GALOIS GROUPS THROUGH INVARIANT RELATIONS

ALEXANDER HULPKE

1. Prolegomena

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n. Then the splitting field $L \geq \mathbb{Q}$ of f is a normal extension. We want to determine the Galois group $G = \mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$ of f which is the group of all field automorphisms of this extension. This task is basic in computational number theory [Coh93] as the Galois group determines a lot of properties of the field extension defined by f.

Because the index $[L : \mathbb{Q}]$ might be large, however, we do not intend to construct L and thus cannot give explicitly the automorphism action of G on L. Instead we consider the action of G on the roots $\{\alpha_1, \ldots, \alpha_n\}$ of f. As f is defined over the rationals the set of these root must remain invariant under G. This permutation action is faithful, because L can be obtained by adjoining all the α_i to $\mathbb{Q}$. This action has to be transitive because f is irreducible. In other words: For a fixed arrangement of the roots, G can be considered as a transitive subgroup of S_n. We will utilize this embedding without explicitly mentioning it.

While the problem itself is initially number-theoretic, the approaches to solve it are mainly based on commutative algebra and permutation group theory. This paper presents a new approach, approximating the Galois group by its closures (subgroups of S_n that stabilizer orbits of G). This in turn gives rise to questions about permutation groups.

In the course of the paper we shall need a few facts from number theory about p-adic extensions and the relation between extensions of $\mathbb{Q}$ and extensions of $\mathbb{F}_p$. These will be provided in an appendix.

2. Identification tools

We will assume that f is a monic integer polynomial of degree n, that is the roots of f are algebraic integers. Obviously we can always enforce this by a transformation of the type $f(x) \mapsto a^n f(x/a) = \tilde{f}(x)$ which yields a polynomial $\tilde{f}$ defining the same extension as f. The degree n will be typically in the range $n \lessapprox 30$.

2.1. Orbits of Elements.

By Dedekind's theorem (appendix, theorem 5) factorization of f modulo a non-ramifying prime yields the cycle structure of an element of $G = \mathrm{Gal}(f)$. Such factorizations are very cheap and it is feasible to factorize f modulo several hundred primes. By this method it is usually very easy to find out whether G is symmetric or alternating [DSar].

Using Tschebotareff's result we may even hope that we have obtained all cycle shapes of G if we look at sufficiently many primes. In practice "sufficiently many" means: Factorize modulo new primes, until $t(n)$ times no new shape emerged (or we can prove already that

Supported by EPSRC Grant GL/L21013.

G contains the alternating group). For small degrees $t(n) = 3n$ seems to be a reasonable choice.

In any case, such factorizations eliminate those groups as candidates for G which do not contain all shapes observed. Unless we are content with a probabilistic result, however, we cannot be certain to have found all shapes and cannot use the frequency of these shapes.

2.2. **Orbits of the Galois group.** The main tool for the identification of Galois groups is the polynomial ring $\mathcal{R} = \mathbb{Z}[x_1, \ldots, x_n]$ and the specialization homomorphism $\varphi = \varphi_f \colon \mathcal{R} \to \mathcal{O}(L)$, $h \mapsto h(\alpha_1, \ldots, \alpha_n)$. As a permutation group, G acts on $\mathcal{R}$ by permuting indeterminants; as a Galois group it acts on $\mathcal{O}(L)$. For these two actions φ is a G-module homomorphism, we have that

$$\varphi(r)^g = \varphi(r^g) \qquad \text{for all} \quad r \in \mathcal{R} \tag{1}$$

The basic idea is to recognize G from G-invariant polynomials in $\mathcal{R}$. G-invariance of an algebraic integer $a \in \mathcal{O}(L)$ implies that $a \in \mathbb{Z}$ and thus G-invariance of $h \in \mathcal{R}$ implies that $\varphi(h) \in \mathbb{Z}$. For example, recall that the discriminant of a monic polynomial with roots $\alpha_1, \ldots, \alpha_n$ is defined as $\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Any transposition of two roots will change a sign of $\sqrt{\operatorname{disc}(f)} = \prod_{i<j}(\alpha_i - \alpha_j)$. Thus this root is invariant under $\operatorname{Gal}(f)$ if and only $\operatorname{Gal}(f)$ consists only of even permutations. Therefore $\operatorname{Gal}(f)$ is a subgroup of A_n if and only if $\operatorname{disc}(f)$ is a square. Otherwise $\mathbb{Q}(\sqrt{\operatorname{disc}(f)})$ is the subfield of L corresponding to the subgroup of even permutations.

In general, the condition $\varphi(h) \in \mathbb{Z}$ is not sufficient to prove G-invariance of h as the following example shows. The polynomial $f = x^4 - 2$ has Galois group $D(4) = \langle (1,2,3,4), (1,3) \rangle$, acting on the roots $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$. Then $h = x_1x_2 + x_3x_4$ is not $D(4)$-invariant, but $\varphi(h) = 0$. It is easy, however, to make the criterion sufficient:

Lemma 2. *Assume that*

$$\varphi(h) \neq \varphi(h') \quad \textit{for all } h' \in h^{S_n}. \tag{3}$$

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

Proof. We have to show sufficiency: Assume that $\varphi(h) \in \mathbb{Z}$ and that there is a $g \in G$ such that $h^g \neq h$. Then by (3) we have $\varphi(h) \neq \varphi(h^g)$, in contradiction to $\varphi(h) \in \mathbb{Z}$ and (1). □

2.3. **Invariant method.** One approach [Sta73, EO95, DF89] uses precomputed invariants h_T for all transitive subgroups of $T \leq S_n$ and filters G from these T by testing which h_T are actually G invariant. This test is done by testing $\varphi(h_T)$ for rationality.

