ALGORITHMS FOR COMPUTING QUARTIC GALOIS GROUPS OVER FIELDS OF CHARACTERISTIC 0

Chad Awtrey¹ ⁵, James Beuerle², Michael Keenan³
¹,²,³Department of Mathematics and Statistics
Elon University
Campus Box 2320, Elon, NC 27244, USA

Abstract: Let \( f(x) \) be an irreducible degree four polynomial defined over a field \( F \) and let \( K = F(\alpha) \) where \( \alpha \) is a root of \( f \) in some fixed algebraic closure \( \overline{F} \) of \( F \). Several methods appear in the literature for computing the Galois group \( G \) of \( f \), most of which rely on forming and factoring resolvent polynomials; i.e., polynomials defining subfields of the splitting field of \( f \). This paper surveys those methods that generalize to arbitrary base fields of characteristic 0. Further, we describe a non-resolvent method that determines if \( K \) has a quadratic subfield by counting the number of roots of \( f \) that are contained in \( K \), and we also describe how to construct explicitly a polynomial defining a quadratic subfield. We end with a comparison of run times for the various algorithms in the case \( F \) is the rational numbers.

AMS Subject Classification: 12Y05, 20B35, 12F10
Key Words: quartic Galois groups, resolvent polynomials, automorphism groups, efficiency

1. Introduction

Galois theory shows it is possible to associate a group structure to a polynomial’s roots. This group, called the polynomial’s Galois group, is a collection of
permutations of the roots that encode arithmetic information concerning the polynomial. For example, the polynomial is solvable by radicals if and only if its Galois group is solvable (see for example [4, p.628]). An important problem in computational algebra therefore is to determine the Galois group of a polynomial \( f(x) \) of degree \( n \) defined over a field \( F \).

For this paper, we focus on quartic polynomials, surveying methods appearing in the literature that apply to arbitrary base fields of characteristic 0. These methods [1, 3, 4, 7] rely on factoring resolvent polynomials [5, 8, 9], which are polynomials that define subfields of the splitting field of \( f \). We also present a non-resolvent method that relies on factoring the quartic polynomial over the extension field it defines. One advantage of this method is that it allows us to determine when the quartic polynomial’s extension field has a quadratic subfield, and it gives us an explicit calculation of a polynomial that defines such a quadratic subfield. As a corollary, we can determine when any irreducible quartic polynomial can be transformed into a biquadratic (i.e., even quartic) polynomial defining the same extension, and hence having the same Galois group.

The remainder of the paper is organized as follows. Section 2 provides a brief overview of the basic notation and terminology related to the Fundamental Theorem of Galois Theory as they relate to our context. In this section, we also show the relationship between the automorphism group of a polynomial’s extension field and its Galois group, paving the way for our non-resolvent approach to computing quartic Galois groups. In Section 3 we give an introduction to resolvent polynomials, including a discussion of the most widely-used resolvent; namely, the discriminant. Section 4 details all of the algorithms under consideration that are based on the resolvent method. For each algorithm, we describe its implementation and prove its correctness. Section 5 discusses our non-resolvent algorithm for computing quartic Galois groups. Additionally, we show every biquadratic irreducible quartic polynomial has a Galois group that is a subgroup of \( D_4 \) (the dihedral group of order 8). Conversely, if a quartic polynomial’s Galois group is a subgroup of \( D_4 \), we describe how to construct explicitly a biquadratic polynomial that defines the same extension (and hence has the same Galois group). Our final section includes an analysis of run times for each algorithm considered in this paper in the case the ground field is the rational numbers. Our findings indicate that the most efficient algorithm is the modification of the traditional cubic resolvent method, as outlined in [7].
2. Overview of Galois Theory

In this section, we give a very brief overview of Galois theory in our context. More details can be found in any standard text on abstract algebra (such as [4]).

Let $F$ be a field and let $\overline{F}$ be a fixed algebraic closure. Let $f(x) \in F[x]$ be an irreducible polynomial of degree $n$ with roots $\alpha = \alpha_1, \ldots, \alpha_n \in \overline{F}$. Let $K$ be the stem field of $f$; that is, $K = F(\alpha)$.

Then it is straightforward to verify that $K$ is a vector space over $F$ with the set $\{1, \alpha, \ldots, \alpha^{-1}\}$ serving as a basis. Since the dimension of $K$ as an $F$-vector space is $n$, we say $K/F$ is an extension field of degree $n$ and we write $[K : F] = n$.

We are interested primarily in automorphisms of $K/F$, which are field isomorphisms from $K$ to itself that restrict to the identity function on $F$.

**Definition 2.1.** An automorphism of $K/F$ is a mapping $\sigma : K \to K$ such that,

1. $\sigma$ is bijective,
2. $\sigma(x + y) = \sigma(x) + \sigma(y)$ for all $x, y \in K$,
3. $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in K$,
4. $\sigma(a) = a$ for all $a \in F$.

The collection of all automorphisms of $K/F$ is denoted $\text{Aut}(K/F)$.

The automorphisms of $K/F$ form a group under function composition. Since automorphisms are field isomorphisms and since a basis for $K/F$ consists of powers of the one root $\alpha$, it follows that each automorphism is completely determined by where it sends $\alpha$. Furthermore, since automorphisms act like the identity function on $F$, we have $0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$ for each $\sigma \in \text{Aut}(K/F)$. This shows that automorphisms send $\alpha$ to some other root of $f$ that lies in $K$.

Therefore, elements in $\text{Aut}(K/F)$ are in a bijective correspondence with the roots of $f$ that are contained in $K$, and each automorphism permutes these roots. In the case where $K$ contains all $n$ roots of $f$, $\text{Aut}(K/F)$ is called the Galois group of $f$. Otherwise, the Galois group of $f$ is the automorphism group of the splitting field of $f$; that is, the smallest subfield of $\overline{F}$ that contains $F$ and all $n$ roots of $f$. 
The Fundamental Theorem

The next result is the Fundamental Theorem of Galois Theory, which gives a bijection between the subfields of $K/F$ and the subgroups of $\text{Aut}(K/F)$ when $K/F$ is a Galois extension (see [4, p. 574]).

**Theorem 2.2** (Fundamental Theorem of Galois Theory). Let $L$ be the splitting field of an irreducible polynomial $f$ of degree $n$ defined over $F$, and let $G$ be the Galois group of $f$ (i.e., the automorphism group of $L/F$). There is a bijective correspondence between the subfields of $L/F$ and the subgroups of $G$. Specifically, if $K$ is a subfield of $L/F$, then $K$ corresponds to the set of all $\sigma \in G$ such that $\sigma(a) = a$ for all $a \in K$. Similarly, if $H$ is a subgroup of $G$, then $H$ corresponds to the set of all $a \in L$ such that $\sigma(a) = a$ for all $\sigma \in H$.

The Galois correspondence has the following properties.

1. If $H_1$ and $H_2$ are subgroups of $G$ that correspond to subfields $K_1$ and $K_2$ respectively, then $H_1 \leq H_2$ if and only if $K_2 \subseteq K_1$.

2. If $K$ defines a subfield of $L$ of degree $d$ over $F$, then $K$ corresponds to a subgroup $H \leq G$ of index $d$.

3. Let $K$ be a subfield of $L/F$ defined by the polynomial $g$ and let $H \leq G$ be the subgroup corresponding to $K$. The splitting field of $g$ corresponds to the largest normal subgroup $N$ of $G$ contained inside $H$; i.e., the kernel of the permutation representation of $G$ acting on $G/H$. The Galois group of $g$ is isomorphic to $G/N$.

4. If we label the roots of $f$ as $\alpha_1, \ldots, \alpha_n$, then $G$ can be identified with a transitive subgroup of $S_n$, well-defined up to conjugation.

5. If we label the roots of $f$ as $\alpha_1, \ldots, \alpha_n$, then the stem field of $f$ (generated by $\alpha_1$) corresponds to $G_1$, the point stabilizer of 1 inside $G$.

**Automorphism Groups and Stem Fields**

We now prove several facts about subfields of $L/F$ and subgroups of $\text{Aut}(L/F)$. The first considers conjugate fields of a subfield $K$ of $L/F$. For $\sigma \in \text{Aut}(L/F)$ and a subfield $K$ of $L/F$, the image $\sigma(K)$ of $K$ under $\sigma$ is called a conjugate field of $K$. The next result shows that conjugate fields correspond to conjugate subgroups.
**Proposition 2.3.** Let $L/F$ be a Galois extension with Galois group $G$. Let $H$ be a subgroup of $G$ and let $K$ be the fixed field of $H$. For $\sigma \in G$, the subgroup fixing $\sigma(K)$ is $\sigma H \sigma^{-1}$.

**Proof.** First we show $\sigma H \sigma^{-1}$ fixes $\sigma(K)$. Let $\sigma h \sigma^{-1} \in \sigma H \sigma^{-1}$ and let $\sigma(x) \in \sigma(K)$. Then $\sigma h \sigma^{-1}(\sigma(x)) = \sigma h(x) = \sigma(x)$, as desired.

Next we show every element that fixes $\sigma(K)$ belongs to $\sigma H \sigma^{-1}$. Suppose $\tau \in G$ fixes $\sigma(K)$. Then for all $x \in K$, $\tau(\sigma(x)) = \sigma(x)$. Thus $\sigma^{-1} \tau \sigma(x) = x$. Thus $\sigma^{-1} \tau \sigma$ fixes $K$, which implies $\sigma^{-1} \tau \sigma \in H$. Thus $\tau \in \sigma H \sigma^{-1}$, as desired. \hfill $\square$

**Proposition 2.4.** Let $L/F$ be a Galois extension with Galois group $G$. Let $H$ be a subgroup of $G$ and let $K$ be the fixed field of $H$. Let $\sigma, \tau \in G$. Then $\sigma(x) = \tau(x)$ for all $x \in K$ if and only if $\tau \in \sigma H$.

**Proof.** Let $\sigma, \tau \in G$ and suppose $\sigma(x) = \tau(x)$ for all $x \in K$. Then $x = \sigma^{-1} \tau(x)$ for all $x \in K$. Thus $\sigma^{-1} \tau$ fixes $K$, which is true if and only if $\sigma^{-1} \tau \in H$. This is true if and only if $\tau \in \sigma H$, as desired. \hfill $\square$

Next we describe the relationship between the automorphism group of a subfield and the Galois group of the splitting field.

**Proposition 2.5.** Let $L/F$ be a Galois extension with Galois group $G$. Let $H$ be a subgroup of $G$ and let $K$ be the fixed field of $H$. Then $\text{Aut}(K/F) \simeq N/H$, where $N$ is the normalizer of $H$ in $G$.

**Proof.** First we note that every element in $\text{Aut}(K/F)$ corresponds to some restriction to $K$ of an element $\sigma \in G$ [4, p. 575]. Such an element $\sigma$ will restrict to an automorphism of $K/F$ precisely when $\sigma(K) = K$. By Proposition 2.3, these are restrictions of elements in the normalizer $N$ of $H$ in $G$. By Proposition 2.4, the elements in $N$ that restrict to distinct functions on $K$ correspond to the cosets of $H$ in $N$. Therefore $\text{Aut}(K/F)$ is isomorphic to the quotient group $N/H$, as desired. \hfill $\square$

As a corollary, the next result explicitly determines the connection between the automorphism group of a polynomial’s stem field and the polynomial’s Galois group. This will be the basis for our non-resolvent method for computing quartic Galois groups, as mentioned in Section 5.

