Some Remarks on the L-conjecture

Qi Cheng*

Abstract

In this paper, we show several connections between the L-conjecture, proposed by Burgisser [3], and the boundedness theorem for the torsion of elliptic curves. Assuming the L-conjecture, a sharper bound is obtained for the number of torsions over extensions of k on an elliptic curve over a number field k, which improves Masser's result [6]. It is also shown that the Torsion Theorem for elliptic curves [10] follows directly from the WL-conjecture, which is a much weaker version of the L-conjecture. Since the WL-conjecture differs from the trivial lower bound only at the constant factor, this result provides an interesting example where increasing the constant factor in a trivial lower bound of straight-line complexity is difficult and important.

1 Introduction

The relation between the number of distinct rational roots of a polynomial and the straight-line complexity of the polynomial has been studied by several researchers. Lipton [5] proved that polynomials with many distinct rational roots can not be evaluated by a short straight-line program, unless 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. It is rather surprising that they showed that this conjecture implies that $NP_{\mathbf{C}} \neq P_{\mathbf{C}}$. Proving τ-conjecture (or disproving it

*School of Computer Science, the University of Oklahoma, Norman, OK 73019, USA. Email: qcheng@cs.ou.edu

in case that it is false) is also known as Smale's 4th problem "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. For Smale's list of the most important problems for the mathematicians of 21st century, see [12].

In [3], a question was raised 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 $f \in k[x]$,*

$$N_d(f) \leq (L(f) + d)^c,$$

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

It is easy to see that the L-conjecture over $\mathbf{Q}$ implies the τ-conjecture. In this paper, we examine the implications of L-conjecture in algebraic geometry and number theory. In particular, we derive some results from this conjecture. These results cover some fundamental problems in number theory and algebraic geometry. Some of them are still open. Those which have been settled require the most advanced mathematical tools.

1.1 Summary of results

First we show that if the L-conjecture is true, then Masser's result [6] on the number of torsions on an elliptic curve can be improved. His results are summarized as follows.

Proposition 1 *Let k be a number field and $E : Y^2 = 4x^3 - g_2x - g_3$ 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 prove the following theorem:

Theorem 1 *Use the notations in the above proposition. The cardinality of the torsion subgroup of $E(K)$ is at most $c_1D^{c_2}$ where c_1 and c_2 are constants depending only on k, if the L-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 our bound is polynomial in D.

We then 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 two constants $c_1 > 0$ and $0 \leq c_2 < 1/72$ such that*

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

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

Not only the WL-conjecture is a special case of L-conjecture, but also it is much weaker than the L-conjecture, as in the WL-conjecture the number of zeros is bounded from above by an exponential function in $L(f)$ while in L-conjecture the number of zeros is bounded from above by a polynomial function in $L(f)$. The other way to view the WL-conjecture is that it states a lower bound of 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 the constant factor. Nevertheless, we show that the WL-conjecture is hard to prove in the sense that 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 torsions 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 torsions in $E(k)$ is bounded from above by a constant depending only on $m = [k : \mathbf{Q}]$.*

We can also prove 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 showed 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.

1.2 Related work

Boneh [2] also observed the connections between the straight-line complexity of polynomials and the bound of torsions over a number field on an abelian variety. In his report, no bound better than currently known was obtained for the number of torsions on elliptic curves. And he assumed the hardness of integer factorization, which essentially means that for any 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-conjectre. 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 torsions. Our results 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.

2 Motivations

The Torsion Theorem and the Strong Torsion Theorem for elliptic curves are very important in number theory and algebraic geometry. The Strong Torsion Theorem has been settled recently. The proof of these theorems, even in the case of the Torsion Theorem, is by no means easy. Having said this, we agree that there is no quantitive measurement on how difficult a mathematical statement can be proved. But certainly if a statement was open for years and was tried by a lot of researchers, even though it was solved eventually, we can safely say that this theorem is hard to prove. In case of the Torsion Theorem for elliptic curves, it is impossible to prove it

without deploying the most advanced tools in modern number theory and algebraic geometry.

In this paper, we find surprising connections between the torsion theorem and the WL-conjecture. We show that the number of torsions over number fields will be 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, our result is still interesting. First it indicates what a future proof of the WL-conjecture looks like if it exists. 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.

Our result clearly indicates that in order to prove the WL-conjecture, we have to look at the modular form and some highly advanced tools in algebraic geometry, which are not apparently related to the theory of computational complexity. There should be no elementary proof of the WL-conjecture, unless the Torsion Theorem can be proved in an elementary way. 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.

Secondly, 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. The Torsion Theorem may be viewed as a lower bound result in computational complexity. Although we don't believe that the Torsion Theorem is equivalent to the WL-conjecture, we think that we can learn a lot from the proof of UBT to construct the proofs the WL-conjecture and even the L-conjecture.

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*

$$v_i \leftarrow v_m \circ v_n \quad or \quad v_i \leftarrow c_i$$

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 denote by $L(f)$.

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, the number of distinct roots in k will not increase even if we increase n. The relation 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 torsions 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 a lot of literatures. 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 the Silverman's book [11]. 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 $L(P_n) \leq 72 \log n + 60$.

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 $8 \log n$ number of $P_i(x)$'s. Evaluating any $P_i(x)$ requires at most 9 more 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 $72 \log n + 60$. □

Lemma 2 *If $P_n(x)$ has one solution in K which is a 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 the infinity point 0 and all of them have orders dividing n. The x-coordinates of these points are in K and they are the roots of $P_n(x)$. Two 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

5.1 Improving Masser's bound

Now we are ready to 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

$$(n-1)/(2D) \leq N_D(P_n) \leq (L(P_n) + D)^c \leq (72 \log n + 60 + D)^c.$$

This gives us $n \leq c_1 D^{c+2}$ for a constant c_1 independent of the curve E. □

5.2 Proving the Torsion Theorem from the WL-conjecture

The rank and torsion of the Mordell-Weil group of an abelian variety are two central topics in the study of algebraic geometry. Although the research on the rank shows only slow progress, remarkable achievements have been made

in the research on torsion, 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 [7] in 1977. He also gave the bound 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 [4]. 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 [8] 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 [9].

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*

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

Now we start to prove the Torsion Theorem from the WL-conjecture. Suppose 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. $z(P_n) \geq (n-1)/2$. 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

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

which is possible only if

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

The c_1 and c_2 in the right hand side 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.

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 L-conjecture. We showed that the Torsion Theorem is a direct consequence of the WL-conjecture, hence there is no elementary proof of the WL-conjecture, unless there is an elementary proof of the Torsion Theorem.

Although the Torsion Theorem has been proved, we believe that our second result is still interesting, because it shows that an elementary proof of the WL-conjecture unlikely exists by the reduction technique, which was widely used in computer science to show a problem is easier than the other problem. Our results strongly suggest that in order to construct a proof of the $(W)L$-conjecture, we should learn from the proof of the Torsion Theorem.

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

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

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

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

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

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

[10] Alice Silverberg. Open questions in arithmetic algebraic geometry. In *Arithmetic Algebraic Geometry(Park City, UT, 1999)*, volume 9 of *Institute for Advanced Study/Park City Mathematics Series*, pages 83–142. American Mathematical Society, 2001.

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

[12] 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.