If G and G' are conjugate under S_n, the invariants of G' are S_n-images of the invariants of G, so it is sufficient to store only representatives of the invariants.

A further reduction is obtained by using relative invariants: The set of transitive groups is a semi-lattice with respect to inclusion. Determination of G then proceeds stepwise down this lattice. If G is known to be contained in U and if V is a subgroup of S_n, then every invariant for V can be used to test whether G is contained in $U \cap V$. Such invariants can be substantially simpler than an invariant for $U \cap V$ as a subgroup of G. Furthermore, the number of invariant images to consider is reduced from $[S_n : V]$ to $[U : V]$. This way the identification process steps down through chains of transitive subgroups, stepping from a subgroup U to a maximal subgroup $V < U$.

However, the number of images will still be prohibitive if every subgroup chain from G to S_n includes a step of large index. This typically holds, as (with few exceptions) all transitive maximal subgroups of the symmetric and alternating groups are of large index [LPS87].

A further problem can be approximation accuracy: The roots $\{\alpha_i\}$ are not known exactly but only by approximation. Therefore instead of φ we only know an approximation $\tilde{\varphi}$. Consequentially can only test $\tilde{\varphi}(h)\widetilde{\in}\mathbb{Z}$ and $\tilde{\varphi}(a) \approx \tilde{\varphi}(b)$. With numerical approximation of the roots this leads to substantial problems with the needed accuracy to prove approximated numbers to be integers or equal. A better approach is to use p-adic approximation, relying on numerical estimates only to deduce the necessary accuracy of the p-adic approximation as done in [DF89].

Instead of testing integrality of $\varphi(h)$ for a V-invariant h, usually it is checked whether the polynomial $R(x) = \prod_{g\in h^U}(x - \varphi(g)) \in \mathbb{Z}[x]$ has an integral root. This permits to round the coefficients of R to the nearest integer and thus reduce the influence of approximation errors.

In a variant, avoiding approximation, it is shown in [Col95] how to compute R by calculations in $\mathcal{R}$, using only rational operations on the coefficients of f.

2.4. **Resolvent method.** Another approach [SM85] tries to overcome the problem with approximation of roots and large numbers of invariant images by using only invariants of very restricted type. The approximation of roots in this case is deferred inside a polynomial factorization (which uses p-adic approximation of the factors).

If $A \subset \mathcal{R}$ is an orbit of G, then every elementary symmetric function in the elements of A is obviously G-invariant. Thus the polynomial $\prod_{a\in A}(x - a)$ is G-invariant as well. (We extend the action of G to the polynomial rings $R[x]$ and $L[x]$ by acting on the coefficients.) Thus the polynomial $\prod_{a\in A}(x - \varphi(a))$ is an integer polynomial.

To get A we consider it as a subset of a larger orbit $\widehat{A}$ of the symmetric group. Suppose that $\widehat{A} = h^{S_n}$. Then $R(h, f) := \prod_{a\in\widehat{A}}(x - \varphi(a))$ is the product of the polynomials of the G-orbits within $\widehat{A}$. We call $R(h, f)$ a *resolvent*. (The name derives from the fact that polynomials of such type were used initially to solve polynomial equations.)

If condition (3) is fulfilled, the $\mathbb{Q}$-irreducible factors of $R(h, f)$ are in bijection to the G-orbits on h^{S_n}. Especially, the factor degrees are the orbit lengths and a factor discriminant is a square if and only if the image of the action on the corresponding orbit is a subgroup of the alternating group.

We define the *parity* of a permutation action to be even if the image of this action is a subgroup of the alternating group and odd otherwise.

By the Galois correspondence we also deduce immediately the same type of correspondence between the orbits of $U \leq G$ and the factorization of $R(g, f)$ over $\mathbb{Q}(\beta)$ when U and $\mathbb{Q}(\beta)$ are Galois correspondents. Such intermediate fields can be obtained by factors of other resolvents or simply by adjoining the root of the discriminant to obtain a field in correspondence to the subgroup of even permutations.

Using this approach one might compute sufficiently many orbit lengths and parities of G and its subgroups to identify up to conjugacy the Galois group uniquely among a list of all transitive subgroups of S_n. A list with the possible orbit lengths and parities therefore has to be prepared a priori. The method will give only the permutational type of the group but not its actual action on the roots. An algorithm of this type has been implemented by the author in GAP 3 [S+97] for $n \leq 15$.

2.5. **Computation of resolvents.** We note that the coefficients of $R(h,f)$ are symmetric in the root of f. So they can be expressed in the elementary symmetric functions in the $\{\alpha_i\}$ (which are up to a sign the coefficients of f) using only ring operations. Practically this could be done using resultants [Loo82].

As these resultant calculations can be computationally expensive, however, we shall restrict ourselves to the orbits of elements of the type $x_1+\cdots+x_k$, $x_1\cdot\cdots\cdot x_k$ or $x_1+2x_2+\cdots+kx_k$. As they correspond to the orbits on k-sets, respectively k-tuples of points, we call the arising resolvents *k-set resolvents* (respectively *k-tuple resolvents*). For computation of the set resolvents $R(x_1+\cdots+x_k,f)$ and $R(x_1\cdot\cdots\cdot x_k,f)$, efficient formulae have been published in [CM94].

For a resolvent $R=R(h,f)$, condition (3) simply means that R is square-free. This can be tested easily by checking whether $\gcd(R,R')=1$ (with $'$ denoting the usual derivative).

