Journal of Symbolic Computation 71 (2015) 73–97

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

# Computing Galois groups of polynomials (especially over function fields of prime characteristic)

Nicole Sutherland

*Computational Algebra Group, School of Mathematics and Statistics, University of Sydney, Australia*

ARTICLE INFO

*Article history:*
Received 27 June 2014
Accepted 25 September 2014
Available online 2 October 2014

*MSC:*
11R32

*Keywords:*
Galois groups
Function fields

ABSTRACT

We describe a general algorithm for the computation of Galois groups of polynomials over global fields from the point of view of using it to compute Galois groups of polynomials over function fields with prime characteristic, including characteristic 2 in which some invariants which are efficient to use in other characteristics are invariant for too large a group. We state new invariants for most of these situations when the characteristic is 2. We also describe the use of this algorithm for computing Galois groups of reducible polynomials over both number fields and function fields.


## 1. Introduction

There are a number of algorithms available for computing Galois groups and some of these algorithms have been known for some time. Chronologically each algorithm published has increased the degrees of the polynomials it accepts as input. A limitation on degrees has been due to the use of tabulated information. Geißler (2003) provides an algorithm for Galois groups of polynomials of degree at most 23 over $\mathbb{Q}$ and $k(t)$. This was the most recent work on algorithms for Galois groups when Fieker and Klüners (2014) developed their algorithm for Galois groups of polynomials. Unlike most previous algorithms the algorithm of Fieker and Klüners (2014) is not degree restricted (Hulpke, 1999, is not degree restricted either, however, it usually cannot determine the Galois group uniquely), and it can compute the Galois group of any polynomial over any algebraic number field or algebraic function field (including of course $\mathbb{Q}$ and $k(t)$ for $k = \mathbb{F}_q, \mathbb{Q}$). It has been implemented in Magma

*E-mail address:* nicole.sutherland@sydney.edu.au.

http://dx.doi.org/10.1016/j.jsc.2014.09.043
0747-7171/

(Cannon et al., 2010) V2.13 for polynomials over $\mathbb{Q}$ and in V2.14 for polynomials over number fields and $\mathbb{Q}(t)$.

We describe here the algorithm of Fieker and Klüners (2014) which we have implemented in Magma (Cannon et al., 2010) for polynomials over $\mathbb{F}_q(t)$ (V2.16) and global algebraic function fields (simple extensions of $\mathbb{F}_q(t)$) (V2.17). This is the first implementation, of which we know, of an algorithm for computing Galois groups over global function fields which is not restricted by the degree of the polynomial. It is also the first algorithm (that we know of) which uses the computation of subfields (and in particular the generating subfields as introduced by van Hoeij et al., 2011) of global function fields in calculating the Galois group. This algorithm is based on Stauduhar (1973).

A particular difficulty in generalizing (Fieker and Klüners, 2014) is that the invariants they provide for some groups $G$ and $H$ are $S_n$-invariant when the characteristic is 2 and so are never $G$-relative $H$-invariants (Definition 2). For such groups $G$ and $H$ we state in this paper (Section 3.5) some new polynomials which are $G$-relative $H$-invariant when the characteristic is 2. These invariants are a key part of the paper.

We will first give an overall view of the algorithm and then expand on the details from the point of view of using this algorithm to compute Galois groups of polynomials over global function fields. We also mention how this algorithm can be used to compute Galois groups of reducible polynomials over algebraic number fields and global algebraic function fields.

We begin with some definitions.

**Definition 1.** The *Galois group*, $\mathrm{Gal}(f)$, of a polynomial $f$ over a field $F$ is the automorphism group of $S_f/F$ where $S_f$ is the splitting field of $f$ over $F$.

When $f$ is irreducible over $F$ and of degree $n$ we compute Galois groups as transitive subgroups of $S_n$.

Invariants and resolvents are an important part of our algorithm. We define invariants and resolvents here and discuss the uses of the different types later. Let $R$ be a commutative unitary domain and $I(x_1, \ldots x_n) \in R[x_1, \ldots x_n]$. A permutation $\tau \in S_n$ acts on $I$ by permuting $x_1 \ldots, x_n$ and we write $I^\tau$ for this action.

**Definition 2.** A polynomial $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ such that $I^\tau = I$ for all $\tau \in H$ for some group $H \subseteq S_n$ is said to be *$H$-invariant*.

An $H$-invariant polynomial $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is a *$G$-relative $H$-invariant* polynomial if $I^\tau \neq I$ for all $\tau \in G \setminus H$, $H \subset G \subseteq S_n$, that is, for the stabilizer in $G$ we have $\mathrm{Stab}_G I = H$.

For a $G$-relative $H$-invariant polynomial $I$ we can compute a $G$-relative $H$-invariant *resolvent polynomial*

$$Q_{(G,H)}(y) = \prod_{\tau \in G//H} \left(y - I^\tau(x_1, \ldots, x_n)\right),$$

where $G//H$ denotes a system of representatives for the right cosets $H\tau$ of $G/H$. If $G = S_n$ then we call $Q$ an *absolute resolvent*, otherwise we call $Q$ a *relative resolvent*.

An $S_n$-relative $H$-invariant is a $G$-relative $H$-invariant and a $G$-relative $H$-invariant is an $H$-invariant but the converse is not always true.

We recall the definition of a block system as found in Geißler and Klüners (2000, Definition 2.14), as it is crucial to the definition of a number of our special invariants.

**Definition 3.** Let $G$ be a transitive permutation group acting on a finite set $\Omega$. A subset $\emptyset \neq \Delta \subset \Omega$ is called a *block* if $\Delta \cap \Delta^\sigma \in \{\emptyset, \Delta\}$ for all $\sigma \in G$. The orbit of a block $\Delta$ under $G$ is called a *block system*.

The blocks we use will be subsets of $\Omega = \{\text{roots of } f\}$. A block system of a group $G$ is a block system for the transitive subgroups of $G$ but the converse does not always hold.

### 1.1. Previous work

Our algorithm is very similar to that of Geißler and Klüners (2000) and Geißler (2003). They use many of the same techniques that we do. Their algorithm is also based on Stauduhar (1973) and uses relative resolvents. They use subfields, short cosets and $p$-adic methods in their algorithm also. However, their algorithm can only be applied to polynomials of degree less than 15 (Geißler and Klüners, 2000) and degree less than 23 (Geißler, 2003).

The method of Stauduhar (1973) is also used by Eichenlaub (1996) who implemented their algorithm in Pari for polynomials of degree up to 11.

Another method is that of the absolute resolvent. Such resolvents can be computed from coefficients of polynomials and a factorization may give enough information about the Galois group to identify it. However, for degrees larger than say 11 these factorizations can be rather expensive. For algorithms using this method see Soicher (1981), Soicher and McKay (1985), Mattman and McKay (1997), Casperson and McKay (1994).

The absolute resolvent method can be combined with the method of Stauduhar as a verification step. This is described in Geißler and Klüners (2000), Geißler (2003). It is used when the index of the maximal subgroup $H$ in $G$, a group which we know contains the Galois group, is large and we choose to use a smaller precision for the approximations of the roots of the polynomial than required for a proven descent to shorten the running time of the algorithm and leave the proof of the descent step from $G$ to $H$ till later (if indeed we decided that the Galois group may be contained in $H$), see Section 3.8.

The use of $p$-adic approximations in the method of Stauduhar was first suggested by Yokoyama (1997). Such approximations were also used by Darmon and Ford (1989) independently of Stauduhar's method. Previous to this complex approximations to roots of rational polynomials were used which required higher precisions to obtain proven results. We have extended this idea in our choice of local splitting fields for polynomials over rational function fields.

## 2. An algorithm for computing Galois groups

We describe here the algorithm used by Fieker and Klüners (2014) with no degree restrictions. A similar algorithm was used by Geißler (2003) and Geißler and Klüners (2000).

Let $f$ be a separable polynomial of degree $n$ over a field $F$ with splitting field $S_f$. An $F$-automorphism of $S_f$ will permute the roots of $f$ and this permutation will determine the automorphism completely, therefore we represent Galois groups as groups of permutations acting on the roots of $f$ in some fixed ordering. We know that a Galois group will be a subgroup of $S_n$, the task is to discover which one.

The algorithm of Stauduhar (1973) traverses maximal subgroups until it finds one the Galois group is contained in or finds that the Galois group is contained in no maximal subgroup so must be the group we know it is contained in. Maximal subgroups are computed in Magma (Cannon et al., 2010) using an algorithm by Cannon and Holt (2004).

**Theorem 4.** *(See Stauduhar, 1973.) Let $f(x)$ be a separable polynomial of degree $n$ over a field $F$. Let $\alpha_1, \ldots, \alpha_n$ be a fixed ordering of the roots of $f(x)$ in $S_f$. Suppose $G$ is a subgroup of $S_n$ and suppose that with respect to the given ordering of the roots, the Galois group $\mathrm{Gal}(f)$ of $f(x)$ is a subgroup of $G$. Let $H$ be a subgroup of $G$ and $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be a $G$-relative $H$-invariant polynomial. Let $\tau_1, \ldots, \tau_k$ be representatives for the right cosets of $H$ in $G$. For all $i$, $I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is a root of the resolvent polynomial*

$$Q_{(G,H)}(y) = \prod_{i=1}^{k} \left(y - I^{\tau_i}(\alpha_1, \ldots, \alpha_n)\right) \in F[y].$$

*Assume $I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is not a repeated root of $Q_{(G,H)}(y)$. Then $\mathrm{Gal}(f) \subseteq \tau_i G \tau_i^{-1}$ iff $I^{\tau_i}(\alpha_1, \ldots, \alpha_n) \in F$.*

For polynomials $f \in \mathbb{F}_q(t)[x]$ this means that $I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is a rational function instead of an algebraic function. The above theorem is a generalization of Theorem 5 of Stauduhar (1973) which is stated for irreducible polynomials, transitive groups and $F = \mathbb{Q}$.

Stauduhar considers roots of $f$ in the complex field, however it is more efficient to compute roots of $f$ in the splitting field of $f$ over the completion of $F$ at some finite prime $P$ which is what the algorithms of Geißler and Klüners (2000), Geißler (2003) and Fieker and Klüners (2014) do following (Yokoyama, 1997). This approach also generalizes more easily between number fields and function fields.

**Algorithm 1** *(Galois group of an irreducible polynomial $f$).* We take as input an irreducible separable polynomial $f$ of degree $n$ over an algebraic number field or algebraic function field $F$ (including $\mathbb{Q}$, $\mathbb{F}_q(t)$ or $\mathbb{Q}(t)$).

(1) Choose a prime $P$ of $F$ such that the image of $f$ is squarefree over the residue field at $P$.
(2) Find a scaling factor $s$ such that $s\alpha_i$ is integral ($s\alpha_i \in \mathbb{Z}, \mathbb{F}_q[t], \mathbb{Q}[t]$ or a finite extension thereof) for all roots $\alpha_i$ of $f$. Each $s\alpha_i$ will be a root of $f_s = s^{n-1} f(x/s)$.
(3) Compute the splitting field $S_{f,P}$ for $f$ over the completion of $F$ at the prime $P$.
(4) Compute the roots of $f$ in $S_{f,P}$ to low precision to fix an ordering.
(5) Find a group $G$ which the Galois group of $f$ is contained in ($S_n$ will always do here, although we can sometimes do better):
  (a) Compute the generating subfields (van Hoeij et al., 2011) of the field extension $F[x]/f$ and the Galois groups of the normal closures of these subfields.
  (b) Compute the intersection of the wreath products of $S_{n/l}$ with the Galois groups of the normal closures of subfields of degree $l$ for all subfields of $F[x]/f$.
(6) While $G$ has maximal subgroups which could contain $\mathrm{Gal}(f)$:
  (a) For each conjugacy class of maximal subgroups of $G$, compute a $G$-relative $H$-invariant polynomial for a representative maximal subgroup $H$ of the conjugacy class.
  (b) Compute a cost for deciding whether $\mathrm{Gal}(f)$ is contained in each conjugacy class. For a representative subgroup $H$, let the cost $c_H$ be the product of the number of cosets in $G//H$, the number of multiplications in the $G$-relative $H$-invariant chosen and a bound on the evaluation of the invariant at the roots $s\alpha_i$ of $f_s$ (Section 3.8).
  (c) Apply Theorem 4: For the conjugacy class of maximal subgroups of $G$ with smallest cost $c_H$ not yet decided on do
    (i) Let $H$ be a representative maximal subgroup from the conjugacy class.
    (ii) Retrieve the $G$-relative $H$-invariant polynomial $I \in R[x_1, \ldots x_n]$ computed in Step (6a) and any Tschirnhaus transformation $T$ selected in a previous iteration (Step 6c.v.B).
    (iii) Compute the precision $m$ needed in the roots of $f$ for transformation by $T$ then evaluation in $I$.
    (iv) Compute the roots of $f$ to precision $m$ in the splitting field $S_{f,P}$.
    (v) for the representatives $\tau \in G//H$ of the right cosets which contain the subgroup corresponding to the Frobenius automorphism $\sigma$, $G//_\sigma H = \{\tau : \sigma \in H^\tau\}$:
      (A) Evaluate $I$ at the transformed roots $s\alpha_i$ of $f_s$ permuted by $\tau$ where $\alpha_i$ has been computed in Step 6c.iv.
      (B) Decide whether this evaluation is the image of an element of $F$. If so then the resolvent has a root in $F$ and if it is a single root $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ so set $G = \tau H \tau^{-1}$ and restart the loop (6) with the new $G$. If the resolvent has a root in $F$ but it is not a single root then a descent into this conjugacy class may be re-attempted after applying another Tschirnhausen transformation. Choose a transformation randomly and update the cost $c_H$ for this transformation.
(7) Galois group of $f$ is $G$.

