DIMACS Technical Report 96-24
July 1996

Elimination of Constants from Machines over Algebraically Closed Fields

by

Pascal Koiran[1]
LIP, Ecole Normale Supérieure de Lyon – CNRS
46 allée d'Italie, 69364 Lyon Cedex 07
France
email: `koiran@lip.ens-lyon.fr`

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Research, Bellcore, and Bell Laboratories.
DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.

Abstract

Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. We show that constants can be removed efficiently from any machine over $\mathbb{K}$ solving a problem which is definable without constants. This gives a new proof of the transfer theorem of Blum, Cucker, Shub & Smale for the problem $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$. We have similar results in positive characteristic for non-uniform complexity classes. We also construct explicit and correct test sequences (in the sense of Heintz and Schnorr) for the class of polynomials which are easy to compute.

An earlier version of this paper appeared as NeuroCOLT Technical Report 96-43. The present paper contains in particular a new bound for the size of explicit correct test sequences.

[1]A part of this work was done when the author was visiting DIMACS at Rutgers University.

1 Introduction

As in discrete complexity theory, the problem P $\stackrel{?}{=}$ NP is a major open problem in the Blum-Shub-Smale model of computation over the reals [3]. It has been possible to show that P$\neq$NP only in very simple structures, e.g., the reals with addition [11]. We note in passing that in contrast to other "non-standard" models of computation (e.g., oracle Turing machines), it is not known whether there exists a structure (even a "pathological" one) for which P = NP (the BSS model was generalized by Goode [7] and Poizat [15] to arbitrary first-order structures). Given this (rather sad) state of affairs, it is of great interest to study relationships between the P = NP problems in various structures. This line of research was pioneered in [2] where it is shown that P = NP over an algebraically closed field $\mathbb{K}$ of characteristic 0 if and only if P = NP over $\mathbb{C}$. Their result is based on an elimination of constants theorem.

In this paper we take a different view: instead of eliminating constants only for inputs in a subfield $K \subseteq \mathbb{K}$ of the original field as in [2], we allow inputs from the original field. There is clearly a price to pay in order to achieve this result: one can no longer deal with arbitrary machines. For instance, it is impossible to recognize the language $L = \{\pi\}$ over $\mathbb{C}$ without transcendental constants. Therefore we only consider languages which are definable without constants. A language is said to be definable without constants if for each input size n there is a formula F_n in the first order-theory of $\mathbb{K}$ such that 0 and 1 are the only constants occurring in F_n, and for any $x \in \mathbb{K}^n$, $x \in L$ if and only if $F_n(x)$ is true. Most problems of interest (e.g., Hilbert's Nullstellensatz $\mathrm{HN}_{\mathbb{K}}$, the canonical NP-complete problem in any field) are definable without constants.

In section 3, we show that algebraic constants can be removed with a polynomial slowdown from any machine solving a problem which is definable without constants (there is no restriction on the size of the defining formulas). This is the most general case in which elimination of constants is possible. Indeed, a language recognized by a constant-free machine is clearly definable without constants (because computations of constant-free machines can be described by constant-free formulas). In other words, if algebraic constants can be at all eliminated, they can be eliminated effectively, and efficiently. For transcendental constants, a similar result is established in section 7. This makes it possible to recover the transfer theorem of [2]. Since the general case is more involved, we start by eliminating transcendental constants from a restricted class of machines in section 4 (as shown in section 5, the transfer theorem can be obtained from this partial result). We have similar results in positive characteristic, but only for the non-uniform classes $\mathbb{P}$ and $\mathbb{NP}$. This gives a partial answer to an open problem in [2]. (for uniform classes, one can expect to have a transfer result at a higher level in the polynomial hierarchy, e.g., for the problem $\Sigma_2 = \Pi_2$.) Our results are based on quantifier elimination instead of algebraic number theory as in [2].

Along the way, we give in section 6 an application of quantifier-elimination to a more "concrete" problem, namely, the construction of correct test sequences in the sense of Heintz and Schnorr [8]. We construct short and correct test sequences for the class of polynomials which are "easy to compute". This result can be viewed as a refinement of the Witness Theorem of [2].

Quantifier elimination techniques also apply to a restricted class of machines over real-closed fields. This will be elaborated in a future publication.

2 Background

2.1 Elimination of Quantifiers

Good bounds for quantifier elimination can be found in a number of papers written in the last 15 years. Here we have followed [5].

Theorem 1 *Let K be an algebraically closed field and Φ a prenex formula in the first-order theory of K. Let $|\Phi|$ be the length of the formula, r be the number of quantifier blocks, n the total number of variables, and $\sigma(\Phi)$ the total degree of Φ, defined as:*

$$\sigma(\Phi) = 2 + \sum_{i=1}^{s} \deg\ F_i$$

where $F_1, \ldots, F_s$ are the polynomials occurring in Φ.

(i) There exists a quantifier elimination algorithm (in the model of uniform arithmetic circuits over K) which works in parallel time

$$n^{O(r)}(\log \sigma(\Phi))^{O(1)} + O(\log |\Phi|)$$

and sequential time $\sigma(\Phi)^{n^{O(r)}}.|\Phi|$.

(ii) The same bounds hold for the complexity of the decision problem in the first-order theory of K.

Note that $|\Phi|$ occurs in these bounds only to account for a preprocessing stage. Therefore this parameter does not appear in the following result. The degree and bit size bounds follow from the parallel complexity bound in (i)

Corollary 1 *With the notations of Theorem 1, Φ is equivalent to a quantifier-free formula Ψ in which all polynomials have degree at most*

$$2^{n^{O(r)}(\log \sigma(\Phi))^{O(1)}}.$$

The number of polynomials occurring in Ψ is $O(\sigma(\Phi)^{n^{O(r)}})$.

