On Computing Algebraic Functions using Logarithms and Exponentials

Dima Grigoriev[1], Michael Singer[2], and Andrew Yao[3]

Abstract

Let ρ be a set of algebraic expressions constructed with radicals and arithmetic operations, and which generate the splitting field F of some polynomial. Let $N_\beta(\rho)$ be the minimum total number of root-takings and exponentiations used in any straightline program for computing the functions in ρ by taking roots, exponentials, logarithms, and performing arithmetic operations. In this paper it is proved that $N_\beta(\rho) = \nu(G)$, where $\nu(G)$ is the minimum length of any cyclic Jordan-Hölder tower for the Galois group G of F. This generalizes a result of Ja'Ja' [1], and shows that the inclusion of certain new primitives, such as taking exponentials and logarithms, does not improve the cost of computing such expressions as compared with programs which use only root-takings.

[1]Departments of Computer Science and Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802.

[2]Department of Mathematics, North Carolina State University, Raleigh, North Carolina 27695-8205.
Partially supported by NSF Grant DMS 90-24624.

[3]Department of Computer Science, Princeton University, Princeton, New Jersey 08544.

1 Introduction

The question of how efficiently one can evaluate expressions such as $\left(\sum_{1\le i<j\le n}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}\right)/\binom{n}{2}$, the *mean distance* among n points in the plane, was raised in Shamos and Yuval [8]. A systematic study of this question was given in Pippenger [6,7]. Let ρ be a family of algebraic expressions constructed from indeterminates using radicals and arithmetic operations. Define the cost of a program to be the number of root-takings used, with arithmetic operations given for free. Let $\mathbf{F}$ be the extension field generated by the members of ρ over the field of rational functions with complex coefficients. It was shown [6,7] that, when the members of ρ are rational functions of the roots of rational functions, the mimimum cost is equal to the number of the torsion orders[4] for the Galois group of $\mathbf{F}$ (an Abelian group in this case). An extension was given in Ja'Ja' [1], who showed that the minimum cost is equal to the minimum length of any cyclic Jordan-Hölder tower for the Galois group of $\mathbf{F}$, provided that $\mathbf{F}$ is a finite Galois extension over the field of rational functions. It is known [1,7] that the former result is a special case of the latter.

These results can be used to determine the minimum cost for computing ρ in many cases. For example, for the mean distance problem, the Galois group can be shown [6] to be isomorphic to $(\mathbf{Z_2})^{\binom{n}{2}}$, which clearly has $\binom{n}{2}$ torsion orders.

As taking a root $y^{1/d}$ can be simulated by taking the logarithm $\log y$ followed by an exponentiation $\exp((\log y)/d)$, a natural question is whether the availability of the lograrithm and exponential operations can substantially reduce the cost of evaluating algebraic expressions. In particular, can one evaluate the expression $\sum_{1\le i\le n}\sqrt{x_i}$ using $o(n)$ exponentiations and logarithm-takings? (Clearly, the expression can be evaluated with n root-takings.) The possible use of logarithms and exponentials, as well as other primitives, was mentioned in [8], but was not studied in later papers [1,6,7].

In this paper, we show that under the same assumption as in [1] (i.e. $\mathbf{F}$ being a finite Galois extension), the availability of taking logarithms and exponentials does not reduce the cost. In particular, we prove that n or more operations are needed to evaluate $\sum_{1\le i\le n}\sqrt{x_i}$, with arithmetic operations given for free. In the next section, we give a precise statement of the main result (Theorem 1), after introducing the needed notations and background. The result is then proved in Section 3; some additional concepts and results from Differential Algebra (see [2-4]) are used in the proof.

[4] Any finite Abelian group G can be uniquely decomposed into a direct sum of cyclic groups $\mathbf{Z_{d_1}} \oplus \mathbf{Z_{d_2}} \oplus \cdots \mathbf{Z_{d_t}}$, such that $d_t > 1$ and d_i is divisible by d_{i+1} for $1 \le i < t$. The integers d_i are called the *torsion orders* of G; t is the number of torsion orders for G.

We remark that the complexity question under other cost measures, in which the cost of taking a d-th root may depend on d, were discussed in [1,6,7]. We will not pursue it here.

2 The Main Result

We use the standard teminology in Algebra (as in Lang [3]). In what follows, let $\mathbf{Z}^+$ be the set of all positive integers.