If $R(h,f)$ is not square-free, f gets replaced by a Tschirnhaus-transform $\hat{f}$ of f that defines the same field. Then $R(h,\hat{f})$ is computed anew. Unless the preimage of R in $\mathcal{R}$ already contains a square, there always is a transform $\hat{f}$ which renders $R(h,\hat{f})$ square-free [Gir83, theorem 3,(2)]. The transformations given in the proof in [Gir83] however not only might involve resultant calculations to compute $\hat{f}$ but also result in a polynomial $\hat{f}$ with very large coefficients. Thus in practice we restrict ourselves to simple combinations of the transformations $\tau_1\colon f(x)\mapsto f(x+1)$ and $\tau_2\colon f(x)\mapsto x^n f(1/x)$. Both together generate (up to a sign) the modular group $PSL(2,\mathbb{Z})$ and so lead to a vast number of possible composite transforms. Most of them, however, have unsuitably large coefficients.

In some cases certain transforms will never yield a square-free resolvent and thus can be discarded immediately. For example if $f(x)=g(x^2)$ roots come in pairs differing by a sign. In such a case resolvents for $h=x_1+x_2$ are never square-free and τ_1 will not remedy this problem.

Instead of changing f it might be possible as well to change h (without changing the equivalence type of G's action, for example x_1+x_2 and x_1x_2 both correspond to the action on 2-sets) to $\hat{h}$ to obtain a square-free resolvent $R(\hat{h},f)$.

On a (square-free) $R(h,f)$, similar transforms can be used profitably to get its coefficients smaller again. (The size of the coefficients is a measure for the amount of lifting necessary in the factoring algorithm. Usually in the literature on polynomial factorization only transformations of type τ_2 are suggested.)

2.6. **Drawbacks.** Both methods mentioned so far rely on explicit lists of all transitive subgroups of the symmetric group of the given degree. Though progress has been made on the determination of such lists [Hul96] it will be hard to compute these lists for further degrees beyond 31. Also the needed determination of properties for all the relevant groups would take substantial time to be spent before running the actual identification algorithms. Finally handling the large lists involved (like for the over 25000 groups needed for degree 24) is a challenge on its own.

Our aim will be to combine both presented methods with a group theoretic approach. From this we obtain an algorithm that is capable of determining the Galois group up to a few possibilities in reasonable time, that will work independently of the degree, provided the Galois group itself is not overly large. It also provides the possibility to obtain the exact Galois group (not just the type but its exact action on approximated roots) if a user is willing to invest further computing resources on this problem. It is understood that there will be

cases remaining that are inherently hard to decide. These are basically highly transitive groups which are maximal with very large index in the symmetric or alternating group. The Mathieu groups are a typical examples of this.

3. A new approach

In general the orbits of G convey more information than only their lengths and the permutation actions parities. Therefore the approach from 2.5 does not necessarily make full use of the information obtained by the resolvent factors.

As an example of two potential Galois groups that have the same orbit lengths but different orbits consider $\frac{1}{2}[3{:}2]_c D(4)$ and $\frac{1}{2}[3{:}2]_d D(4)$, the 12th and 15th transitive group of degree twelve. (The names reflect the composition structure corresponding to a block system. Lists of all the groups and a description of the naming scheme used can be found in [CHM]. The same names are also used in GAP [S$^+$97].) On sets of order 2 both have 5 orbits of length 12 and one orbit of length 6. Even the parities for the actions on all those sets are the same for both groups. On the other hand, both groups are stabilizers of their respective partitions of 2-sets within the symmetric group.

To overcome this shortcoming, L. Soicher suggested the following approach [Soi]:

Suppose S_n acts on a domain Ω and $A \subset \Omega$ is an orbit of G. Then $G \leq \mathrm{Stab}_{S_n}(A)$ and $G \not\subset \mathrm{Stab}_{S_n}(B)$ for $B \subsetneqq A$. So the intersection of the orbit stabilizers is a subgroup of S_n containing G. By computing these stabilizers we therefore obtain approximations to G without the need to refer to tabulations of subgroups of S_n.

If a is a factor of a (square-free) resolvent $R(g, f)$ the orbit corresponding to a consists of those images $\hat{g}$ of g, for which $\varphi(\hat{g})$ is a root of a. We apply this for approximated roots, using approximation modulo a prime. Let p be a prime which does not divide the discriminant of f or $R(g, f)$ and let π be reduction modulo p as defined in the appendix. As π is a ring homomorphism, $\pi(\varphi(g))$ is a root of $\pi(a)$.

As in Lemma 2 this is sufficient to distinguish the orbits if $\pi(R(g, f))$ is square-free over $\mathbb{F}_p$. This holds, if $p \nmid \mathrm{disc}(R(g, f))$, so there are only finitely many unsuitable primes.

If we identify the roots by their approximations $\{\pi(\alpha_i)\}$ modulo p, we have $\pi(\varphi(h)) = h(\pi(\alpha_1), \ldots, \pi(\alpha_n))$ for any $h \in \mathcal{R}$. Once we have factorized the resolvent $R(g, f)$ obtained from the polynomial $g \in \mathcal{R}$ we compute the reduced values $\pi(\varphi(h))$ for all $h \in g^{S_n}$. Then, under the action of G, $\varphi(h)$ is in the orbit corresponding to the factor a of $R(g, f)$ if $\pi(\varphi(h))$ divides $\pi(a)$. Thus simple evaluation of polynomials if $\mathbb{F}_p$ will yield the orbits of G (with respect to the arrangement of the approximated roots $\pi(\alpha_i)$). Computations of this type can be performed very quickly.

3.1. k-Closures.

