Decision Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Summer 2012

Quantifier Elimination

Quantifier Elimination

Quantifier Elimination (QE) removes quantifiers from formulae:

- Given a formula with quantifiers, e.g., $\exists x. F[x, y, z]$.
- Goal: find an equivalent quantifier-free formula $G[y, z]$.
- The free variables of F and G are the same.

$$\exists x. F[x, y, z] \Leftrightarrow G[y, z]$$

QE as Decision Procedure

Decide satisfiabilty for a formula F, e.g. in $T_{\mathbb{Q}}$, using quantifier elimination:

QE as Decision Procedure

Decide satisfiabilty for a formula F, e.g. in $T_{\mathbb{Q}}$, using quantifier elimination:

- Given a formula F, with free variable $x_1, \ldots, x_n$.
- Build $\exists x_1 \ldots \exists x_n . F$.
- Build equivalent quantifier free formula G.

QE as Decision Procedure

Decide satisfiabilty for a formula F, e.g. in $T_{\mathbb{Q}}$, using quantifier elimination:

- Given a formula F, with free variable $x_1, \ldots, x_n$.
- Build $\exists x_1 \ldots \exists x_n . F$.
- Build equivalent quantifier free formula G.
  G contains only constants, functions and predicates
  i.e. $0, 1, +, -, \geq, =$.
- Compute truth value of G.

QE algorithm

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

$$\exists x.\ F$$

for quantifier-free F

QE algorithm

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

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

QE algorithm

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

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

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

QE algorithm

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

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

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

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

QE algorithm

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

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

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

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

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

QE algorithm

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

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

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

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

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

$$G_5\colon F_4$$

G_5 is quantifier-free and T-equivalent to G_1

Syntactic sugar for Rationals

Consider the Signature of Rationals: $\Sigma_{\mathbb{Q}} : \{0, 1, +, -, =, \geq\}$

We extend the signature with the predicate $>$, which is defined as

$$x > y :\Leftrightarrow x \geq y \land \neg(x = y).$$

Additionally we allow predicates $<$ and $\leq$:

$$x < y :\Leftrightarrow y > x \qquad x \leq y :\Leftrightarrow y \geq x.$$

Syntactic sugar for Rationals

Consider the Signature of Rationals: $\Sigma_{\mathbb{Q}} : \{0, 1, +, -, =, \geq\}$

We extend the signature with the predicate $>$, which is defined as

$$x > y :\Leftrightarrow x \geq y \land \neg(x = y).$$

Additionally we allow predicates $<$ and $\leq$:

$$x < y :\Leftrightarrow y > x \qquad x \leq y :\Leftrightarrow y \geq x.$$

We extend the signature by fractions:

$$\frac{\cdot}{a} \in \Sigma_{\mathbb{Q}} \text{ for } a \in \mathbb{Z}^{+}$$

which are unary function symbols, with their usual meaning.

Given a $\Sigma_{\mathbb{Q}}$-formula $\exists x.\ F[x]$, where $F[x]$ is quantifier-free
Generate quantifier-free formula F_4 (four steps) s.t.

F_4 is $\Sigma_{\mathbb{Q}}$-equivalent to $\exists x.\ F[x]$.

1. Put $F[x]$ in NNF.
2. Eliminate negated literals.
3. Solve the literals s.t. x appears isolated on one side.
4. Finite disjunction $\bigvee_{t \in S_F} F[t]$.

$$\exists x. F[x] \Leftrightarrow \bigvee_{t \in S_F} F[t].$$

where S_F depends on the formula F.

Step 1 and 2

Step 1: Put $F[x]$ in NNF. The result is $\exists x.\ F_1[x]$.

Step 2: Eliminate negated literals and $\geq$ (left to right)

$$
\begin{array}{rcl}
s \geq t & \Leftrightarrow & s > t \lor s = t \\
\neg(s > t) & \Leftrightarrow & t > s \lor t = s \\
\neg(s \geq t) & \Leftrightarrow & t > s \\
\neg(s = t) & \Leftrightarrow & t < s \lor t > s
\end{array}
$$

The result $\exists x.\ F_2[x]$ does not contain negations.

Solve for x in each atom of $F_2[x]$, e.g.,

$$ax + t_2 < bx + t_1 \qquad \Rightarrow \qquad x < \frac{t_1 - t_2}{a - b}$$

where $a - b \in \mathbb{Z}^+$.