In what follows we give details about which primes will lead to the most efficient computation (Step 1, Section 3.1), the splitting field that will be used for the computation of the roots of the

polynomial and the mapping into that splitting field (Step 3, Section 3.2), a group to start the computations with (Step 5, Section 3.3), the invariants we can use (dependent on characteristic) (Step 6c.ii, Section 3.4), Tschirnhausen transformations (Step 6c.ii and 6c.v.B, Section 3.7), the computation of a bound and a precision necessary to use that bound to determine whether the evaluation of an invariant at the roots of $f$ to the precision calculated is in $F$ (Step 6b, 6c.iii and 6c.v.B, Section 3.8).

The scaled polynomial $f_s$ is monic and integral, that is $f_s \in R[x]$ where $R = \mathbb{Z}, \mathbb{F}_q[t], \mathbb{Q}[t]$ or a finite extension thereof, and the relationships between its roots are the same as between the roots of $f$. The roots of a monic, integral polynomial will be integral and so have finite expansions in the splitting field over a completion.

## 3. Details of the algorithm (especially for polynomials over a function field of characteristic $p$)

Here we describe the steps of Algorithm 1 considering especially its use for polynomials over a function field of characteristic $p$. Let $f$ be a polynomial of degree $n$ with coefficients in $F$. We give greater detail for $F = \mathbb{F}_q(t)$ or $F = \mathbb{F}_q(t)(\alpha)$ where $q = p^e$ for some $e$ and $\alpha$ is algebraic over $\mathbb{F}_q(t)$. (Any function field $\mathbb{F}_q(t)(\alpha)(\beta)$ is isomorphic to a function field of the form $\mathbb{F}_q(t)(\gamma)$ for some $\gamma$.) We will attempt to keep our description as general as possible and will note when the details we give are specific to $F$ being a global function field and if these details are specific to $F$ being a rational or algebraic function field.

### 3.1. Choosing a Good Prime (Algorithm 1, Step 1)

The prime $P \subset F$ which we use to compute a completion which we extend to a splitting field will affect the performance of our algorithm. In fact, by trying out several primes we can frequently collect enough cycle lengths to determine the Galois group itself, if the Galois group is $A_n$ or $S_n$, which it often is (Davenport and Smith, 2000).

We require that $P$ is finite, unramified in $F[x]/f$ and does not divide the leading coefficient or denominators of $f$. We compute the residue field $K$ of $P$ ($= \mathbb{F}_{q^r}$ when $F$ is a global function field) and factor $\bar{f}$, the image of $f$ over $K$, over $K$. We check $\bar{f}$ is squarefree over $K$ to ensure $P$ is unramified and we can Hensel lift distinct roots.

To choose $P$, we loop through a limited number of primes, keeping at most $5n$ useful primes when $F$ is a global function field. We collect the degrees of the factors of $\bar{f}$ over $K$ and the LCMs ($d_P$) of these degrees multiplied by the degree $r_P$ of $P$. The degrees are cycle lengths of elements in the Galois group (Geißler and Klüners, 2000, Remark 2.4). If there is a cycle of some prime length $n/2 < l < n-2$ then the Galois group is $S_n$ or $A_n$ (Seress, 2003, Corollary 10.2.2). If a group does not contain elements with these cycle lengths then it is not the Galois group of $f$. We can use this test to eliminate groups cheaply from our list of possibilities.

To obtain a ring over the completion $K[[\rho]]$ of $F$ at $P$ which contains all roots of $f$ over $K[[\rho]]$ when $F$ is a global function field we first compute the splitting field $E = \mathbb{F}_{(q^{r_P})^{d_P}}$ for $\bar{f}$ over $K$. We would like arithmetic in $E[[\rho]]$ to be not too expensive as we find roots in $E[[\rho]]$ and evaluate invariants at roots in $E[[\rho]]$. The precision necessary for the roots of $f$ is inversely related to the degree $r_P$ of the prime $P$. So a larger $r_P$ will allow us to work with roots with less precision but this may make $E$ itself large and expensive to work in. We attempt to take a middle ground to balance these factors.

We also make use of the Frobenius automorphism $\sigma$ of $E/\mathbb{F}_q$ so we attempt to compute $E$ large enough so that $\sigma$ is non-trivial. To do this we consider the number of cycles, that is, the number of factors of $f$, $l_{f,P}$, over the residue class field at $P$. Given a group $G$ which we know contains the Galois group and a maximal subgroup $H$ we would usually need to test $[G : H]$ many evaluations $I^\tau(\alpha_1, \ldots, \alpha_n)$ for some invariant $I$. Knowledge of a non-trivial $\sigma$ allows us to reduce this number to the number of $\tau \in G//_\sigma H = \{\tau : \sigma \in H^\tau\}$. This is the use of short coset systems as described in Geißler and Klüners (2000) Section 4 and Elsenhans (in press).

Therefore, when $F$ is a global function field we choose a prime $P$ with the smallest $r_P d_P l_{f,P}^{1.5} > n/4$, if such occurs as a prime we have considered, otherwise a prime we have considered with largest $r_P d_P l_{f,P}^{1.5} \leq n/4$.

### 3.2. Computing roots (Algorithm 1, Step 3 and 6c.iv6c.iv)

Let $F$ be a global function field. We construct $E = \mathbb{F}_{(q^{r_P})^{d_P}} = \mathbb{F}_{q^{r_P d_P}}$ where $\bar{f}$ splits into linear factors. Let $\rho$ be the image of $P$ in $E[[\rho]]$. We use the map $h : F \to E[[\rho]]$ given by the completion mapping at $P$ into $K[[\rho]]$ followed by the inclusion into $E[[\rho]]$. We can find the roots $\bar{\alpha}_i$ of $f$ in $E[[\rho]]$ using Puiseux expansions as in Duval (1989) which is implemented in Magma (Cannon et al., 2010) or by computing the roots of $\bar{f}$ in the finite field $E$ and using any root lifting technique. This shows that $f$ splits in $E[[\rho]]$.

#### 3.2.1. Mapping back to the Function Field (Algorithm 1 Step 6c.v.B)

In Section 3.8, we use the map $h_m^r : K[[\rho]]/\rho^m \to F/(P^m)$, given by the inverse of the completion mapping followed by rational reconstruction (or reduction when $F$ is a rational function field) modulo $P^m$. The map $h_m^r$ is applied to the evaluation of invariants at roots of $f_s$ in $E[[\rho]]$. If the result of an evaluation of an invariant at the roots of $f$ lies in $E[[\rho]] \backslash K[[\rho]]$ then the evaluation does not map back to $F$.

### 3.3. A starting group (Algorithm 1, Step 5)

If the discriminant of $f$ is a square in $F$ (and the characteristic $p \neq 2$) then the Galois group is contained in $A_n$ otherwise it is not (Stauduhar, 1973; van der Waerden, 1966, p. 155, Exercise 4). This is equivalent to the use of the SqrtDisc invariant (Theorem 8) but cheaper.

We looked at the SqrtDisc invariant (Theorem 5) in a similar way for the characteristic 2 case. The discriminant of a polynomial contains information about the roots of the polynomial but can be computed from the coefficients. In the characteristic 2 case we could not compute an element of $F$ related to the SqrtDisc invariant without computing the roots of the polynomial which is too expensive in general for a check which is supposed to be a shortcut.

However, it is possible that the computation of the subfields and the wreath products of their Galois groups with $S_{n/l}$ for a degree $l$ subfield may give us a starting group contained in $A_n$ if the Galois group is contained in $A_n$. So if $F[x]/f$ has subfields then the discriminant check may not provide any unique information. If the characteristic is 2 and $F[x]/f$ has no subfields then we do not currently have an easier way to determine whether we can descend from $S_n$ to $A_n$ than Algorithm 1 Step 6c.

Note that it is also possible to use the factorization of the 2-set or 2-sum resolvent of $f$, the monic polynomial whose roots are the products or sums of pairs of roots of $f$, to compute a smaller starting group (Casperson and McKay, 1994) but we do not have nor have we implemented algorithms to do this in characteristic $p$.

#### 3.3.1. Subfields (Algorithm 1, Step 5a, 5b)

Knowing the subfields of the extension $F[x]/f$ can speed our computation of the Galois group of $f$. In some cases knowing the subfields enables the Galois group to be computed in reasonable time where this would not be possible otherwise. It can avoid the need to check some expensive descents by reducing the starting group to a subgroup of large index in $S_n$.

For a subfield $L$ of degree $l$ of $F' = F[x]/f$ we have that $\mathrm{Gal}(f) \subseteq \mathrm{Gal}(g') \wr \mathrm{Gal}(g) \subseteq S_{n/l} \wr S_l$ where $g$ is the polynomial defining the subfield $L/F$ and $g'$ is a defining polynomial for $F'/L$. We have $|A \wr B| = |A|^l |B|$ when $B \subseteq S_l$ but computing $\mathrm{Gal}(g)$ is easier than computing $\mathrm{Gal}(g')$. We use the approximation for the second factor to gain a smaller starting group, that is, $\mathrm{Gal}(f) \subseteq S_{n/l} \wr \mathrm{Gal}(g)$, (this is the largest group having the block system of the subfield) and since this holds for all subfields $L$ of $F'$ we have that $\mathrm{Gal}(f) \subseteq \bigcap_L S_{n/l_L} \wr \mathrm{Gal}(g_L)$ where $l_L$ is the degree of the subfield $L$ and $g_L$ is a defining polynomial for $L$. This is explained at length in Geißler and Klüners (2000), Section 3.

A general subfields algorithm which also applies to global function fields has recently been developed by van Hoeij et al. (2011). This algorithm can also compute subfields of algebraic function fields represented as an extension of another algebraic function field. This occurs here when $F$ is an algebraic function field. So we are now able to compute and use subfields to improve the efficiency of computing Galois groups over global function fields.

In van Hoeij et al. (2011) subfields are computed by taking intersections of some generating subfields. They explain how to find a set of subfields such that all subfields of a function field $F' = F[x]/f$ can be computed as the intersection of these generating subfields. For our purposes we can use just the generating subfields in the Galois group computation, any other subfields will be subfields of (at least) two of the generating subfields so may be computed in any recursion. By factoring the polynomial $f$ over $F[x]/f$ we compute principal subfields over $F[x]/f$. Some of these subfields will be generating subfields but there will be no more of them than there are factors of $f$ over $F[x]/f$.

### 3.4. Invariants (Algorithm 1, Step 6c.ii)

Let $\mathrm{Gal}(f) \subseteq G \subseteq S_n$. For each maximal subgroup $H$ of $G$ we choose a $G$-relative $H$-invariant. There are a number of different types of invariants which have been used and which we continue to use. They fall into 3 categories: special, generic and combinations. Generic invariants will work for all groups $G$ and their maximal subgroups $H$. Special invariants can only be used when the groups $G$ and $H$ satisfy certain properties, however, they are the cheaper invariants and we should use them when we can. Combination invariants combine invariants for 2 other subgroups to obtain an invariant for a third, they are cheaper than generic invariants and some special invariants. In contrast to some previous algorithms we compute our invariants as we require them rather than looking them up in a table. This is what makes the algorithm of Fieker and Klüners (2014) degree independent.

We are guaranteed to be able to find an invariant. We know from Geißler and Klüners (2000) that

$$I(\underline{X}) = \sum_{\tau \in H} \left( \prod_{i=1}^{n-1} X_i^i \right)^{\tau}$$

is always a $G$-relative $H$-invariant (it is a generic invariant). It is not an efficient one although sometimes it is the best we can do. Geißler and Klüners (2000) also states that using an invariant of smallest total degree has major effects on the efficiency of the program, that multiplications are expensive and the number of them should be minimized and that we can gain during the lifting procedure by using an invariant whose resolvent has smaller absolute value roots. Fieker and Klüners (2014) and Elsenhans (2012) look for invariants which also have a small number of terms or operations. The larger the degree of the invariant the larger will be the bound in Step 6b and the larger will be the precision we then need to work with. So it is important that we choose our $G$-relative $H$-invariants carefully.

Now that we are working with polynomials in characteristic $p$ the invariants are in $\mathbb{F}_q[t][X_1, \ldots, X_n]$ and because of this some polynomials which are relative invariants in characteristic 0 are no longer relative invariants in some positive characteristics. Fortunately we have found this to be the case only in characteristic 2, as we prove in the theorems in Section 3.6, and in some cases we have found formulas for polynomials with similar invariant properties which we can use instead.

Below we give formulas for polynomials which are special $G$-relative $H$-invariants for certain pairs of groups $G$ and $H$. Most of these can be found in Geißler (2003), Geißler and Klüners (2000) or Fieker and Klüners (2014). However we will first look at formulas for polynomials which are $G$-relative $H$-invariants for some $H < G$ only in characteristic 2 (Theorems 5 and 6). Each of these will be analogous to a formula for a polynomial which is $G$-relative $H$-invariant for some $H < G$ in all other characteristics (Theorems 8 and 9). Theorem 7 contains formulas for invariants which are $G$-relative in all characteristics. We will also show that the more expensive but guaranteed to exist generic invariants remain $G$-relative in characteristic 2 (Theorem 10).

