A Survey of Quantifier Elimination: Syntactic and Semantic Approaches

Ting Zhang
Stanford
June 7, 2002

Alfred Tarski

Outline

- Preliminaries
- Basic Theory
- Syntactic Approaches
- Semantic Approaches

Notations

- $\mathscr{L}$: a first-order language.
- C: an arbitrarily large set of new constants.

  The size of C is arbitrarily large so that we never run out of constant symbols to name objects under consideration.
- $\mathscr{L}_C$: the new language augmented by C.
- $\mathfrak{A}$: a $\mathscr{L}$-structure with domain A.

  We identify A with a set of constants such that each of objects in domain A is named by itself in $\mathscr{L}_A$. Also write $\mathscr{L}_{\mathfrak{A}}$ for $\mathscr{L}_A$ when it is clear from the context.
- $(\mathfrak{A}, A)$: the expansion structure of $\mathfrak{A}$ in language $\mathscr{L}_{\mathfrak{A}}$.

Diagrams

Definition 0.1 (Diagrams). *Let $\mathfrak{A}$ and $\mathscr{L}_{\mathfrak{A}}$ as defined above. A digram $\Delta_{\mathfrak{A}}$ is the set of all basic sentences (i.e., atomic sentences or negated atomic sentences) of $\mathscr{L}_{\mathfrak{A}}$ which are true in $\mathfrak{A}$. Similarly an elementary digram $\Theta_{\mathfrak{A}}$ is the set of all sentences of $\mathscr{L}_{\mathfrak{A}}$ which are true in $\mathfrak{A}$, i.e., the theory $Th(\mathfrak{A}, A)$ in language $\mathscr{L}_{\mathfrak{A}}$.*

An elementary digram is a complete description of $\mathfrak{A}$ in language $\mathscr{L}_{\mathfrak{A}}$ and diagram is a partial description using only quantifier-free sentences.

Lemma 0.1 (Robinson's diagram Lemma). *Let $\mathfrak{A}$ and $\mathscr{L}_{\mathfrak{A}}$ as defined above. Let $\mathfrak{B}$ be a $\mathscr{L}_{\mathfrak{A}}$-structure.*

1. *If $\mathfrak{B} \models \Delta_{\mathfrak{A}}$, then $\mathfrak{A}$ can be embedded into $\mathfrak{B}|\mathscr{L}$.*
2. *If $\mathfrak{B} \models \Theta_{\mathfrak{A}}$, then $\mathfrak{A}$ can be elementarily embedded into $\mathfrak{B}|\mathscr{L}$.*

Quantifier Elimination

Definition 0.2 (Quantifier Elimination)**.** *A first-order theory T is said to have quantifier elimination if for any formula $\phi(\bar{x})$ there is a quantifier free formula $\psi(\bar{x})$ such that*

$$T \models \forall \bar{x}(\phi(\bar{x}) \leftrightarrow \psi(\bar{x}))$$

Remark 0.1. *Assume $\mathscr{L}$ contains at least one constant symbol or $\phi(\bar{x})$ contains at least one free variable.*

Remark 0.2. *For any first-order theory T there is a conservative extension T' of T such that T' has elimination of quantifiers.*

Remark 0.3. *If T has elimination of quantifiers, then for any model $\mathfrak{A}$ of T, $Th(\mathfrak{A}, A)$ also admits elimination of quantifiers.*

Elimination Set

Definition 0.3 (Elimination Set)**.** *Let* $\mathbf{K}$ *be a class of* $\mathscr{L}$*-structures. We say a set* Φ *of formulas is an elimination set for* $\mathbf{K}$ *if*

> *any formula* $\phi(\bar{x})$ *is equivalent (in every structure of* $\mathbf{K}$*) to a formula* $\psi(\bar{x})$ *which is a boolean combination of formulas in* Φ*.*

We say Φ is an *elimination set* for theory T if Φ is an elimination set for $Mod(T)$.

Hence T admits quantifier elimination if and only if the set of quantifier-free formulas forms an elimination set of T.

We say a $\mathscr{L}$-structure $\mathfrak{A}$ has elimination of quantifiers if $Th(\mathfrak{A})$ does.

Elimination Set (Cont'd)

Theorem 0.1. *Let Φ be a set of formulas. Suppose that*

- *every atomic formula or negated atomic formula of $\mathscr{L}$ is in Φ, and*
- *for every formula $\theta(\bar{x})$ of $\mathscr{L}$ which is of form $\exists y \bigwedge \psi_i(\bar{x}, y)$ with ψ in Φ (called primitive formula with respect to Φ), there is a formula $\theta^*(\bar{x})$ of $\mathscr{L}$ which*
  - *is a boolean combination of formulas in Φ, and*
  - *is equivalent to θ in every structure in $\mathbf{K}$.*

Then Φ is an elimination set for $\mathbf{K}$.

Critirion of Elimination Set

Desired properties of an elimination set Φ of a theory T.

1. Φ is reasonably small and nonredundant.
2. Every formula in Φ has straightforward mathematical meaning.
3. There exists an effective procedure to reduce every formula to a boolean combination of formulas in Φ.
4. There exists an effective procedure to decide whether a formula in Φ is provable or refutable from T.

With (1)-(4) T is a complete and decidable theory.

The Point of Quantifier Elimination

- Classification up to elementary equivalence
- Completeness proofs
- Decidability proofs
- Constructive decision procedures
- Description of definable relations
- Description of elementary embeddings

Slogan: "..., the method [of elimination of quantifiers] is extremely valuable when we want to beat a particular theory into the ground." (Chang & Keisler)

Schema for syntactic approaches

- Reduce formulas to certain normal forms.
- Guess an elimination set Φ.
- Let Ψ be a set of formulas of the form $\exists x \phi$ where ϕ is a boolean combination of formulas in Φ. Find a ranking function $rank : \Psi \to \mathbb{N}$.
- For every formula ϕ in Ψ find a T-equivalent formula ϕ in Ψ with $rank(\psi) < rank(\phi)$.
- Reduce ϕ of rank 0 to a boolean combination of formulas in Φ.

