Theorems on Field Extensions and Radical Denesting

PRIMES-USA final research paper
by Kaan Dokmeci
Mentor: Yongyi Chen

September 26, 2017

Abstract

The problem of radical denesting is the problem that looks into given nested radical expressions and ways to denest them, or decrease the number of layers of radicals. This is a fairly recent problem, with applications in mathematical software that do algebraic manipulations like denesting given radical expressions. Current algorithms are either limited or inefficient.

We tackle the problem of denesting real radical expressions without the use of Galois Theory. This uses various theorems on field extensions formed by adjoining roots of elements of the original field. These theorems are proven via the roots of unity filter and degree arguments. These theorems culminate in proving a general theorem on denesting and leads to a general algorithm that does not require roots of unity. We optimize this algorithm further. Also, special cases of radical expressions are covered, giving more efficient algorithms in these cases, spanning many examples of radicals. Additionally, a condition for a radical not to denest is given. The results of denesting radicals over $\mathbb{Q}$ are extended to real extensions of $\mathbb{Q}$ and also transcendental extensions like $\mathbb{Q}(t)$. Finally, the case of denesting sums of radicals is explored as well.

1 Introduction

One apparent problem in mathematics involves that of denesting radicals. The Indian mathematician Ramanujan kept a journal of complex radical identities. Among them are the following

- $\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \dfrac{\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}}{3}$
- $\sqrt{\sqrt[3]{28}-3} = \dfrac{\sqrt[3]{98}-\sqrt[3]{28}-1}{3}$
- $\sqrt{\sqrt[5]{\frac{1}{5}}+\sqrt[5]{\frac{4}{5}}} = \sqrt[5]{\frac{16}{125}}+\sqrt[5]{\frac{8}{125}}+\sqrt[5]{\frac{2}{125}}-\sqrt[5]{\frac{1}{125}}$
- $\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}}$
- $\sqrt[8]{4\sqrt[3]{\frac{2}{3}}-5\sqrt[3]{\frac{1}{3}}} = \sqrt[3]{\frac{4}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{1}{9}} = \sqrt[3]{\sqrt[3]{2}-1}$

Of course, it is easy to verify these identities by taking both sides to appropriate powers. The question is whether or not a given nested radical denests in general. Many specific cases of denesting have been examined: for example, in [1] certain identities of Ramanujan are generalized, and [2] deals with denesting solely square roots and gives an algorithm to denest such a radical in general, assuming all the radicands are real. Other papers use Galois theory to denest; for example [3] uses Galois theory to discuss the case of denesting radicals of the form $\sqrt{\sqrt[3]{a}+\sqrt[3]{b}}$. Finally in [4], an algorithm to find the basis of radical extensions of fields is shown. Additionally, [4] briefly discusses using Diophantine equations to denest radicals over $\mathbb{Q}$. However, all these results either are only applicable in specific cases like [1] and [2], or use Galois theory like in [3] or [4]. The use of Galois theory implies that the fields involved are not real anymore due to the presence of roots of unity. In this paper, we give general results on denesting radicals without the use of Galois theory.

For a given radical expression, we can define its **depth**:

- The depth of any rational number is 0.
- If the depth of a radical expression r is d, then the depth of $\sqrt[n]{r}$ is $d+1$.

- If the depth of r_1 is d_1 and the depth of r_2 is d_2, then the depth of any arithmetic combination of r_1, r_2 is $\max(d_1, d_2)$.

In other words, the depth of a radical gives the number of layers of radicals required to write it. For example, the depth of $\sqrt{1+\sqrt[3]{5}}$ is 2. Thus, denesting a radical can be formally described as decreasing the depth of a given radical.

Let an **in-real** field K to be a field extension of $\mathbb{Q}$ that is a subset of $\mathbb{R}$. Note that we can take fields like $\mathbb{Q}(t)$, by treating them as $\mathbb{Q}(\alpha)$ where α is a real, transcendental number. We deal with denestings involving in-real fields. Throughout the paper, fix K to be an in-real field, unless otherwise specified. For an in-real field K, let $\sqrt{K}$ denote the set of real numbers b such that $b^m \in K$ for some integer m. In other words, $\sqrt{K}$ consists of all real numbers of form $\sqrt[m]{k}$ with $k \in K$. Finally, for an integer n and a prime p, let $v_p(n)$ denote the largest integer a such that $p^a \mid n$. For instance, $v_5(325) = 2$, since $325 = 5^2 \cdot 13$. We can extend this definition to include rational numbers, using the rule $v_p(x) + v_p(y) = v_p(xy)$. For example, $v_5\left(\frac{3}{5}\right) = -1$.

The theorems in Sections 2,3, and 4 are motivated by following observation on denested radicals: given a depth 1 radical r, if $\sqrt[n]{r}$ denests as a depth 1 radical, then it is of the form $\sqrt[m]{b} \cdot \alpha$ where $\alpha \in \mathbb{Q}(r)$ and b is some rational. For example, $\sqrt[3]{\sqrt[3]{2}-1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}} = \sqrt[3]{\frac{1}{9}} \cdot (1 - \sqrt[3]{2} + \sqrt[3]{4})$. All the radical identities above satisfy the observation. Section 2 deals with general theorems on extensions of fields. The theorems in Section 2 generalize those in [2], which only deals with the particular case of $p = 2$, applying its theorems to the problem of denesting square roots. Section 2 generalizes these theorems. An algorithm that generates a basis of a field extension involving radicals is also discussed. Section 3 applies the theorems in Section 2 to the problem of denesting radicals by proving the above observation, using it to come up with a general method of denesting. Section 4 looks at special cases of denesting depth 2 radicals into depth 1 radicals over $\mathbb{Q}$. Section 5 discusses denesting radicals in transcendental fields and denesting radicals with higher depths. Finally, Section 6 discusses the matter of denesting a sum of radical expressions.

2 Theorems on Field Extensions

The key part of the following theorems is that the fields involved are in-real, and thus do not contain complex numbers besides ± 1. The following theorems look at degrees of extensions.

Theorem 2.1. *Let K be an in-real field with $a \in K$ and n an integer. Then, if $\sqrt[p]{a} \notin K$ for all primes p that divide n, $K(\sqrt[n]{a})$ has degree n over K.*

Proof. We show that $X^n - a$ is irreducible over K. Indeed, suppose there was a smaller irreducible factor. Since $X^n - a$ factors as $\prod_{i=0}^{n-1}(X - \sqrt[n]{a}\zeta_n^i)$. Thus, any divisor of $X^n - a$ must have constant term of form $\sqrt[n]{a^e} \cdot \zeta_n^j$ for some integers e, j, where e is the degree of the divisor. In particular, if k is the degree of $\sqrt[n]{a}$ over K, then the constant term of the minimal polynomial of $\sqrt[n]{a}$ over K is of the form $\sqrt[n]{a^k} \cdot \zeta_n^j$. Since this quantity must be in K and K is in-real, ζ_n^j is either 1 or -1. Thus, $\sqrt[n]{a^k} \in K$. By assumption, $k < n$. Take some prime p such that $v_p(k) < v_p(n)$ – which must exist, since $k < n$. Then write $k = k' \cdot p_k$ and $n = n' \cdot p_n$ where n_k and p_n are the largest powers of p dividing k and n. Then $a^{\frac{k' \cdot p_k}{n' \cdot p_n}} \in K$. Let $p' = p_n/p_k$; then, taking the quantity to the n' power, $a^{\frac{k'}{p'}} \in K$ where p' is a power of p. But note that $\gcd(k', p') = 1$, since p' is a power of p and k' is relatively prime to p by assumption. Take an x such that $xk' \equiv 1 \pmod{p'}$ which exists by Bezout; then we get $a^{\frac{xk'}{p'}} \in K$, which implies that $a^{\frac{1}{p'}} \in K$. Taking the quantity to the p/p' power, $a^{1/p} \in K$, contradicting the inital assumption. Thus, it follows that $K(\sqrt[n]{a})$ has degree n over K. □