### 3.5. Invariants in characteristic 2

In this subsection we state polynomials and prove that they are relative invariants when the characteristic of $F$ is 2. These polynomials are derived from or inspired by similar polynomials which are known to be relative invariants when the characteristic of $F$ is 0 but are invariant for a larger group than required when the characteristic of $F$ is 2.

**Theorem 5.** *Let $H$ be a maximal subgroup of $G \subseteq S_n$. Then, when the characteristic of $F$ is 2, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are $G$-relative $H$-invariant polynomials when $G$ and $H$ satisfy the conditions given.*

**SqrtDisc** *When $H < A_n, G \not< A_n$*

$$I(\underline{X}) = \prod_{1 \le k < j \le n} (X_k + \bar{u} X_j) = I_1 + \bar{u} I_2 \quad \text{(Elsenhans, 2013a)}$$

*where $I_1$ and $I_2$ are also $G$-relative $H$-invariant and $\bar{u}$ is the image of $u$ in $\mathbb{F}_2[u]/\langle u^2 - 1\rangle$ and*

$$I(\underline{X}) = \sum_{1 \le k < j \le n} X_k \frac{\prod_{1 \le r < s \le n} (X_r + X_s)}{X_k + X_j} \quad \text{(Donnelly and Sutherland, 2012)}$$

*although the former is the most efficient.*

**D** *When $H$ has the same block systems as $G$, $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$ $H$ is a subgroup of $S_{n/l} \wr_\Gamma A_l$, $\Gamma = \{1, \ldots, l\}$,*

$$I(\underline{X}) = E(\underline{y}),$$

*where $E$ is either $I$, $I_1$ or $I_2$ from the (Elsenhans, 2013a) SqrtDisc invariant above and*

$$I(\underline{X}) = \sum_{1 \le k < j \le \#B} y_k \frac{\prod_{1 \le r < s \le \#B} (y_r + y_s)}{y_k + y_j}, \quad \text{using Donnelly and Sutherland (2012),}$$

*where $B = \{b_k\}_{1 \le k \le l}$ is a block system of both $G$ and $H$, $\#b_k = n/l$, $y_k = \sum_{i \in b_k} X_i$ and $\underline{y} = (y_1, \ldots, y_l)$.*

**$s_1 \equiv s_m$** *When $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$ there is a subgroup $H$ with the same block systems as $G$ such that*

$$I(\underline{X}) = \prod_{b \in B} E\big(\{X_j : j \in b\}\big) \qquad (s_m)$$

*is a $G$-relative $H$-invariant polynomial where $E$ is the SqrtDisc (Elsenhans, 2013a) invariant $I$ (not $I_1$ or $I_2$) and*

$$I(\underline{X}) = \sum_{b \in B} \Bigg( \sum_{k, j \in b, k < j} \frac{X_k}{X_k + X_j} \Bigg) \qquad (s_1)$$

*is a $G$-relative $H$-invariant function where $B = \{b_i\}_{1 \le i \le l}$ is a block system of both $G$ and $H$, $\#b_i = n/l$.*

Note that in parallel with Fieker and Klüners (2014) Theorem 5.7 the inner function of the $s_1 \equiv s_m$ invariant (the SqrtDisc function) could be replaced by any $U$-relative $N$-invariant polynomial $E$ satisfying $E^\sigma = \bar{u}E$ $(s_m)$ or $E^\sigma = E + 1$ $(s_1)$ for all $\sigma \in U \setminus N$ where $G = U \wr V$ and $N < U$ is normal of index 2, (the $I_1$ and $I_2$ invariants of the Elsenhans, 2013a, SqrtDisc invariant and the Donnelly and Sutherland, 2012, SqrtDisc invariant do not satisfy these properties). While $(s_1)$ is the $s_1$ polynomial summing over blocks in a system, in characteristic 2 it acts the same way as the $s_m$ polynomial does in other characteristics (which multiplies over blocks in a system). However such polynomials $E$ over $\mathbb{F}_q[t]$ have not been found and so this invariant is not used in the Magma (Cannon et al., 2010) implementation. The situation of $(s_m)$ is covered by the implementation of Factor Delta invariants by Elsenhans (2014). Using Theorem 6 we can then get an invariant similar to $\mathrm{Ds}_\mathrm{m}$ in Theorem 8.

**Proof. SqrtDisc (Elsenhans, 2013a)** Any permutation is a product of transpositions so we look here at the action of a single transposition. Let $\tau = (r, s) \in S_n$ be a transposition,

$$I^\tau(\underline{X}) = \prod_{1\le k<j\le n, k,j\notin\{r,s\}} (X_k + \bar{u}X_j) \prod_{1\le k<j\le n, k \text{ or } j\in\{r,s\}} (X_{k^\tau} + \bar{u}X_{j^\tau}).$$

The first product is invariant under $\tau$, we look at the second. Let $r < s$, then this second product is

$$\begin{aligned}
&(X_{r^\tau} + \bar{u}X_{s^\tau}) \prod_{r<j\le n, j\ne s} (X_{r^\tau} + \bar{u}X_{j^\tau}) \prod_{1\le k<s, k\ne r} (X_{k^\tau} + \bar{u}X_{s^\tau}) \\
&= (X_s + \bar{u}X_r) \prod_{r<j\le n, j\ne s} (X_s + \bar{u}X_j) \prod_{1\le k<s, k\ne r} (X_k + \bar{u}X_r) \\
&= \bar{u}(X_r + \bar{u}X_s) \prod_{r<j<s} (X_s + \bar{u}X_j) \prod_{s<j\le n} (X_s + \bar{u}X_j) \prod_{1\le k<r} (X_k + \bar{u}X_r) \prod_{r<k<s} (X_k + \bar{u}X_r) \\
&= \bar{u}(X_r + \bar{u}X_s) \prod_{r<j<s} \bar{u}(X_j + \bar{u}X_s) \prod_{s<j\le n} (X_s + \bar{u}X_j) \prod_{1\le k<r} (X_k + \bar{u}X_r) \prod_{r<k<s} \bar{u}(X_r + \bar{u}X_k)
\end{aligned}$$

The middle 2 products appear in $I(\underline{X})$, but not in the first product in $I^\tau$ above. The first and last products have the same number of factors (which all appear in $I$ and not in the first product of $I^\tau$ above) so the $\bar{u}$ here will cancel out, which means we are left with the one $\bar{u}$ out the front. So we have $I^\tau = \bar{u}I$. Therefore $I$ is not $\tau$-invariant. However, if a second transposition $\sigma$ was applied to $I$ we would have $I^{\tau\sigma} = \bar{u}I^\sigma = \bar{u}\bar{u}I = I$, therefore $I$ is $H$-invariant for any $H < A_n$ and $G$-relative for $G \not< A_n$.

To see that $I_1$ and $I_2$ are also $G$-relative $H$-invariant we start with $I^\tau = \bar{u}I$. Then

$$\begin{aligned}
(I_1 + \bar{u}I_2)^\tau &= \bar{u}(I_1 + \bar{u}I_2) \\
I_1^\tau + \bar{u}I_2^\tau &= \bar{u}I_1 + \bar{u}^2 I_2
\end{aligned}$$

Equating coefficients of $\bar{u}$ gives $I_1^\tau = I_2$ and $I_2^\tau = I_1$. Note that $I_1 \ne I_2$ otherwise $I$ is invariant under $\tau$ which we have proved above is not the case. Therefore neither $I_1$ nor $I_2$ are $\tau$ invariant but $I_1^{\tau\sigma} = I_2^\sigma = I_1$ therefore $I_1$ and similarly $I_2$ are $A_n$ invariant.

**SqrtDisc (Donnelly and Sutherland, 2012)** For the second SqrtDisc invariant we proceed in a similar fashion. We split the invariant into 2 parts, we write

$$I(\underline{X}) = \left( \sum_{1\le k<j\le n} \frac{X_k}{X_k + X_j} \right) \prod_{1\le r<s\le n} (X_r + X_s)$$

and note that the second factor is $S_n$-invariant. Let $I_1$ be the first factor and let $\tau = (r, s)$ be a transposition,

$$\begin{aligned}
I_1^\tau(\underline{X}) &= \sum_{1\le k<j\le n} \frac{X_{k^\tau}}{X_{k^\tau} + X_{j^\tau}} \\
&= \sum_{1\le k<j\le n, k,j\notin\{r,s\}} \frac{X_{k^\tau}}{X_{k^\tau} + X_{j^\tau}} + \sum_{1\le k<j\le n, k \text{ or } j\in\{r,s\}} \frac{X_{k^\tau}}{X_{k^\tau} + X_{j^\tau}}
\end{aligned}$$

and we note that the first sum is invariant under $\tau$. We continue with the second assuming $r < s$,

$$\begin{aligned}
&\sum_{1\le k<j\le n, k \text{ or } j\in\{r,s\}} \frac{X_{k^\tau}}{X_{k^\tau} + X_{j^\tau}} \\
&= \sum_{r<j\le n, j\ne s} \frac{X_{r^\tau}}{X_{r^\tau} + X_{j^\tau}} + \sum_{1\le k<s, k\ne r} \frac{X_{k^\tau}}{X_{k^\tau} + X_{s^\tau}} + \frac{X_s}{X_s + X_r}
\end{aligned}$$

$$= \sum_{r<j\le n,\, j\neq s} \frac{X_s}{X_s+X_j} + \sum_{1\le k<s, k\neq r} \frac{X_k}{X_k+X_r} + \frac{X_s}{X_s+X_r}$$
$$= \sum_{r<j<s} \frac{X_s}{X_s+X_j} + \sum_{s<j\le n} \frac{X_s}{X_s+X_j} + \sum_{1\le k<r} \frac{X_k}{X_k+X_r} + \sum_{r<k<s} \frac{X_k}{X_k+X_r} + \frac{X_s}{X_s+X_r}$$

The 2nd and 3rd sums appear in $I_1(\underline{X})$ but not in the first sum in $I_1^\tau$ above, the first and fourth sums have the same number of terms but none of their addends appear in $I_1$. However, $\frac{X_j}{X_k+X_j} = \frac{X_k}{X_k+X_j} + 1$ so the first sum becomes $\sum_{r<j<s}(\frac{X_j}{X_s+X_j} + 1)$ and similarly for the fourth sum. Because they have the same number of terms adding the first and the fourth sum now gives $\sum_{r<j<s} \frac{X_j}{X_j+X_s} + \sum_{r<k<s} \frac{X_r}{X_k+X_r}$ where the $+1$ cancel since there are an even number of them and the terms in this sum all appear in $I_1(\underline{X})$ and not in any part of $I^\tau(\underline{X})$ which we have already considered. This leaves us with the last term $\frac{X_s}{X_s+X_r} = \frac{X_r}{X_s+X_r} + 1$ so that $I_1^\tau = I_1 + 1$ and hence $I_1$ is not invariant under $\tau$ and so not $S_n$-invariant. But $I_1^{\tau\sigma} = (I_1+1)^\sigma = I_1 + 2 = I_1$ so $I_1$ and also $I$ are $H$-invariant for $H < A_n$ and $G$-relative for any $G \not< A_n$.

**D** We follow the hint in Fieker and Klüners (2014) following Theorem 5.7. We can use Fieker and Klüners (2014) Lemma 5.4, the $E$ invariant, where $E$ is the polynomial of the SqrtDisc invariant for $S_m$ and $A_m$ since the transitive permutation representations which permute the blocks are subgroups of $S_m$ and $A_m$.

**$s_1$** Since this invariant acts in the same way as the $s_m$ invariant in other characteristics we will refer to the proof of Theorem 5.7 of Fieker and Klüners (2014). Replacing $-d_i$ by $d_i + 1$, $\pm F$ by $F$ or $F+1$ and $F^{u_1} = -F$ by $F^{u_1} = F + 1$ in that proof we have that $I(\underline{X})$ is a $G$-relative $H$-invariant.

**$s_m$** Replacing $-d_i$ by $\bar{u}d_i$, $\pm F$ by $F$ or $\bar{u}F$ and $F^{u_1}$ by $\bar{u}F$ in the proof of Theorem 5.7 of Fieker and Klüners (2014) we have that $I(\underline{X})$ is a $G$-relative $H$-invariant. □

The SqrtDisc invariant is important when $\mathrm{Gal}(f)$ is primitive. This corresponds to the stem field $F[x]/f$ having no subfields (such as when the degree of $f$ is prime) which means that Algorithm 1 Step 5 cannot gain a smaller starting group. It also means there are no non-trivial block systems of any $G \supseteq \mathrm{Gal}(f)$ so none of the other special invariants can be used as they all use block systems. In characteristic 2 we cannot use whether the discriminant is a square to determine whether or not the Galois group of $f$ is a subgroup of $A_n$ which would mean that in characteristic 2 if there are no subfields and no non-trivial block systems then without a SqrtDisc invariant we could only use the more expensive generic invariants to descend all the way from $S_n$.

