Straight Line Programs and Torsion Points on Elliptic Curves *

Qi Cheng†

Abstract

In this paper, we show several connections between the L-conjecture, proposed by Bürgisser [3], and the boundedness theorem for the torsion points of elliptic curves. Assuming the WL-conjecture, which is a much weaker version of the L-conjecture, a sharper bound is obtained for the number of torsion points over extensions of k on an elliptic curve over a number field k, which improves Masser's result [10]. It is also shown that the Torsion Theorem for elliptic curves follows directly from the WL-conjecture. Since the current proof of the Torsion Theorem for elliptic curves uses considerable machinery from arithmetic geometry, and the WL-conjecture differs from the trivial lower bound only at a constant factor, this result provides an interesting example where increasing the constant factor in a trivial lower bound of straight-line complexity is very difficult. Our result suggests that the Torsion Theorem may be viewed as a lower bound result in algebraic complexity, and a lot can be learned from the proof of the Uniformly Boundedness Theorem to construct the proofs the WL-conjecture and even the L-conjecture..

1 Introduction

The intriguing relationship between the number of distinct rational roots of a polynomial and the straight-line complexity of the polynomial has attracted a lot of attention recently. Lipton [9] proved that polynomials with many distinct rational roots can not be evaluated by a short straight-line program, unless that the integer factorization is easy. This observation was explicitly formulated by Blum, Cucker, Shub and Smale [1] in the so called τ-conjecture. Let f be any univariate integral polynomial in x. The conjecture claims that

$$z(f) \leq (\tau(f) + 1)^c,$$

where $z(f)$ is the number of distinct rational roots of f, $\tau(f)$ is the length of the shortest straight-line program computing f from 1 and x, and c is an absolute constant. They showed a rather

*The preliminary version of this paper appeared as Qi Cheng, Some Remarks on the L-conjecture, in the Proceeding of 13th Annual International Symposium on Algorithms and Computation (ISAAC), Lecture Notes in Computer Science 2518, Springer, 2002.

†School of Computer Science, the University of Oklahoma, Norman, OK 73019, USA. Email: qcheng@cs.ou.edu.
This research is partially supported by NSF Career Award CCR-0237845.

surprising fact that this conjecture implies that $\mathbf{N}P_{\mathbf{C}} \neq \mathbf{P}_{\mathbf{C}}$ [1]. Proving the τ-conjecture (or disproving it if it is false) is the fourth problem in the Smale's list [19] of the most important problems for the mathematicians in the 21st century. The original title in [19] was "integer zeros of a polynomial of one variable". It is believed that solving this problem is very hard, and even partial solutions will have great impacts on researches of algebraic geometry and computational complexity. We are not aware of any significant progress towards proving this conjecture.

In [3], Bürgisser raised a question whether a similar conjecture is true for polynomials over any number field k when $\tau(f)$ is replaced by $L(f)$, which is the length of the shortest straight-line program computing $f(x)$ from x and any constants. More precisely, it is conjectured that

Conjecture 1 *(L-conjecture) Given a number field k, there exists a constant c depending only on k, such that for any $f \in k[x]$,*

$$N_{d,k}(f) \leq (L(f) + d)^c,$$

where $N_{d,k}(f)$ is the number of distinct irreducible factors of f over k with degree at most d.

It is easy to see that the special case of the L-Conjecture where $d = 1$ and $k = \mathbf{Q}$ implies the τ-Conjecture. These two problems are sometimes categorized as belonging to algebraic complexity, as opposed to classical complexity theory, because quantities like $\tau(f)$ and $L(f)$ measure just the number of arithmetic operations and do not take into account the size of the underlying operands. However, algebraic complexity is intimately connected with classical complexity: The complexity classes $\mathbf{P}$ and $\mathbf{NP}$ (not to mention many others) can be defined relative to an arbitrary field [1], and this generalization allows one to use a larger arsenal to attack the problems of classical complexity.