All atoms containing x in the result $\exists x.\ F_3[x]$ have form

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

where t is a term that does not contain x.

Step 4 (Part 1)

Construct from $F_3[x]$

- left infinite projection $F_3[-\infty]$ by replacing
  (A) atoms $x < t$ by $\top$
  (B) atoms $t < x$ by $\bot$
  (C) atoms $x = t$ by $\bot$

- right infinite projection $F_3[+\infty]$ by replacing
  (A) atoms $x < t$ by $\bot$
  (B) atoms $t < x$ by $\top$
  (C) atoms $x = t$ by $\bot$

Let S be the set of terms t from (A), (B), (C) atoms.
Construct the formula

$$F_4 : \bigvee_{t \in S_F} F_3[t], \quad \text{where } S_F := \{-\infty, \infty\} \cup \left\{ \frac{s+t}{2} \;\middle|\; s, t \in S \right\}$$

which is $T_{\mathbb{Q}}$-equivalent to $\exists x.\ F[x]$.

- $F_3[-\infty]$ captures the case when small $x \in \mathbb{Q}$ satisfy $F_3[x]$
- $F_3[-\infty]$ captures the case when large $x \in \mathbb{Q}$ satisfy $F_3[x]$
- if $s \equiv t$, $\frac{s+t}{2} = s$ captures the case when $s \in S$ satisfies $F_3[s]$
  if $s < t$ are adjacent numbers, $\frac{s+t}{2}$ represents the whole interval (s, t).

Intuition

Four cases are possible:

1. All numbers x smaller than the smallest term satisfy $F[x]$.

$$\longleftarrow) t_1 \;\; t_2 \cdots t_n$$

Intuition

Four cases are possible:

1. All numbers x smaller than the smallest term satisfy $F[x]$.

$$\longleftarrow) t_1 \;\; t_2 \cdots t_n$$

2. All numbers x larger than the smallest term satisfy $F[x]$.

$$t_1 \;\; t_2 \cdots t_n (\longrightarrow$$

Intuition

Four cases are possible:

1. All numbers x smaller than the smallest term satisfy $F[x]$.

$$\longleftarrow) t_1 \;\; t_2 \cdots t_n$$

2. All numbers x larger than the smallest term satisfy $F[x]$.

$$t_1 \;\; t_2 \cdots t_n (\longrightarrow$$

3. Some t_i,satisfies $F[x]$.

$$\begin{array}{c} t_1 \quad \cdots t_i \cdots \quad t_n \\ \uparrow \end{array}$$

Intuition

Four cases are possible:

1. All numbers x smaller than the smallest term satisfy $F[x]$.

$$\longleftarrow) t_1 \;\; t_2 \cdots t_n$$

2. All numbers x larger than the smallest term satisfy $F[x]$.

$$t_1 \;\; t_2 \cdots t_n (\longrightarrow$$

3. Some t_i,satisfies $F[x]$.

$$\begin{array}{ccccc} t_1 & \cdots & t_i & \cdots & t_n \\ & & \uparrow & & \end{array}$$

4. On an open interval between two terms every element satisfies $F[x]$.

$$t_1 \cdots \quad t_i \underset{\frac{t_i+t_{i+1}}{2}}{(\longleftrightarrow)} t_{i+1} \quad \cdots t_n$$

Theorem

Let S_F be the set of terms constructed from $F_3[x]$ as in Step 4. Then $\exists x.\ F_3[x] \Leftrightarrow \bigvee_{t \in S_F} F_3[t]$.

Proof of Theorem

$\Leftarrow$ If $\bigvee_{t \in S_F} F_3[t]$ is true, then $F_3[t]$ for some $t \in S_F$ is true.
If $F_3[\frac{s+t}{2}]$ is true, then obviously $\exists x.\ F_3[x]$ is true.
If $F_3[-\infty]$ is true, choose some $x < t$ for all $t \in S$. Then $F_3[x]$ is true.
If $F_3[\infty]$ is true, choose some $x > t$ for all $t \in S$. Then $F_3[x]$ is true.

