DE GRUYTER OPEN Open Math. 2015; 13: 83–95

Open Mathematics Open Access

Research Article

Eszter K. Horváth*, Géza Makay, Reinhard Pöschel, and Tamás Waldhauser

Invariance groups of finite functions and orbit equivalence of permutation groups

Abstract: Which subgroups of the symmetric group S_n arise as invariance groups of n-variable functions defined on a k-element domain? It appears that the higher the difference $n-k$, the more difficult it is to answer this question. For $k \geq n$, the answer is easy: all subgroups of S_n are invariance groups. We give a complete answer in the cases $k = n-1$ and $k = n-2$, and we also give a partial answer in the general case: we describe invariance groups when n is much larger than $n-k$. The proof utilizes Galois connections and the corresponding closure operators on S_n, which turn out to provide a generalization of orbit equivalence of permutation groups. We also present some computational results, which show that all primitive groups except for the alternating groups arise as invariance groups of functions defined on a three-element domain.

Keywords: Invariance groups, Symmetry groups, Galois connections, Orbit equivalence of permutation groups, Symmetric and alternating groups, Functions of several variables

MSC: 06A15, 06E30, 20B10, 20B15, 20B25, 20B35, 94C10

DOI 10.1515/math-2015-0010
Received July 25, 2013; accepted July 31, 2014.

1 Introduction

This paper presents a Galois connection that facilitates the study of permutation groups representable as invariance groups of functions of several variables defined on finite domains. We shall assume without loss of generality that our functions are defined on the set $\mathbf{k} := \{1, \ldots, k\}$ for some integer $k \geq 2$. We say that an n-ary function $f : \mathbf{k}^n \to \mathbf{m}$ is *invariant under a permutation* $\sigma \in S_n$, if

$$f(x_1, \ldots, x_n) = f(x_{1\sigma}, \ldots, x_{n\sigma})$$

holds for all $(x_1, \ldots, x_n) \in \mathbf{k}^n$. The *invariance group (or symmetry group) of* f consists of the permutations $\sigma \in S_n$ such that f is invariant under σ. We will say that a group $G \leq S_n$ is (k,m)*-representable* if there exists a function $f : \mathbf{k}^n \to \mathbf{m}$ whose invariance group is G. Furthermore, we call a group (k,∞)*-representable* if it is (k,m)-representable for some natural number m. Note that (k,∞)-representability is equivalent to being the invariance group of a function $f : \mathbf{k}^n \to \mathbb{N}$.

A group $G \leq S_n$ is $(2,2)$-representable if and only if it is the invariance group of a Boolean function (i.e., a function $f : \{0,1\}^n \to \{0,1\}$), and a group is $(2,\infty)$-representable if and only if it is the invariance

***Corresponding Author: Eszter K. Horváth:** Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720, Szeged, Hungary,
E-mail: horeszt@math.u-szeged.hu
Géza Makay: Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720, Szeged, Hungary,
E-mail: makayg@math.u-szeged.hu
Reinhard Pöschel: Institut für Algebra, Technische Universität Dresden, D-01062, Dresden, Germany,
E-mail: Reinhard.Poeschel@tu-dresden.de
Tamás Waldhauser: Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720, Szeged, Hungary,
E-mail: twaldha@math.u-szeged.hu

group of a pseudo-Boolean function (i.e., a function $f:\{0,1\}^n \to \mathbb{R}$, cf. [3, Chapter 13]). Invariance groups of (pseudo-)Boolean functions are important objects of study in computer science (see [2] and the references therein); however, our main motivation comes from the algebraic investigations of A. Kisielewicz [7]. Kisielewicz defines a group G to be *m-representable* if there is a function $f:\{0,1\}^n \to \mathbf{m}$ whose invariance group is G (equivalently, G is $(2,m)$-representable), and G is defined to be *representable* if it is m-representable for some positive integer m (equivalently, G is $(2,\infty)$-representable). It is easy to see that a group is representable if and only if it is the intersection of 2-representable groups (i.e., invariance groups of Boolean functions). It was stated in [2] that every representable group is 2-representable; however, this is not true: as shown by Kisielewicz [7], the Klein four-group is 3-representable but not 2-representable. Moreover, it is also discussed in [7] that it is probably very difficult to find another such example by known constructions for permutation groups.

In this paper we focus on (k,∞)-representability of groups for arbitrary $k \geq 2$. It is straightforward to verify that a group is (k,∞)-representable if and only if it is the intersection of invariance groups of operations $f:\mathbf{k}^n \to \mathbf{k}$ (cf. Fact 2.2). We introduce a Galois connection between operations on $\mathbf{k}$ and permutations on $\mathbf{n}$, such that the Galois closed subsets of S_n are exactly the groups that are representable in this way. Our main goal is to characterize the Galois closed groups; as it turns out, the difficulty of the problem depends on the gap $d := n - k$ between the number of variables and the size of the domain. The easiest case is $d \leq 0$, where all groups are closed (see Proposition 2.5); for $d = 1$ the only non-closed groups are the alternating groups (see Proposition 2.7). The case $d = 2$ is considerably more difficult (see Proposition 4.1), and the general case, which includes representability by invariance groups of Boolean functions, seems to be beyond reach. However, we provide a characterization of Galois closed groups for arbitrary d provided that n is much larger than d (more precisely, $n > \max\left(2^d, d^2 + d\right)$; see Theorem 3.1.)

Clote and Kranakis [2] define a group $G \leq S_n$ to be *weakly representable*, if there exist positive integers k, m with $2 \leq k < n$ and $2 \leq m$ such that G is the invariance group of some function $f:\mathbf{k}^n \to \mathbf{m}$ (equivalently, G is (k,∞)-representable for some $k < n$). In Corollary 2.8 we provide a complete description of weakly representable groups.

Let us mention that our approach is also related to *orbit equivalence* of groups (see subsection 2.2). In the case $k = 2$, two groups have the same Galois closure if and only if they are orbit equivalent, whereas the cases $k > 2$ correspond to finer equivalence relations on the set of subgroups of S_n. Thus our Galois connection provides a parameterized version of orbit equivalence that could be interesting from the viewpoint of the theory of permutation groups.

The paper is organized as follows. In Section 2 we formalize the Galois connection and we make some general observations about Galois closures, orbit equivalence and direct and subdirect products of permutation groups. We state and prove our main result (Theorem 3.1) in Section 3, and in Section 4 we present results of some computer experiments, which, together with Theorem 3.1, settle the case $d = 2$. Finally, in Section 5 we relate our approach to relational definability of permutation groups (cf. [17]) and we formulate some open problems.

2 Definitions and general observations

In this section we define a Galois connection that describes representable groups (subsection 2.1), and we present some auxiliary results that will be needed for the proof of the main result in Section 3. We establish a relationship between Galois closure and orbit closure (subsection 2.2), which allows us to characterize (k,∞)-representable subgroups of S_n in the case $k = n - 1$ (subsection 2.3), and we determine closures of direct products and some special subdirect products of groups (subsection 2.4).

