EFFICIENT COMPUTATION OF GALOIS GROUPS OF EVEN SEXTIC POLYNOMIALS

CHAD AWTREY AND PETER JAKES

ABSTRACT. Let $f(x) = x^6 + ax^4 + bx^2 + c$ be an irreducible sextic polynomial with coefficients from a field F (of characteristic $\neq 2$), and let $g(x) = x^3 + ax^2 + bx + c$. We describe an efficient algorithm to compute the Galois group of f over F that involves the discriminants of f and g and the reducibility of a related sextic polynomial. As an application, we develop one-parameter families for each possible Galois group. Using these families, we compare the timings of our algorithm against those currently available in `Magma` and `Pari/GP`.

1. Introduction

Let F be a field and $f(x) \in F[x]$ an irreducible polynomial. Let K/F denote the splitting field of f in a fixed algebraic closure $\overline{F}$ of F. An important task in computational algebra is the determination of the Galois group of f; that is, the collection of all automorphisms of K that fix F. While several methods for accomplishing this task appear in the literature, most current implementations utilize one of two strategies: (1) absolute resolvent polynomials [12], and (2) relative resolvent polynomials [13].

Both approaches have received much attention in the last 20 years. For example, the absolute resolvent method is implemented in Pari/GP [10] for computing Galois groups of polynomials defined over the rational numbers up to degree 11; details (up to degree 7) can be found in [5]. The relative resolvent method is implemented in Magma [3]. Magma's algorithm is, in principle, not limited by the degree of the polynomial, and the base field can be more general than the rational numbers. Magma's implementation utilizes an extra feature that improves running times for imprimitive extensions; namely, it computes subfields of the stem field of f first (see [15]). By stem field, we mean the field extension obtained by adjoining one root of the polynomial to the base field. This task involves factoring the polynomial over its stem field. Leveraging this subfield information and initial absolute resolvent information, Magma's algorithm proceeds with the relative resolvent method using degree-independent algorithms as described in [8] and [7].

A clear benefit of Magma's algorithm for determining Galois groups is the subfield information it exploits. However, Magma's approach to computing subfields assumes a generic input polynomial, without taking into account inherent subfield information that may be obtained without factoring the polynomial over its stem field. For example, even polynomials come attached with a polynomial defining an index 2 subfield (obtained by halving all exponents). Making use of this included subfield information can be beneficial. For example, as noted in [9], computing the

2010 *Mathematics Subject Classification.* Primary 11Y40, 12F10.
Key words and phrases. even polynomials, sextic, Galois group.

TABLE 1. One-parameter families of even quartic polynomials.

Group	**Polynomials**
E_4	$x^4 + (2t+1)^2$
C_4	$x^4 + 4tx^2 + 2t^2 \quad t \neq 0$
D_4	$x^4 + t^2 + 1 \quad t \neq 0$

Galois group of an even quartic polynomial x^4+ax^2+b requires nothing more than testing whether two numbers are perfect squares; one of those numbers involves the discriminant of the "included" quadratic polynomial x^2+ax+b. The purpose of this paper is to present an algorithm for computing Galois groups of even sextic polynomials that is similar in spirit to algorithm in [9] and that is faster than algorithms implemented in Magma and Pari/GP.

The remainder of the paper is organized as follows. To provide additional context, Section 2 describes an algorithm for computing Galois groups of even quartic polynomials that is based on [9]. This section also provides one-parameter families for each possible Galois group and uses these families to compare run times (over the rational numbers) for this algorithm against those implemented in Magma and Pari/GP. These two software programs were chosen since they are commonly used in number-theoretic computations and they represent the two most common approaches for Galois group computations (absolute vs. relative resolvents). Sections 3, 4, and 5 accomplish analogous goals for even sextic polynomials.

2. Even Quartic Polynomials

As described in [9], the possibilities for the Galois group of an irreducible even quartic polynomial are E_4 (elementary abelian of order 4), C_4 (cyclic of order 4), and D_4 (dihedral of order 4). The authors' algorithm for computing the Galois group of such a polynomial is as follows.

