CS156: The Calculus of Computation

Zohar Manna
Autumn 2008

Chapter 7: Quantified Linear Arithmetic

Quantifier Elimination (QE)

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

Note: Could be enough if F is equisatisfiable to G, that is F is satisfiable iff G is satisfiable

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

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

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 $\widehat{T_\mathbb{Z}}$ be $T_\mathbb{Z}$ with divisibility predicates $|$.
For $\widehat{\Sigma_\mathbb{Z}}$-formula
    $F: \ \exists x. \ 2x = y$,
a quantifier-free $\widehat{T_\mathbb{Z}}$-equivalent $\widehat{\Sigma_\mathbb{Z}}$-formula is
    $G: \ 2 \mid y$.

About 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

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

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

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

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

$$G_5 \ : \ F_4$$

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 $F[y]$ s.t. free($F[y]$) = $\{y\}$.
$F[t]$ represents the set of integers

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

Either $S \cap \mathbb{Z}^+$ or $\mathbb{Z}^+ \setminus S$ is finite.
<u>Note</u>: $\mathbb{Z}^+$ is the set of positive integers.

<u>Example:</u> $\Sigma_{\mathbb{Z}}$-formula $\quad F[y] : \exists x.\ 2x = y$
$\quad S$: 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 $F[y]$.
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 <u>divisibility predicates</u>
$\quad k \mid \cdot \quad$ for $k \in \mathbb{Z}^+$
Intended interpretations:
$\quad k \mid x$ holds iff k divides x without any remainder

<u>Example:</u>
$\quad x > 1 \wedge y > 1 \wedge 2 \mid x + y$
is satisfiable (choose $x = 2, y = 2$).
$\quad \neg(2 \mid x) \wedge 4 \mid x$
is not satisfiable.

<u>Axioms of $\widehat{T_{\mathbb{Z}}}$:</u> 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)

<u>Algorithm:</u> 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.

Cooper's Method: Step 1

Put $F[x]$ in Negation Normal Form (NNF) $F_1[x]$, so that $\exists x.\ F_1[x]$

- ▶ has negations only in literals (only $\wedge$, $\vee$)
- ▶ is $\widehat{T_{\mathbb{Z}}}$-equivalent to $\exists x.\ F[x]$

<u>Example:</u>

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

is equivalent to

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

Cooper's Method: Step 2

Replace (left to right)

$$s = t \iff s < t+1 \land t < s+1$$
$$\neg(s = t) \iff s < t \lor t < s$$
$$\neg(s < t) \iff t < s+1$$

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:

$$\neg(x < y) \land \neg(x = y+3)$$
$$\Downarrow$$
$$y < x+1 \land (x < y+3 \lor y+3 < x)$$

Cooper's Method: Step 3

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 (does not contain x) 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:

$$x + x + y < z + 3z + 2y - 4x \qquad\qquad 5| - 7x + t$$
$$\Downarrow \qquad\qquad\qquad\qquad\qquad \Downarrow$$
$$6x < 4z + y \qquad\qquad\qquad\qquad 5|7x - t$$

Cooper's Method: Step 4 I

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:

$hx < t$	$\iff \delta'x < h't$	where $h'h = \delta'$
$t < hx$	$\iff h't < \delta'x$	where $h'h = \delta'$
$k \mid hx + t$	$\iff h'k \mid \delta'x + h't$	where $h'h = \delta'$
$\neg(k \mid hx + t)$	$\iff \neg(h'k \mid \delta'x + h't)$	where $h'h = \delta'$

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

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

Cooper's Method: Step 4 II

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

Cooper's Method: Step 4 III

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

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

After step 3:

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

Collecting coefficients of x (step 4):

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

Multiply when necessary:

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

Cooper's Method: Step 4 IV

Multiply when necessary:

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

Replacing $30x$ with fresh x' and adding divisibility conjunct:

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

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

Cooper's Method: Step 5

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

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

and B be the set of terms t appearing in (B) literals of $F_4[x']$.

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

Intuition of Step 5 I

Property (Periodicity)

if $m\mid\delta$

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

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

By the choice of δ (lcm of the k's) — no $\mid$ literal in F_5 can distinguish between n and $n+\lambda\delta$, for any $\lambda\in\mathbb{Z}$.

