ON THE CONSTRUCTION OF RELATIVE INVARIANTS

ANDREAS-STEPHAN ELSENHANS

Abstract. An invariant of a group U is called a relative invariant of $U \subsetneq G$ if its stabilizer in G is U. The computation of Galois groups requires the construction of such invariants for permutation groups. In this article, we summarize the constructions of relative invariants as they are implemented in the Galois group package of magma 2.20. These constructions result in practical invariants for all transitive groups up to degree 32.

1. Introduction

The computation of the Galois group of a polynomial is one of the basic questions of algorithmic algebraic number theory [3, Sec. 6.3]. Old algorithms used tables of precomputed data. Thus, they were equipped with an a priori degree limitation. In [8], such an algorithm is described for polynomials up to degree 23. As there are 25000 transitive permutation groups in degree 24, it is clear that any extension will get huge. Thus, one needs a degree independent implementation that computes all required data on the fly. The first implementation of such an algorithm is described in [7]. It was done as a magma [1] package.

The basic idea of the algorithm dates back to [13]. The first observation is that the Galois group of a separable degree n polynomial f is contained in $G_1 := \mathrm{Sym}(n)$. We take this as the starting group and compute the conjugacy classes of maximal subgroups.

For each maximal subgroup class representative U, we compute a *relative invariant polynomial* I, i.e., a polynomial such that its stabilizer in G_1 is U.

We form $I(r_{\sigma(1)}, \ldots, r_{\sigma(n)})$, for r_i the roots of f and $\sigma \in G_1//U$. Here, we denote by $G_1//U$ a system of coset representatives of G/U. Assuming the numerical values of the evaluation of the invariant to be distinct, one can show that the Galois group is contained in $\sigma U \sigma^{-1}$ if and only of the corresponding value of the invariant is rational.

Using this, one can either prove that the Galois group is equal to G_1 or find a maximal subgroup G_2 that contains the Galois group. Now, one iterates this step starting with G_2 instead of G_1 until the Galois group is determined.

One limiting bottleneck of the implementation described in [7] is the complexity of the invariant. In case its evaluation requires a large number of arithmetic operations, the computation gets slow. In extreme cases, the construction of the invariant may even run out of memory.

The aim of this article is to describe the methods to construct relative invariants, as they are implemented in magma 2.20. These constructions cover all transitive groups up to degree 32.

2. Invariants from block systems and the Reynolds operator

2.1. **Block systems.** Let $G \subset \mathrm{Sym}(n)$ be a transitive permutation group. Let $B \subset \{1, \ldots, n\}$ be a non-empty subset. In case

$$\forall \sigma \in G : \sigma B = B \text{ or } \sigma B \cap B = \emptyset$$

we call B a *block* of G. The G-orbit of B is called a *block system*.

In case B is a singleton, we get the trivial block system. Otherwise, we get a non-trivial block system. A permutation group without a non-trivial block system is called *primitive*. Otherwise, it is called *imprimitive*.

We denote a block system $\{B_1, \ldots B_k\}$ by $\mathcal{B}$. As G acts on the block system, this gives us a second permutation representation. We denote it by $\phi_{\mathcal{B}}$.

2.2. **Remarks.**
i) The size of a block is a divisor of the degree of the permutation group. Thus, all groups of prime degree are primitive.

ii) However, most transitive permutation groups have block systems. For example, only five out of the 25000 transitive permutation groups in degree 24 are primitive.

2.3. **Wreath product type constructions.** Let U be a maximal and transitive subgroup of $G \subset \mathrm{Sym}(n)$. In case U is a subgroup of a non-trivial wreath product in $\mathrm{Sym}(n)$ that does not contain G, at least one of the following constructions results in a relative invariant in $K[X_1, \ldots, X_n]$. [8, Satz 6.14, Satz 6.16]

NewBlock-construction: In case $\{B_1, \ldots, B_k\}$ is a block-system for U, but not for G, the following are relative invariants

$$\sum_{i=1}^{k} (\sum_{j \in B_i} X_j)^2, \text{ if } \mathrm{char}(K) \neq 2,$$

$$\sum_{i=1}^{k} (\sum_{j \in B_i} X_j)^3, \text{ if } \mathrm{char}(K) \neq 3,$$

$$\sum_{i=1}^{k} (\prod_{j \in B_i} X_j), \ \prod_{i=1}^{k} (\sum_{j \in B_i} X_j) \text{ in general.}$$

E-construction: Let $\mathcal{B} = \{B_1, \ldots, B_k\}$ be a block system of G with $\phi_{\mathcal{B}}(U) \neq \phi_{\mathcal{B}}(G)$. Then

$$I(\sum_{i \in B_1} X_i, \ldots, \sum_{i \in B_k} X_i)$$

is a relative invariant for $U \subset G$. Here, I denotes a relative invariant for $\phi_{\mathcal{B}}(U) \subset \phi_{\mathcal{B}}(G)$.

F-construction: Let $\mathcal{B} = \{B_1, \ldots, B_k\}$ be a block system of G. Assume $\mathrm{Stab}_U(B_1)|_{B_1} \neq \mathrm{Stab}_G(B_1)|_{B_1}$. Then we get the relative invariant

$$\sum_{s \in U // \mathrm{Stab}_U(B_1)} I^s .$$

Here, I denotes a relative invariant for $\mathrm{Stab}_U(B_1)|_{B_1} \subset \mathrm{Stab}_G(B_1)|_{B_1}$.

