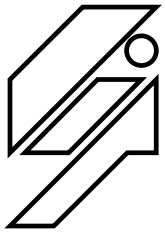
Elimination of parameters in the polynomial hierarchy

Pascal Koiran



Laboratoire de l'Informatique du Parallélisme

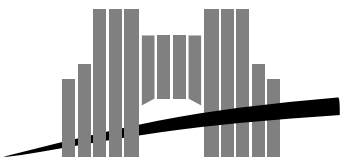
Ecole Normale Supérieure de Lyon
Unité de recherche associée au CNRS n°1398

Elimination of Parameters in the Polynomial Hierarchy

Pascal Koiran

March 1998

Research Report N^{o} 98-15



Ecole Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : (+33) (0)4.72.72.80.00 Télécopieur : (+33) (0)4.72.72.80.80
Adresse électronique : lip@lip.ens−lyon.fr

Elimination of Parameters in the Polynomial Hierarchy

Pascal Koiran

March 1998

Abstract

Blum, Cucker, Shub and Smale have shown that the problem "P = NP ?" has the same answer in all algebraically closed fields of characteristic 0. We generalize this result to the polynomial hierarchy: if it collapses over an algebraically closed field of characteristic 0, then it must collapse at the same level over all algebraically closed fields of characteristic 0. The main ingredient of their proof was a theorem on the elimination of parameters, which we also extend to the polynomial hierarchy. Similar but somewhat weaker results hold in positive characteristic.

The present paper updates a report (LIP Research Report 97-37) with the same title, and in particular includes new results on interactive protocols and boolean parts.

Keywords: elimination of parameters, polynomial hierarchy, Blum-Shub-Smale model.

Résumé

Blum, Cucker, Shub et Smale ont montré que la réponse au problème "P = NP ?" est la même dans tous les corps algébriquement clos de caractéristique 0. Nous généralisons ce résultat à la hiérarchie polynomiale: si elle s'effondre pour un corps algébriquement clos de caractéristique 0, alors elle s'effondre au même niveau pour tous les corps algébriquement clos de caractéristique 0. L'ingrédient principal de leur démonstration est un théorème d'élimination des paramètres, que nous étendons également à la hiérarchie polynomiale. Des résultats similaires mais un peu plus faibles s'appliquent en caractéristique positive.

Cet article met à jour un rapport précédent (rapport de recherche LIP 97-37) portant le même titre, et contient notamment des résultats nouveaux sur les preuves interactives et les parties booléennes.

Mots-clés: élimination des paramètres, hiérarchie polynomiale, modèle de Blum-Shub-Smale.

Elimination of Parameters in the Polynomial Hierarchy

Pascal Koiran
Pascal.Koiran@ens-lyon.fr

March 4, 1998

Abstract

Blum, Cucker, Shub and Smale have shown that the "P = NP ?" problem has the same answer in all algebraically closed fields of characteristic 0. We generalize this result to the polynomial hierarchy: if it collapses over an algebraically closed field of characteristic 0, then it must collapse at the same level over all algebraically closed fields of characteristic 0. The main ingredient of their proof was a theorem on the elimination of parameters, which we also extend to the polynomial hierarchy. Similar but somewhat weaker results hold in positive characteristic.

The present paper updates a report (LIP Research Report 97-37) with the same title, and in particular includes new results on interactive protocols and boolean parts.

Keywords: elimination of parameters, polynomial hierarchy, Blum-Shub-Smale model.

1 Introduction

Blum, Cucker, Shub and Smale [3, 4] have shown that the answer to the question "P=NP ?" is the same in all algebraically closed fields of characteristic 0. This theorem is based on an elimination of parameters: if $K \subseteq \mathbb{K}$ are two algebraically closed fields of characteristic 0, the restriction to K of a problem which is P in $\mathbb{K}$ (possibly with the help of parameters from $\mathbb{K}$) is P in K. In this paper we prove the corresponding theorems for the polynomial hierarchy. Thus, if the hierarchy collapses over an algebraically closed field of characteristic 0, it collapses at the same level over all algebraically closed fields of characteristic 0. We have similar but weaker results in positive characteristic. For instance, we can only show that the collapse of the hierarchy over $\mathbb{K}$ at level k implies its collapse at level $k+1$ over K. It may be possible to avoid losing one level by moving to non-uniform complexity classes, see [13] for such results. Let us also mention that for an

arbitrary structure, one never has to lose more than three levels in the downward transfer for P = NP ([6], Proposition 3.12).

As in these two papers, our methods have a method-theoretic flavor. In particular, we use effective quantifier elimination bounds in characteristic 0. It is not clear whether the present results can be obtained with the number-theoretic techniques of [3, 4].

The rest of this paper is organized as follows. In section 2 we recall some more or less standard material on definable sets and on the polynomial hierarchy. Section 3 is devoted mostly to the elimination of algebraic parameters (in arbitrary characteristic). From this we obtain the transfer theorem in characteristic 0 at the end of that section. As in [3, 4] this theorem follows from the elimination of parameters, but one can give a fairly simple and direct proof sooner. We have found it useful to use the "generic quantifier" $\exists^*$ throughout the paper. It is introduced in section 2, but a systematic investigation of its properties is postponed until section 4. Finally we eliminate parameters in section 5. That section also includes an application to boolean parts, the transfer theorem in positive characteristic, and a study of interactive protocols (at the MA and AM levels) in algebraically closed fields. A study of interactive protocols over the reals (at the higher IP level) has been undertaken recently in [10].

2 Background

2.1 Formulas and the Sets they Define

In this paper we work in the first order theory of an algebraically closed field $\mathbb{K}$. Unless stated otherwise, p denotes the characteristic of $\mathbb{K}$, and F_p its ground field: $F_0 = \mathbb{Q}$ and $F_p = \mathbb{Z}/p\mathbb{Z}$ for $p > 0$. The set defined by a formula $F(x)$ where the free variable lives in $\mathbb{K}^n$ is the set of $u \in \mathbb{K}^n$ such that $\mathbb{K} \models F(u)$. Definable sets are also called *constructible*, or *quasi-algebraic*.

A basic quasi-algebraic set of $\mathbb{K}^m$ is defined by a system of polynomial equalities and inequalities of the form

$$P_1(x) = 0, \ldots, P_k(x) = 0, Q_1(x) \neq 0, \ldots, Q_l(x) \neq 0$$

where $P_1, \ldots, P_k, Q_1, \ldots, Q_l$ are in $\mathbb{K}[X_1, \ldots, X_m]$. By quantifier elimination, every definable set is a finite union of basic quasi-algebraic sets. The following result from [8] gives an effective version of quantifier elimination.