2.1 A Galois connection for invariance groups

We study invariance groups of functions by means of a Galois connection between permutations of $\mathbf{n}$ and n-ary operations on $\mathbf{k}$. Let $O_k^{(n)} = \{f \mid f:\mathbf{k}^n \to \mathbf{k}\}$ denote the set of all n-ary operations on $\mathbf{k}$. For $f \in O_k$ and $\sigma \in S_n$, we write $\sigma \vdash f$ if f is invariant under σ. For $F \subseteq O_k^{(n)}$ and $G \subseteq S_n$ let

$$F^{\vdash} := \{\sigma \in S_n \mid \forall f \in F : \sigma \vdash f\}, \overline{F}^{(k)} := (F^{\vdash})^{\vdash},$$
$$G^{\vdash} := \{f \in O_k^{(n)} \mid \forall \sigma \in G : \sigma \vdash f\}, \overline{G}^{(k)} := (G^{\vdash})^{\vdash}.$$

As for every Galois connection, the assignment $G \mapsto \overline{G}^{(k)}$ is a closure operator on S_n, and it is easy to see that $\overline{G}^{(k)}$ is a subgroup of S_n for every subset $G \subseteq S_n$ (even if G is not a group). For $G \leq S_n$, we call $\overline{G}^{(k)}$ the *Galois closure of G over* $\mathbf{k}$, and we say that G is *Galois closed over* $\mathbf{k}$ if $\overline{G}^{(k)} = G$. Sometimes, when there is no risk of ambiguity, we will omit the reference to $\mathbf{k}$, and speak simply about (Galois) closed groups and (Galois) closures. Similarly, we have a closure operator on $O_k^{(n)}$; the study of this closure operator constitutes a topic of current research of the authors. However, in this paper we focus on the "group side" of the Galois connection; more precisely, we address the following problem.

Problem 2.1. *For arbitrary $k, n \geq 2$, characterize those subgroups of S_n that are Galois closed over* $\mathbf{k}$.

As we shall see, this problem is easy if $k \geq n$, and it is very hard if n is much larger than k. Our main result is a solution in the intermediate case, when $d = n - k > 0$ is relatively small compared to n. Complementing this result with a computer search for small values of n, we obtain an explicit description of Galois closed groups for $n = k - 1$ and $n = k - 2$ for all n. Observe that if $k_1 \geq k_2$, then $\overline{G}^{(k_1)} \leq \overline{G}^{(k_2)}$, hence if G is Galois closed over $\mathbf{k}_2$, then it is also Galois closed over $\mathbf{k}_1$. Thus we have the most non-closed groups in the Boolean case (i.e., in the case $k = 2$), whereas for $k \geq n$ every subgroup of S_n is Galois closed (see Proposition 2.5).

The following fact appears in [2] for $k = 2$, and it remains valid for arbitrary k. We omit the proof, as it is a straightforward generalization of the proof of the equivalence of conditions (1) and (2) in Theorem 12 of [2].

Fact 2.2. *A group $G \leq S_n$ is Galois closed over* $\mathbf{k}$ *if and only if G is (k, ∞)-representable.*

2.2 Orbits and closures

The symmetric group S_n acts naturally on $\mathbf{k}^n$: for $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$ and $\sigma \in S_n$, let $a^\sigma = (a_{1\sigma}, \ldots, a_{n\sigma})$ be the action of σ on a. We denote the orbit of $a \in \mathbf{k}^n$ under the action of the group $G \leq S_n$ by a^G, and we use the notation $\mathrm{Orb}^{(k)}(G)$ for the set of orbits of $G \leq S_n$ acting on $\mathbf{k}^n$:

$$a^G := \left\{a^\sigma \mid \sigma \in G\right\}, \qquad \mathrm{Orb}^{(k)}(G) := \left\{a^G \mid a \in \mathbf{k}^n\right\}.$$

Clearly, $\sigma \vdash f$ holds for a given $\sigma \in S_n$ and $f \in O_k^{(n)}$ if and only if f is constant on the orbits of (the group generated by) σ. Therefore, for any $G, H \leq S_n$, we have $G^{\vdash} = H^{\vdash}$ if and only if $\mathrm{Orb}^{(k)}(G) = \mathrm{Orb}^{(k)}(H)$. On the other hand, from the identity $G^{\vdash\vdash\vdash} = G^{\vdash}$ (which is valid in any Galois connection), it follows that $G^{\vdash} = H^{\vdash}$ is equivalent to $\overline{G}^{(k)} = \overline{H}^{(k)}$. Thus we have

$$\overline{G}^{(k)} = \overline{H}^{(k)} \iff \mathrm{Orb}^{(k)}(G) = \mathrm{Orb}^{(k)}(H) \tag{1}$$

for all subgroups G, H of S_n.

Two groups $G, H \leq S_n$ are *orbit equivalent*, if G and H have the same orbits on the power set of $\mathbf{n}$ (which can be identified naturally with $\mathbf{2}^n$), i.e., if $\mathrm{Orb}^{(2)}(G) = \mathrm{Orb}^{(2)}(H)$ holds [6, 15]. One can define a similar equivalence relation on the set of subgroups of S_n for any $k \geq 2$ by (1), and each class of this equivalence relation contains a greatest group, which is the common closure of all groups in the same equivalence class. In other words, a group is Galois closed over $\mathbf{k}$ if and only if it is the greatest group among those having the same orbits on $\mathbf{k}^n$ (cf. Theorem 2.2 of [7] in the Boolean case). Therefore, the Galois closure of G over $\mathbf{k}$ can be described as follows:

$$\overline{G}^{(k)} = \left\{\sigma \in S_n \mid \forall a \in \mathbf{k}^n : a^\sigma \in a^G\right\}. \tag{2}$$

From (2) we can derive the following useful formula for the Galois closure of a group, which has been discovered independently by K. Kearnes [9]. Here $(S_n)_a$ denotes the stabilizer of $a \in \mathbf{k}^n$ under the action of S_n, i.e., the group of all permutations fixing a:

$$(S_n)_a = \{\sigma \in S_n \mid a^\sigma = a\}.$$

Note that this stabilizer is the direct product of symmetric groups on the sets $\{i \in \mathbf{n} \mid a_i = j\}$, $j \in \mathbf{k}$.

Proposition 2.3. *For every $G \le S_n$, we have*

$$\overline{G}^{(k)} = \bigcap_{a \in \mathbf{k}^n} (S_n)_a \cdot G.$$

Proof. We reformulate the condition $a^\sigma \in a^G$ of (2) for $a \in \mathbf{k}^n, \sigma \in S_n$ as follows:

$$\begin{aligned} a^\sigma \in a^G &\iff \exists \pi \in G : \ a^\sigma = a^\pi \\ &\iff \exists \pi \in G : a^{\sigma\pi^{-1}} = a \\ &\iff \exists \pi \in G : \sigma\pi^{-1} \in (S_n)_a \\ &\iff \sigma \in (S_n)_a \cdot G. \end{aligned}$$

Now from (2) it follows that $\sigma \in \overline{G}^{(k)}$ if and only if $\sigma \in (S_n)_a \cdot G$ holds for all $a \in \mathbf{k}^n$. □

Orbit equivalence of groups has been studied by several authors; let us just mention here a result of Seress [13] that explicitly describes orbit equivalence of primitive groups (see [14] for a more general result). For the definitions of the linear groups appearing in the theorem, we refer the reader to [4].

