Laboratoire de l'Informatique du Parallélisme

École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON n° 8512

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Transfer Theorems via Sign Conditions

Pascal Koiran

March 2000

Research Report N° 2000-13

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : `lip@ens-lyon.fr`

Transfer Theorems via Sign Conditions

Pascal Koiran

March 2000

Abstract

We show that P = PSPACE implies the collapse of the boolean polynomial hierarchy over any structure which admits "efficient enumeration of sign conditions". This fairly rich class of structures contains in particular $\mathbb{R}$ and $\mathbb{C}$.

Keywords: algebraic complexity, polynomial hierarchy, transfer theorems, sign conditions.

Résumé

Nous montrons que si P = PSPACE la hiérarchie polynomiale booléenne s'effondre pour toute structure vérifiant la propriété d'énumération efficace des conditions de signes. Cette classe de structures assez riche contient en particulier $\mathbb{R}$ et $\mathbb{C}$.

Mots-clés: complexité algébrique, hiérarchie polynomiale, théorèmes de transfert, conditions de signe.

Transfer Theorems via Sign Conditions

Pascal Koiran
Laboratoire de l'Informatique du Parallélisme – CNRS
Ecole Normale Supérieure de Lyon
46 allée d'Italie, 69364 Lyon Cedex 07
Pascal.Koiran@ens-lyon.fr
http://www.ens-lyon.fr/~koiran

14th March 2000

Abstract

We show that P = PSPACE implies the collapse of the boolean polynomial hierarchy over any structure which admits "efficient enumeration of sign conditions". This fairly rich class of structures contains in particular $\mathbb{R}$ and $\mathbb{C}$.

Keywords: algebraic complexity, polynomial hierarchy, transfer theorems, sign conditions.

1 Introduction

Algebraic versions of the "P = NP ?" problem for structures such as the real numbers and the complex numbers were introduced in 1989 by Blum, Shub and Smale [4]. The problem is still open for $\mathbb{R}$ and $\mathbb{C}$, but precise answers could be obtained for some other structures. In particular, it was shown that for the reals with addition and order, the problem is equivalent to the (non-uniform) P = NP problem from discrete complexity theory [9]. In the same paper we obtained several transfer theorems for the reals with addition and equality, showing for instance that its polynomial hierarchy collapses if and only if the discrete polynomial hierarchy collapses (note however the unconditional result that P $\neq$ NP in that structure [16]). In this paper we obtain similar transfer theorems for structures with "efficient enumeration of sign conditions". This is a fairly large class of structures which contains in particular $\mathbb{R}$ and $\mathbb{C}$. One caveat is that we can only deal with the boolean polynomial hierarchy: only boolean elements are quantified, not elements from the structure. It turns out that these two notions are equivalent for the reals with addition and equality (as well as for the reals with addition and order [7]), which explains why we could deal with the "full" polynomial hierarchy in [9]. Unfortunately, for $\mathbb{R}$ or $\mathbb{C}$ it is not known whether the full polynomial hierarchy is equal to its boolean counterpart.

The paper is organized as follows. In section 2 we recall some basic definitions from the theory of computation in algebraic structures, introduce the notion of "efficient enumeration of sign conditions", and give some examples. The transfer theorem is obtained in section 3: if M has efficient enumeration of sign conditions and P = PSPACE then the boolean polynomial hierarchy over M collapses at its second level. We also point out some relations with Vapnik-Chervonenkis dimension and with earlier work by Cucker and Grigoriev [6].

2 Circuits and Structures

2.1 Complexity Classes

Here we briefly describe the model of computation used throughout the paper. More details can be found [3, 13, 17].

By "structure", we mean a set M equipped with a finite set of functions $f_i : M^{n_i} \to M$ and relations $r_i \subseteq M^{m_i}$. We always assume that M contains the equality relation and two distinguished elements denoted 0 and 1.

There are several types of gates in a circuit over M:

1. For each function f_i of M, gates of type f_i apply this function to their n_i inputs.

2. For each relation r_i of M, gates of type r_i apply the characteristic function of r_i to their inputs.

3. Finally, selection gates compute a function $s(x, y, z)$ of their three inputs such that $s(0, y, z) = y$ and $s(1, y, z) = z$. The behaviour of s on an input (x, y, z) with $x \notin \{0, 1\}$ is not important. We shall assume that $s(x, y, z)$ is equal in this case to some fixed term $t(x, y, z)$ of M.