Moreover, when K is of characteristic 0 and Φ is a formula in which all constants are integers of bit-size at most L, the constants in ψ are integers of bit size at most $L.2^{n^{O(r)}(\log \sigma(\Phi))^{O(1)}}$. When K is of characteristic $p > 0$ and Φ is a formula in which all constants are in $F_p = \mathbb{Z}/p\mathbb{Z}$, the constants in ψ are also all in F_p.

A subset $S \subseteq \mathbb{K}^n$ is *quasi-algebraic* if it is defined by a first-order formula, i.e., if $S = \{x \in \mathbb{K}^n;\ F(x) \text{ is true}\}$ for some formula F. A *basic* quasi-algebraic set is defined by a system $P_1(x) = 0, \ldots, P_k(x) = 0, Q_1(x) \neq 0, \ldots, Q_l(x) \neq 0$ where $k, l \geq 0$ and each polynomial is in $\mathbb{K}[X_1, \ldots, X_n]$. By quantifier elimination, every quasi-algebraic set is a finite union of basic quasi-algebraic sets.

2.2 Complexity of Computations in Fields

A Blum-Shub-Smale machine over a field $\mathbb{K}$ can perform the four arithmetic operations and branches over equality tests only. It can use a finite number of constants from $\mathbb{K}$ in its program (eliminating these constants is the main goal of this paper). We shall not go into a formal description of the model since there is a concise definition of the main complexity classes in terms of circuits [7, 15]. For more details on the original model, see [3], [12] or the forthcoming book [1].

Definition 1 *A problem over a field $\mathbb{K}$ is a subset of $\mathbb{K}^\infty = \bigcup_{n=0}^{\infty} \mathbb{K}^n$. A problem L is in $\mathrm{P}_{\mathbb{K}}$ if there is an element $\alpha \in \mathbb{K}^p$ and a circuit family $(C_n)_{n \in \mathbb{N}}$ made of arithmetic gates $(+, -, \times, /)$ or equality gates (is the input equal to 0 ?) such that:*

1. *The family is uniform in the sense that an ordinary (discrete) Turing machine can produce C_n in time polynomial in n.*

2. C_n has $n+p$ inputs, and for any $x \in \mathbb{K}^n$, $x \in L$ if and only if $C_n(x, \alpha) = 1$.

We say that a circuit or a machine is without constants (or *constant-free*) if $\alpha = 1$. Note that one can get rid of division gates by computing separately numerators and denominators; this can at most double the circuit size.

One can go from $\mathrm{P}_{\mathbb{K}}$ to $\mathrm{NP}_{\mathbb{K}}$ in the same way as in the discrete setting.

Definition 2 *A problem L is in $\mathrm{NP}_{\mathbb{K}}$ if there exists a polynomial $p(n)$ and a problem L' in $\mathrm{P}_{\mathbb{K}}$ such that for any $x \in \mathbb{K}^n$, $x \in L$ if and only if*

$$\exists y \in \mathbb{K}^{p(n)} (x, y) \in L'.$$

The non-uniform class $\mathbb{P}_{\mathbb{K}}$ is obtained by removing condition 1 from Definition 1; $\mathbb{NP}_{\mathbb{K}}$ is obtained from $\mathbb{P}_{\mathbb{K}}$ in the same way as $\mathrm{NP}_{\mathbb{K}}$ is obtained from $\mathrm{P}_{\mathbb{K}}$. When there is no risk of confusion, we sometimes drop the subscript $\mathbb{K}$. For $K = F_2 = \mathbb{Z}/2\mathbb{Z}$, the familiar complexity classes P, NP, P/poly and NP/poly are recovered.

In any field $\mathbb{K}$, Hilbert's Nullstellensatz (denoted $\mathrm{HN}_{\mathbb{K}}$) is $\mathrm{NP}_{\mathbb{K}}$-complete (for many-one $\mathrm{P}_{\mathbb{K}}$ reductions). The input to this problem is a system

$$P_i(x) = 0, \ 1 \leq i \leq m$$

of polynomial equations in several variables, with coefficients in $\mathbb{K}$ (the polynomials are given as a sum of monomials). The system is in $\mathrm{HN}_{\mathbb{K}}$ if and only if it has a solution over $\mathbb{K}$. By introducing intermediate variables, one can assume without loss of generality that the P_i's have degree at most 2. $\mathrm{HN}_{\mathbb{K}}$ is also $\mathbb{NP}_{\mathbb{K}}$-complete for many-one $\mathbb{P}_{\mathbb{K}}$ reductions. Hence $\mathrm{P}_{\mathbb{K}} = \mathrm{NP}_{\mathbb{K}}$ if and only if $\mathrm{HN}_{\mathbb{K}} \in \mathrm{P}_{\mathbb{K}}$, and $\mathbb{P}_{\mathbb{K}} = \mathbb{NP}_{\mathbb{K}}$ if and only if $\mathrm{HN}_{\mathbb{K}} \in \mathbb{P}_{\mathbb{K}}$.

2.3 Some Model Theory

We often use the following transfer principle: if $K \subseteq \mathbb{K}$ are two algebraically closed fields then $\mathbb{K}$ is an elementary extension of K, i.e., a first-order formula with constants in K only is true in $\mathbb{K}$ if and only if it is true in K.

A structure $\mathbb{K}$ is said to be ω-saturated if for any family $S = \{F_n(x); n \in \mathbb{N}\}$ of first-order formulas where $x \in \mathbb{K}^p$ (for some fixed p independent of n), S is satisfiable if and only if all finite subsets of S are satisfiable (S is said to be satisfiable if there exists an $x \in \mathbb{K}^p$ which satisfies all the F_n simultaneously). In this definition we assume implicitly that the parameters in the F_n come from a fixed, finite set. The algebraic closures $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and

$\overline{F_q}$ of $F_q = \mathbb{Z}/q\mathbb{Z}$ (where q is prime) are not ω-saturated. However, the field of complex numbers is an ω-saturated elementary extension of $\overline{\mathbb{Q}}$. Like any structure, $\overline{F_q}$ also has ω-saturated elementary extensions ([14], Théorème 5.1). In the sequel $\mathbb{F}_q$ denotes such an extension.

