IMPROVED METHODS FOR THE CONSTRUCTION OF RELATIVE INVARIANTS FOR PERMUTATION GROUPS

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. This article reports on the constructions that are implemented in the Galois group package of MAGMA 2.20.

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 had an a priori degree limitation. In [8], such an algorithm is described for irreducible polynomials up to degree 23. As there are 25000 transitive permutation groups in degree 24, it is clear that any extension that follows the old path will get huge. Thus, for a degree independent implementation, one has to compute 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.

Outline of the Galois group algorithm. The basic idea of the algorithm was given by Stauduhar [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 want to construct a path in the subgroup lattice of $\mathrm{Sym}(n)$ that starts at G_1 and ends at the Galois group. For this, we compute the conjugacy classes of maximal subgroups of G_1.

For each maximal subgroup class representative U, we compute a *relative invariant polynomial* $I \in \mathbb{Z}[X_1, \ldots, X_n]$, 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 invariant to be distinct, one can show that the Galois group is contained in $\sigma U \sigma^{-1}$ if and only if 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 reached.

The bottleneck of the implementation. The main limiting bottleneck of the implementation described in [7] is the complexity of the invariants. If an 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 and many in higher degrees with practical invariants.

As we want to study the improvements of the latest MAGMA implementation, we first give an overview of what was implemented in earlier versions.

Generic invariants. It is a well known fact [4, Sec. 3.10] that the ring of invariants of a permutation group is generated by orbit sums of monomials. To turn this into an algorithm for relative invariants, one has to find a monomial m, such that the U-orbit and the G-orbit of m are different. A method to construct such a monomial with minimal degree is described in [7, Sec. 4].

In theory, this approach solves the problem. In practice, for many pairs of groups, this algorithm results in impractical invariants.

Special invariants. The general idea to overcome the above bottelneck is the use so called special invariants. This means, we try to find a structural difference between the two permutation groups that can be used as a starting point to construct an invariant. Usually, this results in an invariant that is by far simpler than the result of the orbit sum approach.

For example, in the case that the group G is not contained in the alternating group $\mathrm{Alt}(n)$ and U is the intersection $G \cap \mathrm{Alt}(n)$, a relative invariant for $U \subset G$ is given by

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

This is called the SqrtDisc-construction. Note that the different ways of writing down the invariant result in evaluation algorithms of different complexity. Here, the best choice is to work with the product representation.

In MAGMA 2.18 the ProdSum-, SqrtDisc-, and Sm-construction are tried to write down a special invariant directly. In the case that this does not apply, the E-, F- and BlockQuotient-constructions are tried to build a relative invariant out of invariants for groups of smaller degree [7, Sec. 5].

In the case that non of these constructions apply, MAGMA 2.18 used the generic approach.

Our starting point. We can overcome the bottleneck by adding further constructions of special invariants, which can be tried when the old constructions fail. Thus, this investigation started with a systematic analysis of those pairs of groups that had to be treated by the generic approach.

To understand the failure, we first have to describe the old special invariants in detail. Using the groups in the database of transitive permutation groups [2, 10], we can study such examples. To describe some examples, we will use the notation T_n^k for the k-th transitive group of degree n in the database.

In the example above, U is a maximal subgroup of G. When we give constructions for relative invariants, we always assume that the subgroup is maximal except when non-maximal subgroups are explicitly included.

The new overall strategy. Given a permutation group g and a maximal subgroup u, the Galois group package of MAGMA performs the following steps and uses the invariant that is found first.

(1) If u has more orbits than g then use the sum of variables on a new orbit as the invariant.
(2) Try the FactorDelta construction (see 4.6).
(3) In the case that the group is intransitive, find a minimal set of orbits such that the actions on these differ. If this results in a transitive representation, apply the overall strategy to it. Otherwise, use the method for subdirect products (see 9).
(4) Try the NewBlock-constuction (see 2.3).
(5) Try the E- and the F-construction (see 2.3).
(6) Try the BlockQuotient-construction (see 3.2).
(7) Try the transfer-construction with a small index limit for the subgroup search (see 5.6).
(8) Try to derive a simple invariant from the action on 2-sets (see 7.1).
(9) In the case that G has a a block-system of block size 2 or 3, use the code based construction given in section 6.
(10) In the case of a primitive group, try the constructions listed in section 8.
(11) Use the generic orbit-sum of monomial approch [7, Sec. 4] to definitively get a relative invariant.

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. If

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

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

When B is a singleton or $\{1, \ldots, n\}$, we get a 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 of G. We denote it by $\phi_{\mathcal{B}}$.

2.2. **Remarks.**

(1) The size of a block is a divisor of the degree of the permutation group. Thus, all groups of prime degree are primitive.
(2) However, most transitive permutation groups have block systems. For example, only five out of the 25000 transitive permutation groups in degree 24 are primitive.
(3) The maximal permutation group with a block system such that the action in one block is given by $A \subset \mathrm{Sym}(k)$ and the action on the block system is given by $B \subset \mathrm{Sym}(l)$ is called the wreath product $A \wr B \subset \mathrm{Sym}(kl)$. It is isomorphic to the semi-direct product $A^l \rtimes B$. The action of B on A^l is given by permuting the components.