In particular, in the BCSS model of computation over an arbitrary ring [1], Turing complexity becomes a special case of BCSS complexity by setting the underlying field to be $\mathbf{F}_2$. When the underlying field is $\mathbf{C}$, we obtain the usual setting of algebraic complexity, and the complexity classes $\mathbf{P}_{\mathbf{C}}$ and $\mathbf{NP}_{\mathbf{C}}$ are the corresponding analogues of the familiar classes $\mathbf{P}$ and $\mathbf{NP}$. More to the point, it is known that $\mathbf{NP} \not\subseteq \mathbf{BPP}$ implies that $\mathbf{P}_{\mathbf{C}} \neq \mathbf{NP}_{\mathbf{C}}$ [8], and assuming the Generalized Riemann Hypothesis (GRH), it is known that $\mathbf{NP}_{\mathbf{Z}}$ is in $\mathbf{RP}^{\mathbf{NP}}$ [6, 7]. The assumption of GRH in the latter result can be replaced by more plausible hypotheses [16]. Although a lot of wonderful results have been obtained recently (See [1] for a survey), proving lower bounds in algebraic complexity seems to be not easier than in the classical setting.

In this paper, we examine the implications of the L-conjecture in algebraic geometry and number theory. In particular, we derive new, significantly sharper estimates in the the theory of elliptic curves, conditional on the truth of a weakening of the L-conjecture. This also implies the possibility of using elliptic curves to give new examples of polynomials of low complexity with many roots in low degree number fields.

1.1 Summary of results

We study how hard it is to prove the L-conjecture. To this end, we consider a much weaker statement. We call it WL-conjecture, standing for *weaker* L-conjecture.

Conjecture 2 *(WL-conjecture) Let k be a number field. For any univariate polynomial $f \in k[x]$, there exists three constants $c_1 > 0$, $0 \leq c_2 < 1/72$ and $c_3 > 0$ such that*

$$N_{d,k}(f) \leq c_1 2^{c_2 L(f)} d^{c_3},$$

where $N_{d,k}(f)$ is the number of distinct irreducible factors of f over k with degree at most d. In particular,

$$z_k(f) \leq c_1 2^{c_2 L(f)},$$

where $z_k(f)$ is the number of distinct roots over k of f.

Note that the WL-conjecture is much weaker than the L-conjecture, as in the WL-conjecture the number of zeros is bounded from above by an exponential function of $L(f)$, while in the L-conjecture the number of zeros is bounded from above by a polynomial function of $L(f)$. The relationship between the τ-conjecture and the WL-conjecture, however, is not clear to us. We believe that the τ-conjecture is much stronger than the WL-conjecture.

The other way to view the WL-conjecture is that it states a lower bound of the straight-line complexity:

$$L(f) \geq c_3 \log z_k(f) + c_4$$

where $c_3 > 72$ and c_4 are two constants depending only on k. Note that $L(f) \geq \log z_k(f)$ is obviously true over any field k because the degree of f is at most $2^{L(f)}$. Unlike the L-conjecture, the WL-conjecture differs from the trivial lower bound only at a constant factor. Nonetheless, we show that if the WL-conjecture is true, then Masser's results on the number of torsion points on an elliptic curve [10] can be improved. His results are summarized as follows.

Proposition 1 *Let k be a number field and $E : Y^2 = 4x^3 - g_2 x - g_3$ be an elliptic curve over k. There is a positive effective constant c, depending only on the degree of k, such that the torsion subgroup of $E(K)$ with $[K : k] = D$ has cardinality at most $c\sqrt{w}D(w + \log D)$, where w is the absolute logarithmic height of $(1 : g_2 : g_3)$ in $\mathbf{P}^2_k$.*

We can prove:

Theorem 1 *Use the notations in the above proposition. The cardinality of the torsion subgroup of $E(K)$ is at most $c_4 D^{c_5}$ where c_4 and c_5 are constants depending only on k, if the WL-conjecture is true in the number field k.*

Note that in Theorem 1, the constants are only dependent on the number field k, and are independent of the curve. The bound in Theorem 1 is lower than Masser's bound when k is fixed and w is large. For example, if $w > 2^D$, Masser's bound is exponential in D but ours is polynomial in D.

We then show the following famous Torsion Theorem is a direct consequence of the WL-conjecture.

Theorem 2 *(Torsion Theorem for Elliptic Curves) Let E be an elliptic curve defined over a number field k. Then the number of torsion points in $E(k)$ is bounded from above by a constant depending only on k.*

This theorem is a part of the following result, also known as the Uniformly Boundedness Theorem (UBT).

