Theories

A signature is a (finite or infinite) set of predicate and function symbols. We fix a signature S.

A theory is a set of formulas T (over S) closed under consequence, i.e., if $F_1, \ldots, F_n \in T$ and $\{F_1, \ldots, F_n\} \models G$ then $G \in T$.

Fact: Let $\mathcal{A}$ be a structure suitable for S. The set F of formulas such that $\mathcal{A}(F) = 1$ is a theory.

We call them model-based theories.

Fact: Let $\mathcal{F}$ be a set of formulas (a set of axioms). The set F of formulas such that $\mathcal{F} \models F$ is a theory.

We call them axiom-based theories.

Examples

Model-based theories:

Arithmetic: $Th(\mathbb{N}, 0, 1, +, \cdot, <)$

Presburger Arithmetic: $Th(\mathbb{N}, 0, 1, +, <)$

Linear Arithmetic: $Th(\mathbb{Q}, 0, 1, +, c \cdot (c \in \mathbb{Q}), <)$

Axiom-based theories:

- Theory of groups, rings, fields, boolean algebras, ...
- Abstract datatypes: stacks, queues, ...

Decidability and axiomatizability

A set $\mathcal{F}$ of formulas over a signature S is decidable if there is an algorithm that decides for every formula F over S whether $F \in \mathcal{F}$ holds.

A theory T is *blue decidable* if it is decidable as a set.

A theory T is axiomatizable if there is a decidable set $\mathcal{F} \subseteq T$ of closed formulas (the axioms) such that every formula of T is a consequence of $\mathcal{F}$.

Quantifier elimination

A quantifier elimination procedure (QE-procedure) for a model-based theory with structure $\mathcal{A}$ is a computable function that maps each formula of the theory of the form $\exists x\ F$ (where F contains no quantifiers) to a formula G without quantifiers such that:

- $\mathcal{A}(\exists x\ F) = \mathcal{A}(G)$.
- Every free variable of G is also a free variable of $\exists x\ F$.

Notation: We abbreviate $\mathcal{A}(F_1) = \mathcal{A}(F_2)$ to $F_1 \equiv_{\mathcal{A}} F_2$.

Theorem: If the set of quantifier-free closed formulas of a theory is decidable and the theory has a quantifier elimination procedure, then the theory is decidable.

Proof:

- Convert the formula into prenex form.
- Eliminate all quantifers inside-out (i.e., starting with the innermost quantifier), where universal quantifiers are transformed into existential ones with the help of the rule $\forall\ F \equiv \neg\exists\ \neg F$.
- Decide the resulting quantifier-free closed formula.

Linear Arithmetic

Linear Arithmetic: $Th(\mathbb{Q}, 0, 1, +, c \cdot (c \in \mathbb{Q}), <)$

Syntax:

Terms:	$t := 0 \mid 1 \mid t_1 + t_2 \mid c \cdot t$
Atomic formulas:	$A := t_1 < t_2 \mid t_1 = t_2$
Formulas:	$F := A \mid \neg F \mid F_1 \vee F_2 \mid F_1 \wedge F_2 \mid \exists F \mid \forall F$

Structure $\mathcal{A}$:

- Universe: $\mathbb{Q}$.
- Interpretation of 0, 1, $+$, $<$ ist clear.
- $\mathcal{A}(c \cdot t) = c \cdot \mathcal{A}(t)$.

Expressiveness

Some assertions that can be formalized in linear arithmetic:

- The system $Ax \leq b$ has no solution.
- Every solution of $A_1x \leq b_1$ is also a solution of $A_2x \leq b_2$.
- For every solution x_1 of $A_1x \leq b_1$ gibt there are solutions x_2 and x_3 of $A_2x \leq b_2$ and $A_3x \leq b_3$ such that $x_1 = x_2 + x_3$.
- The smallest solution of $A_1x \leq b_1$ is larger than the largest solution of $A_2x \leq b_2$.

Fourier-Motzkin elimination

(slides by Prof. Nipkow.)

We present a QE-procedure for linear arithmetic.

> Given: Formula $\exists x F$ where F quantifier-free.
>
> Goal: Quantifier-free formula G such that $G \equiv_{\mathcal{A}} \exists x F$.