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

Intuition of Step 5 II

- ► <u>left disjunct</u> $\bigvee_{j=1}^{\delta} F_{-\infty}[j]$:

    Contains only | literals
    Asserts: no least $n \in \mathbb{Z}$ s.t. $F_4[n]$.
    For if there exists n satisfying $F_{-\infty}$,
    then every $n - \lambda\delta$, for $\lambda \in \mathbb{Z}^+$, also satisfies $F_{-\infty}$

- ► <u>right disjunct</u> $\bigvee_{j=1}^{\delta} \bigvee_{t \in B} F_4[t+j]$:

    Asserts: There is least $n \in \mathbb{Z}$ s.t. $F_4[n]$.
    For let t^* be the largest t in (B) = {largest $t \mid t < x'$ in (B)}.
    If $n \in \mathbb{Z}$ is s.t. $F_4[n]$, then

    $$\exists j (1 \le j \le \delta). \ t^* + j \le n \ \wedge \ F_4[t^* + j]$$

    In other words,
    if there is a solution,
    then one must appear in δ interval to the right of t^*

Example of Step 5 I

$$\exists x. \ \underbrace{3x + 1 > y \ \wedge \ 2x - 6 < z \ \wedge \ 4 \mid 5x + 1}_{F[x]}$$
$$\Downarrow$$
$$\exists x'. \ \underbrace{x' < 15z + 90 \ \wedge \ 10y - 10 < x' \ \wedge \ 24 \mid x' + 6 \ \wedge \ 30 \mid x'}_{F_4[x']}$$

By step 5,

$$F_{-\infty}[x] : \ \top \ \wedge \ \bot \ \wedge \ 24 \mid x' + 6 \ \wedge \ 30 \mid x' \,,$$

which simplifies to $\bot$.

Example of Step 5 II

Compute

$$\delta = \text{lcm}\{24, 30\} = 120 \quad \text{and} \quad B = \{10y - 10\} \,.$$

Then replacing x' by $10y - 10 + j$ in $F_4[x']$ produces

$$F_5 : \bigvee_{j=1}^{120} \left[\begin{array}{l} 10y - 10 + j < 15z + 90 \ \wedge \ 10y - 10 < 10y - 10 + j \\ \wedge \ 24 \mid 10y - 10 + j + 6 \ \wedge \ 30 \mid 10y - 10 + j \end{array} \right]$$

which simplifies to

$$F_5 : \bigvee_{j=1}^{120} \left[\begin{array}{l} 10y + j < 15z + 100 \ \wedge \ 0 < j \\ \wedge \ 24 \mid 10y + j - 4 \ \wedge \ 30 \mid 10y - 10 + j \end{array} \right] \,.$$

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

Cooper's Method: Example I

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

Isolate x terms

$$\exists x. \ (3x < 9 \ \vee \ 13 < 7x) \ \wedge \ 2 \mid x \,,$$

so

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

After multiplying coefficients by proper constants,

$$\exists x. \ (21x < 63 \ \vee \ 39 < 21x) \ \wedge \ 42 \mid 21x \,,$$

we replace $21x$ by x':

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

Cooper's Method: Example II

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

so F_5 :
$$\bigvee_{j=1}^{42} (42 \mid j \land 21 \mid j) \lor$$
$$\bigvee_{j=1}^{42} ((39 + j < 63 \lor 39 < 39 + j) \land 42 \mid 39 + j \land 21 \mid 39 + j) .$$

Since $42 \mid 42$ and $21 \mid 42$, the left main disjunct simplifies to $\top$, so that F_5 is $\widehat{T_{\mathbb{Z}}}$-equivalent to $\top$. Thus, $\exists x.\ F[x]$ is $\widehat{T_{\mathbb{Z}}}$-valid.

Cooper's Method: Example I

$$\exists x.\ \underbrace{2x = y}_{F[x]}$$

Rewriting
$$\exists x.\ \underbrace{y - 1 < 2x \land 2x < y + 1}_{F_3[x]}$$

Then
$$\delta' = \operatorname{lcm}\{2, 2\} = 2 ,$$

so by Step 4
$$\exists x'.\ \underbrace{y - 1 < x' \land x' < y + 1 \land 2 \mid x'}_{F_4[x']}$$

$F_{-\infty}$ produces $\bot$.