**Corollary 2.6.** Let $L$ be the splitting field of the irreducible polynomial $f(x)$ of degree $n$ defined over $F$, and let $G$ be the Galois group of $f$. Let $K/F$ be the stem field of $f$. Let $G_1$ be the point stabilizer of 1 inside $G$, and let
Table 1: The 5 conjugacy classes of transitive subgroups of $S_4$. Generators are for one representative in each conjugacy class.

<table>
<thead>
<tr>
<th>T</th>
<th>Name</th>
<th>Generators</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$C_4$</td>
<td>(1234)</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>$V_4$</td>
<td>(12)(34), (13)(24)</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>$D_4$</td>
<td>(1234), (13)</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>$A_4$</td>
<td>(123), (234)</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>$S_4$</td>
<td>(1234), (12)</td>
<td>24</td>
</tr>
</tbody>
</table>

$N$ be the normalizer of $G_1$ in $G$. Then $\text{Aut}(K/F) \simeq N/G_1$. Furthermore, the number of roots of $f$ that are contained in $K$ is equal to the index $[N : G_1]$.

Proof. Since $K$ is the stem field, $K \simeq F(\alpha_1)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f$ in $\mathbb{F}$. Under the Galois correspondence, the subgroup that corresponds to $K$ consists of those elements that fix $K$; i.e., all $\sigma \in G$ such that $\sigma(\alpha_1) = \alpha_1$. This is precisely the point stabilizer of 1 inside $G$. Therefore $\text{Aut}(K/F) \simeq N/G_1$ by Proposition 2.5. In particular, these two groups have the same order. The final statement of the corollary now follows since the number of automorphisms equals the number of roots of $f$ contained in $K$, and the number of elements in $N/G_1$ is equal to the index $[N : G_1]$.

Notice that by item (4) of Theorem 2.2, we must identify the conjugacy classes of transitive subgroups of $S_4$ in order to determine the group structure of $G$. This information is well known (see [2]). In Table 1, we give information on the 5 conjugacy classes of transitive subgroups of $S_4$, including their transitive number (or T-number, as in [6]), generators of one representative, their size, and a more descriptive name based on their structure. The descriptive names are standard: $C_4$ represents the cyclic group of order $n$, $D_4$ the dihedral group of order 8, $V_4$ the elementary abelian group of order 4, and $A_4$ and $S_4$ the alternating and symmetric groups on 4 letters.

3. Resolvent Polynomials and Splitting Fields

The techniques for computing Galois groups this paper is studying are based on the use of absolute resolvent polynomials [8]. In short, this method works as follows. Let $f(x)$ be an irreducible polynomial (over $F$) of degree $n$. Let $G$ be the Galois group of $f$, and let $H$ be a subgroup of $S_n$. We form a resolvent polynomial $R_H(x)$ whose stem field corresponds to $H$ under the Galois
correspondence. By item (3) of Theorem 2.2, the Galois group of $R_H(x)$ is isomorphic to the image of the permutation representation of $G$ acting on the cosets $S_n/H$. Then as shown in [8], the irreducible factors of $R_H(x)$ therefore correspond to the orbits of this action. In particular, the degrees of the irreducible factors correspond to the orbit lengths.

The most difficult task in the resolvent method is constructing the polynomial $R_H(x)$ that corresponds to a given subgroup $H$ of $S_n$. The following result gives one method for accomplishing such a task. A proof can be found in [8].

**Theorem 3.1.** Let $f(x)$ be an irreducible polynomial of degree $n$ defined over a field $F$, $K$ the splitting field of $f$, and $\alpha_1, \ldots, \alpha_n$ the roots of $f$ in $\overline{F}$. Let $T(x_1, \ldots, x_n)$ be a polynomial with coefficients in $F$, and let $H$ be the stabilizer of $T$ in $S_n$. That is

$$H = \{ \sigma \in S_n : T(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = T(x_1, \ldots, x_n) \}.$$ 

Let $S_n//H$ denote a complete set of coset representatives of $H$ in $S_n$, and define the resolvent polynomial $R_H(x)$ by:

$$R_H(x) = \prod_{\sigma \in S_n//H} (x - T(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})).$$

1. If $R_H(x)$ is squarefree, its Galois group is isomorphic to the image of the permutation representation of $G$ acting on the cosets $S_n/H$.

2. We can ensure $R_H(x)$ is squarefree by taking a suitable Tschirnhaus transformation of $f(x)$ [3, p.324]. This amounts to randomly picking an element in the stem field of $f(x)$ and computing its characteristic polynomial.

3. One choice for $T$ is given by:

$$T(x_1, \ldots, x_n) = \sum_{\sigma \in H} \left( \prod_{i=1}^{n} x_{\sigma(i)}^i \right).$$

Though this is not the only choice.

We now describe how to construct the resolvents used in the following papers: [1, 3, 7]. To illustrate each of these constructions, we will use the following sample polynomials:

<table>
<thead>
<tr>
<th>$t_1$</th>
<th>$x^4 + 5x^2 + 5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t_2$</td>
<td>$x^4 + 1$</td>
</tr>
<tr>
<td>$t_3$</td>
<td>$x^4 + 2$</td>
</tr>
<tr>
<td>$t_4$</td>
<td>$x^4 - 7x^2 - 3x + 1$</td>
</tr>
<tr>
<td>$t_5$</td>
<td>$x^4 - x^3 + 1$</td>
</tr>
</tbody>
</table>
The Discriminant

Perhaps the most well known example of a resolvent polynomial is the discriminant. Recall that the discriminant of a degree \( n \) polynomial \( f(x) \) is given by

\[
\text{disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,
\]

where \( \alpha_i \) are the roots of \( f \). In particular, let

\[
T = \prod_{1 \leq i < j \leq n} (x_i - x_j).
\]

It is well-known that \( T \) is stabilized by \( A_n \) \([4, \text{p.610}]\). Notice that a complete set of coset representatives of \( S_n/A_n \) is \( \{\text{id}, (12)\} \). Also notice that applying the permutation \( (12) \) to the subscripts of \( T \) results in \( -T \). In this case, we can form the resolvent polynomial \( R(x) \) as follows,

\[
R(x) = \prod_{\sigma \in S_n/A_n} (x - \sigma(T)) = x^2 - T^2 = x^2 - \text{disc}(f).
\]

In particular, this resolvent factors if and only if the discriminant is a perfect square in the base field. It is well-known that the discriminant can be computed via the resultant of \( f(x) \) and its derivative; namely,

\[
\text{disc}(f) = (-1)^{n(n-1)} \text{Res}(f, f'),
\]

see \([3, \text{p. 119}]\).

Furthermore, by the theory of elementary symmetric polynomials, it follows that \( \text{disc}(f) \) can be expressed using only the coefficients of \( f \) \([4, \text{p. 611}]\).

For example, in the case of quartic polynomials, we have:

\[
\text{disc}(x^4 + ax^3 + bx^2 + cx + d) = -27a^4d^2 + 2a^3c(9bd - 2c^2)
- a^2(4b^3d - b^2c^2 - 144bd^2 + 6c^2d)
- 2ac(40b^2d - 9bc^2 + 96d^2)
+ 4b(4b^3 - b^2c^2 - 32bd^2 + 36c^2d)
- 27c^4 + 256d^3.
\]

Here are the discriminants of the five sample polynomials \( t_1, \ldots, t_5 \); the final column gives the prime factorization of the discriminant over the rational numbers.
Both the traditional approach to computing quartic Galois groups [4, p. 614] and its refinement [7] rely on factoring a cubic resolvent polynomial. In this case, we let \( T = x_1x_3 + x_2x_4 \). The stabilizer \( H \) of \( T \) in \( S_4 \) is a dihedral group of order 8. The elements of this particular group are,

\[
H = \{(1), (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}.
\]

A complete set of right coset representatives for \( S_4/H \) is given by: \{(1), (12), (14)\}. We can form the cubic resolvent for \( f(x) \) by computing \( R_H \):

\[
R_H(x) = (x - (\alpha_1\alpha_3 + \alpha_2\alpha_4))(x - (\alpha_2\alpha_3 + \alpha_1\alpha_4))(x - (\alpha_4\alpha_3 + \alpha_2\alpha_1)).
\]

We can also express the cubic resolvent in terms of the coefficients of the original quartic. If \( f(x) = x^4 + ax^3 + bx^2 + cx + d \), then the cubic resolvent of \( f \) is:

\[
R_H(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2
\]

Here are the cubic resolvents of the five sample polynomials \( t_1, \ldots, t_5 \); the final column gives the factorization of the cubic resolvent over the rational numbers.

<table>
<thead>
<tr>
<th>Poly</th>
<th>Cubic Res</th>
<th>Factorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>( t_1 )</td>
<td>( x^3 - 5x^2 - 20x + 100 )</td>
<td>( (x^2 - 20)(x - 5) )</td>
</tr>
<tr>
<td>( t_2 )</td>
<td>( x^3 - 4x )</td>
<td>( x(x - 2)(x + 2) )</td>
</tr>
<tr>
<td>( t_3 )</td>
<td>( x^3 - 8x )</td>
<td>( x(x^2 - 8) )</td>
</tr>
<tr>
<td>( t_4 )</td>
<td>( x^3 + 7x^2 - 4x - 37 )</td>
<td>( x^4 + 7x^2 - 4x - 37 )</td>
</tr>
<tr>
<td>( t_5 )</td>
<td>( x^3 - 4x - 1 )</td>
<td>( x^3 - 4x - 1 )</td>
</tr>
</tbody>
</table>

The Degree 6 Resolvent

The method in [3, §6.3] relies on factoring a degree 6 resolvent polynomial. In this case, we let \( T = (x_1 + x_3 - (x_2 + x_4))(x_1 - x_3)(x_2 - x_4) \). The stabilizer \( H \)
of $T$ in $S_4$ is a cyclic group of order 4. The elements of this particular group are,

$$H = \{(1), (1234), (13)(24), (1432)\}.$$ 

A complete set of right coset representatives for $S_4/H$ is given by:

$$\{(1), (12), (13), (14), (23), (34)\}.$$ 

We can form the degree 6 resolvent for $f(x)$ by computing $R_H$:

$$R_H(x) = \prod_{\sigma \in S_4/H} (x - (\alpha_{\sigma(1)} + \alpha_{\sigma(3)} - (\alpha_{\sigma(2)} + \alpha_{\sigma(4)}))(\alpha_{\sigma(1)} - \alpha_{\sigma(3)})(\alpha_{\sigma(2)} - \alpha_{\sigma(4)})).$$