By definition the number of gates in a circuit is its size. In the remainder of this paper we only consider circuits with one output gate. Also since we are only interested in decision problems we will assume without loss of generality that this output gate is an equality gate, to make sure that the output is always boolean.

Now that our basic computation model is defined, we can move on to complexity classes. Recall that a problem is simply a subset of $M^\infty = \bigcup_{n \geq 1} M^n$. By definition, a problem X is in level $B\Pi^2_M$ of the polynomial hierarchy if there exists a tuple $\alpha = (\alpha_1, \ldots, \alpha_k)$ of parameters from M, two polynomials p and q, and a sequence of circuits $(C_n)_{n \geq 1}$ such that C_n can be constructed in time polynomial in n, and such that for any $x \in M^n$, $x \in X$ if and only if:

$$\forall u \in \{0,1\}^{p(n)}\ \exists v \in \{0,1\}^{q(n)}\ C_n(x, u, v, \alpha) = 1. \qquad (1)$$

The other levels of the boolean polynomial hierarchy are defined in a similar way. For instance, if we take $p(n) = 0$ in (1) we obtain $B\Sigma^1_M$, and if we take $p(n) = q(n) = 0$ we obtain the class P_M of polynomial-time problems. A problem in this hierarchy is said to be parameter-free if no parameters are used, i.e., $k = 0$ in (1). Note that 0 and 1 can still be used since they are constants from the structure.

2.2 Sign Conditions

Let $C(x_1, \ldots, x_n, y_1, \ldots, y_m)$ be a circuit over M. A sign condition for C is a system of equations of the form $(C(x, y) = \epsilon_y)_{y \in \{0,1\}^m}$ where $\epsilon_y \in \{0, 1\}$. A sign condition σ can therefore be identified to a boolean vector of length 2^m; component y of σ is denoted $\sigma(y)$. Of course, a sign condition is said to be satisfiable if there exists an input $x \in M^n$ which satisfies it. If σ is satisfiable, $\sigma(y)$ is nothing but $C(x, y)$ where x is any input satisfying σ.

Definition 1 *A structure M is said to have few sign conditions if there exists a polynomial p such that any circuit $C(x_1, \ldots, x_n, y_1, \ldots, y_m)$ has at most $2^{p(mn\mathrm{size}(C))}$ satisfiable sign conditions.*

A standard argument shows that $(\mathbb{R}, +, -, \times, <)$ has few sign conditions:

Proposition 1 *The set of real numbers with its structure of ordered field has few sign conditions.*

Proof. Let $C(x_1, \ldots, x_n, y_1, \ldots, y_m)$ be a circuit of size s. We claim that there exists a set $\mathcal{P}$ of $M = 2^{m+s+1}$ polynomials of degree at most $d = 2^s$ such that for any pair of inputs $x, x' \in M^n$, if $\mathrm{sign}(p(x)) = \mathrm{sign}(p(x'))$ for all $p \in \mathcal{P}$ then x and x' satisfy the same sign condition of C. The proposition then follows from the well-known $(Md)^{O(n)}$ bound on the number of satisfiable sign conditions for a family of polynomials (see [2] for a sharper bound). The claim follows from the fact that for any $y \in \{0, 1\}^m$, $C(., y)$ can be simulated by a decision tree T_y of depth $\leq s$ in which every node is labeled by a test of the form "$p(x) \geq 0$?" where $\deg(p) \leq 2^s$. The set $\mathcal{P}$ is the union for all $y \in \{0, 1\}^m$ of the sets of polynomials tested at the nodes of T_y. $\square$

This property clearly holds in an arbitrary real-closed field (those are the ordered fields which satisfy the same first-order formula as $\mathbb{R}$, see for instance [14]) and therefore in an arbitrary ordered field since there cannot be more sign conditions in an ordered field than in its real closure. A very similar proof shows that algebraically closed fields (of any characteristic) also have few sign conditions. In this case we use the $(1 + Md)^n$ bound on the number of satisfiable sign conditions for a set of M polynomials of degree d in n variables ([10], Corollary 1). It follows again that an arbitrary field has few sign conditions.

