Distinguishing sets of the actions of symmetric groups

Tsai-Lien Wong [*†] Xuding Zhu[‡§]

Abstract

Suppose Γ is a group acting on a set X. An r-labeling $f : X \to \{1, 2, \ldots, r\}$ of X is distinguishing (with respect to the action of Γ) if for any $\sigma \in \Gamma, \sigma \neq \mathrm{id}_X$, there exists an element $x \in X$ such that $f(x) \neq f(\sigma(x))$. The distinguishing number, $D_\Gamma(X)$, of the action of Γ on X is the minimum r for which there is an r-labeling which is distinguishing. In case Γ is the automorphism group of a graph G, then $D_\Gamma(V(G))$ is denoted by $D(G)$, and is called the distinguishing number of the graph G. The distinguishing set of Γ actions is defined to be $D^*(\Gamma) = \{D_\Gamma(X) : \Gamma \text{ acts faithfully on } X\}$, and the distinguishing set of Γ graphs is defined to be $D(\Gamma) = \{D(G) : Aut(G) = \Gamma\}$. This paper studies the distinguishing sets of S_n actions and S_n graphs. It is proved that for any positive integers n, $\{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\} \subseteq D^*(S_n)$. It is known [12] that for any positive integers n, $\{\lceil n^{1/k} \rceil : k \in Z^+\} \subseteq D(S_n)$, and was conjectured in [12] that $D(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\}$ for $n \geq 7$. In this paper, we conjecture that $D^*(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\}$ for $n \geq 7$. We prove that both conjectures are true for almost all n. As consequences of the main results of this paper, a question of Tymoczko concerning the distinguishing set $D^*(S_n)$ of S_n actions is answered in positive, a conjecture of Albertson and Collins concerning the distinguishing set $D(S_n)$ of S_n graphs is proved for $n \geq 9$.

Key words: Distinguishing number; Distinguishing set of group actions; Symmetric groups; Group actions, Graphs.

AMS subject classification (2000): 20G15, 05C25, 20B25

1 Introduction

Distinguishing labeling was first defined by Albertson and Collins [1] for graphs. They quoted the following interesting "key problem" of Frank Rubin [17] to motivate the definition.

[*]Department of Applied Mathematics, National Sun Yat-sen University, Kaohsiung, Taiwan 80424, and National Center for Theoretical Sciences. e-mail: tlwong@math.nsysu.edu.tw

[†]Supported in part by the National Science Council under grant NSC92-2115-M-110-010

[‡]Department of Applied Mathematics, National Sun Yat-sen University, Kaohsiung, Taiwan 80424, and National Center for Theoretical Sciences. e-mail: zhu@math.nsysu.edu.tw

[§]Supported in part by the National Science Council under grant NSC92-2115-M-110-007

Professor X, who is blind, keeps keys on a circular key ring. Suppose there are a variety of handle shapes available that can be distinguished by touch. Assume that all keys are symmetrical so that a rotation of the key ring about an axis in its plane is undetectable from an examination of a single key. How many handle shapes does Professor X need to use in order to keep n keys on the ring and still be able to select the proper key by feel?

It turns out that if six or more keys are on the ring, there need only 2 different handle shapes; but if there are three, four or five keys on the ring, there must be 3 different handle shapes to distinguish them.

Besides a circular key ring, one could have other shapes of key holders. For example, one may have a linear key holder. In this case, 2 handle shapes are always enough: One just use different handle shapes for the keys on the two ends. To consider general shape of key holders, Albertson and Collins [1] defined distinguishing labeling of graphs. A labeling of a graph G, $f : V(G) \to \{1, 2, \cdots, r\}$, is said to be r-distinguishing if no non-trivial automorphism of G preserves all the vertex labels. In other words, f is r-distinguishing if for any $\sigma \in Aut(G)$, $\sigma \neq id$, there is a vertex x such that $f(x) \neq f(\sigma(x))$. The *distinguishing number* of a graph G is defined as

$$D(G) = \min\{r : \text{ there exists an } r\text{-distinguishing labeling of } G\}.$$