Logical Theories

- Dense linear orders (DeLO)
- Discrete linear orders (DiLO)
- Presburger arithmetic (PA)
- Atomless boolean algebras (ABA)
- Algebraically closed fields (ACF)
- Real closed fields (RCF)

Dense Linear Orderings (DeLO)

Dense linear orders with first and last elements.

- **Language**: $\mathscr{L} = \{<, 0, 1\}$.
- **Axioms**:
  - Axioms of linear orders.
  - Axiom of denseness
    - $\forall x \forall y (x < y \rightarrow \forall z (x < z \wedge z < y))$
  - Axioms of boundedness.
    - $\forall x (x < 1 \vee x = 1)$
    - $\forall x (0 < x \vee x = 0)$

QE of DeLO

Primitive formulas of *DeLO* are of the form

$$\exists x(\bigwedge_{i<l} t_i < x \wedge \bigwedge_{j<m} x < u_j \bigwedge_{k<n} x = v_k)$$

where t_i, u_j and v_k are terms not involving x.

Without loss of generality assume $n = 0$. It suffices to show how to eliminate the quantifier in

$$\phi(x) = \exists x(\bigwedge_{i<l} t_i < x \wedge \bigwedge_{j<m} x < u_j)$$

Define $rank(\phi(x)) = l + m$.

QE of DeLO (con'd)

1. $l > 1$. The formula $\phi(x)$ is equivalent to

$$\big(t_0 < t_1 \wedge \exists x(t_1 < x \wedge \bigwedge_{1<i<l} t_i < x \wedge \bigwedge_{j<m} x < u_j)\big)$$
$$\bigvee \big(\neg t_0 < t_1 \wedge \exists x(t_0 < x \wedge \bigwedge_{1<i<l} t_i < x \wedge \bigwedge_{j<m} x < u_j)\big)$$

2. $m > 1$. Similar to $l > 1$.

3. $l = m = 1$. The formula $\phi(x)$ is equivalent to $t_0 < u_0$.

4. $l = 0, m = 1$. The formula $\phi(x)$ is equivalent to $u_0 \neq 0$.

5. $l = 1, m = 0$. The formula $\phi(x)$ is equivalent to $t_0 \neq 1$.

Discrete Linear Orderings (DiLO)

Discrete linear orders with first and last elements.

- **Language**: $\mathscr{L} = \{<, S\}$.
- **Axioms**:
  - Axioms of linear orders.
  - Axiom of discreteness.
    - $\forall x \forall y (x < y \leftrightarrow y = Sx \vee Sx < y))$
  - Axioms of unboundedness.
    - $\forall x \exists y (x = Sy)$
    - $\forall x \exists y (Sy = x)$

QE of DiLO

Primitive formulas of $DiLO$ are of the form

$$\exists x(\bigwedge_{i<l} t_i < S^{p_i}x \wedge \bigwedge_{j<m} S^{q_j}x < u_j \bigwedge_{k<n} S^{r_k}x = v_k)$$

where t_i, u_j and v_k are terms with no occurrence of x.

Since $S^i x < t \leftrightarrow S^{i+j} < S^j t$, by uniforming all terms $S^i x$ to $S^n x$ and replacing $S^n x$ by a new variable y, the primitive formulas of $DiLO$ can be written in the same as those of $DeLO$.

As before it suffices to show how to eliminate the quantifier in

$$\phi(x) = \exists x(\bigwedge_{i<k} t_i < x \wedge \bigwedge_{j<l} x < u_j)$$

QE of DiLO (Cont'd)

- $k > 1$:

$$\big(t_0 < t_1 \wedge \exists x(t_1 < x \wedge \bigwedge_{1<i<k} t_i < x \wedge \bigwedge_{j<l} x < u_j)\big)$$
$$\bigvee \big(\neg t_0 < t_1 \wedge \exists x(t_0 < x \wedge \bigwedge_{1<i<k} t_i < x \wedge \bigwedge_{j<l} x < u_j)\big)$$

- $l > 1$. Similar to $k > 1$.

QE of DiLO (Cont'd)

- $k = l = 1$:

$$\phi(x) \leftrightarrow t_0 < u_0 \wedge St_0 \neq u_0$$

- $k = 0$ or $l = 0$:

$$\phi(x) \leftrightarrow x = x$$

Remark 0.4. *Similar approaches can apply for DeLO, DiLO with all following combinations of conditions on existence of first and last elements.*

DeLO/DiLO + w/o "the first element" + w/o "the last element"

Presburger Arithmetic

- **Language**: $\mathscr{L} = \{0, 1, +, -, <\}$.
- **Axioms**:
  - Axioms of commutative group.
  - Axioms of linear orders with respect to group structure:
    * $\forall x \forall y (x > 0 \wedge y > 0 \rightarrow x + y > 0)$
    * $\forall x \neg (x > 0 \wedge -x > 0)$
    * $\forall x (x = 0 \vee x > 0 \vee -x > 0)$
  - Axiom of discrete orders
    * $\forall x (x > 0 \leftrightarrow (x = 1 \vee x - 1 > 0))$

Presburger Arithmetic (Cont'd)

The theory in $\mathscr{L}$ doesn't admit elimination of quantifiers. E.g.,

$$\exists y(y + y = x)$$

is not equivalent to any quantifier-free formulas.