Theorem 2.2. *Let $b \in \sqrt{K}$. Then if $[K(b) : K] = d$, we have $b^d \in K$.*

Proof. Since $b \in \sqrt{K}$, we have $b^n \in K$ for some integer n. In particular, b is the root of $f(X) = X^n - c$ for $c \in K$. Since $[K(b) : K] = d$, it follows that the minimal polynomial of b has degree d. It must divide f, so its factors are among those of form $(X - b\zeta_n^i)$ for $i = 0, \ldots, n-1$. Note that taking d such factors and multiplying means the constant term of the minimal polynomial of b is $b^d\zeta_n^j$ for some integer j. But since K is in-real, it follows $\zeta_n^j = \pm 1$, so $b^d \in K$. □

We now introduce the **roots of unity filter**, which will be used in this section. For a given polynomial $f(X) = \sum_{i=0}^{k} a_i X^i$, we can compute

$$\sum_{i \equiv k \pmod{n}} a_i X^i = \frac{1}{n} \sum_{i=0}^{n-1} f(X\zeta_n^i) \cdot \zeta_n^{-ik}.$$

Indeed, note that

$$\sum_{i=0}^{n-1} f(X\zeta_n^i) \cdot \zeta_n^{-ik} = \sum_{i=0}^{n-1} \sum_{j=0}^{k} a_j X^j \zeta_n^{i(j-k)} = \sum_{j=0}^{k} a_j X^j \cdot \left(\sum_{j=0}^{n-1} \zeta_n^{i(j-k)} \right).$$

Note that $\sum_{j=0}^{n-1} \zeta_n^{i(j-k)}$ is 0 if $j \neq k \pmod{n}$ and n otherwise. Thus, the equation follows. We use the roots of unity filter to help prove some of the following theorems.

Theorem 2.3. *Let p and q be primes. Let r be a radical expression and K an in-real field such that $\sqrt[p]{r} \in K\left(\sqrt[q]{d}\right)$ with $d \in K$ and $\sqrt[q]{d} \notin K$. Then either*

- *$p = q$, and $\sqrt[p]{r} = \sqrt[p]{d^m} \cdot \alpha$ with $\alpha \in K$ and m an integer or*
- *$p \neq q$, and $\sqrt[p]{r} \in K$.*

Proof. We first introduce the following lemmas:

Lemma 2.4. *If K is an in-real field and $e \in K$ with p prime, then $[K(\sqrt[p]{e}) : K]$ is either 1 or p.*

Proof. By Theorem 2.1. with $n = p$, either $\sqrt[p]{e}$ has degree p over K or $\sqrt[p]{e} \in K$. □

Lemma 2.5. *If $d \in K$, $e \in K(\zeta_p)$ and $e \in K\left(\sqrt[p]{d}\right)$, then $e \in K$.*

Proof. Note that $K(e) \subset K(\zeta_p)$ and $K(e) \subset K\left(\sqrt[p]{d}\right)$. Thus $[K(\zeta_p) : K(e)] \cdot [K(e) : K] = [K(\zeta_p) : K]$. But the RHS is less than p. Thus $[K(e) : K] < p$. On the other hand, $\left[K\left(\sqrt[p]{d}\right) : K(e)\right] \cdot [K(e) : K] = \left[K\left(\sqrt[p]{d}\right) : K\right]$. The RHS is either 1 or p. If it is 1, then $[K(e) : K] = 1$. If it is p, then $[K(e) : K] \mid p$. But $[K(e) : K] < p$, so once again $[K(e) : K] = 1$, so $e \in K$. □

Lemma 2.6. *If $\sqrt[p]{r} \notin K$, then $p = q$.*

Proof. Because $\sqrt[p]{r} \in K\left(\sqrt[q]{d}\right)$ and any element of K is in $K\left(\sqrt[q]{d}\right)$, we have $K(\sqrt[p]{r}) \subset K\left(\sqrt[q]{d}\right)$. But then consider the chain $K \subset K(\sqrt[p]{r}) \subset K\left(\sqrt[q]{d}\right)$. Note that $[K(\sqrt[p]{r}) : K] \mid \left[K\left(\sqrt[q]{d}\right) : K\right]$. By lemma 2.2, the LHS equals p, so p divides the right hand side. Note that since q is prime, the right hand side is either 1 or q. Then clearly $p = q$. □

Therefore, if $p \neq q$, then $\sqrt[p]{r} \in K$, proving the second statement of the theorem. From here on, assume $p = q$. We return to the main part of the proof.

Case 1: p is odd. Write $\sqrt[p]{r} = s_0 + s_1\sqrt[p]{d} + \cdots + s_{p-1}\sqrt[p]{d^{p-1}}$. In other words, $\sqrt[p]{r} = f\left(\sqrt[p]{d}\right)$ where $f(X) = \sum_{i=0}^{p-1} s_i X^i \in K(X)$. Thus $r = f\left(\sqrt[p]{d}\right)^p$. Let $f(X)^p = \sum_{i=0}^{p-1} X^i \cdot f_i(X^p)$. In other words, $X^i \cdot f_i(X^p)$ gives the terms of $f(X)^p$ with degree $i \pmod p$. Then

$$r = f_0(d) + \sqrt[p]{d} \cdot f_1(d) + \sqrt[p]{d^2} \cdot f_2(d) + \cdots + \sqrt[p]{d^{p-1}} \cdot f_{p-1}(d)$$

In particular, the LHS is in K and $f_i(d) \in K$. Since $\sqrt[p]{d}$ has degree p over K, it follows that $f_i(d) = 0$ for $i \neq 0$. That is, $r = f_0(d)$. But then note that

$$r = f_0(d) + \sqrt[p]{d}\zeta_p^k \cdot f_1(d) + \sqrt[p]{d}\zeta_p^{2k} \cdot f_2(d) + \cdots$$

Thus $r = f\left(\sqrt[p]{d} \cdot \zeta_p^k\right)^p$, or $\sqrt[p]{r}\zeta_p^{e_k} = f\left(\sqrt[p]{d} \cdot \zeta_p^k\right)$ for some integer e_k. Suppose $s_m \neq 0$ for some integer m; if all the s_i were zero, then obviously $r = 0$. Then consider the sum $\sum_{i=0}^{p-1} \zeta_p^{-mi} f\left(\sqrt[p]{d}\zeta_p^i\right)$. Because $1 + \zeta_p^k + \zeta_p^{2k} + \cdots$ equals 0 for $p \nmid k$ and p otherwise, it follows that the sum equals $p \cdot s_m \cdot \sqrt[p]{d^m}$. On the other hand, this sum equals $\sum_{i=0}^{p-1} \sqrt[p]{r}\zeta_p^{e_i - mi} = \sqrt[p]{r} \cdot t$ for some $t \in K(\zeta_p)$. Thus $\sqrt[p]{r} \cdot t = p \cdot s_m \cdot \sqrt[p]{d^m}$, or $\sqrt[p]{\dfrac{r}{d^m}} = \dfrac{p \cdot s_m}{t} \in K(\zeta_p)$. On the other hand, $r/d^m \in K$, and obviously $\sqrt[p]{\dfrac{r}{d^m}} \in K\left(\sqrt[p]{\dfrac{r}{d^m}}\right)$. Thus by Lemma 2.3, $\sqrt[p]{\dfrac{r}{d^m}} \in K$; in other words, there is some $\alpha \in K$ such that $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{d^m}$.