Cooper's Method: Example II

However,
$$\delta = \operatorname{lcm}\{2\} = 2 \quad \text{and} \quad B = \{y - 1\} ,$$

so
$$F_5 : \bigvee_{j=1}^{2} (y - 1 < y - 1 + j \land y - 1 + j < y + 1 \land 2 \mid y - 1 + j)$$

Simplifying,
$$F_5 : \bigvee_{j=1}^{2} (0 < j \land j < 2 \land 2 \mid y - 1 + j)$$

and then
$$F_5 : 2 \mid y ,$$

which is quantifier-free and $\widehat{T_{\mathbb{Z}}}$-equivalent to $\exists x.\ F[x]$.

Improvement: Symmetric Elimination

In step 5, if there are fewer

    (A) literals $x' < t$

than

    (B) literals $t < x'$,

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

    (A) literal $x' < t$ by $\bot$

than

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

Then right elimination.

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

Improvement: Eliminating Blocks of Quantifiers I

Given
$$\exists x_1. \cdots \exists x_n. \; F[x_1, \ldots, x_n]$$
where F quantifier-free.
Eliminating x_n (left elimination) produces

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

which is equivalent to

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

Improvement: Eliminating Blocks of Quantifiers II

Treat j as a free variable and examine only $1 + |B|$ formulae
- $\exists x_1. \cdots \exists x_{n-1}. \; F_{-\infty}[x_1, \ldots, x_{n-1}, j]$
- $\exists x_1. \cdots \exists x_{n-1}. \; F_4[x_1, \ldots, x_{n-1}, t+j]$ for each $t \in B$

Example I

$$F: \; \exists y. \exists x. \; x < -2 \; \wedge \; 1 - 5y < x \; \wedge \; 1 + y < 13x$$

Since $\delta' = \text{lcm}\{1, 13\} = 13$

$$\exists y. \exists x. \; 13x < -26 \; \wedge \; 13 - 65y < 13x \; \wedge \; 1 + y < 13x$$

Then

$$\exists y. \exists x'. \; x' < -26 \; \wedge \; 13 - 65y < x' \; \wedge \; 1 + y < x' \; \wedge \; 13 \mid x'$$

There is one (A) literal $x' < \ldots$ and two (B) literals $\ldots < x'$, we use right elimination.

$$F_{+\infty} = \bot \qquad \delta = \{13\} = 13 \qquad A = \{-26\}$$

$$\exists y. \bigvee_{j=1}^{13} \left[\begin{array}{c} -26 - j < -26 \; \wedge \; 13 - 65y < -26 - j \\ \wedge \; 1 + y < -26 - j \; \wedge \; 13 \mid -26 - j \end{array} \right]$$

Example II

Commute

$$G[j]: \; \bigvee_{j=1}^{13} \exists y. \; j > 0 \; \wedge \; 39 + j < 65y \; \wedge \; y < -27 - j \; \wedge \; 13 \mid -26 - j$$

Treating j as free variable (and removing $j > 0$), apply QE to

$$H[j]: \; \exists y. \; 39 + j < 65y \; \wedge \; y < -27 - j \; \wedge \; 13 \mid -26 - j$$

Simplify. . .

$$H'[j]: \; \bigvee_{k=1}^{65} (k < -1794 - 66j \; \wedge \; 13 \mid -26 - j \; \wedge \; 65 \mid 39 + j + k)$$

Replace $H[j]$ with $H'[j]$ in $G[j]$

$$\bigvee_{j=1}^{13} \bigvee_{k=1}^{65} (k < -1794 - 66j \; \wedge \; 13 \mid -26 - j \; \wedge \; 65 \mid 39 + j + k)$$

Example III

This qff formula is $\widehat{\mathcal{T}_{\mathbb{Z}}}$-equivalent to F.

Quantifier Elimination over Rationals

$$\Sigma_{\mathbb{Q}} : \{0, 1, +, -, =, \geq\}$$

Recall: we use $>$ instead of $\geq$, as

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

Ferrante & Rackoff's Method

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.

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

by

1. putting $F[x]$ in NNF,
2. replacing negated literals,
3. solving literals s.t. x appears isolated on one side, and
4. taking finite disjunction $\bigvee_t F[t]$.

Ferrante & Rackoff's Method: Steps 1 and 2

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

Step 2: Replace literals (left to right)

$$\neg(s < t) \ \Leftrightarrow\ t < s \ \lor\ t = s$$
$$\neg(s = t) \ \Leftrightarrow\ t < s \ \lor\ t > s$$

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

Ferrante & Rackoff's Method: Step 3

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

$$t_1 < cx + t_2 \qquad \Rightarrow \qquad \frac{t_1 - t_2}{c} < x$$

where $c \in \mathbb{Z} - \{0\}$.

