

Denesting by bounded degree radicals

Report**Author(s):**

Blömer, Johannes

Publication date:

1997

Permanent link:

<https://doi.org/10.3929/ethz-a-006652170>

Rights / license:

In Copyright - Non-Commercial Use Permitted

Originally published in:

Technical report / Departement Informatik, ETH Zürich 273

Denesting by Bounded Degree Radicals

Johannes Blömer

September 24, 1997

Abstract. Given a nested radical involving only d -th roots we show how to compute an optimal or near optimal depth denesting of this nested radical by a nested radical that involves only D -th roots, where D is an arbitrary multiple of d . As a special case the algorithm can be used to compute denestings as in previous papers by S. Landau and Horng/Huang. The running times of the algorithms are polynomial in the description size of the splitting field for the original nested radical.

Author's address:

Johannes Blömer
Institute for Theoretical Computer Science
ETH Zentrum
CH-8092 Zurich
Switzerland

Technical Report #273, Departement Informatik, ETH Zürich.

Electronically available from:

<ftp://ftp.inf.ethz.ch/pub/publications/tech-reports/>

1 Introduction

Simplification or denesting of radical expressions is a natural simplification problem that algebraic and symbolic manipulation systems face. Denestings are useful for manipulating large formulas as well as understanding the final result. Accordingly, starting in the mid-70's the problem has been studied intensively in Computer Algebra or Algorithmic Algebra (see for example [5],[14],[4],[9],[10],[6],[2], [3] and in particular the survey by Susan Landau [11]). Without doubt, many researches were also attracted by the following seemingly mysterious equations, which can be found in Ramanujan's notebook and which nicely illustrate and explain the general problem.

$$\begin{aligned}\sqrt[3]{\sqrt[3]{2}-1} &= \sqrt[3]{1/9} - \sqrt[3]{2/9} + \sqrt[3]{4/9} \\ \sqrt[6]{7\sqrt[3]{20}-19} &= \sqrt[3]{5/3} - \sqrt[3]{2/3}.\end{aligned}$$

In each of these equations the depth 2 formula on the left is denested by a depth 1 formula on the right.

In denesting radicals an important question is which field to consider as the ground field, the field of constants, so to speak. In the examples given above the ground field is the field of rational numbers. In general, it is not feasible to consider arbitrary ground fields. Dealing symbolically with radicals, nested or just plain roots, usually requires the presence of appropriate roots of unity, that is, roots of the polynomials $X^d - 1, d \in \mathbf{N}$.

Horng/Huang [6] denest a nested radical expression using arbitrary roots. To do so they consider ground fields containing all roots of unity. The nesting depth they achieve is the minimal possible one over such a field. Computing in a field containing all roots of unity is computationally infeasible and Horng/Huang show that a finite number of roots of unity suffice. The bound on the degree of the roots of unity that one needs to consider is, in the worst case, double-exponential in the degrees of the roots appearing in the original expression.

Landau [9] sticks closer to the field over which the original expression was defined. She adjoins to this field roots of unity whose degree is related to the Galois group of the nested radical. Over this extension field she computes an optimal depth denesting using arbitrary roots. She also proves that the depth of this denesting differs at most by 1 from the depth of the optimal denesting over the original field. The worst case bound on the degree of the roots of unity that are adjoined to the original field is single-exponential in the degrees of the roots involved in the original expression.

In this paper, we follow a different strategy than these papers. We believe that adjoining large degree roots of unity may actually hide interesting information about the original expression. As an example, consider $\sqrt{5+2\sqrt{6}}$. It denests over the rational numbers to $\sqrt{2} + \sqrt{3}$. However, $\sqrt{2}$ and $\sqrt{3}$ are contained in the extension of \mathbf{Q} containing all roots of unity. Hence, instead of finding the denesting $\sqrt{2} + \sqrt{3}$ the algorithms in [6], for example, will return some expression involving roots of unity. The most innocent one

being $\sqrt{-1}(\zeta_3 + \zeta_3^2) + (\zeta_8 + \zeta_8^7)$, where ζ_3 and ζ_8 are primitive 3^{rd} and primitive 8^{th} roots of unity.

Therefore, in this paper we do not try to obtain denestings using arbitrary roots. Instead, in our algorithms an integer D can be specified, with the understanding that only roots whose degree divides D are allowed in the denesting. Quite naturally, we require that D is a multiple of the least common multiple of the degrees in the original expression. Accordingly, the only root of unity we have to adjoin to the ground field is a primitive D^{th} root of unity. Similar to the results in [9], the algorithm produces a denesting over this extension field that is optimal for the class of nested radicals that use D^{th} roots. The depth of the denesting is at most the depth of the optimal denesting that is defined over the original field and that uses only D^{th} roots.

In particular, for nested radicals involving only square roots and defined over an arbitrary field the algorithm finds the optimal denesting using square roots but without changing the underlying field. Thus for $\sqrt{5 + 2\sqrt{6}}$ and setting $D = 2$ the algorithm produces the denesting $\sqrt{2} + \sqrt{3}$ rather than some expression in roots of unity. With respect to nested radicals of square roots our result generalizes results in [4], where a restricted class of nested radicals involving square roots was considered.