3 Elimination of Algebraic Constants

In this section $\mathbb{K}$ can be any algebraically closed field.

Theorem 2 *Assume that a problem L over $\mathbb{K}$ can be solved by a machine M whose constants lie in an algebraic extension $K[\beta_1, \ldots, \beta_q]$ of a subfield $K \subseteq \mathbb{K}$.*

If L is definable with constants in K only, this problem can be solved by a machine M' with constants in K only; moreover, for any input $x \in \mathbb{K}^\infty$, the running time of M' satisfies $T_{M'}(x) \leq T_M(x)^c$. The constant c is independent of x.

This is the most general case in which elimination of constants is possible. Indeed, if there exists a machine with constants in K which recognizes L, this implies obviously that L is definable with constants in K only.

For the proof of this Theorem it is possible to assume that $q = 1$. Indeed, in the general case, one can work with the tower of extensions $K[\beta_1][\beta_2]\ldots[\beta_q]$ and remove the constants iteratively (starting from β_q) using the $q = 1$ result. Therefore in the remainder of this section we assume that $\beta = \beta_1$ is the only constant of M. (note also that if $\mathbb{K}$ is of characteristic 0, any finite extension is generated by a single β according to the primitive element theorem.)

Recall that if m is the minimal polynomial of β over K, the conjugates of β are by definition the other roots of m.

Lemma 1 *Let $M_{\beta'}$ be the machine obtained from M by replacing β by the new constant β'. Let $L_{\beta'}$ be the language recognized by $M_{\beta'}$. If β' is a conjugate of β, $L_{\beta'} = L$.*

Proof. Let S_n be the set of constants $\overline{\beta}$ such that $L_{\overline{\beta}}$ agrees with L for inputs in $\mathbb{K}^n$. If $F_n(x)$ is a formula with constants in K defining L for inputs in $\mathbb{K}^n$, S_n can be defined as follows:

$$\forall x \in \mathbb{K}^n, x \in L_{\overline{\beta}} \Leftrightarrow F_n(x).$$

This formula is equivalent to a quantifier-free formula $G_n(\overline{\beta})$ with parameters in K. It is a simple and well-known fact that for any polynomial P with coefficients in K, $P(\beta) = 0$ if and only if $P(\beta') = 0$ (because the gcd of P and m can only be 1 or m). Applying this observation to the polynomials occurring in G_n, we see that β satisfies this formula if and only if β' does. $\square$

Proof of Theorem 2. To each input size n we can associate an algebraic decision tree T_n which represents the computation of machine $M_{\overline{\beta}}$. For each input $x \in \mathbb{K}^n$, M' will explore this tree in a breadth-first way. Only nodes that can be reached for a $\overline{\beta}$ such that $m(\overline{\beta}) = 0$ will be explored. In order to decide whether to explore a child c of a previously explored node, one constructs a system of the form

$$m(\overline{\beta}) = 0, P_1(\overline{\beta}) = 0, \ldots, P_i(\overline{\beta}) = 0, Q_1(\overline{\beta}) \neq 0, \ldots, Q_j(\overline{\beta}) \neq 0. \qquad (1)$$

The P_i's and Q_j's correspond to the outcomes of the tests performed between the root of the tree and c. If (1) is satisfiable, c should be explored. We stop as soon as a leaf of T_n is reached, and accept the input $x \in \mathbb{K}^n$ if and only if this leaf is accepting. The correctness of this algorithm follows from Lemma 1.

Let us now show that it can be implemented in polynomial time. By hypothesis there exists a leaf at depth $T_M(x)$; hence we do not not explore nodes at a greater depth. Let k be the degree of the minimum polynomial m. There are at most k distinct paths in the subtree T'_n of T_n explored by M' since each root of m follows a well-defined path. Hence T'_n has at most $kT_M(x)$ nodes. It just remains to examine the complexity of testing the satisfiability of (1). By computing modulo m, one can assume that the P_i's and Q_j's are of degree less than k. Hence this test can be performed in polynomial time by Theorem 1. (using this result is overkill since (1) is only a one-dimensional problem, but this is sufficient for our purpose.) $\square$

4 Elimination of Transcendental Constants

4.1 Characteristic Zero

In this section $\mathbb{K}$ can be any algebraically closed field of characteristic 0.

Theorem 3 *If* $\mathrm{P}_{\mathbb{K}} = \mathrm{NP}_{\mathbb{K}}$ *then* $\mathrm{HN}_{\mathbb{K}}$ *can be solved in polynomial time without constants.*

Proof. Assume that $\mathrm{P}_{\mathbb{K}} = \mathrm{NP}_{\mathbb{K}}$. Then $\mathrm{HN}_{\mathbb{K}}$ can be solved in polynomial time by a machine M. By standard results of algebra, one may assume that its irrational constants are $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$ where $\alpha_1, \ldots, \alpha_p$ are algebraically independent and $\beta_1, \ldots, \beta_q$ are algebraic over $K[\alpha_1, \ldots, \alpha_p]$. By Theorem 2, $\mathrm{HN}_{\mathbb{K}}$ can be solved in polynomial time with constants in $\{\alpha_1, \ldots, \alpha_p\}$ only. One can get rid of these constants by Proposition 1. □

Proposition 1 *If* $\mathrm{HN}_{\mathbb{K}}$ *can be solved in polynomial time using algebraically independent constants* $\alpha_1, \ldots, \alpha_p$*, it can be solved in polynomial time without constants.*

