MATHEMATICAL LOGIC FOR COMPUTER SCIENCE

A.Y. 20/21, HANDOUT N. 4

Abstract. Quantifier Elimination for the rational ordering and for real addition.

1. Elimination of Quantifiers

The method of Quantifier Elimination was introduced by Alfred Tarski (1902-1983) to prove the decidability of some algebraic theories.

> The theory T of a structure $\mathfrak{A}$ is **decidable** if there exists an algorithm that solves the following decision problem: given a sentence S in the language of T, is it the case that $\mathfrak{A} \models S$ or not?

The idea of quantifier elimination is to prove that every formula in the language of the theory is equivalent (with respect to provability in that theory) to a formula of a particularly simple type: a formula with no quantifiers (also called open or quantifier-free). If the truth of open formulas is all models of the theory is decidable by an algorithm and if the transformation from formulas any simple formulas is effective, this gives a decision algorithm for the theory.

Let's start from a trivial example. Consider the formula $\exists y(x < y \wedge y < z)$. Consider the structure $\mathcal{Q}$. For any $a, b \in \mathbb{Q}$,

$$\mathcal{Q} \models \exists y(x < y \wedge y < z)[\binom{x, z}{a, b}]$$

if and only if

$$\mathcal{Q} \models (x < z)[\binom{x, z}{a, b}].$$

Therefore

$$\mathcal{Q} \models \exists y(x < y \wedge y < z) \leftrightarrow x < z.$$

In other words, the quantified formula $\exists y(x < y \wedge y < z)$ is equivalent – for the structure $\mathcal{Q}$ – to the open formula $x < z$.

Mathematical practice gives many other examples of properties that are normally defined using quantifiers but can be proved equivalent – at least with respect to certain structures of interest – to a property definably by an open formula.

Consider the formula $\exists x(ax^2 + bx + c = 0)$, where a, b, c are constants. In the field of the reals we know that this formula is satisfied if and only if the following open formula is satisfied.

$$(a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge (b \neq 0 \vee c = 0)).$$

In the complex field we have an equivalence with an even simpler open formula:

$$(a \neq 0 \vee b \neq 0 \vee c = 0).$$

Now consider a formula that expresses that the matrix with rows a, b and c, d is invertible.

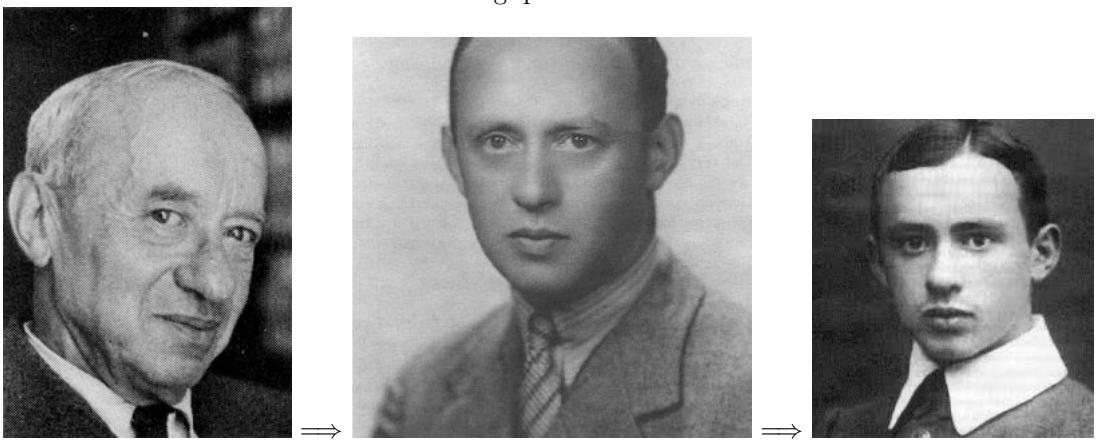
$$\exists x \exists y \exists w \exists z(xa + yc = 1 \wedge xb + yd = 0 \wedge wa + zc = 0 \wedge wb + zd = 1).$$

in any field C, the formula is equivalent to the following open formula (which expresses the test of the determinant):

$$ad - bc \neq 0.$$

Notes by Lorenzo Carlucci, carlucci@di.uniroma1.it.