Distinguishing labeling attracted considerable recent attention [1, 2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 18, 19]. The concept was naturally extended to general group actions [19]. Let Γ be a group acting on a set X. For a positive integer r, an *r-labeling* of X is a mapping $f : X \to \{1, 2, \ldots, r\}$. We say f is a *distinguishing labeling* (with respect to the action of Γ) if for any $\sigma \in \Gamma$, σ is not the identity, there is an element $x \in X$ such that $f(x) \neq f(\sigma(x))$. The *distinguishing number* $D_\Gamma(X)$ of the action of Γ on X is defined as

$$D_\Gamma(X) = \min\{r : \text{ there exists an } r\text{-distinguishing labeling}\}.$$

The distinguishing number of a Γ action depends heavily on the structure of the group Γ. By simply knowing the group Γ, one can say a lot about the distinguishing number of a graph G with $Aut(G) = \Gamma$ and the distinguishing number of an action of Γ on a set X. For example, it was proved in [1] that if Γ is an Abelian group with at least two elements, then for any graph G with $Aut(G) = \Gamma$, $D(G) = 2$, if Γ is a dihedral group, then for any graph G with $Aut(G) = \Gamma$, $D(G) \leq 3$. This result was generalized by Chan [7], who proved that if Γ is a nilpotent of class c or supersolvable of length c then $D_\Gamma(X) \leq c + 1$ for any faithful action of Γ on a set X. It was proved in [19] that for any group Γ, if $|\Gamma| < (k + 1)!$ then $D_\Gamma(X) \leq k$ for any faithful action of Γ on a set X.

For a given group Γ, Albertson and Collins [1] defined the *distinguishing set of Γ graphs* as

$$D(\Gamma) = \{D(G) : G \text{ is a graph with } \ Aut(G) = \Gamma\}.$$

In this paper, we define the *distinguishing set of* Γ *actions* as

$$D^*(\Gamma) = \{D_\Gamma(X) : \Gamma \text{ acts faithfully on } X\}.$$

(The "distinguishing set of Γ graphs" was called the "distinguishing set of Γ" in [1]. We add "graphs" in this paper to avoid confusion with the "distinguishing set of Γ actions".) Observe that for a graph G, $D(G) = D_{Aut(G)}(V(G))$. So for any group Γ, $D(\Gamma)$ is a subset of $D^*(\Gamma)$.

It follows from the above mentioned results of [1] and [7] that if Γ is an Abelian group, then $D^*(\Gamma) = D(\Gamma) = \{2\}$. Let D_n be the dihedral group of order $2n$. It was proved in [1] that $D(D_n) = \{2\}$ unless $n = 3, 4, 5, 6, 10$, in which cases $D(D_n) = \{2, 3\}$. The proof in [1] actually works for general actions of dihedral groups. So we have $D^*(D_n) = \{2\}$ unless $n = 3, 4, 5, 6, 10$, in which cases $D^*(D_n) = \{2, 3\}$. It is a difficult problem to determine the distinguishing set of Γ actions or Γ graphs for an arbitrary group Γ. The distinguishing set of the actions or graphs of symmetric group was discussed in [1, 19, 12]. It was proved in [1] that $D(S_4) = \{2, 4\}$. It was proved in [19] that for any $n \geq 2$, $D^*(S_n) \subseteq \{2, 3, \cdots, n\}$, and $D^*(S_4) = \{2, 3, 4\}$. This result shows that not all faithful group actions are realized as actions of the automorphism group of a graph on its vertex set, and that $D(\Gamma)$ and $D^*(\Gamma)$ could be different. Recently, Klavžar, Wong and Zhu [12] proved that for any positive integer k, $\lceil n^{1/k} \rceil \in D(S_n)$. In general, we know very little about the distinguishing set of S_n actions and the distinguishing set of S_n graphs. The following conjectures and question were proposed by Albertson and Collins [1], Tymoczko [19] and Klavžar, Wong and Zhu [12] respectively:

Conjecture 1.1 *[1] For any $n \geq 4$, $n - 1 \notin D(S_n)$.*

Question 1.2 *[19] Is it true that $n - 1 \in D^*(S_n)$ for arbitrarily large n?*

Conjecture 1.3 *[12] For any integer $n > 6$, $D(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\}$.*

In this paper, we shall prove that for any n, $\{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\} \subseteq D^*(S_n)$. In particular, for any positive integer n, we have $n - 1 \in D^*(S_n)$, This answers Question 1.2 in the affirmative.

