MATHEMATICS OF COMPUTATION
Volume 68, Number 226, April 1999, Pages 881–885
S 0025-5718(99)01060-1

SOLVING POLYNOMIALS BY RADICALS WITH ROOTS OF UNITY IN MINIMUM DEPTH

GWOBOA HORNG AND MING-DEH HUANG

ABSTRACT. Let k be an algebraic number field. Let α be a root of a polynomial $f \in k[x]$ which is solvable by radicals. Let L be the splitting field of α over k. Let n be a natural number divisible by the discriminant of the maximal abelian subextension of L, as well as the exponent of $G(L/k)$, the Galois group of L over k. We show that an optimal nested radical with roots of unity for α can be effectively constructed from the derived series of the solvable Galois group of $L(\zeta_n)$ over $k(\zeta_n)$.

1. INTRODUCTION

It was shown in [8] that whether a polynomial with rational coefficients is solvable by radicals can be decided in polynomial time. Given that a polynomial is solvable by radicals, it is also of interest to construct a nested radical of minimum possible depth for the polynomial. Partial results for this problem can be found in [2, 6, 7, 11]. More recently, a general solution to the problem has been reported in [5].

An interesting relaxation for the problem is to allow roots of unity, in addition to elements of the ground field, to be used as primitives in the construction of nested radicals. No restriction is placed on the roots of unity that can be used for the construction. The goal of this paper is to determine a root of unity for constructing a nested radical of minimum depth for a root of a polynomial which is solvable by radicals.

Throughout this paper, k denotes an algebraic number field, $\bar{k}$ the algebraic closure of k, μ_∞ the set of all roots of unity, and $\zeta_n = e^{2\pi i/n}$.

Let α be a root of a polynomial $f \in k[x]$ that is solvable by radicals. Let L be the splitting field of α over k. Let L_∞ be the splitting field of α over $k(\mu_\infty)$. A near-optimal construction of a nested radical with roots of unity for α is given in [7]. It is also shown in [7] that the minimum depth of a nested radical with roots of unity for α is determined by the length of the derived series of the solvable Galois group of L_∞ over $k(\mu_\infty)$. To effectively construct an optimal nested radical for α, it is desirable to have a similar characterization in terms of a specific root of unity. Let n be a natural number divisible by the discriminant of the maximal abelian subextension of L, as well as the exponent of $G(L/k)$, the Galois group of L over k. We show that the minimum depth of a nested radical with roots of unity for α

Received by the editor April 24, 1996 and, in revised form, December 1, 1997.
1991 *Mathematics Subject Classification.* Primary 11R32; Secondary 11Y16, 12Y05.
Key words and phrases. Polynomials, solvable by radicals.
The first author was supported in part by NSF Grant CCR 8957317.
The second author was supported in part by NSF Grant CCR 9412383.

is determined by the length of the derived series of $G(L(\zeta_n)/k(\zeta_n))$, and that an optimal nested radical with roots of unity for α can be effectively constructed from the tower of extensions corresponding to the derived series.

1.1. **Definitions and main result.** Nested radicals are expressions that can de defined recursively as follows. An element a of $k(\mu_\infty)$ is considered a nested radical of depth 0. Inductively, if A and B are nested radicals of depth $d(A)$ and $d(B)$, respectively, and $* \in \{+, -, \times, \div\}$, then $A * B$ is a nested radical of depth $\max(d(A), d(B))$; and for $n > 1$, $\sqrt[n]{A}$ is a nested radical of depth $d(A)+1$. The two expressions $\sqrt{2} \times \sqrt{3}$ and $\sqrt{6}$, for example, are considered distinct nested radicals of depth 1. Similarly $\sqrt{\sqrt{2} + \sqrt{2}\sqrt{3}}$ and $\sqrt{\sqrt{2}(1 + \sqrt{3})}$ are distinct nested radicals of depth 2.

