Techniques for the Computation of Galois Groups

Alexander Hulpke

School of Mathematical and Computational Sciences,
The University of St. Andrews,
The North Haugh,
St. Andrews, Fife KY16 9SS, United Kingdom
ahulpke@dcs.st-and.ac.uk

Abstract. This note surveys recent developments in the problem of computing Galois groups.

Galois theory stands at the cradle of modern algebra and interacts with many areas of mathematics. The problem of determining Galois groups therefore is of interest not only from the point of view of number theory (for example see the article [39] in this volume), but leads to many questions in other areas of mathematics. An example is its application in computer algebra when simplifying radical expressions [32].

Not surprisingly, this task has been considered in works from number theory, group theory and algebraic geometry. In this note I shall give an overview of methods currently used.

While the techniques used for the identification of Galois groups were known already in the last century [26], the involved calculations made it almost impractical to do computations beyond trivial examples. Thus the problem was only taken up again in the last 25 years with the advent of computers.

In this note we will restrict ourselves to the case of the base field $\mathbb{Q}$. Most methods generalize to other fields like $\mathbb{Q}(t)$, $\mathbb{Q}_p$, $\mathbb{F}_p(t)$ or number fields.

The results presented here are the work of many mathematicians. I tried to give credit by references wherever possible.

1 Introduction

We are given an irreducible polynomial $f \in \mathbb{Q}[x]$ of degree n and asked to determine the Galois group of its splitting field $L = \mathrm{Spl}(f)$. This group $G = \mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$ is usually called the Galois group of f. We denote the roots of f by $\{\alpha_1, \ldots, \alpha_n\}$. Without loss of generality (as one can replace $f(x)$ by $a^n f(x/a)$ without changing splitting field nor Galois group) one can assume that f is monic with integer coefficients. Thus the α_i are algebraic integers. We denote the ring of algebraic integers in L by $\mathcal{O}(L)$. Groups act from the right by exponentiation. The orbit of a under G is written as $a^G = \{a^g \mid g \in G\}$.

The determination of elements of G explicitly is in general infeasible: To express elements of G, we need to represent the splitting field they act on. If the degree of the splitting field in not very small ($[L : Q]$ up to 50 say), however, construction of the splitting field is beyond any reasonable computational capabilities. An algorithm for the calculation of splitting fields has been published in [1], algorithms for the determination of elements of G for number fields are given in [27].

Instead we observe that (as $f(\alpha^\sigma) = f(\alpha)^\sigma = 0^\sigma = 0$ for $\sigma \in G$) the Galois group acts on the roots of f. This action is transitive because f is irreducible and faithful as $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Any arrangement of the roots therefore yields an embedding of G as a subgroup of the symmetric group S_n. Our aim will be to determine this image and – if possible – also identify the arrangement of the roots α_i that yields that image. This arrangement is usually determined by a labelling of approximations of the α_i.

In the sequel we will often use the embedding implicitly and consider G as a transitive permutation group.

2 Local Analysis

For a prime p we denote reduction modulo p by π. This reduction extends naturally to the algebraic integers and to polynomial rings. If p does not divide the discriminant of f, a theorem of DEDEKIND shows that the Galois group $\overline{G}$ of the reduced polynomial $f\pi \in \mathbb{F}_p[x]$ embeds into G ([42, (II.7.12)], a proof in a more computational context can be found in [49, §66]).

This Galois group $\overline{G}$ over $\mathbb{F}_p$ is cyclic, its orbits on the approximate roots $\alpha_i\pi$ are simply given by the $\mathbb{F}_p$-irreducible factors of $f\pi$. We thus have

Lemma 1. *If p does not the discriminant* $\operatorname{disc}(f)$*, the irreducible factors of $f\pi$ correspond to the cycle structure of an element of G; if $f\pi = \prod_i f_i$, this element is of the form* $\underbrace{(\ldots)}_{\deg f_1} \cdot \underbrace{(\ldots)}_{\deg f_2} \cdot \cdots \cdot \underbrace{(\ldots)}_{\deg f_m}$.

(For ramified primes we can embed the Galois groups over $\mathbb{Q}_p$ into G. For practical purposes however this usually does not yield new information.)

While this yields cycle structures of elements of G, the corresponding arrangement of the α_i is only determined modulo p. Without further information about the Galois group G there is no possibility to "connect" the arrangements for different primes. Thus the cycle structures obtained this way can only be used to rule out candidates for G which are too small to contain all cycle structures found. This however permits to identify symmetric and alternating groups quickly [15], which is of practical importance as asymptotically all polynomials have the symmetric group as Galois group [48]. As it requires only factorizations over F_p this test is very cheap and should always be run as a first filter to restrict the type of G.