Usually, we are considering the action on k-tuples or k-sets of points. For these actions the stabilizer of all the orbits of G are "closures" as defined in [Wie69]: The k closure $G^{(k)}$ of $G \leq S_n$ is the largest subgroup of S_n which has the same orbits on k-tuples of points as G has. Similarly, the $\{k\}$-closure $G^{\{k\}}$ of G is the largest subgroup of S_n which has the same orbits on k-sets as G has. We call k the *level* of the closure. ($G^{(2)}$ also can be interpreted as the stabilizer of all the orbital graphs of G. These are directed graphs with vertices Ω and edges given by one orbit of G on $\Omega \times \Omega$.) Properties of such closures have been studied before in the literature [Wie69, Sie82], we list some of them which we shall need later on:

1) $G \leq G^{(k)} \leq G^{\{k\}}$.
2) $G^{(k+1)} \leq G^{(k)}$.
3) $G^{\{k+1\}} \leq G^{\{k\}}$ if $k < \lfloor \frac{n}{2} \rfloor$.
4) If $p \leq k$ then $p \mid |G|$ if and only if $p \mid \left|G^{(k)}\right|$.
5) If G has base length m then $G = G^{(k)}$ for all $k > m$.
6) $\left(G^{(k)}\right)^{(k)} = G^{(k)}$, $\left(G^{\{k\}}\right)^{\{k\}} = G^{\{k\}}$.
7) G has the same block systems as $G^{\{2\}}$.

As $G^{(k)} = S_n$ only if G is k-fold transitive, these closures quickly yield a proper subgroup of S_n. For a given permutation group G, closures can be computed as stabilizers by a backtrack search, the 2-closure can also be computed via the orbital graphs. Algorithms for these tasks have been published in [McK81, IAFM94, Leo91, The97] and are available in programs like nauty, COCO, Magma or GAP.

Suppose we have computed a set of closures of G up to the k-closure and $\{k'\}$-closure. Let C be their intersection. (Due to properties 2. and 3. this is in most cases the smallest of the closures computed. Nevertheless it is worthwhile to compute closures of different level, as knowledge of a closure can be very helpful for the factorization of resolvents, needed to compute a closure of higher level. See 5.2.) Then we know that G is a transitive subgroup of C with the following properties:

- G has the same m-closures and $\{m'\}$-closures as C (for all $m \leq k$ and $m' \leq k'$.);
- G contains elements of prescribed cycle types. (Obtained by factoring f, 2.1.)
- One element of G is known. (The Frobenius-Automorphism for the prime chosen to approximate the roots.)

We denote the set of all these groups by $\mathcal{L}$.

3.2. **Computation of $\mathcal{L}$.** While the computation of $\mathcal{L}$ might be difficult, it is easy to check, whether a given group U is contained in $\mathcal{L}$, as this involves mainly orbit calculations. So the main problem for the computation of $\mathcal{L}$ is to produce a sufficiently small superset of potential candidates.

To do so, we compute the maximal subgroups of C and test which of these are contained in $\mathcal{L}$. For these we compute again the maximal subgroups and so forth. As $\mathcal{L}$ is closed under taking intermediate chains (if $U, W \in \mathcal{L}$ and $U \leq V \leq W$, then also $V \in \mathcal{L}$) this process exhausts all possible groups in $\mathcal{L}$.

3.3. **Determination of G.** Usually $\mathcal{L}$ will contain more than one group. Nevertheless even this may be sufficient information to, say, show the solvability of the extension or give size bounds for the splitting field. If G is needed exactly, we will make use of the invariant method:

Suppose we know already that $G \leq U$. For each conjugacy class of maximal subgroups of U we compute an relative invariant h and check for all of its images under U whether $\varphi(h^u) \in \mathbb{Z}$. We do this using p-adic approximation of the roots of f as in [DF89].

The use of relative invariants requires knowledge of the action of U on the approximated roots. This is fulfilled as we obtained C not only up to conjugacy but also its action.

Of course in practice one should combine the determination of $\mathcal{L}$ with the downward steps and only compute maximal subgroups of a group U after G has been proven to be contained therein.

4. Group theoretic problems

Algorithms published so far for the determination of Galois groups [AV94, SM85, Sta73] were usually limited to a predetermined set of possible degrees (those degrees for which

invariants or orbits information were precomputed). Thus asking for the complexity of these algorithms was not a sensible question. On the other hand the presented approach is, a priori, degree-independent. To estimate its performance, it is crucial, however, to learn more about the set $\mathcal{L}$. Similarly knowledge about $\mathcal{L}$ can determine up to which level closures should be computed.

This leads to purely group-theoretic questions about the set $\mathcal{L}$ of permutation groups. We will state these questions, indicate which type of answer we need for our algorithm to perform well, and give some indication why these hopes are not unreasonable. A full answer seems to be beyond the scope of this article.

Problem 1: How large is $\mathcal{L}$? As the groups in $\mathcal{L}$ have to be distinguished by invariants, we hope that $\mathcal{L}$ is small.

Experiments with degrees up to 16 show that if C is the intersection of the 2- and the $\{4\}$-closure, that $\mathcal{L}$ is typically of size less then 10 and almost always of size less than 20. The worst case is size 106 in degree 16.

If we have computed k-closures we can (property 5) uniquely identify all groups of base length smaller than k. For example, for primitive, not 2-transitive groups, the base length is limited to $4\sqrt{n}\log n$ [DM96, Theorem 5.3A]. (By property 7., we know whether G is primitive, 2-transitivity is determined by the 2-closure.)

Problem 2: How different are the groups in $\mathcal{L}$? Or – in other words – which properties of G can we deduce from $\mathcal{L}$? We hope the groups in $\mathcal{L}$ to be of small index in the largest one, as this reduces the number of conjugate maximal subgroups and thus the number of invariants that have to be tested. Again experiments with degrees up to 16 show that for C the intersection of the 2- and the $\{4\}$-closure, the largest and smallest group in $\mathcal{L}$ differ typically by a factor of less than 10 and almost always by less than 100. By far the worst case is index 5040 in degree 12, which happens for M_{12}. Such highly transitive groups however occur rarely and should be considered as exceptions.