An *α-program* A is a sequence of instructions of the form $z_1 \leftarrow I_1$, $z_2 \leftarrow I_2, \cdots, z_m \leftarrow I_m$, where I_i are of the form $(r_i(x_1, x_2, \cdots, x_n, z_1, \cdots, z_{i-1}))^{1/d_i}$ with r_i is a rational function in $x_1, \cdots, x_n, z_1, \cdots, z_{i-1}$ with complex coefficients and $d_i \in \mathbf{Z}^+$. We call m the *cost* of A. For $1 \leq i \leq m$, let $g_i(x_1, x_2, \cdots, x_n)$ be the functions defined inductively by $g_i(x_1, x_2, \cdots, x_n) = (r_i(x_1, x_2, \cdots, x_n, g_1(x_1, \cdots, x_n), \cdots, g_{i-1}(x_1, \cdots, x_n)))^{1/d_i}$. We shall always assume that the r_i have been chosen so that the denominators of these functions do not vanish identically. Informally, $g_i(x_1, x_2, \cdots, x_n)$ are the values assumed by the variables z_i for input $(x_1, x_2, \cdots, x_n)$. Let E_A denote the set of all functions of the form $r(x_1, x_2, \cdots, x_n, g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$ where r is a rational function with complex coefficients whose denominator does not vanish identically when the substitution is made. We note that each element of E_A defines a function algebraic over the field $\mathbf{F_0} = \mathbf{C}(x_1, \cdots, x_n)$ of rational functions in n variables with coeffcients in the complex numbers $\mathbf{C}$.

A *solvable algebraic expression* is any element of E_A for any α-program A. Let $\rho = (f_1, f_2, \cdots, f_s)$ be a finite set of solvable algebraic expressions. We say that ρ *is computed by* A, if each $f_i \in E_A$. Let $N_\alpha(\rho)$ be the minimum cost of any α-program computing ρ. Clearly, $N_\alpha(\rho)$ is finite. For any such ρ, we can form the field $\mathbf{F_0}(\rho)$ which is the algebraic extension of $\mathbf{F_0}$ formed by adjoining the functions corredponding to the elements $f_1, \cdots, f_s$ of ρ.

Following [1], ρ is said to be *normal*, if $\mathbf{F_0}(\rho)$ is a finite Galois extension of $\mathbf{F_0}$. In other words, ρ is normal if ρ generates the splitting field of some polynomial over $\mathbf{F_0}$.

For any solvable group G, a *cyclic Jordan-Hölder tower* is a normal tower of groups

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{m-1} \triangleright G_m = 1,$$

where G_{i-1}/G_i is cyclic for each $1 \leq i \leq m$. Let $\nu(G)$ be the length m of the shortest cyclic Jordan-Hölder tower for G.

The next result is from Ja'Ja' [1] which we state as a lemma:

Lemma 1 [1] If ρ is normal, then $N_\alpha(\rho) = \nu(G)$, where G is the Galois group for $\mathbf{F_0}(\rho)$ over $\mathbf{F_0}$.

A *β-program* B is a sequence of instructions of the form $z_1 \leftarrow I_1, z_2 \leftarrow I_2, \cdots, z_m \leftarrow I_m$, where I_i are of the form a_i^{1/d_i}, $\exp(a_i)$, or $\log(a_i)$, where $a_i = r_i(x_1, x_2, \cdots, x_n, z_1, \cdots, z_{i-1})$ with r_i is a rational function in $x_1, \cdots, x_n, z_1, \cdots, z_{i-1}$ with complex coefficients and $d_i \in \mathbf{Z}^+$. We shall again always assume that the r_i have been chosen so that the denominators of these functions do not vanish identically. Let $\tau(B)$ be the number of instructions which either take roots or exponentials. Let $g_i(x_1, x_2, \cdots, x_n)$ be the functions associated with variables z_i, defined exactly as in the case for α-programs. Let E_B denote the set of all functions of the form $r(x_1, x_2, \cdots, x_n, g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$ where r is a rational function with complex coefficients whose denomincators do not vanish identically when the substituion is made.

Let $\rho = (f_1, f_2, \cdots, f_s)$ be a finite set of solvable algebraic expressions. We say that *ρ is computed by B*, if each element f_i of ρ equals a function in E_B. Let $N_\beta(\rho)$ be the minimum $\tau(B)$ of any β-program B computing ρ.