Theorem 2.1 *Let $\mathbb{K}$ be an algebraically closed field and F a prenex formula in the first-order theory of $\mathbb{K}$. Let k be the number of quantifier blocks, m the total number of variables, and σ the total degree of F, defined as $\sigma = 2 + \sum_i \deg F_i$ where the F_i's are the polynomials occurring in F. F is equivalent to a quantifier-free formula G in which all polynomials have degree at most*

$$2^{m^{O(k)}(\log \sigma)^{O(1)}}.$$

The number of polynomials occurring in G is $O(\sigma^{m^{O(k)}})$.

Moreover, when $\mathbb{K}$ is of characteristic 0 and F is a formula in which all parameters are integers of bit-size at most L, the parameters in G are integers of bit size at most $L.2^{m^{O(k)}(\log\sigma)^{O(1)}}$.

In the remainder of section 2.1 we assume that $\mathbb{K}$ is of characteristic 0.

Let $F(x)$ be a first-order formula in the theory of $\mathbb{K}$ where the free variable x lives in $\mathbb{K}^n$. If the set of $w \in \mathbb{K}^n$ such that $\mathbb{K} \models F(w)$ is dense in $\mathbb{K}^n$ we say that $\mathbb{K} \models \exists^* x\ F(x)$ (more on this "generic quantifier" in section 4). Let $T(F)$ (for "test set") be the set of $w \in \mathbb{K}^n$ such that $\mathbb{K} \models F(w)$ iff $\mathbb{K} \models \exists^* x\ F(x)$.

Proposition 2.2 *Let $F(x)$ be a quantifier-free first-order formula where $x \in \mathbb{K}^n$. Assume that the polynomials in F are of degree at most D, with integer coefficients bounded by M in absolute value. Any point $\alpha = (\alpha_1, \ldots, \alpha_n)$ satisfying $\alpha_1 \geq M+1$ and $\alpha_j \geq 1 + M(D+1)^{j-1}\alpha_{j-1}^D$ for $j \geq 2$ is in $T(F)$.*

Proof. Replacing F by $\neg F$ if necessary, we assume that $\mathbb{K} \models \exists^* x\ F(x)$.

The subset of $\mathbb{K}^n$ defined by F is a finite union of basic quasi-algebraic sets (obtained by putting F in disjunctive normal form), and one of them must be dense. Such a set S is of the form $P_1(x) \neq 0, \ldots, P_m(x) \neq 0$ where the P_i's are non-zero polynomials of degree at most D, with integer coefficients bounded by M in absolute value. Then the α defined in the statement of the theorem satisfies $P_i(\alpha) \neq 0$ for any $i = 1, \ldots, m$ (this is not hard to prove, see e.g. [13] and its erratum). This implies $\alpha \in S$, hence $F(\alpha)$ holds. $\square$

Note that the sequence in this lemma can be constructed in a polynomial number of arithmetic operations (more precisely in $O(\log\log M + n \log D)$ operations starting from the integer 1). Nonetheless the components of α are of bit size exponential in n. The next result shows (non-constructively) that there exist integer points of polynomial size in $T(F)$.

Proposition 2.3 *Let $F(x)$ be a quantifier-free first-order formula where $x \in \mathbb{K}^n$. Let s be the number of atomic predicates in F and D an upper bound on their degrees. There exists a point in $T(F)$ whose coordinates are non-negative integers bounded by sDn.*

Proof. We may assume again that $\mathbb{K} \models \exists^* x\ F(x)$. As in the proof of Proposition 2.2, $T(F)$ contains a set of the form $P_1(x) \neq 0, \ldots, P_m(x) \neq 0$ where $m \leq s$ and the P_i's are non-zero polynomials of degree at most D. Let $P = \prod_{i=1}^m P_i$. By Schwarz's Lemma [18], there exists α such that $P(\alpha) \neq 0$ and $\alpha_1, \ldots, \alpha_n$ are integers in $\{0, 1, \ldots, sDn\}$. $\square$

Note that the parameters in F may be arbitrary elements from $\mathbb{K}$. One can apply these two propositions to quantified formulas by eliminating quantifiers first.

Corollary 2.4 *Let F a prenex formula in the first-order theory of $\mathbb{K}$. Let σ be its total degree, k be the number of quantifier blocks, and m the total number of variables. There exists a point in $T(F)$ with integer coordinates of bit size $m^{O(k)}(\log\sigma)^{O(1)}$. Moreover, if the parameters in F are integers of bit size at most L, one can construct in $O(\log L) + m^{O(k)}\sigma^{O(1)}$ arithmetic operations an integer point in $T(F)$. This point depends only on L, m and σ.*

Proof. Immediate from Proposition 2.2, Proposition 2.3 and Theorem 2.1. □

2.2 The Polynomial Hierarchy

Here we want to recall the definition and basic properties of the polynomial hierarchy. We will work over algebraically closed fields since this is the example we have in mind for this paper, but everything holds true in much greater generality (see [17] and [6], in particular sections 2 and 3). For an introduction to the Blum-Shub-Smale model of computation, see [4] or [17].

For any $k \geq 1$, a problem $A \subseteq \mathbb{K}^\infty$ is in $\Sigma^k_{\mathbb{K}}$ if there exists a problem $B \in \mathrm{P}_{\mathbb{K}}$ such that for each $n > 0$, $A \cap \mathbb{K}^n$ is defined by the formula

$$Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} \langle x, y_1, \ldots, y_k \rangle \in B$$

where the quantifiers alternate, starting with $Q_1 = \exists$. If $Q_1 = \forall$ instead, $A \in \Pi^k_{\mathbb{K}}$. Of course the polynomial hierarchy is the union of the $\Sigma^k_{\mathbb{K}}$ for $k \geq 1$. By convention one can set $\Sigma^0_{\mathbb{K}} = \Pi^0_{\mathbb{K}} = \mathrm{P}_{\mathbb{K}}$. In the notations Σ^k and Π^k, we always assume implicitly that $k \geq 1$ unless otherwise stated.

We recall that the polynomial hierarchy is said to collapse at level k if any of these three equivalent properties holds: (i) $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$; (ii) $\Sigma^k_{\mathbb{K}} = \Sigma^{k+1}_{\mathbb{K}}$; (iii) $\Pi^k_{\mathbb{K}} = \Pi^{k+1}_{\mathbb{K}}$. We also recall that the decision problem $D\Sigma^k_{\mathbb{K}}$ for Σ^k formulas is $\Sigma^k_{\mathbb{K}}$-complete (for polynomial-time reductions), and that the decision problem $D\Pi^k_{\mathbb{K}}$ for Π^k formulas is $\Pi^k_{\mathbb{K}}$-complete. Therefore $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$ iff $D\Pi^k_{\mathbb{K}} \in \Sigma^k_{\mathbb{K}}$. Moreover, $D\Pi^k_{\mathbb{K}}$ and $D\Sigma^k_{\mathbb{K}}$ are defined by the same parameter-free formulas in any algebraically closed field. From this an upward transfer theorem follows easily.

