Theorems and Algorithms Associated with Solving the General Quintic

Matthew Moore

August 7, 2005

Abstract

This paper addresses two published works: D.S. Dummit's 1991 paper, *Solving Solvable Quintics* and Jerry Shurman's *Geometry of the Quintic*. Dummit's paper introduces two theorems. The first theorem gives a criteria for the solvability of the quintic by radicals. The second theorem gives additional criteria to determine the Galois group of a quintic which is solvable by radicals. Shurman's book introduces two different ways to solve a quintic: a geometric method utilizing the icosahedron and a transcendental iterative algorithm. This paper details the associated definitions, theorems, and algorithms involved in the implementation of the two theorems and the transcendental iterative algorithm in the *Python* programming language.

1 Definitions

Definition: Irreducible: A polynomial $f(x)$ is *irreducible* over a field F ($\mathbb{Q}$ in this paper) if it cannot be expressed as the product of two or more polynomials with coefficients in F, each of lower degree than $f(x)$.

Definition: Splitting Field: The *splitting field* of a polynomial, $f(x) \in \mathbb{Q}[x]$, is a field extension $K[x]$ such that $f(x)$ can be written as the product of linear factors in $K[x]$ and cannot be written as the product of linear factors over any subfields of $K[x]$. In other words, the *splitting field* of $f(x)$ is the lowest order field such that $f(x)$ splits.

Definition: Galois Group: Let K be the field extension of $\mathbb{Q}$. The *Galois Group* of K is the group of automorphisms of K such that $\mathbb{Q}$ is fixed. In this paper, the *Galois Groups* associated with the splitting field of various

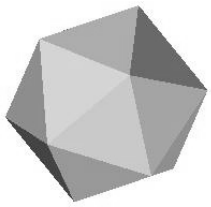
quintics shall be considered as a permutation group on the roots of various quintics.

Definition: Solvable by Radicals A polynomial $f(x)$ is *solvable by radicals* if its splitting field is constructible by extending $\mathbb{Q}$ with roots of specific elements in $\mathbb{Q}$.

Definition: Discriminant: Let $\{x_1, ..., x_5\}$ be the roots of a quintic polynomial. The *discriminant*, D, of this polynomial is then defined to be:

$$D = \prod_{i=1}^{5} \prod_{j=i+1}^{5} (x_i - x_j)^2 \text{ and } \sqrt{D} = \prod_{i=1}^{5} \prod_{j=i+1}^{5} (x_i - x_j)$$

Definition: Icosahedron: The *icosahedron* is one of the platonic solids. It has 20 faces, 30 edges, and 12 verticies.



Each vertex hosts five faces, and each face contains three verticies. Each face is a equilateral triangle.

Definition: $\widehat{C}$: Also known as the *complex sphere* or the *Riemann sphere*, it is the complex plane with a point at infinity:

$$\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

From a topological standpoint, this "extended plane" may be viewed as a sphere.

Definition: Γ-invariant: Let Γ represent an automorphism group of the complex sphere. A function f is Γ-*invariant* if

$$f \circ \gamma = f \qquad \forall \gamma \in \Gamma$$

2 Implementation of D.S. Dummit's Theorems

2.1 D.S. Dummit's Theorems

Theorem 1 *The irreducible quintic* $f(x) = x^5+px^3+qx^2+rx+s$ *is solvable by radicals if and only if the resolvent sextic,* $f_{20}(x)$*, as in D.S. Dummit's* Solving Solvable Quintics*, has exactly one rational root.*

Theorem 2 *If the irreducible quintic* $f(x) = x^5 + px^3 + qx^2 + rx + s$ *is solvable by radicals and* l_1*,* l_2*,* l_3*,* l_4 *as defined in D.S. Dummit's* Solving Solvable Quintics*, then the Galois group of f(x) is:*

