How to Denest Ramanujan's Nested Radicals *

Johannes Blömer
Institut für Informatik, Fachbereich Mathematik
Freie Universität Berlin
Arnimallee 2-6, W-1000 Berlin 33, Germany

Abstract

We present a simple condition when nested radical expressions of depth two can be denested using real radicals or radicals of some bounded degree. We describe the structure of these denestings and determine an upper bound on the maximum size of a denesting. Also for depth two radicals we describe an algorithm that will find such a denesting whenever one exists. Unlike all previous denesting algorithms our algorithm does not use Galois theory. In particular, we avoid the construction of the minimal polynomial and splitting field of a nested radical expression. Thus we can obtain the first denesting algorithm whose run time is at most, and in general much less, than polynomial in description size of the minimal polynomial. The algorithm can be used to determine non-trivial denestings for expressions of depth larger than two.

1 Introduction

Throughout the last years the problem of denesting or simplifying radicals has been studied intensively by various mathematicians and computer scientists ([2],[3],[6],[7],[12]). Many of them have been attracted by equations of Ramanujan [9] such as the following:

$$\sqrt[3]{\sqrt[3]{2}-1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}} \quad (1)$$

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \frac{1}{3}\left(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}\right) \quad (2)$$

$$\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{\frac{5}{3}} - \sqrt[3]{\frac{2}{3}}. \quad (3)$$

These examples sufficiently explain the problem itself. Denesting a radical expression means decreasing its nesting depth over a field F. For example, the depth over $\mathbb{Q}$ of the left-hand side of Ramanujan's equations is 2 while the depth of the right-hand side is 1.

But if we are given a nested radical expression and are asked to denest it then this is at first not a meaningful question because for different values of the roots involved we may get different denestings. For example, if $\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$ has to be denested in general we will assume that the two square roots have the same value and that perhaps the real third roots are meant. In this case the formula denests to 1. But if one of the square roots is positive and the other one negative the formula denests to a square root of 5, provided we still take real third roots. And for the complex third roots the denestings are again different. So the values of the roots involved in the nested radical expression have to be specified in advance and denesting a radical means finding a radical expression with the same value and of smaller depth.

In the last years a lot of progress has been made for the general problem of denesting radicals. S. Landau [6] showed how to compute a denesting for a nested radical expression that is just one off the optimal one. Horng and Huang [3] achieved a minimal denesting and also showed how to solve a polynomial by radicals of minimum nesting depth, if it is solvable by radicals at all. However, in both cases the denestings are with respect to a field containing all roots of unity. As it turns out to compute these denestings one need not consider a field containing all roots of unity which would clearly be computationally infeasible. Rather it suffices to work with a field generated by a single root of unity. Unfortunately, the order of this root is either one- (Landau) or even double-exponential (Horng, Huang) in the description size of the minimal polynomial of the expression to be denested.

These results still leave many theoretical and practical problems unanswered. For example, the denestings of Landau and Horng, Huang will always use roots of unity. On the other hand, Ramanujan's examples above use no roots of unity at all. Hence the role roots

*This research was supported by the ESPRIT II Basic Research Action of the European Community under contract No. 3075 (project ALCOM)

0-8186-2900-2/92 $3.00 © 1992 IEEE

of unity play in denesting radicals is not satisfactorily explained.

Moreover, the algorithms in [3] and [6] are inefficient. Their run time is (double-)exponential in the description size of the minimal polynomial of the nested radical expression. There is good reason to believe that this behavior is unavoidable in the approach taken in these papers. Both results use Galois theory and rely on computing the splitting field of the radical expression. But the degree of this field over $\mathbf{Q}$, say, is in general exponential in the degree of the minimal polynomial. Hence from a practical point of view it would be interesting to obtain algorithms with a better run time. Perhaps one would even be satisfied with denesting algorithms that may not achieve minimal depth but compute certain non-trivial denestings and run efficiently.

Taking a totally different approach than Landau and Horng, Huang, and especially avoiding Galois theory, in this paper we answer some open questions concerning nested radicals.

Consider for example Equation (3) given above. Multiplying the equation by $\sqrt[3]{12}$ for a real third root yields

$$\sqrt[6]{1008\sqrt[3]{20} - 2736} = \sqrt[3]{20} - 2.$$

And both, the right-hand side of this equation and the expression under the six root, are elements of the field generated by $\mathbf{Q}$ and $\sqrt[3]{20}$. We prove that there is a general pattern behind this behavior. To be more specific, we show the following generalization of a theorem due to Borodin et al. [2].

Let $F \subset \mathbf{R}$ be a real field and $F' = F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k}), \sqrt[d_1]{q_1}, \ldots, \sqrt[d_k]{q_k} \in F$, a radical extension of F such that any $\sqrt[d_i]{q_i}$ is real. If $\sqrt[d]{\gamma}$, $d \in \mathbf{N}$, is contained in some radical extension of F generated by real radicals of depth one over F then there exists an element $q \in F \setminus \{0\}$ with $\sqrt[Nd]{q}\sqrt[d]{\gamma} \in F'$. Here N is the degree of the extension $F' : F$.

Since F' has a basis over F consisting of depth one radicals this theorem leads to a denesting for $\sqrt[d]{\gamma}$. In particular, it applies to Ramanujan's examples and explains why no roots of unity appear in his denestings.

To some extend this result generalizes to complex radicals. In that case the base field has to contain a certain root of unity. But its degree is much smaller than the degree of the roots of unity required by the results of Landau and Horng, Huang.

These theorems explain the structure of certain denestings but in order to compute the denestings we need to determine the elements q in F with $\sqrt[Nd]{q}\sqrt[d]{\gamma} \in F'$. The main part of this paper is devoted to this problem.

In case F' is a Galois extension of F (which in general cannot be the case if F is real and F' is a radical extension) this problem has already been considered in [7],[12]. We give a much simpler characterization of the elements in F with this property that applies to arbitrary extensions.

If the field F is an algebraic number field this characterization leads to an algorithm that determines whether such an element exists, and if so, computes it. The run time of the algorithm is polynomial in the degree N of the extension $F' : F$, in d, and in the bit size of the representation of γ.

N may be as large as the product of the degree of the radicals appearing in γ but - as the basic theorem shows - the output size may also be $\Omega(N)$; so with respect to N this is the best we can hope for. Moreover, it can be shown that if γ is a linear combination of $\sqrt[d_i]{q_i}$ such that the radicals $\sqrt[d_i]{q_i}$ are linearly independent over F, then N is the degree of the minimal polynomial of γ.

