Quantifier Elimination

Helpful lemmas

Let S be a set of sentences.

Lemma

$S \models F$ iff $S \models \forall F$

Lemma

If $S \models F \leftrightarrow G$ then $S \models H[F] \leftrightarrow H[G]$,
i.e. one can replace a subformula F of H by G.

Quantifier elimination

Definition

If $T \models F \leftrightarrow F'$ we say that F and F' are T-equivalent.

Definition

A theory T admits quantifier elimination if for every formula F there is a quantifier-free T-equivalent formula G such that $fv(G) \subseteq fv(F)$. We call G a quantifier-free T-equivalent of F.

Examples

In linear real arithmetic:

$$\exists x \exists y\ (3 * x + 5 * y = 7)\ \leftrightarrow\ ?$$
$$\forall y\ (x < y \land y < z)\ \leftrightarrow\ ?$$
$$\exists y\ (x < y \land y < z)\ \leftrightarrow\ ?$$

Quantifier elimination

A quantifier-elimination procedure (QEP) for a theory T and a set of formulas $\mathcal{F}$ is a function that computes for every $F \in \mathcal{F}$ a quantifier-free T-equivalent.

Lemma

Let T be a theory such that

- *T has a QEP for all formulas and*
- *for all ground formulas G, $T \models G$ or $T \models \neg G$, and it is decidable which is the case.*

Then T is decidable and complete.

Simplifying quantifier elimination: one $\exists$

Fact
If T has a QEP for all $\exists x\, F$ where F is quantifier-free, then T has a QEP for all formulas.

Essence: It is sufficient to be able to eliminate a single $\exists$

Construction:

Given: a QEP $qe1$ for formulas of the form $\exists x\, F$ where F is quantifier-free

Define: a QEP for all formulas
Method: Eliminate quantifiers bottom-up by $qe1$, use $\forall \equiv \neg\exists\neg$

Simplifying quantifier elimination: $\exists x \bigwedge literals$

Lemma

If T has a QEP for all $\exists x\, F$ where F is a conjunction of literals,
all of which contain x,
then T has a QEP for all $\exists x\, F$ where F is quantifier-free.

Construction:

Given: a QEP $qe1c$ for formulas of the form $\exists x\, (L_1 \wedge \cdots \wedge L_n)$
where each L_i is a literal that contains x

Define: $qe1(\exists x\, F)$ where F is quantifier-free
Method: DNF; miniscoping; $qe1c$

This is the end of the generic part of quantifier elimination.
The rest is theory specific.

Eliminating "$\neg$"

Motivation: $\neg x < y \;\leftrightarrow\; y < x \lor y = x$ for linear orderings

Assume that there is a computable function *aneg* that maps every negated atom to a quantifier-free and negation-free T-equivalent formula.

Lemma

If T has a QEP for all $\exists x\, F$ where F is a conjunction of atoms, all of which contain x,
then T has a QEP for all $\exists x\, F$ where F is quantifier-free.

Construction:

Given: a QEP *qe1ca* for formulas of the form $\exists x\,(A_1 \land \cdots \land A_n)$ where each atom A_i contains x

Define: $qe1(\exists x\, F)$ where F quantifier-free
Method: NNF; *aneg*; DNF; miniscoping; *qe1ca*

Quantifier Elimination
Dense Linear Orders Without Endpoints

Dense Linear Orders Without Endpoints

$\Sigma = \{<, =\}$

Let DLO stand for "dense linear order without endpoints" and for the following set of axioms:

$$\forall x \forall y \forall z\, (x < y \land y < z \to x < z)$$

$$\forall x\, \neg(x < x)$$

$$\forall x \forall y\, (x < y \lor x = y \lor y < x)$$

$$\forall x \forall z\, (x < z \to \exists y\, (x < y \land y < z))$$

$$\forall x \exists y\, x < y$$

$$\forall x \exists y\, y < x$$

Models of DLO?

Theorem

All countable DLOs are isomorphic.

Quantifier elimination example

Example

$DLO \models \exists y\ (x < y \land y < z)\ \leftrightarrow$

Eliminiation of "$\neg$"

Elimination of negative literals (function *aneg*):

$DLO \models \neg x = y \leftrightarrow x < y \lor y < x$

$DLO \models \neg x < y \leftrightarrow x = y \lor y < x$

Quantifier elimination for conjunctions of atoms

QEP $qe1ca(\exists x\ (A_1 \wedge \cdots \wedge A_n)$ where x occurs in all A_i:

1. Eliminate "$=$": Drop all A_i of the form $x = x$.

If some A_i is of the form $x = y$ (x and y different), eliminate $\exists x$:

$$\exists x\ (x = t \wedge F) \ \equiv\ F[t/x] \qquad (x \text{ does not occur in } t)$$

Otherwise:

2. Eliminate $x < x$: return $\bot$

3. Separate atoms into lower and upper bounds for x and use

$$DLO \models\ \exists x(\bigwedge_{i=1}^{m} l_i < x \wedge \bigwedge_{j=1}^{n} x < u_j)\ \leftrightarrow\ \bigwedge_{i=1}^{m}\bigwedge_{j=1}^{n} l_i < u_j$$

Special case: $\bigwedge_{k=1}^{0} F_k = \top$

Examples

$\exists x\ (x < z \wedge y < x \wedge x < y')\ \leftrightarrow$?