2.4. **Remark.** The F-construction lifts an invariant of a subgroup to a U-invariant by forming its orbit sum. This is a general strategy in invariant theory, usually called the *Reynolds operator*. The general construction is as follows:

Let $U \subset G$ be a subgroup of finite index. Then the *Reynolds operator* maps U-invariants to G-invariants by

$$R_{G/U}(f) = \frac{1}{[G:U]} \sum_{\sigma \in G//U} \sigma f \,.$$

It may happen that the result degenerates. For example, if U is an index 2 subgroup of G and G acts on f by change of sign then we get $R_{G/U}(f) = 0$. In the situation of the F-construction, it is obviously impossible that the invariant degenerates to a G-invariant. In later constructions, we will use the following lemma to exclude degeneration.

2.5. **Lemma.** Let $U_0, G \subset G_0 \subset \mathrm{Sym}(n)$ be permutation groups. Define $U := U_0 \cap G \neq G$. We assume $[U_0 : U] = [G_0 : G] > 1$. Further let f be an U-invariant that is not G invariant. If the K-vector space $\mathrm{span}\{\sigma f \mid \sigma \in U_0\}$ is of dimension $[U_0 : U]$ and $\mathrm{span}\{\sigma f \mid \sigma \in G\}$ is one dimensional then $R_{U_0/U}(f)$ is not G_0-invariant.

Proof: In this situation, U_0/U coset representatives are G_0/G coset representatives. Thus, G acts on $\mathrm{span}\{\sigma f \mid \sigma \in U_0\}$, as well.

Pick an element $\tau \in G$ with $\tau f \neq f$ (i.e., f and τf differ by a scalar). τ acts on the sum $\sum_{\sigma \in U_0//U} \sigma f$ by permutation and scaling of the summands. As the summands are linearly independent, τ will not stabilize the sum as it does not stabilize f. □

3. Change of representation and the BlockQuotient-construction

3.1. **Change of representation.** Let $H \subset G$ be a subgroup. Then the coset action of G on G/H coincides with the G-action on the G-orbit of a $(H \subset G)$-relative invariant. We denote the coset action homomorphism by $\phi_{G/H}$. For a maximal subgroup $U \subset G$ with $\phi_{G/H}(U) \neq \phi_{G/H}(G)$, we can use a relative invariant for $\phi_{G/H}(U) \subset \phi_{G/H}(G)$ and plug the G-orbit of a $(H \subset G)$-relative invariant into it. This leads to a U-invariant. In case the construction does not degenerate, we get a relative invariant. In case of a degeneration, we replace the $(H \subset G)$-relative invariant I by $T(I)$ with a random univariate polynomial T [8, Bemerkung 6.19].

3.2. **The BlockQuotient-Construction.** The following strategy to pick H leads to the *BlockQuotient-Construction*:

i) For each block-system $\mathcal{B} = \{B_1, \ldots, B_k\}$ of G, compute the stabilizer $S := \mathrm{Stab}_G(B_1)$. Denote by π the action of S on B_1.

ii) Compute the subgroups of $\pi(S)$ of index $2, \ldots, \#B_1$.

iii) For each subgroup $T \subset \pi(S)$ found, take its preimage $H := \pi^{-1}(T)$.

iv) In case $\phi_{G/H}(U) \neq \phi_{G/H}(G)$ and $\phi_{G/H}(G)$ has smaller degree or order than G, return H as the subgroup to be used.

One advantage of this construction is that a $(H \subset G)$-relative invariant is given by a $(T \subset \pi(S))$-relative invariant. The later groups are much simpler as they have at most half the degree as the initial ones.

3.3. **Remark.** The index limit $\#B_1$ for the subgroup search is somehow random. It is a trade-off between the time spent to search for and test the subgroups and the chance of getting a significant simplification by passing to $\phi_{G/H}(U) \subset \phi_{G/H}(G)$.

3.4. **Interpretation.**
i) One can interpret the Block-Quotient construction as follows. Let a tower of fields $\mathbb{Q} \subset K \subset L$ be given. The field L is the stem field $\mathbb{Q}[x]/(f)$, for f the polynomial we are treating. The field K corresponds to the stabilizer of one block of a block system of the Galois group.

The BlockQuotient-construction passes to the tower $\mathbb{Q} \subset K \subset L_1$. Here, the field L_1 is chosen as a subfield of the Galois hull of L/K with the degree limit $[L_1 : K] \leq [L : K]$. The Galois group of the Galois hull of $L_1/\mathbb{Q}$ is a quotient of the Galois group of the Galois hull of $L/\mathbb{Q}$. The new representation used by the BlockQuotient-construction is the projection.

Typical examples for this are $\mathbb{Q} \subset K := \mathbb{Q}[a] \subset \mathbb{Q}[\sqrt[n]{a}]$, for $L_1 := K[\zeta_n]$ and $\mathbb{Q} \subset K := \mathbb{Q}[a] \subset \mathbb{Q}[\sqrt[16]{a}]$ for $L_1 := \mathbb{Q}[\sqrt{a}]$ or $L_1 := \mathbb{Q}[\sqrt[4]{a}, \sqrt{-1}]$.
ii) In the category of permutation groups the Block-Quotient-construction can be described as follows: Given transitive subgroups $G_1 \subset \mathrm{Sym}(n_1)$, $G_2 \subset \mathrm{Sym}(n_2)$ and a surjective homomorphism $\phi\colon G_1 \to G_2$. Then ϕ induces a homomorphism of wreath products

$$\begin{aligned} \Phi\colon G_1^n \rtimes \mathrm{Sym}(n) &\to G_2^n \rtimes \mathrm{Sym}(n) \\ ((\sigma_1, \ldots, \sigma_n), \tau) &\mapsto ((\phi(\sigma_1), \ldots, \phi(\sigma_n)), \tau)\,. \end{aligned}$$

In the notation we used in 3.2 we have $G_1 = \pi(S)$ and ϕ is the action on $\pi(S)/T$. Further, $\Phi|_G$ is $\phi_{G/H}$.

