Radical Denesting

Kaan Dokmeci
Mentor: Yongyi Chen
MIT PRIMES Conference

May 20, 2017

INTRODUCTION TO DENESTING

The goal of this project is to find ways to efficiently denest given radicals.

Introduction to Denesting

The goal of this project is to find ways to efficiently denest given radicals.
Ramanujan's radicals:

- $\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \frac{1}{3}\left(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}\right)$
- $\sqrt{\sqrt[5]{\frac{1}{5}}+\sqrt[5]{\frac{4}{5}}} = \sqrt[5]{\frac{16}{125}}+\sqrt[5]{\frac{8}{125}}+\sqrt[5]{\frac{2}{125}}-\sqrt[5]{\frac{1}{125}}$
- $\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}}$

Introduction to Denesting

The goal of this project is to find ways to efficiently denest given radicals.
Ramanujan's radicals:

- $\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \frac{1}{3}\left(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}\right)$
- $\sqrt{\sqrt[5]{\frac{1}{5}}+\sqrt[5]{\frac{4}{5}}} = \sqrt[5]{\frac{16}{125}}+\sqrt[5]{\frac{8}{125}}+\sqrt[5]{\frac{2}{125}}-\sqrt[5]{\frac{1}{125}}$
- $\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}}$

We can also denest radical expressions of rational functions

Introduction to Denesting

The goal of this project is to find ways to efficiently denest given radicals.
Ramanujan's radicals:

- $\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \frac{1}{3}\left(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}\right)$
- $\sqrt{\sqrt[5]{\frac{1}{5}}+\sqrt[5]{\frac{4}{5}}} = \sqrt[5]{\frac{16}{125}}+\sqrt[5]{\frac{8}{125}}+\sqrt[5]{\frac{2}{125}}-\sqrt[5]{\frac{1}{125}}$
- $\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}}$

We can also denest radical expressions of rational functions $\sqrt{2t+2\sqrt{t^2-1}} = \sqrt{t-1}+\sqrt{t+1}$.

Introduction to Denesting

The goal of this project is to find ways to efficiently denest given radicals.
Ramanujan's radicals:

- $\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \frac{1}{3}\left(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}\right)$
- $\sqrt{\sqrt[5]{\frac{1}{5}}+\sqrt[5]{\frac{4}{5}}} = \sqrt[5]{\frac{16}{125}}+\sqrt[5]{\frac{8}{125}}+\sqrt[5]{\frac{2}{125}}-\sqrt[5]{\frac{1}{125}}$
- $\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{\frac{5}{3}}-\sqrt[3]{\frac{2}{3}}$

We can also denest radical expressions of rational functions $\sqrt{2t+2\sqrt{t^2-1}} = \sqrt{t-1}+\sqrt{t+1}$.
It is easy to verify that the equations are true, but it is not immediately clear how Ramanujan would have gotten to the RHS solely from the LHS.

FIELDS

In a field, one can add, subtract, multiply, and divide, as in the rationals or the reals.

FIELDS

In a field, one can add, subtract, multiply, and divide, as in the rationals or the reals.

- Additive and multiplicative inverses exist, except for a multiplicative inverse of 0

FIELDS

In a field, one can add, subtract, multiply, and divide, as in the rationals or the reals.

- Additive and multiplicative inverses exist, except for a multiplicative inverse of 0
- Additive and multiplicative identities are 0 and 1, respectively.

Fields

In a field, one can add, subtract, multiply, and divide, as in the rationals or the reals.

- Additive and multiplicative inverses exist, except for a multiplicative inverse of 0
- Additive and multiplicative identities are 0 and 1, respectively.
- Addition and multiplication are associative and commutative.

Fields

In a field, one can add, subtract, multiply, and divide, as in the rationals or the reals.

- Additive and multiplicative inverses exist, except for a multiplicative inverse of 0
- Additive and multiplicative identities are 0 and 1, respectively.
- Addition and multiplication are associative and commutative.
- Multiplication is distributive over addition

Fields

In a field, one can add, subtract, multiply, and divide, as in the rationals or the reals.