We also believe that the dependence on d is best possible, i.e., no algorithm with run time polynomial in $\log d$, for example, exists. Although so far we cannot prove this, the characterizations of elements q with $\sqrt[Nd]{q}\sqrt[d]{\gamma} \in F'$ indicates that the representation of q may be of size $\Omega(d)$.

As it turns out these results already suffice to denest sums and quotients of nested radicals. In particular, it is shown that for sums of nested radicals one only needs to consider any ratio of two terms in the sum.

To prove the run time we use a general technique that may be of independent interest. We show how to compute in polynomial time the exact representation of an element β in a number field $\mathbf{Q}(\alpha)$, provided an upper bound B on the representation size of β is given and an approximation $\overline{\beta}$ to β is known such that the number of correct bits in $\overline{\beta}$ is roughly quadratic in B. The algorithm is an application of the lattice basis reduction of Lenstra et al. [8]. We believe that this algorithm will prove to be useful in many other algebraic problems.

Since the denesting algorithms of this paper work for arbitrary number fields they can be applied to radical expressions of depth larger than two in order to detect non-trivial denestings. But even if applied repeatedly the algorithms are not guaranteed to produce such general minimum depth denestings as in [6] and [3]. On the other hand, the algorithms of this paper do compute certain denestings that cannot be obtained by the algorithms of S. Landau, for example, they compute denestings like the ones found by Ramanujan.

2 The structure of radical extensions

In this section we state a few facts on radical extensions which have already been used in [1] and were originally proven by C. L. Siegel [10].

Definition 1 *Let F be a subfield of the complex numbers $\mathbb{C}$. An element $\rho \in \mathbb{C}$ is called a* **radical of order** *d over F, $d \in \mathbb{N}$, if*

$$\rho^d \in F.$$

An extension $F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k})$ of F generated by radicals over F is called a **radical extension**.

Observe that the order of a radical over F need not be the degree of its minimal polynomial over F. The order is not even uniquely defined rather if ρ is of order d then it is also a radical of order D for all multiples D of d.

As it turns out the following lemmata which appear in Siegel's paper as corollaries can easily be shown directly. Siegel's main result is an immediate consequence of these lemmata.

Lemma 2 *Let F be a real field and let $\sqrt[d_i]{q_i}$, $i = 1, \ldots, k$, be real radicals over F. By n_i denote the degree of the extension $F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_i]{q_i}) : F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_{i-1}]{q_{i-1}})$.*
If $\sqrt[d_k]{q_k} \in F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_{k-1}]{q_{k-1}})$ then

$$\sqrt[d_k]{q_k} = c \prod_{i=1}^{k-1} \sqrt[d_i]{q_i}^{e_i}$$

for some $c \in F$ and $e_i \in \mathbb{N}$, $0 \leq e_i < n_i$.

For complex radicals this lemma generalizes in the following way.

Lemma 3 *Let F be a field and let $\sqrt[d_i]{q_i}$, $i = 1, \ldots, k$, be arbitrary radicals over F. Furthermore assume that the field F contains primitive d_i-th roots of unity. If $\sqrt[d_k]{q_k}$ is an element of $F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_{k-1}]{q_{k-1}})$ then $\sqrt[d_k]{q_k}$ has the form*

$$\sqrt[d_k]{q_k} = c \prod_{i=1}^{k-1} \sqrt[d_i]{q_i}^{e_i}$$

for some $c \in F$ and positive integers e_i satisfying $0 \leq e_i < n_i$, where n_i is defined as above.

Throughout this paper we consider only radical extensions $F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k})$ such that either $F \subset \mathbb{R}$ and $\sqrt[d_i]{q_i} \in \mathbb{R}$ or such that F contains primitive d_i-th roots of unity. We refer to these cases as the *real* and *complex case*, respectively.

It will not be used in this paper but for the sake of completeness let us state Siegel's original result.

Theorem 4 (Siegel) *Let $\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k}$ be radicals over a field F. In both the real and complex case the minimal polynomial $p_i(X)$ of $\sqrt[d_i]{q_i}$ over $F(\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_{i-1}]{q_{i-1}})$ has the form*

$$p_i(X) = X^{n_i} - c_i \prod_{j=1}^{i-1} \sqrt[d_j]{q_j}^{e_j}$$

for some $c_i \in F$ and positive integers e_j.

3 The basic theorems

In this section we prove the basic theorems on denesting radical expressions. Basically we restrict ourselves to a single nested radical.

Given a nested radical $\sqrt[d]{\sum_{i=1}^{k} p_i \sqrt[d_i]{q_i}}$, say, of depth two over some field F. To describe and compute possible denestings of this radical we consider $\gamma = \sum_{i=1}^{k} p_i \sqrt[d_i]{q_i}$ as an element of the radical extension $F' = F(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_k]{q_k})$ generated by the depth one radicals appearing in $\sum_{i=1}^{k} p_i \sqrt[d_i]{q_i}$. The theorems that we are going to prove in this section show that this field is in fact the right place to look for denestings.

Let us fix some notation. By $F^{(i)}$ denote the radical extension $F(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_i]{q_i})$, $F^{(0)} = F$, and let n_i be the the degree of the extension $F^{(i)} : F^{(i-1)}$. Furthermore, the degree of $F' : F$ is denoted by N. Hence $N = \prod_{i=1}^{k} n_i$ and a basis for the field extension $F' : F$ is given by

$$B = \left\{ \prod_{j=1}^{k} \sqrt[d_j]{q_j}^{e_j},\ 0 \leq e_1 < n_1, \ldots, 0 \leq e_k < n_k \right\}.$$

B will be called the *standard basis* of $F' : F$.

The first theorem generalizes and simplifies the proof of a result due to Borodin et al. [2] who studied real nested square roots.

Theorem 5 *Let F be a real field and $F' = F(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_k]{q_k})$ be a real radical extension of F whose degree is N. By $B = \{\beta_0, \ldots, \beta_{N-1}\}$ denote the standard basis of F' over F. Assume furthermore $\gamma \in F'$ and $d \in \mathbb{N}$ such that $\sqrt[d]{\gamma}$ denests over F using only real radicals, that is, $\sqrt[d]{\gamma} \in F(\sqrt[t_1]{a_1}, \ldots, \sqrt[t_m]{a_m})$ for some $t_i \in \mathbb{N}$, $a_i \in F$, $a_i > 0$. Then*

$$\sqrt[d]{q}\, \sqrt[d]{\beta_j}\, \sqrt[d]{\gamma} \in F'$$

for some $q \in F \backslash \{0\}$ and some $\beta_j \in B$.