3.5. **Statistics.** We used the database of transitive groups [2, 10] up to degree 32 to test the constructions above. This led to the statistics in Table 1.

n	# pairs	# NewBlock/E/F	# Block-Quot	# Remaining
4	5	3	0	2
6	30	21	2	7
8	141	100	20	21
9	78	40	8	30
10	100	66	12	22
12	1083	795	201	87
15	264	171	55	38
16	12533	9613	2663	257
18	4189	3217	892	80
20	4856	3448	1082	326
24	178753	135464	42101	1188
27	12964	8558	3549	857
28	8293	5775	1879	639
30	28012	20505	7048	459
32	53804069	46347960	7443119	12990

Table 1 – Number of pairs of groups $U \subset G \subset \mathrm{Sym}(n)$ covered

3.6. **Inspecting other representations.** As explained above, the BlockQuotient construction leads to a simplification, as it maps to a smaller group. In some cases even an injective map may be helpful.

i) The primitive wreath product [5, Sec. 2.7] is a permutation representation of $\mathrm{Sym}(n) \wr \mathrm{Sym}(m)$ of degree n^m. Mapping to the imprimitive wreath product of degree nm is an isomorphism. Aside from the degree reduction the main advantage is that this map makes the group structure more visible.

ii) The action on 2-sets of $U \subset G \subset \mathrm{Sym}(n)$ coincides with the action on the monomials $\{X_iX_j : i \neq j\}$. This is a faithful representation of degree $\binom{n}{2}$. One could try to use this new representation to get an invariant. The main problem of this approach is that it is not clear how to decide wether this is simpler than the initial representation. Of course, one can use it in case U has more orbits than G or U has a new block system. The first possibility is an example of a generic invariant, as they are analyzed in [7, Section 4].

4. Constructions for index 2 subgroups

4.1. **Example.** Let $\mathrm{Alt}(n) \subset \mathrm{Sym}(n)$ be the alternating group inside the symmetric group of degree n. An element of $\mathrm{Sym}(n)$ is contained in $\mathrm{Alt}(n)$ if and only if it is in the kernel of the sign homomorphism. We denote by Δ the polynomial

$$\begin{aligned}\prod_{1\le i<j\le n}(X_j - X_i) &= \sum_{\sigma\in\mathrm{Sym}(n)} \mathrm{sgn}(\sigma) X_{\sigma(2)}X_{\sigma(3)}^2\cdots X_{\sigma(n)}^{n-1} \\ &= \begin{vmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{vmatrix}.\end{aligned}$$

Then $\mathrm{Sym}(n)$ operates on Δ via the sign homomorphism. Thus, Δ is a relative invariant for $\mathrm{Alt}(n) \subset \mathrm{Sym}(n)$.

4.2. **Generalization.** The product formula above for the invariant Δ can be interpreted as follows: The $\mathrm{Sym}(n)$-orbit of $(X_1 - X_2)$ is $\{\pm(X_i - X_j) \mid 1 \le i < j \le n\}$. In this situation, the signed permutations give us a $\binom{n}{2}$-dimensional monomial representation of $\mathrm{Sym}(n)$.

Thus, the action on the product

$$\prod_{1\le i<j\le n}(X_i - X_j)$$

results in a one-dimensional representation.

In case $G \subset \mathrm{Sym}(n)$ is a subgroup that is not transitive on 2-sets, the above representation decomposes into monomial subrepresentations. We get one summand for each orbit of G on 2-sets. Denote by O_2 one G-orbit on 2-sets. This orbit leads to a 1-dimensional representation, given by the action on

$$\prod_{\{i,j\}\in O_2}(X_{\min\{i,j\}} - X_{\max\{i,j\}}).$$

4.3. **Combining invariants.** Given the index 2 subgroups $U_1, U_2 \subset G$, there is a third index 2 subgroup

$$U_3 := (U_1 \cap U_2) \cup (G \setminus (U_1 \cup U_2)) .$$

Let I_1, I_2 be relative invariants for $U_1, U_2 \subset G$. We assume that the action of G on these invariants is by change of sign. If this is not the case then we replace the invariants by $I_j - \sigma I_j$ for a $\sigma \in G \setminus U_j$. Then $I_3 := I_1 I_2$ is a relative invariant for U_3. [8, Satz 6.21]

More generally, given two 1-dimensional representations of G by action on polynomials, we get the tensor product of these representations as the product of the polynomials. This will be a relative invariant for the kernel of the representation.

4.4. **The FactorDelta-construction.** Let a subgroup $G \subset \mathrm{Sym}(n)$ be given. Then we apply the following steps to find invariants for index 2 subgroups of G:

i) Compute all orbits of G and all block systems of each orbit.

ii) List transitive representations of G by taking the actions on orbits and on block systems.

iii) For each transitive representation found, compute the orbits of the action on 2-sets.

iv) For each orbit on 2-sets found compute the 1-dimensional representations of G as formulated in the generalization above.

v) Compute the kernel of each representation.

vi) In case a representation is trivial, delete it.

vii) In case two representations have the same kernel, pick the simpler one.

viii) For each pair of representations found, apply the above combine step to get a third representation having an other index 2 subgroup as kernel.

ix) In case a representation with this kernel is already known, pick the one with the simpler polynomial.

x) Iterate the combine step until no further representations are found.

xi) Return the list of 1-dimensional representations found and the list of kernels.