Using analytic number theory, one can generalize Lemma 1 to TSCHEBOTAREFF's theorem [47], by which the density of primes corresponding to a given

cycle structure equals the frequency of this cycle structure among the elements of G. Effective bounds for the probability that all shapes have been found when considering only a limited number of primes are given in [31]. This permits a probabilistic approach to finding G by factoring f modulo different non-ramified primes and checking for which transitive subgroup of S_n this approximates the shape distribution best. Besides its probabilistic nature, this approach gets into problems if the shape distribution does not identify groups uniquely. It happens first in degree 8 with the groups $T_8N_{10} = [2^2]4$ and $T_8N_{11} = Q_8 : 2$.

As the Galois group of f over a local field $\mathbb{Q}_p$ is usually a proper subgroup of G, such local methods alone cannot determine G, but we have to look at global properties:

3 Invariants

The approach to identifying the Galois group G will be to show that certain relations between the roots of f are respected by G. This permits to identify G from a list of transitive subgroups of S_n by finding enough relations that hold (or do not hold) to determine one subgroup from this list uniquely.

The algorithms therefore usually rely on lists of transitive subgroups of S_n. These subgroups are classified up to degree 31 [24] which covers the currently interesting range for n. Explicit lists up to degree 15 can be found in [12].

The tool for the identification of G is the polynomial ring $\mathcal{R} = \mathbb{Z}[x_1, \ldots, x_n]$. The symmetric group S_n acts on $\mathcal{R}$ by permutation of indeterminants. We call $h \in \mathcal{R}$ an *invariant* for $U \leq S_n$ if $h^u = h$ for all $u \in U$. The ring of all U-invariants is traditionally denoted by $\mathcal{R}^U$. To abbreviate notation we shall write $\underline{\mathbf{x}}$ for $(x_1, \ldots, x_n)$.

The specialization homomorphism $\varphi: \mathcal{R} \to \mathcal{O}(L), h \mapsto h(\alpha_1, \ldots, \alpha_n)$ connects the permutation action of G on $\mathcal{R}$ (by permuting the indeterminants) with the Galois action of G on L; it is a homomorphism of G-modules. As $\mathcal{O}(L) \cap \mathbb{Q} = \mathbb{Z}$, G-invariance of $h \in R$ implies that $\varphi(h) \in \mathbb{Z}$. The converse of this is not true in general: The polynomial $f = x^4 - 2$ has Galois group $D(4)$, generated by the permutations $(1,2,3,4), (1,3)$ with respect to the root arrangement $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$. Then $h = x_1x_2 - x_3x_4$ is not $D(4)$-invariant, though $\varphi(h) = 0 \in \mathbb{Z}$. This however is an "accidental" relation among the roots which is not due to the Galois group. The following lemma shows under which conditions this can be avoided

Lemma 2. *If*

$$\varphi(l) \neq \varphi(h) \quad \textit{for all} \quad l \in h^{S_n} \setminus \{h\} \tag{1}$$

then h is G-invariant if and only if $\varphi(h) \in \mathbb{Z}$.

Proof. Assume that h is not G-invariant and $\varphi(h) \in \mathbb{Z}$. Then there is a $g \in G$ such that $h^g \neq h$, so we have by the assumption (1) that $\varphi(h) \neq \varphi(h^g)$, and because φ respects the actions $\varphi(h^g) = \varphi(h)^g = \varphi(h)$ holds, contradiction.

If the condition (1) is not fulfilled, one can change f by a Tschirnhaus transformation to another polynomial $\hat{f}$ which defines the same field (and thus has the same Galois group). It is shown in [21] that for a given h it is always possible to find such a transform $\hat{f}$ such that condition (1) is fulfilled for $\varphi_{\hat{f}}$. Care however has to be taken to ensure that the coefficients of $\hat{f}$ do not become too big. Therefore in practice only very simple Tschirnhaus transformations are used and it may be well worth to try an alternative h instead.

As the roots α_i are only known by approximations $\widetilde{\alpha}_i$, in practice however φ is only known by an approximation $\widetilde{\varphi}\colon h \mapsto h(\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n)$. The test for integrality therefore has to rely on the approximation being good enough.

4 Descending Approach

If $V < U$ we call $h \in \mathcal{R}$ a *U-relative invariant for V*, if h is invariant under V but not under U. If G is known to be a subgroup of U then $G \leq V$ if and only if h is G-invariant.