Proposition 2.5 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields. If $\Sigma^k_K = \Pi^k_K$ then $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$.*

Proof Sketch. By hypothesis $D\Pi^k_K \in \Sigma^k_K$, and the corresponding algorithm will also solve $D\Pi^k_{\mathbb{K}}$ since these two problems are defined by the same formulas. This implies $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$ (see [6], Lemma 3.5 for more details). □

There is a partial converse.

Proposition 2.6 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields. If $D\Pi^k_{\mathbb{K}}$ is in $\Sigma^k_{\mathbb{K}}$ and the corresponding algorithm uses only parameters from K then $\Sigma^k_K = \Pi^k_K$.*

Proof Sketch. As in the proof of Proposition 2.5, the $\Sigma^k_{\mathbb{K}}$ algorithm for $D\Pi^k_{\mathbb{K}}$ will also solve $D\Pi^k_K$. Hence $D\Pi^k_K \in \Sigma^k_K$, and $\Sigma^k_K = \Pi^k_K$. $\square$

In the proof of the transfer theorem (Theorem 3.4) we will show that this proposition can be applied if the polynomial hierarchy collapses in characteristic 0. More precisely, if $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$ then $D\Pi^k_{\mathbb{K}}$ can be solved by a *parameter-free* $\Sigma^k_{\mathbb{K}}$ algorithm.

3 A Transfer Theorem in Characteristic 0

The main goal of this section is to establish the transfer theorem for the collapse of the polynomial hierarchy. First, we show that algebraic parameters can be eliminated. This will also be useful for the proof of the general elimination result in section 5.

Lemma 3.1 *Let $\mathbb{K}$ be an algebraically closed field of any characteristic, and K a subfield of $\mathbb{K}$. Let A be a problem in $\Sigma^k_{\mathbb{K}}$ with parameters in an algebraic extension $K[\alpha]$ of K (here $\alpha \in \mathbb{K}$). There exists a problem A' in $\Sigma^k_{\mathbb{K}}$ with parameters in K such that A and A' have the same restriction to K. Moreover, $A = A'$ if A is definable with parameters in K.*

Proof. There is a problem B in $\mathrm{P}_{\mathbb{K}}$ with parameters in K such that for $x \in \mathbb{K}^n$, x is in A iff

$$Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} \langle x, y_1, \ldots, y_k, \alpha \rangle \in B.$$

Let m be the minimal polynomial of α over K. We define A' as follows: if $Q_k = \exists$, $x \in \mathbb{K}^n \cap A'$ iff

$$Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} Q_k \beta \in \mathbb{K}[m(\beta) = 0 \wedge \langle x, y_1, \ldots, y_k, \beta \rangle \in B].$$

If $Q_k = \forall$, $x \in \mathbb{K}^n \cap A'$ iff

$$Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} Q_k \beta \in \mathbb{K}[m(\beta) = 0 \Rightarrow \langle x, y_1, \ldots, y_k, \beta \rangle \in B].$$

It is clear that A' is in $\Sigma^k_{\mathbb{K}}$ with parameters in K. We claim that A and A' have the same restriction to K, and that $A = A'$ if A is definable with parameters in K.

For the first part of the claim, fix any $x \in K^n$, and consider the set $G_x \subseteq \mathbb{K}$ of parameters that can "play the role" of α on input x. That is, $\beta \in G_x$ iff:

$$x \in A \Leftrightarrow Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} \langle x, y_1, \ldots, y_k, \beta \rangle \in B.$$

Note that in this formula, "$x \in A$" is just a boolean value since x is fixed. Since $\alpha \in G_x$ by definition, its conjugates (the other roots of m) are also in G_x. Indeed, by quantifier elimination G_x is defined by a quantifier-free formula $F_x(\beta)$ with

parameters in K. An atomic predicate $P(\beta) = 0$ in that formula is satisfied by α iff P is a multiple of m, that is, iff it is satisfied by all the roots of m. This property of G_x implies the first part of the claim.

The proof of the second part is very similar. Let F_n be a formula with parameters in K defining $A \cap \mathbb{K}^n$. Consider the set $G \subseteq \mathbb{K}$ of parameters that can "play the role" of α for any input $x \in \mathbb{K}^n$. That is, $\beta \in G$ iff:

$$\forall x \in \mathbb{K}^n \; [F_n(x) \Leftrightarrow Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} \langle x, y_1, \ldots, y_k, \beta \rangle \in B].$$

For the same reason as above, the roots of m are all in G and this implies $A = A'$. □

Theorem 3.2 *Let $\mathbb{K}$ be an algebraically closed field of any characteristic, and K a subfield of $\mathbb{K}$. Let A be a problem in $\Sigma^k_{\mathbb{K}}$ with parameters in an algebraic extension $K[\alpha_1, \ldots, \alpha_p]$ of K. There exists a problem A' in $\Sigma^k_{\mathbb{K}}$ with parameters in K such that A and A' have the same restriction to K. Moreover, $A = A'$ if A is definable with parameters in K.*

Proof. By induction on k. The case $p = 1$ is Lemma 3.1. To go from p to $p + 1$, write $K[\alpha_1, \ldots, \alpha_{p+1}]$ as $K[\alpha_1, \ldots, \alpha_p][\alpha_{p+1}]$, apply the lemma to get rid of α_{p+1}, and then the induction hypothesis to get rid of $\alpha_1, \ldots, \alpha_p$. □

In particular, if K is algebraically closed the restriction of A is in Σ^k_K since $\mathbb{K}$ is an elementary extension of K in this case. Note that if K is of characteristic 0, we can assume that $p = 1$ by the primitive element theorem.

Corollary 3.3 *Let $\mathbb{K}$ be an algebraically closed field of any characteristic, and K a subfield of $\mathbb{K}$. Let A be a problem in $\Sigma^k_{\mathbb{K}}$. There exists an extension $L = K(\beta_1, \ldots, \beta_q)$ with algebraically independent β_i's and a problem A' in $\Sigma^k_{\mathbb{K}}$ with parameters in L such that A and A' have the same restriction to K. Moreover, $A = A'$ if A is definable with parameters in K.*

Proof. A is in $\Sigma^k_{\mathbb{K}}$ with parameters in an algebraic extension

$$K(\beta_1, \ldots, \beta_q)[\alpha_1, \ldots, \alpha_p]$$

of a transcendental extension $K(\beta_1, \ldots, \beta_q)$. Now apply Theorem 3.2 to $K(\beta_1, \ldots, \beta_q)$. □

Here is the main result of section 3. The proof is quite similar to that of Proposition 1 in [13].