2.3. **Wreath product type constructions .** Let U be a maximal and transitive subgroup of $G \subset \mathrm{Sym}(n)$. If U is a subgroup of a non-trivial wreath product in $\mathrm{Sym}(n)$ that does not contain G then 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: If $\{B_1, \ldots, B_k\}$ is a block-system for U, but not for G, then the following are relative invariants

$$\sum_{i=1}^{k} (\sum_{j \in B_i} X_j)^2, \text{ if } \mathrm{char}(K) \neq 2,$$
$$\sum_{i=1}^{k} (\sum_{j \in B_i} X_j)^3, \text{ if } \mathrm{char}(K) \neq 3,$$
$$\sum_{i=1}^{k} (\prod_{j \in B_i} X_j), \ \prod_{i=1}^{k} (\sum_{j \in B_i} X_j), \text{ in general.}$$

Because of the last invariant, this was called the *ProdSum-construction.*

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. **Examples.**

(1) Let $K_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle \subset D_8 := \langle (1,3), (1,2,3,4) \rangle$ be the Klein four-group as a subgroup of the dihedral group of order 8. D_8 has exactly one system of blocks $\{\{1,3\},\{2,4\}\}$ whereas K_4 has the additional blocksystems $\{\{1,2\},\{3,4\}\}$ and $\{\{1,4\},\{2,3\}\}$. Any of these new blocksystems can be used to write down a relative invariant. E.g.,

$$I_1 := X_1X_2 + X_3X_4 \text{ or } I_2 := (X_1 + X_4)(X_2 + X_3) \, .$$

Furthermore, K_4 is an even permutation group but D_8 is not. Thus, the SqrtDisc-construction would apply as well and result in the invariant

$$I_3 := (X_1 - X_2)(X_1 - X_3)(X_1 - X_4)(X_2 - X_3)(X_2 - X_4)(X_3 - X_4) \, .$$

(2) Let $G := T_6^{11} = \langle (1,2), (1,3)(2,4), (3,5)(4,6) \rangle = \mathrm{Sym}(2) \wr \mathrm{Sym}(3)$ and $U := T_6^6 = \langle (1,2), (1,3,5)(2,4,6) \rangle = \mathrm{Sym}(2) \wr \mathrm{Alt}(3) \subset G$ be two permutation groups. They only have the blocksystem $\mathcal{B} := \{\{1,2\},\{3,4\},\{5,6\}\}$. The structural difference between the two groups is that the action $\phi_{\mathcal{B}}$ on the

blocksystem results in the full symmetric group for G, but in the alternating group for U. Thus, the E-construction applies. It results in the invariant

$$\begin{aligned} I &:= ((X_1+X_2)-(X_3+X_4))\cdot((X_1+X_2)-(X_5+X_6))\cdot \\ &\quad ((X_3+X_4)-(X_5+X_6))\,, \end{aligned}$$

when we start with the invariant $(Y_1-Y_2)(Y_1-Y_3)(Y_2-Y_3)$ for the $\phi_{\mathcal{B}}$-images $\mathrm{Alt}(3)\subset\mathrm{Sym}(3)$.

(3) Let $G := T_6^9 = \langle (1,2,3),(1,2)(4,5),(1,4)(2,5)(3,6)\rangle \subset \mathrm{Sym}(3)\wr\mathrm{Sym}(2)$ and $U := T_6^5 = \langle (1,2,3),(1,4)(2,5)(3,6)\rangle = \mathrm{Alt}(3)\wr\mathrm{Sym}(2)\subset G$ be two permutation groups. They only have the block system $\{\{1,2,3\},\{4,5,6\}\}$.

The structural difference between the two permutation groups is that the stabilizer of one block results in an $\mathrm{Sym}(3)$-action (if we start with G) and in an $\mathrm{Alt}(3)$-action (if we start with U) on the block stabilized. Thus, these block-stabilizer groups have the relative invariant

$$I_0 := (X_1-X_2)(X_1-X_3)(X_2-X_3)\,.$$

The F-construction lifts this to

$$\begin{aligned} I &:= I_0 + (1,4)(2,5)(3,6)\cdot I_0 \\ &= (X_1-X_2)(X_1-X_3)(X_2-X_3) + \\ &\quad (X_4-X_5)(X_4-X_6)(X_5-X_6)\,. \end{aligned}$$

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

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

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

Here, $U//H$ denotes a list of coset representatives of U/H. It may happen that the result degenerates. For example, if H is an index 2 subgroup of U and U acts on f by change of sign then we get $R_{U/H}(f)=0$. 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.

2.6. **A lemma . 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 a 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 (not necessarily maximal) 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 the case that the construction does not degenerate, we get a relative invariant. In case of degeneration, we replace the $(H \subset G)$-relative invariant I by $t(I)$ for a random univariate polynomial t [8, Bemerkung 6.19].

