Lectures in Applied Mathematics
Volume **00**, 19xx

Algebraic Settings for the Problem "P $\neq$ NP?"

Lenore Blum, Felipe Cucker, Mike Shub, and Steve Smale

ABSTRACT. When complexity theory is studied over an arbitrary unordered field K, the classical theory is recaptured with $K = \mathbb{Z}_2$. The fundamental result that the Hilbert Nullstellensatz as a decision problem is NP-complete over K allows us to reformulate and investigate complexity questions within an algebraic framework and to develop transfer principles for complexity theory.

Here we show that over algebraically closed fields K of characteristic 0 the fundamental problem "P $\neq$ NP?" has a single answer that depends on the tractability of the Hilbert Nullstellensatz over the complex numbers $\mathbb{C}$. A key component of the proof is the Witness Theorem enabling the elimination of transcendental constants in polynomial time.

1. Statement of Main Theorems

We consider the Hilbert Nullstellensatz in the form HN/K: given a finite set of polynomials in n variables over a field K, decide if there is a common zero over K. At first the field is taken as the complex number field $\mathbb{C}$. Relationships with other fields and with problems in number theory will be developed here.

This article is essentially Chapter 6 of our book *Complexity and Real Computation* (to be published by Springer). Background material can be found in [Blum, Shub, and Smale 1989].

Only machines and algorithms which branch on "$h(x) = 0$?" are considered here. The symbol $\leq$ is not used. Thus the development is quite algebraic, eventually using properties of the height function of algebraic number theory. A main theme is eliminating constants. The moral is roughly: using transcendental and algebraic numbers doesn't help much in speeding up integer decision problems.

Let $\overline{\mathbb{Q}}$ be the algebraic closure of the rational number field $\mathbb{Q}$. The following will be proved.

THEOREM 1. *If* P = NP *over* $\mathbb{C}$, *then* P = NP *over* $\overline{\mathbb{Q}}$, *and the converse is also true.*

1991 *Mathematics Subject Classification.* 68Q (Computer Science, Theory of Computation), 11G (Number Theory, Arithmetic Algebraic Geometry).

Blum was partially supported by the Letts-Villard Chair at Mills College. Cucker was partially supported by DGICyT PB 920498, the ESPRIT BRA Program of the EC under contracts no. 7141 and 8556, projects ALCOM II and NeuroCOLT. Cucker, Smale, and Shub were partially supported by NSF grants.

REMARK 1. Here $\mathbb{C}$ may be replaced by any algebraically closed field containing $\overline{\mathbb{Q}}$.

Now we are going to define an invariant τ of integers (and polynomials over $\mathbb{Z}$) which describes how many arithmetic operations are necessary to build up an integer starting from 1. More precisely, a *computation of length l* of the integer m is a sequence of integers, $x_0, x_1, \ldots, x_l$ where $x_0 = 1$, $x_l = m$ and given k, $1 \le k \le l$, there are i, j, $0 \le i, j < k$ such that $x_k = x_i \circ x_j$ where $\circ$ is addition, subtraction or multiplication. We define $\tau : \mathbb{Z} \to \mathbb{N}$ by $\tau(m)$ is the minimum length of a computation of m.

The following is easy to check, where here and in the sequel log denotes $\log_2$.

PROPOSITION 1. *For all $m \in \mathbb{N}$ one has $\tau(m) \le 2 \log m$.*

If m is of the form 2^{2^k}, then $\tau(m) = \log\log m + 1$. The same is essentially true even if m is any power of 2.

Open Problem. Is there a constant c such that

$$\tau(k!) \le (\log k)^c \text{ all } k \in \mathbb{N}?$$

We remark that if "factoring is hard" using inequailities then the open problem has a negative answer.[1]

DEFINITION 1. Given a sequence of integers a_k we say that a_k is *easy to compute* if there is a constant c such that $\tau(a_k) \le (\log k)^c$, all $k > 2$, and hard to compute otherwise. We say that the sequence a_k is *ultimately easy to compute* if there are non-zero integers m_k such that $m_k a_k$ is easy to compute and *ultimately hard to compute* otherwise.

In Sections 5 and 6 we will prove:

THEOREM 2. *If the sequence of integers $k!$ is ultimately hard to compute, then* HN/$\mathbb{C}$, *the Hilbert Nullstellensatz over $\mathbb{C}$, is intractable and hence* P $\neq$ NP *over $\mathbb{C}$. Thus in that case,* P $\neq$ NP *over $\overline{\mathbb{Q}}$.*

Next consider the analogous situation for polynomials with integer coefficients $f \in \mathbb{Z}[t]$. A *computation* of length l of f is a sequence of $u_i \in \mathbb{Z}[t]$ where $u_0 = 1$, $u_1 = t$, $u_l = f$ and given k, $1 \le k \le l$ there are i, j, $0 \le i, j < k$ such that $u_k = u_i \circ u_j$ where $\circ$ is addition, subtraction or multiplication. Define $\tau : \mathbb{Z}[t] \to \mathbb{N}$ by $\tau(f)$ is the minimum length of a computation of f.

Let $\mathrm{Zer}(f)$ be the number of distinct integral zeros of f. The following has a certain plausibility:

HYPOTHESIS. $\mathrm{Zer}(f) \le \tau(f)^c$ for all non-zero $f \in \mathbb{Z}[t]$.

Here c is a universal constant. We don't know if the hypothesis is true or false, even, for example, with the constant $c = 1$.

---

[1] Here is a sketch of the proof. Suppose to the contrary that $k!$ is *easy to compute* and n is the product of primes p and q where $p < k < q$. We will show how to easily factor n.

Let $x_0, x_1, \ldots, x_l = k!$ be a short computation of $k!$, $l \le (\log k)^c$. Then we induce a short computation of $r = k! \bmod n$ using

$$(x_0 \bmod n, x_1 \bmod n, \ldots, r = x_l \bmod n).$$

By the Euclidean Algorithm, $y = gcd(r, n)$ may be easily computed. By our hypothesis it follows that $y = p$, and thus our assertion is proved.

THEOREM 3. *If the above Hypothesis is true then* NP $\neq$ P *over* $\mathbb{C}$, *and* NP $\neq$ P *over* $\overline{\mathbb{Q}}$.

2. Eliminating constants: Easy cases

In this section we begin a study of the problem of eliminating the constants of a computation without an exponential increase in the time. Our first result asserts that this can always be done if the constants lie in an algebraic extension of the given field K. The result holds for fields of any characteristic.

To start we briefly and informally recall some notation and definitions. Suppose M is a *machine* over a commutative ring (or field) R with unit. Then both the *input* and *output spaces* of M are R^∞, and the *state space* is R_∞. Here R^∞ is the *disjoint union*

$$R^\infty = \cup_{n\geq 0} R^n$$

and R_∞ is the bi-*infinite direct sum* space over R. Elements of R_∞ have the form

$$x = (\dots, x_{-2}, x_{-1}, x_0 \,.\, x_1, x_2, \dots)$$

where $x_i \in R$ for all integers i, $x_k = 0$ for $|k|$ sufficiently large, and . is a distinguished marker between x_0 and x_1. We call x_i the "i-th coordinate" of x and $x_1, \dots, x_n$ the "first n coordinates" of x. For brevity, and when the intent is clear from context, we sometimes omit the negative coordinates and write elements of the state space as $(n, x_1, x_2, \dots, x_n, 0, \dots)$ or $(x_1, x_2, \dots, x_n, 0, \dots)$, or even $(x_1, x_2, \dots, x_n)$.

The machine's *input map*, associated with its *input node*, takes a point $x \in R^n \subset R^\infty$ and maps it to

$$(\dots, 0, 0, n \,.\, x_1, x_2, \dots, x_n, 0, 0, \dots) \in R_\infty.$$

Here n is the *size* of x.

The *output map*, associated with the machines's *output node*, takes a point $x = (\dots, m \,.\, x_1, x_2, \dots) \in R_\infty$ and maps it to $(x_1, \dots, x_m)$ if m is a positive integer, to the unique point of R^0 if $m = 0$, and is undefined otherwise. These maps make sense if the characteristic of R is 0. If the characteristic is positive, we replace n and m here by the appropriate number of 1's to the left of the distinguished marker.

