A lower bound for the complexity of linear optimization from a quantifier-elimination point of view (extended abstract)

Rafael Grimson
Theoretical Computer Science Group
Hasselt University and Transnational University of Limburg, Belgium

Abstract

We analyze the arithmetic complexity of the feasibility problem in linear optimization theory as a quantifier-elimination problem. For the case of polyhedra defined by $2n$ halfspaces in $\mathbf{R}^n$ we prove that, if dense representation is used to code polynomials, any quantifier-free formula expressing the set of parameters describing nonempty polyhedra has size $\Omega(4^n)$.

1 Introduction

For real closed fields, modern quantifier-elimination algorithms work in doubly exponential time in the number of quantifier alternations of the input formula (see [BPR06]). Davenport and Heintz [DH88] gave a doubly exponential lower bound for the general quantifier-elimination problem over the reals, for dense and sparse codification of polynomials. Thus, in order of magnitude, upper and lower complexity bounds meet for this kind of data structure.

A natural question is whether using boolean arithmetic circuits to codify first order formulas, a faster algorithm can be implemented for the elimination of quantifiers. Not much is known about lower bounds for this kind of data structures (see Heintz-Morgenstern [HM93]) and no algorithm has been designed substantially improving—in worst-case complexity—the ones using classical data structures.

This research has been partially funded by the Research Foundation Flanders (FWO-Vlaanderen), Research Project G.0344.05 and the European Union under the FP6-IST-FET programme, Project n. FP6-14915, GeoPKDD: Geographic Privacy-Aware Knowledge Discovery and Delivery.

Dagstuhl Seminar Proceedings 07212
Constraint Databases, Geometric Elimination and Geographic Information Systems
http://drops.dagstuhl.de/opus/volltexte/2007/1283

In this paper we analyze the feasibility problem over the reals in linear optimization theory as a quantifier-elimination problem. We concentrate on the impact of data structures in quantifier elimination.

The *feasibility problem* can be informally stated as: given a matrix $H \in \mathbf{R}^{m\times n}$ and $h \in \mathbf{R}^m$ decide whether there exists an $x \in \mathbf{R}^n$ such that $H \cdot x \leq h$.

This is a classic example of quantifier-elimination problem. We prove that, for $m = 2n$, any quantifier-free formula using dense representation of polynomials and expressing the set $\{(H|h) \in \mathbf{R}^{m\times(n+1)} \mid \exists x\, H \cdot x \leq h\}$, must have size $\Omega(4^n)$.

As a corollary we get a quasi-exponential lower bound in the size of the input formula for the elimination of one quantifier block. The proof is based on the number of different *limiting hypersurfaces* of the set to be described; these hypersurfaces turn to be intrinsic to the set in the sense that any description of the set must involve the descriptions of its limiting hypersurfaces. Lazard used a similar technique to prove the optimality of solutions to two classical quantifier-elimination problems (see [Laz88]).

Although the Ellipsoid algorithm solves the feasibility problem over the rational numbers in polynomial time in the bit model (see [Kha79]) it is an open problem whether there exists a boolean arithmetic circuit, of size polynomial in n and m, codifying such a quantifier-free description. From our results it follows that, even for this representation, polynomials describing all limiting hypersurfaces must *intervene* in the circuit.

This paper is organized as follows: in Section 2 we state the feasibility problem as a quantifier-elimination problem and define the set $\mathcal{I}^{(m,n)} \subseteq \mathbf{R}^{m\times(n+1)}$ as the set of parameters defining m half-spaces in $\mathbf{R}^n$ with nonempty intersection. In Section 3 we define the notions of *limiting hypersurface* of a semi-algebraic set and of a polynomial *intervening* in a formula. Afterwards, we prove Proposition 3.2 stating that if Z is a limiting hypersurface for a set W and Q is a irreducible polynomial defining Z, then Q intervenes in any quantifier-free description of W. A section devoted to the study of the geometry of the set $\mathcal{I}^{(m,n)}$ is missing in this extended abstract. Finally, in Section 4 we state the intermediary results leading to the proofs of the lower bounds.

2 The Parametric Feasibility Problem

The feasibility problem for linear optimization over the reals can be stated as:

Given a matrix $H \in \mathbf{R}^{m\times n}$ and a column vector $h \in \mathbf{R}^m$ determine whether there exists $x \in \mathbf{R}^n$ such that $H \cdot x \leq h$.