Proof. For each (m, n), the vector of constants $\alpha = (\alpha_1, \ldots, \alpha_p)$ can be used by a machine M to decide in polynomial time whether a system of m equations of degree 2 in n unknowns has a solution. The idea of the proof is to replace for each (m, n) the vector α by a new vector of integers $\overline{\alpha}$ (a *witness*) which will play the same role. These integers will be explicitly constructed by the new machine M'. Let $L_{\overline{\alpha}}$ be the language recognized by M when α is replaced by $\overline{\alpha}$. The set S of suitable $\overline{\alpha}$'s can be defined by the following first-order formula:

$$\forall (a_{i,\nu})_{1 \le i \le m, |\nu| \le 2}, (a_{i,\nu}) \in L_{\overline{\alpha}} \Leftrightarrow \exists x \in \mathbb{K}^n \bigwedge_{i=1}^{m} \sum_{|\nu| \le 2} a_{i,\nu} x^{\nu} = 0$$

(here ν is a multi-index). Note that strictly speaking, this is not a first-order formula. However, the predicate $(a_{i,\nu}) \in L_{\overline{\alpha}}$ can be replaced by a polynomial-size first-order formula (we introduce one new existentially quantified variable for each gate in the circuit C_n of Definition 2). One could also obtain directly a quantifier-free formula for $(a_{i,\nu}) \in L_{\overline{\alpha}}$ by going through all the computation paths of M, but this would cause an exponential blowup in size.

By quantifier elimination, S is a finite union of basic quasi-algebraic sets $S_1, \ldots, S_k$, i.e., each S_i is defined by a system $P_1(x) = 0, \ldots, P_{m_i}(x) = 0, Q_1(x) \neq 0, \ldots, Q_{n_i}(x) \neq 0$ where each polynomial is in $\mathbb{Z}[X_1, \ldots, X_p]$. Since $\alpha \in S$ and $\alpha_1, \ldots, \alpha_p$ are algebraically independent, there must be at least one S_i for which $m_i = 0$. Hence $\overline{\alpha}$ can be any vector of integers which satisfies the constraints $Q_1(\overline{\alpha}) \neq 0, \ldots, Q_{n_i}(\overline{\alpha}) \neq 0$. Such a vector can be constructed in polynomial time by Corollary 1 and Lemma 2 (we use repeated squaring). □

The next lemma is similar to [8], Lemma 4.2.

Lemma 2 *Let $P \in \mathbb{Z}[X_1, \ldots, X_p]$ be a degree d polynomial with coefficients bounded by M in absolute value. Let $\alpha = (\alpha_1, \ldots, \alpha_p)$ be any sequence of integers satisfying $\alpha_1 \geq M + 1$ and $\alpha_k \geq 1 + d^{k-1}\alpha_{k-1}^d$ for $k \geq 2$. Then if P is not identically zero, $P(\alpha) \neq 0$.*

Proof. For $p = 1$, this follows from the standard bound on polynomial roots. Assume by induction that the result holds for $p - 1$, and write $P(x) = \sum_{j=0}^{d} P_j(x_1, \ldots, x_{p-1})x_p^j$. If $P \not\equiv 0$, one of the P_j's must be non-zero. By induction hypothesis, such a P_j takes a non-zero value at $(\alpha_1, \ldots, \alpha_{p-1})$. consider the polynomial $Q(x) = \sum_{j=0}^{d} P_j(\alpha_1, \ldots, \alpha_{p-1})x_p^j$. Since P_j is of degree at most d, it cannot have more than d^{p-1} monomials. Therefore the coefficients of Q are bounded by $d^{p-1}\alpha_{k-1}^d$. The result now follows from the case $p = 1$. □

4.2 Positive Characteristic

In this section $\mathbb{K}$ can be any algebraically closed field of characteristic $q > 0$.

Theorem 4 *If $\mathrm{HN}_{\mathbb{K}} \in \mathrm{P}_{\mathbb{K}}$ then $\mathrm{HN}_{\mathbb{K}}$ can be solved by a polynomial size constant-free circuit family.*

Proof. It proceeds as in Theorem 3. We can assume that the constants $\alpha_1, \ldots, \alpha_p$ in the circuit family are algebraically independent by Theorem 2 (it is clear that the uniformity hypothesis can be removed from that theorem). One can get rid of these constants iteratively (starting with α_p) by Proposition 2. □

Proposition 2 *Assume that $\mathrm{HN}_{\mathbb{K}}$ can be solved by a polynomial size circuit family with constants in a transcendental extension $K[\alpha]$ of a subfield $K \subseteq \mathbb{K}$. Then $\mathrm{HN}_{\mathbb{K}}$ can be solved by a polynomial size circuit family with constants in K only.*

Proof. We need an element $\overline{\alpha}$ satisfying a system $Q_1(\overline{\alpha}) \neq 0, \ldots, Q_{n_i}(\overline{\alpha}) \neq 0$ as in Proposition 1. We can no longer use Lemma 2 to construct $\overline{\alpha}$; however, it follows (non-constructively) from Corollary 1 and Lemma 4 that $\overline{\alpha}$ can be taken to be any root of an irreducible polynomial $m \in F_p[X]$ of degree $(n \log m)^{O(1)}$. One can get rid of the new constant $\overline{\alpha}$ by Theorem 2 (in that theorem we assumed that the degree k of m was fixed; however, it is clear from the proof that the simulation remains polynomial-time even when k is not a constant). □

Before proving Lemma 4 we need the following result. For a proof, see [13], section 6.2, Proposition 2 or [9], section 4.6.2, exercise 4.

