} \vee \bigvee_{s,t \in S} \varphi_3\left(\frac{s+t}{2}\right)$$

Example

- $\exists y\, x.\, 3x + 1 < y \wedge 2x - y > 7$
- $\exists y\, x.\, x < \frac{y-1}{3} \wedge x > \frac{7+y}{2}$
- left infinite projection: $\top \wedge \bot \equiv \bot$

  right infinite projection: $\bot \wedge \top \equiv \bot$

  $S = \{\frac{y-1}{3}, \frac{7+y}{2}\}$

$$\exists y.\bigvee_{s,t \in S} \frac{s+t}{2} < \frac{y-1}{3} \wedge \frac{s+t}{2} > \frac{7+y}{2} \equiv \exists y.\frac{\frac{y-1}{3}+\frac{7+y}{2}}{2} < \frac{y-1}{3} \wedge \frac{\frac{y-1}{3}+\frac{7+y}{2}}{2} > \frac{7+y}{2}$$

$$\equiv \exists y.\, \frac{y-1}{3} > \frac{7+y}{2} \equiv \exists y.\, y < -23$$

- another quantifier elimination for y yields equivalent formula $\top$ via left infinite projection
- extract solution $y := -24$ and $x := \frac{\frac{y-1}{3}+\frac{7+y}{2}}{2} = -\frac{101}{12}$

Outline

1. Quantifier Elimination
2. Ferrante and Rackoff's Method
3. Cooper's Method
Soundness Optimizations
4. Further Reading

Definition (Augmented Linear Integer Arithmetic)

- syntax:

$$\varphi ::= P \mid \neg\varphi \mid \varphi\wedge\varphi \mid \varphi\vee\varphi \mid \exists x.\,\varphi \mid \forall x.\,\varphi$$
$$P ::= t = t \mid t < t \mid 1 \,|\, t \mid 2 \,|\, t \mid 3 \,|\, t \mid \cdots$$
$$t ::= t + t \mid t - t \mid x \mid \cdots \mid -2 \mid -1 \mid 0 \mid 1 \mid 2 \mid \cdots$$

- semantics: $\mathbb{Z}$ with standard interpretations

Remarks

- multiplication with constants is definable:

$$2x \quad \text{stands for} \quad x + x$$
$$-3x \quad \text{stands for} \quad 0 - x - x - x$$

- quantifier elimination is possible

$$\exists x.\, 2x = y \iff 2 \mid y$$

Cooper's Method

input: QLIA formula $\exists x.\,\varphi(x)$ with φ quantifier-free
output: equivalent quantifier-free formula

1. $\varphi_1(x)$ is NNF of $\varphi(x)$
2. $\varphi_2(x)$ is result of replacing literals in $\varphi_1(x)$ as follows:

$$\begin{aligned} s = t &\implies s < t+1 \wedge t < s+1 \\ \neg(s=t) &\implies s < t \vee t < s \\ \neg(s<t) &\implies t < s+1 \end{aligned}$$

3. $\varphi_3(x)$ is result of collecting terms containing x such that literals have form

$$ax < t \qquad t < ax \qquad c \mid ax+t \qquad \neg(c \mid ax+t)$$

with $a > 0$

Example

- $\exists x.\,\varphi = \exists x.\, -3x+2y-1<y \wedge 2x-6<z \wedge 4 \mid 5x+1 = \exists x.\,\varphi_1 = \exists x.\,\varphi_2$
- $\exists x.\,\varphi_3 = \exists x.\, y-1<3x \wedge 2x<z+6 \wedge 4 \mid 5x+1$
- $\delta' = \mathrm{lcm}\,\{3,2,5\} = 30$

  $\exists x.\, 10y-10 < 30x \wedge 30x < 15z+90 \wedge 24 \mid 30x+6$
- $\exists x'.\,\varphi_4 = \exists x'.\, 10y-10<x' \wedge x'<15z+90 \wedge 24 \mid x'+6 \wedge 30 \mid x'$
- left infinite projection: $\varphi_{-\infty} = \bot \wedge \top \wedge 24 \mid x'+6 \wedge 30 \mid x' \equiv \bot$

  $\delta = \mathrm{lcm}\,\{24,30\} = 120 \qquad B = \{10y-10\}$

$$\varphi_5 = \bigvee_{j=1}^{120} \left[\begin{array}{l} 10y-10 < 10y-10+j \wedge 10y-10+j < 15z+90 \\ \wedge\ 24 \mid 10y-10+j+6 \wedge 30 \mid 10y-10+j \end{array} \right]$$

$$\equiv \bigvee_{j=1}^{120} \left[\begin{array}{l} 0 < j \wedge 10y+j < 15z+100 \\ \wedge\ 24 \mid 10y+j-4 \wedge 30 \mid 10y+j-10 \end{array} \right]$$

Cooper's Method (cont'd)

4. $\delta' = \mathrm{lcm}\,\{a \mid a \text{ is coefficient of } x \text{ in } \varphi_3(x)\}$

   multiply atoms in $\varphi_3(x)$ by constants such that δ' is coefficient of every x

   replace every occurrence of $\delta' x$ by fresh variable x'

   add conjunct $\delta' \mid x'$ to obtain $\varphi_4(x')$
5. four types of literals in $\varphi_4(x')$:

   (A) $x' < t$ (B) $t < x'$ (C) $a \mid x'+t$ (D) $\neg(a \mid x'+t)$

   left infinite projection $\varphi_{-\infty}(x')$ is obtained from $\varphi_4(x')$ by replacing all (A) literals with $\top$ and all (B) literals with $\bot$ (and subsequent simplification)

   $\delta = \mathrm{lcm}\,\{a \mid a \text{ is constant of division predicate in } \varphi_4(x')\}$

   B is set of terms t in (B) literals

$$\varphi_5 = \bigvee_{j=1}^{\delta} \varphi_{-\infty}(j) \vee \bigvee_{j=1}^{\delta} \bigvee_{t \in B} \varphi_4(t+j)$$

Outline

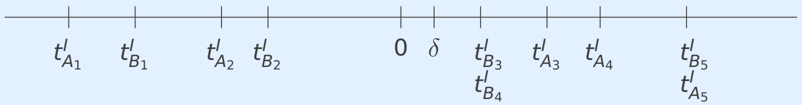
1. Quantifier Elimination
2. Ferrante and Rackoff's Method
3. Cooper's Method
   Soundness Optimizations
4. Further Reading

Elimination of Quantifier in Cooper's Method: From $\exists x.\varphi_4(x)$ to φ_5

- literals in NNF $\varphi_4(x)$: (A) $x < t$ (B) $t < x$ (C) $a \mid x + t$ (D) $\neg(a \mid x + t)$
- $\varphi_{-\infty}(x)$ is $\varphi_4(x)$ where (A) literals are replaced by $\top$ and (B) literals by $\perp$
- $\delta = \{a \mid a$ is constant of division predicate in $\varphi_4(x)\}$
- B is set of terms t in (B) literals
- $\varphi_5 = \bigvee_{j=1}^{\delta} \varphi_{-\infty}(j) \vee \bigvee_{j=1}^{\delta} \bigvee_{t \in B} \varphi_4(t+j)$

Soundness Proof: $\exists x.\varphi_4(x)$ and φ_5 are Equivalent

- $\Longleftarrow$: if $\models_I \varphi_5$ then $\models_I \exists x.\varphi_4(x)$ for arbitrary environment I
- $\Longrightarrow$: if $\models_I \exists x.\varphi_4(x)$ then $\models_I \varphi_5$ for arbitrary environment I



Outline

1. **Quantifier Elimination**
2. **Ferrante and Rackoff's Method**
3. **Cooper's Method**
   Soundness Optimizations
4. **Further Reading**

5 four types of literals in $\varphi_4(x')$:

(A) $x' < t$ (B) $t < x'$ (C) $a \mid x' + t$ (D) $\neg(a \mid x' + t)$

right infinite projection $\varphi_{+\infty}(x')$ is obtained from $\varphi_4(x')$ by replacing all (A) literals with $\perp$ and all (B) literals with $\top$

$\delta = \mathrm{lcm}\,\{a \mid a$ is constant of division predicate in $\varphi_4(x')\}$

A is set of terms t in (A) literals

$$\varphi'_5 = \bigvee_{j=1}^{\delta} \varphi_{+\infty}(-j) \vee \bigvee_{j=1}^{\delta} \bigvee_{t \in A} \varphi_4(t-j)$$

Left or Right Infinite Projection?

use right infinite projection if $|A| < |B|$ to reduce number of disjuncts

Eliminating Block of Quantifiers

$$\begin{aligned}
&\exists x_1 \dots x_n.\, \varphi(x_1,\dots,x_n) \\
&\quad\equiv \exists x_1 \dots x_{n-1}.\, \bigvee_{j=1}^{\delta} \varphi_{-\infty}(x_1,\dots,x_{n-1},j) \vee \bigvee_{j=1}^{\delta} \bigvee_{t \in B} \varphi_4(x_1,\dots,x_{n-1},t+j) \\
&\quad\equiv \bigvee_{j=1}^{\delta} \exists x_1 \dots x_{n-1}.\, \varphi_{-\infty}(x_1,\dots,x_{n-1},j) \\
&\qquad \vee \bigvee_{j=1}^{\delta} \bigvee_{t \in B} \exists x_1 \dots x_{n-1}.\, \varphi_4(x_1,\dots,x_{n-1},t+j)
\end{aligned}$$

treat j as free variable and examine only $1 + |B|$ formulas:

- $\exists x_1 \dots x_{n-1}.\, \varphi_{-\infty}(x_1,\dots,x_{n-1},j)$
- $\exists x_1 \dots x_{n-1}.\, \varphi_4(x_1,\dots,x_{n-1},t+j)$ for each $t \in B$

Outline

1. Quantifier Elimination
2. Ferrante and Rackoff's Method
3. Cooper's Method
4. **Further Reading**

Bradley and Manna

- Sections 7.2 and 7.3

Further Reading

- Jeanne Ferrante and Charles Rackoff
  A Decision Procedure for the First Order Theory of Real Addition with Order
  SIAM Journal on Computing 4(1), pp. 69 – 76, 1975
- David C. Cooper
  Theorem Proving in Arithmetic without Multiplication
  Chapter 5 in Machine Intelligence 7, Edinburgh University Press, pp. 91 – 100, 1972

Important Concepts

- augmented linear integer arithmetic
- Cooper's method
- divisibility constraint
- Ferrante and Rackoff's method
- left infinite projection
- quantifier elimination
- right infinite projection