We conjecture that $D^*(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\}$ for all $n \neq 6$. We prove that the conjectured equality holds true for almost all n.

As a tool used in the study of the above conjecture, we analysis the orbit of group actions. Suppose a group Γ acts on a set X and $Stab_x = \{\sigma \in \Gamma : \sigma(x) = x\}$ is the stabilizer of an element x. Then for any $\sigma, \tau \in \Gamma$, $\sigma(x) = \tau(x)$ if and only if $\tau^{-1}\sigma \in Stab_x$, i.e., σ, τ are in the same (left) coset of $Stab_x$. Thus $\phi(\sigma(x)) = \sigma Stab_x$ is a one to one correspondence from O, the orbit containing x, to the cosets of $Stab_x$. In this sense, each orbit of the action of Γ on a set X is associated with a subgroup of Γ, and we may identify the elements of an orbit with the cosets of its associated subgroup. The action of Γ on the cosets (which are identified with elements of X) are simply left multiplication. It follows from the definition that the cardinality of an orbit O is equal

to the index $[\Gamma : H]$ of its associated subgroup H. In particular, orbits of cardinality 1 are associated with the group Γ itself.

Consider an action of S_n on a set X without orbits of cardinality 1. An orbit O is called small if the associated subgroup is isomorphic to S_{n-1}, A_n or A_{n-1}. So a small orbit has cardinality at most $2n$. We prove that if each orbit of S_n on X is small, then

$$D_{S_n}(X) \in \{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\}.$$

Then we consider those S_n actions for which there is a big orbit, i.e., an orbit O whose associated subgroup is not isomorphic to S_{n-1}, A_n, A_{n-1}. In Section 5, we prove that if there is an orbit whose associated subgroup is an intransitive subgroup H of S_n and $H \neq S_{n-1}, A_{n-1}$, then the action is 2-distinguishable. In Section 6, we prove that if there is an orbit whose associated subgroup is a transitive but imprimitive subgroup H of S_n, then the action is 2-distinguishable. It is known [4] that for almost all positive integers n, the only primitive subgroups of S_n are S_n and A_n. In other words, for almost all positive integers n, any subgroup H of S_n with $H \neq S_n, A_n$ is intransitive or imprimitive. Thus we conclude that for almost all positive integers n, $D^*(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\}$. Combined with a result in [12], we also conclude that for almost all positive integers n, $D(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\}$.

For those integers n for which S_n does contain primitive subgroups $H \neq S_n, A_n$, it is known that $|H|$ is relatively small, and hence $[S_n : H]$ is large. For example, by Bochert's Theorem (Theorem 14.2 of [20]): if H is a primitive subgroup of S_n and $H \neq S_n, A_n$, then the index of H is $[S_n : H] \geq \lfloor \frac{n+1}{2} \rfloor !$. Using Bochert's Theorem, we prove that if $n! < \ell! \lfloor \frac{n+1}{2} \rfloor !$ and an action of S_n on X has an orbit whose associated subgroup H is not isomorphic to S_{n-1}, A_n, A_{n-1}, then $D_{S_n}(X) \leq \ell$. This implies that if $n \geq 9$ and G is a graph with $Aut(G) = S_n$, then $D(G) \neq n-1$, i.e., Conjecture 1.1 is true for $n \geq 9$. For large values of n, Bochert's Theorem has been improved by many authors. It was proved by Maróti [16] that if H is a primitive subgroup of S_n and $H \neq S_n, A_n$, then $|H| < 50n^{\sqrt{n}}$. Using this result, we prove that for any integer n, if an action of S_n on X has an orbit whose associated subgroup is not isomorphic to S_{n-1}, A_n, A_{n-1}, then $D_{S_n}(X) \leq \lceil e\sqrt{n} \rceil$.