Machines also have *computation, shift* and *branch nodes* with associated *operations* (polynomial or rational maps, right/left shifts and the identity) and associated *next state* and *next node* maps. Without loss of generality, we assume that at branch nodes, machines branch right or left depending on whether or not the first coordinate x_1 of the current *state* x is 0.

A *decision problem* over R is a pair (Y, Y_0) where $Y_0 \subset Y \subset R^\infty$. Here Y is the set of *problem instances* and Y_0 is the set of `yes` *instances.* For example, HN/K is a decision problem over K where $Y = \{$finite polynomial systems over $K\}$ and $Y_0 = \{$finite polynomial systems over K that are solvable over $K\}$. A finite polynomial system over K is represented as an element of K^∞ assuming some standard listing of its coefficients.

A machine M over R *decides* the problem (Y, Y_0) if, for all inputs $y \in Y$, M outputs 1 if $y \in Y_0$ and 0 if not. The *halting time*, $T_M(y)$, is the length of the *computation path*, or sequence of nodes, traversed from input y to output. The problem (Y, Y_0) is in *class* P or in *polynomial time* over R if it can be decided by a machine with halting time bounded by a fixed polynomial in the *size* of y, for all $y \in Y$. Polynomial time is our notion of tractability.

The problem (Y, Y_0) is in *class* NP over R if there is a machine M' such that for all $y \in Y$, $y \in Y_0$ if and only if there is a *witness* $w \in R^\infty$ such that, given input (y, w), M' outputs 1 in time bounded by a fixed polynomial in the *size* of y. We say (Y, Y_0) is NP-*complete* over R if it is in *class* NP$/R$ and every problem in class NP$/R$ can be *encoded* in (Y, Y_0) in polynomial time. It follows from [Blum, Shub, and Smale 1989] that, for any field K, HN$/K$ is NP-complete over K.

Definition 2. Suppose $K \subset L$ are fields and (Y, Y_0) is a decision problem over L. The *restriction of* (Y, Y_0) *to* K is $(Y \cap K^\infty, Y_0 \cap K^\infty)$. The same applies to the case where K is a ring.

Proposition 2. *Let M be a machine over a field L which is an algebraic extension of a field K. Then there is a machine M' over K and a constant $c > 0$ (depending on M) with the following property. For any decision problem (Y, Y_0) over L decided by M, the restriction of (Y, Y_0) to K is decided by M', and the halting time satisfies*

$$T_{M'}(y) \leq c T_M(y), \text{ for all } y \in Y \cap K^\infty.$$

Proof. Since M has only a finite number of constants, then by restriction, M is also a machine over a subfield of L that is a finite algebraic extension of K. Thus, our proposition will follow if we assume that L is a finite algebraic extension of K, and show it for this case. So we make this assumption.

Consider L as a vector space over K of dimension q. Thus L may be represented as K^q where the inclusion $K \subset L$ is represented as the inclusion of K in K^q as the first coordinate.

We now construct a machine M' over K that on inputs from K^∞ simulates M on these inputs with halting time increased by no more than a multiplicative constant. The state space of M' is considered as $(K^q)_\infty$ so that it also represents L_∞. An initial subroutine of M' in effect takes an input from K^∞ and writes it as the first coordinates in $(K^q)_\infty$.

Without loss of generality, we may assume that at any computation node of M, the computation performed is either addition, multiplication, subtraction or division of two elements of L. (Any machine can be so converted with at most a multiplicative constant increase in halting time.) Since addition and multiplication in L are represented by fixed symmetric bilinear maps over K

$$\begin{aligned} B_+ &: K^q \times K^q \to K^q \\ B_\times &: K^q \times K^q \to K^q, \end{aligned}$$

M' can simulate the addition and multiplication nodes of M by incorporating these polynomial maps in computation nodes. Subtraction nodes of M are simulated in M' by multiplication by (-1) followed by B_+. Division of b by a is accomplished by solving the linear system $B_\times(a, y) = b$ for y by Gaussian elimination. This requires on the order of q^3 steps. In each of these simulations, constants from L that occur in M are replaced by their corresponding q-tuples over K.

Since $x = (x_1, \ldots, x_q)$ represents the zero element in L if and only if $x_i = 0$ for $i = 1, \ldots, q$, branching in M is simulated by checking if the first q coordinates of an element in the state space of M' are zero. Shifting right or left in M is simulated by shifting right or left q times in M'. Care is taken to keep track of the intended lengths of sequences in the computation. A final subroutine ensures that the appropriate finite sequence $(x_1, x_{q+1}, x_{2q+1}, \ldots, x_{mq+1})$ of the coordinates of the "final state" x in a computation is output.

Using the isomorphism between K^q and L, one can see that on inputs $y \in Y \cap K^\infty$, M' gives the same answers as M with the desired time bound where c is on the order of q^3. □

The proof doesn't require M to be a decision machine, merely that the outputs of M are defined over K, i.e. are in K^∞, for inputs over K.

PROPOSITION 3. *Let R be an integral domain and K its quotient field. Let (Y, Y_0) be a decision problem solved by a machine M over K in time T. Then M can be replaced by an equivalent machine without division, with constants only from R, and with halting time cT for some $c \in \mathbb{N}$. Thus, there is a machine over R solving the restriction of (Y, Y_0) to R in time cT for some $c \in \mathbb{N}$.*

PROOF. A machine M' without division that simulates M is obtained by "doubling" the space used in the computation. An initial subroutine of M' takes an input $(x_1, x_2, \ldots, x_s)$ to $(2s, x_1, 1, x_2, 1, \ldots, x_s, 1, 0, \ldots)$ in the state space of M'. Note that elements $x = (x_1, x_2, \ldots, x_s, 0, \ldots)$ in the state space of M may be represented (non-uniqueley) by elements in the state space of M' of the form

$$(x_1^{[n]}, x_1^{[d]}, x_2^{[n]}, x_2^{[d]}, \ldots, x_s^{[n]}, x_s^{[d]}, 0, \ldots)$$

where $x_i = \frac{x_i^{[n]}}{x_i^{[d]}}$ for all $i \leq s$. Since K is the quotient field of R, elements of K_∞ have representation in R_∞.

Computation nodes of M' perform the natural modification of the operations associated with the computation nodes of M which, as above, are assumed to be the basic arithmetic operations over K. In particular, a computation node in M that performs a division $f(x_1, x_2) = (x_1/x_2)$ is replaced in M' by a computation node with associated map

$$g(x_1^{[n]}, x_1^{[d]}, x_2^{[n]}, x_2^{[d]}) = (x_1^{[n]} x_2^{[d]}, x_1^{[d]} x_2^{[n]})$$

Constants from K in M are replaced in M' by pairs of constants from R. So for example, a computation node of M with associated map $f(x_1) = kx_1$ with constant $k \in K$, is replaced in M' by a computation node with associated map $g(x_1^{[n]}, x_1^{[d]}) = (px_1^{[n]}, qx_1^{[d]})$ for some $p, q \in R$ with $k = p/q$. Thus, if an initial input to M' comes from R^∞, all states in the subsequent computation will be in R_∞.

A branch node in M that tests if $x_1 = 0$ is replaced in M' by one that tests if $x_1^{[n]} = 0$ and $x_1^{[d]} \neq 0$.

Finally, M accepts an input x, i.e. M outputs the value 1 given input x, if the first coordinate of the final state in the computation is 1 (and the 0-th coordinate is 1). Consequently, M' is designed to accept an input if the first and second coordinates of the final state in the computation are equal but not 0 (and the 0-th coordinate is 2). Similar considerations apply for rejecting an input.

The overall slowdown of M' with respect to M is linear.

Thus, M' has the requisite properties for both conclusions in the statement of the proposition. □

3. Witness Theorem

We need an algebraic theorem, which we call the Witness Theorem, for the proof of our main results. This section is devoted to that theorem.

The first step is to extend the definition of τ to polynomials in several variables over $\mathbb{Z}$. Let $G \in \mathbb{Z}[t_1, \ldots, t_n]$. Quite similarly to the one variable case, consider finite sequences

$$(t_1, \ldots, t_n, 1, u_1, \ldots, u_s = G)$$

where for $1 \le k \le s$, $u_k = v \circ w$ for some $v, w \in \{t_1, \ldots, t_n, u_0 = 1, u_1, \ldots, u_{k-1}\}$ and $\circ$ is $+$, $-$ or $\times$. Then $\tau(G)$ is the minimum such s.