- **(a)** *the Frobenius group of order 20 if and only if the discriminant of* $f(x)$ *is not a square.*
- **(b)** *the dihedral group of order 10 if and only if the discriminant of* $f(x)$ *is a square and* $l_i \notin \mathbb{Q}$ *for* $i \in \mathbb{N}$ *and* $1 \leq i \leq 4$*.*
- **(c)** *the cyclic group of order 5 if and only if the discriminant of* $f(x)$ *is a square and* $l_i \in \mathbb{Q}$ *for* $i \in \mathbb{N}$ *and* $1 \leq i \leq 4$*.*

2.2 Methods and Algorithms

2.2.1 Root Finding: Halley's Irrational Formula

We shall make use of the third order Taylor approximation of the function in question, $f(x)$:

$$f(x) \approx f(x_n) + f^{'}(x_n)(x - x_n) + \frac{f^{''}(x_n)(x - x_n)^2}{2}$$

Letting $f(x_{n+1}) = 0$ and solving for x_{n+1}, we get:

$$\begin{aligned} f(x) &\approx f(x_n) + f^{'}(x_n)(x_{n+1} - x_n) + \frac{f^{''}(x_n)(x_{n+1} - x_n)^2}{2} \\ \Rightarrow\ x_{n+1} &= x_n + \frac{-f^{'}(x_n) \pm \sqrt{[f^{'}(x_n)]^2 - 2f(x_n)f^{''}(x_n)}}{f^{''}(x_n)} \\ \Rightarrow\ x_{n+1} &= x_n - \frac{1 - \sqrt{1 - \frac{2f(x_n)f^{''}(x_n)}{[f^{'}(x_n)]^2}}}{\frac{f^{''}(x_n)}{f^{'}(x_n)}} \end{aligned}$$

This provides us with an iterative method akin to Newton's method. The obvious advantage, however, is that this method allows the the detection of imaginary number solutions and has cubic convergence.

Using this method, zeros of $f(x)$ are isolated by first using a logarithmic progressive step size to find zeros in the upper half of the complex plane (conjugates are added as they are found, so searching the lower half is unnecessary). If this fails to isolate all zeros, Halley's method is then run at midpoints between each of the zeros to try to isolate zeros missed due to too large of a step size. Finally, if all of the zeros are still not isolated, logarithmically increasing neighborhoods of each root are searched to attempt to isolate roots which are close together.

2.2.2 Fraction Recognition

The algorithm employed for fraction recognition first computes a continued fraction approximation for the decimal to be converted. This is done as follows:

> Let x be the decimal to be converted to a continued fraction and let c_i represent the i^{th} entry in the continued fraction representation of x.
>
> [Step 1] `Let` $i = 0$`.`
>
> [Step 2] $c_i =$`integer part of` x`.`
>
> [Step 3] `If decimal part of` x `is zero, go to Step 5.`
>
> [Step 4] $i = i + 1$`.  Go to Step 2.`
>
> [Step 5] `Return the continued fraction array.`

This algorithm, however, has several flaws when implemented on a computer. Since on a computer all number are inherently rational, the algorithm must be told not to find so precise a fraction that it represents an irrational number exactly on the computer. This is done by limiting the number of iterations which the algorithm is allowed to perform. Furthermore, since errors are introduced when inverting the fraction, it will often be the case that a zero decimal part is never reached for a rational number and thus the algorithm will never naturally terminate. To correct this, a zero tolerance is defined so that a number can be a certain distance away from zero but still be considered zero.

Since the continued fraction expansion is finite, we are able to simplify it into a single fraction. This fraction is the fraction approximation of the given decimal.

2.2.3 Irreducibility Test

The Eisenstein irreducibility criterion is used to perform a test of irreducibility:

Let $f(x) = a_n x^n + an_{n-1}x^{n-1} ... + a_1 x + a_0$.

If there exists a prime number p such that: p divides $a_{n-1},\ ..., a_1,\ a_0$, p does not divide a_n, and p^2 does not divide a_0, then $f(x)$ is irreducible.

