The computation of Galois groups over function fields

Thomas W. Mattman
Department of Mathematics and Statistics
McGill University, Montréal
December 1992

A Thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements of the degree of M.Sc.

Abstract

Practical computational techniques are described to determine the Galois group of a degree 8 polynomial over a function field of the form $\mathbf{Q}(t_1, \ldots, t_r)$. Each transitive permutation group of degree 8 is realized as a Galois group over the rationals. The techniques of Soicher and McKay [SM] for rational polynomials of degree less than 8 are also extended to function fields. Timing and efficiency of a MAPLE V implementation are discussed.

Résumé

Nous décrivons des techniques pratiques de calcul pour la détermination du groupe de Galois sur un corps de fonctions de la forme $\mathbf{Q}(t_1, \ldots, t_r)$ d'un polynome de degré 8. Chaque groupe transitif de permutations de degré 8 est réalisé comme un groupe de Galois sur les rationnels. Les techniques de Soicher et McKay [SM] pour les polynomes rationnels de degré moins que 8 sont aussi généralisées aux corps de fonctions. L'éfficacité et le problème du temps requis de l'utilisation de MAPLE V sont discutés.

Acknowledgements

I would like to thank my supervisor, Prof. J. McKay, for his guidance throughout the preparation of this thesis which is in large part the consequence of his many excellent suggestions. I have much appreciated his patient encouragement and his insistence on rigour is the source of any quality this work may have.

I am indebted to G. Butler, D. Ford, L. Kwok-On, C. Lam, and G. Smith for many fruitful discussions and the use of their programs and results.

To my family I say thank you for your many years of support and love.

This research was funded by the Natural Sciences and Engineering Research Council of Canada.

Maybe it has become too hard for us unless we are given some outside help, be it even by such devilish devices as high speed computing machines.

H Weyl

Contents

Abstract

Acknowledgements

Table of Contents 1

List Of Tables 3

Notation 4

1 Introduction 6

1.1 History 6

1.2 The Fundamental Theorem of Galois Theory 7

1.3 The Galois Group of a Polynomial 8

1.4 Imprimitive Groups 10

1.5 Resolvent Polynomials 12

2 The Problem in Degree 8 17

2.1 History 17

2.1.1 Stauduhar's Method 17

2.1.2 The Method of Soicher and McKay 18

2.2 Distinguishing Groups of Degree 8 19

2.2.1 Discriminant and Shapes 19

2.2.2 Imprimitivity 21

2.2.3 Orbit-Length Partitions 23

2.2.4 Factorization Over $k(\sqrt{\Delta})$ 25

2.2.5 Galois Groups of Resolvent Factors 27

3 An Implementation of the Degree 8 Algorithm 33

3.1 Discriminant and Shapes 33

3.2 Construction of Resolvents 35

3.3 Factorization over $k(\sqrt{\Delta})$ 37

3.4 Distinguishing G_{192a}, G_{192b} and G_{384} 37

4 Avenues for Further Exploration 39

4.1 Improving Polynomial Factorization 39

4.2 Improving the Imprimitivity Algorithm 41

4.3 Small Degree Resolvents 46

A Rational Polynomials With Given Galois Groups 48

A.1 Polynomials of the form $f(x^2)$ 53

A.2 Additional Remarks on the Derivation of the Polynomials 54

A.3 Generalizations of Soicher's Method for $(2^3 \, L(3,2))^4$ 58

B Polynomials over $\mathbf{Q}(t)$ 64

C Distinguishing G_{288}^+ from G_{576}^+ 67

D Tables of Degree 8 Transitive Groups 70

References 80

List of Tables

1 Distinguishing groups by testing irreducibility over $k(\sqrt{\Delta})$. 26

2 Distinguishing groups using Galois groups of resolvent factors. 28

3 Distinguishing degree 8 Galois groups - $G \subseteq \mathcal{A}_8$ 30

4 Distinguishing degree 8 Galois groups - $G \not\subseteq \mathcal{A}_8$ 32

5 Statistics of CPU usage by MAPLE V implementation 40

6 Rational polynomials with degree 8 Galois groups - $G \subseteq \mathcal{A}_8$ 49

7 Rational polynomials with degree 8 Galois groups - $G \not\subseteq \mathcal{A}_8$ 51

8 Polynomials over $\mathbf{Q}(t)$ with selected Galois groups 65

9 Transitive groups of degree 8 72

10 Group generators 75

11 Shapes occurring in each group 76

12 Orbit length partitions of sets and sequences under G 77

Notation

$k(a_1, \ldots, a_n)$	The field k extended by the elements $a_1, \ldots, a_n$
$k[x]$	The ring of polynomials over the field (or ring) k
$\mathcal{G}(K/k)$	The Galois group of K over k. See Definition 1.2.6
K^H	The subfield of K fixed by H. See page 8.
G/H	The quotient of the group G by its normal subgroup H
$\mathcal{G}al_k(f)$	The Galois group of f over k. See Definition 1.3.1
$\mathcal{S}_n$	The symmetric group on n letters
$\mathcal{A}_n$	The alternating group on n letters
$G^{\sigma}_{n\alpha}$	Standard notation for the transitive degree 8 groups. If σ = 1, the group has only even permutations. The 'n' indicates the order of the group. If there are several groups of the same parity and order, they are distinguished as α = a,b,c,... See Appendix D for more details
$char(k)$	The characteristic of the field k.
Δ	The discriminant of a polynomial. See Definition 1.3.1
$\mathbf{Q}$	The field of rationals
$\mathbf{Q}(t_1, \ldots, t_r)$	$\mathbf{Q}$ extended by the transcendental elements $t_1, \ldots, t_r$
$\mathbf{Z}$	The ring of integers.
$R[t_1, \ldots, t_r]$	The ring of polynomials in r indeterminates over the ring R
UFD	Unique factorization domain.
∂f	The degree of the polynomial f.
$g \circ h$	The composition $g(h(x))$ of the polynomials g and h
$f \mid g \circ h$	The polynomial f divides the composition of the polynomials g and h
$k[\alpha]$	Ring generated over k by α.
F^{σ}, $F^{\mathcal{S}_n}$	See page 13.
$stab_G(F)$	The stabilizer of F in G. The group G is omitted if it is $\mathcal{S}_n$ where

	$F \subset k[x_1, \ldots, x_n]$. See page 13.
$R(F, f)$	The resolvent polynomial associated with F and f. See Definition 1.5.4.
$\|S\|$	The cardinal of the set S.
$k(x)$	The field k extended by the transcendental element x.
$T_\phi f$	The Tschirnhaus transformation of f by ϕ. See Definition 1.5.6.
$\lfloor x \rfloor$	The greatest integer less than or equal to x.
$f\|_{t=a}$	The specialization of the polynomial f under the substitution $t = a$.
$P_k(f)$	The degree k power-sum symmetric function of f.
$\mathbf{Z}_n$, p^k, V_4, D_n, Q_8	See page 70.
$A \cdot B$, AB	See page 70.
$\mathbf{F}_p$	The finite field of p elements.
ζ_k	A primitive kth root of unity.
$spl(f)$	The splitting field of the polynomial f.
$rts(f)$	The set of roots of the polynomial f.
$<l, m\|n>$, $(l, m\|n, k)$	See page 70.
$A \circ B$, $A \triangle B$, $A \wr B$	See page 70.
$Hol(A)$, $Syl_p(A)$	See page 71.

1 Introduction

1.1 History. The original definition of the Galois group leads to a means of computing it and this has been pointed out by several authors (see for example [vW, p.189]). But, as Galois himself said [BA],

> Si maintenant vous me donnez une équation que vous aurez choisie à votre gré, et que vous desiriez connaître si elle est ou non resoluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot les calculs sont impraticables

The technique involves factoring a polynomial of degree $n!$ in order to find the Galois group of a degree n polynomial f. Hence it is feasible for only the smallest values of n.

However, with the advent of high speed digital computers, powerful new methods have been developed to quickly determine the Galois group of higher degree polynomials. In 1969, Stauduhar [St1] presented an algorithm for rational polynomials of degree 8 and less. This algorithm has recently been extended to degree 9 [O]. A decade later, Soicher and McKay [S1, SM] presented a different approach which was implemented for polynomials of degree 7 and less.

The principal advantage of the method of Soicher and McKay is that it is easily generalized to polynomials over fields other than the rationals. In this thesis we realize this potential by demonstrating an extension of the technique to function fields of the form $\mathbb{Q}(t_1, \ldots, t_r)$ (where $t_1, \ldots, t_r$ are transcendental over $\mathbb{Q}$) and polynomials of degree 8 and less.

Following an introductory section outlining the theory required, Section 2 shows how the ideas of Soicher and McKay may be extended to the degree 8 case. In Section 3 we give details of an implementation of the algorithm in the MAPLE V [CGG]

language. This is followed by an analysis of the program with timing results in Section 4. The appendices include, in Appendix A, a list of polynomials realizing each transitive degree 8 group as a Galois group over the rationals and, in Appendix B, a list of polynomials over $\mathbf{Q}(t)$ of degrees 3 through 8 with selected Galois groups.

1.2 The Fundamental Theorem of Galois Theory. We begin with some definitions leading to the fundamental theorem of Galois theory. Details can be found in any standard algebra text such as [L, pp.263-313]. In the following k is a field, K an extension field of k and f a non-constant polynomial in $k[x]$.

Definition 1.2.1 *The field K is a* **splitting field** *of f over k if f splits (into linear factors) in K and K is minimal with respect to this property. If S is a set of polynomials in $k[x]$ then K is a splitting field for S if each $f \in S$ splits in K and K is minimal.*

Since a splitting field is unique up to isomorphism, we often refer to *the* splitting field.

Definition 1.2.2 *The polynomial f is* **separable** *over k if it has distinct roots in the splitting field. The element α of K is* **separable** *over k if it is the root of a separable polynomial in $k[x]$. If every α in K is separable then K is a* **separable extension** *of k.*

Definition 1.2.3 *An element α of K is* **primitive** *if $K = k(\alpha)$.*

Proposition 1.2.4 *If K is a separable extension of k, then K has a primitive element.*

Definition 1.2.5 *The extension K is* **normal** *over k if it is the splitting field of a set of polynomials in $k[x]$.*

Definition 1.2.6 *The extension K is* **Galois** *over k if it is normal and separable. In this case, $\mathcal{G}(K/k)$, the* **Galois group** *of K over k, is the group of field automorphisms of K fixing k.*

Notation: Let H be a subgroup of $\mathcal{G}(K/k)$. We denote the subfield of K fixed by H by K^H.

Theorem 1.2.7 (The Fundamental Theorem of Galois Theory) *Let K be a Galois extension of k. There is a bijection between the set of subfields E of K containing k, and the set of subgroups H of $\mathcal{G}(K/k)$, given by $E \mapsto K^H$. The field E is Galois over k if and only H is normal in G, and if that is the case, then the map $\sigma \mapsto \sigma|_E$ induces an isomorphism of G/H onto the Galois group of E over k*

1.3 The Galois Group of a Polynomial. We define the Galois group of a polynomial and introduce some invariants of the group easily derived from the polynomial.

Definition 1.3.1 *If $f \in k[x]$ is separable, then the splitting field K of f is a Galois extension. In this case we call $\mathcal{G}(K/k)$ the Galois group of f over k and denote it by $\mathcal{G}\mathrm{al}_k(f)$.*

We will generally assume that f is irreducible and $char(k) = 0$ so that f is separable. Let $\sigma \in \mathcal{G}al_k(f)$. If α is a root of f, then, since σ is a field homomorphism, we see that $\sigma(\alpha)$ is again a root of f. But since σ is also a monomorphism it permutes the roots of f. Hence $\mathcal{G}al_k(f)$ acts on the roots $\alpha_1, \ldots, \alpha_n$ of f by permutation.

In this way $\mathcal{G}al_k(f)$ is a subgroup of $\mathcal{S}_n$, the symmetric group on n letters However, this injection depends on the labelling of the roots; relabelling the roots amounts to conjugation by an element of $\mathcal{S}_n$.

Definition 1.3.2 *Groups G_1, G_2 in $\mathcal{S}_n$ are* **permutation isomorphic** *if $G_1 = \alpha^{-1}G_2\alpha$ for some $\alpha \in \mathcal{S}_n$.*

Here, we identify the group only up to permutation isomorphism. This equivalence is stronger than abstract group isomorphism; isomorphic transitive subgroups of $\mathcal{S}_n$ will be permutation isomorphic only if the isomorphism is realizable by a permutation in $\mathcal{S}_n$. For example the groups G^+_{32b} and G_{32d} (see Table 9) are both isomorphic to $< x, y | x^4, y^2, (xy)^4, x^2yxyx^2yx^3y >$ in $\mathcal{S}_8$. However, since no permutation isomorphism can change the parity of a group, they are not permutation isomorphic.

Proposition 1.3.3 *The polynomial f in $k[x]$ is irreducible iff $\mathcal{G}\mathrm{al}_k(f)$ is transitive.*

Definition 1.3.4 *Let k be a field with* $\mathrm{char}(k) \neq 2$ *and $f \in k[x]$ of degree n with roots $\alpha_1, \ldots, \alpha_n$ in the splitting field K. The* **discriminant** *of f is*

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in k.$$

Proposition 1.3.5 *Let k, f, K and Δ be as above. Then Δ is a square in k iff $\mathcal{G}\mathrm{al}_k(f) \subseteq \mathcal{A}_n$.*

Although the theory developed to this point applies generally to any field k, we will assume henceforth that k is of the form $\mathbf{Q}(t_1, \ldots, t_r)$ (including the case $k = \mathbf{Q}$) whence k is the quotient field of the unique factorization domain (UFD) $D = \mathbf{Z}[t_1, \ldots, t_r]$. We can relate factorization modulo maximal ideals in D to cycle shapes in $\mathcal{G}al(f)$ (using the monomorphism $\mathcal{G}al(f) \hookrightarrow \mathcal{S}_n$).

Definition 1.3.6 *The* **shape** *of σ in $\mathcal{S}_n$ is the partition of n determined by the lengths of its disjoint cyclic factors.*

Notation: We denote the degree of the polynomial f by ∂f.

Proposition 1.3.7 *Let $\overline{k}$ be the quotient field of $\overline{D} = D/\mathbf{p}$ where $\mathbf{p}$ is a maximal ideal in D and suppose $\overline{f} = f \bmod \mathbf{p}$ has no repeated roots. Then $\mathcal{G}\mathrm{al}_{\overline{k}}(\overline{f})$ is a subgroup of $\mathcal{G}\mathrm{al}_k(f)$.*

Corollary 1.3.8 *The partition of ∂f induced by the degrees of the irreducible factors of $\overline{f}$ is the shape of an element of $\mathcal{G}\mathrm{al}_k(f)$.*

Proof. See [vW, pp.190-191]. □

In case $D = \mathbf{Z}$, we have the following result (see [LO]):

Theorem 1.3.9 (Čebotarev Density Theorem) *Let π be a partition of n. Then as $l \to \infty$, the proportion of occurrences of π as the factor type of $f \bmod p_i$, $i = 1, \ldots, l$, ($p_1, \ldots, p_l$ distinct primes) tends to the proportion of permutations of that shape in $\mathcal{G}\mathrm{al}_{\mathbf{Q}}(f)$.*

1.4 Imprimitive Groups. A reference for the material in this section is [W, pp.11-15].

Definition 1.4.1 *Let G be a transitive permutation group on Ω, $|\Omega| = n$. The group G is* **imprimitive** *if it stabilizes a partition of Ω into l sets of size m (i.e. $n = lm$) with $1 < m < n$. In this case the stabilized sets are called* **blocks** *(of imprimitivity).*

Proposition 1.4.2 *Let $f \in k[x]$ be an irreducible, separable polynomial of degree n. Then $\mathcal{G}\mathrm{al}_k(f)$ is imprimitive iff there exist polynomials $g, h \in k[x]$, with $\partial g, \partial h < \partial f$ and g irreducible, such that $f \mid goh$. In this case, $\mathcal{G}\mathrm{al}_k(f)$ has a decomposition into ∂g blocks.*

We shall call such a polynomial f **imprimitive.**

Proof Let K be the splitting field of f and let the roots of f be $\alpha_1, \ldots, \alpha_n$. Let $G = Gal_k(f)$.

Suppose first that G is imprimitive with l blocks of size m. Let B be the block containing α_1. Let G_{α_1} be the stabilizer of α_1 in G and G_B the setwise stabilizer of B. By the fundamental theorem of Galois theory,

$$k \subseteq K^{G_B} \subseteq K^{G_{\alpha_1}} \subseteq K.$$

Evidently,

$$K^{G_{\alpha_1}} = k(\alpha_1) = k[\alpha_1].$$

Now, K^{G_B} is separable over k so it has a primitive element β such that $K^{G_B} = k(\beta)$ Since $\beta \in k[\alpha_1]$, we see that $\beta = h(\alpha_1)$ for some $h \in k[x]$. Let $g \in k[x]$ be the minimal polynomial of β over k. Then $\partial g = [k(\beta) : k] = |G : G_B| = n/m = l$ and since $goh(\alpha_1) = 0$, we have $f \mid goh$ as required.

Conversely, suppose $f \mid goh$ where $\partial g = l$. Let $\beta_1, \ldots, \beta_l$ be the roots of g. Let

$$B_i = \{\alpha_j | h(\alpha_j) = \beta_i\}.$$

Since the β_i are all roots of the same irreducible polynomial, any $\sigma \in G$ acts on the β_i by permutation. Suppose $\alpha_{j_1}, \alpha_{j_2} \in B_{i_1}$ and $\sigma(\beta_{i_1}) = \beta_{i_2}$ for some $\sigma \in G$. Then

$$h(\sigma(\alpha_{j_1})) = h(\sigma(\alpha_{j_2})) = \beta_{i_2}$$

and $\sigma(\alpha_{j_1}), \sigma(\alpha_{j_2}) \in B_{i_2}$. Thus G stabilizes the partition of the α_j into l sets B_i and is imprimitive. □

Casperson and McKay [CM2] have recently described a practical algorithm for finding decompositions $f \mid goh$ when $f \in \mathbf{Q}[x]$. Let f have degree $\partial f = n$ with roots $\alpha_1, \ldots, \alpha_n$. Let

$$h = \sum_{j=0}^{n-1} c_j x^j.$$

If $\alpha_{i_1}, \alpha_{i_2}$ are in the same block, then $h(\alpha_{i_1}) = h(\alpha_{i_2})$ whence

$$\sum_{j=0}^{n-1} c_j(\alpha_{i_1}^j - \alpha_{i_2}^j) = 0.$$

So, using approximations to the roots α_i of f, we can use a $\mathbf{Z}$ linear dependence algorithm such as the LLL [LLL] algorithm to determine the coefficients c_j, $j \neq 0$ of h. (It should be noted however that since we have no bounds for the coefficients of h, we do not know how accurate the root approximations must be. For this reason, the algorithm may miss decompositions.)