Our main result is the following theorem:

Theorem 1 If ρ is normal, then $N_\beta(\rho) = \nu(G)$, where G is the Galois group for $\mathbf{F_0}(\rho)$ over $\mathbf{F_0}$.

Corollary 1 If ρ is normal, then $N_\beta(\rho) = N_\alpha(\rho)$.

Corollary 2 Let $\rho = \{ f \}$, where $f = \sum_{1 \leq i \leq n} \sqrt{x_i}$. Then $N_\beta(\rho) = n$.

Remark It is an interesting open question whether $N_\beta(\rho)$ is equal to $N_\alpha(\rho)$ when ρ is not required to be normal.

3 Proof of Theorem 1

Before proving the theorem, we introduce some terms in Differential Algebra (see [2], [3], [4]). A *differential field* is a field k together with a set $\Delta = \{\delta_i\}$ of mappings $\delta_i : k \rightarrow k$, called *derivations*, such that eachδ_i satisfies the conditions $\delta_i(a+b) = \delta_i(a) + \delta_i(b)$, $\delta_i(ab) = \delta_i(a)b + a\delta_i(b)$, and $\delta_i(\delta_j(a)) = \delta_j(\delta_i(a))$ for all $\delta_i, \delta_j \in \Delta, a, b \in k$. For example, $\mathbf{F_0}$ can be considered a differential field when we use the derivations $\Delta = \{\delta_1, \cdots, \delta_n\}$ where $\delta_i(f) = \partial f / \partial x_i$. In this paper we are concerned only with differential fields that come from fields of differentiable functions a and that are extensions of this differential field. These extensions will be gotten by adjoining elements that can be interpreted as functions on some suitable region in complex n-space $\mathbf{C}^n$. We will use $\mathbf{K_0}$ to denote the differential field obtained from the field $\mathbf{F_0}$ equipped with these standard derivations Δ. Note that if $\mathbf{K}$ is a differential field containing $\mathbf{K_0}$ and if $a \in \mathbf{K}$, then the field obtained by adjoining $\exp(a)$ to $\mathbf{K}$ gives a differential field. The element $\exp(a)$ will satisfy the differential equations $\delta_i(\exp(a)) = \delta_i(a) \cdot \exp(a)$ for $i = 1, \cdots, n$. Similarly, the adjoining of $\log(a)$ gives a differential field and the element $\log(a)$ satisfies $\delta_i(\log(a)) = \delta_i(a)/a$for $i = 1, \cdots, n$. We also note that if $\rho = (f_1, \cdots, f_s)$ is a set of solvable algebraic expressions (or, more generally, any set of algebraic functions), the derivations Δ can be extended uniquely to derivations on $\mathbf{F_0}(\rho)$ ([4], Lemma 1, p.90).

The classical Galois theory for field theory can be extended to a *differential Galois theory* for differential fields (See [3] and [4] for definitions and discussions of these concepts; [2] contains an excellent exposition of the theory in the case of only one derivation and the essential results extend, *mutatis mutandi* to the case of several derivations). This galois theory can be used to study the structure of the solutions of a system of partial linear differential equations, provided that the equations generate a differential ideal of finite linear dimension or, equivalently (see [4], Chapter IV.5), the solution space is a finite dimensional vector space (i.e., the system is holonomic). This is the case for the equations defining exponentials and logarithms (see [3] and [4]). To avoid possible confusions, we will reserve the term *Galois group* for the classical Galois group, and use the term *differential* Galois group when differential fields are being discussed. It should be noted, though, that if k_1 is an algebraic extension of k_0, a differential field of characteristic zero, then since all derivations on k_0 can be extended uniquely to derivations on k_1, we can identify the Galois group of k_1 over k_0 with the differential galois group of k_1 over k_0 (with respect to these derivations). To see this note that any differential automorphism is by definition a usual automorphism. Conversely, for any automorphism σ of k_1 over k_0 and any derivation δ of k_1 that leaves k_0 invariant, we have that $\sigma^{-1} \circ \delta \circ \sigma$ is a derivation of k_1 agreeing with δ on k_0. Uniqueness implies that they must be equal on all of k_1 and so σ must be a differential automorphism. This remark allows us to apply results concerning differential galois theory to the galois theory of algebraic extensions of differential fields.

To prove Theorem 1, we first show that if $\mathbf{F_0}(\rho)$ is contained in a certain tower of differential fields, then there is a tower of algebraic extension fields of no greater length containing $\mathbf{F_0}(\rho)$. This result (Lemma 2 below) is at the heart of the proof for Theorem 1.