Definition 3. Define a *witness* $w \in \overline{\mathbb{Q}}^l$ for $f \in \overline{\mathbb{Q}}[t_1, \ldots, t_l]$ as a w satisfying the property that if $f(w) = 0$ then $f = 0$, i.e. f is the zero polynomial.

In situations we encounter, f is presented so that it is not obvious if it is zero.

Theorem 4 (Witness Theorem). *Let $F(x, t) = F(x_1, \ldots, x_r, t_1, \ldots, t_l)$ be a polynomial in $r + l = n$ variables with coefficients in $\mathbb{Z}$ and let $F_x \in \overline{\mathbb{Q}}[t_1, \ldots, t_l]$ be defined by $F_x(t) = F(x, t)$ for each $x \in \overline{\mathbb{Q}}^r$. Suppose that N is a positive integer satisfying:*

$$\log N \ge 4n\tau^2 + 4, \ \ \tau = \tau(F).$$

Then for $x \in \overline{\mathbb{Q}}^r$, there exists an algebraic number w_1 in $\{2^N, x_1^N, \ldots, x_r^N\}$ such that the point $w = (w_1, \ldots, w_l)$ where $w_i = w_{i-1}^N$, $i = 2, \ldots, l$ is a witness for $F_x \in \overline{\mathbb{Q}}[t_1, \ldots, t_l]$.

Our proof of the Witness Theorem depends heavily on the use of *heights* of algebraic numbers.

The height $H : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ is a function whose properties are summarized in the following proposition.

Proposition 4. **(a):** $H(1) = H(0) = 1$, $H(2) = 2$, $H(w) \ge 1$, $H(-w) = H(w)$, $H\left(\frac{1}{w}\right) = H(w)$
(b): $H(v + w) \le 2H(v)H(w)$
(c): $H(w^k) = H(w)^k$, $H(vw) \le H(v)H(w)$
(d): $H(v + w) \ge \frac{1}{2}\frac{H(v)}{H(w)}$
(e): $H(vw) \ge \frac{H(v)}{H(w)}$ *if* $w \ne 0$.

A definition of H and proofs of (a) and (c) are given in [Lang 1991]. Moreover (b) is proved in the appendix to this section. Note that (d) follows from (b) by

$$H(v) = H((v + w) - w) \le 2H(v + w)H(w).$$

Now divide by $2H(w)$.

Similarly we obtain (e) from (c) by

$$H(v) = H\left((vw)\frac{1}{w}\right) \le H(vw)H(w).$$

Note that, in general,

$$H\left(\sum_{i=0}^{n} x_i\right) \le 2^n \prod_{i=0}^{n} H(x_i).$$

All that is used in this section is the existence of a function $H : \overline{\mathbb{Q}} \to \mathbb{Z}_+$ with properties (a), (b) and (c) (and hence also (d) and (e)). It is a good exercise to prove Proposition 4 for $\mathbb{Q}$ with $H(r) = \max(|p|, |q|)$ where $r = \frac{p}{q}$ and $\gcd(p, q) = 1$.

If $g \in \overline{\mathbb{Q}}[t]$ is a one variable polynomial, and $g(t) = \sum_{i=0}^{d} a_i t^i$, define $H(g) = \prod_{i=0}^{d} H(a_i)$.

PROPOSITION 5. *For all $g \in \overline{\mathbb{Q}}[t]$ and all $w \in \overline{\mathbb{Q}}$*

$$H(g(w)) \leq 2^d H(w)^d H(g).$$

PROOF. Use Horner's argument

$$\begin{aligned} H\left(\sum_{i=0}^{d} a_i w^i\right) &= H(a_0 + w(a_1 + w(a_2 + \cdots + w(a_{d-1} + wa_d))\dots)) \\ &\leq 2^d H(a_0)H(w)H(a_1)H(w)H(a_2)\dots \\ &= 2^d \prod_{i=0}^{d} H(a_i)H(w)^d. \end{aligned}$$

□

If $G(x) = \sum a_\alpha x^\alpha$ is a polynomial in n variables over $\overline{\mathbb{Q}}$, let

$$H(G) = \prod_{\alpha} H(a_\alpha).$$

PROPOSITION 6. *For $G \in \mathbb{Z}[t_1, \dots, t_n]$, let $\tau = \tau(G)$. Then*

$$H(G) \leq 2^{2^{2n\tau^2}}.$$

Toward the proof we have the following lemma whose proof is simple and straightforward.

LEMMA 1. *The degree of G is less than or equal to 2^τ. The number of monomials in G, indexed by α, is less than D^n, where $D = 2^\tau$.* □

We prove now Proposition 6.

PROOF OF PROPOSITION 6. It goes by induction on τ. One checks it by inspection for $\tau = 1$.

Now let $G = FF'$ where $\tau(F)$, $\tau(F') < \tau$ (the case $G = F + F'$ or $G = F - F'$, is even simpler). Write $F(x) = \sum a_\alpha x^\alpha$, $F'(x) = \sum b_\beta x^\beta$ and $G(x) = \sum c_\gamma x^\gamma$. Then

$$c_\gamma = \sum_{\beta} a_{\gamma - \beta} b_\beta.$$

Note that by Lemma 1, the degrees of F, F' and G are less than or equal to D and the number of terms in F, F' and G is even less than D^n. Then

$$\begin{aligned} H(c_\gamma) &\leq \prod_{\beta} 2H(a_{\gamma-\beta})H(b_\beta) \\ &\leq 2^{D^n} H(F)H(F'). \end{aligned}$$

Thus

$$H(G) \leq (2^{D^n} H(F)H(F'))^{D^n}.$$

By the induction hypothesis

$$H(G) \leq 2^{D^{2n}} \cdot 2^{D^n \cdot 2^{2n(\tau-1)^2+1}}$$

so

$$\begin{aligned} \log H(G) &\leq D^{2n} + D^n \cdot 2^{2n(\tau-1)^2+1} \\ &\leq 2^{2n\tau} + 2^{n\tau} 2^{2n(\tau-1)^2+1} \\ &\leq 2^{2n\tau^2} \end{aligned}$$

for $\tau \geq 2$. □

The next proposition while simple, with a short proof, is crucial for the Witness Theorem.

Proposition 7. *Let $g \in \overline{\mathbb{Q}}[t]$ be a non-constant polynomial in one variable of degree d. Then for every $x \in \overline{\mathbb{Q}}$,*

$$H(g(x)) \geq \frac{H(x)}{2^d H(g)}.$$

Proof. Write

$$g(t) = \sum_{i=0}^{d} a_i t^i, \; a_d \neq 0, \; d > 0.$$

Then

$$\begin{aligned} H(g(x)) &= H\left(a_d x^d + \sum_{i=0}^{d-1} a_i x^i\right) \\ &\geq \frac{1}{2} \frac{H(a_d x^d)}{H\left(\sum_{i=0}^{d-1} a_i x^i\right)} \\ &\geq \frac{1}{2^d} \frac{H(x)^d}{H(a_d) H(x)^{d-1} H(a_0) \ldots H(a_{d-1})} \\ &\geq \frac{1}{2^d} \frac{H(x)}{H(g)}. \end{aligned}$$

Here we have used Propositions 4 and 5. □

Corollary 1. *For $g \in \overline{\mathbb{Q}}[t]$, if $H(x) > 2^d H(g)$, then $g(x) \neq 0$ unless g is zero.* □

For $x \in \overline{\mathbb{Q}}^n$ let

$$H(x) = \max_{1 \leq i \leq n} H(x_i).$$

For $G \in \overline{\mathbb{Q}}[t_1, \ldots, t_n]$ and $x = (x_1, \ldots, x_r) \in \overline{\mathbb{Q}}^r$, $r < n$, let

$$G_{x_1, \ldots, x_r}(t_{r+1}, \ldots, t_n) = G(x_1, \ldots, x_r, t_{r+1}, \ldots, t_n).$$

Proposition 8. *For any $G \in \overline{\mathbb{Q}}[t_1, \ldots, t_n]$ and $x = (x_1, \ldots, x_r) \in \overline{\mathbb{Q}}^r$ with $r < n$ we have*

$$H(G_{x_1, \ldots, x_r}) \leq H(G)(2H(x))^{D^{n+1}}$$

where degree $G \leq D$, and $H(x) = H(x_1, \ldots, x_r)$.

