SIAM J. COMPUT.
Vol. 20, No. 3, pp. 553-590, June 1991
© 1991 Society for Industrial and Applied Mathematics
011

BOOLEAN FUNCTIONS, INVARIANCE GROUPS, AND PARALLEL COMPLEXITY*

PETER CLOTE† AND EVANGELOS KRANAKIS‡

Abstract. This paper studies the invariance groups $\mathbf{S}(f)$ of boolean functions $f \in \mathbf{B}_n$ (i.e., $f:\{0,1\}^n \to \{0,1\}$) on n variables, i.e., the set of all permutations on n elements which leave f invariant. After building intuition by presenting several examples that suggest relations between algebraic properties of groups and computational complexity of languages, necessary and sufficient conditions are given via Pólya's cycle index for an arbitrary finite permutation group to be of the form $\mathbf{S}(f)$, for some $f \in \mathbf{B}_n$. It is shown that asymptotically "almost all" boolean functions have trivial invariance groups. For cyclic groups $G \leqq \mathbf{S}_n$ a logspace algorithm for determining whether the given group is of the form $\mathbf{S}(f)$, for some $f \in \mathbf{B}_n$ is given. The applicability of group theoretic techniques in the study of the parallel complexity of languages is demonstrated. For any language L let L_n be the characteristic function of the set of all strings in L which have length exactly n and let $\mathbf{S}_n(L)$ be the invariance group of L_n. The index $|\mathbf{S}_n:\mathbf{S}_n(L)|$ are considered as a function of n and the class of languages whose index is polynomial in n is studied. Bochert's lower bound on the index of primitive permutation groups is used together with the O'Nan-Scott theorem, a deep result in the classification of finite simple groups, in order to show that any language with polynomial index is in (nonuniform) TC^0 and hence in (nonuniform) NC^1. As a corollary, an extension is given of a result of Fagin-Klawe-Pippenger-Stockmeyer, giving necessary and sufficient conditions for a language with polynomial index to be computable by a constant depth polynomial size circuit family. As another corollary, it is shown that the problem of "weight-swapping" for a sequence of groups of polynomial index is in (nonuniform) NC^1.

Key words. abelian group, boolean function, circuit, classification theory, cyclic-, dihedral-, hyperoctahedral-groups, index of a group, invariance group of boolean function, NC, parallel complexity, permutation group, Pólya cycle index, pumping lemma, representable group, regular language, symmetric boolean function, wreath product

AMS(MOS) subject classifications. 68Q15, 68Q25, 68Q45

1. Introduction. The aim of this paper is to study the invariance groups of boolean functions, provide efficient algorithms for determining the representability of a given group as the invariance group of a boolean function, and use group theoretic techniques in order to deduce results about the parallel complexity of formal languages.

Given n input values, each of which can assume one of two possible states 0, 1, a "module" M outputs a value which assumes one of the states 0, 1. The output of the module when the input values are $x_1, \cdots, x_n$ depends in general on the *order* of the inputs. There are certain permutations of the input states which leave the output state *invariant* or unchanged. For example, it may be that the output is independent of any permutation of the input states, in which case the given module is called symmetric. In general, for a given module, the set of permutations which, when applied to any set of input states, leave the output invariant is easily seen to form a permutation group.

* Received by the editors November 7, 1988; accepted for publication (in revised form) June 28, 1990. This article first appeared as an extended abstract in the Proceedings of the Fourth Annual IEEE Conference on Structure in Complexity Theory, 1989, pp. 55-65.

† Department of Computer Science, Boston College, Chestnut Hill, Massachusetts 02167. This author's research was supported in part by National Science Foundation grant DCR-8606165. Some of this research was performed while the author was visiting the Université de Paris VII, Equipe de Logique Mathématique, Centre Nationale de la Recherche Scientifique-UA 753, 2 Place Jussieu, Paris, France.

‡ Centrum voor Wiskunde en Informatica, P.O. Box 4079, 1009 AB Amsterdam, the Netherlands.

Formally, the operation performed by such an n-ary module M is usually represented by an n-ary boolean function[1] $f: 2^n \to 2$. For fixed n, let the set of all such n-ary boolean functions be denoted by $\mathbf{B}_n$. If the input states of the module are assigned the boolean values $x_1, \cdots, x_n$ then by definition $f(x_1, \cdots, x_n)$ is the value of the output state of the module M on input $x_1, \cdots, x_n$. Given such an n-ary boolean function f let $\mathrm{S}(f)$ be the set of all permutations on the n elements $1, 2, \cdots, n$ such that for all input values $(x_1, \cdots, x_n) \in 2^n$, $f(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$. Clearly, the group $\mathrm{S}(f)$ equals the full symmetric group $\mathbf{S}_n$ exactly in the special case when the boolean function f is symmetric.

By a counting argument Lupanov, Shannon, and Strassen have shown that almost all boolean functions have exponential size circuit complexity. Despite this result, very little is known concerning specific languages or families of boolean functions. Our interest in the present study arose from attempting to use group theoretic techniques in order to generalize the simple observation that any family $\{f_n : f_n \in \mathbf{B}_n,\ n \in \mathbf{N}\}$ of symmetric boolean functions is computable by a logarithmic depth, polynomial size circuit family. Probabilistic techniques have been successfully used by several authors (Furst, Saxe, and Sipser [FSS84], Yao [Yao85], etc.) in order to obtain lower bounds on the size and/or depth of circuit families which compute certain symmetric languages (families of symmetric boolean functions). However, there are few results giving tight upper bounds, apart from the above cited fact that any family of symmetric boolean functions is computable by a nonuniform circuit family of logarithmic depth and polynomial size (formula size bounds have been obtained by various authors in this case). In this paper we indicate the applicability of group theory in obtaining upper bounds for the parallel complexity of families of boolean functions. Our work is different from, but somewhat related to, studies on the automorphism groups of error-correcting codes (e.g., kth order Reed–Muller codes, which are specific k-dimensional subspaces of 2^n [MS78]), as well as to work in [Har64] where group theoretic methods are used to calculate the number of nonequivalent boolean functions, where the equivalence relation is defined by $f \equiv g$ if and only if there exists $\sigma \in \mathbf{S}_n$ such that for all $x_1, \cdots, x_n \in \{0, 1\}$ $(f(x_1, \cdots, x_n) = g(x_{\sigma(1)}, \cdots, x_{\sigma(n)}))$.

In [FKL88] it was indicated how the classification theorem for finite simple groups could be applied to VLSI technology by giving an algorithm to minimize pin-count in a sequence of circuits. Here we consider the problem of placement of modules on a chip where permutation of input wires is allowed. It is expected that study of the invariance groups of boolean functions may lead to algorithms for optimizing space in VLSI design, e.g., knowledge that certain modules leading into a block can be permuted without changing the function computed.

It is interesting to point out that invariance groups are also relevant to the computability problem for boolean functions in anonymous networks as used in distributed computing. For example, we are interested in computing n-ary boolean functions in an n-node anonymous network $\mathcal{N}$. To compute the value of a given function f at the input $(b_1, \cdots, b_n)$ the processors $p_1, \cdots, p_n$ are initialized with the inputs $b_1, \cdots, b_n$, respectively. By exchanging messages through the links all the processors must eventually compute the same bit $b = f(b_1, \cdots, b_n)$. It has been the focus of several papers to determine and study networks for which

$$f \text{ is computable in } \mathcal{N} \Leftrightarrow S(f) \supseteq Aut(\mathcal{N}),$$

[1] Throughout the paper we identify a positive integer n with the set $\{0, 1, \cdots, n-1\}$, e.g., $2 = \{0, 1\}$; in general, however, we will prefer the set-notation when we want to emphasize the elements of the language under consideration.

where $Aut(\mathcal{N})$ denotes the group of automorphisms of $\mathcal{N}$. In fact, this is the case for several types of networks, like directed and unlabeled rings [ASW85], labeled tori [BB89], and labeled hypercubes [KK89].

1.1. Results of the paper. Following is an outline of the main results and contents of the paper. We begin in § 2 by providing some preliminary results regarding the size of the index of a permutation group. We remind the reader of the essential parts of Pólya's beautiful enumeration theory that will be used in the present study.

In §§ 3 and 4, to build intuition for the reader, we present a number of examples concerning the invariance groups of certain types of languages, such as palindromes, parentheses, and regular languages, and study the reverse problem of constructing languages realizing specific types of groups. We compute the invariance groups of Dyck palindrome languages and give an efficient algorithm for determining membership in the invariance group of regular languages. We show that each of the cyclic (for $n \neq 3, 4, 5$), dihedral, and hyperoctahedral sequences of groups are representable by regular languages and construct groups which cannot be represented by regular languages.

In § 5 we study the representation problem for general permutation groups. We define a subgroup $G \leqq \mathbf{S}_n$ to be *strongly representable* if G is the invariance group of an n-ary boolean function—i.e., there exists $f \in \mathbf{B}_n$ for which $G = \mathrm{S}(f)$. We distinguish between groups which are "strongly representable" and groups which are "isomorphic to strongly representable." In the latter case, we show that every permutation subgroup of $\mathbf{S}_n$ is isomorphic to a strongly representable group $\mathrm{S}(f)$, for some $f: 2^{n(\log n+1)} \to 2$; but as stated, this isomorphism is at the expense of increasing the number of variables in the boolean function from n to $n(\log n+1)$. The problem is more interesting in the former case, where we give a necessary and sufficient condition in terms of the Pólya index, for an arbitrary subgroup of $\mathbf{S}_n$ to be of the form $\mathrm{S}(f)$, for some n-ary boolean function $f: 2^n \to 2$. Using the classification theorem for maximal permutation groups we show that "with few exceptions" (essentially, only the alternating group $\mathbf{A}_n$, for $n \geqq 10$) all maximal permutation groups on n letters are strongly representable. This contrasts with the fact that there are numerous nonrepresentable permutation groups. We also give a logspace algorithm which, on input of a cyclic group $G \leqq \mathbf{S}_n$, decides whether G is strongly representable, in which case it outputs a boolean function $f: 2^n \to 2$ such that $G = \mathrm{S}(f)$. Our last result in this section concerns asymptotics. For any sequence of nonidentity permutation groups $\langle G_n \leqq \mathbf{S}_n : n \geqq 1 \rangle$ we prove that

$$\lim_{n\to\infty} \frac{|\{f \in \mathbf{B}_n : \mathrm{S}(f) \geqq G_n\}|}{2^{2^n}} = 0.$$

It then immediately follows that asymptotically "almost all" boolean functions have a trivial invariance group; i.e., they are equal to the identity permutation group.

Given a language $L \subseteq \{0, 1\}^*$, let L_n be the characteristic function of the set of words of L of length exactly n. Section 6 is concerned with the complexity of languages of polynomial index, i.e., languages L for which there exists a polynomial $p(n)$ such that $|\mathbf{S}_n : \mathbf{S}_n(L)| \leqq p(n)$, where $\mathbf{S}_n(L)$ denotes the invariance group of the boolean function L_n. We study the closure properties of the class of these languages and apply the NC algorithm for permutation group membership of [BLS87] in order to show that languages of polynomial index are in (nonuniform) NC. By using the O'Nan–Scott theorem, a deep result in classification theory of finite simple groups, we improve the last result to show that any language of polynomial index is in (nonuniform) TC^0 and hence NC^1.

In [FKPS85], Fagin, Klawe, Pippenger, and Stockmeyer used group theoretic techniques together with the exponential size lower bound for constant depth circuits accepting parity [Yao85] to give a necessary and sufficient condition for a symmetric language $L \subseteq \{0, 1\}^*$ to belong to AC^0; i.e., for L to be computable by a nonuniform circuit family of constant depth and polynomial size. Our characterization of languages of polynomial index allows an immediate extension of this result. Namely, for $L \subseteq \{0, 1\}^*$ of polynomial index, L is in AC^0 if and only if the least number of input bits which must be set to a constant in order for the resulting language $L_n = L \cap \{0, 1\}^n$ to be constant is polylogarithmic in n.

As mentioned in the introduction, we believe that group theoretic considerations may possibly play a role in VLSI design. In particular, knowledge of the invariance group of "modules" might allow minimization of the surface area for automated circuit layout. Toward a mathematical formalization of this idea, we introduce some notation. For any sequence $\mathbf{G} = \{G_n: G_n \leqq \mathbf{S}_n, n \in \mathbf{N}\}$ of permutation groups the problem SWAP ($\mathbf{G}$) is given by the following.

Input. $n \in \mathbf{N}$, $a_1, \cdots, a_n$ positive rationals.

Output. A permutation $\sigma \in G_n$ such that for all $1 \leqq i < n$, $a_{\sigma(i)} + a_{\sigma(i+1)} \leqq 2$, if such a permutation exists, and the response "NO" otherwise.

The intuition behind the problem SWAP ($\mathbf{G}$) is that the output wires of modules $M_1, \cdots, M_n$ are the inputs to module M, and that the invariance group of M is G_n. The "width" of module M_i is the rational number a_i. Modules M_i and M_j can be placed next to each other if they do not "overlap"; i.e., exactly when $a_i + a_j \leqq 2$, where we imagine an average size of 1 per module. Thus, the output for SWAP ($\mathbf{G}$) indicates whether there exists a permutation of the input modules M_i which does not change the output of M and which allows a layout of $M_{\sigma(1)}, \cdots, M_{\sigma(n)}$ without overlap. A simple application of our work yields an NC^1 algorithm for the problem SWAP ($\mathbf{G}$), where $\mathbf{G} = \{G_n: G_n \leqq \mathbf{S}_n, n \in \mathbf{N}\}$ is of polynomial index.

Recall that the stipulation of the layout problem is to find an optimal layout given a number of modules together with their connections. A popular algorithm that attempts to solve the layout problem is due to Kernighan and Lin [KL82] and partitions the chip into an upper and a lower half, swapping modules on either side, trying to minimize a certain parameter, then recursively partitioning simultaneously the top and bottom into left and right parts, swapping modules between left and right parts to minimize a parameter, etc. Our problem stipulation in SWAP is quite different: instead of being given a list of modules and their connections (including which input port of a target module), we allow the input ports of the target module to be swapped, provided that the resultant function is not changed.

Finally, in § 7, we discuss some open problems and give directions for further research.

An acquaintance with the standard results on group theory and finite permutation groups, as presented for example in [Hal57] and [Wie64], will be essential for an adequate understanding of the results of the present paper.

2. Preliminaries. Here we give some introductory definitions and results regarding permutation groups and complexity of circuits that will be used in our subsequent investigations. The three topics we will discuss are:

- the size of the group index,
- the size of the cycle index and its computation via Pólya's formula, and
- complexity of boolean functions with respect to the size and/or depth of boolean circuits computing them.

2.1. Index of a permutation group. In the sequel it will be convenient to think of permutations on the set $\{1, 2, \cdots, n\}$ as bijective mappings on the set of all positive integers such that $\sigma(k) = k$ for all $k > n$. Part of this paper is primarily concerned with "large" permutation subgroups of the full symmetric group. Let $\mathbf{S}_n$ denote the group of all permutations of n elements, and $\mathbf{A}_n$ be the subgroup of even permutations (also known as the alternating group on n letters). In general, for any nonempty set Ω let $\mathbf{S}_\Omega$ denote the set of all permutations of Ω. For any group G the symbol $H \leqq G$ means that H is a subgroup of G. Regarding the sizes of permutation groups the following theorem summarizes some known results on the sizes permutation groups.

THEOREM 1. *Let $H \leqq \mathbf{S}_n$ be a permutation group which does not contain $\mathbf{A}_n$.*

(1) $|\mathbf{S}_n : H| \geqq n$.

(2) *If the order of H is maximal then $|\mathbf{S}_n : H| = n$. In fact, for $n \neq 6$ the subgroups H of $\mathbf{S}_n$ with $|\mathbf{S}_n : H| = n$ are exactly the one point stabilizers of $\mathbf{S}_n$.*

(3) *If H is primitive then*

(*Bochert*) $|\mathbf{S}_n : H| \geqq [(n+1)/2]!$.

(*Praeger and Saxl*) $|H| < 4^n$.

(*Cameron*) *either H is a "known" group or $|H| < n^{10 \log\log n}$.*

Proof. For all three parts and further information, consult [Wie64], [Tzu82], as well as the references in [KL88] (in particular, the proof of (3) is very hard). Part (1) follows from the following claim.

CLAIM. *If H is a subgroup of G and $|G : H| = n$ then there exists a normal subgroup N of G such that $N \leqq H$ and $|G: N|$ divides $n!$.*

Indeed, consider the set $\Omega = \{Hg: g \in G\}$ of cosets of the quotient group G/H. By assumption, this set has size n. Let S_Ω be the group of permutations on Ω. For each $x \in G$ consider the permutation $\phi(x): \Omega \to \Omega$, where $\phi(x)(Hg) = Hgx$. Clearly, $\phi: G \to S_\Omega$ is a group homomorphism. Moreover, it is easy to see that

$$N := Ker(\phi) = \bigcap_{g \in G} H^g$$

is a normal subgroup of G, where $H^g = g^{-1}Hg$. By the homomorphism theorem, the order of the quotient group G/N divides the order of the permutation group S_Ω. This proves the claim.

Now let us prove (1) by the above claim there exists a normal subgroup N of $\mathbf{S}_n$ such that $N \leqq H$ and $|\mathbf{S}_n : N|$ divides $(n-1)!$. It follows that $N \neq 1$. Since the only normal subgroups of $\mathbf{S}_n$ are $\mathbf{A}_n$, $\mathbf{S}_n$, and 1, the result is clear. □

2.2. Cycle index of a permutation group. Let G be a permutation group on n elements. Define an equivalence relation $i \equiv j$ if and only if for some $\sigma \in G$, $\sigma(i) = j$. The equivalence classes under this equivalence relation are called orbits. Let $G_i = \{\sigma \in G: \sigma(i) = i\}$ be the stabilizer of i, and let i^G be the orbit of i. An elementary theorem asserts that $|G: G_i| = |i^G|$. Using this, we can obtain the well-known theorem of Burnside and Frobenius, which states that for any permutation group G on n elements, the number of orbits of G is equal to the average number of fixed points of a permutation $\sigma \in G$,

$$\omega_n(G) = \frac{1}{|G|} \sum_{\sigma \in G} |\{i: \sigma(i) = i\}|, \tag{1}$$

where $\omega_n(G)$ is the number of orbits of G [Com70]. Any permutation $\sigma \in \mathbf{S}_n$ can be identified with a permutation on 2^n defined as follows:

$$x = (x_1, \cdots, x_n) \to x^\sigma = (x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

Hence, any permutation group G on n elements can also be thought of as a permutation group on the set 2^n. It follows from (1) that

$$|\{x^G : x \in 2^n\}| = \frac{1}{|G|} \sum_{\sigma \in G} |\{x \in 2^n : x^\sigma = x\}|,$$

where $x^G = \{x^\sigma : \sigma \in G\}$ is the orbit of x. We would like to find a more explicit formula for the right-hand side of the above equation. To do this, note that $x^\sigma = x$ if and only if x is invariant on the orbits of σ. It follows that $|\{x \in 2^n : x^\sigma = x\}| = 2^{o(\sigma)}$, where $o(\sigma)$ is the number of orbits of (the group generated by) σ. Using the fact that $o(\sigma) = c_1(\sigma) + \cdots + c_n(\sigma)$, where $c_i(\sigma)$ is the number of i-cycles in σ (i.e., in the cycle decomposition of σ), we obtain Pólya's formula:

$$(2) \qquad |\{x^G : x \in 2^n\}| = \frac{1}{|G|} \sum_{\sigma \in G} 2^{o(\sigma)} = \frac{1}{|G|} \sum_{\sigma \in G} 2^{c_1(\sigma) + \cdots + c_n(\sigma)}.$$

The number $|\{x^G : x \in 2^n\}|$ is called the **cycle index** of the permutation group G and will be denoted by $\Theta(G)$. If we want to stress that G is a permutation group on n letters, then we write $\Theta_n(G)$, instead of $\Theta(G)$. For more information on Pólya's enumeration theory the reader should consult [Ber71] and [PR87].

Since the invariance group $\mathbf{S}(f)$ of a function $f \in \mathbf{B}_n$ contains G if and only if it is invariant on each of the different orbits x^G, $x \in 2^n$, we obtain that

$$|\{f \in \mathbf{B}_n : \mathbf{S}(f) \geqq G\}| = 2^{\Theta(G)}.$$

It is also not difficult to compare the size of $\Theta(G)$ and $|\mathbf{S}_n : G|$. Indeed, let $H \leqq G \leqq \mathbf{S}_n$. If

$$Hg_1, Hg_2, \cdots, Hg_k$$

are the distinct right cosets of G modulo H then for any $x \in 2^n$ we have that

$$x^G = x^{Hg_1} \cup x^{Hg_2} \cup \cdots \cup x^{Hg_k}.$$

It follows that $\Theta_n(H) \leqq \Theta_n(G) \cdot |G : H|$. Using the fact that $\Theta_n(\mathbf{S}_n) = n+1$ we obtain as a special case that $\Theta_n(G) \leqq (n+1)|\mathbf{S}_n : G|$. In addition, using a simple argument concerning the size of the orbits of a permutation group we obtain that if $\Delta_1, \cdots, \Delta_\omega$ are different orbits of the group $G \leqq \mathbf{S}_n$ acting on $\{1, 2, \cdots, n\}$ then

$$(|\Delta_1| + 1) \cdots (|\Delta_\omega| + 1) \leqq \Theta_n(G).$$

We summarize these results in the following useful theorem.