The first computational approach towards finding G has been described in [46]: We form the partial lattice of transitive subgroups of S_n and determine for each minimal "step" $U > V$ (V being a maximal subgroup of U) in this partial lattice a U-relative invariant for V. This information is determined once and for all. As the invariants for a conjugate of V are simply images of the invariants of V, it is sufficient to determine these invariants up to S_n conjugation.

The algorithm now determines G by stepping downwards through this partial lattice, starting with $U = S_n$. For a maximal subgroup $V < U$ it then tests whether a V-invariant h is invariant under G and if this is the case continues with V being the U for the next step. If on the other hand G is not contained in any proper transitive maximal subgroup of U, G must be equal to U and the algorithm stops. As there are only finitely many transitive subgroups, this will always happen. Of course all subgroups V, which do not contain cycle shapes known to occur in G by Lemma 1, can be excluded as well.

The test for G-invariance of a V-invariant h is performed by testing whether $\varphi(h) \in \mathbb{Z}$ (provided of course that condition (1) holds). An example for this is $\sqrt{\operatorname{disc}(f)} = \prod_{i<j}(\alpha_i - \alpha_j)$ which is integral if and only if G is contained in A_n.

To reduce the storage requirements of transitive groups down to storing only representatives up to conjugacy, the following approach is used: For each pair $U > V$, the subgroups V are stored up to U-conjugacy (respectively: for each pair of S_n-representatives U,V the embeddings $V \hookrightarrow U$ are stored up to U-conjugacy). For each class representative V with invariant h the *resolvent polynomial*[1] $R = \prod_{g \in (h^U)}(x - \varphi(g)) \in \mathbb{Z}[x]$ is formed. As h is not U-invariant, the degree of R is $[U : V]$. Then R is tested for integer roots. An integer root of R determines a U-image of h and thus a U-conjugate of V in which G is contained.

[1] The name *resolvent* dates back to Lagrange. Polynomials of this type can be used to construct subfields and thus were used for solving polynomial equations.

Instead of continuing with this conjugate, the algorithm then re-sorts the roots appropriately and continues with V.

A further advantage of forming the resolvent R is that R must be invariant under the Galois action of G and thus has integer coefficients. When computing with approximate roots (and using $\widetilde{\varphi}$ instead of φ) therefore the coefficients of R can be rounded to the next integer. This permits to use exact methods to test for integral roots.

Finally, as G-invariance is tested via φ, a condition like (1) must be fulfilled. As $G \leq U$ the symmetric group S_n can be replaced in (1) by U; sufficiency holds if R is square-free (a formal proof can be found in [46]).

4.1 Root Approximation

Bounds for the needed accuracy of root approximation are given in [17, 2.1.3]. If the coefficients of f become big, however, these bounds can become infeasibly large and thus some of the implementations work by standard with lower, non-guaranteed bounds.

For the approximation of the roots α_i essentially two methods have been used; numerical approximation and p-adic approximation. The main advantage of numerical approximation is that it is probably more likely available in a programming language and that it allows to obtain quickly results which are not guaranteed to be correct. Its main disadvantage is that approximation is not a ring homomorphism and thus error propagation is difficult to keep under control. To the authors knowledge there are neither theoretical results, nor implementations ("validated numerics") which analyze error propagation in these cases and thus give proven results.

On the other hand p-adic approximation behaves much nicer from an algebraic viewpoint in that the approximation is a ring homomorphism and thus no error propagation will happen. To compute bounds, estimates for the absolute values $|\alpha_i|$ are still needed. These can be obtained from general estimates as found in [41, section 4.3].

The approach of p-adic approximation, combined with numerical approximation to obtain better bounds for the $|\alpha_i|$, has been used in [14] to verify polynomials with Galois groups M_{11} and M_{12}.

The problem of approximation can be avoided completely if deferring the evaluation φ as shown in [9]: If h is a U-relative invariant for V, the coefficients of the unevaluated resolvent $R = \prod_{g \in (h^U)} (t - g) \in \mathbb{Q}(\underline{\mathbf{x}})[t]$ are invariant under U and therefore expressible in generators of the invariant ring $\mathbb{Q}[\underline{\mathbf{x}}]^U$. On the other hand, the elements $\{1, h, h^2, \ldots, h^{[U:V]}\}$ form a $\mathbb{Q}(\underline{\mathbf{x}})^U$-Basis of $\mathbb{Q}(\underline{\mathbf{x}})^V$ and [11] gives an algorithm to express V-invariants in this basis explicitly. This permits the following inductive approach: We start with $U := S_n$ whose invariants are generated by the elementary symmetric polynomials. At each step we assume that we can express every U invariant polynomial in terms of the elementary symmetric polynomials and known relative invariants of U and of subgroups $S_n \geq W \geq U$. This certainly holds for $U = S_n$. If we descend to a subgroup V