Lemma 3 *The number $I_{n,q}$ of monic irreducible polynomials of degree n in F_q satisfies:*

$$q^n - 2q^{n/2} < nI_{n,q} \leq q^n.$$

Lemma 4 *Let $(Q_i)_{1 \leq i \leq N}$ be a sequence of polynomials in $\mathbb{K}[X]$, of degree $d_i \in \{1, \ldots, d\}$. For any $n \geq 4 + 2\log Nd/\log q$, there exists an irreducible polynomial $m \in F_q[X]$ of degree n which has no common root with $Q_1, Q_2, \ldots$ or Q_n.*

Proof. Altogether the Q_i's have at most Nd roots. Since two distinct irreducible monic polynomials cannot have a common root, it is sufficient to have $I_{n,q} > Nd$. It follows easily from Lemma 3 that this condition will be satisfied if $n \geq 4$ and $q^n \geq 2nNd$. A sufficient condition for this to be true is: $\log 2Nd \leq (n \log q)/2$ and $\log n \leq (n \log q)/2$. The second condition always holds for $n \geq 2$, whence the result. $\square$

5 Transfer

In characteristic 0, we recover the main result of [2].

Theorem 5 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields of characteristic 0.* P = NP *over $\mathbb{K}$ if and only if* P = NP *over K.*

Proof Sketch. If P = NP over K, HN_K can be solved in polynomial time by a machine over K. By the transfer principle of section 2.3, this machine solves $\mathrm{HN}_{\mathbb{K}}$ for inputs in $\mathbb{K}$. Hence P = NP over $\mathbb{K}$.

If P = NP over $\mathbb{K}$, $\mathrm{HN}_{\mathbb{K}}$ can be solved in polynomial time by a machine M. By Theorem 3, we can assume that M is constant-free. Therefore M also solves HN_K by the transfer principle, and P = NP over K. $\square$

In positive characteristic, we can prove a transfer result only for non-uniform complexity classes (it is clear from the proof that the same result holds in characteristic 0).

Theorem 6 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields of characteristic 0. $\mathbb{P} = \mathbb{NP}$ over $\mathbb{K}$ if and only if $\mathbb{P} = \mathbb{NP}$ over K.*

Proof Sketch. If $\mathbb{P} = \mathbb{NP}$ over K, HN_K is in $\mathbb{P}$ over K. By the transfer principle, the same circuit family will solve $\mathrm{HN}_{\mathbb{K}}$ for inputs in $\mathbb{K}$. Hence $\mathbb{P} = \mathbb{NP}$ over $\mathbb{K}$.

If $\mathbb{P} = \mathbb{NP}$ over $\mathbb{K}$, $\mathrm{HN}_{\mathbb{K}}$ is in $\mathbb{P}$ over $\mathbb{K}$. By Theorem 4, we can assume that the corresponding circuit family is constant free. Therefore this circuit family also solves HN_K by the transfer principle, and $\mathbb{P} = \mathbb{NP}$ over K. □

As pointed out in [2], in characteristic 0 the problem P = NP over $\mathbb{K}$ reduces to the single problem P = NP over $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. In characteristic $p > 0$, it follows from Theorem 6 that if $\mathbb{K}$ is algebraically closed, $\mathbb{P}_{\mathbb{K}} = \mathbb{NP}_{\mathbb{K}}$ if and only if $\mathbb{P} = \mathbb{NP}$ over $\overline{F_p}$, the algebraic closure of F_p. Note that if $\mathbb{K}$ is infinite but not algebraically closed, it cannot have elimination of quantifiers [10], and thus $\mathbb{P}_{\mathbb{K}} \neq \mathbb{NP}_{\mathbb{K}}$.

6 Correct Test Sequences

The notion of *correct test sequence* plays a crucial role in section 7. Let $\mathcal{F}$ be a family of polynomials in $\mathbb{K}[X_1, \ldots, X_p]$. A sequence $(a_i)_{1 \leq i \leq s}$ of points in $\mathbb{K}^p$ is a correct test sequence for $\mathcal{F}$ if for any $P \in \mathcal{F}$, $P(a_i) = 0$ for all $i = 1, \ldots, s$ implies $P \equiv 0$.

Definition 3 *A straight-line program of length v is a sequence $P_1, \ldots, P_v$ of polynomials in $\mathbb{K}[X_1, \ldots, X_p]$ such that each P_i is a constant of $\mathbb{K}$, or one of the indeterminates $X_1, \ldots, X_p$, or $P_i = P_j \perp P_k$ with $\perp \in \{+, \times\}$ and $1 \leq j \leq k < i$. The result of the computation is P_v. The set of polynomials of degree $\leq d$ which can be computed by straight-line programs of length v is denoted $W(d, p, v)$.*

The following result is due to Heintz & Schnorr ([8], Theorem 4.4). It establishes the existence of small test sequences for family of polynomials computed by short straight-line programs (see [4] for an alternative proof of a similar result).

Theorem 7 *Let $\mathbb{K}$ be an algebraically closed field and U a subset of $\mathbb{K}$ of cardinality at least $u = 2v(d + 1)^2$. There exists a correct test sequence of length $s = 6(v + p)(v + p + 1)$ for $W(d, p, v)$ such that $a_i \in U^p$ for all $i = 1, \ldots, s$.*

In fact, v can be replaced by the number of so-called *nonscalar* operations, i.e., multiplications between two non-constant polynomials [8]. In that paper Theorem 7 was stated only for fields of characteristic 0 and for $U = \{1, 2, \dots, u\}$ (we apply it in this form in section 7.1). The present formulation is used for instance in [6].

Theorem 7 is a non-constructive result. Heintz and Schnorr do give explicit constructions for polynomials with bounded integer coefficients in Lemma 4.2 of [8] (this result is similar to our Lemma 2), and for polynomials with unbounded rational coefficients in Lemma 4.3. We describe in this section explicit correct test sequences for the class of all polynomials that are easy to compute (in characteristic 0 only). The construction is surprisingly similar to that of Lemma 2: any sufficiently fast growing sequence of integers can do the job. Note that this result provides an alternative to the Witness Theorem of [2]. In that Theorem, it is shown that given the parameters of a straight line-program, one can dynamically construct a short test sequence which is correct for the corresponding polynomial. Here we show that, in fact, the same test sequence can be used for all values of the parameters. The points in this sequence have exponential binary length, but they can nonetheless be constructed in polynomial time by repeated squaring. As in the Witness Theorem, the sequence has length $p+1$, where p is the number of parameters.