THEOREM 2. *For any permutation groups $H \leqq G \leqq \mathbf{S}_n$ we have*

(1) $\Theta_n(G) \leqq \Theta_n(H) \leqq \Theta_n(G) \cdot |G : H|$.

(2) $\Theta_n(G) \leqq (n+1) \cdot |\mathbf{S}_n : G|$.

(3) $n+1 \leqq \Theta_n(G) \leqq 2^n$.

(4) *If $\Delta_1, \cdots, \Delta_\omega$ are different orbits of G then* $(|\Delta_1|+1) \cdots (|\Delta_\omega|+1) \leqq \Theta_n(G)$.

It is easy to see that in general $|\mathbf{S}_n : G|$ and $\Theta_n(G)$ can diverge widely. For example, let $f(n) = n - \log n$ and let G be the group $\{\sigma \in \mathbf{S}_n : \forall i > f(n)(\sigma(i) = i)\}$. It is then clear that $\Theta_n(G) = (f(n)+1) \cdot 2^{\log n}$ is of order n^2, while $|\mathbf{S}_n : G|$ is of order $n^{\log n}$. Another simpler example is obtained when G is the identity subgroup of $\mathbf{S}_n$.

2.3. Circuits. An n-circuit α_n is a labeled, directed acyclic graph whose nodes are labeled by $x_1, \cdots, x_n$ (input bits), $\neg$, $\wedge$, $\vee$. The input nodes are of in-degree 0 and there is a unique output node whose out-degree is 0. The size $c(\alpha)$ of α_n is the number of internal (i.e., noninput) nodes, while the depth $d(\alpha)$ of α_n is the maximal length of a path from an input node to the output node. A word $x \in \{0, 1\}^n$ is *accepted* by an n-circuit α_n if each input node labeled by x_i has as value the ith bit of x. An n-circuit α_n *recognizes* or *computes* a language $L_n \subseteq \{0, 1\}^n$ (respectively, boolean function $f \in \mathbf{B}_n$) if and only if for all words x in $\{0, 1\}^n$,

$$x \in L_n \text{ (respectively } f(x) = 1) \Leftrightarrow \alpha_n \text{ accepts } x.$$

A circuit family $\langle \alpha_n : \alpha_n$ is an n-circuit, $n \in \mathbf{N}\rangle$ *recognizes* or *computes* a language $L \subseteq \{0, 1\}^*$ if and only if for all n (α_n accepts $L \cap \{0, 1\}^n$). In this paper, we usually consider *nonuniform* circuit families as defined above—of course, such families can recognize nonrecursive languages. A circuit family $\langle \alpha_n : n \in \mathbf{N}\rangle$ is *logspace uniform* if there is a logspace computable function $F: 1^n \mapsto \bar{\alpha}_n$ for constructing the circuits. There are stronger and weaker uniformity notions. See [Coo85] for further discussion and for a survey of parallel complexity theory. The class *SIZE-DEPTH*(f, g) is the collection of languages accepted by a family $\langle \alpha_n : n \in \mathbf{N}\rangle$ where $c(\alpha_n) \leqq f(n)$ and $d(\alpha_n) \leqq g(n)$. The class AC^k (respectively, NC^k) is the collection of languages[2] belonging to *SIZE-DEPTH*$(n^{O(1)}, O(\log^k(n)))$ where the in-degree of nodes labeled by $\wedge$, $\vee$ is arbitrary (respectively, 2). Of importance to this paper is the class AC^0 of languages accepted by (nonuniform) circuit families of constant depth and polynomial size with *arbitrary fanin*, and the class NC^1 of languages accepted by (nonuniform) circuit families of logarithmic depth (and a fortiori polynomial size) with *fanin* 2. By unwinding a circuit into an equivalent boolean formula (circuit with fanout 1), NC^1 is easily seen to be the class of languages computable by (nonuniform) polynomial size boolean formulas. The class TC^0 is the collection of languages computable by (nonuniform) circuit families with constant depth and polynomial size, whose gates are arbitrary fanin *threshold* gates. NC is defined to be $\bigcup_{n \in \mathbf{N}} \mathrm{NC}^k$. Trivially, $\mathrm{NC}^k \subseteq \mathrm{AC}^k$, and by replacing an arbitrary fanin gate by a binary tree of fanin 2 gates, it is clear that $\mathrm{AC}^k \subseteq \mathrm{NC}^{k+1}$. A language $L \subseteq \{0, 1\}^*$ is said to have (or be computable by) polynomial size circuits, denoted $L \in SIZE(n^{O(1)})$, if there is a circuit family $\langle \alpha_n : n \in \mathbf{N}\rangle$ where α_n computes the characteristic function of $L_n = L \cap \{0, 1\}^n$ and $c(\alpha_n) \leqq p(n)$ for some polynomial p. Note that $SIZE(n^{O(1)})$ is the same class, whether one considers arbitrary fanin or fanin 2 circuits. Since the out-degree of a node is arbitrary, partial computations may be reused; thus the circuit provides a model for parallel computation. Stockmeyer and Vishkin [SV84] have shown that AC^k is the class of languages computed in $O(\log^k(n))$ time with a polynomial number of processors on a *parallel random access machine* (PRAM).

For a boolean function $f: 2^n \to 2$, we define

$$c(f) = \min\{c(\alpha): \alpha \text{ computes } f\}$$

where α has fanin 2. The following results are well known (e.g., see [Sav76] or [Yab83]). In particular, we shall use the second fact in a later proof.

(1) For any symmetric function $f \in \mathbf{B}_n$, $c(f) = O(n)$.

(2) (Lupanov-Shannon-Strassen) $|\{f \in \mathbf{B}_n : c(f) < q\}| = O(q^{q+1})$.

(3) For any $\varepsilon > 0$, the ratio of $f \in \mathbf{B}_n$ such that $c(f) > (1-\varepsilon)2^{n-1}/n$ tends to 1 as $n \to \infty$.

3. Invariance groups of certain languages. The main objects of study in this paper are boolean functions and their invariance groups. Let $\mathbf{B}_{n,k}$ be the set of all k-valued

[2] Usually these classes are defined to be classes of functions rather than languages. Since we will not discuss function computations in this paper, we adopt the above definition.

functions $f: 2^n \to k$ on n boolean variables. If $k=2$ then we abbreviate $\mathbf{B}_{n,2}$ by $\mathbf{B}_n$. If $\mathbf{Z}_2$ denotes the finite two-element field then it is clear that

$$\mathbf{B}_n = \frac{\mathbf{Z}_2[x_1, \cdots, x_n]}{(x_i^2 - x_i,\ i=1,2,\cdots,n)}.$$

For $x=(x_1, \cdots, x_n) \in 2^n$ and $\sigma \in \mathbf{S}_n$, let $x^\sigma = (x_{\sigma(1)}, \cdots, x_{\sigma(n)})$. For any n-ary boolean function $f \in \mathbf{B}_n$ let f^σ be defined by

$$f^\sigma(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

The *invariance group* of f is defined by

$$\begin{aligned} \mathbf{S}(f) &= \{\sigma \in \mathbf{S}_n : f = f^\sigma\} \\ &= \{\sigma \in \mathbf{S}_n : \forall x \in 2^n f^\sigma(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})\}. \end{aligned}$$

If $K \subseteq \{0,1\}^n$ is a set of words of length n, then by abuse of notation we shall write $\mathbf{S}(K)$ for the invariance group of the characteristic function of the set K. If $L \subseteq \{0,1\}^*$ is a set of finite words and $n \geqq 1$ then $\mathbf{S}_n(L)$ denotes the invariance group of the n-ary boolean function L_n. Clearly, $\mathbf{S}(f)$, being nonempty and closed under multiplication, is a subgroup of $\mathbf{S}_n$.

Here we compute the invariance groups of well-known formal languages. We begin with the Dyck (or parenthesis) and palindrome languages and conclude with an "efficient" algorithm for computing the invariance group of regular languages.

3.1. Dyck languages. The semiDyck language D [Harr78] is defined as the least set of strings in the alphabet 0, 1 such that $\Lambda \in D$ and (for all $x, y \in D$) ($xy \in D$ and $0x1 \in D$). The semiDyck language is not regular, as can be seen from the fact that the elements 0^n give rise to infinitely many distinct equivalence classes in the right congruence relation for D. The Dyck languages D^r, $r \geqq 1$, are defined in the alphabet $\Sigma_r = \{0_i, 1_i : i = 1, \cdots, r\}$ in a similar fashion: D^r is the least set of strings in the alphabet Σ_r such that $\Lambda \in D^r$ and (for all $x, y \in D^r$) (for all $i \leqq r$) ($xy \in D^r \wedge 0_i x 1_i \in D^r$). Clearly, $D = D^1$. Next we determine the invariance group of the Dyck languages.

THEOREM 3. *For the Dyck language D^r defined above we have that*

$$\mathbf{S}_n(D^r) = \begin{cases} 1 & \textit{if } n \textit{ is odd or } r \geqq 2 \\ \langle (i, i+1) : i < n \textit{ is even} \rangle & \textit{if } n \textit{ is even and } r = 1. \end{cases}$$

Proof. First, notice that D is a homomorphic image of D^r. The homomorphism $h_r : \Sigma_r \to \Sigma$ is defined by setting $h_r(b_i) = b$, where $b \in \{0, 1\}$. It follows that for all strings x of length n, and all permutations $\sigma \in \mathbf{S}_n$, $h_r(x^\sigma) = (h_r(x))^\sigma$, which in turn implies that $\mathbf{S}_n(D^r) \subseteq \mathbf{S}_n(D)$. Now, if n is odd, then trivially $\mathbf{S}(D) = 1$ and so $\mathbf{S}(D^r) = 1$. Suppose that $n = 4$, $r = 2$, and, respectively, write "(", "[", ")", "]" in place of 0_1, 0_2, 1_1, 1_2. Then ([ ]) $\in D_4^2$, but (] [) $\notin D_4^2$. Similar examples can be constructed to verify that $\mathbf{S}(D^r) = 1$ for $2 \leqq r$. To prove the theorem, it is enough to show that, for n even,

$$\mathbf{S}_n(D) = \langle (i, i+1) : i < n \text{ is even} \rangle.$$

For any string $x = x_1 \cdots x_k$ let $l(x) = k$ be its length and $s(x)$ its signature, where

$$s(x) = \sum_{i=1}^{k} (-1)^{x_i}.$$

Then we can prove the following claims.

CLAIM 1. *For any string* x, $x \in D \Leftrightarrow s(x) = 0$ *and for all* $i \leqq l(x)(s(x \upharpoonright i) \geqq 0)$.

Proof of Claim 1. The direction from left to right is trivial by induction on the construction of $x \in D$. To prove the other direction, assume the right-hand side is true. We use induction on the length of x. If for some $k < l(x)$, $s(x \upharpoonright k) = 0$ then $x = (x \upharpoonright k)y$, for some y. Clearly, the induction hypothesis applies to $x \upharpoonright k$ and y. Consequently, both $x \upharpoonright k$, $y \in D$ and hence also $x \in D$. Otherwise, for all $k < l(x)$, $s(x \upharpoonright k) > 0$. Clearly, $x_{l(x)} = 1$ (otherwise $s(x) > 0$). We also know that $x_1 = 0$. Hence, $x = 0y1$, for some y. Clearly, this y satisfies the induction hypothesis stated in the right-hand side of Claim 1. Hence, $y \in D$ and consequently also $x \in D$.

As mentioned above, if n is odd the theorem is trivial. Hence, in all the proofs below we assume that n is even.

CLAIM 2. *For any* $b \in \{0, 1\}$ *and any* $1 < i < n$ *there exists a string* $x \in D_n$ *such that* $x_i = b$.

Proof of Claim 2. The proof is by induction on n. The claim is trivial if $n = 2$. So assume $n > 2$. If $i = 2$ then consider the strings $01y$, $0011z \in D_n$. If $i = n - 1$, then consider the strings $y01$, $z0011 \in D_n$. Hence, without loss of generality, we can assume that $2 < i < n - 1$. But then consider strings of the form $0y1$, where $y \in D_{n-2}$, and use the induction hypothesis.

CLAIM 3. $\sigma \in S_n(D) \Rightarrow \sigma(1) = 1$, $\sigma(n) = n$.

Proof of Claim 3. Assume $\sigma(1) = i \neq 1$. Consider an $x \in D_n$ such that $x_i = 1$ (use Claim 2). Then note that $x^\sigma = 1y \notin D_n$, for some string y, which is a contradiction. A similar proof shows that $\sigma(n) = n$.

CLAIM 4. *If* $\sigma \in S_n(D)$ *and* $\sigma[\{1, \cdots, i-1\}] = [\{1, \cdots, i-1\}]$ *and* $\sigma(i) < i$ *then* (a) i *is even*, (b) $\sigma(i) = i+1$, (c) $\sigma(i+1) = i$.

Proof of Claim 4. To prove (a) assume on the contrary that i is odd. Consider an $x \in D_n$ such that $x = y0 \cdots 1z$, where $x_i = 0$ and $x_{\sigma(i)} = 1$ and $s(y) = 0$. Applying σ to x we obtain that $x^\sigma = y^\sigma 1 \cdots$. But then $s(y^\sigma 1) = s(y^\sigma) - 1 = s(y) - 1 = -1 \; 0$. Hence, $x^\sigma \notin D_n$, by Claim 1, a contradiction.

To prove (b) assume on the contrary that $\sigma(i) > i+1$. For simplicity, assume that $\sigma(i) = i+2$ (a similar proof will work if $\sigma(i) \geqq i+2$). We distinguish several cases. If $\sigma(i+1) = i+1$ then consider the string $x = y0011 \cdots \in D_n$, with $l(y) = i-2$, $x_{i-1} = x_i = 0$ and $x_{i+1} = x_{i+2} = 1$. Then it is clear that $x^\sigma = y^\sigma 011 \cdots \notin D_n$, a contradiction. If $\sigma(i+1) = i+3$ then consider the string $x = y000111 \cdots \in D_n$, with $l(y) = i-2$, $x_{i-1} = x_i = x_{i+1} = 0$ and $x_{i+2} = x_{i+3} = x_{i+4} = 1$. Then it is clear that $x^\sigma = y^\sigma 011 \cdots \notin D_n$, a contradiction. If $\sigma(i+1) > i+3$ then consider the string $x = y0011 \cdots 1 \cdots \in D_n$, with $l(y) = i-2$, $x_{i-1} = x_i = 0$ and $x_{i+1} = x_{i+2} = x_{\sigma(i+1)} = 1$. Then it is clear that $x^\sigma = y^\sigma 011 \cdots \notin D_n$, a contradiction. Thus, we obtain a contradiction in all cases considered above. Hence, $\sigma(i) = i+1$. This completes the proof of (b).

To prove (c) use an argument similar to (b). Indeed, assume on the contrary, $\sigma(i+1) \neq i$. It follows that $\sigma(i+1) \geqq i+2$. If $\sigma(i+1) = i+2$ then take $x = y0011 \cdots \in D_n$, with $x_{i-1} = x_i = 0$, $x_{i+1} = x_{i+2} = 1$. If we apply σ to x then we obtain $x^\sigma = y^\sigma 011 \cdots \notin D_n$, which is a contradiction. If $\sigma(i+1) = i+3$ then take $x = y00101 \cdots \in D_n$, with $x_{i-1} = x_i = x_{i+2} = 0$, $x_{i+1} = x_{i+3} = 1$. If we apply σ to x then we obtain $x^\sigma = y^\sigma 011 \cdots \notin D_n$, which is a contradiction. In general, a similar proof works if $\sigma(i+1) \geqq i+3$. This completes the proof of (c).

Now we are ready to complete the proof of the theorem. Let $\sigma \in D_n$. We know that $\sigma(1) = 1$. Let i_1 be minimal such that $\sigma(i_1) \neq i_1$ and for all $i < i_1(\sigma(i) < i_1)$. By minimality $\sigma(i_1) > i_1$. It follows from Claim 4 that i_1 is even and $\sigma(i_1) = i_1 + 1$ and $\sigma(i_1 + 1) = i_1$. Let i_2 be minimal i_1 such that $\sigma(i_2) \neq i_2$ and for all $i < i_2(\sigma(i) \; i_2)$. By minimality $\sigma(i_2) \; i_2$. Hence, Claim 4 applies again to show that i_2 is even and $\sigma(i_2) = i_2 + 1$

and $\sigma(i_2+1)=i_2$. Proceeding in this fashion we show that $\mathbf{S}_n(D)\subseteq\langle(i, i+1)$: $i\ n$ is even$\rangle$. It remains to show that, in fact, equality holds. Indeed, let $i<n$ be even. There are four possibilities for x_ix_{i+1} in the string x:

$$X_1=y00\cdots,\qquad X_2=y01\cdots,\qquad X_3=y10\cdots,\qquad X_4=y11\cdots,$$

where y is a string of odd length. But then it is easy to see that for all $j=1,2,3,4$,

$$X_j\in D_n \Leftrightarrow X_j^{(i,i+1)}\in D_n,$$

which completes the proof of the theorem. □

3.2. Palindrome language. The palindrome language is defined as the set of all strings (in the alphabet Σ, with at least two elements) $u=u_1\cdots u_n$ such that for all i $(u_i=u_{n-i+1})$.

THEOREM 4. *If L is the palindrome then*

$$\sigma\in\mathbf{S}_n(L)\Leftrightarrow(\forall i\leqq n)(\sigma(n=n-\sigma(i)+1)).$$

Moreover, $\mathbf{S}_n(L)$ *is isomorphic to* $\mathbf{S}_{[n/2]}\times(\mathbf{Z}_2)^{[n/2]}$.

Proof. ($\Rightarrow$) Let $\sigma\in\mathbf{S}_n(L)$. Suppose that $\sigma(i)=j$. Consider the string $u=u_1\cdots u_n$ such that $u_j=u_{n-j+1}=0$, and $u_k=1$, for all $k\neq i$, $n-j-1$. Clearly, $u\in L_m$. Hence, also $u^\sigma\in L_n$. It follows that $u_{\sigma(i)}=u_j=0$ and consequently $u_{\sigma(n-i+1)}=0$. But this is true only if $\sigma(n-i+1)=n-j+1$, as desired.

($\Leftarrow$) This direction is obvious from the very definition of the palindrome.

To determine the group $\mathbf{S}_n(L)$, notice that by the previous result, a permutation $\sigma\in\mathbf{S}_n(L)$, is determined by the values $\sigma(1),\cdots,\sigma([n/2])$. Furthermore, note that if n is odd then $\sigma((n+1)/2)=(n+1)/2$. Now consider the permutation σ_0 such that for all $i\leqq n$, $\sigma_0(i)=n+1-i$ and put $G_n=\{\sigma\sigma_0\sigma\sigma_0^{-1}: \sigma\in\mathbf{S}_{[n/2]}\}$. It is easy to see that G_n is isomorphic to $\mathbf{S}_{[n/2]}$, moreover the group H_n generated by G_n and the transpositions $(i, n-i+1)$ is exactly the group

$$G_n\times(1,n)\times(2,n-1)\times\cdots\times([n/2],n-[n/2]-1).$$

Moreover, $H_n=\mathbf{S}_n(L)$. This completes the proof of the theorem. □

3.3. An algorithm for the invariance group of regular languages. Here we are interested in studying the complexity of membership in the invariance group of a regular language. To this end consider a term $t(x,y)$ built up from the variables x, y by concatenation. For example, $t(x,y)=xyx$, $t(x,y)=x^2yx^5y^3$, etc. are such terms. The number of occurrences of x and y in the term $t(x,y)$ is called the length of t and is denoted by $|t|$, e.g., $|t|=3$ and $|t|=11$, in the two previous examples. For any permutations σ, τ let the permutation $t(\sigma,\tau)$ be obtained from the term $t(x,y)$ by substituting each occurrence of x, y by σ, τ, respectively, and interpreting concatenation as the product of permutations. We know that the symmetry group $\mathbf{S}_n$ is generated by the cyclic permutation $c_n=(1,2,\cdots,n)$ and the transposition $\tau=(1,2)$ (in fact any transposition will do) [Wie64]. A sequence $\sigma=\langle\sigma_n: n\geqq1\rangle$ of permutations is term-generated by the permutations c_n, τ if there is a term $t(x,y)$ such that for all $n\geqq2$, $\sigma_n=t(c_n,\tau)$. We have the following theorem.