A *simple nested radical* is either an element of $k(\mu_\infty)$ or a nested radical of the form $\sqrt[n]{A}$ where A is a nested radical and $n > 1$. Let E be a nested radical. Then $S(E)$ denotes the set of simple nested radicals that appear in E. To be precise, if $E = a$ for some $a \in k(\mu_\infty)$, then $S(E) = \{a\}$; inductively if $E = B * C$ for nested radicals B and C, then $S(E) = S(B) \cup S(C)$; if $E = \sqrt[n]{B}$, then $S(E) = S(B) \cup \{\sqrt[n]{B}\}$. For example,

$$E = \sqrt{\sqrt[5]{\sqrt[3]{2} + 1} + \sqrt[3]{2}} + \sqrt[3]{2}$$

has depth 3 and $S(E)$ consists of $\sqrt{\sqrt[5]{\sqrt[3]{2} + 1} + \sqrt[3]{2}}$, $\sqrt[5]{\sqrt[3]{2} + 1}$, and $\sqrt[3]{2}$.

A field extension K over k is a *root extension* if $K = k(\alpha_1, \ldots, \alpha_m)$ where, for all $1 \le i \le m$, $\alpha_i^{n_i} = a_i \in k$ for some integer $n_i > 1$. $\alpha_1, \ldots, \alpha_m$ form a set of *generating roots* for K/k, and α_i is called a *generating root* of degree n_i if n_i is the least positive integer such that $\alpha_i^{n_i} \in k$. A *root tower* over k is a tower of extensions $k = k_0 \subset k_1 \subset \cdots \subset k_n$ such that k_i/k_{i-1} is a root extension for $1 \le i \le n$. If α is a generating root of degree m for k_i/k_{i-1}, then it is called a *generating root of degree m for the tower at level i.*

An element of $\bar{k}$ represented by a nested radical E is called a *root* of E. If $E = a \in k(\mu_\infty)$, then it has a unique root a. If E has depth $d > 0$, then a root of E can be determined after a consistent assignment of roots is made for the simple nested radicals associated with E. To be precise, suppose inductively a root $r(A)$ has been determined for every simple nested radical $A \in S(E)$ of depth less than d. Then a root has also been determined for every arithmetic expression in these simple nested radicals. Let $B \in S(E)$ be of depth d. Then $B = \sqrt[n]{A}$ where $n > 1$ and A is an arithmetic expression in the simple nested radicals in $S(E)$ of depth less than d. Since a root $r(A) \in \bar{k}$ is already determined for A, an $r(B) \in \bar{k}$ can be assigned as a root for B if $r(B)^n = r(A)$. When a root is assigned for each simple nested radical associated with E, then a root γ is also assigned for E. Let $k = k_0$ and inductively for $i > 0$, let k_i be the field over k_{i-1} generated by the roots assigned to the simple nested radicals of depth i in $S(E)$. Then $k = k_0 \subset k_1 \subset \cdots \subset k_d$ is called *a root tower determined by E* and γ is said to be a root of E determined from the root tower.

Take $E = \sqrt[5]{\sqrt[3]{2} + 1} + \sqrt[3]{2}$ as an example. Let u be the unique real root of $x^3 = 2$ and v be a real root of $y^5 = u + 1$. Then $v + u$ is a root of E. However, it would be inconsistent to assign v to $\sqrt[5]{\sqrt[3]{2} + 1}$ and a root u' different from u to $\sqrt[3]{2}$. Consequently $v + u'$ is not a root of E. The root tower of $v + u$ determined by

E is $\mathbf{Q} \subset \mathbf{Q}(u) \subset \mathbf{Q}(u,v)$. For another example let $A = 2\sqrt{6}$ and $B = \sqrt{2}\sqrt{3} + \sqrt{6}$. We note that every root of A is a root of B but not vice versa. Indeed B has the additional root 0 as a result of assigning the positive real root to $\sqrt{2}$ and $\sqrt{6}$ and the negative real root to $\sqrt{3}$.