PROOF. Let $G(t) = \sum_\alpha a_\alpha t^\alpha$. Note that $G_{x_1,\dots,x_r} \in \overline{\mathbb{Q}}[t_{r+1},\dots,t_n]$ is a polynomial whose coefficients may be indexed by $(\alpha_{r+1},\dots,\alpha_n)$ and, for each $(\alpha_{r+1},\dots,\alpha_n)$, have the form

$$\sum a_\alpha x_1^{\alpha_1},\dots,x_r^{\alpha_r}$$

where the sum is over $\alpha = (\alpha_1,\dots,\alpha_n)$ such that the last $n-r$ entries of α are $(\alpha_{r+1},\dots,\alpha_n)$. We must estimate the product of the heights of these coefficients to obtain the proposition. The estimate is similar to that used in Proposition 5.

The estimate for the height of a coefficient of $G_{x_1,\dots,x_r}$ is

$$\begin{aligned} &\leq \; 2^{D^r} \prod_{\alpha=(\alpha_1,\dots,\alpha_r)} H(a_\alpha)H(x_1)^{\alpha_1}\dots H(x_r)^{\alpha_r} \\ &\leq \; 2^{D^r} \prod_{\alpha=(\alpha_1,\dots,\alpha_r)} H(a_\alpha)H(x)^D. \end{aligned}$$

Take the product over all the coefficients to get

$$H(G_{x_1,\dots,x_r}) \leq 2^{D^n} H(G) H(x)^{D^{n+1}}$$

yielding the necessary estimate. □

For the proof of the Witness Theorem we may assume that w_1 is one of $2^N, x_1^N,\dots,x_r^N$ with largest height so

$$H(w_1) \geq \max(2^N, H(x_i)^N).$$

Then $H(w_1) > 1$ and $H(w_i) > H(w_{i-1})$.

Now with these x, w as in the Witness Theorem, for each $j = 1,\dots,l$ and $\hat\beta = (\hat\beta_{j+1},\dots,\hat\beta_l)$, we will define a one variable polynomial $G^j_{\hat\beta}$ so that we will be able to apply the one variable lower bound of Proposition 7.

Write

$$F(x,t) = \sum_{\substack{\alpha=(\alpha_1,\dots,\alpha_r)\\ \beta=(\beta_1,\dots,\beta_l)}} a_{\alpha,\beta} x^\alpha t^\beta$$

then define

$$G^j_{\hat\beta}(t) = \sum_{\substack{\alpha=(\alpha_1,\dots,\alpha_r)\\ \beta=(\beta_1,\dots,\beta_j,\hat\beta_{j+1},\dots,\hat\beta_l)}} a_{\alpha,\beta} x^\alpha w_1^{\beta_1}\dots w_{j-1}^{\beta_{j-1}} t^{\beta_j}.$$

LEMMA 2. *For each $j = 1,\dots,l$ and $\hat\beta$ as above*

$$H(w_j) > 2^D H(G^j_{\hat\beta}).$$

PROOF. Fix j. It is sufficient to prove that

$$H(w_j) > 2^D H(F_{x,w_1,\dots,w_{j-1}}),$$

or yet by Proposition 8 that

$$H(w_j) > 2^D H(F)(2H(x_1,\dots,x_r,w_1,\dots,w_{j-1}))^{D^{n+1}}.$$

Now use Proposition 6. The needed estimate is:

$$H(w_j) > \begin{cases} 2^D \cdot 2^{2^{2nr^2}} (2H(w_{j-1}))^{D^{n+1}} & \text{if } j > 1 \\ 2^D \cdot 2^{2^{2nr^2}} 2(\max(2, H(x)))^{D^{n+1}} & \text{if } j = 1. \end{cases}$$

Now use $D = 2^\tau$, and verify that

$$\log N > \tau + 2n\tau^2 + 2(n+1)\tau. \qquad \square$$

The Witness Theorem is almost proved. Use Proposition 7 with $j = l$ in Lemma 2. We obtain

$$G^l_\emptyset(t) = F_{x,w_1,\ldots,w_{l-1}}(t), \;\; \hat\beta = \emptyset$$

and

$$H(w_l) > 2^D H(G^l_\emptyset).$$

Therefore $F_{x,w_1,\ldots,w_{l-1}}$ is zero. So for each $\hat\beta_l$,

$$\sum_{\substack{\alpha=(\alpha_1,\ldots,\alpha_n)\\ \beta=(\beta_1,\ldots,\beta_{l-1},\hat\beta_l)}} a_{\alpha,\beta} x^\alpha w_1^{\beta_1}\ldots w_{l-1}^{\beta_{l-1}} = 0.$$

Continuing the same process for $l-1, l-2, \ldots, 1$, we obtain eventually for any $\hat\beta = (\hat\beta_1, \ldots, \hat\beta_l)$ that

$$\sum_\alpha a_{\alpha,\hat\beta} x^\alpha = 0.$$

This yields our theorem. $\square$

Appendix to Section 3

In this appendix we prove part (b) of Proposition 4. We could not find it in the literature.

To do so, we need to use some notions from algebraic number theory. References for these notions can be found in Section 9.

Definition 4. $H_K(u) = \prod_{\nu\in M_K} \max(1, |u|_\nu^{N_\nu})$, where M_K is the set of valuations of K. If ν restricts to v_0 then define

$$N_\nu = [K_v : F_{v_0}],$$

the degree relative to the completions.

Definition 5. $H(u) = H_K(u)^{\frac{1}{[K:Q]}}$, for $u \in K$. It can be shown that this is independent of K.

Lemma 3. *$\sum_{\nu\in M_K^\infty} N_\nu = [K : Q]$, where $M_K = M_K^\infty \cup M_K^*$, M_K^∞ the archimedean valuations and M_K^* the non-archimedean valuations.* $\square$

Now for the proof of part (b) of Proposition 4.

Proof of Proposition 4 (b). We may write:

$$\begin{aligned} H_K(x+y) &= \prod_{\nu\in M_K^\infty} \max(1, |x+y|_\nu^{N_\nu}) \prod_{\nu\in M_K^*} \max(1, |x+y|_\nu^{N_\nu}) \\ &\le \prod_{\nu\in M_K^\infty} 2^{N_\nu} \prod_{\nu\in M_K^\infty} (\max(1, |x|_\nu, |y_\nu|))^{N_\nu} \prod_{\nu\in M_K^*} (\max(1, |x|_\nu, |y|_\nu))^{N_\nu} \end{aligned}$$

from properties of $|\;|_\nu$, archimedean and non-archimedean respectively.

Since

$$\max(1,|x|_\nu,|y|_\nu) \leq \max(1,|x|_\nu)\max(1,|y|_\nu),$$

$$H_K(x+y) \leq 2^{\sum_{\nu\in M_K^\infty} N_\nu} \prod_{\nu\in M_K} (\max(1,|x|_\nu))^{N_\nu} \prod_{\nu\in M_K} (\max(1,|y|_\nu))^{N_\nu}.$$

Using the lemma it follows that

$$H_K(x+y) \leq 2^{[K:Q]} H_K(x) H_K(y).$$

Taking roots we thus obtain

$$H(x+y) \leq 2H(x)H(y). \qquad \square$$

4. Elimination of Constants: General Case

The main focus of this section is the following proposition.

PROPOSITION 9 (Elimination of Constants). *Let $K \subset L$ be fields where $K \subset \overline{\mathbb{Q}}$. Let (Y, Y_0) be a decision problem solved by a machine M over L. Then there is a machine M' over K solving the restriction of (Y, Y_0) to K and a constant $c \in \mathbb{N}$ such that $T_{M'}(y) \leq T_M(y)^c$ for all $y \in Y \cap K^\infty$.*

LEMMA 4. *For the proof of the preceding proposition, it is sufficient to consider the case $L = K(s_1, \dots, s_l)$ where $s_1, \dots, s_l$ is a transcendence base for L over K (i. e., the s_i are algebraically independent over K).*

PROOF. The machine M over L uses a finite number of constants $\eta_1, \dots, \eta_r \in L$. Therefore M can be considered as a machine over $K(\eta_1, \dots, \eta_r) \subset L$ by restriction.