All atoms 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.

Ferrante & Rackoff's Method: Step 4 I

Construct from $F_3[x]$
- left infinite projection $F_{-\infty}$ by replacing
  - (A) atoms $x < t$ by $\top$
  - (B) atoms $t < x$ by $\bot$
  - (C) atoms $x = t$ by $\bot$
- right infinite projection $F_{+\infty}$ 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 t terms from (A), (B), (C) atoms.
Construct the final

$$F_4: \ F_{-\infty} \lor F_{+\infty} \lor \bigvee_{s,t \in S} F_3\left[\frac{s+t}{2}\right] ,$$

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

Ferrante & Rackoff's Method: Step 4 II

- $F_{-\infty}$ captures the case when small $x \in \mathbb{Q}$ satisfy $F_3[x]$
- $F_{+\infty}$ captures the case when large $x \in \mathbb{Q}$ satisfy $F_3[x]$
- last disjunct: for $s, t \in S$
  if $s \equiv t$, check whether $s \in S$ satisfies $F_3[s]$
  if $s \not\equiv t$, in any $T_{\mathbb{Q}}$-interpretation,
  - $|S| - 1$ pairs $s, t \in S$ are adjacent. For each such pair, (s, t) is an interval in which no other $s' \in S$ lies.
  - Since $\frac{s+t}{2}$ represents the whole interval (s, t), simply check $F_3[\frac{s+t}{2}]$.

Ferrante & Rackoff's Method: Intuition

Step 4 says that four cases are possible:

1. There is a left open interval s.t. all elements satisfy $F(x)$.

$$\overline{\qquad\longleftrightarrow)\qquad}$$

2. There is a right open interval s.t. all elements satisfy $F(x)$.

$$\overline{\qquad(\longleftrightarrow\qquad}$$

3. Some term t satisfies $F(x)$.

$$\overline{\cdots \quad t \quad \cdots}$$

4. There is an open interval between two s, t terms s.t. every element satisfies $F(x)$.

$$\overline{\cdots \ \ s \uparrow t \ \ \cdots} \atop \frac{s+t}{2}$$

Correctness of Step 4 I
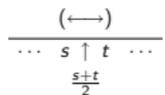
Theorem
*Let F_4 be the formula constructed from $\exists x.\ F_3[x]$ as in Step 4.
Then $\exists x.\ F_3[x] \Leftrightarrow F_4$.*

Proof:
$\Leftarrow$ If F_4 is true, then $F_{-\infty}$, F_∞ or $F_3[\frac{s+t}{2}]$ is true.
If $F_3[\frac{s+t}{2}]$ is true, then obviously $\exists x.\ F_3[x]$ is true.
If $F_{-\infty}$ is true, choose some small $x, x < t$ for all $t \in S$.
Then $F_3[x]$ is true.
If $F_{+\infty}$ is true, choose some big $x, x > t$ for all $t \in S$.
Then $F_3[x]$ is true.

Correctness of Step 4 II

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

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

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

Otherwise choose largest $s \in S$ with $\alpha_I[s] < v$ and smallest
$t \in S$ with $\alpha_I[t] > v$.

Since no atom of F_3 can distinguish between values in interval
(s, t),

$$I \models F_3[v] \text{ iff } I \models F_3 \left[\frac{s+t}{2} \right] .$$

Hence, $I \models F[\frac{s+t}{2}]$.

Correctness of Step 4 III

In all cases $I \models F_4$.

Ferrante & Rackoff's Method: Example I

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

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

Solving for x

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

Step 4: $x < 3$ in (A) $\Rightarrow$ $F_{-\infty} = \bot$
 $x > \frac{13}{7}$ in (B) $\Rightarrow$ $F_{+\infty} = \bot$

$$F_4 : \bigvee_{s,t \in S} \underbrace{\left(\frac{s+t}{2} < 3 \ \wedge \ \frac{s+t}{2} > \frac{13}{7} \right)}_{F_3[\frac{s+t}{2}]}$$

Ferrante & Rackoff's Method: Example II

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

$$F_3 \left[\frac{3+3}{2} \right] = \bot \qquad F_3 \left[\frac{\frac{13}{7} + \frac{13}{7}}{2} \right] = \bot$$

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

simplifies to $\top$.

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

Example

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

Solving for x

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

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

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

which simplifies to:

$$F_4 : 2z > 3y$$

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