Theorem 2.4 ([13]). *If $n \ge 11$, then two different primitive subgroups of S_n are orbit equivalent if and only if one of them is A_n and the other one is S_n. For $n \le 10$, the nontrivial orbit equivalence classes of primitive subgroups of S_n are the following:*

(i) *for $n = 3$:* $\{A_3, S_3\}$;
(ii) *for $n = 4$:* $\{A_4, S_4\}$;
(iii) *for $n = 5$:* $\{C_5, D_{10}\}$ *and* $\{\mathrm{AGL}(1,5), A_5, S_5\}$;
(iv) *for $n = 6$:* $\{\mathrm{PGL}(2,5), A_6, S_6\}$;
(v) *for $n = 7$:* $\{A_7, S_7\}$;
(vi) *for $n = 8$:* $\{\mathrm{AGL}(1,8), \mathrm{A\Gamma L}(1,8), \mathrm{ASL}(3,2)\}$ *and* $\{A_8, S_8\}$;
(vii) *for $n = 9$:* $\{\mathrm{AGL}(1,9), \mathrm{A\Gamma L}(1,9)\}$, $\{\mathrm{ASL}(2,3), \mathrm{AGL}(2,3)\}$ *and* $\{\mathrm{PSL}(2,8), \mathrm{P\Gamma L}(2,8), A_9, S_9\}$;
(viii) *for $n = 10$:* $\{\mathrm{PGL}(2,9), \mathrm{P\Gamma L}(2,9)\}$ *and* $\{A_{10}, S_{10}\}$.

In our terminology, Theorem 2.4 states that for $n \ge 11$ every primitive subgroup of S_n except A_n is Galois closed over **2**, whereas for $n \le 10$ the only primitive subgroups of S_n that are not Galois closed over **2** are the ones listed above (omitting the last group from each block, which is the closure of the other groups in the same block).

2.3 The case $k = n - 1$

With the help of Proposition 2.3, we can prove that all subgroups of S_n are Galois closed over $\mathbf{k}$ if and only if $k \ge n$.

Proposition 2.5. *If $k \ge n \ge 2$, then each subgroup $G \le S_n$ is Galois closed over* $\mathbf{k}$*; if $2 \le k < n$, then A_n is not Galois closed over* $\mathbf{k}$.

Proof. Clearly, if $k \ge n$ then there exists a tuple $a \in \mathbf{k}^n$ whose components are pairwise different. Consequently, $(S_n)_a$ is trivial and therefore $\overline{G}^{(k)} \subseteq (S_n)_a \cdot G = G$ for all $G \le S_n$ by Proposition 2.3. On the other hand, if $k < n$ then there is a repetition in every tuple $a \in \mathbf{k}^n$, hence $(S_n)_a$ contains a transposition. Therefore $(S_n)_a \cdot A_n = S_n$ for all $a \in \mathbf{k}^n$, thus $\overline{A_n}^{(k)} = S_n$ by Proposition 2.3. □

Remark 2.6. *From Proposition 2.5 it follows that the Galois closures of a group $G \leq S_n$ over* **k** *for $k = 2, 3, \ldots$ form a nonincreasing sequence, eventually stabilizing at G itself:*

$$\overline{G}^{(2)} \geq \overline{G}^{(3)} \geq \cdots \geq \overline{G}^{(n-1)} \geq \overline{G}^{(n)} = \overline{G}^{(n+1)} = \cdots = G. \tag{3}$$

Now we can solve Problem 2.1 in the case $k = n-1$, which is the simplest nontrivial case. The proof of the following proposition already contains the key steps of the proof of Theorem 3.1.

Proposition 2.7. *For $k = n - 1 \geq 2$, each subgroup of S_n except A_n is Galois closed over* **k***.*

Proof. If $G \leq S_n$ is not Galois closed over **k**, then Proposition 2.3 shows that for all $\pi \in \overline{G}^{(k)} \setminus G$ and for all $a \in \mathbf{k}^n$, we have $\pi \in (S_n)_a \cdot G$, hence $\pi = \gamma\sigma$ for some $\gamma \in (S_n)_a$ and $\sigma \in G$. Therefore, $\gamma = \pi\sigma^{-1} \in \overline{G}^{(k)}$; moreover, $\gamma \neq \mathrm{id}$ follows from $\pi \notin G$. Thus we see that $\overline{G}^{(k)}$ contains at least one non-identity permutation from every stabilizer:

$$\overline{G}^{(k)} \neq G \implies \forall a \in \mathbf{k}^n \ \exists \gamma \in (S_n)_a \setminus \{\mathrm{id}\} : \ \gamma \in \overline{G}^{(k)}. \tag{4}$$

Now fix $i, j \in \mathbf{n}$, $i \neq j$, and let $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$ be a tuple such that $a_r = a_s \iff \{r, s\} = \{i, j\}$ or $r = s$. Then $(S_n)_a = \{\mathrm{id}, (ij)\}$, where $(ij) \in S_n$ denotes the transposition of i and j. Applying (4), we see that $(ij) \in \overline{G}^{(k)}$ for all $i, j \in \mathbf{n}$, hence $\overline{G}^{(k)} = S_n$. From Proposition 2.3 it follows that $\overline{G}^{(k)} \subseteq (S_n)_a \cdot G \subseteq S_n = \overline{G}^{(k)}$, i.e., $S_n = (S_n)_a \cdot G$ for every $a \in \mathbf{k}^n$. Choosing a as above, we have $S_n = \{\mathrm{id}, (ij)\} \cdot G$, hence G is of index at most 2 in S_n. Therefore, we have either $G = A_n$ or $G = S_n$; the latter is obviously Galois closed, whereas A_n is not Galois closed over **k** by Proposition 2.5. □

From Proposition 2.7 we can derive the following complete description of weakly representable groups.

Corollary 2.8. *All subgroups of $G \leq S_n$ except for A_n are weakly representable.*

Proof. According to Fact 2.2, a subgroup of S_n is weakly representable if and only if it is Galois closed over **k** for some $k < n$. By Remark 2.6, this is equivalent to G being Galois closed over $\mathbf{n-1}$. From Proposition 2.7 it follows that all subgroups of S_n are Galois closed over $\mathbf{n-1}$ except for A_n. □

2.4 Closures of direct and subdirect products

In the sequel, B and D always denote disjoint subsets of **n** such that $\mathbf{n} = B \cup D$, and $G \times H$ stands for the direct product of $G \leq S_B$ and $H \leq S_D$. In this paper we only consider direct products with the intransitive action, i.e., the two groups act independently on disjoint sets. Given permutations $\beta \in S_B$ and $\delta \in S_D$, we write $\beta \times \delta$ for the corresponding element of $S_B \times S_D$. Let π_1 and π_2 denote the first and second projections on the direct product $S_B \times S_D$. Then we have $\pi_1(\beta \times \delta) = \beta$ and $\pi_2(\beta \times \delta) = \delta$ for every $\beta \in S_B, \delta \in S_D$, and $\sigma = \pi_1(\sigma) \times \pi_2(\sigma)$ for every $\sigma \in S_B \times S_D$.

The following proposition describes closures of direct products, and, as a corollary, we obtain a generalization of [7, Theorem 3.1].