2 Integers contained in $D^*(S_n)$

An action of S_n on a set X is actually a homomorphism from S_n to the permutation group $Sym(X)$ on X. However, for simplicity, an group element $\sigma \in S_n$ and its image in $Sym(X)$ under the homomorphism is denoted by the same letter σ. So σ is a permutation on the set $\{1, 2, \cdots, n\}$ as well as a permutation on X, and hence $\sigma(x)$ for $x \in X$ and $\sigma(j)$ for $j = \{1, 2, \cdots, n\}$ are well-defined.

Lemma 2.1 *For any integer $n \geq 1$, $n, n-1 \in D^*(S_n)$.*

Proof. Let $X = \{x_1, x_2, \cdots, x_n\}$ and let $\sigma(x_i) = x_{\sigma(i)}$. Then it is obvious that $D_{S_n}(X) = n$. Let $X' = \{x_1, x_2, \cdots, x_n, u, v\}$, and let $\sigma(x_i) = x_{\sigma(i)}$. Let $\sigma(u) =$

$u, \sigma(v) = v$ if σ is even, and let $\sigma(u) = v$ and $\sigma(v) = u$ if σ is odd. First we show that $D_{S_n}(X') \leq n-1$. Let $f(u) = 1, f(v) = 2$, and let $f(x_i) = i$ for $i = 1, 2, \cdots, n-1$ and $f(x_n) = n-1$. If σ is labeling preserving, then we must have $\sigma(i) = i$ for $i = 1, 2, \cdots, n-2$. Thus if $\sigma \neq id$, then $\sigma = ((n-1)\ n)$. But then σ is odd and hence σ interchanges u and v. This is a contradiction, as u and v have distinct labels.

Next we show that $D_{S_n}(X') \geq n-1$. Let f be an $(n-2)$-labeling of X'. Then either there exist three indices i, j, s such that $f(x_i) = f(x_j) = f(x_s)$, or there are two pairs of indices i, i' and j, j' such that $f(x_i) = f(x_{i'})$ and $f(x_j) = f(x_{j'})$. In the former case (ijs) is a labeling preserving permutation, and in the latter case $(ii')(jj')$ is a labeling preserving permutation. Therefore $D_{S_n}(X') = n-1$. □

Lemma 2.2 *For any group Γ, if $t \in D^*(\Gamma)$, then for any positive integer k, $\lceil t^{1/k} \rceil \in D^*(\Gamma)$.*

Proof. Assume Γ acts faithfully on X and $D_\Gamma(X) = t$. Let $X' = X \times \{0, 1, \cdots, k-1\}$. Define an action of Γ on X' as $\sigma((x,i)) = (\sigma(x), i)$ for $\sigma \in \Gamma$ and $(x,i) \in X'$. First we show that if $d^k \geq t$, then there is a d-distinguishing of X'.

For a d-labeling g of X', let $f(x) = (g(x,0), g(x,1), \cdots, g(x,k-1))$. If $d^k \geq t$, then we can define g in such a way that f is a distinguishing labeling of X. Thus for any $\sigma \in \Gamma$ such that $\sigma \neq id$, there is an $x \in X$ such that $f(x) \neq f(\sigma(x))$. This means that there is an $i \in \{0, 1, \cdots, k-1\}$, $g(x,i) \neq g(\sigma(x), i) = g(\sigma((x,i)))$. Therefore g is a d-distinguishing labeling of X'. On the other hand, if $d^k < t$, then for any choice of g, f is not a distinguishing labeling of X. I.e., there exists $\sigma \in \Gamma$ such that $\sigma \neq id$ and $f(x) = f(\sigma(x))$ for every x. This implies that $g((x,i)) = g(\sigma(x,i))$ for every $(x,i) \in X'$. Therefore $D_\Gamma(X') = \lceil t^{1/k} \rceil$. □

Corollary 2.3 *For any positive integers n, $\{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\} \subseteq D^*(S_n)$.*

3 Actions of S_n with small orbits

Suppose Γ is a group which acts faithfully on X. Let $v \in X$ be an element of X, and let $H = Stab_v$ be the stabilizer of v. Let $g_1, g_2, \cdots, g_m$ be any representatives of the left cosets of H. Then for $i \neq j$, $g_i(v) \neq g_j(v)$ and $O = \{g_1(v), g_2(v), \cdots, g_m(v)\}$ is the orbit of X containing v. So there is a one to one correspondence between the elements of O and the cosets of H. We call the subgroup H the *associated subgroup* of orbit O. Observe that the associated subgroup of an orbit is unique up to isomorphism, since the stabilizers of the elements of an orbit are conjugate. In the following, an orbit O of a group Γ on X is identified with the cosets of its associated subgroup. The action of Γ on the cosets is just the (left) multiplication of the cosets.