For higher degrees however closures of higher level will be needed: If U and V have the same $\{k\}$-closure then for any transitive T the groups $U \wr T$ and $V \wr T$ (acting naturally) have the same $\{k\}$-closure, but $[U \wr T : V \wr T] = [U : V]^{\deg T}$. Therefore the size range for groups with the same $\{k\}$-closure can grow exponentially.

The properties of the closures show that we can obtain small prime divisors of $|G|$ and block systems of G from knowledge of C.

Problem 3: Compute the maximal subgroups. If the group is small, one can simply compute the full subgroup lattice to obtain maximal subgroups iteratively. For solvable groups in general, there is an efficient algorithm to compute maximal subgroups [Eic93]. In the insolvable case such an algorithm (without computing the full lattice first) is still a desideratum. However use of the O'Nan-Scott theorem [DM96, 4.1A] could provide an approach. Finally, for degrees up to 31, the lists of transitive permutation groups computed in [Hul96] can be used.

4.1. **Problem 4: Determination of invariants.** When computing relative invariants for $V < U$ we need *one* invariant of V that is not invariant under U. Furthermore, we want this invariant to be "small", not only to reduce the amount of work needed to evaluate one invariant but also to reduce the magnitude of $|\varphi(h)|$ (which determines the needed p-adic lifting accuracy). As sum of monomials this magnitude is determined primarily by the degree

of the monomials. As we use p-adic instead of numerical approximation, error propagation is not a problem. Thus it is not critical to express h in a special way.

The permutation image of a monomial is a monomial of the same degree. So we can assume without loss of generality that we are looking for a homogeneous invariant which is the V-orbit sum $b = \sum_{c \in a^V} c$ of a "defining" monomial a. It is a V-invariant for U if $\left|a^U\right| > \left|a^V\right|$. If V is normal in U (note that V is maximal in U anyhow) this holds if and only if $\mathrm{Stab}_U(a) \leq V$, otherwise this criterion is sufficient but not necessary.

Classical results on the generation of invariant rings [Noe16] concentrate on generating the full invariant ring and so give an unsuitably large bound (namely $|G|$) for the degree of a.

To restrict the degree we observe the following bounds: If $(b_1, \ldots, b_m)$ is a base of U the monomial $x_{b_1} \cdot x_{b_2}^2 \cdot \cdots \cdot x_{b_m}^m$ has a regular orbit under U and so may serve as an a. So $\deg(a) \leq \frac{m(m+1)}{2}$. Similarly $\deg(a) > k$ if both groups have the same k-closure.

If U and V are small enough to compute their conjugacy classes, one can also compute the Molien series $F_U(\lambda)$ for the permutation action [Sta79]. (It is sufficient to know the conjugacy classes of U to compute this series.) In expanded form $F_U(\lambda) = \sum_{i \geq 0} d(U)_i \lambda^i$ with $d(U)_i$ being the dimension of the space of the i-dimensional homogeneous invariants of U. So the smallest i for which $d(V)_i > d(U)_i$ is the smallest possible degree.

As we are interested only in invariance and not in absolute degrees we can assume that the exponent i occurs in a only if the exponent $i-1$ occurs as well. So we may assume that

$$a = (x_{i_1} \cdots x_{i_{l_1}})(x_{i_{l_1+1}} \cdots x_{i_{l_2}})^2 \cdot \cdots \cdot \left(x_{i_{l_{m-1}+1}} \cdots x_{i_{l_m}}\right)^m \tag{4}$$

with $l_1 \geq l_2 - l_1 \geq \cdots \geq l_m - l_{m-1}$. The stabilizer of such a monomial is an m-times iterated stabilizer of sets of length $l_i - l_{i-1}$. (As the computation of set stabilizers is usually easier for smaller sets, this stabilizer should be computed backwards from m to 1.)

A general strategy to compute invariants is discussed in [Gir87].

It is shown in [Göb95] that a orbit sums of a subset of the monomials of the form (4) of degree at most $\max(n, n(n-1)/2)$ generate the full invariant ring.

5. Factoring resolvents

The hardest subtask of the proposed algorithm usually will be the factorization of the resolvents.

5.1. **Difficulties.** For the usual factoring approach [Zas69],[DST88, §4.2.2] of Hensel lifting combined with trial quotients of the polynomial with products of the lifted factors, the resolvent polynomials $R(g, f)$ are of the worst possible kind: By Dedekind's theorem (5) the degrees of the factors of $R(g, f)$ modulo any prime divide the order of elements in $\mathrm{Gal}(f)$, but the degrees of the irreducible factors of $R(f, g)$ are orbit lengths of $\mathrm{Gal}(f)$ and so of magnitude $|\mathrm{Gal}(f)|$ instead of $|\sigma|$ ($\sigma \in \mathrm{Gal}(f)$). Thus as soon as the Galois group is not regular, resolvent polynomials will split into many factors modulo any prime while splitting only in few factors over $\mathbb{Q}$. So not only many factors have to be lifted first, but also the exponential combination step might become extremely hard.

An obvious remedy seems to be the use of a polynomial time factoring algorithm as suggested in [LLL82]. Unfortunately this algorithm requires substantially better lifting and thus has a comparatively worse runtime in "small" cases. However, on current computers

within reasonable run times only such "small" examples can be computed anyhow. The break-even point of the exponential algorithm can not yet be reached.