5. Using monomial representations and transfer

5.1. **Recall.**

i) A matrix is called monomial if each row and each column have exactly one non-zero entry.

ii) A matrix group is called monomial if all elements are monomial matrices.

iii) A representation is called monomial if its image is a monomial group.

iv) For a field K the group of $n \times n$ monomial matrices $N_n(K)$ is isomorphic to $(K^*)^n \rtimes \mathrm{Sym}(n)$.

v) The monomial group has a 1-dimensional representation given by the determinant and a second one given by the sign of the permutation in $\mathrm{Sym}(n)$.

vi) The tensor product of these two 1-dimensional representations is a third 1-dimensional representation. It is the product of all the non-zero entries of the matrix.

vii) More generally, each group with a monomial representation has these three 1-dimension representations associated to the monomial representation.

viii) The induced representation $\mathrm{Ind}_U^G(\phi)$ of a 1-dimension representation ϕ of a subgroup U of finite index in G is a monomial representation of G. All monomial representations are direct sums of such representations.

5.2. **Notation.** In case the monomial representation is given as $\mathrm{Ind}_U^G(\phi)$ for a 1-dimensional representation ϕ, we call the tensor product of vi) the ϕ-transfer of G. For a general introduction to the transfer, we refer to [11, Kap. IV] and in particular to [11, IV, Hilfssatz 1.2].

5.3. **Monomial representations from block systems.** Given the wreath product $G := C_k \wr \mathrm{Sym}(n) \subset \mathrm{Sym}(kn)$ of the cyclic group of order k and the symmetric group of degree n, we get a monomial representation by mapping C_k to the group of k-th roots of unity $\langle\zeta_k\rangle$. I.e., we use the isomorphism of the wreath product to $\langle\zeta_k\rangle^n \rtimes \mathrm{Sym}(n)$.

We get the required 1-dimension representation ϕ of $C_k \subset \mathrm{Sym}(k)$ as the action on $X_1 + \zeta_k X_2 + \cdots + \zeta_k^{k-1} X_k$. The ϕ-transfer representation of G is given by the action on the product

$$(X_1 + \zeta_k X_2 + \cdots + \zeta_k^{k-1} X_k) \cdot \ldots \cdot (X_{(k-1)n+1} + \zeta_k X_{(k-1)n+2} + \cdots + \zeta_k^{k-1} X_{nk}) .$$

5.4. **Remarks.**
i) Let the wreath product $G = G_1 \wr G_2$ be given. In case G_1 is not cyclic, one would like to start with a more complicated 1-dimensional representation ϕ (i.e., a quotient) of G_1 to get a representation of G with an interesting kernel. However, this is implicitly done by the BlockQuotient-construction described above, as the projection $G_1 \wr G_2 \to \phi(G_1) \wr G_2$ is a possible block quotient.

ii) In practice, we are interested in invariants with rational coefficients instead of roots of unity. As shown in [6, Sec. 4], this problem can be solved by splitting the invariants into components.

5.5. **Generalization.** In some cases we have to combine the transfer construction with the Reynolds operator. Thus, we start with $U_0 \subset G_0$. Then we pick an auxiliary group G and put $U := G \cap U_0$. In the lucky case that the transfer construction gives us a relative invariant for $U \subset G$, we can lift it with the Reynolds operator to a relative invariant for $U_0 \subset G_0$.

5.6. **Examples.**
i) We inspect the groups $U_0 := T_{30}^{5396}$, $G_0 := T_{30}^{5421}$,

$$\begin{aligned} & T_{30}^{5396} = (\{(\sigma_1, \ldots, \sigma_{10}) \in \mathrm{Alt}(3)^{10} \mid \sigma_1 \cdots \sigma_{10} = \mathrm{id}\} \rtimes \mathrm{Sym}(10)) \rtimes \mathbb{Z}/2\mathbb{Z} \\ \subset \quad & T_{30}^{5421} = (\mathrm{Alt}(3) \wr \mathrm{Sym}(10)) \rtimes \mathbb{Z}/2\mathbb{Z} . \end{aligned}$$

Here, we first have to remove the extension by $\mathbb{Z}/2\mathbb{Z}$. Then we get an invariant for $U := T_{30}^{5368} \subset G := T_{30}^{5405}$ by transfer. Finally, the Reynolds operator lifts this to a relative invariant for the initial groups. The decomposition of the cyclotomic coefficients into components leads to an evaluation algorithm of the invariant that involves 103 multiplications over the base field.

In this case, the subgroup U can be constructed as the kernel of the coset action of G_0 on G_0/U_0.

ii) The dihedral group D_4 can be constructed as the semi-direct product $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Using this, we can construct $(\mathbb{Z}/4\mathbb{Z})^7 \rtimes \mathbb{Z}/2\mathbb{Z}$ by acting on each factor in the same way. In this case, we have the subgroups

$$\begin{aligned} U_2 &:= \{(x_1,\ldots,x_7) \in (\mathbb{Z}/4\mathbb{Z})^7 \mid \sum x_i = 0 \bmod 2\} \rtimes \mathbb{Z}/2\mathbb{Z}, \\ U_4 &:= \{(x_1,\ldots,x_7) \in (\mathbb{Z}/4\mathbb{Z})^7 \mid \sum x_i = 0 \bmod 4\} \rtimes \mathbb{Z}/2\mathbb{Z}\,. \end{aligned}$$

As U_2 and U_4 are Sym(7) invariant, we get the extensions

$$U_0 := T_{28}^{1610} = U_4 \rtimes \mathrm{Sym}(7) \subset G_0 := T_{28}^{1651} = U_2 \rtimes \mathrm{Sym}(7)\,.$$

To construct an invariant, we have to remove the $\mathbb{Z}/2\mathbb{Z}$ in U_2 and U_4. After that, we can use the transfer to construct an invariant for $T_{28}^{1541} \subset T_{28}^{1601}$ that can be evaluated by 42 multiplications. The Reynolds operator lifts this to an invariant for $U_0 \subset G_0$. This doubles the number of multiplications.