Algorithm 2.1 (Even Quartic Polynomials)**.** *Let $f(x) = x^4 + ax^2 + b \in F[x]$ be an irreducible polynomial. This algorithm returns the Galois group of f over F.*

1. *If b is a perfect square in F, return E_4 and terminate.*
2. *Else, if $b(a^2-4b)$ is a perfect square in F, return C_4 and terminate. Otherwise return D_4 and terminate.*

Briefly, here is why this algorithm works. Since the discriminant of f is $b(4a^2-16b)^2$, it follows that the discriminant of f is a perfect square if and only if b is a perfect square if and only if the Galois group of f is contained in A_4 (the alternating group of degree 4). Among E_4, C_4, and D_4, only E_4 is a subgroup of A_4. Now, the polynomial $g(x) = x^2 + ax + b$ defines a quadratic subfield of the stem field of f; note, the discriminant of g is a^2-4b. When b is not a perfect square, the polynomial x^2-b defines a quadratic subfield of the splitting field of f. When the Galois group is cyclic, these two subfields coincide; reflected in the fact that $b(a^2-4b)$ must be a perfect square. When the Galois group is dihedral, these two quadratic extensions are not the same; so $b(a^2-4b)$ is not a perfect square. Both statements can be verified using group-theoretic arguments combined with the Galois correspondence.

Using Algorithm 2.1, it is not difficult to produce families of polynomials that have the indicated Galois group. See Table 1 for examples.

TABLE 2. A comparison of run times of Algorithm 2.1 with the standard Galois group algorithms implemented in Magma and Pari/GP. Each row corresponds to a polynomial $f(x) = x^4+ax^2+b$ whose Galois group is specified in column **Polynomial**. Columns **a** and **b** give the number of digits of a and b, respectively. Run times are given in milliseconds.

Polynomial	**a**	**b**	**Alg 2.1**	**Magma**	**Pari/GP**
E_4	4977	9955	1	760	2027
C_4	5857	10220	1	310	2060
D_4	5824	11646	1	380	2238

We implemented this algorithm in Pari/GP and compared its timings to the standard Galois group algorithms available in Magma (v2.22) and Pari/GP (v2.5.3). The test polynomials we employed are available from [1]. These polynomials, as well as test polynomials referenced in Section 4, were computed as follows. We start with a polynomial in Table 1 (respectively Table 5) and set $t = 101$. We then call Pari/GP's `poltschirnhaus` command 11 times (respectively 8 times) to produce a polynomial defining the same stem field but whose coefficients are roughly 5000–11000 (respectively 500–4500) digits long. We then use Algorithm 3.4 to transform the polynomial into an even polynomial that defines the same stem field. For each of these polynomials $x^4 + ax^2 + b$, Table 2 contains the number of digits of a and b as well as the timings for Algorithm 2.1, Magma, and Pari/GP. All timings are in milliseconds. Computations were done on a machine with a 3 GHz Intel Core i7 processor and 8 GB of RAM.

As Table 2 shows, Algorithm 2.1 is significantly faster than the standard Galois group algorithms implemented in Magma and Pari/GP. This observation reinforces our claim that it is beneficial to exploit inherent subfield information given by even polynomials when designing Galois group algorithms. In the remaining sections, we show how this is possible to do with even sextic polynomials.

3. Algorithm for Even Sextic Polynomials

Let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be an irreducible polynomial. Let K/F denote the stem field of f and G the Galois group of f. After ordering the roots of f, we can identify G as a transitive subgroup of S_6, well defined up to conjugation (different orderings correspond to conjugate groups). Let $g(x) = x^3 + ax^2 + bx + c$. Then g defines a cubic subfield of K/F. The automorphism group of K/F is isomorphic to the centralizer of G in S_6, as shown in [2] for example. Since K/F has an index two subfield, it follows from the Galois correspondence that the order of the centralizer of G in S_6 must be even. Of the 16 transitive subgroups of S_6, only 8 have centralizer orders that are even. Table 3 gives these 8 groups, their transitive numbers (as given in Magma, based on [4]), their centralizer orders, their orders, and a descriptive name for each group.