THEOREM 5. (1) *Let $\sigma=\langle\sigma_n: n\geqq1\rangle$ be a sequence of permutations which is term-generated by the permutations $c_n=(1,2,\cdots,n)$, $\tau=(1,2)$. Then for any regular language L, L^σ is also regular.*

(2) *For any term t of length $|t|$ the problem of testing whether, for a regular language L, $L=L^\sigma$, where $\sigma=\langle\sigma_n: n\geqq1\rangle$ is a sequence of permutations generated by the term t via the permutations $c_n=(1,2,\cdots,n)$, $\tau=(1,2)$, is decidable; in fact it has complexity $O(2^{|t|})$.*

Proof. Part (2) is an immediate consequence of the proof of part (1) and the solvability of the equality problem for regular languages [Harr 78]. So we concentrate only on the proof of (1). To prove the theorem we need the following claim, whose proof is easy and left to the reader.

CLAIM.

$$L \in \mathbf{REG} \Rightarrow \{x: 0x \in L\} \in \mathbf{REG}.$$

$$L \in \mathbf{REG} \Rightarrow \{x: x1 \in L\} \in \mathbf{REG}.$$

$$L \in \mathbf{REG} \Rightarrow \{x: 0x1 \in L\} \in \mathbf{REG}.$$

$$L \in \mathbf{REG} \Rightarrow \{x: 1x0 \in L\} \in \mathbf{REG}.$$

First we show how to prove the theorem when $\sigma_n = (1, n)$. Indeed,

$$L_n^{(1,n)} = \{x \in 2^n: x_n x_2 \cdots x_{n-1} x_1 \in L\}$$

and this last set is the union of the following four sets:

$$\{x \in 2^n: 0x_2 \cdots x_{n-1}0 \in L\}, \qquad \{x \in 2^n: 1x_2 \cdots x_{n-1}1 \in L\},$$

$$\{x \in 2^n: 0x_2 \cdots x_{n-1}1 \in L\}, \qquad \{x \in 2^n: 1x_2 \cdots x_{n-1}0 \in L\}.$$

This completes the proof in view of the above claim. A similar proof will yield the result when each $\sigma_n = (1, 2)$. Next we use the above result for the transpositions $(1, n)$ to prove the result for the n-cycles, $\sigma_n = c_n$. Indeed,

$$\begin{aligned} L \in \mathbf{REG} &\Rightarrow \{x_1 \cdots x_n: x1 \in L\} \in \mathbf{REG} \\ &\Rightarrow \{x_1 \cdots x_n: x_1 \cdots x_n 1 \in L\} \in \mathbf{REG} \\ &\Rightarrow \{x_1 \cdots x_n: 1x_2 \cdots x_n x_1 \in L\} \in \mathbf{REG} \\ &\Rightarrow \{x_1 \cdots x_n: x_2 \cdots x_n x_1 \in L\} \in \mathbf{REG}. \end{aligned}$$

Finally, the theorem follows by using the following product formula, which is valid for any permutations $\tau_1, \tau_2 \in \mathbf{S}_n$,

$$L_n^{\tau_1\tau_2} = (L_n^{\tau_1})^{\tau_2}.$$

This completes the proof of the theorem. □

The assumption on term generation of the sequence $\langle \sigma_n: n \geqq 1 \rangle$ of permutations, made in the last theorem, is necessary as the following example shows.

Example 6. Let R be a recursively enumerable but nonrecursive set. Consider the permutation σ_n, which is equal to $(1, n)$, if $n \in R$, and is equal to id_n, if $n \notin R$, where id_n is the identity permutation on n letters. Consider the regular language defined by $L = 10^*$. Then it is easy to see that $L_n^\sigma = \{10^n: n+1 \notin R\} \cup \{0^n 1: n+1 \in R\}$. It follows that $n \in R \Leftrightarrow 0^{n-1}1 \in L^\sigma$. Hence, L^σ is not even a recursive language, although L is regular.

4. Constructing languages with given invariance groups. This section is concerned with the problem of realizing specific sequences of finite permutation groups by languages $L \subseteq \{0, 1\}^*$. A language L is said to realize a sequence $\mathbf{G} = \langle G_n: n \geqq 1 \rangle$ of permutation groups $G_n \leqq \mathbf{S}_n$ if it is true that $\mathbf{S}_n(L) = G_n$, for all n. We consider the following types of groups and determine regular as well as nonregular languages realizing them.

Reflection. $R_n = \langle \rho \rangle$, where $\rho(i) = n+1-i$ is the reflection permutation,

Cyclic. $C_n = \langle (1, 2, \cdots, n) \rangle$.

Dihedral. $D_n = C_n \times R_n$.

Hyperoctahedral. $O_n = \langle (i, i+1) \colon i \text{ is even} \leqq n \rangle$.

THEOREM 7. (1) *Each of the identity, reflection, cyclic (for $n \neq 3, 4, 5$), dihedral, and hyperoctahedral groups can be realized by regular languages.*

(2) *Each of the identity, cyclic, and dihedral groups can be realized by languages L such that $L \notin SIZE(n^{O(1)})$.*

Proof. (1) For each of the above-mentioned types of groups we provide a regular language realizing it.

Identity. This case is simple: take $L = 0^*1_*$.

Dihedral. Let $L = 0^*1^*0^* \cup 1^*0^*1^*$. It is clear that $D_n \subseteq \mathrm{S}_n(L)$. Let ρ be the reflection permutation defined by $\rho(i) = n+1-i$ and let $\sigma = (1, 2, \cdots, n)$. It is easy to check that $\sigma\rho\sigma = \rho$. It follows that $D_n = \{\sigma^k \rho^l \colon k \leqq n,\ l = 0, 1\}$. Next we prove the following claim.

CLAIM. *For all $\tau \in \mathrm{S}_n$, if addition is modulo n,*

$$\tau \in D_n \Leftrightarrow \forall i \leqq n (\tau(i+1) = \tau(i) + 1)$$

or

$$\forall i \leqq n (\tau(i) = \tau(i+1) + 1).$$

Proof of the claim. From left to right the equivalence is easily verified for the permutations $\sigma^k \rho^l$ $(1 \leqq k \leqq n,\ l = 0, 1)$. For example, $\sigma(i+1) = \sigma(i) + 1$ and $\rho(i) = \rho(i+1) + 1$. To prove the other direction, assume that τ satisfies the right-hand side. Say, $\tau(1) = k$. It is then easy to see that either $\tau = \sigma^{k-1}$ or $\tau = \sigma^k \rho$. This completes the proof of the claim.

It remains to show that $\mathrm{S}_n(L) \subseteq D_n$. If $n \leqq 3$ the result is trivial. So assume that $n \geqq 4$. Let $\tau \notin D_n$. There exists an $i \leqq n-1$ such that $|\tau(i+1) - \tau(i)| \geqq 2$. Let us suppose that $1 \leqq \tau(i) + 1 < \tau(i+1) \leqq n$. Then we have that

$$x = 0^{i-1} 1^2 0^{n+1-i} \in L_n, \qquad x^\tau = 0^{\tau(i)-1} 1 0^{\tau(i+1)-1} 1^{n-\tau(i+1)} \notin L_n.$$

Reflection. Let $L = 0^*1^*0^*$. It is clear that $R_n \subseteq \mathrm{S}_n(L)$. We want to show that $\mathrm{S}_n(L) \subseteq R_n$. By the proof given in the case of dihedral groups we have that $\mathrm{S}_n(L_n) \subseteq D_n$. Assume on the contrary that $\tau \in \mathrm{S}_n(L)$, but $\tau \in D_n - R_n$. It follows that $\tau = \sigma^i \rho$, for some $i \geqq 1$. Since $\rho \in \mathrm{S}_n(L)$ we obtain that $\sigma^i \in \mathrm{S}_n(L)$, which is a contradiction.

Cyclic. First assume that $n = 2$. Then consider the regular language

$$L = (01 \cup 10)0^*1^*$$

and notice that $\mathrm{S}_n(L) = (1, 2)$.

Next assume that $n \geqq 6$. Consider the regular language $L = L^1 \cap L^2$ where L^1 is the language

$$1^*0^*1^* \cup 0^*1^*0^* \cup 101000^*1 \cup 0^*1101000^* \cup 0^*011010$$
$$\cup\, 0^*001101 \cup 10^*00110 \cup 010^*0011$$

and L^2 is the language

$$\overline{10^*00101}.$$

Clearly, $C_n \subseteq \mathbf{S}_n(L)$. In view of the result on dihedral groups we have that $\mathbf{S}_n(L) \subsetneq D_n$. Let $x = 101000^{n-6}1 \in L_n$. Then $x^{\rho} = 10^{n-6}00101 \notin L_n$, where $\rho(i) = n+1-i$. Hence, $C_n = \mathbf{S}_n(L)$, for $n \geqq 6$.

It is interesting to note that for $3 \leqq n \leqq 5$ the groups C_n are not representable. This is obvious for $n=3$, since $C_3 = \mathbf{A}_3$. For $n = 4, 5$, one can show directly that for any boolean function $f \in \mathbf{B}_n$, if $C_n \subseteq \mathbf{S}(f) \subseteq D_n$ then $\mathbf{S}(f) = D_n$.

Hyperoctahedral. Consider the language L consisting of the set of all finite strings $x = (x_1, \cdots, x_k)$ such that for some $i \leqq k/2$, $x_{2i-1} = x_{2i}$. The regularity of the language follows from the obvious equality

$$L = (\Sigma\Sigma)^*(00 \cup 11)\Sigma^*.$$

For any set $I = \{i, j\}$ of indices, let f_I be the n-ary boolean function defined by

$$f_I(x) = \begin{cases} 1 & \text{if } x_i = x_j \\ 0 & \text{if } x_i \neq x_j. \end{cases}$$

Put $m = [n/2]$. For each $i = 1, \cdots, m$ consider the two-element sets $I_i = \{2i-1, 2i\}$ and the functions f_{I_i} defined above. Consider the boolean function

$$f = f_{I_1} \vee \cdots \vee f_{I_m}.$$

It is then clear that $\mathbf{S}_n(L) = \mathbf{S}(f)$. It is also easy to see that this last group consists of all permutations $\sigma \in \mathbf{S}_n$ which permute the blocks I_i, $i = 1, \cdots, m$. In fact this last group has exactly $2^{[n/2]} \cdot [n/2]!$ elements.

To prove part (2) of the theorem we use Lupanov's theorem (see § 2.3), i.e.,

$$|\{f \in \mathbf{B}_n \colon c(f) < q\}| = O(q^{q+1}).$$

Identity. By Lupanov's theorem we have that

$$|\{f \in \mathbf{B}_n \colon c(f) \leqq n^{\log n}\}| = 2^{O(n^{\log n}(\log n)^2)} \ll 2^{2^n} \sim |\{f \in \mathbf{B}_n \colon S(f) = 1\}|.$$

It follows that for all but a finite number of n there exists $f_n \in \mathbf{B}_n$ such that $L(f_n) \geqq n^{\log n}$ and $\mathbf{S}(f_n) = 1$. If we define a language L such that for all n, $L_n = f_n$, then the proof is complete.

Cyclic. The result will follow by a proof similar to the above if we could prove that

$$(3) \qquad |\{f \in \mathbf{B}_n \colon S(f) = D_n\}| \geqq 2^{2^n/n - n(n-1)/2} \gg 2^{O(n^{\log n}/n(\log n)^2)}.$$

Indeed, the left part of the above inequality is true because one may independently assign a value of 0, 1 to each orbit, except for orbits of words having 2 or 3 occurrences of the symbol 1. Let $\sigma = (1, 2, \cdots, n)$ be the n-cycle and let ρ be the reflection on n letters. We agree to have $f(v) \neq f(w)$, where $|v|_1 = |w|_1 = 2$ and

$$v \in \{(1^2 0^{n-2})^{\sigma^i} \colon 0 \leqq i \leqq n-1\}, \qquad w \in 2^n - \{(1^2 0^{n-2})^{\sigma^i} \colon 0 \leqq i \leqq n-1\}.$$

This removes n. Choose 2 independent choices while adding one choice of 0 or 1. We agree to have $f(v) \neq f(w)$, where $|v|_1 = |w|_1 = 3$ and

$$v \in \{(101000^{n-6}1)^{\sigma^i} \colon 0 \leqq i \leqq n-1\}, \qquad w \in \{(10^{n-6}00101)^{\sigma^i} \colon 0 \leqq i \leqq n-1\}.$$

Again, this removes n. Choose 2 independent choices while adding one choice of 0 or 1. Hence, the proof of the desired lower bound (1) is complete.

Dihedral. By [Ber71, p. 171], $\Theta(D_n) \geqq 2^{n-1}/n$. An argument similar to the one for cyclic groups used above shows that

$$|\{f \in \mathbf{B}_n : \mathrm{S}(f) = D_n\}| \geqq 2^{2^{n-1}/n - n(n-1)/2} \gg 2^{O(n^{\log n}/n(\log n)^2)}.$$

This completes the proof of the theorem. □

There is another interesting way for realizing the cyclic groups C_n, for $n \geqq 4$. For any groups G, H, put $[G, H] = \{g^{-1}h^{-1}gh : g \in G, h \in H\}$. Let $G, H \leqq \mathrm{S}_n$ be two permutation groups. Consider the set of words in G^* defined by

$$L_{G,H} = \{w \in G^* : w \in H\}.$$

(The reader should be warned of the different interpretation of w in the expressions $w \in G^*$ and $w \in H$; the former is a word in G^* and the latter is an element of a group.)

THEOREM 8. *For any permutation groups $G, H \leqq \mathrm{S}_n$, if $[G, G]$ is not a subset of the normal subgroup H of G, then $\mathrm{S}_n(L_{G,H}) = C_n$, for $n \geqq 4$.*

Proof. First we show that $C_n \subseteq \mathrm{S}_n^+(L_{G,H})$. Indeed, consider the cyclic permutation $c_n = (1, 2, \cdots, n)$ and notice that for $w = \sigma_1 \cdots \sigma_n \in G^*$,

$$w^{c_n} = \sigma_{c_n(1)} \cdots \sigma_{c_n(n)} = \sigma_2\sigma_3 \cdots \sigma_n\sigma_1 = \sigma_1^{-1} w \sigma_n.$$

It follows from the normality of H in G that $c_n \in \mathrm{S}_n^+(L_{G,H})$. This completes the proof of $C_n \subseteq \mathrm{S}_n^+(L_{G,H})$. Next we prove that $\mathrm{S}_n(L_{G,H}) \subseteq C_n$. Indeed, let ρ be a permutation in $\mathrm{S}_n - D_n$. It follows from the proof of Theorem 7 that either (A) there exists an i such that $|\rho(i+1) - \rho(i)| \bmod n > 1$, or (B) $|\rho(n) - \rho(1)| \bmod n > 1$. We show that $\rho \notin \mathrm{S}_n(L_{G,H})$. First we consider case (A) and distinguish four subcases.

Case 1. $1 \leqq \rho(i) < \rho(i+1)n$.

Let σ, τ be given such that $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \notin H$. Let $j = \rho^{-1}(\rho(i)+1)$, $k = \rho^{-1}(\rho(i+1)+1)$. Consider $w = \sigma_1 \cdots \sigma_n \in G^n$, where $\sigma_i = \sigma$, $\sigma_{i+1} = \sigma^{-1}$, $\sigma_j = \tau$, $\sigma_k = \tau^{-1}$, and all other σ_l's are equal to 1. Then we have that $w = \sigma\sigma^{-1}\tau\tau^{-1}$ or $\sigma\sigma^{-1}\tau^{-1}\tau$ depending, respectively, on whether or not $j < k$ or $k < j$. In either case $w = 1$, but $w^\rho = \sigma\tau\sigma^{-1}\tau^{-1} \notin H$.

Case 2. $\rho(i) < \rho(i+1) \leqq n$.

Let σ, τ be given such that $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \notin H$. Let $j = \rho^{-1}(\rho(i) - 1)$ and $k = \rho^{-1}(\rho(i)+1)$. Choose w such that $w = \sigma_1 \cdots \sigma_n \in G^n$, where $\sigma_j = \sigma$, $\sigma_{i+1} = \tau^{-1}$, $\sigma_i = \tau$, $\sigma_k = \sigma^{-1}$ and all other σ_l's are equal to 1. Then it is clear that $w = 1$, while $w^\rho \notin H$.

Case 3. $1 \leqq \rho(i+1) < \rho(i) < n$. This is similar to case 1.

Case 4. $1 < \rho(i+1) < \rho(i) \leqq n$. This is similar to case 1.

Case (B) is handled exactly as before. Hence, we have proved that $\mathrm{S}_n(L_{G,H}) \subseteq D_n$. It remains to show that in fact $\mathrm{S}_n(L_{G,H}) = C_n$. Since $[G, G]$ is not a subset of H, G/H cannot be abelian. Therefore, there exist elements $g_1, g_2, g_3, g_4 \in G$ such that

$$g_1g_2g_3g_4 \in H, \quad \text{but} \quad g_4g_3g_2g_1 \notin H.$$

It follows that the reflection permutation does not belong to $\mathrm{S}_n(L_{G,H})$, which completes the proof of the theorem. □

Given a language $L \subseteq \Sigma^*$ over the alphabet Σ the syntactic semigroup G_L of L is defined as follows. Define $w \equiv w' \bmod L$ if for all $u, v \in \Sigma^*$, $uwv \in L \Leftrightarrow uw'v \in L$. Then let G_L be the quotient of Σ^* modulo the equivalence relation $\equiv \bmod L$. Recall that the Krohn-Rhodes theorem [Arb69] states that the syntactic semigroup G_L of any given regular language L is the homomorphic image of a wreath product of cyclic simple groups, noncyclic simple groups, and three particular nongroup semigroups called "units." If G is abelian and $H = 1$, then it is clear that $\mathrm{S}_n(L_{G,H}) = \mathrm{S}_n$. If G is a nonabelian group and $H = 1$, then Theorem 8 yields that $\mathrm{S}_n(L_{G,H}) = C_n$. We have seen families of these groups as invariance groups of regular languages. However, we have examples of representable groups whose homomorphic image is not representable, (e.g., $(1, 2, 3)$ is the homomorphic image of $(1, 2, 3)(4, 5, 6)$), thus indicating that it is unlikely that the Krohn–Rhodes theorem can be used to characterize those families of invariance groups of regular languages. Similarly, from the examples given in the paper, there is no invariance group structure preserved when taking regular operations: from $S_n(L)$ and $S_n(L')$, we cannot say anything in general about $S_n(M)$, where $M = L \# L'$ and $\#$ is a boolean operation or language concatenation or where $M = L^*$ (Kleene star). This blocks a natural attempt to inductively define the families of invariance groups of regular languages.

It is not known whether there is a characterization of those sequences of groups which can be realized by regular languages. However, it is interesting to note that for regular languages L the invariance group $S_{2n}(L)$ can never be equal to the $\{1, 2, \cdots, n\}$ point-stabilizer of S_{2n}.

THEOREM 9. (1) *There is no regular language L such that for all but a finite number of n we have that*

$$S_{2n}(L) = (S_{2n})_{\{1,2,\cdots,n\}}.$$

(2) *There is a regular language L such that for all n we have that*

$$S_{2n}(L) = (S_{2n})_{\{2i: i \leqq n/2\}}.$$

Proof. (1) By the pumping lemma for regular languages [Harr78] there exist words a_i, b_i, $i < m$ and $\bar{a}_j$, $\bar{b}_j$, $j < \bar{m}$ and languages L_i, $\bar{L}_j$ such that

$$L = \bigcup_{im} a_i b_i^* L_i, \qquad \bar{L} = \bigcup_{i\bar{m}} \bar{a}_j \bar{b}_j^* \bar{L}_j,$$

where $\neg L = \{0, 1\}^* - L$ is the complement of L. Let r be the least common multiple of the lengths of all the above words. Put $i = r + 1$, $j = i + r$, and $n_0 = 3r$. Consider the transposition $\tau = (i, j)$ and let $n \geqq n_0$. Then for any word w of length n we consider the following two cases.

Case 1. $w \in L_n$.

Then for some $i_0 < m$ and some s we have that w must be of the form $a_{i_0} b_{i_0}^s c_{i_0}$. The ith position in the word w falls within the block b_{i_0}. Since the length of b_{i_0} divides r the jth position of the word w falls in exactly the same position with respect to the block b_{i_0}. It follows that $w_i = w_j$ and hence $w^\tau = w$.

Case 2. $w \notin L_n$.

This is similar to the proof of Case 1.

It follows from the above that $\tau \in S_n(L)$, as desired. This completes the proof of part (1).

(2) Consider the languages $L' = 0^*$ and $L'' = 1^*0^*$. It is clear that for all n, $S_n(L') = S_n$, and $S_n(L'') = 1$. Let L be the set of all words w of even length $2n$ such that

$$w_1 w_3 \cdots w_{2n-1} \in L', \qquad w_2 w_4 \cdots w_{2n} \in L''.$$

Clearly, L is a regular language and $S_{2n}(L) \supseteq (S_{2n})_{\{2i: i \leqq n/2\}}$. It remains to show that in fact $S_{2n}(L) \subseteq (S_{2n})_{\{2i: i \leqq n/2\}}$. Indeed, let $\sigma \in S_{2n}(L)$ and decompose σ as a product of the disjoint cycles $\sigma_1 \cdots \sigma_k$. Assume on the contrary that there exists an i_0 such that $\sigma_{i_0} = (a_1, \cdots, a_r)$ and

(i) either there exists a $1 \leqq j_0 < r$ such that a_{j_0} is even and a_{j_0+1} is odd,

(ii) or a_r is even and a_1 is odd.