Case 2: $p = 2$. In this case, $\sqrt{r} = s_0 + s_1\sqrt{d}$ with $s_0, s_1 \in K$. Now, squaring we get $r = s_0^2 + s_1^2 d + 2s_0 s_1\sqrt{d}$ or $r - s_0^2 - s_1^2 d = 2s_0 s_1\sqrt{d}$. But note that the LHS is in K. Thus it follows that $s_0 s_1 = 0$, since $\sqrt{d} \notin K$. If $s_0 = 0$, then $\sqrt{r} = s_1\sqrt{d}$. If $s_1 = 0$, then $\sqrt{r} = s_0$. In both cases, the theorem is true. □

We generalize Theorem 2.3 with the following two theorems:

Theorem 2.7. *Let K be an in-real field such that $r \in K$. Fix $a_1, a_2, \ldots, a_k \in K$ such that none of the a_i are pth powers in K. Moreover, let L be an extension $K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ such that $\sqrt[p]{r} \in L$ and $[L : K] = \prod n_i$. Then $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{a_1^{e_1} \cdots a_k^{e_k}}$ for integers e_i and $\alpha \in K$.*

Proof. First, we can assume that the n_i are powers of p. Indeed, say $q \mid n_j$ and $q \neq p$. Let $L' = K(\sqrt[n_1']{a_1}, \ldots, \sqrt[n_k']{a_k})$ with $n_i = n_i'$ for $i \neq j$ and $n_j' = n_j/q$. Then by Theorem 2.3, $\sqrt[p]{r} \in L'$ since $q \neq p$. Thus we can assume the n_i are powers of p.

We induct on k. The claim is obvious for $k = 0$. Now assume $k > 0$. First, suppose $n_k = p$. Then let $L' = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{k-1}]{a_{k-1}})$. Then note that $\sqrt[p]{r} = \sqrt[p]{a_k^m} \cdot \alpha$ with $\alpha \in L'$ by Theorem 2.3. Now we use the inductive hypothesis on α: note $\alpha = \sqrt[p]{r \cdot a_k^{-m}} \in L'$ and $\alpha^p = r \cdot a_k^{-m} \in K$. Thus by the inductive hypothesis, $\alpha = \alpha' \cdot \sqrt[p]{a_1^{e_1} \cdots a_{k-1}^{e_{k-1}}}$ where $\alpha' \in K$, and with $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{a_k^m}$ we are done.

Now, suppose $n_k \neq p$. For simplicity, write $a = a_k$ and $n = n_k$. Suppose $\sqrt[p]{r} \notin K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n/p]{a_k})$. We claim this gives a contradiction. We split up on cases depending on the parity of p.

Case 1: p is odd. Now, write $L_1 = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n/p]{a})$ and $L_2 = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n/p^2]{a})$. First, note that $\sqrt[p]{r} = s \cdot \sqrt[n]{a^m}$ with $s \in L_1$ and $p \nmid m$ by Theorem 2.3. Write $s = \sum_{i=0}^{p-1} s_i \sqrt[n/p]{a^i}$ with $s_i \in L_2$. Also, write $f(X) = \sum_{i=0}^{p-1} s_i X^i \in L_2[X]$. Now note that $r = f\left(\sqrt[n/p]{a}\right)^p \cdot \sqrt[n/p]{a^m}$. Once again, write $f(X)^p = \sum_{i=0}^{p-1} X^i f_i(X^p)$; in other words, $X^i \cdot f_i(X^p)$ gives the terms of $f(X)^p$ with degree $i \pmod p$. Note that

$$r = \sqrt[n/p]{a^m} \cdot (f_0(\sqrt[n/p^2]{a}) + f_1(\sqrt[n/p^2]{a}) \cdot \sqrt[n/p]{a} + \cdots + f_{p-1}(\sqrt[n/p^2]{a}) \cdot \sqrt[n/p]{a^{p-1}})$$

Now, write $f_i = f_{i+p}$ for simplicity. Note that since $r \in L_2$, it follows that the only nonzero f_i

can be f_{-m}. In particular, note that

$$f(\sqrt[n/p]{a}\cdot\zeta_p^k)^p=\sum_{i=0}^{p-1}\left(\sqrt[n/p]{a}\zeta_p^k\right)^i\cdot f_i(\sqrt[n/p^2]{a})=f_{-m}(\sqrt[n/p^2]{a})\cdot\sqrt[n/p]{a^{-m}}\cdot\zeta_p^{-mk}=f(\sqrt[n/p]{a})^p\cdot\zeta_p^{-mk}$$

Thus, for any given k, note that $r=f(\sqrt[n/p]{a}\cdot\zeta_p^k)^p\cdot\zeta_p^{mk}\cdot\sqrt[n/p]{a^m}$. Thus $\sqrt[p]{r}=f(\sqrt[n/p]{a}\cdot\zeta_p^k)\cdot\zeta_{p^2}^{d_k}\cdot\sqrt[n]{a^m}$ for some integers d_k such that $d_k\equiv mk \pmod p$.

Suppose $s_j\neq 0$. Then note that $\sum_{i=0}^{p-1}\zeta_p^{-ij}f(\sqrt[n/p]{a}\cdot\zeta_p^i)=p\cdot s_j\cdot\sqrt[n/p]{a^j}$. In particular, this means that $p\cdot s_j\cdot\sqrt[n/p]{a^j}=\sum_{k=0}^{p-1}\sqrt[p]{r}\cdot\zeta_{p^2}^{-d_k}\cdot\zeta_p^{-kj}\cdot\sqrt[n]{a^{-m}}$. Now write $t=\sum_{k=0}^{p-1}\zeta_{p^2}^{-d_k}\cdot\zeta_p^{-kj}=\sum_{k=0}^{p-1}\zeta_{p^2}^{d'_k}$ where each d'_k is distinct $\pmod p$. Then we have $p\cdot s_j\cdot\sqrt[n]{a^{pj+m}}=\sqrt[p]{r}\cdot t$ for $t\in\mathbb{Q}(\zeta_{p^2})$. Now, recall that $\sqrt[p]{r}/\sqrt[n]{a^m}\in L_1$. Thus $\frac{t}{p\cdot s_j\cdot\sqrt[n/p]{a^j}}\in L_1$. Now, s_j and $\sqrt[n/p]{a^j}\in L_1$. Thus $t\in L_1$. Also, note that $(p\cdot s_j)^p\cdot\sqrt[n/p^2]{a^j}\cdot\sqrt[n/p]{a^m}=r\cdot t^p$. Thus, we also have $\frac{t^p}{\sqrt[n/p]{a^m}}\in L_2$. Also, $t^{p^2}\in L_2$. But note that $t^p\notin L_2$ since $\sqrt[n/p]{a^m}\notin L_2$. But $t\in L_1$, so $L_2\subset L_2(t)\subset L_1$. Since $[L_1:L_2]=p$ and $t\notin L_2$, it follows $[L_2(t):L_2]=p$. However, since $t^{p^2}\in L_2$, it follows $t\in\sqrt{L_2}$. By Theorem 2.2, it follows that $t^p\in L_2$, contradiction! Thus it follows that our initial assumption gives a contradiction, and the proof is complete in the case where p is odd.

