Verification

Lecture 30

Martin Zimmermann

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- Deductive verification
    - Quantifier Elimination

Quantifier Elimination (QE)

Algorithm for elimination of all quantifiers of formula F until quantifier-free formula G that is equivalent to F remains

Note: Could be enough to require that F is equisatisfiable to F', that is F is satisfiable iff F' is satisfiable

A theory T admits quantifier elimination if there is an algorithm that given Σ-formula F returns a quantifier-free Σ-formula G that is T-equivalent to F.

Example

- For $\Sigma_{\mathbb{Q}}$-formula

  $$F:\ \exists x.\ 2x = y,$$

  quantifier-free $T_{\mathbb{Q}}$-equivalent $\Sigma_{\mathbb{Q}}$-formula is

  $$G:\ \top$$

- For $\Sigma_{\mathbb{Z}}$-formula

  $$F:\ \exists x.\ 2x = y,$$

  there is no quantifier-free $T_{\mathbb{Z}}$-equivalent $\Sigma_{\mathbb{Z}}$-formula.

- Let $T_{\widehat{\mathbb{Z}}}$ be $T_{\mathbb{Z}}$ with divisibility predicates $|$.
  For $\Sigma_{\widehat{\mathbb{Z}}}$-formula

  $$F:\ \exists x.\ 2x = y,$$

  a quantifier-free $T_{\widehat{\mathbb{Z}}}$-equivalent $\Sigma_{\widehat{\mathbb{Z}}}$-formula is

  $$G:\ 2 \mid y.$$

In developing a QE algorithm for theory T, we need only consider formulae of the form

$$\exists x.\ F$$

for quantifier-free F

Example: For Σ-formula

$$G_1 :\ \exists x.\ \forall y.\ \underbrace{\exists z.\ F_1[x, y, z]}_{F_2[x,y]}$$

$$G_2 :\ \exists x.\ \forall y.\ F_2[x, y]$$

$$G_3 :\ \exists x.\ \neg\, \underbrace{\exists y.\ \neg F_2[x, y]}_{F_3[x]}$$

$$G_4 :\ \underbrace{\exists x.\ \neg F_3[x]}_{F_4}$$

$$G_5 :\ F_4$$

G_5 is quantifier-free and T-equivalent to G_1

Quantifier Elimination for $T_{\mathbb{Z}}$

$\Sigma_{\mathbb{Z}}: \{\ldots, -2, -1, 0, 1, 2, \ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots, +, -, =, <\}$

Lemma:

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$.
F represents the set of integers

$$S : \{n \in \mathbb{Z} : F\{y \mapsto n\} \text{ is } T_{\mathbb{Z}}\text{-valid}\} .$$

Either $S \cap \mathbb{Z}^+$ or $\mathbb{Z}^+ \setminus S$ is finite.
where $\mathbb{Z}^+$ is the set of positive integers

Example: $\Sigma_{\mathbb{Z}}$-formula $\quad F : \exists x.\, 2x = y$

S: even integers

$S \cap \mathbb{Z}^+$: positive even integers — infinite
$\mathbb{Z}^+ \setminus S$: positive odd integers — infinite

Therefore, by the lemma, there is no quantifier-free $T_{\mathbb{Z}}$-formula that is $T_{\mathbb{Z}}$-equivalent to F.

Thus, $T_{\mathbb{Z}}$ does not admit QE.

Augmented theory $\widehat{T_{\mathbb{Z}}}$

$\widehat{\Sigma_{\mathbb{Z}}}$: $\Sigma_{\mathbb{Z}}$ with countable number of unary divisibility predicates

$$k \mid \cdot \quad \text{for } k \in \mathbb{Z}^+$$

Intended interpretations:

$k \mid x$ holds iff k divides x without any remainder

Example:

$$x > 1 \ \land \ y > 1 \ \land \ 2 \mid x + y$$

is satisfiable (choose $x = 2, y = 2$).

$$\neg(2 \mid x) \ \land \ 4 \mid x$$

is not satisfiable.

Axioms of $\widehat{T_{\mathbb{Z}}}$: axioms of $T_{\mathbb{Z}}$ with additional countable set of axioms

$$\forall x.\, k \mid x \ \leftrightarrow \ \exists y.\, x = ky \quad \text{for } k \in \mathbb{Z}^+$$

$\widehat{T_{\mathbb{Z}}}$ admits QE (Cooper's method)

Algorithm: Given $\widehat{\Sigma_{\mathbb{Z}}}$-formula $\exists x.\ F[x]$, where F is quantifier-free, construct quantifier-free $\widehat{\Sigma_{\mathbb{Z}}}$-formula that is equivalent to $\exists x.\ F[x]$.