Since K/F has a cubic subfield defined by $g(x)$, we can determine properties of G from properties of $g(x)$ using the Galois correspondence.

Proposition 3.1. *Let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be irreducible, K the stem field of f, G the Galois group of f, and $g(x) = x^3 + ax^2 + bx + c$. Let d denote the discriminant of g so that $d = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$. Then*

TABLE 3. Possible Galois groups of irreducible even sextic polynomials. **Size** gives the order of the group and **CentOrd** gives the order of the centralizer of the group in S_6.

T	**Name**	**Size**	**CentOrd**
1	C_6	6	6
2	S_3	6	6
3	D_6	12	2
4	A_4	12	2
6	$A_4 \times C_2$	24	2
7	S_4^+	24	2
8	S_4^-	24	2
11	$S_4 \times C_2$	48	2

(1) *$-c$ is a perfect square in F if and only if G is either A_4 or S_4^+.*
(2) *d is a perfect square in F if and only if G is either C_6, A_4, or $A_4 \times C_2$.*
(3) *$-cd$ is a perfect square in F if and only if G is either S_3, A_4, or S_4^-.*

Proof. The discriminant of $f(x) = x^6 + ax^4 + bx^2 + c$ is $-c(8d)^2$. Therefore G is a subgroup of A_6 if and only if $-c$ is a square in F. Of the 8 possibilities for G, only A_4 and S_4^+ are subgroups of A_6. This proves item (1).

Since d is the discriminant of the cubic polynomial $g(x) = x^3 + ax^2 + bx + c$, d is a perfect square if and only if the Galois group of $g(x)$ is C_3. But since $g(x)$ defines a cubic subfield of K/F, the stem field of $g(x)$ corresponds to an index 3 subgroup H of G containing the point stabilizer of 1 in G. By the Galois correspondence, the Galois group of $g(x)$ is isomorphic to the image of the permutation representation of G acting on the cosets G/H. Among the 8 possibilities for G, only C_6, A_4, and $A_4 \times C_2$ possess such a subgroup H with a cyclic permutation representation image. This proves item (2).

If both $-c$ and d are perfect squares, then clearly $-cd$ is a perfect square. Based on the previous two paragraphs, there is only one group among the 8 where this occurs; namely, A_4. Otherwise, if $-cd$ is a perfect square, it must be the case that both $-c$ and d are not perfect squares. For the remainder of the proof, we suppose neither $-c$ nor d are perfect squares. In this case, the polynomials $x^2 + c$ and $x^2 - d$ define quadratic subfields of the splitting field of $f(x)$. By the Galois correspondence, the stem field of $x^2 + c$ corresponds to $H_c = A_6 \cap G$. Similarly, if K' is the normal closure of $g(x)$, then the subgroup fixing K' is the normal core, $\mathrm{Core}_G(H)$, of H in G (recall H is the subgroup fixing the stem field of $g(x)$). Thus the stem field of $x^2 - d$ corresponds to the unique subgroup H_d of G of index 2 (up to conjugation) that contains $\mathrm{Core}_G(H)$. It follows that $-cd$ is a perfect square if and only if $H_c = H_d$. Among the four remaining possible Galois groups, direct computation shows S_3 and S_4^- have $H_c = H_d$. The groups D_6 and $S_4 \times C_2$ have $H_c \neq H_d$. □

Based on Proposition 3.1, we can now determine when the Galois group of $f(x) = x^6 + ax^4 + bx^2 + c$ is either A_4 or S_4^+. If $-c$ is a perfect square, then the Galois group of $f(x)$ is A_4 if d is a perfect square and S_4^+ if d is not a perfect square.

To determine the Galois group in the remaining six cases, we introduce a degree six resolvent polynomial.

Proposition 3.2. *Let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be irreducible, K the stem field of f, and G the Galois group of f. Define $h(x)$ to be the following degree 6 polynomial:*

$$x^6 + 4ax^5 + (6a^2 - 2b)x^4 + (4a^3 - 2ab - 26c)x^3 + (a^4 + 2a^2b - 7b^2 - 24ac)x^2 + 2(a^2 - 3b)(ab - 9c)x + (a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2).$$

Suppose $h(x)$ is squarefree. Then $h(x)$ is reducible if and only if G is either C_6, S_3, or D_6.