Theorem 3 *(Strong Torsion Theorem for Elliptic Curves) Let E be an elliptic curve defined over a number field k, then the number of torsion points in $E(k)$ is bounded from above by a constant depending only on $m = [k : \mathbf{Q}]$.*

We will prove the theorem in Section 5. From the proof, it is easy to see that if c_1 in the WL-conjecture depends only on $[k : \mathbf{Q}]$, the UBT follows from the WL-conjecture. All the results in this paper are obtained by studying the division polynomial $P_n(x)$. We show that if there is one point on an elliptic curve $E(k)$ with order n, then the division polynomial $P_n(x)$ must have at least $(n-1)/2$ distinct solutions in k. On the other hand, $P_n(x)$ can be computed by a straight-line program of length at most $72 \log n + 60$. The WL-conjecture is violated if n is bigger than a certain constant.

2 Motivations and related works

It is observed that current mathematical techniques have very limited capability to prove lower bounds. This motivates a line of research on this phenomenon. Relativizing proof techniques were shown to be too weak to separate several major complexity classes such as **P** and **NP**. Razborov and Rudich [14] showed that the natural proofs, arguably including all the proof techniques in current circuit complexity research, will not produce a separation either. In this paper, under the context of algebraic complexity theory, we examine the power of the *elementary proofs*. The proofs of mathematical statements are usually categorized into two kinds: elementary and analytical. An elementary one uses direct reasoning and relys on the combinatorial arguments. An analytical proof, on the other hand, uses the tools from complex analysis. The modular forms are sometimes involved in analytical proofs. The famous examples of analytical proofs include the proofs of the Fermat Last Theorem and the UBT. These theorems are believed not to have elementary proofs. To the contrary, the results in theoretical computer science are usually obtained by elementary methods.

Proving the Strong Torsion Theorem for elliptic curves is one of the major achievements in number theory and algebraic geometry recently. In this paper, we find surprising connections between the torsion theorem and the WL-conjecture. We show that the number of torsion points over number fields is severely limited if the WL-conjecture is true, hence the Torsion Theorem follows directly from the WL-conjecture. Our argument is simple and elementary. It is quite astonishing, considering how weak the WL-conjecture is and how much effort people have put into proving the Torsion Theorem.

Although the UBT has been proved, this result is still interesting. The $(W)L$-conjecture claims that there is no short straight-line program to compute a polynomial which has many distinct roots in a fixed number field. This is a typical lower bound result in computational complexity. It is a common belief that we lack techniques to obtain lower bounds in computational complexity. Our results add one more example to this phenomenon and shed light on its reason. They indicate that proving a better constant factor in the trivial straight-line complexity lower bound is very hard, hence illustrate the difficulties of proving a superpolynomial lower bound and proving the hardness of factoring.

Our result clearly indicates that in order to prove the WL-conjecture, we may need to look at very deep techniques in algebraic geometry, which are not apparently related to the theory of computational complexity. Since it is unlikely that the Torsion Theorem for elliptic curves has an elementary proof, our result implies that even improving the constant factor in a trivial straight-line complexity lower bound requires the advanced analytical tools.

2.1 Related work

Boneh [2] observed the connections between the straight-line complexity of polynomials and the bound of the number of torsion points over a number field on an abelian variety. In his report, however, no bound better than what is currently known was obtained for the number of torsion points on elliptic curves. And he assumed the hardness of integer factorization, which essentially means that for some number field k and any constant c,

$$\tau(f) \geq (\log z_k(f))^c,$$

if $\tau(f)$ is sufficiently large. The condition that the integer factorization is hard seems stronger than the WL-conjecture. In our paper, we obtain a better bound for the number of torsion points over extension fields on an elliptic curve and improve Masser's results, which is the best estimation currently known. We also assume the WL-conjecture to study the property of the torsion points.

Other than $\tau(f)$ and $L(f)$, there is another important algebraic complexity measurement, additive complexity, denoted by $\sigma(f)$, which counts only the number of additions in the straight line program computing the polynomial f. The study of the relationship between the number of real (or rational) roots and the additive complexity of a polynomial has a longer history. Grigorev [4] and Risler [15] proved that the number of distinct real roots of f is less than $C^{\sigma(f)^2}$ for an absolute constant C. This result has been dramatically improved recently by Rojas [17], who

obtained an upper bound of $O(e^{\sigma(f)\log\sigma(f)})$ for the number of distinct rational roots of f. When $\sigma(f)$ is much less than $L(f)$, this bound is better than the trivial bounds of $2^{\tau(f)}$ or $2^{L(f)}$.