$\forall x\ (x < y)\ \leftrightarrow$?

$\exists x \exists y \exists z\ (x < y \wedge y < z \wedge z < x)\ \leftrightarrow$?

Complexity

Quadratic blow-up with each elimination step

$\Rightarrow$ Eliminating all $\exists$ from

$$\exists x_1 \dots \exists x_m \; F$$

where F has length n needs $O(\quad)$, assuming F is DNF.

Consequences

- $Cn(DLO)$ has quantifier elimination
- $Cn(DLO)$ is decidable and complete
- All models of DLO (for example $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$) are elementarily equivalent:
  you cannot distinguish models of DLO by first-order formulas.

Quantifier Elimination
Linear real arithmetic

Linear real arithmetic

$\mathcal{R}_+ = (\mathbb{R}, 0, 1, +, <, =)$, $R_+ = Th(\mathcal{R}_+)$

For convenience we allow the following additional function symbols:
For every $c \in \mathbb{Q}$:

- c is a constant symbol
- $c\cdot$, multiplication with c, is a unary function symbol

A term in normal form: $c_1 \cdot x_1 + \ldots + c_n \cdot x_n + c$
where $c_i \neq 0$, $x_i \neq x_j$ if $i \neq j$.

Every atom A is R_+-equivalent to an atom $0 \bowtie t$ in normal form (NF) where $\bowtie \in \{<, =\}$ and t is in normal form.

An atom is solved for x if it is of the form $x < t$, $x = t$ or $t < x$ where x does not occur in t.
Any atom A in normal form that contains x can be transformed into an R_+-equivalent atom solved for x.
Function $sol_x(A)$ solves A for x.

Eliminiation of "¬"

Elimination of negative literals (function *aneg*):

$R_+ \models \neg x = y \leftrightarrow x < y \vee y < x$

$R_+ \models \neg x < y \leftrightarrow x = y \vee y < x$

Fourier-Motzkin Elimination

QEP $qe1ca(\exists x\ (A_1 \wedge \cdots \wedge A_n)$, all A_i in NF and contain x:

1. Let $S = \{sol_x(A_1), \ldots, sol_x(A_n)\}$
2. Eliminate "$=$":

If $(x = t) \in S$ for some t, eliminate $\exists x$:

$$\exists x\ (x = t \wedge F)\ \equiv\ F[t/x] \qquad (x \text{ does not occur in } t)$$

Otherwise return

$$\bigwedge_{(l<x)\in S}\ \bigwedge_{(x<u)\in S} l < u$$

Special case: empty $\bigwedge$ is $\top$

All returned formulas are implicitly put into NF.

Examples

$\exists x \exists y\ (3x + 5y < 7 \wedge 2x - 3y < 2)\ \leftrightarrow$?
$\exists x \forall y\ (3y \leq x \vee x \leq 2y)\ \leftrightarrow$?

Can DNF be avoided?

Ferrante and Rackoff's theorem

Theorem

Let F be quantifier-free and negation-free and assume all atoms that contain x are solved for x. Let S_x be the set of atoms in F that contain x. Let $L = \{l \mid (l < x) \in S_x\}$, $U = \{u \mid (x < u) \in S_x\}$, $E = \{t \mid (x = t) \in S_x\}$. Then

$$R_+ \models \exists x\, F \;\leftrightarrow\; F[-\infty/x] \vee F[\infty/x] \vee \bigvee_{t \in E} F[t/x] \vee \bigvee_{l \in L} \bigvee_{u \in U} F[0.5(l+u)/x]$$

(note: empty $\bigvee$ is $\bot$) where $F[-\infty/x]$ ($F[\infty/x]$) is the following transformation of all solved atoms in F:

$$\begin{aligned} x < t &\mapsto \top\ (\bot) \\ t < x &\mapsto \bot\ (\top) \\ x = t &\mapsto \bot\ (\bot) \end{aligned}$$

Examples

$\exists x\, (y < x \wedge x < z) \;\leftrightarrow\; ?$

$\exists x\, x < y \;\leftrightarrow\; ?$

Ferrante and Rackoff's procedure

Define $qe1(\exists x\ F)$:

1. Put F into NNF, eliminate all negations, put all atoms into normal form, solve those atoms for x that contain x.
2. Apply Ferrante and Rackoff's theorem.