- Additive and multiplicative inverses exist, except for a multiplicative inverse of 0
- Additive and multiplicative identities are 0 and 1, respectively.
- Addition and multiplication are associative and commutative.
- Multiplication is distributive over addition

Some examples of fields are $\mathbb{F}_p$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Q}(t)$, and $\mathbb{Q}(\sqrt{2})$.

Field Extensions

In a field K, we can define a polynomial in K to be a polynomial
$f(t) = \sum_{i=0}^{d} k_i t^i$.

Field Extensions

In a field K, we can define a polynomial in K to be a polynomial

$$f(t) = \sum_{i=0}^{d} k_i t^i.$$

If α is the root of some polynomial in K, then we can define the extension $K(\alpha)$.

Field Extensions

In a field K, we can define a polynomial in K to be a polynomial $f(t) = \sum_{i=0}^{d} k_i t^i$.

If α is the root of some polynomial in K, then we can define the extension $K(\alpha)$.

Let d be the degree of the minimal polynomial of α: namely, the polynomial f such that $f(\alpha) = 0$ and f has smallest degree.

Field Extensions

In a field K, we can define a polynomial in K to be a polynomial $f(t) = \sum_{i=0}^{d} k_i t^i$.

If α is the root of some polynomial in K, then we can define the extension $K(\alpha)$.

Let d be the degree of the minimal polynomial of α: namely, the polynomial f such that $f(\alpha) = 0$ and f has smallest degree.

Then $1, \alpha, ..., \alpha^{d-1}$ form the basis of $K(\alpha)$ over K.

Field Extensions

In a field K, we can define a polynomial in K to be a polynomial $f(t) = \sum_{i=0}^{d} k_i t^i$.

If α is the root of some polynomial in K, then we can define the extension $K(\alpha)$.

Let d be the degree of the minimal polynomial of α: namely, the polynomial f such that $f(\alpha) = 0$ and f has smallest degree.

Then $1, \alpha, ..., \alpha^{d-1}$ form the basis of $K(\alpha)$ over K.

For example, $\mathbb{Q}(i)$ is the field containing all numbers of form $a + bi$ with $a, b \in \mathbb{Q}$.

Field Extensions

In a field K, we can define a polynomial in K to be a polynomial $f(t) = \sum_{i=0}^{d} k_i t^i$.

If α is the root of some polynomial in K, then we can define the extension $K(\alpha)$.

Let d be the degree of the minimal polynomial of α: namely, the polynomial f such that $f(\alpha) = 0$ and f has smallest degree.

Then $1, \alpha, ..., \alpha^{d-1}$ form the basis of $K(\alpha)$ over K.

For example, $\mathbb{Q}(i)$ is the field containing all numbers of form $a + bi$ with $a, b \in \mathbb{Q}$.

Some fields, like $\mathbb{Q}(t)$ or $\mathbb{Q}(\pi)$ will have an infinite basis.

Depth of a Radical

Informally, we can define the depth of a radical expression to be the number of layers of radicals needed to express it.

Depth of a Radical

Informally, we can define the depth of a radical expression to be the number of layers of radicals needed to express it.
For example, the depth of $\sqrt{\sqrt[3]{2}-1}$ is two.

DEPTH OF A RADICAL

Informally, we can define the depth of a radical expression to be the number of layers of radicals needed to express it.
For example, the depth of $\sqrt{\sqrt[3]{2}-1}$ is two.
The goal of radical denesting is to decrease the depth of a radical.

THEOREM 1

We'll define a real-embeddable field to be a field K to be an extension of $\mathbb{Q}$ that is embeddable in $\mathbb{R}$.

THEOREM 1

We'll define a real-embeddable field to be a field K to be an extension of $\mathbb{Q}$ that is embeddable in $\mathbb{R}$.
This encompasses fields like $\mathbb{Q}, \mathbb{Q}(\sqrt{2})$, and also transcendental extensions like $\mathbb{Q}(t)$.