Proof: $\sqrt[d]{\gamma} \in F(\sqrt[t_1]{a_1}, \ldots, \sqrt[t_m]{a_m})$ clearly implies $\sqrt[d]{\gamma} \in F'(\sqrt[t_1]{a_1}, \ldots, \sqrt[t_m]{a_m})$. Hence $\sqrt[d]{\gamma}$ is a radical

over F' contained in $F'(\sqrt[t]{a_1}, \ldots, \sqrt[t]{a_m})$. Since F' and $F'(\sqrt[t]{a_1}, \ldots, \sqrt[t]{a_m})$ are real fields, we can apply Lemma 2, which shows

$$\sqrt[d]{\gamma} = \rho \prod_{i=1}^{m} \sqrt[t]{a_i}^{e_i},$$

for some $\rho \in F'$, $e_i \in \mathbf{N}$.

But $\prod_{i=1}^{m} \sqrt[t]{a_i}^{e_i}$ can be written as $\sqrt[t]{a}$ for some $a \in F$ and $t = \prod_{i=1}^{m} t_i$. Taking d-th powers this yields

$$\gamma/\rho^d = \sqrt[t]{a^d}.$$

$\gamma/\rho^d \in F'$ and $a^d \in F$ therefore $\sqrt[t]{a^d}$ is a radical over F that is contained in $F' \subseteq \mathbf{R}$. By Lemma 2 $\sqrt[t]{a^d} = q'\beta_h$ for $q' \in F$ and some basis element β_h.

Since $\sqrt[t]{a} = \frac{1}{\rho}\sqrt[d]{\gamma} \in \mathbf{R}$ this shows that $\sqrt[t]{a}$ can be written as a real d-th root of $q'\beta_h$. We easily deduce

$$\sqrt[d]{\frac{1}{q'}}\sqrt[d]{\frac{1}{\beta_h}}\sqrt[d]{\gamma} \in F'.$$

Finally observe that β_h^{-1} is a radical of F' over F. Hence it can be written as $q''\beta_j$ for a basis element β_j and $q'' \in F$. So q may be chosen as $\frac{q''}{q'} \neq 0$ to prove the theorem. □

Note that each basis element $\beta_j \in B$ can be written as a real N-th root of some element in F. Therefore the representation of $\sqrt[d]{q}\sqrt[d]{\beta_j}\sqrt[d]{\gamma}$ as a linear combination of elements in B will lead to a denesting of $\sqrt[d]{\gamma}$ using only real radicals and we can interpret Theorem 5 as saying that in denesting $\sqrt[d]{\gamma}$ by real radicals only radicals of order dN will help. Moreover, using the results of section 2 it is not hard to show that no denesting of $\sqrt[d]{\gamma}$ by a linear combination of real radicals of depth one can consist of fewer terms than the one described by Theorem 5. Additional results, however, are necessary to prove that if γ is a sum of linearly independent radicals that generate an extension of degree N then N is also the degree of the minimal polynomial of γ.

Next observe that, given the equation $q\beta_j\gamma = \rho^d$, $\rho \in F'$, we can apply the distinct field embeddings σ_i of F' over F to this equation. This yields $q\sigma_i(\beta_j)\sigma_i(\gamma) = \sigma_i(\rho)^d$, for all i.

Hence

$$\sqrt[d]{\sigma_i(\gamma)} = \sqrt[d]{q}^{-1}\sqrt[d]{\sigma_i(\beta_j)}^{-1}\sigma_i(\rho),$$

and by choosing an appropriate d-th root of q this is true for any d-th root of $\sigma_i(\gamma)$.

The different d-th roots of $\sigma_i(\gamma)$, $i = 0, 1, \ldots, N-1$, are the roots of the minimal polynomial of $\sqrt[d]{\gamma}$, provided $\sqrt[d]{\gamma}$ is of degree d. By Siegel's Theorem the radicals appearing in the expression for γ, β_j and ρ will be mapped by σ_i onto certain complex radicals. Hence the equation $q\beta_j\gamma = \rho^d$ leads to a denesting for all conjugates of $\sqrt[d]{\gamma}$ over F. In [3] this has been called an *exact denesting*.

For linear combinations of radicals we have the following result.

Theorem 6 *Suppose $S = \sum_{i=1}^{h} \kappa_i \sqrt[d]{\gamma_i}$ is a sum of real nested radicals such that $\gamma_i \in F_i$, $i = 1, \ldots, h$, $\kappa_i \in L_i$, $i = 1, \ldots, h$, and each F_i, L_i is a real radical extension of $F \subseteq \mathbf{R}$. Furthermore assume that no nested radical $\sqrt[d]{\gamma_i}$ denests using real radicals. Then using real radicals*

- *S can only denest to zero,*
- *If no quotient $\frac{\sqrt[d]{\gamma_i}}{\sqrt[d]{\gamma_j}}$ denests then $S = 0$ if and only if $\kappa_i = 0$ for all i.*

Proof: Omitted. □

This theorem together with Theorem 5 implies that a denesting of a linear combination of nested radicals $S = \sum_{i=1}^{h} \kappa_i \sqrt[d]{\gamma_i}$ consists of at most $\mathcal{O}(h \max\{m_i\} \max\{n_i^2\})$ terms, where n_i, m_i are the degrees of F_i, L_i over F. Observe that in general the minimal polynomial of S has degree $\prod_{i=1}^{h} m_i n_i d_i$, hence is exponential in h. So if we want a denesting algorithm whose run time is polynomial in the maximal output size we can not afford to compute the minimal polynomial or even the splitting field of a radical expression.

Like above it can be shown that the denestings for S using real radicals apply also to certain complex values of the roots in S.

For complex radicals we get a similar result. It partially proves a conjecture of R. Zippel [12].

Theorem 7 *Assume F contains all roots of unity. Let F' be an arbitrary radical extension of F with basis B as above. Assume $\gamma \in F'$ and $d \in \mathbf{N}$ such that $\sqrt[d]{\gamma}$ denests over F, that is, $\sqrt[d]{\gamma} \in F(\sqrt[t]{a_1}, \ldots, \sqrt[t]{a_m})$, for some $a_i \in F$. Then*

$$\sqrt[d]{q}\sqrt[d]{\beta_j}\sqrt[d]{\gamma} \in F'$$

for some $q \in F \backslash \{0\}$ and some $\beta_j \in B$.

The proof of this theorem is exactly the same as for Theorem 5 except that Lemma 2 is replaced by Lemma 3.

