A Note on "Zippel Denesting"

Susan Landau*
Mathematics Department
Wesleyan University
COINS
University of Massachusetts

July 16, 1993

Abstract

Radical simplification is an important part of symbolic computation systems. Zippel [7] gave a sufficient condition for a nested radical to be expressed in terms of radicals of lower nesting depth. We fill a lacuna in his proof, and show that his sufficient condition is also necessary. Previous work by Landau and Miller [4] leads to an algorithm for the problem.

Ramanujan observed a number of curiosities amongst nested radicals:

$$\begin{aligned} \sqrt[4]{\frac{3+2\sqrt[4]{5}}{3-2\sqrt[4]{5}}} &= \frac{\sqrt[4]{5}+1}{\sqrt[4]{5}-1} \\ \sqrt{\sqrt[3]{28}-\sqrt[3]{27}} &= 1/3(\sqrt[3]{98}-\sqrt[3]{28}-1) \\ \sqrt[3]{\sqrt[5]{32/5}-\sqrt[5]{27/5}} &= \sqrt[5]{1/25}+\sqrt[5]{3/25}-\sqrt[5]{9/25} \end{aligned}$$

Symbolic computation made such manipulations more than curiosities. For example:

$$\sqrt{5+2\sqrt{6}} = \sqrt{2}+\sqrt{3}$$

means that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $Q(\sqrt{5+2\sqrt{6}})$ over Q. The basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is simple to manipulate. An important issue then, is the

*Supported by NSF grants DMS-8807202, and CCR-8802835. Part of this work was done while the author was visiting the Yale University Math Department.

"denesting" of radicals – a term which will be precisely defined in the next section.

In 1985, Borodin, Fagin, Hopcroft and Tompa [1] gave an efficient algorithm for decreasing the nesting depth of a class of expressions involving square roots. More recently Landau showed how to denest radicals by computing in the splitting field of the nested radical [3].

Earlier work by Zippel [7] in 1985 gave a simple sufficient condition under which a radical could denest. Zippel's theorem omitted a hypothesis. We repair this lacuna, and show that Zippel's sufficient condition is also necessary. Finally we observe that previous work by Landau and Miller [4] yields an exponential time algorithm for this technique.

1 An Algorithm for a Subclass of Nested Radicals

We begin with the defition of nesting depth. Following [1], a *formula* over a field k and its *depth of nesting* are defined as follows:
(1) an element of k is a formula of depth 0 over k,
(2) an arithmetic combination (A$\pm$B, A $\times$ B, A/B) of formulas A and B is a formula whose depth over k is max(depth(A), depth(B)), and
(3) a root $\sqrt[n]{A}$ of a formula A is a formula whose depth over k is 1+ depth(A).

We will say the formula A *can be denested over the field k* if there is a formula B of lower depth than A such that value(A)=value(B). For any α, we define the depth of α over k to be minimum$\{depth(A) \mid value(A) = \alpha\}$. When we are given a formula A of value α such that A can be denested, we will sometimes instead say that α can be denested.

We will be using several classic theorems. Let ξ_n be a primitive n^{th} root of unity.

Theorem 1.1 *Let k be a field, with K a cyclic extension of k of degree n, and suppose ξ_n is in k. Then there is a β in K such that $K = k(\beta)$, and β is a root of $x^n - b$ for some b in k.*

Theorem 1.2 *Let k be a field with ξ_n in k, and suppose β is a root of $x^n - b$. Then $k(\beta)$ is cyclic over k of degree d, where d divides n, and β^d is an element of k.*

Consider the following tower of fields:

$$\begin{array}{ccc} & L = KF & \\ K & & F \\ & K \cap F & \\ & k & \end{array}$$

Then the following is well-known:

Theorem 1.3 *(Lang[5], pp. 196-7) Let the fields be as above, and assume that F is a Galois extension of k. Then KF is Galois over K, and F is Galois over $K \cap F$. Let G be the Galois group of KF over K, and H the group of F over $K \cap F$. If σ is in G, then the restriction of σ to F is in H, and that restriction map is an isomorphism from G onto H.*

Zippel studied the circumstances under which a radical in L can be denested in a field of lower nesting depth. That is, suppose $L = K(\sqrt[d]{\alpha})$ for some α in K. He sought an element β in k such that $\alpha\beta$ is a d^{th} power of an element in K, say λ. (Assume that ξ_d lies in k.) Then $(\alpha\beta) = \lambda^d$ implies that $\sqrt[d]{\alpha} = \lambda / \sqrt[d]{\beta}$.[1] Thus $\sqrt[d]{\alpha}$ may be expressed in terms of an element of lower nesting depth. We call such a denesting a "Zippel denesting." Zippel [7] presented the following example: let $k = Q$, $K = Q(\sqrt{6})$, and $\alpha = 5 + 2\sqrt{6}, d = 2$. Since

$$2(5 + 2\sqrt{6}) = (2 + \sqrt{6})^2,$$

we know that

$$\sqrt{5 + 2\sqrt{6}} = \frac{2 + \sqrt{6}}{\sqrt{2}} = \sqrt{2} + \sqrt{3}.$$

Zippel observed that in some cases, information about the associated fields will tell us enough to compute a denesting. The following theorem which omitted, but implicitly assumed, the hypothesis that F is a Galois extension of k, first appeared in Zippel's paper.