The algorithm is similar to the algorithm in [9] and for a special choice of D it is the same. The running time is polynomial in size of the splitting field of the input expression and can therefore be in the worst case exponential in the input size. Depending on the choice of the parameter D , compared to Landau's algorithm we need to work in field extensions of smaller degree. In these cases the algorithm will be more efficient than Landau's algorithm. Both, the algorithms in this paper and in [9] are always more efficient than the algorithms in [6]

The restriction that D is a multiple of the least common multiple of the degrees in the original expression can be avoided. Without this restriction the original expression may not be expressible at all using only D^{th} roots. Therefore, we show that for arbitrary D and an arbitrary algebraic number α , it can be decided in time polynomial in the size of the minimal polynomial of α whether α can be expressed as a nested radical involving only D^{th} roots. Here we have to assume that the ground field contains a primitive D^{th} root of unity. This result is a consequence of the breakthrough result on solvability by radicals obtained in [12] and the techniques presented in our paper.

The techniques of this paper provide alternative proofs to the structure theorems in [9]. Our proofs are simpler and more direct than the original proofs in [9]. In many respects we reverse the order of arguments in [9]. Instead of deriving field theoretic consequences from group theoretic arguments, we obtain the necessary field theoretic facts directly. Then we use these results to derive group theoretic consequences, which in turn lead to the algorithms. We thus provide a rather general framework to prove many of the known results on denestings.

The paper is organized as follows. Section 2 recalls the basic definitions and facts about (nested) radicals. Section 3 contains the basic structure theorems, while Section 4

shows how these structure theorems yield denesting algorithms. Section 5 describes the alternative proofs for Landau's results and Section 6 briefly deals with issues of solvability by radicals.

2 Definitions and basic facts

Except for some minor changes we follow the notation used in [6]. Let $K \supseteq \mathbf{Q}$ be an algebraic number field. In the following $*$ $\in \{+, -, \times, \div\}$. Nested radicals and their nesting depth are defined inductively. Hence an element $a \in K$ is a *nested radical of depth 0* over K , denoted $\text{depth}_K(a) = 0$. For any two nested radicals α, β over K , $\alpha * \beta$ is a nested radical over K . The depth of $\alpha * \beta$ is defined as $\text{depth}_K(\alpha * \beta) = \max\{\text{depth}_K(\alpha), \text{depth}_K(\beta)\}$. If α is a nested radical over K and $d \in \mathbf{N}, d > 1$, then $\sqrt[d]{\alpha}$ is a nested radical over K . The depth of $\sqrt[d]{\alpha}$ is $\text{depth}_K(\alpha) + 1$.

Let α be a nested radical over K . The *set of associated simple radicals* of α , denoted $S(\alpha)$, is defined as follows. If $\alpha \in K$ then $S(\alpha) = \{\alpha\}$. If $\alpha = \beta * \gamma$ then $S(\alpha) = S(\beta) \cup S(\gamma)$. Finally, if $\alpha = \sqrt[d]{\beta}$ then $S(\alpha) = S(\beta) \cup \{\sqrt[d]{\beta}\}$.

Due to the ambiguity of the symbol $\sqrt[d]{\alpha}$ a nested radical α over K does not refer to a unique algebraic number over K . A *radical valuation* resolves this ambiguity. Let R be the set of all nested radicals over K . A radical valuation v is a function $v : R \rightarrow \mathbf{C}$ such that $v(a) = a, a \in K$, $v(\alpha * \beta) = v(\alpha) * v(\beta)$, for all $\alpha, \beta \in R$, and $(v(\sqrt[d]{\alpha}))^d = v(\alpha)$, for all $\alpha \in R$ and all $d \in \mathbf{N}$. Let $\alpha \in K$. Informally, assuming that $v(\alpha)$ is already defined, a radical valuation v relates the symbol $\sqrt[d]{\alpha}$ to some specific d^{th} root of $v(\alpha) \in \mathbf{C}$. To simplify the notation, we will not mention the radical valuation v explicitly, writing $\sqrt[d]{\alpha}$, instead of $v(\sqrt[d]{\alpha})$. But it is always understood that $\sqrt[d]{\alpha}$ refers to some fixed algebraic number over K .

Let α, β be nested radicals over k . β is called a *denesting of α* iff the values of α and β are the same and $\text{depth}_K(\beta) \leq \text{depth}_K(\alpha)$. The nested radical β is called a *denested form of α* iff in addition for every denesting $\gamma \in R$ of α we have $\text{depth}_K(\beta) \leq \text{depth}_K(\gamma)$.

A radical α of depth 1 over K is called an *order d radical* iff $\alpha^d \in K$. An extension $K(\alpha_1, \dots, \alpha_n)$ is a *radical extension of K* iff α_i is a depth 1 radical for $i = 1, \dots, n$. The extension $K(\alpha_1, \dots, \alpha_n)$ is called an *order d radical extension* iff α_i is an order d radical for $i = 1, \dots, n$. By this definition an order d radical (an order d radical extension) is also an order D radical (an order D radical extension) for all D that are divisible by d .

As was done in [9] and [6] we will relate the nesting depth of nested radicals to the length of certain field towers. A field tower $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ is called a *radical tower over K* iff K_i is a radical extension of K_{i-1} for all $i = 1, \dots, n$. It is called an *order d radical tower* iff K_i is an order d radical extension of K_{i-1} for all $i = 1, \dots, n$. The integer n is called the *length* of the radical tower.

If $S(\alpha)$ is the set of associated radicals of some nested radical α , then we denote by $S_i \subseteq S(\alpha)$ the set of elements in $S(\alpha)$ of depth at most i . The *radical tower associated to*

α is given by the fields $K_i = K(S_i)$. Using these notions we can generalize the notion of order d radicals to that of order d nested radicals. A nested radical α is called an *order d nested radical* iff its associated radical tower is an order d radical tower. As before, an order d nested radical is also an order D nested radical for all D divisible by d .