Theorem 3.4 *Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. If the polynomial hierarchy over $\mathbb{K}$ collapses, it collapses at the same level over any algebraically closed field of characteristic 0.*

Proof. It suffices to show that $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$ if and only if $\Sigma^k_{\overline{\mathbb{Q}}} = \Pi^k_{\overline{\mathbb{Q}}}$. The "if" part follows from Proposition 2.5.

Assume now that $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$: in this case $D\Pi^k_{\mathbb{K}}$ can be solved by a $\Sigma^k_{\mathbb{K}}$ algorithm using p parameters $\alpha_1, \ldots, \alpha_p$. For each n there is a parameter-free formula F_n which is satisfied by $\beta \in \mathbb{K}^p$ iff β can be used by this algorithm as a vector of parameters to solve all instances of $D\Pi^k_{\mathbb{K}}$ of size n. Observe that (when put in prenex form) F_n is of polynomial size and has a bounded number of quantifier alternations. Also $\mathbb{K} \models F_n(\alpha)$ by definition.

By Corollary 3.3 (applied with $K = \mathbb{Q}$) we can assume that $\alpha_1, \ldots, \alpha_p$ are algebraically independent. From $\mathbb{K} \models F_n(\alpha)$ it follows that $\mathbb{K} \models \exists^* x\ F_n(x)$ (if this is not clear to you, read the proof of Proposition 4.3). By Corollary 2.4, one can construct in time polynomial in n a vector $\beta \in \mathbb{N}^p$ satisfying F_n. We can then use β to solve $D\Pi^k_{\mathbb{K}}$ with a *parameter-free* $\Sigma^k_{\mathbb{K}}$ algorithm. We conclude that $\Sigma^k_{\overline{\mathbb{Q}}} = \Pi^k_{\overline{\mathbb{Q}}}$ by Proposition 2.6. □

4 The Generic Quantifier

The results of sections 4.1 and 4.2 apply to algebraically closed fields of arbitrary characteristic.

4.1 Definition and Basic Properties

We have already introduced the generic quantifier in section 2: given an algebraically closed field $\mathbb{K}$ (of any characteristic) and a first-order formula $F(v)$ where $v \in \mathbb{K}^q$, $\mathbb{K} \models \exists^* v\ F(v)$ iff the set of v's such that $F(v)$ holds is (Zariski) dense in $\mathbb{K}^q$. This means that there exists a nonzero polynomial p such that $\mathbb{K} \models F(v)$ whenever $p(v) \neq 0$. One could also define a $\forall^*$ quantifier as:

$$\forall^* v\ F(v) \ \equiv\ \neg\exists^* v\ \neg F(v),$$

but this would be redundant since this double negation is equivalent to $\exists^* v\ F(v)$. (Note however that in real-closed fields, one can similarly define two distinct quantifiers $\exists^*$ and $\forall^*$ [15].)

First-order formulas involving this new quantifier will be called "generalized formulas". Ordinary formulas will just be referred to as "formulas", or "first-order formulas". This distinction will be dropped shortly since, as we now show, generalized formulas are equivalent to ordinary formulas.

Proposition 4.1 *Let $F(u_1, \ldots, u_s)$ be a generalized formula in the language $\{0, 1, +, -, \cdot\}$, and $\mathbb{K}$ an algebraically closed field of characteristic $p \geq 0$. There exists an ordinary formula F^* in the same language such that for all $u \in \mathbb{K}^s$, $\mathbb{K} \models F(u)$ if and only if $\mathbb{K} \models F^*(u)$. Moreover, F^* depends only on F.*

Proof. Reasoning by induction on the structure of F, it suffices to consider formulas of the form $F(u) \equiv \exists^* v\ G(u,v)$ where $v \in \mathbb{K}^q$. Moreover, we may assume that G is quantifier-free and in disjunctive normal form. Then $G = C_1 \vee \cdots \vee C_m$ where each C_i is a conjunction of the form

$$p_{i,1}(u,v) = 0 \wedge \cdots \wedge p_{i,m_i}(u,v) = 0 \wedge q_i(u,v) \neq 0.$$

$\exists^* v\ G(u,v)$ is equivalent to $\bigvee_{i=1}^m \exists^* v\ C_i(u,v)$. Given $u \in \mathbb{K}^s$, $\exists^* v\ C_i(u,v)$ holds if as a polynomial in v, $q(u,.)$ is not identically zero and if all the $p_{ij}(u,.)$ are identically zero. This yields the desired ordinary formula. Since G depends only on F (in particular G can be made independent of p), the same is true for F^*. □

As a consequence, we see that elementary equivalence also holds for generalized formulas.

Corollary 4.2 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields, and F a generalized statement (closed formula) with parameters in K. Then $K \models F$ if and only if $\mathbb{K} \models F$.*

Proof. Write $F = G(u)$ where u is the vector of parameters of F, and apply Proposition 4.1 to G. The result then follows from elementary equivalence for ordinary formulas. □

Proposition 4.3 *Let $\mathbb{K}$ be an algebraically closed field and $F(v)$ a first-order formula where the free variable v lives in $\mathbb{K}^q$. Let $K \subseteq \mathbb{K}$ be a field containing the parameters of F. If $\mathbb{K}$ is of transcendence degree at least q over K, the three following properties are equivalent.*

(i) $\mathbb{K} \models \exists^* v\ F(v)$.

(ii) For any $v = (v_1, \ldots, v_q)$ of transcendence degree q over K, $\mathbb{K} \models F(v)$.

(iii) There exists $v = (v_1, \ldots, v_q)$ of transcendence degree q over K such that $\mathbb{K} \models F(v)$.

Proof. As in the proof of Proposition 4.1, we assume that F is in disjunctive normal form: $F \equiv C_1 \vee \cdots \vee C_m$ where each C_i is a conjunction of the form

$$p_{i,1}(v) = 0 \wedge \cdots \wedge p_{i,m_i}(v) = 0 \wedge q_i(v) \neq 0.$$

$\mathbb{K} \models \exists^* v\ F(v)$ if and only if there exists a C_i with q_i not identically zero and all the p_{ij} identically zero. In this case, if v is of of transcendence degree q over K then $q_i(v) \neq 0$ by definition. Therefore (i) implies (ii). The implication (ii) $\Rightarrow$ (iii) is trivial (but uses the assumption on $\mathbb{K}$). To show that (iii) implies (i), we use the disjunctive normal form again. Let $v_1, \ldots, v_q$ be algebraically independent elements such that $\mathbb{K} \models F(v)$. There exists a C_i such that $\mathbb{K} \models C_i(v)$. Again by definition of algebraic independence, this implies that all the p_{ij} are 0 and q_i is not identically 0. Hence $\mathbb{K} \models \exists^* v\ F(v)$. □

As ordinary quantifiers, $\exists^*$ is commutative. The proof of this Fubini-style property is based on Proposition 4.3.