We can also express the degree 6 resolvent in terms of the coefficients of the original quartic. If $f(x) = x^4 + ax^3 + bx^2 + cx + d$, then the degree 6 resolvent of $f$ is:

$$R_H(x) = x^6 + Ax^4 + Bx^2 + C,$$

where:

$$A = -2a^2b^2 + 8b^3 + 6a^3c - 28abc + 36c^2 + 12a^2d - 32bd,$$

$$B = a^4b^4 - 8a^2b^5 + 16b^6 + 6a^5b^2c + 52a^3b^3c - 112ab^4c + 9a^6c^2 - 84a^4bc^2 + 156a^2b^2c^2 + 160b^3c^2 + 124a^3c^3 - 576abc^3 + 432c^4 - 12a^4b^2d + 96a^2b^3d - 192b^4d + 36a^5cd - 336a^3bcd + 768ab^2cd + 240a^2c^2d - 1152bc^2d + 144a^4d^2 - 768a^2bd^2 + 768b^2d^2 + 768ac^2d^2 - 1024d^3,$$

$$C = -a^8b^2c^2 + 12a^6b^3c^2 - 48a^4b^4c^2 + 64a^2b^5c^2 + 4a^9c^3 - 50a^7bc^3 + 192a^5b^2c^3 - 160a^3b^3c^3 - 256ab^4c^3 + 91a^6c^4 - 760a^4bc^4 + 1520a^2b^2c^4 + 256b^3c^4 + 688a^3c^5 - 2880abc^5 + 1728c^6 + 4a^8b^3d - 48a^6b^4d + 192a^4b^5d - 256a^2b^6d - 18a^9bcd + 22a^7b^2cd + 864a^5b^3cd + 768a^3b^4cd + 1024ab^5cd + 6a^8c^2d - 480a^6bc^2d + 3680a^4b^2c^2d - 7168a^2b^3c^2d - 1024b^4c^2d + 96a^5c^3d - 3840a^3bc^3d + 14336a^2bc^4d + 384a^2c^4d - 9216bc^4d + 27a^10d^2 - 360a^8bd^2 + 1712a^6b^2d^2 - 3328a^4b^3d^2 + 2048a^2b^4d^2 + 624a^7cd^2 - 5568a^5bcd^2 + 14336a^3b^2d^2 - 8192ab^3cd^2 + 4800a^4c^2d^2 - 21504a^2b^2c^2d^2 + 8192b^3c^2d^2 + 12288ac^3d^2 - 256a^6d^3 + 2048a^4bd^3 - 4096a^2b^2d^3 - 4096a^3cd^3 + 16384abcd^3 - 16384c^2d^3.$$ (2)

Here are the degree 6 resolvents of the five sample polynomials $t_1, \ldots, t_5$. Note that we need to take a tschirnhaus transformation of $t_1, t_2,$ and $t_3$, since
their degree 6 resolvents are not squarefree. In each case, we give the transformed polynomial, the degree 6 resolvent, and the factorization of the degree 6 polynomial over the rationals. For \( t_4 \) and \( t_5 \), the resolvent is irreducible, so we only give it.

\( t_1 \)

**tschirnhaus:** \( x^4 + 8x^3 + 34x^2 + 32x + 181 \)

**degree 6 res:** \( x^6 - 8388608000x^2 - 214748364800000 \)

**factorization:** \((x - 320)(x + 320)(x^4 + 102400x^2 + 2097152000)\)

\( t_2 \)

**tschirnhaus:** \( x^4 - 12x^3 + 62x^2 - 84x + 34 \)

**degree 6 res:** \( x^6 + 165888x^4 + 6855736320x^2 - 1988235362304 \)

**factorization:** \((x^2 - 288)(x^2 + 82944)(x^2 + 83232)\)

\( t_3 \)

**tschirnhaus:** \( x^4 - 12x^3 + 58x^2 - 124x + 99 \)

**degree 6 res:** \( x^6 + 648x^5 + 173360x^4 + 24478976x^3 + 1921577216x^2 + 79384270848x + 1346049994752 \)

**factorization:** \((x^2 + 280x + 19856)(x^4 + 368x^3 + 50464x^2 + 3042048x + 67790592)\)

\( t_4 \)

**degree 6 res:** \( x^6 + 8x^5 + 8x^4 - 384x^3 - 2176x^2 - 4864x - 6656 \)

\( t_5 \)

**degree 6 res:** \( x^6 + x^4 - 30x^3 - 57x^2 - 15x - 4 \)

The Degree 12 Resolvent

The method in [1] relies on factoring a degree 12 resolvent polynomial. In this case, we let \( T = x_1 + x_2 + (x_1 - x_2)(x_3 - x_4) \). The stabilizer \( H \) of \( T \) in \( S_4 \) is a cyclic group of order 2. The elements of this particular group are,

\[ H = \{(1), (12)(34)\} \]
A complete set of right coset representatives for $S_4/H$ is given by:

\{ (1), (12), (13), (14), (23), (24), (123), (124), (132), (142), (13)(24), (1324) \}.

We can form the degree 12 resolvent for $f(x)$ by computing $R_H$:

$$R_H(x) = \prod_{\sigma \in S_4/H} (x - (\alpha_{\sigma(1)} + \alpha_{\sigma(2)} + (\alpha_{\sigma(1)} - \alpha_{\sigma(2)})(\alpha_{\sigma(3)} - \alpha_{\sigma(4)}))).$$

We can also express the degree 12 resolvent in terms of the coefficients of the original quartic. If $f(x) = x^4 + ax^3 + bx^2 + cx + d$, then the degree 12 resolvent of $f$ is:

$$R_H(x) = \sum_{i=0}^{12} A_i x^i,$$

where

$$A_{12} = 1,$$
$$A_{11} = -6a,$$
$$A_{10} = 15a^2 + 4b - 4b^2 + 12ac - 48d,$$
$$A_9 = -20a^3 - 20ab + 20ab^2 - 60a^2 c + 240ad,$$
$$A_8 = 15a^4 + 40a^2b + 6b^2 - 42a^2b^2 - 4b^3 + 6b^4 + 2ac + 126a^3c + 6abc$$
$$- 36a^2bc + 54c^2 + 54a^2c^2 - 8d - 450a^2d - 240bd + 144b^2d$$
$$- 432acd + 864d^2,$$
$$A_7 = -6a^5 - 40a^3b - 24ab^2 + 48a^3b^2 + 16ab^3 - 24ab^4 - 8a^2c$$
$$- 144a^4c - 24a^2bc + 144a^2b^2c - 216ac^2 - 216a^3c^2 + 32ad$$
$$+ 360a^3d + 960abd - 576ab^2d + 1728a^2cd - 3456ad^2,$$
$$A_6 = a^6 + 20a^4b + 36a^2b^2 - 32a^4b^2 + 4b^3 - 28a^2b^3 + 4b^4$$
$$+ 40a^2b^4 - 4b^5 - 4b^6 + 12a^3c + 96a^5c + 6abc + 46abc + 24ab^2c$$
$$- 240a^3b^2c + 38ab^3c + 36ab^4c - 2c^2 + 346a^2c^2 + 360a^4c^2 + 96bc^2$$
$$- 78a^2bc^2 - 126b^2c^2 - 110a^2b^2c^2 + 8b^3c^2 + 378ac^3 + 116a^3c^3$$
$$- 36abc + 54c^4 - 50a^2d - 42a^4d - 16bd - 1456a^2bd - 288b^2d$$
$$+ 834a^2b^2d + 352b^3d + 8a^2b^3d - 176b^4d - 32acd - 2502a^3cd$$
$$- 888abcd - 36a^3bcd + 1024a^2bcd - 1512e^2d - 128a^2e^2d$$
$$- 288be^2d + 64d^2 + 4248a^2d^2 + 54a^4d^2 + 4800bd^2 - 288a^2bd^2$$
$$- 1472b^2d^2 + 5568acd^2 - 7424d^3,
$A_5 = -4a^5b - 24a^3b^2 + 12a^5b^2 - 12ab^3 + 28a^3b^3 - 12a^4b^4 - 36a^3b^4 + 12ab^5$
+ $12ab^6 - 8a^4c - 36a^6c - 18a^2bc - 54a^4bc + 72a^2b^2c + 216a^4b^2c$
$- 114a^2b^3c - 108a^2b^4c + 6ac^2 - 282a^3c^2 - 324a^5c^2 - 288abc^2$
+ $234a^3bc^2 + 378ab^2c^2 + 330a^3b^2c^2 - 24ab^3c^2 - 1134a^2c^3$
$- 348a^4c^3 + 108a^2bc^3 - 162ac^4 + 38a^3d - 126a^5d + 48abd$
+ $1008a^3bd + 864ab^2d - 486a^3b^2d - 1056ab^3d - 24a^3b^3d + 528ab^4d$
+ $96a^2cd + 1458a^4cd + 2664a^2bcd + 108a^4bcd - 3072a^2b^2cd$
+ $4536ac^2d + 3852a^3c^2d + 864abc^2d - 192ad^2 - 648a^3d^2 - 162a^5d^2$
$- 14400abd^2 + 864a^3bd^2 + 4416ab^2d^2 - 16704a^2cd^2 + 22272ad^3$