Once h is known, there are several ways of determining g. We can use a $\mathbf{Z}$ linear dependence algorithm to find g as the minimal polynomial for $h(\alpha)$ where α is a root of f. Another method is to form

$$r(y) = resultant_x(y - h(x), f(x)).$$

(The subscript x indicates that x is eliminated.) Then $g = r/(gcd(r, r'))$.

It appears however that the best method for constructing $g(y)$ is by generating equations of the form

$$y^k \equiv (h(x))^k \bmod f, \quad k = 0, \ldots, M$$

until $\mathbf{Z}$-linear dependence occurs. At most M such equations are necessary where M is the greatest proper divisor of n.

So the algorithm proceeds as follows. Calculate approximations to the roots of f. Fix one root α_1. For each distinct pair α_1, α_i construct h and g and test if $f \mid g \circ h$; if so, f is imprimitive and α_1 and α_i are in the same block. For this pair, then, we have found the polynomials h and g.

1.5 Resolvent Polynomials. A reference for the material in this section is [MD] We begin with the Fundamental Theorem of Symmetric Polynomials. In the follow

ing, A is a commutative ring and $t_1, \ldots, t_n$ algebraically independent elements over A

Definition 1.5.1 *Let* $F \in A[t_1, \ldots, t_n][x]$ *be defined as*

$$F = \prod_{i=1}^{n}(x - t_i) = \sum_{j=0}^{n}(-1)^j s_j x^{n-j}.$$

Each s_j *is a polynomial of total degree* j *in* $t_1, \ldots, t_n$. *These are the* **elementary symmetric polynomials** *of* $t_1, \ldots, t_n$.

Note that, up to sign, the elementary symmetric polynomials are just the coefficients of F

Definition 1.5.2 *The polynomial* $f \in A[t_1, \ldots, t_n]$ *is* **symmetric** *if*

$$f(t_1, \ldots, t_n) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$$

for each $\sigma \in \mathcal{S}_n$.

Theorem 1.5.3 (Fundamental Theorem of Symmetric Polynomials) *Let* $f \in A[t_1, \ldots, t_n]$ *be symmetric. Then there exists a polynomial* $g \in A[t_1, \ldots, t_n]$ *such that* $f = g(s_1, \ldots, s_n)$ *where the* s_i *are the elementary symmetric polynomials.*

The resolvent polynomial is a very useful tool in the determination of Galois groups. We define it and give some of its properties. In the following, let $f \in k[x]$ be a polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ over the field k.

Notation: For $F \in k[x_1, \ldots, x_n]$ and $\sigma \in \mathcal{S}_n$, we denote $F(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ by F^σ and $\{F^\sigma | \sigma \in \mathcal{S}_n\}$ by $F^{\mathcal{S}_n}$.

Notation: Let $H = stab(F)$ be the stabilizer in $\mathcal{S}_n$ of F. (That is, H is the largest subgroup of $\mathcal{S}_n$ fixing F. Note that any subgroup of H will also fix F.) For

$\sigma \in \mathcal{S}_n$, $H\sigma = \{h\sigma | h \in H\}$ is a right coset of H in $\mathcal{S}_n$ and σ is a representative for $H\sigma$. (We use the permutation multiplication convention consistent with the equation $(b,c)(a,b) = (a,b,c)$.)

Definition 1.5.4 *For $F \in k[x_1, \ldots, x_n]$, let $\sigma_1, \ldots, \sigma_m$ be a set of right coset representatives of* stab(F) *in $\mathcal{S}_n$. The* **resolvent polynomial** *$R(F, f)$ associated with F and f is defined by*

$$R(F,f) = \prod_{i=1}^{m} (x - F^{\sigma_i}(\alpha_1, \ldots, \alpha_n)).$$

Since the σ_i represent different cosets, we know that if $i \neq j$ then $F^{\sigma_i} \neq F^{\sigma_j}$. However, it may turn out that $F^{\sigma_i}(\alpha_1, \ldots, \alpha_n) = F^{\sigma_j}(\alpha_1, \ldots, \alpha_n)$. We will say that $R(F,f)$ has distinct zeroes in case $i \neq j$ implies $F^{\sigma_i}(\alpha_1, \ldots, \alpha_n) \neq F^{\sigma_j}(\alpha_1, \ldots, \alpha_n)$ (whence $R(F,f)$ has no repeated roots).

If k is the quotient field of the UFD D, then, by clearing denominators, we may assume $f \in D[x]$. The coefficients of the resolvent polynomial $R(F,f)$ are symmetric functions in the roots of f. Hence, by the fundamental theorem of symmetric functions, they are polynomials in the coefficients of f. Thus $R(F,f) \subset D[x]$.

Definition 1.5.5 *For a group G acting on a finite set S, we call the partition of $|S|$ induced by the lengths of the orbits of S under G the* **orbit-length partition** *of S under G.*

Notation: Any element γ of $k(x)$ may be written uniquely as g_n/g_d where g_n, g_d are in $k[x]$, g_n is monic and g_n, g_d have no common factors. We will denote g_n by $N(\gamma)$.

We shall define the Tschirnhaus transformations as follows (see [B, pp 171 178] for a more standard exposition):

Definition 1.5.6 *If $\phi, \psi \in k(x)$ are inverses, (i.e. $\phi \circ \psi = \psi \circ \phi \equiv 1$) then $T_\phi f = N(f \circ \phi)$ is a* **Tschirnhaus transformation** *of f.*

Proposition 1.5.7 *The Galois group is invariant under a Tschirnhaus transformation, if $T_\phi f$ is a Tschirnhaus transformation of f, then $\mathcal{G}\mathrm{al}_k(T_\phi f) = \mathcal{G}\mathrm{al}_k(f)$.*

In this way, Tschirnhaus transformations induce a partition of the set of polynomials into Galois equivalence classes.

Proposition 1.5.8 *Suppose $R(F, f)$ has distinct zeroes. The orbit-length partition of $F^{\mathcal{S}_n}$ under $\mathcal{G}\mathrm{al}(f)$ is the same as the partition of $\partial R(F, f)$ induced by the degrees of the irreducible factors of $R(F, f)$.*

Thus the factorization of resolvent polynomials is determined by $\mathcal{G}al_k(f)$. The factorization of f over $k(\sqrt{\Delta})$ when Δ is not a square is also an invariant of the Galois group:

Proposition 1.5.9 *Let g be an irreducible factor of a resolvent polynomial $R(F, f)$ such that $F_j(\underline{\alpha})$ (where $\underline{\alpha} = \alpha_1, \ldots, \alpha_n$)) is a zero of g for some $F_j \in F^{\mathcal{S}_n}$. The following are equivalent:*

1. $\mathrm{stab}_{\mathcal{G}\mathrm{al}_k(f)}(F_j)$ *is a subgroup of $\mathcal{A}_n$.*
2. $k(F_j(\underline{\alpha}))$ *contains $k(\sqrt{\Delta})$.*
3. *g is reducible in $k(\sqrt{\Delta})[x]$.*

Proof. The equivalence of 1 and 2 follows immediately from the fundamental theorem of Galois theory and the observation that

$$k(F_j(\underline{\alpha})) = K^{stab_{\mathcal{G}al_k(f)}(F_j)}$$

and

$$k(\sqrt{\Delta}) = K^{Gal_k(f) \bigcap A_n}$$

where K is the splitting field of f.

Let h be the minimal polynomial of $F_j(\underline{\alpha})$ over $k(\sqrt{\Delta})$.

$$\begin{aligned}
& g \text{ is irreducible over } k(\sqrt{\Delta}) \\
\Leftrightarrow\ & g = h \\
\Leftrightarrow\ & [k(F_j(\underline{\alpha})) : k] = [k(F_j(\underline{\alpha}), \sqrt{\Delta}) : k(\sqrt{\Delta})] \\
\Leftrightarrow\ & [k(F_j(\underline{\alpha}), \sqrt{\Delta}) : k(F_j(\underline{\alpha}))] = [k(\sqrt{\Delta}) : k] = 2 \\
\Leftrightarrow\ & k(\sqrt{\Delta}) \not\subseteq k(F_j(\underline{\alpha}))
\end{aligned}$$

Hence 2 and 3 are also equivalent. □

The Galois groups of factors of resolvent polynomials are also invariants of $Gal_k(f)$.

Proposition 1.5.10 *Let g be an irreducible factor of a resolvent polynomial $R(F, f)$ with roots $F_1(\underline{\alpha}), \ldots, F_m(\underline{\alpha})$ where $F_i \in F^{S_n}$, $1 \leq i \leq m$, are distinct and $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Then $\mathrm{Gal}_k(g) \subseteq S_m$ is a representation of $\mathrm{Gal}_k(f)$ as a permutation group acting on $\{F_1, \ldots, F_m\}$. To each $\sigma \in \mathrm{Gal}_k(g)$ there corresponds $\sigma^* \in \mathrm{Gal}_k(f)$ such that the action of σ on the F_j is that induced by σ^* on the α_i.*

Proof. This is an immediate consequence of the fundamental theorem of Galois theory. Note that $Gal_k(g)$ is a quotient of $Gal_k(f)$. □

2 The Problem in Degree 8

2.1 History. At present there are two basic approaches to computer aided computation of Galois groups. We briefly review these and discuss their relative merits.

2.1.1 Stauduhar's Method. Stauduhar's method [St1, St2] relies on the idea of a polynomial belonging to a group (see page 13 for a definition of $stab(F)$):

Definition 2.1.1 *We say that* $F \in k[x_1, \ldots, x_n]$ **belongs** *to* $G = \mathrm{stab}(F)$.

We will call a sequence

$$S_n = G_0 \supset G_1 \supset G_2 \supset, \ldots, \supset G_m$$

of subgroups of S_n a *chain* if G_{i+1} is a maximal transitive subgroup of G_i for each $i = 0, \ldots, m-1$. A monic, irreducible polynomial f with integral coefficients determines a chain as follows.

Suppose we know that $Gal(f) \subseteq G_i$ (initially $G_i = S_n$) with respect to some ordering $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of the roots of f. Let H be a maximal transitive subgroup of G_i and $\sigma_1, \ldots, \sigma_k$ a set of right coset representatives for H in G_i (see page 14). Let

$$R_H(F, f) = \prod_{i=1}^{k} (x - F^{\sigma_i}(\underline{\alpha}))$$

be a factor of $R(F, f)$ where F belongs to H.

Proposition 2.1.2 *$R_H(F, f)$ has a linear factor in $\mathbf{Z}[x]$ iff $Gal(f)$ is contained in a conjugate of H.*

So for each maximal transitive subgroup H of G_1, we test $R_H(F, f)$ for a linear factor. If it has one, then $G_{i+1} = H$ and the factor determines a new ordering of the roots such that $Gal(f) \subseteq H$. If none of the $R_H(F, f)$ have a linear factor the chain terminates at G_i. In this way, we extend the chain until one of the two things happens.

1. We find that G_i is a minimal transitive group. In this case the chain terminates with $G_m = G_i$.

2. For all maximal transitive subgroups H of G_i, $R_H(F, f)$ has no linear factor. In this case the chain terminates with $G_m = G_i$.

Note that if $G_0 \supset, \ldots, \supset G_m$ is the chain associated with f in this way, then $\mathcal{G}al(f) = G_m$. So in Stauduhar's method, given a polynomial f we determine its chain and return the tail element of the chain as the Galois group. For each degree n, we need to store a set of chains passing through each transitive subgroup of S_n, and, for each subgroup in a chain, a polynomial belonging to the subgroup and coset representatives of the subgroup in its predecessor in the chain must be tabulated.

The polynomials $R_H(F, f)$ are constructed using high-precision approximations to the roots of f. We know that $R_H(F, f)$ has integer coefficients since the roots are ordered such that $\mathcal{G}al(f) \subseteq H$ (see [St2]). So to construct $R_H(F, f)$ we approximate the roots to sufficient precision that the resulting error in the absolute value of the coefficients of $R_H(F, f)$ is less than 0.5. This required precision can be very large. For example, Stauduhar [St2] reports calculations using 192 bit (≈ 60 digit) approximations to the roots of a degree 6 polynomial. In [CM1] it is stated that calculations for certain degree 11 and 12 polynomials require thousands of digits of precision.

Since Stauduhar's method relies on calculations using approximations to the roots of f, it is not easily generalized to fields other than the rationals. In particular, it cannot be extended to function fields $\mathbf{Q}(t_1, \ldots, t_r)$. On the other hand, the technique is very fast over $\mathbf{Q}$ in comparison with that of Soicher and McKay.

2.1.2 The Method of Soicher and McKay. The algorithm of Soicher and McKay [S1, SM] uses shapes (see Section 1.3) to indicate what the Galois group

may be, followed by the use of resolvent polynomials to fix it. Rather than test for a linear factor, as was the case in Stauduhar's method, the resolvents are completely factored so that the resultant orbit-length partition (see Proposition 1.5.8) may be brought to full use. In this way, only a few resolvents are required to distinguish all the groups of a given degree.

Moreover, the resolvents are relatively simple. For a degree n polynomial we make use of the orbit-length partition on r-sets ($r = 1, 2, \ldots, \lfloor n/2 \rfloor$) and 2-sequences. In these cases, the polynomials relating the coefficients of the resolvent to those of the initial polynomial are easily derived. (See [EFM] for example.) Hence, there is no need to work with approximations to the roots of the polynomials. For this reason, the method is easy to generalize to fields other than the rationals. The storage requirements of this technique are minimal. For each group we record its shapes and the orbit-length partitions of r-sets and 2-sequences under its action.

2.2 Distinguishing Groups of Degree 8. The method is essentially the same as that outlined by Soicher and McKay [SM] for the groups of degree up to 7. Let f be an irreducible polynomial in $k[x]$ of degree 8 where $k = \mathbf{Q}(t_1, \ldots, t_r)$. To determine the Galois group it suffices to distinguish it among the 50 transitive subgroups of $\mathcal{S}_8$ (see [BM]). So we begin with a list of 50 candidates for the Galois group. At each stage we make a calculation based on f which yields some further property of the Galois group. Those groups which do not have the requisite property are removed from the list. This continues until there is only one candidate left which must therefore be the Galois group.

2.2.1 Discriminant and Shapes. We first determine whether $\mathcal{G}al_k(f)$ is even by calculating the discriminant. Since k is the quotient of the UFD $\mathbf{Z}[t_1, \ldots, t_r]$, we can look for cycle shapes by factoring f modulo maximal ideals. For each shape

found in this manner, we may eliminate all candidate groups which do not exhibit this shape. The groups $\mathcal{S}_8$ and $\mathcal{A}_8$ contain respectively three and two shapes found in no other groups. In both cases, elements of these shapes make up 1/5th of the group. As is illustrated in the following examples, if $\mathcal{G}al_k(f)$ is $\mathcal{S}_8$ or $\mathcal{A}_8$, we can usually already prove it at this stage by finding shapes unique to these groups (they are distinguished from one another by parity; $\mathcal{A}_8$ is even and $\mathcal{S}_8$ is not).

Example 1: According to Matzat [M], the polynomial

$$x^n - nx^{n-1} + (-1)^{n/2}(n-1)^{n-1}((n-1)t^2 + 1)$$

over $\mathbf{Q}(t)$ has Galois group $\mathcal{A}_n$ when $n \equiv 0 \bmod 2$. In particular, if $n = 8$, we have

$$f = x^8 - 8x^7 + 7^7(7t^2 + 1).$$

Since f is irreducible, $\mathcal{G}al_{\mathbf{Q}(t)}(f)$ is a transitive subgroup of $\mathcal{S}_8$. The discriminant of f is

$$\Delta = (2^{12}7^{25}t(7t^2 + 1))^2.$$

As Δ is a square in $\mathbf{Q}(t)$, we know that $\mathcal{G}al_{\mathbf{Q}(t)}(f) \subseteq \mathcal{A}_8$.

We next find shapes by factoring modulo maximal ideals. It is convenient to use ideals of the form $\mathbf{p} = (p, t - a)$ where $a, p \in \mathbf{Z}$ and p is prime. Then $\mathbf{Z}[t]/\mathbf{p} \simeq \mathbf{Z}_p$ is a field and so $\mathbf{p}$ is maximal. To factor f modulo $\mathbf{p}$, we first 'specialize' f by setting $t = a$ and then factor $f|_{t=a} \bmod p$. (Note that $\mathcal{G}al_{\mathbf{Q}}(f|_{t=a})$ is a quotient of a subgroup of $\mathcal{G}al_{\mathbf{Q}(t)}(f)$.) To ensure that $f \bmod \mathbf{p}$ has no repeated roots we choose a and p such that $\Delta \not\equiv 0 \bmod p$ under the specialization $t = a$. (In particular $p \neq 2, 7$.) The choice $a = 1$, $p = 3$, gives the specialization

$$\begin{aligned} f|_{t=a} &= x^8 - 8x^7 + 2^3 7^7 \\ &\equiv (x^3 + 2x^2 + x + 1)(x^5 + 2x^4 + x^3 + x^2 + x + 2) \bmod 3, \end{aligned}$$

and so $Gal_{\mathbf{Q}(t)}(f)$ has an element of shape $3,5$, but the only transitive subgroup of $\mathcal{A}_8$ with this shape is $\mathcal{A}_8$ itself (see Table 11). So $Gal_{\mathbf{Q}(t)}(f) = \mathcal{A}_8$, as required.

Example 2: Matzat [M] also provides examples of polynomials with Galois group $\mathcal{S}_n$:

$$x^n - tx + t.$$

In the case $n = 8$, we have $f = x^8 - tx + t$. As the discriminant $2^{24}t^7 - 7^7t^8$ of f is not a square in $\mathbf{Q}(t)$, we see that $Gal_{\mathbf{Q}(t)}(f) \not\subseteq \mathcal{A}_8$.

$$\begin{aligned}
f|_{t=1} &= x^8 - x + 1 \\
&\equiv (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \bmod 2 \\
f|_{t=3} &= x^8 - 3x + 3 \\
&\equiv (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \bmod 2 \\
f|_{t=5} &= x^8 - 5x + 5 \\
&\equiv (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \bmod 2 \\
f|_{t=7} &= x^8 - 7x + 7 \\
&\equiv (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \bmod 2
\end{aligned}$$

(Specializations with $t \equiv 0 \bmod 2$ are omitted as the discriminant is trivial mod 2 in those cases.) So the Galois group has an element of shape $2,6$. Consulting Table 11, we see that $Gal_{\mathbf{Q}(t)}(f)$ must be one of the following: G_{48}, G_{192a}, G_{192b}, G_{384}, G_{1152} or $\mathcal{S}_8$. Under the specialization $t = 8$, f has factors of degrees 3 and 5 mod 3. The only group in the list just given with the shape $3,5$ is $\mathcal{S}_8$. So $Gal_{\mathbf{Q}(t)}(f) = \mathcal{S}_8$ as required.