We treat only case (ii), the other case being entirely similar. Consider a word w defined as follows. Let $w_1 = w_3 = \cdots = w_{2n-1} = 0$ and $w_2 = w_4 = \cdots = w_{a_r} = 1$ and the remaining w_i's equal to 0. Then $w \in L$. However, $(w^\sigma)_{a_1} = 1$, where a_1 is odd, and so

$$(w^\sigma)_1 (w^\sigma)_3 \cdots (w^\sigma)_{2n-1} \notin L'.$$

It follows that $w^\sigma \notin L$. Hence, $\sigma \notin \mathbf{S}_{2n}(L)$, a contradiction. □

5. Representations of permutation groups. The aim of this section is to give general results on permutation groups $G \leqq \mathbf{S}_n$ which can be represented as the invariance groups of boolean functions, i.e., $G = \mathbf{S}(f)$ for some $f \in \mathbf{B}_n$. It will be seen in the sequel that there is a rich class of permutation groups which are representable in this way.

The main motivation for the results of the present section is the simple observation that the alternating group $\mathbf{A}_n$ is not the invariance group of any boolean function $f \in \mathbf{B}_n$, provided that $n \geqq 3$. Although this will follow directly from our representation theorem it will be instructive to give a direct proof. Suppose that the invariance group of $f \in \mathbf{B}_n$ contains $\mathbf{A}_n$. Given $x \in 2^n$, for $3 \leqq n$, there exist $1 \leqq i < j \leqq n$ such that $x_i = x_j$. It follows that the alternating group $\mathbf{A}_n$ and a transposition fix f on x, and hence $\mathbf{S}_n$ does as well. As this holds for every $x \in 2^n$, it follows that $\mathbf{S}(f) = \mathbf{S}_n$. In fact it is clear, using part (1) of Theorem 1, that $\mathbf{A}_n$ is not isomorphic to the invariance group $\mathbf{S}(f)$ of any $f \in \mathbf{B}_n$. However, $\mathbf{A}_n$ is isomorphic to the invariance group $\mathbf{S}(f)$ for some boolean function $f \in \mathbf{B}_{n(\log n + 1)}$ (see Theorem 11 below).

One can generalize the notion of invariance group for any language $L \subseteq \{0, 1, \cdots, k\}^*$ by setting $L_n = L \cap \{0, \cdots, k\}^n$ and $\mathbf{S}(L_n)$ to be

$$\{\sigma \in \mathbf{S}_n : \forall x_1, \cdots, x_n \in \{0, 1, \cdots, k\}(x_1, \cdots, x_k \in L_n \Leftrightarrow x_{\sigma(1)}, \cdots, x_{\sigma(n)} \in L_n)\}.$$

We leave the details of the proof of the following fact as an exercise for the reader.

FACT. *For all n, there exist groups $G_n \leqq \mathbf{S}_n$ which are strongly representable as $G_n = \mathbf{S}(L_n)$ for some $L \subseteq \{0, 1, \cdots, n-1\}^n$ but which are not so representable for any language $L' \subseteq \{0, 1, \cdots, n-2\}^n$.*

Proof. The alternating group $\mathbf{A}_n = \mathbf{S}(L_n)$, where $L_n = \{w \in \{0, \cdots, n-1\}^n : \sigma_w \in \mathbf{A}_n\}$, where $\sigma_w : i \mapsto w(i-1)+1$. By a variant of the previous argument, $\mathbf{A}_n$ is not so representable by any language $L' \subseteq \{0, 1, \cdots, n-2\}^n$. □

Compared to the difficulties regarding the question of representing permutation groups $G \leqq \mathbf{S}_n$ in the form $G = \mathbf{S}(f)$, for some $f \in \mathbf{B}_n$, it is interesting to note that a similar representation theorem for the groups $\mathbf{S}(x) = \{\sigma \in \mathbf{S}_n : x^\sigma = x\}$, where $x \in 2^n$, is relatively easy. It turns out that these last groups are exactly the permutation groups which are isomorphic to $\mathbf{S}_k \times \mathbf{S}_{n-k}$ for some k. Indeed, given $x \in 2^n$ let

$$X = \{i : 1 \leqq i \leqq n \text{ and } x_i = 0\}, \qquad Y = \{i : 1 \leqq i \leqq n \text{ and } x_i = 1\}.$$

It is then easy to see that $\mathbf{S}(x)$ is isomorphic to $\mathbf{S}_X \times \mathbf{S}_Y$. In fact, $\sigma \in \mathbf{S}(x)$ if and only if $X^\sigma = X$ and $Y^\sigma = Y$.

5.1. Elementary properties. Before we proceed with the general results we will prove several simple observations that will be used frequently in the sequel. We begin with a few useful definitions. For any $f \in \mathbf{B}_n$, let $\mathbf{S}^+(f) = \{\sigma \in \mathbf{S}_n$: for all $x \in 2^n (f(x) = 0 \Rightarrow f(x^\sigma) = 0)\}$. For any permutation group $G \leqq \mathbf{S}_n$ and any $\Delta \subseteq \{1, 2, \cdots, n\}$ let G_Δ be the set of permutations $\sigma \in G$ such that (for all $i \in \Delta)(\sigma(i) = i)$. G_Δ is called the pointwise stabilizer of G on Δ. Notice that $(\mathbf{S}_n)_{\{k+1, \cdots, n\}} = S_k$, for $k \leqq n$. For any permutation σ and permutation group G let $G^\sigma = \sigma^{-1} G \sigma$, also called a conjugate of G by σ. For any $f \in \mathbf{B}_n$ let $1 \oplus f \in \mathbf{B}_n$ be defined by $(1 \oplus f)(x) = 1 \oplus f(x)$, for $x \in 2^n$. If $f_1, \cdots, f_k \in \mathbf{B}_n$ and $f \in \mathbf{B}_k$ then $g = f(f_1, \cdots, f_k) \in \mathbf{B}_n$ is defined by $g(x) = f(f_1(x), \cdots, f_k(x))$. The following theorem contains several useful observations that will be used frequently in the sequel.

THEOREM 10. (1) *If* $f \in \mathbf{B}_n$ *is symmetric then* $\mathbf{S}(f) = \mathbf{S}_n$.

(2) $\mathbf{S}(f) = \mathbf{S}(1 \oplus f)$, *for all* $f \in \mathbf{B}_n$.

(3) *For any permutation* σ, $\mathbf{S}(f^\sigma) = \mathbf{S}(f)^\sigma$.

(4) *For each* $f \in \mathbf{B}_n$, $\mathbf{S}(f) = \mathbf{S}^+(f)$.

(5) *If* $f_1, \cdots, f_k \in \mathbf{B}_n$ *and* $f \in \mathbf{B}_k$ *and* $g = f(f_1, \cdots, f_k) \in \mathbf{B}_n$ *then* $\mathbf{S}(f_1) \cap \cdots \cap \mathbf{S}(f_k) \subseteq \mathbf{S}(g)$.

(6) (*For all* $k \leqq n$)$(\exists f \in \mathbf{B}_n)\mathbf{S}(f) = \mathbf{S}_k$.

Proof. The proofs of (1)–(3), (5) are easy and are left as an exercise to the reader. To prove (4), notice that $\mathbf{S}^+(f)$ is a group and trivially $\mathbf{S}(f) \subseteq \mathbf{S}^+(f)$. Now let $\sigma \in \mathbf{S}^+(f)$ and suppose that $f(x^\sigma) = 0$ holds. Since, $\sigma^{-1} \in \mathbf{S}^+(f)$ we have that $f(x) = f((x^\sigma)^{\sigma^{-1}}) = 0$. It follows that $\mathbf{S}^+(f) \subseteq \mathbf{S}(f)$, as desired. To prove (6) we consider two cases. If $k+2 \leqq n$, define f by

$$f(x) = \begin{cases} 1 & \textit{if } x_{k+1} \leqq x_{k+2} \leqq \cdots \leqq x_n \\ 0 & \text{otherwise.} \end{cases}$$

Let $\sigma \in \mathbf{S}(f)$. First notice that for all $i > k(\sigma(i) > k)$. Next, it is easy to show that if σ is a nontrivial permutation then there can be no $k \leqq i < j \leqq n$ such that $\sigma(j) < \sigma(i)$. This proves the desired result. If $k = n-1$, then the function f must be defined as follows.

$$f(x) = \begin{cases} 1 & \textit{if } x_1, \cdots, x_{n-1} \leqq x_n \\ 0 & \text{otherwise.} \end{cases}$$

A similar proof will show that $\mathbf{S}(f) = \mathbf{S}_{n-1}$. This completes the proof of the theorem. □

We define a permutation group $G \leqq \mathbf{S}_n$ to be *representable* (respectively, *strongly representable*) if there exists an integer k and a function $f \in \mathbf{B}_{n,k}$ (respectively, with $k = 2$) such that $G = \mathbf{S}(f)$. $G \leqq \mathbf{S}_n$ is called *weakly representable* if there exists an integer k, an integer $m < n$, and a function $f: m^n \to k$ such that $G = \mathbf{S}(f)$. It will be seen in the sequel (representability theorem) that the distinction between representable and strongly representable is superfluous since these two notions coincide.

Notice the importance of assuming $m < n$ in the above definition of weak representability. If $m = n$ were allowed, then every permutation group would be weakly representable. Indeed, given any permutation group $G \leqq \mathbf{S}_n$ define the function f as follows:

$$f(x_1, \cdots, x_n) = \begin{cases} 0 & \textit{if } (x_1, \cdots, x_n) \in G \\ 1 & \text{otherwise} \end{cases}$$

(here, we think of $(x_1, \cdots, x_n)$ as the function $i \to x_i$ in n^n) and notice that for all $\sigma \in \mathbf{S}_n$, $\sigma \in \mathbf{S}(f)$ if and only if for all $\tau \in \mathbf{S}_n$ $(\tau \in G \Leftrightarrow \tau\sigma \in G)$. Hence $G = \mathbf{S}(f)$, as desired.

Another issue concerns the number of variables allowed in a boolean function in order to represent a permutation group $G \leqq \mathbf{S}_n$. We can also consider representing functions by using additional variables, but as the following theorem shows, every group becomes representable if enough variables are allowed.

THEOREM 11 (Isomorphism Theorem). *Every finite permutation group* $G \leqq \mathbf{S}_n$ *is isomorphic to the invariance group of a boolean function* $f \in \mathbf{B}_{n(\log n+1)}$.

Proof. First, let us give some notation. Let w be a word in $\{0, 1\}^*$. $|w|_1$ is the number of occurrences of 1 in w, and w_i is the ith symbol in w, where $1 \leqq i \leqq |w| =$ length of w. The word w is monotone if for all $1 \leqq i < j \leqq |w|$, $w_i = 1 \Rightarrow w_j = 1$. The complement of w, denoted by $\bar{w}$ is the word which is obtained from w by "flipping" each bit w_i, i.e., $|w| = |\bar{w}|$ and $\bar{w}_i = 1 \oplus w_i$, for all $1 \leqq i \leqq |w|$. Fix n and let $s = \log n + 1$. View each word $w \in \{0, 1\}^{ns}$ (of length ns) as consisting of n-many blocks, each of length s, and let $w(i) = w_{(i-1)s+1} \cdots w_{is}$ denote the ith such block. For a given permutation group $G \leqq \mathbf{S}_n$ let L_G be the set of all words $w \in \{0, 1\}^{ns}$ such that

- either (i) $|w|_1 = s$, and if the word w is divided into n-many blocks $w(1), w(2), \cdots, w(n)$, each of length s, then exactly one of these blocks consists of 1's, while the rest of the blocks consist only of 0's,
- or (ii) $|w|_1 \leqq s-1$ and for each $1 \leqq i \leqq n$, the complement $\bar{w}$ of the ith block of w is monotone (this implies that each $w(i)$ consists of a sequence of 1's concatenated with a sequence of 0's),
- or (iii) $|w|_1 \geqq n$ and for each $1 \leqq i \leqq n$, $w(i)_1 = 0$ (i.e., the first bit of $w(i)$ is 0) and the binary representations of the words $w(i)$, say $bin(w, i)$, are mutually distinct integers and $\sigma_w \in G$, where σ_w: $\{1, \cdots, n\} \to \{1, \cdots, n\}$ is the permutation defined by

$$\sigma_w(i) = bin(w, i).$$

The intuition for items (i) and (ii) above is the following. The words with exactly s-many 1's have all these 1's in exactly one block. This guarantees that any permutation "respecting" the language L_G must map blocks to blocks. By considering words with a single 1 (which by monotonicity must be located at the first position of a block) we guarantee that each permutation "respecting" L_G must map the first bit of a block to the first bit of some other block. Inductively, by considering the word with exactly $(r-1)$-many 1's, all located at the beginning of a single block, while all other bits of the word are 0's, we guarantee that each permutation "respecting" L_G must map the $(r-1)$st bit of each block to the $(r-1)$st bit of some other block. It follows that any permutation respecting L_G must respect blocks as well as the order of elements in the blocks; i.e., for every permutation $\tau \in \mathbf{S}_{ns}(L_G)$,

$$(\forall 0 \leqq k < n)(\exists 0 \leqq m < n)(\forall 1 \leqq i \leqq n)\tau(ks + i) = ms + i.$$

Call such a permutation "s-block invariant." Given a permutation $\tau \in \mathbf{S}_{ns}(L_G)$ let $\bar{\tau} \in \mathbf{S}_n$ be the induced permutation defined by

$$\bar{\tau}(k) = m \Leftrightarrow (\forall 1 \leqq i \leqq n)\tau(ks+i) = ms + i.$$

We claim that $G = \{\bar{\tau}\colon \tau \in \mathbf{S}^+_{ns}(L_G)\}$. Indeed, to prove ($\subseteq$) notice that every element $\bar{\tau}$ of G gives rise to a unique "s-block invariant" permutation τ. If $w \in L_G$ and $|w|_1 \leqq s$, then by s-block invariance of τ, $w^\tau \in L_G$. This proves ($\subseteq$). If $w \in L_G$ and $\sigma_w \in G$, then $\sigma_{(w^\tau)} = \sigma_w \bar{\tau} \in G$ (composition is from the right). To prove ($\supseteq$) let $w \in L_G$ be such that σ_w is the identity on $\mathbf{S}_n$. Then for any $\tau \in \mathbf{S}_{ns}(L_G)$, $w^\tau \in L_G$, so $\sigma_{(w^\tau)} = \sigma_w \bar{\tau} = \bar{\tau} \in G$, which proves the above claim. This completes the proof of the theorem. □

Clearly, the idea of the proof of the previous theorem can also be used to show that for any alphabet Σ, if $L \subseteq \Sigma^n$, then $\mathbf{S}_n(L)$ (the set of permutations in $\mathbf{S}_n$ "respecting" the language L) is isomorphic to $\mathbf{S}_{ns}(L')$, for some $L' \subseteq \{0, 1\}^{ns}$, where $s = 1 + \log|\Sigma|$.

We conclude by comparing the different definitions of representability given above.

THEOREM 12. *For any permutation group $G \leqq \mathbf{S}_n$ the following statements are equivalent*:

(1) *G is representable.*

(2) *G is the intersection of a finite family of strongly representable permutation groups.*

(3) *For some m, G is a pointwise stabilizer of a strongly representable group over $\mathbf{S}_{n+m}$, i.e., $G = (\mathbf{S}_{n+m}(f))_{\{n+1,\cdots,n+m\}}$, for some $f \in \mathbf{B}_{n+m}$ and $m \leqq n$.*

Proof. First we prove that (1)⇒(2). Indeed, let $f \in \mathbf{B}_{n,k}$ such that $G = \mathbf{S}(f)$. For each $b < k$ define as follows a 2-valued function $f_b: 2^n \to \{b, k\}$:

$$f_b(x) = \begin{cases} b & \text{if } f(x) = b \\ k & \text{if } f(x) \neq b. \end{cases}$$

It is straightforward to show that

$$\mathbf{S}(f) = \mathbf{S}(f_0) \cap \cdots \cap \mathbf{S}(f_{k-1}).$$

But also, conversely, we can prove that (2)⇒(1). Indeed, assume that $f_b \in \mathbf{B}_n$, $b < k$, is a given family of boolean valued functions such that G is the intersection of the strongly representable groups $\mathbf{S}(f_b)$. Define $f \in \mathbf{B}_{n,2^k}$ as follows:

$$f(x) = \langle f_0(x), \cdots, f_{k-1}(x) \rangle,$$

where for any integers $n_0, \cdots, n_{k-1}$, the symbol $\langle n_0, \cdots, n_{k-1} \rangle$ represents a standard coding of the k-tuple $(n_0, \cdots, n_{k-1})$. It is then clear that $\mathbf{S}(f) = \mathbf{S}(f_0) \cap \cdots \cap \mathbf{S}(f_{k-1})$, as desired.

To prove that (3) is equivalent to statements (1) and (2) it is enough to show that (i) for any family $\{f_i: 0 \leqq i \leqq k\}$ of boolean functions $f_i \in \mathbf{B}_n$ there exists an integer $0 \leqq m \leqq \log k$ and a boolean function $f \in \mathbf{B}_{n+m}$ such that

$$(\mathbf{S}(f))_{\{n+1, \cdots, n+m\}} = \mathbf{S}(f_1) \cap \cdots \cap \mathbf{S}(f_k), \tag{4}$$

and (ii) also conversely, for any integer $m \geqq 0$, and any boolean function $f \in \mathbf{B}_{n+m}$ there exist boolean functions $\{f_i: 0 \leqq i \leqq k\}$, with $k \leqq 2^m$ such that equation (1) holds.

Indeed, part (i) of the above statement follows by repeated application of part (6) of Theorem 10 and the case $k = 2$ of the above statement. To prove the case $k = 2$, define $f(x_1, \cdots, x_n, i) = f_i(x_1, \cdots, x_n)$. The desired equality is now easily proved. To prove the converse part (ii), let m, f be as in the hypothesis and define the desired family of functions $f_{b_1, \cdots, b_m}$ as follows.

$$f_{b_1, \cdots, b_m}(x_1, \cdots, x_n) = f(x_1, \cdots, x_n, b_1, \cdots, b_m).$$

It is now easy to see that equation (1) is satisfied. This completes the proof of the theorem. □

5.2. Representation theorems for general permutation groups. Here we study the representability problem for general permutation groups, give a necessary and sufficient condition via Pólya's cycle index for a permutation group to be representable, and show that the notions of representable and strongly representable coincide. In order to state the first general representation theorem we define, for any $n + 1 \leqq \theta \leqq 2^n$ and any permutation group $G \leqq \mathbf{S}_n$, the set $\mathbf{G}_\theta^{(n)} = \{M \leqq G: \Theta_n(M) = \theta\}$. Also, for any $H \subseteq \mathbf{S}_n$, and any $g \in \mathbf{S}_n$, the notation $\langle H, g \rangle$ denotes the least subgroup of $\mathbf{S}_n$ containing the set $H \cup \{g\}$.

THEOREM 13 (Representation Theorem). *The following statements are equivalent for any permutation groups $H < G \leqq \mathbf{S}_n$.*

(1) *$H = G \cap K$, for some strongly representable permutation group $K \leqq \mathbf{S}_n$.*

(2) *$H = G \cap K$, for some representable permutation group $K \leqq \mathbf{S}_n$.*

(3) *(for all $g \in G - H$)$(\Theta_n(\langle H, g \rangle) < \Theta_n(H))$.*

(4) *H is maximal in $\mathbf{G}_\theta^{(n)}$, where $\Theta_n(H) = \theta$.*

Proof. We prove the equivalence of the above statements by showing the following sequence of implications: (1)⇒(2)⇒(3)⇒(1) and (4)⇒(3)⇒(4). The proof of (1)⇒(2) is trivial. First, we prove (2)⇒(3). By Theorem 12, K is the intersection of a family of strongly representable groups. Hence, by assumption let $\mathbf{S}(f_i)$, where $\{f_i\} \subseteq \mathbf{B}_n$, be a finite family of invariance groups such that

$$H = \bigcap_i \mathbf{S}(f_i) \cap G.$$

Assume on the contrary that there exists an $H\ K \leqq G$ such that $\Theta(K) = \Theta(H)$. This last statement is equivalent to the statement

$$\forall x \in 2^n\ (x^K = x^H).$$

We show that in fact

$$K \subseteq \bigcap_i \mathbf{S}(f_i) \cap G,$$

which is a contradiction, since the right-hand side of the above inequality is equal to H. Indeed, let $\sigma \in K$ and $x \in 2^n$. Then we know that

$$x^K = (x^\sigma)^K = (x^\sigma)^H.$$

It follows that $x = (x^\sigma)^\tau$, for some $\tau \in H$. Consequently, $f_i(x) = f_i((x^\sigma)^\tau) = f_i(x^\sigma)$, as desired.