Case 2: $p=2$. Define L_1,L_2 similarly. Note that we have $\sqrt{r}=s\cdot\sqrt[n]{a}$ where $s\in L_1$ by Theorem 2.3. Now, since $s\in L_1$, we have $s=s_0+s_1\sqrt[n/2]{a}$ where $s_0,s_1\in L_2$. Thus, $\sqrt{r}=(s_0+s_1\sqrt[n/2]{a})\sqrt[n]{a}$, and squaring both sides we have $r=(2s_0s_1)\sqrt[n/4]{a}+(s_0^2+s_1^2\sqrt[n/4]{a})\sqrt[n/2]{a}$. Since $s_0,s_1,\sqrt[n/4]{a},r\in L_2$ but $\sqrt[n/2]{a}\notin L_2$ we have $s_0^2+s_1^2\sqrt[n/4]{a}=0$. Since all the expressions here are nonnegative, $s_0=s_1=0$, meaning $r=0$, contradiction. Thus the $p=2$ case is proven as well. □

Theorem 2.8. *Let K be an in-real field, and $r,d\in K$ such that $\sqrt[n]{r}\in K(\sqrt[m]{d})$ with $\sqrt[n]{r}$ having degree n over K and $\sqrt[m]{d}$ having degree m over K. Then $\sqrt[n]{r}=\alpha\cdot\sqrt[n]{d^e}$ for $\alpha\in K$ and e an integer.*

Proof. We prove the result via induction on the number of prime divisors of n (including multiplicities). Note that the case where n is prime is given by Theorem 2.7.

Suppose the theorem is true for all integers with fewer prime divisors than n. We prove it for n. First, note that since $K(\sqrt[p]{r}) \subseteq K(\sqrt[m]{d})$. It follows that $n \mid m$. Let p divide n. Since $\sqrt[p]{r} \in K(\sqrt[m]{d})$, it follows $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{d^e}$ for $\alpha \in K$ and e an integer. Now note that $\sqrt[n]{rd^{-e}} = \sqrt[n/p]{\alpha}$. Moreover, since $n \mid m$, we have $\sqrt[n]{d^{-e}} \in K(\sqrt[m]{d})$. It follows that $\alpha \in K$ and $\sqrt[n/p]{\alpha} \in K(\sqrt[m]{d})$. By the inductive hypothesis, this means $\sqrt[n/p]{\alpha} = \alpha' \cdot \sqrt[n/p]{d^f}$ for $\alpha' \in K$ and f an integer. Thus $\sqrt[n]{rd^{-e}} = \alpha' \cdot \sqrt[n/p]{d^f}$. In other words, $\sqrt[n]{r} = \alpha' \cdot \sqrt[n]{d^{e+pf}}$, and thus the inductive step is complete. □

Define an extension $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ to be simple if $a_i \in K$ and $[L : K] = \prod n_i$. We show that any extension $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ can be made simple with the following theorem:

Theorem 2.9. *Let K be an in-real field and $a_1, \ldots, a_k \in K$, and $n_1, \ldots, n_k$ integers. If $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ and $[L : K] \neq \prod n_i$, then there exist n'_i and a'_i such that $L = K(\sqrt[n'_1]{a'_1}, \ldots, \sqrt[n'_j]{a'_j})$ and $\prod n'_i = [L : K]$.*

Proof. We start with a lemma:

Lemma 2.10. *If K is an in-real field and $a \in K$, and $n = \prod q_i$ where q_i are prime powers, each pairwise relatively prime, then $K(\sqrt[n]{a}) = K(\sqrt[q_1]{a}, \ldots, \sqrt[q_k]{a})$.*

Proof. We show that $\sqrt[q_i]{a} \in K(\sqrt[n]{a})$, which shows that $K(\sqrt[q_1]{a}, \ldots, \sqrt[q_k]{a}) \subset K(\sqrt[n]{a})$. But note that $\sqrt[n]{a} \in K(\sqrt[n]{a})$. Taking the expression to the n/q_i power, $\sqrt[q_i]{a} \in K(\sqrt[n]{a})$.

Next, we show that $\sqrt[n]{a} \in K(\sqrt[q_1]{a}, \ldots, \sqrt[q_k]{a})$. But this follows by Bezout on a^{1/q_i}. Thus, $K(\sqrt[n]{a}) \subset K(\sqrt[q_1]{a}, \ldots, \sqrt[q_k]{a})$. Taking both inclusions proves the lemma. □

Thus, we can assume all the n_i are prime powers by the separation into prime powers by Lemma 2.10.

We first consider the case where the n_i are prime powers of the same prime p. First, order the $\sqrt[n_i]{a_i}$ in decreasing order of n_i, so that $n_1 \geq n_2 \geq \ldots \geq n_k$. Next, consider the chain of extensions

$$K \subset K(\sqrt[p]{a_1}) \subset \cdots \subset K(\sqrt[n_1]{a_1}) \subset K(\sqrt[n_1]{a_1}, \sqrt[p]{a_2}) \subset \cdots \subset K(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}) \subset \cdots \subset K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$$

Consider the first step the extension is not proper. This must be at a point where $\sqrt[p]{a_{j+1}} \in K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_j]{a_j})$. Indeed, if $\sqrt[p^{e+1}]{a_{j+1}} \in K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_j]{a_j}, \sqrt[p^e]{a_{j+1}})$, then by taking $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_j]{a_j})$ we get $\sqrt[p^{e+1}]{a_{j+1}} \in L(\sqrt[p^e]{a_{j+1}})$. By Theorem 2.1, this means $\sqrt[p]{a_j} \in L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_j]{a_j})$. In this case, $\sqrt[p]{a_{j+1}} = \alpha \cdot \sqrt[p]{a_1^{e_1} \cdots a_j^{e_j}}$ for $\alpha \in K$ and integers e_i by Theorem 2.7. Now, we claim that $K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_j]{a_j}, \sqrt[n_{j+1}/p]{\alpha}) = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_{j+1}]{a_{j+1}})$. Indeed, $\sqrt[n_{j+1}/p]{\alpha} = \sqrt[n_{j+1}]{\frac{a_{j+1}}{a_1^{e_1} \cdots a_j^{e_j}}}$. Because of the ordering of n_i, we have $\sqrt[n_{j+1}]{a_1^{e_1} \cdots a_j^{e_j}} \in K(\sqrt[n_1]{a_1}, \cdots, \sqrt[n_j]{a_j})$. Note that this replacement decreases $\prod n_i$. Repeating this procedure, we eventually get $[L : K] = \prod n_i$ in the case when all the n_i are powers of the same prime p.

Now, in the general case, we once again assume all the n_i are prime powers by Lemma 2.8. We generate the chain of extensions as follows:

- Let the prime divisors of $[L : K]$ be p_1 through p_k
- Let $K = K_0$
- Define K_{i+1} as K_i adjoin all the radicals $\sqrt[n]{a}$ such that n is a prime power of p_{i+1} for $i = 0, \ldots, k-1$.
- $L = K_k$.

Now, by applying the procedure for prime powers on each K_i with respect to K_{i-1}, inductively, the theorem holds. Note that the a_i' are still roots of combinations of products of the a_i; we will use this in the proof of Theorem 3.1. □

We end the section with a theorem that generalizes Theorem 2.8:

Theorem 2.11. *Let K be an in-real field and $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ with $[L : K] = \prod n_i$. If $b \in \sqrt{K}$ and $b \in L$, then $b = \alpha \cdot \prod \sqrt[n_i]{a_i^{e_i}}$ for some choice of integers e_i and $\alpha \in K$.*

Proof. We induct on k. Note that the case $k = 1$ is given by Theorem 2.8.