At first sight Theorem 7 seems to be of theoretical interest only since it is computationally infeasible to

work with a field containing all roots of unity. The results of Landau [6] and Horng, Huang [3], however, show that instead of dealing with a field containing all roots of unity we can restrict ourselves to a field generated by a single root of unity. Unfortunately, so far the best bounds on the degree of this root of unity are (double-)exponential in the description size of the radical. In any case the theorem indicates that even in the general denesting problem the denestings we consider below may be the right thing to look at.

From a practical point of view the following restricted version of Theorem 7 seems to be of greater interest since it allows us to bound the maximum degree of roots of unity we want to creep into the denestings.

Theorem 8 *Assume F contains a primitive d-th root of unity. Let F' be a radical extension of F generated by radicals of order d and with basis B as above. Assume $\gamma \in F'$ such that $\sqrt[d]{\gamma}$ denests over F using radicals of order d only. Then*

$$\sqrt[d]{q}\,\sqrt[d]{\beta_j}\,\sqrt[d]{\gamma} \in F'$$

for some $q \in F\backslash\{0\}$ and some $\beta_j \in B$.

Observe that any element in B is a radical of order d so the conclusion of the theorem really leads to a denesting of $\sqrt[d]{\gamma}$ by radicals by order d radicals. It can also be shown that any denesting for $\sqrt[d]{\gamma}$ of this kind will have at least as many terms as the one in Theorem 8. Furthermore, as in the real case, if γ is a sum of linearly independent radicals generating an extension of degree N then γ is of degree N also.

Finally let us mention that Theorem 6 easily generalizes if "denest using real radicals" is replaced by "denest using radicals of order d" .

4 Denesting sets and admissible sequences

Observe that if we knew how to determine for a nested radical $\sqrt[d]{\gamma}$ in time polynomial in N one element $q \in F$ with $\sqrt[d]{q}\,\sqrt[d]{\gamma} \in F'$ then we could compute the denestings of Theorem 5, say, in time polynomial in N. We only had to try to compute such an element for all nested radicals $\sqrt[d]{\beta_j \gamma}$ which increases the run time of the algorithm only by a factor of N. Likewise by applying the algorithm to all ratios of nested radicals we could transform any sum S of nested radicals into a sum of nested radicals satisfying the conditions of Theorem 6. After this transformation step we easily check whether the coefficients are zero by applying results of [1].

Hence it remains to characterize and compute those elements in F with $\sqrt[d]{q}\,\sqrt[d]{\gamma} \in F'$.

Definition 9 *Assume $F \subset \mathbb{C}$ and let F' be an algebraic extension of F, $\gamma \in F'$, $d \in \mathbb{N}$. We say that $q \in F\backslash\{0\}$* **denests** *$\sqrt[d]{\gamma}$ or that it* **leads to a denesting** *of $\sqrt[d]{\gamma}$ if $\sqrt[d]{q}\,\sqrt[d]{\gamma} \in F'$ for some d-th root $\sqrt[d]{q}$ of q.*

A finite set $S \subset F$ with the property that any element denesting $\sqrt[d]{\gamma}$ differs from some element in this set only by a d-th power of some element in F is called a **denesting set** *for $\sqrt[d]{\gamma}$ over F. If no two elements in a denestings set differ from one another by a d-th power of an element in F then the denesting set is called* **irreducible**.

It is easily seen that by this definition the set of elements denesting $\sqrt[d]{\gamma}$ is independent of the specific d-th root of γ.

So far it is not clear that a radical $\sqrt[d]{\gamma}$ possesses a finite denesting set. The next lemma, that is an immediate consequence of Lemma 2 or Lemma 3, proves the existence of such a set.

Lemma 10 *Let the fields F, F', the basis B, d, and γ be either as in Theorem 5 or as in Theorem 8. If $q \in F$ denests $\sqrt[d]{\gamma}$ then any other element in F that denests $\sqrt[d]{\gamma}$ has the form*

$$p^d \beta_j^d q,$$

for some $p \in F$ and $\beta_j \in B$ such that $\beta_j^d \in F$. Likewise, any element denesting $\sqrt[d]{\gamma}$ can be written as

$$p^d \beta_j^{-d} q$$

with p, β_j as before.

For the complex case $\beta_j^d \in F$ is no restriction since any basis element is a radical of order d. The second formula has been included since it turns out to be more convenient from a computational point of view.

Although the lemma shows that a denesting set is of size N at most it is nevertheless quite restricted since it does not tell us how a single element denesting $\sqrt[d]{\gamma}$ looks like or how to compute such an element. Rather it shows how to compute a denesting set given a single element denesting $\sqrt[d]{\gamma}$. Below we give a *constructive* description of the elements denesting $\sqrt[d]{\gamma}$ which applies not only to radical extensions but to arbitrary extensions. The characterization is based on a simple lemma about the *trace* of an extension.

Definition 11 *Let F' be an algebraic extension of a field $F \subset \mathbb{C}$. Denote by $\sigma_0, \ldots, \sigma_{N-1}$ the distinct field*

embeddings of F' over F. For any element $\gamma \in F$ the **trace** *of γ over F, denoted by $\mathrm{tr}_{F':F}(\gamma)$, is the sum $\sum_{i=0}^{N-1} \sigma_i(\gamma)$ of the conjugates of γ.*

Lemma 12 *Let F' be an algebraic extension of some field $F \subset \mathbb{C}$. If $\{\beta_0, \beta_1, \ldots, \beta_{N-1}\}$ is a F-basis for F' and γ a non-zero element of E then*

$$\mathrm{tr}_{F':F}(\beta_i \gamma) \neq 0$$

for some $i \in \{0, 1, \ldots, N-1\}$.

Proof: Assume that $\mathrm{tr}_{F':F}(\beta_i \gamma) = 0$ for all i. Since the set $\{\beta_0\gamma, \beta_1\gamma, \ldots, \beta_{N-1}\gamma\}$ is also a basis of the extension this implies that the trace function is identically zero. But $\mathrm{tr}_{F':F}(1) = N \neq 0$, which proves the lemma. □

Lemma 13 *Let F be an arbitrary field and F' an algebraic extension of F with basis $\{\beta_0, \beta_1, \ldots, \beta_{N-1}\}$. Denote the distinct field extensions by σ_i, $i = 0, \ldots, N-1$. Assume $\gamma \in F'$, $d \in \mathbb{N}$. If there exists an element $q \in F$ with $\sqrt[d]{q}\sqrt[d]{\gamma} \in F'$ for certain d-th roots of q and γ then there exist d-th roots $\sqrt[d]{\sigma_i(\gamma)}$ of $\sigma_i(\gamma)$, $i = 0, \ldots, N-1$, such that for some basis element β_j*

$$\left(\sum_{i=0}^{N-1} \sigma_i(\beta_j)\sqrt[d]{\sigma_i(\gamma)}\right)^d \in F\backslash\{0\}.$$

Moreover, any element $q \in F$ with $\sqrt[d]{q}\sqrt[d]{\gamma} \in F'$ for certain d-th roots can be written as a product of a d-th power of an element in F and an inverse of an element in F satisfying the description above.