3.2. **The BlockQuotient-Construction.** In this generality, it is not clear which choice of the auxiliary group H results in a simplification of the problem. Placing the block systems in the center of our focus, one could try to simplify the action of a block stabilizer on the block stabilized. This results in the so called BlockQuotient-construction. The formal description is as follows:

(1) For each block system $\mathcal{B} = \{B_1, \ldots, B_k\}$ of G of block size at least 3, compute the stabilizer $S := \mathrm{Stab}_G(B_1)$. Denote by π the action of S on B_1.
(2) Compute the subgroups of $\pi(S)$ of index $2, \ldots, \#B_1 - 1$.
(3) For each subgroup $T \subset \pi(S)$ found, take its preimage $H := \pi^{-1}(T)$.
(4) If $\phi_{G/H}(U) \neq \phi_{G/H}(G)$ then return (B_1, π, H, S) as the initial data for the construction.

In the case that an initial block B_1 and a subgroup H are found, one continues as follows:

(1) Compute a relative invariant I_0 for $\pi(H) \subset \pi(S)$. This is automatically a relative invariant for $H \subset G$.
(2) Compute a relative invariant I_1 for $\phi_{G/H}(U) \subset \phi_{G/H}(G)$.
(3) To piece these two invariants together, we have to find at random a univariate polynomial t such that
$$I := I_1(t(\sigma_1 I_0), t(\sigma_2 I_0), \ldots, t(\sigma_k I_0))$$
is a relative invariant for $U \subset G$. Here, $\sigma_1, \ldots, \sigma_k$ denote coset representatives of $H \subset G$.

3.3. **Remarks.**

(1) The index limit $\#B_1 - 1$ for the subgroup search is somewhat random. It means that the new permutation representation $\phi_{G/H}(G)$ has a smaller degree than G. This ensures that the algorithm does not run into an infinite recursion when searching for a relative invariant for $\phi_{G/H}(U) \subset \phi_{G/H}(G)$. Any other subgroup selection strategy that does not result in infinite recursions could be used as well.
(2) We exclude block systems of block size 2 from the inspection, because the block-action would result in $\pi(S) = \mathrm{Sym}(2)$. Choosing $T = \{\mathrm{id}\}$ would result in $\phi_{G/H} = \mathrm{id}_G$. Choosing $T = \mathrm{Sym}(2)$ would result in $\phi_{G/H} = \phi_{\mathcal{B}}$. Thus, either this does not lead to a simplification or we get back to the E-construction.
(3) The proof that I is not a G-invariant can be done by evaluation. This means that, for some random numbers $r_1, \ldots, r_n$ and all the generators σ

of G, we test whether

$$I(r_1, \ldots, r_n) = I(r_{\sigma(1)}, \ldots, r_{\sigma(n)})\,.$$

If this equality fails at least once then we have confirmed that I is not G-invariant.

3.4. **Interpretation.**

(1) 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 a 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 $[L_1 : K] < [L : K]$. 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 $\mathbb{Q} \subset K := \mathbb{Q}[a] \subset L := \mathbb{Q}[\sqrt[n]{a}]$, for $L_1 := K[\zeta_n]$ and $\mathbb{Q} \subset K := \mathbb{Q}[a] \subset L := \mathbb{Q}[\sqrt[16]{a}]$ for $L_1 := \mathbb{Q}[\sqrt{a}]$ or $L_1 := \mathbb{Q}[\sqrt[4]{a}, \sqrt{-1}]$.

(2) In the category of permutation groups, the BlockQuotient-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

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

In the notation 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. **Example.** Let $G := T_8^{45} = \langle (1,4)(5,8), (1,5,2,6,3,7)(4,8)\rangle = \mathrm{Sym}(4) \wr \mathrm{Sym}(2) \cap \mathrm{Alt}(8)$ be a permutation group and $U := T_8^{41} = \langle (1,4)(5,8), (1,8,3,7,2,5)(4,6)\rangle$ be an index 3 subgroup. The SqrtDisc-, NewBlock-, E-, and F-constructions do not apply to this pair of groups.

The BlockQuotient-construction starts with the homomorphism $\phi\colon \mathrm{Sym}(4) \to \mathrm{Sym}(3)$ that is given by the coset action on a 2-Sylow subgroup. This induces a homomorphism $\Phi\colon G \to \mathrm{Sym}(3) \wr \mathrm{Sym}(2)$. The image $\Phi(G)$ is the transitive group T_6^9 and $\Phi(U) = T_6^3$.

Now, we need relative invariants for the 2-Sylow subgroup of $\mathrm{Sym}(4)$ as a subgroup of $\mathrm{Sym}(4)$ and another one for $T_6^3 \subset T_6^9$. In both cases, the smaller group has more block systems than the bigger one. Thus, the NewBlock-construction applies. This gives us the invariants

$$I_0 := X_1X_2 + X_3X_4 \quad \text{and} \quad I_1 := Y_1Y_2 + Y_3Y_4 + Y_5Y_6\,.$$

The BlockQuotient-construction composes them to the relative invariant

$$\begin{array}{rcl} I & := & (X_1X_2 + X_3X_4)(X_5X_6 + X_7X_8) + \\ & & (X_1X_3 + X_2X_4)(X_5X_7 + X_6X_8) + \\ & & (X_1X_4 + X_2X_3)(X_5X_8 + X_6X_7) \end{array}$$

for $U \subset G$. Thus, in this case we can choose $t(X) := X$.