We state our result for the class $W'(n, p, v)$ of polynomials over $\mathbb{C}$ in n variables that can be computed by straight-line programs of length at most v using p complex parameters. (By transfer it holds in any algebraically closed field of characteristic 0.) The following lemma is needed.

Lemma 5 *Let $P : \mathbb{C}^p \times \mathbb{C}^n \to \mathbb{C}$ be a polynomial map. For $l \in \mathbb{N}$, let*

$$A_l = \{(u_1, \dots, u_l) \in \mathbb{C}^{ln};\ \exists \alpha \in \mathbb{C}^p\, P(\alpha, .)\not\equiv 0 \wedge P(\alpha, u_1) = 0 \wedge \dots \wedge P(\alpha, u_l) = 0\}.$$

A_l is a quasi-algebraic set of dimension at most $p + l(n-1)$. In particular, A_{p+1} has positive codimension.

The meaning of this lemma is that "most" sequences of length $p+1$ are correct test sequences for the family $\{x \mapsto P(\alpha, x);\ \alpha \in \mathbb{C}^p\}$. A proof of a similar result for real-analytic functions can be found in [16]. The proof carries over to the present situation with minor modifications (Eduardo Sontag, personal communication). This lemma is also implicit in [8].

Theorem 8 *There are universal constants c_1 and c_2 such that the following property holds:*

Set $d = 2^{(n+v)^{c_1}}$ and $M = 2^{2^{(n+v)^{c_2}}}$. Let $v_1, \dots, v_{n(p+1)}$ be a sequence of integers such that $v_1 \geq M + 1$ and $v_k \geq 1 + d^{k-1} v_{k-1}^d$ for $k \geq 2$. Let

$u_1, \ldots, u_s$ *be the sequence of points in* $\mathbb{N}^n$ *defined by:*

$$u_i = (v_{1+n(i-1)}, v_{2+n(i-1)}, \ldots, v_{ni}). \tag{2}$$

Then $(u_1, \ldots, u_{p+1})$ *is a correct test sequence for* $W'(n, p, v)$.

Proof. Let us fix a straight-line program of length $\leq v$ which uses p complex parameters, and let $\mathcal{P} = \{P_\alpha; \alpha \in \mathbb{C}^n\}$ be the family of polynomials computed by the straight-line program as the vector $(\alpha_1, \ldots, \alpha_p)$ of parameters ranges over $\mathbb{C}^p$. We shall see that (2) is a correct test sequence for $\mathcal{P}$. The set S of test sequences $u = (u_1, \ldots, u_{p+1})$ which are correct for $\mathcal{P}$ can be defined by the following formula:

$$\forall \alpha \in \mathbb{C}^p \ \forall x \in \mathbb{C}^n \left[\bigvee_{i=1}^{p+1} P_\alpha(u_i) \neq 0 \vee P_\alpha(x) = 0 \right]. \tag{3}$$

By introducing v universally quantified variables for the values computed at each step of the straight-line program, the condition $P_\alpha(x) = 0$ can be expressed by a well-formed first-order formula of length $O(v)$; the same is true for the $p+1$ conditions $P_\alpha(u_i) \neq 0$ (this technique was used in the proof of Proposition 1). Having done this, one can put (3) in prenex form. The resulting formula has a single block of (universal) quantifiers, and at most $p + (n+v)(p+2)$ variables.

Since the map $(\alpha, x) \mapsto P_\alpha(x)$ is polynomial, S is non-empty by Lemma 5 and, in fact, has full dimension. One can thus argue as in the proof of Proposition 1: by quantifier elimination, S must contain a set of the form $Q_1(u) \neq 0, \ldots, Q_m(u) \neq 0$. By Corollary 1, there is a $2^{(n+v)^{O(1)}}$ bound on the degree and bit size of the Q_i's. The claimed result then follows from Lemma 2. □

It would be interesting to have a direct proof (bypassing Lemma 5) that sequences of points with exponentially fast-growing components are correct test sequences for $W'(n, p, v)$.

It is shown in [8] that $W(d, n, v)$ can be embedded in a set of dimension $(v+n)(v+n+1)$. This implies as in Lemma 5 that "most" test sequences of length $(v+n)(v+n+1)+1$ are correct for $W(d, n, v)$ (this is implicit in the proof of Theorem 4.4 in [8]). In some cases this may be better than the $p+1$ bound of Lemma 5 since v counts only non-scalar operations. One can work out as in Theorem 8 a single-exponential bound for the bit size of a an explicit correct test sequence of length $(v+n)(v+n+1)+1$. The *total* number of operations would appear in this bound.

7 Transcendental Constants: the General Case

The following result is similar to Lemma 1.