Correctness of Step 4

$\Rightarrow$ If $I \models \exists x.\ F_3[x]$ then there is value v such that

$$I \triangleleft \{x \mapsto \mathrm{v}\} \models F_3\,.$$

Correctness of Step 4

$\Rightarrow$ If $I \models \exists x.\ F_3[x]$ then there is value v such that

$$I \lhd \{x \mapsto \mathrm{v}\} \models F_3\,.$$

If $\mathrm{v} < \alpha_I[t]$ for all $t \in S$, then $I \models F_3[-\infty]$.

$\Rightarrow$ If $I \models \exists x.\ F_3[x]$ then there is value v such that

$$I \lhd \{x \mapsto \mathrm{v}\} \models F_3\,.$$

If $\mathrm{v} < \alpha_I[t]$ for all $t \in S$, then $I \models F_3[-\infty]$.
If $\mathrm{v} > \alpha_I[t]$ for all $t \in S$, then $I \models F_3[\infty]$.

Correctness of Step 4

$\Rightarrow$ If $I \models \exists x.\ F_3[x]$ then there is value v such that

$$I \lhd \{x \mapsto \mathrm{v}\} \models F_3\,.$$

If $\mathrm{v} < \alpha_I[t]$ for all $t \in S$, then $I \models F_3[-\infty]$.
If $\mathrm{v} > \alpha_I[t]$ for all $t \in S$, then $I \models F_3[\infty]$.
If $\mathrm{v} = \alpha_I[t]$ for some $t \in S$, then $I \models F[\frac{t+t}{2}]$.

Correctness of Step 4

$\Rightarrow$ If $I \models \exists x.\ F_3[x]$ then there is value v such that

$$I \triangleleft \{x \mapsto \mathrm{v}\} \models F_3\,.$$

If $\mathrm{v} < \alpha_I[t]$ for all $t \in S$, then $I \models F_3[-\infty]$.
If $\mathrm{v} > \alpha_I[t]$ for all $t \in S$, then $I \models F_3[\infty]$.
If $\mathrm{v} = \alpha_I[t]$ for some $t \in S$, then $I \models F[\frac{t+t}{2}]$.

Otherwise choose largest $s \in S$ with $\alpha_I[s] < \mathrm{v}$ and smallest $t \in S$ with $\alpha_I[t] > \mathrm{v}$.
Since no atom of F_3 can distinguish between values in interval (s, t), $F_3[\mathrm{v}] \Leftrightarrow F_3[\frac{s+t}{2}]$. Hence, $I \models F[\frac{s+t}{2}]$.

Correctness of Step 4

⇒ If $I \models \exists x.\ F_3[x]$ then there is value v such that

$$I \lhd \{x \mapsto \mathrm{v}\} \models F_3\,.$$

If $\mathrm{v} < \alpha_I[t]$ for all $t \in S$, then $I \models F_3[-\infty]$.
If $\mathrm{v} > \alpha_I[t]$ for all $t \in S$, then $I \models F_3[\infty]$.
If $\mathrm{v} = \alpha_I[t]$ for some $t \in S$, then $I \models F[\frac{t+t}{2}]$.

Otherwise choose largest $s \in S$ with $\alpha_I[s] < \mathrm{v}$ and smallest $t \in S$ with $\alpha_I[t] > \mathrm{v}$.
Since no atom of F_3 can distinguish between values in interval (s, t), $F_3[\mathrm{v}] \Leftrightarrow F_3[\frac{s+t}{2}]$. Hence, $I \models F[\frac{s+t}{2}]$.

In all cases $I \models \bigvee_{t \in S_F} F_3[t]$.

Example

$$\exists x.\ \underbrace{3x + 1 < 10 \land 7x - 6 > 7}_{F[x]}$$

Example

$$\exists x.\ \underbrace{3x + 1 < 10 \land 7x - 6 > 7}_{F[x]}$$

Solving for x

$$\exists x.\ \underbrace{x < 3 \land x > \frac{13}{7}}_{F_3[x]}$$

Example

$$\exists x.\ \underbrace{3x + 1 < 10 \land 7x - 6 > 7}_{F[x]}$$

Solving for x

$$\exists x.\ \underbrace{x < 3 \land x > \frac{13}{7}}_{F_3[x]}$$

Step 4:

$$F_4 : \bigvee_{t \in S_F} \underbrace{\left(t < 3 \land t > \frac{13}{7}\right)}_{F_3[t]}$$

Example contd.