3.6. **Statistics.** We used the database of transitive groups 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	16	25
9	78	40	8	30
10	100	66	12	22
12	1083	795	191	97
14	149	97	18	34
15	264	171	55	38
16	12533	9613	2327	593
18	4189	3217	866	106
20	4856	3448	984	424
21	500	301	149	50
22	134	97	18	19
24	178753	135464	41087	2202
25	660	379	112	169
26	261	170	64	27
27	12964	8558	2469	1937
28	8293	5775	1555	963
30	28012	20505	7004	503
32	53804069	46347960	7443119	12990

TABLE 1 – Number of pairs of groups $U \subset G \subset \mathrm{Sym}(n)$ covered, prime degrees omitted

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

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

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 $\{\pm(X_i - X_j) \mid 1 \le i < j \le n\}$. Thus, the action of $\mathrm{Sym}(n)$ on the set above can be viewed as signed permutations or as a $\binom{n}{2}$-dimensional monomial representation of $\mathrm{Sym}(n)$.

From this, we derive that the action on

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

results in a one-dimensional representation.

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

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

If this representation is not trivial then its kernel is an index two subgroup of G, for which we have an invariant.

4.3. **Remark.** The Sm-construction listed in the introduction is a special case of this. It corresponds to the orbit of $\{1,2\}$ by $\mathrm{Sym}(k) \wr \mathrm{Sym}(m)$.

4.4. **Remarks.**

(1) The construction above can easily be combined with the idea of the E-construction. This means, we take the action of G on a system of blocks $\mathcal{B} = \{B_1, \ldots, B_k\}$ and decompose the 2-sets of blocks

$$\{\{B_i, B_j\} | 1 \le i < j \le k\}$$

into G-orbits. Now an orbit on 2-sets of blocks results in the 1-dimensional representation, given by the action on

$$I := \prod_{(i,j)\in J} \left(\sum_{k\in B_i} X_k - \sum_{k\in B_j} X_k \right) .$$

Here, J is an index set encoding the orbit $\{\{B_i, B_j\} : (i,j) \in J\}$ on 2-sets of blocks. This representation is either trivial or its kernel is an index 2 subgroup with relative invariant I.

(2) It may happen that several representations have the same kernel. This can be explained by the following fact:

Let $B_j := \{(j-1)k+1, \ldots, jk\}$ and $\{B_1, \ldots, B_m\}$ be a system of blocks for the permutation group G. Further, we denote by

$$\pi \colon \{1, \ldots, km\} \to \{1, \ldots, m\}$$

the projection that maps each element to the number of the block it is contained in. I.e., $i \in B_{\pi(i)}$ for all $i = 1, \ldots, km$.

Denote by J_1 an index set of the G-orbit of $\{1, k+1\}$ and by J_2 an index set of the G-orbit of $\{B_1, B_2\}$. Then the representations given by

$$I_1 := \prod_{(i,j)\in J_1} (X_i - X_j) \text{ and } I_2 := \prod_{(i,j)\in J_2} \left(\sum_{\in B_i} X_l - \sum_{l\in B_j} X_l \right)$$

are either equal to each other or I_1 corresponds to the trivial representation.

Proof: We have the subgroups

$$U_1 := \mathrm{Stab}(\{1, k+1\}) \subset U_2 := \mathrm{Stab}(\{1, \ldots, 2k\}) \subset G .$$

We can identify J_1 with a transversal of G/U_1 and J_2 with a transversal of G/U_2. Thus, the pairs $\{i,j\}$ $((i,j) \in J_1)$ hit each pair of blocks in $\{\{B_i, B_j\} : (i,j) \in J_2\}$ equally often.

We have to count how many factors of the products are mapped to factors with the sign opposite to that occurring. An element $\sigma \in G$ maps

the factor $X_i - X_j$ ($(i,j) \in J_1$) to one of the sign opposite to that occurring if and only if the blocks $B_{\pi(i)}, B_{\pi(j)}$ are not in order. I.e., if $\pi(i) - \pi(j)$ and $\pi(\sigma(i)) - \pi(\sigma(j))$ differ in sign.

The latter sign changes are the changes in sign that describe the action of σ on I_2. Thus, the number of sign changes in the product representation of I_1 is the $[U_2 : U_1]$-multiple of the one in I_2. If this multiplicity is odd, then the representations are equal. If the multiplicity is even, then I_1 is the trivial representation. □

(3) The statement proved can be used to speed up the construction of invariants, as we can skip the treatment of I_1. It will be either trivial or I_2 will result in the same representation. Indeed, the degree of I_2 will be at most equal to the degree of I_1.

4.5. **Combining invariants .** Given two 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 product representation.

4.6. **The FactorDelta-construction .** Combining the constructions listed above, we get the FactorDelta-construction, which works as follows.