**Theorem 6** *(Fieker, 2009). Let $H_1, H_2 \subset G \subseteq S_n$ be two distinct subgroups of index 2 in $G$ with $G$-relative $H_i$-invariants $I_i$, $G//H_i = \{\mathrm{Id}, \tau_i\}$. Then, when the characteristic of $F$ is 2,*

$$I(\underline{X}) = \begin{cases} I_1 + I_2, & \text{if } I_i^{\tau_i} = I_i + 1 \\ I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1} & \text{otherwise} \end{cases}$$

*is a $G$-relative $H$-invariant where $H = \langle H_1 \cap H_2, \tau_1\tau_2 \rangle$.*

**Proof.** (Fieker, 2009.) The first formula follows easily from substitution into the second, however the proof for the second follows from a substitution into the first which is simpler to prove so we will prove only the first and note the necessary substitution.

Assume $I_i^{\tau_i} = I_i + 1$, then we have resolvent polynomials $R_i = x^2 + (I_i^{\tau_i} + I_i)x + I_i^{\tau_i} I_i = x^2 + x + I_i^2 + I_i$. These resolvent polynomials define quadratic Artin–Schreier extensions of the invariant ring $\mathbb{F}_q[t](\underline{X})^G$ (Fieker and Klüners, 2014, Remark 2.1). Since there are 2 such extensions there must be a third and by Artin–Schreier theory $x^2 + x + I_1^2 + I_1 + I_2^2 + I_2$ is a generating polynomial for the third quadratic subfield of the degree 4 extension generated by $R_i$ with Galois group $V_4 \cong C_2 \times C_2$. Its roots will be primitive elements in the extension and as such will be invariants. Therefore $I_1 + I_2$ (and $I_1 + I_2 + 1$) are $G$-relative $H$-invariants for some index 2 subgroup $H$. It can easily be seen that $I(\underline{X})$ is both

$H_1 \cap H_2$-invariant and invariant under $\tau_1\tau_2$ so $H \supset \langle H_1 \cap H_2, \tau_1\tau_2\rangle$. Since $\langle H_1 \cap H_2, \tau_1\tau_2\rangle$ has index 2 in $G$ we must have that $H = \langle H_1 \cap H_2, \tau_1\tau_2\rangle$.

To prove the second formula repeat the above argument with $\tilde{I}_i = I_i/(I_i + I_i^{\tau_i})$, since $\tilde{I}_i^{\tau_i} = \tilde{I}_i + 1$. Then we have that $x^2 + x + \frac{I_1 I_1^{\tau_1}}{(I_1+I_1^{\tau_1})^2} + \frac{I_2 I_2^{\tau_2}}{(I_2+I_2^{\tau_2})}$ is a generating polynomial for the third quadratic subfield of the degree 4 extension generated by the $R_i$ with Galois group $V_4$ and using the transformation $x \mapsto x/(I_1 + I_1^{\tau_1})(I_2 + I_2^{\tau_2})$ and clearing denominators we have that $x^2 + (I_1 + I_1^{\tau_1})(I_2 + I_2^{\tau_2})x + I_1 I_1^{\tau_1}(I_1 + I_1^{\tau_1})^2 + I_2 I_2^{\tau_2}(I_2 + I_2^{\tau_2})^2$ is also a generating polynomial for that subfield and it can be seen that $I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1}$ and $I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1} + 1$ are roots of that polynomial and hence are $G$-relative $H$-invariants. □

### 3.6. Invariants in characteristic other than 2

In this subsection we state polynomials and prove that they are relative invariants either when the characteristic of $F$ is $p > 0$ or $p > 2$. These polynomials are known to be relative invariants when the characteristic of $F$ is 0.

**Theorem 7.** *Let $H$ be a maximal subgroup of $G \subseteq S_n$. Then for all characteristics of $F$, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are $G$-relative $H$-invariant polynomials when $G$ and $H$ satisfy the conditions given.*

**Intransitive** *(Fieker and Klüners, 2014) **Lemma 5.1** When $H$ is an intransitive group and there is an orbit $\mathcal{O}$ of $H$ which is not invariant under $G$,*

$$I(\underline{X}) = \sum_{i\in\mathcal{O}} X_i.$$

**ProdSum** *(Geißler, 2003) **Algorithm 6.24 Step 3.1**, (Fieker and Klüners, 2014) **Lemma 5.3**, (Elsenhans, 2014) When there exists a block system $B$ of $H$ which is not a block system of $G$,*

$$I(\underline{X}) = \prod_{b\in B}\left(\sum_{i\in b} X_i\right) \quad \text{and} \quad I(\underline{X}) = \sum_{b\in B}\left(\sum_{i\in b} X_i\right)^e$$

*where $e = 2$ unless $p = 2$ then $e = 3$.*

**E** *(Geißler, 2003) **Satz 6.14, Algorithm 6.24 Step 4.1.2** When $H$ has the same block systems as $G$, $\overline{H} < \overline{G}$ are transitive permutation representations on $l$ points which permute the blocks in a block system, $B = \{B_1, \ldots, B_l\}$ is a block system for $G$ and $H$ and $E$ is a $\overline{G}$-relative $\overline{H}$-invariant,*

$$I(\underline{X}) = E(y_1, \ldots, y_l)$$

*where $y_j = \sum_{i\in B_j} X_i$.*

**F** *(Geißler, 2003) **Satz 6.16, Algorithm 6.24 Step 4.1.4** When $H$ has the same block systems as $G$, $\overline{H} = \overline{G}$, $\mathrm{Stab}_H(B_i)|_{B_i} < \mathrm{Stab}_G(B_i)|_{B_i}$ for $B_i = \{b_{i1}, \ldots, b_{il}\}$ a block in the block system $B = \{B_1, \ldots, B_k\}$ of $G$ and $H$, $\tilde{F}$ is a $\mathrm{Stab}_G(B_i)|_{B_i}$-relative $\mathrm{Stab}_H(B_i)|_{B_i}$-invariant, and $\tau$ is a system of representatives of left cosets of $\mathrm{Stab}_H(B_i)$,*

$$I(\underline{X}) = \sum_{\tau_j\in\tau} \tilde{F}^{\tau_j}(X_{b_{i1}}, \ldots, X_{b_{il}}).$$

**BlockQuotient** *(Geißler, 2003) **Algorithm 6.24, Step 6**, (Fieker and Klüners, 2014) **Lemma 5.6** When $H$ has the same block systems as $G$, $\overline{H} = \overline{G}$, $\mathrm{Stab}_H(B_i)|_{B_i} = \mathrm{Stab}_G(B_i)|_{B_i}$ for all blocks $B_i$ in the block system $B$ of $G$ and $H$, where $f$ is a $G|_{\underline{Y}}$-relative $H|_{\underline{Y}}$-invariant and $Y$ is a $K_2$-relative $K_1$-invariant polynomial for some groups $K_1 < K_2 < \mathrm{Stab}_G(B_i)|_{B_i}$ and $H|_{\underline{Y}} < G|_{\underline{Y}}$,*

$$I(\underline{X}) = f(\underline{Y}) \quad \text{where } \underline{Y} = \mathrm{Orb}_G(Y).$$

**Proof.** We mostly refer to existing proofs but note dependence on the characteristic.

**Intransitive** Let $h \in H$, $I^h(\underline{X}) = \sum_{i \in \mathrm{Orb}_H(1)} X_{i^h} = I(\underline{X})$ since $i^h \in \mathrm{Orb}_H(1)$ as the orbit is invariant under $H$. Let $g \in G \setminus H$, $I^g(\underline{X}) = \sum_{i \in \mathrm{Orb}_H(1)} X_{i^g}$. Since the orbit is not invariant under $G$, there exists $i$ such that $i^g \notin \mathrm{Orb}_H(1)$ therefore $I^g \neq I$. Therefore $I$ is a $G$-relative $H$-invariant polynomial independent of the characteristic.

**ProdSum** The first formula is proved to be a $G$-relative $H$-invariant independent of characteristic in Fieker and Klüners (2014) Lemma 5.3, so we will give a similar proof for the second formula which contains less multiplications and is characteristic dependent. Let $h \in H$, $I^h(\underline{X}) = \sum_{b \in B} (\sum_{i \in b} X_{i^h})^e$. Since $B$ is a block system $h \in H$ will only reorder either the outer sum or all of the inner sums which leaves $I$ invariant under $H$. However $g \in G \setminus H$ will map $X_i$ and $X_j$ with $i, j$ in different blocks to the same block so that $I^g$ contains a monomial $X_{i^g} X_{j^g}$ which is not present in $I$. Note that if in characteristic 2 we used $e = 2$ such monomials (with coefficient $e = 2$) would not be present for any $i, j$ and the invariant would be only a sum of squares which would also be $G$-invariant and so not $G$-relative.

**E** A proof that this $I(\underline{X})$ is a $G$-relative $H$-invariant is given in both Geißler (2003) Satz 6.14 and Fieker and Klüners (2014) Lemma 5.4. Note that addition of indeterminates is independent of characteristic and that $E$ is an invariant in the characteristic of $F$.

**F** A proof that this $I(\underline{X})$ is a $G$-relative $H$-invariant is given in both Geißler (2003) Satz 6.16 and Fieker and Klüners (2014) Lemma 5.5. Note that addition of indeterminates is independent of characteristic and that $\tilde{F}$ is an invariant in the characteristic of $F$.

**BlockQuotient** This invariant $I(\underline{X})$ is discussed in Geißler (2003) Bemerkung 6.19 and in Fieker and Klüners (2014) Lemma 5.6. Note that $f$ and $Y$ will be chosen dependent on the characteristic and that evaluation is independent of characteristic. □

**Theorem 8.** *When the characteristic of $F$ is not 2, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are $G$-relative $H$-invariant polynomials for some maximal subgroup $H$ when $G$ satisfies the conditions given.*

**SqrtDisc** ***(Geißler, 2003) Algorithm 6.24 Step 1*** *When $G \not\leq A_n$, $H < A_n$*

$$I(\underline{X}) = \prod_{1 \leq k < j \leq n} (X_k - X_j)$$

*[Note that if we checked whether the discriminant was a square then this invariant gives no additional information used on its own since if $G \not\leq A_n$ no even permutation group will be the Galois group and we can make that decision purely on the parity of the groups.]*

**D** ***(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.2*** *When $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, $H$ is a subgroup of $S_{n/l} \wr_\Gamma A_l$ having the same block systems as $G$, $B$ is a block system of both $G$ and $H$, $|B| = l$, $\#b_k = n/l$, $b_k \in B$,*

$$I(\underline{X}) = \prod_{1 \leq k < j \leq \#B} (y_k - y_j)$$

*where $y_k = \sum_{i \in b_k} X_i$.*

**$\mathbf{s_m}$** ***(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.4*** *When $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, there is a subgroup $H$ of index 2 with the same block systems as $G$ such that*

$$I(\underline{X}) = \prod_{b \in B} \prod_{k, j \in b, k < j} (X_j - X_k)$$

*is a $G$-relative $H$-invariant polynomial, for all block systems $B$ of both $G$ and $H$, $|B| = l$, $\#b_k = n/l$, $b_k \in B$,*

**$\mathbf{Ds_m}$** ***(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.6*** *When $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, there is a subgroup $H$ of index 2 with the same block systems as $G$ such that*

$$I(\underline{X}) = D(\underline{X}) \times s_m(\underline{X})$$

*is a $G$-relative $H$-invariant polynomial.*

**$s_1$** *(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.3 When $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, $H$ is a subgroup of $A_{n/l} \wr_\Gamma S_l$ with the same block systems as $G$,*

$$I(\underline{X}) = \sum_{b \in B} \prod_{k,j \in b, k<j} (X_k - X_j)$$

*where $B$ is a block system of both $G$ and $H$, $|B| = l$, $\#b = n/l$, $b \in B$.*

**$s_2$** *(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.5 When $G$ is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, there is a subgroup $H$ of index $2^{l-1}$ with the same block systems as $G$ such that*

$$I(\underline{X}) = \sum_{b_{i_1}, b_{i_2} \in B, i_1 \neq i_2} d_{i_1} d_{i_2}$$

*is a $G$-relative $H$-invariant polynomial where $B$ is a block system of $G$ and $H$, $|B| = l$, $\#b = n/l$, $b \in B$, where $d_i = \prod_{k,j \in b_i, k<j} (X_k - X_j)$.*

**Proof.** We refer to existing proofs where possible.

**SqrtDisc**, **(Geißler, 2003) Algorithm 6.24 Step 1** Note that the proof that this $I$ is $G$-relative $H$-invariant follows from substituting $\bar{u} = -1$ in the SqrtDisc proof of Theorem 5. Note that this $I$ is invariant in characteristic 2 also.

**D**, **(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.2** Since this invariant has been considered elsewhere (Geißler, 2003; Geißler and Klüners, 2000 Lemma 2.13 and Fieker and Klüners, 2014 following Theorem 5.7) we will not prove this is an invariant. Note that this is not a $G$-relative $H$-invariant in characteristic 2, since it relies on multiplications of $-1$.

**$s_m$**, **(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.4** See Fieker and Klüners (2014) Theorem 5.7. Note that this is not a $G$-relative $H$-invariant in characteristic 2, since it relies on multiplications of $-1$.

**$Ds_m$**, **(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.6** See Geißler and Klüners (2000) Lemma 2.13 and Fieker and Klüners (2014) following Theorem 5.7. Note that this is not a $G$-relative $H$-invariant in characteristic 2, since it relies on multiplications of $-1$.