5.7. **Remark.** A summary of the general construction is as follows. Given $U_0 \subset G_0$, we first search for an auxiliary group G. Then we construct a relative invariant for $U_0 \cap G \subset G$ by ϕ-transfer. Finally, we lift the invariant by using the Reynolds operator.

In practice, the main problem is to find the auxiliary group. As we are only interested in subgroups of small index, one could in principle enumerate all subgroups of bounded index and test them. In some cases, we can do better as we will show in the next section.

6. Invariants in case of a block system of block size 2

6.1. **Setup.** Let $U \subset G$ be a maximal subgroup of a transitive permutation group of degree $n = 2k$ with the block system $\mathcal{B} = \{\{1,2\},\{3,4\},\ldots,\{2k-1,2k\}\}$. Further, we assume that the E-construction does not work, i.e., $\phi_{\mathcal{B}}(U) = \phi_{\mathcal{B}}(G)$. As

$$\mathrm{Stab}_G(B_1)|_{B_1} = \mathrm{Stab}_U(B_1)|_{B_1} \cong \mathrm{Sym}(2)\,,$$

the F-construction and the BlockQuotient construction do not lead to anything when applied to this block-system. Table 2 gives an overview of the number of transitive groups having such a block system.

6.2. **Invariants for the kernel of the block action.** Let $U \subset G$ and the block system $\mathcal{B}$ be given as in 6.1. Then, the difference of U and G is hidden in the kernel of $\phi_{\mathcal{B}}$. Let us inspect the kernel a bit closer:

$$U_0 := U \cap \ker(\phi_{\mathcal{B}}) \subsetneq G_0 := \ker(\phi_{\mathcal{B}}) \subset \mathrm{Sym}(2)^k \cong (\mathbb{Z}/2\mathbb{Z})^k \cong \{\pm 1\}^k\,.$$

The last isomorphism is given by the action on the polynomials

$$X_1 - X_2, X_3 - X_4, \ldots, X_{2k-1} - X_{2k}\,.$$

From this, we can easily write down an $U \cap \ker(\phi_{\mathcal{B}})$-invariant that is not a $\ker(\phi_{\mathcal{B}})$-invariant. Even better, we can construct one of minimal degree as follows:
i) Write $U \cap \ker(\phi_{\mathcal{B}})$ and $\ker(\phi_{\mathcal{B}})$ as subgroups of $(\mathbb{Z}/2\mathbb{Z})^k$.
ii) View these groups as $\mathbb{F}_2$-codes $C_U \subsetneq C_G$.
iii) Compute the dual codes $C_G^{\perp} \subsetneq C_U^{\perp}$.
iv) Find a word w of minimal weight in $C_U^{\perp} \setminus C_G^{\perp}$.
v) Return $I_w := \prod_{i,w_i=1}(X_{2i-1} - X_{2i})$ as invariant of U_0 that is not G_0 invariant.

Degree	# groups	with a block of size 2
4	5	3
6	16	8
8	50	36
10	45	21
12	301	182
14	63	37
16	1954	1754
18	983	387
20	1117	621
22	59	32
24	25000	20733
26	96	39
28	1854	1238
30	5712	1955
32	2801324	2793029

Table 2 – Number of transitive groups with blocks of size 2

6.3. **Remarks.**
i) Note that $\phi_{\mathcal{B}}(G)$ consists of automorphisms of all the codes involved. These code automorphisms can be used to speed up the code analysis.

ii) In case, one is not interested in an invariant of minimal degree, one can choose w as the first element of an LLL-basis of $C_U^{\perp}$ that is not in $C_G^{\perp}$.

6.4. **First lifting step.** Naively, one would try to lift the invariant I_w to a $(U \subset G)$-invariant by applying the Reynolds operator. This would lead to a U-invariant consisting of $\#\phi_{\mathcal{B}}(G)$ summands. Further, it could degenerate to a G-invariant. We do the lifting in two steps to reduce the number of summands and to deal with the degeneration.

We compute $G_1 := \phi_{\mathcal{B}}^{-1}\mathrm{Stab}_{\phi_{\mathcal{B}}(G)}(w)$. This is the largest subgroup of G that acts on I_w by change of sign. In general, $U_1 := G_1 \cap U$ will act on I_w by change of sign, as well.

We compute the kernel of the U_1-action on I_w as the index 2 subgroup $U_{1,w}$. Note that $\ker(\phi_{\mathcal{B}}) \cap U_1 \subset U_{1,w}$. Thus, we can use the E-construction applied to the block system $\mathcal{B}$ to find a second relative invariant I_c for $U_{1,w} \subset U_1$. As G_1 acts on I_c in the same way as U_1, the combination of invariants applied to I_w and I_c will lead to a U_1-invariant that is not G_1-invariant. Summarizing, $I_p := I_w$ or the product $I_p := I_w I_c$ is a $(U_1 \subset G_1)$-invariant.