From these definitions we immediately get

Lemma 2.1 *A nested radical α has depth n over K iff the associated radical tower has length n . The nesting depth of a denested form of α is the length of a shortest radical tower $K \subset K_1 \subset \dots \subset K_n$, such that $\alpha \in K_n$.*

The interesting part in computing a denesting for α is to determine the radical tower $K \subset K_1 \subset \dots \subset K_n$. Once the tower has been computed standard techniques can be used to express α as a nested radical of depth at most n [9].

Since we are mostly interested in order d radicals we make the following, final definition of this section.

Definition 2.2 *Let α be an order d nested radical over K . An order d nested radical β is called an order d denesting of α iff β has the same value as α and $\text{depth}_K(\beta) \leq \text{depth}_K(\alpha)$. β is called an order d denested form of α if in addition for all order d nested radicals γ having the same value as α , $\text{depth}_K(\beta) \leq \text{depth}_K(\gamma)$.*

Analogously to Lemma 2.1 we have

Lemma 2.3 *Let α be an order d nested radical. The nesting depth of an order d denested form of α is the length of a shortest order d radical tower $K \subset K_1 \subset \dots \subset K_n$, such that $\alpha \in K_n$.*

Frequently, the following basic facts about order d radicals and order d radical extensions will be used. Proofs for these facts can be found in [7]

Theorem 2.4 *Let $K \supseteq \mathbf{Q}$ be a field that contains a primitive d^{th} root of unity. If α is an order d radical over K , then its minimal polynomial over K is of the form $X^t - a$, where t divides d and $a \in K$. The extension $K(\alpha)$ is a Galois extension of K with cyclic Galois group of order t .*

Theorem 2.4 fails if K does not contain a primitive d^{th} root of unity. A simple counterexample is given by the 3^{rd} roots of unity. Over \mathbf{Q} they are the roots of $X^3 - 1$ which factors as $(X - 1)(X^2 + X + 1)$. Only the minimal polynomial of 1 has the form stated in the theorem. For the primitive 3^{rd} roots of unity the minimal polynomial is $X^2 + X + 1$. Hence only if K contains a primitive d^{th} root of unity can we assume that the degree of the field extension generated by an order d radical over K is a divisor of d . Theorem 2.4 is the reason that almost any algorithm dealing symbolically with radicals assumes that the ground field contains appropriate roots of unity. The exception being the algorithms

described in [2],[3]. Those algorithms deal with real radicals over real fields, in which case a theorem similar to Theorem 2.4 holds.

If the assumption of Theorem 2.4 hold, the structure of order d radical extensions is easy to describe.

Theorem 2.5 *Assume K contains a primitive d^{th} root of unity.*

(i) *If $L = K(\alpha_1, \dots, \alpha_n)$ is an order d radical extension of K , then L is a Galois extension of K . The Galois group $G(L/K)$ of L over K is an abelian group of exponent d .*

Conversely, if L is a Galois extension of K with abelian Galois group of exponent d , then L is an order d radical extension $K(\alpha_1, \dots, \alpha_n)$ of K .

(ii) *Every subfield of an order d radical extension $K(\alpha_1, \dots, \alpha_n)$ is an order d radical extension of K .*

3 Algebraic structure of denestings

Since any d^{th} root can also be considered a D^{th} root, provided d divides D , denesting a nested radicals involving only d^{th} roots by a nested radical involving only D^{th} roots is a special case of denesting a nested radical with d^{th} roots by a nested radical also containing only d^{th} roots. Therefore we will state all our results in this simpler form. However, the reader should bear in mind the more general formulation.

Throughout this section let $K \supseteq \mathbf{Q}$ be an algebraic number field, α is an order d nested radical over K . Let ζ_d be a primitive d^{th} root of unity. The field $K(\zeta_d)$ is denoted by F and the Galois closure of $F(\alpha) : F$ is denoted by L . The goal of this section is to prove the following theorem.

Theorem 3.1 *If β is an order d denesting of α with depth $\text{depth}_K(\beta) = n$, then there is an order d radical tower $F \subseteq F_1 \subseteq \dots \subseteq F_n = L$ such that F_i is a Galois extension of F for all $i = 1, \dots, n$.*

Combined with Lemma 2.3, the theorem guarantees a near optimal denesting of α . It is not optimal because the ground field for radical tower is $K(\zeta_d)$ rather than K . Therefore the denesting γ guaranteed by Theorem 3.1 will have the same nesting depth as β , but γ will be defined over the field F , not K . As will be seen in the proof, this is because Theorem 2.4 fails for fields not containing appropriate roots of unity. If we consider a primitive d^{th} root of unity an order d radical the theorem shows how to find a denesting of α over K whose depth differs from the optimal depth by 1.

The interesting part in computing a denesting for α is to determine the radical tower $F \subset F_1 \subset \dots \subset F_n$. Once the tower has been computed standard techniques can be used to express α as a nested radical of depth at most n .

To prove Theorem 3.1 first it is shown that we often may assume that a radical tower consists of Galois extensions of the ground field.

Definition 3.2 Let $M \subseteq \mathbf{Q}$ be an algebraic number field and let $M \subseteq M_1 \subseteq \dots \subseteq M_n$ be an order d radical tower over M . The corresponding Galois tower $M \subseteq L_0 \subseteq L_1 \subseteq \dots \subseteq L_n$ is defined as follows:

- $L_0 = M(\zeta_d)$
- If $M_i = M_{i-1}(\sqrt[d]{\gamma_1}, \dots, \sqrt[d]{\gamma_k})$ then

$$L_i = L_{i-1} \left(\sqrt[d]{\gamma_1^{(1)}}, \dots, \sqrt[d]{\gamma_1^{(n_1)}}, \dots, \sqrt[d]{\gamma_k^{(1)}}, \dots, \sqrt[d]{\gamma_k^{(n_k)}} \right),$$

where $\gamma_j^{(1)}, \dots, \gamma_j^{(n_j)}$ are the conjugates of $\gamma_j, j = 1, \dots, k$, over M , and for all j, ℓ , $\sqrt[d]{\gamma_j^{(\ell)}}$ is an arbitrary d^{th} -root of $\gamma_j^{(\ell)}$.