- Extended language:
  $\mathscr{L}' = \{0, 1, +, -, <, n \mid, n \nmid \text{ for each } n > 1\}$.
- Definitional axioms: $\forall x(\neg n \mid x \leftrightarrow n \nmid x)$ for each $n > 1$.
- Axioms of divisibility
  - $\forall x(n \mid x \leftrightarrow \exists y(x = ny))$ for each $n > 1$
  - $\forall x(n \mid x \vee n \mid x + 1 \vee \cdots \vee n \mid x + n - 1)$ for each $n > 1$

QE of PA

- Eliminate negations. Replace $\neg t_1 = t_2$ by $t_2 < t_1 \vee t_1 < t_2$. Replace $\neg(t_1 < t_2)$ by $t_2 < t_1 \vee t_1 = t_2$. And replace $\neg n \mid x$ by $n \nmid x$ and $\neg n \nmid x$ by $n \mid x$.

  Atomic formulas are in the following forms

  $$ax < t,\ u < bx,\ e \mid cx + v,\ f \nmid dx + w$$

  where t, u, v and w are terms not involving x and $a, b, c, d, e,\ f$ are positive integers. It suffices to show to how to eliminate quantifiers of $\exists x \varphi(x)$ with $\varphi(x)$ be a positive boolean combination of atomic formulas of the above form.

  $\exists x \varphi(x) = \exists x \mathcal{B}^+(a_i x < t_i,\ u_j < b_j x,\ e_k \mid c_k x + v_k,\ f_l \nmid d_l x + w_l)$

QE of PA (Cont'd)

- Unify the coefficient of x. Let n be the LCM of all coefficients of x in $\phi(x)$. Raise the coefficient of x to n by multiplying appropriate factors. Observe that

$$\exists x \phi(x) \leftrightarrow \exists x \phi'(nx)$$

where ϕ' is obtained from ϕ by multiplying appropriate factors to terms.

- Eliminate the coefficient of x. Use the fact that

$$\exists x \phi(nx) \leftrightarrow \exists x (\phi(x) \wedge n \mid x)$$

QE of PA (Cont'd)

- Instantiate x with all combinations.

  δ: the L.C.M. of all e, f in $\phi(x)$.

  $\varphi_{-\infty}(x)$: the formula obtained from $\varphi(x)$ with formulas of form $x < t$ replaced by $true$ and formulas of form $u < x$ replaced by $false$.

  The formula $\exists x \phi(x)$ is equivalent to

$$\bigvee_{i=1}^{\delta} \varphi_{-\infty}(i) \vee \bigvee_{i=1}^{\delta} \bigvee_{u_j} \varphi(u_j + i)$$

QE of PA (Cont'd)

- Example

$$\exists x \varphi(x) = \exists x F(3x < y + 2,\ 2y + 1 < 5x,\ z < 2x,\ 2 \nmid 3x)$$

where F is a positive boolean function.

- Normalization

$$\begin{aligned} & \exists x \varphi(x) \\ \leftrightarrow\quad & \exists x F(30x < 10y + 20,\ 12y + 6 < 30x, \\ & \qquad 15z < 30x,\ 20 \nmid 30x) \\ \leftrightarrow\quad & \exists x \big(F'(x < 10y + 20,\ 12y + 6 < x, \\ & \qquad 15z < x,\ 20 \nmid x) \wedge 30 \mid x\big) \end{aligned}$$

QE of PA (Cont'd)

- Instantiation

$$\bigvee_{i=1}^{30} F'\ (true,\ false,\ false,\ 20 \nmid i,\ 30 \mid i) \vee$$

$$\bigvee_{i=1}^{30} \big(F'(12y + 6 + i < 10y + 20,\ 12y + 6 < 12y + 6 + i,$$

$$15z < 12y + 6 + i,\ 20 \nmid 12y + 6 + i,\ 30 \mid 12y + 6 + i)$$

$$\wedge\ \ F'(15z + i < 10y + 20,\ 12y + 6 < 15z + i,$$

$$15z < 15z + i,\ 20 \nmid 15z + i,\ 30 \mid 15z + i)\big)$$

Atomless Boolean Algebra

- **Language**: $\mathscr{L} = \{0, 1, +, \cdot, -, <\}$.
- **Axioms**:
  - Axioms of boolean algebra.
  - Axioms of dense partial ordering:
    - $\forall x \forall y (x < y \rightarrow \exists z (x < z \wedge z < y))$, or equivalently $\forall x (0 < x \rightarrow \exists z (0 < z \wedge z < x))$
- **Example**

$$\mathcal{A} = \langle\ \mathbb{Q}^*,\ \cup,\ \cap,\ \setminus,\ \emptyset,\ \mathbb{Q}^+\ \rangle$$

where $\mathbb{Q}^+$ are non-negative rational numbers and $\mathbb{Q}^*$ is the set of finite unions of intervals of the form $[a, b)$ with $a, b \in \mathbb{Q}^+$.

QE of ABA

- Eliminate symbol <.

$$x < y \leftrightarrow x \cdot y = y \wedge x \neq y$$

- Normalize equalities and inequalities.

$$t_1 = t_2 \leftrightarrow t_1 \cdot (-t_2) = 0 \;\wedge\; (-t_1) \cdot t_2 = 0$$

$$t_1 \neq t_2 \leftrightarrow t_1 \cdot (-t_2) \neq 0 \;\vee\; (-t_1) \cdot t_2 \neq 0$$

$$t_1 + t_2 = 0 \leftrightarrow t_1 = 0 \wedge t_2 = 0$$

$$t_1 + t_2 \neq 0 \leftrightarrow t_1 \neq 0 \vee t_2 \neq 0$$

QE of ABA (Cont'd)

- Primitive formulas are in the following form:

$$\exists x \varphi(x) = \exists x (f(x) = 0 \wedge \bigwedge_i g_i(x) \neq 0)$$

Theorem 0.2. *Let $f_x(a)$ denote the formula obtained by replacing all occurrence of x in f by a.*