Two phases:

- Phase I: Simplification of the problem through logical manipulations.
- Phase II: QE-procedure for the simplified case.

Phase I

Step 1: Bring negations in and eliminate them using

$$\begin{aligned} \neg(t_1 = t_2) \quad &\equiv_{\mathcal{A}} \quad (t_2 < t_1) \vee (t_1 < t_2) \\ \neg(t_1 < t_2) \quad &\equiv_{\mathcal{A}} \quad (t_2 < t_1) \vee (t_2 = t_1) \end{aligned}$$

Step 2: Convert into DNF and move $\exists x$ through $\vee$ using

$$\exists x (F_1 \vee F_2) \equiv \exists x F_1 \vee \exists x F_2$$

The result is of the form $\bigvee_{i=1}^{n} \exists x \ (\bigwedge_{j=1}^{m_i} A_{ij})$. So w.l.o.g. we restrict our attention to the case

$$F = A_1 \wedge \ldots \wedge A_n$$

Phase I (Con.)

Step 3: Miniscoping: consider only the A_i containing x. The rule

$$\exists x\ (A_1 \wedge A_2) \equiv (\exists x\ A_1) \wedge A_2 \quad \text{if } x \text{ does not occur free in } A_2$$

allows us to restrict our attention w.l.o.g. to the case

$$F = A_1 \wedge \ldots \wedge A_n \qquad \text{and } x \text{ occurs free in every } A_i$$

Phase I (Con.)

Step 4: Isolate x in A_i.

Define x-atoms: $A^x := \; x = t \mid x < t \mid t < x$ where x does not occur in t.

Fact: For every $i \in [1..n]$ there is a x-Atom A_i^x such that $A_i^x \equiv_{\mathcal{A}} A_i$. (requires linearity!!)

Example:

$$\begin{array}{rrcl} \text{If} & A_i & = & 3 \cdot x + 5 \cdot y < 7 \cdot x + 3 \cdot z \\ \text{then take} & A_i^x & = & \frac{5}{4} \cdot y + \left(-\frac{3}{4}\right) \cdot z < x \end{array}$$

W.l.o.g. we can restrict our attention to the case

$$F = A_1^x \wedge \ldots \wedge A_n^x$$

Phase II

Case 1. There exists $k \in [1..n]$ such that $A_k^x = (x = t_k)$.

Then: $\exists x F \equiv_{\mathcal{A}} F[x/t_k]$.

Set $G := F[x/t_k] = A_1^x[x/t_k] \wedge \ldots \wedge A_n^x[x/t_k]$.

Case 2. For every $k \in [1..n]$: $A_k^x = (x < t_k)$ or $A_k^x = (t_k < x)$.

Classify the A_i^x into lower and upper bounds:

$$F = \bigwedge_{i=1}^{l} L_i \wedge \bigwedge_{j=1}^{u} U_j \quad \text{where } L_i = (l_i < x) \text{ and } U_j = (x < u_j)$$

I.e., l_i is a (lower bound) and u_j an (upper bound) for x.

Phase II (Con.)

Case 2a: $l = 0$ or $u = 0$. (Only lower or upper bounds.)

Then: $\exists x F \equiv_{\mathcal{A}} 1$.

Set $G := 1$

Case 2b: $l > 0$ and $u > 0$. (Both lower and upper bounds.)

Then: $\exists x F \ \equiv_{\mathcal{A}} \ \bigwedge_{i=1}^{l} \bigwedge_{j=1}^{u} (l_i < u_j)$.

($\mathcal{A}(\exists x F) = 1$ iff all lower bounds smaller than all upper bounds.
Observe: this holds because $\mathbb{Q}$ is a dense order!)

Set $G = \bigwedge_{i=1}^{l} \bigwedge_{j=1}^{u} (l_i < u_j)$.

Complexity

Dominated by the case 2b.

If $|F| = O(n)$ then $|G| = O(n^2)$.

The procedure needs $O(n^{2^m})$ for a formula $\exists x_1 \ldots \exists x_m\ F$ of length n.
(Assuming F is in DNF.)