**$s_1$**, **(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.3** Note that this equivalent to the F invariant of Theorem 7 where the inner invariant $F$ is the SqrtDisc invariant.

**$s_2$**, **(Geißler, 2003) Satz 6.8, Algorithm 6.24 Step 3.2.5** Since (Geißler, 2003) and (Eichenlaub, 1996) both state this invariant we will not prove that it is an invariant. Note that this is not a $G$-relative $H$-invariant in characteristic 2 since it relies on multiplications of $-1$. □

Note the order in Geißler (2003) Algorithm 6.24. The SqrtDisc, ProdSum, D, $s_1, s_m, s_2$ and $Ds_m$ invariants appear first in the algorithm as these are the cheaper invariants to apply (although we may use techniques from later steps to calculate them). Although in characteristic 2 we cannot use most of them, the ones we can use are listed first in Geißler (2003) Algorithm 6.24, (Steps 1 (SqrtDisc), 3.1 (ProdSum) and 3.2.2 (D)). Note also that Geißler (2003) Algorithm 6.24 can be recursive so that some invariants are computed from the invariants of related groups. This occurs in Steps 4, 5 and 6.

We now state a theorem for combining invariants similar to Theorem 6.

**Theorem 9.** *(See Geißler, 2003 Satz 6.21, Algorithm 6.24 Step 5; Fieker and Klüners, 2014 Lemma 5.8.) Let $H_1, H_2 \subset G \subseteq S_n$ be two distinct subgroups of index 2 in $G$ with $G$-relative $H_i$-invariants $I_i$ and $G//H_i = \{\mathrm{Id}, \tau_i\}$. Then*

$$I(\underline{X}) = I_1 I_2, \quad \text{if } I_i^{\tau_i} = \pm I_i$$
$$I(\underline{X}) = \left(I_1 - I_1^{\tau_1}\right)\left(I_2 - I_2^{\tau_2}\right) \quad \text{otherwise}$$

*is a $G$-relative $H$-invariant where $H = (H_1 \cap H_2) \cup ((G \setminus H_1) \cap (G \setminus H_2))$ when the characteristic of $F$ is not 2.*

**Proof.** That these $I(\underline{X})$ are $G$-relative $H$-invariants is proven in Fieker and Klüners (2014) Lemma 5.8. We note that negation is equivalent to the identity and subtraction is equivalent to addition in characteristic 2 hence there cannot be $G$-relative $H_i$-invariants $I_1, I_2$ such that $I_i^{\tau_i} = -I_i = I_i$ since any such polynomial is $G$-invariant and $I_i - I_i^{\tau_i} = I_i + I_i^{\tau_i}$ is $G$-invariant also. □

Further combinations of invariants are possible, see Fieker and Klüners (2014) following Lemma 5.8.

**Theorem 10.** *The generic invariants*

$$I(\underline{X}) = \sum_{h \in H // \operatorname{Stab}_H b^\sigma} b^{\sigma h} = \sum_{m \in \operatorname{Orb}_H(b^\sigma)} m,$$

*where $b$ is a monomial and $\sigma \in S_n$ is such that $|\operatorname{Orb}_G(b^\sigma)| > |\operatorname{Orb}_H(b^\sigma)|$ or equivalently $(G : \operatorname{Stab}_G b^\sigma) \neq (H : \operatorname{Stab}_H b^\sigma)$, and*

$$I(\underline{X}) = \sum_{\tau \in H} \left( \prod_{i=1}^{n-1} X_i^i \right)^\tau,$$

*are $G$-relative $H$-invariants for all groups $G$ and maximal subgroups $H$ independent of characteristic.*

See Fieker and Klüners (2014) Section 4 for a discussion on computing efficient monomials, also Geißler (2003), Geißler and Klüners (2000).

**Proof.** In the first formula, for $h \in H$, $I^h(\underline{X}) = \sum_{m \in \operatorname{Orb}_H(b^\sigma)} m^h$, and since $h \in H, m^h \in \operatorname{Orb}_H(b^\sigma)$, $I^h = I$. However, for $g \in G \setminus H$, $I^g(\underline{X}) = \sum_{m \in \operatorname{Orb}_H(b^\sigma)} m^g$, but since $g \notin H$, $|\operatorname{Orb}_G(b^\sigma)| > |\operatorname{Orb}_H(b^\sigma)|, m^g \notin \operatorname{Orb}_H(b^\sigma)$, $I^g \neq I$. This proof is independent of characteristic.

In the last formula, for $h \in H$, $I^h(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^{h\tau}$, but since $h\tau \in H$, $I^h = I$. However, for $g \in G \setminus H$, $I^g(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^{g\tau} = I(\underline{X}) \Longrightarrow (\prod_{i=1}^{n-1} X_i^i)^{g\tau} = (\prod_{i=1}^{n-1} X_i^i)^h$ for some $h \in H \Longrightarrow g\tau = h \Longrightarrow g \in H$ – a contradiction, therefore $I^g \neq I$. This proof is independent of characteristic. □

Note that in characteristic $p$ $\sum_{h \in H} b^{\sigma h}$ is not necessarily $G$-relative (but it is in characteristic 0) as we may get cancellations which make the polynomial invariant outside of $H$.

### 3.7. Tschirnhausen transformations (Algorithm 1, Step 6c.ii)

To use Theorem 4 the resolvent polynomial needs to have a root in $F$ which is a single root. We can make this happen by applying a suitable Tschirnhaus transformation to the invariant we are using. A Tschirnhaus transformation is a polynomial which gives a change of variable (Tignol, 2001, Section 6.4). We use Tschirnhaus transformations on all of the variables in an invariant. When $F$ has characteristic $p$ Tschirnhaus transformations are in $R = \mathbb{F}_q[t]$. We cannot use $R = \mathbb{F}_q$ because there may not be enough polynomials over $\mathbb{F}_q$ to ensure that the application of one of them will make a root of the resolvent in $F$ be a single root. These transformations then need to be mapped to the chosen $E[[\rho]]$ using the map $h$ in Section 3.2 for evaluation at the roots of $f$ in $E[[\rho]]$ as do the invariants themselves.

### 3.8. Determining a descent (Algorithm 1, Steps 6b and 6c.v.B)

We have a group $G$ such that $\operatorname{Gal}(f) \subseteq G$ and a maximal subgroup $H$ of $G$ for which we are testing whether $\operatorname{Gal}(f) \subseteq H$. We have chosen a $G$-relative $H$-invariant polynomial $I$ and a Tschirnhausen transformation $T$ if found to be necessary to gain a single root of the resolvent $Q_{(G,H)}(y)$ in $F$ (Step 6c.ii). Now we need to decide whether $I^\tau(T(\alpha_1), \ldots, T(\alpha_n)) \in F$ for some $\tau \in G//H$, then it may follow from Theorem 4 whether $\operatorname{Gal}(f) \subseteq H$. If $I^\tau(T(\alpha_1), \ldots, T(\alpha_n)) \in F$ is not a single root then we need to apply a different Tschirnhausen transformation and try again.

We can evaluate $I^\tau(T(s\bar{\alpha}_1),\dots,T(s\bar{\alpha}_n))$ in $E[[\rho]]$ to some precision $m$ which we have chosen and we can map this evaluation back to $F/P^m$ using $h_{r,m}$. Here it is important that we use the scaled roots of $f$ which are integral. Integral elements of $F$ will have finite expansions in $E[[\rho]]$. We can bound the image of the evaluation and we use this bound to compute a precision such that all non-zero $P$-adic digits of $I^\tau(T(s\alpha_1),\dots,T(s\alpha_n))$ can be computed. When $F$ is a global function field we use a bound on the degree (if $F$ is rational) or, more generally, the infinite valuations of the image. This will either prove that $\mathrm{Gal}(f)\subseteq H$ (if $-v_\infty(h_{r,m}(I^\tau(T(s\bar{\alpha}_1),\dots,T(s\bar{\alpha}_n))))\le\tilde{B}$ for all infinite valuations $v_\infty$ of $F$ and some bound $\tilde{B}$), suggest that this is probably true (if the previous inequality holds but we use less precision than we should) or prove that it is not true (if the inequality doesn't hold).

To compute such a bound $\tilde{B}$ we use the minimum infinite valuation of the roots of $f_s$. When $F$ is a rational function field, the infinite valuation is the negative of the degree of a root. We compute these valuations using the Newton polygons of the polynomial $f_s$ over $F$ at all infinite places of $F$ and call the smallest one $v_0$.

Let

$$I^\tau\big(T(s\alpha_1),\dots,T(s\alpha_n)\big)=\sum_j c_j\prod_i T(s\alpha_i)^{d_{ij}}$$

(in which form any invariant can be written), remembering that the invariants may have coefficients $c_j$ in $F_q[t]$ and not only in $\mathbb{Z}$ as in the case when the characteristic is 0. Then

$$v_\infty\big(I^\tau\big(T(s\alpha_1),\dots,T(s\alpha_n)\big)\big)\ge\min_j\left\{v_\infty(c_j)+\sum_i v_\infty\big(T(s\alpha_i)\big)d_{ij}\right\}$$

but since $v_\infty(s\alpha_i)\ge v_0$ for all $i$ and $v_\infty(T(s\alpha_i))\ge\min_k\{v_\infty(T_k)+kv_\infty(s\alpha_i)\}$, where $T_k$ are the non-zero coefficients of $T$, we have

$$v_\infty\big(I^\tau\big(T(s\alpha_1),\dots,T(s\alpha_n)\big)\big)\ge\min_j\left\{v_\infty(c_j)+\min_k\big\{v_\infty(T_k)+kv_0\big\}\sum_i d_{ij}\right\}.$$

But $v_0\le 0$ (since $f_s$ is over $\mathbb{F}_q[t]$ or some extension thereof) and $v_\infty(T_k)\le 0$ so $(v_\infty(T_k)+kv_0)\sum_i d_{ij}\le 0$ for all $k,j$ so we use $d=\max_j\{\sum_i d_{ij}\}$ to minimize $\min_j\{v_\infty(c_j)+\min_k\{v_\infty(T_k)+kv_0\}\sum_i d_{ij}\}$. Therefore

$$v_\infty\big(I^\tau\big(T(s\alpha_1),\dots,T(s\alpha_n)\big)\big)\ge\min_j\big\{v_\infty(c_j)\big\}+\min_k\big\{v_\infty(T_k)+kv_0\big\}d$$

since $v_\infty(c_j)\le 0$ and when $F$ is a rational function field $\deg(I^\tau(T(s\alpha_1),\dots,T(s\alpha_n)))=-v_\infty(I^\tau(T(s\alpha_1),\dots,T(s\alpha_n)))\le\max_j\{-v_\infty(c_j)\}+\max_k\{-v_\infty(T_k)-kv_0\}d$.

When $F$ is a global algebraic function field there is possibly more than one infinite place. The minimum infinite valuation $v_0$ is taken as the minimum over all infinite places. We have the bound $-v_\infty(I^\tau(T(s\alpha_1),\dots,T(s\alpha_n)))\le\max_j\{-v_\infty(c_j)\}+\max_k\{-v_\infty(T_k)-kv_0\}d$ where this holds for all infinite valuations $v_\infty$.

In practice the $d=\deg(I)$ we use in this multiplication may be larger than $\max_j\{\sum_i d_{ij}\}$ because we compute the degree of an unreduced invariant, so this will cost us in using more precision than necessary but will not decrease the accuracy of the result.