Proposition 4.4 *Let $\mathbb{K}$ be an algebraically closed field and $F(u,v)$ a first-order formula in the theory of $\mathbb{K}$. The three following properties are equivalent.*

(i) $\mathbb{K} \models \exists^*(u,v)\ F(u,v)$.

(ii) $\mathbb{K} \models \exists^* u \exists^* v\ F(u,v)$.

(iii) $\mathbb{K} \models \exists^* v \exists^* u\ F(u,v)$.

Proof. By Corollary 4.2, we may assume without loss of generality that $\mathbb{K}$ is of infinite transcendence degree over F_p. Let K be the extension of F_p generated by the parameters of F. Assume first that (i) holds. Then by Proposition 4.3, there exists a tuple (a,b) with algebraically independent (over K) components such that $\mathbb{K} \models F(a,b)$. Since the components of b are algebraically independent over $K(a)$, it follows again from Proposition 4.3 that $K \models \exists^* v F(a,v)$. Finally, since the components of a are algebraically independent over the parameters of the formula $\exists^* v F(.,v)$ (they are in K) we conclude that (ii) holds. The proof that (i) implies (iii) is similar.

Assume now that (ii) holds. By Proposition 4.3, there exists a tuple a with components that are algebraically independent over K such that $K \models \exists^* v F(a,v)$, and a tuple b with components that are algebraically independent over $K(a)$ such that $K \models F(a,b)$. Since the components of tuple (a,b) are algebraically independent over K, we conclude from Proposition 4.3 that (i) holds. The proof that (iii) implies (i) is similar. □

Of course, in this proof one could also work with a field $\mathbb{K}$ of finite, but "large enough" transcendence degree.

4.2 Efficient Elimination of the Generic Quantifier

We have seen in section 4.1 that generalized formulas can be replaced by ordinary first-order formulas. In this section we will see that this transformation can be made "efficiently".

Theorem 4.5 *Let $\mathbb{K}$ be an algebraically closed field of any characteristic. Let $F(u,v)$ be a first-order formula where $u \in \mathbb{K}^s$ and $v \in \mathbb{K}^q$. The set $W(F)$ of sequences $(v_1, \ldots, v_{2s+1}) \in \mathbb{K}^{q(2s+1)}$ satisfying:*

$$\forall u\ [\exists^* v F(u,v) \Leftrightarrow |\{i;\ F(u,v_i)\}| \geq s+1] \tag{1}$$

is dense in $\mathbb{K}^{q(2s+1)}$.

This means that to decide whether $F(u,v)$ holds for "most" v's, one just has to check whether it holds for a majority of $v_1,\ldots,v_{2s+1}$. Moreover, the same $2s+1$ test points can be used for any choice of u and "most" tuples of $2s+1$ points are good for that purpose.

The proof given below relies on transcendence degree arguments, and was suggested by Bruno Poizat (personal communication). In model theory there is an abstract version of arguments of this kind, see e.g. [16], Chapter 12 (a sequence of algebraically independent elements of $\mathbb{K}$ is an example of an "indiscernible" sequence). It is also possible to use the dimension of definable sets. These two proofs are essentially equivalent, but the first one is much more concise. We begin with a simple lemma.

Lemma 4.6 *Let K be a subfield of $\mathbb{K}$ and $a=(a_1,\ldots,a_k)$ a sequence of elements of $\mathbb{K}$ that are algebraically independent over K. For any $s<k$ and $(v_1,\ldots,v_s)\in\mathbb{K}^s$, there exists a subsequence $(a_{i_j})_{1\leq j\leq k-s}$ whose elements are algebraically independent over the the field $K'=K(v_1,\ldots,v_s)$.*

Proof. Let K'' be the field extension of K' generated by the a_i's: $\mathrm{tr.deg}_{K'}K''\geq k-s$ since $\mathrm{tr.deg}_K K''=\mathrm{tr.deg}_{K'}K''+\mathrm{tr.deg}_K K'$ (this is e.g. the corollary of Theorem 4 in section V.14.3 of [5]), $\mathrm{tr.deg}_K K'\leq s$ and $\mathrm{tr.deg}_K K''\geq k$ by definition of a. Let B be a transcendence base of K'' over K' made up of elements of a. B has at least $k-s$ elements, and they are algebraically independent over K' as needed. □

Proof of Theorem 4.5. Let K be the field extension of F_p generated by the parameters of F. As in the proof of Proposition 4.4, we can assume by Corollary 4.2 that $\mathbb{K}$ has infinite transcendence degree over K. By Proposition 4.3, it suffices to show that if the components of $w\in\mathbb{K}^{q(2s+1)}$ are algebraically independent over K, then $w\in W(F)$. Let $w=(v_1,\ldots,v_{2s+1})$ be such a sequence, and fix any $u\in\mathbb{K}^s$.

Assume for instance that $\exists^* v F(u,v)$ holds: we need to show that $|\{i;\ F(u,v_i)\}|\geq s+1$. By Lemma 4.6, at least $q(2s+1)-s$ among the $q(2s+1)$ components of the v_i's are algebraically independent over $K'=K(v_1,\ldots,v_s)$. This implies that at least $(2s+1)-s=s+1$ of the v_i's have all their components algebraically independent over K'. By Proposition 4.3, $\mathbb{K}\models F(u,v_i)$ for any such v_i.

If $\exists^* v F(u,v)$ does not hold then $\exists^* v\neg F(u,v)$ holds and applying the argument above to $\neg F$ shows that $|\{i;\ \neg F(u,v_i)\}|\geq s+1$. □

The example $F(u,v)\equiv[(v-u_1)(v-u_2)\ldots(v-u_s)\neq 0]$ shows that $2s+1$ cannot be replaced by $2s$ in this theorem. However, for certain formulas one can get away with fewer test points in the following sense.

Theorem 4.7 *Let $F(u,v)$ be a first-order formula such that for any $u \in \mathbb{K}^s$, if $\exists^* v F(u,v)$ does not hold then $F(u,v)$ does not hold for any $v \in \mathbb{K}^q$. The set $G(F)$ of sequences $(v_1,\ldots,v_{s+1}) \in \mathbb{K}^{q(s+1)}$ satisfying:*

$$\forall u \ [\exists^* v F(u,v) \Leftrightarrow |\{i;\ F(u,v_i)\}| \geq 1] \tag{2}$$

is dense in $\mathbb{K}^{q(s+1)}$.

Proof. Let K be as in the proof of Theorem 4.5. We claim that if the components of $w \in \mathbb{K}^{q(s+1)}$ are algebraically independent over K, then $w \in G(F)$. Indeed, it follows again from Lemma 4.6 that for such a w and any $u \in \mathbb{K}^q$, there must exist at least one v_i with components that are algebraically independent over $K(u_1,\ldots,u_q)$. Then $\exists^* v F(u,v)$ implies $F(u,v_i)$. Conversely, if $F(u,v_i)$ holds for some i then by the hypothesis on F, $\exists^* v F(u,v)$ must hold as well. □

The hypothesis in this theorem is satisfied in particular by formulas of the form $F(u,v) \equiv [P(u,v) \neq 0]$, where P is a polynomial. Such formulas have been considered in the study of "correct test sequences" [9] and in the Witness Theorem [3, 4]. The same example shows that the $s+1$ bound cannot be improved in general (there is a similar remark in [9]).