Since M_1 is generated over M by radicals $\sqrt[d]{\gamma}, \gamma \in M$, we see that $L_1 = M_1(\zeta_d)$. Other properties of the Galois tower corresponding to a radical tower are collected in the next lemma.

Lemma 3.3 The Galois tower $M \subseteq L_0 \subseteq L_1 \subseteq \dots \subseteq L_n$ corresponding to an order d radical tower $M \subseteq M_1 \subseteq \dots \subseteq M_n$ has the following properties:

- (i) $L_i, i = 0, \dots, n$, is a Galois extensions of M .
- (ii) The Galois closure of M_i over M is contained in $L_i, i = 1, \dots, n$.
- (iii) The extensions $L_i : L_{i-1}, i = 1, \dots, n$, are order d radical extensions.

Proof:

- (i) The proof is by induction on i . Since L_0 is generated by a root of unity it is a Galois extension. So assume that it has already been shown that $L_{i-1}, i \geq 1$, is a Galois extension. To prove that L_i is a Galois extension of F , let $M_i = M_{i-1}(\sqrt[d]{\gamma_1}, \dots, \sqrt[d]{\gamma_k})$ and let $\gamma_i^{(1)}, \dots, \gamma_i^{(n_i)}$ be the conjugates of γ_j over M . Consider the polynomial

$$g(X) = \prod_{j=1}^k \prod_{\ell=1}^{n_j} (X^d - \gamma_j^{(\ell)}).$$

By Galois theory $g(X)$ is a polynomial in $M[X]$. Hence, for arbitrary values of $\sqrt[d]{\gamma_j^{(\ell)}}$ the extension $M \left(\zeta_d, \sqrt[d]{\gamma_1^{(1)}}, \dots, \sqrt[d]{\gamma_1^{(n_1)}}, \dots, \sqrt[d]{\gamma_k^{(1)}}, \dots, \sqrt[d]{\gamma_k^{(n_k)}} \right)$ is a Galois extension of M . But then $L_{i-1}M \left(\zeta_d, \sqrt[d]{\gamma_1^{(1)}}, \dots, \sqrt[d]{\gamma_1^{(n_1)}}, \dots, \sqrt[d]{\gamma_k^{(1)}}, \dots, \sqrt[d]{\gamma_k^{(n_k)}} \right) = L_i$ is the composite of two Galois extension and hence a Galois extension.

Let $F \subseteq L_1 \subseteq \dots \subseteq L_n$ be the Galois tower corresponding to the order d radical tower of $F \subseteq K_1F \subseteq \dots \subseteq K_nF$. By Corollary 3.4 the fields L_i also form an order d radical tower over F . Since $\alpha \in K_n$ we have $L \subseteq L_n$.

Define $F_i = L_i \cap L, i = 1, \dots, n$. For convenience set $F = F_0$. Note that as an intersection of two Galois extensions F_i is a Galois extension of $F = F_0$. We claim that the fields $F_i, i = 0, \dots, n$, form an order d radical tower over $F = F_0$. Since $F_n = L$, this will prove the theorem.

To show that F_i is an order d radical extension of $F_{i-1}, i = 1, \dots, n$, we apply Theorem 3.5 with $k = F, F_i = M$, and $E = L_{i-1}$ (recall Figure 1).

The extension $F_i L_{i-1}$ of L_{i-1} is a subfield of the order d radical extension L_i of L_{i-1} . By Theorem 2.5 it is itself an order d radical extension of L_{i-1} . Since F and hence L_{i-1} contain a primitive d^{th} root of unity, Theorem 2.5 also shows that $F_i L_{i-1}$ is Galois over L_{i-1} with abelian Galois group of exponent d . By Theorem 3.5 the extension F_i over $L_{i-1} \cap F_i = L_{i-1} \cap L = F_{i-1}$ is Galois with abelian Galois group of exponent d . Applying Theorem 2.5 shows that F_i is an order d radical extension of F_{i-1} . \square

In Section 5 we will show that similar proofs can be used to prove the two main structure theorems in [9]. The proofs we obtain are simpler and more direct than the original proofs in [9].

4 Computing an order d denesting

As in the previous sections, $K \supseteq \mathbf{Q}$ is an algebraic number field. $F = K(\zeta_d)$, where ζ_d is a primitive d^{th} root of unity. α is an order d nested radical over K and L is the Galois closure of $F(\alpha)$ over F . By $G = G(L/F)$ denote the Galois group of L over F . The neutral element of G is denoted id .

By Theorem 3.1 the depth of a denested form β of α is related to the length of radical towers between F and L . Hence we make the following definition.

Definition 4.1 *A radical tower $F \subset F_1 \subset \dots \subset F_n = L$ is called the shortest radical tower for L iff for any other radical tower $F \subseteq L_1 \subseteq \dots \subseteq L_m = L$ between F and L*

(i) $n \leq m$

(ii) $L_i \subseteq F_i$ for all $i = 1, \dots, m$, setting $F_j = F_n$ for $j > n$.

The order d radical tower $F \subset F_1 \subset \dots \subset F_n = L$ is the shortest radical tower of order d for L if these conditions are met by any order d radical tower $F \subseteq L_1 \subseteq \dots \subseteq L_m = L$ between F and L .