Suppose the theorem is true for all values less than k. We prove it for k. Write $b_i = \sqrt[n_i]{a_i} \in \sqrt{K}$. Taking $K' = K(b_1, \ldots, b_{k-1})$, we have $b \in L$ and $b \in \sqrt{K'}$; Thus $b = \alpha \cdot b_k^{e_k}$ for $\alpha \in K'$

and e_k an integer. However, note that $\sqrt{K}$ is closed under multiplication. Since $b, b_k^{e_k} \in \sqrt{K}$, it follows $\alpha \in \sqrt{K}$. Moreover, $\alpha \in K'$. By the inductive hypothesis on α, K, K', it follows $\alpha = \alpha' \cdot \prod_{i=1}^{k-1} b_i^{e_i}$ where $\alpha' \in K$. Then we have $b = \alpha' \cdot \prod b_i^{e_i}$, completing the induction. □

We now present an algorithm that computes the basis of $\mathbb{Q}(r)$ over $\mathbb{Q}$ where r is a depth one radical $r = \sum \sqrt[n_i]{a_i}$. First, assume that the a_i are integers; we can do this by multiplying by a suitable constant We can define a radical to be an ordered pair (n, a) representing $\sqrt[n]{a}$ where n, a are integers with $n \geq 2$. We can also define a power-radical to be one of the form $\sqrt[p^k]{a}$ where p is a prime and k, a are integers. We represent such a value through the triple (p, k, a). We can represent a radical extension K of $\mathbb{Q}$ through a vector consisting of power-radicals by Lemma 2.10.

Given a vector of power-radicals, we sort it according to the following rules:

- (p_1, k_1, a_1) comes before (p_2, k_2, a_2) if $p_1 > p_2$.
- If $p_1 = p_2$, then (p_1, k_1, a_1) comes before (p_2, k_2, a_2) if $k_1 > k_2$.
- If $p_1 = p_2$ and $k_1 = k_2$ then (p_1, k_1, a_1) comes before (p_2, k_2, a_2) if $a_1 > a_2$.

This sections off the vector into radicals with the same prime power. Then we can find the simple basis involving solely the prime powers of the same prime as in the beginning of the proof of Theorem 2.9. Namely, take all the ordered triples (p_i, k_i, a_i) with $p_i = p$, and let this set be S. Among the triples in S, take the set of prime factors of the a_i's, and let this set be $A = \{p_1, p_2, \ldots, p_n\}$. Then note that each a_i can be written in the form $a_i = \prod_{p_j \in A} p_j^{e_{i,j}}$. We have a set of vectors $v_i = (e_{i,1}, \ldots, e_{i,n})$. To find the basis, note that we need to ensure that all the v_i are linearly independent $\pmod p$. If not, suppose WLOG $b_1 v_1 + \ldots + b_{m-1} v_{m-1} + v_m = 0$ (by multiplying by a suitable constant, we can assume that the coefficent of v_m is one). Then replace a_m with $\sqrt[p]{\frac{a_1^{b_1} \cdots a_{m-1}^{b_{m-1}}}{a_m}}$ and k_m with $k_m - 1$. If $k_m = 0$ after this, then simply discard the mth ordered triple from S. Now repeat the process until all the v_i are linearly independent. This finishes the algorithm described by Theorem 2.9, and repeating for all the other primes gives us $\mathbb{Q}(r)$ as a simple extension over $\mathbb{Q}$. In particular, note that if $\mathbb{Q}(r) = \mathbb{Q}(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ and $[\mathbb{Q}(r) : \mathbb{Q}] = \prod n_i$, we have the basis equal to the set of all numbers of form $\prod \sqrt[n_i]{a_i^{e_i}}$ where e_i ranges from 0 to $n_i - 1$.

3 Applications to Denesting

We can apply the above theorems to deduce the following

Theorem 3.1. *Let r be a depth 1 radical over K, an in-real field. Then, if $\sqrt[n]{r}$ denests as a depth 1 radical in K, it takes the form $b \cdot \alpha$ where $b \in \sqrt{K}$ and $\alpha \in K(r)$.*

Proof. We induct on the number of prime factors of n. If $n = 1$, the theorem obviously holds. Now we prove the inductive step.

Let p be a prime divisor of n. Clearly, $\sqrt[p]{r}$ must denest. Let $K(\sqrt[p]{r}) = L$. Since $\sqrt[p]{r}$ denests as a depth 1 radical in K, it follows that $L = K(r, \sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ such that $a_i \in K$. Now, choose a'_i and n'_i as in Theorem 2.9 such that $[L : K(r)] = \prod n'_i$ and $L = K(r, \sqrt[n'_1]{a'_1}, \ldots, \sqrt[n'_j]{a'_j})$; note that the a'_i are still roots of products of a_i (by the discussion at the end of Theorem 2.9), and thus the a'_i are in $\sqrt{K}$. It follows that by Theorem 2.11 that $\sqrt[p]{r} = \prod \sqrt[n'_i]{a'^{e_i}_i} \cdot \alpha$ with $\alpha \in K(r)$. In other words, $\sqrt[p]{r} = b \cdot \alpha$ with $\alpha \in K(r)$ and $b \in \sqrt{K}$.

Now we use the inductive step: note $\alpha \in K(r)$, and is therefore a depth 1 radical. Now, since $\sqrt[n]{r} = \sqrt[n/p]{b \cdot \alpha}$ denests, it follows $\sqrt[n/p]{\alpha}$ denests. Thus, it equals $b' \cdot \alpha'$ with $b' \in \sqrt{K}$ and $\alpha' \in K(\alpha) \subset K(r)$. Therefore, $\sqrt[n]{r} = \sqrt[n/p]{b} \cdot b' \cdot \alpha'$, which proves the theorem. $\square$

As an example, $\sqrt[3]{\sqrt[3]{2} - 1} = \frac{1}{\sqrt[3]{9}} \cdot (1 - \sqrt[3]{2} + \sqrt[3]{4})$ and $\sqrt{4\sqrt{3} - 6} = \sqrt[4]{3} \cdot (\sqrt{3} - 1)$. Now, given r, b, α as above with $\sqrt[n]{r} = b \cdot \alpha$ with $b \in \sqrt{K}$ and $\alpha \in K(r)$, we show a theorem that describes the possible values of b.

Theorem 3.2. *Let r be a depth 1 radical over K such that $\sqrt[n]{r}$ denests as a depth 1 radical over K. Write $r = b_1 + b_2 + \cdots + b_k$ where $b_i \in \sqrt{K}$ for all i. Then if $\sqrt[n]{r}$ denests in the form $b \cdot \alpha$ with $\alpha \in K(r)$ and $b \in \sqrt{K}$, then $b^n = c \cdot \prod b_i^{e_i}$ for some $c \in K$ and integers e_i.*

Proof. First, note that $r = b^n \cdot \alpha^n$. Thus, $b^n \in K(r)$. We also have $b^n \in \sqrt{K}$. Write $d = b^n$. We wish to prove that if $d \in \sqrt{K}$ and $d \in K(b_1, \ldots, b_k)$, then $d = c \cdot \prod b_i^{e_i}$ for some integers e_i and $c \in K$.