Theorem 1.4 *(Zippel [7]) Assume K is an extension of k, a field containing a primitive d^{th} root of unity. Let $L = K(\sqrt[d]{\alpha})$ be an extension of degree d, where α is in K. If there is a field F which is a Galois extension of $k = K \cap F$, and $L = KF$, then there is a β in k such that $\alpha\beta$ is a d^{th} power of an element of K. Furthermore, $F = k(\sqrt[d]{\beta})$.*

[1] Note that Zippel is using the convention of choosing the root $\sqrt[d]{\alpha}$, rather than some other d^{th} root. A different root $\xi_d^i \sqrt[d]{\alpha}$ may have a higher depth of nesting due to the nesting in the root of unity.

Proof By Theorem 1.3, $L = KF$ is Galois over K. If G is the Galois group of L over K, and H is the group of F over k, then there is a map $\rho : G \to H$ which sends σ in G to σ restricted to the field F. This map is an isomorphism. Then by Theorem 1.2, the extension L over K is cyclic of degree d, and thus so is F over k. Therefore, by Theorem 1.1, $F = k(\sqrt[d]{\gamma})$ for some γ in k.

Let σ be a generator of G, then $\sigma(\sqrt[d]{\alpha}) = \xi_d \sqrt[d]{\alpha}$. Since there is an isomorphism from G to H, we know $\sigma(\sqrt[d]{\gamma}) = \xi_d^c \sqrt[d]{\gamma}$ for some c relatively prime to d. Let $u \equiv c^{-1} \pmod{d}$, and $m = -u$. Then $\xi_d^{cm} = \xi_d^{-cc^{-1}} = \xi_d^{-1}$. We let $\beta = \gamma^m$. Then we have:

$$\sigma(\sqrt[d]{\alpha}\sqrt[d]{\beta}) = \sigma(\sqrt[d]{\alpha})\sigma(\sqrt[d]{\beta}) = \xi_d \sqrt[d]{\alpha}\ \sigma((\sqrt[d]{\gamma})^m) = \xi_d \sqrt[d]{\alpha}\xi_d^{cm}(\sqrt[d]{\gamma})^m = \xi_d\xi_d^{-1}\sqrt[d]{\alpha}\sqrt[d]{\beta} = \sqrt[d]{\alpha}\sqrt[d]{\beta}.$$

Thus $\sqrt[d]{\alpha}\sqrt[d]{\beta}$ is fixed by G, and is therefore in K. So $\alpha\beta = \lambda^d$ for some λ in K. Then $\sqrt[d]{\alpha} = \lambda/\sqrt[d]{\beta}$.

Finally observe that m and d are relatively prime. Thus $k(\sqrt[d]{\beta}) = k(\sqrt[d]{\gamma^m}) = k(\sqrt[d]{\gamma}) = F$. ∎

Any denesting of this form will cause certain behavior of associated fields. We have the following converse to Zippel's theorem.

Theorem 1.5 *Let α be an element of a field K. Suppose that $\sqrt[d]{\alpha}$ is of degree d over K, and that $\sqrt[d]{\alpha} = \lambda/\sqrt[d]{\beta}$ with λ in K, and β in $k \subset K$. Assume that the d^{th} roots of unity lie in k. Then the field $F = k(\sqrt[d]{\beta})$ satisfies: (i) F over k is Galois and the Galois group of F over $F \cap K$ is isomorphic to the group of FK over K, (ii) $FK = K(\sqrt[d]{\alpha})$, and (iii) $k = F \cap K$.*

Proof Since $F = k(\sqrt[d]{\beta})$, it is clear that F over k is a Galois extension. Then the fields k, F, K, FK satisfy the hypothesis of Theorem 1.3, and $G =$ the Galois group of FK over K is isomorphic to H, the Galois group of F over $F \cap K$. Note that we have $FK = k(\sqrt[d]{\beta})K = K(\sqrt[d]{\beta}) = K(\sqrt[d]{\alpha})$. That $k \subseteq F \cap K$ is clear. To show that the containment is an equality it suffices to observe that $d = [K(\sqrt[d]{\alpha}) : K] = [F : F \cap K] \leq [F : k] \leq d$. This is possible only if $k = F \cap K$. ∎

Note that the hypothesis "$\sqrt[d]{\alpha}$ is of degree d over K" is necessary. For example

$$\sqrt[6]{7\sqrt[3]{20} - 19},$$

is of degree 3 over $Q(\sqrt[3]{20})$, because $7\sqrt[3]{20}-19$ is a square in $Q(\sqrt[3]{20})$. In this case there is more than the usual ambiguity in the denesting: if $\sqrt[d]{\alpha}$ is not of degree d over K, then the roots of $x^d-\alpha$ are not conjugate over K.