Proof: Assume $q \in F$ has the property $\sqrt[d]{q}\sqrt[d]{\gamma} = \rho \in F'$. Hence $q\gamma = \rho^d$ and $q\sigma_i(\gamma) = (\sigma_i(\rho))^d$. Equivalently, there exist certain d-th roots of q and $\sigma_i(\gamma)$ such that

$$\sqrt[d]{q}\sqrt[d]{\sigma_i(\gamma)} = \sigma_i(\rho),\ i = 0, \ldots, N-1.$$

We can assume that the d-th root of q is the same for all N equations since we may choose the root of $\sigma_i(\gamma)$ accordingly. Applying Lemma 12 to $\rho \in F'$ yields

$$\mathrm{tr}(\beta_j\rho) = \sum_{i=0}^{N-1} \sigma_i(\beta_j)\sigma_i(\rho) =$$

$$= \sqrt[d]{q}\sum_{i=0}^{N-1} \sigma_i(\beta_j)\sqrt[d]{\sigma_i(\gamma)} = p \in F\backslash\{0\}.$$

Therefore

$$q = \left(\frac{p}{\sum_{i=0}^{N-1} \sigma_i(\beta_j)\sqrt[d]{\sigma_i(\gamma)}}\right)^d.$$

$p \in F$ hence $\left(\sum_{i=0}^{N-1} \sigma_i(\beta_j)\sqrt[d]{\sigma_i(\gamma)}\right)^d$ is also an element of F.

Moreover, as a d-th power p^d will not help in denesting $\sqrt[d]{\gamma}$, so a d-th root of $\left(\sum_{i=0}^{N-1} \sigma_i(\beta_j)\sqrt[d]{\sigma_i(\gamma)}\right)^{-d}$ will also denest $\sqrt[d]{\gamma}$.

The claim that any number $q \in F$ denesting $\sqrt[d]{\gamma}$ can be written in the stated form follows from the fact that the process above can be applied to all these elements of the field F. □

This lemma generalizes results of R. Zippel [12] and S. Landau [7] who characterized elements denesting a d-th root $\sqrt[d]{\gamma}$ if F' is a Galois extension of F. Lemma 13 is correct for arbitrary extensions of a field F.

Based on this lemma an $\mathcal{O}(d)$-bound on the size of elements in a denesting set can be derived. We guess that this is also a lower bound for the size of the elements leading to a denesting although we cannot prove it. Since the algorithms we describe below will have run time polynomial in d such a bound would imply that this is the best we can hope for.

Observe that Lemma 13 almost immediately leads to an algorithm for denesting $\sqrt[d]{\gamma}$:

For all basis elements β_j and all expressions in Lemma 13 corresponding to $\sqrt[d]{\beta_j\gamma}$ check whether the expression describes an element q in F and, if so, check whether $\sqrt[d]{q\beta_j\gamma} \in F'$.

So far it is not clear how to compute the elements in F corresponding to the expressions in Lemma 13. But if we really had to check all possible expressions this could only lead to an algorithm with run time $\Omega(Nd^{N-1})$, since Nd^{N-1} is the number of different combinations of d-th roots of $\sigma_i(\beta_j\gamma)$ (the d-th root of $\beta_j\gamma$ can be fixed arbitrarily). On the other hand, considering the proof of Lemma 13 again it is obvious that we are only interested in those combinations that correspond to what we call admissible sequences.

Definition 14 *Let F be an arbitrary field and F' an extension of F. Denote the field embeddings of F' over F by σ_i, $i = 0, 1, \ldots, N-1$. Furthermore let $\sqrt[d]{\sigma_i(\gamma)}$, $i = 0, \ldots, N-1$, be fixed d-th roots of $\sigma(\gamma)$. A sequence $(1, \zeta^{(1)}, \zeta^{(2)}, \ldots, \zeta^{(N-1)})$ of d-th roots of unity is called* **admissible** *if elements $q \in F$ and $\beta \in F'$ exist such that $\zeta^{(i)}\sqrt[d]{q}\sqrt[d]{\sigma_j(\gamma)} = \sigma_j(\beta)$ for all $j = 0, 1, \ldots, N-1$, and for a fixed d-th root $\sqrt[d]{q}$ of q*

Observe that whether a sequence of d-th roots of unity is admissible or not depends on the values chosen for $\sqrt[d]{\sigma_i(\gamma)}$.

The fact that the first element in an admissible sequence is 1 corresponds to our definition of a denesting set which is independent of the specific d-th root of γ that is meant by $\sqrt[d]{\gamma}$.

As will be shown below any denesting problem for radical extensions can be reduced to several denesting problems over simple radical extensions. For these extensions we show that any admissible sequence is already determined by the triple $(\zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)})$ in the real case and by $\zeta^{(1)}$ alone in the complex case.

So for the time being let F be an arbitrary field and $F' = F(\sqrt[m]{p})$ a simple radical extension of F such that $\sqrt[m]{p}$ is of degree m over F. As usual γ is an element of F'. Before we can prove the main result on admissible sequences we need one auxiliary lemmata. In the complex case $\zeta_m \in F$, equivalently, $F(\zeta_m) = F$. In the real case we have to determine the degree of $\sqrt[m]{p}$ over $F(\zeta_m)$.

Lemma 15 *Let F be a real field. Suppose $f(X) = X^m - p$, $p \in F$, $p > 0$, is irreducible in $F[X]$. Furthermore let ζ_m be a primitive m-th root of unity. Then $f(X)$ is either irreducible in $F(\zeta_m)[X]$, or $\sqrt{p} \in F(\zeta_m)$ and $f(X)$ factors as $(X^{\frac{m}{2}} - \sqrt{p})(X^{\frac{m}{2}} + \sqrt{p})$ over $F(\zeta_m)[X]$. In the latter case m must be even.*

Proof: Consider the Galois group G of $F(\zeta_m)$ over F. By Galois theory this group is isomorphic to a subgroup of the group $\mathbf{Z}_m^*$. Since $\mathbf{Z}_m^*$ is abelian the same is true for G. The fundamental theorem of Galois theory shows that all subfields between $F(\zeta_m)$ and F are Galois extensions of F.