Let $\mathbf{K_0} \subset \mathbf{K_1} \subset \mathbf{K_2} \subset \ldots \subset \mathbf{K_m}$ be a tower of differential fields, where each $\mathbf{K_i}$ is obtained from $\mathbf{K_{i-1}}$ by adjoining an element u_i; u_i is either $\exp(a_i)$ or $\log(a_i)$ with $a_i \in \mathbf{K_{i-1}}$. Let I be the set of $1 \leq i \leq m$ such that u_i is $\exp(a_i)$. We recall from differential Galois theory that in this case each $\mathbf{K_i}$ is a Picard-Vessiot extension of $\mathbf{K_{i-1}}$. Furthermore, it is known (see [3, Section 4], or [4, Chapter VI.6]; [2, Lemmas 3.9 and

3.10] contains simillar results for the case of one derivation) that, if $i \in I$, the differential Galois group of $\mathbf{K_i}$ over $\mathbf{K_{i-1}}$ is an algebraic subgroup of $\mathbf{C}^*$, the multiplicative group of non-zero complex numbers, and if $i \notin I$, then the differential Galois group of $\mathbf{K_i}$ over $\mathbf{K_{i-1}}$ is an algebraic subgroup of $\mathbf{C}^+$, the additive group of complex numbers. Finally, we note that the proper algebraic subgroups of $\mathbf{C}^*$ are precisely the finite cyclic groups and the only proper algebraic subgroup of $\mathbf{C}^+$ is the trivial group. This can be seen by noting that a proper Zariski closed subset of either of these two groups must be finite and that in the first case, we will have a finite multiplicative subgroup of a field and in the second case we will have a finite subgroup of a torsion free group.

Lemma 2 If $\mathbf{F}_0(\rho) \subset \mathbf{K_m}$ then $\nu(G) \leq \mid I \mid$.

Proof Let $\mathbf{F_i} = \mathbf{F}_0(\rho) \cap \mathbf{K_i}$ for $1 \leq i \leq m$. Then $\mathbf{F_m} = \mathbf{F}_0(\rho)$. Note that $\mathbf{F_0} = \mathbf{F}_0(\rho) \cap \mathbf{K_0}$. Let H_i be the differential Galois group of $\mathbf{K_i}$ over $\mathbf{K_{i-1}}$. We claim that the following statement is true for $1 \leq i \leq m$:

Fact 1 $\mathbf{F_i}$ is a Galois extension of $\mathbf{F_{i-1}}$.

To prove this fact, let $\mathbf{E_i}$ be the subfield of elements of $\mathbf{K_i}$ algebraic over $\mathbf{K_{i-1}}$. $\mathbf{E_i}$ is a differential field and is left invariant by all elements of H_i. Therefore the differential Galois group of $\mathbf{K_i}$ over $\mathbf{E_i}$ is a normal subgroup of H_i and so $\mathbf{E_i}$ is a Galois extension of $\mathbf{K_{i-1}}$. Note that $\mathbf{F_i} = \mathbf{E_i} \cap \mathbf{F}_0(\rho)$. Let $p(x)$ be a polynomial with coeffcients in $\mathbf{F_{i-1}}$. If $p(x) = 0$ has a root in $\mathbf{F_i}$, it must split in both $\mathbf{E_i}$ and $\mathbf{F}_0(\rho)$ (since $\mathbf{F}_0(\rho)$ is *a fortiori* normal over $\mathbf{F_{i-1}}$). Therefore $p(x) = 0$ splits in $\mathbf{F_i}$ and so $\mathbf{F_i}$ is a Galois extension of $\mathbf{F_{i-1}}$.

Now let J_i be the Galois group of $\mathbf{F_i}$ over $\mathbf{F_{i-1}}$. We claim that the following statement is true:

Fact 2 For $1 \leq i \leq m$, J_i is the trivial group if $i \notin I$, and a cyclic group if $i \in I$.