- *for boolean algebra*

$$\exists x (f(x) = 0 \wedge g(x) \neq 0) \leftrightarrow$$
$$f_x(0) \cdot f_x(1) = 0 \wedge (-f_x(1)) \cdot g_x(1) + (-f_x(0)) \cdot g_x(0) \neq 0$$

- *for atomless boolean algebra*

$$\exists x (f(x) = 0 \wedge \bigwedge_i g_i(x) \neq 0) \leftrightarrow \bigwedge \exists x (f(x) = 0 \wedge g_i(x) \neq 0)$$

Algebraically Closed Fields

- **Language**: $\mathscr{L} = \{0, 1, +, -, \cdot\}$.
- **Axioms**:
  - Axioms of fields.
  - Axioms of algebraic closure.

    for all $n \geq 0$,

$$\forall x_0 \cdots \forall x_n \exists y (x_n \cdot y^n + \cdots + x_1 \cdot y + x_0 = 0)$$

QE of ACF

The primitive formulas of ACF are of the form

$$\exists x(\bigwedge_{i<m} t_i = 0 \wedge \bigwedge_{j<n} u_j \neq 0)$$

Note that $u \neq 0$ is equivalent to

$$\exists z(z \cdot u - 1 = 0)$$

So it suffices to show how to eliminate the quantifier in

$$\varphi(x) = \exists x(\bigwedge_{i<m} t_i = 0)$$

QE of ACF (Cont'd)

- $m = 1$. $\varphi(x)$ is equivalent to $0 = 0$.
- $m > 1$. Let the term of the highest degree in t_i be $a_i x^{n_i}$. Define $rank(\phi(x)) = \Sigma_{i=0}^{m} n_i$. Assume that $n_0 \geq n_1$. Let

$$t'_0 = a_1 t_0 - a_0 x^{n_0 - n_1} t_1 \text{ and } t'_1 = t_1 - a_1 x^{n_1}$$

The formula $\varphi(x)$ is equivalent to (by Euclidean algorithm)

$$\big(a_1 = 0 \land \exists x(t_0 = 0 \land t'_1 = 0 \land \bigwedge_{1<i<m} t_i = 0)\big)$$
$$\bigvee \big(a_1 \neq 0 \land \exists x(t'_0 = 0 \land t_1 = 0 \land \bigwedge_{1<i<m} t_i = 0)\big)$$

Note that $deg(t'_0) < deg(t_0)$ and $deg(t'_1) < deg(t_1)$, i.e., the rank is decreasing.

QE of ACF (Cont'd)

- **Example**

$$
\begin{aligned}
\varphi(x) &= \exists x(6x^2 + 3x + 10 = 0 \wedge 3x + 1 = 0) \\
&\leftrightarrow \big(3 = 0 \wedge \exists x(6x^2 + 3x + 10 = 0 \wedge 1 = 0)\big) \\
&\qquad \bigvee \big(3 \neq 0 \wedge \exists x(x + 10 = 0 \wedge 3x + 1 = 0)\big) \\
&\leftrightarrow 3 \neq 0 \wedge \Big(\big(3 = 0 \wedge \exists x(x + 10 = 0 \wedge 1 = 0)\big) \\
&\qquad \bigvee \big(3 \neq 0 \wedge \exists x(29 = 0 \wedge 3x + 1 = 0)\big)\Big) \\
&\leftrightarrow 3 \neq 0 \wedge 29 = 0 \wedge \exists x(3x + 1 = 0) \\
&\leftrightarrow 29 = 0
\end{aligned}
$$

Real Closed Fields

- **Language**: $\mathscr{L} = \{0, 1, +, -, \cdot, <\}$.
- **Axioms**:
  - Axioms of ordered fields.
    * Axioms of fields.
    * Axioms of linear orders.
    * $\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$
    * $\forall x \forall y \forall z (x < y \wedge 0 < z \rightarrow x \cdot z < y \cdot z)$
  - Axioms of real closure.
    * $\forall x (0 < x \rightarrow \exists y (y^2 = x))$
    * for all odd $n > 0$

$$\forall x_0 \cdots \forall x_n \exists y (x_n \cdot y^n + \cdots + x_1 \cdot y + x_0 = 0)$$

QE of RCF

- Normalization.

  Let $\varphi(y_1, \ldots, y_m)$ be a formula with $y_1, \ldots, y_m$ free. The formula φ can be written in the following prenex form

  $$Q_1 x_1, \ldots, Q_n x_n \psi(y_1, \ldots, y_m, x_1, \ldots, x_n)$$

  where $Q_i \in \{\exists, \forall\}$ and ψ is a boolean combination of polynomial equalities and inequalities of the following two forms:

  $$f_i(y_1, \ldots, y_m, x_1, \ldots, x_n) = 0$$

  $$f_i(y_1, \ldots, y_m, x_1, \ldots, x_n) > 0$$

  Let $\mathcal{F}$ denote all polynomials which occur in ψ.

QE of RCF (Cont'd)

- Cylindrical algebraic decomposition. Construct a sequence of finite partitions $\Pi_1, \ldots, \Pi_{m+n}$ with the following properties.
  - Each Π_i is a finite partition of $\mathbb{R}^i$. The elements in Π_i are called i-dimensional "cells".
  - Π_{i+1} is a refinement of $\Pi_i \times \mathbb{R}$ in the sense that the cells of Π_i are exactly projections of cells of Π_{i+1} and for each cell C of Π_i we can effectively construct the stack of cells C_{i+1} of Π_{i+1} which partition $C \times \mathbb{R}$.