there is a new invariant ring $\mathbb{Q}(\underline{\mathbf{x}})^V$ which is generated by $\mathbb{Q}(\underline{\mathbf{x}})^U$ and the invariant h. The above mentioned algorithm now permits to express every V-invariant in terms of $\mathbb{Q}(\underline{\mathbf{x}})^U$ and h. By the assumption on $\mathbb{Q}(\underline{\mathbf{x}})^U$ this yields an expression of every V-invariant in terms of the elementary symmetric polynomials and known invariants of subgroups $S_n \geq W \geq V$. This however is the necessary assumption for the induction once V becomes itself a new U in the next step. By using the evaluations $\varphi(e_i)$ of the elementary symmetric polynomials, which are (up to a sign) the coefficients of f, and the evaluations $\varphi(h)$ of invariants of larger subgroups, which are the integral roots obtained in earlier steps, we can thereby express any φ-evaluated U-invariant. One thus obtains the evaluated resolvents $\prod_{g\in(h^U)}(t-\varphi(g))$ needed for the algorithm.

If not $\varphi(h)$ but the evaluation $\varphi(g)$ of a conjugate is an integral root, of course this conjugate $g = h^u$ (which is an invariant for the corresponding subgroup V^u) must be used.

In the process of specialization, denominators in expressions in $\mathbb{Q}(\underline{\mathbf{x}})$ might vanish. If this is the case, another invariant $h(p(x_1),\ldots,p(x_n))$ for $p \in \mathbb{Q}[t]$ is chosen. It is shown in [9] that there always is a transform for which denominators do not vanish when specializing.

There are various implementations of the descent method available [20,18,17,19] as standalones or in the systems PARI [4] and KANT [13].

4.2 Variations

To overcome the problem of a large index $[U:V]$ when evaluating invariants, J. McKay suggested the following approach: Suppose we know an element $e \in G$ by its explicit action on the approximate roots. This is the case, for example, for the complex conjugation when using numerical approximation of the roots, or for the Frobenius automorphism when using p-adic approximation. If $h \in \mathcal{R}$ is an invariant for $V < U$, an invariant image h^g ($g \in G$) is invariant under G only if it is invariant under e. This permits to reduce the number of images of h^g that have to be evaluated via φ from $[U:V]$ to $|E|$ with

$$\begin{aligned} E &= \{g \in \mathrm{Repres}(V\backslash U) \mid h^g = (h^g)^e = h^{ge}\} \\ &= \{g \in \mathrm{Repres}(V\backslash U) \mid Vg = Vge\}. \end{aligned}$$

A group theoretic argument shows that if the class of e in G is stable under automorphisms, it is possible to choose $E = \mathrm{Repres}(C_V(e)\backslash C_U(e))$ and therefore $|E| = [C_U(e) : C_V(e)]$. In the case of $M_{12} < A_{12}$, for example this permits to reduce 2520 potential images to 24.

For identification purposes, of course, E may not be chosen a priori for one representative V, but must be selected from h and e. The reduction saves however evaluations $\widetilde{\varphi}$. Usually the images h^g ($g \in E$) do not contain full orbits of G, therefore no resolvent is formed and the evaluated images $\widetilde{\varphi}(h^g)$ must be tested directly.

Another variant of the descending approach has been suggested in [51]: Here the test for rationality of $\varphi(h)$ is replaced by testing whether $(h - \varphi(h))$ is

contained in $\ker\varphi \lhd \mathcal{R}$. This ideal is generated by the elementary symmetric functions equating the coefficients of f. The ideal membership test is done using p-adic approximation of idempotents in $\mathcal{R}/\ker\varphi$.

In reversion of the identification process, knowledge of the Galois group can be used to deduce relations among the roots of f [40].

4.3 Invariants

For the determination of invariant polynomials it is of course sufficient to obtain one V-invariant polynomial which is not U-invariant, instead of generating the full invariant ring for V. This invariant however should be chosen in a way to keep the necessary approximation accuracy low for deducing that $\varphi(h) \in \mathbb{Z}$ from the value of $\widetilde{\varphi}(h)$. The needed accuracy grows with the absolute value $|\varphi(h)|$. A good heuristic to keep this value low is to select h to be of lowest possible degree. Therefore the trivial possibility $h = \sum_{v\in V}(x_1x_2^2\cdot\dots\cdot x_n^n)^v$ is usually unsuitable. An algorithm to compute a better h is given in [22].

If numerical approximation of the roots is used, the evaluation order in $\widetilde{\varphi}$ can become crucial. In this situation it might be necessary to use the invariant h in factorized form or to select other invariants to avoid exaggerated error propagation.