Proposition 2.9. *For all $G \leq S_B$ and $H \leq S_D$, we have $\overline{G \times H}^{(k)} = \overline{G}^{(k)} \times \overline{H}^{(k)}$.*

Proof. For notational convenience, let us assume that $B = \{1, \ldots, t\}$ and $D = \{t+1, \ldots, n\}$. If $a = (1, \ldots, 1, 2, \ldots, 2) \in \mathbf{k}^n$ with t ones followed by $n - t$ twos, then the stabilizer of a in S_n is $S_B \times S_D$. Hence from Proposition 2.3 it follows that $\overline{G \times H}^{(k)} \leq (S_B \times S_D) \cdot (G \times H) = S_B \times S_D$, i.e., every element of $\overline{G \times H}^{(k)}$ is of the form $\beta \times \delta$ for some $\beta \in S_B, \delta \in S_D$. For arbitrary $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$, let $a_B = (a_1, \ldots, a_t) \in \mathbf{k}^t$ and $a_D = (a_{t+1}, \ldots, a_n) \in \mathbf{k}^{n-t}$. It is straightforward to verify that $a^{\beta \times \delta} \in a^{G \times H}$ if and only if $a_B^{\beta} \in a_B^{G}$ and $a_D^{\delta} \in a_D^{H}$. Thus applying (2), we have

$$\begin{aligned}\beta\times\delta\in\overline{G\times H}^{(k)} &\iff \forall a\in\mathbf{k}^n : a^{\beta\times\delta}\in a^{G\times H}\\ &\iff \forall a\in\mathbf{k}^n : \left(a_B^{\beta}\in a_B^{G}\text{ and } a_D^{\delta}\in a_D^{H}\right)\\ &\iff \left(\forall a_B\in\mathbf{k}^t : a_B^{\beta}\in a_B^{G}\right)\text{ and }\left(\forall a_D\in\mathbf{k}^{n-t} : a_D^{\delta}\in a_D^{H}\right)\\ &\iff \beta\in\overline{G}^{(k)}\text{ and }\delta\in\overline{H}^{(k)}\\ &\iff \beta\times\delta\in\overline{G}^{(k)}\times\overline{H}^{(k)}.\end{aligned}$$ □

Corollary 2.10. *For all $G\le S_B$ and $H\le S_D$, the direct product $G\times H$ is Galois closed over* $\mathbf{k}$ *if and only if both G and H are Galois closed over* $\mathbf{k}$.

Proof. The "if" part follows immediately from Proposition 2.9. For the "only if" part, assume that $G\times H$ is Galois closed over $\mathbf{k}$. From Proposition 2.9 we get $G\times H=\overline{G}^{(k)}\times\overline{H}^{(k)}$, and this implies $G=\overline{G}^{(k)}$ and $H=\overline{H}^{(k)}$. □

Remark 2.11. *If $n<m$, then any subgroup G of S_n can be naturally embedded into S_m as the subgroup $G\times\{\mathrm{id}_{\mathbf{m}\setminus\mathbf{n}}\}$. From Proposition 2.9 it follows that $\overline{G\times\{\mathrm{id}_{\mathbf{m}\setminus\mathbf{n}}\}}^{(k)}=\overline{G}^{(k)}\times\{\mathrm{id}_{\mathbf{m}\setminus\mathbf{n}}\}$, i.e., there is no danger of ambiguity in not specifying whether we regard G as a subgroup of S_n or as a subgroup of S_m.*

Remark 2.12. *Proposition 2.9 and Corollary 2.10 do not generalize to subdirect products. It is possible that a subdirect product of two Galois closed groups is not Galois closed. For example, let*

$$G=\{\mathrm{id},(123),(132),(12)(45),(13)(45),(23)(45)\}<_{\mathrm{sd}}S_{\{1,2,3\}}\times S_{\{4,5\}};$$

then $\overline{G}^{(2)}=S_{\{1,2,3\}}\times S_{\{4,5\}}$, hence G is not Galois closed over $\mathbf{2}$. *It is also possible that a subdirect product is closed, although the factors are not both closed: let*

$$G=\{\mathrm{id},(13)(24),(1234)(56),(1432)(56)\}<_{\mathrm{sd}}\langle(1234)\rangle\times\langle(56)\rangle;$$

then G is Galois closed over $\mathbf{2}$*, but the* 4*-element cyclic group is not Galois closed over* $\mathbf{2}$ *(its Galois closure is the dihedral group of degree* 4*).*

Next we determine the closures of some special subdirect products involving symmetric and alternating groups that we will need in the proof of our main result. Recall that a subdirect product is a subgroup of a direct product such that the projection to each coordinate is surjective. Hence, if $G\le S_B\times S_D$ and $G_1=\pi_1(G)$, $G_2=\pi_2(G)$, then G is a subdirect product of G_1 and G_2. We denote this fact by $G\le_{\mathrm{sd}}G_1\times G_2$, and by $G<_{\mathrm{sd}}G_1\times G_2$ we mean a proper subdirect subgroup of $G_1\times G_2$. According to Remak [12], the following description of subdirect products of groups is due to Klein [8]. (Of course, the theorem is valid for abstract groups, not just for permutation groups. For an English reference, see Theorem 5.5.1 of [5].)

Theorem 2.13 ([8, 12])**.** *If $G\le_{\mathrm{sd}}G_1\times G_2$, then there exists a group K and surjective homomorphisms $\varphi_i\colon G_i\to K$ $(i=1,2)$ such that*

$$G=\{g_1\times g_2\mid\varphi_1(g_1)=\varphi_2(g_2)\}.$$

Note that in the above theorem we have $G=G_1\times G_2$ if and only if K is the trivial (one-element) group.

Proposition 2.14. *Let $|B|>\max(|D|,4)$ and $L\le S_D$. If $G\le_{\mathrm{sd}}A_B\times L$, then $G=A_B\times L$. If $G\le_{\mathrm{sd}}S_B\times L$, then either $G=S_B\times L$, or there exists a subgroup $L_0\le L$ of index* 2*, such that*

$$G=(A_B\times L_0)\cup\big((S_B\setminus A_B)\times(L\setminus L_0)\big). \tag{5}$$

Proof. Suppose that $G\le_{\mathrm{sd}}A_B\times L$, and let K and φ_1,φ_2 be as in Theorem 2.13 (for $G_1=A_B$ and $G_2=L$). Since A_B is simple, the kernel of φ_1 is either $\{\mathrm{id}_B\}$ or A_B. In the first case, K is isomorphic to A_B; however, this cannot be a homomorphic image of L, as $|L|\le|S_D|<|A_B|$. In the second case, K is trivial and $G=A_B\times L$. If $G\le_{\mathrm{sd}}S_B\times L$, then there are three possibilities for the kernel of φ_1, namely $\{\mathrm{id}_B\}$, A_B and S_B. Just as above, the first case is impossible, while in the third case we have $G = S_B \times L$. In the second case, K is a two-element group, hence by letting L_0 be the kernel of φ_2, we obtain (5). □

Proposition 2.15. *Let $|D| < d \leq n - d$ and let G be any one of the subdirect products considered in Proposition 2.14. Then $\overline{G}^{(k)} = S_B \times L$.*

Proof. Since $k = n - d > |D|$, all subgroups of S_D are closed by Proposition 2.5, hence $\overline{L}^{(k)} = L$. On the other hand, $k < |B|$ implies that A_B is not closed; in fact, we have $\overline{A_B}^{(k)} = S_B$. Therefore $\overline{A_B \times L}^{(k)} = \overline{A_B}^{(k)} \times \overline{L}^{(k)} = S_B \times L$, and also $\overline{S_B \times L}^{(k)} = S_B \times L$. It remains to consider the case when G is of the form (5). Then we have $A_B \times L_0 \leq G \leq S_B \times L$, thus

$$S_B \times L_0 = \overline{A_B \times L_0}^{(k)} \leq \overline{G}^{(k)} \leq \overline{S_B \times L}^{(k)} = S_B \times L. \tag{6}$$

Moreover, $\overline{G}^{(k)}$ contains $(S_B \setminus A_B) \times (L \setminus L_0)$, and this shows that the first containment in (6) is strict. However, $S_B \times L_0$ is of index 2 in $S_B \times L$, therefore we can conclude that $\overline{G}^{(k)} = S_B \times L$. □

3 The main result

Our main result is the following partial solution of Problem 2.1 for the case when n is "much larger" than $d = n - k$.