QE of RCF (Cont'd)

- Cylindrical algebraic decomposition (Cont'd).
  - Each cell C in Π_m is described by a quantifier free formula $\delta_C(y_1, \ldots, y_m)$.
  - For each cell C in Π_{m+n}, $\mathcal{F}$ is sign invariant and there is a sample point α_C which is described by a quantifier free formula.
- Complexity

$$\left(|\mathcal{F}| \cdot deg(\mathcal{F})\right)^{2^{O(m+n)}}$$

where $|\mathcal{F}|$ is the number of polynomials in $\mathcal{F}$ and $deg(\mathcal{F})$ is the maximum degree of any polynomial in $\mathcal{F}$.

QE of RCF (Cont'd)

- Construct decision trees from partitions $\Pi_{m+1}, \ldots, \Pi_{m+n}$.

  For each cell C in $\mathbb{R}^m$ build a decision tree T_C as follows.

  - The tree is of depth n with the root C at depth 0.
  - If C is a node at depth i, its children are all cells of Π_{m+i+1} which are cylindrical over C.
  - If Q_i is $\forall$ (resp. $\exists$) then all nodes at depth $i-1$ is conjunctive (resp. disjunctive).
  - Let the valuation of T_C be $\theta_C(y_1, \ldots, y_m)$. Then formula $\varphi(y_1, \ldots, y_m, x_1, \ldots, x_n)$ is equivalent to

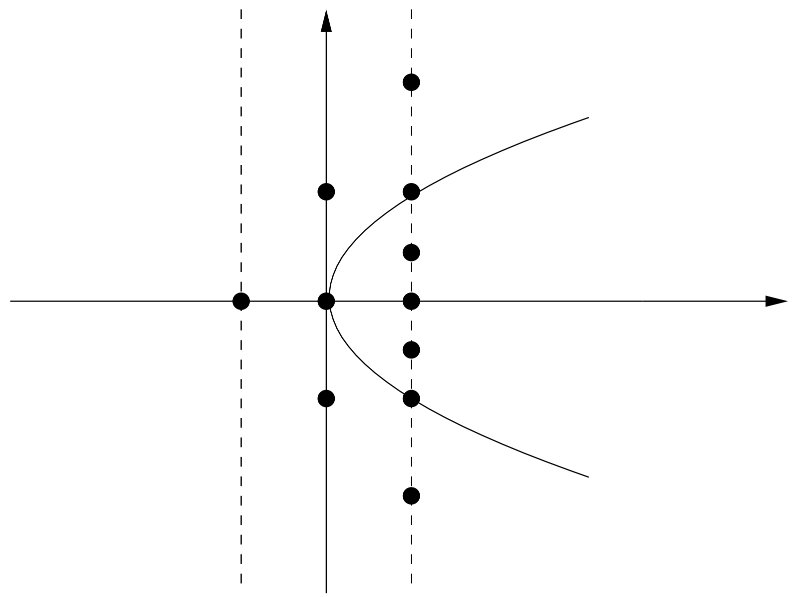
$$\bigvee_{C \in \Pi_m} \delta_C(y_1, \ldots, y_m) \wedge \theta_C(y_1, \ldots, y_m)$$

QE of RCF (Cont'd)

Example

$$(\exists x)(\forall y)(y^2 - x > 0)$$

CAD of $\{y^2 - x\}$:



QE of RCF (Cont'd)

Sample points for the CAD of $\{y^2 - x\}$ are as follows:

$$\{\ (-1,0)\ \},\quad \left\{\begin{array}{c}(0,1)\\(0,0)\\(0,-1)\end{array}\right\},\quad \left\{\begin{array}{c}(1,2)\\(1,1)\\(1,1/2)\\(1,0)\\(1,-1/2)\\(1,-1)\\(1,-2)\end{array}\right\}$$

QE of RCF (Cont'd)

The equivalent quantifier-free sentence is

$$
\begin{array}{ll}
 & (0 - (-1) > 0) \\
\bigvee & \big((1 - 0 > 0) \wedge (0 - 0 > 0) \wedge (1 - 0 > 0)\big) \\
\bigvee & \big((4 - 1 > 0) \wedge (1 - 1 > 0) \wedge (1/4 - 1 > 0) \\
 & (0 - 1 > 0) \wedge (1/4 - 1 > 0) \wedge (1 - 1 > 0) \wedge (4 - 1 > 0)\big)
\end{array}
$$

which is $true$.

A Bit of History on RCF

- Artin & Schreier [1927]
- Tarski [1948, 1951], Seidenberg [1954]
- Lojasiewicz [1964, 1965]
- Fischer & Rabin [1974]
- Collins [1975], Monk & Solovay [1972]
- Grigor'ev [1988], Renegar [1992]
- Basu, Pollack & Roy [1996], Basu [1999]

Model Completeness

Definition 0.4. *A first-order theory T is said to be model complete if for every model $\mathfrak{A}$ of T, $T \cup \Delta_{\mathfrak{A}}$ is a complete theory in language $\mathscr{L}_{\mathfrak{A}}$.*

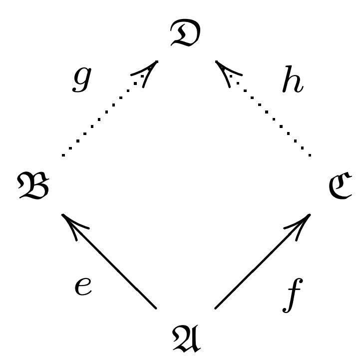
Theorem 0.3 (Robinson)**.** *A first-order theory T is model complete if and only if every formula is equivalent (modulo T) to an existential formula.*

Remark 0.5. *Completeness and model completeness are two different properties of a theory. Generally neither one implies the other. The theory $Th(\mathfrak{N})$ of Peano arithmetic is a complete theory, but obviously it is not model complete. The theory of algebraically closed field is model complete, but not complete.*