Theorems 4.5 and 4.7 do not provide an explicit construction of a sequence in $W(F)$ or $G(F)$. Here is a completely constructive way of eliminating the generic quantifier.

Theorem 4.8 *For any first-order formula $F(v)$ where $v \in \mathbb{K}^q$, $\mathbb{K} \models \exists^* v\ F(v)$ if and only if $\mathbb{K} \models \exists t_1,\ldots,t_{q+1} \in \mathbb{K}^q\ \forall v \in \mathbb{K}^q \bigvee_{i=1}^{q+1} F(v-t_i)$.*

Proof. Assume first that $\mathbb{K} \models \exists^* v\ F(v)$. Let K be the extension of F_p generated by the parameters of F, and $t_1,\ldots,t_{q+1}$ a sequence with components that are algebraically independent over K. Arguing as in the proof of Theorem 4.7, we see that for any $v \in \mathbb{K}^q$ there exists a t_i whose components are algebraically independent over $K(v_1,\ldots,v_q)$. The components of $v-t_i$ are then algebraically independent over K, and thus $K \models F(v-t_i)$ by Proposition 4.3.

For the converse, let E be the subset of $\mathbb{K}^q$ defined by F and $E+t_i$ the image of E by the translation of vector t_i. If $\bigcup_{i=1}^{q+1}(E+t_i) = \mathbb{K}^q$ then one of the translates of E must be dense in $\mathbb{K}^q$. This implies that E is dense, too. □

The three theorems of section 4.2 are adaptations to the BSS model of classical theorems of complexity theory (BPP $\subseteq$ P/poly, RP $\subseteq$ P/poly and BPP $\subseteq \Sigma^2$). See e.g. [2] for the classical theory and [7, 11] for adaptations of these results to the BSS model of computation over the reals.

4.3 Construction in Characteristic 0

In this subsection we assume that the algebraically closed field $\mathbb{K}$ is of characteristic 0. We will see in Theorem 4.11 that it is possible to construct explicitly a sequence in $W(F)$. Before that, we show that $W(F)$ contains a sequence of points with integer coordinates of polynomial size. The proof given here relies on effective quantifier elimination. In [14] a more precise bound is provided using connected component arguments.

First, note that $W(F)$ is an equivalence class of the equivalence relation $\sim$ on $\mathbb{K}^{q(2s+1)}$ defined by: $v \sim w$ iff

$$\forall u \in \mathbb{K}^s \ [|\{i;\ F(u, v_i)\}| \geq s+1 \Leftrightarrow |\{i;\ F(u, w_i)\}| \geq s+1]. \tag{3}$$

Lemma 4.9 *Let $F(u, v)$ be a quantifier-free formula of total degree σ (with $u \in \mathbb{K}^s$ and $v \in \mathbb{K}^q$). There exists a sequence in $W(F)$ with integer coordinates of bit size $(qs \log \sigma)^{O(1)}$.*

Proof. Fix any $w \in W(F)$. Then $W(F)$ is defined by (3). The total number of variables in this formula is $s + q(2s+1)$, its total degree is upper bounded by $2(2s+1)\sigma$, and it has a single block of quantifiers. By Theorem 4.5, $W(F)$ is dense in $\mathbb{K}^{q(2s+1)}$ and the result follows from Corollary 2.4. □

An explicit construction follows from this non-constructive bound.

Lemma 4.10 *Let $F(u, v)$ be a quantifier-free formula where $u \in \mathbb{K}^s$ and $v \in \mathbb{K}^q$, with integer parameters of bit size at most L. Let σ be its total degree. One can construct in $O(\log L) + (qs \log \sigma)^{O(1)}$ arithmetic operations a sequence $(v_1, \ldots, v_{2s+1}) \in W(F)$ with integer coordinates. Moreover, this sequence depends only on L, q, s and σ.*

Proof. We proceed as in the proof of Lemma 4.9, but instead of an arbitrary point $w \in W(F)$ we use in (3) the point with "small" integer coordinates whose existence is asserted by that lemma. The result then follows again from Corollary 2.4. □

There is another proof of this lemma. Instead of defining $W(F)$ by (3) one can replace the generic quantifier in (1) by the Σ^2 formula provided by Theorem 4.8. One can then apply Corollary 2.4 as in the proof above.

A generalization to quantified formulas follows easily from Lemma 4.10.

Theorem 4.11 *Let $\mathbb{K}$ be an algebraically closed field of characteristic 0 and $F(u, v)$ a prenex formula with k blocks of quantifiers, and integer parameters of bit size at most L. Let σ be its total degree, and m the total number of variables (thus if $u \in \mathbb{K}^s$ and $v \in \mathbb{K}^q$, there are $m - s - q$ quantified variables). One can construct in $O(\log L) + (m \log \sigma)^{O(k)}$ arithmetic operations a sequence $(v_1, \ldots, v_{2s+1}) \in W(F)$ with integer coordinates. Moreover, this sequence depends only on L, m, k and σ.*

Proof. Eliminate quantifiers in F with Theorem 2.1 and then apply Lemma 4.10. □

5 Stability in the Polynomial Hierarchy

The main goal of this section is to prove the following "effective stability" result.

Theorem 5.1 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields of characteristic 0, and A a problem in $\Sigma^k_{\mathbb{K}}$. The restriction of A to K is in Σ^k_K.*

An application to boolean parts is also discussed in section 5.3, and interactive protocols over $\mathbb{C}$ are studied in section 5.2.

5.1 Elimination of Parameters

Proof of Theorem 5.1. By Corollary 3.3, we may assume without loss of generality that A is $\Sigma^k_{\mathbb{K}}$ with parameters $(\beta_1, \ldots, \beta_q, \gamma_1, \ldots, \gamma_r)$ where the β_i are algebraically independent over K, and the γ_i are in K. Our goal is to show that for inputs in K, the β_i's can be simulated by computations in K.