Theorem 3.1. *Let $n > \max\left(2^d, d^2 + d\right)$ and $G \leq S_n$. Then G is not Galois closed over $\mathbf{k}$ if and only if $G = A_B \times L$ or $G <_{\mathrm{sd}} S_B \times L$, where $B \subseteq \mathbf{n}$ is such that $D := \mathbf{n} \setminus B$ has less than d elements, and L is an arbitrary permutation group on D.*

Note that the set D in the theorem above is much smaller than B, thus B is a "big" subset of $\mathbf{n}$, and $L \leq S_D$ is a "little group", hence the notation. The subdirect product $G <_{\mathrm{sd}} S_B \times L$ is not determined by B and L, but in Proposition 2.14 we gave a fairly concrete description of these groups. Proposition 2.15 shows that the groups given in Theorem 3.1 are indeed not Galois closed over $\mathbf{k}$ (and that their Galois closure is $S_B \times L$). Therefore, it only remains to verify that these are the only non-closed groups, and we will achieve this by an argument that is based on the same idea as the proof of Proposition 2.7:

1) first we use (4) with specific tuples a to show that $\overline{G}^{(k)}$ must be a "large" group (see subsection 3.1 below), and then
2) we prove that G is of "small" index in $\overline{G}^{(k)}$ (see subsection 3.2 below).

For the first step, we will need to apply (4) for several groups acting on different sets, hence, for easier reference, we give a name to this property.

Definition 3.2. *Let $\Omega \subseteq \mathbf{n}$ be a nonempty set, and let us consider the natural action of S_Ω on $\mathbf{k}^\Omega$ for a positive integer $k \geq 2$. We say that $H \leq S_\Omega$ is k-*thick*, if*

$$\forall a \in \mathbf{k}^\Omega \ \exists \gamma \in (S_\Omega)_a \setminus \{\mathrm{id}_\Omega\} : \ \gamma \in H.$$

We will use thickness with two types of tuples $a \in \mathbf{k}^\Omega$. First, let a contain only one repeated value, which is repeated exactly $d + 1$ times, say at the coordinates $i_1, \ldots, i_{d+1} \in \Omega$ (note that such a tuple exists only if $|\Omega| \geq d + 1$). Then the stabilizer of a is the full symmetric group on $\{i_1, \ldots, i_{d+1}\}$, therefore k-thickness of H implies that

$$\exists \gamma \in S_{\{i_1, \ldots, i_{d+1}\}} \setminus \{\mathrm{id}\} : \ \gamma \in H. \tag{7}$$

Next, let d values be repeated in a, each of them repeated exactly two times, say at the coordinates $i_1, j_1;\ i_2, j_2; \ldots;$ i_d, j_d (here we need $|\Omega| \geq 2d$). Then the stabilizer of a is the group generated by the transpositions $(i_1\, j_1), (i_2\, j_2),$

$\ldots, (i_d\, j_d)$. Thus k-thickness of H implies that

$$\exists \gamma \in \langle (i_1 j_1), (i_2 j_2), \ldots, (i_d j_d) \rangle \setminus \{\mathrm{id}\} : \gamma \in H. \tag{8}$$

The first paragraph of the proof of Proposition 2.7 can be reformulated as follows:

Fact 3.3. *If $G \leq S_n$ is not Galois closed over $\mathbf{k}$, then $\overline{G}^{(k)}$ is k-thick.*

3.1 The closures of non-closed groups

The goal of this subsection is to prove the following description of the closures of non-closed groups.

Proposition 3.4. *Let $n > d^2 + d$. If $G \leq S_n$ is not Galois closed over $\mathbf{k}$, then $\overline{G}^{(k)}$ is of the form $S_B \times L$, where $B \subseteq \mathbf{n}$ is such that $D := \mathbf{n} \setminus B$ has less than d elements, and L is a permutation group on D.*

Throughout this subsection we will always assume that $G < \overline{G}^{(k)} \leq S_n$ with $n > d^2 + d$, where $d = n - k \geq 1$. We consider the action of $\overline{G}^{(k)}$ on $\mathbf{n}$ (not on $\mathbf{k}^n$), and we separate two cases upon the transitivity of this action. First we deal with the transitive case, for which we will make use of the following theorem of Bochert [1] (see also [4, 16]).

Theorem 3.5 ([1]). *If G is a primitive subgroup of S_Ω not containing A_Ω, then there exists a subset $I \subseteq \Omega$ with $|I| \leq \frac{|\Omega|}{2}$ such that the pointwise stabilizer of I in G is trivial.*

Lemma 3.6. *Let $\Omega \subseteq \mathbf{n}$ such that $|\Omega| > \max\left(2d, d^2\right)$. If H is a transitive k-thick subgroup of S_Ω, then $H = A_\Omega$ or $H = S_\Omega$.*

Proof. Assume for contradiction that H satisfies the assumptions of the lemma, but H does not contain A_Ω. If H is primitive, then let us consider the set I given in Theorem 3.5. Since $|\Omega \setminus I| \geq \frac{|\Omega|}{2} > d$, we can find $d+1$ elements $i_1, \ldots, i_{d+1}$ in $\Omega \setminus I$. Since H is k-thick and $|\Omega| \geq d+1$, we can apply (7) for $i_1, \ldots, i_{d+1}$, and we obtain a permutation $\gamma \neq \mathrm{id}$ in the pointwise stabilizer of I in H, which is a contradiction.

Thus H cannot be primitive. Since it is transitive, there exists a nontrivial partition

$$\Omega = B_1 \cup \cdots \cup B_r \tag{9}$$

with $|B_1| = \cdots = |B_r| = s$ and $r, s \geq 2$ such that every element of H preserves this partition. We will prove by contradiction that $r \leq d$ and $s \leq d$. First let us assume that $r > d$; let $B_1 = \{i_1, j_1, \ldots\}, \ldots, B_{d+1} = \{i_{d+1}, j_{d+1}, \ldots\}$, and let γ be the permutation provided by (7). Since $\gamma \neq \mathrm{id}$, there exist $p, q \in \{1, \ldots, d+1\}$, $p \neq q$ such that $i_p\gamma = i_q$. On the other hand, we have $j_p\gamma = j_p$, and this means that γ does not preserve the partition (9). Next let us assume that $s > d$; let $B_1 = \{i_1, \ldots, i_{d+1}, \ldots\}$, $B_2 = \{j_1, \ldots, j_{d+1}, \ldots\}$, and let γ be the permutation provided by (8). Since $\gamma \neq \mathrm{id}$, there exists $p \in \{1, \ldots, d\}$ such that $i_p\gamma = j_p$. On the other hand, we have $i_{d+1}\gamma = i_{d+1}$, and this means that γ does not preserve the partition (9). We can conclude that $r, s \leq d$, hence we have $|\Omega| = rs \leq d^2 < |\Omega|$, a contradiction. □

Lemma 3.7. *If $\overline{G}^{(k)}$ is transitive, then $\overline{G}^{(k)} = S_n$.*

Proof. Since $n > d^2 + d$, we have $n > \max\left(2d, d^2\right)$. Thus from Fact 3.3 and Lemma 3.6 it follows that either $\overline{G}^{(k)} = A_n$ or $\overline{G}^{(k)} = S_n$. However, A_n is not Galois closed over $\mathbf{k}$ by Proposition 2.5, because $n > k$. □

Now let us consider the intransitive case. The first step is to prove that in this case there is a unique “big” orbit.