FIGURE 1. Eliminating quantifiers from Alfred Tarski



2. Quantifier Elimination for the rational ordering

We illustrate the method by a simple example. For technical convenience we make the following extension of the notions of atomic formula: let $\top$ and $\bot$ be two logical constants, whose intended meaning are True and False, respectively.

Theorem 2.1. *For every formula $F(x_1, \ldots, x_n)$ with free variables $\{x_1, \ldots, x_n\}$ in the language of orders $\mathcal{L} = \{<\}$ there exists a quantifier-free formula F' with free variables in $\{x_1, \ldots, x_n\}$ such that*

$$\mathcal{Q} \models \forall x_1 \ldots \forall x_n (F(x_1, \ldots, x_n) \leftrightarrow F'(x_1, \ldots, x_n)).$$

We say that F' is $\mathcal{Q}$-equivalent (or equivalent modulo $\mathcal{Q}$) to F. Moreover, F' can be found algorithmically from F.

Proof. Let F be a formula in the language of orders. We can assume that F is in **prenex normal form**, i.e.,

$$F = Q_1 x_1 \ldots Q_n x_n G,$$

where G open, all the x_is are distinct and each Q_i is either $\exists$ or $\forall$. If $Q_n x_n$ is $\forall x_n$, replace $\forall x_n G$ with $\neg \exists x_n \neg G$. Thus we can in any case focus on a formula of the type $\exists x G$ with G open. We show how to transform it into an open formula consisting of a combination of atomic formulas.

Essentially, after the first three steps we reduce to the case of formulas of the following type:

$$\exists x (\bigwedge_{i<\ell} t_i < x \wedge \bigwedge_{j<m} x < s_j \wedge \bigwedge_{k<n} r_k = x),$$

where t_i, s_j, r_k are terms not containing x (i.e., variables different from x).

At each step we preserve equivalence modulo $\mathcal{Q}$, in the sense that if a formula A is transformed into a formula B then we want to ensure $\mathcal{Q} \models \forall \vec{x}(A \leftrightarrow B)$, where $\vec{x}$ contains all free variables occurring in A and B.

Step 1. We first push all negations so that they only appear in front of atomic formulas (Negation Normal Form). We then replace negated atomic formulas by atomic formulas. Use the following facts:

$$\mathcal{Q} \models \forall x \forall y (\neg(x = y) \leftrightarrow ((x < y) \vee (y < x))$$

$$\mathcal{Q} \models \forall x \forall y (\neg(x < y) \leftrightarrow ((x = y) \vee (y < x)).$$

We can thus assume that the formula contains no negation sign.

Step 2. Write G in *Disjunctive Normal Form*, i.e., as a disjunction of conjunctions of atomic formulas or negated atomic formulas. No negation is introduced in the process so we can assume that G is written as a disjunction of conjunctions of atomic formulas only. Let $F_1 \vee \cdots \vee F_k$ be the result of this transformation.

Step 3. Consider all possible conjuncts in each $F_i = \bigwedge_p H_p$. Note that $\exists x_n(F_1 \vee \cdots \vee F_k)$ is logically equivalent to $\exists x_n F_1 \vee \cdots \vee \exists x_n F_k$. So we can focus on formulas of the form $\exists x_n F_i$ with F_i a conjunction of atoms.

Step 3.1. x_n does not appear in $\bigwedge_p H_p$. Then we delete $\exists x_n$ from the formula. This preserves equivalence since, if x is not a free variable in a formula A, then

$$\models \exists x A \leftrightarrow A.$$

Step 3.2. We collect all atoms containing x_n.

$$\bigwedge_p H_p \equiv (x_n < u_0) \wedge \cdots \wedge (x_n < u_p) \wedge (v_0 < x_n) \wedge \cdots \wedge (v_q < x_n) \wedge (w_0 = x_n) \wedge \cdots \wedge (w_r = x_m) \wedge J$$

where J is a formula not containing x_n. We abbreviate the above formula as

$$\bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n \wedge \bigwedge_k w_k = x_n \wedge J$$

By logical equivalence, since x_n does not appear in J, we have

$$\models \exists x_n(\bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n \wedge \bigwedge_k w_k = x_n \wedge J) \leftrightarrow \exists x_n(\bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n \wedge \bigwedge_k w_k = x_n) \wedge J.$$

A fortiori, the two formulas are $\mathcal{Q}$-equivalent. So we only have to consider $\exists x_n B$ for B a conjunction of atomic formulas **all containing x_n as a variable**.