2.2.2 Imprimitivity. If k is $\mathbf{Q}$, the algorithm of Casperson and Mckay [CM2] (see Section 1.1) can be used to test f for imprimitivity. If a decomposition $f \mid goh$

is found, groups which are not imprimitive with ∂g blocks may be eliminated. There are several more groups which may be identified at this stage using this technique in concert with those mentioned previously.

Example 3: The polynomial $f = x^8 + 4x^6 + 7x^4 + 6x^2 + 5$ has discriminant $\Delta = 2^{16}3^2 11^4 5$ and $\mathcal{G}al_{\mathbf{Q}}(f) \not\subseteq \mathcal{A}_8$. Since $\Delta \equiv 0 \bmod p$ for $p = 2, 3, 5, 11$ we begin looking for shapes by factoring mod 7. Since f is irreducible mod 7, the groups G_{32d}, G_{64d}, G_{64e} and G_{192a}, which have no element of shape 8, can be removed from the list of candidates.

Modulo 13, f has two factors of degree 2 and one of degree 4. The groups $\mathbf{Z}_8$, G_{16a}, G_{16b}, G_{16c}, G_{32a}, G_{32b}, G_{48} and $PGL(2,7)$ may be eliminated as they lack an element of shape $2^2 4$. By factoring mod 17, 19 and 23 we find shapes 8, 4^2 and $1^2 2^3$. The first two give no new information as all remaining candidate groups have these shapes. However G_{32c}, G_{64c} and G_{576} have no element of shape $1^2 2^4$ and can be eliminated. The shape 4^2 occurs again mod 29, but mod 31 we find the shape $1^2 2, 4$, allowing us to remove G_{64a}, G_{64b} and G_{192b} and leaving only G_{128}, G_{384}, G_{1152} and $\mathcal{S}_8$ as candidates for $\mathcal{G}al_{\mathbf{Q}}(f)$.

Evidently, setting $g = x^4 + 4x^3 + 7x^2 + 6x + 5$ and $h = x^2$, we see that $f = g \circ h$ so that $f \mid g \circ h$. An additional decomposition is: $f \mid ((x^2 + 3x + 5) \circ (x^4 + 2x^2))$. Since G_{128} is the only group amongst the remaining candidates which has systems of imprimitivity with both 2 and 4 blocks (see Table 9), we conclude that the Galois group is G_{128}.

Example 4: The polynomial $f = x^8 + x^2 + 1$ has discriminant $2^8 229^2$ whence $\mathcal{G}al_{\mathbf{Q}}(f) \subseteq \mathcal{A}_8$. Factoring modulo p for $p = 3, 5, 7, \ldots, 23$, we find the shapes $1^2 3^2$, 26, 4^2 and $1^2 24$. This leaves G^+_{192a}, G^+_{192b}, G^+_{576}, $(2^3.L(3,2))^+$ and $\mathcal{A}_8^+$ as candidates for $\mathcal{G}al_{\mathbf{Q}}(f)$. Clearly $f \mid ((x^4 + x + 1) \circ x^2)$. Since G^+_{192a} is the only one

of the remaining groups with a decomposition into four blocks of imprimitivity, we conclude that $\mathcal{G}al_{\mathbf{Q}}(f) = G^{+}_{192a}$.

2.2.3 Orbit-Length Partitions. Although testing shapes and imprimitivity are efficient ways of reducing the list of candidate Galois groups, they do not, in general, provide a proof; for this we must turn to resolvent polynomials. As was the case for smaller degree polynomials [S1, SM], we make use of r-set ($r = 2, 3, 4$) and 2-sequence resolvents. The orbit-length partition of these four resolvents distinguishes 24 of the 50 groups.

Notation: We will refer to the resolvent whose roots are sums (respectively products) of r-sets of the roots of f as the r_+-set (respectively $r_\times$-set) resolvent. Thus, the 2_+-set resolvent is $R(x_1 + x_2, f)$ and the $2_\times$-set resolvent is $R(x_1 x_2, f)$. We use $R(x_1 + 2x_2, f)$ as a 2-sequence resolvent.

Example 5: Let $f = x^8 - 2$. The discriminant of f is -2^{31} so $\mathcal{G}al_{\mathbf{Q}}(f) \not\subseteq \mathcal{A}_8$. Factoring f modulo p for the primes $3 \leq p \leq 41$, we find the shapes $1^2 2^3$, 4^2 and 8. After removing subgroups of $\mathcal{A}_8$ and those missing any of these shapes, the remaining candidates for $\mathcal{G}al_{\mathbf{Q}}(f)$ are G_{16a}, G_{16c}, G_{32a}, G_{48}, G_{64a}, G_{64b}, G_{128}, G_{192b}, $PGL(2,7)$, G_{384}, G_{1152}, and $\mathcal{S}_8$. However, by the Čebotarev density theorem, we expect that the Galois group is G_{16c}; all the other groups have shapes not yet observed in the first 12 primes, but which should occur more frequently than 1/12. (In fact we shall see that $\mathcal{G}al(f)$ is G_{16c}. All shapes of G_{16c} occur in each of the other remaining candidates. So we can not further reduce the list of candidates by testing shapes.)

Clearly $f \mid ((x^2 - 2) \circ x^4)$ and $f \mid ((x^4 - 2) \circ x^2)$. The groups G_{48}, G_{192b},

$PGL(2,7)$, G_{384}, G_{1152} and $\mathcal{S}_8$ are removed from the list of candidates as they do not have decompositions into both 2 and 4 blocks.

The group G_{16c} may be distinguished from the other groups in the list of candidates by orbit-length partition of 2-sets and 3-sets. Since we have not yet proved that the group is G_{16c}, we start with the 2-set resolvent as it has smaller degree and is therefore easier to construct and factor. The remaining candidates for $Gal_{\mathbf{Q}}(f)$ have differing orbit-length partition on this resolvent, so we will be able to eliminate candidates using it.

The $2_\times$-set resolvent

$$x^{28} + 2x^{24} - 12x^{20} - 24x^{16} + 48x^{12} + 96x^8 - 64x^4 - 128$$

has repeated roots. In order to apply Proposition 1.5.8 we first construct f^* from f by the Tschirnhaus transformation $x \mapsto x + 1$

$$f^* = x^8 + 8x^7 + 28x^6 + 56x^5 + 70x^4 + 56x^3 + 28x^2 + 8x - 1.$$

The $2_\times$-set resolvent of f^* factors as

$$\begin{aligned}
&(x^4 - 4x^3 + 6x^2 - 4x - 1) \times \\
&(x^8 - 8x^7 + 28x^6 - 56x^5 + 66x^4 - 104x^3 + 36x^2 + 8x + 1) \times \\
&(x^{16} - 16x^{15} + 120x^{14} - 560x^{13} + 1828x^{12} - 4336x^{11} + 7608x^{10} \\
&- 10320x^9 + 11846x^8 - 11952x^7 + 11976x^6 - 8720x^5 + 1828x^4 \\
&+ 1584x^3 + 264x^2 + 16x + 1)
\end{aligned}$$

so the orbit-length partition is $4, 8, 16$ and we may eliminate G_{16a} from the list of candidates.

Finally, the orbit-length partition for the 3-set resolvent is $8^3 16^2$. The only remaining candidate with this partition of 3-sets is G_{16c} (see Table 12). So the Galois group of $x^8 - 2$ is G_{16c}.

Example 6: Let $f = x^8 + 2x^4 + 2$. The discriminant, 2^{27}, is not a square so that $Gal_{\mathbf{Q}}(f) \not\subset A_8$. Factoring mod p for $3 \leq p \leq 37$ yields shapes 8, $1^4 4$, 4^2, $2^2 4$ and 2^1 so that G_{32c}, G_{64a}, G_{128}, G_{192b}, G_{384}, G_{1152} and S_8 remain as candidates for $Gal_{\mathbf{Q}}(f)$. By Čebotarev, the most likely candidate is G_{32c}.

Since $f \mid ((x^4+2x^2+2)\circ x^2)$ and $f \mid ((x^2+2x+2)\circ x^4)$ we may eliminate G_{192b}, G_{384}, G_{1152} and S_8. The resolvent of least degree which allows us to further reduce the number of candidates is the 2-sequence resolvent. As it has an orbit-length partition of $8^4 32$, we conclude that $Gal_{\mathbf{Q}}(f) = G_{32c}$.

2.2.4 Factorization Over $k(\sqrt{\Delta})$. Amongst the groups not distinguished by orbit-length partitions, all but three of those with discriminant Δ not a square in k can be identified by testing irreducibility of factors of resolvents over $k(\sqrt{\Delta})$ (See Table 1).

Example 7: Let $f = x^8 - 4x^6 + 4x^4 - 2$. The discriminant $-(2)^{29}$ is not a square so $Gal_{\mathbf{Q}}(f)$ is not even. Factoring modulo p for p from 3 to 71, we find the shapes $1^2 2^1$, $1^4 4$, $2^2 4$ and 4^2. So the list of candidates for the Galois group is G_{64a}, G_{64d}, G_{128}, G_{192b}, G_{384}, G_{1152} and S_8. Using the Čebotarev density theorem, the most likely candidate is G_{64d}.

Clearly $f \mid ((x^4-4x^3+4x^2-2)\circ x^2)$. On the other hand, $f \mid (x^2-2)\circ(x^4-2x^2)$ as well. Consequently, only G_{64a}, G_{64d} and G_{128} remain as candidates for the Galois group. Since these groups all have the same orbit-length partition for the four resolvents, there is nothing to be gained by attempting to factor them.

Instead, we use factorization over $\mathbf{Q}(\sqrt{-2})$. From Table 1 we see that, the Galois group may be identified by examining the degree 16 factors of the 2-set and 3-set resolvents. The 2-set resolvent is of lesser degree (and is therefore easier to construct and factor) so it is best to start with it.

Group	Factor(s) to be Tested (Resolvent/Degree of Factor)		
	2-set/4		
G_{32b}	reducible		
G_{64b}	irreducible		
	2-set/4		
G_{32d}	reducible		
G_{64c}	irreducible		
	2-set/4	2-set/16	3-set/16
G_{64a}	irreducible	reducible	reducible
G_{64c}	reducible	irreducible	reducible
G_{64d}	irreducible	irreducible	reducible
G_{128}	irreducible	irreducible	irreducible
	2-set/12		
G_{576}	reducible		
G_{1152}	irreducible		

Table 1: Distinguishing groups by testing irreducibility of factors of resolvents over $k(\sqrt{\Delta})$.

Since the 2_x-set resolvent of f has repeated roots we first construct f^* from f via the Tschirnhaus transformation $x \mapsto x+1$. The required factor of the 2_x-set resolvent polynomial of f^* is

$$\begin{aligned} g = \quad & x^{16} - 16x^{15} + 96x^{14} - 256x^{13} + 196x^{12} + 528x^{11} - 1056x^{10} \\ & + 902x^8 + 592x^7 + 1440x^6 + 256x^5 + 196x^4 + 48x^3 + 32x^2 + 1. \end{aligned}$$

As g is irreducible over $\mathbf{Q}(\sqrt{-2})$ we may eliminate G_{64a}.

The 3_x-set resolvent of f also has repeated roots, but, again, that of f^* does not. The degree 16 factor is

$$\begin{aligned} h &= x^{16} - 16x^{14} + 36x^{12} + 336x^{10} + 322x^8 + 240x^6 + 92x^4 + 16x^2 + 1 \\ &= (x^8 - 8x^6 - 8\sqrt{-2}x^5 - 14x^4 - 8x^2 - 1) \times \\ &\quad (x^8 - 8x^6 + 8\sqrt{-2}x^5 - 14x^4 - 8x^2 - 1). \end{aligned}$$

Since h factors over $\mathbf{Q}(\sqrt{-2})$, we conclude that $\mathcal{G}al_{\mathbf{Q}}(f) = G_{64d}$.

2.2.5 Galois Groups of Resolvent Factors. The remaining sixteen groups can be determined by calculating the Galois groups of factors of the resolvents as indicated in Table 2. For example, to distinguish $(\mathbf{Z}_2 \times \mathcal{A}_4)^+$ from $(\mathbf{Z}_2 \times \mathcal{S}_4)^+$ we make use of the 2-set resolvent. The resolvent has an irreducible factor g of degree 4. (Since $(\mathbf{Z}_2 \times \mathcal{A}_4)^+$ and $(\mathbf{Z}_2 \times \mathcal{S}_4)^+$ have the same orbit-length partitions for the resolvents, both groups will have such a degree 4 factor.) Using the methods in [SM] we can find $\mathcal{G}al_k(g)$. If $\mathcal{G}al_k(g) = \mathcal{A}_4$ then $\mathcal{G}al_k(f) = (\mathbf{Z}_2 \times \mathcal{A}_4)^+$. If $\mathcal{G}al_k(g) = \mathcal{S}_4$ then $\mathcal{G}al_k(f) = (\mathbf{Z}_2 \times \mathcal{S}_4)^+$.

The '1-diff' resolvent polynomial referred to in Table 2 is

$$R((x_1 + x_2 + x_3 + x_4 - x_5 - x_6 - x_7 - x_8)^2, f).$$

$Gal_k(f)$	Resolvent	∂g	$Gal_k(g)$
$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$	2-set	4	$\mathcal{A}_4$
$(\mathbf{Z}_2 \times \mathcal{S}_4)^+$			$\mathcal{S}_4$
G_{32b}^+	2-set	8	G_{32d}
G_{64}^+			G_{64c}
$(2^3.\mathbf{Z}_7)^+$			$\mathbf{Z}_7^+$
$(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$	4-diff	7	$(\mathbf{Z}_7.\mathbf{Z}_3)^+$
$(2^3.L(3,2))^+$			$PSL(3,2)^+$
G_{96a}^+	2-set	4	$\mathcal{A}_4$
G_{192a}^+			$\mathcal{S}_4$
G_{96b}^+	4-diff	6	$\mathcal{A}_4$
G_{192b}^+			$\mathcal{S}_4/V_4$
G_{288}^+	2-set	12	$12T1^+$
G_{576}^+			$12T2^+$
$12T1^+$	2-set	6	$\mathbf{Z}_3.\mathcal{S}_3$
$12T2^+$			$3^2.2^2$
G_{192a}			G_{96b}^+
G_{192b}	4-diff	8	G_{96c}^+
G_{384}			G_{192b}^+

Table 2: Distinguishing groups using Galois groups of resolvent factors

Example 8: Let

$$f = x^8 - x^7 + 2x^6 + 2x^5 + 7x^4 + 3x^3 + 4x^2 + 3x + 5.$$

The discriminant $\Delta = 29^6 157^2$ is a square whence $\mathcal{G}al_{\mathbf{Q}}(f) \subseteq \mathcal{A}_8$. The shapes found amongst the primes between 2 and 31 (excluding 29) are $1, 7$ and 2^4 so that the candidates are $(2^4.\mathbf{Z}_7)^+$, $(2^3\ (\mathbf{Z}_7\ \mathbf{Z}_3))^+$, $L(2,7)^+$, $(2^3.L(3,2))^+$ and $\mathcal{A}_8^+$ with $(2^3.\mathbf{Z}_7)^+$ most likely according to Čebotarev. As the remaining groups are all primitive, there is no need to test for imprimitivity.

The groups $L(2,7)^+$ and $\mathcal{A}_8^+$ may be removed from the list using orbit-length partitions on 4-sets. By Table 2, the remaining groups may be distinguished from one another using the degree 7 factor g of the 4-diff resolvent. Following [SM], we find $\mathcal{G}al_{\mathbf{Q}}(g) = \mathbf{Z}_7$. The Galois group is therefore $(2^3.\mathbf{Z}_7)^+$.

For $\partial g \leq 8$ we can use either the techniques of Soicher and McKay or those we are presenting here to find $\mathcal{G}al_k(g)$. However, to distinguish between G_{288}^+ and G_{576}^+ we make use of a factor g of degree 12. In this case, we denote $\mathcal{G}al_k(g)$ by $12T1^+$ (respectively $12T2^+$) when $\mathcal{G}al_k(f)$ is G_{288}^+ (respectively G_{576}^+). Then as indicated in Table 2, the Galois group of the degree 6 factor of the 2-set resolvent of g depends on whether $\mathcal{G}al_k(g)$ is $12T1^+$ or $12T2^+$ ($12T1^+$ and $12T2^+$ have the same orbit-length partition for the 2-set resolvent).

Tables 3 and 4 summarize how to distinguish the 50 degree 8 groups. For each group G, we indicate orbit-length partitions for a set Σ of resolvent polynomials. If H is another group, of the same parity as G, such that G and H have the same orbit-length partition for each resolvent in Σ, then G and H have the same partition for all resolvents. Moreover, no proper subset of Σ has this property; Σ is minimal. The tables also show whether it is necessary to find the Galois groups of resolvent factors or factor them over $k(\sqrt{\Delta})$.

Group	Orbit-Length Partition				Galois Groups of
$(G \subseteq \mathcal{A}_8)$	2	3	4	2	Resolvent Factors
	set	set	set	seq	(see Table 2)
$(\mathbf{Z}_2 \times \mathbf{Z}_4)^+$	$4^3 8^2$	8^7			
$(2^3)^+$	4^7				
D_4^+	$4^5 8$				
Q_8^+	$4, 8^3$	8^7			
G_{16a}^+	$4^3 8^2$	$8^3 16^2$			
G_{16b}^+	$4^3 16$	$8^3 16^2$			
G_{16c}^+	$4, 8^3$	$8^3 16^2$			
$SL(2,3)^+$	$4, 24$	$8, 24^2$			
$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$			$2, 6^2 8, 24^2$		Needed
$\mathcal{S}_4^+$			$2, 6^2 8, 12^2 24$		
G_{32a}^+				$8^3 32$	
G_{32b}^+				$8, 16, 32$	Needed
G_{32c}^+	$4, 8, 16$	$8^3 32$			
G_{32d}^+	$4, 8^3$	$8^3 32$			

Table 3: Distinguishing degree 8 Galois groups - $G \subseteq \mathcal{A}_8$

Group ($G \subseteq \mathcal{A}_8$)	Orbit-Length Partition				Galois Groups of Resolvent Factors (see Table 2)
	2 set	3 set	4 set	2 seq	
$(\mathbf{Z}_2 \times \mathcal{S}_4)^+$			$2, 6^2 8, 24^2$		Needed
$(2^3.\mathbf{Z}_7)^+$			$14, 56$		Needed
G_{64}^+				$8, 16, 32$	Needed
G_{96a}^+				$8, 48$	Needed
G_{96b}^+			$2, 12, 24, 32$		Needed
G_{96c}^+			$2, 12^3 32$		
$(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$			$14, 56$		Needed
$L(2,7)^+$			$14^2 42$		
G_{192a}^+				$8, 48$	Needed
G_{192b}^+			$2, 12, 24, 32$		Needed
G_{288}^+			$2, 32, 36$		Needed
G_{576}^+			$2, 32, 36$		Needed
$(2^3.L(3,2))^+$			$14, 56$		Needed
$\mathcal{A}_8^+$			70		

Table 3: (continued) Distinguishing degree 8 Galois groups - $G \subseteq \mathcal{A}_8$

Group	Orbit-Length Partition				Factorization	Galois Groups of
($G \not\subseteq \mathcal{A}_8$)	2	3	4	2	over $k(\sqrt{\Delta})$	Resolvent Factors
	set	set	set	seq	(see Table 1)	(see Table 2)
$\mathbf{Z}_8$		8^7				
G_{16a}	$4, 8^3$	$8^3 16^2$				
G_{16b}				$8^3 16^2$		
G_{16c}	$4, 8, 16$	$8^3 16^2$		$8, 16^3$		
G_{32a}		$8, 16^3$				
G_{32b}	$4, 8, 16$	$8^3 32$			Needed	
G_{32c}				$8^3 32$		
G_{32d}	$4, 8^3$	$8^3 32$			Needed	
G_{48}	$4, 24$	$8, 24^2$				
G_{64a}		$8, 16, 32$		$8, 16, 32$	Needed	
G_{64b}	$4, 8, 16$	$8^3 32$			Needed	
G_{64c}		$8, 16, 32$		$8, 16, 32$	Needed	
G_{64d}		$8, 16, 32$		$8, 16, 32$	Needed	
G_{64e}	$4, 8^3$	$8^3 32$			Needed	
G_{128}		$8, 16, 32$		$8, 16, 32$	Needed	
G_{192a}		$24, 32$				Needed
G_{192b}		$24, 32$				Needed
$PGL(2, 7)$			$28, 42$			
G_{384}		$24, 32$				Needed
G_{576}	$12, 16$				Needed	
G_{1152}	$12, 16$				Needed	
$\mathcal{S}_8$			70			

Table 4: Distinguishing degree 8 Galois groups - $G \not\subseteq \mathcal{A}_8$

3 An Implementation of the Degree 8 Algorithm

The algorithm of the previous section has been implemented in the MAPLE V [CGG] language. The current program extends MAPLE code written by Ron Sommeling to find Galois groups of rational polynomials of degree up to 7 using the ideas outlined in [SM]. The polynomials (of all degrees up to 8) may now be defined over a function field of the form $\mathbf{Q}(t_1, \ldots, t_r)$ where $t_1, \ldots, t_r$ are transcendental over $\mathbf{Q}$. We describe some aspects of the implementation.