Lemma 3.8. *If $\overline{G}^{(k)}$ is not transitive, then it has an orbit B such that $D = \mathbf{n} \setminus B$ has less than d elements.*

Proof. We claim that $\overline{G}^{(k)}$ has at most d orbits. Suppose to the contrary, that there exists $d+1$ elements $i_1, \ldots, i_{d+1} \in \mathbf{n}$, each belonging to a different orbit. If $\gamma \in \overline{G}^{(k)}$ is the permutation given by (7), then there exist $p, q \in \{1, \dots, d+1\}$, $p \neq q$ such that $i_p \gamma = i_q$, and this contradicts the fact that i_p and i_q belong to different orbits of $\overline{G}^{(k)}$. Now, the average orbit size is at least $\frac{n}{d} > d$, therefore there exists an orbit $B = \{i_1, \dots, i_d, \dots\}$ of size at least d. We will show that the complement of B has at most $d-1$ elements. Suppose this is not true, i.e., there are at least d elements $j_1, \dots, j_d$ outside B. With the help of (8) we obtain a permutation $\gamma \in \overline{G}^{(k)}$ for which there exists $p \in \{1, \dots, d\}$ such that $i_p \gamma = j_p$. This is clearly a contradiction, since i_p belongs to the orbit B, whereas j_p belongs to some other orbit. □

At this point we know that $\overline{G}^{(k)} \leq S_B \times S_D$. Using the the notation $G_1 = \pi_1\big(\overline{G}^{(k)}\big)$ and $L = \pi_2\big(\overline{G}^{(k)}\big)$ for the projections of $\overline{G}^{(k)}$, we have $\overline{G}^{(k)} \leq_{\mathrm{sd}} G_1 \times L$.

Lemma 3.9. *If $\overline{G}^{(k)}$ is not transitive and B is the big orbit given in Lemma 3.8, then $\overline{G}^{(k)} = S_B \times L$ for some $L \leq S_D$.*

Proof. First we show that G_1 inherits k-thickness from $\overline{G}^{(k)}$. Let $b \in \mathbf{k}^B$, and extend b to a tuple $a \in \mathbf{k}^n$ such that the components a_i $(i \in D)$ are pairwise different (this is possible, since $|D| < k$). The k-thickness of $\overline{G}^{(k)}$ implies that there exists a permutation $\gamma \in (S_n)_a \cap \overline{G}^{(k)} \setminus \{\mathrm{id}\}$, and from $\overline{G}^{(k)} \leq_{\mathrm{sd}} G_1 \times L$ it follows that $\gamma = \beta \times \delta$ for some $\beta \in G_1, \delta \in L$. The construction of the tuple a ensures that $\delta = \mathrm{id}_D$, hence we have $\mathrm{id}_B \neq \beta \in (S_B)_b \cap G_1$, and this proves that G_1 is a k-thick subgroup of S_B.

Since B is an orbit of $\overline{G}^{(k)}$, the action of G_1 on B is transitive. From $n > d^2+d$ it follows that $|B| = n-|D| > n-d \geq \max\big(2d, d^2\big)$, hence applying Lemma 3.6 with $H = G_1$ and $\Omega = B$, we obtain that $G_1 \geq A_B$. This means that either $\overline{G}^{(k)} \leq_{\mathrm{sd}} A_B \times L$ or $\overline{G}^{(k)} \leq_{\mathrm{sd}} S_B \times L$. Now with the help of Proposition 2.14 and Proposition 2.15 we can conclude that $\overline{G}^{(k)} = S_B \times L$. (Note that the assumption $|B| > 4$ in Proposition 2.14 is not satisfied if $d = 1$ and $n \leq 4$. However, $d = 1$ implies $D = \emptyset$, which contradicts the intransitivity of $\overline{G}^{(k)}$.) □

Combining Lemmas 3.7 and 3.9, we obtain Proposition 3.4, q.e.d.

3.2 The non-closed groups

In this subsection we prove the following Proposition 3.10. It describes the groups G with $\overline{G}^{(k)} = S_B \times L$ and therefore completes also the proof of Theorem 3.1.

Proposition 3.10. *Let $n > \max\big(2^d, d^2+d\big)$, let $B \subseteq \mathbf{n}$ and $D = \mathbf{n} \setminus B$ such that $|D| < d$, and let $L \leq S_D$. If $G \leq S_n$ is a group whose Galois closure over $\mathbf{k}$ is $S_B \times L$, then $G \leq_{\mathrm{sd}} A_B \times L$ or $G \leq_{\mathrm{sd}} S_B \times L$.*

Throughout this subsection we will assume that $n > \max\big(2^d, d^2+d\big)$, where $d = n-k \geq 1$, and $\overline{G}^{(k)} = S_B \times L$, where B and L are as in the proposition above. Let $G_1 = \pi_1(G) \leq S_B$ and $G_2 = \pi_2(G) \leq S_D$; then we have $G \leq_{\mathrm{sd}} G_1 \times G_2$. As in subsection 3.1, we begin with the transitive case (i.e., $D = \emptyset$), and we will use the following well-known result (see, e.g., [16, Exercise 14.3]).

Proposition 3.11. *If $n > 4$ and H is a proper subgroup of S_n different from A_n, then the index of H is at least n.*

Lemma 3.12. *If $\overline{G}^{(k)} = S_n$, then $G = A_n$ or $G = S_n$.*

Proof. Let $a \in \mathbf{k}^n$ be the tuple which was used to obtain (8); then we have $(S_n)_a = \langle (i_1 j_1), (i_2 j_2), \dots, (i_d j_d) \rangle$. From Proposition 2.3 we obtain

$$S_n = \overline{G}^{(k)} \subseteq (S_n)_a \cdot G,$$

hence we have $(S_n)_a \cdot G = S_n$. Since $|(S_n)_a| = 2^d$, the index of G in S_n is at most $2^d < n$, and therefore Proposition 3.11 implies that $G \geq A_n$ if $n > 4$. If $n \leq 4$, then $d = 1$, thus we can apply Proposition 2.7. □

Lemma 3.13. *If $\overline{G}^{(k)} = S_B \times L$, then $G_1 \geq A_B$ and $G_2 = L$.*

Proof. Clearly, $G \leq G_1 \times G_2$ implies $S_B \times L = \overline{G}^{(k)} \leq \overline{G_1 \times G_2}^{(k)} = \overline{G_1}^{(k)} \times \overline{G_2}^{(k)}$ by Proposition 2.9. This implies that $\overline{G}_1^{(k)} = S_B$.

Now we would like to apply Lemma 3.12 for the group G_1. Note that we assume throughout this section (in particular, also in Lemma 3.12) that $n > \max\left(2^d, d^2 + d\right)$, therefore we need to verify first that this inequality holds for G_1. Since G_1 acts on B, we must replace n by $|B|$ and d by $|B| - k$, hence we have to prove that

$$|B| > \max\left(2^{|B|-k}, (|B|-k)^2 + |B| - k\right). \tag{10}$$

Observe that $|B| = n - |D| > n - d$, as $|D| < d$; furthermore, $|B| - k = n - k - |D| = d - |D|$. First let us show that $|B| > 2^{|B|-k}$:

$$|B| > n - d > 2^d - d \geq 2^d - 2^{d-1} = 2^{d-1} \geq 2^{d-|D|} = 2^{|B|-k}.$$

Next we prove that $|B| > (|B| - k)^2 + (|B| - k)$:

$$|B| > n - d > d^2 + d - d = d^2 > (d-1)^2 + (d-1) \geq (d - |D|)^2 + (d - |D|) = (|B| - k)^2 + (|B| - k).$$

Thus Lemma 3.12 indeed applies to G_1, and it yields $G_1 \geq A_B$. On the other hand, $k > |D|$ implies that $\overline{G_2}^{(k)} = G_2$ by Proposition 2.5, hence

$$G \leq S_B \times L = \overline{G}^{(k)} \leq \overline{G_1}^{(k)} \times \overline{G_2}^{(k)} = \overline{G_1}^{(k)} \times G_2.$$

Applying π_2 to these inequalities, we obtain $G_2 \leq L \leq G_2$, and this proves $G_2 = L$. $\square$

Since $G \leq_{\text{sd}} G_1 \times G_2$, Lemma 3.13 immediately implies Proposition 3.10, q.e.d.