Step 3.2.0 We can remove all conjuncts of type $(x_n = x_n)$. If these are the only conjuncts in the formula we replace the entire formula by $\top$.

If a conjunct is of the form $(x_n < x_n)$ then we replace the entire formula $\exists x_n F_i$ by $\bot$, since no assignment in $\mathbb{Q}$ satisfies a formula containing such a conjunct.

We can from now on assume that there are no atomic formulas of type $(x_n = x_n)$ or $(x_n < x_n)$ in the formula.

Step 3.2.1 B contains atoms of all three possible types, i.e.

$$B = \bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n \wedge \bigwedge_k w_k = x_n$$

where we can assume that $w_0, \ldots, w_k$ are distinct from x_n.

Let

$$B' = \bigwedge_i w_0 < u_i \wedge \bigwedge_j v_j < w_0 \wedge \bigwedge_k w_k = w_0$$

where w_0 is the first variable among the w_ks and B' is obtained by substituting x_n by w_0 everywhere in B. Then

$$\mathcal{Q} \models \exists x_n B \leftrightarrow B'.$$

In fact, the following holds in general: $\exists x((x = y) \wedge F(x, y) \equiv F(y, y)$, where $F(y, y)$ is obtained from $F(x, y)$ by replacing all free occurrences of x by y.

Step 3.2.2 B contains inequality atoms of both types but no identity atom, i.e.,

$$B = \bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n.$$

We claim that

$$\mathcal{Q} \models B \leftrightarrow \bigwedge_{i,j} v_j < u_i,$$

where $\bigwedge_{i,j} v_j < u_i$ abbreviates

$$(v_0 < u_0) \wedge \cdots \wedge (v_0 < u_p) \wedge (v_1 < u_0) \wedge \cdots \wedge (v_1 < u_p) \wedge \cdots \wedge (v_q < u_0) \wedge \cdots \wedge (v_q < u_p).$$

The latter formula correctly expresses the finite quantification "all v_js are smaller than all u_is".

Fix an assignment α in $\mathbb{Q}$. Suppose

$$\mathcal{Q} \models \exists x_n(\bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n)[\alpha].$$

By definition of satisfaction this is true if and only if there exists a rational $c \in \mathbb{Q}$ such that

$$\mathcal{Q} \models (\bigwedge_i x_n < u_i \wedge \bigwedge_j v_j < x_n)[\alpha\binom{x_n}{c}],$$

since the variables u_i and v_j are distinct from x_n. Let a_i's and b_j's be elements of $\mathbb{Q}$ assigned to the variables u_is and v_js respectively. It is obvious that in $\mathcal{Q}$ this is possible if and only if the maximum of the b_js is smaller than the minimum of the a_is, or, equivalently, if all the b_js are smaller than all the a_is. This is so since $\mathbb{Q}$ is densely ordered by $<$. Thus we have that, for any α, the following equivalence holds.

$$\mathcal{Q} \models (\exists x_n B \leftrightarrow \bigwedge_{i,j} v_j < u_i)[\alpha]$$

Step 3.2.3 B contains no $(v_j < x_n)$-type atoms but contains atoms of the other two types, i.e.,

$$B = \bigwedge_i x_n < u_i \wedge \bigwedge_k w_k = x_n.$$

Then

$$\mathcal{Q} \models \exists x_n B \leftrightarrow (\bigwedge_i w_0 < u_i \wedge \bigwedge_k w_k = w_0).$$

Step 3.2.4 B contains no $(x_n < u_i)$-type atoms but contains atoms of the other two types, i.e.,

$$B = \bigwedge_j v_j < x_n \wedge \bigwedge_k w_k = x_n.$$

This is analogous to the previous step.