On the other hand, let $T : k = k_0 \subset k_1 \subset \cdots \subset k_n$ be a root tower. Then there is a natural way to associate an element in k_i to a nested radical of depth no greater than i. Fix a set of generating roots for each k_i/k_{i-1} for $i = 1$ to n. Let γ be an element of k_d in the root tower. Let α be a generating root at level 1 of degree m such that $\alpha^m = a \in k_0$. Then $\sqrt[m]{a}$ is a nested radical of depth 1 associated with α and has α as a root. Inductively suppose a nested radical B_i of depth less than d is determined for every generating root β_i at level less than d so that β_i is a root of B_i. Suppose β is a generating root at level d of degree e, with $\beta^e = g(\beta_1, \ldots, \beta_l)$, where β_i are the generating roots at level $< d$ and $g \in k(x_1, \ldots, x_l)$. Then $\sqrt[e]{g(B_1, \ldots, B_l)}$ is a nested radical of depth no greater than d associated with β and has β as a root. Once a nested radical is determined for every generating root at level 1 to d, a nested radical with γ as a root is also determined for γ. We call it a *nested radical for γ determined by the root tower T*.

Let G be a group and let $x, y \in G$. The *commutator* of x and y is the element $x^{-1}y^{-1}xy$. The *commutator subgroup* of G is the subgroup generated by all the commutators of G. We shall use $G^{(1)}$ to denote the commutator subgroup of G and use $G^{(i)}$ to denote the commutator subgroup of $G^{(i-1)}$ for $i > 1$. We also let $G^{(0)} = G$. When G is solvable, the chain of groups $G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots$ is called the *derived series* of G. The *length* of the derived series, denoted $l(G)$, is the smallest positive integer n such that $G^{(n)} = \{1\}$.

Let G be a group and let H be a normal subgroup of G. Then $(G/H)^{(i)} \cong G^{(i)}H/H$ for all $i \geq 0$, and $l(G/H) \leq l(G)$. Moreover if G/H is abelian then $G^{(1)} \subseteq H$.

We are ready to state the main theorem.

Theorem 1.1. *Let k be a number field. Let α be a root of an irreducible polynomial in $k[x]$ that is solvable by radicals. Let L be the splitting field of the polynomial over k. Let L^{ab} be the maximal abelian subextension of L over $\mathbf{Q}$. Let n be a natural number that is divisible by the discriminant of L^{ab} over $\mathbf{Q}$ and the exponent of $G(L/k)$, the Galois group of L over k. Then the tower of field extensions corresponding to the derived series of $G(L(\zeta_n)/k(\zeta_n))$ is a root tower, and a nested radical for α determined by this root tower is a nested radical for α of minimum depth with roots of unity.*

2. Proof of the main theorem

Lemma 2.1. *Let k be a number field. Let $k_0 \subset k_1 \subset \cdots \subset k_d$ be a root tower with $k \subset k_0$. Let K_i be the composite of k_i^σ for all $\sigma \in G(\bar{k}/k)$. Then K_i/k, $K_i(\mu_\infty)/K_0(\mu_\infty)$ are Galois for $i = 0, ..., d$, $K_0(\mu_\infty) \subset K_1(\mu_\infty) \subset \cdots \subset K_d(\mu_\infty)$ is a root tower, and $l(G(K_d(\mu_\infty)/K_0(\mu_\infty))) \leq d$.*

Proof. For all $\sigma \in G(\bar{k}/k)$, $k_0^\sigma \subset k_1^\sigma \subset \cdots \subset k_d^\sigma$ is again a root tower. Since each k_i has finitely many conjugates over k, it follows that $K_0 \subset K_1 \subset \cdots \subset K_d$ is a root tower. Hence, writing $K_i' = K_i(\mu_\infty)$, K_i'/K_{i-1}' is abelian, and $K_0' \subset K_1' \subset \cdots \subset K_d'$ is a root tower of abelian extensions. In particular $G(K_d'/K_0')$ is solvable of length at most d.