*3.8.1. Precision (Algorithm 1, Step 6c.iii)*

Let $\beta=I(T(s\alpha_1),\dots,T(s\alpha_n))$ whose infinite valuations are bounded below by $-B$ where

$$B=\deg(I)\max_{0\le k\le\deg(T)}\left\{-v_0k-\max_{v_\infty}\big\{v_\infty(T_j)\big\}\right\}+\max_{j,v_\infty}\big\{-v_\infty(c_j)\big\}$$

where $T_k$ are the coefficients of $T$, $c_j$ are the coefficients of $I$ and let $\beta\in\beta_0+P^m$ for some precision $m$, that is, $\beta_0$ is an approximation to $\beta$. We need to compute $m$ which ensures that $\beta-\beta_0=0$, that is, $\beta$ is a finite expansion and so an element of $F$. For all infinite valuations $v_\infty$ we have

$-v_\infty(\beta) \le B$, $-v_\infty(\beta_0) \le B$ and $-v_\infty(\beta^{(i)}) \le B$ for all conjugates $\beta^{(i)}$ of $\beta$, so $-v_\infty(\beta-\beta_0) \le B$ and $-v_\infty((\beta-\beta_0)^{(i)}) \le B$. Therefore

$$\begin{aligned} -v_\infty\big(\operatorname{norm}(\beta-\beta_0)\big) &= -v_\infty\left(\prod_i (\beta-\beta_0)^{(i)}\right) \\ &= \sum_i -v_\infty\big((\beta-\beta_0)^{(i)}\big) \\ &\le \sum_i B \\ &\le [G:H]B \end{aligned}$$

where the number of conjugates is the degree of the smallest subfield of the splitting field which $\beta$ lies in which is less than $[G:H]$. Since $\beta-\beta_0 \in P^m$, $\operatorname{norm}(\beta-\beta_0) \in P^m$. We have $\deg((\beta-\beta_0)_0) = \deg((\beta-\beta_0)_\infty)$ where $(\beta-\beta_0)_0$ and $(\beta-\beta_0)_\infty$ are the zero divisor and the pole divisor of $\beta-\beta_0$ respectively so

$$\sum_{Q\in\mathbb{P}_F^0} v_Q(\beta-\beta_0)\deg(Q) = \sum_{Q\in\mathbb{P}_F^\infty} -v_Q(\beta-\beta_0)\deg(Q),$$

where $\mathbb{P}_F^0$ and $\mathbb{P}_F^\infty$ are the places of $F$ which lie above a polynomial in $k[t]$ and those that don't, and

$$\begin{aligned} m\deg(P) \le v_P(\beta-\beta_0)\deg(P) &\le \sum_{Q\in\mathbb{P}_F^\infty} -v_Q(\beta-\beta_0)\deg(Q) \\ &\le \sum_{Q\in\mathbb{P}_F^\infty} -v_Q\big(\operatorname{norm}(\beta-\beta_0)\big)\deg(Q) \\ &\le \#\mathbb{P}_F^\infty \max_{Q\in\mathbb{P}_F^\infty}\big\{-v_Q\big(\operatorname{norm}(\beta-\beta_0)\big)\big\} \max_{Q\in\mathbb{P}_F^\infty}\big\{\deg(Q)\big\} \\ &\le \#\mathbb{P}_F^\infty [G:H]B \max_{Q\in\mathbb{P}_F^\infty}\big\{\deg(Q)\big\} \end{aligned}$$

so we must choose $m$ such that $m > \max_{Q\in\mathbb{P}_F^\infty}\{\deg(Q)\}\#\mathbb{P}_F^\infty[G:H]B/\deg(P)$ so that $\beta-\beta_0=0$. If $F$ is a rational function field the above can be expressed more simply as

$$m\deg(P) = \deg\big(\operatorname{norm}\big(P^m\big)\big) \le \deg\big(\operatorname{norm}(\beta-\beta_0)\big) = -v_\infty\big(\operatorname{norm}(\beta-\beta_0)\big) \le [G:H]B$$

so $m > [G:H]B/\deg(P)$ is enough precision to ensure that $\beta-\beta_0=0$.

But this means that $m \sim [G:H]$ which can be quite large. Such a precision $m$ will prove whether or not $\operatorname{Gal}(f) \subseteq H$ but we only want to use this proven precision if it is not too large, otherwise we can prove this descent step later (if necessary) using absolute resolvents as done in Geißler and Klüners (2000) Algorithm 5.1. If $[G:H]$ is large we instead use $lB$ where $l$ is some limit we place on the index $[G:H]$. Since it is very possible that $\operatorname{Gal}(f) \not\subseteq H$, the limit $l$ will give us a smaller precision which may allow us to determine that $\operatorname{Gal}(f) \not\subseteq H$. We use a precision of $\lceil l \max_{Q\in P_F^\infty}\{\deg(Q)\}\#\mathbb{P}_F^\infty B/\deg(P)\rceil + \epsilon$ to allow us to check that the few digits above where we expect the series expansion of an exact root to finish are zero.

## 4. An algorithm for reducible polynomials

Since Galois groups describe relationships between the roots of a polynomial we can also compute Galois groups of reducible polynomials in a similar way to those of irreducible polynomials. Magma Cannon et al. (2010) has contained an implementation of an algorithm for Galois groups of reducible polynomials over $\mathbb{Q}$ since V2.13. This has since been extended to accept input of reducible polynomials over number fields (V2.17) and reducible polynomials over global rational and algebraic function fields (V2.18).

The algorithm we give for Galois groups of reducible polynomials extends Algorithm 1 as we factorize the input polynomial into its factors so we can use the product of the Galois groups of the factors as a group in which we know the Galois group of the product is contained. We need to make sure the prime chosen is good for all factors of the input polynomial and that we compute a ring which contains all roots of all factors of the input.

**Algorithm 2** *(Galois group of a reducible polynomial $f$).* We take as input a polynomial $f$ over a number field $F$ (including $\mathbb{Q}$) or global function field $F$ (rational or algebraic), whose factors are separable.

(1) Factorize $f$ over $F$ as $\prod_i f_i^{e_i}$ and compute the squarefree product $\tilde{f}$ of the non-linear factors (without multiplicities).
(2) Choose a prime $P$ such that the image of $\tilde{f}$ is also squarefree over the residue field at $P$.
(3) Compute the Galois group $G_1$ of $f_1$.
(4) Compute the splitting field $S_{f,P}$ for $f$ over the completion of $F$ at $P$ as an extension of $S_{f_1,P}$ where $S_{f_1,P}$ is the splitting field for $f_1$ over the completion of $F$ at $P$ used in the computation of $G_1$.
(5) Compute the Galois groups $G_i$ of the remaining (non-linear) $f_i$ using roots of $f$ in the splitting field $S_{f,P}$. The Galois group $G_i$ will be $S_1$ when $f_i$ is linear.
(6) Divide the factors $f_i$ into 2 groups – one containing those factors for which we can easily prove the splitting field $S_{f_i}$ intersects with the splitting field of the product of the other factors in $F$ only and one containing the other factors. Compute the direct product $G = \bigoplus G_i$ for the factors $f_i$ in this second group.
(7) Apply Algorithm 1 Step 5 to compute the Galois group $G'$ of the product of the factors in the second group by descent from $G$.
(8) Compute the direct product $\bigoplus G_i \oplus G'$ for the groups $G_i$ corresponding to factors $f_i$ in the first group in Step 6 and map this to a subgroup of the direct product of all $G_i$ which is the Galois group of $\tilde{f}$, $G_{\tilde{f}}$.
(9) Handle multiple and linear factors by computing the image of $G_{\tilde{f}}$ under the embedding

$$G_{\tilde{f}} \to G_{\tilde{f}} \bigoplus_{f_i \text{ not linear}} G_i^{e_i-1} \bigoplus_{f_i \text{ linear}} S_1^{e_i} \tag{1}$$

which maps a generator of $G_{\tilde{f}}$ to the product of its projections onto each addend, to gain $\mathrm{Gal}(f)$.

### 4.1. Details of the algorithm

Here we detail the steps of Algorithm 2 for Galois groups of reducible polynomials, considering especially its implementation for polynomials over a function field of characteristic $p$. We will attempt to describe the details as generally as possible and will note when the details we give are specific to $F$ being a global function field.

#### 4.1.1. Choosing a Good Prime (Algorithm 2, Step 2)

Most of Section 3.1 holds when $f$ is a reducible polynomial. However we cannot determine whether the Galois group is $S_n$ or $A_n$ by looking at the cycle lengths. In fact the Galois group of a reducible polynomial will not be $S_n$ or $A_n$ as the Galois group is not transitive because the polynomial is not irreducible (Davenport and Smith, 2000). We choose our prime with the smallest $r_P d_P l_{f,P}^{1.5} > n_i/4$ for all $n_i$, where $n_i$ is the degree of $f_i$ and $l_{f,P}$ is the number of factors of $f$ mod $P$, if such a prime occurs in those we have considered otherwise a prime we considered with largest $r_P d_P l_{f,P}^{1.5}$. This makes the prime as good as possible for the computation of the Galois groups of each $f_i$.

#### 4.1.2. Computing roots in the splitting field over the completion (Algorithm 2, Step 4)

We compute the splitting field $S_{f_1,P}$ of $f_1$ over the completion of $F$ at $P$ using Section 3.2. We then extend this splitting field to include the roots of the other $f_i$. There is a map $h_1 : F \to S_{f_1,P}$

as described in Section 3.2 which we use to map $\tilde{f}$ from a polynomial over $F$ to a polynomial over $S_{f_1,P}$. The splitting field $S_{f,P}$ for $f$ is then computed by factoring $f$ over $S_{f_1,P}$ and extending the field until it includes all the roots of $f$. The map $h : F \to S_{f,P}$ is then given as a composition $h : F \to S_{f_1,P} \hookrightarrow S_{f,P}$, $h = \iota \circ h_1$ where $\iota$ is the inclusion map $\iota : S_{f_1,P} \hookrightarrow S_{f,P}$.

*4.1.3. Check disjointness of splitting fields (Algorithm 2, Steps 6 and 8)*

If the splitting fields $S_{f_i}$ of the factors $f_i$ overlap with the splitting fields

$$\bar{S}_{f_i} = S_{\prod_{j \neq i} f_j}$$

of the products of the other factors only in $F$ then the Galois group of the product will be the direct product of the Galois groups of the factors. We therefore attempt to divide our factors into 2 groups – those for which we can easily prove $S_{f_i}$ does not overlap with $\bar{S}_{f_i}$ and those for which we cannot easily prove this.

Since the orders of the Galois groups are the degrees of the splitting fields we first check whether the orders of the Galois groups $G_i$ of the $f_i$ are pairwise coprime. For those $G_i$ whose order is coprime to that of all others, the degrees of the splitting fields $S_{f_i}$ are pairwise coprime, hence the degrees of $S_{f_i}$ and $\bar{S}_{f_i}$ are coprime so there can be no overlap between the splitting fields $S_{f_i}$ and $\bar{S}_{f_i}$ outside of $F$ and so the Galois group of the product of the corresponding $f_i$ is the direct product of those $G_i$. For those factors $f_i$ whose Galois group orders are not pairwise coprime we continue this check. Note that we can only use the remainder of this check when we know something about the ramification of extensions of $F$. This occurs when $F$ is $\mathbb{Q}$ or a rational function field.

If $F$ is $\mathbb{Q}$ we check whether the discriminants of the remaining $f_i$ are pairwise coprime. If they are then the splitting fields $S_{f_i}$ must overlap with the $\bar{S}_{f_i}$ in an unramified extension, of which $\mathbb{Q}$ has none non-trivial. Therefore the Galois group of the product of those $f_i$ with coprime discriminants is the direct product of their Galois groups $G_i$ (rather than a subgroup of).

If $F$ is a rational function field then any constant field extension will be unramified (Stichtenoth, 1993, Theorem III.6.3) and any separable extension which does not extend the constant field will be ramified (Stichtenoth, 1993, Corollary III.5.8). To obtain information from the discriminants as when $F = \mathbb{Q}$ we also ensure that the intersection of $S_{f_i}$ and $\bar{S}_{f_i}$ does not contain a constant field extension, that is, is ramified. We can easily check whether the stem fields $F[y]/f_i$ contain a constant field extension. Let the degree of the constant field extension in $S_{f_i}$ be $c_i$. The constant field extension contained in $\bar{S}_{f_i}$ has degree $\bar{c}_i = \mathrm{lcm}(\{c_j\}_{j \neq i})$. These two constant field extensions meet only in the coefficient ring of $F$ if $\gcd(c_i, \bar{c}_i) = 1$ which is the same as checking whether the $c_i$ are pairwise coprime.

We first check for pairwise coprime discriminants. For those factors $f_i$ whose Galois groups $G_i$ have order not coprime to some other group we collect those whose discriminants are pairwise coprime to those of all other factors we are still checking (the factors which have non-coprime discriminants we cannot prove non-overlap easily). For these factors we check whether it is possible for there to be an unramified extension in the splitting field. We first check whether the dimensions of the exact constant fields of the $F[x]/f_i$ are pairwise coprime. For those factors for which this holds we compute normal subgroups of the $G_i$ and for those subgroups whose quotient is cyclic, we compute the fixed fields of these subgroups and check whether the LCMs of the dimensions of the exact constant fields of these fixed fields are pairwise coprime, these fixed fields contain the possible constant field extensions. If we determine that the intersection of splitting fields $S_{f_i}$ and $\bar{S}_{f_i}$ does not extend the constant field of $F$ (that is, the intersection is a ramified extension of $F$) and that the discriminant of $f_i$ is pairwise coprime to those of other factors still being considered (the intersection is unramified) then the intersection must be a trivial extension of $F$, that is $F$ itself.

Now we have divided our factors into 2 groups. We take the direct product of the $G_i$ corresponding to the factors whose splitting fields $S_{f_i}$ *may* intersect in a non-trivial extension of $F$ with $\bar{S}_{f_i}$ and we compute a descent (Step 7) from this direct product only. We take the direct product of the result of this descent with the direct product of those $G_i$ corresponding to the factors for which we could prove the splitting fields $S_{f_i}$ overlap with $\bar{S}_{f_i}$ in $F$ only as the Galois group of the polynomial $\tilde{f}$.

*4.1.4. Invariants (Algorithm 2, Step 7)*

There is an invariant stated in Theorem 7 which may be able to be used when $H < G$ are intransitive groups (independent of characteristic), however we do not satisfy the additional conditions to use this invariant directly during this descent. When all the orbits of $H$ are invariant under $G$ we compute the actions of $G$ and $H$ on the orbits of $G$. If this action is not the same for some orbit we compute an invariant for these actions (dependent on characteristic) and evaluate this at the appropriate $X_i$ (Elsenhans, 2014). Otherwise we can map to the transitive representation of $G$, independent of characteristic, for details see Fieker and Klüners (2014) Section 6.