Due to condition (ii) the shortest radical tower is unique. Lemma 3.3 and Corollary 3.4 show that in the shortest order d radical tower $F \subset F_1 \subset \dots \subset F_{n-1} \subset F_n = L$, each intermediate field F_i is a Galois extension of F .

By Galois theory an order d radical tower between F and L corresponds to a chain of normal subgroups $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_{n-1} \supset G_n = \{\text{id}\}$, where the factor groups $G_i/G_{i+1}, i = 0, \dots, n-1$, are abelian of exponent d . We will call such a chain of groups an *abelian chain of exponent d for G* . The *shortest abelian chain of exponent d* is the chain of groups $G = G_0 \supset G_1 \supset \dots \supset G_{n-1} \supset G_n = \{\text{id}\}$ such that for any other chain $G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_{m-1} \supset H_m = \{\text{id}\}$, that is abelian and of exponent d , we have $n \leq m$ and $H_i \supseteq G_i$ for all $i = 1, \dots, m$. Here $G_j = \{\text{id}\}$ for $j > n$. Due to the condition $H_i \supseteq G_i$, the shortest abelian chain of exponent d is unique.

We say that the multiplicatively written group G is given by a group table, if we have a table that contains for every pair of elements $x, y \in G$ its product $z = xy$.

Theorem 4.2 *Let G be given by a group table. The shortest abelian chain of exponent d for G can be computed in time polynomial in $|G|$.*

Proof: We need some terminology from group theory. Let H be an arbitrary group. For any subset S of H the *normal closure* of S is the smallest normal subgroup of H containing S . The *commutator subgroup* of H is the smallest normal subgroup $C = C(H)$ of H whose factor group H/C is abelian. C is uniquely defined, that is, any normal subgroup N of H with abelian factor group H/N contains the commutator C .

To prove the theorem we define a specific abelian chain of exponent d , show that it is the shortest abelian chain of exponent d , and finally show that it can be computed in polynomial time.

Let $G_0 = G$. Assuming $G_i, i \geq 0$, has already been defined and is not the trivial group, G_{i+1} is defined as follows. By G_i^d denote the set of all d^{th} powers of elements in G_i . By $C(G_i)$ denote the commutator subgroup of G_i . Then G_{i+1} is defined as the normal closure of $G_i^d \cup C(G_i)$ in G_i .

Let $G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_{m-1} \supseteq H_m = \{\text{id}\}$ be an arbitrary abelian chain of order d . We show by induction that $G_i \subseteq H_i$. Obviously, $G_0 \subseteq H_0$. So assume that $G_j \subseteq H_j$ has already been proven for all $j \leq i$. We need to show $G_{i+1} \subseteq H_{i+1}$.

By definition H_i/H_{i+1} is abelian of exponent d , hence $H_i^d \subseteq H_{i+1}$. Since $G_i \subseteq H_i$ we also have $G_i^d \subseteq H_{i+1} \cap G_i$. By the isomorphism theorems for groups (see [7]) $H_{i+1} \cap G_i$ is a normal subgroup of G_i and $G_i/(H_{i+1} \cap G_i)$ is isomorphic to $G_i H_{i+1}/H_{i+1}$. As a subgroup of H_i/H_{i+1} the group $G_i H_{i+1}/H_{i+1}$ is abelian. Hence $H_{i+1} \cap G_i$ contains the commutator of G_i .

So far it has been shown, that the normal subgroup $H_{i+1} \cap G_i$ contains G_i^d and the commutator $C(G_i)$, but then it contains the normal closure of $G_i^d \cup C(G_i)$ in G_i , proving that $G_{i+1} \subseteq H_{i+1}$.

It remains to prove that the G_i 's can be computed in polynomial time. Given G_i the set G_i^d can be computed in polynomial time. The commutator $C(G_i)$ can also be computed in polynomial time. An efficient algorithms for this problem can be found in [1]. Finally, given G_i^d and $C(G_i)$ the normal closure of their union can again be computed by using algorithms described in [1]. \square

Before we can state and prove the main theorem of this paper some terminology from algorithmic algebra is needed.

Every algebraic number field has the form $\mathbf{Q}(\gamma)$, where we can assume that γ is an algebraic integer. The length of a polynomial $p(X) \in \mathbf{Q}[X]$ is defined as the sum of the absolute values of its coefficients.

If $\beta = \frac{1}{b} \sum_{i=0}^{n-1} b_i \gamma^i$ is an element of the algebraic number field $\mathbf{Q}(\gamma)$, the representation size $[\beta]$ of β is defined as $\max\{|b|, |b_0|, |b_1|, \dots, |b_{n-1}|\}$. For a polynomial f in $\mathbf{Q}(\gamma)[X]$ its length is defined as the sum of the representation sizes of its coefficients.

Theorem 4.3 *Let $K = \mathbf{Q}(\gamma)$ be an algebraic number field, where the field generator is an algebraic integer with minimal polynomial $p(X) \in \mathbf{Z}[X]$. Let α be an order d nested radical over K . If an order d denested form of α over K has depth n , then an order d denesting over $F = K(\zeta_d)$ of α of depth at most n can be found in time polynomial in the length of p , in the representation size of the minimal polynomial of α over K and in the degree of the Galois closure of $F(\alpha)$ over F .*

In the theorem we assume that the minimal polynomial of α over K is given. If that is not the case, that is, if we only have a nested radical expression for α , the minimal polynomial of α can be computed in time polynomial in the representation size of the minimal polynomial (see [9]).