Lemma 6 *Let $\mathbb{K}$ be algebraically closed field and $L \subseteq \mathbb{K}^\infty$ a problem which is definable without constants. Let M be a machine which recognizes L using only algebraically independent constants $\alpha_1, \ldots, \alpha_p$, and $M_{\alpha'}$ the machine obtained from M by replacing $\alpha = (\alpha_1, \ldots, \alpha_p)$ by a new vector of constants $\alpha' = (\alpha'_1, \ldots, \alpha'_p)$. Let $L_{\alpha'}$ be the language recognized by $M_{\alpha'}$. If $\alpha'_1, \ldots, \alpha'_p$ are algebraically independent, $L_{\alpha'} = L$.*

Proof. Let S be the set of constants $\overline{\alpha}$ such that $L_{\overline{\alpha}}$ agrees with L for inputs in $\mathbb{K}^n$. If $F_n(x)$ is a formula without constants defining L for inputs in $\mathbb{K}^n$, S can be defined as follows:

$$\forall x \in \mathbb{K}^n, x \in L_{\overline{\alpha}} \Leftrightarrow F_n(x).$$

We can now argue as in Proposition 1: by quantifier elimination, S_n is a finite union of basic quasi-algebraic sets $S_1, \ldots, S_k$, and these sets are defined by polynomial (in)equations with rational coefficients only. Since $\alpha \in S$, at least one S_i must be defined by disequalities only. Hence $\alpha' \in S_i$ if $\alpha'_1, \ldots, \alpha'_p$ are algebraically independent, and *a fortiori* $\alpha' \in S$. □

7.1 Characteristic Zero

Theorem 9 *Let $L \subseteq \mathbb{C}^\infty$ be a problem which is definable without constants. If $L \in \mathrm{P}_\mathbb{C}$, L can be recognized in polynomial time by a constant-free machine.*

Proof. We can assume that the constants $\alpha_1, \ldots, \alpha_p$ of a polynomial-time machine M recognizing L are algebraically independent: if there are additional constants $\beta_1, \ldots, \beta_q$ which are algebraic over $\alpha_1, \ldots, \alpha_p$, they can be removed by Theorem 2 (as in Theorems 3 and 4).

Moreover, given an input $x \in \mathbb{C}^n$, we can assume by Lemma 6 that $\alpha_1, \ldots, \alpha_p$ are algebraically independent over $\mathbb{Q}[x_1, \ldots, x_n]$ (i.e., for any polynomial P with coefficients in $\mathbb{Q}[x_1, \ldots, x_n]$, $P(\alpha) = 0$ implies $P \equiv 0$). This means that $\alpha_1, \ldots, \alpha_p$ can be viewed as indeterminates rather than specific elements of $\mathbb{C}$; and that M can be viewed as computing over $\mathbb{C}[X_1, \ldots, X_p]$ instead of $\mathbb{C}$. In particular, a test of the form "$y = 0$?" with $y \in \mathbb{C}$ can be viewed as a test "$P \equiv 0$?" with $P \in \mathbb{C}[X_1, \ldots, X_p]$.

A precise justification is as follows: let $P_1, \ldots, P_m$ be the sequence of polynomials that are tested for nullity during the computation of M on input x. If $P_i(X_1, \ldots, X_p) \equiv 0$ then $P_i(\alpha_1, \ldots, \alpha_p) = 0$ for any $(\alpha_1, \ldots, \alpha_p)$; conversely, if $P_i(X_1, \ldots, X_p) \not\equiv 0$ then $P_i(\alpha) \neq 0$ since $\alpha_1, \ldots, \alpha_p$ are algebraically independent over $\mathbb{Q}[x_1, \ldots, x_n]$.

We can use Theorem 8 to perform the tests "$P_i \equiv 0$?". If $T(n)$ is an upper bound on the running time of M for inputs in $\mathbb{C}^n$, the P_i's are in $W'(p, n, T(n))$. Hence the test sequence (2) can be constructed in polynomial time. $\square$

Corollary 2 *Let $\mathbb{K}$ be an algebraically closed field of characteristic 0, and $L \subseteq \mathbb{K}^\infty$ a problem which is definable without constants. If $L \in \mathrm{P}_{\mathbb{K}}$, L can be recognized in polynomial time by a constant-free machine.*

Proof. Let M be a machine recognizing L in polynomial time, and $F_n(x)$ a constant-free formula defining $L \cap \mathbb{K}^n$. Using $F_1, F_2, \ldots, F_n$, one can construct a statement G_n expressing that there exist constants $\alpha_1, \ldots, \alpha_p$ which, when plugged in M, can be used to recognize L for inputs of size 1 through n. Let $L' \subseteq \mathbb{C}^\infty$ be the language defined by the formulas $(F_n)_{n \in \mathbb{N}}$ interpreted over $\mathbb{C}$. By transfer, G_n is also true when interpreted over $\mathbb{C}$. This means that for each n, there exist constants $\alpha_1, \ldots, \alpha_p$ which, when plugged in M, can be used to recognize L' for inputs of size 1 through n. In fact, by ω-saturation of $\mathbb{C}$ there exists a vector of constants which works for any input size. Hence $L' \in \mathrm{P}_{\mathbb{C}}$. By Theorem 9, L' can be recognized in polynomial time by a constant-free machine M'. By transfer, M' also recognizes L in polynomial time for inputs in $\mathbb{K}^\infty$. $\square$

7.2 Positive Characteristic

In this section $\mathbb{K}$ can be any algebraically closed field of characteristic $q > 0$.

Lemma 7 *Let $\mathbb{K}$ be an algebraically closed field of characteristic $q > 0$ and p a fixed integer. The following problem can be solved by a polynomial-size constant-free circuit family: given a straight-line program L (with parameters in $\mathbb{K}$) computing a polynomial $P_L \in \mathbb{K}[X_1, \ldots, X_p]$, determine whether $P_L \equiv 0$.*

Proof. Take U to be the set of all roots of irreducible polynomials in $F_q[X]$ of degree m. In order to apply Theorem 7, we need to have $|U| \geq 2v(d+1)^2$. By Lemma 3, it is sufficient to have $q^m - 2q^{m/2} \geq 2mv(d+1)^2$. This gives a polynomial bound on m since $L \in W(2^v, p, v)$. Let $\alpha_1, \ldots, \alpha_s$ be the correct test sequence whose existence is guaranteed by Theorem 7; let α_{ij} $(j = 1, \ldots, p)$ be the components of α_i and P_{ij} the corresponding irreducible polynomials (such that $P_{ij}(\alpha_{ij}) = 0$). We claim that $P_L \equiv 0$ if and only if the following assertions

$$\forall y \in \mathbb{K}^p, P_{i1}(y_1) = 0 \wedge \ldots \wedge P_{ip}(y_p) = 0 \Rightarrow P_L(y_1, \ldots, y_p) = 0 \qquad (4)$$

hold for $i = 1, \ldots, s$. The "only if" part is clear. Conversely, if the s assertions hold then $P_L(\alpha_i) = 0$ for $i = 1, \ldots, s$. This implies $P_L \equiv 0$ by definition of a correct test sequence.