By a standard theorem of algebra (in field theory) one may rewrite the sequence $\eta_1, \dots, \eta_r$ as $s_1, \dots, s_l, \mu_1, \dots, \mu_q$ where the $s_1, \dots, s_l$ form a transcendence basis for $K(s_1, \dots, s_l)$ over K and the $\mu_1, \dots, \mu_q$ are algebraic over $K(s_1, \dots, s_l)$. Now apply Proposition 2 to obtain a machine over $K(s_1, \dots, s_l)$ with the same values on inputs from K^∞ as M and only a constant multiple increase in time. $\square$

PROOF OF PROPOSITION 9. We give the proof of the Elimination of Constants Proposition where L has the form given in Lemma 4. By Proposition 3 we may suppose that each computation node of the machine M is an arithmetic node ($+$, $-$, $\times$) and that each constant in M is a polynomial in $s = (s_1, \dots, s_l)$ over K. Let $\alpha = (\alpha_1, \dots, \alpha_m)$ be a sequence of all the coefficients occuring in these polynomials. We may then suppose each constant in M is of the form $p(\alpha, s)$ where p is a polynomial over $\mathbb{Z}$. Let C be the sum of the $\tau(p)$ over all constants in M.

We construct a machine M' over K that given input $y = (y_1, \dots, y_n) \in Y \cap K^\infty$ generates a computation path that simulates the computation path $\gamma_y = (\eta_0, \dots, \eta_t, \dots)$ generated by M on input y. The critical construction is to simulate the branching structure of γ_y, and to do this with at most a polynomial increase in time.

So suppose η_t is a branch node and g_t the associated *step t branching polynomial.* That is, g_t is the composition of the successive computations occuring along the computation path γ_y through step t. We may consider g_t as a polynomial in y, α, and s over $\mathbb{Z}$ with $\tau(g_t) \leq t + C$. The computation path γ_t branches right or left according to whether or not $g_t(y, \alpha, s) = 0$.

We construct M' so that given input $y = (y_1, \ldots, y_n)$ and "time" t, M' generates elements $w_1, \ldots, w_l$ in K to replace $s_1, \ldots, s_l$ and thus obtain a machine over K. To produce w_1, let $N = 4(n+m+l)(t+C)^2 + 4$ and repeat squaring of each $2, y_1, \ldots, y_n, \alpha_1, \ldots, \alpha_m$ N times (not giving a unique w_1, but a set of them). Let $w_1, \ldots, w_l$ be as in the Witness Theorem. Now test if $g_t(y, \alpha, w) = 0$ successively for each one of the $n + m + 1$ choices.

If any one of these $g_t(y, \alpha, w) \neq 0$ then $g_t(y, \alpha, s) \neq 0$ and we branch accordingly. On the other hand by the Witness Theorem, if $y \in K^\infty$ and all the $g_t(y, \alpha, w) = 0$, then $g_t(y, \alpha, s) = 0$. It is easy to check that the total increase in time is polynomial so that we have proved our proposition. $\square$

Denote the decision problem HN over a field K by (Y_K, Y_{0K}).

Lemma 5. *If $K \subset L$ are algebraically closed fields then*

$$(Y_L \cap K^\infty, Y_{0L} \cap K^\infty) = (Y_K, Y_{0K}).$$

That is, the restriction of HN$/L$ *to* K *is* HN$/K$.

Proof. Write $Y_L = \bigcup Y_{L,n,k,d}$ where $Y_{L,n,k,d}$ is the space of k-tuples of polynomials, each of degree $\leq d$, in n variables over L. Let $Y_{0,L,n,k,d}$ be the subset with a common zero. Since clearly $Y_L \cap K^\infty = Y_K$ it is sufficient to show that $Y_{0,L,n,k,d} \cap K^\infty = Y_{0,K,n,k,d}$.

This latter amounts to showing that if $\{f_i\}_{i=1}^k \in Y_{L,n,k,d} \cap K^\infty$ have a common zero $\zeta \in L^n$, then the f_i must have a common zero in K^n. But this follows directly from the model completeness of the theory of algebraically closed fields. Alternatively, if the f_i have no common zero in K^n, then by Hilbert's Nullstellensatz, there exist g_i, $i = 1, \ldots, k$, polynomials in n variables, such that $\sum g_i f_i = 1$. Evaluation at ζ gives a contradiction. This proves Lemma 5. $\square$

Now we can prove the first statement of Theorem 1.

Proof of Theorem 1 ("if" direction). Suppose P = NP over $\mathbb{C}$. Then HN$/\mathbb{C} \in$ P by a machine M over $\mathbb{C}$. Then M "solves" HN$/\overline{\mathbb{Q}}$, (inputs from $\overline{\mathbb{Q}}^\infty$) by Lemma 5, but M is still a machine over $\mathbb{C}$. Now apply Proposition 9 to obtain a machine over $\overline{\mathbb{Q}}$ solving HN$/\overline{\mathbb{Q}}$ in polynomial time. By the NP-completeness of this problem, P = NP over $\overline{\mathbb{Q}}$. $\square$

5. Twenty Questions

Toward the proofs of Theorems 2 and 3 we introduce a decision problem we call "Twenty Questions" which is of independent interest.

Let R be a ring (integral domain) or field of characteristic 0 which we consider without order and let $\mathbb{N}$ be the positive integers. Then *Twenty Questions over R* is the problem:

Given input $(k, \mathrm{ht}(k), z) \in \mathbb{N} \times \mathbb{N} \times R$, decide if $z \in \{1, 2, \ldots, k\}$.

Here $\mathrm{ht}(k)$ is defined to be the largest natural number less than or equal to $\log k$.

Even if R happens to be an ordered ring as $\mathbb{Z}$, we continue to branch only on equality tests.

Twenty Questions over any ring R can be decided in time $3k$ by the machine in Figure 1. Can one do better? We don't know. But if $R = \mathbb{Z}$, and branching on order is permitted, then the decision time is approximately $\log k$, with the algorithm used in the parlor game called Twenty Questions.

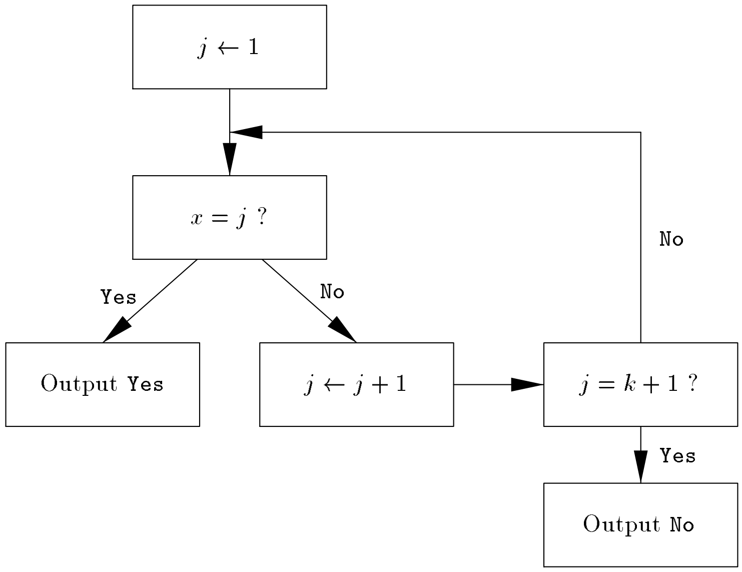

FIGURE 1. A machine for Twenty Questions.

We say that *Twenty Questions over R is tractable* if it can be decided in time $(\log k)^c$ over R where c is some constant (depending only on R). The next theorem shows that if Twenty Questions over $\mathbb{Z}$ is tractable, then so is the order relationship itself.

THEOREM 5. *If Twenty Questions over $\mathbb{Z}$ is tractable, then on input $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, one can decide if $x < y$ in time polynomial in* $\max(\log|x|, \log|y|)$.