$A_4 = 6a^4b^2 - 2a^6b^2 + 12a^2b^3 - 16a^4b^3 + b^4 + 10a^2b^4 + 19a^4b^4 + 4b^5$
$- 16a^2b^5 + 6b^6 - 14a^2b^6 + 4b^7 + b^8 + 2a^5c + 6a^7c + 18a^3bc + 36a^5bc$
$+ 6ab^2c - 72a^3b^2c - 114a^5b^2c - 10ab^3c + 148a^3b^3c - 50ab^4c$
$+ 126a^3b^4c - 46ab^5c - 12ab^6c - 5a^2c^2 + 126a^4c^2 + 171a^6c^2 - 4bc^2$
$+ 302a^2bc^2 - 300a^4bc^2 + 34b^2c^2 - 345a^2b^2c^2 - 393a^4b^2c^2$
$+ 64b^3c^2 + 248a^2b^3c^2 + 10b^4c^2 + 58a^2b^4c^2 - 16b^5c^2 + 42ac^3$
$+ 1342a^3c^3 + 438a^5c^3 - 306abc^3 - 548a^3bc^3 - 180ab^2c^3$
$- 136a^3b^2c^3 + 120ab^3c^3 + 513ac^4 + 1215a^2c^4 + 129a^4c^4 - 540bc^4$
$- 216a^2bc^4 - 108b^2c^4 + 324ac^5 - 14a^4d + 84a^6d - 52a^2bd - 252a^4bd$
$- 8b^2d - 974a^2b^2d - 12a^4b^2d - 96b^3d + 1344a^2b^3d + 60a^4b^3d$
$- 56b^4d - 734a^2b^4d + 144b^5d - 16a^2b^5d + 112b^6d - 8acd - 102a^3cd$
$+ 36a^5cd + 8abcd - 3522a^3bcd - 270a^5bcd + 240ab^2cd + 4044a^3b^2cd$
$- 784ab^3cd + 120a^3b^3cd - 944ab^4cd + 168c^2d - 3846a^2c^2d$
$- 3636a^4c^2d - 2880bc^2d - 3144a^2bc^2d - 216a^4bc^2d + 5040b^2c^2d$
$+ 2280a^2b^2c^2d + 384b^3c^2d - 6480ac^3d - 1416a^3c^3d - 864abc^3d$
$- 1296c^4d + 16d^2 + 120a^2d^2 - 2367a^4d^2 + 405a^6d^2 + 320bd^2$
$+ 14784a^2bd^2 - 2700a^4bd^2 + 5280b^2d^2 + 912a^2b^2d^2 - 108a^4b^2d^2$
$- 8512b^3d^2 + 384a^2b^3d^2 + 1120b^4d^2 - 2976abcd^2 + 14544a^3cd^2$
$+ 324a^5cd^2 + 12576abcd^2 - 864a^3bcd^2 - 8256ab^2cd^2 + 12960c^2d^2$
$+ 9792a^2c^2d^2 + 6912bc^2d^2 + 3968d^3 - 15072a^2d^3 - 1296a^4d^3$
$- 34048bd^3 + 6912a^2bd^3 + 1792b^2d^3 - 33024acd^3 + 33024d^4$. 
\[ A_3 = -4a^3b^3 + 4a^5b^3 - 2ab^4 - 6a^5b^4 - 8ab^5 + 12a^3b^5 - 12ab^6 \\
+ 8a^3b^6 - 8ab^7 - 2ab^8 - 6a^4bc - 10a^6bc - 12a^2b^2c + 24a^4b^2c \\
+ 36a^6b^2c + 20a^2b^3c - 106a^4b^3c + 100a^2b^4c - 72a^4b^4c \\
+ 92a^2b^5c + 24a^2b^6c - 34a^5c^2 - 54a^7c^2 + 8abc^2 - 124a^3bc^2 \\
+ 210a^5bc^2 - 68ab^2c^2 + 60a^3b^2c^2 + 236a^5b^2c^2 - 128ab^3c^2 \\
- 456a^3b^3c^2 - 20ab^4c^2 - 116a^3b^4c^2 + 32ab^5c^2 - 84a^2c^3 \\
- 794a^4c^3 - 296a^6c^3 + 612a^2bc^3 + 916a^4bc^3 + 360a^2b^2c^3 \\
+ 272a^4b^2c^3 - 240a^2b^3c^3 - 1026ac^4 - 2160a^3c^4 - 258a^5c^4 \\
+ 1080abc^4 + 432a^3bc^4 + 216ab^2c^4 - 648a^2c^5 + 2a^5d - 18a^7d \\
+ 24a^3bd - 56a^5bd + 16ab^2d + 508a^3b^2d + 162a^5b^2d + 192ab^3d \\
- 928a^3b^3d - 80a^5b^4d + 112a^3b^4d + 588a^3b^3d - 288ab^5d + 32a^3b^5d \\
- 224ab^5d + 16a^2cd + 44a^4cd - 486a^6cd - 16a^2bcd + 2604a^4bcd \\
+ 360a^6bcd - 480a^2b^2cd - 2968a^4b^2cd + 1468a^2b^3cd - 240a^4b^3cd \\
+ 1888a^4bcd + 336ac^2d + 132a^3c^2d + 852a^5c^2d + 5760abc^2d \\
+ 4848a^3bc^2d + 432a^3b^2c^2d - 10080ab^2c^2d - 4560a^3b^2c^2d \\
- 768ab^3c^2d + 12960a^2c^3d + 2832a^4c^3d + 1728a^2bc^3d + 2592ac^4d \\
- 32ad^2 + 80a^3d^2 + 1782a^5d^2 - 540a^7d^2 - 640abd^2 - 5568a^3bd^2 \\
+ 3960a^5bd^2 - 10560ab^2d^2 - 9184a^3b^2d^2 + 216a^5b^2d^2 \\
+ 17024ab^3d^2 - 768a^3b^3d^2 - 2240ab^4d^2 + 5952a^2cd^2 \\
- 1248a^4cd^2 - 648a^6cd^2 - 25152a^2bcd^2 + 1728a^4bcd^2 \\
+ 16512a^2b^2cd^2 - 2592ac^2d^2 - 19584a^3c^2d^2 - 13824abc^2d^2 \\
- 7936ad^3 + 6976a^3d^3 + 2592a^5d^3 + 68096abd^3 - 13824a^3bd^3 \\
- 3584ab^2d^3 + 66048a^2cd^3 - 66048ad^4, \\
A_2 = a^2b^4 - 2a^4b^4 + a^6b^4 + 4a^2b^5 - 4a^4b^5 + 6a^2b^6 - 2a^4b^6 \\
+ 4a^2b^7 + a^2b^8 + 6a^3b^2c - 6a^7b^2c + 2ab^3c - 14a^3b^3c + 36a^5b^3c \\
+ 8ab^4c - 58a^3b^4c + 18a^5b^4c + 12ab^5c - 50a^3b^5c + 8ab^6c - 12a^3b^6c \\
+ 2ab^7c + a^4c^2 + 6a^6c^2 + 9a^8c^2 - 2a^2bc^2 + 18a^4bc^2 - 72a^6bc^2 - 2b^2c^2 \\
+ 28a^2b^2c^2 + 63a^4b^2c^2 - 69a^6b^2c^2 + 2b^8c^2 - 292a^4b^3c^2 \\
+ 20b^4c^2 - 118a^4b^4c^2 + 66a^4b^4c^2 + 40b^5c^2 - 78a^2b^5c^2 + 30b^6c^2 \\
- 2a^2b^6c^2 + 8b^7c^2 - 2ac^3 + 62a^3c^3 + 198a^5c^3 + 114a^7c^3 - 12abc^3 \]
\[-230a^3bc^3 - 664a^5bc^3 - 24ab^2c^3 + 216a^3b^2c^3 - 192a^5b^2c^3 - 104ab^3c^3 + 492a^3b^3c^3 - 174ab^4c^3 + 20a^3b^4c^3 - 84ab^5c^3 + 54c^4 + 549a^2c^4 + 1363a^4c^4 + 225a^6c^4 + 108bc^4 - 1368a^2bc^4 - 822a^4bc^4 + 108b^2c^4 - 216a^2b^2c^4 - 66a^4b^2c^4 + 108b^6c^4 + 288a^2b^3c^4 + 54b^4c^4 + 756ac^5 + 1242a^3c^5 + 72a^5c^5 + 162abc^5 - 324a^3bc^5 - 324ab^2c^5 - 1458c^6 + 486c^6 - 4a^4bd + 36a^6bd - 10a^2b^2d - 90a^4b^2d - 84a^6b^2d - 160a^2b^3d + 360a^4b^3d + 60a^6b^3d - 32b^4d - 36a^2b^4d - 346a^4b^4d - 128b^5d + 376a^2b^5d - 48a^4b^5d - 192b^6d + 270a^2b^6d - 128b^7d + 8a^2b^7d - 32b^8d - 10a^3cd + 6a^5cd + 252a^7cd - 8abcd - 84a^3bcd - 1098a^5bcd - 270a^7bcd + 256ab^5cd + 120a^3b^2cd + 1596a^5b^2cd + 768ab^3cd - 1816a^3b^3cd + 360ab^5cd + 1088ab^4cd - 2142a^3b^4cd + 936ab^5cd - 84a^3b^5cd + 352ab^6cd + 8c^2d - 204a^2c^2d + 1494a^4c^2d + 576a^6c^2d - 384bc^2d - 5160a^2bc^2d - 4416a^4bc^2d - 648a^6bc^2d - 768b^2c^2d + 7128a^2b^2c^2d + 4356a^4b^2c^2d - 44863c^2d - 648a^2b^3c^2d + 288a^4b^3c^2d - 168b^4c^2d - 1284a^2b^5c^2d - 96b^5c^2d + 1440ac^3d - 4744a^3c^3d - 1386a^5c^3d - 3744abc^3d - 564a^3bc^3d - 324a^5bc^3d - 2160ab^2c^3d + 1704a^3b^2c^3d + 288ab^3c^3d + 3024ac^4d - 11502a^2c^4d - 468a^4c^4d + 16848bc^4d + 1296b^4c^4d - 3888ac^5d + 24a^2d^2 - 664a^4d^2 - 423a^6d^2 + 405a^8d^2 + 192a^2bd^2 - 180a^4bd^2 - 3240a^6bd^2 + 256b^2d^2 + 7584a^2b^2d^2 + 9948a^4b^2d^2 - 324a^6b^2d^2 - 14592a^2b^3d^2 + 1260a^4b^3d^2 - 1280b^4d^2 + 1464a^2b^4d^2 + 54a^4b^4d^2 - 1536b^5d^2 - 96a^2b^5d^2 - 512b^6d^2 + 384acd^2 - 4608a^3cd^2 - 2844a^5cd^2 + 972a^7cd^2 + 1344abcd^2 + 13632a^3bcd^2 - 2430a^5bcd^2 + 14976ab^2cd^2 - 16560a^3b^2cd^2 - 324a^5b^2cd^2 + 12384ab^3cd^2 + 288a^3b^3cd^2 + 4992ab^4cd^2 - 2880c^2d^2 - 4800a^2c^2d^2 + 6210a^4c^2d^2 + 486a^6c^2d^2 + 19584bc^2d^2 + 50688a^2bc^2d^2 - 63072b^2c^2d^2 - 11520a^2b^2c^2d^2 - 5760b^3c^2d^2 + 12960ac^3d^2 + 3744a^3c^3d^2 + 15552abc^3d^2 + 7776a^4d^2 - 512d^3 + 5184a^2d^3 + 7824a^4d^3 - 5346a^6d^3 + 2048bd^3 - 27776a^2bd^3 + 37584a^4bd^3 - 46080b^2d^3 - 71520a^2b^2d^3 + 1296a^4b^2d^3 + 67584b^3d^3 - 5760a^2b^3d^3 + 1024b^4d^3 + 45056acd^3 - 44640a^3cd^3 - 3888a^5cd^3]
$$A_1 = -2a^2b^3c + 4a^4b^3c - 2a^6b^3c - 8a^2b^4c + 8a^4b^4c - 12a^2b^5c$$
$$+ 4a^4b^5c - 8a^2b^6c - 2a^2b^7c - 2a^3b^2c^2 - 4a^5bc^2 + 6a^7bc^2 + 2ab^2c^2$$