A main problem of this approach is in the first steps down from the symmetric group. It is known [37] that almost all transitive maximal subgroups of S_n or A_n have large index. Thus for almost all possible Galois groups G every descendant chain from S_n down to G will contain a step with large index. A large index however implies a large resolvent degree and in turn the need for a high approximation accuracy.

5 Subfields

Subfields of $\mathbb{Q}(\alpha)$ form an important Galois invariant. Over the past years a couple of algorithms for their computation have been suggested [33,16,34,5,23,28,27], the last probably being the most effective at the moment. By the Galois correspondence subfields correspond to subgroups of G which properly contain the point stabilizer $\mathrm{Stab}_G(\alpha)$. They therefore correspond to block systems of G as permutation group. Suppose that $\mathbb{Q} < \mathbb{Q}(\beta) < \mathbb{Q}(\alpha)$ is a subfield with $\beta = k(\alpha)$ and that m is the minimal polynomial of β. Then by the embedding theorem for imprimitive groups [29], G is a subgroup of the wreath product $W := S_n \wr M$, where M is the Galois group of m. This embedding information can be used to start the descent for the determination of G not with S_n but with W. To this end, one has to determine the arrangement of the roots corresponding to this wreath product: The arrangement of the blocks is determined by the arrangement of the roots β_j of m corresponding to M, the root α_i is in the block corresponding to β_j if $k(\alpha_i) = \beta_j$. This arrangement of the roots to the blocks

determines a conjugate W' of W such that the descent process can be started with $U = W$. If several block systems exist one can embed simultaneously in different wreath products and thus start with U being the intersection of all these wreath products.

For imprimitive groups, this approach permits to avoid the large steps down to maximal subgroups (which are in most cases wreath products and thus contain W) of S_n, respectively A_n. It has been used successfully in the KANT implementation [19].

6 Orbits of the Galois Group

As the computation of resolvents can be hard any information they convey should be used. The descent method just checks for linear factors, that is orbits of G of length one. As the roots of an irreducible polynomial form an orbit of the Galois group, a complete factorization of a resolvent however exhibits also other orbits of G and therefore may give further information about the Galois group. For example [10] obtains an invariant for a subgroup of U containing G by complete factorization of a resolvent for another subgroup $V < U$ which not necessarily contains G.

Let $\mathcal{H} \subset \mathcal{R}$ be a set of polynomials which is invariant under G. Then $R = R(\mathcal{H}, f) = \prod_{h\in\mathcal{H}}(x - \varphi(h))$ has rational coefficients. If condition (1) is fulfilled (that is if R is square-free, again this can be ensured by a Tschirnhaus transformation on f) the irreducible factors of R correspond to the orbits of G on $\mathcal{H}$ in the following way: Every orbit $\mathcal{K} \subset \mathcal{H}$ corresponds to a factor $\prod_{k\in\mathcal{K}}(x - \varphi(k))$ and all factors of R arise this way. Furthermore, the image of the operation of G on the orbit $\mathcal{K}$ is the Galois group of the corresponding polynomial factors. So for example the factor discriminant is a square if and only if the image group is a subgroup of the alternating group.

Similarly, by the Galois correspondence, orbits of a subgroup $U < G$ correspond to factors over a subfield $\mathbb{Q} < \mathbb{Q}(\beta) < L$ which is the field of elements fixed by U. Such subfields of the splitting field can be obtained for example from factors of (other) resolvents.

For a given degree and certain resolvents this information (mainly orbit lengths) can be tabulated for all transitive subgroups of S_n a priori by simple group theoretic calculations. By considering sufficiently many resolvents to distinguish all groups this permits to eliminate all but one conjugacy class of transitive groups (all properties are conjugacy invariant as no roots are labelled), which in turn has to contain the Galois group. This approach has been suggested in [44,45]. In this form no arrangement of (approximate) roots will be obtained.

Because usually no subgroup $U < S_n$ with corresponding root arrangement is known a priori, the sets $\mathcal{H}$ are typically full orbits of S_n. We shall write $R(h, f)$ for $R(h^{S_n}, f)$. In [45] it is suggested to use linear polynomials for h. For $h = x_1 + \cdots + x_m$ or $h = x_1 \cdot \cdots \cdot x_m$ the set $\mathcal{H}$ correspond to the family of m-subsets of $\{1, \ldots, n\}$, similarly $h = x_1 + 2x_2 + \cdots + mx_m$ corresponds to m-tuples. In [6] formulae for both types of set resolvents are given which require

only rational arithmetic. Resolvents arising from more general h are considered in [3] and [35] which use techniques from commutative algebra like resultants for the computation.