$A \cap \mathbb{K}^n$ is defined by a formula $F_n(x, \beta, \gamma)$ of the form

$$Q_1 y_1 \in \mathbb{K}^{p_1(n)} \cdots Q_k y_k \in \mathbb{K}^{p_k(n)} \langle x, y_1, \ldots, y_k, \beta \rangle \in B$$

where $\beta = (\beta_1, \ldots, \beta_q)$ and B is $\mathrm{P}_{\mathbb{K}}$ with parameters γ. By Proposition 4.3, this is equivalent for $x \in K^n$ to

$$\exists^* z \in \mathbb{K}^q \ F_n(x, z, \gamma) \tag{4}$$

since the β_i are algebraically independent. Hence we are led to consider the problem $A' \subseteq \mathbb{K}^n$ defined by (4). As we have just seen, A and A' have the same restriction to K. Let $w = (v_1, \ldots, v_{2(n+r)+1}) \in \mathbb{K}^{q(2(n+r)+1)}$ be a sequence in $W(F_n)$. By definition of $W(F_n)$, an input $x \in \mathbb{K}^n$ is in A' iff $|\{i;\ F_n(x, v_i, \gamma)\}| \geq n + r + 1$, or in other words:

$$\exists i_1, \ldots, i_{n+r+1} \bigwedge_{j=1}^{n+r+1} F_n(x, v_{i_j}, \gamma). \tag{5}$$

Each term in the conjunction is a Σ^k formula. One can put (5) in Σ^k (prenex) form by interleaving the quantifiers blocks coming from each term. Since $B \in \mathrm{P}_{\mathbb{K}}$ and the v_i can be constructed in polynomial time by Theorem 4.11, this shows that A' is in $\Sigma^k_{\mathbb{K}}$ with parameter $\gamma \in K^r$. By elementary equivalence, we conclude that the restriction of A' to K is in Σ^k_K (with the same parameter γ). □

This proof also applies with a minor modification to $\mathrm{P}_{\mathbb{K}} = \Sigma^0_{\mathbb{K}}$. In this case we do not need the existential formula (5). Instead, one can decide directly in polynomial time whether $|\{i;\ F_n(x, v_i, \gamma)\}| \geq n+r+1$ since F_n is polynomial-time decidable. Note the following consequence of Theorem 5.1.

Corollary 5.2 *Let $\mathbb{K}$ be an algebraically closed field of characteristic 0, and K a subfield of $\mathbb{K}$. Let A be a problem in $\Sigma^k_{\mathbb{K}}$. If A is definable with parameters in K, A is in $\Sigma^k_{\mathbb{K}}$ with parameters in K.*

Proof. Let $\overline{K} \subseteq \mathbb{K}$ be the algebraic closure of K. Since the extension $\overline{K} \leq \mathbb{K}$ is elementary, it follows from Proposition 3.17 of [6] and Theorem 5.1 that A is $\Sigma^k_{\mathbb{K}}$ with parameters in $\overline{K}$. Hence by Theorem 3.2, A is in fact $\Sigma^k_{\mathbb{K}}$ with parameters in K. $\square$

Theorem 5.3 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields of any characteristic, and $k \geq 1$ an integer. The restriction to A of a problem in $\Sigma^k_{\mathbb{K}}$ is in Π^{k+1}_K and the restriction of a problem in $\Pi^k_{\mathbb{K}}$ is in Σ^{k+1}_K.*

Proof. By complementation it suffices to prove the first part of the theorem. We keep the same notations as in the proof of Theorem 5.1. By Theorem 4.8, $A' \cap \mathbb{K}^n$ is defined by the formula:

$$\exists t_1, \ldots, t_{q+1} \in \mathbb{K}^q \ \forall z \in \mathbb{K}^q \ \bigvee_{i=1}^{q+1} F_n(x, z - t_i, \gamma). \tag{6}$$

Proceeding as in the proof of Theorem 5.1, one can put the disjunction above in Π^k form. This gives a (polynomial size) Σ^{k+1} form for (6), and the parameter γ is in K^r. Hence the restriction of A' to K is in Σ^{k+1}_K. $\square$

A transfer theorem in arbitrary characteristic follows.

Theorem 5.4 *Let $K \subseteq \mathbb{K}$ be two algebraically closed fields of any characteristic, and $k \geq 1$ an integer. If $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$ then $\Sigma^{k+1}_K = \Pi^{k+1}_K$.*

Proof. If $\Sigma^k_{\mathbb{K}} = \Pi^k_{\mathbb{K}}$ then $\Sigma^k_{\mathbb{K}} = \Sigma^{k+1}_{\mathbb{K}}$, hence the $\Sigma^{k+1}_{\mathbb{K}}$-complete problem $D\Sigma^{k+1}_{\mathbb{K}}$ is in $\Sigma^k_{\mathbb{K}}$. By Theorem 5.3, the restriction of $D\Sigma^{k+1}_{\mathbb{K}}$ to K is in Π^{k+1}_K. This restriction is nothing but $D\Sigma^{k+1}_K$, so $D\Sigma^{k+1}_K \in \Pi^{k+1}_K$. This implies $\Sigma^{k+1}_K = \Pi^{k+1}_K$. $\square$

5.2 Interactive Protocols

In this section we introduce complex version of the classical complexity classes AM ("Arthur-Merlin") and MA ("Merlin-Arthur"). Here we just recall that these two classes are randomized versions of NP located between NP and Π^2. See [1] for more details.

Let $\mathbb{K}$ be an algebraically closed field. A problem $A \subseteq \mathbb{K}^\infty$ is said to be in $\mathrm{MA}_\mathbb{K}$ if there exist two polynomials p and q and a problem $B \in \mathrm{P}_\mathbb{K}$ such that for each $n > 0$, $A \cap \mathbb{K}^n$ is defined by the formula

$$\exists y \in \mathbb{K}^{p(n)} \exists^* z \in \mathbb{K}^{q(n)} \langle x, y, z \rangle \in B. \tag{7}$$

The complexity class $\mathrm{AM}_\mathbb{K}$ is defined by a similar condition: for $x \in \mathbb{K}^n$,

$$x \in A \Leftrightarrow \exists^* z \in \mathbb{K}^{q(n)} \exists y \in \mathbb{K}^{p(n)} \langle x, y, z \rangle \in B.$$

Theorem 5.5 *For any algebraically closed field* $\mathrm{MA}_\mathbb{K}$ *is included in* $\mathrm{AM}_\mathbb{K}$*, and moreover* $\mathrm{MA}_\mathbb{K} = \mathrm{AM}_\mathbb{K} = \mathrm{NP}_\mathbb{K}$ *in characteristic zero.*

Proof. Let A be a problem in $\mathrm{MA}_\mathbb{K}$ and let $B \in \mathrm{P}_\mathbb{K}$ be the "corresponding problem." Given an input $x \in \mathbb{K}^n$, let $F_x(y, z)$ be the formula defining $B \cap \{x\} \times \mathbb{K}^{p(n)+q(n)}$.