5.2. **Use of partial information.** If we use the fact that we do not factor arbitrary polynomials but resolvents, we can help the factoring algorithm: The partial knowledge about the Galois group and its possible actions will limit the possible orbit lengths and thus the possible factor degrees:

Factoring a polynomial a means to find the orbits of the Galois group on its roots. The first approximation are the orbits of one element (the Frobenius automorphism) of this Galois group. They are given by factorization modulo p: $a \equiv \prod_i a_i \pmod p$. This approximation is used in the standard Hensel lifting. Suppose, we have already computed a closure C from the factorization of some resolvents R_i. Reduction of the factors of the R_i modulo this prime p gives (by the save process as described in section 3) the action of C on the roots of f modulo p and in turn (if a is a resolvent) on the roots of a. G is a subgroup of C and so the orbits of G refine the orbits of C. This yields a partition $\mathcal{J}$ of the $\{a_i\}$ (modulo p). When combining the lifted factors, only the $a_i \pmod{p^m}$ in the same block $J \in \mathcal{J}$ of the partition (i.e. $i \in J$) have to be combined. Furthermore this will give better bounds for the degrees of potential factors, probably reducing the necessary lifting bound.

If we even know $\mathcal{L}$ (or a reasonably small superset) we can also test whether modulo p the roots of two factors – say a_i and a_j – always lie in the *same* orbit of U for all $U \in \mathcal{L}$. If this is the case, the factorization will not separate a_i and a_j and we can replace them by their product even before starting the lifting. (Note that Hensel lifting only requires coprime factors. They do not need to be irreducible.)

Both reductions will substantially reduce the work needed for the factorization.

6. Block systems

We have noted already that we obtain the imprimitivity structure of the Galois group G even from the $\{2\}$-closure of G. If the degree n is high, however, factorizing the 2-set resolvent might be initially too hard while computation of block systems [Hul95, KP97] is still feasible. Then we can compute the intersection of the corresponding wreath products and take this as a group C to simplify the polynomial factorization (5.2).

Recall that each block system corresponds to a subfield of $\mathbb{Q}(\alpha)$. We can express a primitive element γ of this subfield as a polynomial $\gamma = h(\alpha)$ and take the minimal polynomial g of γ. So $g(h(\alpha)) = 0$, respectively $f(x) | g(h(x))$.

Then the evaluation of h at any root α_i of f will yield a root of g, which corresponds to a block. So every block consists of those roots α_i of f which evaluate under h to the same number γ_j. Again this test can be done modulo any non-ramifying prime.

If a system of m blocks of size l has been found G is a subgroup of $S_l \wr S_m$. By calling the identification algorithm recursively to determine the action of G on the blocks we can further restrict to the wreath product $S_a \wr \mathrm{Gal}(g)$, its top group acting on the blocks as $\mathrm{Gal}(g)$ does. While the $\{2\}$-closure already determines the block systems, it does not necessarily determine this block action $\mathrm{Gal}(g)$. Therefore this identification may reduce C to a smaller group and improve the discrimination of groups.

Theoretically, by the theorem of Krasner and Kaloujnine [KK51], one could even replace S_a by the action of a block stabilizer on its block. However, the determination of this action requires the identification of Galois groups over algebraic extensions which seems

to be too expensive for the gain possible.Also, for obtaining the correct permutation action, this identification would have to take place for any block, as we do not get the action of $\mathrm{Gal}(g)$ on the roots of f.

The method of [KP97] utilizes p-adic approximation of the roots of f. Therefore it might be desirable to use the same prime later on for determining G's action, as the root approximations can be re-used.

We finish this section with the remark that though the best known practical algorithm [KP97] to find block systems is of exponential nature the problem is known to be polynomial in theory [LM85].

Appendix: Reduction modulo a prime

The aim of this appendix is to establish some facts about the relation of field extensions over $\mathbb{Q}$ defined by a polynomial f with extensions of the prime field $\mathbb{F}_p$ defined by a reduction of f modulo p. We shall consider only extensions of the base fields. Generalization to relative extensions is possible, but will not be needed here. For this as well as for proofs we refer to the literature [Cas86, Mar77, Neu92]. We assume knowledge of basic Galois theory. (This appendix proceeds relatively quickly through material which is not needed elsewhere in the paper. The faint-hearted may want to skip it almost completely and only take theorem 5 and the existence of the homomorphisms established in the last paragraph of this appendix as facts.)

For any prime p there is the p-adic valuation ν_p of the rational numbers given by $\nu_p(\frac{a}{b}) = n$ if $\frac{a}{b} = p^n\frac{c}{d}$ with $p \nmid c, d$. Taking the completion of the rationals with respect to this valuation we obtain the p-adic field $\mathbb{Q}_p$. There is a natural embedding of $\mathbb{Q}$ into $\mathbb{Q}_p$ and we will from now on consider $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$ without explicitly mentioning this embedding. This implies that we can embed the algebraic closure $\overline{\mathbb{Q}}$ of the rationals into the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. If we embed L (as L is a normal extension this image is unambiguous) into $\overline{\mathbb{Q}}_p$ we get a normal extension $L_p = \langle L, \mathbb{Q}_p\rangle$ of $\mathbb{Q}_p$. The Galois group $\mathrm{Gal}(L_p/\mathbb{Q}_p)$ of this extension then naturally embeds into $\mathrm{Gal}(L/\mathbb{Q})$. Note that $[L_p : \mathbb{Q}_p]$ might be strictly smaller than $[L : \mathbb{Q}]$ and the Galois groups be strictly contained in each other, because $\mathbb{Q}_p$ already contains algebraic irrationalities.