Again shapes are used as a first filter. The existence of subfields, respectively block systems, can be used as a further restriction.

A possible advantage of this method is that the resolvents considered do not necessarily have to be "fitted" to subgroups containing the Galois group: The resolvent $R(h, f)$ can be considered as an resolvent for the pair $\mathrm{Stab}_{S_n}(h) < S_n$, but if $G \not\leq \mathrm{Stab}_{S_n}(h)$ (up to conjugacy) this resolvent has no linear factor, nevertheless the factor degrees will restrict the possibilities for G. This sometimes permits to use resolvents of smaller degree than used in the pure descent approach. Also for groups G for which the chain $G < U_m < \cdots < U_1 < S_n$ contains many steps, not for every step a new resolvent has to be evaluated.

In this approach the approximation of roots takes place in the polynomial factorizing algorithm and can therefore be considered to be under control. The factorization of resolvents however can become a major obstacle: Because it is an orbit length of S_n, the set sizes $|h^{s_n}|$ – and thus the resolvent degrees – soon become big. In addition, the resolvent polynomials are essentially of the worst possible kind for the traditionally used Hensel-lifting based factorizing approach [52]: By Lemma 1 they will split modulo each prime in factors whose degrees are orders of elements of G while they factorize in characteristic zero in factors whose degrees are orbit lengths of G. Unless G is in regular representation both measures can differ substantially and therefore many potential combinations of the lifted factors have to be tried before the true factorization is found. The most extreme are elementary abelian 2-groups, for which the resolvents are Swinnerton-Dyer polynomials.

On the other hand the coefficients of the resolvents become that big, that the break-even point for a polynomial time factoring algorithm [36] is yet beyond the runtime for the classical approach.

The algorithm of [45] is implemented in Maple [7] up to degree 7. An extension to degree 8 for polynomials over $\mathbb{Q}(t)$ is described in [38]. It is again implemented in Maple. Tabulating further data for linear resolvents and using also factorization over algebraic extensions to determine orbits of subgroups, this approach has been implemented by the author in GAP 3 [43] up to degree 15, but for some groups calculations in degrees 12 and beyond become infeasibly slow. The factorizations of various resolvents not arising from the symmetric group is tabulated for degree up to 11 in [2].

7 Relation Stabilizers

Evaluation of $\widetilde{\varphi}(h)$ ($h \in \mathcal{H}$) and a test, of which resolvent factor the result is an approximate root, permits to obtain the orbits of G on $\mathcal{H}$ from the factorized resolvent. If approximation modulo p is used the additional computing time for this is neglectable. This permits to compute the set-wise stabilizer $\mathrm{Stab}_{S_n}(\mathcal{H})$ of the orbit in the symmetric group. This stabilizer certainly must contain the

Galois group G. Thus subgroups containing G can be obtained without requiring precomputed subgroup lattices and invariants or factorization tables [25]. Such stabilizers can be different even if all orbit lengths are the same. Therefore they yield a better distinction of groups.

For the linear resolvents which correspond to the action on sets and tuples, these stabilizers are the m-closure $G^{(m)}$, respectively the m-set closure $G^{\{m\}}$ of the Galois group G. These closures have been studied in permutation group literature [50]. The problem of identifying G uniquely then can be interpreted as a permutation group theoretic problem about groups having the same closure. A result that some closures (obviously $G^{(n)} = G$, but then $|\mathcal{H}| = n!$ which is infeasible) determine G uniquely would lead to an effective algorithm that does not rely on precomputed information. This is of importance as the number of transitive groups grows substantially for higher n (there are 301 classes of degree 12, 1954 classes of degree 16 and 26813 classes of degree 24) and therefore such a preparation will not be reasonable beyond degree 15.

As this approach does not only filter the group abstractly from a list of candidates but also obtains an (partial) arrangement of the approximate roots, it is possible to use not only resolvents arising from full orbits of S_n, but also resolvents from orbits of the current approximation $U > G$. The resolvents used in the descent method are exactly of this type and the methods described in Sect. 4 can be used for their computation.

An additional advantage of this approach is that the partial root arrangement obtained from the factors of previous resolvents can be used to pre-sort the resolvent factors modulo p when factoring which in turn can help to ease the exponential factor combination step.

The use of block stabilizers is of course also possible here. However as the 2-set closure $G^{\{2\}}$ already determines all block systems this will not necessarily improve the discrimination of potential Galois groups.