Let a subgroup $G \subset \mathrm{Sym}(n)$ be given. Then we perform the following steps to find invariants for index 2 subgroups of G:

(1) Compute all orbits of G and all block systems of each orbit.
(2) List transitive representations of G by taking the actions on orbits and on block systems.
(3) For each transitive representation found, compute the orbits of the action on 2-sets.
(4) For each orbit on 2-sets found, compute the 1-dimensional representation of G, as described above.
(5) Compute the kernel of each representation.
(6) Delete all the trivial representations found.
(7) In the case that two representations have the same kernel, pick the simpler one.
(8) For each pair of representations found, apply construction 4.5 to get a third representation having another index 2 subgroup as its kernel.
(9) In the case that a representation with this kernel is already known, pick the one with the simpler polynomial.
(10) Iterate construction 4.5 until no further representations are found.
(11) Return the list of 1-dimensional representations found together with the list of the kernels.

4.7. **Example.** Let $D_8 = T_4^3 = \langle (1,2),(1,3,2,4)\rangle$ be the dihedral group of order 8. It has the Klein four-group K_4 and the cyclic group C_4 as maximal transitive subgroups. The above constructions give us two 1-dimensional representations by the action on

$$I_1 := (X_1 + X_2) - (X_3 + X_4) \quad \text{and} \quad I_2 := (X_1 - X_2)(X_3 - X_4)\,.$$

The Klein four-group is the kernel of I_2 and C_4 is the kernel of $I_1 I_2$.

5. Using monomial representations and transfer

5.1. **Recall .**

(1) A matrix is called monomial if each row and each column have exactly one non-zero entry.
(2) A matrix group is called monomial if all elements are monomial matrices.
(3) A representation is called monomial if its image is a monomial group.
(4) For a field K, the group of $n \times n$ monomial matrices $N_n(K)$ is isomorphic to $(K^*)^n \rtimes \mathrm{Sym}(n)$.
(5) The monomial group has a 1-dimensional representation given by the determinant and a second one given by the sign of the permutation in $\mathrm{Sym}(n)$.
(6) 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.
(7) More generally, each group with a monomial representation has these three 1-dimensional representations associated to the monomial representation.
(8) 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 the case that the monomial representation is given as $\mathrm{Ind}_U^G(\phi)$ for a 1-dimensional representation ϕ, we call the tensor product in 5.1.6. 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-dimensional 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.**

(1) Consider the wreath product $G = G_1 \wr G_2$. In the case that G_1 is not cyclic, one would like to start with a more interesting 1-dimensional representation ϕ (i.e., a quotient) of G_1. 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.

(2) 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 a relative invariant for $U \subset G$, we can lift that with the Reynolds operator to a relative invariant for $U_0 \subset G_0$.

5.6. **Algorithm .** The considerations above result in the following construction for a relative invariant of $U_0 \subset G_0$.

(1) Let G run through all transitive subgroups of small index of G_0. Start with G_0 itself as an index 1 subgroup.
(2) Compute a representing block for each block system of G.
(3) For each representing block B, compute the block stabilizer $\mathrm{Stab}_B(G)$.
(4) Test whether the action $\phi\colon \mathrm{Stab}_B(G) \to \mathrm{Sym}(B)$ has cyclic image.
(5) If the image is cyclic, then compute the kernel U of the ϕ-transfer.
(6) If $U = U_0 \cap G$ then construct a relative invariant I of $U \subset G$ as the product above.
(7) Apply the Reynolds operator the convert I into a U_0-invariant I_0.
(8) If I_0 is not a G_0-invariant then return I_0.

5.7. **Remarks.**

(1) In this generality, it is not clear which strategy to pick low index subgroups is optimal. Further, the restriction to transitive groups is somehow artificial. In the next section, we will give another algorithm that computes G directly. In contrast to the above approach, it can result in intransitive groups but it works only for block size 2 or 3.
(2) In the case that the subgroups G or $U_0 \cap G$ that are inspected in the algorithm above have even more blocksystems than G, one might try the other block system based constructions (e.g. E- or the F-constriction) on these block systems to get an invariant for $U \subset G$, in addition to the transfer approach.

5.8. **Examples.**

(1) We denote by K the group

$$\{(\sigma_1, \ldots, \sigma_{10}) \in \mathrm{Alt}(3)^{10} \mid \sigma_1 \cdots \sigma_{10} = \mathrm{id}\} \subset \mathrm{Alt}(3)^{10}\,.$$

Using this notation, we inspect the groups $U_0 := T_{30}^{5396}$, $G_0 := T_{30}^{5421}$,

$$\begin{aligned} T_{30}^{5396} &= (K \rtimes \mathrm{Sym}(10)) \rtimes \mathbb{Z}/2\mathbb{Z} \\ &\subset T_{30}^{5421} = (\mathrm{Alt}(3) \wr \mathrm{Sym}(10)) \rtimes \mathbb{Z}/2\mathbb{Z}\,. \end{aligned}$$

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 the transfer construction. It is given by

$$I := (X_1 + \zeta_3 X_2 + \zeta_3^2 X_3) \cdots (X_{28} + \zeta_3 X_{29} + \zeta_3^2 X_{30})\,.$$

Finally, the Reynolds operator lifts this to the relative invariant

$$I_0 := I + \sigma I \ (\sigma = (1,2)(4,5)\cdots(28,29))$$

for the initial groups. The decomposition of the invariant into components leads to an invariant with an evaluation algorithm that involves 103 multiplications over the base field.