As $\mathbb{Q}_p$ is complete there is a unique extension of ν_p to L_p. For $K \in \{\mathbb{Q}_p, L_p\}$ we consider the discrete valuation rings $\mathcal{O}(K) = \{k \in K \mid \nu_p(k) \geq 0\}$ and their maximal ideals $\mathcal{P}(K) = \{k \in K \mid \nu_p(k) > 0\} \lhd \mathcal{O}(K)$. We note that $\mathcal{O}(\mathbb{Q}_p) = \mathbb{Z}_p$. By definition we have $\mathcal{O}(L_p) \cap \mathbb{Q}_p = \mathbb{Z}_p$ and $\mathcal{P}(L_p) \cap \mathbb{Q}_p = \mathcal{P}(\mathbb{Q}_p)$. As $1/k \in \mathcal{O}(K)$ for $k \in K \setminus \mathcal{O}(K)$ (by the definition of a valuation ring), we have $\langle \mathbb{Q}_p, \mathcal{O}(L_p)\rangle = L_p$ while $M := \langle \mathbb{Z}_p, \mathcal{P}(L_p)\rangle$ usually is smaller than $\mathcal{O}(L_p)$. We also note that the ring $\mathcal{O}(L)$ of algebraic integers in L is contained in $\mathcal{O}(L_p)$, because $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathcal{O}(L_p)$ and because valuation rings are integrally closed. Table 1 illustrates this situation.

As $\mathcal{P}(K)$ is a maximal ideal in the integral domain $\mathcal{O}(K)$ the quotient ring $\mathcal{O}(K)/\mathcal{P}(K)$ is a field. This field is finite because the valuation is discrete. We have $\mathbb{Z}_p/\mathcal{P}(\mathbb{Q}_p) \cong \mathbb{F}_p$, the field with p elements. By the isomorphism theorem we get a natural embedding

$$\mathbb{Z}_p/\mathcal{P}(\mathbb{Q}_p) \cong M/\mathcal{P}(L_p) \hookrightarrow \mathcal{O}(L_p)/\mathcal{P}(L_p) =: \mathbb{F}_q,$$

thus $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_p$.

There is a natural homomorphism (action modulo $\mathcal{P}(L_p)$) from $\mathrm{Gal}(L_p/\mathbb{Q}_p)$ onto $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. The kernel of this mapping is usually called the *ramification subgroup*. If it is nontrivial we

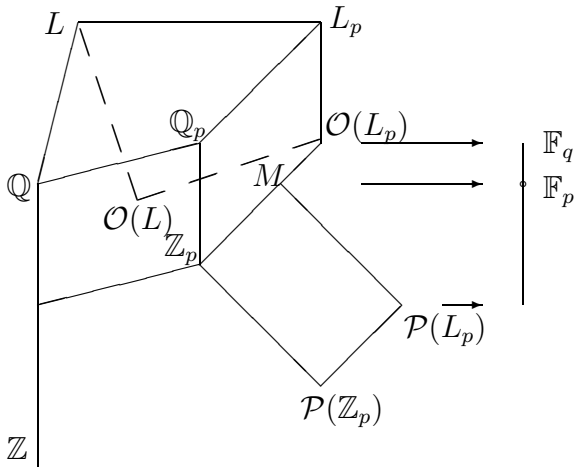

TABLE 1. Algebraic extensions

call p a *ramifying prime*. If L is the splitting field of f, every ramifying prime must divide the discriminant of $\mathbb{Q}(\alpha)/\mathbb{Q}$ and thus divides the discriminant of f. So there are only finitely many ramifying primes and we can avoid these when choosing a prime.

If $L_p/\mathbb{Q}_p$ does not ramify we have $\mathrm{Gal}(L_p/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Accordingly, there is an element in $\mathrm{Gal}(L/\mathbb{Q})$ that corresponds to the Frobenius automorphism (taking p-th powers) generating $\mathrm{Gal}(\mathbb{F}_q, \mathbb{F}_p)$. We call this element in $\mathrm{Gal}(L/\mathbb{Q})$ the p-Frobenius automorphism. If L is the splitting field of f, the action of the p-Frobenius automorphism on the roots of f is the same as the action of the Frobenius automorphism on the roots of the reduction of f modulo p. The orbits of this automorphism then are in correspondence to the irreducible factors of f modulo p. We have shown:

Theorem 5 (DEDEKIND's theorem[vdW71, §66])**.** *For a prime p not dividing the discriminant of an irreducible rational polynomial f the degrees of the irreducible factors of f modulo p give the cycle shape of one element in the Galois group of f.*

Using analytic number theory this result can be strengthened to the TSCHEBOTAREFF density theorem [Tsc25], by which the density of the non-ramifying primes for which the Frobenius automorphism has a given shape equals the proportion of elements of this shape in the Galois group G.

It can be shown that $\mathrm{Gal}(L/\mathbb{Q})$ is generated by all ramification subgroups. Unfortunately this property cannot be utilized easily, as each ramification subgroup is given by its action on the roots in L_p. However, there is no simple way (without knowing G) to identify the roots in L_p with those in $L_{p'}$ for two different primes p and p'. This identification would be needed to obtain the group they generate together.

Finally, for all powers of $\mathcal{P}(L_p)$ there is a natural ring homomorphism ("reduction modulo p^n"), the approximation map $\pi_i \colon \mathcal{O}(L_p) \to \mathcal{O}(L_p)/\mathcal{P}^i(L_p)$ that restricts to $\pi_i|_{\mathbb{Z}_p} \colon \mathbb{Z}_p \to \mathbb{Z}_p/\mathcal{P}^i(\mathbb{Q}_p) \cong \mathbb{Z}/p^i\mathbb{Z}$. Restricted to $\mathbb{Z}$ this is the well known reduction modulo p^n. We usually abbreviate π_1 to π.