$$+ 6a^3b^2c^2 - 30a^5b^2c^2 + 6a^7b^2c^2 + 76a^3b^3c^2 - 68a^5b^3c^2$$
$$- 20ab^4c^2 + 128a^3b^4c^2 - 8a^5b^4c^2 - 40ab^5c^2 + 62a^3b^5c^2 - 30ab^6c^2$$
$$+ 2a^3b^6c^2 - 8ab^7c^2 + 2a^2c^3 - 20a^4c^3 + 10a^6c^3 - 24a^8c^3 + 12a^2bc^3$$
$$- 76a^4bc^3 + 224a^6bc^3 + 24a^2b^2c^3 - 396a^4b^2c^3 + 56a^6b^2c^3$$
$$+ 104a^2b^3c^3 - 372a^4b^3c^3 + 174a^2b^4c^3 - 20a^4b^4c^3 + 84a^2b^5c^3$$
$$- 54ac^4 - 36a^2c^4 - 310a^5c^4 - 96a^7c^4 - 108abc^4 + 828a^3bc^4 + 606a^5bc^4$$
$$- 108ab^2c^4 + 108a^3b^2c^4 + 66a^5b^2c^4 - 108a^3b^3c^4 - 288a^3b^3c^4$$
$$- 54abc^4 - 756a^2c^5 - 918a^4c^5 - 72a^6c^5 - 162a^2bc^5 + 324a^4bc^5$$
$$+ 324a^2b^2c^5 + 1458ac^6 - 486a^3c^6 + 2a^3b^2d - 20a^5b^2d + 18a^7b^2d$$
$$+ 64a^3b^3d - 72a^5b^3d - 24a^7b^3d + 32ab^4d - 20a^3b^4d + 140a^5b^4d + 128ab^5d$$
$$- 232a^3b^5d + 32a^5b^5d + 192ab^6d - 158a^3b^6d + 128ab^7d - 8a^3b^7d + 32ab^8d$$
$$+ 2a^4cd - 12a^6cd - 54a^8cd + 8a^2bcd + 92a^4bcd + 240a^6bcd + 108a^8bcd$$
$$- 256a^2b^2cd + 120a^4b^2cd - 624a^6b^2cd - 768a^2b^3cd + 1032a^4b^3cd$$
$$- 240a^6b^3cd - 108a^2b^4cd + 1198a^4b^4cd - 936a^2b^5cd + 84a^4b^5cd$$
$$- 352a^2b^6cd - 8ac^2d + 36a^3c^2d - 804a^5c^2d - 360a^7c^2d + 384abc^2d$$
$$+ 2280a^3bc^2d + 2136a^5bc^2d + 432a^7bc^2d + 768ab^2c^2d - 2088a^3b^2c^2d$$
$$- 2076a^5b^2c^2d + 448ab^3c^2d + 1032a^3b^3c^2d - 288a^5b^3c^2d + 168ab^4c^2d$$
$$+ 1284a^3b^4c^2d + 96ab^5c^2d - 1440a^2c^3d - 1736a^4c^3d - 30a^6c^3d$$
$$+ 3744a^2bc^3d - 300a^4bc^3d + 32a^6bc^3d + 2160a^2b^2c^3d - 704a^4b^2c^3d$$
$$- 288a^2b^3c^3d + 3024ac^4d + 10206a^3c^4d + 468a^5c^4d - 1684abc^4d$$
$$- 1296a^2c^4d + 3888a^2c^5d - 8a^3d^2 - 6a^5d^2 - 162a^9d^2 + 128a^3bd^2$$
$$+ 564a^5bd^2 + 1404a^7bd^2 - 256ab^2d^2 - 2304a^3b^2d^2 - 4620a^5b^2d^2$$
$$+ 216a^7b^2d^2 + 6080a^3b^3d^2 - 876a^5b^3d^2 + 1280ab^4d^2 - 344a^3b^4d^2$$
$$- 54a^5b^5d^2 + 1536ab^5d^2 + 96a^3b^5d^2 + 512a^6d^2 - 384a^2bcd^2$$
$$+ 1632a^4cd^2 + 684a^6cd^2 - 648a^8cd^2 - 1344a^2bcd^2 - 1056a^4bcd^2$$
\[ A_0 = a^2b^2c^2 - 3a^4b^2c^2 + 3a^6b^2c^2 - a^8b^2c^2 + 8a^2b^3c^2 - 16a^4b^3c^2 + 8a^6b^3c^2 + 22a^2b^4c^2 - 24a^4b^4c^2 + 2a^6b^4c^2 + 28a^2b^5c^2 - 12a^4b^5c^2 + 17a^2b^6c^2 - a^4b^6c^2 + 4a^2b^7c^2 + 4a^5c^3 - 8a^7c^3 + 4a^9c^3 - 2abc^3 - 6a^3bc^3 + 42a^5bc^3 - 34a^7bc^3 - 16ab^2c^3 - 46a^3b^2c^3 + 108a^5b^2c^3 - 14a^7b^2c^3 - 44ab^3c^3 - 114a^3b^3c^3 - 86a^5b^3c^3 - 56ab^4c^3 - 114a^3b^4c^3 + 10a^5b^4c^3 - 34ab^5c^3 - 40a^3b^5c^3 - 8ab^6c^3 + c^4 + 17a^2c^4 - 29a^4c^4 + 3a^6c^4 + 24a^8c^4 + 12bc^4 + 108a^2bc^4 - 92a^4bc^4 - 148a^6bc^4 + 54b^2c^4 + 250a^2b^2c^4 + 129a^4b^2c^4 - 33a^6b^2c^4 + 116b^3c^4 + 236a^2b^3c^4 + 130a^4b^3c^4 + 129b^4c^4 + 69a^2b^4c^4 + a^4b^4c^4 + 72b^5c^4 - 8ab^5c^4 + 16b^6c^4 - 54ac^5 + 116a^3c^5 + 122a^5c^5 + 36a^7c^5 - 414abc^5 - 204a^3bc^5 - 138a^5bc^5 - 810ab^2c^5 - 144a^3b^2c^5 - 8a^5b^2c^5 - 594ab^3c^5 + 68a^3b^3c^5 - 144ab^4c^5 + 54c^6 + 459a^2c^6 + 27a^4c^6 + 16a^6c^6 + 324bc^6 + 1134a^2bc^6 - 144a^4bc^6 + 486b^2c^6 + 270a^2b^2c^6 + 216b^3c^6 - 1458ac^7 + 216a^3c^7 - 972abc^7 + 729c^8 + 4a^4b^3d - 8a^6b^3d + 4a^8b^3d - 16a^2b^4d + 48a^4b^4d + 32a^6b^4d - 64a^2b^5d + 88a^4b^5d - 8a^6b^5d - 96a^2b^6d + 48a^4b^6d - 64a^2b^7d + 4a^4b^7d - 16a^2b^8d - 2a^3bcd + 2a^5bcd + 18a^7bcd - 18a^9bcd - 120a^5b^2cd + 152a^7b^2cd + 32ab^5cd + 116a^5b^2cd - 416a^5b^3cd + 60a^7b^3cd + 128ab^5cd + 392a^3b^4cd - 368a^5b^4cd + 192ab^5cd + 446a^3b^5cd - 42a^5b^5cd
\[ + 128a^6b^2d + 168a^3b^6c + 32ab^7cd + 2a^2c^2d - 22a^4c^2d + 78a^6c^2d \\
+ 6a^8c^2d + 8a^2b^2c^2d - 180a^4b^2c^2d - 168a^6bc^2d - 108a^8bc^2d - 32b^2c^2d \\
+ 36a^2b^2c^2d + 394a^4b^2c^2d + 690a^6b^2c^2d - 256b^3c^2d - 168a^2b^3c^2d \\
- 64a^4b^3c^2d + 144a^6b^3c^2d - 704b^4c^2d - 358a^2b^4c^2d \\
- 600a^4b^4c^2d - 896b^5c^2d - 96a^2b^5c^2d - 8a^4b^5c^2d - 544b^6c^2d \\
+ 64a^2b^6c^2d - 128b^7c^2d - 64ac^3d + 212a^3c^3d + 824a^5c^3d - 132a^7c^3d \\
- 432abc^3d - 2844a^3bc^3d + 346a^5bc^3d - 162a^7bc^3d + 1312ab^2c^3d \\
- 2364a^3b^2c^3d + 870a^5b^2c^3d + 4880ab^3c^3d - 892a^3b^3c^3d \\
+ 68a^5b^3c^3d + 4416ab^4c^3d + 5763b^3c^4d + 1216ab^5c^3d + 216c^4d \\
+ 1362a^2c^4d + 8a^4c^4d - 450a^6c^4d + 1008bc^4d + 2124a^2bc^4d + 2652a^4bc^4d \\
- 144a^6bc^4d - 648b^2c^4d - 7182a^2b^2c^4d + 1276a^4b^2c^4d - 3456b^3c^4d \\
- 2328a^3b^3c^4d - 2016b^4c^4d - 7560ac^5d - 2862a^3c^5d + 48a^5c^5d \\
+ 8424abc^5d - 2340a^3bc^5d + 9504ab^2c^5d + 5832c^6d + 324a^2c^6d - 7776bc^6d \\
+ a^4d^2 + 9a^6d^2 + 27a^8d^2 + 27a^1od^2 - 68a^4bd^2 - 288a^6bd^2 - 252a^8bd^2 \\
+ 96a^2b^2d^2 + 918a^4b^2d^2 + 704a^6b^2d^2 - 54a^8b^2d^2 - 768a^2b^3d^2 \\
- 12a^4b^3d^2 + 228a^6b^3d^2 + 256b^4d^2 - 2368a^2b^4d^2 + 417a^4b^4d^2 \\
+ 27a^6b^4d^2 + 1024b^5d^2 - 2176a^2b^5d^2 + 24a^4b^5d^2 + 1536b^6d^2 \\
- 800a^2b^6d^2 + 16a^4b^6d^2 + 1024b^7d^2 - 128a^2b^7d^2 + 256b^8d^2 + 128a^3c^2d^2 \\
+ 138a^5cd^2 + 516a^7cd^2 + 162a^9cd^2 - 128abcd^2 - 1584a^3bcd^2 - 3774a^5bcd^2 \\
- 378b^7cd^2 + 1536ab^2cd^2 + 8224a^3b^2cd^2 - 4362a^5b^2cd^2 - 162a^7b^2cd^2 \\
+ 512ab^3cd^2 + 13328a^3b^3cd^2 - 450a^5b^3cd^2 - 6656ab^4cd^2 + 6912a^3b^4cd^2 \\
- 144a^5b^4cd^2 - 8064ab^5cd^2 + 1216a^3b^5cd^2 - 2560ab^6cd^2 + 128c^2d^2 \\
+ 816a^2c^2d^2 - 2238a^4c^2d^2 + 1359a^6c^2d^2 + 243a^8c^2d^2 + 3936a^2bc^2d^2 \\
- 3900a^4bc^2d^2 + 1134a^6bc^2d^2 - 6656b^2c^2d^2 - 18432a^2b^2c^2d^2 \\
- 13590a^4b^2c^2d^2 + 270a^6b^2c^2d^2 - 7168b^3c^2d^2 + 7872a^2b^3c^2d^2 \\
- 2328a^4b^3c^2d^2 + 4992b^4c^2d^2 + 3648a^2b^4c^2d^2 + 5632b^2c^2d^2 \\
- 9984ac^3d^2 - 13456a^3c^3d^2 + 954a^5c^3d^2 + 216a^7c^3d^2 + 48096abc^3d^2 \\
+ 14640a^3bc^3d^2 - 2340a^5bc^3d^2 + 3456ab^2c^3d^2 + 11968a^3b^2c^3d^2 \\
- 26112ab^3c^3d^2 + 15120a^4c^3d^2 + 648a^2c^4d^2 + 3030a^4c^4d^2 - 51840bc^4d^2 \\
- 16416a^2bc^4d^2 + 27648b^2c^4d^2 + 10368ac^5d^2 - 128a^2d^3 - 424a^3d^3 \]
Note that we need to take a tschirnhaus transformation of degree 12 polynomial over the rationals. For polynomial (if required), the degree 12 resolvent, and the factorization of the degree 12 resolvents are not squarefree. In all cases, we give the transformed we only give it.