6.5. **Second lifting step.** Again, one would try to lift I_p to a $(U \subset G)$-invariant by using the Reynolds operator. This would lead to an invariant with $[G : G_1]$ summands. We can take it, in case it does not degenerate to a G-invariant.

At this point, we can add an optimization. We require that the word w in $C_U^{\perp} \setminus C_G^{\perp}$ has a $\phi_{\mathcal{B}}(G)$-orbit of minimal length.

Now, we have to treat the possibility of a degeneration. The group G_1 is the stabilizer of the variable sum $I_1 := \sum_{i,w_i=1} X_i$ in G. We can replace I_p by $I_p I_1^e$,

for any positive integer e. We claim that there is an

$$e \leq e_0 := \#\{i \mid w_i = 1\}(\deg(I_p) + 1)$$

that solves the degeneration problem. To prove this, it suffices to show that the polynomials $(I_p I_1^e)^\sigma, \sigma \in U//U_1$ are linearly independent.

Recall that monomials are linearly independent. Thus, it suffices to show that $(I_p I_1^{e_0})$ has at least one monomial that is not contained in any other summand. When we multiply out $I_1^{e_0}$, we find the summand $P := \prod_{i,w_i=1} X_i^{\deg(I_p)+1}$. When we look at σI_1 for $\sigma \in G \setminus G_1$, we replace at least one variable in I_1. Thus, a monomial in $\sigma I_p I_1^{e_0}$ will contain the factor P only in case $\sigma \in G_1$. □

6.6. **Remark.** In case of finite characteristics, the expression I_1^e may not contain the monomial we used in the proof. One way to solve this problem, is to replace I_1 by $\prod_{i,w_i=1} X_i$.

6.7. **Complexity.** The complexity of the invariant constructed will depend on the complexity of the invariant I_c and the number of summands generated in the second lifting step. The latter question is a coding theoretic problem.

To get an impression of what happens here, we enumerate all codes over $\mathbb{F}_2$ up to length 23 with a transitive automorphism group. This covers all the cases that may appear for polynomials up to degree 46. We end up with the following extreme examples.

i) The sum zero subspace of $\mathbb{F}_2^n$ is generated by the S_n orbit of $(1, 1, 0, \ldots, 0)$. It is of length $\binom{n}{2}$. In case n is even, shorter orbits can not generate this subspace.

ii) Let $G := \mathrm{Sym}(2) \wr \mathrm{Sym}(n)$ and consider the block system $\{\{1, 2\}, \ldots, \{2n - 1, 2n\}\}$. The orbit O of $(1, 0, 1, 0, \ldots, 0, 1, 0)$ is of length 2^n. It generates an $(n+1)$-dimensional subspace U. The complement of O in U is a n-dimensional subspace.

iii) Let $G := \mathrm{Sym}(4) \wr \mathrm{Sym}(n)$ with block system $\{\{1, 2, 3, 4\}, \ldots, \{4n - 3, 4n - 2, 4n-1, 4n\}\}$. The G-orbit of $\{4, 8, 12, \ldots, 4n\}$ is of length 2^{2n}. It spans a $(3n+1)$-dimensional subspace U. All elements of U with shorter orbits are contained in a $3n$-dimensional subspace.

To summarize, for permutation groups up to degree 46 with a block of size 2, we have an algorithm to generate invariants with at most 2048 summands. The extreme examples relate to permutation groups with a second block system of block size 4 or 8. It may be used to find simpler invariants for these cases.

6.8. **Example.** Let us inspect the groups

$$G = T_{30}^{4831} = (\mathbb{Z}/2\mathbb{Z})^{15} \rtimes \mathrm{Gl}(4, \mathbb{F}_2) = \mathrm{Sym}(2) \wr \mathrm{Gl}(4, \mathbb{F}_2) \subset \mathrm{Sym}(2) \wr \mathrm{Alt}(15)$$

and

$$H = T_{30}^{3819} = N \rtimes \mathrm{Gl}(4, \mathbb{F}_2) \subset G\,.$$

Here, N is the Hamming code in $\mathbb{F}_2^{15}$. We get $\#G = 660602880$ and $[G : H] = 16$. Recall the following description of the Hamming code.

i) $\mathbf{P}^3(\mathbb{F}_2)$ has 15 planes and 15 points.

ii) Each plane has 7 points and its complement has 8 points.

iii) We use the points of $\mathbf{P}^3(\mathbb{F}_2)$ as index set. I.e., we fix a bijection $\iota\colon \mathbf{P}^3(\mathbb{F}_2) \to \{1, \ldots, 15\}$.

iv) For each plane $E \subset \mathbf{P}^3(\mathbb{F}_2)$ we get the linear form $l_E := \sum_{P \in \mathbf{P}^3(\mathbb{F}_2) \setminus E} X_{\iota(P)}$.

v) N is the intersection of the kernel of the 15 linear forms l_E.

vi) The linear forms l_E are the non-zero words in the dual code of the Hamming code.

As the code analysis is done on the dual codes, it will inspect the trivial code as a subcode of the dual of the Hamming code. It will find one of the linear forms l_E of weight 8 as w. As there are 15 planes in $\mathbf{P}^3(\mathbb{F}_2)$, the stabilizer of l_E (resp. w) in $\mathrm{Gl}(4,\mathbb{F}_2)$ is of index 15. Thus, we end up with an invariant of degree 8 and 15 summands. It involves 105 multiplications.