$$S_F = \{-\infty, +\infty, 3, \frac{13}{7}, \frac{3+\frac{13}{7}}{2}\}.$$

$$F_3[x] = x < 3 \land x > 13/7$$

$$F_{-\infty} \Leftrightarrow \top \land \bot \Leftrightarrow \bot \qquad F_{+\infty} \Leftrightarrow \bot \land \top \Leftrightarrow \bot$$

$$F_3\left[3\right] \bot \land \top \Leftrightarrow \bot \qquad F_3\left[\frac{13}{7}\right] \Leftrightarrow \top \land \bot \Leftrightarrow \bot$$

$$F_3\left[\frac{\frac{13}{7}+3}{2}\right] : \frac{\frac{13}{7}+3}{2} < 3 \land \frac{\frac{13}{7}+3}{2} > \frac{13}{7} \Leftrightarrow \top$$

Thus, $F_4 : \bigvee_{t \in S_F} F_3[t] \Leftrightarrow \top$ is $T_{\mathbb{Q}}$-equivalent to $\exists x.\ F[x]$, so $\exists x.\ F[x]$ is $T_{\mathbb{Q}}$-valid.

Example

$$\exists x.\ \underbrace{2x > y \wedge 3x < z}_{F[x]}$$

Example

$$\exists x.\ \underbrace{2x > y \wedge 3x < z}_{F[x]}$$

Solving for x

$$\exists x.\ \underbrace{x > \frac{y}{2} \wedge x < \frac{z}{3}}_{F_3[x]}$$

Example

$$\exists x.\ \underbrace{2x > y \wedge 3x < z}_{F[x]}$$

Solving for x

$$\exists x.\ \underbrace{x > \frac{y}{2} \wedge x < \frac{z}{3}}_{F_3[x]}$$

Step 4: $F_{-\infty} \Leftrightarrow \bot$, $F_{+\infty} \Leftrightarrow \bot$, $F_3[\frac{y}{2}] \Leftrightarrow \bot$ and $F_3[\frac{z}{3}] \Leftrightarrow \bot$.

$$F_4\ :\ \frac{\frac{y}{2} + \frac{z}{3}}{2} > \frac{y}{2} \wedge \frac{\frac{y}{2} + \frac{z}{3}}{2} < \frac{z}{3}$$

Example

$$\exists x.\ \underbrace{2x > y \land 3x < z}_{F[x]}$$

Solving for x

$$\exists x.\ \underbrace{x > \frac{y}{2} \land x < \frac{z}{3}}_{F_3[x]}$$

Step 4: $F_{-\infty} \Leftrightarrow \bot$, $F_{+\infty} \Leftrightarrow \bot$, $F_3[\frac{y}{2}] \Leftrightarrow \bot$ and $F_3[\frac{z}{3}] \Leftrightarrow \bot$.

$$F_4 \ :\ \frac{\frac{y}{2} + \frac{z}{3}}{2} > \frac{y}{2} \land \frac{\frac{y}{2} + \frac{z}{3}}{2} < \frac{z}{3}$$

which simplifies to:

$$F_4 \ :\ 2z > 3y$$

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

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

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

Which quantifier free formula $G[y]$ is equivalent to F?

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

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

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

Which quantifier free formula $G[y]$ is equivalent to F?

There is no such formula!

No QE for $T_{\mathbb{Z}}$

UNI FREIBURG

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$*-formula* F *s.t.* $\text{free}(F) = \{y\}$. *Let*

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

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

No QE for $T_{\mathbb{Z}}$

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$. *Let*

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

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

Proof (Structural Induction over F)

Base case: F is an atomic formula:

$\top, \bot, t_1 = t_2, a \cdot y = t, t_1 < t_2, a \cdot y < t$.

- $\mathbb{Z}^+ \setminus S_\top = \mathbb{Z}^+ \cap S_\bot = \emptyset$ is finite
- $S_{t_1=t_2}$ and $S_{t_1<t_2}$ are either $S_\top$ or $S_\bot$.
- $\mathbb{Z}^+ \cap S_{a \cdot y = t}$, $(a \neq 0)$ has at most one element.
- $\mathbb{Z}^+ \cap S_{a \cdot y < t}$, $a > 0$ is finite.
- $\mathbb{Z}^+ \setminus S_{a \cdot y < t}$, $a < 0$ is finite.