*4.1.5. Determination (Algorithm 2, Step 7)*

To determine whether $I^\tau(\alpha_1, \ldots, \alpha_{\tilde{n}}) \in F$ for a $G$-relative $H$-invariant $I$ for groups $H \subset G$ we use Section 3.8 but we need to ensure that $v_0$ is the minimum infinite valuation of all the scaled roots of $f$ not just the roots corresponding to any one factor of $f$. The computation of the precision necessary is still

$$[G : H]B/\deg(P), \quad \text{or} \quad \max_{Q \in \mathbb{P}_F^\infty} \{\deg(Q)\}[G : H]B\#\mathbb{P}_F^\infty/\deg(P)$$

when $F$ is a global function field (rational or algebraic respectively), where $B$ is the bound for the evaluation of the invariant $I$ at all scaled roots of $f$. As in Section 3.8 we can replace $[G : H]$ when it is very large by some smaller value $l$ and attempt an unproven descent which can be proven later if it succeeds.

As noted in Fieker and Klüners (2014) Section 7.5, the final Galois group will be a subdirect product of the $G_i$ so only such subgroups need to be considered.

*4.1.6. Multiple and linear factors (Algorithm 2, Step 9)*

In the process of computing the Galois group one computes the roots of the polynomial in the splitting field chosen. When the polynomial has linear factors or multiple roots such roots will not have been "computed" in the computation of the Galois group, however they can easily be accounted for. The Galois group is adjusted to ensure it acts on all the roots of $f$ by mapping it to a subgroup of the direct product given in Algorithm 2 Step 9.

## 5. Examples

The timings given in this section are for computations on an Intel(R) Core(TM) i7-3770 CPU 3.4 GHz (32 GB RAM) using Magma V2.19-9.

### 5.1. Irreducible polynomials

We identify transitive groups in the form $dTn$, the $n$th transitive group of degree $d \leq 32$ according to the ordering in the database of transitive groups in Magma (Cannon et al., 2010). This is the same numbering used in GAP (The GAP Group, 2002) when $d < 32$ where the groups have been either confirmed or provided by Hulpke (2005). The transitive groups of degree 32 were provided by Cannon and Holt (2008).

**Example 1.** Let $p = 7$, $F = \mathbb{F}_7(t)$ and $f = x^8 + t + 1$ over $F$. The field $F[x]/f$ has 2 proper subfields of degrees 4 and 2 which are both generating subfields. Using the Galois groups of these subfields, we compute $8T26$ as a starting group which has order 64. This starting group has 6 conjugacy classes of transitive maximal subgroups, however only 2 of them contain the cycle shapes computed when choosing the prime $t^2 + 2$ from which we computed $\mathbb{F}_{7^{16}}[[z]]$ over which $f$ splits. We first attempt to compute a descent to $8T15$. Using a BlockQuotient invariant from Theorem 7 we find we need to transform by a Tschirnhausen transformation. However this is too expensive so instead we attempt a descent to another subgroup conjugate to $8T15$ in $S_8$. Here we use an invariant computed by applying Theorem 9 and again we need to apply a Tschirnhausen transformation. Instead we return to the attempt on the first subgroup and after applying a few transformations we decide not to descend

into this subgroup. Moving back to the other possible conjugacy class of subgroups, which are also conjugate to $8T15$ in $S_8$, we transform once before we decide that the Galois group of $f$ is contained in this conjugacy class of subgroups of order 16.

Now we compute the maximal subgroups of $8T15$ of which there are 6 transitive conjugacy classes but we need only consider 4. We first attempt descents using generic invariants into 2 subgroups conjugate to $8T6$ in $S_8$ but after applying several transformations we move on to attempting a descent into $8T8$. After applying a Tschirnhausen transformation to a generic invariant we attempt a descent into one conjugate of $8T6$ in $S_8$ using a generic invariant and decide not to descend. We make several more attempts with transformations and a generic invariant to descend into the first subgroup and decide that the first subgroup conjugate to $8T6$ which we attempted contains the Galois group of $f$. This group has 2 classes of transitive maximal subgroups however neither of them contain the cycle shapes so there are no more subgroups to consider and the Galois group of $f$ is $8T6$.

This computation took 0.38 s.

We move on to some examples in characteristic 2.

**Example 2.** Let $p = 2$, $F = \mathbb{F}_2(t)$ and $f = x^5 + x^4 + tx^3 + x + 1$ or $f = x^8 + x^7 + tx^6 + x^5 + x^2 + tx + 1$. In both of these simple examples there are subgroups of $S_n$ but none of them need consideration for a descent because either the subgroups are not transitive or the cycle structure of the group is not contained in the information we have about the cycle structure of the Galois group from the computation of the prime. Therefore the Galois groups of these polynomials are $S_5$ and $S_8$ respectively.

**Example 3.** Let $p = 2$, $F = \mathbb{F}_2(t)$ and $f = x^8 + x^4 + x - t$ over $F$. The field $F[x]/f$ has no proper subfields so we start descending from $S_8$ which has 4 conjugacy classes of transitive maximal subgroups, 2 of which contain the cycle shapes computed when choosing the prime $t^2 + t + 1$ from which we computed $\mathbb{F}_{2^{14}}[[z]]$ over which $f$ splits. We first attempt to compute a descent to $8T49$ using a SqrtDisc invariant from Theorem 5 since this class of subgroups contains $A_n$ and immediately gain a descent. This subgroup has 3 classes of transitive maximal subgroups, only 2 which we need consider. Using a generic invariant we gain a descent to a class conjugate to $8T48$ which has 4 classes of transitive maximal subgroups, 2 of which we consider. We attempt a descent into $8T37$ but find we need to apply a transformation to the generic invariant used and after doing so decide the Galois group is not contained in $8T37$. We decide that the Galois group is contained in $8T36$ after using a transformation with another generic invariant. This subgroup has 2 classes of transitive maximal subgroups, only 1 which is worth considering. Several transformations on a generic invariant later we decide that the Galois group is contained in $8T25$ which has one class of transitive maximal subgroups which is not worth considering, hence $8T25$ is the Galois group of $f$.

This computation took 0.19 s.

**Example 4.** Let $p = 2$, $F = \mathbb{F}_2(t)$ and $f = x^9 + (t^6 + t^3 + 1)x^7 + (t^9 + t^8 + t^5 + t^2 + 1)x^5 + (t^{11} + t^{10} + t^2 + t)x^4 + (t^{14} + t^{13} + t^{11} + t^8 + t^7 + t)x^3 + (t^{15} + t^{14} + t^{13} + t^{12} + t^9 + t^7 + t^5 + t)x^2 + (t^{15} + t^{14} + t^{12} + t^{11} + t^{10} + t^5 + t^2 + t + 1)x + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^6 + t^5 + t^4 + t^2 + t + 1$ over $F$ (Klüners and Malle, 1999). The field $F[x]/f$ has 1 generating subfield of degree 3 from which we compute a starting group as $9T31$ which has 4 classes of transitive subgroups. We first consider the class of $9T28$ using a D invariant from Theorem 5. After applying a Tschirnhausen transformation we decide that the Galois group is contained in this class of subgroups which themselves have 2 subgroups. Using a BlockQuotient invariant from Theorem 7 and a transformation we decide that the Galois group is contained in $9T22$ which has only one class of transitive subgroups containing the cycle shapes computed when choosing the prime $t^2 + t + 1$ from which we computed $\mathbb{F}_{2^{18}}[[z]]$ over which $f$ splits. With the class of subgroups $9T17$ we use a SqrtDisc invariant from Theorem 5 to decide that it does contain the Galois group. Now there are 2 classes of subgroups to consider, both conjugate to $9T6$ in $S_9$ and we attempt a descent with a generic invariant which fails, however the descent into the other class also with a generic invariant succeeds. Next we attempt descents to 3 classes of subgroups conjugate to $9T1$ in $S_9$ and after applying a Tschirnhausen transformation to

**Table 1**
Galois group computation over $\mathbb{F}_2(t)$.

| $F = \mathbb{F}_2(t)$ | $f = x^{10} + tx^7 + (t^2+t)x^5 + tx^4 + tx^3 + (t^2+1)x^2 + (t^2+t)x + t$ | | | |
|---|---|---|---|---|
| Prime: $t^2+t+1$ | Splits over: $\mathbb{F}_{2^{20}}[[z]]$ | | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| $10T43$ | – | Subfields | – | |
| $10T41$ | 1 | Factor Delta (Elsenhans, 2014) | Yes | |
| $10T22$ | 2 | Theorem 7 ProdSum | No | |
| $10T27$ | 1 | Theorem 7 F | Yes | |
| $10T17$ | 2 | Theorem 7 BlockQuotient | No | |
| $10T19$ | 1 | Theorem 7 BlockQuotient | Yes | 0.57 s |

**Table 2**
Galois group computation for Elsenhans (2013b).

| $F = \mathbb{F}_2(t)$ | $f = x^6 + x^5 + x^4 + x^3 + (t^2+t+1)x^2 + (t^2+t+1)x + t^2 + t + 1$ | | | |
|---|---|---|---|---|
| Prime: $t^3+t^2+1$ | Splits over: $\mathbb{F}_{2^9}[[z]]$ | | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| $6T11$ | – | Subfields | – | |
| $6T6$ | 1 | Theorem 5 D | undecided | |
| $6T3$ | 1 | Theorem 7 ProdSum | No | |
| $6T8$ | 1 | FactorDelta (Elsenhans, 2014) | undecided | |
| $6T6$ | 1 | Theorem 5 D | Yes | |
| $6T4$ | 1 | Theorem 5 SqrtDisc | Yes | 0.18 s |

one of these we gain a descent. This group has no transitive subgroups so it must be the Galois group of $f$ over $F$.

This computation took 0.79 s.

**Example 5.** In Tables 1 to 8 we summarize the subgroups and invariants used in the descent of the computation of Galois groups of some polynomials mostly from Klüners and Malle (1999) or polynomials defining subfields of the fields defined by these polynomials.

When there are 2 or more classes of subgroups which are conjugate in $S_n$ and we use the same invariant for 2 or more of these classes we do not list the subgroup class and invariant twice consecutively but note the number of such conjugate classes for which we attempt a descent in "No. classes attempted". The entry in the "Successful" column means that we were successful in a descent into one of these classes.

Note that it is possible that a descent will not be decided since another attempt after a transformation may have become more expensive than attempting a descent for another subgroup. A descent on a cheaper subgroup will first be attempted and if this fails or becomes more expensive we may return to continue to attempt a descent on a subgroup we had not decided on, hence some subgroups may appear more than once in the list of "Subgroup Class".

### 5.2. Reducible polynomials

**Example 6.** Let $F = \mathbb{F}_{101}(t)$, $f = (x^2+x+3t)(x^5+5t)(x^7+7t)((x+1)^7+7t)$. The first 2 factors of $f$ have splitting fields $S_{f_i}$ which overlap with the splitting fields of the products of the other factors, $\bar{S}_{f_i}$, in $F$ only. The last factor has a root in the splitting field of the second last factor so the overlap of their splitting fields will be larger than $F$ and a descent will be required but not from the whole direct product of the 4 Galois groups of the factors. We compute the Galois groups $2T1, 5T1, 7T4$ and $7T4$ of the factors of $f$ using prime $t^2+35t+77$ and field $F_{101^6}[[z]]$ over which $f$ splits. The order of the Galois group of the second factor is coprime to the orders of the other groups so $5T1$ does not need to be included in the direct product to descend from. By checking discriminants we discover the overlap in the splitting fields of the 3rd and 4th factors so their Galois groups will need to be

**Table 3**
Galois group computation over $\mathbb{F}_2(t)$.

| $F = \mathbb{F}_2(t)$ | $f = x^{15} + t^2x^{11} + x^{10} + tx^8 + t^4x^7 + x^5 + t^6x^3 + t^4x^2 + t^5$ | | | |
|---|---|---|---|---|
| Prime: $t^2 + t + 1$ | Splits over: $\mathbb{F}_{2^{10}}[[z]]$ | | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| 15T93 | – | Subfields | – | |
| 15T87 | 1 | Theorem 7 E | No | |
| 15T83 | 1 | Theorem 7 BlockQuotient | Yes | |
| 15T70 | 1 | Block Transfer (Elsenhans, 2014) | Yes | |
| 15T52 | 1 | Theorem 7 E | No | |
| 15T62 | 1 | Theorem 5 SqrtDisc | Yes | |
| 15T42 | 1 | Theorem 7 E | No | |
| 15T10 | 2 | Generic | Yes | 1.58 s |

**Table 4**
Galois group computation over $\mathbb{F}_{2^2}(t)$.

| $F = \mathbb{F}_{2^2}(t)$ | $f = x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + t + 1$ | | | |
|---|---|---|---|---|
| Prime: $t^3 + wt^2 + w^2t + w, \mathbb{F}_{2^2} = \mathbb{F}_2\langle w\rangle$ | | Splits over: $\mathbb{F}_{2^{36}}[[z]]$ | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| 12T56 | – | Subfields | – | |
| 12T7 | 2 | Theorem 7 ProdSum | undecided | |
| 12T6 | 2 | Generic | undecided | |
| 12T7 | 2 | Theorem 7 ProdSum | undecided | |
| 12T6 | 1 | Generic | undecided | |
| 12T7 | 2 | Theorem 7 ProdSum | undecided | |
| 12T6 | 1 | Generic | undecided | |
| 12T7 | 2 | Theorem 7 ProdSum | No | |
| 12T6 | 2 | Generic | Yes | 0.82 s |