Amalgamation Property

Definition 0.5. *Let* $\mathbf{K}$ *be a class of* $\mathscr{L}$*-structures. We say that* $\mathbf{K}$ *has amalgamation property if the following property holds:*

> *If* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ *are in* $\mathbf{K}$ *and* $e : \mathfrak{A} \mapsto \mathfrak{B}$ *and* $f : \mathfrak{A} \mapsto \mathfrak{C}$ *are embeddings, then there exists* $\mathfrak{D}$ *in* $\mathbf{K}$ *and embeddings* $g : \mathfrak{B} \mapsto \mathfrak{D}$ *and* $h : \mathfrak{C} \mapsto \mathfrak{D}$ *such that* $e \circ g = f \circ h$*, i.e., the following diagram commutes.*



Theorem 0.4. *If* $\mathbf{K}$ *is closed under direct product, then* $\mathbf{K}$ *has amalgamation property.*

Existentially Closed Structures

Definition 0.6. *Let* $\mathbf{K}$ *be a class of* $\mathscr{L}$*-structures. We say that a structure* $\mathfrak{A}$ *in* $\mathbf{K}$ *is existentially closed (e.c.) if*

> *for every existential formula* $\phi(\bar{x})$ *of* $\mathscr{L}$ *and every tuple* $\bar{a}$ *in* A*, if there exists a structure* $\mathfrak{B}$ *such that* $\mathfrak{A} \subseteq \mathfrak{B}$ *and* $\mathfrak{B} \models \phi(\bar{a})$*, then* $\mathfrak{A} \models \phi(\bar{a})$*.*

Theorem 0.5 (Hilbert's Nullstellensatz)**.** *If* $\mathfrak{A}$ *is a algebraically closed field, then a finite system of equalities and inequalities is solvable in an extension field* $\mathfrak{B}$ *of* $\mathfrak{A}$ *if and only if it is already solvable in* $\mathfrak{A}$*.*

Corollary 0.1. *Existentially closed fields are exactly algebraically closed fields.*

Eklof-Sabbagh's Test

Theorem 0.6. *Let* $\mathbf{K}$ *be a class of* $\mathscr{L}$*-structures. If the class of all substructures of structures in* $\mathbf{K}$ *has amalgamation property, then the class of all existentially closed structures in* $\mathbf{K}$ *admits quantifier elimination.*

Theorem 0.7. *A first-order theory* T *has elimination of quantifiers if and only if* T *is model complete and* $T_\forall$ *has amalgamation property.*

Eklof-Sabbagh's Test (Cont'd)

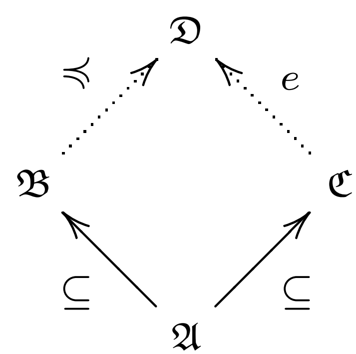
Example 0.1. *Algebraically closed fields have elimination of quantifiers. Justification:*

- *The class of existentially closed fields is exactly the class of algebraically closed fields.*
- *The class of substructures of fields is exactly the class of integral domains.*
- *The class of integral domains has amalgamation property since it is closed under direct product.*

Shoenfield's Test I (Submodel Completeness)

Definition 0.7. *A first-order theory T is said to be submodel complete if for every substructure $\mathfrak{A}$ of a model of T, $T \cup \Delta_{\mathfrak{A}}$ is a complete theory in language $\mathscr{L}_{\mathfrak{A}}$.*

Equivalently the following diagram commutes where $\mathfrak{A}$ is a common substructure of models $\mathfrak{B}$, $\mathfrak{C}$ and $\mathfrak{D}$ of T, and e is an elementary embedding of $\mathfrak{C}$ over $\mathfrak{A}$ into $\mathfrak{D}$.



Theorem 0.8 (Shoenfield)**.** *A theory T admits elimination of quantifiers if and only if T is submodel complete.*

Type

Definition 0.8. *Let $\mathfrak{A}$ be a structure and X a subset of domain of $\mathfrak{A}$. A set $\Phi(x)$ of formulas with parameters of X is called to be a* 1*-type over X with respect to $\mathfrak{A}$ if there exists an elementary extension $\mathfrak{B}$ of $\mathfrak{A}$ such that $\mathfrak{B} \models \Phi(b)$ for some $b \in B$. $\Phi(x)$ is called a complete* 1*-type if it is maximal w.r.t. the above property.*

A complete 1-type over X w.r.t. $\mathfrak{A}$ is all that we can say about a possible element using parameters in X. Such an element may already exist in $\mathfrak{A}$ or only exists in an elementary extension of $\mathfrak{A}$.

Example 0.2. *Consider the structure $\mathfrak{A} = \langle \mathbb{Q}, < \rangle$. Since $\mathfrak{A}$ admits elimination of quantifiers, all* 1*-types are quantifier-free* 1*-types. The subset of $\mathbb{Q}$ defined by a* 1*-type over X ($X \subseteq A$) is a finite union of open intervals or points.*

Saturation

Definition 0.9. *A $\mathscr{L}$-structure $\mathfrak{A}$ is said to be λ-saturated if*

> *For any $X \subseteq A$ with $|X| < \lambda$, $\mathfrak{A}$ realizes all types over X with respect to $\mathfrak{A}$.*

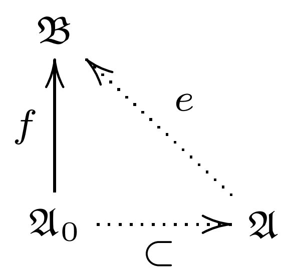
We say that $\mathfrak{A}$ is saturated if $\mathfrak{A}$ is $|A|$-saturated.