Finally, for all i, since K_i is the composite of k_i^σ for all $\sigma \in G(\bar{k}/k)$, K_i/k is Galois, and it follows that K_i/K_0 and K_i'/K_0' are Galois as well. □

Proposition 2.2. *Let K be an abelian extension over $\mathbf{Q}$. Let $n \in \mathbf{N}$ be divisible by the discriminant of K over $\mathbf{Q}$. Then $K \subset \mathbf{Q}(\zeta_n)$.*

Proof. From the conductor-discriminant formula (see [3] p. 160), it follows that the conductor of K over $\mathbf{Q}$ divides the discriminant of K over $\mathbf{Q}$. Hence $n\infty$ is divisible by the conductor of $K/\mathbf{Q}$, and it follows from the Kronecker-Weber Theorem (see [4] p. 175) that $K \subset \mathbf{Q}(\zeta_n)$. □

Proof of the main theorem. Let $F = k \cap \mathbf{Q}(\mu_\infty)$. Then there is a canonical isomorphism ϕ from the abelian group $G(k(\mu_\infty)/k)$ onto $G(\mathbf{Q}(\mu_\infty)/F)$.

Let $K = L \cap k(\mu_\infty)$. Since $L^{ab} = L \cap \mathbf{Q}(\mu_\infty) = K \cap \mathbf{Q}(\mu_\infty)$, $G(k(\mu_\infty)/K) \cong G(\mathbf{Q}(\mu_\infty)/L^{ab})$ under ϕ. Consequently $G(K/k)$ and $G(L^{ab}/F)$ are isomorphic. It follows that $K = kL^{ab}$.

Since n is divisible by the discriminant of L^{ab} over $\mathbf{Q}$, it follows from Proposition 2.2 that $L^{ab} \subset \mathbf{Q}(\zeta_n)$. Hence $K = kL^{ab} \subset k(\zeta_n)$. It follows that $K = L \cap k(\zeta_n)$.

Since $L(\mu_\infty)$ is the composite of L and $k(\mu_\infty)$, $G(L/K) \cong G(L(\mu_\infty)/k(\mu_\infty))$. On the other hand since $L(\zeta_n)$ is the composite of L and $k(\zeta_n)$, and since $K = L \cap k(\zeta_n)$, $G(L/K) \cong G(L(\zeta_n)/k(\zeta_n))$. Hence $G(L(\zeta_n)/k(\zeta_n)) \cong G(L(\mu_\infty)/k(\mu_\infty))$, and so $l(G(L(\zeta_n)/k(\zeta_n))) = l(G(L(\mu_\infty)/k(\mu_\infty)))$.

Since n is divisible by the exponent of $G(L/k)$, the tower of subfields of $L(\zeta_n)$ corresponding to the derived series of $G(L(\zeta_n)/k(\zeta_n))$ is a root tower T by Kummer theory. Let B be a nested radical for α determined by T. Then $\text{depth}(B) \leq l(G(L(\zeta_n)/k(\zeta_n))) = l(G(L(\mu_\infty)/k(\mu_\infty)))$.

Let d be the depth of a nested radical B' for α of minimum depth with roots of unity. Let m be such that all the roots of unity used in B' are powers of ζ_m. Let $k_0 = k(\zeta_m) \subset k_1 \subset \cdots \subset k_d$ be the root tower for α determined by B'. Let $K_i, 0 \leq i \leq d$, be the composite of k_i^σ for all $\sigma \in G(\bar{k}/k)$. Then by Lemma 2.1, K_i/k and $K_i(\mu_\infty)/K_0(\mu_\infty)$ are Galois for $i = 0, ..., d$, $K_0(\mu_\infty) \subset K_1(\mu_\infty) \subset \cdots \subset K_d(\mu_\infty)$ is a root tower and $l(G(K_d(\mu_\infty)/K_0(\mu_\infty))) \leq d$. Note that $K_0 = k_0$ as k_0/k is Galois. Hence $K_0(\mu_\infty) = k_0(\mu_\infty) = k(\mu_\infty)$, and so $l(G(K_d(\mu_\infty)/k(\mu_\infty))) \leq d$.

Since K_d is Galois over k and $\alpha \in K_d$, we have $L \subseteq K_d$. Let

$$G = G(K_d(\mu_\infty)/k(\mu_\infty)) \quad \text{and} \quad H = G(K_d(\mu_\infty)/L(\mu_\infty)).$$

Since $L(\mu_\infty)/k(\mu_\infty)$ is Galois, H is a normal subgroup of G, so $l(G(L(\mu_\infty)/k(\mu_\infty)))$ $= l(G/H) \leq l(G) \leq d$. Therefore, $\text{depth}(B) \leq l(G(L(\mu_\infty)/k(\mu_\infty))) \leq d$. This implies $\text{depth}(B) = d$; hence B is a nested radical of minimum depth for α with roots of unity. This completes the proof of the main theorem.