Note that the converse is not true. Due to this, the irreducibility test is not always conclusive. This creates the need for an additional check which will be performed if Eisenstein's test is inconclusive. Since we require all coefficients to be integers for Eisenstein's test, we simply exploit this by means of a brute force factoring approach which checks for linear and quadratic factors.

2.2.4 Test for Solvabiliy by Radicals

Theorem 1 gives a clear criteria for the solvability of a quintic. Thus, we first generate the resolvent sextic $f_{20}(x)$. Next, the roots of the resolvent sextic, $f_{20}(x)$, are approximated to a high degree of accuracy (approx 10^{14}) and are converted to fractions. Next, the decimal expansions of the fractions are compared with the original roots. If the two are sufficiently close (their difference is within the zero tolerance from the fraction algorithm), the approximated roots are replaced with the fractions. To verify that these fractional solutions are valid, synthetic division is performed on the sextic.

Once the rational roots have been verified, they are counted. If there is exactly one, then $f(x)$ is considered solvable. If there is more than one, a serious error has occurred and the method terminates with an error message. If there are no rational roots, then $f(x)$ is considered unsolvable.

2.2.5 Determination of the Galois Group

Theorem 2 gives the criteria for the determination of the Galois group. The first task is to determine if the discriminant, D, is a square. D is a square if and only if $\sqrt{D}$ does not have an imaginary component and is rational. Thus, D is not a square if and only if $\sqrt{D}$ has an imaginary component or is not rational. If D is found to not be a square, then, by Theorem 2 (a), the Galois group is the *Frobenius group of order 20.*

Once the discriminant is determined to be a square, the l_i for $i \in \mathbf{N}$ and $1 \leq i \leq 4$ as defined in D.S. Dummit's *Solving Solvable Quintics* are examined. if all of the l_i are not rational, then, by Theorem 2 (b), the Galois group is the *dihedral group of order 10.* Otherwise, if the l_i are rational, then, by Theorem 2 (c), the Galois group is the *cyclic group of order 5.*

2.3 Examples

An analysis of polynomials of the form $f(x) = x^5 + px^3 + qx^2 + rx + s$ with $\{p,\ q,\ r,\ s\} \in \mathbb{Z}$ and bounded by -10 and 10 was performed. This set of polynomials consists of 10000 distinct elements and thus cannot possibly be included in this section. However, the results of this analysis as well as the the program accompany this report on a separate disk.

2.3.1 Example 1

We will compute the Galois group for $f(x) = x^3 - 2$:

$$f(x) = x^3 - 2 = 0 \ \Rightarrow\ x = \{x_1,\ x_2,\ x_3\} = \{\sqrt[3]{2},\ \sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2\}$$

$\{x_1, x_2, x_3\}$ uniquely identify the automorphisms which make up the Galois group:

$$\begin{array}{lrcl} \sigma_1\text{:} & \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\,\zeta_3 \\ & \zeta_3 & \mapsto & \zeta_3 \\ \sigma_2\text{:} & \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ & \zeta_3 & \mapsto & \zeta_3^2 \\ \sigma_1^2\text{:} & \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\,\zeta_3^2 \\ & \zeta_3 & \mapsto & \zeta_3 \end{array} \qquad \begin{array}{lrcl} \sigma_1\sigma_2\text{:} & \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\,\zeta_3 \\ & \zeta_3 & \mapsto & \zeta_3^s \\ \sigma_1^2\sigma_2\text{:} & \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\,\zeta_3^2 \\ & \zeta_3 & \mapsto & \zeta_3^2 \end{array}$$

Writing this in permutation notation, we have:

$$\begin{array}{llll} \sigma_1 = (1\ 2\ 3) & \sigma_1\sigma_2 = (1\ 2) & \sigma_2 = (2\ 3) \\ \sigma_1^2 = (1\ 3\ 2) & \sigma_1^2\sigma_2 = (1\ 3) & \sigma_1^3 = \sigma_2^2 = 1 \end{array}$$