8 Capabilities of the Algorithms

As mentioned before current implementations are all still degree-dependent. They work in theory (that is information is precomputed) for degrees up to 9 [20], 11 [18], 12 [19] or 15 [43], but sometimes for higher degrees the actual computations required to identify the group (using proven bounds) are too hard to make them feasible. In general for degrees up to 10 the algorithms should always finish in reasonable time, for the higher degrees they will work for some cases but for some groups it will not finish in reasonable time. Concretely, calculations for degree 8 will usually finish in under a minute, degree 10 may take a few minutes, but degree 12 (and some particular groups in lower degrees) may take an hour or even much more.

The worst case for the identification are (for all algorithms likewise) highly transitive groups which do not contain the alternating group. Such groups are usually maximal of high index in the alternating group and because of their high transitivity require resolvents of high degree to distinguish them from S_n

or A_n by their orbits. Fortunately, as a corollary of the classification of finite simple groups it is known that beyond triply transitivity the only offenders are the Mathieu groups.

9 Final Remarks

Many of the implementations mentioned are available on the internet:

- The implementation of Y. Eichenlaub and M. Olivier can be found at `ftp://megrez.math.u-bordeaux.fr/pub/galois`
- KANT (containing the routines by K. Geissler) is obtainable from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash/`
- GAP (which contains the authors implementation) can be found under `http://www-gap.dcs.st-and.ac.uk/~gap/Info/distrib.html`

This article benefitted implicitly from explanations by and discussions with J. Klüners, J. McKay, and L. Soicher, whom I would like to thank. The authors implementation would have been impossible without many example polynomials constructed by G. Malle, whom I would also like to thank for extensive tests of the algorithms. Last, but not least, I would like to thank DFG, EPSRC and the EU HCM program for their financial support.

References

1. Anai, H., Noro, M., Yokoyama, K.: Computation of the splitting fields and Galois groups of polynomials. In *Algorithms in Algebraic Geometry and Applications* (L. Gonzáles-Vega, T. Recio, eds.), volume 145 of *Progress in Mathematics*. Birkhäuser, Boston, 1996 22–50
2. Arnaudies, J.-M., Valibouze, A.: Groupes de Galois de polynômes en degré 10 ou 11. Rapport interne 94.50, Laboratoire informatique théoretique et programmation, Université Paris VI, (1994)
3. Arnaudies, J.-M., Valibouze, A.: Lagrange resolvents. In Cohen and Roy [8], 1997 23–40
4. Batut, C., Bernardi, D., Cohen, H., Olivier, M.: User's guide to pari-gp. Technical report, Université Bordeaux I, (1993)
5. Casperson, D., Ford, D., McKay, J.: An ideal decomposition algorithm. J. Symb. Comput. **21** (1996) 133–137
6. Casperson, D., McKay, J.: Symmetric functions, m-Sets and Galois groups. Math. Comp. **63** (1994) 208 749–757
7. Char, B. W., Geddes, K. O., Gonnet, G. H., Monagan, M. B., Watt, S. M.: MAPLE – Reference Manual, 5th edition. University of Waterloo, (1988)
8. Cohen, A. M., Roy, M.-F. (eds.): Proceedings MEGA'96, volume 117–118 of *J. Pure Appl. Algebra*, (1997)
9. Colin, A.: Formal computation of Galois groups with relative resolvents. In *Applied algebra, Algebraic algorithms and Error-correcting Codes* (G. Cohen, M. Giustini, T. Mora, eds.), volume 948 of *Lecture Notes in Computer Science*. Springer, Heidelberg, 1995 169–182