Finally we describe an algorithm for the construction of an optimal nested radical with roots of unity for a solvable irreducible polynomial h.

Let h be the irreducible polynomial of α. An irreducible polynomial g and the Galois group for the splitting field L of α over k can be computed by an algorithm in [7]. The time complexity as well as the length of g are polynomial in the length of h and the degree of L over k. From the Galois group the exponent l of the group can be computed in time polynomial in the size of the group.

Let G be the norm of g over $\mathbf{Q}$. Let $H = G/(G, G')$. Then H is an irreducible polynomial for L over $\mathbf{Q}$. We can convert H into an monic integral irreducible polynomial by a standard technique as follows. Without loss of generality assume

$H = \sum_{i=0}^{N} a_i x^i$, where $a_i \in \mathbf{Z}$. Let α be a root of H. Then $a_N\alpha$ is a root of the monic integral polynomial $H_1 = x^N + \sum_{i=0}^{N-1} a_N^{N-1-i} a_i x^i$. Hence H_1 is a monic integral irreducible polynomial for L over $\mathbf{Q}$. It follows that the discriminant of H_1, $D(H_1)$, is divisible by $D(L/\mathbf{Q})$, hence by $D(L^{ab}/\mathbf{Q})$. So by Theorem 1.1, the root of unity can be taken to be ζ_n where $n = |D(H_1)|l$. We remark that the length of n is polynomial in the length of the irreducible polynomial for specifying k, the length of h, and $[L : k]$. Hence n may be doubly exponential in the degree of h, as $[L : k]$ may be exponential in the degree of h.

Once n is computed, we can compute a nested radical corresponding to the derived series of $G(L(\zeta_n)/k(\zeta_n))$ by applying the procedures developed in [7]. The running time is polynomial in n, $[L : k]$, and the length of the irreducible polynomial for α, hence it is, in the worst case, doubly exponential in the input size.

References

[1] E. Artin and J. Tate. *Class field theory.* W.A. Benjamin, Inc, 1968. MR **36:**6383

[2] A. Borodin and R. Fagin and J. Hopcroft and M. Tompa. Decreasing the Nesting Depth of expressions Involving Square Roots. *J. Symbolic Computation*, 1:169-188, 1985. MR **87a:**68087

[3] J.W.S. Cassels and A. Frölich, editors. *Algebraic number theory.* Academic Press, 1967. MR **35:**6500

[4] H. Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer-Verlag, 1978. MR **80c:**12001

[5] C.F. Cotner, *The Nesting Depth of Radical Expressions*, Ph.D. Thesis, Berkeley, 1995.

[6] G. Horng and M.-D. Huang. Simplifying Nested Radicals and solving polynomials by radicals in minimum depth. In *Proc. 31th IEEE FOCS*, 847-856, 1990. MR **93g:**68061

[7] S. Landau. Simplification of Nested Radicals. *SIAM J. Computing*, 21:85-110, 1992. MR **92k:**12008

[8] S. Landau and G. Miller. Solvability by radicals is in polynomial time. *JCSS*, 30:179-208, 1985. MR **86k:**12001

[9] J. Neukirch. *Class Field Theory.* Springer-Verlag Heidelberg, 1986. MR **87i:**11005

[10] L. C. Washington. *Introduction to cyclotomic fields.* Springer-Verlag, New York, 1982. MR **85g:**11001

[11] R. Zippel. Simplification of expressions involving radicals. *J. Symbolic Computation*, 1:189-210, 1985. MR **87b:**68058

Department of Computer Science, University of Southern California, Los Angeles, CA90089-0781

Current address: Department of Computer Science, National Chung Hsing University, Taichung, Taiwan, R.O.C.

E-mail address: gbhorng@cs.nchu.edu.tw

Department of Computer Science, University of Southern California, Los Angeles, CA90089-0781

E-mail address: huang@cs.usc.edu