Theorem 1

We'll define a real-embeddable field to be a field K to be an extension of $\mathbb{Q}$ that is embeddable in $\mathbb{R}$.
This encompasses fields like $\mathbb{Q}, \mathbb{Q}(\sqrt{2})$, and also transcendental extensions like $\mathbb{Q}(t)$.
We have the following:

Theorem 1

We'll define a real-embeddable field to be a field K to be an extension of $\mathbb{Q}$ that is embeddable in $\mathbb{R}$.
This encompasses fields like $\mathbb{Q}, \mathbb{Q}(\sqrt{2})$, and also transcendental extensions like $\mathbb{Q}(t)$.
We have the following:

Theorem

Let p and q be primes. Let $r \in K$ be a radical expression and K a real-embeddable field such that $\sqrt[p]{r} \in K(\sqrt[q]{d})$ 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

If $p \neq q$, then one can use degrees of extensions to get a contradiction.

Proof

If $p \neq q$, then one can use degrees of extensions to get a contradiction.
Otherwise, we can write
$\sqrt[p]{r} = s_0 + s_1\sqrt[p]{d} + \cdots + s_{p-1}\sqrt[p]{d^{p-1}} = f(\sqrt[p]{d})$ where $s_i \in K$.

Proof

If $p \neq q$, then one can use degrees of extensions to get a contradiction.
Otherwise, we can write
$\sqrt[p]{r} = s_0 + s_1\sqrt[p]{d} + \cdots + s_{p-1}\sqrt[p]{d^{p-1}} = f(\sqrt[p]{d})$ where $s_i \in K$.
Taking both sides to the pth power, $r = f(\sqrt[p]{d})^p$. Because $\sqrt[p]{d} \notin K$, only the terms with degree p are nonzero.

Proof

If $p \neq q$, then one can use degrees of extensions to get a contradiction.
Otherwise, we can write
$\sqrt[p]{r} = s_0 + s_1\sqrt[p]{d} + \cdots + s_{p-1}\sqrt[p]{d^{p-1}} = f(\sqrt[p]{d})$ where $s_i \in K$.
Taking both sides to the pth power, $r = f(\sqrt[p]{d})^p$. Because $\sqrt[p]{d} \notin K$, only the terms with degree p are nonzero.
We can then use the roots of unity filter to show that $r = f(\sqrt[p]{d}\zeta_p)^p$.

Proof

If $p \neq q$, then one can use degrees of extensions to get a contradiction.
Otherwise, we can write
$\sqrt[p]{r} = s_0 + s_1\sqrt[p]{d} + \cdots + s_{p-1}\sqrt[p]{d^{p-1}} = f(\sqrt[p]{d})$ where $s_i \in K$.
Taking both sides to the pth power, $r = f(\sqrt[p]{d})^p$. Because $\sqrt[p]{d} \notin K$, only the terms with degree p are nonzero.
We can then use the roots of unity filter to show that $r = f(\sqrt[p]{d}\zeta_p)^p$.
Taking the pth root, we know that $\sqrt[p]{r} \cdot \zeta_p^k = f(\sqrt[p]{d}\zeta_p)$. We can replace ζ_p with any power of p and then sum the equations to get $\sqrt[p]{r} \cdot t = s_m \cdot \sqrt[p]{d^m}$ where t is a sum of pth roots of unity.

Proof

If $p \neq q$, then one can use degrees of extensions to get a contradiction.
Otherwise, we can write
$\sqrt[p]{r} = s_0 + s_1\sqrt[p]{d} + \cdots + s_{p-1}\sqrt[p]{d^{p-1}} = f(\sqrt[p]{d})$ where $s_i \in K$.
Taking both sides to the pth power, $r = f(\sqrt[p]{d})^p$. Because $\sqrt[p]{d} \notin K$, only the terms with degree p are nonzero.
We can then use the roots of unity filter to show that $r = f(\sqrt[p]{d}\zeta_p)^p$.
Taking the pth root, we know that $\sqrt[p]{r} \cdot \zeta_p^k = f(\sqrt[p]{d}\zeta_p)$. We can replace ζ_p with any power of p and then sum the equations to get $\sqrt[p]{r} \cdot t = s_m \cdot \sqrt[p]{d^m}$ where t is a sum of pth roots of unity.
After more degree manipulations, this gets us $\sqrt[p]{r} = \sqrt[p]{d^m} \cdot \alpha$ with $\alpha \in K$.