Next we prove that (3)$\Rightarrow$(1). Let $P_n(X)$ be the property of subgroups stated by $X \leqq \mathbf{S}_n \wedge (\text{for all } L > X)(\Theta_n(L) < \Theta_n(X))$. (When n and $X \leqq S_n$ are clear from context, we say simply that X satisfies property P.)

Claim. *For all n and subgroups X of $\mathbf{S}_n$,*

$$P_n(X) \Leftrightarrow X \textit{ is strongly representable.}$$

Proof. As the direction from right to left is obvious, we only consider the direction from left to right. Suppose, in order to obtain a contradiction, that this direction fails. Let $X \leqq \mathbf{S}_n$ be of *maximal* size such that $P_n(X)$ holds, but that X is not strongly representable. It follows that

$$(\forall L > X)(L \text{ satisfies } P \Rightarrow L \text{ is strongly representable}).$$

Since the full symmetric group $\mathbf{S}_n$ is strongly representable we can assume, without loss of generality, that $X < \mathbf{S}_n$. In particular, there is a strongly representable group $L > X$ of *minimal* size. Let $h \in \mathbf{B}_n$ be such that $L = \mathbf{S}(h)$. Thus,

$$(*) \qquad \forall M(X < M < L \Rightarrow M \text{ does not satisfy } P).$$

Since $P_n(X)$ holds, we have that $\Theta_n(L) < \Theta_n(K)$. It follows that there exist $x, y \in 2^n$ such that

$$x = y \bmod L, \qquad x \neq y \bmod X,$$

where for $H \leqq \mathbf{S}_n$ and $x, y \in 2^n$ the symbol $x = y \bmod H$ means that $y = x^\sigma$, for some $\sigma \in H$. Define a boolean function $g \in \mathbf{B}_n$ as follows, for $w \in 2^n$,

$$g(w) = \begin{cases} h(w) & \textit{if } w \neq x \bmod X, \quad w \neq y \bmod X \\ 0 & \textit{if } w = x \bmod X \\ 1 & \textit{if } w = y \bmod X. \end{cases}$$

It follows from the definition of g that $X \leqq \mathbf{S}(g) < \mathbf{S}(h) = L$. Since every strongly representable group satisfies property P, an immediate consequence of $(*)$ is that $X = \mathbf{S}(g)$. This completes the proof of the claim. $\square$

Now returning to the proof of (3)⇒(1), by assumption, for all $g \in G-H$, $2^{\Theta_n(\langle H,g\rangle)} < 2^{\Theta_n(H)}$. In particular, for all $g \in G-H$, there exists a boolean function $f_g \in \mathbf{B}_n$ such that $H \leqq \mathbf{S}_n(f_g)$, but $\langle H, g\rangle$ is not a subset of $\mathbf{S}_n(f_g)$. Consider the representable group K defined by

$$K = \bigcap_{g \in G-H} \mathbf{S}(f_g).$$

It is now trivial to check that $H = K \cap G$. Moreover, as in the implication (2)⇒(3) above, it follows that the permutation group K satisfies property P. By the above claim, K is strongly representable. This concludes the proof (3)⇒(1).

It remains to prove the equivalence of the last statement of the theorem. First we prove (4)⇒(3). Assume that H is a maximal element of $\mathbf{G}_\theta^{(n)}$, but that for some $g \in G-H$, we have that $\Theta_n(\langle H, g\rangle) = \Theta_n(H)$. But then $H < \langle H, g\rangle \leqq G$, contradicting the maximality of H. Finally, we prove (3)⇒(4). Assume on the contrary that (3) is true but that H is not maximal in $\mathbf{G}_\theta^{(n)}$. This means there exists $H < K \leqq G$ such that $\Theta_n(K) = \Theta_n(H)$. Take any $g \in K-H$ and notice that

$$\Theta_n(\langle H, g\rangle) \geqq \Theta_n(K) = \theta = \Theta_n(H) \geqq \Theta_n(\langle H, g\rangle).$$

Hence, $\Theta_n(H) = \Theta_n(\langle H, g\rangle)$, contradicting (3). □

A "naive" algorithm for testing the representability of a general permutation group $G \leqq \mathbf{S}_n$ is to test all boolean functions $f \in \mathbf{B}_n$ to see if $G = \mathbf{S}_n(f)$. Clearly, this requires time 2^{2^n}. An immediate consequence of the representation theorem is the following algorithm whose running time is $O((n!)^2) = 2^{O(n \log n)}$.

Algorithm for Deciding the Representability of Permutation Groups Input
A permutation group $G \leqq \mathbf{S}_n$.
for each $\sigma \in \mathbf{S}_n - G$ **do**
  if $\Theta_n(\langle G, \sigma\rangle) = \Theta_n(G)$
  then output G is not representable.
od
else output G is representable.
end

The well-known graph nonisomorphism problem (**NGIP**) is related to the above group representation problem. Indeed, let

$$G = (\{v_1, \cdots, v_n\}, E_G), \qquad H = (\{u_1, \cdots, u_n\}, E_H)$$

be two graphs on n vertices each. Consider the permutation group $ISO(G, H) \leqq \mathbf{S}_{n+3}$ whose generators σ satisfy:

$$\forall 1 \leqq i, \qquad j \leqq n(E_G(v_i, v_j) \Leftrightarrow E_H(u_{\sigma(i)}, u_{\sigma(j)})),$$

and in addition the permutation $n+i \to \sigma(n+i)$, $i = 1, 2, 3$, belongs to the group $C_3 = (n+1, n+2, n+3)$. It is easy to show that if G, H are isomorphic, then there exists a group $K \leqq \mathbf{S}_n$ such that $ISO(G, H) = K \times C_3$. On the other hand, if G, H are not isomorphic, then $ISO(G, H) = \langle id_{n+3}\rangle$. As a consequence of the nonrepresentability of C_3, and the representability theorem of direct products, it follows that G, H are not isomorphic if and only if $ISO(G, H) = \langle id_{n+3}\rangle$.

Remark. An idea similar to that used in the proof of the representation theorem can also be used to show that for any representable permutation groups $G < H \leqq \mathbf{S}_n$,

$$2 \cdot |\{h \in \mathbf{B}_n : H = \mathbf{S}(h)\}| \leqq |\{g \in \mathbf{B}_n : G = \mathbf{S}(g)\}|.$$

Indeed, assume that G, H are as above. Without loss of generality we may assume that there is no representable group K such that $G < K < H$. As in the proof of the representation theorem there exist $x, y \in 2^n$ such that $x = y \bmod H$, $x \neq y \bmod G$. Define two boolean functions $h_b \in \mathbf{B}_n$, $b = 0, 1$, as follows from $w \in 2^n$,

$$h_b(w) = \begin{cases} h(w) & \text{if } w \neq x \bmod G, \quad w \neq y \bmod G \\ b & \text{if } w = x \bmod G \\ \bar{b} & \text{if } w = y \bmod G. \end{cases}$$

Since $G \leqq \mathbf{S}(h_b) < \mathbf{S}(h)$, it follows from the above definition that each $h \in \mathbf{B}_n$ with $H = \mathbf{S}(h)$ gives rise to two distinct $h_b \in \mathbf{B}_n$, $b = 0, 1$, such that $G = \mathbf{S}(h_b)$. Moreover, it is not difficult to check that the mapping $h \to \{h_0, h_1\}$, where $H = \mathbf{S}(h)$, is $1-1$. It is now easy to complete the proof of the assertion.

An immediate consequence of the representation theorem is that all cycle indices $\Theta_n(G)$ can in fact be realized by representable permutation groups. The previous theorem also has a consequence concerning the representation of "maximal" permutation groups.

THEOREM 14 (Maximality Theorem). (1) *If H is a maximal proper subgroup of $G \leqq \mathbf{S}_n$ then*

$$\Theta_n(G) < \Theta_n(H) \Leftrightarrow (\exists f \in \mathbf{B}_n)(H = G \cap \mathbf{S}(f)).$$

(2) *All maximal subgroups of $\mathbf{S}_n$ are strongly representable, the only exceptions being*: (a) *the alternating group $\mathbf{A}_n$, for all $n \geqq 3$*; (b) *the 1-dimensional, linear, affine group $AGL_1(5)$ over the field of five elements, for $n = 5$*; (c) *the group of linear transformations $PGL_2(5)$ of the projective line over the field of five elements, for $n = 6$*; (d) *the group of semilinear transformations $P\Gamma L_2(8)$ of the projective line of the field of eight elements, for $n = 9$.*

Proof. To prove (1) let H be a maximal proper subgroup of G such that $\Theta_n(G) < \Theta_n(H)$. Put $\theta = \Theta_n(H)$. Since condition (4) of the representation theorem is satisfied, H is of the form $\mathbf{S}(f)$, for some $f \in \mathbf{B}_n$. This completes the proof of ($\Rightarrow$). To prove the other direction, assume that $\Theta_n(G) = \Theta_n(H)$. Then for all $g \in G - H$, $\Theta_n(\langle H, g\rangle) = \Theta_n(H)$. Hence, again by the representation theorem, there is no $f \in \mathbf{B}_n$ such that $H = G \cap \mathbf{S}(f)$. This completes the proof of (1).

To prove (2) let M be a maximal subgroup of $\mathbf{S}_n$. We distinguish two cases.

Case 1. $\Theta_n(M) > n+1$.

In this case, part (1) of this theorem implies that M is strongly representable, since $\Theta_n(\mathbf{S}_n) = n+1$. (Note that by Theorem 2(4), the condition of Case 1 is satisfied by all intransitive groups M, i.e., groups with $\omega_n(M) \geqq 2$.)

Case 2. $\Theta_n(M) = n+1$.

In this case we know from the main theorem of [BP55] that M is of one of the forms in the statement of the theorem. □

As noted above, all maximal permutation groups with the exception of $\mathbf{A}_n$ are of the form $\mathbf{S}(f)$, provided that $n \geqq 10$. Such maximal permutation groups include: the cartesian products $\mathbf{S}_k \times \mathbf{S}_{n-k}$ $(k \leqq n/2)$, the wreath products $\mathbf{S}_k \wr \mathbf{S}_l$ $(n = kl,\ k, l > 1)$, the affine groups $AGL_d(p)$, for $n = p^d$, etc. The interested reader will find a complete survey of classification results for maximal permutation groups in [KL88]. It should also be pointed out that there are plenty of nonmaximal permutation groups which are not representable. In fact, it can be verified that examples of such groups are the wreath products $G \wr \mathbf{A}_n$. In general we can prove the following theorem. For any permutation groups $G \leqq \mathbf{S}_m$, $H \leqq \mathbf{S}_n$.

THEOREM 15. *Let* $G \leqq \mathbf{S}_m$, $H \leqq \mathbf{S}_n$. *Then*

(1) *G and H representable* $\Rightarrow G \wr H$ *is representable.*

(2) $G \wr H$ *is representable* $\Rightarrow H$ *is representable.*

(3) $G \wr H$ *is representable and* $2^n < m \Rightarrow G$ *is weakly representable.*

(4) *For p prime, a p-Sylow subgroup P of* $\mathbf{S}_n$ *is representable* $\Leftrightarrow p \neq 3, 4, 5$.

Proof. (1) Suppose we are given two representable groups $G = \mathbf{S}(L_G) \leqq \mathbf{S}_m$, $H = \mathbf{S}(L_H) \leqq \mathbf{S}_n$, where $L_G \subseteq \{0, 1\}^m$, $L_H \subseteq \{0, 1\}^n$. We want to show that the wreath product $G \wr H \leqq \mathbf{S}_{mn}$ is representable. The wreath product $G \wr H$ consists of all permutations $\rho = [\sigma; \tau_1, \cdots, \tau_m]$, where $\sigma \in G$ and $\tau_1, \cdots, \tau_m \in H$, such that

$$\rho((k-1)n + i) = \sigma(k)n + \tau_{\sigma(k)}(i),$$

for $1 \leqq k \leqq m$, $1 \leqq i \leqq n$. (Intuitively speaking, ρ acts on $m \times n$ matrices in such a way that τ_i acts only on the ith row and σ permutes rows.) Without loss of generality we can assume that $0^m, 1^m \in L_G$ and $0^n, 1^n \in L_H$. Define a set $L \subseteq \{0, 1\}^{mn}$ of words w by the disjunctoin of the following three clauses:

(a) $|w|_1 = n$, and for some $0 \leqq k < m$, $w_{kn+1} = \cdots = w_{kn+n} = 1$ (i.e., the $(k+1)$st row consists only of 1's).

(b) $|w|_1 > n$, and w is of the form $e_1^n e_2^n \cdots e_m^n$, where the word $e_1 e_2 \cdots e_m \in L_G$.

(c) $|w|_1 > n$ and w is not of the form $e_1^n e_2^n \cdots e_m^n$, but $w_{kn+1} \cdots w_{kn+n} \in L_H$, for all $0 \leqq k < m$.

We claim that $\mathbf{S}_{mn}(L) = G \wr H$. Indeed, the inequality $G \wr H \subseteq \mathbf{S}_{mn}(L)$ is clear. To prove the other direction assume that $\rho \in \mathbf{S}_{mn}(L)$. By clause (a), ρ respects the n-blocks of words of length mn. Hence, ρ is of the form $\rho = [\sigma; \tau_1, \cdots, \tau_m]$, and $\tau_i \in \mathbf{S}_n$, $\sigma \in G$, where $i = 1, \cdots, m$. If $\sigma \notin G$, then there is a word v of length m, with $v \in L_G$ and $v^\sigma \notin L_G$. Then (using clause (b) above) we have that $w = v_1^n v_2^n \cdots v_m^n \in L$, but $w^\rho \notin L$, which is a contradiction. If for some i, $\tau_i \notin H$, then there is a word v of length n such that $v \in L_H$ and $v^{\tau_i} \notin L_H$. It follows (by clause (c) above) that the word $w = v \cdots v \in L$, but $w^\rho \notin L$, a contradiction. This completes the proof of (1).

(2) By assumption, $G \wr H = \mathbf{S}_{mn}(f)$, for some $f \in \mathbf{B}_{mn}$. Hence,

$$G \wr H = \{[\sigma; \tau_1, \cdots, \tau_m] \in \mathbf{S}_m \wr \mathbf{S}_n \colon (\forall X_1, \cdots, X_m) f(X_{\sigma(1)}^{\tau_1}, \cdots, X_{\sigma(m)}^{\tau_m}) = f(X_1, \cdots, X_m)\}.$$

In particular, we have that

$$\begin{aligned} \tau \in H &\Leftrightarrow [id_m; \tau, id_n, \cdots, id_n] \in G \wr H \\ &\Leftrightarrow \forall X_1[\forall X_2, \cdots, X_m(f_{X_2,\cdots,X_m}(X_1^\tau) = f_{X_2,\cdots,X_m}(X_1))] \\ &\Leftrightarrow \tau \in \bigcap_{X_2,\cdots,X_m \in 2^n} \mathbf{S}(f_{X_2,\cdots,X_m}), \end{aligned}$$

as desired.

The proof of (3) is similar and uses the simple observation that for any permutation $\sigma \in \mathbf{S}_m$,

$$[\sigma; id_n, \cdots, id_n] \in G \wr 1 \Leftrightarrow (\forall X_1, \cdots, X_m) f(X_{\sigma(1)}, \cdots, X_{\sigma(m)}) = f(X_1, \cdots, X_m).$$

(4) Let p be a prime $p \leqq n$. By Sylow's theorem, all the p-Sylow subgroups of $\mathbf{S}_n$ are conjugates of one another. Moreover, by [Pas66, pp. 8-11], if C is the cyclic group $(1, 2, \cdots, p)$, then there exists an integer r such if we iterate the wreath product r times on C then the group $C \wr C \cdots \wr C$ obtained is a p-Sylow subgroup of $\mathbf{S}_n$. Combining this with the previous assertions of the theorem, as well as part (3) of Theorem 10, we obtain the desired result. □

The converse of part (1) of the above theorem is not necessarily true. This is easy to see from the following example. We show that the wreath product $\mathbf{A}_3 \wr \mathbf{S}_2$ is representable, but that $\mathbf{A}_3$ is not. Indeed, consider the language

$$L = \{001101, 010011, 110100, 001110, 100011, 111000\} \subseteq 2^6.$$

We already proved that $\mathbf{A}_3$ is not representable. We claim that $\mathbf{A}_3 \wr \mathbf{S}_2 = \mathbf{S}_6(L)$. Consider the three-cycle $\tau = (\{1,2\}, \{3,4\}, \{5,6\})$. It is easy to see $\mathbf{A}_3 \wr \mathbf{S}_2$ consists of the 24 permutations σ in $\mathbf{S}_6$ which permute the two-element sets $\{1,2\}$, $\{3,4\}$, $\{5,6\}$ as in the three-cycles τ, τ^2, τ^3. A straightforward (but tedious) computation shows that $\mathbf{S}_6(L)$ also consists of exactly the above 24 permutations.

Another class of examples of nonrepresentable groups is given by the direct products of the form $\mathbf{A}_m \times G$, $G \times \mathbf{A}_m$, where G is any permutation group acting on a set which is disjoint from $\{1, 2, \cdots, m\}$, $m \geqq 3$ (for a proof of this, see the next subsection).

We conclude this section by showing the representability of the normalizers of groups G generated by a family of "disjoint" transpositions. Let G be a subgroup of $\mathbf{S}_n$ and let $H = \langle H(x)\colon x \in 2^n \rangle$ be a family of normal subgroups of $N(G)$ (the normalizer of G in $\mathbf{S}_n$) such that for all $\sigma \in N(G)$, $x \in 2^n$, $H(x) = H(\sigma(x))$. (This last condition is satisfied if, for example, each $H(x) = 1$ or each $H(x) = G$.) For any $x \in 2^n$ let $G_x = \{\sigma \in G\colon x^\sigma = x\}$ be the stabilizer of G at x. Define the function $f_{G,H}: 2^n \to 2$ as follows:

$$f_{G,H}(x) = \begin{cases} 1 & \text{if } G_x = H(x) \\ 0 & \text{if } G_x \neq H(x). \end{cases}$$

Normalizers of certain permutation groups can be written in the form $\mathbf{S}(f)$. To see this observe the following two claims.

(1) $N(G) \subseteq \mathbf{S}(f_{G,H})$.

(2) If (for all $\sigma \in \mathbf{S}_n$) [(for all $x \in 2^n$) $(G_x = H(x) \Leftrightarrow G_{\sigma(x)} = H(x)) \Rightarrow G^\sigma = G$] then there exists an $f \in \mathbf{B}_n$ such that $N(G) = \mathbf{S}(f)$.

For convenience, let $\sigma(x)$ denote x^σ. To prove (1) let $\sigma \in N(G)$. This means that $G^\sigma = G$. We want to show that

$$\forall x \in 2^n (G_x = H(x) \Leftrightarrow G_{\sigma(x)} = H(x)).$$

To prove the implication ($\Rightarrow$) notice that

$$H(x) = G_x = (G^\sigma)_x = (G_{\sigma(x)})^\sigma = H(x)^\sigma.$$

Hence, $H(x) = G_{\sigma(x)}$, as desired. The converse ($\Leftarrow$) is similar.

The proof of assertion (2) is immediate. The hypothesis is simply a restatement of the condition $\mathbf{S}(f_{G,H}) \subseteq N(G)$.

5.3. A logspace algorithm for the representability of cyclic groups. This section is devoted to the proof of the existence and correctness of a logspace algorithm which, when given as input a cyclic group $G \leqq \mathbf{S}_n$, decides whether the group is representable, in which case it outputs a boolean function $f \in \mathbf{B}_{n,k}$ such that $G = \mathbf{S}(f)$. The algorithm is as follows.

Algorithm for Representing Cyclic Groups

Input

$G = \langle \sigma \rangle$ cyclic group.

Step 1

Decompose $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$, where $\sigma_1, \sigma_2, \cdots, \sigma_k$ are disjoint cycles of lengths $l_1, l_2, \cdots, l_k \geqq 2$, respectively.

Step 2
if for all $1 \leqq i \leqq k$,
$l_i = 3 \Rightarrow (\exists j \neq i)(3 \mid l_j)$ **and**
$l_i = 4 \Rightarrow (\exists j \neq i)(\gcd(4, l_j) \neq 1)$ **and**
$l_i = 5 \Rightarrow (\exists j \neq i)(5 \mid l_j)$
then output G is representable.
else output G is not representable.
end

At the present time, we do not know how to efficiently test the representability of arbitrary abelian groups (or other natural classes of groups such as solvable, nilpotent, etc.). *If* a given abelian group K can be decomposed into *disjoint* cyclic factors, *then* we have the following NC algorithm for testing representability: (1) use an NC algorithm [LM85], [MC85], [Mul86] to "factor" K into its cyclic factors and then (2) apply the "cyclic-group" algorithm to each of the cyclic factors of K. In view of the lemma below, the group K is representable exactly when each of its disjoint, cyclic factors is.