PROOF. Figure 2 shows a machine that solves the problem. This machine halts after visiting at most $3k + 2$ nodes where k is the first integer greater than $\max(\log|x|, \log|y|)$. Of these nodes, $2k$ are Twenty Questions for $2, 2^2, \ldots, 2^k$ twice each, hence the total time is

$$2\sum_{j=1}^{k} j^c + k + 2$$

which is less than or equal to

$$2\left(\frac{k(k+1)}{2}\right)^c + k + 2. \qquad \square$$

THEOREM 6. *If* $\mathrm{P} = \mathrm{NP}$ *over $\mathbb{C}$, then Twenty Questions over $\mathbb{C}$ is tractable.*

PROOF. The method is to embed Twenty Questions in a decision problem (Y, Y_{yes}) which is in NP over $\mathbb{C}$. Then if $\mathrm{NP} = \mathrm{P}$ over $\mathbb{C}$, (Y, Y_{yes}) is in P over $\mathbb{C}$ and there is a machine M which decides Twenty Questions in time bounded by $(\log k)^c$, c a constant. Here M is the restriction of the machine which decides (Y, Y_{yes}) in polynomial time.

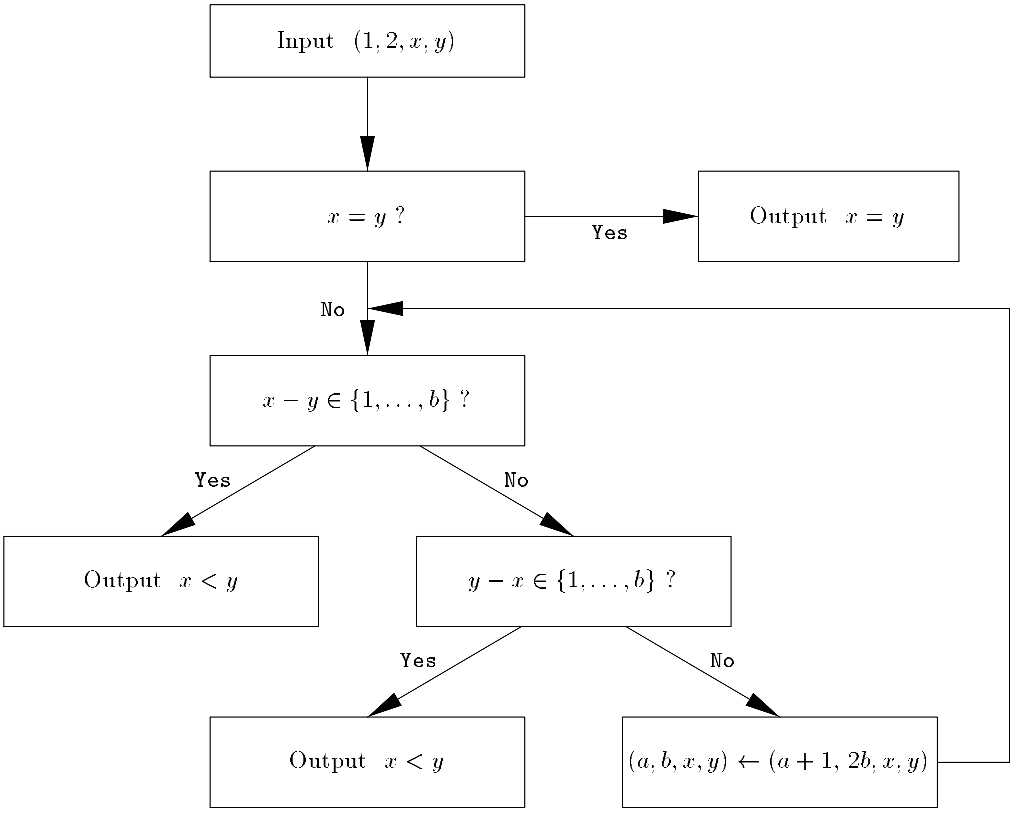

FIGURE 2. A machine computing $\leq$ in $\mathbb{Z}$.

The decision problem (Y, Y_{yes}) is described as follows:

$$Y = \mathbb{C}^{\infty} \quad \text{and} \quad Y_{\text{yes}} = \bigcup_{k \in \mathbb{N}} Y_{\text{yes},k} \quad \text{where}$$

$$Y_{\text{yes},k} = \{(k, \text{ht}(k), z_1, \ldots, z_{\text{ht}(k)}) \mid z_1 \in \{1, \ldots, k\}\}.$$

The embedding of Twenty Questions in (Y, Y_{yes}) is simply:

$$(k, \text{ht}(k), z) \to (k, \text{ht}(k), z, 1, \ldots, 1)$$

where the number of ones is $\text{ht}(k) - 1$. The proof is finished by the next lemma. $\square$

LEMMA 6. *(Y, Y_{yes}) is in* NP *over* $\mathbb{C}$.

PROOF. The $\text{NP}_{\mathbb{C}}$ machine operates on variables

$$(u_1, u_2, z_1, \ldots, z_n, w_0, \ldots, w_n, v_{j0}, \ldots, v_{jn}) \quad \text{for } j = 1, 2, 3, 4.$$

It checks if u_2 is an integer by addition of 1's. It checks if the input size (given with the input by definition) is $6u_2 + 5$. If so $n = u_2$. It checks if $w_n = 1$, $w_i(w_i - 1) = 0$ and $v_{ji}(v_{ji} - 1) = 0$ for $i = 0, \ldots, n$ and $j = 1, 2, 3, 4$. It checks if $u_1 = \sum_{i=0}^{n} 2^i w_i$. It sets $x_j = \sum_{i=0}^{n} 2^i v_{ji}$ for $j = 1, 2, 3, 4$. Finally it checks if $u_1 = z_1 + \sum_{j=1}^{4} x_j^2$. If so it outputs `Yes`. Note that if the tests are verified, the w's and v's are 0 or 1; u_1, the x_j and hence z_1 are non-negative integers and $u_2 = \mathrm{ht}(u_1)$. The time required is a constant times u_2.

Finally we show that every element of $Y_{\mathrm{yes},k}$ has a positive test. Let

$$(k, \mathrm{ht}(k), z_1, \ldots, z_{\mathrm{ht}(k)}) \in Y_{\mathrm{yes},k}.$$

Then z_1 is a non-negative integer so that $k - z$, is sum of four integers squared,

$$k - z_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2. \qquad \square$$

REMARK 2. The result and proof of Theorem 6 are valid if $\mathbb{C}$ is replaced by $\overline{\mathbb{Q}}$ everywhere in the statement.

THEOREM 7. *If Twenty Questions over $\mathbb{C}$ is tractable, then Twenty Questions over $\mathbb{Z}$ is tractable.*

PROOF. It follows immediately from the elimination of constants in Sections 2 and 4. $\square$

6. Proof of Theorems 2 and 3

PROOF OF THEOREM 3. Suppose that P = NP over $\mathbb{C}$. Then by Theorems 6 and 7, Twenty Questions over $\mathbb{Z}$ is tractable. Thus there is a machine over $\mathbb{Z}$ deciding

$$\text{Given } (k, \mathrm{ht}(k), z) \in \mathbb{Z} \times \mathbb{N} \times \mathbb{N} \times \mathbb{Z}, \text{ does } z \in [1, k]?$$

in time $(\log k)^c$. By the Canonical Path Theorem for each k there is a one variable non-trivial polynomial $g_k \in \mathbb{Z}[t]$ vanishing on the set $\{1, 2, \ldots, k\}$ with $\tau(g_k) \leq (\log k)^c$.

Observe that the hypothesis preceeding Theorem 3 is now violated. That is

$$\mathrm{Zer}(g_k) \geq k \geq (\log k)^c \geq \tau(g_k) \text{ for } k \geq k_0.$$

$\square$

We now prove Theorem 2.