Here are the degree 12 resolvents of the five sample polynomials $t_1, \ldots, t_5$. Note that we need to take a tschirnhaus transformation of $t_2$ and $t_3$, since their degree 12 resolvents are not squarefree. In all cases, we give the transformed polynomial (if required), the degree 12 resolvent, and the factorization of the degree 12 polynomial over the rationals. For $t_5$, the resolvent is irreducible, so we only give it.

$$t_1$$

**degree 12 res:** $x^{12} + 6x^{11} - 21x^{10} - 160x^9105x^8 + 1446x^7 + 211x^6 - 5166x^5 + 1120x^4 + 12890x^3 - 32546x^2 - 40146x34441$

**factorization:** $(x^2 + x - 11)(x^2 + x - 1)(x^4 - 8x^3 + 24x^2 - 37x + 31)(x^4 + 12x^3 + 54x^2 + 113x + 101)$

$$t_2$$

**tschirnhaus:** $x^4 - 12x^3 + 62x^2 - 84x + 34$
degree 12 res: \[ x^{12} + 72x^{11} - 2504x^{10} - 245280x^9 + 1875080x^8 + 318348672x^7 + 87377344x^6 - 181028775168x^5 - 749536378480x^4 + 34794601092480x^3 + 336921864635776x^2 + 718430161516032x - 194650798165760 \]

factorization: \((x^2 - 60x + 916)(x^2 - 56x + 802)(x^2 + 8x - 2)(x^2 + 16x + 46)(x^2 + 80x + 1618)(x^2 + 84x + 1780)\)

\(t_3\)

tschirnhaus: \[ x^4 - 16x^3 + 160x^2 - 256x + 768 \]

degree 12 res: \[ x^{12} + 96x^{11} - 85632x^{10} - 7075840x^9 + 2777833472x^8 + 188719038464x^7 - 4362099626752x^6 - 2264865590738944x^5 + 36425192150089728x^4 + 12636857700441915392x^3 - 15739588385915193192x^2 - 26826134476797392191488x + 2785096457651006069538816 \]

factorization: \((x^4 - 480x^3 + 82304x^2 - 5920768x + 151586816)(x^4 + 32x^3 - 15744x^2 - 256000x + 68194304)(x^4 + 544x^3 + 106880x^2 + 8939520x + 269420544)\)

\(t_4\)

degree 12 res: \[ x^{12} + 12x^{11} - 44x^{10} - 880x^9 + 8x^8 + 23296x^7 + 18320x^6 - 283808x^5 - 101744x^4 + 2049472x^3 - 2031360x^2 - 9244800x + 7496000 \]

factorization: \((x^6 + 6x^5 - 40x^4 - 312x^3 + 68x^2 + 4248x + 7496)(x^6 + 6x^5 - 40x^4 - 88x^3 + 740x^2 - 1800x + 1000)\)

\(t_5\)

degree 12 res: \[ x^{12} + 6x^{11} - 33x^{10} - 220x^9 + 421x^8 + 3070x^7 - 3149x^6 - 21182x^5 + 18868x^4 + 77094x^3 - 63598x^2 - 106258x - 28751 \]

4. Algorithms

In this section, we describe the algorithms for computing quartic Galois groups as described in [1, 3, 4, 7]. We also describe the simple method in [7] for computing the Galois group of a biquadratic polynomial; i.e., a polynomial of the form \(x^4 + ax^2 + b\).
Table 2: The top row contains the transitive subgroups $G$ of $S_4$, as listed in Table 1. The left column contains the subgroups $H$ referenced in Section 3. Note the group $C_2$ is generated by $(12)(34)$. For a particular pair $(H, G)$, the entry in the table gives the lengths of the orbits of $G$ acting on the cosets $S_4/H$. In particular, this list is equivalent to the list of irreducible factors of the resolvent polynomial $R_H(x)$ of a quartic polynomial $f(x)$ where $G$ is the Galois group of $f$.

<table>
<thead>
<tr>
<th>$H/G$</th>
<th>$C_4$</th>
<th>$V_4$</th>
<th>$D_4$</th>
<th>$A_4$</th>
<th>$S_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_2$</td>
<td>2,2,4,4</td>
<td>2,2,2,2,2</td>
<td>4,4,4</td>
<td>6,6</td>
<td>12</td>
</tr>
<tr>
<td>$C_4$</td>
<td>1,1,4</td>
<td>2,2</td>
<td>2,4</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>$D_4$</td>
<td>1,2</td>
<td>1,1,1</td>
<td>1,2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$A_4$</td>
<td>2</td>
<td>1,1</td>
<td>2</td>
<td>1,1</td>
<td>2</td>
</tr>
</tbody>
</table>

**Resolvent Factorizations**

As mentioned in the opening paragraph of Section 3, if $G$ is the Galois group of the quartic polynomial $f$, $H$ is a subgroup of $S_4$, and $R_H(x)$ is the resolvent polynomial of $f$ corresponding to $H$, then the Galois group of $R_H(x)$ is isomorphic to the image of the permutation representation of $G$ acting on the cosets $S_4/H$. The irreducible factors of $R_H(x)$ correspond to the orbits of this action, and therefore the degrees of the irreducible factors correspond to the orbit lengths. Table 2 shows the orbit lengths of the four resolvent polynomials mentioned in Section 3. In particular, the discriminant corresponds to $A_4$ row, the cubic resolvent corresponds to the $D_4$ row, the sextic resolvent corresponds to the $C_4$ row, and the degree 12 resolvent corresponds to the $C_2$ row.

**Cubic Resolvent Algorithm**

The following algorithm is found in [4] and is based on the cubic resolvent.

*Algorithm 4.1.* Given an irreducible quartic polynomial defined over a field $F$, this algorithm outputs the name of the Galois group of $f(x)$ from among those listed in Table 1.

1. Form the cubic resolvent $g(x)$, as described in Section 3. Factor $g(x)$ over $F$. Let $L$ be the list of the degrees of the irreducible factors.
2. If $L = \{1, 1, 1\}$, return $V_4$.
3. Let $d$ be the discriminant of $f(x)$.
4. If \( L = \{3\} \), return \( A_4 \) if \( d \) is a perfect square in \( F \) and \( S_4 \) otherwise.

5. Factor \( f(x) \) over \( K = F(\sqrt{d}) \). Return \( C_4 \) if \( f(x) \) is reducible over \( K \) and \( D_4 \) otherwise.

**Proof.** Steps (2) and (4) follow immediately from Table 2. To prove Step (5), we note that \( f(x) \) will be reducible over \( K = F(\sqrt{d}) \) if and only if \( K \) defines a quadratic subfield of \( f \)'s stem field. By the Galois correspondence, quadratic subfields of \( f \)'s stem field correspond to subgroups \( H \) of \( G \) of index 2 that contain \( G_1 \), the point stabilizer of 1. On the other hand, the subgroup that corresponds to \( F(\sqrt{d}) \) is \( A_4 \cap G \). For the group \( C_4 \), these two subgroups are the same; namely, \( \{(1), (13)(24)\} \). For \( D_4 \), these two groups are different: \( A_4 \cap D_4 = V_4 \) (the transitive \( V_4 \)), while the subgroup of \( D_4 \) of index 2 containing the point stabilizer of 1 in \( D_4 \) is an intransitive \( V_4 = \{(1), (13), (24), (13)(24)\} \). This proves that if \( G \in \{C_4, D_4\} \), then \( f(x) \) is reducible over \( K \) if and only if \( G = C_4 \). \( \square \)

We note that [7] contains a modification of Algorithm 4.1. The need to factor \( f(x) \) over \( F(\sqrt{d}) \) is replaced by factoring two additional quadratic polynomials over \( F \); these two quadratic polynomials make use of the unique simple root of the cubic resolvent. See their paper for complete details.

**Sextic Resolvent Algorithm**

The following algorithm is found in [3] and is based on the sextic resolvent.

**Algorithm 4.2.** Given an irreducible quartic polynomial defined over a field \( F \), this algorithm outputs the name of the Galois group of \( f(x) \) from among those listed in Table 1.

1. Form the degree 6 resolvent \( g(x) \), as described in Section 3. Factor \( g(x) \) over \( F \).

2. If \( g \) is squarefree (that is, if \( \gcd(g(x), g'(x)) = 1 \)), let \( L \) be the list of the degrees of the irreducible factors. Otherwise, replace \( f \) by a Tschirnhaus transformation and repeat step 1.

3. Return \( C_4, V_4, \) or \( D_4 \) if \( L = \{1, 1, 4\}, \{2, 2, 2\}, \) or \( \{2, 4\} \), respectively.

4. Let \( d \) be the discriminant of \( f(x) \).

5. Return \( A_4 \) if \( d \) is a perfect square in \( F \) and \( S_4 \) otherwise.

**Proof.** Follows immediately from Table 2. \( \square \)
Degree 12 Resolvent Algorithm

The following algorithm is found in [1] and is based on the degree 12 resolvent.

Algorithm 4.3. Given an irreducible quartic polynomial defined over a field $F$, this algorithm outputs the name of the Galois group of $f(x)$ from among those listed in Table 1.

1. Form the degree 12 resolvent $g(x)$, as described in Section 3. Factor $g(x)$ over $F$.

2. If $g$ is squarefree (that is, if $\gcd(g(x), g'(x)) = 1$), let $L$ be the list of the degrees of the irreducible factors. Otherwise, replace $f$ by a Tschirnhaus transformation and repeat step 1.

3. Return $C_4$, $V_4$, $D_4$, $A_4$, or $S_4$ if $L = \{2, 2, 4, 4\}$, $\{2, 2, 2, 2, 2, 2\}$, $\{4, 4, 4\}$, $\{6, 6\}$, or $\{12\}$, respectively.

Proof. Follows immediately from Table 2.

Biquadratic Algorithm

The following algorithm is found in [7].

Algorithm 4.4. Given an irreducible biquadratic polynomial $f(x) = x^4 + ax^2 + b$ defined over a field $F$, this algorithm outputs the name of the Galois group of $f(x)$ from among those listed in Table 1.

1. Let $d = 16a^4b - 128a^2b^2 + 256b^3$.

2. Return $V_4$ if $d$ is a perfect square in $F$.

3. Let $e = a^2 - 4b$

4. Return $C_4$ if $de$ is a perfect square in $F$ and $D_4$ otherwise.

Proof. Let $G$ be the Galois group of $f$ and $K$ the stem field of $f$. Clearly, $K$ has a quadratic subfield, defined by the polynomial $g(x) = x^2 + ax + b$. As noted in the proof of Algorithm 4.1, the presence of a quadratic subfield is equivalent to the existence of a subgroup $H$ of $G$ of index 2 that contains $G_1$, the point stabilizer of 1. Direct computation shows the groups $C_4$, $V_4$, and $D_4$ have such a subgroup $H$, while $A_4$ and $S_4$ do not. Therefore $G \in \{C_4, V_4, D_4\}$.