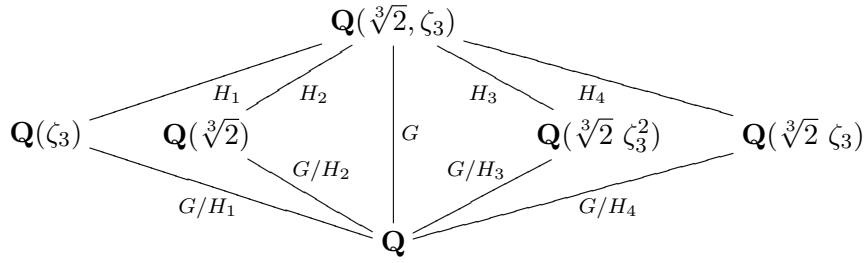
Thus,

$$G = \{\sigma_1,\ \sigma_2,\ \sigma_1^2,\ \sigma_1\sigma_2,\ \sigma_1^2\sigma_2,\ 1\}$$

Which has subgroups:

$$H_1 = \{\sigma_1,\ \sigma_1^2,\ 1\},\ H_2 = \{\sigma_2,\ 1\},\ H_3 = \{\sigma_1\sigma_2,\ 1\},\ \textit{and}\ H_4 = \{\sigma_1^2\sigma_2,\ 1\}$$

The corresponding field diagram is:

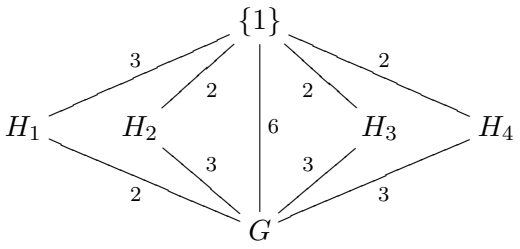


Where the G/H_i are defined to be:

$$G/H_1 = \{[\sigma_1],\ [\sigma_2]\}, \qquad G/H_2 = \{[\sigma_1],\ [\sigma_2],\ [\sigma_1\sigma_2]\},$$
$$G/H_3 = \{[\sigma_1],\ [\sigma_1^2],\ [\sigma_1\sigma_2]\}, \quad G/H_4 = \{[\sigma_1],\ [\sigma_2],\ [\sigma_1^2\sigma_2]\}$$

$$Where\ [x] = \{y \in G :\ xy^{-1} \in H_i\}$$

The group diagram corresponding to the above field diagram is:



2.3.2 Example 2

The polynomial $f(x) = x^5 + 15x + 12$ shall be analyzed by the program accompanying this paper. Output:

```
Output of analysis started on 06/30/05 00:26:25:

By Eisenstein's criterion, f is irreducible.
```

```
f20(x)=x^6+120*x^5+9000*x^4+540000*x^3+20250000*x^2+
                                                    324000000*x
Roots of f20:
x={(0+0i), (-42.7711093851+0i),
(-39.2517239503+21.1901552426i),
(-39.2517239503-21.1901552426i),
(0.637278642854+61.6989884597i),
(0.637278642854-61.6989884597i)}

f is solvable by radicals.

Roots of f:
x={(-0.78066943209325823+0j),
(-1.1688562730842484-1.4510383696004412j),
(-1.1688562730842484+1.4510383696004412j),
(1.5591909891308775+1.4129796738683194j),
(1.5591909891308775-1.4129796738683194j}.

The Galois group of f is the Frobenius group of order 20.

Elapsed time: 13.2786859782 seconds.
Analysis ended on 06/30/05 00:26:42.
-------------------------------------------------
```