The rank of the Mordell-Weil group of an abelian variety and its torsion subgroup are two central topics in the study of arithmetic of algebraic curves. Although the research on the rank shows only slow progress, remarkable achievements have been made in the research on torsion subgroup, culminating in the recent proof of the Uniform Boundedness Theorem(UBT).

First we briefly review the history. The Torsion Theorem in some special cases was conjectured by Beppo Levi as early as the beginning of the 20th century. Mazur proved the case of $k = \mathbf{Q}$ in his landmark paper [11] in 1977. He also gave the bound (which is 16) explicitly. Mazur's result requires a deep research on modular forms. Little progress was made on the torsion theorem until in 1992 Kamienny announced his ground-breaking result [5]. He settled the cases when k is any quadratic number field, and suggested the techniques to attack the whole conjecture. His method led to the proofs of the Strong Torsion Theorem for $d \leq 14$. It was Merel [12] who finally managed to prove the Strong Torsion Theorem for all the positive integers d in 1996. The following effective version of the UBT was proved by Parent [13].

Proposition 2 *Let $\mathcal{E}$ be an elliptic curve over a number field K. Denote the order of the torsion subgroup of $E(K)$ by N. Let $d = [K : \mathbf{Q}]$. Suppose that p is a prime divisor of N, and p^n is the largest power of p dividing N. We have*

$$\begin{aligned} p &\leq (1 + 3^{d/2})^2, \\ p^n &\leq 65(3^d - 1)(2d)^6. \end{aligned}$$

3 Straight-line programs of polynomials

A straight-line program of a polynomial over a field k is a sequence of ring operations, which outputs the polynomial in the last operation. Formally,

Definition 1 *A straight-line program of a polynomial $f(x)$ is a sequence of instructions. The i-th instruction is*

$$v_i \leftarrow v_m \circ v_n \quad \text{or} \quad v_i \leftarrow c_i$$

where $\circ \in \{+, -, *\}$, $i > m$, $i > n$, c_i is x or any constant in k, and the last variable v_n equals to $f(x)$. The length of the program is the number of the instructions. The length of the shortest straight-line program of $f(x)$ is called the straight-line complexity of $f(x)$ and is denoted by $L(f)$. The minimum number of additions and substractions in any straight line program to compute f is called the additive complexity *of f and is denoted by $\sigma(f)$.*

The polynomial x^n has a straight-line complexity at most $2\log n$. In some cases, a straight-line program is a very compact description of a polynomial. It can represent a polynomial with a huge number of terms in a small length. For example, the polynomial $(x+1)^n$ can be computed using

the repeated squaring technique and hence has a straight-line complexity at most $2\log n$, while it has $n+1$ terms.

The number of distinct roots over a number field k of a polynomial with small straight-line complexity seems limited. For example, the equation $(x+1)^n = 0$ has only one distinct root. The equation $x^n - 1 = 0$ has n distinct roots, but if we fix a number field k and let n grow, the number of distinct roots in k will not increase. The relationship between the number of distinct roots of a polynomial f over a number field and $L(f)$ is not well understood.

4 Division polynomials

An elliptic curve E over a field k is a smooth cubic curve. If the characteristic of k is neither 2 nor 3, we may assume that the elliptic curve is given by an equation of the form

$$y^2 = x^3 + ax + b, \qquad a, b \in k.$$

Let K be an extension field of k. The solution set of the equation in K, plus the infinity point, forms an abelian group. We use $E(K)$ to denote the group.