To prove this fact, consider the field $\mathbf{K_{i-1}} \cdot \mathbf{F_i}$. This is a subfield of $\mathbf{K_i}$. Since H_i is an abelian group, all of its subgroups are normal, so $\mathbf{K_{i-1}} \cdot \mathbf{F_i}$ is a normal extension of $\mathbf{K_{i-1}}$ whose differential Galois group L_i is the quotient of H_i by a closed subgroup of H_i. Furthermore, since $\mathbf{K_{i-1}} \cdot \mathbf{F_i}$ is a finite extension of $\mathbf{K_{i-1}}$, L_i is finite and thus coincides with the Galois group of this extension. If $i \notin I$, then H_i is either $\mathbf{C}^+$ or the trivial group. The only finite quotient of either of these groups by a closed subgroup is trivial. If $i \in I$, then H_i is either $\mathbf{C}^*$ or a finite cyclic group. The only possible finite quotients of these groups by closed subgroups are cyclic. To finish the proof of Fact 2, we note that $\mathbf{K_{i-1}} \cap \mathbf{F_i} = \mathbf{F_{i-1}}$ and so the Galois group J_i of $\mathbf{F_i}$ over $\mathbf{F_{i-1}}$ is isomorphic to L_i (see [5, Corollary, p. 400] or [4, Chapter VII, Theorem 1.12]; [2, Lemma 5.10] is a related result but deals only with the case of one derivation.)

We can now finish the proof of Lemma 2. Let G_i denote the group of automorphisms of $\mathbf{F}_0(\rho)$ leaving $\mathbf{F_i}$ fixed. By Facts 1 and 2, one concludes from the Galois theory that the series $G = G_0, G_1, G_2, \ldots, G_m = 1$ forms a cyclic Jordan-Hölder tower, with G_{i-1}/G_i being isomorphic to J_i. Deleting all $i \notin I$, we have a tower of length $\mid I \mid$. Hence $\nu(G) \leq \mid I \mid$. $\square$

We now turn to the proof of Theorem 1. Observe that $N_\beta(\rho) \leq N_\alpha(\rho)$, which is no greater than $\nu(G)$ by Lemma 1. Thus, we only need to prove that $N_\beta(\rho) \geq \nu(G)$.

Let B be any β-program for computing ρ. Without loss of generality, we may assume that no root-taking operations are used in B, as we can replace any instruction $z \leftarrow r^{1/d}$ by two instructions $y \leftarrow (\log r)/d$, $z \leftarrow \exp(y)$ without changing the value of $\tau(B)$. Let the instructions be $z_1 \leftarrow I_1$, $z_2 \leftarrow I_2, \cdots, z_m \leftarrow I_m$. Let $g_i(x_1, x_2, \cdots, x_n)$ be the functions associated with variables z_i.

For $1 \leq i \leq m$, let $\mathbf{K_i}$ be the differential field obatained by adjoining g_i to $\mathbf{K_{i-1}}$. By definition, the functions of E_B correspond to elements of $\mathbf{K_m}$ and $\mathbf{F_0}(\rho) \subset \mathbf{K_m}$. By Lemma 2, this implies $\nu(G) \leq \tau(B)$. This proves $\nu(G) \leq N_\beta(\rho)$, and completes the proof of Theorem 1. Corollary 1 follows immediately from the theorem and Lemma 1.

To prove Corollary 2, we note that ρ is normal and the Galois group G of $\mathbf{F_0}(\rho)$ over $\mathbf{F_0}$ is isomorphic to $\mathbf{Z_2}^n$. ¿From the result in [1, 7] (see [7, p. 399, Lemma 3.2]), $\nu(G)$ is equal to the number of torsion orders of G which is cleary n. Corollary 2 follows from the theorem immediately.

References

[1] J. Ja' Ja', "Computation of algebraic functions with root extractions," *Proceedings of 22nd IEEE Symposium on Foundations of Computer Science*, 1981, 95-100.

[2] I. Kaplansky, *An Introduction to Differential Algebra*, Hermann, Paris, 1957.

[3] E. R. Kolchin, "Picard–Vessiot theory of partial differential fields," *Proceedings of the American Mathematical Society*, **3** (1952), 596–603.

[4] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[5] S. Lang, *Algebra*, Addison-Wesley, Menlo Park, California, 1984 (Second Edition).

[6] N. Pippenger, "Computational complexity of algebraic functions," *Journal of Computer and System Sciences* **22** (1981), 454-470.

[7] N. Pippenger, "Corrections to 'Computational complexity of algebraic functions'," *Journal of Computer and System Sciences* **37** (1988), 395-399.

[8] M. Shamos and G. Yuval, "Lower bounds from complex function theory," *Proceedings of 17th IEEE Symposium on Foundations of Computer Science*, 1976, 268-273.