Next consider the degree of $\sqrt[m]{p}$ over $F(\zeta_m)$. By Lemma 3, this is the smallest positive integer e such that $\sqrt[m]{p^e} \in F(\zeta_m)$. Moreover, e divides m.

If $\sqrt[m]{p^e} \in F(\zeta)$ then it generates a subfield of $F(\zeta_m)$ over F. Since $\sqrt[m]{p}$ has degree m over F the element $\sqrt[m]{p^e}$ must have degree $\frac{m}{e}$ and its minimal polynomial is $X^{\frac{m}{e}} - p$. By the observation above the field generated by $\sqrt[m]{p^e}$ must be a Galois extension of F. But if F is a real field and $\frac{m}{e} > 2$ then $\sqrt[m]{p^e} \in \mathbf{R}$ cannot generate a Galois extension since some of the roots of $X^{\frac{m}{e}} - p$ are not real. Hence $\frac{m}{e} = 2$ or $\frac{m}{e} = 1$, which proves the lemma. □

Remark 1: It follows from the proof that no field extension $F(\zeta_m) : F$ for a real field F and an m-th root of unity has subfields generated by real radicals of degree strictly larger than 2. At first sight this seems to contradict the famous Kronecker-Weber Theorem which states that any abelian extension of $\mathbf{Q}$ is contained in some cyclotomic field $\mathbf{Q}(\zeta_m)$. But although the Galois group of $\mathbf{Q}(\zeta_m, \sqrt[m]{p})$ over $\mathbf{Q}(\zeta_m)$ is abelian, for $m > 2$ this is not true for the Galois group of $\mathbf{Q}(\zeta_m, \sqrt[m]{p})$ over $\mathbf{Q}$.

Remark 2: As follows from the lemma whenever m is odd then the degrees of $\sqrt[m]{p}$ over $\mathbf{Q}$ and over $\mathbf{Q}(\zeta_m)$ are the same. The following example shows that the second situation described by the lemma can also occur. Consider the positive 10-th root of 5. Its degree over $\mathbf{Q}$ is 10. On the other we will see later that $\mathbf{Q}(\zeta_{10})$ contains the square roots of 5. Hence the degree of $\sqrt[10]{5}$ over the 10-th cyclotomic field is 5.

Lemma 16 *If F is a real field and $\sqrt[m]{p} \in \mathbf{R}$ then any two admissible sequences for $\sqrt[d]{\gamma}$ that have a common prefix $(1, \zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)})$ are equal.*

If F contains a primitive m-th root of unity and $\sqrt[m]{p}$ is arbitrary then $\zeta^{(1)}$ alone determines an admissible sequence.

Proof: We prove the lemma only in the real case.

Let $(1, \zeta_1, \zeta_2, \zeta_3)$ be a common prefix of two different admissible sequences

$$\left(1, \zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)}, \zeta^{(4)}, \ldots, \zeta^{(m-1)}\right)$$

and

$$\left(1, \zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)}, \zeta'^{(4)}, \ldots, \zeta'^{(m-1)}\right).$$

Hence $p_j \in F$ and $\beta_j \in F'$, $j = 1, 2$, exist such that $\sqrt[d]{p_j}\sqrt[d]{\gamma} = \beta_j$, $\zeta^{(i)}\sqrt[d]{p_j}\sqrt[d]{\sigma_i(\gamma)} = \sigma_i(\beta_j)$, $i = 1, 2, 3$, $j = 1, 2$, for fixed d-th roots of p_1, p_2. This implies

$$\frac{1}{p_1}\beta_1\left(\sigma_2(\beta_1)\right)^{d-1} = \zeta^{(2)d-1}\sqrt[d]{\gamma}\left(\sqrt[d]{\sigma_2(\gamma)}\right)^{d-1} =$$

$$= \rho \in F(\sqrt[m]{p}, \zeta_m)$$

and

$$\frac{1}{p_2}\beta_2\left(\sigma_2(\beta_2)\right)^{d-1} = \zeta^{(2)d-1}\sqrt[d]{\gamma}\left(\sqrt[d]{\sigma_2(\gamma)}\right)^{d-1} = \rho,$$

where ζ_m is a primitive m-th root of unity.

By the previous lemma an field isomorphism τ of $F(\sqrt[m]{p}, \zeta_m)$ exists that maps ζ_m onto itself and $\sqrt[m]{p}$ onto $\zeta_m^2\sqrt[m]{p}$. We apply τ to both equations above. As is easily checked this yields

$$\zeta^{(2)}\zeta^{(4)d-1}\sqrt[d]{\sigma_2(\gamma)}\left(\sqrt[d]{\sigma_4(\gamma)}\right)^{d-1} = \tau(\rho)$$

and

$$\zeta^{(2)}\left(\zeta'^{(4)}\right)^{d-1}\sqrt[d]{\sigma_2(\gamma)}\left(\sqrt[d]{\sigma_4(\gamma)}\right)^{d-1} = \tau(\rho).$$

One easily deduces $\zeta^{(4)} = \zeta'^{(4)}$. Moreover, $\zeta^{(2)} = \zeta'^{(2)}$ and $\zeta^{(4)} = \zeta'^{(4)}$ imply $\zeta^{(6)} = \zeta'^{(6)}$ etc.. Hence for all even indices the two sequences coincide. Starting the process above with $\zeta^{(1)}$ and $\zeta^{(3)}$ instead of $\zeta^{(0)} = 1$ and $\zeta^{(2)}$ shows that the same is true for the odd indices. □

Observe that the proof of Lemma 16 more or less is an algorithm to compute a subset for the set of admissible sequences of size d^3 in the real case and of size d in the complex case.

5 The algorithms

We are now in a position to sketch the basic algorithms. We claim that the following procedure computes for a nested radical γ over an algebraic number field $F = \mathbb{Q}(\alpha)$ an element denesting it, if any such element exists.

Algorithm Denesting Element

Input

A nested radical $\sqrt[d]{\gamma} = \sqrt[d]{\sum_{i=1}^{K} \kappa_i \sqrt[d_i]{\rho_i}}$, $\rho_i \in F$, of depth two over F, where F is either real and the radicals defining γ are also real or F contains a primitive d-th root of unity and $d_i = d$ for all i.

Output

"Yes", if any element in F leads to a denesting, and witnesses $\gamma^{(0)} \in F$, $\rho \in F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_K]{\rho_K})$ such that $\sqrt[d]{\gamma^{(0)}\gamma} = \rho$; "No", otherwise.