We say that M has efficient enumeration of sign conditions if it has few sign conditions and they can be enumerated in polynomial space:

Definition 2 *A structure M is said to have efficient enumeration of sign conditions if it has few sign conditions and there exists a* PSPACE *algorithm $\mathcal{A}$ with the following property.*

Let $C(x_1, \ldots, x_n, y_1, \ldots, y_m)$ be a circuit with N satisfiable sign conditions. There exists an enumeration $\sigma_1, \ldots, \sigma_N$ of these sign conditions such that when $\mathcal{A}$ receives as input a triplet of the form (C, y, c) where $y \in \{0, 1\}^m$ and $c \geq 1$ is an integer:

(i) if $c \leq N$, the algorithm outputs $\sigma_c(y)$;

(ii) if $c > N$, the input is rejected.

Proposition 2 *The set of real numbers with its structure of ordered field has efficient enumeration of sign conditions.*

Proof. By the equivalence between space and parallel time, our main task is the following: given C, construct the set $\mathcal{C}$ of all satisfiable sign conditions of C in parallel polynomial time (using exponentially many processors). We first construct the set $\mathcal{P}$ of polynomials in the proof of Proposition 1. According to Proposition 4.1 of [18], the set of satisfiable sign conditions for a family of M polynomials of degree at most d in n variables can be constructed in parallel time $(\log L)[n \log(Md)]^{O(1)}$, where L is the maximum bit length of the coefficients of these polynomials. Since L is exponentially bounded for the polynomials of $\mathcal{P}$, the set $\mathcal{C}'$ of all satisfiable sign conditions of $\mathcal{P}$ can be constructed in parallel polynomial time. The construction of $\mathcal{C}$ from $\mathcal{C}'$ is straightforward (note that each sign condition of $\mathcal{C}'$ determines uniquely a sign condition of $\mathcal{C}$, but the converse is not always true). It just remains to choose some arbitrary order on the elements of $\mathcal{C}$, and given (y, c), to output $\sigma_c(y)$. □

The same property holds for algebraically closed fields (of any characteristic). We just have to replace Renegar's enumeration algorithm by the algorithm from [8].

3 The Transfer Theorem

Before proving our main theorem it is worth pointing out the following property, which was obtained by Cucker and Grigoriev [6] in the case $M = \mathbb{R}$. Recall that the boolean part of P_M is the set of problems in P_M which are boolean, i.e., contain only words.

Theorem 1 *If M has efficient enumeration of sign conditions, the boolean part of P_M is included in* PSPACE/poly.

Proof. Let Y be a boolean problem of P_M. There exist parameters $\alpha_1, \ldots, \alpha_k$ of M and a family of circuits $(C_n)_{n \geq 1}$ such that C_n can be constructed in time polynomial in n, and such that for any input $y \in \{0,1\}^n$, $y \in Y$ if and only if $C_n(\alpha, y) = 1$. Let N be the number of satisfiable sign conditions of $C_n(x, y)$. Since M has few sign conditions, N has polynomial bit size. Let $\sigma_1, \ldots, \sigma_N$ be the enumeration of these sign conditions given by the PSPACE algorithm of Definition 2. Let σ_{c_n} be the sign condition satisfied by α. Since $C_n(\alpha, y) = \sigma_{c_n}(y)$, Y can be solved in polynomial space using c_n as advice for inputs of size n. □

Theorem 2 *Let M be a structure which has efficient enumeration of sign conditions. If* $\mathrm{P} = \mathrm{PSPACE}$ *then $B\Sigma^2_M = B\Pi^2_M$.*

Proof. Let X be a problem which is $B\Pi^2_M$ without parameters. There exists a polynomial p and a sequence of parameter free circuits $(C_n)_{n \geq 1}$ such that C_n

can be constructed in time polynomial in n, and such that for any $x \in M^n$, $x \in X$ if and only if:

$$\forall u \in \{0,1\}^{p(n)} \; \exists v \in \{0,1\}^{p(n)} \; C_n(x,u,v) = 1.$$

Let N be the number of satisfiable sign conditions of $C_n(x,y)$, where y is the vector of boolean variables obtained by concatenation of u and v. Since M has few sign conditions, N has polynomial bit size. Let $\sigma_1, \ldots, \sigma_N$ be the enumeration of these sign conditions given by the PSPACE algorithm of Definition 2. Observe that $X \cap M^n$ is defined by the formula $\exists c \; \forall u, v \; F(c,u,v,x)$ where $F(c,u,v,x)$ stands for

$$(\sigma_c(u,v) = C_n(x,u,v)) \wedge \text{accept}(c)$$

and accept(c) stands for $\forall u \; \exists v \; \sigma_c(u,v) = 1$. By hypothesis on M, $\sigma_c(u,v)$ and thus accept(c) can be computed in polynomial space. If P = PSPACE, $F(c,u,v,x)$ can therefore be evaluated in polynomial time and X is $B\Sigma^2_M$.