Proof. Let H be the subgroup of S_6 generated by $(1,2)$, $(3,4)$, and $(3,4,5,6)$. Thus H is a group of order 48 isomorphic to $S_2 \times S_4$. Define a function $R(x)$ by

$$R(x^2) = \frac{\text{Resultant}_y(f(y), f(x-y))}{2^6 \cdot f(x/2)}.$$

Using a computer algebra system, we can show $R(x)$ is the product of x^3 and an even degree 12 polynomial. In fact, this degree 12 polynomial is $h(x^2)$. In the language of [5], $R(x)$ is the (absolute) resolvent polynomial corresponding to the multivariable function $T = x_1 + x_2$ that is stabilized by H. As shown in [11], the irreducible factors of $R(x)$ that occur with multiplicity one correspond to orbits of the action of G on the cosets G/H. By direct computation on the 8 possible groups, all have an orbit of length 12 except C_6, S_3, and D_6. It follows that if $h(x^2)$ is squarefree, it is reducible if and only if G is one of these three groups. Hence $h(x)$ is reducible if and only if G is either C_6, S_3, or D_6. □

We point out that Proposition 3.2 includes the assumption that $h(x)$ is squarefree. This is always possible to do by performing a suitable tschirnhaus transformation on f (see [5, Algorithm 3.6.4]) and then using Algorithm 3.4 to produce an even polynomial defining the same field as the transformed polynomial. The algorithm makes use of a stem field automorphism of order two. As described in the first paragraph of this section, such an automorphism always exists in the case of irreducible even polynomials.

Here is how to construct even polynomials. Suppose $f'(x)$ is an irreducible sextic polynomial obtained by performing a tschirnhaus transformation on the even sextic polynomial $f(x)$. Thus f' and f define the same stem field. If we factor f' over its stem field, the automorphisms of the stem field can be represented as the roots of the linear factors; i.e., they will be polynomials of degree strictly less than the degree of f'. One of the automorphisms will be the identity function, $\iota(x) = x$. Let $\sigma(x) \neq \iota(x)$ be an automorphism of order 2; that is, $\sigma(\sigma(x)) \equiv x \pmod{f'(x)}$. The characteristic polynomial of $x - \sigma(x)$ is the desired even polynomial, as we show in Proposition 3.3. Note, characteristic polynomials can be computed with resultants (see Algorithm 3.4).

Proposition 3.3. *Let $f(x)$ be an irreducible polynomial in $F[x]$ and K/F its stem field. Suppose there exists an automorphism $\sigma(x)$ of K/F of order 2. Let $\sigma(x)$ be represented as a root of a linear factor obtained by factoring f over K and let $\tilde{f}(x)$ be the characteristic polynomial of $x - \sigma(x)$. Then $\tilde{f}$ is an even polynomial. If $\tilde{f}$ is irreducible, it is a defining polynomial for K.*

Proof. Since $\sigma(x)$ is a root of f contained in K/F, it follows that $f(\sigma(x)) \equiv 0 \pmod{f(x)}$. Thus as a mapping from $\overline{F} \to \overline{F}$ that fixes F, σ permutes all roots of f (no root is left fixed since f is irreducible). Since σ has order 2, as a permutation

it is a product of two cycles; i.e., if $a, b \in \overline{F}$ are roots of f such that $\sigma(a) = b$, then $\sigma(b) = a$. Thus the function $\tau(x) = x - \sigma(x)$ naturally partitions the images of the roots of f into sets of size two. That is, for roots a and b of f, if $\sigma(a) = b$, then $\tau(a) = -\tau(b)$. Let $\tilde{f}(x)$ be the characteristic polynomial of τ so that $\tilde{f}(x) = \prod_i (x - \tau(r_i))$ where r_i are the roots of f. It follows that $\tilde{f}(x)$ is of the form $(x^2 - a_1) \cdots (x^2 - a_k)$ for some $a_i \in \overline{F}$. Thus $\tilde{f}(x)$ is even and is equal to a power of the minimal polynomial of τ. Since the minimal polynomial of τ defines a subfield of K, if $\tilde{f}$ is irreducible it is a defining polynomial for K. □

Proposition 3.3 shows an extension K/F can be defined by an even polynomial if its automorphism group has even order. If the stem field of $f(x)$ has an automorphism group of even order, Algorithm 3.4 produces an even polynomial defining the same stem field.