Proof: If α has an order d denested form of depth n over K , then Theorem 3.1 shows that there is an order radical tower $F \subseteq F_1 \subseteq \dots \subseteq F_{n-1} \subseteq F_n = L$ of length n between F and the Galois closure L of $F(\alpha)$. The fields in this tower are Galois over F . Hence this radical tower corresponds to an abelian chain of exponent d for the Galois group G of L over F . Therefore a shortest abelian chain of exponent d has length at most n .

The group G can be computed within the time bounds stated in the theorem (see [8]). By Theorem 4.2 within this time bound we can compute the shortest abelian chain of exponent d for G . This chain corresponds to an order d radical tower $F = L_0 \subset L_1 \subset \dots \subset L_m = L$ between F and L , with $m \leq n$.

To obtain the desired denesting for α it suffices to compute for each extension $L_i : L_{i-1}$ a set of order d radicals that generate the extension and to express α as an element of $L_m = L$. For these problems we can use the algorithms described in [9]. Also, the analysis given there can be applied to the present case. \square

For $d = 2$ a primitive root is given by -1 . Hence the theorem implies that over arbitrary number fields for a nested radical α involving only square roots an order 2 denested form can be computed within the time bounds stated in the theorem. Therefore Theorem 4.3 generalizes the results in [4].

5 Alternative proofs for Landau's structure theorems

In this section we show how to use the methods of the previous sections to prove the main theorems of Landau's paper [9].

Theorem 5.1 (Landau) *Suppose α is a nested radical over a field $K \supset \mathbf{Q}$ that contains all roots of unity. Then there is a denested form γ of α over K such that the radical tower associated to γ is contained in the Galois closure L of $K(\alpha)$.*

Proof: Let β be any denested form of α . Let d be the least common multiple of the orders of the radicals appearing in β . We now apply Theorem 3.1. In the present case $F = K(\zeta_d) = K$. Hence the theorem gives a radical tower of length n between K and the Galois closure of $K(\alpha)$ over K . This radical tower corresponds to a denesting as stated in the theorem (see Lemma 2.1). \square

Landau's second main structure theorem for denestings avoids fields containing all roots of unity. To state and prove this result we need additional facts from group theory and Galois theory. Let G be a group. As mentioned before, the commutator subgroup $C(G)$ of G is the smallest subgroup of G with abelian factor group. The *derived series* $D^i(G)$, $i = 0, 1, \dots$, is inductively defined as follows: $D^0(G) = G$ and for $i > 0$, $D^i(G) = C(D^{i-1}(G))$, that is, $D^i(G)$ is the commutator of $D^{i-1}(G)$. A group G is called solvable iff there is an $s > 0$ with $D^s(G) = \{\text{id}\}$, where $\text{id} \in G$ is the neutral element in G . In this case, the derived series is the finite chain of subgroups $G = D^0(G) \supset D^1(G) \supset \dots \supset D^{i-1}(G) \supset D^s(G) = \{\text{id}\}$.

By definition, the chain of subgroups $G = D^0(G) \supset D^1(G) \supset \dots \supset D^{i-1}(G) \supset D^n(G) = \{\text{id}\}$ has the property that for each i the factor group $D^{i-1}/D^i(G)$ is abelian. If G is solvable, then the derived sequence is the shortest chain of subgroups with this property. More precisely, if $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_t$ is any chain of subgroups of G such that G_{i-1}/G_i is abelian, then $G_i \supseteq D^i(G)$.

A classical result in Galois theory states that a polynomial f defined over some extension K of \mathbf{Q} is solvable by radicals iff the Galois group of f is a solvable group. Here the Galois group of f is the Galois group of the extension of K generated by all roots of f .

Let $K \supseteq \mathbf{Q}$ and let L be a Galois extension of K with solvable Galois group G . By Galois theory, there is a one-to-one correspondence between subfield towers $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{n-1} \subseteq K_n = L$ such that K_i is a Galois extension of K and is an abelian extension of K_{i-1} , and chains of subgroups $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_{n-1} \supseteq G_n = \{\text{id}\}$

such that $G_i, i = 1, \dots, n$, is a normal subgroup of G_{i-1} with abelian factor group. In particular, the shortest subfield tower with the property that each intermediate extension is abelian corresponds to the derived series of G .

Now we are in a position to state Landau's second structure theorem on denestings using roots of arbitrary order.

Theorem 5.2 (Landau) *Let α be a nested radical over a field $K \supseteq \mathbb{Q}$. Let L be the Galois closure of $K(\alpha) : K$ with Galois group G . Let l be the least common multiple of the exponents of the derived series of G and let ζ_l be a primitive l^{th} root of unity. If there is a denesting β for α of depth n over K , then there is a denesting γ of α of depth $n + 1$ over $K(\zeta_l)$, such that each field in the radical tower associated to γ is contained in $L(\zeta_l)$.*

Proof: Let d be the least common multiples of the orders of the radicals appearing in β . Let ζ_d be a primitive d^{th} root of unity. Let $K \subseteq K_1 \subseteq \dots \subseteq K_n$ be the order d radical tower associated to β . By $K \subseteq L_0 \subseteq L_1 \subseteq \dots \subseteq L_n$ denote the Galois tower corresponding to this order d radical tower. Define $F_i = L \cap L_i, i = 0, \dots, n$. Observe that $\alpha \in K_n \subseteq L_n$. Furthermore L_n is a Galois extension of K , therefore $L \subseteq L_n$ and $F_n = L$.