An orbit of size 1 is associated with the trivial subgroup of Γ, namely the group Γ itself. It is obvious that orbits of Γ on X of size 1 can be deleted from the set X

without changing the distinguishing number $D_\Gamma(X)$. In the following, we assume that each orbit has size greater than 1. In other words, each orbit is associated with a proper subgroup of Γ.

In the following we only consider actions of the symmetric group S_n on a set X. We say an orbit O is a *small orbit* if the associated subgroup of O is isomorphic to A_n, S_{n-1} or A_{n-1}. As an orbit O associated with a subgroup H has cardinality $|O| = [S_n : H]$, it follows that a small orbit has cardinality $2, n$ or $2n$. The other orbits are called *big orbits*.

It was proved in [14] that if $n > 6$ and H is a subgroup with $[S_n : H] < \binom{n}{2}$, then H is isomorphic to A_n, S_{n-1} or A_{n-1}. This implies that a big orbit has cardinality at least $\binom{n}{2}$.

In this section, we study the distinguishing number of those S_n actions for which each orbit is small. The same question concerning graphs was discussed in [12], where the following result was proved:

Theorem 3.1 *Suppose $n > 6$ and G is a graph with $Aut(G) = S_n$. If each orbit of G is small, then $D(G) = \lceil n^{1/k} \rceil$ for some positive integer k.*

In this section, we prove that an analogue result holds for general S_n actions.

Theorem 3.2 *Suppose $n > 6$ and S_n acts faithfully on X. If each orbit is small, then either $D_{S_n}(X) = \lceil n^{1/k} \rceil$ for some $k \geq 1$, or $D_{S_n}(X) = \lceil (n-1)^{1/k} \rceil$ for some $k \geq 1$.*

Proof. Suppose S_n acts faithfully on X, and the associated subgroup of each orbit is isomorphic to A_n, S_{n-1} or A_{n-1}.

Let $X_1, X_2, \cdots, X_q$ be orbits of X of cardinality n, let $Y_1, Y_2, \cdots, Y_p$ be orbits of X of cardinality $2n$, and let $Z_1, Z_2, \cdots, Z_r$ be orbits of X of cardinality 2.

As each X_i is associated with S_{n-1}, we can rename the vertices of X_i as $\{x_{i1}, x_{i2}, \cdots, x_{in}\}$, so that the action of S_n on X_i is defined as $\tau(x_{ij}) = x_{i\tau(j)}$.

Similarly, we can rename the vertices of Y_i as $\{a_{i1}, b_{i1}, a_{i2}, b_{i2}, \cdots, a_{in}, b_{in}\}$. The action of S_n on Y_i is defined as follows: If τ is even then $\tau(a_{ij}) = a_{i\tau(j)}, \tau(b_{ij}) = b_{i\tau(j)}$. If τ is odd, then $\tau(a_{ij}) = b_{i\tau(j)}, \tau(b_{ij}) = a_{i\tau(j)}$.

Each Z_i is associated with A_n. The vertices of Z_i can be renamed as $\{u_i, v_i\}$. Then the action of S_n on Z_i is defined as follows: If τ is even then $\tau(u_i) = u_i, \tau(v_i) = v_i$. If τ is odd, then $\tau(u_i) = v_i, \tau(v_i) = u_i$.

Now we claim that if $p = r = 0$, then $D_{S_n}(X) = \lceil n^{1/q} \rceil$; otherwise, $D_{S_n}(X) = \lceil (n-1)^{1/(q+2p)} \rceil$.