Example 0.3. *Consider again the structure $\mathfrak{A} = \langle \mathbb{Q}, < \rangle$. By the property of denseness, $\mathfrak{A}$ realizes all 1-types over any X of finite cardinality. Hence $\mathfrak{A}$ is saturated.*

Shoenfield's Test II

Theorem 0.9. *A theory T admits elimination of quantifiers if and only if the following condition is satisfied.*

> *For any models $\mathfrak{A}$, $\mathfrak{B}$ of T such that $|A| \leq \lambda$ and $\mathfrak{B}$ is λ^+-saturated, any embedding f of a substructure $\mathfrak{A}_0$ of $\mathfrak{A}$ into $\mathfrak{B}$ can be extended to an embedding e of $\mathfrak{A}$ into $\mathfrak{B}$.*
> *I.e., the following diagram commutes.*



Shoenfield's Test II (Cont'd)

Example 0.4. *ACF admits elimination of quantifier.*

Let f be an embedding of a substructure $\mathfrak{A}_0$ of $\mathfrak{A}$ into $\mathfrak{B}$. Suppose $A_0 \neq A$ and let $a \in A \setminus A_0$. Find corresponding a' in B as follows.

1. The element a is algebraic over A.

   Let g be minimal polynomial defining a with coefficients from A_0. Choose solution a' in B such that $g(a') = 0$.

2. The element a is transcendental over A. Let $\Phi(x)$ be

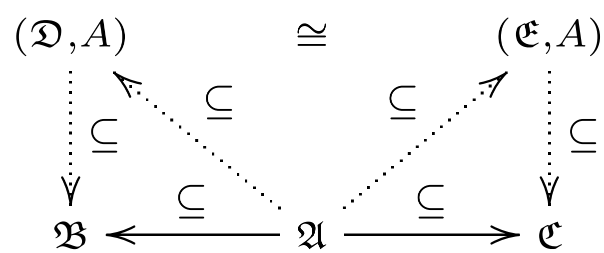
   $$\{g(x) \neq 0 : g(x) \text{ is a polynomial with coefficients from } A_0.\}$$

   Choose $a' \in B$ such that $\mathfrak{B} \models \Phi(a')$.

Almost Universal Theories

Theorem 0.10. *A theory T is said to be almost universal*

if $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ are $\mathscr{L}$-structures such that $\mathfrak{B}$, $\mathfrak{C}$ are models of T, $\mathfrak{A} \subseteq \mathfrak{C}$ and $\mathfrak{B} \subseteq \mathfrak{C}$, then there exists models $\mathfrak{D}$, $\mathfrak{E}$ of T such that $\mathfrak{A} \subseteq \mathfrak{D} \subseteq \mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{E} \subseteq \mathfrak{C}$ and $(\mathfrak{D}, A) \cong (\mathfrak{E}, A)$.



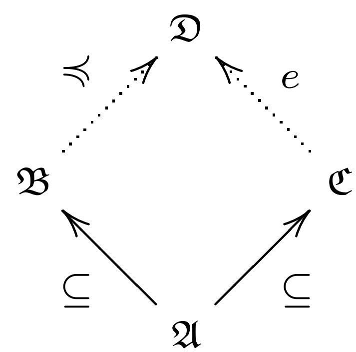
Lemma 0.2. *Universal theories are almost universal.*

Theorem 0.11. *LOR, FEI, ORF are almost universal theories.*

Model Completion

Definition 0.10. *Let T, T^* be two theories with $T \subseteq T^*$. T^* is said to be model-completion of T if*

> *For any three $\mathscr{L}$-structures $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ such that $\mathfrak{B}$, $\mathfrak{C}$ are models of T^*, $\mathfrak{A}$ is a model of T and $\mathfrak{A} \subseteq \mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{C}$, there exists an elementary extension $\mathfrak{D}$ of $\mathfrak{B}$ such that $\mathfrak{C}$ can be elementarily embedded into $\mathfrak{D}$ over A. I.e, the following diagram commutes.*



Robinson's Test

Theorem 0.12. *If T is almost universal theory and T^* is the model completion of T, then T^* admits quantifier elimination.*

Lemma 0.3. *Each of the following pairs of theories have the model completion relation.*

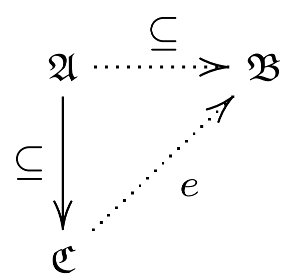
- *ACF is the model completion of FEI.*
- *RCF is the model completion of ORF.*
- *DeLO is the model completion of LOR.*

Corollary 0.2. *ACF, RCF and DeLO all admit quantifier elimination.*

Existence of T-Closure

Definition 0.11. *Let T be a theory in $\mathscr{L}$ and $\mathfrak{A}$ be a substructure of a model of T. A structure $\mathfrak{C}$ is said to be a T-closure of $\mathfrak{A}$ if*

> *$\mathfrak{C}$ is a model of T and $\mathfrak{C}$ can be embedded over $\mathfrak{A}$ into any model $\mathfrak{B}$ of T which extends $\mathfrak{A}$. In other words, the following diagram commutes.*



A theory T is said to have T-closure property if every substructure of a model of T has a T-closure.