PROOF OF THEOREM 2. We know that for each k, the degree of g_k is less than or equal to $2^{\tau(g_k)}$. So there is an integer l, $|l| \leq 2^{\tau(g_k)}$ with $g_r(l) \neq 0$. We may assume $|l|$ is minimal satisfying $g_k(l) \neq 0$. By Proposition 1, $\tau(l) \leq 2\tau(g_k)$ so that $\tau(l) \leq 2(\log k)^c$. Then g_k is zero at each integer between 0 and l. Observe that $g_k(l)$ has $k!$ as a factor by checking the 2 cases $l \leq 0$ and $l > k$. Moreover by evaluating g_k at l,

$$\tau(g_k(l)) \leq 3(\log k)^c.$$

Let $m_k = g_k(l)/k!$ (l depends on k also) in the definition of ultimately hard to compute. This finishes the proof of Theorem 2. $\square$

7. Main Theorem, An Algebraic Proof of the Converse

Let K be an algebraically closed field and L a field, $K \subset L$. A set $S \subset K[t_1, \ldots, t_n]$ determines an algebraic set $V_K \subset K^n$ by $x \in V_K$ if and only if $f(x) = 0$ for all $f \in S$. Moreover S also determines an algebraic set $V_L \subset L^n$ by $x \in V_L$ if and only if $f(x) = 0$ all $f \in S$.

LEMMA 7. *With S and notation as above, let V'_L be the algebraic set defined by*

$$V'_L = \{x \in (L)^n \mid f(x) = 0 \text{ all } f \in K[t_1, \dots, t_n] \ni f \equiv 0 \text{ on } V_K\}.$$

Then $V'_L = V_L$.

PROOF. Since clearly $V'_L \subset V_L$, it is sufficient to show that any $f \in K[t_1, \dots, t_n]$ vanishing on V_K, must also vanish on V_L. But by the Hilbert Nullstellensatz such an f satisfies, for some $l > 0$, $f^l \in I_K(S)$, the ideal generated by S over K. Therefore f^l also vanishes on V_L and hence f does. ☐

Therefore V_L is determined by V_K.

PROPOSITION 10. *Let $S \subset K[x_1, \dots, x_n]$ and $g_1, \dots, g_l \in K[x_1, \dots, x_n]$. Let V_K and V_L be defined by S. If there is a point $z \in V_L$ such that $g_i(z) \neq 0$,for all $i = 1, \dots, l$ then there is a point $z' \in V_K$ such that $g_i(z') \neq 0$, $\forall i = 1, \dots, l$.*

PROOF. We first prove the proposition in case V_K is irreducible. Now proceed by induction on l. The case $l = 0$ is already done in the proof of Lemma 4.

By induction we suppose the assertion proven for $l - 1$ and establish it for l. Assume that $z \in V_L$ and $g_i(z) \neq 0$ for all $i = 1, \dots, l$. By induction the set U of $z' \in V_K$ such that $g_i(z') \neq 0$, for all $i = 1, \dots, l - 1$ is non-empty and Zariski open. If there is no $z' \in U$ such that $g_l(z') \neq 0$ then g_l is zero on U and hence zero on V_K by the irreducibility of V_K. Hence by the Nullstellensatz there is an m such that g_l^m is in the ideal $I_K(S)$ generated by S in $K[x_1, \dots, x_n]$. Hence g_l^m is also in the ideal $I_L(S)$ generated by S in $L[x_1, \dots, x_n]$ and g_l vanishes on V_L which is a contradiction. The general case is finished by the next lemma. ☐

LEMMA 8. *Let $V_K \subset K^n$ be an algebraic set with V_K the union of algebraic sets V_1 and V_2. Then*

$$V_L = V_{1,L} \cup V_{2,L}.$$

PROOF. For $i = 1, 2$, the ideals satisfy $I(V_i) \supset I(V_K)$. Thus if $x \in L_{i,L}$, $i = 1$ and 2, then $x \in V_L$. On the other hand if $x \notin V_{1,L} \cup V_{2,L}$, then there exist $f_i \in I(V_{1,K})$, $i = 1, 2$ such that $f_i(x) \neq 0$. Thus $f_1 f_2(x) \neq 0$ and $f_1 f_2 \notin I(V_1) \cup I(V_2) = I(V_K)$ so $x \notin V_L$. ☐

A *basic quasi-algebraic formula* over a ring R is:

$$\begin{gathered} f_1(x) = 0, \dots, f_l(x) = 0 \\ g_1(x) \neq 0, \dots, g_k(x) \neq 0 \end{gathered}$$

where the f_i and g_j are elements of $R[t_1, \dots, t_m]$, for some $m \in \mathbb{N}$.

A basic quasi-algebraic formula over $R \subset K$, K a field, defines a *basic quasi-algebraic set* over R in K^n by

$$V = \{x \in K^m \mid f_i(x) = 0,\ i = 1, \dots, l,\ g_j(x) \neq 0,\ j = 1, \dots, k\}.$$

A basic quasi-algebraic formula over $\mathbb{Z}$ defines a basic quasi-algebraic set over $\mathbb{Z}$ in K^m for any field K.

A subset of K^m is *quasi-algebraic over R* if it is the union of a finite number of basic quasi-algebraic sets over R. Quasi-algebraic sets over R in K^m are closed under finite union, finite intersection and the operation of taking complements.

PROPOSITION 11. *Given n, m there is a finite set of basic quasi-algebraic formulas over $\mathbb{Z}$ such that: given any field K, $n \times m$ matrix A over K, and vector $b \in K^n$ then the linear equation $A(x) = b$ has a solution in K^m if and only if (A, b) is in the quasi-algebraic set in $K^{n \times m + n}$ defined by these formulas.*

PROOF. The system $A(X) = b$ has a solution if and only if there are k columns of A such that the $(n \times k)$ matrix B determined by them has rank k while the $n \times (k+1)$ matrix obtained by adjoining the column b also has rank k, $0 \leq k \leq m$.

This condition is expressed in terms of the determinants of the minors of A which are polynomial over $\mathbb{Z}$ in the coefficients of A. $\square$

COROLLARY 2. *Given m, n, and a vector of degrees $d = (d_1, \ldots, d_m)$, there is a finite set of basic quasi-algebraic formulas over $\mathbb{Z}$ such that for any algebraically closed field K, the system of equations*

$$f_1(x) = 0, \ldots, f_m(x) = 0, \ \deg\, f_i = d_i$$

has a solution in K^n if and only if the coefficients of the f_i lie in the quasi-algebraic set determined by these formulas.

PROOF. By the effective Nullstellensatz, the system $f_1(x) = 0, \ldots, f_m(x) = 0$ has no common zero if and only if there exist g_i, $i = 1, \ldots, m$ of degree $\leq C$ such that $\sum_{i=1}^{m} f_i g_i = 1$. This is a system of linear equations in the coefficients of the f_i and the above proposition finishes the proof. $\square$

THEOREM 8. *Let $K \subset L$ be algebraically closed fields. If* $\mathrm{P} = \mathrm{NP}$ *over K, then* $\mathrm{P} = \mathrm{NP}$ *over L.*

PROOF. It suffices to show that the machine M which decides Hilbert's Nullstellensatz over K in polynomial time decides it over L with the same polynomial time bounds.

Fix n, m and d. Let $K_{n,m,d}$ be the set of corresponding inputs of HN/K, and $L_{n,m,d}$ for HN/L. Thus $f \in K_{n,m,d}$ consists of m polynomials $f_1, \ldots, f_m$ of $K[t_1, \ldots, t_n]$ with degree $f_i = d_i$. The `yes` subset of $K_{n,m,d}$ will be denoted by $K_{n,m,d,o}$, and the `yes` subset of $L_{n,m,d}$ by $L_{n,m,d,o}$.

Assume M has two output nodes, `yes` and `no` and that the time bound for inputs of $K_{n,m,d}$ is T.

Consider a `yes` instance y of HN/L and let $N_{y,T}$ be the node of M in the orbit of y at time T.

Since $K_{n,m,d,o}$ and $L_{n,m,d,o}$ are defined by the same sets of basic quasi-algebraic formulas over $\mathbb{Z}$ and the node is determined by the basic quasi-algebraic formulas over K determined by the branch nodes in the orbit of y up to time T, Proposition 10 implies that there is a `yes` instance of $K_{n,m,d}$ at node $N_{y,T}$ at time T. Thus $N_{y,T}$ is the `yes` node.

The same argument applies to a `no` instance, interchanging `yes` and `no`. $\square$

8. Main Theorem, A Model Theoretic Proof of the Converse

In this section we give an alternate proof of Theorem 8 using model theoretic results and techniques. Assuming $K \subset L$ are algebraically closed fields, it suffices to prove the following two lemmas.