Now, with the aid of Theorem 2.7, we can find $b_i' \in \sqrt{K}$ such that $K(r) = K(b_1', \ldots, b_k')$ and $[K(r) : K] = \prod [K(b_i') : K]$. Now, $d \in K(b_1', \ldots, b_k')$. But now the required statement is precisely Theorem 2.11, after noting that the b_i''s can be written as a product of b_i's and elements of K. □

This gives us a general algorithm that will always denest a radical $\sqrt[n]{r}$, where r has depth 1 over K. Moreover, suppose $K(r) = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ such that $a_i \in K$ and $[K(r) : K] = \prod n_i$, guaranteed by Theorem 2.9. Then a basis of $K(r)$ over K is S where S consists of all products of form $\prod_{i=1}^{k} \sqrt[n_i]{a_i^{e_i}}$ where e_i ranges from 0 to $n_i - 1$. Let this basis be $\{1, b_1, \ldots, b_M\}$ where $M = \prod n_i - 1$. Then if $\sqrt[n]{r}$ denests, we have

$$r = c \cdot b \cdot (x_0 + x_1 \cdot b_1 + \ldots + x_M \cdot b_M)^n$$

for some $b \in S$ and $c \in K$. But note that we can replace x_i with x_i/x_0 and c with $c \cdot x_0^n$ to WLOG that $x_0 = 1$. To optimize further, we only have to consider $b = \prod_{i=1}^{k} \sqrt[n_i]{a_i^{e_i}}$ where e_i ranges from 0 to $\gcd(n_i, n) - 1$. Indeed, write $d = \gcd(n_i, n)$. Then take A, B with $An + Bn_i = d$. Then

$$b \cdot b_i^d (1 + x_1 \cdot b_1 + \cdots + x_M \cdot b_M)^n = b \cdot b_i^{An+Bn_i} (1 + x_1 \cdot b_1 + \cdots + x_M \cdot b_M)^n = (b_i^{n_i})^B \cdot b \cdot [b_i^A (1 + x_1 \cdot b_1 + \cdots + x_M \cdot b_M)]^n$$

Thus any denesting with $b = \prod_{i=1}^{k} \sqrt[n_i]{a_i^{e_i}}$ is equivalent to one where $e_i = e_i + \gcd(n_i, n)$.

Now, for each of the possible b's, we have

$$r = c \cdot [b \cdot (1 + x_1 \cdot b_1 + \ldots + x_M \cdot b_M)^n] = c \cdot [f_0 + f_1 \cdot b_1 + \ldots + f_M \cdot b_M]$$

where $f_0, \ldots, f_M$ are polynomials in $x_1, \ldots, x_M$. If we write $r = r_0 + r_1 \cdot b_1 + \ldots + r_M \cdot b_M$, then we have M polynomial equations, each of the form $r_i \cdot f_0(x_1, \ldots, x_M) - r_0 \cdot f_i(x_1 \ldots, x_M) = 0$ for $i = 1, \ldots, M$. We then have a system of M polynomials in M variables that we need to solve over K. If $K = \mathbb{Q}$, then we can use the Rational Root Theorem to quickly solve this.

For example, to denest $\sqrt[3]{\sqrt[3]{2} - 1}$ as a depth 1 radical in the rationals, one would consider the three possible equations

- $\sqrt[3]{2}-1 = c\cdot(1+x_1\sqrt[3]{2}+x_2\sqrt[3]{4})^3$
- $\sqrt[3]{2}-1 = c\cdot\sqrt[3]{2}\cdot(1+x_1\sqrt[3]{2}+x_2\sqrt[3]{4})^3$
- $\sqrt[3]{2}-1 = c\cdot\sqrt[3]{4}\cdot(1+x_1\sqrt[3]{2}+x_2\sqrt[3]{4})^3$

Here, $b\in\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ and $b_1=\sqrt[3]{2}, b_2=\sqrt[3]{4}$. To solve this system, one would expand the right hand sides and equate corresponding terms – since c and the x_i are rational, the constant, $\sqrt[3]{2}$, and $\sqrt[3]{4}$ terms must equal. If any of these has a solution (c, x_1, x_2) in rationals, then $\sqrt[3]{\sqrt[3]{2}-1}$ denests. Indeed, note that $\sqrt[3]{2}-1=\frac{1}{9}(1-\sqrt[3]{2}+\sqrt[3]{4})^3$, and thus $\sqrt[3]{\sqrt[3]{2}-1}=\frac{1-\sqrt[3]{2}+\sqrt[3]{4}}{\sqrt[3]{9}}$.

4 Cases of Denesting

In this section, we explore certain cases of denesting using Theorem 3.2.

Theorem 4.1. *Let r be a depth 1 radical over K, and n an integer. Let $N: K(r)\to K$ denote the norm of an element x of $K(r)$ with respect to K. Moreover, let $K(r)=K(\sqrt[n_1]{a_1},\ldots,\sqrt[n_k]{a_k})$ be a simple extension of K. Let B be the set of numbers of form $\prod\sqrt[n_i]{a_i^{e_i}}$ where each $0\le e_i<\gcd(n_i,n)$. Finally, let $g=\gcd(n,[K(r):K])$. Then if $N(r/b)$ is not a perfect gth power in K for some $b\in B$, then $\sqrt[n]{r}$ does not denest.*

Proof. We show the contrapositive: that if $\sqrt[n]{r}$ denests, then $N(r/b)$ must be a perfect gth power for some $b\in B$. Since $\sqrt[n]{r}$ denests, we have $r=c{\cdot}b{\cdot}\alpha^n$ where $\alpha\in K(r)$ and $b\in B, c\in K$. Taking the norm, $N(r)=N(b)\cdot N(c)\cdot N(\alpha^n)$. Now, since $c\in K$, $N(c)=c^{[K(r):K]}$. Thus, $N(r/b)=c^{[K(r):K]}\cdot N(\alpha)^n$. Since N maps to K, it follows that $N(r/b)$ is a perfect gth power in K, as desired. □

While this theorem is useless in cases where $[K(r):K]$ and n are relatively prime, such as the problem of denesting $\sqrt{\sqrt[3]{a}+\sqrt[3]{b}}$, it still reduces the cases of denesting certain radicals. For example, $\sqrt[n]{\sqrt[n]{r}-1}$ will not denest for n odd and $r\in\mathbb{Q}$ if $r^k\cdot(r-1)$ is not a perfect nth power in $\mathbb{Q}$ for any integer k. Note that the converse is not true in general: the norm of $\sqrt[3]{9}-1$ in $\mathbb{Q}(\sqrt[3]{3})$ with respect to $\mathbb{Q}$ is 8 and $\sqrt[3]{8}=2\in\mathbb{Q}$, but it can be checked that $\sqrt[3]{\sqrt[3]{9}-1}$ fails to denest.

We now recount a theorem proven in [2] that follows from Theorem 4.1:

Theorem 4.2. *If K is an in-real field with $a,b,r\in K$ and $\sqrt{r}\notin K$ and $\sqrt{a+b\sqrt{r}}$ denests in K, then either $\sqrt{a^2-b^2r}\in K$ or $\sqrt{-r(a^2-b^2r)}\in K$. (Borodin, et. al)*

Proof. Let N be the norm of an element x of $K(\sqrt{r})$ with respect to K. Then it follows that either $N(a+b\sqrt{r})$ or $N((a+b\sqrt{r})/\sqrt{r})$ is a perfect square in K. The former is equal to a^2-b^2r, and the latter is equal to $-1/r(a^2-b^2r)$, which is a perfect square if and only if $-r(a^2-b^2r)$ is a square, as desired. □

In fact, the converse of Theorem 4.2 holds. Suppose $\sqrt{a^2-b^2r}=c\in K$. Then we actually have $\sqrt{a+b\sqrt{r}}=\sqrt{\frac{a+c}{2}}+\sqrt{\frac{a-c}{2}}$. If $\sqrt{-r(a^2-b^2r)}=c\in K$, then we have $\sqrt{a+b\sqrt{r}}=\frac{1}{\sqrt[4]{r}}\left(\sqrt{\frac{br+c}{2}}+\sqrt{\frac{br-c}{2}}\right)$.