THEOREM 2

We can use Theorem 1 to prove the following

Theorem 2

We can use Theorem 1 to prove the following

Theorem

Let K be a real-embeddable field such that $r \in K$. 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 $\prod n_i$ is minimal. Then $n_1 = \ldots = n_k = p$ and $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{a_1^{e_1} \cdots a_k^{e_k}}$ for integers e_i and $\alpha \in K$.

Theorem 2

We can use Theorem 1 to prove the following

Theorem

Let K be a real-embeddable field such that $r \in K$. 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 $\prod n_i$ is minimal. Then $n_1 = \ldots = n_k = p$ and $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{a_1^{e_1} \cdots a_k^{e_k}}$ for integers e_i and $\alpha \in K$.

If some n_i has a prime divisor other than q, we could then replace $\sqrt[n_i]{a_i}$ with $\sqrt[n_i/q]{a_i}$, so the n_i's are powers of p.

Theorem 2

We can use Theorem 1 to prove the following

Theorem

Let K be a real-embeddable field such that $r \in K$. 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 $\prod n_i$ is minimal. Then $n_1 = \ldots = n_k = p$ and $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{a_1^{e_1} \cdots a_k^{e_k}}$ for integers e_i and $\alpha \in K$.

If some n_i has a prime divisor other than q, we could then replace $\sqrt[n_i]{a_i}$ with $\sqrt[n_i/q]{a_i}$, so the n_i's are powers of p.
If $n_k = p$, we can induct on k; if $n_k \geq p^2$, one can show that a contradiction arises.

Theorem 2

We can use Theorem 1 to prove the following

Theorem

Let K be a real-embeddable field such that $r \in K$. 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 $\prod n_i$ is minimal. Then $n_1 = \ldots = n_k = p$ and $\sqrt[p]{r} = \alpha \cdot \sqrt[p]{a_1^{e_1} \cdots a_k^{e_k}}$ for integers e_i and $\alpha \in K$.

If some n_i has a prime divisor other than q, we could then replace $\sqrt[n_i]{a_i}$ with $\sqrt[n_i/q]{a_i}$, so the n_i's are powers of p.
If $n_k = p$, we can induct on k; if $n_k \geq p^2$, one can show that a contradiction arises.
The theorem is was proven for $p = 2$ in a paper by Borodin, et al.

COROLLARY

As a result of Theorem 2, we have the following corollary:

Corollary

As a result of Theorem 2, we have the following corollary:

Theorem

Let r be a depth one radical in a real-embeddable field K. Then if $\sqrt[n]{r}$ denests as a depth one radical in K, it denests in the form $\sqrt[m]{b} \cdot \alpha$ where $b \in K$ and $\alpha \in K(r)$.

Corollary

As a result of Theorem 2, we have the following corollary:

Theorem

Let r be a depth one radical in a real-embeddable field K. Then if $\sqrt[n]{r}$ denests as a depth one radical in K, it denests in the form $\sqrt[m]{b} \cdot \alpha$ where $b \in K$ and $\alpha \in K(r)$.

For example, we have

$$\sqrt[6]{7\sqrt[3]{20} - 19} = \sqrt[3]{\frac{5}{3}} - \sqrt[3]{\frac{2}{3}} = \sqrt[3]{\frac{2}{3}} \cdot \left(\frac{1}{2}\sqrt[3]{20} - 1 \right)$$

where $r = 7\sqrt[3]{20} - 19$ and $K = \mathbb{Q}$.

Corollary

As a result of Theorem 2, we have the following corollary:

Theorem

Let r be a depth one radical in a real-embeddable field K. Then if $\sqrt[n]{r}$ denests as a depth one radical in K, it denests in the form $\sqrt[m]{b} \cdot \alpha$ where $b \in K$ and $\alpha \in K(r)$.

For example, we have

$$\sqrt[6]{7\sqrt[3]{20} - 19} = \sqrt[3]{\frac{5}{3}} - \sqrt[3]{\frac{2}{3}} = \sqrt[3]{\frac{2}{3}} \cdot \left(\frac{1}{2}\sqrt[3]{20} - 1\right)$$

where $r = 7\sqrt[3]{20} - 19$ and $K = \mathbb{Q}$.
Indeed, every example tested satisfies the corollary.