Algorithm 3.4. *Let $f(x) \in F[x]$ be an irreducible polynomial and let K/F be the stem field of f. Assume the automorphism group of K/F has even order. This algorithm produces an irreducible even polynomial $\tilde{f}(x) \in F[x]$ of the same degree as f that also defines K.*

1. *Factor f over K and let A be the collection of roots of linear factors of this factorization. Thus A is the collection of automorphisms of K/F.*
2. *Set B equal to the empty set. For each nonidentity automorphism $\sigma(x) \in A$, add $\sigma(x)$ to B if $\sigma(\sigma(x)) \equiv x \pmod{f(x)}$. Thus B is the collection of automorphisms of order 2.*
3. *For each $\sigma(x) \in B$:*
   (a) *Set $\tilde{f}(x) = \mathrm{Resultant}_y(x - (y - \sigma(y)), f(y))$. Thus $\tilde{f}(x)$ is the characteristic polynomial of $x - \sigma(x)$.*
   (b) *If $\tilde{f}$ is irreducible, return $\tilde{f}(x)$ and terminate.*
4. *If none of the functions $\tilde{f}$ are irreducible, let $f'(x)$ be a tschirnhaus transformation of $f(x)$ and K'/F the stem field of f'. Factor f' over K' and redefine A to be the collection of roots of linear factors of this factorization. Repeat steps (2)–(4).*

Note, Algorithm 3.4 requires an irreducible characteristic polynomial to terminate. In the case of reducible characteristic polynomials, Step (4) employs a tschirnhaus transformation. Only finitely many tschirnhaus transformations result in reducible characteristic polynomials (see for example [6] or [14]). In practice, we have found that zero or one such transformations are typically needed.

In Table 4, we summarize the information presented in Propositions 3.1 and 3.2. This table forms the basis for our algorithm for computing the Galois group of an irreducible even sextic polynomial.

Algorithm 3.5. *Let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be irreducible, d as in Proposition 3.1, and $h(x)$ as in Proposition 3.2. Assume $h(x)$ is squarefree (using Algorithm 3.4 if necessary). This algorithm returns the Galois group of $f(x)$.*

1. *If $-c$ is a perfect square in F, then*
   (a) *If d is a perfect square, return A_4 and terminate.*
   (b) *Otherwise return S_4^+ and terminate.*
2. *Else if d is a perfect square, then*
   (a) *If $h(x)$ is reducible, return C_6 and terminate.*
   (b) *Otherwise return $A_4 \times C_2$ and terminate.*

TABLE 4. For an irreducible even sextic polynomial $f(x) = x^6 + ax^4+bx^2+c$, let d be the discriminant of $g(x) = x^3+ax^2+bx+c$ and let $h(x)$ be defined as in Proposition 3.2. The table lists whether the values of $-c$, d, and $-cd$ are perfect squares and whether $h(x)$ is reducible, according to the Galois group G of f.

T	**G**	$-\mathbf{c}$ **= square**	**d = square**	$-\mathbf{cd}$ **= square**	$\mathbf{h(x)}$ **= reducible**
1	C_6	no	yes	no	yes
2	S_3	no	no	yes	yes
3	D_6	no	no	no	yes
4	A_4	yes	yes	yes	no
6	$A_4 \times C_2$	no	yes	no	no
7	S_4^+	yes	no	no	no
8	S_4^-	no	no	yes	no
11	$S_4 \times C_2$	no	no	no	no

(3) *Else if $-cd$ is a perfect square, then*
   (a) *If $h(x)$ is reducible, return S_3 and terminate.*
   (b) *Otherwise return S_4^- and terminate.*

(4) *Else if $h(x)$ is reducible, return D_6 and terminate. Otherwise return $S_4 \times C_2$ and terminate*

Two Examples. To illustrate Algorithm 3.5, we will use it to compute the Galois groups of the polynomials $f_1(x) = x^6 + 2$ and $f_2 = x^6 + 3$.