In the general case, X is solved by a $B\Pi^2_M$ algorithm using k parameters $\alpha_1, \ldots, \alpha_k$. The conclusion follows from a routine argument: there exists a parameter-free $B\Pi^2_M$ problem Y such that an input $(x_1, \ldots, x_n)$ is in X if and only if $(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_k)$ is in Y. We have just seen that $Y \in B\Sigma^2_M$ if P = PSPACE. Under this assumption, X is therefore $B\Sigma^2_M$ as well. $\square$

Note that the collapse at the second level obtained here is optimal since the unconditional separation $B\Sigma^1_M \cup B\Pi^1_M \neq B\Sigma^2_M \cap B\Pi^2_M$ holds for the structure $M = (\mathbb{R}, +, -, =)$ of the reals with addition and equality [9], which admits efficient enumeration of sign conditions.

For some structures one can give a partial converse to this transfer theorem. In particular, it is known that the boolean part of $\mathrm{P}_{\mathbb{C}}$ is included in BPP (the boolean part of P_M for the structure $M = (\mathbb{R}, +, -, =)$ is included in BPP by Theorem 9 of [12], and the proof for $\mathbb{C}$ is identical). Since BPP $\subseteq$ P/poly [1] the collapse $B\Sigma^2_{\mathbb{C}} = B\Pi^2_{\mathbb{C}}$ would imply $\Sigma^2/\text{poly} = \Pi^2/\text{poly}$. We conclude that the separation $B\Sigma^2_{\mathbb{C}} \neq B\Pi^2_{\mathbb{C}}$ is most likely true, but extremely hard to prove. The collapse $B\Sigma^2_{\mathbb{R}} = B\Pi^2_{\mathbb{R}}$ also seems highly unlikely, but we cannot point to such a dramatic consequence as $\Sigma^2/\text{poly} = \Pi^2/\text{poly}$.

It is possible to give good bounds on the number of sign conditions in even richer structures than ordered fields. This is not surprising since, in light of the following observation, any structure which admits "good" VC dimension bounds has few sign conditions.

Remark 1 *Given a circuit $C(x_1, \ldots, x_n, y_1, \ldots, y_m)$, denote by $\mathcal{F}_C$ the family of functions $\{f_x;\; x \in M^n\}$ where $f_x : \{0,1\}^m \to \{0,1\}$ maps y to $C(x,y)$. The two following properties are equivalent.*

- *(i) there exists a polynomial q such that for any circuit $C(x_1, \ldots, x_n, y_1, \ldots, y_m)$ of size s, $\mathcal{F}_C$ has VC dimension at most $q(mns)$.*
- *(ii) M has few sign conditions.*

We recall that the Vapnik-Chervonenkis dimension of $\mathcal{F}_C$ is the cardinality of the largest set $X \subseteq \{0,1\}^m$ such that the restriction of $\mathcal{F}_C$ to X has cardinality $2^{|X|}$ (one says that X is *shattered* by $\mathcal{F}_C$).

Proof. If C has $\leq 2^{p(smn)}$ satisfiable sign conditions, $\mathcal{F}_C$ cannot shatter any set of cardinality larger than $p(smn)$. Conversely, if $\mathcal{F}_C$ has VC dimension bounded by $q(smn)$ then C has at most $(e2^m/q(smn))^{q(smn)}$ satisfiable sign conditions by Sauer's lemma (see for instance [5] and the references there). $\Box$

For instance, it follows from [11] that if we expand the ordered field of the real numbers with the exponential function, or even with Pfaffian functions, the resulting structure still has few sign conditions. It is however not known whether these structures have efficient enumeration of sign conditions. If one wishes to obtain sharp bounds on the number of sign conditions in a given structure, Remark 1 should probably not be applied directly since VC dimension bounds are usually obtained by bounding the number of satisfiable sign conditions!