Now $d$ equals the discriminant of $f(x)$ and $e$ is the discriminant of $g(x)$. According to Table 2, $d$ is a perfect square if and only if $G = V_4$. This proves Step (2).
Since $K$ is defined by $g$, $K = F(\sqrt{e})$. Note, $F(\sqrt{d})$ also defines a quadratic extension of $F$. As shown in the proof of Algorithm 4.1, $F(\sqrt{d}) = K$ if and only if $G = C_4$. But $F(\sqrt{d}) = F(\sqrt{e})$ if and only if $de$ is a perfect square. This proves Step (4).

5. New Method

In this section, we outline our non-resolvent approach to computing quartic Galois groups. We also show our approach gives rise to an application to biquadratic quartics.

Algorithm 5.1. Given an irreducible quartic polynomial $f(x)$ defined over a field $F$, this algorithm outputs the name of the Galois group of $f(x)$ from among those listed in Table 1.

1. Let $K$ be the stem field $f$. Factor $f$ over $K$ and let $r$ denote the number of linear factors.

2. Return $D_4$ if $r = 2$.

3. Let $d$ be the discriminant of $f(x)$.

4. If $r = 4$, return $V_4$ if $d$ is a perfect square in $F$ and $C_4$ otherwise.

5. If $r = 1$, return $A_4$ if $d$ is a perfect square in $F$ and $S_4$ otherwise.

Proof. Let $G$ be the Galois group of $f$, $K$ the stem field of $f$, $G_1$ the point stabilizer of 1 in $G$, and $N$ the normalizer of $G_1$ in $G$. By Corollary 2.6, $r = [N : G_1]$. Direct computation on the groups $\{C_4, V_4, D_4, A_4, S_4\}$ shows the corresponding values of $[N : G_1]$ are $\{4, 4, 2, 1, 1\}$, respectively. The algorithm now follows by combining this information with row $A_4$ in Table 2.

Biquadratic Polynomials

The proof of Algorithm 4.4 shows if $f(x)$ is biquadratic, then the Galois group of $f$ is either $C_4$, $V_4$, or $D_4$. In this section, we show the converse is true. That is, we show if $K$ is the stem of $f(x)$ where the Galois group of $f$ is $C_4$, $V_4$, or $D_4$, then there exists a biquadratic polynomial $g(x)$ that defines $K$. Our proof is constructive.
Algorithm 5.2. Given an irreducible quartic polynomial $f(x)$ defined over a field $F$ whose Galois group is either $C_4$, $V_4$, or $D_4$, this algorithm outputs a biquadratic polynomial defining the same extension as $f$.

1. Let $K$ be the stem field $f$ generated by a root $r$ of $f$. Factor $f$ over $K$ and let $L$ denote the roots of linear factors; these will necessarily be polynomials in the variable $r$ of degree $\leq 3$ (they will be the automorphisms of $K/F$).

2. Pick $g(r) \in L$ such that $g(r) \neq r$ and $g(g(r)) \equiv r \pmod{f(r)}$. So $g(r)$ is an automorphism of order 2.

3. Let $h(x)$ be the characteristic polynomial of $r - g(r)$. That is, $h(x) = \text{Resultant}_{r}(x - (r - g(r)), f(r))$.

4. Return $h(x)$ if it is squarefree. Otherwise, replace $f$ by a Tschirnhaus transformation and repeat steps 1–4.

Proof. Let $G$ be the Galois group of $f(x)$, $K$ the stem field of $f$, and $\text{Aut}(K)$ the automorphism group of $K/F$. Corollary 2.6 shows $\text{Aut}(K)$ is isomorphic to $N/G_1$ where $G_1$ is the point stabilizer of 1 in $G$ and $N$ the normalizer of $G_1$ in $G$. The proof of Algorithm 4.4 shows that since $G \in \{C_4, V_4, D_4\}$, $K$ contains a quadratic subfield. Thus $\text{Aut}(K)$ contains a subgroup of order 2, and hence an element of order 2. This proves Step (2) is possible.

Direct computation shows that if $G = V_4$, there are 3 such choices for $g(r)$. As permutations, these automorphisms are given by: $(12)(34), (13)(24), (14)(23)$. Otherwise, there is a unique choice for $g(r)$. If $G = C_4$ or $D_4$, $g(r)$ is the permutation $(13)(24)$. Note that these permutations depend on the ordering of the roots of $f$. Different orderings will correspond to conjugate permutations. But the cycle type is invariant under conjugation. So in any case, the permutation $g(r)$ leaves no root fixed.

Let $h(x) = \text{Resultant}_{r}(x - (r - g(r)), f(r))$. Thus $h(x) \in F[x]$, and therefore the irreducible factors of $h$ define subfields of $K$. Suppose the roots of $f$ are $a, b, c, d$. Suppose further that $g(r)$ permutes the roots in the following way: $(ab)(cd)$. Then

$$h(x) = (x - (a - b))(x - (b - a))(x - (c - d))(x - (d - c))$$
$$= (x^2 - (a - b)^2)(x^2 - (c - d)^2)$$
$$= x^4 - [(a - b)^2 + (c - d)^2]x^2 + [(a - b)(c - d)]^2.$$

Thus $h(x)$ is biquadratic. If $h$ is irreducible, then since it defines a subfield of $K$, it must be the case that the stem field of $h$ is exactly $K$. \qed
5.1. Example

For example, let $f(x) = x^4 - x^3 + x^2 - x + 1$. Let $K/\mathbb{Q}$ be the stem field of $f$. Then factoring $f$ over $K$ shows that $K$ contains all four roots of $f$. The four automorphisms of $K$ are:

$$r, -r^2, -r^3 + r^2 - r + 1, r^3$$

Direct computation on the 3 nontrivial automorphisms shows that when the 2nd and 4th automorphisms are composed with themselves, they yield the 3rd automorphism. When the 3rd automorphism is composed with itself, it yields $r$. Note, this proves the Galois group of $f$ is $C_4$. Let $g(r) = -r^3 + r^2 - r + 1$. Forming the characteristic polynomial $h(x)$ of $r - g(r)$, we obtain $h(x) = x^4 + 5x^2 + 5$, an irreducible biquadratic polynomial.

6. Comparison

In this section, we give an analysis of run times of the various algorithms. In an effort to conduct a timing analysis, we implemented 6 quartic Galois group algorithms into Wolfram Mathematica and used the built-in `Timing` function to calculate run times. The algorithms are the resolvent methods described in Section 3 as well as two non-resolvent methods. We label the resolvent methods as Cubic ([4]), Sextic ([3]), Deg 12 ([1]), and [7]. We label the non-resolvent methods as Algorithm 5.1 and SF. The SF algorithm computes a polynomial defining the splitting field of the original quartic. The splitting field algorithm proceeds by factoring the original quartic over its stem field $K$. If $f$ does not factor into linear factors, $K$ does not contain all four roots. Thus we adjoin to $K$ a root of a non-linear factor and factor $f$ over this new extension. We continue in this fashion until we obtain an extension which contains all four roots of $f$.

The sample polynomials for each Galois group are shown below:

- $C4 : x^4 - x^3 + x^2 - x + 1$
- $V4 : x^4 + 1$
- $D4 : x^4 + 2$
- $A4 : x^4 - 2x^3 + 2x^2 - x + 2$
- $S4 : x^4 - x^3 + 1$
Using these polynomials, we applied between one and ten Tschirnhaus transformations in order to test the speed of each algorithm at varying sizes of polynomial coefficients. By doing so, we can test whether certain algorithms are relatively faster or slower for different polynomial sizes. The table below shows the average coefficient size (given as the number of digits) of each polynomial, ranging from one Tschirnhaus transformation to ten Tschirnhaus transformations. Notice that each application of a Tschirnhaus transformation roughly doubles the average number of digits in the polynomial’s coefficients.

<table>
<thead>
<tr>
<th></th>
<th>V4</th>
<th>D4</th>
<th>C4</th>
<th>A4</th>
<th>S4</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>T2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>T3</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>T4</td>
<td>16</td>
<td>18</td>
<td>17</td>
<td>19</td>
<td>17</td>
</tr>
<tr>
<td>T5</td>
<td>34</td>
<td>35</td>
<td>33</td>
<td>37</td>
<td>36</td>
</tr>
<tr>
<td>T6</td>
<td>65</td>
<td>67</td>
<td>65</td>
<td>77</td>
<td>72</td>
</tr>
<tr>
<td>T7</td>
<td>129</td>
<td>142</td>
<td>137</td>
<td>148</td>
<td>133</td>
</tr>
<tr>
<td>T8</td>
<td>269</td>
<td>274</td>
<td>268</td>
<td>308</td>
<td>275</td>
</tr>
<tr>
<td>T9</td>
<td>504</td>
<td>575</td>
<td>521</td>
<td>607</td>
<td>551</td>
</tr>
<tr>
<td>T10</td>
<td>1021</td>
<td>1047</td>
<td>1016</td>
<td>1173</td>
<td>1145</td>
</tr>
</tbody>
</table>

6.1. Timings

We present the ratios of timings for all methods except [7] (because it is the fastest). For the algorithm in [7], we list its actual run time on our machine (Macbook Pro, 3 GHz, Intel Core i7). For the other methods, their actual run times are divided by the timing of the fastest method. By doing so, we can control for the hardware constraints of the machine on which the algorithms are run. The absolute timings of each algorithm may change from machine to machine, but the ratios should not. Additionally, analyzing ratios allow us to easily interpret the speed of each algorithm by explicitly showing how many times slower each method is than the fastest method. We present the timings of each method below.
Timings when the Galois group is $V_4$

<table>
<thead>
<tr>
<th></th>
<th>[7]</th>
<th>SF</th>
<th>Alg. 5.1</th>
<th>Sextic</th>
<th>Deg 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0.004</td>
<td>22.13</td>
<td>21.58</td>
<td>361.04</td>
<td>21.79</td>
</tr>
<tr>
<td>T2</td>
<td>0.005</td>
<td>14.54</td>
<td>15.44</td>
<td>187.73</td>
<td>13.12</td>
</tr>
<tr>
<td>T3</td>
<td>0.0056</td>
<td>9.59</td>
<td>10.51</td>
<td>92.28</td>
<td>7.59</td>
</tr>
<tr>
<td>T4</td>
<td>0.0067</td>
<td>9.01</td>
<td>9.93</td>
<td>59.74</td>
<td>5.67</td>
</tr>
<tr>
<td>T5</td>
<td>0.0079</td>
<td>10.3</td>
<td>10.78</td>
<td>44.36</td>
<td>4.88</td>
</tr>
<tr>
<td>T6</td>
<td>0.0097</td>
<td>13.6</td>
<td>13.09</td>
<td>33.02</td>
<td>4.47</td>
</tr>
<tr>
<td>T7</td>
<td>0.0133</td>
<td>19.94</td>
<td>20.72</td>
<td>24.49</td>
<td>4.51</td>
</tr>
<tr>
<td>T8</td>
<td>0.0177</td>
<td>39.32</td>
<td>36.77</td>
<td>17.76</td>
<td>5.46</td>
</tr>
<tr>
<td>T9</td>
<td>0.0279</td>
<td>84.76</td>
<td>89.18</td>
<td>13.91</td>
<td>8.6</td>
</tr>
<tr>
<td>T10</td>
<td>0.0494</td>
<td>239.67</td>
<td>234.11</td>
<td>12.4</td>
<td>16.23</td>
</tr>
</tbody>
</table>