3.1 Discriminant and Shapes. Expressing the algorithm in a symbolic algebra language such as MAPLE is straightforward. For example, *discrim(f,x)* finds the discriminant of a polynomial $f(x)$. The command *Factor(f) mod p*, which factors f over $\mathbf{F}_p$ (for p prime), can be used to generate shapes. According to Corollary 1.3.8, we can find shapes in $\mathcal{G}al(f)$ by factoring f modulo maximal ideals. We use ideals in $\mathbf{Z}[t_1, \ldots, t_r]$ of the form $\mathfrak{p} = (p, t_1 - a_1, \ldots, t_r - a_r)$ where $p, a_1, \ldots, a_r \in \mathbf{Z}$ and p is prime. Then $\mathbf{Z}[t_1, \ldots, t_r]/\mathfrak{p} = \mathbf{Z}_\mathfrak{p}$ is a field and so $\mathfrak{p}$ is maximal. To factor $f \in \mathbf{Q}(t_1, \ldots, t_r)$ modulo $\mathfrak{p}$ we first 'specialize' f to $f^* \in \mathbf{Z}[x]$ by substituting a_i for t_i and then factor $f^* \bmod p$. In particular, if the base field is $\mathbf{Q}$, we simply factor mod p.

However, in order to apply the proposition, we must ensure that f has no repeated roots in $\mathbf{Z}[t_1, \ldots, t_r]/\mathfrak{p}$. Consequently, we do not attempt to factor f mod $\mathfrak{p}$ if the discriminant or leading coefficient of f is zero modulo $\mathfrak{p}$.

Although generating shapes is rather easy, they will not determine $\mathcal{G}al(f)$ unless it is $\mathcal{A}_8$ or $\mathcal{S}_8$. The question then arises as to how many shapes should be generated before moving on to other techniques. In our program, we continue generating shapes until the following three conditions all obtain.

- The set C of candidate Galois groups remains stable after computing shapes for 16 consecutive primes.
- C contains an element γ such that $\Sigma_\gamma \subseteq \Sigma_c$ for all c in C where Σ_c is the set of shapes of c.
- All shapes of γ have been observed.

The first condition is motivated by the Čebotarev density theorem. Let Σ_G be the set of shapes occurring in group G. If G_1 and G_2 are degree 8 groups of similar parity such that Σ_{G_1} is a proper subset of Σ_{G_2}, then the elements with shapes in $\Sigma_{12} = \Sigma_{G_2} \setminus \Sigma_{G_1}$ make up at least 1/16th of G_2. So, by Čebotarev's theorem, if $\mathcal{G}al(f) = G_2$, we expect a shape in Σ_{12} to occur amongst the 16 consecutive primes and hence allow us to eliminate G_1 as a candidate.

The advantage of the second condition is clear, if there is no minimal group, then, continuing, we will eventually be able to eliminate some candidates when we find a shape they lack. The third condition gives us further confidence that γ is in fact the Galois group and therefore there is nothing to be gained by generating more shapes. (If $\Sigma_{\mathcal{G}al(f)} \subseteq \Sigma_G$, then we can never eliminate G as a candidate by testing shapes.) Note however that we needn't explicitly demonstrate all shapes of γ (by factoring modulo maximal ideals), if we find a shape corresponding to the element x, then we know that the shapes of all powers of x will also occur.

As further evidence for the validity of our stopping criteria, we note that, with one single exception, $\Sigma_\gamma = \Sigma_{\mathcal{G}al(f)}$, for the polynomials of Tables 6 and 7. The exceptional case is $f = x^8 - x^6 - 3x^2 + 4$ ($\mathcal{G}al(f) = G_{8,4}^+$). In order to select the correct γ in this case, we would need to extend the first condition to require stability under 26 consecutive primes.

3.2 Construction of Resolvents. The r-set ($r = 2,3,4$) resolvents may be constructed as having roots which are either the sum or the product of r-sets of roots of the original polynomial. Casperson and McKay [CM1] have demonstrated efficient methods for both of these cases. It appears to be faster to construct the resolvent using products. For example, on a SPARC station 2, the 3-set resolvent of

$$f = x^8 + 14x^5 + 7x^4 - 14x^3 + 4x + 14$$

($Gal(f) = (2^3.L(3,2))^+$) was constructed in two ways. Using sums of roots took 20 seconds of CPU while products required less than 3 seconds. On the other hand, products tend to give a polynomial with larger coefficients since the roots of the resolvent are of homogeneous weight r in the roots of the original polynomial as opposed to weight one in the case of sums. Such a polynomial is therefore more difficult to factor. In the case of the resolvents just mentioned, it took twice as long to factor the products polynomial as compared to the sums polynomial; 15 versus 8 seconds of CPU. For the 2-set and 3-set resolvents we use the product construction.

To construct the 4-set polynomial of a degree 8 polynomial f, we make use of the following observation of Soicher and McKay [SM]: When $R(F,f)$ is a resolvent such that $F^\sigma = -F$ for some $\sigma \in \mathcal{S}_n$ ($n = \partial f$), then $R(F^2,f)(x^2) = R(F,f)(x)$. In particular, let

$$F = x_1 + x_2 + x_3 + x_4 - x_5 - x_6 - x_7 - x_8$$

(so that $R(F^2,f)$ is the 4-diff resolvent of Table 2). By making an appropriate Tschirnhaus transformation we can ensure that the sum of the roots of f is 0. But then we see that $R(F,f)$ is the 4_+-set resolvent. (Actually the roots have been doubled, but this is again just a Tschirnhaus transformation.) So by constructing the 4_+-set resolvent in this way, we find that we have in fact constructed $R(F^2,f)(x^2)$.

To factor the resolvent, we first factor $R(F^2,f)(x)$. This polynomial has half the degree of the 4_+-set resolvent and therefore is much easier to factor. This gives

a partial factorization of $R(F^2, f)(x^2)$ or, equivalently, the 1_+-set resolvent. By examining the possible orbit-length partitions which may arise under a degree 8 transitive group (see Table 12), we see that the only factors of the 1_+-set resolvent which may be further reduced after the initial partial factorization, are those of degree 16, 32 and 48. To complete the factorization, we factor any factors of these degrees.

The method used to construct the 2-sequence resolvent is similar to that outlined by Casperson and McKay [CM1] for the r-set resolvents. We represent the 2-sequence resolvent as $R_{2s} = R(x_1 + 2x_2, f)$. To construct R_{2s}, it suffices to demonstrate how the power-sum symmetric functions of R_{2s} depend on those of f; the coefficients of a polynomial are simply related to these symmetric functions (see [CM1]). For f a polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ let

$$\mathcal{P}_k(f) = \sum_{i=1}^{n} \alpha_i^k.$$

Proposition 3.2.1

$$\mathcal{P}_k(R_{2s}) = \sum_{i=0}^{k} 2^i \binom{k}{i} (\mathcal{P}_i(f)\mathcal{P}_{k-i}(f) - \mathcal{P}_k(f)), \quad k \geq 1.$$

Proof. Let $\alpha_1, \ldots, \alpha_8$ be the roots of f. The roots of R_{2s} are then $\{\alpha_i + 2\alpha_j | i \neq j, 1 \leq i, j \leq 8\}$. So,

$$\begin{aligned}
\mathcal{P}_k(R_{2s}) &= \sum_{i=1}^{8} \sum_{j \neq i, j=1}^{8} (\alpha_i + 2\alpha_j)^k \\
&= \sum_{i=1}^{8} \sum_{j \neq i} \sum_{l=0}^{k} \binom{k}{l} (2\alpha_j)^l \alpha_i^{k-l} \\
&= \sum_{l=0}^{k} 2^l \binom{k}{l} \sum_{i=1}^{8} \sum_{j \neq i} \alpha_j^l \alpha_i^{k-l}
\end{aligned}$$

$$= \sum_{l=0}^{k} 2^l \binom{k}{l} (\sum_{i=1}^{8} \alpha_i^l \sum_{i=1}^{8} \alpha_i^{k-l} - \sum_{i=1}^{8} \alpha_i^k)$$
$$= \sum_{l=0}^{k} 2^l \binom{k}{l} (\mathcal{P}_l(f)\mathcal{P}_{k-l}(f) - \mathcal{P}_k(f))$$

□

3.3 Factorization over $k(\sqrt{\Delta})$. To distinguish between certain groups not contained in $\mathcal{A}_8$, we use factorization over $k(\sqrt{\Delta})$, where Δ is the discriminant of the input polynomial f. We can avoid working over an extension field using a technique of Soicher [S1, p.31]. To see whether the polynomial g is irreducible over $k(\sqrt{\Delta})$, we construct the polynomial g_Δ with roots $\beta_i \pm \sqrt{\Delta}$ where the β_i run through the roots of g (so $\partial g_\Delta = 2\partial g$). Then $g_\Delta \in k[x]$ and g is irreducible over $k(\sqrt{\Delta})$ iff g_Δ is irreducible over k. The polynomial g_Δ may be constructed as a resultant:

$$g_\Delta(y) = resultant_x(g(x), (x-y)^2 - \Delta)$$

It is convenient to use δ, the square-free part of Δ, in place of Δ in the construction; the polynomial g_δ is irreducible iff g_Δ is irreducible and the former will have smaller coefficients and hence be easier to factor.

3.4 Distinguishing G_{192a}, G_{192b} and G_{384}. In the current implementation, to improve performance, we use methods slightly different from those outlined above to distinguish among G_{192a}, G_{192b} and G_{384}. As indicated in Table 2, these groups may be identified by finding the Galois group of the degree 8 factor g of the 4-diff resolvent. For example, if we have narrowed the list of candidates for $\mathcal{G}al(f)$ down to G_{192a} and G_{384} then we know that $\mathcal{G}al(g)$ is either G_{96b}^+ or G_{192b}^+. Again, by referring to Table 2 we see that $\mathcal{G}al(g)$ is determined by the Galois group of h, the

degree 6 factor of the 4-diff resolvent of g; the process of finding the Galois group of a resolvent factor is repeated.

We can avoid repeated construction of Galois groups of resolvent factors as follows. First G_{192a} may be identified by finding the Galois group of g, the degree 4 factor of the 2-set resolvent. If $\mathcal{G}al(f) = G_{192a}$ then $\mathcal{G}al(g) = \mathcal{A}_4$. Otherwise, $\mathcal{G}al(g) = \mathcal{S}_4$. To distinguish between G_{192b} and G_{384} we use the degree 6 factor of the 4-set resolvent. This polynomial, g, can also be constructed as the 2-set resolvent of the degree 4 factor of the 2-set resolvent of f (and this is faster unless the 4-set resolvent is already available from previous calculations since the degrees of the resolvents used are smaller). The 3-set resolvent of g has an irreducible factor h of degree 12. If $\mathcal{G}al(f) = G_{192b}$ (respectively G_{384}), then h factors (respectively is irreducible) over $k(\sqrt{\Delta})$, where Δ is the discriminant of f.

4 Avenues for Further Exploration

In Table 5 we give some statistics on the CPU use of the implementation discussed in the previous section. In particular, we have included data on the time spent factoring polynomials and testing polynomials for imprimitivity.

The imprimitivity algorithm (see Section 1.4) tests pairs of roots in an effort to construct a decomposition $f \mid goh$. The algorithm will only be able to find such a decomposition if the pair is in the same block of imprimitivity. Hence, the performance of the algorithm depends on which root pairs are examined. In the tables we have indicated statistics for the best case, in which the first pair of roots tested yields a decomposition, and the worst case, in which as many bad choices of root pairs as possible is made before hitting on one which yields a decomposition. (If there is a system of imprimitivity with blocks of size m, then we can be sure that a pair in the same block occurs amongst the first $n - m + 1$ pairs. However, since the algorithm sometimes misses decompositions, the worst case may be to unsuccessfully test all 7 pairs even when the polynomial is imprimitive.) The data for the polynomial factorization is taken with respect to the best case.

In the worst case, polynomial factorization and the imprimitivity algorithm account for 74% of the CPU used in calculating the fifty Galois groups. Even in the best case, the percentage is 58%. Improving either of the two processes would be a good way to improve our algorithm.

4.1 Improving Polynomial Factorization. There are several ways in which we may speed up polynomial factorization. By finding shapes in the Galois group, we have a good idea of what it is before we examine resolvents. As Casperson and McKay [CM1] have discussed, we can use this knowledge to construct factors of the resolvent

Group	CPU Used (seconds)		Polynomial Factorization (%)	Imprimitivity Algorithm (%)	
	Best	Worst		Best	Worst
$\mathbf{Z}_8$	10.3	40.7	28.1	38.7	81.3
$(\mathbf{Z}_2 \times \mathbf{Z}_4)^+$	46.5	105.7	66.5	23.2	66.2
$(2^3)^+$	8.9	37.7	58.5	15.3	80.0
D_4^+	13.3	13.3	10.7	70.6	70.6
Q_8^+	58.4	86.1	83.8	2.3	33.7
G_{16a}	5.2	61.2	18.1	35.5	91.5
G_{16b}	13.7	42.6	44.2	10.4	71.3
G_{16c}	18.3	67.1	51.9	10.6	75.6
G_{16a}^+	43.8	52.6	6.2	88.2	90.2
G_{16b}^+	50.9	113.8	80.6	4.3	57.2
G_{16c}^+	73.2	82.9	87.5	2.4	13.8
$SL(2,3)^+$	96.5	625.9	87.5	2.5	85.0
$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$	27.6	99.9	8.5	79.6	94.4
$\mathcal{S}_4^+$	292.2	369.1	7.9	5.7	25.1
G_{32a}	78.5	143.0	86.0	3.5	47.0
G_{32b}	22.8	147.6	51.5	9.3	86.0
G_{32c}	16.6	45.0	27.8	18.7	70.0

Table 5: Statistics on CPU usage and percentage of time spent factoring polynomials and testing them for imprimitivity - Data from a MAPLE V implementation run on a SPARC station 2 using polynomials of Tables 6 and 7 as input.

Group	CPU Used (seconds)		Polynomial Factorization (%)	Imprimitivity Algorithm (%)	
	Best	Worst		Best	Worst
G^+_{32a}	205.7	248.5	89.4	6.3	22.5
G^+_{32b}	34.0	70.0	43.6	41.8	71.8
G^+_{32c}	147.9	267.6	56.1	37.9	65.7
G_{32d}	32.1	32.1	29.0	60.4	60.4
G^+_{32d}	169.8	288.5	55.5	38.9	64.0
G_{48}	116.5	295.5	91.7	1.7	61.2
$(\mathbf{Z}_2 \times \mathcal{S}_4)^+$	21.6	92.0	11.9	76.3	94.4
$(2^3.\mathbf{Z}_7)^+$	227.8	227.8	3.9	0.0	0.0
G_{64a}	10.0	10.0	41.5	15.9	15.9
G_{64b}	32.0	91.6	51.1	24.6	73.6
G_{64c}	14.1	86.5	13.1	63.8	94.1
G^+_{64}	35.1	90.8	34.1	50.1	80.7
G_{64d}	434.6	499.1	85.0	12.6	23.9
G_{64e}	15.8	15.8	39.2	34.5	34.5
G^+_{96a}	69.3	169.4	83.1	3.4	60.5
G^+_{96b}	238.3	238.3	7.5	31.2	31.2
G^+_{96c}	389.6	389.6	9.0	30.6	30.6

Table 5: (continued)

Group	CPU Used (seconds)		Polynomial Factorization (%)	Imprimitivity Algorithm (%)	
	Best	Worst		Best	Worst
G_{128}	23.1	71.2	8.3	77.8	92.8
$(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$	216.6	216.6	8.6	0.0	0.0
$L(2,7)^+$	221.7	221.7	8.3	0.0	0.0
G_{192a}	10.2	95.8	45.0	25.0	92.0
G^+_{192a}	4.1	86.5	3.6	58.5	98.0
G_{192b}	15.1	91.1	45.5	15.1	85.9
G^+_{192b}	289.1	289.1	3.7	71.3	71.3
G^+_{288}	131.9	131.9	4.7	80.6	80.6
$PGL(2,7)$	218.3	218.3	3.7	0.0	0.0
G_{384}	3.7	97.2	2.3	69.1	98.8
G^+_{576}	21.6	129.4	1.3	92.5	98.8
G_{576}	31.9	100.3	19.5	71.1	91.4
G_{1152}	21.1	96.1	0.5	94.6	98.8
$(2^3.L(3,2))^+$	101.1	101.1	4.4	0.0	0.0
$\mathcal{A}_8^+$	0.6	0.6	16.7	0.0	0.0
$\mathcal{S}_8$	0.6	0.6	24.3	0.0	0.0

Table 5: (continued)

It is often not necessary to find a complete factorization of the resolvent polynomial. For example, if we are going to distinguish groups by forming the Galois group of a certain factor of the resolvent, it suffices to find that factor. Some symbolic algebra programs have factorization routines which only look for factors of given degree (e.g. PARI [BBCO]). MAPLE V does not.