LEMMA 16. *Let $G \leqq \mathbf{S}_m$, $H \leqq \mathbf{S}_n$ be permutation groups. Then $G \times H$ is representable $\Leftrightarrow$ both G, H are representable.*

Proof. ($\Rightarrow$) By the representability of the groups G, H there exist boolean functions $f \in \mathbf{B}_m$ and $g \in \mathbf{B}_n$ such that $G \times H = \mathbf{S}(f) \times \mathbf{S}(g)$. By the maximality theorem there exists a function $h: 2^{m+n} \to 2$ such that $\mathbf{S}(h) = \mathbf{S}_m \times \mathbf{S}_n$. Hence, if we put $F(x, y) = \langle f(x), g(y) \rangle$, then it is easy to see that

$$\mathbf{S}(f) \times \mathbf{S}(g) = \mathbf{S}(h) \cap \mathbf{S}(F).$$

This implies that $G \times H$ is representable, and hence also strongly representable.

To prove ($\Leftarrow$) assume that $G \times H = \mathbf{S}(f)$, for some $f: 2^{m+n} \to k$. It is then easy to see that

$$\begin{aligned} G &= \{\sigma \in \mathbf{S}_m : \langle \sigma, id_n \rangle \in G \times H\} \\ &= \{\sigma \in \mathbf{S}_m : (\forall x, y)(f(x^\sigma, y) = f(x, y))\} \\ &= \{\sigma \in \mathbf{S}_m : (\forall y)(f_y^\sigma = f_y)\} \\ &= \bigcap_{y \in 2^n} \mathbf{S}(f_y). \end{aligned}$$

A similar proof works for the group H. □

The main result of the present section is the following theorem.

THEOREM 17 (Cyclic Group Representability Theorem). *There is a logspace algorithm which, when given as input a cyclic group $G \leqq \mathbf{S}_n$, decides whether the group is representable, in which case it outputs a function $f \in \mathbf{B}_n$ such that $G = \mathbf{S}(f)$.*

The rest of this section is dedicated to the proof (sketch) of correctness of the above algorithm. The proof is in a series of lemmas. For technical reasons, we introduce two definitions. A boolean function $f \in \mathbf{B}_n$ is called *special* if for all words w of length n,

$$|w|_1 = 1 \Rightarrow f(w) = 1.$$

Let $\sigma_1, \cdots, \sigma_k$ be a collection of cycles. We say that the group $G = \sigma_1, \cdots, \sigma_k$, generated by the permutations $\sigma_1, \cdots, \sigma_k$, is *specially representable* if there exists a special boolean function $f: 2^\Omega \to 2$ (where Ω is the union of the supports of the σ_i's) such that $G = \mathbf{S}(f)$. The support of a permutation σ, denoted by *Supp*(σ), is the set of i such that $\sigma(i) \neq i$. The support of a permutation group G, denoted $Supp(G)$, is the union of the supports of the elements of G.

5.4. Main ideas of the proof. Before proceeding with the details, it will be instructive to give an outline of the main ideas needed for the corectness proof. We are given a cyclic group G generated by a permutation σ. Decompose σ into disjoint cycles $\sigma_1, \sigma_2, \cdots, \sigma_k$ of lengths $l_1, l_2, \cdots, l_k \geqq 2$, respectively.

If $k=1$ then we know that G is specially representable exactly when $l_1 \neq 3, 4, 5$. (The representability of the cyclic group C_s, for $s \neq 3, 4, 5$ is proved in § 4; for $s = 3, 4, 5$ observe that for any $f \in \mathbf{B}_s$, if $C_s \subseteq \mathbf{S}(f)$ then $D_s \subseteq \mathbf{S}(f)$, where D_s is the dihedral group. We refrain from repeating the proof and refer the reader to § 4 for the details.)

If $k=2$ then the result will follow by considering several possibilities for the pairs (l_1, l_2):

- if gcd $(l_1, l_2) = 1$, then $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ is the direct product of σ_1 and σ_2. Hence, G is specially representable exactly when both factors are specially representable,
- if $(l_1, l_2) = (3, 3)$ or $(4, 4)$ or $(5, 5)$ then G is specially representable,
- if $(l_1, l_2) = (3, m)$ (with $3 | m$) or $(4, m)$ (with gcd $(4, m) \neq 1$) or $(5, m)$ (with $5 | m$), then G is specially representable.

This will take care of deciding the representability of G for all possible pairs (l_1, l_2). A similar argument will work for $k \geqq 3$. This concludes the outline of the proof of correctness.

5.4.1. Sketch of proof. The details of the above constructions are rather tedious but a sufficient indication is given in the sequel.

LEMMA 18. *Suppose that $\sigma_1, \cdots, \sigma_{n+1}$ is a collection of cycles such that both $\langle\sigma_1, \cdots, \sigma_n\rangle$ and $\langle\sigma_{n+1}\rangle$ are specially representable and have disjoint supports. Then $\langle\sigma_1, \cdots, \sigma_{n+1}\rangle$ is specially representable.*

Proof.

Put

$$\Omega_0 = \bigcup_{i=1}^{n} Supp(\sigma_i), \qquad \Omega_1 = Supp(\sigma_{n+1})$$

and let $|\Omega_0| = m$, $|\Omega_1| = k$. Suppose that $f_0: 2^{\Omega_0} \to 2$ and $f_1: 2^{\Omega_1} \to 2$ are special boolean functions representing the groups $\langle\sigma_1, \cdots, \sigma_n\rangle$ and $\langle\sigma_{n+1}\rangle$, respectively. Without loss of generality, we may assume that $1 = f_0(0^m) \neq f_1(0^k) = 0$. Let $\Omega = \Omega_0 \cup \Omega_1$ and define the function $f: 2^\Omega \to 2$ by

$$f(w) = f_0(w \restriction \Omega_0) f_1(w \restriction \Omega_1).$$

Clearly, $\langle\sigma_1, \cdots, \sigma_{n+1}\rangle \subseteq \mathbf{S}_\Omega(f)$. Hence, it remains to prove that

$$\mathbf{S}_\Omega(f) \subseteq \langle\sigma_1, \cdots, \sigma_{n+1}\rangle.$$

Assume on the contrary that $\tau \in \mathbf{S}_\Omega(f) - \langle\sigma_1, \cdots, \sigma_{n+1}\rangle$. We distinguish two cases.

Case 1. $(\exists i \in \Omega_0)(\exists j \in \Omega_1)(\tau(i) = j)$.

Let $w \in \{0, 1\}^\Omega$ be defined by $w \restriction \Omega_0 = 0^m$, and

$$(w \restriction \Omega_1)(l) = \begin{cases} 0 & \text{if } l \neq j \\ 1 & \text{if } l = j, \end{cases}$$

for $l \in \Omega_1$. Since f is a special boolean function and using the fact that $f_0(0^m) \neq f_1(0^k)$ we obtain that $f(w) = 1 \neq f(w^\tau) = 0$, which is a contradiction.

Case 2. (For all $i \in \Omega_0)(\tau(i) \in \Omega_0)$.

Put $\tau_0 = (\tau \upharpoonright \Omega_0) \in \mathbf{S}_{\Omega_0}$ and $\tau_1 = (\tau \upharpoonright \Omega_1) \in \mathbf{S}_{\Omega_1}$. By hypothesis, for all $w \in 2^{\Omega}$, we have that

$$f(w) = f_0(w \upharpoonright \Omega_0) f_1(w \upharpoonright \Omega_1) = f(w^{\tau}) = f_0((w \upharpoonright \Omega_0)^{\tau_0}) f_1((w \upharpoonright \Omega_1)^{\tau_1}),$$

which implies $\tau_0 \in \mathbf{S}^+_{\Omega_0}(f_0)$ and $\tau_1 \in \mathbf{S}^+_{\Omega_1}(f_1)$. This completes the proof of the lemma.

An immediate consequence of the previous lemma is the following.

LEMMA 19. *If G, H have disjoint support and are specially representable then $G \times H$ is specially representable.*

Next we will be concerned with the problem of representing cyclic groups. In view of Theorem 7 in § 4, we know that the cyclic group $\langle(1, 2, \cdots, n)\rangle$ is representable exactly when $n \neq 3, 4, 5$. In particular, the groups $\langle(1, 2, 3)\rangle$, $\langle(1, 2, 3, 4)\rangle$, $\langle(1, 2, 3, 4, 5)\rangle$ are not representable. The following lemma may be somewhat surprising, since it implies that the group $\langle(1, 2, 3)(4, 5, 6)\rangle$, though isomorphic to $\langle(1, 2, 3)\rangle$, *is* representable.

LEMMA 20. *Let the cyclic group G be generated by a permutation σ which is the product of two disjoint cycles of lengths l_1, l_2, respectively. Then G is specially representable exactly when the following conditions are satisfied*: $(l_1 = 3 \Rightarrow 3 \mid l_2)$ *and* $(l_2 = 3 \Rightarrow 3 \mid l_1)$, $(l_1 = 4 \Rightarrow \gcd(4, l_2) \neq 1)$ *and* $(l_2 = 4 \Rightarrow \gcd(4, l_1) \neq 1)$, $(l_1 = 5 \Rightarrow 5 \mid l_2)$ *and* $(l_2 = 5 \Rightarrow 5 \mid l_1)$.

Sketch of proof. It is clear that the assertion of the lemma will follow if we can prove that the three assertions below are true.

(1) The groups $\langle(1, 2, \cdots, n)(n+1, n+2, \cdots, kn)\rangle$ are specially representable when $n = 3, 4, 5$.

(2) The groups $\langle(1, 2, 3, 4)(5, \cdots, m+4)\rangle$ are specially representable when $\gcd(4, m) \neq 1$.

(3) Let m, n be given integers such that either $m = n = 2$ or $m = 2$ and $n \geqq 6$ or $n = 2$ and $m \geqq 6$ or $m, n \geqq 6$. Then $\langle(1, 2, \cdots, m)(m+1, m+2, \cdots, m+n)\rangle$ is specially representable.

Proof of (1). We give the proof only for the case $n = 5$ and $k = 2$. The other cases $n = 3$, $n = 4$, and $k \geqq 3$ are treated similarly. Details of these constructions are left to the reader. Let $\sigma = \sigma_0\sigma_1$, where $\sigma_0 = (1, 2, 3, 4, 5)$ and $\sigma_1 = (6, 7, 8, 9, 10)$. From the proof of Theorem 7 in § 4 we know that

$$D_5 = \mathbf{S}_5(L') = \mathbf{S}_5(L''),$$

where $L' = 0^*1^*0^* \cup 1^*0^*1^*$ and $L'' = \{w \in L' : \rceil |w|_0 \geqq 1\}$. Let L consist of all words w of length 10 such that

—either $|w|_1 = 1$

—or $|w|_1 = 2$ and $(\exists 1 \leqq i \leqq 5)$ $(w_i = w_{5+i}$ and $(\forall j \neq i, 5+i)$ $(w_j = 0))$

—or $|w|_1 = 3$ and $(\exists 0 \leqq i \leqq 4)$ $(w = (1000011000)^{\sigma^i}$ or $w = (1100010000)^{\sigma^i})$

—or $|w|_1$ 3 and $w_1 \cdots w_5 \in L'$ and $w_6 \cdots w_{10} \in L''$.

We want to show that in fact $\langle(1, 2, 3, 4, 5)(6, 7, 8, 9, 10)\rangle = \mathbf{S}_{10}(L)$. It is clear that

$$\langle(1, 2, 3, 4, 5)(6, 7, 8, 9, 10)\rangle \subseteq \mathbf{S}_{10}(L).$$

Conversely, suppose that $\tau \in \mathbf{S}_{10}(L)$. Assume on the contrary there exists an $1 \leqq i \leqq 5$ and a $6 \leqq j \leqq 10$ such that $\tau(i) = j$. Let the word w be defined such that $w_l = 0$, if $l = j$, and $= 1$ otherwise. It follows from the last clause in the definition of L and the fact that $0^5 \notin L''$ that $w \notin L$ and $w^{\tau} \in L$, contradicting the assumption $\tau \in \mathbf{S}_{10}(L)$. It follows that τ is the product of two disjoint permutations τ_0 and τ_1 acting on $1, 2, \cdots, 5$ and $6, 7, \cdots, 10$, respectively. It follows from the last clause in the definition of L that $\tau_0 \in D_5$ and $\tau_1 \in \pi^{-1}D_5\pi$, where $\pi(i) = 5 + i$, for $i = 1, \cdots, 5$. Let $\rho_0 = (1, 5)(2, 4)$ and

$\rho_1=(6,10)(7,9)$ be the reflection permutations on $1,2,\cdots,5$ and $6,7,\cdots,10$, respectively. To complete the proof of (1), it is enough to show that none of the permutations

$$\rho_0,\rho_1,\rho_0\rho_1,\rho_0\sigma_1^i,\sigma_0^i\rho_1,\sigma_0^i\sigma_1^j,$$

for $i\neq j$, belong to $S_{10}(L)$. To see this, let $x=1000011000\in L$. Then for the permutations $\tau=\rho_0,\rho_1,\rho_0\rho_1,\rho_0\sigma_1^i$ for $i=1,2,3,5$, and $\tau=\sigma_0^i\rho_1$ for $i=1,2,4,5$ it is easy to check that $x^\tau\notin L$. Let $x=110001000$. Then for $\tau=\rho_0\sigma_1^4$ and $\tau=\sigma_0^3\rho_1$ it is easy to check that $x^\tau\notin L$. Finally, for $x=1000010000\in L$ and $\sigma_0^i\sigma_1^j$, where $i\neq j$, we have that $x^\tau\notin L$. This completes the proof of part (1) of the lemma.

Proof of (2). Put $\sigma_0=(1,2,3,4)$, $\sigma_1=(5,6,\cdots,m+4)$, $\sigma=\sigma_0\sigma_1$. Let L be the set of words of length $m+4$ such that

either $|w|_1=1$

or $|w|_1=2$ and $(\exists 0\leqq i\leqq \text{lcm}(4,m)-1)(w=(100010^{m-1})^{\sigma^i})$

or $|w|_1=3$ and $(\exists 0\leqq i\leqq \text{lcm}(4,m)-1)(w=(110010^{m-1})^{\sigma^i})$

or $|w|_1=3$ and $w_1\cdots w_4\in L'$ and $w_5\cdots w_{m+5}\in L''$,

where $L'=0^*1^*0^*\cup 1^*0^*1^*$ and L'' are as in Theorem 7 of § 4 satisfying $S_m(L'')=C_m$ and moreover for all $i\geqq 1$, $0^i\notin L''$. Clearly, $\langle(1,2,3,4)(5,6,\cdots,m+4)\rangle\subseteq S_{m+4}(L)$. It remains to prove that

$$S_{m+4}(L)\subseteq\langle(1,2,3,4)(5,6,\cdots,m+4)\rangle.$$

Let $\tau\in\langle(1,2,3,4)(5,6,\cdots,m+4)\rangle$. As before, $\tau=\tau_0\tau_1$, where $\tau_0\in D_4$ and $\tau_1\in\pi^{-1}D_m\pi$, where $\pi(i)=4+i$ for $i=1,2,\cdots,m$. Let $\rho=(1,4)(2,3)$ be the reflection on $1,2,3,4$. It suffices to show that none of the permutations

$$\rho\sigma_1^i,\sigma_0^i\sigma_1^j,$$

for $i\neq j \bmod 4$ are in $S_{m+4}(L)$. Indeed, if $\tau=\sigma_0^i\sigma_1^j$, then let $x=100010^{m-1}$. So it is clear that $x\in L$, but $x^\tau\notin L$. Next assume that $\tau=\rho\sigma_1^i$. We distinguish the following two cases.

Case 1. $m=4k$, i.e., a multiple of 4.

Let $x=100010^{m-1}$. Then $x\in L$, but $x^\tau\notin L$ unless $x^\tau=x^{\sigma^j}$ for some j. In this case $j=3 \bmod 4$ and $j=i \bmod 4k$. So it follows that $i=3,7,11,\cdots,4k-1$. Now let $y=110010^{m-1}$. Then $y\in L$, but $y^\tau\notin L$ for the above values of i, unless $y^\tau=y^{\sigma^l}$ for some l. In that case we have that $l=2 \bmod 4$ *and* $l=i \bmod 4k$. So it follows that $i=2,6,10,\cdots,4k-2$. Consequently, $\tau\notin S_{m+4}(L)$.

Case 2. $\gcd(4,m)=2$.

Let $x=100010^{m-1}$. Then $x\in L$, but $x^\tau\notin L$ unless $x^\tau=x^{\sigma^j}$ for some j. In this case $j=3 \bmod 4$ and $j=i \bmod 4k$. So it follows that for even values of i, $\tau\notin S_{m+4}(L)$. Let $y=110010^{m-1}$. Then $y\in L$, but $y^\tau\notin L$ unless $y^\tau=y^{\sigma^l}$ for some l. In that case we have that $l=2 \bmod 4$ and $l=i \bmod m$. So it follows that for odd values of i, $\tau\notin S_{m+4}(L)$. This completes the proof of (2).

Proof of (3). A similar technique can be used to generalize the representability result to more general types of cycles. Details are left as an exercise to the reader.

A straightforward generalization of Lemma 20 is given in the next lemma.

LEMMA 21. *Let G be a permutation group generated by a permutation σ which can be decomposed into k-many disjoint cycles of lengths $l_1,l_2,\cdots,l_k$, respectively. The group G is specially representable exactly when the following conditions are satisfied for all $1\leqq i\leqq k$,*

$$l_i=3\Rightarrow(\exists j\neq i)(3\,|\,l_j)\quad\textbf{and}$$
$$l_i=4\Rightarrow(\exists j\neq i)(\gcd(4,l_j)\neq 1)\quad\textbf{and}$$
$$l_i=5\Rightarrow(\exists j\neq i)(5\,|\,l_j).$$

Now the correctness of the algorithm is an immediate consequence of Lemmas 1-5. This completes the proof of Theorem 17. □

5.5. Asymptotic behavior. Finally, for any sequence $\langle G_n \leqq \mathbf{S}_n \colon n \geqq 1 \rangle$ of permutation groups we consider the value of the limit

$$\lim_{n\to\infty} \frac{|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) = G_n\}|}{2^{2^n}}.$$

We have the following theorem.

THEOREM 22. (Almost all boolean functions have trivial invariance groups.) *For any family $\langle G_n \colon n \geqq 1 \rangle$ of permutation groups such that each $G_n \leqq \mathbf{S}_n$, we have that*

$$\lim_{n\to\infty} \frac{|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) = \{id_n\}\}|}{2^{2^n}} = \lim_{n\to\infty} \frac{|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) \leqq G_n\}|}{2^{2^n}} = 1.$$

Moreover, if $\liminf |G_n| > 1$ *then*

$$\lim_{n\to\infty} \frac{|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) \geqq G_n\}|}{2^{2^n}} = \lim_{n\to\infty} \frac{|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) = G_n\}|}{2^{2^n}} = 0.$$

Proof. During the course of this proof we use the abbreviation $\Theta(m) := \Theta_m(\langle(1, 2, \cdots, m)\rangle)$. First we prove the second part of the theorem. By assumption there exists an n_0 such that for all $n \geqq n_0$, $|G_n| > 1$. Hence, for each $n \geqq n_0$, G_n contains a permutation of order $k(n) \geqq 2$, say σ_n. Without loss of generality we can assume that each $k(n)$ is a prime number. Since $k(n)$ is prime, σ_n is a product of $k(n)$-cycles. If $(i_1, \cdots, i_{k(n)})$ is the first $k(n)$-cycle in this product then it is easy to see that

$$\Theta_n(\langle \sigma_n \rangle) \leqq \Theta_n(\langle(i_1, \cdots, i_{k(n)})\rangle).$$

It follows that

$$|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) \geqq G_n\}| \leqq |\{f \in \mathbf{B}_n \colon \sigma_n \in \mathrm{S}(f)\}| = 2^{\Theta_n(\sigma_n)} \leqq 2^{\Theta(k(n)) \cdot 2^{n-k(n)}}.$$

$$|\{f \in \mathbf{B}_n \colon \mathrm{S}(f) \geqq G_n\}| \leqq |\{f \in \mathbf{B}_n \colon \sigma_n \in \mathrm{S}(f)\}| = 2^{\Theta_n(\sigma_n)} \leqq 2^{\Theta(k(n)) \cdot 2^{n-k(n)}}.$$

Recall from [Ber71] that the formula

$$\Theta(m) = \frac{1}{m} \cdot \sum_{k|m} \phi(k) \cdot 2^{m/k}$$

gives the Pólya cycle index of the group $\langle(1, 2, \cdots, m)\rangle$ acting on $\{1, 2, \cdots, m\}$, where $\phi(k)$ is Euler's totient function. However, it is easy to see that for k prime

$$\frac{\Theta(k)}{2^k} = \frac{1}{k} + \frac{2}{2^k} - \frac{2}{k2^k}.$$

In fact the function in the right-hand side of the above equation is decreasing in k. Hence, for k prime,

$$\frac{\Theta(k)}{2^k} \leqq \frac{\Theta(2)}{2^2} = \frac{3}{4}.$$

It follows that

$$\frac{|\{f\in \mathbf{B}_n: \mathbf{S}(f)\geqq G_n\}|}{2^{2^n}}\leqq 2^{2^n\cdot[\Theta(k(n))\cdot 2^{-k(n)}-1]}\leqq 2^{-2^{n-2}}.$$

Since the right-hand side of the above inequality converges to 0 the proof of the second part of the theorem is complete. To prove the first part notice that

$$\{f\in \mathbf{B}_n: \mathbf{S}(f)\neq id_n\}\subseteq \bigcup_{\sigma\neq id_n}\{f\in \mathbf{B}_n: \sigma\in \mathbf{S}(f)\},$$

where σ ranges over cyclic permutations of order a prime number $\leqq n$. Since there are at most $n!$ permutations on n letters we obtain from the last inequality that

$$\frac{|\{f\in \mathbf{B}_n: \mathbf{S}(f)\neq \{id_n\}\}|}{2^{2^n}}\leqq n!\cdot 2^{-2^{n-2}}=2^{O(n\log n)}\cdot 2^{-2^{n-2}}\to 0,$$

as desired. □

As a consequence of the above theorem we obtain that asymptotically almost all boolean functions have trivial invariance group.