No QE for $T_{\mathbb{Z}}$

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$. *Let*

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

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

Proof (Structural Induction over F)

Induction step: Assume property holds for F, G. Show it for $\neg F, F \wedge G, F \vee G, F \rightarrow G, F \leftrightarrow G$.

- $\neg F$: We have $\mathbb{Z}^+ \cap S_{\neg F} = \mathbb{Z}^+ \setminus S$ and $\mathbb{Z}^+ \setminus S_{\neg F} = \mathbb{Z}^+ \cap S$ and by ind.-hyp one of these sets is finite.
- $F \wedge G$: We have $\mathbb{Z}^+ \cap S_{F \wedge G} = (\mathbb{Z}^+ \cap S_F) \cap (\mathbb{Z}^+ \cap S_G)$ and $\mathbb{Z}^+ \setminus S_{F \wedge G} = (\mathbb{Z}^+ \setminus S_F) \cup (\mathbb{Z}^+ \setminus S_G)$.
  If the latter set is not finite then one of $\mathbb{Z}^+ \cap S_F$ or $\mathbb{Z}^+ \cap S_G$ is finite.
  In both cases $\mathbb{Z}^+ \cap S_{F \wedge G}$ is finite.

No QE for $T_{\mathbb{Z}}$

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$. Let

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

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

Proof (Structural Induction over F)

Induction step: Assume property holds for F, G. Show it for $\neg F, F \wedge G, F \vee G, F \rightarrow G, F \leftrightarrow G$.

- $F \vee G$ follows from previous, since $S_{F \vee G} = S_{\neg(\neg F \wedge \neg G)}$.
- $F \rightarrow G$ follows from $S_{F \rightarrow G} = S_{(\neg F \vee G)}$.
- $F \leftrightarrow G$ follows from $S_{F \leftrightarrow G} = S_{(F \rightarrow G) \wedge (G \rightarrow F)}$.

No QE for $T_{\mathbb{Z}}$

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$*. Let*

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

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

$\Sigma_{\mathbb{Z}}$-formula $\quad F \;:\; \exists x.\ 2x = y$ (with quantifier)

$\quad S_F$: even integers

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

No QE for $T_{\mathbb{Z}}$

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$. Let

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

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

$\Sigma_{\mathbb{Z}}$-formula $F : \exists x.\ 2x = y$ (with quantifier)

S_F: even integers

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

No QE for $T_{\mathbb{Z}}$

UNI FREIBURG

Lemma

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. $\text{free}(F) = \{y\}$. *Let*

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

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

$\Sigma_{\mathbb{Z}}$-formula $\quad F \; : \; \exists x.\, 2x = y$ (with quantifier)

$\quad S_F$: even integers

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

$$\Sigma_{\mathbb{Z}} \cup \{1|\cdot, 2|\cdot, 3|\cdot, \dots\}$$

Intended interpretations:

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

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

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

$$\Sigma_{\mathbb{Z}} \cup \{1|\cdot, 2|\cdot, 3|\cdot, \dots\}$$

Intended interpretations:

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

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

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

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

$$\Sigma_{\mathbb{Z}} \cup \{1|\cdot, 2|\cdot, 3|\cdot, \dots\}$$

Intended interpretations:

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

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

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

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.

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.

Put $F[x]$ in 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 $\exists x.\ F[x]$

Put $F[x]$ in 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 $\exists x.\ F[x]$

Example:

$$\exists x.\ \neg(x - 6 < z - x \wedge 4 \mid 5x + 1 \rightarrow 3x < y)$$

Cooper's Method: Step 1

Put $F[x]$ in 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 $\exists x.\ F[x]$

Example:

$$\exists x.\ \neg(x - 6 < z - x \wedge 4 \mid 5x + 1 \rightarrow 3x < y)$$

is equivalent to

$$\exists x.\ \neg(3x < y) \wedge x - 6 < z - x \wedge 4 \mid 5x + 1$$

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 $k \in \mathbb{Z}^+$.

Cooper's Method: Step 2

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 $k \in \mathbb{Z}^+$.

Example:

$\exists x.\ \neg(3x < y) \wedge x - 6 < z - x \wedge 4 \mid 5x + 1$

is equivalent to

$\exists x.\ y < 3x + 1 \wedge x - 6 < z - x \wedge 4 \mid 5x + 1$

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 $\exists x.\ F[x]$.

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 $\exists x.\ F[x]$.