Step 3.2.5 B contains only $(x_n < u_i)$-type atoms, i.e.,

$$B = \bigwedge_i x_n < u_i.$$

Since x_n is (syntactically) distinct from all the variables u_i, then note that $\exists x_n B$ holds in $\mathcal{Q}$ because it's a dense linear order without end-points. So

$$\mathcal{Q} \models \exists x_n B \leftrightarrow \top.$$

Step 3.2.6 B contains only $(v_j < x_n)$-type atoms, i.e.,

$$B = \bigwedge_j v_j < x_n.$$

This is analogous to the previous Step.

Step 3.2.7 B contains only identity atoms, i.e.,

$$B = \bigwedge_k w_k = x_n.$$

Observe that

$$\mathcal{Q} \models \exists x_n B \leftrightarrow \bigwedge_k w_k = w_0.$$

We reduced our initial formula $Q_1 x_1 \dots Q_n x_n G$ to a formula $Q_1 x_1 \dots Q_{n-1} x_{n-1} G'$ where G' is open and contains no new free variables. The procedure can be repeated to eliminate the quantifiers $Q_1, \dots Q_{n-1}$, starting from the innermost, Q_{n-1}. At the end of this procedure we are left with a quantifier-free formula with no new free variables and $\mathcal{Q}$-equivalent to the initial formula. □

Corollary 2.2. *$Th(\mathcal{Q})$ is decidable.*

Proof. By the previous Theorem, if we start with a sentence we end up with a quantifier free $\mathcal{Q}$-equivalent quantifier-free sentence. But the only quantifier-free formulas with no free variables in the language of $\mathcal{Q}$ are the boolean combinations of the logical constants $\top$ and $\bot$. Obviously any such combination is logically equivalent to either $\top$ or $\bot$. Therefore any sentence is $\mathcal{Q}$-equivalent either to $\top$ or else to $\bot$. □

An analysis of the above algorithm shows that each step of elimination of an existential quantifier results in a quadratic blow-up, so that the overall procedure has complexity $O(n^{2^m})$ where n is the size of the formula G and m is the number of quantifiers in its prenex normal form.

3. Quantifier Elimination for Real Addition

We give a proof of quantifier elimination for the theory of the real numbers with addition and order. That is, we are interested in the sentences satisfied by the single structure $\mathcal{R}_+ = (\mathbb{R}, +, <, 0, 1)$.

The procedure is due to Ferrante and Rackhoff and the proof below comes almost verbatim from their paper *A decision procedure for the first order theory of real addition with order*, Siam Journal of Computing, Vol. 4, N. 1, 1975, pp. 69–76. The result itself is a corollary of an important quantifier elimination result of Alfred Tarski showing that the first-order theory of the structure $(\mathbb{R}, +, \cdot, <)$ is decidable, but the procedure below is significantly more efficient than Tarski's for the theory of real addition.

First of all we choose an adequate language with expressions that do not change the scope of the result but facilitate quantifier elimination. The choice of language below is justified by the following observations. Real numbers with addition ($+$) and order ($<$) is an ordered ($r, s, p \in \mathbb{R}$, $r \leq s$ implies $r + p \leq s + p$ and $p + r \leq p + s$) non-trivial group that satisfies the following additional algebraic properties:

(1) Torsion-free: For every $n \in \mathbf{N}^+$, $\forall x(x \neq 0 \rightarrow \underbrace{x + \cdots + x}_{n \text{ times}} \neq 0)$,

(2) Divisible: For every $n \in \mathbf{N}^+$, $\forall y \exists x(\underbrace{x + \cdots + x}_{n \text{ times}} = y)$.

For every $r \in \mathbb{R}$ and every positive integer n there exists at most one $s \in \mathbb{R}$ such that $\underbrace{s + \cdots + s}_{n \text{ times}} = r$.

Therefore it makes sense to speak about division by positive integers, i.e. multiplication by a rational constant. This motivates the choice of the language.