6. Invariance groups of languages and circuits. In this section we classify languages according to the size of their invariance groups. Furthermore, we consider questions concerning their structural properties and complexity. Recall that for each $L\subseteq \{0, 1\}^*$ and n, L_n is the set of strings in L of length exactly n. By abuse of notation we also denote the characteristic function of L_n with the same symbol. Let $\mathbf{S}_n(L)$ denote the invariance group of the n-ary boolean function L_n. For any language L and any sequence $\sigma=\langle\sigma_n: n\geqq 1\rangle$ of permutations such that each $\sigma_n\in \mathbf{S}_n$ we define the language

$$L_n^\sigma=\{x\in 2^n: x^{\sigma_n}\in L_n\}.$$

For each n let $G_n\leqq \mathbf{S}_n$ and put $\mathbf{G}=\langle G_n: n\geqq 1\rangle$. Define

$$L^{\mathbf{G}}=\bigcup_{\sigma_n\in G_n} L_n^{\sigma_n}.$$

For each $1\leqq k\leqq\infty$, let $\mathbf{F}_k$ be the class of functions $n^{c\log^{(k)} n}$, $c>0$, where $\log^{(1)} n = \log n$, $\log^{(k+1)} n=\log\log^{(k)} n$, and $\log^{(\infty)} n=1$. Clearly, $\mathbf{F}_\infty$ is the class $\mathbf{P}$ of polynomial functions. We also define $\mathbf{F}_0$ as the class of functions 2^{cn}, $c>0$. Let $\mathbf{L}(\mathbf{F}_k)$ be the set languages $L\subseteq\{0, 1\}^*$ such that there exists a function $f\in \mathbf{F}_k$ satisfying

$$\forall n(|\mathbf{S}_n: \mathbf{S}_n(L)|\leqq f(n)).$$

We will also use the notation $L(\mathbf{EXP})$ and $L(\mathbf{P})$ for the classes $\mathbf{L}(\mathbf{F}_0)$ and $\mathbf{L}(\mathbf{F}_\infty)$, respectively. Occasionally, a language $L\in L(\mathbf{P})$ will also be called a language which has *polynomial index* or is even *almost symmetric.*

6.1. Structural properties. The following theorem gives some of the structural properties of the classes of languages $\mathbf{L}(\mathbf{F}_k)$.

THEOREM 23. *For any* $0\leqq k\leqq\infty$ *and any language* $L\in \mathbf{L}(\mathbf{F}_k)$,

(1) $\mathbf{L}(\mathbf{F}_k)$ *is closed under boolean operations and homomorphisms,*

(2) $(L\cdot\Sigma)\in \mathbf{L}(\mathbf{F}_k)$,

(3) $L^\sigma\in \mathbf{L}(\mathbf{F}_k)$, *where* $\sigma=\langle\sigma_n: n\geqq 1\rangle$, *with each* $\sigma_n\in \mathbf{S}_n$,

(4) *if* $|\mathbf{S}_n: N_{\mathbf{S}_n}(G_n)|\leqq f(n)$ *and* $f\in \mathbf{F}_k$ *then* $L^{\mathbf{G}}\in \mathbf{L}(\mathbf{F}_k)$, *where* $\mathbf{G}=\langle G_n: n\geqq 1\rangle$.

Proof. We use extensively (even without explicit mention) the results of Theorem 10. To prove (1) notice first that $\mathbf{S}_n(\neg L)=\mathbf{S}_n(L)$. To prove that $\mathbf{L}(\mathbf{F}_k)$ is closed under union and intersection use the following inequality from group theory: for $K, K'\leqq G$,

$$|G:K\cap K'|\leqq|G:K|\cdot|G:K'|.$$

For example, for closure under intersection we have that $\mathbf{S}_n(L)\cap\mathbf{S}_n(L')\subseteq\mathbf{S}_n(L\cap L')$, which implies that

$$|\mathbf{S}_n:\mathbf{S}_n(L\cap L')|\leqq|\mathbf{S}_n:\mathbf{S}_n(L)\cap\mathbf{S}_n(L')|\leqq|\mathbf{S}_n:\mathbf{S}_n(L)|\cdot|\mathbf{S}_n:\mathbf{S}_n(L')|.$$

To prove closure under a homomorphism $h: L\to L'$ note that $\mathbf{S}_n(L)\subseteq\mathbf{S}_n(h(L))$. Hence,

$$|\mathbf{S}_n:\mathbf{S}_n(L')|=|\mathbf{S}_n:\mathbf{S}_n(h(L))|\leqq|\mathbf{S}_n:\mathbf{S}_n(L)|.$$

To prove (2) let $L'=L\cdot\Sigma=\{xa: x\in L,\ a\in\Sigma\}$ and note that

$$|\mathbf{S}_n:\mathbf{S}_n(L')|\leqq n\cdot|\mathbf{S}_{n-1}:\mathbf{S}_{n-1}(L)|.$$

To prove (3) note that $\mathbf{S}_n(L)^{\sigma_n}=\mathbf{S}_n(L^\sigma)$. To prove (4), note that we have $N_{\mathbf{S}_n}(G_n)\cap\mathbf{S}_n(L)\subseteq\mathbf{S}_n(L^{\mathbf{G}})$. Indeed, for $\tau\in N_{\mathbf{S}_n}(G_n)\cap\mathbf{S}_n(L)$ we have that $G_n\tau=\tau G_n$, which in turn implies that

$$L_n^{G_n\tau}=L_n^{\tau G_n}=\bigcup_{\sigma_n\in G_n}L_n^{\tau\sigma_n}=\bigcup_{\sigma_n\in G_n}L_n^{\sigma_n}=L_n^{G_n}.$$

Hence,

$$|\mathbf{S}_n:\mathbf{S}_n(L^{\mathbf{G}})|\leqq|\mathbf{S}_n:N(G_n)|\cdot|\mathbf{S}_n:\mathbf{S}_n(L)|,$$

as desired. □

The classes $L(\mathbf{P})$ and $L(\mathbf{EXP})$ enjoy the closure properties mentioned below.

THEOREM 24.

$$L\in L(\mathbf{P})\quad and\quad p\in\mathbf{P}\Rightarrow|\mathbf{S}_{p(n)}:\mathbf{S}_{p(n)}(L)|=n^{O(1)}.$$

Proof. The proof is obvious, since the class of polynomials is closed under composition. □

THEOREM 25.

$$L^1, L^2\in L(\mathbf{EXP})\Rightarrow L=\{xy: x\in L^1, y\in L^2, l(x)=l(y)\}\in L(\mathbf{EXP}).$$

Proof. It is clear that $\mathbf{S}_n(L^1)\times\mathbf{S}_n(L^2)\subseteq\mathbf{S}_{2n}(L)$. It follows from Stirling's formula that

$$\begin{aligned}|\mathbf{S}_{2n}:\mathbf{S}_{2n}(L)|&\leqq\frac{(2n)!}{|\mathbf{S}_n(L)|\cdot|\mathbf{S}_n(L)|}\\&=\frac{(2n)!}{n!\cdot n!}\cdot|\mathbf{S}_n:\mathbf{S}_n(L)|^2\\&\leqq\frac{(2n)!}{n!\cdot n!}\cdot 2^{O(n)}=2^{O(n)}.\end{aligned}$$ □

Let **REG** denote the class of regular languages.

THEOREM 26. *The following properties hold for any* $1\leqq k<\infty$,

(1) $$\mathbf{L}(\mathbf{F}_\infty)=L(\mathbf{P})\subset\cdots\subset\mathbf{L}(\mathbf{F}_{k+1})\subset\mathbf{L}(\mathbf{F}_k)\subset\cdots\subset L(\mathbf{EXP})=\mathbf{L}(\mathbf{F}_0),$$

(2) $$\mathbf{REG}\cap L(\mathbf{P})\neq\varnothing,\quad \mathbf{REG}-L(\mathbf{EXP})\neq\varnothing,\quad L(\mathbf{P})-\mathbf{REG}\neq\varnothing.$$

Proof. To prove $\mathbf{L}(\mathbf{F}_{k+1})\subset\mathbf{L}(\mathbf{F}_k)$, for $1\leqq k<\infty$, put $f(n)=n-\log^{(k)}n$ and consid the language

$$L=\{x\in 2^n: x_{f(n)+1}\leqq\cdots\leqq x_n\}.$$

Then we have that

$$|\mathbf{S}_n : \mathbf{S}_n(L)| = \frac{n!}{f(n)!} = n^{O(\log^{(k)} n)}.$$

It follows that $\mathbf{L}(\mathbf{F}_{k+1}) \subset \mathbf{L}(\mathbf{F}_k)$. (Note that by the pumping lemma for regular languages L cannot be regular.) The proof of $\mathbf{L}(\mathbf{F}_k) \subset \mathbf{L}(\mathbf{F}_0)$ is more delicate. The group $\mathbf{S}_n \times \mathbf{S}_n$ is maximal in $\mathbf{S}_{2n}$. It follows from our representation theorem for maximal groups that there exists a language L such that for all n,

$$\mathbf{S}_{2n}(L) = \mathbf{S}_n \times \mathbf{S}_n.$$

It follows from Stirling's formula that $|\mathbf{S}_{2n} : \mathbf{S}_{2n}(L)| = 2^{O(n)}$, as desired. The proof of $\mathbf{L}(\mathbf{F}_\infty) \subset \mathbf{L}(\mathbf{F}_k)$, $k \geqq 1$, follows from the above remarks. This completes the proof of (1). To prove $\mathbf{REG} \cap L(\mathbf{P}) \neq \emptyset$, consider the trivial language $L = \{0, 1\}^*$. To prove $\mathbf{REG} - L(\mathbf{EXP}) \neq \emptyset$, consider the language $L = 0^*1^*$. To prove $L(\mathbf{P}) - \mathbf{REG} \neq \emptyset$. For any set S of positive integers let $L^S = \{0^n : n \in S\}$. Clearly, $L^S_n(x) = 1$ if $n \in S$ and $x = 0^n$, and $=0$ otherwise. It is easy to see that for all S, $L^S \in L(\mathbf{P})$, and hence $L(\mathbf{P})$ is uncoutable. (In fact, $\mathbf{S}_n(L^S) = \mathbf{S}_n$, for all n and S.) In particular, the nonregular language $L = \{0^p : p$ is a prime number$\} \in L(\mathbf{P})$. □

A few useful and illuminating examples are now in order.

Examples. (1) Let $L^k = \{x \in \{0, 1\}^* : l(x) \geqq k,\ x_1 \leqq \cdots \leqq x_k\}$. Then $\mathbf{S}_n(L^k) = \mathbf{S}_{n-k}$ and therefore $|\mathbf{S}_n : \mathbf{S}_n(L)| = n!/(n-k)! = O(n^k)$. Hence, for all k, $L^k \in L(\mathbf{P})$.

(2) For each word $x = x_1 \cdots x_n$ let $x^T = x_n \cdots x_1$ and $L^T = \{x^T : x \in L\}$. Put $\sigma_n(i) = n - i + 1$. Then $L^\sigma = L^T$, where $\sigma = \langle \sigma_n : n \geqq 1 \rangle$.

(3) There exist languages $L^0, L^1 \in L(\mathbf{P})$ such that $L^0 \cdot L^1 \notin L(\mathbf{EXP})$. Indeed, put $L^0 = \{0\}^*$, $L^1 = \{1\}^*$. Then $L = L^0 \cdot L^1 = \{0^n 1^m : n, m \geqq 0\}$. It is easy to see that $|\mathbf{S} : \mathbf{S}_n(L)| = n!$.

(4) There exists a language $L \in L(\mathbf{P})$ such that $L^* \notin L(\mathbf{P})$. Indeed, put $L = \{01\}$. Then for n even, $\sigma \in \mathbf{S}$ if and only if for all $i \leqq n$ (i is even if and only if $\sigma(i)$ is even). It follows that $|\mathbf{S}_n : \mathbf{S}_n(L)| = n!/(n/2)!(n/2)!$. Hence, $L^* \in L(\mathbf{EXP}) - L(\mathbf{P})$.

(5) $L(\mathbf{P})$ is not closed under inverse homomorphism. Indeed, let D be the Dyck language on one parenthesis and $h : D \to L$ be the homomorphism $h(0) = h(1) = 0$. In view of the results of § 3, $D \notin L(\mathbf{P})$.

(6) For each function $f : \mathbf{N} \to \mathbf{N}$ such that for all $n \geqq 1$, $f(n) \leqq n$, we define the language

$$L^f_n = \{x \in 2^n : x_1 \leqq \cdots \leqq x_{f(n)}\}, \qquad L^f = \bigcup_n L^f_n.$$

Using the pumping lemma for regular languages we can show that $L^f \in \mathbf{REG} \Rightarrow \sup_n f(n) < \infty$.

Similar classes of languages corresponding to the cycle index can be defined as follows. Let $L_\Theta(\mathbf{F}_k)$ be the set of languages L such that there exists a function $f \in \mathbf{F}_k$ satisfying

$$\forall n (\Theta(\mathbf{S}(L_n)) \leqq f(n)).$$

Since, $\Theta(\mathbf{S}_n(L)) \leqq (n+1) \cdot |\mathbf{S}_n : \mathbf{S}_n(L)|$, it is clear that $\mathbf{L}(\mathbf{F}_k) \subseteq L_\Theta(\mathbf{F}_k)$. In fact we can show that $\mathbf{L}(\mathbf{F}_k) \subset L_\Theta(\mathbf{F}_k)$. To see this take $f(n) = n - \log^{(k)} n$. Define $x \in L_n$ if and only if $x_1 \leqq x_2 \leqq \cdots \leqq x_{f(n)}$. Then it is easy to see that $\mathbf{S}_n(L) = \mathbf{S}_{f(n)}$. Hence, $|\mathbf{S}_n : \mathbf{S}_n(L)| = O(n^{\log n})$, while $\Theta(\mathbf{S}_n(L)) = (f(n)+1)2^{\log^{(k)} n} = O(n^2)$.

6.2. Circuit complexity of formal languages. In this section, we study the complexity of languages $L \in L(\mathbf{P})$. The following result is proved by applying the intricate

NC algorithm of [BLS87] for permutation group membership. By delving into a deep result in classification theory of finite simple groups, we improve the conclusion to that of Theorem 29. For clarity however, we present the following.

THEOREM 27. *For any language* $L \subseteq \{0,1\}^*$, *if* $L \in L(\mathbf{P})$ *then* L *is nonuniform* NC.

Proof. As a first step in the proof we will need the following claim.

CLAIM. *There is an* NC^1 *algorithm which, when given* $x \in \{0,1\}^n$, *outputs* $\sigma \in \mathbf{S}_n$ *such that* $x^\sigma = 1^m 0^{n-m}$, *for some* m.

Proof of the claim. Before giving the proof of the claim, we illustrate the idea by citing an example. Suppose that $x = 101100111$. By simultaneously going from left to right and from right to left, we swap an "out-of-place" 0 with an "out-of-place" 1, keeping track of the respective positions.[3] This gives rise to the desired permutation σ. In the case at hand we find $\sigma = (2,9)(5,8)(6,7)$ and $x^\sigma = 1^6 0^3$.

Now we proceed with the proof of the main claim. Define the predicates $E_{k,b}(u)$, to hold when there are exactly k occurrences of b in the word u ($b = 0, 1$) are in NC^1. The predicates $E_{k,b}$ are obviously computable in constant depth, polynomial size threshold circuits, i.e., in TC^0. By the work of Ajtai, Komlós, and Szemerédi [AKS83] $\mathrm{TC}^0 \subseteq \mathrm{NC}^1$. For $k = 1, \cdots, [n/2]$ and $1 \leqq i < j \leqq n$, let $\alpha_{i,j,k}$ be a log depth circuit which outputs 1 exactly when the kth "out-of-place" 0 is in position i and the kth "out-of-place" 1 is in position j. It follows that $\alpha_{i,j,k}(x) = 1$ if and only if "there exist $k-1$ zeros to the left of position i, the ith bit of x is zero, and there exist k ones to the right of position i" and "there exist $k-1$ ones to the right of position j, the jth bit of x is one, and there exist k zeros to the left of position j." This in turn is equivalent to

$$E_{k-1,0}(x_1, \cdots, x_{i-1}) \quad \text{and } x_i = 0 \quad \text{and } E_{k,1}(x_{i+1}, \cdots, x_n) \quad \text{and}$$

$$E_{k-1,1}(x_{j+1}, \cdots, x_n) \quad \text{and } x_j = 1 \quad \text{and } E_{k,0}(x_1 \cdots x_{j-1}).$$

This implies that the required permutation can be defined by

$$\sigma = \prod \left\{ (i,j) \colon i < j \text{ and } \bigvee_{k=1}^{[n/2]} \alpha_{i,j,k} \right\}.$$

Converting the fanin, $[n/2]$-$\vee$-gate into a $\log([n/2])$ depth tree of fanin, 2-$\vee$-gates, we have an NC^1 procedure for computing σ. This completes the proof of the claim.

Next we continue with the proof of the main theorem. Put $G_n = \mathbf{S}_n(L)$ and let $R_n = \{h_1, \cdots, h_q\}$ be a complete set of representatives for the left cosets of G_n, where $q \leqq p(n)$ and $p(n)$ is a polynomial such that $|\mathbf{S}_n : G_n| \leqq p(n)$. Fix $x \in \{0,1\}^n$. By the previous claim there is a permutation σ which is the product of disjoint transpositions and an integer $0 \leqq k \leqq n$ such that $x^\sigma = 1^k 0^{n-k}$. So $x = (1^k 0^{n-k})^\sigma$. In parallel for $i = 1, \cdots, q$ test whether $h_i^{-1}\sigma \in G_n$ by using the principal result of [BLS87], thus determining i such that $\sigma = h_i g$, for some $g \in G_n$. Then we obtain that

$$L_n(x) = L_n((1^k 0^{n-k})^\sigma) = L_n((1^k 0^{n-k})^{h_i g}) = L_n((1^k 0^{n-k})^{h_i}).$$

By hardwiring the polynomially many values $L_n((1^k 0^{n-k})^{h_i})$ for $0 \leqq k \leqq n$ and $1 \leqq i \leqq q$, we produce a polynomial size polylogarithmic depth circuit family for L. □

Theorem 27 involves a straightforward application of the beautiful NC algorithm of Babai, Luks, and Seress [BLS87] for testing membership in a finite permutation group. By using the deep structure consequences of the O'Nan-Scott theorem below, together with Bochert's result on the size of the index of primitive permutation groups

[3] This is a well-known trick for improving the efficiency of the "partition" or "split" algorithm used in quick-sort.

(see Theorem 1(3) in § 2), we can improve the NC algorithm of Theorem 27 to an optimal TC^0 algorithm (and hence NC^1). First, we take the following discussion and statement of the O'Nan-Scott theorem from [KL88, p. 376].

Let $I=\{1, 2, \cdots, n\}$ and let $\mathbf{S}_n$ act naturally on I. Consider all subgroups of the following five classes of subgroups of $\mathbf{S}_n$.

$\alpha_1: \mathbf{S}_k \times \mathbf{S}_{n-k}$, where $1 \leqq k \leqq n/2$,

$\alpha_2: \mathbf{S}_a \wr \mathbf{S}_b$, where either ($n=ab$ and $a, b \quad 1$) or ($n=a^b$ and $a \geqq 5$, $b \geqq 2$),

α_3: the affine groups $AGL_d(p)$, where $n=p^d$,

α_4: $T^k \cdot (Out(T) \times \mathbf{S}_k)$, where T is a nonabelian simple group, $k \geqq 2$ and $n=|T|^{k-1}$, as well as all groups in the class,

α_5: almost simple groups acting primitively on I.

THEOREM 28 (O'Nan-Scott). *Every subgroup of* $\mathbf{S}_n$ *not containing* $\mathbf{A}_n$ *is a member of* $\alpha_1 \cup \cdots \cup \alpha_5$.

Now we can improve the result of Theorem 27 in the following way.

THEOREM 29 (Parallel complexity of Languages of Polynomial Index). *For any language* $L \subseteq \{0, 1\}^*$, *if* $L \in L(\mathbf{P})$ *then* L *is in 9-nonuniform* TC^0 *and hence in (nonuniform)* NC^1.