$F_i, i = 0, \dots, n$, is an intersection of two Galois extensions of K , hence F_i is a Galois extension of K . Next it is shown that the extensions $F_0 : K$ and $F_i : F_{i-1}, i = 1, \dots, n$, are abelian extensions. L_0 is a field generated over K by a root of unity. Hence L_0 and all of its subfields, including F_0 , are abelian extensions of K .

To prove that $F_i : F_{i-1}, i \geq 1$, is an abelian extension, we will apply Theorem 3.5 with $k = K, M = F_i$, and $E = L_{i-1}$. Consider the field $F_i L_{i-1}$. It is a subfield of the extension $L_i : L_{i-1}$, which by Lemma 3.3 is an order d radical extension. By Theorem 2.5 $F_i L_{i-1} : L_{i-1}$ is an order d radical extension of L_{i-1} . In particular, it is an abelian extension of L_{i-1} . Theorem 3.5 implies that F_i is an abelian extension of $L_{i-1} \cap F_i = F_{i-1}$.

Summarizing, we have shown that the existence of a denesting β of α of depth n implies the existence of a subfield tower $K \subseteq F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = L$ between K and L with the property that the F_i 's are Galois extensions of K and the intermediate extensions $F_i : F_{i-1}$ are abelian. Hence the shortest tower with this property has length at most $n + 1$. But from what has been said above, this implies that the derived series of G has length at most $n + 1$, that is $D^{n+1}(G) = \{\text{id}\}$.

Consider the subfield tower $K = E_0 \subset E_1 \subset E_2 \subset \dots \subset E_m = L, m \leq n + 1$, corresponding to the derived series of G . It is a tower of Galois extension, where the intermediate extensions $E_i : E_{i-1}$ are abelian. Moreover, by definition of l the Galois groups of the intermediate extensions have exponent l . By Theorem 2.5 the field tower $K(\zeta_l) \subseteq E_1(\zeta_l) \subseteq \dots \subseteq E_m(\zeta_l) = L(\zeta_l)$ is an order l radical tower. Since $\alpha \in L(\zeta_l)$ this radical tower gives rise to a denesting γ of α as stated in the theorem. \square

If we adjoin ζ_l and ζ_d to every element in the tower $K \subset E_1 \subset \dots \subset E_m = L$, then $K(\zeta_d, \zeta_l) = E_0(\zeta_d, \zeta_l)$ and we obtain a radical tower of length at most n and therefore a

denesting of α over $K(\zeta_d, \zeta_l)$ of depth at most n . This gives the following corollary, also originally proved in Landau's paper [9].

Corollary 5.3 (Landau) *Let α be an order d nested radical over a field $K \supseteq \mathbf{Q}$. Let L be the Galois closure of $K(\alpha) : K$ with Galois group G . Let l be the least common multiple of the exponents of the derived series of G and let ζ_d, ζ_l be primitive d^{th} and primitive l^{th} roots of unity. If there is a denesting β for α of depth n over K , then there is a denesting γ of α of depth n over $K(\zeta_d, \zeta_l)$, such that each field in the radical tower associated to γ is contained in $L(\zeta_d, \zeta_l)$.*

In Landau's and in our proofs of Theorem 5.2 the main step is the construction of the field tower $K \subset E_1 \subset \dots \subset E_m = L$. In the original proofs this was done using group theory. In the proofs given above this is done directly using field theory. Hence these proofs are somewhat more intuitive. The basic argument of the proofs of Theorem 3.1, Theorem 5.1, and Theorem 5.2 is that, given a denesting β for α and the radical tower associated to β , intersect the elements of this radical tower with the Galois closure L of $K(\alpha)$ over K to obtain a field tower between K and L with properties similar to those of the radical tower associated to β . However, some technical difficulties arise in order to transfer the properties of the associated radical tower to the subfield tower between K and L . For arbitrary fields most field theoretic properties are lost by taking intersections. For Galois extensions, on the other hand, many properties are preserved if we take intersections. Hence we introduced the Galois tower corresponding to a radical tower.

6 Solvability by order d radicals

The algorithm leading to Theorem 4.3 can be used to determine whether the root α of a polynomial f over some algebraic number field $K = \mathbf{Q}(\gamma)$, that contains a primitive d^{th} root of unity, can be expressed as an order d nested radical. First compute the Galois group of $K(\alpha)$ over K , then try to compute an abelian chain of exponent d for this group. If this fails, α cannot be expressed as an order d nested radical. Otherwise, the algorithm will find such an expression for α .

In this section we will show that if we are only interested in deciding whether α can be expressed as an order d nested radical we can do much better. In fact, we will see that the decision problem can be solved in polynomial time.

A polynomial f over some field K is called *solvable by radicals over K* iff there is a nested radical α over K that solves f , that is, $f(\alpha) = 0$. We say that *the field extension $F : K$ is solvable by radicals over K* iff $F = K(\alpha)$ and the minimal polynomial f of α is solvable. Analogously, we can define what it means for a polynomial or a field extension to be *solvable by order d radicals*.

In [12] Landau and Miller showed that, given a polynomial f over some algebraic number field K , the question whether the polynomial is solvable by radicals can be decided

in time polynomial in the representation size of f , as defined in Section 4. We need to review the proof in [12]. Given the polynomial f , Landau and Miller consider the field F generated by a root of f . They construct a tower of subfields $K = F_0 \subset F_1 \subset \dots \subset F_n = F$ such that if f , and hence $F : K$, is solvable then the degree of the Galois closure of $F_i : F_{i-1}$, $i = 1, \dots, n$, is bounded by $[F_i : F_{i-1}]^4$, where $[F_i : F_{i-1}]$ is the degree of the extension $F_i : F_{i-1}$. A classical result in algebra says that $F : K$ is solvable iff the Galois group of $F : K$ is solvable. Hence $F : K$ is solvable iff all extensions $F_i : F_{i-1}$ are solvable. Due to the fact that, if f is solvable, then the Galois closures of these extensions have polynomial degree, this can be tested in polynomial time in a straightforward manner.