10. Colin, A.: Relative resolvents and partition tables in Galois group computations. In Küchlin [30], 1997 169–182
11. Colin, A.: Théorie des invariants effective. Applications à la théorie de Galois et à la résolution de systèmes algébriques. Implantation en AXIOM. Ph.D. thesis, École polytechnique, (1997)
12. Conway, J. H., Hulpke, A., McKay, J.: On transitive permutation groups. to appear in LMS Journal of Computation and Mathematics ()
13. Daberkow, M., Fieker, C., Klüners, J., Pohst, M., Roegner, K., Schörnig, M., Wildanger, K.: KANT V4. J. Symb. Comput. **24** (1997) 267–283
14. Darmon, H., Ford, D.: Computational verification of M_{11} and M_{12} as Galois groups over Q. Comm. Algebra **17** (1989) 2941–2943
15. Davenport, J. H., Smith, G.: Fast recognition of symmetric and alternating Galois groups, (to appear)
16. Dixon, J. D.: Computing subfields in algebraic number fields. J. Austral. Math. Soc. Ser. A **49** (1990) 434–448
17. Eichenlaub, Y.: Problèmes effectifs de théorie de Galois en degrés 8 à 11. Ph.D. thesis, Université Bordeaux I, (1996)
18. Eichenlaub, Y., Olivier, M.: Computation of Galois groups for polynomials with degree up to eleven. Preprint, Université Bordeaux I, (1995)
19. Geissler, K.: Zur Berechnung von Galoisgruppen. Diplomarbeit, Fachbereich Mathematik der TU Berlin, (1997)
20. Geyer, H.: Programme zur Berechnung der Galoisgruppen von Polynomen 8. und 9. Grades. Preprint 93-10, IWR Heidelberg, (1993)
21. Girstmair, K.: On the computation of resolvents and Galois groups. Manuscripta Math. **43** (1983) 289–307
22. Girstmair, K.: On invariant polynomials and their application in field theory. Math. Comp. **48** (1987) 781–797
23. Hulpke, A.: Block systems of a Galois group. Experimental Mathematics **4** (1995) 1 1–9
24. Hulpke, A.: Konstruktion transitiver Permutationsgruppen. Ph.D. thesis, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, (1996)
25. Hulpke, A.: Galois groups through invariant relations. In *Groups '97 Bath/St. Andrews* (C. M. Campbell, E. F. Robertson, G. C. Smith, eds.). Cambridge University Press, to appear
26. Jordan, C.: Traité des substitutions et des équations algébriques. Gauthier–Villars, (1870)
27. Klüners, J.: Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper. Ph.D. thesis, Technische Universität, Berlin, (1997)
28. Klüners, J., Pohst, M. E.: On computing subfields. J. Symb. Comput. **24** (1997) 385–397
29. Krasner, M., Kaloujnine, L. A.: Produit complet des groupes de permutations et problème d'extension de groupes II. Acta Sci. Math. (Szeged) **14** (1951) 39–66
30. Küchlin, W. (ed.): Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation. The Association for Computing Machinery, ACM Press, (1997)
31. Lagarias, J. C., Odlyzko, A. M.: Effective versions of the Chebotarev density theorem. In *Algebraic Number Fields (L-functions and Galois properties)* (A. Fröhlich, ed.). Academic Press, 1977 409–464
32. Landau, S.: How to tangle with a nested radical. Math. Intelligencer **16** (1994) 2 49–55

33. Landau, S., Miller, G.: Solvability by radical is in polynomial time. J. Comput. System Sci. **30** (1985) 179–208
34. Lazard, D., Valibouze, A.: Computing subfields: Reverse of the primitive element problem. In *Computational Algebraic Geometry* (F. Eyssette, A. Galligo, eds.), volume 109 of *Progress in Mathematics*. Birkhäuser, Boston, 1993 163–176
35. Lehobey, F.: Resolvent computations by resultants without extraneous powers. In Küchlin [30], 1997 85–92
36. Lenstra, A., Lenstra, H., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261** (1982) 515–534
37. Liebeck, M. W., Praeger, C. E., Saxl, J.: A classification of the maximal subgroups of the finite alternating and symmetric groups. J. Algebra **111** (1987) 365–383
38. Mattman, T. W., McKay, J.: Computation of Galois groups over function fields. Math. Comp. **66** (1997) 218 823–831
39. Matzat, B. H.: Fortschritte in der inversen Galoistheorie. This volume
40. McKay, J., Stauduhar, R.: Finding relations among the roots of an irreducible polynomial. In Küchlin [30], 1997 75–77
41. Mignotte, M.: Mathematics for Computer Algebra. Springer, Heidelberg, (1992)
42. Neukirch, J.: Algebraische Zahlentheorie. Springer, Heidelberg, (1992)
43. Schönert, M., et al.: GAP 3.4, patchlevel 4. Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, (1997)
44. Soicher, L. H.: The computation of Galois groups. Master's thesis, Concordia University, (1981)
45. Soicher, L. H., McKay, J.: Computing Galois groups over the rationals. J. Number Theory **20** (1985) 273–281
46. Stauduhar, R. P.: The determination of Galois groups. Math. Comp. **27** (1973) 981–996
47. Tschebotareff, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann. **95** (1925) 191–228
48. van der Waerden, B. L.: Die Seltenheit der Gleichungen mit Affekt. Math. Ann. **109** (1934) 13–16
49. van der Waerden, B. L.: Algebra, erster Teil. Springer, Heidelberg, eighth edition, (1971)
50. Wielandt, H.: Permutation groups through invariant relations and invariant functions. Lecture notes, Department of Mathematics, The Ohio State University, (1969)
51. Yokoyama, K.: A modular method for computing the Galois group of polynomials. In Cohen and Roy [8], 1997 617–636
52. Zassenhaus, H.: On Hensel factorization I. J. Number Theory **1** (1969) 291–311