By Theorems 1.4 and 1.5, a Zippel denesting exists iff there is a field F, with $FK = K(\sqrt[d]{\alpha})$ and F Galois over $k = F \cap K$. To do so, we search subfields of $L = K(\sqrt[d]{\alpha})$ containing k.

In [4] efficient algorithms were given for computing maximal subfields. It follows immediately from Theorem 2.9 and Algorithm 2.2 of [4] that:

Theorem 1.6 *(Landau & Miller [4]) If $f(x)$ in $Z[x]$ is irreducible of degree m with roots $\alpha, \alpha_2, \ldots, \alpha_m$, then there is an algorithm to compute $\beta_0, \ldots, \beta_j$, where $Q(\beta_0, \ldots, \beta_j)$ is a maximal subfield of $Q(\alpha)$. The running time for the algorithm is the time required to factor $f(x)$ over $Q[z]/f(z)$ plus the time needed to calculate m^3 gcd's of polynomials (of degree less than deg$(f(x))$, with coefficient length less than $m^2 \log ||f(x)||$) over a field containing two roots of $f(z)$.*

Theorem 1.7 *(Landau & Miller [4]) Let $f(x), g(x)$ in $Z[x]$ be irreducible and monic of degree m and r respectively, and $h(x)$ of degree n in $Q[z,x]/f(z)$ be an irreducible factor of $g(x)$ in $Q[z]/f(z)$. There is an algorithm to compute $B(x) = b_l x^l + b_{l-1}x^{l-1} + \ldots + b_0$, a polynomial in $Q[x,z]/f(x)$ whose coefficients determine the field $Q[x]/f(x) \cap Q[x]/g(x)$, in the sense that $Q(b_l, \ldots, b_0) = Q[x]/f(x) \cap Q[x]/g(x)$. The algorithm runs in the time required to factor $N_{Q[z]/f(z)}(h(x-cz))$, $(c < (mn)^2)$, over $Q[z]/f(z)$, plus the time needed to calculate $(mn)^3$ gcd's of polynomials of degree less than max(m,n) with coefficient length less than $(m+n)^2 \log ||h(x)|| \log |f(z)|$.*

As before, it is easy to generalize the algorithms to work over a general field k of characteristic 0. We informally describe how to find the field F, if it exists.

First determine if $d = [K(\sqrt[d]{\alpha}) : K]$. Use the Landau & Miller algorithm to find all maximal subfields F_i of L. If $KF_i \subset L$ for each i, then we are done, since no such F exists.

Otherwise, suppose that $F_1, \ldots, F_t$ satisfy $KF_i = L$. If any of the F_i are Galois over $K \cap F_i = k$ for some i, then we are done by Theorem 1.4. Check that $K \cap F_i \supseteq k$ for each i. Let $F_1, \ldots, F_s$ satisfy $KF_i = L$ and $K \cap F_i \supseteq k$ for each i. If not, compute the maximal subfields of the F_i and repeat the process. If we do not find a field F such that $K(\sqrt[d]{\alpha}) = KF$ and F is Galois over $K \cap F = k$, then by Theorem 1.5, there is no denesting of $\sqrt[d]{\alpha}$ of the form $\lambda/\sqrt[d]{\beta}$, with λ in K, β in k.

The exponential character of the algorithm comes from searching potentially all the subfields of $K(\sqrt[d]{\alpha})$ in order to find F. We conjecture that there is a faster way to handle the search than the essentially brute force approach we are suggesting here. Despite its exponential character, for α of small degree over k, this algorithm is reasonably efficient.

Observe that this method, even if used repeatedly, is not guaranteed to find a minimal denesting of the radical.

Acknowledgements: Thanks to Tsuneo Tamagawa and Walter Feit for several interesting and informative conversations.

References

[1] A. Borodin, R. Fagin, J. Hopcroft and M. Tompa, *Decreasing the Nesting Depth of Expressions Involving Square Roots*, J. Symb. Comput., 1 (1985), pp. 169-188.

[2] B. Caviness and R. Fateman, *Simplification of Radical Expressions*, Proc. SYMSAC 77, pp. 329-338.

[3] S. Landau, *Simplification of Nested Radicals*, to appear, SIAM J. of Comput.

[4] S. Landau and G. Miller, *Solvability by Radicals is in Polynomial Time*, J. Comput. and Sys. Sci., 30 (1985), pp. 179- 208.

[5] S. Lang, *Algebra,* Addison-Wesley, Reading, Mass., 1971.

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

[7] R. Zippel, *Simplification of Expressions Involving Radicals*, J. Symbolic Computation, 1 (1985), pp. 189-210.