For polynomials with $V_4$ as Galois group, the method in [7] and the cubic resolvent method are equivalent. They appear to be the fastest, regardless of the size of the polynomial. These methods only take 0.004 seconds for a polynomial with 1 Tschirnhaus transformation and under 0.05 seconds for a polynomial with ten Tschirnhaus transformations. Both the ratios in the timings of the SF and Alg. 5.1 methods become much larger as we increase the number of Tschirnhaus transformations. Interestingly, the sextic resolvent methods get relatively faster compared to [7], but seems to level off compared to [7] for a higher number of Tschirnhaus transformations. Lastly, the degree 12 method appears to be inconsistent, as its timing ratios decrease until six Tschirnhaus transformations and then increase until ten Tschirnhaus transformations. Seeing that the smallest ratio of timings occurs with the degree 12 resolvent method at 6 Tschirnhaus transformations, the method in [7] is at least 4.47 times faster than any other method for polynomials with Galois group $V_4$. 
Timings when the Galois group is $D_4$

<table>
<thead>
<tr>
<th></th>
<th>[7]</th>
<th>SF</th>
<th>Alg. 5.1</th>
<th>Cubic</th>
<th>Sextic</th>
<th>Deg 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0.0044</td>
<td>15.44</td>
<td>16.57</td>
<td>17.69</td>
<td>308.94</td>
<td>20.4</td>
</tr>
<tr>
<td>T2</td>
<td>0.0048</td>
<td>10.56</td>
<td>11.43</td>
<td>10.38</td>
<td>163.39</td>
<td>11.32</td>
</tr>
<tr>
<td>T3</td>
<td>0.0059</td>
<td>9.18</td>
<td>9.92</td>
<td>7.51</td>
<td>102.8</td>
<td>8.36</td>
</tr>
<tr>
<td>T4</td>
<td>0.0069</td>
<td>9.25</td>
<td>10.26</td>
<td>7</td>
<td>75.05</td>
<td>7.2</td>
</tr>
<tr>
<td>T5</td>
<td>0.0083</td>
<td>9.8</td>
<td>11.2</td>
<td>6.16</td>
<td>55.59</td>
<td>6.59</td>
</tr>
<tr>
<td>T6</td>
<td>0.0101</td>
<td>11.87</td>
<td>13.33</td>
<td>6.23</td>
<td>42.04</td>
<td>6.36</td>
</tr>
<tr>
<td>T7</td>
<td>0.0138</td>
<td>15.31</td>
<td>15.99</td>
<td>6.62</td>
<td>30.83</td>
<td>6.73</td>
</tr>
<tr>
<td>T8</td>
<td>0.0204</td>
<td>20.2</td>
<td>21.53</td>
<td>8</td>
<td>23.98</td>
<td>9.29</td>
</tr>
<tr>
<td>T9</td>
<td>0.0348</td>
<td>26.04</td>
<td>26.41</td>
<td>9.27</td>
<td>18.9</td>
<td>13.78</td>
</tr>
<tr>
<td>T10</td>
<td>0.0694</td>
<td>37.82</td>
<td>37.72</td>
<td>14.55</td>
<td>28.6</td>
<td>33.67</td>
</tr>
</tbody>
</table>

For polynomials with $D_4$ as Galois group, we can see that the method in [7] is again the quickest regardless of the size of polynomial coefficients. For a polynomial with one Tschirnhaus transformation, this method takes 0.004 seconds to compute the polynomial’s Galois group, and for polynomials with ten Tschirnhaus transformations, it takes just under 0.7 seconds. Every other method’s timing ratios decrease in size before increasing in size at various Tschirnhaus levels. Since the minimum timing ratio is the cubic method at five Tschirnhaus transformations, we can conclude that the method in [7] is at least 6.16 times faster than any other method for polynomials with Galois group $D_4$.

Timings when the Galois group is $C_4$

<table>
<thead>
<tr>
<th></th>
<th>[7]</th>
<th>SF</th>
<th>Alg. 5.1</th>
<th>Cubic</th>
<th>Sextic</th>
<th>Deg 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0.0048</td>
<td>16.19</td>
<td>15.32</td>
<td>19.37</td>
<td>255.32</td>
<td>17.23</td>
</tr>
<tr>
<td>T2</td>
<td>0.0055</td>
<td>10.06</td>
<td>9.56</td>
<td>10.72</td>
<td>140.06</td>
<td>10.17</td>
</tr>
<tr>
<td>T3</td>
<td>0.0065</td>
<td>8.4</td>
<td>8.26</td>
<td>7.42</td>
<td>84.47</td>
<td>7.42</td>
</tr>
<tr>
<td>T4</td>
<td>0.0074</td>
<td>8.3</td>
<td>8</td>
<td>5.83</td>
<td>58.63</td>
<td>5.74</td>
</tr>
<tr>
<td>T5</td>
<td>0.0089</td>
<td>8.9</td>
<td>8.67</td>
<td>5.36</td>
<td>45.16</td>
<td>5.26</td>
</tr>
<tr>
<td>T6</td>
<td>0.0112</td>
<td>10.67</td>
<td>10.29</td>
<td>5.27</td>
<td>34.43</td>
<td>5.03</td>
</tr>
<tr>
<td>T7</td>
<td>0.0146</td>
<td>13.65</td>
<td>12.8</td>
<td>5.55</td>
<td>25.21</td>
<td>5.04</td>
</tr>
<tr>
<td>T8</td>
<td>0.0216</td>
<td>17.93</td>
<td>16.82</td>
<td>6.13</td>
<td>18.45</td>
<td>5.72</td>
</tr>
<tr>
<td>T9</td>
<td>0.0343</td>
<td>23.21</td>
<td>21.58</td>
<td>7.02</td>
<td>12.72</td>
<td>8.01</td>
</tr>
<tr>
<td>T10</td>
<td>0.0703</td>
<td>32.49</td>
<td>32.77</td>
<td>9.37</td>
<td>10.05</td>
<td>15.27</td>
</tr>
</tbody>
</table>

Again, we see that the method in [7] is the fastest method for quartic polyno-
mials with Galois group $C_4$. This method takes $0.0048$ seconds for polynomials with one Tschirnhaus transformation and $0.0703$ seconds for polynomials with ten Tschirnhaus transformations. The timing ratios of all methods except the sextic resolvent method become smaller before becoming larger compared to [7] as we increase the size of the polynomial coefficients. The sextic resolvent method becomes relatively faster as we increase coefficient size. We can say that the method in [7] is at least 5 times faster than any other method for polynomials with Galois group $C_4$, as the smallest ratio is 5.03. This occurs when we use the degree 12 method on polynomials with six Tschirnhaus transformations.

Timings when the Galois group is $A_4$

<table>
<thead>
<tr>
<th></th>
<th>[7]</th>
<th>SF</th>
<th>Alg. 5.1</th>
<th>Sextic</th>
<th>Deg 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0.004</td>
<td>233.39</td>
<td>17.82</td>
<td>325.28</td>
<td>22.25</td>
</tr>
<tr>
<td>T2</td>
<td>0.0045</td>
<td>198.96</td>
<td>13.17</td>
<td>175.58</td>
<td>14.01</td>
</tr>
<tr>
<td>T3</td>
<td>0.0055</td>
<td>186.3</td>
<td>10.41</td>
<td>97.92</td>
<td>9.8</td>
</tr>
<tr>
<td>T4</td>
<td>0.0065</td>
<td>245.72</td>
<td>10.05</td>
<td>65.04</td>
<td>8.83</td>
</tr>
<tr>
<td>T5</td>
<td>0.0077</td>
<td>463.4</td>
<td>11.97</td>
<td>47.33</td>
<td>10.13</td>
</tr>
<tr>
<td>T6</td>
<td>0.0094</td>
<td>1026.79</td>
<td>16.11</td>
<td>36.55</td>
<td>14.47</td>
</tr>
<tr>
<td>T7</td>
<td>0.0124</td>
<td>3305.62</td>
<td>24.37</td>
<td>28.47</td>
<td>28.25</td>
</tr>
<tr>
<td>T8</td>
<td>0.0178</td>
<td>9043.24</td>
<td>44.08</td>
<td>21.43</td>
<td>71.57</td>
</tr>
</tbody>
</table>

For quartic polynomials with Galois group $A_4$, the method in [7] and the cubic resolvent method are equivalent, and they are the fastest. We only used eight Tschirnhaus transformations for polynomials with this Galois group due to computational constraints of our machine. The ratios of the SF, Alg. 5.1, the degree 12 methods decrease in size initially, and then increase in size as we increase the size of polynomial coefficients. On the other hand, the sextic resolvent method becomes relatively faster as we increase the size of coefficients, when compared to [7]. This method is at least 47% faster than any other method, given a random quartic polynomial with Galois group $A_4$, as the smallest ratio is 1.47, occurring when we apply the cubic resolvent method to a polynomial with eight Tschirnhaus transformations.
Timings when the Galois group is $S_4$

<table>
<thead>
<tr>
<th></th>
<th>[7]</th>
<th>SF</th>
<th>Alg. 5.1</th>
<th>Sextic</th>
<th>Deg 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0.0043</td>
<td>229.75</td>
<td>17.27</td>
<td>362.22</td>
<td>22.56</td>
</tr>
<tr>
<td>T2</td>
<td>0.0046</td>
<td>181.17</td>
<td>12.36</td>
<td>183.85</td>
<td>12.43</td>
</tr>
<tr>
<td>T3</td>
<td>0.0057</td>
<td>179.99</td>
<td>11.01</td>
<td>112.48</td>
<td>8.91</td>
</tr>
<tr>
<td>T4</td>
<td>0.0067</td>
<td>227.81</td>
<td>10.8</td>
<td>78.39</td>
<td>7.76</td>
</tr>
<tr>
<td>T5</td>
<td>0.0088</td>
<td>376.59</td>
<td>12.37</td>
<td>58.65</td>
<td>7.75</td>
</tr>
<tr>
<td>T6</td>
<td>0.0113</td>
<td>742.86</td>
<td>14.24</td>
<td>42.68</td>
<td>9.59</td>
</tr>
<tr>
<td>T7</td>
<td>0.0165</td>
<td>1665.3</td>
<td>19.11</td>
<td>31.19</td>
<td>14.28</td>
</tr>
<tr>
<td>T8</td>
<td>0.0263</td>
<td>4820.63</td>
<td>25.98</td>
<td>21.33</td>
<td>34.11</td>
</tr>
</tbody>
</table>

Lastly, the method in [7] and the cubic resolvent method are equivalent for polynomials with Galois group $S_4$. They are the quickest methods in this case. The timing ratios of the SF method appear to increase at an exponential rate. The timing ratios of Alg. 5.1 and the degree 12 methods decrease before increasing five and six Tschirnhaus transformations, respectively. The sextic resolvent method increases in relative speed as we increase the size of the coefficients. The method in [7] is at least 7.75 times faster than any other method, as the smallest timing ratio occurs when we apply the degree 12 resolvent method to a polynomial with 5 Tschirnhaus transformations.

References