We call a point *torsion* if it has a finite order in the group. The x-coordinates of the torsion points of order $n > 3$ are the solutions of $P_n(x)$, the n-th division polynomial of E. The polynomial $P_n(x)$ can be computed recursively. The recursion formula can be found in many papers, e.g. [18]. For completeness we list them below.

$$\begin{aligned}
P_1 &= 1 \\
P_2 &= 1 \\
P_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
P_4 &= 2(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
P_{4n+1} &= 16(x^3 + ax + b)P_{2n+2}P_{2n}^3 - P_{2n-1}P_{2n+1}^3 \\
P_{4n+2} &= P_{2n+1}(P_{2n+3}P_{2n}^2 - P_{2n-1}P_{2n+2}^2) \\
P_{4n+3} &= P_{2n+3}P_{2n+1}^3 - 16(x^3 + ax + b)P_{2n}P_{2n+2}^3 \\
P_{4n+4} &= P_{2n+2}(P_{2n+4}P_{2n+1}^2 - P_{2n}P_{2n+3}^2)
\end{aligned}$$

Note that our division polynomials are a little different from the division polynomial $\psi_n(x, y)$ in some literatures, for example Silverman's book [18]. When n is even, $P_n = \psi_n$. When n is odd, $P_n = (2y)^{-1}\psi_n$. We use P_n because it is a univariate polynomial and the computation of P_n does not involve division.

Lemma 1 $L(P_n) \le 72\log n + 60$.

Proof: We deploy the dynamical programming technique to construct the straight-line program. Before evaluating $P_n(x)$, we need to evaluate up to 5 division polynomials with indices

around $n/2$, according to the recursion. For the same reason, in order to compute these 5 or less division polynomials, we need to compute up to 8 division polynomials with indices about $n/4$. However, this does not mean that the number of division polynomials we need to evaluate in each recursion level grows unlimitedly as the level increases. In fact, in order to evaluate the list of division polynomials $P_i(x), P_{i+1}(x), \cdots, P_{i+j}(x)$, we only need to evaluate $P_{\lceil i/2 \rceil - 2}, P_{\lceil i/2 \rceil - 1}, \cdots, P_{\lfloor (i+j)/2 \rfloor + 1}, P_{\lfloor (i+j)/2 \rfloor + 2}$. If $j > 7$, the latter list is shorter than the former one. On the other hand, if $j \leq 7$, then the latter list contains at most 8 polynomials. Hence if we want to evaluate $P_n(x)$, we only go through $\log n$ recursion levels and evaluate at most $8 \log n$ many $P_i(x)$. Evaluating any $P_i(x)$ requires at most 9 ring operations from the division polynomials in the previous level. The overhead of computing P_1, P_2, P_3, P_4 and $16(x^3 + ax + b)$ is less than 60 steps. The total number of arithmetic operations is thus less than $72 \log n + 60$. □

Corollary 1 $\sigma(P_n) \leq 8 \log n + 12$.

Lemma 2 *If $P_n(x)$ has one solution in K which is an x-coordinate of a point P in $E(K)$ of order n, then it must have at least $(n-1)/2$ distinct solutions in K.*

Proof: If there exists a point P in $E(K)$ with order n, then the points $P, 2P, 3P, \cdots, (n-1)P$ are distinct, none of them is 0 (the point at infinity of $E(K)$) and all of them have orders dividing n. The x-coordinates of these points are in K and they are the roots of $P_n(x)$. Any pair of points have different x-coordinates, unless the sum of these two points are 0. If n is odd, we have exactly $(n-1)/2$ distinct x-coordinates. If n is even, we have $n/2$ distinct x-coordinates. □

5 Outlines of proofs

We first prove Theorem 1.

Proof: Suppose there is a point $P \in E(K)$ of order n. Denote the x-coordinates of $P, 2P, 3P, \cdots, (n-1)P$ by $x_1, x_2, \cdots, x_{n-1}$ respectively. According to Lemma 2 there are at least $(n-1)/2$ different numbers in $x_1, x_2, \cdots, x_{n-1}$. All of them are the roots of the n-th division polynomial $P_n(x)$ of the curve E. We also know that the minimal polynomial over k of $x_i \in K$, $1 \leq i \leq n-1$, has degree at most $[K : k] = D$. Hence there are at least $(n-1)/(2D)$ factors of $P_n(x)$ which have degrees less than or equal to D. According to the L-conjecture, we have

$$(n-1)/(2D) \leq N_{D,k}(P_n) \leq c_1 2^{c_2 L(P_n)} D^{c_3} \leq c_1 2^{c_2(72 \log n + 60)} D^{c_3}.$$

This gives us $n \leq c_4 D^{c_5}$ for a constant c_4 and c_5 independent of the curve E. □

It is interesting to note that if we let the bound in WL-conjecture grow exponentially not just with $L(f)$ but also with D, then we cannot obtain a better bound than Masser did. This suggests an interesting parametrized phenomenon in algebraic complexity.