Case 1. $p = r = 0$. Since S_n acts faithfully on X, we must have $q > 0$. Let f be a d-labeling of X. For $i = 1, 2, \cdots, n$, let

$$\vec{s}_i = (f(x_{1i}), f(x_{2i}), \cdots, f(x_{qi})).$$

If $d^q \geq n$, then we can choose f in such a way that all the $\vec{s}_i$'s are distinct. The argument in the proof of Lemma 2.2 shows that such a labeling is distinguishing. If

$d^q < n$, then for any d-labeling f, there exists distinct indices i, i' such that $\vec{s}_i = \vec{s}_{i'}$. Then (ii') is a permutation which preserves the labels. So f is not a distinguishing labeling. Therefore $D_{S_n}(X) = \lceil n^{1/q} \rceil$.

Case 2. $r \neq 0$ or $p \neq 0$. First we show that if $d^{q+2p} \geq n-1$, then there is a d-distinguishing labeling. Again since S_n acts faithfully on X, we must have $q + 2p > 0$. Assume $d^{q+2p} \geq n-1$. Let f be a d-labeling of X. For $i = 1, 2, \cdots, n$, let

$$\vec{s}_i = (f(x_{1i}), f(x_{2i}), \cdots, f(x_{qi}), f(a_{1i}), f(b_{1i}), f(a_{2i}), f(b_{2i}), \cdots, f(a_{pi}), f(b_{pi})),$$

and let

$$\vec{s'}_i = (f(x_{1i}), f(x_{2i}), \cdots, f(x_{qi}), f(b_{1i}), f(a_{1i}), f(b_{2i}), f(a_{2i}), \cdots, f(b_{pi}), f(a_{pi})).$$

As $d^{q+2p} \geq n-1$, we can choose f in such a way that $\vec{s}_2, \vec{s}_3, \cdots, \vec{s}_n$ are all distinct and $\vec{s}_1 = \vec{s}_2$. Moreover, if $p > 0$, then we can choose f so that $f(a_{11}) \neq f(b_{11})$. Hence $\vec{s}_1 \neq \vec{s'}_1$. If $r > 0$, then we choose the labeling f such that $f(u_1) = 1$ and $f(v_1) = 2$. Now suppose $\tau \in S_n$ preserves the labels. First we show that τ must be even. If $r > 0$, then τ is even because u_1 and v_1 have different labels. Assume $r = 0$. Then $p > 0$. If τ is odd, then we should have $\vec{s}_1 = \vec{s'}_{\tau(1)}$ and $\vec{s}_2 = \vec{s'}_{\tau(2)}$. This implies that $\vec{s}_{\tau(1)} = \vec{s}_{\tau(2)}$. By our choice of f, if $j \neq 1, 2$, then $\vec{s}_j$ is different from $\vec{s}_{j'}$ for any $j' \neq j$. So we should have $\{\tau(1), \tau(2)\} = \{1, 2\}$. However, $\vec{s}_1 = \vec{s}_2 \neq \vec{s'}_1 = \vec{s'}_2$, in contrary to the requirement that $\vec{s}_1 = \vec{s'}_{\tau(1)}$ and $\vec{s}_2 = \vec{s'}_{\tau(2)}$. This proves that τ is even.

Since τ is even, it follows that for any i, $\vec{s}_i = \vec{s}_{\tau(i)}$. Hence $\tau(i) = i$ for $i = 3, 4, \cdots, n$. As τ is even, we conclude that $\tau = id$.

On the other hand, if $d^{q+2p} \leq n-2$, then for any d-labeling f, either $\vec{s}_i = \vec{s}_j = \vec{s}_t$ for three distinct indices i, j, t, or there are two disjoint pairs of indices i, i', and j, j' such that $\vec{s}_i = \vec{s}_{i'}, \vec{s}_j = \vec{s}_{j'}$. In the former case, $\tau = (ijt)$ preserves the labels. In the latter case, $\tau = (ii')(jj')$ preserves the labels. □

4 Conjectures

The concern of this paper is the distinguishing set $D^*(S_n)$ of S_n actions and the distinguishing set $D(S_n)$ of S_n graphs. As mentioned in introduction, for the set $D(S_n)$, it was conjectured in [12] that if $n > 6$, then $D(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\}$.