Example:

$\exists x.\ y < 3x + 1 \wedge x - 6 < z - x \wedge 4 \mid 5x + 1$

is equivalent to

$\exists x.\ y - 1 < 3x \wedge 2x < z + 6 \wedge 4 \mid 5x + 1$

Cooper's Method: Step 4

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:

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

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

Replace δx terms in F_3' with a fresh variable x' to form

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

Finally, construct

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

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

(A) $x' < t$

(B) $t < x'$

(C) $k \mid x' + t$

(D) $\neg(k \mid x' + t)$

where t is a term that does not contain x, and $k \in \mathbb{Z}^+$.

Example: $\widehat{T_{\mathbb{Z}}}$-formula

$$\exists x.\ \underbrace{2x < z + 6 \land y - 1 < 3x \land 4 \mid 5x + 1}_{F_3[x]}$$

Collecting coefficients of x:

$$\delta = \text{lcm}(2, 3, 5) = 30$$

Multiply when necessary

$$\exists x.\ 30x < 15z + 90 \land 10y - 10 < 30x \land 24 \mid 30x + 6$$

Replacing $30x$ with fresh x'

$$\exists x'.\ \underbrace{x' < 15z + 90 \ \land\ 10y - 10 < x' \ \land\ 24 \mid x' + 6 \ \land\ 30 \mid x'}_{F_4[x']}$$

$\exists x'.\ F_4[x']$ is equivalent to $\exists x.\ F_3[x]$

Cooper's Method: Result of Step 4

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

(A) $x' < t$

(B) $t < x'$

(C) $k \mid x' + t$

(D) $\neg(k \mid x' + t)$

where t is a term that does not contain x, and $k \in \mathbb{Z}^+$.

Construct

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

of $F_4[x']$ by

(A) replacing literals $x' < t$ by $\top$

(B) replacing literals $t < x'$ by $\bot$

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

Let

$$\delta = \text{lcm}\left\{ \begin{array}{l} k \text{ of (C) literals } k \mid x' + t \\ k \text{ of (D) literals } \neg(k \mid x' + t) \end{array} \right\}$$

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

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

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

Cooper's Method: Step 5 (Example)

$$\exists x'.\ \underbrace{x' < 15z + 90 \land 10y - 10 < x' \land 24 \mid x' + 6 \land 30 \mid x'}_{F_4[x']}$$

Compute lcm: $\delta = lcm(24, 30) = 120$
Then

$$\begin{aligned} F_5 = & \bigvee_{j=1}^{120} \top \land \bot \land 24 \mid j + 6 \land 30 \mid j \\ & \lor \bigvee_{j=1}^{120} 10y - 10 + j < 15z + 90 \land 10y - 10 < 10y - 10 + j \\ & \qquad \land 24 \mid 10y - 10 + j + 6 \land 30 \mid 10y - 10 + j \end{aligned}$$

The formula can be simplified to:

$$F_5 = \bigvee_{j=1}^{120} 10y - 10 + j < 15z + 90 \land 24 \mid 10y - 10 + j + 6 \land 30 \mid 10y - 10 + j$$

Correctness of Step 5

Theorem

Let F_5 be the formula constructed from $\exists x'.\ F_4[x']$ as in Step 5. Then $\exists x'.\ F_4[x'] \Leftrightarrow F_5$.

Theorem

Let F_5 be the formula constructed from $\exists x'.\ F_4[x']$ as in Step 5. Then $\exists x'.\ F_4[x'] \Leftrightarrow F_5$.

Lemma[Periodicity]: For all atoms $k \mid x' + t$ in F_4, we have $k \mid \delta$.
Therefore, $k \mid x' + t$ iff $k \mid x' + \lambda\delta + t$ for all $\lambda \in \mathbb{Z}$.

Theorem

Let F_5 be the formula constructed from $\exists x'.\ F_4[x']$ as in Step 5. Then $\exists x'.\ F_4[x'] \Leftrightarrow F_5$.

Lemma[Periodicity]: For all atoms $k \mid x' + t$ in F_4, we have $k \mid \delta$.
Therefore, $k \mid x' + t$ iff $k \mid x' + \lambda\delta + t$ for all $\lambda \in \mathbb{Z}$.

Proof of Theorem

Theorem

Let F_5 be the formula constructed from $\exists x'.\ F_4[x']$ as in Step 5. Then $\exists x'.\ F_4[x'] \Leftrightarrow F_5$.