The most time consuming part of the standard Zassenhaus [Z] factorization algorithm is recombination of modular factors after Hensel lifting; in the absence of other information it is necessary to try multiplying all possible combinations of the modular factors together and testing if the result is a factor of the original polynomial. But since we know what orbit-length partitions may occur, we can speed this up by rejecting those combinations of modular factors whose degree is inconsistent with any of the possible partitions.

Moreover, because our resolvents are derived from degree 8 polynomials, their modular factors will be relatively small. Note that the elements of largest order which occur amongst the degree 8 Galois groups have order 15, corresponding to the shape 3,5. Since the factors of resolvents have Galois groups which are quotients of the original degree 8 group (see Proposition 1.5.10), these groups will also have elements of order not exceeding 15. But then, since the factorization of the resolvent factor modulo a prime represents the shape of an element in the Galois group, we see that the modular factors can never exceed degree 15.

So the Zassenhaus method is a poor choice for the situation of factoring resolvents derived from degree 8 polynomials; there will be many modular factors of relatively small degree (≤ 15) to be recombined. It may be worthwhile to investigate other approaches to polynomial factorization such as that proposed by Lenstra, Lenstra and Lovász [LLL]. Unlike the Zassenhaus algorithm, which is exponential in the worst case, the LLL algorithm is polynomial.

The LLL algorithm begins with a low-degree factor $h \in \mathbf{Z}_{(p)}[x]$ (where $\mathbf{Z}_{(p)}$ is the

p-adic integers) of f with coefficients accurate modulo $q = p^m$ (for m 'sufficiently' large). Such a factor may be found using Berlekamp's algorithm with Hensel lifting. From h, we construct the $\mathbf{Z}$-lattice

$$q, qx, qx^2, \ldots, qx^{k-1}, h(x), xh(x), x^2h(x), \ldots, x^{n-k-1}h(x)$$

where $n = \partial f$, $k = \partial h$. If $h \mid h_0$ for $h_0 \in \mathbf{Z}[x]$, then h_0 is in the lattice. If h_0 divides f, then the coefficients of h_0 are relatively small. So finding h_0 corresponds to looking for a short vector in the lattice. This process is repeated to generate all irreducible factors of f.

4.2 Improving the Imprimitivity Algorithm. There is also some possibility of making better use of the imprimitivity algorithm of Casperson and McKay [CM2] It would be useful to get a bound on the coefficients of h. In particular, we have a bound if we know $f = g \circ h$ so conditions under which $f \mid g \circ h$ implies $f = g \circ h$ are worth investigating. If such a bound were available, then we could be sure that if no decomposition $f \mid g \circ h$ is found (with coefficients of h less than the bound), then none exists. Such a negative result could be used to prove primitivity We could also test for the different block sizes; given a bound for the coefficients of h, the imprimitivity algorithm is definitive.

In our implementation, the use of the LLL algorithm to find the $\mathbf{Z}$-linear dependence determining the coefficients of h (see Section 1.4) accounts for most of the CPU used in testing imprimitivity. For example, in the worst case of Table 5 ($\mathcal{G}al(f) = SL(2,3)^+$), the imprimitivity algorithm uses 532 CPU seconds; 83% of this time is consumed by the LLL algorithm. So efficiency of the algorithm depends on a good implementation of LLL.

We compared the MAPLE V [CGG] and PARI 1.36 [BBCO] implementations of LLL on a SUN 3/50 for the case of $SL(2,3)^+$. In PARI, LLL takes 10 seconds

of CPU if real arithmetic is used, and 1500 seconds for rational arithmetic. Although the two versions came up with the same result in this case, in general, the real arithmetic version is 'numerically unstable' (see [BBCO, p.30]). The MAPLE implementation requires 2040 seconds of CPU and uses rational arithmetic.

LLL is used for basis reduction in a lattice generated by differences of powers of a pair of roots (see Section 1.4). The vectors used in the computation become smaller when a pair of real roots are used since these differences are then real (we may drop the imaginary component of the vector). So the calculation will be faster for pairs of real roots. It may be advantageous to first test all real pairs before proceeding to any imaginary roots

It is evident from the data in the tables that the worst case for the imprimitivity algorithm can be much worse than the best case. Over the 50 groups, the percentage of time used increases from 23% to 50%. So it would be useful to develop a means of quickly testing whether a given pair of roots might lead to a decomposition; one can waste a lot of time trying to get a decomposition from a pair of roots which are not in the same block of imprimitivity and hence can never result in a decomposition. Even a test which sometimes labels good pairs as bad may be worthwhile; a big saving of time in the worst case scenario might be worth a small increase in the best case. In any event, we do not rely on imprimitivity to identify the groups so it is not critical if we lose some accuracy in exchange for speeding the algorithm up.

A decomposition $f \mid g \circ h$ also gives information about certain subfields of the splitting field of f. Let f be an imprimitive polynomial of degree n with splitting field K such that the roots $\{\alpha_1, \ldots, \alpha_l\}$ are representatives of the l blocks of imprimitivity. Then each $\beta_i = h(\alpha_i)$ is a root of g. Let $H \subseteq Gal_k(f)$ be the subgroup of automorphisms which fix the blocks. Then H fixes each β_i and consequently, by

the fundamental theorem of Galois theory,

$$K^H = k(\beta_1) = k(\beta_2) = \ldots = k(\beta_l).$$

So the decomposition $f \mid goh$ implies the existence of a field $k(\beta)$ such that $[k(\beta) : k] = l$.

If the "improper" decompositions of the set of roots into one block of size n and n blocks of size one are included, then the systems of imprimitivity of a group define a lattice L. To each system of imprimitivity with l blocks we may associate a field $k(\beta)$ with $[k(\beta) : k] = l$. The lattice operations then correspond to the intersection and compositum of the corresponding fields. In this way L determines part of the lattice of subfields of K over k. But L is an invariant of $Gal_k(f)$ and so the resulting subfield structure may also be used to help identify the Galois group.

4.3 Small Degree Resolvents. Another means of potentially improving our technique arises from the idea of a polynomial belonging to a group (see Definition 2.1.1). It is not difficult to see that every group $G \subseteq S_n$ has a polynomial belonging to it. For example let $F^*(x_1, \ldots, x_n) = x_1^1 x_2^2, \ldots, x_n^n$. Then $\sum_{\sigma \in G} \sigma(F^*)$ belongs to G. Generally there are many polynomials belonging to a given group G.

If F belongs to G, then $\partial R(F, f) = |S_n : G|$. This gives us a method for constructing new resolvents of small degree; find a large subgroup and take a polynomial belonging to it. For example, a resolvent associated with $(2^3.L(3,2))^+$ has degree $|S_8 : (2^3.L(3,2))^+| = 30$. In Appendix C we show how such a resolvent can be used to distinguish G_{288}^+ from G_{576}^+.

There remains however the question of how to construct these resolvents. If $k = \mathbf{Q}$, we could use complex approximations to the roots. But, as mentioned in Section 2.1.1, there are certain disadvantages to this approach. It is preferable to take advantage of the coefficients of the resolvent being polynomials in the coeffi-

cients of f (see Section 1.5). Although we know of no easy way to find these polynomials, it is worth noting that we need only to do it once; once we have expressed the coefficients of the resolvent in terms of those of f, constructing the resolvent is simply a matter of evaluating the polynomials.

As mentioned, one bottleneck in our method lies in factoring the r-set and 2-sequence resolvents. The degrees of these resolvents increase with ∂f so that they are more difficult to factor; consequently, using polynomials belonging to groups to generate small degree resolvents becomes more attractive as ∂f increases.

A Rational Polynomials With Given Galois Groups

Tables 6 and 7 give, for each transitive subgroup G of $\mathcal{S}_8$, a rational polynomial f such that $\mathcal{G}al_{\mathbf{Q}}(f) = G$. In the tables, ζ_k denotes a primitive kth root of unity. Many of these polynomials were suggested to us in earlier work by Darmon [D]. In Section A.2 we indicate how they were derived. Examples for $SL(2,3)^1$, $L(2,7)^1$ and $PGL(2,7)$ are drawn from [HK] and [M]. In [S2], Soicher gives a polynomial for $(2^3.L(3,2))^+$ and mentions that the same method may be used for $(2^1.\mathbf{Z}_7)^1$ and $(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$. We discuss this method and how it may be extended to derive polynomials for G_{96b}^+ and G_{96c}^+ in Section A.3. The remaining polynomials were found by computer searching. We were guided in our searches by Soicher [S1, pp 85-87]. In particular, we used his ideas for generating polynomials with square discriminant.

Group ($G \subseteq \mathcal{A}_8$)	$f(x)$	Remarks
$(\mathbf{Z}_2 \wr \mathbf{Z}_4)^+$	$x^8+2x^6+4x^4+8x^2+16$	$spl(f) = \mathbf{Q}(\zeta_5, \sqrt{2})$ [D]
$(2^3)^+$	$x^8-12x^6+23x^4-12x^2+1$	$spl(f) = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ [D]
D_4^+	$x^8+4x^6+8x^4+4x^2+1$	$spl(f) = spl(x^2-4)$ [D]
Q_8^+	$x^8-21x^6+144x^4-288x^2+144$	$spl(f) =$ $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})})$ [D]
G_{16a}^+	x^8-10x^4+1	$f = \prod(x \pm \sqrt{\pm\sqrt{2} \pm \sqrt{3}})$ [D]
G_{16b}^+	$x^8-3x^6+9x^4-12x^2+16$	$f = \prod_{i=1}^{i=4}(x^2-\zeta_5^i x-2)$ [D]
G_{16c}^+	x^8-18x^4+9	$spl(f) =$ normal closure of $\mathbf{Q}(\sqrt{12+7\sqrt{6}+12\sqrt{2}+7\sqrt{3}})$ [D]
$SL(2,3)^+$	$x^8+9x^6+23x^4+14x^2+1$	[HK]
$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$	$x^8+21x^4+61x^2+141$	$spl(f) = \mathbf{Q}(rts(x^4+8x+12), i)$
S_4^+	$x^8+150x^4-500x^2+5625$	$spl(f) = spl(x^4+2x+3)$
G_{32a}^+	x^8+8x^2+9	
G_{32b}^+	$x^8-4x^6+12x^4-8x^2+4$	[D]
G_{32c}^+	$x^8+4x^6+x^4-6x^2+1$	$f = (x^2+1)^4-5(x^2+1)^2+5$ [D]
G_{32d}^+	x^8-28x^4+100	$f = \prod(x^2-(\pm 2\sqrt{3} \pm \sqrt{2}))$ [D]

Table 6: Rational polynomials with degree 8 Galois groups - $G \subseteq \mathcal{A}_8$

Group ($G \subseteq \mathcal{A}_8$)	$f(x)$	Remarks
$(\mathbf{Z}_2 \times \mathcal{S}_4)^+$	$x^8 - 4x^2 + 4$	
$(2^3.\mathbf{Z}_7)^+$	$x^8 - x^7 + 2x^6 + 2x^5 + 7x^4$ $+3x^3 + 4x^2 + 3x + 5$	See accompanying text
G_{64}^+	$x^8 + 4x^6 + 7x^4 + 6x^2 + 4$	$Gal(x^4 + 4x^3 + 7x^2 + 6x + 4)$ D_4 [D]
G_{96a}^+	$x^8 - x^6 - 3x^2 + 4$	
G_{96b}^+	$x^8 - 4x^7 - 8x^6 + 24x^5 + 36x^4$ $-24x^3 - 48x^2 + 48x - 12$	See text
G_{96c}^+	$x^8 - 6x^6 - 4x^5 + 24x^4 - 28x^2 + 18$	See text
$(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$	$x^8 + 2x^7 + 28x^6 + 84x^5 + 224x^4$ $+392x^3 - 336x + 112$	See text
$L(2,7)^+$	$x^8 + 2x^7 + 28x^6 + 1728x + 3456$	[M]
G_{192a}^+	$x^8 + x^2 + 1$	
G_{192b}^+	$x^8 + 16x^4 + 16x^3 + 8$	
G_{288}^+	$x^8 + 7x^4 + 8x^3 + 9$	
G_{576}^+	$x^8 - 8x^6 - 8x^5 + 8$	
$(2^3.L(3,2))^+$	$x^8 + 14x^5 + 7x^4 - 14x^3 + 4x + 14$	[S2]
$\mathcal{A}_8^+$	$x^8 + 8x^3 + 10$	

Table 6: (continued) Rational polynomials with degree 8 Galois groups - $G \subset \mathcal{A}_8$

Group ($G \not\subseteq \mathcal{A}_8$)	$f(x)$	Remarks
$\mathbf{Z}_8$	$x^8 - 68x^6 + 918x^4 - 612x^2 + 17$	$spl(f) = \mathbf{Q}(\zeta_{17} + \zeta_{17}^{-1})$ [D]
G_{16a}	$x^8 - 8x^4 - 2$	$f = (x^4 - (2^{1/4} + 2^{3/4})^2) \times$ $(x^4 + (2^{1/4} - 2^{3/4})^2)$ [D]
G_{16b}	$x^8 - 20x^6 + 100x^4 - 160x^2 + 80$	$f = \prod_{\sigma \in \mathbf{Z}_4}(x^2 - \sigma(\alpha + 2\sqrt{\alpha/2} + 2\sqrt{\beta/2}))$ $\alpha = 5 + \sqrt{5}$, $\beta = 5 - \sqrt{5}$ [D]
G_{16c}	$x^8 - 2$	[D]
G_{32a}	$x^8 - 16x^4 - 98$	$f = (x^4 - (2^{1/4} + 2(2)^{3/4})^2) \times$ $(x^4 + (2^{1/4} - 2(2)^{3/4})^2)$ [D]
G_{32b}	$x^8 - 5x^4 + 5$	$Gal(x^4 - 5x^2 + 5) = \mathbf{Z}_4$ [D]
G_{32c}	$x^8 + 2x^4 + 2$	
G_{32d}	$x^8 + 8x^6 + 31x^4 + 60x^2 + 45$	$f = (x^2 + 2)^4 + 7(x^2 + 2)^2 + 4$ [D]
G_{48}	$x^8 - 44x^2 - 44$	
G_{64a}	$x^8 + x^4 + 2$	$Gal(x^4 + x^2 + 2) = D_4$ [D]
G_{64b}	$x^8 + 4x^6 + 10x^4 + 12x^2 + 7$	$Gal(x^4 + 4x^3 + 10x^2 + 12x + 7) = \mathbf{Z}_4$ [D]

Table 7: Rational polynomials with degree 8 Galois groups - $G \not\subseteq \mathcal{A}_8$

Group ($G \not\subseteq \mathcal{A}_8$)	$f(x)$	Remarks
G_{64c}	$x^8+4x^6+8x^4+8x^2+2$	$Gal(x^4+4x^3+8x^2+8x+2) = D_4$ [D]
G_{64d}	$x^8-4x^6+4x^4-2$	
G_{64e}	$x^8+4x^6+7x^4+6x^2+6$	$Gal(x^4+4x^3+7x^2+6x+6) = V_4^1$ [D]
G_{128}	$x^8+4x^6+7x^4+6x^2+5$	$Gal(x^4+4x^3+7x^2+6x+5) = D_4$ [D]
G_{192a}	x^8+8x^2+12	
G_{192b}	x^8+12x^2-9	
$PGL(2,i)$	$x^8+x^7+7x^6+x+1$	[M]
G_{384}	x^8+x^2+2	
G_{576}	$x^8-4x^6+x^4-4x^3$ $+2x^2+4x+2$	
G_{1152}	x^8+4x^5+8	
$\mathcal{S}_8$	x^8+x+2	

Table 7: (continued) Rational polynomials with degree 8 Galois groups $G \not\subseteq \mathcal{A}_8$

A.1 Polynomials of the form $f(x^2)$. Notice that if $f = f(x^2)$ then $\mathcal{G}al(f)$ has a system of imprimitivity with blocks of size 2 (see Section 1.4). Conversely, given f such that $\mathcal{G}al(f)$ is imprimitive with blocks of size 2, we can construct $\tilde{f}$ with $\mathcal{G}al(\tilde{f}) = \mathcal{G}al(f)$ and such that $\tilde{f} = \tilde{f}(x^2)$. For let f be such a polynomial, $\partial f = 2n$. Then by Proposition 1.4.2 there are g and h such that $f \mid goh$ with g irreducible and $\partial g = n$. Roots α_i and α_j of f are in the same block iff $h(\alpha_i) = h(\alpha_j)$ (see proof of Proposition 1.4.2). We may order the roots such that $h(\alpha_{2i}) = h(\alpha_{2i-1})$.

Let

$$\tilde{f} = \prod_{i=1}^{n}(x^2 - (\alpha_{2i} - \alpha_{2i-1})^2).$$

(If $\tilde{f}$ is reducible, apply a Tschirnhaus transformation to the original f. Alternatively, choose $l \in k[x]$ and let $\gamma_i = (\alpha_{2i} - \alpha_{2i-1})l(h(\alpha_{2i}))$. Then $\tilde{f} = \prod_{i=1}^{n}(x^2 - \gamma_i^2)$ will also work provided it is irreducible.)

Evidently $\tilde{f} = \tilde{f}(x^2)$ and $spl(\tilde{f}) \subseteq spl(f)$. By the fundamental theorem of Galois theory (see also Proposition 1.5.10), $\mathcal{G}al(\tilde{f})$ is a representation of $\mathcal{G}al(f)$ acting on

$$rts(\tilde{f}) = \{\pm(\alpha_{2i} - \alpha_{2i-1}) \mid i = 1, \ldots, n\}.$$

It suffices to show that the representation is faithful. Suppose a $\sigma \in \mathcal{G}al(f)$ acts as the identity on $rts(\tilde{f})$. Since $\tilde{f}$ is constructed to be irreducible and $char(k) = 0$, the roots are distinct. Hence σ fixes each of the blocks. On the other hand σ also fixes the two elements within each block for otherwise it interchanges the roots $\alpha_{2i} - \alpha_{2i-1}$ and $\alpha_{2i-1} - \alpha_{2i}$ of $\tilde{f}$. Thus σ is the identity of $\mathcal{G}al(f)$ and the representation is faithful.

Note that $\tilde{f}$ may also be constructed as a resultant. Let $\beta_1 = h(\alpha_1)$ be a root of g. Let ϕ be the minimal polynomial of α_1 over $k(\beta_1)$. Then

$$\begin{aligned}\partial\phi &= [k(\alpha_1) : k(\beta_1)] \\ &= [k(\alpha_1) : k]/[k(\beta_1) : k] \\ &= \partial f/\partial g \\ &= 2n/n = 2\end{aligned}$$

Since $\beta_1 = h(\alpha_1) = h(\alpha_2)$, the roots α_1 and α_2 of f are conjugate over $k(\beta_1)$. Of course α_1 is one root of ϕ; the other must be α_2. Hence the discriminant of ϕ is $\Delta_\phi = (\alpha_1 - \alpha_2)^2$. Since $\Delta_\phi \in k(\beta_1)$, it may be written as a function of β_1 and we can construct the resultant

$$resultant_{\beta_1}(x^2 - \Delta_\phi^2, g(\beta_1)) = \tilde{f} = \prod_{i=1}^{n}(x^2 - (\alpha_{2i} - \alpha_{2i-1})^2).$$

(Again, if the resultant is reducible, apply a Tschirnhaus transformation to f.)