For each i, let us execute L on input $y_1, \ldots, y_p$ by computing modulo $P_{i1}, \ldots, P_{ip}$. We obtain in polynomial time a polynomial Q_i such that $Q_i(y_1, \ldots, y_p) = P_L(y_1, \ldots, y_p)$ for any y such that $P_{i1}(y_1) = 0, \ldots, P_{ip}(y_p) = 0$. The degree of Q_i in each of the variables $y_1, \ldots, y_p$ is less than m. Since the number of variables (p) is constant, by Theorem 1 one can decide in polynomial time whether (4) holds (note that we have used a similar argument in the proof of Theorem 2). $\Box$

It is convenient to work first with $\mathbb{K} = \mathbb{F}_q$, an ω-saturated elementary extension of $\overline{F_q}$. The following result is useful in the proof of Theorem 10.

Lemma 8 *For any $x \in \mathbb{F}_q^n$, there exists $\alpha \in \mathbb{F}_q^p$ such that $\alpha_1, \ldots, \alpha_p$ are algebraically independent over $F_q[x_1, \ldots, x_n]$.*

Proof. Let $(Q_i)_{i \in \mathbb{N}}$ be an enumeration of the non-zero polynomials in $F_q[x_1, \ldots, x_n][X_1, \ldots, X_p]$. For any finite k there exists α such that $Q_i(\alpha) \neq 0$ for $i = 1, \ldots, k$ since the polynomial $\prod_{i=1}^k Q_i$ is not identically 0. The result follows by ω-saturation. $\Box$

Theorem 10 *Let $L \subseteq \mathbb{F}_q^\infty$ be a problem which is definable without constants. If $L \in \mathbb{P}_{\mathbb{F}_q}$, L can be recognized by a polynomial size, constant-free circuit family.*

Proof. As in Theorem 4 or Theorem 9, we can assume that the constants $\alpha_1, \ldots, \alpha_p$ of a circuit family $(C_n)_{n \in \mathbb{N}}$ recognizing L are algebraically independent.

As in Theorem 9, C_n can be viewed as computing over $\mathbb{F}_q[X_1, \ldots, X_p]$. This can be justified exactly as in the proof of that theorem. In particular, given an input $x \in \mathbb{F}_q^n$, the existence of constants $\alpha_1, \ldots, \alpha_p$ which are algebraically independent over $F_q[x_1, \ldots, x_n]$ is guaranteed by Lemma 8. The tests "$P_i \stackrel{?}{=} 0$" can be performed by polynomial-size constant-free circuits according to Lemma 7. □

Corollary 3 *Let $\mathbb{K}$ be an algebraically closed field of characteristic $q > 0$ and $L \subseteq \mathbb{K}^\infty$ a problem which is definable without constants. If $L \in \mathrm{P}_\mathbb{K}$, L can be recognized by a polynomial size, constant free circuit family.*

Proof. Identical to the proof of Corollary 2 (with $\mathbb{C}$ replaced by $\mathbb{F}_q$) since the uniformity hypothesis does not play any role in the proof of that result. □

Acknowledgment

I am grateful to Olivier Chapuis and Bruno Poizat for introducing me to model-theoretic techniques.

References

[1] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer Verlag, to appear.

[2] L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic settings for the problem "P≠NP?". To appear in *Proc. 25th AMS-SIAM Summer Seminar in Applied Mathematics*, LAM series of the AMS, 1996.

[3] 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.

[4] F. Cucker, M. Karpinski, P. Koiran, T. Lickteig, and K. Werther. On real Turing machines that toss coins. In *Proc. 27th ACM Symposium on Theory of Computing*, pages 335–342, 1995.

[5] 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.

[6] M. Giusti, J. Heintz, and J. Sabia. On the efficiency of effective Nullstellensätze. *Computational Complexity*, 3:56–95, 1993.

[7] J. B. Goode. Accessible telephone directories. *Journal of Symbolic Logic*, 59(1), 1994.

[8] J. Heintz and C.-P. Schnorr. Testing polynomials which are easy to compute. In *Logic and Algorithmic (an International Symposium held in honour of Ernst Specker)*, pages 237–254. Monographie n^o 30 de L'Enseignement Mathématique, 1982. Preliminary version in *Proc. 12th ACM Symposium on Theory of Computing*, pages 262-272, 1980.

[9] D. E. Knuth. *The Art of Computer Programming.* Addison-Wesley, 1981. volume 2, second edition.

[10] A. Macintyre. On ω_1-categorical theories of fields. *Fund. Math.*, 71:1–25, 1971.

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

[12] K. Meer and C. Michaux. A survey on real structural complexity. preprint, 1995.

[13] M. Mignotte. *Mathématiques pour le Calcul Formel.* Presses Universitaires de France, 1989.

[14] B. Poizat. *Cours de Théorie des Modèles.* Nur Al-Mantiq Wal-Ma'rifah, 1985.

[15] B. Poizat. *Les Petits Cailloux.* Aléas, 1995.

[16] E. D. Sontag. Shattering all sets of k points in "general position" requires $k/2$ parameters. Technical Report NC-TR-96-042, NeuroCOLT project (http://www.dcs.rhbnc.ac.uk/neurocolt.html), 1996.