2.1 A Quantifier-Elimination Problem

The above decision problem can be stated as a quantifier-elimination problem. Let us fix the notation. For each $n, m \in \mathbf{N}$, $m \geq n+1$, we consider the variables $x := (x_1, \ldots, x_n)$ and call parameters the elements in the matrix

$$T := \begin{pmatrix} t_1^{(1)} & \dots & t_n^{(1)} & b^{(1)} \\ \vdots & \ddots & \vdots & \vdots \\ t_1^{(m)} & \dots & t_n^{(m)} & b^{(m)} \end{pmatrix}.$$

We further define the formulas

$$\sigma_i^n(x,T) := t_1^{(i)} \cdot x_1 + \ldots + t_n^{(i)} \cdot x_n - b^{(i)} \leq 0, \; (i = 1 \ldots m),$$

$$\phi^{(m,n)}(T) := \exists x \, \sigma_1^n(x,T) \wedge \ldots \wedge \sigma_m^n(x,T) \tag{2.1}$$

and call $\mathcal{I}^{(m,n)}$ the realization of $\phi^{(m,n)}$ in the parameter space. Observe that $\mathcal{I}^{(m,n)} \subseteq \mathbf{R}^{m\times(n+1)}$; it is the set of parameters defining m half-spaces in $\mathbf{R}^n$ with nonempty intersection.

Finding quantifier-free formulas $\psi^{(m,n)}$ expressing the sets $\mathcal{I}^{(m,n)}$ is a way to solve the parametric feasibility problem. We will prove that they do not exist formulas $\psi^{(m,n)}$ expressing the sets $\mathcal{I}^{(m,n)}$ with size bounded by a polynomial function in m and n.

2.2 Statement of the Main Theorem

Theorem 2.1. *For $m = 2n$, the formula $\phi^{(m,n)}$ defined in Equation* (2.1) *has size $O(n^2 log(n))$ and any quantifier-free equivalent formula using dense representation of polynomials has size $\Omega(4^n)$.*

In the next pages we prove this theorem; we show that the set $\mathcal{I}^{(2n,n)}$, determined taking $m = 2n$, has an exponential (in n) number of limiting hypersurfaces (Corollary 4.3), each of them given by a different irreducible polynomial (a determinant). All these polynomial (or multiples of them) have to figure in any quantifier-free formula expressing the set $\mathcal{I}^{(2n,n)}$ (Proposition 3.2). From this and a last immediate result (Proposition 4.4), we get the lower bound for the size of any quantifier-free formula expressing this set. In that way, we will get the following quasi-exponential lower bound for the elimination of one existential quantifier block using dense representation.

Corollary 2.2. *If polynomials are codified using the dense representation then any algorithm for the elimination of one existential block performs $\Omega(2^{\sqrt{L}})$ operations in the worst case on inputs of length L.*

3 Limiting Hypersurfaces

Let $W \subseteq \mathbf{R}^k$ be a semi-algebraic set. We give the definition of limiting hypersurface of W and prove that a description of each of these hypersurfaces must intervene in any quantifier-free description of W. We can say that limiting hypersurfaces of a set are intrinsic.

For definitions (from real algebraic geometry) for the notions of semi-algebraic set, dimension of a set, set of zeros of an ideal, we refer the reader to [BCR98].

We denote by ∂W the set of points in the border of W (not interior nor interior to the complement). We call $Z \subseteq \mathbf{R}^k$ an *irreducible hypersurface* if $dim(Z) = k-1$ and there exists an irreducible polynomial $P \in \mathbf{R}[x_1, \ldots, x_k]$ such that $Z = \mathcal{Z}(P) = \{(x_1, \ldots, x_k) \in \mathbf{R}^k \mid P(x_1, \ldots, x_k) = 0\}$.

Definition 3.1. Let Z be an irreducible hypersurface in $\mathbf{R}^k$. We call Z a *limiting hypersurface* of W if its intersection with the border of W has dimension $k-1$.