The language $\mathcal{L}$ has a constant symbol i (written in binary) for every integer. It has rational constant symbols: if a and b are non-zero integers, then a/b is a rational constant symbol of the language. For each non-zero integers a and b there is a unary function symbol $a/b \cdot x$. The terms of $\mathcal{L}$ are allowed to be of the form:

$$a_1/b_1 \cdot y_1 + \cdots + a_n/b_n \cdot y_n,$$

abbreviated $\sum_{i=1}^{n} a_i/b_i \cdot y_i$. The atomic formulas of $\mathcal{L}$ are of the form

$$t_1 = t_2, \;\; t_1 < t_2,$$

for terms t_1, t_2, and we furthermore include logical constants $\top$ and $\bot$ as atomic formulas.

All symbols have the standard interpretation.

Theorem 3.1 (Ferrante-Rackhoff)**.** *For every formula $\varphi(x_1, \ldots, x_n)$ there exists a quantifier-free formula $\varphi'(x_1, \ldots, x_n)$ such that for every $r_1, \ldots, r_n \in \mathbb{R}$,*

$$\mathcal{R}_+ \models \varphi(x_1, \ldots, x_n)[r_1, \ldots, r_n] \Leftrightarrow \mathcal{R}_+ \models \varphi'(x_1, \ldots, x_n)[r_1, \ldots, r_n].$$

Moreover, φ' can be found effectively from φ.

Proof. As observed for the case of $\mathcal{Q}$ we only have to show that if $B(x, x_1, \ldots, x_n)$ is quantifier-free we can effectively find a quantifier-free $B'(x_1, \ldots, x_n)$ that is $\mathcal{R}_+$-equivalent to $\exists x B(x, x_1, \ldots, x_n)$.

The basic underlying idea of the procedure is similar to what we did for $\mathcal{Q}$. An existential of the form $\exists x D(x, x_1, \ldots, x_n)$ with D as described above is satisfied in the reals relative to an assignment α to the free

variables $x_1, \ldots, x_n$ if and only if there is a real r that satisfies all the equalities and inequalities occurring in D, when the other terms (not involving x) are evaluated according to α. In principle the witness can be of four types:

(1) a number larger than all the values of the terms mentioned in the formula; or
(2) a number smaller than all the values of the terms mentioned in the formula;
(3) or a number equal to one of the value of the terms mentioned in the formula; or
(4) a number sandwiched between to values of terms mentioned in the formula.

The idea is then to replace $\exists x D$ by a disjunction of formulas not mentioning x that cover these four possible cases.

Step 1: We solve for x in each atomic formula of B so as to bring it into the form $\exists x D(x, x_1, \ldots, x_n)$ where each atomic formula in D either does not involve x or has the form $t < x$, $t = x$, $x < t$, with t a term not involving x.

Step 2: We define $D_\infty(x_1, \ldots, x_n)$ and $D_{-\infty}(x_1, \ldots, x_n)$ by replacing in D as follows.

For D_∞:

$$x < t \mapsto \bot$$
$$x = t \mapsto \bot$$
$$t < x \mapsto \top$$

For $D_{-\infty}$:

$$x < t \mapsto \top$$
$$x = t \mapsto \bot$$
$$x < t \mapsto \bot$$

We have that for all $r_1, \ldots, r_n \in \mathbb{R}$, if r is a sufficiently large real, then

$$\mathcal{R}_+ \models D(x_1, \ldots, x_n, x)[r_1, \ldots, r_n, r] \Leftrightarrow \mathcal{R}_+ \models D_\infty(x_1, \ldots, x_n)[r_1, \ldots, r_n].$$

Dually for $D_{-\infty}$ and a sufficiently small r.

Step 3: We now eliminate the quantifier in $\exists x D(x, x_1, \ldots, x_n)$. Let U be the set of terms t that do not contain x and such that $t < x$ or $x < t$ or $x = t$ appears in D. For each $u, v \in U$ we define $D_{u,v}(x_1, \ldots, x_n)$ by substituting in D as follows:

$$x \mapsto (u + v)/2.$$

We now claim that $\exists x D(x, x_1, \ldots, x_n)$ is $\mathcal{R}_+$-equivalent to the quantifier-free formula

$$B'(x_1, \ldots, x_n) := D_{-\infty}(x_1, \ldots, x_n) \vee D_\infty(x_1, \ldots, x_n) \vee \bigvee_{u,v \in U} D_{u,v}(x_1, \ldots, x_n).$$

Notice that $u, v \in U$ are not required to be distinct.