1. Put $F[x]$ into Negation Normal Form (NNF).
2. Normalize literals: $s < t$, $k|t$, or $\neg(k|t)$
3. Put x in $s < t$ on one side: $hx < t$ or $s < hx$
4. Replace hx with x' without a factor
5. Replace $F[x']$ by $\bigvee F[j]$ for finitely many j.

Step 1: NNF

Put $F[x]$ into NNF $F_1[x]$, that is,
$\exists x.\ F_1[x]$ has negations only in literals (only $\wedge$, $\vee$)
and $\widehat{T}_{\mathbb{Z}}$-equivalent to $\exists x.\ F[x]$

To transform F to equivalent F' in NNF use recursively the following template equivalences (left-to-right):

$$\neg\neg F_1 \Leftrightarrow F_1 \qquad \neg\top \Leftrightarrow \bot \qquad \neg\bot \Leftrightarrow \top$$

$$\left.\begin{array}{l} \neg(F_1 \wedge F_2) \Leftrightarrow \neg F_1 \vee \neg F_2 \\ \neg(F_1 \vee F_2) \Leftrightarrow \neg F_1 \wedge \neg F_2 \end{array}\right\}\text{De Morgan's Law}$$

$$F_1 \rightarrow F_2 \Leftrightarrow \neg F_1 \vee F_2$$

$$F_1 \leftrightarrow F_2 \Leftrightarrow (F_1 \rightarrow F_2) \wedge (F_2 \rightarrow F_1)$$

Step 2: Normalize literals

Normalize literals: $s < t$, $k|t$, or $\neg(k|t)$

Replace (left to right)

$$\begin{array}{rcl} s = t & \Leftrightarrow & s < t + 1 \,\wedge\, t < s + 1 \\ \neg(s = t) & \Leftrightarrow & s < t \,\vee\, t < s \\ \neg(s < t) & \Leftrightarrow & t < s + 1 \end{array}$$

The output $\exists x.\, F_2[x]$ contains only literals of form

$$s < t\,, \quad k \mid t\,, \quad \text{or} \quad \neg(k \mid t)\,,$$

where s, t are $\widehat{T_{\mathbb{Z}}}$-terms and $k \in \mathbb{Z}^+$.

Step 3: Put x on one side

Put x in $s < t$ on one side: $hx < t$ or $s < hx$

Collect terms containing x so that literals have the form

$$hx < t\,, \quad t < hx\,, \quad k \mid hx + t\,, \quad \text{or} \quad \neg(k \mid hx + t)\,,$$

where t is a term and $h, k \in \mathbb{Z}^+$. The output is the formula $\exists x.\ F_3[x]$, which is $\widehat{T_{\mathbb{Z}}}$-equivalent to $\exists x.\ F[x]$.

Step 4: Eliminate coefficients

Replace hx with x' without a factor

Let

$$\delta' = \text{lcm}\{h \;:\; h \text{ is a coefficient of } x \text{ in } F_3[x]\}\,,$$

where lcm is the least common multiple. Multiply atoms in $F_3[x]$ by constants so that δ' is the coefficient of x everywhere:

$$\begin{array}{rcll}
hx < t & \Leftrightarrow & \delta' x < h' t & \text{where} \quad h'h = \delta' \\
t < hx & \Leftrightarrow & h' t < \delta' x & \text{where} \quad h'h = \delta' \\
k \mid hx + t & \Leftrightarrow & h'k \mid \delta' x + h' t & \text{where} \quad h'h = \delta' \\
\neg(k \mid hx + t) & \Leftrightarrow & \neg(h'k \mid \delta' x + h' t) & \text{where} \quad h'h = \delta'
\end{array}$$

The result $\exists x.\, F_3'[x]$, in which all occurrences of x in $F_3'[x]$ are in terms $\delta' x$.

Replace $\delta' x$ terms in F_3' with a fresh variable x' to form

$$F_3'' \;:\; F_3\{\delta' x \mapsto x'\}$$

Finally, construct

$$\exists x'.\ \underbrace{F_3''[x'] \ \wedge \ \delta' \mid x'}_{F_4[x']}$$

$\exists x'.F_4[x']$ is equivalent to $\exists x.\ F[x]$ and each literal of $F_4[x']$ has one of the forms:

(A) $x' < a$

(B) $b < x'$

(C) $h \mid x' + c$

(D) $\neg(k \mid x' + d)$

where a, b, c, d are terms that do not contain x, and $h, k \in \mathbb{Z}^+$.