(2) 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

$$U_2 := \{(x_1, \dots, x_7) \in (\mathbb{Z}/4\mathbb{Z})^7 \mid \sum x_i = 0 \bmod 2\} \rtimes \mathbb{Z}/2\mathbb{Z},$$

and

$$U_4 := \{(x_1, \dots, x_7) \in (\mathbb{Z}/4\mathbb{Z})^7 \mid \sum x_i = 0 \bmod 4\} \rtimes \mathbb{Z}/2\mathbb{Z}\,.$$

As U_2 and U_4 are $\mathrm{Sym}(7)$ 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 the invariant

$$(X_1 + \zeta_4 X_2 - X_3 - \zeta_4 X_4) \cdots (X_{25} + \zeta_4 X_{26} - X_{27} - \zeta_4 X_{28})$$

for $T_{28}^{1541} \subset T_{28}^{1601}$, which 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.

6. Invariants in case of a block system of block size 2 or 3

6.1. **Setup.** Let $U \subset G$ be a maximal subgroup of a transitive permutation group of degree $n = 2k$ with the block system $\mathcal{B} = \{\{1,2\},\{3,4\},\dots,\{2k-1,2k\}\}$. 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 will not apply to this block-system. Table 2 gives an overview of the number of transitive groups having such a block system.

Now, we describe the construction of the relative invariant as a 3-step process.

6.2. **Step 1: 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 this 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

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

From this, we can easily write down a $U \cap \ker(\phi_{\mathcal{B}})$-invariant that is not a $\ker(\phi_{\mathcal{B}})$-invariant. Even better, we can construct one of minimal degree as follows:

(1) Write $U \cap \ker(\phi_{\mathcal{B}})$ and $\ker(\phi_{\mathcal{B}})$ as subgroups of $(\mathbb{Z}/2\mathbb{Z})^k$.
(2) View these groups as $\mathbb{F}_2$-codes $C_U \subsetneq C_G \subset \mathbb{F}_2^k$.
(3) Compute the dual codes $C_G^\perp \subsetneq C_U^\perp$.
(4) Find a word w of minimal weight in $C_U^\perp \setminus C_G^\perp$.
(5) Return $I_w := \prod_{i,w_i=1}(X_{2i-1} - X_{2i})$ as an invariant of U_0 that is not G_0 invariant.

Degree	# groups	#2, #3, # 2 or 3
4	5	3, –, 3
6	16	8, 7, 12
8	50	36, –, 36
9	34	–, 23, 23
10	45	21, –, 21
12	301	182, 106, 255
14	63	37, –, 37
16	1954	1754, –, 1754
18	983	387, 624, 867
20	1117	621, –, 621
21	164	–, 83, 83
22	59	32, –, 32
24	25000	20733, 4847, 23955
26	96	39, –, 39
27	2392	–, 2079, 2079
28	1854	1238, –, 1238
30	5712	1955, 1881, 3452
32	2801324	2793029, –, 2793029

TABLE 2 – Number of transitive groups with blocks of size 2 or 3

6.3. **Remark.** In the case that 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. **Step 2: Lifting to the word stabilizer.** 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 (see 4.5) 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. **Step 3: Final lifting.** 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 that if it does not degenerate to a G-invariant.

Next, we have to treat the possibility of a degeneration. The group G_1 is the stabilizer of the sum over the variables $I_1 := \sum_{i,w_i=1} X_i$ 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. Using 2.6, this can be proved by showing 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 if $\sigma \in G_1$. □

6.6. **Remarks.**

(1) The main advantage of the coding theoretic approach is that we can compute the auxiliary group G_1 as the stabilizer of a code word, which is far more efficient than an enumeration of all low index subgroups.
(2) In the case of finite characteristics, the expression I_1^e may not contain the monomial that we used in the proof. One way to solve this problem is to replace I_1 by $\prod_{i,w_i=1} X_i$.
(3) The case of a block-system of block size 3 can be treated in a similar way. When we assume that the E-construction and the BlockQuotient-construction fail, the index of the subgroup must be a power of 3. Thus, we can work with the 3-Sylow-subgroup of the kernel of $\phi_{\mathcal{B}}$. This group will be isomorphic to $(\mathbb{Z}/3\mathbb{Z})^k$ and we deal with $\mathbb{F}_3$-codes instead of $\mathbb{F}_2$-codes. All the other steps of the construction carry over to this situation as well.

    This leads to the following question: Can more general codes be used for the construction of invariants in the case of block sizes larger than 3?

6.7. **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.

(1) $\mathbf{P}^3(\mathbb{F}_2)$ has 15 planes and 15 points.
(2) Each plane has 7 points and its complement has 8 points.
(3) We use the points of $\mathbf{P}^3(\mathbb{F}_2)$ as an index set. I.e., we fix a bijection $\iota\colon \mathbf{P}^3(\mathbb{F}_2) \to \{1,\dots,15\}$.
(4) For each plane $E \subset \mathbf{P}^3(\mathbb{F}_2)$, we get the linear form $l_E := \sum_{P \in \mathbf{P}^3(\mathbb{F}_2)\setminus E} X_{\iota(P)}$.
(5) N is the intersection of the kernels of the 15 linear forms l_E.
(6) 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.