Next, we discuss the denesting of $\sqrt{|\sqrt[3]{r}+1|}$ and recount a theorem proven in [3].

Theorem 4.3. *For $r\in\mathbb{Q}$, $\sqrt{|\sqrt[3]{r}+1|}$ denests if and only if $t^4r+4t^3r+8t-4=0$ has a rational solution t. (Sury)*

Proof. If the radical denests, then note that $|\sqrt[3]{r}+1|=c\cdot\sqrt[3]{r^k}\cdot(1+x\sqrt[3]{r}+y\sqrt[3]{r^2})^2$ for some integer k and $c,x,y\in\mathbb{Q}$. But we can assume $k=0$ by the discussion following Theorem 3.2. Then $|\sqrt[3]{r}+1|=c\cdot(1+x\sqrt[3]{r}+y\sqrt[3]{r^2})^2$. Expanding, we have $|\sqrt[3]{r}+1|=c\cdot[(1+2xyr)+\sqrt[3]{r}(y^2r+2x)+\sqrt[3]{r^2}(x^2+2y)]$. It follows that $x^2+2y=0$ and $1+2xyr=y^2r+2x$. Substituting $y=\frac{-x^2}{2}$, we have $1-x^3r=\frac{x^4r}{4}+2x$, or $x^4r+4x^3r+8x-4=0$, which must have a rational solution.

□

Once again, solving the polynomial is simplified by the fact that the solutions need to be rational. Note that the general case of denesting $\sqrt{\sqrt[3]{a}+\sqrt[3]{b}}$ is also solved by writing it as $\sqrt[6]{b}\cdot\left(\sqrt{1+\sqrt[3]{b/a}}\right)$ and denesting $\sqrt{1+\sqrt[3]{b/a}}$.

Next, we give an algorithm that describes how to denest $\sqrt[n]{\sqrt{r} \pm 1}$ for a given rational r. We first take care of the case when r is odd:

Theorem 4.4. *Let $r = r_1/r_2 \in \mathbb{Q}$ where $\gcd(r_1, r_2) = 1$. If $\sqrt{r} \pm 1 = a(1 + x\sqrt{r})^n$ with $a, x \in \mathbb{Q}$, and $x = x_1/x_2$ with $\gcd(x_1, x_2) = 1$, then $x_1 \mid r_2^{\lfloor n/2 \rfloor}$ and $x_2 \mid r_1^{\lfloor n/2 \rfloor}$.*

Proof. Since $\sqrt{r} \pm 1 = a(1 + x\sqrt{r})^n$, it follows that $1 + x^2 r\binom{n}{2} + x^4 r^2 \binom{n}{4} + \ldots = \pm\left(x\binom{n}{1} + x^3 r\binom{n}{3} + \ldots\right)$. Multiplying the polynomial equation by $r_2^{\lfloor n/2 \rfloor}$, we get an integer polynomial equation that x satisfies with constant term $r_2^{\lfloor n/2 \rfloor}$ and lead term $r_1^{\lfloor n/2 \rfloor} x^n$. Thus by the rational root theorem, we are done. □

Now, if $\sqrt[n]{\sqrt{r} \pm 1}$ denests when r is odd, then $\sqrt{r} \pm 1 = c \cdot \sqrt{r^k} \cdot (1 + x\sqrt{r})^n$. But since $\gcd(n, 2) = 1$, we can assume $k = 0$. Thus we can denest $\sqrt[n]{\sqrt{r} \pm 1}$ as follows:

- Make a list of all rationals $s = s_1/s_2$ where $s_1 \mid r_2^{\lfloor n/2 \rfloor}$ and $s_2 \mid r_1^{\lfloor n/2 \rfloor}$.
- For each rational s in the list, compute $(1 + s\sqrt{r})^n$. If the value is of the form $a \pm a\sqrt{r}$, then $(1 + s\sqrt{r})^n = a(1 \pm \sqrt{r})$, and so $\sqrt[n]{1 \pm \sqrt{r}}$ denests as $\frac{1+s\sqrt{r}}{\sqrt[n]{a}}$.
- If no such s exists, then $\sqrt[n]{\sqrt{r} \pm 1}$ has no denesting.

In the general case of denesting $\sqrt[n]{|\sqrt{r} \pm 1|}$, we can take n' to be the largest odd divisor of n with $n = n' \cdot e$ where e is a power of two. Then, given $\sqrt[n']{|\sqrt{r} \pm 1|}$ denests as $\sqrt[n]{a}(1 + x\sqrt{r})$, we need to denest $\sqrt[e]{|1 + x\sqrt{r}|} = \sqrt[e]{|1 \pm \sqrt{rx^2}|}$. But we can denest this using Theorem 4.2 repeatedly.

5 Extensions to Other Fields

We extend the previous results to other fields. Note the only requirement of K in Theorem 3.2 is that it is a real extension of $\mathbb{Q}$. While it is easiest to denest over $\mathbb{Q}$ because of the rational root theorem, in theory a denesting can be done over any in-real field K.

One such field we can extend the results of Theorem 3.2. is the field of depth d radicals. As such, we define the set $\mathbb{Q}_{(d)}$ to be the set of all depth-d radicals over $\mathbb{Q}$. Note that $\mathbb{Q}_{(0)} = \mathbb{Q}$. Section 4, therefore, deals with denesting roots of radicals in $\mathbb{Q}_{(1)}$.

We prove the following:

Theorem 5.1. $\mathbb{Q}_{(d)}$ *is a field.*

Proof. The only difficulty is that multiplicative inverses exist; note that all other properties are satisfied. Take $r \in \mathbb{Q}_{(d)}$. Consider the inclusion $\mathbb{Q}(r) \subset \mathbb{Q}_{(d)}$. Now, since $1/r \in \mathbb{Q}(r)$, we have $1/r \in \mathbb{Q}_{(d)}$. All other requirements for a field are met by the definition of depth. $\square$

Now, taking $K = \mathbb{Q}_{(d)}$ in Theorem 3.2 shows how to denest in general. The difficulty is that the general method for denesting in Section 4 is more difficult since the Rational Root Theorem cannot be applied.

Other fields we can extend the results of the previous sections to are transcendental extensions of $\mathbb{Q}$. Consider the field $\mathbb{Q}(X)$. While $\mathbb{Q}(X)$ is not in-real, it is isomorphic to $\mathbb{Q}(t)$ where t is a real, transcendental number. Since t is transcendental, any radical relationship involving t must be true replacing t with a variable X. In fact, in the same way, we can extend the results to any field $\mathbb{Q}(X_1, X_2, \ldots, X_n)$, by replacing the X_i with suitable real, independent transcendental numbers. An example of a radical expression in $\mathbb{Q}(X)$ is the following: $\sqrt{2X + 2\sqrt{X^2 - 1}} = \sqrt{X - 1} + \sqrt{X + 1}$. Note that Theorem 3.1 holds, as $\sqrt{X - 1} + \sqrt{X + 1} = \sqrt{X - 1}\left(1 + \frac{\sqrt{X^2-1}}{X-1}\right)$ which satisfies the form $b \cdot \alpha$ with $b \in \sqrt{\mathbb{Q}(X)}$ and $\alpha \in \mathbb{Q}(X, \sqrt{X^2 - 1})$.

6 Sums of Nested Radicals

In this section, we explore sums of nested radicals.