For each of the 36 degree 8 groups with a system of imprimitivity consisting of blocks of size 2 the example in the tables is of the form $f(x^2)$. The remarks for these examples indicate other methods for obtaining polynomials of the form $f \sim f(x^2)$.

A.2 Additional Remarks on the Derivation of the Polynomials. We have given some indication of the derivation of the polynomials in remarks in the tables. However, more details are in order in several cases:

$(\mathbf{Z}_2 \times \mathbf{Z}_4)^+$

Let g be the polynomial with roots $\zeta_5^i \pm \sqrt{2}$, $i = 1, \ldots, 4$. The example f of Table 6 is derived from g via the *smallpolred* command of PARI [BBCO]. (This command performs Tschirnhaus transformations on a polynomial in an attempt to find a new polynomial with smaller coefficients and the same splitting field.)

$(2^5)^+$

Let $g = \prod(x \pm \sqrt{2} \pm \sqrt{3} \pm \sqrt{5})$. The example f of Table 6 is derived from g using *smallpolred*.

D_4^+

Note that $Gal(x^4 - 2) = D_4$. Hence, $R(x_1 + 2x_2, x^4 - 2)$ (the 2-sequence resolvent) has a factor g of degree 8. The example f of Table 6 is derived from g by *smallpolred*.

Q_8^+

$$f = \prod(x \pm \sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})})$$

G_{16a}^+

With the generators of Table 10, G_{16a}^+ acts on the system

$$\{(i, i+4) | i = 1, \ldots, 4\}$$

as the Klein *Vierergruppe* V_4. Therefore, an extension of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ was sought. The extension $\mathbf{Q}(\sqrt{2}, \sqrt{3}, i, \sqrt{\sqrt{2} + \sqrt{3}})$ has degree 16.

G_{16b}^+

Since G_{16b}^+ acts as $\mathbf{Z}_4$ on the system of imprimitivity $\{(12), (34), (56), (78)\}$, we are lead to an extension of $\mathbf{Q}(\zeta_5)$.

G_{16c}^+

Since G_{16c}^+ acts as V_4 on its system of imprimitivity, we seek an extension of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$. The normal closure of $\mathbf{Q}(\sqrt{12 + 7\sqrt{6} + 12\sqrt{2} + 7\sqrt{3}})$ has degree 16. The polynomial f given in Table 6 is derived by *smallpolred* from

$$g = \prod_{\sigma \in \mathcal{G}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})} (x^2 - \sigma(12 + 7\sqrt{6} + 12\sqrt{2} + 7\sqrt{3})).$$

$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$

The polynomial has roots $\{\alpha i, -\alpha i | \alpha \in rts(x^4 + 8x + 12)\}$. Note that the Galois group of $x^4 + 8x + 12$ is $\mathcal{A}_4$.

$\mathcal{S}_4^+$

Let $g = x^4 + 2x + 3$. Then $\mathcal{G}al(g) = \mathcal{S}_4$ and g has discriminant $\Delta = 5(36)^2$. The polynomial f of Table 6 has roots $\{\pm\sqrt{5}\alpha \mid \alpha \in rts(g)\}$.

G_{64}^+

Let $\alpha_1, \ldots, \alpha_8$ be the roots of f with $\alpha_1^2 = \alpha_3^2$, $\alpha_2^2 = \alpha_4^2$, $\alpha_5^2 = \alpha_7^2$ and $\alpha_6^2 = \alpha_8^2$. Let $\beta_i = \alpha_i^2$, $i = 1, \ldots, 4$. Let

$$\begin{aligned}
\tau_1 &= (\alpha_2\alpha_3 + \alpha_1\alpha_4)(\alpha_5\alpha_7 + \alpha_6\alpha_8) \\
\tau_2 &= (\alpha_3\alpha_4 + \alpha_1\alpha_2)(\alpha_5\alpha_7 + \alpha_6\alpha_8) \\
\tau_3 &= (\alpha_6\alpha_7 + \alpha_5\alpha_8)(\alpha_1\alpha_3 + \alpha_2\alpha_4) \\
\tau_4 &= (\alpha_5\alpha_6 + \alpha_7\alpha_8)(\alpha_1\alpha_3 + \alpha_2\alpha_4)
\end{aligned}$$

Then using the representation given by Table 10, G_{64}^+ acts as D_4 on the β_i and as V_4 on the τ_i.

$\mathbf{Z}_8$

Let g be the polynomial with roots $\zeta_{17}^i + \zeta_{17}^{-i}$, $i = 1, \ldots, 8$ (so that $\mathcal{G}al(g) \cong \mathbf{Z}_8$). The $3_\times$-set resolvent of g has a factor

$$h(x) = x^8 + 4x^7 - 10x^6 - 44x^5 - 2x^4 + 74x^3 + 61x^2 + 16x + 1$$

The polynomial of Table 7 is $256h((x-1)/2)$.

G_{16a}

For the polynomial with roots $\pm\sqrt{\pm(a2^{1/4}+b2^{3/4})}$, $\pm\sqrt{\pm(ai2^{1/4}-bi2^{3/4})}$, let δ_1, δ_2 be the roots $\sqrt{a2^{1/4}+b2^{3/4}}$ and $\sqrt{ai2^{1/4}-bi2^{3/4}}$. Then

$$\begin{aligned}\delta_1\delta_2 &= \sqrt{i}\sqrt[4]{2}\sqrt{a^2-2b^2}\\ &= ((1+i)/\sqrt{2})\sqrt[4]{2}\sqrt{a^2-2b^2}.\end{aligned}$$

So, we want to choose a, b such that $\sqrt{a^2-2b^2} \in \mathbf{Q}(i,\sqrt{2})$. The polynomial in the table corresponds to the choice $a=b=1$.

G_{16b}

Note that $\mathcal{G}(\mathbf{Q}(\zeta_5)/\mathbf{Q}) = \mathbf{Z}_4$. But $\mathbf{Q}(\zeta_5) = \mathbf{Q}(\sqrt{5+\sqrt{5}})$. This explains how $\sigma \in \mathbf{Z}_4$ acts on $\alpha + 2\sqrt{\alpha/2} + 2\sqrt{\beta/2}$ $(\alpha, \beta = 5 \pm \sqrt{5})$.

G_{16c}

See G_{16a} above. For this polynomial we take $a=1, b=0$.

G_{32a}

Similar to G_{16a} above. In this case we choose a, b such that a^2-2b^2 is not a square in $spl(x^4-2)$. The example given corresponds to the choice $a=1$, $b=2$.

G_{32b}

Note that G_{32b} acts as $\mathbf{Z}_4$ on its 2^4 system of imprimitivity. The polynomial x^8-5x^4+5 is a good candidate since $\mathcal{G}al(x^4-5x^2+5) = \mathbf{Z}_4$ and the product of its roots is a square in $\mathbf{Q}(\sqrt{5}) = \mathbf{Q}(\sqrt{\Delta})$ (Δ is the discriminant).

G_{64a}, G_{64b}, G_{64c}, G_{64e}, G_{128}

For these groups we again use the β_i and τ_i defined for G_{64}^+ above.

Group	Action on β_i	Action on τ_i
G_{64a}	D_4	D_4
G_{64b}	$\mathbf{Z}_4$	D_4
G_{64c}	D_4	$\mathbf{Z}_4$
G_{64e}	V_4	D_4
G_{128}	D_4	D_4

A.3 Generalizations of Soicher's Method for $(2^3.L(3,2))^+$. We begin by repeating Soicher's [S2] construction of a polynomial with Galois group $(2^3.L(3,2))^+$. Let $f = x^7 - 7x^3 + 14x^2 - 7x + 1$ ($\mathcal{G}al(f) = L(3,2)^+$). Under an appropriate labelling of the roots $\alpha_1, \ldots, \alpha_7$ of f,

$$\mathcal{G}al(f) = <(1,2,3,4,5,6,7),(1,3)(4,5)> .$$

Taking $h(x) = f(x^2)$ we may label the roots $\beta_1, \ldots, \beta_{14}$ of h such that $\beta_{2i} = \alpha_i^{1/2}$ and $\beta_{2i-1} = -\beta_{2i}$ $(i = 1, \ldots, 7)$. Then, $H = \mathcal{G}al(h) = <A, B, C> = 2^7.L(3,2)$ where

$$A = (1,3,5,7,9,11,13)(2,4,6,8,10,12,14),$$

$$B = (1,5)(2,7)(7,9)(8,10), \quad C = (1,2).$$

Let $K = <A, B, D, E> = 2^4.L(3,2)$ be the subgroup of H with generators A, B as above and

$$D = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14),$$

$$E = (1,2)(7,8)(11,12)(13,14).$$

Then, if we define

$$\begin{aligned}\gamma &= \sum \beta_{2i}\beta_{2j}\beta_{2k}\beta_{2l}(i,j,k,l \in \{1,4,6,7\}^{\mathcal{G}al(f)}) \\ &= \beta_{2(1)}\beta_{2(4)}\beta_{2(6)}\beta_{2(7)} + \beta_{2(1)}\beta_{2(2)}\beta_{2(3)}\beta_{2(6)} + \beta_{2(1)}\beta_{2(2)}\beta_{2(5)}\beta_{2(7)} + \beta_{2(1)}\beta_{2(3)}\beta_{2(4)}\beta_{2(5)} \\ &\quad + \beta_{2(2)}\beta_{2(3)}\beta_{2(4)}\beta_{2(7)} + \beta_{2(2)}\beta_{2(4)}\beta_{2(5)}\beta_{2(6)} + \beta_{2(3)}\beta_{2(5)}\beta_{2(6)}\beta_{2(7)},\end{aligned}$$

we see that $stab_H(\gamma) = K$.

The images of γ under H are $\gamma_i = \gamma^{(2i-1,2i)}$ $(i = 1, \ldots, 7)$ and $\gamma_8 = \gamma$. So using high-precision approximations to the roots of f, we may construct

$$t(x) = \prod_{i=1}^{8}(x - \gamma_i)$$

and it follows from the method of construction that

$$\mathcal{G}al(t) = H/(\bigcap_{P \in H} P^{-1}KP) = (2^3.L(3,2))^+.$$

The polynomials for $(2^3.\mathbf{Z}_7)^+$ and $(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$ may be generated in exactly the same way except that we begin with polynomials f such that $\mathcal{G}al(f) = \mathbf{Z}_7$ and $\mathbf{Z}_7.\mathbf{Z}_3$ respectively. For $(2^3.\mathbf{Z}_7)^+$ we take

$$f = x^7 - 13x^6 - 27x^5 + 299x^4 - 83x^3 - 113x^2 - 6x + 1$$

and label the roots as

$$\alpha_1 \approx -4.98,\ \alpha_2 \approx -0.14,\ \alpha_3 \approx -0.43,\ \alpha_4 \approx 0.07,$$

$$\alpha_5 \approx 0.84,\ \alpha_6 \approx 4.25,\ \alpha_7 \approx 13.4.$$

(Although Soicher relates his root labelling to a specific permutation representation of $(2^3.L(3,2))^+$, we found it easier to simply experiment with different labellings until we find one which results in integer coefficients for $t(x)$. Once we have $t(x)$, we can check that $\mathcal{G}al(t) = (2^3.\mathbf{Z}_7)^+$ using the algorithm of Section 2.2.) We find that

$$u(x) = t(2x)/256 = x^8 + 34x^6 + 12x^5 + 405x^4 - 402x^3 - 912x^2 + 721x + 2063.$$

The polynomial reported in Table 6 is derived from u by the *smallpolred* command of PARI.

In the case of $(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$, we use

$$f = x^7 - 28x^5 + 224x^3 - 448x + 192$$

with roots

$$\alpha_1 \approx 3.76,\ \alpha_2 \approx 3.41,\ \alpha_3 \approx 1.29,\ \alpha_4 \approx -2.16,$$

$$\alpha_5 \approx 0.48,\ \alpha_6 \approx -2.80,\ \alpha_7 \approx -3.98.$$

Then,

$$u(x) = t(4x)/4^8 = x^8 + 28x^6 + 112x^5 + 294x^4 + 1568x^3 + 4508x^2 + 5968x + 21553.$$

The polynomial given in the tables is constructed from u by *smallpolred*

We may use a similar technique to find polynomials for G^1_{96b} and G^1_{96a}. Let us begin with G^+_{96b}. This group can be written as $2^3.\mathcal{A}_4$. If we notice that G_{192a} $2^4.\mathcal{A}_4$, then, in analogy with the $(2^3.L(3,2))^+$ case, we are led to look for subgroups K of G_{192a} of index 8 such that $|\bigcap_{P\in G_{192a}} P^{-1}KP| = 2$.

Let

$$\begin{aligned} f &= (x+1)^8 + 8(x+1)^2 + 12 \\ &= x^8 + 8x^7 + 28x^6 + 56x^5 + 70x^4 + 56x^3 + 36x^2 + 24x + 21 \end{aligned}$$

so that $\mathcal{G}al(f) = G_{192a}$. To find an appropriate ordering of the roots, it is convenient to use Stauduhar's [St1] method. In the notation of [St1], $G_{192a} = G^2_{192}$ and although different generators are given, the permutation representation of G^2_{192} is in fact that of Table 10: $G_{192a} = <e, n, v>$ where

$$e = (1,7)(2,8)(3,5)(4,6),$$

$$n = (3,5,7)(4,6,8),\quad v = (3,4).$$

Then, to fix a correct ordering of the roots $\alpha_1, \ldots, \alpha_8$ of f, we must ensure that $\Delta(\alpha_1\alpha_2, \alpha_3\alpha_4, \alpha_5\alpha_6, \alpha_7\alpha_8)$ (that is, the discriminant of the polynomial with roots $\alpha_1\alpha_2, \ldots, \alpha_7\alpha_8$) is an integer. One such ordering is

$$\alpha_1 \approx -2.35 + 0.68i,\ \alpha_2 \approx 0.35 - 0.68i,\ \alpha_3 = \overline{\alpha_1},\ \alpha_4 = \overline{\alpha_2},$$

$$\alpha_5 \approx -1.27 - 1.20i,\ \alpha_6 \approx -0.73 + 1.20i,\ \alpha_7 = \overline{\alpha_5},\ \alpha_8 = \overline{\alpha_6}.$$

A suitable choice for K is $(\mathbf{Z}_2 \times \mathcal{A}_4)^+$ represented as $<A, B, C>$ where

$$A = (1,6,8)(2,5,7),\ \ B = (3,8,6)(4,7,5),$$

$$C = (1,5)(2,6)(3,7)(4,8).$$

An element γ such that $stab_{2^4.\mathcal{A}_4}(\gamma) = (\mathbf{Z}_2 \times \mathcal{A}_4)^+$ is

$$\gamma = \alpha_1\alpha_3\alpha_6 + \alpha_1\alpha_3\alpha_8 + \alpha_1\alpha_6\alpha_8 + \alpha_2\alpha_4\alpha_5 +$$
$$\alpha_2\alpha_4\alpha_7 + \alpha_2\alpha_5\alpha_7 + \alpha_3\alpha_6\alpha_8 + \alpha_4\alpha_5\alpha_7.$$

(We constructed γ by looking at the orbit of $\{3,6,8\}$ under the action of the group $(\mathbf{Z}_2 \times \mathcal{A}_4)^+$.)

The images of γ under $2^4.\mathcal{A}_4$ are $\gamma_i = \gamma^{\sigma_i}$ $(i = 1, \ldots, 8)$ where the σ_i are right coset representatives (see page 14) of $(\mathbf{Z}_2 \times \mathcal{A}_4)^+$ in $2^4.\mathcal{A}_4$:

$$(3,4),\ (5,6),\ (7,8),\ (3,4)(7,8),\ (3,4)(5,6),\ (3,4)(5,6)(7,8),\ (5,6)(7,8).$$

(Note that if we take $x^8 + 8x^2 + 12$ as the polynomial f, then we find that all the γ_i are zero. This is why we first make a Tschirnhaus transformation $x \mapsto x + 1$.)

Finally, we construct $t = \prod_{i=1}^{8}(x - \gamma_i)$ using high-precision approximations to the roots of f. Taking

$$u(x) = t(8(x-1))/8^8 = x^8 - 16x^5 - 102x^4 + 64x^2 - 48x + 9$$

we have,

$$\mathcal{G}al(u) = 2^4.\mathcal{A}_4/(\bigcap_{P\in 2^4.\mathcal{A}_4} P^{-1}(2\times\mathcal{A}_4)P) = 2^3.\mathcal{A}_4 = G^+_{96b}.$$

The polynomial given in Table 6 is derived from u by the *smallpolred* command of PARI.

In the case of G^+_{96c}, we note that G^+_{192a} has a normal subgroup N of order 2 such that $G^+_{192a}/N = G^+_{96c}$. So, again we look for a subgroup K of index 8 in G^+_{192a} such that $\bigcap_{P\in G^+_{192a}} P^{-1}KP = N$. In Stauduhar's [St1] notation, $G^+_{192a} = G^+_{192}$ and his representation is the same as that of Table 10: $G^+_{192a} = <j, n, s>$ where

$$j = (1,6)(2,5)(3,7)(4,8),$$

$$n = (3,5,7)(4,6,8), \quad s = (1,3)(2,4).$$

Let

$$f = x^8 - 10x^7 + 87x^6 - 504x^5 + 1890x^4 - 4536x^3 + 6804x^2 - 5832x + 2187$$

with $\mathcal{G}al(f) = G^+_{192a}$. ($f$ is a Tschirnhaus transformation of $x^8 + x^2 + 1$.) By [St1], a correct labelling of the roots $\alpha_1, \ldots, \alpha_8$ of f, results in an integer value for $\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_5\alpha_6 + \alpha_7\alpha_8$. One such labelling is

$$\alpha_1 \approx 0.30 + 6.26i,\ \alpha_2 \approx 1.43 - 0.35i,\ \alpha_3 = \overline{\alpha_1},\ \alpha_4 = \overline{\alpha_2},$$

$$\alpha_5 \approx 1.60 + 1.14i,\ \alpha_6 \approx 1.67 - 1.96i,\ \alpha_7 = \overline{\alpha_5},\ \alpha_8 = \overline{\alpha_6}.$$

A suitable candidate for K is $<A, B, C>$ where

$$A = (1,6,2,5)(3,7,4,8), \quad B = (1,3,5)(2,4,6),$$

$$C = (1,7,2,8)(3,5,4,6).$$

Let

$$\gamma = \alpha_1\alpha_3\alpha_5 + \alpha_1\alpha_4\alpha_8 + \alpha_1\alpha_6\alpha_7 + \alpha_2\alpha_3\alpha_7 +$$

$$\alpha_2\alpha_4\alpha_6 + \alpha_2\alpha_5\alpha_8 + \alpha_3\alpha_6\alpha_8 + \alpha_4\alpha_5\alpha_7$$

so that $stab_{G_{192a}^+}(\gamma) = K$. As before, we define $\gamma_i = \gamma^{\sigma_i}$ for a set $\{\sigma_1, \ldots, \sigma_8\}$ of coset representatives of K in G_{192a}^+ and construct $t = \prod_{i=1}^{8}(x - \gamma_i)$. Then

$$u(x) = t(18(x+4))/18^8 = x^8 + 64x^6 - 16x^5 + 1280x^4 - 512x^3 + 8256x^2 - 2048x + 1728$$

has Galois group G_{96c}^+.