Proof. The proof requires the following consequence of the O'Nan-Scott theorem.

CLAIM. *Suppose that* $\langle G_n \leqq \mathbf{S}_n : n \geqq 1\rangle$ *is a family of permutation groups such that for all* n, $|\mathbf{S}_n : G_n| \leqq n^k$, *for some* k. *Then for sufficiently large* N, *there exists an* $i_n \leqq k$ *for which* $G_n = U_n \times V_n$ *with the supports of* U_n, V_n *disjoint and* $U_n \leqq \mathbf{S}_{i_n}$, $V_n = \mathbf{S}_{n-i_n}$.

Before proving the claim we complete the details of the proof of Theorem 29. Apply the claim to $G_n = \mathbf{S}_n(L)$ and notice that given $x \in 2^n$, the question of whether x belongs to L is decided completely by the number of 1's in the support of $K_n = \mathbf{S}_{n-i_n}$, together with information about the action of a finite group $H_n \leqq \mathbf{S}_{i_n}$, for $i_n \leqq k$. Using the counting predicates as in the proof of Theorem 27, it is clear that this is a TC^0 and hence NC^1 algorithm. Thus, the proof of the theorem is complete, assuming the claim.

Proof of the claim. We have already observed at the beginning of § 5 that $G_n \neq \mathbf{A}_n$. By the O'Nan-Scott theorem, G_n is a member of $\alpha_1 \cup \cdots \cup \alpha_5$. Using Bochert's theorem on the size of the index of primitive permutation groups (§ 2, Theorem 1(3)), the observations of [LPS88] concerning the primitivity of the maximal groups in $\alpha_3 \cup \alpha_4 \cup \alpha_5$ and the fact that G_n has polynomial index with respect to $\mathbf{S}_n$, we conclude that the subgroup G_n cannot be a member of the class $\alpha_3 \cup \alpha_4 \cup \alpha_5$. It follows that $G_n \in \alpha_1 \cup \alpha_2$. We show that in fact $G_n \notin \alpha_2$. Assume on the contrary that $G_n \leqq H_n = \mathbf{S}_a \wr \mathbf{S}_b$. It follows that $|H_n| = a!(b!)^a$. We distinguish the following two cases.

Case 1. $n=ab$, for $a, b>1$.

In this case it is easy to verify using Stirling's interpolation formula

$$(n/e)^n\sqrt{n} < n! < (n/e)^n 3\sqrt{n}$$

that

$$|\mathbf{S}_n : H_n| = \frac{n!}{a!(b!)^a} \sim \frac{a^{n-a}}{3b^{a/2}(3/a)^a\sqrt{a}}.$$

Moreover, it is clear that the right-hand side of this last inequality cannot be asymptotically polynomial in n, since $a \leqq n$ is a proper divisor of n, which is a contradiction.

Case 2. $n=a^b$, for $a \geqq 5$, $b \geqq 2$.

A similar calculation shows that asymptotically

$$|\mathbf{S}_n : H_n| = \frac{n!}{a!(b!)^a} = \frac{n!}{a!(b'!)^a},$$

where $b' = a^{b-1}$. It follows from the argument of Case 1 that this last quantity cannot be asymptotically polynomial in n, which is a contradiction. It follows that $G_n \in \alpha_1$. Let $G_n \leqq \mathbf{S}_i \times \mathbf{S}_{n-i}$, for some $1 \leqq i_n n/2$. We claim that, in fact, $i_n \leqq k$ for all but a finite number of n's. Indeed, put $i_n = i$ and notice that

$$|\mathbf{S}_n : \mathbf{S}_i \times \mathbf{S}_{n-i}| = \frac{n!}{i!(n-i)!} = \Omega(n^i) \leqq |\mathbf{S}_n : G_n| \leqq n^k,$$

which proves that $i \leqq k$. It follows that $G_n = U_n \times V_n$, where $U_n \leqq \mathbf{S}_{i_n}$ and $V_n \leqq \mathbf{S}_{n-i_n}$. Since $i_n \leqq k$ and $|\mathbf{S}_n : G_n| \leqq n^k$ it follows that for n large enough $V_n = \mathbf{S}_{n-i_n}$. This completes the proof of the claim. Now let $L \subseteq \{0, 1\}^*$ have polynomial index. Given a word $x \in \{0, 1\}^n$, in TC^0 one can test whether the number of 1's occurring in the $n - i_n$ positions (where $V_n = \mathbf{S}_{n-i_n}$) is equal to a fixed value, hardwired into the nth circuit. This, together with a finite look-up table corresponding to the U_n part, furnishes a TC^0 algorithm for testing membership in L. □

6.3. Applications. An immediate consequence of our analysis is that if $\langle G_n \leqq \mathbf{S}_n : n \geqq 1\rangle$ is a family of transitive permutation groups such that $|\mathbf{S}_n : G_n| = n^{O(1)}$ then $G_n = \mathbf{S}_n$, for all but a finite number of n's (this answers a conjecture of Perrin). It is also possible to give a more algebraic formulation of the main consequence of Theorem 29. For p_n a polynomial in the variables $x_1, \cdots, x_n$ and with coefficients from the two element field $\mathbf{Z}_2$, let

$$\mathrm{S}(p_n) = \{\sigma \in \mathbf{S}_n : \forall x_1, \cdots, x_n (p_n(x_1, \cdots, x_n) = p_n(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \bmod 2)\}.$$

A family $\langle p_n : n \geqq 1\rangle$ of multivariate polynomials in $\mathbf{Z}_2[x_1, \cdots, x_n]$ is of polynomial index if $|\mathbf{S}_n : \mathrm{S}(p_n)| = n^{O(1)}$.

THEOREM 30. *If $\langle p_n : n \geqq 1\rangle$ is family of multivariate polynomials (in $\mathbf{Z}_2[x_1, \cdots, x_n]$) of polynomial index then there is a family $\langle q_n : n \geqq 1\rangle$ of multivariate polynomials (in $\mathbf{Z}_2[x_1, \cdots, x_n]$) of polynomial length such that $p_n = q_n$.*

Because of the limitations of families of groups of polynomial index proved in the claim above, we obtain a generalization of the principal results of [FKPS85]. Namely, for $L \subseteq \{0, 1\}^*$ let $\mu_L(n)$ be the least number of input bits which must be set to a constant in order for the resulting language $L_n = L \cap \{0, 1\}^n$ to be constant (see [FKPS85] for more details). Then we can prove the following theorem.

THEOREM 31. *If $L \in L(\mathbf{P})$* (i.e., *L is a language of polynomial index*) *then*

$$\mu_L(n) \leqq (\log n)^{O(1)} \Leftrightarrow L \in \mathrm{AC}^0.$$

Our characterization of permutation groups of polynomial index given during the proof of Theorem 29 can also be used to determine the parallel complexity of the following problem concerning "weight-swapping." Let $\mathbf{G} = \langle G_n : n \in \mathbf{N}\rangle$ denote a sequence of permutation groups such that $G_n \leqq \mathbf{S}_n$, for all n. By SWAP ($\mathbf{G}$) we understand the following problem:

Input. $n \in \mathbf{N}$, $a_1, \cdots, a_n$ positive rationals, each of whose (binary) representations is of length at most n.

Output. A permutation $\sigma \in G_n$ such that for all $1 \leqq i\ n$, $a_{\alpha(i)} + a_{\sigma(i+1)} \leqq 2$, if such a permutation exists, and the response "NO" otherwise.

THEOREM 32. *For any sequence $\mathbf{G}$ of permutation groups of polynomial index, the problem* SWAP ($\mathbf{G}$) *is in nonuniform* NC^1.

Proof. By the characterization of sequences of groups of polynomial index, there exist integers k, N such that for all $n \geqq N$, $G_n = H_n \times K_n$, where $H_n \leqq \mathbf{S}_{i_n}$ and $K_n = \mathbf{S}_{n-i_n}$, with $i_n \leqq k$. Given $n \geqq N$, and n positive rational weights $a_1, \cdots, a_n$ test whether there exist permutations $\sigma \in H_n$ and $\tau \in K_n$ such that for $1 \leqq i \leqq n$, $a_{(\sigma \times \tau)(i)} + a_{(\sigma+\tau)(i+1)} \leqq 2$, as follows. For τ, sort the set of weights $\{a_i: i \in Supp(K_n)\}$ in decreasing order. Assume wlog that $Supp(K_n) = \{1, \cdots, n-i_n\}$. Let $\rho \in K_n$ be a "sorting" permutation such that $a_{\rho(1)} \geqq a_{\rho(2)} \geqq \cdots \geqq a_{\rho(n-i_n)}$. Test in parallel whether

$$a_{\rho(1)} + a_{\rho(n-i_n)} \leqq 2, \qquad a_{\rho(2)} + a_{\rho(n-i_n-1)} \leqq 2, \cdots, \text{etc.}$$

If so, then let τ be the appropriate permutation such that

$$1 \mapsto \rho(1), \quad 2 \mapsto \rho(n-i_n), \cdots, n-i_n-1 \mapsto \rho\left(\frac{n-i_n}{2}-1\right), \quad n-i_n \mapsto \rho\left(\frac{n-i_n}{2}\right),$$

if $n-i_n$ is even, and a variant of this, if $n-i_n$ is odd. Since sorting n many n-bit numbers is in NC^1, computing τ is in NC^1. Since $H_n \leqq \mathbf{S}_{i_n}$, where $i_n \leqq k$, there are only a finite number of possibilities to test for σ. These are hardwired (by nonuniformity) into the circuit. □

The following conjecture would relate the cycle index of a sequence $\mathbf{G} = \langle G_n: n \geqq 1\rangle$ of groups with the circuit complexity of the language L.

CONJECTURE 33. *For any language $L \subseteq \{0, 1\}^*$, if $L \in L_\Theta(\mathbf{P})$ then L is nonuniform* NC.

This conjecture appears somewhat plausible, since it follows from the next theorem that if $\mathbf{G} = \langle G_n \leqq \mathbf{S}_n: n \geqq 1\rangle$ is a sequence of groups whose cycle index $\Theta_n(G_n)$, as a function of n, majorizes all polynomials, then there is a language L with $\mathbf{S}_n(L) \supseteq G_n$ and $L \notin SIZE(n^{O(1)})$.

THEOREM 34. *For any sequence $\mathbf{G} = \langle G_n: n \geqq 1\rangle$ of permutation groups $G_n \leqq \mathbf{S}_n$ it is possible to find a language L such that*

$$L \notin SIZE(\sqrt{\Theta(G_n)}), \quad \text{and} \quad \forall n(\mathbf{S}(L_n) \supseteq G_n).$$

Proof. By Lupanov's theorem $|\{f \in \mathbf{B}_n: c(f) \leqq q\}| = O(q^{q+1}) = 2^{O(q \log q)}$. Hence, if $q_n \to \infty$ then $|\{f \in \mathbf{B}_n: c(f) \leqq q_n\}| < 2^{q_n^2}$. In particular, setting $q_n = \sqrt{\Theta(G_n)}$ we obtain

$$|\{f \in \mathbf{B}_n: c(f) \leqq \sqrt{\Theta(G_n)}\}| < 2^{\Theta(G_n)} = |\{f \in \mathbf{B}_n: \mathbf{S}(f) \supseteq G_n\}|.$$

It follows that for n big enough there exists an $f_n \in \mathbf{B}_n$ such that $\mathbf{S}(f_n) \supseteq G_n$ and $c(f_n) > \sqrt{\Theta(G_n)}$. This completes the proof of the theorem. □

7. Discussion and open problems. Three of the main questions we have tried to answer in the present paper are (1) which permutation groups arise as (or are isomorphic to) the invariance groups of boolean functions, (2) determining the complexity of deciding the representability of a permutation group, (3) determining the relation between the family of invariance groups of a formal language L and the parallel complexity of L.

Concerning question (1), we saw that most (i.e., with a few exceptions) maximal permutation subgroups of $\mathbf{S}_n$ are representable. We have shown that every permutation group $G\,\mathbf{S}_n$ is isomorphic to the invariance group of a boolean function $f \in \mathbf{B}_{n(\log n+1)}$. However, we do not know if this last "upper bound" can be improved to $f \in \mathbf{B}_{cn}$, for some constant c independent of n. In the case of question (2), we gave a logspace algorithm for deciding the representability of cyclic groups. In general however, we do not know of any efficient algorithm for deciding the representability of any other natural classes of permutation groups (e.g., abelian, nilpotent, solvable, etc.). The existence of a polynomial time algorithm for testing representability of an arbitrary permutation group is related to the question of whether *graph nonisomorphism* is in polynomial time.

Concerning question (3), we have shown a relation between the size of the index of the invariance group of a formal language and its complexity. We showed that any language of "polynomial size index" is in (nonuniform) TC^0. It is possible that a finer analysis of the structure results for maximal permutation groups will yield a similar result for other classes of languages, like the ones with subexponential or even exponential size index. We conjecture that a similar result is true for any language of "polynomial size Pólya index." We believe as well that there should be a relation between the algebraic structure of the syntactic monoid of a regular language $L \subseteq \{0, 1\}^*$ (Krohn-Rhodes theorem) and the family of invariance groups of L_n. As indicated by our preliminary work, straightforward approaches to such an investigation are not likely—the property of a group being representable is not preserved under homomorphism. Our parallel complexity results concern nonuniform families of boolean circuits. A natural sequel to our work might investigate uniform versions of some of our results. For instance, if $L \subseteq \{0, 1\}^*$ is a regular (or context free, or logspace computable, etc.) language with polynomial index (or polynomial size Pólya index) then is L in logspace uniform TC^0?

Another interesting question concerns the problem of giving an efficient algorithm A which on input a formal language L, a permutation $\sigma \in \mathbf{S}_n$, and an integer n, determines whether or not $\sigma \in \mathbf{S}_n(L)$, i.e.,

$$A(L, n, \sigma) = \begin{cases} 1 & \text{if } \sigma \in \mathbf{S}_n(L) \\ 0 & \text{otherwise.} \end{cases}$$

We investigated this question in the present paper for regular languages. The obvious algorithm has complexity $O(2^n)$ (to check membership of a permutation σ in $\mathbf{S}_n(L)$ test whether for all $x \in 2^n$, $x \in L_n \Leftrightarrow x^\sigma \in L_n$). A similar question applies to right-quotient representatives of $\mathbf{S}_n(L)$. It would also be interesting to investigate these questions for other types of languages, such as *CFL*, etc.

Acknowledgments. Discussions with Peter van Emde Boas, Danny Krizanc, Dominique Perrin, Paul Schupp, and Paul Vitányi are gratefully acknowledged. A. M. Cohen was extremely helpful with the literature on maximal permutation groups. Lambert Meertens made comments that significantly improved the presentation and pointed out that essentially our original n^2-upper-bound proof of the isomorphism theorem could yield the improved, $n(\log n+1)$-upper-bound.

REFERENCES

[AKS83] M. AJTAI, J. KOMLÓS, AND E. SZEMERÉDI, *An $O(n \log(n))$ sorting network*, in Proc. 15th Annual ACM Symposium on Theory of Computing, 1983, pp. 1-9.

[Arb69] M. A. ARBIB, *Theories of Abstract Automata*, Prentice-Hall Series in Automatic Computation, Prentice-Hall, Englewood Cliffs, NJ, 1969.

[ASW85] C. ATTIYA, M. SNIR, AND M. WARMUTH, *Computing on an anonymous ring*, in Proc. 4th Annual ACM Symposium on Principles of Distributed Computation, 1985.

[BLS87] L. BABAI, E. LUKS, AND A. SERESS, *Permutation Groups in* NC, in Proc. 19th ACM Symposium on Theory of Computing, New York, 1987.

[BB89] P. BEAME AND H. BODLAENDER, *Distributed computing on transitive networks: The torus*, in Proc. 6th Annual Symposium on Theoretical Aspects of Computer Science (STACS), 1989.

[BP55] R. A. BEAUMONT AND R. P. PETERSON, *Set-transitive permutation groups*, Canad. J. Math., 7 (1955), pp. 35-42.

[Ber71] C. BERGE, *Principles of Combinatorics*, Academic Press, New York, 1971.

[Com70] L. COMTET, *Analyse Combinatoire*, Deuxième Tome; Collection SUP, Presses Universitaires de France, 1970.

[Coo85] S. A. COOK, *A taxonomy of problems with fast parallel algorithms*, Inform. and Control, 64 (1985), pp. 2-22.

[FKPS85] R. FAGIN, M. KLAWE, N. PIPPENGER, AND L. STOCKMEYER, *Bounded-Depth, Polynomial-Size Circuits for Symmetric Functions*, Theoret. Comput. Sci., 36 (1985), pp. 239-250.

[FKL88] L. FINKELSTEIN, D. KLEITMAN, AND T. LEIGHTON, *Applying the classification theorem for finite simple groups to minimize pin count in uniform permutation architectures*, VLSI Algorithms and Architectures, 3rd Aegean Workshop on Computing (AWOC)88, Corfu, Greece, June/July 1988, J. H. Reif, ed., Lecture Notes in Computer Science 319, Springer-Verlag, Berlin, New York, pp. 247-256.

[FHL80] M. FURST, J. HOPCROFT, AND E. LUKS, *Polynomial-time algorithms for permutation groups*, in Proc. 21st IEEE Symposium on Foundations of Computer Science, Syracuse, NY, 1980.

[FSS84] M. FURST, J. SAXE, AND M. SIPSER, *Parity circuits and the polynomial time hierarchy*, Math. Systems Theory, 17 (1984), pp. 13-27.

[Hal57] M. HALL, *The Theory of Groups*, Macmillan, New York, 1957.

[Har64] M. HARRISON, *On the classification of Boolean functions by the general linear and affine groups*, J. Soc. Indust. Appl. Math., 12 (1964), pp. 285-299.

[Harr78] M. HARRISON, *Introduction to Formal Language Theory*, Addison Wesley, New York, 1978.

[KL82] B. W. KERNIGHAN AND S. LIN, *An efficient heuristic procedure for partitioning graphs*, Bell Systems Tech. J., 49 (1982).

[KL88] P. B. KLEIDMAN AND M. W. LIEBECK, *A survey of the maximal subgroups of the finite simple groups*, in Geometries and Groups, M. Aschbacher, A. M. Cohen, and W. M. Kantor, eds., reprinted from Geometriae Dedicata 25(1-3), pp. 375-389, D. Reidel, Dordrecht, the Netherlands, 1988.

[KK89] E. KRANAKIS AND D. KRIZANC, *Computing Boolean functions on anonymous networks*, Centrum voor Wiskunde en Informatica, Tech. Report CS-8935, Amsterdam, the Netherlands, September 1989.

[LPS88] M. W. LIEBECK, C. E. PRAEGER, AND J. SAXL, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A, 44 (1988), pp. 389-396.

[LM85] E. M. LUKS AND P. MCKENZIE, *Fast parallel computation with permutation groups*, in Proc. 26th IEEE Symposium on Foundations of Computer Science, 1985.

[MS78] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam 1978.

[McC56] E. J. MCCLUSKEY, JR., *Detection of group invariance or total symmetry of a Boolean function*, Bell Systems Tech. J., 35 (1956), pp. 1445-1453.

[McK84] P. MCKENZIE, *Parallel complexity and permutation groups*, Ph.D. thesis, Department of Computer Science, University of Toronto, Toronto, Ontario, Canada, 1984.

[MC85] P. MCKENZIE AND S. A. COOK, *The parallel complexity of abelian permutation group problems*, Tech. Report 181/85, Department of Computer Science, University of Toronto, Toronto, Ontario, Canada, 1985.

[Mul86] K. MULMULEY, *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field*, in Proc. 18th ACM Symposium on Theory of Computing, 1986, pp. 338-339.

[Pas66] D. S. PASSMAN, *Permutation Groups*, W. A. Benjamin, New York, Amsterdam, 1966.

[Pip79] N. PIPPENGER, *On simultaneous resource bounds*, in Proc. 20th IEEE Symposium on Foundations of Computer Science, 1979, pp. 307-311.

[PR87] G. PÓLYA AND R. C. READ, *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*, Springer-Verlag, Berlin, New York, 1987.

[Sav76] J. E. SAVAGE, *The Complexity of Computing*, John Wiley, New York, 1976.

[Sha49] C. SHANNON, *The synthesis of two-terminal switching circuits*, Bell Systems Tech. J. (1949), pp. 59-98.

[SV84] L. STOCKMEYER AND U. VISHKIN, *Simulation of parallel random access machines by circuits*, SIAM J. Comput., 13 (1984), pp. 409-422.

[Tzu82] T. TSUZUKU, *Finite Groups and Finite Geometries*, Cambridge University Press, Cambridge, U.K., 1982.

[Wie64] H. WIELANDT, *Finite Permutation Groups*, Academic Press, New York, 1964.

[Yab83] S. YABLONSKY, *Introduction aux mathématiques discrètes*, MIR, (translated from the Russian), 1983.

[Yao85] A. YAO, *Separating the polynomial time hierarchy by oracles*, in Proc. 26th IEEE Symposium on Foundations of Computer Science, 1985, pp. 1-10.