Denesting with Diophantines

Using the corollary, we can come up with ways to see if radicals generally denest.

Denesting with Diophantines

Using the corollary, we can come up with ways to see if radicals generally denest.
For example, if $\sqrt[3]{\sqrt[3]{2}-1}$ denests, then we know it is of form $\sqrt[3]{\sqrt[3]{2}-1} = \alpha \cdot (x + y\sqrt[3]{2} + z\sqrt[3]{4})$ where α is some root of a radical number and x, y, z rational.

Denesting with Diophantines

Using the corollary, we can come up with ways to see if radicals generally denest.
For example, if $\sqrt[3]{\sqrt[3]{2}-1}$ denests, then we know it is of form $\sqrt[3]{\sqrt[3]{2}-1} = \alpha \cdot (x + y\sqrt[3]{2} + z\sqrt[3]{4})$ where α is some root of a radical number and x, y, z rational.
We can WLOG $x = 1$ and then cube both sides of the equation.
We can then "equate" coefficients of $1, \sqrt[3]{2}, \sqrt[3]{4}$.

Denesting with Diophantines

Using the corollary, we can come up with ways to see if radicals generally denest.

For example, if $\sqrt[3]{\sqrt[3]{2}-1}$ denests, then we know it is of form $\sqrt[3]{\sqrt[3]{2}-1} = \alpha \cdot (x + y\sqrt[3]{2} + z\sqrt[3]{4})$ where α is some root of a radical number and x, y, z rational.

We can WLOG $x = 1$ and then cube both sides of the equation.

We can then "equate" coefficients of $1, \sqrt[3]{2}, \sqrt[3]{4}$.

When we solve the system, we can eliminate α and get $y = -1$ and $z = 1$. Plugging back in, $\alpha = \frac{1}{\sqrt[3]{9}}$.

Denesting with Diophantines

Using the corollary, we can come up with ways to see if radicals generally denest.

For example, if $\sqrt[3]{\sqrt[3]{2}-1}$ denests, then we know it is of form $\sqrt[3]{\sqrt[3]{2}-1} = \alpha \cdot (x + y\sqrt[3]{2} + z\sqrt[3]{4})$ where α is some root of a radical number and x, y, z rational.

We can WLOG $x = 1$ and then cube both sides of the equation.

We can then "equate" coefficients of $1, \sqrt[3]{2}, \sqrt[3]{4}$.

When we solve the system, we can eliminate α and get $y = -1$ and $z = 1$. Plugging back in, $\alpha = \frac{1}{\sqrt[3]{9}}$.

Thus, we denested $\sqrt[3]{\sqrt[3]{2}-1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}$.

Future Research

While the theorems shown do not show how to denest radicals in general, it shows that all radicals follow a rule if they denest. This lets us create rules to denest radicals without potentially missing cases.

Future Research

While the theorems shown do not show how to denest radicals in general, it shows that all radicals follow a rule if they denest. This lets us create rules to denest radicals without potentially missing cases.

There is an algorithm discussed in the paper by Borodin, et al that will denest any square root in a field.

Future Research

While the theorems shown do not show how to denest radicals in general, it shows that all radicals follow a rule if they denest. This lets us create rules to denest radicals without potentially missing cases.

There is an algorithm discussed in the paper by Borodin, et al that will denest any square root in a field.

The goal of future research is to come up with conditions for denesting in specific cases using Diophantines. Additionally, an algorithm that could come up with these conditions is being researched.

Acknowledgements

The author would like to acknowledge his mentor, Yongyi Chen of MIT, for helping out with this project and giving advice to advance the author's research. He would also like to acknowledge the head mentor Stefan Wehmeier for suggesting the project and for giving access to download the MATLAB software. He would like to acknowledge Tanya Khovanova and Slava Gerovitch for general advice and for helping run MIT-PRIMES USA.

References

Borodin, Allan, Ronald Fagin, John E. Hopcroft, and Martin Tompa. "Decreasing the Nesting Depth of Expressions Involving Square Roots." Journal of Symbolic Computation 1.2 (1985): 169-88. Web.

Zippel, Richard. "Simplification of Expressions Involving Radicals." Journal of Symbolic Computation 1.2 (1985): 189-210. Web.