We consider first order formulas built from atomic formulas of the form $P = 0$, $P \leq 0$, where $P \in \mathbf{R}[x_1, \ldots, x_k]$ is a polynomial with real coefficients. Let ψ be a first order formula and $P \in \mathbf{R}[x_1, \ldots, x_k]$. If ψ contains an atomic subformula of the form $P = 0$ or $P \leq 0$, we say that P *appears* in ψ. If a nonzero polynomial P appears in ψ and $Q \in \mathbf{R}[x_1, \ldots, x_k]$ is nonconstant and divides P, then we say that Q *intervenes* in ψ.

Proposition 3.2. *Suppose that $W \subseteq \mathbf{R}^k$ is a semi-algebraic set described by the quantifier-free formula ψ. Let Z_Q be a limiting hypersurface for W and let Q be the (unique) monic irreducible polynomial describing Z_Q. Then Q intervenes in ψ.*

Proof. Let us call $P_1, \ldots, P_s$ the polynomials appearing in ψ and suppose, without loss of generality, that none of them is the zero polynomial. We call $U = Z_Q \cap \partial W$ and we remark that, by hypothesis, it is a semi-algebraic subset of Z_Q of dimension $k-1$.

First, we remark that since $dim(Z_Q) = k-1$ and Q is irreducible, a particular form of the real Nullstellensatz for principal ideals (see Theorem 4.5.1 in [BPR06]) implies that a polynomial $P \in \mathbf{R}[x_1, \ldots, x_k]$ vanishes on $Z_Q = \mathcal{Z}(Q)$ if and only if Q divides P. Then, it remains to show that at least one P_j $(1 \leq j \leq s)$ vanishes on Z_Q.

To prove this, we consider, for any $u \in U$, the sign conditions $C(u) \in \{-1, 0, 1\}^s$ satisfied by the polynomials $P_1, \ldots, P_s$ in this point. It is clear that the truth value of the formula ψ in a point u depends only on $C(u)$ since the truth value of atomic formulas depend only on them.

These sign conditions partition the set U is a finite number of disjoint semi-algebraic components, $U_1, \ldots, U_t$, namely the nonempty supports in U of each possible sign condition. By Proposition 2.8.5 in [BCR98], one of these sets, say U_i, must have the same dimension as U, namely $k-1$.

Now, since the polynomials $P_1, \ldots, P_s$ have constant signs over U_i, $U_i \subseteq W$ or $U_i \subseteq W^c$. Let us suppose, with out loss of generality, $U_i \subseteq W$.

We claim that one of the polynomials $P_1, \ldots, P_s$ vanishes in U_i. Let $u \in U_i$; if none of the polynomials is zero in u then there exists and open neighborhood in $\mathbf{R}^k$ of this point with the same sign conditions implying that u is an interior point of W, contradicting $u \in \partial W$. Hence, there exists $j \in \mathbf{N}$, $j \leq s$ such that P_j is vanishes on U_i. Now, since $U_i \subseteq Z_Q$, Z_Q is irreducible and both set have the same dimension, we conclude that the Zariski closure of U_i, $\overline{U_i} = Z_Q$. Hence, P_j vanishes on the whole Z_Q. Thus, Q intervenes in ψ. $\square$

4 Sketch of the proof of Theorem 2.1

4.1 Counting the Limiting Hypersurfaces

In this section we consider $T \in \mathbf{R}^{m\times(n+1)}$ with $m \geq n+1$. We will prove that there exists a limiting hypersurface for $\mathcal{I} = \mathcal{I}^{(m,n)}$, associated to the first $n+1$ rows of T (among the original m), involving all the $(n+1)\times(n+1)$ parameters in these rows. Afterwards, by a simple symmetry argument, it will follow that there are at least $\binom{m}{n+1}$ different limiting hypersurfaces for $\mathcal{I}$.

Consider M, the square submatrix of T, consisting of the first $n+1$ rows of T. Define $D(T) := det(M)$.

Lemma 4.1. *The set* $Z_D = \mathcal{Z}(D) = \{T \in \mathbf{R}^{m\times(n+1)} \mid D(T) = 0\}$ *is an irreducible hypersurface.*

Proof. Since the polynomial D takes positive and negative values in $\mathbf{R}^{m\times(n+1)}$, Proposition 4.5.1 in [BCR98] implies that, $dim(Z_D) = m(n+1)-1$. The fact that Z_D is an irreducible hypersurface follows now from the irreducibility of the determinant. $\square$

Proposition 4.2. *The irreducible hypersurface in the parameters space* Z_D *defined by the equation* $D(T) = 0$ *is a limiting hypersurface for the set* $\mathcal{I}$.