6.8. **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.

(1) 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 the case that n is even, shorter orbits can not generate this subspace.
(2) Let $G := \mathrm{Sym}(2) \wr \mathrm{Sym}(n)$ with 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.
(3) 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 $(0,0,0,1,0,0,0,1,\ldots,0,0,0,1\}$ 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 are related to permutation groups with a second block system of block size 4 or 8.

7. Inspecting other representations

As explained above, the BlockQuotient construction leads to a simplification, as it maps to groups of smaller degree. In some cases, even an injective map may be helpful.

7.1. **The action on 2-sets .** The simplest change of the permutation representation is probably given by the action on 2-sets. This action is the same as the action on
$$M_2 := \{X_iX_j : i,j = 1,\ldots,n \mid i<j\}\,.$$
In the case that U and G decompose M_2 in different ways into orbits, we can use the orbit sum as a relative invariant. More precisely, let $m := X_iX_j$ be a monomial with $Um \subsetneq Gm$. Then
$$\sum_{\sigma\in U//\mathrm{Stab}_U(\{i,j\})} \sigma(X_iX_j)$$
is a relative invariant for $U \subset G$.

In the case that the above construction does not apply, we can try the following variant: Let $U \subset G$ be given such that the G-orbit and the U-orbit of X_iX_j coincide, but the U-action results in more block systems.

Denote by $B_1,\ldots,B_k \subset \{\{l,m\} : l,m = 1,\ldots,n \mid l \neq m\}$ a block system of the U-action that is not a block-system of the G action. Then we can use
$$\sum_{j=1}^{k}\Big(\sum_{\{l,m\}\in B_j} X_lX_m\Big)^e\,,$$
for a sufficiently large exponent e, as a relative invariant for $U \subset G$.

7.2. **Example.** Let the groups $U := T_6^{14} \subset G = \mathrm{Sym}(6)$ be given. U is the transitive representation of $\mathrm{Sym}(5) \cong \mathrm{PGL}_2(\mathbb{F}_5)$ on six points.

Both groups act transitively on 2-sets. However, $\mathrm{Stab}_G(\{1,2\}) \subset G$ is a maximal subgroup, but $\mathrm{Stab}_U(\{1,2\}) \subset U$ is not. Thus, the resulting degree 15 representation of U is not primitive. It has exactly one block system

$$\{\{1,2\},\{3,4\},\{5,6\}\},\quad \{\{1,3\},\{2,6\},\{4,5\}\},\quad \{\{1,4\},\{2,5\},\{3,6\}\},$$
$$\{\{1,5\},\{2,3\},\{4,6\}\},\quad \{\{1,6\},\{2,4\},\{3,5\}\}\,.$$

We can use this to write down the relative invariant

$$(X_1X_2 + X_3X_4 + X_5X_6)^3 + (X_1X_3 + X_2X_6 + X_4X_5)^3 +$$
$$(X_1X_4 + X_2X_5 + X_3X_6)^3 + (X_1X_5 + X_2X_3 + X_4X_6)^3 +$$
$$(X_1X_6 + X_2X_4 + X_3X_5)^3\,.$$

The Molien series [4, Sec. 3.2.1] of G and U with $R = \mathbb{C}[X_1, \ldots, X_6]$ are

$$H(R^G, t) = 1 + t + 2t^2 + 3t^3 + 5t^4 + 7t^5 + 11t^6 + 14t^7 + 20t^8 + \cdots$$
$$H(R^U, t) = 1 + t + 2t^2 + 3t^3 + 5t^4 + 7t^5 + 12t^6 + 15t^7 + 23t^8 + \cdots\,.$$

Thus, there is no relative invariant of degree smaller than 6.

7.3. **Remark.** One could try to continue the analysis of the new representation by applying the E- or the BlockQuotient-construction. However, a direct implementation of this may run into an infinite recursion as the action on 2-sets increases the degree of the permutation representation. Whereas all the earlier recursions reduced the degree.

8. Proper primitive groups

A primitive group that does not contain the alternating group is called proper. Let $U \subset G \subset \mathrm{Sym}(n)$ be given. In case U and G are both proper primitive groups there may be a more standard permutation representation of G that makes the the structure of $U \subset G$ more visible.

Further, we have a special approach to handle proper primitive subgroups of $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ that multiply transitive group.

8.1. **Primitive representations of Sym(n).** The symmetric group $\mathrm{Sym}(n)$ has primitive permutation representations of degree $\binom{n}{k}$ $(k < \frac{n}{2})$ by the action on sets of size k. To map this action back to an action on n points, we compute all index n subgroups of $G \subset \mathrm{Sym}(\binom{n}{k})$. We expect to find exactly one $H \subset G$ with an orbit O of length $\binom{n-1}{k-1}$. The action of G on the G-orbit of O will be the presentation we are looking for.