Lemma[Periodicity]: For all atoms $k \mid x' + t$ in F_4, we have $k \mid \delta$.
Therefore, $k \mid x' + t$ iff $k \mid x' + \lambda\delta + t$ for all $\lambda \in \mathbb{Z}$.

Proof of Theorem

$\Leftarrow$ If F_5 is true, there are two cases: $F_{-\infty}[j]$ is true or $F_4[t + j]$ is true.
If $F_4[t + j]$ is true, than obviously $\exists x'.\ F_4[x']$ is true. If $F_{-\infty}[j]$ is true, then (due to periodicity) $F_{-\infty}[j + \lambda \cdot \delta]$ is true.
If $\lambda < t - 1$ for all $t \in A \cup B$, then
$j + \lambda \cdot \delta < \delta + (t - 1)\delta = \delta t \leq t$. Thus,

$$F_{-\infty}[j + \lambda \cdot \delta] \Leftrightarrow F_4[j + \lambda \cdot \delta] \Rightarrow \exists x'.\ F_4[x'].$$

Correctness of Step 5

$\Rightarrow$ Assume for some x', $F_4[x']$ is true.

$\Rightarrow$ Assume for some x', $F_4[x']$ is true. If $\neg(t < x')$ for all $t \in B$, then choose $j_{x'} \in \{1, \dots, \delta\}$ such that $\delta \mid (j_{x'} - x')$. $j_{x'}$ will satisfy all (C) and (D) literals that x' satisfies. x' does not satisfy any (B) literal. Therefore if $F_4[x']$ is true, $F_{-\infty}[j]$ must be true. Therefore F_5 is true.
If $t < x'$ for some $t \in B$, then let

$$t_{x'} = \max\{t \in B | t < x'\}$$

and choose $j_{x'} \in \{1, \dots, \delta\}$ such that $\delta \mid (t_{x'} + j_{x'} - x')$. We claim that $F_4[t_{x'} + j_{x'}]$ is true.
Since $x' = t_{x'} + j_{x'} + \lambda\delta$, x' and $t_{x'} + j_{x'}$ satisfy the same (C) and (D) literals (due to periodicity).
Since $t_{x'} + j_{x'} > t_{x'} = \max\{t \in B | t < x'\}$, $t_{x'} + j_{x'}$ satisfies all (B) literals that are satisfied by x'.
Since $t_{x'} < x' = t_{x'} + j_{x'} + \lambda\delta \leq t_{x'} + (\lambda + 1)\delta$, we conclude that $\lambda \geq 0$. Hence, $x' \geq t_{x'} + j_{x'}$ and $t_{x'} + j_{x'}$ satisfies all (A) literals satisfied by x'.
Thus $F_4[t_x + j_x']$ is true. Therefore, F_5 is true.

Construct

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

of $F_4[x']$ by

(A) replacing literals $x' < t$ by $\top$

(B) replacing literals $t < x'$ by $\bot$

Let

$$\delta = \mathrm{lcm} \left\{ \begin{array}{l} k \text{ of (C) literals } k \mid x' + t \\ k \text{ of (D) literals } \neg(k \mid x' + t) \end{array} \right\}$$

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

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

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

In step 5, if there are fewer

(A) literals $x' < t$

than

(B) literals $t < x'$.

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

each (A) literal $x' < t$ by $\perp$

and

each (B) literal $t < x'$ by $\top$.

Then <u>right elimination</u>.

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

Symmetric Elimination (Example)

$$\exists x'.\ \underbrace{x' < 15z + 90 \land 10y - 10 < x' \land 24 \,|\, x' + 6 \land 30 \,|\, x'}_{F_4[x']}$$

Compute lcm: $\delta = lcm(24, 30) = 120$
Then

$$F_5 = \bigvee_{j=1}^{120} \bot \land \top \land 24 \,|\, -j + 6 \land 30 \,|\, -j$$
$$\lor \bigvee_{j=1}^{120} 15z + 90 - j < 15z + 90 \land 10y - 10 < 15z + 90 - j$$
$$\land\ 24 \,|\, 15z + 90 - j + 6 \land 30 \,|\, 15z + 90 - j$$