6.9. **Remark.** The main advantage of the coding theoretic approach is that we can compute the auxiliary group as the stabilizer of a code word. This leads to the following question for groups with a block of size bigger than 2: Can more general codes (i.e., codes over different rings) be used to construct the auxiliary group more efficiently than this is done by searching in the subgroup lattice?

7. Invariants for intransitive groups

7.1. **Remark.** At a first glance, invariants for intransitive groups seem to be necessary only, when one wants to compute Galois groups of reducible polynomials. However, several of the constructions above may recursively construct intransitive subgroups and need invariants to handle them.

7.2. **Subdirect products.** Let $G \subset G_1 \times G_2 \subset \mathrm{Sym}(n) \times \mathrm{Sym}(m)$ be intransitive groups. We denote the projections of G to G_1 and G_2 by π_1 and π_2. In case one of the projections is not surjective, one can use this projection to get a G-invariant that is not $G_1 \times G_2$ invariant.

The interesting case is that both projections are surjective. Then G is called a *subdirect product* of G_1 and G_2.

The main theorem of subdirect products gives us two surjective homomorphisms $\phi_i \colon G_i \to H$ such that

$$G = \{(g_1, g_2) \in G_1 \times G_2 \mid \phi_1(g_1) = \phi_2(g_2)\}\,.$$

In [6, Sec. 3], we used this theorem to construct relative invariants by using linear representations.

Here, we will explain how to do this by using permutation representations.

7.3. **Construction.** Let a subdirect product $G \subset G_1 \times G_2$ be given.

i) Compute the kernel of ϕ_1 as $K_1 := \pi_1(G \cap (G_1 \times \{\mathrm{id}_{G_2}\}))$.

ii) Find a subgroup $U_1 \subset G_1$ of minimal index such that the kernel of the coset action coincides with K_1.

iii) Put $U_2 := \pi_2(G \cap (U_1 \times G_2))$.

iv) Choose ϕ_i as the coset action on U_i.

v) Construct relative invariants I_i for $U_i \subset G_i$.

vi) Chose univariate polynomials T_1, T_2, randomly.

vii) Compute the G-invariant $I := \sum_{\sigma \in G//G\cap(U_1\times G_2)} T_1(I_1)^\sigma T_2(I_2)^\sigma$.

viii) In case I is a relative invariant, return I. Otherwise, try with other transformations T_1, T_2.

7.4. **Remarks.**
i) The complexity of the invariant depends on the index $[G_1 : U_1]$. It would be very helpful to have an algorithm available that yields a fast construction of a subgroup U_1 of minimal index. For transitive groups of moderate degree, a naive scan of the subgroup lattice works. Table 3 gives an overview of the minimal degrees of transitive permutation representations of all non-trivial quotients of transitive groups in degree n.

n	Degree of quotient	n	Degree of quotient
3	2	4	4
5	4	6	6
7	6	8	16
9	9	10	10
11	10	12	30
13	12	14	14
15	15	16	128
17	16	18	32
19	18	20	128
21	21	22	22
23	22		

Table 3 – Degrees occuring for representations of subquotients of $\mathrm{Sym}(n)$

In case we are interested in intransitive permutation representations of the quotients, we have to deal with orbits up to length 90. The extreme examples are given the quotients $G/Z(G)$ for $G := \mathrm{Sym}(2) \wr \mathrm{Sym}(2k)$.

ii) The effect of the transformation polynomials T_i can be explained by inspecting the linear representation of the G_i on $\mathrm{span}\{I_i^\sigma \mid \sigma \in G_i\}$. In case both representations are of dimension $[G_1 : U_1]$, we are exactly in the situation of [6, 3.3, 3.4]. If this representation is of smaller dimension than expected, we only get quotients of the expected linear representations. However, there are always transformations T_1, T_2 that result in linear representations of the expected dimensions.

8. Relative invariants for non-maximal subgroups

The above constructions focus on the case of maximal subgroups. However, the recursion may require relative invariants for non-maximal subgroups $U \subset G$ of small index. A solution for this is as follows.

First, we compute all the minimal over-groups Z_i of U in G. Then, we compute relative invariants I_i for $U \subset Z_i$. In case, the base ring has infinitely many elements, there is a linear combination of the I_i that is a G-relative U-invariant. To construct it, one can form random linear combinations of the I_i and check by evaluation that each Z_i has an element that does not stabilize it.

9. Timings, tests, and examples

All tests are done on one core of an Intel i7-3770 CPU with 3.4GHz running magma 2.20.

9.1. **Test on irreducible polynomials.** For each transitive permutation group in degree 16,18, 20, and 21 we picked one irreducible polynomial out of the database [12]. These are 1954, 983, 1117, resp. 164 test cases. We can compute all these Galois groups in 1359, 444, 1227, resp. 227 seconds.

The example $x^{20} - 308x^{16} + 33396x^{12} - 1554608x^8 + 28579232x^4 - 113379904$, cf. [7, Sec. 8], can be done in 0.85 seconds. Using MAGMA 2.18 on the same machine, it takes 47 seconds.