Sketch of the Proof: We prove the proposition directly from the definition of limiting hypersurface, *i.e.*, we prove that $dim(Z_D \cap \partial\mathcal{I}) = m(n+1)-1$. To do so, we construct a nonsingular point $\widetilde{T} \in Z_D$. We then prove that there exists $\varepsilon > 0$ such that any $T \in B_\varepsilon(\widetilde{T}) \cap Z_D$ satisfies $T \in \partial\mathcal{I}$.

Corollary 4.3. *The set* $\mathcal{I}$ *has* $\Omega(\binom{m}{n+1})$ *different limiting hypersurfaces given by the* $(n+1)\times(n+1)$ *minors of the parameters matrix.*

Proof. By the previous proposition, the first minor defines a limiting hypersurface. Considering any other $(n+1)\times(n+1)$ minor of the parameters matrix T we can reason analogously getting an irreducible hypersurface. Since there are $\binom{m}{n+1}$ such minors and the variables involved in each minor are different there are at least $\binom{m}{n+1}$ different limiting hypersurfaces. $\square$

4.2 Dense Representation

Proposition 4.4. *Let* ψ *be a first order formula with polynomials codified in dense form. Then, the size of* ψ *is inferiorly bounded by the sum of the degrees of the different irreducible polynomials intervening in* ψ.

Proof. Let $Q_1, \dots, Q_s$ be the non-constant polynomials appearing in ψ, with factorizations $Q_i = P_{i,1} \cdots P_{i,k_i}$ where $P_{i,j}$ are the irreducible polynomials of positive degree intervening in ψ. Let $d_i = deg(Q_i)$. Clearly, the dense representation of Q_i uses at least $(d_i + 1)$ space units. Then, the size of ψ is lowery bounded by $\sum_{i=1}^{s} d_i$. Since $d_i = \sum_{j=1}^{k_i} deg(P_{i,j})$, the sum of the degrees of the different irreducible polynomials intervening in ψ is a lower bound for the size of ψ. $\square$

Corollary 4.5. *The formula ϕ_{2n}^{n}, defined in Equation* (2.1)*, has size $O(n^2 log(n))$ and any quantifier-free equivalent formula has size $\Omega(4^n)$.*

Proof. A straightforward computation shows that $\phi^{(2n,n)}$ uses $O(n^2)$ symbols. Since variable symbols require $O(log(n))$ bits to be written down, we have $|\phi^{(2n,n)}| = O(n^2 log(n))$ bits.

Let ψ be a quantifier-free formula describing the set $\mathcal{I}^{(2n,n)}$. The Corollary 4.3 shows that the $\binom{2n}{n+1}$ minors of the parameter matrix T define different limiting hypersurfaces for $\mathcal{I}^{(2n,n)}$. The Proposition 3.2 shows that these minors intervene in ψ. Since these polynomials have degree $n + 1$, the Proposition 4.4 implies that the size of a quantifier-free formula describing this set has size $\Omega(\binom{2n}{n+1}(n + 1))$. The conclusion follows immediately from the application of Stirling's formula. $\square$

This proves Theorem 2.1 and Corollary 2.2.

References

[BCR98] J. Bochnak, M. Coste, and M. F. Roy, *Real algebraic geometry*, Springer-Verlag, 1998.

[BPR06] Saugata Basu, Richard Pollack, and Marie-Françoise Roy, *Algorithms in real algebraic geometry (algorithms and computation in mathematics)*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[DH88] J. H. Davenport and J. Heintz, *Real quantifier elimination is doubly exponential*, J. Symbolic Comput. **5** (1988), 29–35.

[HM93] J. Heintz and J. Morgenstern, *On the intrinsic complexity of elimination theory.*, J. Complexity **9** (1993), no. 4, 471–498.

[Kha79] L. G. Khachiyan, *A polynomial algorithm in linear programming*, Soviet Mathematics Doklady **20** (1979), 191–194.

[Laz88] D. Lazard, *Quantifier elimination: optimal solution for two classical examples*, J. Symb. Comput. **5** (1988), no. 1-2, 261–266.