Of course, there are also expansions of the real field which do not have few sign conditions.

Proposition 3 *The structure* $(\mathbb{R}, +, -, \times, \cos, <)$ *does not have few sign conditions.*

Proof. It is a variation on Sontag's proof that this structure does not admit finite VC dimension bounds [19]. By "fast exponentiation", there exists a circuit $C_m(x_1, x_2, y_1, \ldots, y_m)$ of size $O(m)$ such that $C_m(x_1, x_2, y_1, \ldots, y_m) = 1$ if $\cos(x_1.x_2^y) \geq 0$, and $C_m(x_1, x_2, y_1, \ldots, y_m) = 0$ otherwise. Here y denotes the integer with binary representation $y_1 y_2 \ldots y_m$.

We claim that C_m has 2^{2^m} satisfiable sign conditions. Choose x_2 so that π and x_2 are algebraically independent over $\mathbb{Q}$. The $2^m + 1$ real numbers $\pi, 1, x_2, x_2^2, \ldots, x_2^{2^m-1}$ are linearly independent over $\mathbb{Q}$. By Theorem 3.2 and Proposition 2.7 of ([15], chapter II), this implies that the values of $(x_1, x_1.x_2, x_1.x_2^2, \ldots, x_1.x_2^{2^m-1})$ modulo 2π are dense in $[0, 2\pi]^{2^m}$ as x_1 ranges over $\mathbb{R}$. The vectors of the form $(\cos(x_1), \cos(x_1.x_2), \cos(x_1.x_2^2), \ldots, \cos(x_1.x_2^{2^m-1}))$ as x_1 ranges over $\mathbb{R}$ are therefore dense in $[-1, 1]^{2^m}$. The claim and the proposition then follow immediately. $\Box$

References

[1] J.L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* EATCS Monographs on Theoretical Computer Science. Springer-Verlag, 1988.

[2] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM*, 43(6):1002–1045, 1996.

[3] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer-Verlag, 1998.

[4] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, July 1989.

[5] A. Blumer, A Ehrenfeucht, D. Haussler, and M. Warmuth. Learnability and the Vapnik-Chervonenkis dimension. *Journal of the ACM*, 36(4):929–965, 1989.

[6] F. Cucker and D. Grigoriev. On the power of real Turing machines with binary inputs. *SIAM Journal on Computing*, 26(1):243–254, 1997.

[7] F. Cucker and P. Koiran. Computing over the reals with addition and order: Higher complexity classes. *Journal of Complexity*, 11:358–376, 1995.

[8] N. Fichtas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *Journal of Pure and Applied Algebra*, 67:1–14, 1990.

[9] H. Fournier and P. Koiran. Lower bounds are not easier over the reals: Inside PH. LIP Research Report 99-21, Ecole Normale Supérieure de Lyon, 1999.

[10] J. Heintz. Definability and fast quantifier elimination over algebraically closed fields. *Theoretical Computer Science*, 24:239–277, 1983.

[11] M. Karpinski and A. Macintyre. Polynomial bounds for VC dimension of sigmoidal and general Pfaffian neural networks. *Journal of Computer and System Sciences*, 54:169–176, 1997.

[12] P. Koiran. A weak version of the Blum, Shub & Smale model. *Journal of Computer and System Sciences*, 54:177–189, 1997.

[13] P. Koiran. Circuits versus trees in algebraic complexity. In *Proc. STACS 2000*, volume 1770 of *Lecture Notes in Computer Science*, pages 35–54. Springer-Verlag, 2000.

[14] S. Lang. *Algebra*. Addison-Wesley, 1993.

[15] R. Mañé. *Ergodic Theory and Differentiable Dynamics*. Springer-Verlag, New York, 1987.

[16] K. Meer. A note on a $P \neq NP$ result for a restricted class of real machines. *Journal of Complexity*, 8:451–453, 1992.

[17] B. Poizat. *Les Petits Cailloux*. Nur Al-Mantiq Wal-Ma'rifah **3**. Aléas, Lyon, 1995.

[18] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. part I. *Journal of Symbolic Computation*, 13(3):255–299, March 1992.

[19] E. D. Sontag. Feedforward nets for interpolation and classification. *J. Comp. Syst. Sci.*, 45:20–48, 1992.