Theorem

Eliminating all quantifiers with Ferrante and Rackoff's procedure from a formula of size n takes space $O(2^{cn})$ and time $O(2^{2^{dn}})$.

Quantifier Elimination

Presburger Arithmetic

See [Harrison] or [Enderton] under “Presburger”

Presburger Arithmetic

Linear integer arithmetic: $\mathcal{Z}_+ := (\mathbb{Z}, +, 0, 1, \leq)$

A problem with $\mathcal{Z}_+$:

$\mathcal{Z}_+ \models \exists x \; x + x = y \;\; \leftrightarrow$?

Fact Linear integer arithmetic does not have quantifier elimination

Presburger Arithmetic is linear integer arithmetic extended with the unary functions "$2 \mid .$", "$3 \mid .$", ...

(Alternative: "$. = . \pmod 2$", "$. = . \pmod 3$", ...)

Notation: $\mathcal{P} := \mathcal{Z}_+$ extended with "$k \mid .$"

For convenience: add constants $c \in \mathbb{Z}$ and multiplication with constants $c \in \mathbb{Z}$

Normal form of atoms:

$0 \leq c_1 \cdot x_1 + \ldots + c_n \cdot x_n + c$

$k \mid c_1 \cdot x_1 + \ldots + c_n \cdot x_n + c$

where $c_i \neq 0$ and $k \geq 1$

Where necessary, atoms are put into normal form

Presburger Arithmetic

Elimination of $\neg$:

$$\mathcal{Z}_+ \models \neg\, s \leq t \leftrightarrow t+1 \leq s$$

$$\mathcal{Z}_+ \models \neg\, k \mid t \leftrightarrow k \mid t+1 \vee k \mid t+2 \vee \cdots \vee k \mid t+(k-1)$$

Elimination of $\neg \mid$ expensive and not really necessary.
Can treat $\neg \mid$ like $\mid$

Quantifier Elimination for $\mathcal{P}$

Step 1

$qe1ca(\exists x\ F)$
where $F = A_1 \wedge \cdots \wedge A_l$
where all A_i are atoms in normal form which contain x

Step 1: Set all coeffs of x in F to 1 or -1:

1. Set all coeffs of x in F to the lcm m of all coeffs of x
2. Set all coeffs of x to 1 or -1 and add $\wedge\ m \mid x$

Quantifier Elimination for $\mathcal{P}$

Step 1

$qe1ca(\exists x\ A_1 \wedge \cdots \wedge A_l)$

Step 1: Set all coeffs of x in F to 1 or -1

The details, in one step:

Let m be the (positive) lcm of all coeffs of x (eg lcm $\{-6, 9\} = 18$)

Let R be $coeff1(A_1) \wedge \cdots \wedge coeff1(A_l)\ \wedge m \mid x$ (result)

where

$coeff1(0 \leq c_1 \cdot x_1 + \ldots + c_n \cdot x_n + c) = (0 \leq c'_1 \cdot x_1 + \ldots + c'_n \cdot x_n + c')$

$coeff1(d \mid c_1 \cdot x_1 + \ldots + c_n \cdot x_n + c) = (d' \mid c'_1 \cdot x_1 + \ldots + c'_n \cdot x_n + c')$

$x_k = x$

$m' = m/|c_k|$

$c'_i = m' \cdot c_i$ if $i \neq k$

$c'_k = if\ \ c_k > 0\ then\ 1\ else\ -1$

$c' = m' \cdot c$

$d' = m' \cdot d$

Lemma $\mathcal{P} \models (\exists x\ F) \leftrightarrow (\exists x\ R)$

Quantifier Elimination for $\mathcal{P}$

Step 2

$$A_L := \text{set of all } 0 \le x + t \text{ in } R \qquad L := \{-t \mid (0 \le x + t) \in A_L\}$$
$$A_U := \text{set of all } 0 \le -x + t \text{ in } R \qquad U := \{t \mid (0 \le -x + t) \in A_U\}$$

$D :=$ the set of all $d \mid t$ in R

$m :=$ the (pos.) lcm of $\{d \mid (d \mid t) \in D \text{ for some } t\}$

The quantifier-free result:

$$R' := \quad \textit{if } L = \emptyset$$
$$\text{then } \bigvee_{i=0}^{m-1} \bigwedge D[i/x]$$
$$\text{else } \bigvee_{i=0}^{m-1} \bigvee_{l \in L} R[l+i/x]$$

Optimisation: use U instead of L

Lemma (Periodicity Lemma)

If $A \in D$, i.e. $A = (d \mid x + t)$ and $x \notin fv(T)$, and $i \equiv j \pmod d$ then $\mathcal{P} \models A[i/x] \leftrightarrow A[j/x]$.