**Table 5**
Galois group computation over $\mathbb{F}_{29}(t)$.

| $F = \mathbb{F}_{29}(t)$ | $f = x^4 + 26x^3 + (4t^2 + 28)x^2 + (6t^2 + 17)x + 4t^4 + 13t^2 + 16$ | | | |
|---|---|---|---|---|
| Prime: $t^2 + 2$ | Splits over: $\mathbb{F}_{29^2}[[z]]$ | | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| 4T3 | – | Subfields | – | |
| 4T1 | 1 | Theorem 8 DSm | No | |
| 4T2 | 1 | Theorem 8 SqrtDisc | No | 0.14 s |

**Table 6**
Galois group computation over $\mathbb{F}_{29}(t)$.

| $F = \mathbb{F}_{29}(t)$ | $f = x^{12} + 4x^{10} + 4tx^9 + 21x^8 + tx^7 + (15t^2 + 13)x^6 + 7tx^5 + (13t^2 + 24)x^4 + (26t^3 + 2t)x^3 + (11t^2 + 21)x^2 + (10t^3 + 21t)x + 4t^2 + 10$ | | | |
|---|---|---|---|---|
| Prime: $t^2 + 2$ | Splits over: $\mathbb{F}_{29^2}[[z]]$ | | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| 12T292 | – | Subfields | – | |
| 12T273 | 1 | Theorem 8 $s_2$ | Yes | |
| 12T253 | 1 | Theorem 7 BlockQuotient | Yes | |
| 12T205 | 1 | Theorem 7 BlockQuotient | Yes | |
| 12T142 | 1 | Theorem 7 ProdSum | No | |
| 12T45 | 1 | Theorem 7 ProdSum | No | |
| 12T129 | 1 | Generic | Yes | |
| 12T59 | 1 | Theorem 7 ProdSum | No | |
| 12T85 | 1 | Theorem 8 SqrtDisc | No | 0.46 s |

**Table 7**
Galois group computation over $\mathbb{F}_{29}(t)$.

| $F = \mathbb{F}_{29}(t)$ | $f = x^{12} + 26tx^8 + 13t^2x^6 + 20t^2x^4 + 27t^3$ | | | |
|---|---|---|---|---|
| Prime: $t^2 + 13t + 21$ | | Splits over: $\mathbb{F}_{29^8}[[z]]$ | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| 12T227 | – | Subfields | – | |
| 12T137 | 1 | Theorem 7 BlockQuotient | Yes | |
| 12T111 | 2 | Generic | undecided | |
| 12T110 | 1 | Theorem 9 | undecided | |
| 12T111 | 1 | Generic | undecided | |
| 12T110 | 2 | Theorem 9 | undecided | |
| 12T111 | 2 | Generic | No | |
| 12T110 | 2 | Theorem 9 | No, Yes | 2.22 s |

**Table 8**
Galois group computation over $\mathbb{F}_{29}(t)$.

| $F = \mathbb{F}_{29}(t)$ | $f = x^{12} + 15x^{10} + 16x^9 + 3x^8 + 4x^7 + (19t + 9)x^6 + (26t + 9)x^5 + (25t + 7)x^4 + 21tx^3 + 20tx^2 + 12tx + 3t$ | | | |
|---|---|---|---|---|
| Prime: $t^2 + 15t + 9$ | Splits over: $\mathbb{F}_{29^6}[[z]]$ | | | |
| Subgroup class | No. classes attempted | Invariant type | Successful | Time |
| 12T136 | – | Subfields | – | |
| 12T108 | 2 | Theorem 7 F | undecided, No | |
| 12T109 | 2 | Theorem 7 F | undecided, No | |
| 12T108 | 1 | Theorem 7 F | No | |
| 12T109 | 1 | Theorem 7 F | Yes | 0.52 s |

included in the direct product we descend from. We continue to check whether $S_{f_1}$ overlaps with $S_{f_3 f_4}$ outside of $F$. The discriminant of the first factor is coprime to those of the third and fourth factors and the dimension of the exact constant field of $F[x]/f_1$ is coprime to the dimensions of the exact constant fields of $F[x]/f_3$ and $F[x]/f_4$. The Galois group of the first factor has a cyclic subgroup and the order of that cyclic subgroup is not coprime to the orders of the cyclic subgroups of the Galois groups of the third and fourth factors so we compute the fixed fields of the quotients of the Galois groups of the first, third and fourth factors by their normal subgroups where that quotient is cyclic. We compute the exact constant fields of these fixed fields and check whether their dimensions are coprime as well as the orders of the normal subgroups. Here we find that the dimension for the first factor is coprime to that of the third and fourth factors (the dimension for the first factor is 1), hence the Galois group of the first factor does not need to be included in the direct product we descend from.

So we need to descend from the direct product of the third and fourth factors. This direct product of order 1764 has 9 subgroups, 3 of which are subdirect products of $G_3$ and $G_4$. We attempt descents to 2 subgroups of index 3, order 588, using an invariant which is a more general combination than Theorem 9 (see Fieker and Klüners, 2014 following Lemma 5.8) and an invariant gained by mapping to the transitive representation of the subgroup. We apply transformations for both subgroups but none of these attempts succeed. We attempt a descent into a subgroup of index 2, order 882, using a Factor Delta invariant from Elsenhans (2014) and this succeeds immediately. This subgroup has 7 subgroups of which 2 are subdirect products of $G_3$ and $G_4$. We again use an invariant from the transitive representation for this subgroup of order 294 and this descent succeeds after applying transformations. Now there are 6 subgroups out of 10 which are subdirect products and we attempt descents to all 6 subgroups of order 42 using invariants from the transitive representation. After applying several transformations to the invariants for 4 of these groups we have 4 failed descents but for one of these subgroups the descent succeeds after applying several transformations. This subgroup has 3 subgroups but since none of these are subdirect products of $G_3$ and $G_4$ the descent is finished.

**Table 9**
Timings for Galois group computations for some irreducible polynomials.

| | $p=2$ | | | | | $p=3$ | | |
|---|---|---|---|---|---|---|---|---|
| $d$ | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 |
| Average time | 0.014 s | 0.008 s | 0.058 s | 0.47 s | 131.72 s | 0.016 s | 0.108 s | 6.936 s |
| Min/Max time | | | | | 33 s / 490 s | | | 2 s / 22 s |

| | $p=5$ | | $p=7$ | | $p=11$ | | $p=29$ |
|---|---|---|---|---|---|---|---|
| $d$ | 1 | 2 | 1 | 2 | 1 | 2 | 1 |
| Average time | 0.032 s | 7.866 s | 1.762 s | 533.104 s | 0.662 s | – | 57.360 s |
| Min/Max time | | 2 s / 24 s | | 350 s / 1210 s | | | 7 s / 122 s |

**Table 10**
Timings for Galois group computations for some reducible polynomials.

| | $p=2$ | | | | $p=3$ | | |
|---|---|---|---|---|---|---|---|
| $d$ | 1 | 2 | 3 | 4 | 1 | 2 | 3 |
| Degree | 6 | 10 | 20 | 40 | 9 | 21 | 63 |
| Average time | 0.082 s | 0.77 s | 87.796 s | 2175.798 s | 0.166 s | 82.782 s | 2203.21 s |
| Min/Max time | | | 2 s / 315 s | 224 s / 8670 s | | 46 s / 156 s | 510 s / 5906 s |

| | $p=5$ | | $p=7$ | $p=11$ |
|---|---|---|---|---|
| $d$ | 1 | 2 | 1 | 1 |
| Degree | 15 | 55 | 21 | 33 |
| Average time | 0.490 s | 48.4 hours | 296.684 s | 2010.78 s |
| Min/Max time | | 21.6 hours / 116.3 hours | | 1208 s / 4009 s |

We take the direct product of the Galois groups of the first 2 factors and the result of the descent as the Galois group of $f$ which has order 420.

This computation took 2.1 s.

## 6. Results

The computations we give timings for in this section were run on an Intel(R) Core(TM) i7-3770 CPU 3.4 GHz (32 GB RAM) using Magma V2.19-9.

### 6.1. Irreducible polynomials

In Table 9 are average times and minimum and maximum times where they differ substantially, for the computations of Galois groups of 5 random monic additive polynomials over $\mathbb{F}_p[t]$ of degree $p^d$. We have used additive polynomials for these timings since we know the result of the Galois group computation is not $S_n$.

The polynomials for which we can compute a Galois group in some reasonable time are restricted by the Subfields algorithm which factors the polynomial over the field it defines, unless it can be determined using the cycle information that the field has no subfields. This is why we do not report a time for $p=11$, $d=2$.

### 6.2. Reducible polynomials

In Table 10 are average times for the computations of Galois groups of 5 products of 2 random additive polynomials with the evaluation of one of these at $x+1$. At least two factors of each polynomial are of degree $p^d$ and the remaining factor is of degree $p^{d-1}$ when $d \neq 1$. The factors were chosen with the intention that one factor (of degree $p^{d-1}$) would have splitting field disjoint from the splitting field of the product of the other two factors which would have splitting fields which are

not disjoint. Therefore the descent will mostly be from the direct product of the Galois groups of the two degree $p^d$ factors.

## Acknowledgements

The author would like to thank Claus Fieker for his help in working with his implementation of Fieker and Klüners (2014), Stephen Donnelly for a number of helpful conversations and A.-Stephan Elsenhans for his suggestions.

## References

Cannon, J.J., Holt, D.F., 2004. Computing the maximal subgroups of a finite group. J. Symb. Comput. 37, 589–609.
Cannon, J.J., Holt, D.F., 2008. The transitive permutation groups of degree 32. Exp. Math. 17, 307–314.
Cannon, J.J., Bosma, W., Fieker, C., Steel, A. (Eds.), 2010. Handbook of Magma functions (V 2.17), Computational Algebra Group. University of Sydney. http://magma.maths.usyd.edu.au.
Casperson, D., McKay, J., 1994. Symmetric functions, $m$-sets and Galois groups. Math. Comput. 63, 749–757.
Darmon, Henri, Ford, David, 1989. Computational verification of $M_{11}$ and $M_{12}$ as Galois groups over $Q$. Commun. Algebra 17, 2941–2943.
Davenport, J.H., Smith, G.C., 2000. Fast recognition of symmetric and alternating Galois groups. J. Pure Appl. Algebra 153, 17–25.
Donnelly, S., Sutherland, N., 2012. Personal communication.
Duval, Dominique, 1989. Rational Puiseux expansions. Compos. Math. 70, 119–154.
Eichenlaub, Y., 1996. Problémes effectifs de théorie de Galois en degrés 8 á 11. PhD thesis. Université Bordeaux I.
Elsenhans, A.-S., 2012. Invariants for the computation of intransitive and transitive Galois groups. J. Symb. Comput. 47, 315–326.
Elsenhans, A.-S., 2013a. Personal communication.
Elsenhans, A.-S., 2013b. Personal communication.
Elsenhans, A.-S., in press. A note on short cosets. Exp. Math. http://dx.doi.org/10.1080/10586458.2014.922908.
Elsenhans, A.-S., 2014. On the construction of relative invariants.
Fieker, C., 2009. Magma implementation and personal communication.
Fieker, C., Klüners, J., 2014. Computation of Galois groups of rational polynomials. LMS J. Comput. Math. 17 (1), 141–158. http://arxiv.org/abs/1211.3588.
Geißler, K., 2003. Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern. PhD thesis. Technische Universität Berlin. Available at http://www.math.tu-berlin.de/~kant/publications/diss/geissler.pdf.
Geißler, K., Klüners, J., 2000. Galois group computation for rational polynomials. J. Symb. Comput. 30 (6), 653–674.
Hulpke, Alexander, 2005. Constructing transitive permutation groups. J. Symb. Comput. 39 (1), 1–30. MR 2168238.
Hulpke, Alexander, 1999. Galois groups through invariant relations. In: Campbell, C.M., et al. (Eds.), Groups St. Andrews 1997 in Bath. Selected Papers of the International Conference, vol. 2. Bath, UK, July 26–August 9, 1997 (Cambridge). In: Lond. Math. Soc. Lect. Note Ser., vol. 261. Cambridge University Press, pp. 379–393.
Klüners, J., Malle, G. 1999. Database of polynomials over $\mathbb{Q}(t)$ with known Galois groups based on the polynomials in the appendix of Malle and Matzat (1999).
Malle, G., Matzat, B.-H., 1999. Inverse Galois Theory. Springer.
Mattman, T., McKay, J., 1997. Computation of Galois groups over function fields. Math. Comput. 66, 823–831.
Seress, Ákos, 2003. Permutation Group Algorithms. Cambridge University Press.
Soicher, L., 1981. The computation of Galois groups. Master's thesis. Concordia University, Montreal.
Soicher, J., McKay, L., 1985. Computing Galois groups over the rationals. J. Number Theory 20, 273–281.
Stauduhar, Richard P., 1973. The determination of Galois groups. Math. Comput. 27, 981–996.
Stichtenoth, H., 1993. Algebraic Function Fields and Codes. Springer-Verlag.
The GAP Group, 2002. Gap – groups, algorithms, and programming, version 4.3.
Tignol, Jean-Pierre, 2001. Galois' Theory of Algebraic Equations. World Scientific.
van der Waerden, B.L., 1966. Modern Algebra. Frederick Ungar Publishing Co.
van Hoeij, M., Klüners, J., Novocin, A., 2011. Generating subfields. In: ISSAC 2011.
Yokoyama, K., 1997. A modular method for computing Galois groups of polynomials. J. Pure Appl. Algebra 117–118, 617–636.