In fact, the polynomial of Table 6 is derived in a different way; it is a transformation (by *smallpolred*) of the degree 8 factor of the 4-diff resolvent of a polynomial with Galois group G_{192b}.

B Polynomials over $\mathbf{Q}(t)$

In Table 8 we present polynomials over $\mathbf{Q}(t)$ with selected Galois groups. Except where otherwise noted, these polynomials were all provided to us by Gene Smith [Sm]. Note that we can always construct a polynomial over $\mathbf{Q}(t)$ with group G simply by homogenizing a rational polynomial with that group. None of the polynomials in the table are of this form.

The table also reports CPU use by our MAPLE V implementation running on a SPARC station 2. For those computations which took particularly long, the main reason was the manipulation of a resolvent polynomial. We have included comments indicating x-degree and percentage of time spent factoring or constructing such a resolvent in these cases.

LaMacchia [LM] has given an example of a polynomial with group $PSL(3,2)^4$ over $\mathbf{Q}(t_1,t_2)$

$$(x+1)(x^3+2(1-2t_1)x^2+2(4t_1-1)x-4t_1)(x^3-(1+2t_1)x^2+2t_1x+2t_1^2)+t_2x^3(1-x).$$

The program requires 6765.8 seconds of CPU to determine the Galois group. Most of the time was spent on a 3_x-set resolvent (x-degree = 35); construction of the resolvent required 79% of the total and factoring took 20%.

Group	$f(x) \in \mathbf{Q}(t)[x]$	CPU Used (seconds)
$\mathcal{A}_3^+$	$x^3 + tx^2 + (t-3)x - 1$	0.2
$\mathcal{S}_3$	$x^3 - tx + t$ [M]	0.4
$\mathcal{A}_4^+$	$x^3(x-4) + t^2 + 27$	0.3
$\mathbf{Z}_4$	$x^4 + tx^3 - 6x^2 - tx + 1$	7.9
D_4	$x^4 - (-1 + t^2 - t)x^3 + (1 + 2t^2 - 2t)x^2 - (-1 + t^2 - t)x + 1$	5.7
$\mathcal{S}_4$	$x^4 - tx + t$ [M]	0.1
$\mathbf{Z}_5^+$	$1 - 10t^9 - 4t^{10} - 5tx^2 - 25t^2x^2 + 15t^3x + 30t^2x - 10t^5x$ $+20tx + x^5 - 10x^3 + 5x^2 - 25t^4x^2 - 10tx^3 - 25t^3x^2 - 10t^2x^3$ $+28t^5 + 20t^2 + 15t^6 + 10t + 10x + 30t^3 + 35t^4 - 10t^3x^3$ $+5t^7 - 5t^8 - 10t^4x^3 - 15t^8x - 30t^7x - 20t^6x - 20t^6x^2 - 30t^5x^2$	289.0
D_5^+	$x(x-5)^2(x+5)^2 - t(x-1)^2(x+3)$	8.3
$\mathcal{A}_5^+$	$x^5 + (t^2 - 3125)(x-4)$	1.9
$\mathbf{Z}_5.\mathbf{Z}_1$	$x^5 - 10tx^3 - 10t^2x^2 - 10tx^2 - 5t^2x - 5t^3x - 5tx - t^2 - t - t^4 - t^3$	6.4
$\mathcal{S}_5$	$x^5 - tx + t$ [M]	0.3
$\mathcal{A}_6^+$	$x^6 + tx^4 + (t-3)x^2 - 1$	29.5
$(\mathcal{S}_4/V_4)^+$	$x^6 - 4x^2 - t^2$	16.6
$(3^2.\mathbf{Z}_4)^+$	$x^4(x-6)^2 - t^2 - 1024$	23.1
$\mathcal{A}_6^+$	$x^5(x-6) - t^2 + 3125$	1.6

Table 8: Polynomials over $\mathbf{Q}(t)$ with selected Galois groups

Group	$f(x) \in \mathbf{Q}(t)[x]$	CPU (sec)	Remarks
D_6	$x^6 + tx^3 + 1$	12.0	
$\mathcal{S}_4/\mathbf{Z}_4$	$(x(x-t)+t^2)^3 - 4x(x-t) - 5t^2$	1327.3	81% factoring, $\partial_r = 21$ resolvent
$3^2.D_4$	$x^4(x-1)^2 - t$	13.3	
$PGL(2,5)$	$x^5(x-4) - t(x+1)$	153.1	
$\mathcal{S}_6$	$x^6 - tx + t$ [M]	2.0	
$PSL(3,2)^+$	$x(x-7)^3(x+7)^3 - t(x-9)(x-1)^3$	61.6	
$\mathcal{A}_7^+$	$x^7 - (t^2 + 823543)(x-6)$	3.3	
$\mathbf{Z}_7.\mathbf{Z}_6$	$x^7 - 21tx^5 - 35tx^4 - 35t^2x^4 - 35t^3x^3$ $-35t^2x^3 - 35tx^3 - 21t^3x^2 - 21t^4x^2 - 21tx^2$ $-21t^2x^2 - 7t^3x - 7t^2x - 7t^5x - 7t^4x$ $-7tx - t^4 - t^3 - t^2 - t - t^5 - t^6$	3404.4	97% factoring, $\partial_r = 35$ resolvent
$\mathcal{S}_7$	$x^7 - tx + t$ [M]	1.1	
G_{32a}	$x^8 - t$	487.9	
$PGL(2,7)$	$x^6(x^2+x+7) + t(x+1)$ [M]	16228.9	99% constructing, $\partial_r = 70$ resolvent
$(2^3.L(3,2))^+$	$x^8 - 24x^7 + 2128x^5 + 2184x^4 - 66528t^3$ $-28672x^2 - 243648x + 104976 - 87808x^2t$ [M]	8605.3	99% constructing, $\partial_r = 70$ resolvent
$\mathcal{A}_8^+$	$x^8 - 8x^7 + 5764801t^2 + 823543$ [M]	0.7	
$\mathcal{S}_8$	$x^8 - tx + t$ [M]	1.6	

Table 8: (continued) Polynomials over $\mathbf{Q}(t)$ with selected Galois groups

C Distinguishing G_{288}^+ from G_{576}^+

We have mentioned in Section 4.3 that a resolvent derived from a polynomial belonging to $(2^3.L(3,2))^+$ has degree 30 $(= |\mathcal{S}_8 : (2^3.L(3,2))^+|)$. Aside from its low degree, this resolvent is attractive because it provides a simple test which distinguishes between G_{288}^+ and G_{576}^+.

An example of a polynomial belonging to $(2^3.L(3,2))^+$ is

$$F = x_1x_5x_6x_8 + x_2x_3x_4x_7 + x_2x_6x_7x_8 + x_1x_3x_4x_5 + x_1x_3x_7x_8 +$$
$$x_2x_4x_5x_6 + x_1x_2x_4x_8 + x_3x_5x_6x_7 + x_1x_4x_6x_7 + x_2x_3x_5x_8 +$$
$$x_3x_4x_6x_8 + x_1x_2x_5x_7 + x_4x_5x_7x_8 + x_1x_2x_3x_6.$$

Given a labelling $\alpha_1, \ldots, \alpha_8$ of the roots of f, the root $F(\alpha_1, \ldots, \alpha_8)$ of $R_{30} = R(F, f)$ may be represented (using the subscripts) as

$$1568 + 1345 + 1378 + 1248 + 1467 + 1257 + 1236 +$$
$$2347 + 2678 + 2456 + 3567 + 2358 + 3468 + 4578.$$

However, on examining this notation, we see that for every 4-ad its complement in $\{1, 2, 3, \ldots, 8\}$ also occurs. So we can simplify our notation by writing only the 4-ads in which '1' occurs:

$$F(\alpha_1, \ldots, \alpha_8) = 1568 + 1345 + 1378 + 1248 + 1467 + 1257 + 1236.$$

According to Table 10,

$$G_{288}^+ = < s, z, m >$$

and

$$G_{576}^+ = < s, z, m, y >$$

where

$$s = (1,3)(2,4), \quad m = (1,5)(2,6)(3,7)(4,8),$$

$$z = (6,8,7), \quad y = (1,8)(2,5)(3,6)(1,7).$$

Using this representation, we find that both groups partition the roots of R_{30} into 4 orbits; 2 of length 12 and 2 of length 3. The two orbits of length 3 are $\mathcal{O}_1 = \{\beta_1, \beta_2, \beta_3\}$ and $\mathcal{O}_2 = \{\beta_4, \beta_5, \beta_6\}$ where

$$\begin{aligned}
\beta_1 &= 1367 + 1468 + 1256 + 1358 + 1457 + 1278 + 1234 \\
\beta_2 &= 1234 + 1368 + 1267 + 1456 + 1478 + 1258 + 1357 \\
\beta_3 &= 1378 + 1467 + 1257 + 1234 + 1458 + 1268 + 1356 \\
\beta_4 &= 1378 + 1468 + 1457 + 1234 + 1267 + 1258 + 1356 \\
\beta_5 &= 1257 + 1367 + 1358 + 1234 + 1268 + 1456 + 1178 \\
\beta_6 &= 1467 + 1256 + 1278 + 1234 + 1458 + 1368 + 1357
\end{aligned}$$

The action of G_{288}^+ on $\mathcal{O}_1$ yields the permutations $(\beta_1, \beta_2, \beta_3)$ and $(\beta_3, \beta_2, \beta_1)$ as well as the identity. So G_{288}^+ acts as $\mathcal{A}_3$ on $\mathcal{O}_1$. On the other hand, the action on $\mathcal{O}_2$ gives all possible permutations. Hence G_{288}^+ acts on $\mathcal{O}_2$ as $\mathcal{S}_3$.

Since $G_{288}^+ \subseteq G_{576}^+$, we see that G_{576}^+ will likewise act as $\mathcal{S}_3$ on $\mathcal{O}_2$. But the generator y of G_{576}^+ induces the transposition (β_1, β_3). Combined with the permutations already found for G_{288}^+, this proves that the action on $\mathcal{O}_1$ is now $\mathcal{S}_3$.

So R_{30} can be used to distinguish between G_{288}^+ and G_{576}^+. Under either of these groups it has two irreducible factors g_1 and g_2 of degree 3. If $Gal(f) = G_{576}^+$ then both g_1 and g_2 have $\mathcal{S}_3$ as Galois group. But if $Gal(f) = G_{288}^+$ then one of g_1 and g_2 has Galois group $\mathcal{A}_3$ and the other has Galois group $\mathcal{S}_3$.

This may be contrasted with the algorithm we have presented in Section 2.2 which, in order to distinguish these groups, requires factorization of a degree 66 polynomial (the 2_X-set resolvent derived from the degree 12 factor of the 2_Y set resolvent of the original polynomial f; see Table 2). As this resolvent has higher

degree than R_{30}, it may take longer to factor. For example, let

$$f = x^8 + 7x^4 + 8x^3 + 9$$

($Gal(f) = G_{288}^+$). Factoring the degree 66 resolvent of f requires 1200 seconds of CPU on a SPARC station 2. Factoring R_{30} (constructed using complex approximations to the roots) takes only 4 seconds of CPU.

Since it is much faster to factor R_{30} than the degree 66 polynomial required by our algorithm, it appears that we could improve the algorithm by using this new resolvent. However, as noted in Section 4.3, it is not clear how to construct it; construction by complex approximations to the roots is available only when $k = \mathbf{Q}$ and even then it is to be avoided.

D Tables of Degree 8 Transitive Groups

The following tables, taken from [BM] and [MR], give information about the degree 8 transitive groups. Table 9 includes the group order, parity and which systems of imprimitivity it admits to. If there is more than one system for a given block size, we indicate how many such systems there are. This table also relates the 'Tn' notation of [BM, MR] to the '$G^{\sigma}_{n\alpha}$' notation used here. In the final column of Table 9 we give a description of the group structure. The descriptions of the imprimitive groups are drawn from [HK]. The notation is as follows:

$\mathbf{Z}_n$ The cyclic group of order n.

p^k An elementary abelian group of order p^k where p is prime.

V_4 The Klein *Vierergruppe*.

D_n The dihedral group of degree n and order $2n$.

Q_8 The quaternions.

$<l,m|n>$ The group $<x,y|x^l=y^m,(xy)^n=e>$ where e is the identity

$(l,m|n,k)$ The group $<x,y|x^l=y^m=(xy)^n=(x^{-1}y)^k=e>$.

$A \times B$ The direct product of the groups A and B.

$A.B$ denotes a group with a normal subgroup isomorphic to A such that $A.B/A$ is isomorphic to B.

$A \circ B$ The central product of groups A and B. Let A and B have common center isomorphic to C. Then we have injections $\alpha : C \hookrightarrow A$, $\beta : C \hookrightarrow B$. The group $A \circ B$ is the quotient of $A \times B$ by the set of ordered pairs of the form $(\alpha(c), \beta(c))$, $c \in C$.

$A\Delta B$ The diagonal product of A and B. Let D be the largest common homomorphic image of the groups A and B. Then we have surjections $\gamma : A \to D$, $\delta : B \to D$. The group $A\Delta B$ is the subgroup of $A \times B$ consisting of the (a, b) for which $\gamma(a) = \delta(b)$.

$A \wr B$ The wreath product of the groups A and B. The group B is a permutation group on n letters. The wreath product is the semidirect product $A^n.B$ where

$$A^n = \underbrace{A \times \ldots \times A}_{n}$$

and B acts by permuting factors.

$Hol(A)$ The holomorph of the group A. Let $Aut(A)$ be the group of automorphisms. We construct $Hol(A)$ on the Cartesian product $A \times Hol(A)$ with the operation

$$(a_1, \phi_1)(a_2, \phi_2) = (a_1 a_2^{\phi_1^{-1}}, \phi_1\phi_2).$$

$Syl_p(A)$ The Sylow p-subgroup of the group A.

A superscript of '+' indicates that the group consists of even permutations.

Table 10 exhibits generators for each group. The shapes belonging to each group are shown in Table 11. Since every transitive degree 8 group has the shapes 1^8 and 2^4, we do not include these in the table. However, these are the only shapes in T3. Finally, Table 12 lists the orbit-length partition of sets and sequences under the action of the groups

Group	Order	Even	Imprimitive		Name	Description
			$[2^4]$	$[4^2]$		
T1	8		√	√	$\mathbf{Z}_8$	$\mathbf{Z}_8$
T2	8	+	3	√	$(\mathbf{Z}_2 \times \mathbf{Z}_4)^+$	$(\mathbf{Z}_2 \times \mathbf{Z}_4)^+$
T3	8	+	7	√	$(2^3)^+$	$(2^3)^+$
T4	8	+	5	√	D_4^+	D_4^+
T5	8	+	√	√	Q_8^+	Q_8^+
T6	16		√	√	G_{16a}	D_8
T7	16		√	√	G_{16b}	$<2,2\|2>$
T8	16		√	√	G_{16c}	$<-2,4\|2>$
T9	16	+	3	√	G_{16a}^+	$(\mathbf{Z}_2 \times D_4)^+$
T10	16	+	3	√	G_{16b}^+	$(4,4\|2,2)^+$
T11	16	+	√	√	G_{16c}^+	$<x^2, y^2, z^2, xyz - yzx - zxy$
T12	24	+	√		$SL(2,3)^+$	$SL(2,3)^+$
T13	24	+	√	√	$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$	$(\mathbf{Z}_2 \times \mathcal{A}_4)^+$
T14	24	+	√	√	$\mathcal{S}_4^+$	$\mathcal{S}_4^+$
T15	32		√	√	G_{32a}	$\mathbf{Z}_8.V_4$
T16	32		√	√	G_{32b}	$<x^8, (xy)^2, x^4y^4, y^2x^{-1}y^2x$
T17	32		√	√	G_{32c}	$\mathbf{Z}_4 \wr \mathbf{Z}_2$

Table 9: Transitive groups of degree 8

Group	Order	Even	Imprimitive		Name	Description
			$[2^4]$	$[4^2]$		
T18	32	+	3	√	G^+_{32a}	$(V_4 \wr \mathbf{Z}_2)^+$
T19	32	+	√	√	G^+_{32b}	$<x^4, y^2, (xy)^4, x^2yxyx^2yx^3y>^+$
T20	32	+	√	√	G^+_{32c}	$<x^4, y^2, (xy)^4, x^2yxyx^2yx^3y>^+$
T21	32		√	√	G_{32d}	$<x^4, y^2, (xy)^4, x^2yxyx^2yx^3y>$
T22	32	+	√	√	G^+_{32d}	$(Q_8 \circ Q_8)^+$
T23	48		√		G_{48}	$GL(2,3)$
T24	48	+	√	√	$(\mathbf{Z}_2 \times \mathcal{S}_4)^+$	$(\mathbf{Z}_2 \times \mathcal{S}_4)^+$
T25	56	+			$(2^3.\mathbf{Z}_7)^+$	$(2^3.\mathbf{Z}_7)^+$
T26	64		√	√	G_{64a}	$Hol(\mathbf{Z}_2 \times \mathbf{Z}_4)$
T27	64		√	√	G_{64b}	$<x^8, y^4, (xy)^2, (x^3y)^4, (x^2y^2)^2>$
T28	64		√	√	G_{64c}	$<x^8, y^4, (xy)^2, (x^3y)^4, (x^2y^2)^2>$
T29	64	+	√	√	G^+_{64}	$Syl_2(\mathbf{Z}_2 \wr \mathcal{A}_4)^+$
T30	64		√	√	G_{64d}	$<x^4, y^4, (xy)^2, (xy^2)^4, (x^3y)^4>$
T31	64		√	√	G_{64e}	$Syl_2(\mathbf{Z}_2 \times \mathcal{A}_4)$
T32	96	+	√		G^+_{96a}	$((Q_8 \circ Q_8).\mathbf{Z}_3)^+$
T33	96	+		√	G^+_{96b}	$((V_4 \wr \mathbf{Z}_2).\mathbf{Z}_3)^+$
T34	96	+		√	G^+_{96c}	$((\mathcal{A}_4 \triangle \mathcal{A}_4).\mathbf{Z}_2)^+$