Acknowledgements

I'm indebted to Leonard Soicher for suggesting to me the use of stabilizers as described in section 3 instead of orbit lengths. This collaboration was enabled by an HCM grant of the European Union, whose support I gratefully acknowledge. I would also like to thank Werner Nickel for many helpful comments on a first draft of this paper and Andrew Cutting for rectifying my English.

References

[AV94] Jean-Marie Arnaudies and Annick Valibouze, *Groupes de Galois de polynômes en degré 10 ou 11*, Rapport interne 94.50, Laboratoire informatique théoretique et programmation, Université Paris VI, 1994.

[Cas86] J.W.S. Cassels, *Local fields*, L.M.S. Student Texts, no. 3, Cambridge University Press, 1986.

[CHM] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, to appear in LMS Journal of Computation and Mathematics ().

[CM94] David Casperson and John McKay, *Symmetric functions, m-Sets and Galois groups*, Math. Comp. **63** (1994), no. 208, 749–757.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, Heidelberg, 1993.

[Col95] Antoine Colin, *Formal computation of Galois groups with relative resolvents*, Applied algebra, Algebraic algorithms and Error-correcting Codes (Gérard Cohen, Marc Giustini, and Teo Mora, eds.), Lecture Notes in Computer Science, vol. 948, Springer, Heidelberg, 1995, pp. 169–182.

[DF89] Henri Darmon and David Ford, *Computational verification of M_{11} and M_{12} as Galois groups over Q*, Comm. Algebra **17** (1989), 2941–2943.

[DM96] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer, Heidelberg, 1996.

[DSar] J[ames] H. Davenport and Geoff Smith, *Fast recognition of symmetric and alternating galois groups*, to appear.

[DST88] J[ames] H. Davenport, Y. Siret, and E. Tournier, *Computer algebra*, Academic Press, 1988.

[Eic93] Bettina Eick, *PAG-Systeme im Computeralgebrasystem GAP*, Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1993.

[EO95] Y[ves] Eichenlaub and M[ichel] Olivier, *Computation of Galois groups for polynomials with degree up to eleven*, Preprint, Université Bordeaux I, 1995.

[Gir83] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), 289–307.

[Gir87] K. Girstmair, *On invariant polynomials and their application in field theory*, Math. Comp. **48** (1987), 781–797.

[Göb95] Manfred Göbel, *Computing bases for rings of permutation-invariant polynomials*, J. Symb. Comput. **19** (1995), 285–291.

[Hul95] Alexander Hulpke, *Block systems of a Galois group*, Experimental Mathematics **4** (1995), no. 1, 1–9.

[Hul96] Alexander Hulpke, *Konstruktion transitiver Permutationsgruppen*, Ph.D. thesis, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1996.

[IAFM94] M. H. Klin I. A. Faradžev and M. E. Muzichuk, *Cellular rings and groups of automorphisms of graphs*, Investigations in algebraic theory of combinatorial objects (I. A. Faradžev, A. A. Ivanov, M. H. Klin, and A. J. Woldar, eds.), Mathematics and its Applications (Soviet Series), vol. 84, Kluwer, 1994, pp. 1–152.

[KK51] Marc Krasner and Leo [A.] Kaloujnine, *Produit complet des groupes de permutations et problème d'extension de groupes II*, Acta Sci. Math. (Szeged) **14** (1951), 39–66.

[KP97] J[ürgen] Klüners and M[ichael E.] Pohst, *On computing subfields*, J. Symb. Comput. **24** (1997), 385–397.

[Leo91] Jeffrey S. Leon, *Permutation group algorithms based on partitions, I: theory and algorithms*, J. Symb. Comput. **12** (1991), 533–583.

[LLL82] A.K. Lenstra, H.W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[LM85] Susan Landau and Garry Miller, *Solvability by radical is in polynomial time*, J. Comput. System Sci. **30** (1985), 179–208.

[Loo82] Rüdiger Loos, *Computing in algebraic extensions*, Symbolic and Algebraic Computation (Bruno Buchberger, George Edwin Collins, and Rüdiger Loos, eds.), Springer, Wien, 1982, pp. 173–187.

[LPS87] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), 365–383.

[Mar77] Daniel A. Marcus, *Number fields*, Springer, Heidelberg, 1977.

[McK81] Brendan D. McKay, *Practical graph isomorphism*, Congr. Numer. **30** (1981), 45–87.

[Neu92] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer, Heidelberg, 1992.

[Noe16] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89–92.

[S$^+$97] Martin Schönert et al., *GAP 3.4, patchlevel 4*, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1997.

[Sie82] Johannes Siemons, *On partitions and permutation groups on unordered sets*, Arch. Math. (Basel) **38** (1982), 391–403.

[SM85] Leonard [H.] Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

[Soi] Leonard H. Soicher, personal communication.

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[Sta79] Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), no. 3, 475–511.

[The97] Heiko Theißen, *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen*, Dissertation, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1997.

[Tsc25] Nikolaj Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95** (1925), 191–228.

[vdW71] B[artel] L. van der Waerden, *Algebra, erster Teil*, eighth ed., Heidelberger Taschenbücher, vol. 12, Springer, Heidelberg, 1971.

[Wie69] Helmut Wielandt, *Permutation groups through invariant relations and invariant functions*, Lecture notes, Department of Mathematics, The Ohio State University, 1969.

[Zas69] Hans Zassenhaus, *On Hensel factorization I*, J. Number Theory **1** (1969), 291–311.

University of St. Andrews, School of Mathematical and Computational Sciences, The North Haugh, UK-St. Andrews, Fife KY16 9SS

E-mail address: ahulpke@dcs.st-and.ac.uk