2.3.3 Example 3

The polynomial $f(x) = x^5 - 5x + 12$ shall be analyized by the program accompanying this paper. Output:

```
Output of analysis started on 06/30/05 00:27:41:

Eisenstein's criterion was not met, f may or may not be
irreducible.

f20(x)=x^6-40*x^5+1000*x^4-20000*x^3+250000*x^2-66400000*x+
                                                    976000000
Roots of f20:
x={(364291730/24276309+0i), (-22.6582909569-23.1569341153i),
(-22.6582909569+23.1569341153i),
(15.1552613571+36.3239233098i),
(15.1552613571-36.3239233098i), (40+0i)}.

f is solvable by radicals.

Roots of f:
```

```
x={(1.2728972239224992+0.7197986814838615j),
(1.2728972239224992-0.7197986814838615j),
(-0.35185424082737199+1.7095610433703288j),
(-0.35185424082737199-1.7095610433703288j),
(-1.8420859661902544+0j}.

The Galois group of f is the dihedral group of order 10.

Elapsed time: 24.466843691 seconds.
Analysis ended on 06/30/05 00:28:09.
------------------------------------------------
```

3 Geometric and Transcendental Methods

3.1 The Icosahedral Method

Consider the icosahedron. Note that the symmetry group contains 120 elements and may be considered as an automorphism group. As there exists a geometric figure (the icosahedron) which is invariant under this automorphism group, there also exists a function on $\widehat{C}$ which is invariant under the same automorphism group. If Γ is the automorphism group of the icosahedron, this invariant function is called Γ-invariant. The following is the icosahedral invariant function:

$$f_I = \frac{(-z^{20} + 228z^{15} - 494z^{10} - 228z^5 - 1)^3}{1728z^5(z^{10} + 11z^5 - 1)^5}.$$

Calculating the inverse of this function involves solving a quintic, which is done through the use of a Brioschi resolvent - a parametrized quintic polynomial. The Brioschi quintic arises when one examines the five tetrahedral subgroups of the icosahedral group. Introducing the parameter

$$w' = \frac{1}{1728(1 - f_I)},$$

the calculated icosahedral Brioschi resolvent of f_I then reduces to the tetrahedral resolvent. When expressed in terms of w', this is:

$$R_{\tilde{s}} = t^5 - 10w't^3 + 45w't - w'^2.$$

Which is exactly the Brioschi quintic. At this point, a general algorithm exists to invert the icosahedral invariant. Since the Brioschi quintic is the

resolvent of an invariant of a subgroup of the icosahedral group, the inverse of the icosahedral invariant may be used to solve a general Brioschi quintic.

An additional chapter in Shurman's *Geometry of the Quintic* outlines the complicated task of how to reduce a general quintic to its Brioschi form and thus solves the general quintic.

3.2 The Trascendental Iterative Method

The following algorithm is given:

> Consider the Brioschi quintic: $b = t^5 - 10w't^3 + 45w't - w'^2$. To find its roots:
>
> [Step 1] `Let` $\hat{w} = 1 - 1728w'$ `and compute` $h_{\hat{w}}, k_{\hat{w}} \in \mathbb{C}[t]$.
>
> [Step 2] `Iterate` $F_{\hat{w}} = t - 12\frac{h_{\hat{w}}}{h'_{\hat{w}}}$ `an even number of times on an initial guess until it converges to a value,` t_0. `Set` $t_1 = F_{\hat{w}}(t_0)$.
>
> [Step 3] `Set` $\mu_0 = \frac{k_{\hat{w}}(t_0)}{h_{\hat{w}}(t_0)}$ `and` $\mu_1 = \frac{k_{\hat{w}}(t_1)}{h_{\hat{w}}(t_1)}$
>
> [Step 4] `Then,`
> $s_0 = \frac{9-i\sqrt{15}}{90}\mu_0 + \frac{9+i\sqrt{15}}{90}\mu_1$ `and` $s_1 = \frac{9+i\sqrt{15}}{90}\mu_0 + \frac{9-i\sqrt{15}}{90}\mu_1$ `are Brioschi roots. Finding the remaining roots reduces to solving a cubic equation, which may be done by radicals.`

[Step 1] Renormalizing w' to $\hat{w}$ serves to convert back to a non-rotated icosahedron, which is necessary for the computation of $h_{\hat{w}}$ and $k_{\hat{w}}$. H is the icosahedral vertex form, and $h = H_*$ dehomogenizes (z_1, z_2) to t. Solving a large system of linear equations then results in $h_{\hat{w}}$, which is in terms of $\hat{w}$ instead of t or (z_1, z_2).