4 Computational results

We computed the Galois closures of all subgroups of S_n for $2 \leq k \leq n \leq 6$ by computer, and we found that for most of these groups the chain of closures (3) contains only G (i.e., G is Galois closed over **2**), and for all other groups (3) consists only of two different groups (namely $\overline{G}^{(2)}$ and G). Table 1 shows the list of groups corresponding to the latter case, up to conjugacy. For each group, the first column gives the smallest n for which G can be embedded into S_n (here we mean an embedding as a permutation group, not as an abstract group; cf. Remark 2.11). We also give the largest k such that $\overline{G}^{(k)} \neq G$, i.e., (3) takes the form $\overline{G}^{(2)} = \ldots = \overline{G}^{(k)} > \overline{G}^{(k+1)} = \ldots = G$.

Some of the entries in Table 1 may need some explanation. Using the notation of Theorem 2.13, each subdirect product in the table corresponds to a two-element quotient group K: for symmetric groups S_n we take the homomorphism $\varphi\colon S_n \to K$ with kernel A_n (cf. Proposition 2.14), whereas for the dihedral group D_4 we take the homomorphism $\varphi\colon D_4 \to K$ whose kernel is the group of rotations in D_4. The group $S_3 \wr S_2$ is the wreath product of S_3 and S_2 (with the imprimitive action); equivalently, it is the semidirect product $(S_3 \times S_3) \rtimes S_2$ (with S_2 acting on the direct product by permuting the two components). By $S_3 \wr_{\text{sd}} S_2$ we mean the "subdirect wreath product" $(S_3 \times_{\text{sd}} S_3) \rtimes S_2$. Finally, the groups $S\,(\square)$ and $R\,(\square)$ denote the group of all symmetries and the group of all rotations (orientation-preserving symmetries) of the cube, acting on the six faces of the cube.

Combining these computational results with Theorem 3.1, we get the solution of Problem 2.1 for the case $d = 2$.

Proposition 4.1. *For $k = n - 2 \geq 2$, each subgroup of S_n except A_n and A_{n-1} (for $n \geq 4$) and C_4 (for $n = 4$) is Galois closed over* **k**.

Proof. If $n > 6$, then we can apply Theorem 3.1, and we obtain the exceptional groups A_n and A_{n-1} from the direct product $A_B \times L$ with $|D| = 0$ and $|D| = 1$, respectively. If $n \leq 6$, then the non-closed groups can be read from Table 1. $\square$

We have also examined the linear groups appearing in Theorem 2.4 by computer, and we have found that all of them are Galois closed over **3**. Thus we have the following result for primitive groups.

Proposition 4.2. *Every primitive permutation group except for A_n ($n \geq 4$) is Galois closed over* **3**.

Table 1. Nontrivial closures for $n \leq 6$.

	$G \leq S_n$	$\overline{G}^{(k)}$
$n = 3,\ k = 2$	A_3	S_3
$n = 4,\ k = 3$	A_4	S_4
$n = 4,\ k = 2$	C_4	D_4
$n = 5,\ k = 4$	A_5	S_5
$n = 5,\ k = 2$	$\mathrm{AGL}(1,5)$	S_5
$n = 5,\ k = 2$	$S_3 \times_{\mathrm{sd}} S_2$	$S_3 \times S_2$
$n = 5,\ k = 2$	$A_3 \times S_2$	$S_3 \times S_2$
$n = 5,\ k = 2$	C_5	D_5
$n = 6,\ k = 5$	A_6	S_6
$n = 6,\ k = 2$	$\mathrm{PGL}(2,5)$	S_6
$n = 6,\ k = 3$	$S_4 \times_{\mathrm{sd}} S_2$	$S_4 \times S_2$
$n = 6,\ k = 3$	$A_4 \times S_2$	$S_4 \times S_2$
$n = 6,\ k = 2$	$S_3 \times_{\mathrm{sd}} S_3$	$S_3 \times S_3$
$n = 6,\ k = 2$	$A_3 \times S_3$	$S_3 \times S_3$
$n = 6,\ k = 2$	$A_3 \times A_3$	$S_3 \times S_3$
$n = 6,\ k = 2$	$D_4 \times_{\mathrm{sd}} S_2$	$D_4 \times S_2$
$n = 6,\ k = 2$	$C_4 \times S_2$	$D_4 \times S_2$
$n = 6,\ k = 3$	$(S_3 \wr S_2) \cap A_6$	$S_3 \wr S_2$
$n = 6,\ k = 2$	$S_3 \wr_{\mathrm{sd}} S_2$	$S_3 \wr S_2$
$n = 6,\ k = 2$	$A_3 \wr S_2$	$S_3 \wr S_2$
$n = 6,\ k = 2$	$R(\square)$	$S(\square)$

5 Concluding remarks and open problems

We have introduced a Galois connection to study invariance groups of n-variable functions defined on a k-element domain, and we have studied the corresponding closure operator. Our main result is that if the difference $d = n - k$ is relatively small compared to n, then "most groups" are Galois closed, and we have explicitly described the non-closed groups. The bound $\max\left(2^d, d^2 + d\right)$ of Theorem 3.1 is probably not the best possible; it remains an open problem to improve it.

Problem 5.1. *Determine the smallest number $f(d)$ such that Theorem 3.1 is valid for all $n \geq f(d)$.*

For fixed d, the inequality $n > \max\left(2^d, d^2 + d\right)$ fails only for "small" values of n, so one might hope that these cases can be dealt with easily. However, our investigations indicate that there is a simple pattern in the closures if n is much larger than d, and exactly those exceptional groups corresponding to small values of n are the ones that make the problem difficult. (We can say that the Boolean case is the hardest, as in this case n is just $d + 2$.) We have fully settled only the cases $d \leq 2$; perhaps it is feasible to attack the problem for the next few values of d.

Problem 5.2. *Describe the (non-)closed groups for $d = 3, 4, \ldots$.*

The chain of closures (3) for the groups that we investigated in our computer experiments has length at most two: for all $k \geq 2$, we have either $\overline{G}^{(k)} = \overline{G}^{(2)}$ or $\overline{G}^{(k)} = G$. This is certainly not true in general; for example, we have

$$\overline{A_3 \times \cdots \times A_t}^{(k)} = A_3 \times \cdots \times A_k \times S_{k+1} \times \cdots \times S_t,$$

hence $\overline{G}^{(2)} > \overline{G}^{(3)} > \cdots > \overline{G}^{(t-1)} > \overline{G}^{(t)} = G$ holds for $G = A_3 \times \cdots \times A_t$. It is natural to ask if there exist groups with long chains of closures that are not direct products of groups acting on smaller sets. As Proposition 4.2 shows, we cannot find such groups among primitive groups.