The formula can be simplified to:

$$F_5 = \bigvee_{j=1}^{120} 10y - 10 < 15z + 90 - j \land 24 \,|\, 15z + 90 - j + 6 \land 30 \,|\, 15z + 90 - j$$

Example

$$\underbrace{\exists x.\ (3x + 1 < 10 \lor 7x - 6 > 7) \land 2 \mid x}_{F[x]}$$

Example

$$\underbrace{\exists x.\ (3x + 1 < 10 \lor 7x - 6 > 7) \land 2 \mid x}_{F[x]}$$

Isolate x terms

$$\exists x.\ (3x < 9 \lor 13 < 7x) \land 2 \mid x\ ,$$

Example

$$\underbrace{\exists x.\ (3x + 1 < 10 \lor 7x - 6 > 7) \land 2 \mid x}_{F[x]}$$

Isolate x terms

$$\exists x.\ (3x < 9 \lor 13 < 7x) \land 2 \mid x\ ,$$

so

$$\delta = \mathrm{lcm}\{3, 7\} = 21\ .$$

Example

$$\underbrace{\exists x.\ (3x + 1 < 10 \lor 7x - 6 > 7) \land 2 \mid x}_{F[x]}$$

Isolate x terms

$$\exists x.\ (3x < 9 \lor 13 < 7x) \land 2 \mid x\ ,$$

so

$$\delta = \mathrm{lcm}\{3, 7\} = 21\ .$$

After multiplying coefficients by proper constants,

$$\exists x.\ (21x < 63 \lor 39 < 21x) \land 42 \mid 21x\ ,$$

we replace $21x$ by x':

$$\exists x'.\ \underbrace{(x' < 63 \lor 39 < x') \land 42 \mid x' \land 21 \mid x'}_{F_4[x']}\ .$$

Then

$$F_{-\infty}[x'] : \; (\top \vee \bot) \wedge 42 \mid x' \wedge 21 \mid x' \;,$$

Then

$$F_{-\infty}[x'] : \ (\top \vee \bot) \wedge 42 \mid x' \wedge 21 \mid x' \ ,$$

or, simplifying,

$$F_{-\infty}[x'] : \ 42 \mid x' \wedge 21 \mid x' \ .$$

Then

$$F_{-\infty}[x'] \;:\; (\top \lor \bot) \land 42 \mid x' \land 21 \mid x' \;,$$

or, simplifying,

$$F_{-\infty}[x'] \;:\; 42 \mid x' \land 21 \mid x' \;.$$

Finally,

$$\delta \;=\; \mathrm{lcm}\{21, 42\} \;=\; 42 \quad \text{and} \quad B \;=\; \{39\} \;,$$

so

$$F_5 \;:\; \begin{array}{l} \displaystyle\bigvee_{j=1}^{42} (42 \mid j \land 21 \mid j) \;\lor \\ \quad \displaystyle\bigvee_{j=1}^{42} ((39 + j \;<\; 63 \lor 39 \;<\; 39 + j) \land 42 \mid 39 + j \land 21 \mid 39 + j) \;. \end{array}$$

Since $42 \mid 42$ and $21 \mid 42$, the left main disjunct simplifies to $\top$, so that F is $\widehat{T_{\mathbb{Z}}}$-equivalent to $\top$. Thus, F is $\widehat{T_{\mathbb{Z}}}$-valid.

Quantifier elimination decides validity/satisfiable quantified formulae.

Can also be used for quantifier free formulae:
To decide satisfiability of $F[x_1, \ldots, x_n]$,
apply QE on $\exists x_1, \ldots, x_n.\ F[x_1, \ldots, x_n]$.

Quantifier elimination decides validity/satisfiable quantified formulae.

Can also be used for quantifier free formulae:
To decide satisfiability of $F[x_1, \ldots, x_n]$,
apply QE on $\exists x_1, \ldots, x_n.\ F[x_1, \ldots, x_n]$.

But high complexity (doubly exponential for $T_{\mathbb{Q}}$).

Decision Procedures for Quantifier-free Fragments

Quantifier elimination decides validity/satisfiable quantified formulae.

Can also be used for quantifier free formulae:
To decide satisfiability of $F[x_1, \ldots, x_n]$,
apply QE on $\exists x_1, \ldots, x_n.\ F[x_1, \ldots, x_n]$.

But high complexity (doubly exponential for $T_{\mathbb{Q}}$).

Therefore, we are looking for a fast procedure.