Step 5: Eliminate x'

Replace $F[x']$ by $\bigvee F[j]$ for finitely many j.

1. Construct

   left infinite projection $F_{-\infty}[x']$

   of $F_4[x']$ by

   (A) replacing literals $x' < a$ by $\top$

   (B) replacing literals $b < x'$ by $\bot$

   idea: very small numbers satisfy (A) literals but not (B) literals

2. Let

   $$\delta = \text{lcm}\left\{\begin{array}{l} h \text{ of (C) literals } h \mid x' + c \\ k \text{ of (D) literals } \neg(k \mid x' + d) \end{array}\right\}$$

   and B be the set of b terms appearing in (B) literals. Construct

   $$F_5 : \bigvee_{j=1}^{\delta} F_{-\infty}[j] \;\vee\; \bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[b+j]\,.$$

F_5 is quantifier-free and $\widehat{T_{\mathbb{Z}}}$-equivalent to F.

Intuition of Step 5

Property (Periodicity)

if $k \mid \delta$

then $k \mid n$ iff $k \mid n + \lambda\delta$ for all $\lambda \in \mathbb{Z}$

That is, $k \mid \cdot$ cannot distinguish between $k \mid n$ and $k \mid n + \lambda\delta$.

By the choice of δ (lcm of the h's and k's) — no $\mid$ literal in F_5 can distinguish between n and $n + \delta$.

$$F_5 : \bigvee_{j=1}^{\delta} F_{-\infty}[j] \;\vee\; \bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[b + j]$$

Intuition of Step 5

left disjunct $\bigvee_{j=1}^{\delta} F_{-\infty}[j]$:

Contains only $|$ literals

Asserts: no least $n \in \mathbb{Z}$ s.t. $F[n]$.

If there exists n satisfying $F_{-\infty}$,
then every $n - \lambda\delta$, for $\lambda \in \mathbb{Z}^+$, also satisfies $F_{-\infty}$

right disjunct $\bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[b + j]$:

If $n \in \mathbb{Z}$ is s.t. $F[n]$,

let b^* be the largest b in (B) such that $b < n$ is satisfied

then

$$\exists j(1 \le j \le \delta).\ b^* + j \le n \ \land\ F[b^* + j]$$

In other words,

if there is a solution,
then one must already appear in δ interval to the right of some b

Improvement: Symmetric Elimination

In Step 5, if there are fewer

(A) literals $x' < a$

than

(B) literals $b < x'$.

Construct the right infinite projection $F_{+\infty}[x']$ from $F_4[x']$ by replacing

each (A) literal $x' < a$ by $\perp$

and

each (B) literal $b < x'$ by $\top$.

Then right elimination.

$$F_5 : \bigvee_{j=1}^{\delta} F_{+\infty}[-j] \;\vee\; \bigvee_{j=1}^{\delta} \bigvee_{a \in A} F_4[a - j]\,.$$

Improvement: Eliminating Blocks of Quantifiers

$$\exists x_1.\cdots\exists x_n.\, F[x_1,\ldots,x_n]$$

where F quantifier-free.
Eliminating x_n (left elimination) produces

$$G_1:\quad \exists x_1.\cdots\exists x_{n-1}.\ \bigvee_{j=1}^{\delta} F_{-\infty}[x_1,\ldots,x_{n-1},j]\ \vee$$
$$\bigvee_{j=1}^{\delta}\bigvee_{b\in B} F_4[x_1,\ldots,x_{n-1},b+j]$$

which is equivalent to

$$G_2:\quad \bigvee_{j=1}^{\delta}\exists x_1.\cdots\exists x_{n-1}.\, F_{-\infty}[x_1,\ldots,x_{n-1},j]\ \vee$$
$$\bigvee_{j=1}^{\delta}\bigvee_{b\in B}\exists x_1.\cdots\exists x_{n-1}.\, F_4[x_1,\ldots,x_{n-1},b+j]$$

Treat j as a free variable and examine only $1+|B|$ formulae

- $\exists x_1.\cdots\exists x_{n-1}.\, F_{-\infty}[x_1,\ldots,x_{n-1},j]$
- $\exists x_1.\cdots\exists x_{n-1}.\, F_4[x_1,\ldots,x_{n-1},b+j]$ for each $b\in B$