Problem 5.3. *Find transitive groups with arbitrarily long chains of closures.*

The closure operator defined in subsection 2.1 concerns the Galois closure with respect to the Galois connection induced by the relation $\vdash \subseteq S_n \times O_k^{(n)}$, based on a natural action of S_n on $\mathbf{k}^n$. In permutation group theory also another closure operator, called *k-closure* is used, which was introduced by H. Wielandt ([17, Definition 5.3]). This notion describes Galois closures with respect to a Galois connection between permutations of $\mathbf{n}$ and k-tuples in $\mathbf{n}^k$. Let $\sigma \in S_n$ act on $r = (r_1, \ldots, r_k) \in \mathbf{n}^k$ according to $r^\sigma := (r_1\sigma, \ldots, r_k\sigma)$, and, for a k-ary relation $\varrho \subseteq \mathbf{n}^k$, let us write $\sigma \rhd \varrho$ if and only if σ preserves ϱ, i.e., $r^\sigma \in \varrho$ for all $r \in \varrho$. For $G \subseteq S_n$, the Galois closure $(G^{\rhd})^{\rhd}$ is defined analogously to $(G^{\vdash})^{\vdash}$ (see subsection 2.1). The group $(G^{\rhd})^{\rhd}$ is called the *k-closure* of G, and it is denoted by $\operatorname{Aut}\operatorname{Inv}^{(k)} G$ in [11] and by $G^{(k)} = \operatorname{gp}(k\text{-rel } G)$ in [17]. A group $G \leq S_n$ is k-closed if and only if it can be defined by k-ary relations, i.e., if there exists a set R of k-ary relations on $\mathbf{n}$ such that G consists of the permutations that preserve every member of R. The following proposition establishes a connection between the two notions of closure.

Proposition 5.4. *For every $G \leq S_n$ and $k \geq 1$, the Galois closure $\overline{G}^{(k+1)}$ is contained in the k-closure of G. In particular, every k-closed group is Galois closed over $\mathbf{k+1}$.*

Proof. The proof is based on a suitable correspondence between $\mathbf{n}^k$ and $(\mathbf{k+1})^n$. Let $r = (r_1, \ldots, r_k) \in \mathbf{n}^k$ be a k-tuple whose components are pairwise different. We define $\varkappa(r) = (a_1, \ldots, a_n) \in (\mathbf{k+1})^n$ as follows:

$$a_i = \begin{cases} \ell, & \text{if } i = r_\ell; \\ k+1, & \text{if } i \notin \{r_1, \ldots, r_k\}. \end{cases}$$

Thus $\varkappa$ is a partial map from $\mathbf{n}^k$ to $(\mathbf{k+1})^n$, and it is straightforward to verify that $\varkappa$ is injective, and $\varkappa(r)^{\sigma^{-1}} = \varkappa(r^\sigma)$ holds for all $\sigma \in S_n$ and $r \in \mathbf{n}^k$ with mutually different components. (Here $\varkappa(r)^{\sigma^{-1}}$ refers to the action of S_n on $(\mathbf{k+1})^n$ by permuting the components of n-tuples, while r^σ refers to the action of S_n on $\mathbf{n}^k$ by mapping k-tuples componentwise.)

Now let $G \leq S_n$ and $\pi \in \overline{G}^{(k+1)}$; we need to show that $r^\pi \in r^G$ for every $r \in \mathbf{n}^k$. We may assume that the components of r are pairwise distinct (otherwise we can remove the repetitions and work with a smaller k). From $\pi \in \overline{G}^{(k+1)}$ it follows that $\varkappa(r)^{\pi^{-1}} \in \varkappa(r)^G$. Therefore, we have $\varkappa(r^\pi) = \varkappa(r)^{\pi^{-1}} \in \varkappa(r)^G = \varkappa\left(r^G\right)$, and then the injectivity of $\varkappa$ gives that $r^\pi \in r^G$. □

Note that the proposition above implies that each group that is not Galois closed over $\mathbf{k}$ (such as the ones in Theorem 3.1) is also an example of a permutation group that cannot be characterized by $(k-1)$-ary relations.

The connection between the two notions of closure in the other direction is much weaker. For example, the *Mathieu group* M_{12} is Galois closed over $\mathbf{2}$ (since it is the automorphism group of a hypergraph), but it is not 5-closed (since it is 5-transitive, and this implies that the 5-closure of M_{12} is the full symmetric group S_{12}). In some sense, this is a worst possible case, as it is not difficult to prove that if a subgroup of S_n is Galois closed over $\mathbf{2}$, then it is $\lfloor \frac{n}{2} \rfloor$-closed (in particular, M_{12} is 6-closed).

Problem 5.5. *Determine the smallest number $w(n,k)$ such that every subgroup of S_n that is Galois closed over $\mathbf{k}$ is also $w(n,k)$-closed.*

Acknowledgement: The authors are grateful to Keith Kearnes, Erkko Lehtonen and Sándor Radeleczki for stimulating discussions, and also to Péter Pál Pálfy who suggested the example mentioned before Problem 5.3. We also thank the referee whose hints considerably improved the presentation of the paper.

Research of the first and fourth author is partially supported by the NFSR of Hungary (OTKA), grant no. K83219. Research of the first, second and fourth author is supported by the European Union and co-funded by the European Social Fund under the project "Telemedicine-focused research activities on the field of Mathematics, Informatics and Medical sciences" of project number "TÁMOP-4.2.2.A-11/1/KONV-2012-0073". Research of the fourth author is partially supported by the NFSR of Hungary (OTKA), grant no. K77409.

References

[1] Bochert A., Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann, Math. Ann., 1889, 33, 584–590

[2] Clote P., Kranakis E., Boolean functions, invariance groups, and parallel complexity, SIAM J. Comput., 1991, 20, 553–590

[3] Crama Y., Hammer P.L., Boolean functions. Theory, algorithms, and applications., Encyclopedia of Mathematics and its Applications 142. Cambridge University Press, 2011

[4] Dixon J. D., Mortimer B., Permutation groups, Graduate Texts in Mathematics, 163, Springer-Verlag, 1996

[5] Hall M.,The theory of groups, Chelsea Publishing Company, New York, 1976

[6] Inglis N.F.J., On orbit equivalent permutation groups, Arch. Math., 1984, 43, 297–300

[7] Kisielewicz A., Symmetry groups of Boolean functions and constructions of permutation groups, J. Algebra, 1998, 199, 379–403

[8] Klein F., Vorlesungen über die Theorie der elliptischen Modulfunctionen. Ausgearbeitet und vervollständigt von Dr. Robert Fricke, Teubner, Leipzig, 1890

[9] Kearnes K., personal communication, 2010

[10] Pöschel R., Galois connections for operations and relations, In: K. Denecke, M. Erné, and S.L. Wismath (Eds.), Galois connections and applications, Mathematics and its Applications, 565, Kluwer Academic Publishers, Dordrecht, 2004, 231–258

[11] Pöschel R. and Kalužnin L. A., *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wissenschaften, Berlin, 1979, Birkhäuser Verlag Basel, Math. Reihe Bd. 67, 1979

[12] Remak R., Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte, J. Reine Angew. Math., 1930, 163, 1–44

[13] Seress Á., Primitive groups with no regular orbits on the set of subsets, Bull. Lond. Math. Soc., 1997, 29, 697–704

[14] Seress Á., Yang K., On orbit-equivalent, two-step imprimitive permutation groups, Computational Group Theory and the Theory of Groups, Contemp. Math., 2008, 470, 271–285

[15] Siemons J., Wagner A., On finite permutation groups with the same orbits on unordered sets, Arch. Math. 1985, 45, 492–500

[16] Wielandt H., Finite permutation groups, Academic Press, New York and London, 1964

[17] Wielandt H., Permutation groups through invariant relations and invariant functions, Dept. of Mathematics, Ohio State University Columbus, Ohio, 1969