In higher degrees, we can not do a systematic test with polynomials, as there is no complete database available for polynomials of degree ≥ 24. Table 4 lists a few examples.

polynomial	MAGMA 2.18	MAGMA 2.20	group
$x^{21} + x^3 + 8 \in \mathbb{Q}[x]$	1.1 sec	0.7 sec	T_{21}^{138}
$x^{24} + x^3 + 8 \in \mathbb{Q}[x]$	1.5 sec	1.2 sec	T_{24}^{24648}
$x^{24} + x^4 + 16 \in \mathbb{Q}[x]$	54 sec	2.0 sec	T_{24}^{21844}
$x^{27} + x^3 + 8 \in \mathbb{Q}[x]$	impossible	2.4 sec	T_{27}^{2357}
$x^{28} + x^4 - 16 \in \mathbb{Q}[x]$	impossible	3.2 sec	T_{28}^{1610}
$x^{30} + x^3 + 8 \in \mathbb{Q}[x]$	impossible	3.8 sec	T_{30}^{5396}
$x^{24} + x + t \in \mathbb{F}_2(t)[x]$	impossible	12.5 sec	M_{24}

Table 4 – Test polynomials and computation time

Impossible means that MAGMA reaches the memory limit of 10GB.

9.2. **Testing with the group database.** The database [2, 10] of transitive permutation groups is available up to degree 32. For all groups up to degree 30 in the database, we computed its maximal subgroups and searched for relative invariants. This enumeration took 2.5 hours. Most of the time was spent to treat the 25000 transitive groups in degree 24. All the other cases were done within 21 minutes.

For the Galois group computation, the number of multiplications for an evaluation and the polynomial degree of the invariant determine the costs. The Δ-invariant of degree $\binom{n}{2}$ for $\mathrm{Alt}(n) \subset \mathrm{Sym}(n)$ is of minimal degree. Thus, in degree 30 we have to handle invariants of degree 435. In theory, a larger degree is never necessary but the BlockQuotient-construction may result in invariants of larger degree.

Table 5 shows the maximal number of multiplications used and the largest polynomial degree of the invariants found for the transitive subgroups in degree $n = 3, \ldots, 30$.

The hardest case in degree 26 is an index 2 subgroup of $\mathrm{P\Gamma l}_2(\mathbb{F}_{25}) \subset \mathrm{Sym}(26)$. Here, none of the new constructions applies. Thus, the generic invariant algorithm [7, Sec. 4] has to be used. It results in a degree 5 invariant that involves 14735 multiplications.

The action on 2-sets of $\mathrm{Alt}(8) \subset \mathrm{Sym}(8)$ leads to primitive subgroups in $\mathrm{Sym}(28)$. Again, only a generic invariant of degree 6 with 14123 multiplications is found for this index 2 example. Because of this invariant, the computation of the Galois group $A_8 \subset \mathrm{Sym}(28)$ of a test polynomial takes 4.5 seconds. Of course, one could easily map back to the degree 8 representation and use the invariant Δ. However, this is not yet implemented.

n	multiplications	deg(invariant)	n	multiplications	deg(invariant)
3	2	3	4	5	6
5	15	10	6	35	10
7	20	21	8	159	28
9	542	36	10	760	45
11	264	55	12	660	66
13	77	78	14	364	91
15	436	105	16	2653	120
17	4040	136	18	2900	216
19	170	171	20	2811	190
21	306	210	22	1540	231
23	1012	253	24	9252	792
25	5952	300	26	14735	325
27	4733	351	28	14123	378
29	405	406	30	5224	600

Table 5 – Largest number of multiplications and degrees

In degree 32, we have 2801324 transitive groups in the data base. The NewBlock-, E-, F-, and BlockQuotient-constructions fail only for subgroups of 2154 groups. This results in 12990 pairs $U \subset G$. For 4074 of them, the action on pairs results in an invariant as a new orbit or a new block system comes up. In 8639 cases, we have a minimal block system of size 2. Here, the coding theoretic approach works. Only four of the remaining 277 pairs of groups result in generic invariants.

One example is $T_{32}^{2713815}$ of order $2^{17} \cdot 3^2 \cdot 7$ with an index 8 subgroup. These groups have exactly one block system with block size 8. Another example are the groups $A\Gamma l_1(\mathbb{F}_{2^5}) \subset \mathrm{ASl}_5(\mathbb{F}_2)$ of index 64512. Here, the generic invariants used involve up to 50000 multiplications.

References

[1] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (1997), 235–265

[2] J. Cannon, D. Holt: The transitive permutation groups of degree 32. Experiment. Math. **17** (2008), no. 3, 307–314.

[3] H. Cohen: A course in computational algebraic number theory. Springer-Verlag, Berlin 1993.

[4] H. Derksen, G. Kemper: Computational invariant theory. Springer-Verlag, Berlin, 2002.

[5] J. Dixon, B. Mortimer: Permutation groups. Springer-Verlag, New York 1996.

[6] A.-S. Elsenhans: Invariants for the computation of intransitive and transitive Galois groups, Journal of Symbolic Computation **47** (2012) 315–326.

[7] J. Klüners, C. Fieker: Computation of Galois Groups of rational polynomials, Preprint 2012

[8] K. Geißler: Berechnung von Galoisgruppen ber Zahl- und Funktionenkörpern, Dissertation, Berlin, 2003.

[9] K. Geißler,J. Klüners: Galois group computation for rational polynomials. In: Algorithmic Methods in Galois Theory. J. Symbolic Comput. **30** (2000) no. 6, 653–674.

[10] A. Hulpke: Constructing transitive permutation groups. J. Symbolic Comput. **39** (2005), no. 1, 1–30

[11] B. Huppert: Endliche Gruppen. I. Springer-Verlag, Berlin-New York 1967

[12] J. Klüners: Database of number fields. `http://galoisdb.math.upb.de/`

[13] R. Stauduhar: The determination of Galois groups. Math. Comp. **27** (1973), 981 – 996.