Table 9: (continued) Transitive groups of degree 8

Group	Order	Even	Imprimitive		Name	Description
			$[2^4]$	$[4^2]$		
T35	128		√	√	G_{128}	$Syl_2(\mathcal{S}_8)$
T36	168	+			$(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$	$(2^3.(\mathbf{Z}_7.\mathbf{Z}_3))^+$
T37	168	+			$L(2,7)^+$	$L(2,7)^+$
T38	192		√		G_{192a}	$\mathbf{Z}_2 \wr \mathcal{A}_4$
T39	192	+	√		G^+_{192a}	$(2^3.\mathcal{S}_4)^+$
T40	192		√		G_{192b}	$Hol(Q_8)$
T41	192	+		√	G^+_{192b}	$((\mathcal{S}_4 \triangle \mathcal{S}_4).\mathbf{Z}_2)^+$
T42	288	+		√	G^+_{288}	$(\mathcal{A}_4 \wr \mathbf{Z}_2)^+$
T43	336				$PGL(2,7)$	$PGL(2,7)$
T44	384		√		G_{384}	$\mathbf{Z}_2 \wr \mathcal{S}_4$
T45	576	+		√	G^+_{576}	$((\mathcal{S}_4 \times \mathcal{S}_4)^+.\mathbf{Z}_2)^+$
T46	576			√	G_{576}	$<x^6, y^4, (xy^2)^2, (x^3y^3)^4, (y^3xyx)^3>$
T47	1152			√	G_{1152}	$\mathcal{S}_4 \wr \mathbf{Z}_2$
T48	1344	+			$(2^3.L(3,2))^+$	$(2^3.L(3,2))^+$
T49	20160	+			$\mathcal{A}_8^+$	$\mathcal{A}_8^+$
T50	40320				$\mathcal{S}_8$	$\mathcal{S}_8$

Table 9: (continued) Transitive groups of degree 8

a	=	(1,4,6,8,2,3,5,7)	l	=	(1,3)(2,4)(5,8)(6,7)	w	=	(1,3)(2,4)(7,8)
b	=	(1,3,5,7)(2,4,6,8)	m	=	(1,5)(2,6)(3,7)(4,8)	x	=	(2,4,3)(6,8,7)
c	=	(1,6)(2,5)(3,8)(4,7)	n	=	(3,5,7)(4,6,8)	y	=	(1,8)(2,5)(3,6)(4,7)
d	=	(1,8)(2,7)(3,6)(4,5)	o	=	(1,4)(2,3)(5,6)(7,8)	z	=	(6,8,7)
e	=	(1,7)(2,8)(3,5)(4,6)	p	=	(1,2)(7,8)	A	=	(1,2,3,4,5,6,7)
f	=	(1,7)(2,8)(3,6)(4,5)	q	=	(1,6,2,5)(3,7)(4,8)	B	=	(2,4,3,7,5,6)
g	=	(1,7,2,8)(3,5,4,6)	r	=	(5,6)	C	=	(2,3)(4,7)
h	=	(3,4)(7,8)	s	=	(1,3)(2,4)	D	=	(1,8)(2,4)(3,7)(5,6)
i	=	(1,6)(2,5)(3,4)	t	=	(1,2)	E	=	(1,8)(2,7)(3,4)(5,6)
j	=	(1,6)(2,5)(3,7)(4,8)	u	=	(1,5)(2,6)	F	=	(1,7,3,5)(2,8,4,6)
k	=	(1,6)(2,5)	v	=	(3,4)			

T1	=	$<a>$	T18	=	$<b,e,j>$	T35	=	$<a,f,t>$
T2	=	$<b,c>$	T19	=	$<b,f>$	T36	=	$<A,D,B^2>$
T3	=	$<b^2,c,c>$	T20	=	$<b,p>$	T37	=	$<A,B^2,E>$
T4	=	$<b,d>$	T21	=	$<q,e>$	T38	=	$<v,e,n>$
T5	=	$<a^2,g>$	T22	=	$<a^2,b^2,j,e>$	T39	=	$<j,n,s>$
T6	=	$<a,f>$	T23	=	$<n,w>$	T40	=	$<j,n,shv>$
T7	=	$<a,h>$	T24	=	$<c,n,s>$	T41	=	$<F,x,y>$
T8	=	$<a,i>$	T25	=	$<A,D>$	T42	=	$<s,z,m>$
T9	=	$<b,c,c>$	T26	=	$<a,f,b^2>$	T43	=	$<A,B,E>$
T10	=	$<b,j>$	T27	=	$<a,t>$	T44	=	$<t,b,s>$
T11	=	$<a^2,b^2,l>$	T28	=	$<a,u>$	T45	=	$<s,z,m,y>$

Table 10: Group generators

T12	$=$	$<g,n>$	T29	$=$	$<b,e,f>$
T13	$=$	$<hj,n>$	T30	$=$	$<b,p,\iota ku>$
T14	$=$	$<n,o>$	T31	$=$	$<q,e,t>$
T15	$=$	$<a,f,h>$	T32	$=$	$<e,j,n>$
T16	$=$	$<a,b^2>$	T33	$=$	$<F,x>$
T17	$=$	$<a,e>$	T34	$=$	$<vsv,x,y>$

T46	$=$	$\prec s,z,q\succ$	
T47	$=$	$\prec vsxz^{-1},t,m\succ$	
T48	$=$	$\prec A,C,D\succ$	
T49	$=$	$\prec A,z\succ$	
T50	$=$	$\prec A,z,t\succ$	

Table 10: (continued) Group generators

Groups	Shapes	Groups	Shapes
T1	4^2, 8	T23	1^22^3, 1^23^2, 4^2, 26, 8
T2,T4,T5	4^2	T24,T32,T33	1^12^2, 1^23^2, 1^2, 26
T3	$(1^8, 2^4)$	T25	17
T6,T8	1^22^3, 4^2, 8	T26	1^12^2, 1^22^3, 1^14, 2^24, 4^2, 8
T7,T16	1^42^2, 4^2, 8	T27	1^62, 1^12^2, 1^22^3, 2^24, 4^2, 8
T9,T10,T11	1^42^2, 4^2	T28	1^12^2, 1^221, 2^24, 4^2, 8
T18,T20,T22		T30	1^42^2, 1^22^3, 1^14, 2^24, 4^2
T12	1^23^2, 4^2, 26	T31	1^62, 1^12^2, 1^22^3, 2^24, 4^2
T13	1^23^2, 26	T34	1^42^2, 1^23^2, 4^2
T14	1^23^2, 4^2	T35	1^62, 1^42^2, 1^22^3, 1^14,
T15	1^12^2. 1^22^3, 4^2,8		1^224, 2^24, 4^2, 8
T17	1^42^2, 1^14, 2^24, 4^2, 8	T36	1^23^2, 26, 17
T19,T29	1^42^2, 1^224, 4^2	T37	1^23^2, 4^2, 17
T21	1^42^2, 2^24, 4^2	T39,T41	1^42^2, 1^23^2, 1^224, 4^2, 26

Table 11: Shapes occurring in each group

Group	Shapes
T38	$1^6 2$, $1^4 2^2$, $1^2 2^3$, $1^2 3^2$, $2 3^2$, $2^2 4$, 4^2, $1^2 6$, 26
T40	$1^4 2^2$, $1^2 2^3$, $1^2 3^2$, $1^4 4$, $2^2 4$, 4^2, 26, 8
T42	$1^4 2^2$, $1^5 3$, $1 2^2 3$, $1^2 3^2$, 4^2, 26
T43	$1^2 2^3$, $1^2 3^2$, 4^2, $1^2 6$, 17, 8
T44	$1^6 2$, $1^4 2^2$, $1^4 2^3$, $1^2 3^2$, $2 3^2$, $1^4 4$, $1^2 24$, $2^2 4$, 4^2, $1^2 6$, 26, 8
T45	$1^4 2^2$, $1^5 3$, $1 2^2 3$, $1^2 3^2$, $1^2 24$, 4^2, 26
T46	$1^4 2^2$, $1^5 3$, $1 2^2 3$, $1^2 3^2$, $1^2 24$, $2^2 4$, 4^2, 8
T47	$1^6 2$, $1^4 2^2$, $1^4 2^3$, $1^5 3$, $1^3 23$, $1 2^2 3$, $1^2 3^2$, $1^4 4$, $1^2 24$, $2^2 4$, 134, 4^2, 26, 8
T48	$1^4 2^2$, $1^2 3^2$, $1^2 21$, 4^2, 26, 17
T49	$1^4 2^2$, $1^5 3$, $1 2^2 3$, $1^2 3^2$, $1^2 21$, 4^2, $1^3 5$, 35, 26, 17
T50	$1^6 2$, $1^4 2^2$, $1^4 2^3$, $1^5 3$, $1^3 23$, $1 2^2 3$, $1^2 3^2$, $2 3^2$, $1^4 4$, $1^2 24$, $2^2 21$, 131, 4^2, $1^3 5$, 125, 35, $1^2 6$, 26, 17, 8

Table 11: (continued) Shapes occurring in each group

G $G \subseteq \mathcal{A}_8$	2-sets	3-sets	4-sets	4-diff	2-seq
T2	$4^1 8^2$	8^7	$2^3 4^2 8^7$	$1^3 2^2 4^1 8^2$	8^7
T3	4^7	8^7	$2^7 8^7$	$1^7 4^7$	8^7
T4	$4^5 8$	8^7	$2^1 4^1 8^6$	$1^3 2^1 4^1 8$	8^7
T5	$4, 8^1$	8^7	$2^3 8^8$	$1^3 4^2 8^3$	8^7
T9	$1^1 8^2$	$8^3 16^2$	$2^3 1^2 8^3 16^2$	$1^3 2^2 4^3 8^2$	$8^3 16^2$
T10	$1^3 16$	$8^3 16^2$	$2, 4^3 8^3 16^2$	$1, 2^3 1^3 16$	$8^3 16^2$

Table 12: Orbit-length partitions of sets and sequences under G

G $G \subseteq \mathcal{A}_8$	2-sets	3-sets	4-sets	4-diff	2 seq
T11	$4, 8^3$	$8^3 16^2$	$2^3 8^4 16^2$	$1^3 4^2 8^3$	$8^3 16^2$
T12	$4, 24$	$8, 24^2$	$6, 8^2 24^2$	$3, 4^2 24$	$8, 24^2$
T13	$4, 12^2$	$8, 24^2$	$2, 6^2 8, 24^2$	$1, 3^2 4, 12^2$	$8, 24^2$
T14	$4, 12^2$	$8, 24^2$	$2, 6^2 8, 12^2 24$	$1, 3^2 4, 6^2 12$	$8, 24^2$
T18	$4^3 16$	$8, 16^3$	$2, 4^3 8^3 32$	$1, 2^4 4^3 16$	$8^3 32$
T19	$4, 8, 16$	$8, 16, 32$	$2, 4, 8^2 16, 32$	$1, 2, 4^2 8, 16$	$8, 16, 32$
T20	$4, 8, 16$	$8^3 32$	$2, 4, 8^2 16^3$	$1, 2, 4^2 8, 16$	$8, 16^3$
T22	$4, 8^3$	$8^3 32$	$2^3 8^2 16^3$	$1^3 4^2 8^3$	$8, 16^3$
T24	$4, 12^2$	$8, 24^2$	$2, 6^2 8, 24^2$	$1, 3^2 4, 12^2$	$8, 24^2$
T25	28	56	14, 56	7, 28	56
T29	$4, 8, 16$	$8, 16, 32$	$2, 4, 8^2 16, 32$	$1, 2, 4^2 8, 16$	$8, 16, 32$
T32	$1, 24$	$24, 32$	$6, 8^2 48$	$3, 4^2 24$	$8, 48$
T33	$12, 16$	$8, 48$	$2, 12, 24, 32$	$1, 6, 12, 16$	$24, 32$
T34	$12, 16$	$8, 48$	$2, 12^3 32$	$1, 6^3 16$	$24, 32$
T36	28	56	14, 56	7, 28	56
T37	28	56	$14^2 42$	$7^2 21$	56
T39	$4, 24$	$24, 32$	$6, 8^2 48$	$3, 4^2 24$	$8, 48$
T41	$12, 16$	$8, 48$	$2, 12, 24, 32$	$1, 6, 12, 16$	$24, 32$
T42	$12, 16$	$8, 48$	$2, 32, 36$	$1, 16, 18$	$24, 32$
T45	$12, 16$	$8, 48$	$2, 32, 36$	$1, 16, 18$	$24, 32$
T48	28	56	14, 56	7, 28	56
T49	28	56	70	35	56

Table 12: (continued) Orbit-length partitions of sets and sequences under G

G $G \leq \mathcal{A}_8$	2-sets	3-sets	4-sets	4-diff	2-seq
T1	$4, 8^3$	8^7	$2, 4, 8^8$	$1, 2, 4^2 8^3$	8^7
T6	$4, 8^3$	$8^3 16^2$	$2, 4, 8^4 16^2$	$1, 2, 4^2 8^3$	$8, 16^3$
T7	$4, 8, 16$	$8^3 16^2$	$2, 4, 8^2 16^3$	$1, 2, 8^2 16$	$8^3 16^2$
T8	$4, 8, 16$	$8^3 16^2$	$2, 4, 8^2 16^3$	$1, 2, 8^2 16$	$8, 16^3$
T15	$4, 8, 16$	$8, 16^3$	$2, 4, 8^2 16, 32$	$1, 2, 8^2 16$	$8, 16, 32$
T16	$4, 8, 16$	$8^3 32$	$2, 4, 16^4$	$1, 2, 8^2 16$	$8, 16^3$
T17	$4, 8, 16$	$8, 16, 32$	$2, 4, 16^2 32$	$1, 2, 8^2 16$	$8^3 32$
T21	$4, 8^3$	$8^3 32$	$2^3 16^4$	$1^3 8^4$	$8, 16^3$
T23	$4, 21$	$8, 21^2$	$6, 16, 24^2$	$3, 8, 21$	$8, 48$
T26	$4, 8, 16$	$8, 16, 32$	$2, 4, 16^2 32$	$1, 2, 8^2 16$	$8, 16, 32$
T27	$4, 8, 16$	$8^3 32$	$2, 4, 16^4$	$1, 2, 8^2 16$	$8, 16^3$
T28	$4, 8, 16$	$8, 16, 32$	$2, 4, 16^2 32$	$1, 2, 8^2 16$	$8, 16, 32$
T30	$4, 8, 16$	$8, 16, 32$	$2, 4, 16^2 32$	$1, 2, 8^2 16$	$8, 16, 32$
T31	$4, 8^3$	$8^3 32$	$2^3 16^4$	$1^3 8^4$	$8, 16^3$
T35	$4, 8, 16$	$8, 16, 32$	$2, 4, 16^2 32$	$1, 2, 8^2 16$	$8, 16, 32$
T38	$4, 21$	$21, 32$	$6, 16, 48$	$3, 8, 21$	$8, 48$
T40	$4, 21$	$21, 32$	$6, 16, 48$	$3, 8, 24$	$8, 48$
T43	28	56	$28, 42$	$14, 21$	56
T44	$4, 21$	$21, 32$	$6, 16, 48$	$3, 8, 24$	$8, 48$
T46	$12, 16$	$8, 48$	$2, 32, 36$	$1, 16, 18$	$24, 32$
T47	$12, 16$	$8, 48$	$2, 32, 36$	$1, 16, 18$	$24, 32$
T50	28	56	70	35	56

Table 12: (continued) Orbit-length partitions of sets and sequences under G

References

[B] W. S. Burnside and A. W. Panton, *The Theory of Equations*, vol. 2, Dublin University Press, 1916.

[BA] R. Bourgne and J-P. Azra, *Écrits et Mémoires Mathematiques d'Evariste Galois*. Gauthier-Villars, 1926.

[BBCO] C. Batut, D. Bernardi, H. Cohen, and M. Olivier, *User's Guide to PARI-GP*, March 1990.

[BM] G. Butler and J. McKay, 'The transitive groups of degree up to 11', *Comm Algebra* **11** (1983), 863-911.

[CGG] B. W. Char, K. O. Geddes, G. H. Gonnet, B. L. Leong, M. B Monagan and S. M. Watt, *Maple Library Reference Manual*, Springer Verlag, 1991

[CM1] D. Casperson and J. McKay, 'Symmetric functions, m-sets, and Galois groups', to appear.

[CM2] D. Casperson and J. McKay, 'An ideal decomposition algorithm', preliminary report, *AMS Abstracts* **13** (1992) 405.

[D] H. Darmon, private communication.

[EFM] D. W. Erbach, J. Fischer, and J. McKay, 'Polynomials with PSL(2,7) as Galois group', *J. Number Theory* **11** (1979) 69-75.

[HK] F-P. Heider and P. Kolvenbach, 'The construction of SL(2,3) Polynomials', *J. Number Theory* **19** (1984) 392-411.

[L] S. Lang, *Algebra*. Addison-Wesley, 1984.

[LLL] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, 'Factoring Polynomials with Rational Coefficients', *Math. Ann.* **261** (1982), 515-534.

[LM] S. E. LaMacchia, 'Polynomials with Galois group $PSL(2,7)$', *Comm. Algebra* **8** (1980) 983-992.

[LO] J. C. Lagarias and A. M. Odlyzko, 'Effective versions of the Chebotarev density theorem', in *Algebraic Number Fields (L-functions and Galois properties)* (A. Fröhlich, Ed.), pp. 409-464, Academic Press, 1977.

[M] B. H. Matzat, 'Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe', *J. reine angew. Math.* **349** (1984), 179-220.

[MD] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, 1979.

[Ml] G. Malle, 'Polynomials for Primitive Nonsolvable Permutation Groups of Degree $d \leq 15$', *J. Symb. Comp.* **4** (1987), 93-97.

[MR] J. McKay and E. Regener, 'Actions of permutation groups on r-sets', *Comm. Algebra* **13** (1985) 619-630.

[O] M. Olivier, preprint.

[S1] L. Soicher, *The computation of Galois groups.* Master's thesis, University of Concordia, Montréal, Québec, Canada, April 1981.

[S2] L. Soicher, 'An Algorithm for Computing Galois Groups', in *Computational Group Theory* (M. D. Atkinson, Ed.), pp. 291-296, Academic Press, 1984.

[SM] L. Soicher and J. McKay, 'Computing Galois groups over the rationals', *J. Number Theory* **20** (1985), 273-281.

[Sm] G. Smith, private communication.

[St1] R. P. Stauduhar, *The automatic determination of Galois groups* Ph D Dissertation, University of California, Berkeley, 1969.

[St2] R. P. Stauduhar, 'The determination of Galois groups', *Math Comp* **27** (1973) 981-996.

[vW] B. van der Waerden, *Modern Algebra.* Vol. I, Ungar, 1949.

[W] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964

[Z] H. Zassenhaus, 'On Hensel Factorization I', *J. Number Theory* **1** (1969) 291-311.