Now we prove the Torsion Theorem from the WL-conjecture. Suppose that an elliptic curve E/K has a point with order n in K. The division polynomial $P_n(x)$ has at least $(n-1)/2$ distinct solutions over K, i.e. $z_K(P_n) \geq (n-1)/2$. But $P_n(x)$ can be computed by a straight-line program of length at most $72 \log n + 60$, i.e. $L(f) \leq 72 \log n + 60$. If the WL-conjecture is true, we have

$$(n-1)/2 \leq z_K(P_n) \leq c_1 2^{c_2 L(P_n)} \leq c_1 2^{c_2(72 \log n + 60)},$$

which is possible only if

$$n \leq (3c_1 2^{60c_2})^{\frac{1}{1-72c_2}}.$$

The c_1 and c_2 depend only on k. This argument shows that the Torsion Theorem is the direct consequence of the WL-conjecture. Similar arguments show that if in the WL-conjecture c_1 depends only on $[k : \mathbf{Q}]$, then the Strong Torsion Theorem follows from the WL-conjecture as well.

It is easy to see that in Theorem 1, the assumption of WL-conjecture can be replaced by a bound in additive complexity, namely, $N_{d,k} = O(2^{c_6 \sigma(f)} d^{c_7})$ for $c_6 < 1/8$. This bound also implies the Torsion Theorem.

6 Conclusion

In this paper, we improved Masser's upper bound of the number of torsion points over extension number fields on an elliptic curve assuming the WL-conjecture. We showed that the Torsion Theorem is a direct consequence of the WL-conjecture.

Acknowledgment

We thank two anonymous referees for their helpful comments.

References

[1] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and Real Computation*. Springer-Verlag, 1997.

[2] Dan Boneh. Studies in computational number theory with applications to cryptography. Technical report, Princeton University, 1996.

[3] Peter Burgisser. On implications between P-NP-Hypotheses: Decision versus computation in algebraic complexity. In *Proceedings of MFCS*, volume 2136 of *Lecture Notes in Computer Science*, 2001.

[4] D. Yu. Grigorev. Lower bounds in the algebraic complexity of computations. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 118:25–82, 1982. The theory of the complexity of computations, I.

[5] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones Mathematicae*, 109:221–229, 1992.

[6] Pascal Koiran. Hilbert's nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996.

[7] Pascal Koiran. Hilbert's nullstellensatz is in the polynomial hierarchy. Technical Report 96-27, DIMACS, 1996.

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

[9] Richard J. Lipton. Straight-line complexity and integer factorization. In *Algorithmic number theory (Ithaca, NY, 1994)*, pages 71–79, Berlin, 1994. Springer.

[10] D. W. Masser. Counting points of small height on elliptic curves. *Bull. Soc. Math. France*, 117(2):247–265, 1989.

[11] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44, 1978.

[12] L. Merel. Bounds for the torsion of elliptic curves over number fields. *Invent. Math.*, 124(1-3):437–449, 1996.

[13] P. Parent. Effective bounds for the torsion of elliptic curves over number fields. *J. Reine Angew. Math*, 506:85–116, 1999.

[14] Alexander A. Razborov and Steven Rudich. Natural proofs. In *Proc. 26th ACM Symp. on Theory of Computing*, 1994.

[15] J. J. Risler. Additive complexity and zeros of real polynomials. *SIAM J. Comput.*, 14(1):178–183, 1985.

[16] J. Maurice Rojas. Dedekind zeta functions and the complexity of hilbert's nullstellensatz. http://arxiv.org/abs/math/0301111, 2003.

[17] J. Maurice Rojas. A direct ultrametric approach to additive complexity and the shub-smale tau conjecture. http://arxiv.org/abs/math/0304100, 2003.

[18] J.H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[19] S. Smale. Mathematical problems for the next century. In V. Arnold, M. Atiyah, P. Lax, and B. Mazur, editors, *Mathematics: Frontiers and Perspectives, 2000*. AMS, 2000.