By Theorem 4.5, the set $W(F_x)$ of sequences $(z_1, \ldots, z_{2p(n)+1}) \in \mathbb{K}^{q(n).(2p(n)+1)}$ satisfying:

$$\forall y \ [\exists^* z \ F_x(y, z) \Leftrightarrow |\{i; \ F_x(y, z_i)\}| \geq p(n) + 1]$$

is dense in $\mathbb{K}^{q(n).(2p(n)+1)}$. Hence condition (7) is equivalent to

$$\exists^* z_1, \ldots, z_{2p(n)+1} \ \exists y \ |\{i; \ F_x(y, z_i)\}| \geq p(n) + 1.$$

This shows that $A \in \mathrm{AM}_\mathbb{K}$.

Assume now that $\mathbb{K}$ is of characteristic 0, and take a problem A in $\mathrm{AM}_\mathbb{K}$. The restriction of A to $\mathbb{K}^n$ is defined by formula (4) with $q = q(n)$, γ the tuple of parameters used by B, and F_n an existential formula of polynomial size. We have seen in the proof of Theorem 5.1 that this condition can be verified by a $\mathrm{NP}_\mathbb{K}$ algorithm (and more generally by a $\Sigma^k_\mathbb{K}$ algorithm if the F_n's define a $\Sigma^k_\mathbb{K}$ problem). Hence $A \in \mathrm{NP}_\mathbb{K}$. (Note: q is a constant in Theorem 5.1. However, it follows from Theorem 4.11 that the witness points v_i can still be constructed in polynomial time even when $q = q(n)$.) This completes the proof of the theorem since the inclusion $\mathrm{NP}_\mathbb{K} \subseteq \mathrm{MA}_\mathbb{K}$ obviously holds true (in any characteristic). □

As in the classical case, it is possible to prove by induction on the number of rounds that interactive protocols with a constant number of rounds are not more powerful than AM protocols.

In positive characteristic the inclusion $\mathrm{NP}_\mathbb{K} \subset \mathrm{AM}_\mathbb{K}$ is presumably strict, but it may be possible to prove as in the classical setting that $\mathrm{AM}_\mathbb{K} \subseteq \mathrm{NP}_\mathbb{K}/\mathrm{polybool}$,

where "polybool" denotes a boolean advice of polynomial size (in characteristic 0, this result can be established without Corollary 2.4 using Lemma 4.9). Note also that $\mathrm{AM}_{\mathbb{K}} \subseteq \Pi^2_{\mathbb{K}}$ follows from Theorem 4.8 by complementation.

One interpretation of Theorem 5.5 is that interactive protocols are not as interesting in characteristic 0 as in the classical setting since they do not increase the power of nondeterminism. More optimistically, we prefer to point out that this theorem makes it possible to convert automatically an MA or an AM algorithm into an NP algorithm. In particular, this may yield an "optimal" algorithm if the problem under consideration is $\mathrm{NP}_{\mathbb{K}}$-hard. See [14] for an example of a conversion of an AM algorithm into an NP algorithm. Also the $\mathrm{NP}_{\mathbb{R}}$-completeness result of [15] can be seen as a conversion of an MA algorithm over the reals into an NP algorithm.

5.3 Boolean Parts

Let K be an algebraically closed field of characteristic 0. We recall that the boolean part $\mathrm{BP}(\mathrm{NP}_K)$ of NP_K is the set of boolean problems (subsets of $\{0,1\}^\infty$) that belong to NP_K. Equivalently, $\mathrm{BP}(\mathrm{NP}_K)$ can be defined as the set of problems of the form $A \cap \{0,1\}^\infty$ where $A \in \mathrm{NP}_K$. We also recall that HN is the problem of deciding whether a system of polynomial equations in several variables (with integer coefficients given in bits) has a solution in an algebraically closed field of characteristic 0.

Theorem 5.6 *Assuming the generalized Riemann hypothesis,* $\mathrm{BP}(\mathrm{NP}_K) \subseteq \mathrm{AM}$.

Proof. Let A be a boolean problem in NP_K. By Theorem 5.1, we can assume that the corresponding NP_K algorithm is parameter-free. It is thus possible to reduce A to HN in polynomial time in the bit model (this follows basically from the NP_K-completeness of Σ^1_K). Since $\mathrm{HN} \in \mathrm{AM}$ under GRH (see the long version of [12]), the same is true of A. □

It was shown in [14] that the dimension problem DIM_K for algebraic varieties is NP_K-complete. For the DIM problem (concerning varieties defined by polynomial equations with integer coefficients given in bits) we have the following consequence.

Corollary 5.7 *Assuming the generalized Riemann hypothesis,* $\mathrm{DIM} \in \mathrm{AM}$.

Proof. $\mathrm{DIM} \in \mathrm{BP}(\mathrm{NP}_K) \subseteq \mathrm{AM}$ since $\mathrm{DIM}_K \in \mathrm{NP}_K$. □

The observation that $\mathrm{DIM} \in \mathrm{AM}$ assuming GRH was already made in [14].

References

[1] L. Babai and S. Moran. Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36:254–276, 1988.

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

[3] L. Blum, F. Cucker, M. Shub, and S. Smale. Algebraic settings for the problem "P≠NP?". In J. Renegar, M. Shub, and S. Smale, editors, *The Mathematics of Numerical Analysis*, volume 32 of *Lectures in Applied Mathematics*, pages 125–144. American Mathematical Society, 1996.

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

[5] N. Bourbaki. *Algèbre (Chapitres 4 à 7).* Masson, Paris, 1981.

[6] O. Chapuis and P. Koiran. Saturation and stability in the theory of computation over the reals. Technical Report 1997/3, Institut Girard Desargues, Université Claude Bernard Lyon I, 1997.

[7] 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.

[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] 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.

[10] S. Ivanov and M. de Rougemont. Interactive protocols on the reals. In *Proc. 15th Annual Symposium on Theoretical Aspects of Computer Science*, volume 1373 of *Lecture Notes in Computer Science*, pages 499–510. Springer-Verlag, 1998.

[11] P. Koiran. Approximating the volume of definable sets. In *Proc. 36th IEEE Symposium on Foundations of Computer Science*, pages 134–141, 1995.

[12] P. Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996. Long version: DIMACS report 96-27.

[13] P. Koiran. Elimination of constants from machines over algebraically closed fields. *Journal of Complexity*, 13(1):65–82, 1997. Erratum on *http://www.ens-lyon.fr/∼koiran.*

[14] P. Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proc. 38th IEEE Symposium on Foundations of Computer Science*, pages 36–45, 1997.

[15] P. Koiran. The real dimension problem is $\mathrm{NP}_{\mathbb{R}}$-complete. LIP Research Report 97-36, Ecole Normale Supérieure de Lyon, 1997.

[16] B. Poizat. *Groupes Stables.* Nur Al-Mantiq Wal-Ma'rifah **2**. 1987.

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

[18] J. T. Schwarz. Fast probabilistic algorithms for verification of polynomials identities. *Journal of the ACM*, 27:701–717, 1980.