LEMMA 9. *If M is a polynomial time machine over K that outputs the value* 0 *or* 1 *when input an element of K^∞, then the same is true when K is replaced by L (and hence by any field extension of K).*

LEMMA 10. *If M is a time-bounded machine over K that decides* HN$/K$, *then the set of inputs to M from L^∞ that output the value* 1 *is exactly the set of* `yes` *instances of* HN$/L$.

Lemmas 9 and 10 follow easily from the **Model Completeness** (**Strong Transfer Principle**) of the theory of algebraically closed fields:

Suppose $K \subset L$ are algebraically closed fields and Φ is a first order sentence in the language of fields with constants from K. Then Φ is true when interpreted in K if and only if Φ is true when interpreted in L.

To prove Lemma 9, let p be the polynomial time bound for M over K and let H be the computing endomorphism of M over K. We apply the Strong Transfer Principle to each sentence Φ_n, $n > 0$ (seen easily to be writable as a first order sentence over K):

$$\forall y \exists z_0 \ldots \exists z_{p(n)} \exists w [z_0 = (1, y) \ \&_{k=1}^{p(n)} \ z_k = H(z_{k-1}) \ \& \ z_{p(n)} = (N, w) \\ \& \ (O(w) = 0 \text{ or } O(w) = 1)]$$

where $y = (y_1, \ldots, y_n)$ and $w = (w_1, \ldots, w_{p(n)})$.

The sentence Φ_n asserts that for each input to M of size n, the computation halts in time bounded by $p(n)$ with output value 0 or 1. Each sentence Φ_n is true in K, so each is true in L.

We use the same technique to prove Lemma 10. For each m, d, n let

$$f_1(y^1, x) = 0, \ldots, f_m(y^m, x) = 0$$

be the general system of m polynomial equations of degree d in n variables $x = (x_1, \ldots, x_n)$ and variable coefficients $y^i = ({y^i}_1, \ldots, {y^i}_l)$, $i = 1, \ldots, m$ (here l depends on d and n). Let $p(n)$ be a (not necessarily polynomial) time bound for M. We apply the Strong Transfer Principle to each sentence $\Phi_{m,d,n}$, $m, d, n > 0$:

$$\forall y^1 \ldots \forall y^m \{ \exists x (\&_{i=1}^m f_i(y^i, x) = 0) \Longleftrightarrow$$

$$\exists z_0 \ldots \exists z_{p(ml)} \exists w [z_0 = (1, (y^1, \ldots, y^m)) \ \&_{k=1}^{p(ml)} \ z_k = H(z_{k-1}) \ \& \ z_{p(ml)} = (N, w) \\ \& \ O(w) = 1]\}$$

The sentence $\Phi_{m,d,n}$ asserts that for each sequence of coefficients $y^1, \ldots, y^m$ (from the given field), the system $f_1(y^1, x) = 0, \ldots, f_m(y^m, x) = 0$ has a solution (in the given field) if and only if M with input $(y^1, \ldots, y^m)$ halts with output 1. Each such sentence is true in K, therefore each is true in L.

9. Additional comments and bibliographical remarks

The part of Theorem 1 asserting P = NP over $\mathbb{C}$ implies P = NP over $\overline{\mathbb{Q}}$, is proved here for the first time. The same is true for the Witness Theorem of Section 3 and Proposition 9 as well. The converse in Theorem 1 is due to Michaux [1994] who gave a model theoretic proof similar to ours. Much of the rest is from [Shub and Smale TA]. In particular Theorems 2 and 6 are proved in that paper. A version of Theorem 5 is used in [Shub 1993].

The function τ is a version of standard concepts in algebraic complexity theory as for example in Heintz and Morgenstern [1993] There is also a simpler function without multiplication in the old subject of additive chains (see Scholz [1937] and Knuth [1981]). Some results on τ are in [de Melo and Svaiter TA] and in [Moreira 1995].

The relationship of the open problem in Section 1 to factoring was first pointed out to us by Don Coppersmith. For related results on factoring see [Strassen 1976]. For the necessary material on heights needed in Section 3 and its appendix see [Lang 1991]. Lang [1993] is a good background in general for the algebra and in particular for the field theory (e.g. Lemma 4 of Section 4).

REMARK 3. Michaux [1994] also proves that if $\mathbb{C} \subset K \subset L$ where K is algebraically closed, then $\mathrm{P} = \mathrm{NP}$ over L implies $\mathrm{P} = \mathrm{NP}$ over K.

REMARK 4. Bruno Poizat has pointed out the following result.

THEOREM 9. *If* $\mathrm{P} = \mathrm{NP}$ *over an infinite field* K*, then* K *is algebraicaly closed.*

The proof is based on a result of Angus Mcintyre [1971] stating that if an infinite field admits elimination of quantifiers then it is algebraicaly closed. Then the idea is that if $\mathrm{P} = \mathrm{NP}$ over K, HN/K is solved by a time bounded machine over K. Then it can be shown that K admits elimination of quantifiers. An analogue of Mcintire's result to ordered and valued fields can be found in [Mcintyre, McKenna, and van den Dries 1983].

REMARK 5. It follows from Theorem 1 and the previous remark that the problem $\mathrm{P} = \mathrm{NP}$ over K reduces to the single problem $\mathrm{P} = \mathrm{NP}$ over $\overline{\mathbb{Q}}$ in characteristic zero.

Open Problem Does a similar result prevail in characteristic $p \neq 0$? And for real fields?

References

BLUM, L., M. SHUB, and S. SMALE (1989). On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the Amer. Math. Soc. 21*, 1–46.

DE MELO, W. and B. SVAITER (TA). The cost of computing integers. To appear in Proceedings of the Amer. Math. Soc..

HEINTZ, J. and J. MORGENSTERN (1993). On the intrinsic complexity of elimination theory. *Journal of Complexity 9*, 471–498.

KNUTH, D. (1981). *The Art of Computer Programming*, Volume 2. Addison-Wesley.

LANG, S. (1991). *Diophantine Geometry*. Springer-Verlag.

LANG, S. (1993). *Algebra, 3rd edition*. Addison-Wesley.

MCINTYRE, A. (1971). On ω_1-categorical theories of fields. *Fund. Math. 71*, 1–25.

MCINTYRE, A., K. MCKENNA, and L. VAN DEN DRIES (1983). Elimination of quantifiers in algebraic structures. *Adv. in Math. 47*, 74–87.

MICHAUX, C. (1994). $\mathrm{P} \neq \mathrm{NP}$ over the nonstandard reals implies $\mathrm{P} \neq \mathrm{NP}$ over $\mathbb{R}$. *Theoretical Computer Science 133*, 95–104.

MOREIRA, C. (1995). On asymptotical estimates for arithmetical cost functions. Preprint.

SCHOLZ, A. (1937). Aufgabe 253. *Jahresber. Deutsch. Math.-Verein. 47*, 41–42.

SHUB, M. (1993). Some remarks on Bezout's theorem and complexity theory. In M. Hirsch, J. Marsden, and M. Shub (Eds.), *From Topology to Computation: Proceedings of the Smalefest*, pp. 443–455. Springer-Verlag.

Shub, M. and S. Smale (TA). On the intractability of Hilbert's Nullstellensatz and an algebraic verion of "P = NP". To appear in *Duke J. of Math.*

Strassen, V. (1976). Einige resutate uber berechungskomplexitat. *Jber. Deutsch. Math.-Verein. 78*, 1–8.

Lenore Blum, International Computer Science Institute, 1947 Center St., Berkeley, CA 94704, U.S.A., and Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, CA 94720

E-mail address: `lblum@@icsi.berkeley.edu or lblum@@msri.org`

Felipe Cucker, Universitat Pompeu Fabra, Balmes 132, Barcelona 08008, Spain

E-mail address: `cucker@@upf.es`

Mike Shub, IBM T. J. Watson Research Center, Yorktown Heights, NY 10598-0218, U.S.A.

E-mail address: `shub@@watson.ibm.com`

Steve Smale, Department of Mathematics, City University of Hong Kong, Tat Chee Ave, Kowloon, Hong Kong

E-mail address: `masmale@@sobolev.cityu.edu`