We now prove equivalence over $\mathcal{R}_+$.

Let $r_1, \ldots, r_n$ be reals and suppose

$$\mathcal{R}_+ \models B'(x_1, \ldots, x_n)[r_1, \ldots, r_n].$$

If $\mathcal{R}_+ \models D_{u,v}(x_1, \ldots, x_n)[r_1, \ldots, r_n]$ for some $u, v \in U$ then obviously $\mathcal{R}_+ \models \exists x D(x, x_1, \ldots, x_n)[r_1, \ldots, r_n]$.
If $\mathcal{R}_+ \models D_\infty(x_1, \ldots, x_n)[r_1, \ldots, r_n]$ then for all sufficiently large $r \in \mathbb{R}$ we have $\mathcal{R}_+ \models D(x_1, \ldots, x_n, x)[r_1, \ldots, r_n, r]$, and thus $\mathcal{R}_+ \models \exists x D(x, x_1, \ldots, x_n)[r_1, \ldots, r_n]$. Similarly for $D_{-\infty}(x_1, \ldots, x_n)$.

We now prove the converse. Suppose

$$\mathcal{R}_+ \models \exists x D(x_1, \ldots, x_n, x)[r_1, \ldots, r_n].$$

Then for some $r \in \mathbb{R}$ we have

$$\mathcal{R}_+ \models D(x_1, \ldots, x_n, x)[r_1, \ldots, r_n, r].$$

Let $t_1, \ldots, t_m$ be the distinct real numbers in increasing order obtained by evaluating the terms in U by the values $r_1, \ldots, r_n$. It may happen that two terms u and v in U evaluate to the same real. In general we have $m \leq |U|$.

Exactly one of the following conditions holds:

(1) $r < t_1$,

(2) $t_m < r$,
(3) $r = t_i$ for some $i \in [1, m]$,
(4) $t_i < r < t_{i+1}$ for some $i \in [1, m-1]$.

Note that if any other real number r' satisfies the same order relations with respect to $t_1, \ldots, t_m$ as r does, then $D(x_1, \ldots, x_n, x)[r_1, \ldots, r_n, r']$ is also true.

So, if (1) holds then

$$\mathcal{R}_+ \models D_{-\infty}(x_1, \ldots, x_n)[r_1, \ldots, r_n].$$

If (2) holds then

$$\mathcal{R}_+ \models D_{\infty}(x_1, \ldots, x_n)[r_1, \ldots, r_n].$$

If (3) holds, then

$$\mathcal{R}_+ \models D_{u,u}(x_1, \ldots, x_n)[r_1, \ldots, r_n],$$

where u is a term in U that evaluates to t_i. If (4) holds, then

$$\mathcal{R}_+ \models D_{u,v}(x_1, \ldots, x_n)[r_1, \ldots, r_n],$$

where u is a term in U that evaluates to t_i and v is a term in U that evaluates to t_{i+1}.

Thus, in any case,

$$\mathcal{R}_+ \models B'(x_1, \ldots, x_n)[r_1, \ldots, r_n].$$

□

The above decision procedure can be shown to require at most $2^{2^{cn}}$ time and 2^{cn} space to decide a formula of length n. It is known that any decision procedure for real addition must run in time at least 2^{cn} (Fischer-Rabin).

The method above applies with some modifications to the so-called Presburger Arithmetic, i.e. the theory of addition on $\mathbb{N}$, and to the theory of real multiplication. It is a particular case of an important theorem of Tarski showing that the real numbers with times ($\times$), plus ($+$) and order ($<$) is a decidable structure. The method of quantifier elimination can also be applied to more complex theories. Two fundamental examples are elementary algebra (the theory of real closed fields - this is a famous result of Tarski's), the theory of algebraically closed fields, and the theory of abelian groups.