(1) For $f_1(x)$, we have $-c = -2$ which is not a square. Let $g(x) = x^3 + 2$. The discriminant d of g is $-108 = -2^2.3^3$, which is also not a perfect square. It follows that $-cd = 6^3$ is not a perfect square either. As defined in Proposition 3.2, $h(x) = x^6 - 52x^3 - 108 = (x^3 - 54)(x^3 + 2)$. Since $h(x)$ is reducible, the Galois group of f_1 is D_6.

(2) For $f_2(x) = x^6 + 3$, we have $-c = -3$, which is not a square. Let $g(x) = x^3 + 3$. The discriminant d of g_2 is $-243 = -3^5$, which is also not a square. However, $-cd = 3^6$ which is a perfect square. The polynomial $h(x) = x^6 - 78x^3 - 243 = (x^3 - 81)(x^3 + 3)$. Since $h(x)$ is reducible, the Galois group of f_2 is S_3.

4. One-Parameter Families

In this section, we determine one-parameter families of even sextic polynomials defined over the rational numbers for each of the 8 possible Galois groups.

Proposition 4.1. *The polynomials in Table 5 have the indicated Galois group over the rationals, except for values of t that result in reducible polynomials.*

Proof. Let $f(x) = x^6 + ax^4 + bx^2 + c$ be one of the polynomials in Table 5 and let $g(x) = x^3 + ax^2 + bx + c$. Let d be defined as in Proposition 3.1 and $h(x)$ as defined in Proposition 3.2. Using a computer algebra system, it can be verified that $h(x)$ is reducible (over $\mathbf{Q}(t)$) precisely in the cases C_6, S_3, and D_6. In particular, for C_6, $h(x)$ factors as $x^3+(2t^2-2t+14)x^2+(t^4-2t^3+15t^2-14t+49)x+(t^4-2t^3+15t^2-14t+49)$ times $x^3+(2t^2+2t+6)x^2+(t^4+2t^3+7t^2+2t+5)x+(t^4-2t^3-t^2+2t+1)$.

TABLE 5. One-parameter families of even sextic polynomials with specified Galois group over the rationals.

T	**G**	**Polynomials**
1	C_6	$x^6 + (t^2+5)x^4 + ((t-1)^2+5)x^2 + 1$
2	S_3	$x^6 + 3t^2$
3	D_6	$x^6 + 2t^2$
4	A_4	$x^6 - 3t^4x^2 - t^6$
6	$A_4 \times C_2$	$x^6 - 3t^2x^2 + t^3$
7	S_4^+	$x^6 + t^2x^4 - t^6$
8	S_4^-	$x^6 + (31t^2)^2x^2 + (31t^2)^3$
11	$S_4 \times C_2$	$x^6 + (2t^2)^2x^2 + (2t^2)^3$

TABLE 6. Discriminant data for polynomials listed in Table 5.

T	**G**	$\mathbf{-c}$	**d**	$\mathbf{-cd}$
1	C_6	-1	$[(t^2-t-1)(t^2-t+7)]^2$	$-[(t^2-t-1)(t^2-t+7)]^2$
2	S_3	$-3t^2$	$-3(3t)^4$	$(3t)^6$
3	D_6	$-2t^2$	$-3(6t^2)^2$	$(6t^2)^3$
4	A_4	t^6	$(3t^3)^4$	$(9t^9)^2$
6	$A_4 \times C_2$	$-t^3$	$(9t^3)^2$	$-t(3t^2)^4$
7	S_4^+	t^6	$-23t^{12}$	$-23t^{18}$
8	S_4^-	$-(31t^2)^3$	$-31(31t^2)^6$	$(31^5t^9)^2$
11	$S_4 \times C_2$	$-(2t^2)^3$	$-31(2t^2)^6$	$31(2t^2)^9$

For S_3, $h(x)$ factors as x^3+3t^2 times x^3+81t^2. And for D_6, $h(x)$ factors as x^3+2t^2 times x^3+54t^2.