The relative invariant for $H \subset G$ used for the construction of the map is given by $\sum_{i \in O} X_i$.

8.2. **The primitive wreath product.** The primitive wreath product [5, Sec. 2.7] is a permutation representation of $\mathrm{Sym}(n) \wr \mathrm{Sym}(m)$ of degree n^m. This primitive representation can be described as follows. Starting with $M := \{1, \ldots, n\}$, we get an action of $\mathrm{Sym}(n)$ on M and an action of $\mathrm{Sym}(n)^m$ on M^m by treating each component individually. The action of $\mathrm{Sym}(m)$ on M^n is simply the permutation of coordinates.

We can recover the standard presentation from this by computing all the subgroups of index mn of $G \subset \mathrm{Sym}(n^m)$. In the case that a subgroup H with an orbit O of length n^{m-1} is found, we compute the action of G on the G-orbit of O. If this results in a faithful permutation representation (of degree mn) of G, we can take $\sum_{i \in O} X_i$ as an $H \subset G$ relative invariant and continue as in the BlockQuotient construction.

Aside from the degree reduction, the main advantage is that this map makes the group structure more visible.

8.3. **Multiply transitive subgroups.** Let $\mathrm{Alt}(n) \neq U \subset G = \mathrm{Sym}(n)$ or (or $U \subset G = \mathrm{Alt}(n)$) be a maximal and primitive subgroup. Then U is known to be at most 5-transitive. Thus, we have a chance to find a combinatorial difference in the action on small sets. For this, we compute intransitive subgroups of small index in U until we find a subgroup $U_0 \subset U$ with an orbit $O \subsetneq \{1, \ldots, n\}$ that is shorter than $\binom{n}{\#O}$. Then there will be an exponent k such that $\sum_{\sigma \in U/\!/U_0} (\sum_{i \in O} \sigma X_i)^e$ is a $U \subset G$ relative invariant.

Examples for this are the Mathieu group $M_{24} \subset \mathrm{Alt}(24)$ and its intransitive subgroup of index 759 that stabilizes a set of size 8. Another example is $\mathrm{PSp}(6,2) \subset \mathrm{Alt}(28)$. It has an intransitive subgroup of index 63 with an orbit of length 12.

9. Invariants for intransitive groups

9.1. **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 recursive constructions above can use intransitive subgroups and ask for relative invariants to handle them.

9.2. **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. If one of the projections is not surjective then 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 on 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 to construct relative invariants using linear representations.

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

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

(1) Compute the kernel of ϕ_1 as $K_1 := \pi_1(G \cap (G_1 \times \{\mathrm{id}_{G_2}\}))$.
(2) Find a subgroup $U_1 \subset G_1$ of minimal index such that the kernel of the coset action coincides with K_1.
(3) Put $U_2 := \pi_2(G \cap (U_1 \times G_2))$.
(4) Choose ϕ_i as the coset action on U_i.
(5) Construct relative invariants I_i for $U_i \subset G_i$.
(6) Chose univariate polynomials T_1, T_2 randomly.
(7) Compute the G-invariant $I := \sum_{\sigma \in G/\!/G \cap (U_1 \times G_2)} T_1(I_1)^\sigma T_2(I_2)^\sigma$.

(8) If I is a relative invariant then return I. Otherwise, try with other transformations T_1, T_2.

9.4. **Remarks.**

(1) 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 $\mathrm{Sym}(n)$

If 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 by the quotients $G/Z(G)$ for $G := \mathrm{Sym}(2) \wr \mathrm{Sym}(2k)$.

(2) The effect of the transformation polynomials T_i can be explained by inspecting the linear representation of the groups G_i on $\mathrm{span}\{I_i^\sigma \mid \sigma \in G_i\}$. If both representations are of dimension $[G_1 : U_1]$ then we are exactly in the situation of [6, 3.3, 3.4]. If this representation is of smaller dimension than expected then 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.

10. Relative invariants for non-maximal subgroups

The constructions above 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 the case that the base ring has infinitely many elements, there is a linear combination of the I_i that is a relative invariant for $U \subset G$. 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.

11. Timings, tests, and examples

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

11.1. **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.

11.2. **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 degrees $n = 3, \ldots, 30$.

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 4 invariant that involves 14735 multiplications.

In degree 32, we have 2801324 transitive groups in the database. The NewBlock-, E-, F-, and BlockQuotient-constructions fail only for subgroups of 2154 groups.

n	multiplications	deg(invariant)	n	multiplications	deg(invariant)
3	2	3	4	5	6
5	15	10	6	35	15
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	2906	190
21	310	210	22	1578	231
23	1012	253	24	3036	276
25	5952	300	26	14735	325
27	4733	351	28	7390	378
29	405	406	30	5213	435

TABLE 5 – Largest number of multiplications and degrees

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. Thus, the coding theoretic approach works. Finally, a generic invariant has to be used only for 4 pairs of groups. None of the generic invariants has more than 5000 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,* LMS Journal of Computation and Mathematics, 17, 2014, 141–158

[8] K. Geißler: *Berechnung von Galoisgruppen über 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.