To extend the result of Landau and Miller to solvability by order d radicals observe that as before a field extension $F : K$ is solvable by order d radicals iff for all subfields $K \subset E \subset F$ the extensions $E : K$ and $F : E$ are solvable by order d radicals. Hence we can use the field tower $K = F_0 \subset F_1 \subset \dots \subset F_n = F$ constructed in [12] to reduce solvability of f and of $F : K$ by order d radicals to solvability of the extensions $F_i : F_{i-1}$ by order d radicals. But assuming that K and hence all F_i contain a primitive d^{th} root of unity, Theorem 4.3 shows that in polynomial time we can compute an order d denested form of a generator of the extension $F_i : F_{i-1}$. In particular, it can be decided in polynomial time whether the extension $F_i : F_{i-1}$ is solvable by order d radicals. Hence we have

Theorem 6.1 *Let $K = \mathbf{Q}(\gamma)$ be an algebraic number field, where the field generator is an algebraic integer with minimal polynomial $p(X) \in \mathbf{Z}[X]$. Assume that K contains a primitive d^{th} root of unity. Let f be a polynomial over K . It can be decided in time polynomial in the length of p and in the length of f , whether f is solvable by order d radicals over K .*

Under the assumptions of the previous theorem, if f is solvable by an order d nested radical α then such a radical can also be computed in polynomial time. This can be done as follows. Let the field tower $K \subset F_1 \subset \dots \subset F_n = F$ be as in the proof above. Define fields L_i , $i = 1, \dots, n$, inductively as follows. L_1 is the Galois closure of F_1 over K and having defined L_{i-1} , $i \geq 1$, L_i is the Galois closure of F_i over L_{i-1} . If f is solvable by an order d radical then the extensions $F_i : F_{i-1}$, $i = 1 \dots, n$ are solvable by order d radicals. Using the same arguments as in the proof of Lemma 3.3 it can be shown that each extension $L_i : L_{i-1}$ is solvable by order d radicals. The algorithm to compute a nested radical α solving f first computes the F_i 's and L_i 's, then it computes the Galois groups G_i of the extensions $L_i : L_{i-1}$. For each G_i the derived series is computed. Using the derived series the algorithms in [9] are used to compute a nested radical α_i generating $L_i : L_{i-1}$. Finally, a nested radical α solving f is an element of L_n and therefore can be expressed in terms of the α_i 's.

From what has been shown in Section 4 and by the results in [9] the running time is bounded by a polynomial in the length of p and f , and in the degree $[L_n : K]$. We know that the degree of $L_i : L_{i-1}$ is less than the degree of the the Galois closure of F_i over F_{i-1} , which by construction of the F_i is less than $[F_i : F_{i-1}]^4$, Hence the degree $L_n : K$ is

bounded by

$$[L_n : K] \leq \prod_{i=1}^n [L_i : L_{i-1}] \prod_{i=1}^n [F_i : F_{i-1}]^4 \leq [F : K]^4.$$

This proves that the running time of the algorithm is polynomial.

References

- [1] L. Babai, E. Luks, Á. Seress, “Fast management of permutation groups”, *Proc. 29th Symposium on Foundations of Computer Science* 1988, pp. 272-282.
- [2] J. Blömer, “Computing Sums of Radicals in Polynomial Time”, *Proc. 32nd Symposium on Foundations of Computer Science* 1991, pp. 670-677.
- [3] J. Blömer, “Denesting Ramanujan’s Nested Radicals”, *Proc. 33rd Symposium on Foundations of Computer Science* 1992, pp. 447-456.
- [4] A. Borodin, R. Fagin, J. E. Hopcroft, M. Tompa, “Decreasing the Nesting Depth of Expressions Involving Square Roots”, *Journal of Symbolic Computation* Vol. 1, pp. 169-188, 1985.
- [5] B. Caviness, R. Fateman, “Simplification of Radical Expressions”, *Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation*, ACM, New York, 1976.
- [6] G. Horng, M. -D. Huang, “Simplifying Nested Radicals and Solving Polynomials by Radicals in Minimum Depth”, *Proc. 31st Symposium on Foundations of Computer Science* 1990, pp. 847-854.
- [7] S. Lang, *Algebra*, 3rd edition, Addison-Wesley, 1993.
- [8] S. Landau, “Factoring polynomials over algebraic number fields”, *SIAM Journal on Computing* Vol. 14, No. 1, pp. 184-195, 1985.
- [9] S. Landau, “Simplification of Nested Radicals”, *SIAM Journal on Computing* Vol. 21, No. 1, pp. 85-110, 1992.
- [10] S. Landau, “A Note on Zippel-Denesting”, *Journal of Symbolic Computation*, Vol. 13, pp. 41-46, 1992.
- [11] S. Landau, “How to Tangle with a Nested Radical,” *Mathematical Intelligencer*, Vol. 16, No. 2, pp. 49-55, Spring 1994.
- [12] S. Landau, G. L. Miller, “Solvability by Radicals is in Polynomial Time”, *Journal of Computer and System Sciences* Vol. 30, pp. 179-208, 1985.
- [13] S. Ramanujan, *Problems and Solutions, Collected Works of S. Ramanujan*, Cambridge University Press, 1927.
- [14] R. Zippel, “Simplification of Expressions Involving Radicals”, *Journal of Symbolic Computation* Vol. 1, pp. 189-210, 1985.