Specializability of Selected Elements

Definition 0.12. *A theory T is said to have the property of specializability of selected elements if it satisfies the following condition:*

> *If $\mathfrak{A}$ is a model of T and $\mathfrak{B}$ is a proper substructure of $\mathfrak{A}$, then there are an element $b \in B \setminus A$ and a set $\Phi(x)$ of quantifier-free formulas such that $\mathfrak{B} \models \bigwedge \Phi(b)$, $\Phi(x)$ determines quantifier-free type of b over A and for any finite subset $\Psi(x)$ of $\Phi(x)$, $\mathfrak{A} \models \exists \bigwedge \Psi(x)$.*

Dries-Hodges' Test

Definition 0.13. *A theory T is said to be* 1*-model-complete if*

> *For any two models $\mathfrak{A}$ and $\mathfrak{B}$ of T with $\mathfrak{A} \subseteq \mathfrak{B}$, any quantifier-free formula $\varphi(\bar{x}, y)$ of $\mathscr{L}$ and any tuple $\bar{a} \subseteq A$, $\mathfrak{B} \models \exists y \varphi(\bar{a}, y)$ implies $\mathfrak{A} \models \exists y \varphi(\bar{a}, y)$*

Theorem 0.13. *A theory T admits quantifier elimination if it satisfies either of the following two conditions:*

- *T has properties of existence of T-closure and specializability of selected elements. (Dries)*
- *T has T-closure property and is* 1*-model-completeness. (Hodges)*

Dries-Hodges' Test (Cont'd)

Example 0.5. *Real closed fields have quantifier elimination.*

Justification:

Theorem 0.14 (Artin-Schreier). *The following properties hold for a real closed field $\mathfrak{A}$.*

- *If $f(X) \in A[X]$, and $a, b \in A$ such that $a < b$ and $f(a) < f(b)$, then there exists $c \in A$ such that $a < b < c$ and $f(c) = 0$.*
- *If $\mathfrak{B}$ is an ordered subfield of $\mathfrak{A}$, then there exists a smallest real closed field $\mathfrak{C}$ such that $\mathfrak{B} \subseteq \mathfrak{C} \subseteq \mathfrak{A}$. Moreover, if $\mathfrak{A}'$ is any real closed field extension of $\mathfrak{B}$, then $\mathfrak{C}$ is embeddable into $\mathfrak{A}'$ over $\mathfrak{B}$. ($\mathfrak{C}$ is called the real closure of $\mathfrak{B}$ in $\mathfrak{A}$.)*

Feferman's Test

Theorem 0.15. *Let T be a first-order thoery of $\mathscr{L}$. Let $\mathfrak{A}$, $\mathfrak{B}$ be models of T and $\bar{a}$, $\bar{b}$ tuples from $\mathfrak{A}$, $\mathfrak{B}$ respectively. The following are equivalent.*

1. *T has elimination of quantifiers.*
2. *If $(\mathfrak{A}, \bar{a}) \equiv_0 (\mathfrak{B}, \bar{b})$, then $(\mathfrak{A}, \bar{a}) \Rrightarrow_1 (\mathfrak{B}, \bar{b})$.*
3. *If $(\mathfrak{A}, \bar{a}) \equiv_0 (\mathfrak{B}, \bar{b})$, then $(\mathfrak{A}, \bar{a}) \equiv (\mathfrak{B}, \bar{b})$.*
4. *If $(\mathfrak{A}, \bar{a}) \equiv_0 (\mathfrak{B}, \bar{b})$, then $(\bar{a}, \bar{b})$ is a winning position for player $\exists$ in the game $EF_n[(\mathfrak{A}, \bar{a}), (\mathfrak{B}, \bar{b})]$ for each $n < \omega$.*

Feferman's Test (Cont'd)

Example 0.6. *The theory of atomless boolean algebra admits quantifier elimination. Justification:*

Let $\mathfrak{A}$, $\mathfrak{B}$ *be two models of atomless boolean algebra and* $\bar{a} \subseteq A$, $\bar{b} \subseteq B$. *Let* $\mathfrak{A}_0 = \langle \bar{a} \rangle_{\mathfrak{A}}$, $\mathfrak{B}_0 = \langle \bar{b} \rangle_{\mathfrak{B}}$.

- $(\mathfrak{A}, \bar{a}) \equiv_0 (\mathfrak{B}, \bar{b})$ *implies* $\mathfrak{A}_0$ *is isomorphic to* $\mathfrak{B}_0$.
- *Assume* $f_n : \mathfrak{A}_n \mapsto \mathfrak{B}_n$ *is an isomorphism. For any* $a \in A \setminus A_n$, *find* $b \in B \setminus B_n$ *such that for every atom* $x \in A$

$$(a \cdot x) = 0 \quad \leftrightarrow \quad (b \cdot f(x)) = 0$$

$$((-a) \cdot x) = 0 \quad \leftrightarrow \quad ((-b) \cdot f(x)) = 0$$

Such b *can always be found since* $\mathfrak{B}$ *is atomless.*

Feferman's Test (Cont'd)

- Extend f_n to f_{n+1} with a being mapped to b.

  Note that atoms of $\mathfrak{A}_{n+1}$ are of forms $a \cdot x$ or $(-a) \cdot x$ where x is an atom of $\mathfrak{A}_n$. Moreover, f_{n+1} is a 1-1 mappings from atoms of $\mathfrak{A}_{n+1}$ to atoms of $\mathfrak{B}_{n+1}$.

- Let $A_{n+1} = \langle A_n \cup \{a\} \rangle_{\mathfrak{A}}$ and $B_{n+1} = \langle B_n \cup \{b\} \rangle_{\mathfrak{B}}$.

  Clearly, f_{n+1} is an isomorphism between A_{n+1} and B_{n+1} since any element of $\mathfrak{A}_{n+1}$ (resp. $\mathfrak{B}_{n+1}$) is a unique sum of disjoint atoms of $\mathfrak{A}_{n+1}$ (resp. $\mathfrak{B}_{n+1}$).

- $(\bar{a}, \bar{b})$ is a winning position for player $\exists$.

More ...

- Term algebras
- Separable boolean rings
- Vector spaces
- Finite fields
- p-adic fields
- Differentially closed fields
- Real fields with exponentiation
- Generic algebraic curves
- ...