Step 1

Determine for each i the relative degree $n_i = [F(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_i]{q_i}) : F(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_{i-1}]{q_{i-1}})]$. Renumber the radicals such that $n_i > 1$ for the first k indices and $n_i = 1$ for the remaining indices. Hence $F^{(K)} = F^{(k)}$ and $[F^{(k)} : F] = \prod_{i=1}^{k} n_i = N$. Also compute the set $E^{(i)}$ of those $s \in \mathbb{N}$, $s < n_i$, such that $\sqrt[d_i]{\rho_i^{sd}} \in F^{(i-1)}$.

Step 2

Set $D^{(k)} := \{\gamma\}$.

For $i = 0, 1, \ldots, k-1$ do the following:

Compute for all elements $\gamma_j^{(k-i)}$ in $D^{(k-i)}$ a superset of its set of admissible sequences. Use these sequences and the formula given in Lemma 13 to determine the inverse $\gamma^{(k-i-1)}$ of an element in $F^{(k-i-1)}$ denesting $\gamma^{(k-i)}$.

Set $D_{\gamma^{(k-i)}} = \{\gamma^{(k-i-1)} \sqrt[d_k]{q_{k-i}^{sd}} \mid s \in E^{(k-i)}\}$ and

$$D^{(k-i-1)} = \bigcup_{\gamma^{(k-i)} \in D^{(k-i)}} D_{\gamma^{(k-i)}}.$$

Step 3

Decide whether any inverse $\gamma^{(0)}$ of an element in $D^{(0)}$ has the property

$$\sqrt[d]{\gamma^{(0)}}\sqrt[d]{\gamma} = \rho \in F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k}),$$

if this is the case output $\gamma^{(0)}$ and ρ; otherwise output "No".

To prove the claim that **Algorithm Denesting Element** finds an element denesting $\sqrt[d]{\gamma}$ we use the following observation.

Assume $E \supset F$ is a proper subfield of $F^{(k)}$. We consider γ as an element of the algebraic extension F' of the field E. If $\sqrt[d]{\gamma}$ denests over F then it denests over E. Moreover, let D be a set containing the *inverses* of a denesting set for $\sqrt[d]{\gamma}$ over E. For each element in D we consider a denesting set over F of an arbitrary d-th root of this element. As mentioned these subsets of F are independent of the d-th root.

Observe that any element $q \in F$ that denests $\sqrt[d]{\gamma}$ over F also denests $\sqrt[d]{\gamma}$ over E. Hence it differs from some element $\gamma'^{-1} \in D$ by a d-th power of an element in E, i.e.,

$$q = \rho^d \frac{1}{\gamma'}, \ \rho \in E.$$

Therefore d-th roots of q and γ' exist such that $\sqrt[d]{q} = \rho\sqrt[d]{\frac{1}{\gamma'}}$, equivalently,

$$\sqrt[d]{q}\sqrt[d]{\gamma'} = \rho \in E.$$

By definition of a denesting set the union of the denesting sets for elements in D form a denesting set for $\sqrt[d]{\gamma}$ over F.

If we apply this result to the sets $D^{(k-i)}$, $i = 1, \ldots, k$, from the basic denesting algorithm and use Lemma 10 it easily follows by induction that $D^{(0)}$ is a denesting set for $\sqrt[d]{\gamma}$ which proves the correctness of **Algorithm Denesting Element** .

Observe that the set $D^{(k-i)}$ has at most $\prod_{j=0}^{i-1} n_{k-j}$ elements. Assume that for each element in $D^{(k-i)}$

the admissible sequences determined by the prefixes $(1, \zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)})$ or $(1, \zeta^{(1)})$ can be computed efficiently. Then at each level of the algorithm we have to check for at most $d^3 \prod_{j=0}^{i} n_{k-j}$ or $d \prod_{j=0}^{i} n_{k-j}$ different complex numbers fitting into the description of Lemma 13 whether they correspond to an element in $F^{(k-i-1)}$. Hence overall this step has to be done at most

$$d^3 \sum_{i=1}^{k} \prod_{j=0}^{i} n_{k-j} =$$

$$= d^3 N \left(1 + \frac{1}{n_1} + \ldots + \frac{1}{n_1 n_2 \cdots n_{k-1}}\right) \leq 2d^3 N$$

times in the real case, and accordingly, at most $2dN$ times in the complex case.

It remains to describe how to perform the single steps of **Algorithm Denesting Element** . Taking a closer look at the algorithm shows that we basically need to solve two problems. First, we need an algorithm that determines the minimal polynomial of an algebraic number γ from an approximation to γ. Using this algorithm primitive elements and their minimal polynomials for the fields $F^{(i)}$ are computed. These informations are needed for exact arithmetic in $F^{(i)}$.

Second, we need an algorithm that computes the exact representation of an algebraic number γ as an element in some number field $\mathbf{Q}(\alpha)$, provided a good approximation to γ is given.

The first problem has been solved by Kannan et al. [5] and by Schönhage [11] using the lattice basis reduction algorithm originally invented by Lenstra et al. [8] in their break-through paper on polynomial factorization. As the following theorem shows the same technique solves the second problem.

Theorem 17 *Let $\mathbf{Q}(\alpha)$ be an algebraic number field, where α is an algebraic integer with minimal polynomial $p(X) = \sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z}$. Let $\gamma = \frac{1}{c} \sum_{i=0}^{n-1} c_i \alpha^i$, $c, c_i \in \mathbf{Z}$, be an element in $\mathbf{Q}(\alpha)$ such that $|c|, |c_i| < K$, K a positive number. Assume s and ϵ are real numbers satisfying*

$$s > 2^{2n^2} 2^{7n} n^n |p|_2^n K^{4n}, \quad \epsilon = 3s^{-1}.$$

Moreover, suppose $\overline{\gamma}, \overline{\alpha}$ are approximations to γ and α, respectively, such that the following estimates for the real and imaginary parts $\Re, \Im$ of γ, α hold

$$|\Re(\overline{\gamma}) - \Re(\gamma)| < \epsilon, \quad |\Im(\overline{\gamma}) - \Im(\gamma)| < \epsilon,$$

$$|\Re(\overline{\alpha}^i) - \Re(\alpha^i)| < \epsilon, \quad |\Im(\overline{\alpha}^i) - \Im(\alpha^i)| < \epsilon,$$

for all $i \in \{1, 2, \ldots, n-1\}$.