[Step 2] The iterative function $F_{\hat{w}}$ does not actually convergent for any point when it is iterated in single steps. However, this divergence produces orbits of 2-cycles. Thus, when $F_{\hat{w}}$ is iterated an even number of times it becomes convergent. Iterating it an additional time to produce t_1 results in finding the convergent number of the other orbit.

[Step 3] The polynomial $\mu_{\hat{w}}(t)$ is the dual of the tetrahedral invariant, which is expressed in terms of resolvents which in turn are expressed in terms of the roots of the quintic. This then simplifies to $\frac{k_{\hat{w}}}{h_{\hat{w}}}$.

[Step 4] Considering $\mu_{\hat{w}}(\phi_z^{-1}(\pm a))$, where ϕ_z^{-1} takes the output field of the iterative function to the face-centers of the icosahedron, gives a system of two linear equations in terms of the two roots of the Brioschi quintic. Utilizing linear algebra, the roots of the Brioschi quintic are isolated and are expressed in terms of μ_0 and μ_1.

3.3 Examples

The following examples were computed by an implementation of the above algorithm. Note the similarity in runtime for each of the examples. This indicates that the algorithm given quickly converges regardless of the polynomial being analyzed.

3.3.1 Example 1

For this example, we consider the case when $w' = 10$. Thus, we solve the quintic $f(t) = b = t^5 - 100t^3 + 4500t - 100$.

```
f(t)=b_w=t^5-10*w'*t^3+45*w'^2*t-w'^2, w' in C
w'=10
The roots of f(t) are:
{(7.6456402297692847-2.916272772389958j),
(7.6456402297692847+2.916272772389958j),
(0.022222466094177329+4.207887051250108e-016j),
(-7.6567514628163726-2.9286955325577666j),
(-7.6567514628163726+2.9286955325577657j)}

Analysis took 0.0120532078798 seconds.
```

3.3.2 Example 2

For this example, we consider the case when $w' = 0.001$. Thus, we solve the quintic $f(t) = b = t^5 - 0.01t^3 + 0.000045t - 0.000001$.

```
f(t)=b_w=t^5-10*w'*t^3+45*w'^2*t-w'^2, w' in C
w'=0.001
The roots of f(t) are:
{(0.068141422690924103-0.019350319721344517j),
(0.068141422690924103+0.019350319721344517j),
(0.02577446013872255-2.1557239449248707e-018j),
(-0.081028652760285369-0.034155857168180315j),
(-0.081028652760285369+0.034155857168180315j)}

Analysis took 0.0122610555252 seconds.
```

3.3.3 Example 3

For this example, we consider the case when $w' = 100000$. Thus, we solve the quintic $f(t)b = t^5 - 1000000t^3 + 450000000000t - 10000000000$.

```
f(t)=b_w=t^5-10*w'*t^3+45*w'^2*t-w'^2, w' in C
w'=100000
The roots of f(t) are:
{(765.1154782705828-292.24401798812437j),
(765.1154782705828+292.24401798812437j),
(0.022222222249169477+0j),
(-765.12658938170739-292.25644058801674j),
(-765.12658938170739+292.25644058801674j)}

Analysis took 0.0123353666458 seconds.
```

4 References

I would like to thank Ben Levitt for many useful conversations and for directing my research.

1. Dummit, D.S.. "Solving Solvable Quintics". Mathematics of Computation 57.195 (1991): pp. 387-401.
2. McMullen, Curt. "Families of Rational Maps and Iterative Root-Finding Algorithms". Annals of Mathematics, The 2nd Ser. Vol. 125 No. 3 (May 1987): pp. 467-493
3. Shurman, Jerry. Geometry of the Quintic. Wiley-Interscience: 1997.
4. Weisstein, Eric. Mathworld. Wolfram Research, Inc. $\langle http://mathworld.wolfram.com \rangle$.