It remains to analyze whether the following are perfect squares: $-c$, d, and $-cd$. But this is a straightforward computation. The results are listed in Table 6. Comparing the data in Table 6 and the reducibility of $h(x)$ with the data in Table 4, it follows that each of the polynomials in Table 5 has the indicated Galois group (for values of t that result in irreducible polynomials). □

5. Timing Comparisons

As we did with even quartic polynomials, we implemented Algorithm 3.5 in Pari/GP and compared its timings to the standard Galois group algorithms available in Magma and Pari/GP. The test polynomials we employed are also available from [1], and they were computed as described in Section 2. For each of these polynomials $x^6 + ax^4 + bx^2 + c$, Table 7 contains the number of digits of a, b, and c as well as the timings for Algorithm 3.5, Magma, and Pari/GP. All timings are in milliseconds.

As Table 7 shows, Algorithm 3.5 is significantly faster than the standard Galois group algorithms implemented in Magma and Pari/GP.

References

1. Chad Awtrey, *Examples of even polynomials*, Available from: `http://facstaff.elon.edu/cawtrey/evenpols.html`.

TABLE 7. A comparison of run times of Algorithm 3.5 with the standard Galois group algorithms implemented in Magma and Pari/GP. Each row corresponds to a polynomial $f(x) = x^6 + ax^4 + bx^2 + c$ whose Galois group is specified in column **G**. Columns **a**, **b**, and **c** give the number of digits of a, b, and c, respectively. Run times are given in milliseconds.

T	**G**	**a**	**b**	**c**	**Alg. 3.5**	**Magma**	**Pari/GP**
1	C_6	1070	1270	1330	8	340	2153
2	S_3	513	1025	1519	4	450	746
3	D_6	591	1181	1770	5	250	902
4	A_4	1177	2329	3316	6	1330	1665
6	$A_4 \times C_2$	722	1413	1942	1	460	1399
7	S_4^+	1147	2294	3394	4	1330	1949
8	S_4^-	1513	3026	4475	18	1380	3071
11	$S_4 \times C_2$	1205	2408	3549	11	830	2545

2. Chad Awtrey, Nakhila Mistry, and Nicole Soltz, *Centralizers of transitive permutation groups and applications to Galois theory*, Missouri J. Math. Sci. **27** (2015), no. 1, 16–32. MR 3431112
3. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
4. Gregory Butler and John McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911. MR 695893 (84f:20005)
5. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206 (94i:11105)
6. John D. Dixon, *Computing subfields in algebraic number fields*, J. Austral. Math. Soc. Ser. A **49** (1990), no. 3, 434–448. MR 1074513
7. Andreas-Stephan Elsenhans, *Improved methods for the construction of relative invariants for permutation groups*, J. Symbolic Comput. **79** (2017), no. part 2, 211–231. MR 3550907
8. Claus Fieker and Jürgen Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17** (2014), no. 1, 141–158. MR 3230862
9. Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), no. 2, 133–137. MR 992075 (90i:12006)
10. PARI Group, The, *PARI/GP – Computational Number Theory, version 2.5.3*, 2013, available from `http://pari.math.u-bordeaux.fr/`.
11. Leonard Soicher, *The computation of Galois groups*, Master's thesis, Concordia University, Montreal, 1981.
12. Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)
13. Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996. MR 0327712 (48 #6054)
14. Barry Trager, *Algebraic factoring and rational function integration*, Proceedings of the third ACM symposium on Symbolic and algebraic computation (Yorktown Heights, NY), ACM, 1976, pp. 219–226.
15. Mark van Hoeij, Jürgen Klüners, and Andrew Novocin, *Generating subfields*, J. Symbolic Comput. **52** (2013), 17–34. MR 3018126

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244
E-mail address: cawtrey@elon.edu

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244
E-mail address: pjakes@elon.edu