If $\Lambda(V)$ is generated by the columns of the following $(n+3) \times (n+1)$ matrix

$$V = \begin{bmatrix} s\Re(\overline{\gamma}) & s & s\Re(\overline{\alpha}) & s\Re(\overline{\alpha}^2) & \ldots & s\Re(\overline{\alpha}^{n-1}) \\ s\Im(\overline{\gamma}) & 0 & s\Im(\overline{\alpha}) & s\Im(\overline{\alpha}^2) & \ldots & s\Im(\overline{\alpha}^{n-1}) \\ 1 & 0 & \ldots & & & 0 \\ 0 & 1 & 0 & \ldots & & 0 \\ & & \ddots & & & \\ & & & \ldots & & \\ 0 & 0 & \ldots & & 0 & 1 \end{bmatrix},$$

then the shortest vector $g = V(c, c_0, c_1, \ldots, c_{n-1})^T$ of a reduced basis for $\Lambda(V)$ satisfies

$$\gamma = \frac{-1}{c} \sum_{i=0}^{n-1} c_i \alpha^i.$$

Moreover, $\gcd(c, c_0, c_1, \ldots, c_{n-1}) = 1$.

If we want to use this result in **Algorithm Denesting Element** for any application of the lattice basis reduction algorithm we need to deduce an upper bound on the representation size K of the number whose exact representation we want to reconstruct. As it turns out this is no serious problem and a detailed analysis which will be given in the full paper proves the following theorems.

Theorem 18 *When applied to $d \in \mathbf{N}$ and $\gamma = \sum_{i=1}^{K} \kappa_i \sqrt[d]{\rho_i}$, where κ_i, ρ_i are elements of some real algebraic number field $\mathbf{Q}(\alpha)$, the number of bit operations* **Algorithm Denesting Element** *uses to determine whether an element $\gamma^{(0)}$ with*

$$\sqrt[d]{\gamma^{(0)}}\sqrt[d]{\gamma} \in F(\sqrt[d]{\rho_1}, \sqrt[d]{\rho_2}, \ldots, \sqrt[d]{\rho_K})$$

for real d-th roots exists, is bounded by a polynomial in the parameters n, l, L, N, d. n is the degree of the minimal polynomial p of α, 2^l is a bound on the 2-norm of p, 2^L is an upper bound on the size of the coefficients in the representation of κ_i, ρ_i as elements of $\mathbf{Q}(\alpha)$, and N is the degree of $F(\sqrt[d]{\rho_1}, \sqrt[d]{\rho_2}, \ldots, \sqrt[d]{\rho_K})$ over F.

An upper bound on the number of bit operations is given by

$$\mathcal{O}(d^4 n^6 N^{12} (\log n + l + L) M(d^2 n^5 N^7 (\log n + l + L))).$$

Using at most N times this number of bit operations it can decided whether $\sqrt[d]{\gamma}$ can be written as a linear combination of real depth one radicals over $\mathbf{Q}(\alpha)$.

Here $M(m)$ denotes the number of bit operations needed for multiplying two m-bit integers.

The input of **Algorithm Denesting Element** need not be of the form $\sqrt[d]{\sum_{i=1}^{K} \kappa_i \sqrt[d]{\rho_i}}$ rather the sum can

be replaced by any rational expression in the radicals $\sqrt[d]{\rho_i}$ and with coefficients in $\mathbf{Q}(\alpha)$. In this case the run time gets slightly worse but is still polynomial in the parameters mentioned above.

The corresponding theorem for complex radicals is

Theorem 19 Algorithm Denesting Element *when applied to* $d \in \mathbf{N}$ *and* $\gamma = \sum_{i=1}^{K} \kappa_i \sqrt[d]{\rho_i}$, *where* κ_i, ρ_i *are elements of some algebraic number field* $\mathbf{Q}(\alpha)$ *containing a primitive* d*-th root of unity determines in time polynomial in* n, l, L, N, d *whether an element an element* $\gamma^{(0)}$ *with*

$$\sqrt[d]{\gamma^{(0)}}\sqrt[d]{\gamma} \in F(\sqrt[d]{\rho_1}, \sqrt[d]{\rho_2}, \ldots, \sqrt[d]{\rho_K})$$

for arbitrary d*-th roots exists. The parameters* n, l, L, N, d *are as above.*

An upper bound for the number of operations used is

$$\mathcal{O}(d^2n^6N^6(\log n + l + L)M(d^2n^5N^4(\log n + l + L))).$$

Using at most N *times this number of bit operations it can be decided whether* $\sqrt[d]{\gamma}$ *can be written as a linear combination of radicals of depth one and of order* d *over* $\mathbf{Q}(\alpha)$.

For sums of nested radicals we get similar results. In particular, the algorithms are polynomial in the number of terms of the sum and the maximum degree of a radical extension generated by the depth one radicals appearing in a *single* term of the sum. The generalization of these results to quotients of sums of nested radicals turns out to be straightforward.

As mentioned in the introduction the algorithms sketched above are correct for number fields and so they can be applied to nested radicals of depth larger than two. But they are not guaranteed to find a minimum depth denesting.

Acknowledgment I would like to thank Susan Landau for bringing the problem of denesting radicals to my attention.

References

[1] J. Blömer, "Computing Sums of Radicals in Polynomial Time", *Proc. 32nd Symposium on Foundations of Computer Science* 1991, pp. 670-677.

[2] 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.

[3] 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.

[4] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, 1974.

[5] R. Kannan, A. K. Lenstra, L. Lovász, "Polynomial Factorization and Nonrandomness of Bits of Algebraic and Some Transcendental Numbers", *Mathematics of Computation* Vol. 50, No. 181, pp. 235-250, 1988.

[6] S. Landau, "Simplification of Nested Radicals", *SIAM Journal on Computing* Vol. 21, No. 1, pp 85-110, 1992.

[7] S. Landau, "A Note on Zippel-Denesting", *Journal of Symbolic Computation*, Vol. 13, pp. 41-46, 1992.

[8] A. K. Lenstra, H. W. Lenstra, Jr. L. Lovász, "Factoring Polynomials with Rational Coefficients", *Mathematische Annalen* Vol. 261, pp. 515-534, 1982.

[9] S. Ramanujan, *Problems and Solutions, Collected Works of S. Ramanujan*, Cambridge University Press, 1927.

[10] C. L. Siegel, "Algebraische Abhängigkeit von Wurzeln", *Acta Arithmetica*, Vol. 21, pp. 59-64, 1971.

[11] A. Schönhage, "Factorization of Univariate Integer Polynomials by Diophantine Approximation and an Improved Basis Reduction Algorithm", *Proc. 11th ICALP*, LNCS 172, pp. 437-447, 1984.

[12] R. Zippel, "Simplification of Expressions Involving Radicals", *Journal of Symbolic Computation* Vol. 1, pp. 189-210, 1985.