We start with a theorem:

Theorem 6.1. *Let* $r_1, r_2, \ldots, r_m \in K$ *be distinct such that* $\sqrt[n_i]{r_i}$ *has degree* n_i *over* K *for all* i. *Moreover, suppose that* $\sqrt[n_1]{r_1} + \sqrt[n_2]{r_2} + \ldots + \sqrt[n_m]{r_m} = s \in K$. *Then* $s = 0$. *(Here, we can take* $\sqrt[n_i]{r_i}$ *to be possibly negative, but real).*

Proof. We prove the result by induction on m. First, suppose $m = 2$. Then $\sqrt[n_1]{r_1} + \sqrt[n_2]{r_2} = s \in K$. It follows that $\sqrt[n_1]{r_1} = s - \sqrt[n_2]{r_2} \in K(\sqrt[n_2]{r_2})$. By Theorem 2.11, it follows that $\sqrt[n_1]{r_1} = \alpha \cdot \sqrt[n_2]{r_2^e}$ for some $\alpha \in K$ and e an integer. Take $e \pmod{n_2}$. Note that $\sqrt[n_2]{r_2} + \alpha \cdot \sqrt[n_2]{r_2^e} = s$. Either $s = 0$, or $\sqrt[n_2]{r_2}$ is the root of $f(X) = X + \alpha \cdot X^e - s \in K[X]$. But in the latter case, it follows that $[K(\sqrt[n_2]{r_2}) : K] < n_2$, contradiction! Thus the result holds for $m = 2$.

Now we use strong induction. Suppose the result holds for 2 through $m-1$ variables. We prove it for m variables. First, take the subset of $\{1, 2, \ldots, m-1\}$ such that $\sqrt[n_i]{r_i} \notin K(\sqrt[n_m]{r_m})$; WLOG this subset is $\{1, 2, \ldots, j\}$ (note that this subset is possibly empty). Then $\sqrt[n_1]{r_1} + \ldots + \sqrt[n_j]{r_j} = s - \sqrt[n_{j+1}]{r_{j+1}} - \ldots - \sqrt[n_m]{r_m} \in K(\sqrt[n_m]{r_m})$.

- If $j = 1$, then $\sqrt[n_1]{r_1} \in K(\sqrt[n_m]{r_m})$, contradiction.
- If $j = 0$, then $\sqrt[n_i]{r_i} \in K(\sqrt[n_m]{r_m})$ for all $i < m$. By Theorem 2.11, it follows that $\sqrt[n_i]{r_i} = \alpha_i \cdot \sqrt[n_m]{r_m^{e_i}}$ for α_i, e_i. Reduce $e_i \pmod{n_m}$ and note that $\alpha_1 \sqrt[n_m]{r_m^{e_1}} + \cdots + \alpha_{m-1} \sqrt[n_m]{r_m^{e_{m-1}}} + \sqrt[n_m]{r_m} = s$. Either $s = 0$, or $\sqrt[n_m]{r_m}$ is a root of the polynomial $f(X) = \alpha_1 X^{e_1} + \ldots + \alpha_{m-1} X^{e_{m-1}} + X - s$. But the latter case gives a degree contradiction, so $s = 0$.
- If $j > 1$, then take $K' = K(\sqrt[n_m]{r_m})$ and $s' = s - \sqrt[n_{j+1}]{r_{j+1}} - \ldots - \sqrt[n_m]{r_m}$. Then $\sqrt[n_1]{r_1} + \ldots + \sqrt[n_j]{r_j} = s' \in K'$. If necessary, replace $\sqrt[n_i]{r_i}$ with $\sqrt[n_i']{r_i'}$ such that $[K'(\sqrt[n_i]{r_i}) : K] = n_i'$. By the inductive hypothesis, it follows $s' = 0$, so $\sqrt[n_{j+1}]{r_{j+1}} + \ldots + \sqrt[n_m]{r_m} = s$. Now, recall that $\sqrt[n_i]{r_i} \in K'$ for $i > j$. Thus $\sqrt[n_i]{r_i} = \alpha_i \cdot \sqrt[n_m]{r_m^{e_i}}$ for $\alpha_i \in K$ and e_i integers. Then it follows that either $s = 0$ or $\sqrt[n_m]{r_m}$ is a root of $f(X) = \alpha_{j+1} X^{e_{j+1}} + \ldots + \alpha_{m-1} X^{e_{m-1}} + X - s$. The latter case gives a degree contradiction, and thus $s = 0$ as desired.

This completes the induction, and thus we are done.

□

In particular, this proves that:

Theorem 6.2. *Let $b_1, b_2, \ldots, b_m$ be depth d radicals such that $\sqrt[n_i]{b_i}$ fails to denest as a depth d radical for $i = 1, \ldots, m$. If $\sqrt[n_1]{b_1} + \sqrt[n_2]{b_2} + \ldots + \sqrt[n_m]{b_m}$ denests as a depth d radical (or* *lower depth), then* $\sqrt[n_1]{b_1} + \sqrt[n_2]{b_2} + \ldots + \sqrt[n_m]{b_m} = 0$.

Proof. Take $K = \mathbb{Q}_{(d)}$ in Theorem 6.1. If necessary, replace $\sqrt[n_i]{b_i}$ with $\sqrt[n_i']{b_i'}$ such that $n_i' < n_i$ and $b_i' \in \mathbb{Q}_{(d)}$, guaranteed by Theorem 2.6. □

The consequence of Theorem 6.2 is that denesting a general radical expression reduces to denesting individual radicals or showing that the expression is actually 0. As an example, note that

$$\sqrt{1+\sqrt{3}} + \sqrt{3+3\sqrt{3}} - \sqrt{10+6\sqrt{3}} = 0$$

and that none of $\sqrt{1+\sqrt{3}}, \sqrt{3+3\sqrt{3}}, \sqrt{10+6\sqrt{3}}$ denest on their own. As another example,

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

However, $\sqrt[3]{\sqrt{5}+2}$ actually denests as $\frac{1}{2}(1+\sqrt{5})$.

7 Conclusion and Future Work

The paper derives a general result for when nested radicals of depth 2 denest in in-real fields, proven as a culmination of the theorems in Sections 2 and 3. This is extended to radicals of general depth over $\mathbb{Q}$ and also transcendental fields like $\mathbb{Q}(t)$. Additionally, an algorithm that makes a radical extension of $\mathbb{Q}$ simple is also given. Specific cases of denesting radicals are examined, including those that denest $\sqrt[n]{|\sqrt{r}+1|}$ and those that determine when a radical cannot be denested using norms over fields. Finally, we show that a sum of radicals that do not denest on their own either does not denest or equals 0.

The main difficulty encountered was that of computation. Denesting a general radical involves an extraordinary amount of computation - for example, figuring out if $\sqrt[3]{\sqrt[3]{2}-1}$ denests involves finding the appropriate degree 9 polynomial. For radicals with higher degrees, the computations involved become much greater. While an algorithm was given that can denest a radical in general, the algorithm is ineffective. One direction of research may be finding a way to optimize the algorithm, for example with the Rational Root Theorem.

References

[1] Bruce C. Berndt, Heng Huat Chan, and Liang-Cheng Zhang. Radicals and units in ramanujan's work. *National University of Singapore*, 1998.

[2] Allan Borodin, Ronald Fagin, John E. Hopcrofts, and Martin Tompa. Decreasing the nesting depth of expressions involving square roots. *J. Symbolic Computation*, 1:169–188, 1985.

[3] B. Sury. Ramanujan's route to roots of roots. *Talk in IIT Madras*, 2007.

[4] Richard Zippel. Simplification of expressions involving radicals. *J. Symbolic Computation*, 1:189–210, 1985.