In this paper, we propose an analogue conjecture for the distinguishing set $D^*(S_n)$ of S_n actions.

Conjecture 4.1 *For any positive integer $n \neq 6$, then $D^*(S_n) = \{\lceil n^{1/k} \rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k} \rceil : k \in Z^+\}$.*

If $n \leq 5$, then it follows from Corollary 2.3 and a result in [19] that $D^*(S_n) = \{2, 3, \cdots, n\}$. Thus for Conjecture 4.1, we only need to consider the case that $n > 6$. By Theorem 3.2, to determine the distinguishing set of S_n actions, we only need to

consider those actions of S_n on X for which there is a big orbit O, i.e., an orbit O whose associated subgroup is not isomorphic to A_n, S_{n-1}, A_{n-1}. Note that if $n > 6$, H is a subgroup of S_n and $H \neq A_n$, then since H does not contain a normal subgroup of S_n, the action of S_n on the cosets of H is faithful. A d-labeling f of the cosets of a subgroup H is called distinguishing labeling if for any $\tau \in S_n$ which is not the identity, there is a coset $gH \in X$ such that gH and τgH are labeled by distinct labels. A subgroup H of S_n is called *d-distinguishing* if there is a d-distinguishing labeling of the set of cosets of H. The following lemma follows from the definition, and can also be used as the definition of d-distinguishing subgroups.

Lemma 4.2 *Suppose S_n acts on X and O is an orbit associated to H. If H is a d-distinguishing subgroup of S_n and the action of S_n on O is faithful, then $D_{S_n}(X) \leq d$*

The question we are interested now is that if H is a proper subgroup of S_n and $H \neq A_n, S_{n-1}, A_{n-1}$, what is the smallest d for which H is d-distinguishing. We propose the following conjecture:

Conjecture 4.3 *Suppose $n > 6$ and H is a proper subgroup of S_n. If $H \neq A_n, S_{n-1}, A_{n-1}$, then H is 2-distinguishing.*

Conjecture 4.3 is equivalent to say that if $n > 6$ and S_n acts faithfully on X and there is an element $x \in X$ whose stabilizer $Stab_x \neq A_n, S_{n-1}, A_{n-1}$, then the action is 2-distinguishable. Conjecture 1.3 and Conjecture 4.1 are consequences of Conjecture 4.3.

Theorem 4.4 *Conjecture 4.3 implies Conjecture 4.1 and Conjecture 1.3.*

Proof. Assume Conjecture 4.3 is true. If the action of S_n on X has a big orbit, then by Conjecture 4.3 and Lemma 4.2, $D_{S_n}(X) = 2 = \lceil n^{1/k} \rceil$ for a sufficiently large k. Otherwise, each orbit of S_n on X is small, and hence by Lemma 3.2, $D_{S_n}(X) = \lceil n^{1/k} \rceil$ or $\lceil (n-1)^{1/k} \rceil$ for some positive integer k. So Conjecture 4.1 is true.

If G is a graph with $Aut(G) = S_n$. If there is a big orbit, then Conjecture 4.3 and Lemma 4.2 implies that $D(G) = 2 = \lceil n^{1/k} \rceil$ for a sufficiently large k. Otherwise, each orbit of S_n on X is small, by Theorem 3.1, in this case $D(G) = \lceil n^{1/k} \rceil$ for some positive integer k. So Conjecture 1.3 is true. □

5 Intransitive subgroups

A subgroup H of S_n is called *transitive* if for any $i, j \in \{1, 2, \cdots, n\}$, there is a $\tau \in H$ such that $\tau(i) = j$. Otherwise H is called intransitive. Thus if H is intransitive, then the action of H on $\{1, 2, \cdots, n\}$ has more than one orbit. A subgroup H of S_n is called *imprimitive* if H is transitive and there is a partition of $\{1, 2, \cdots, n\}$ into subsets $B_1, B_2, \cdots, B_m$ for some $1 < m < n$ such that for any $\tau \in H$, for any $j \in \{1, 2, \cdots, m\}$,

$\tau(B_j) = B_{j'}$ for some $j' \in \{1, 2, \cdots, m\}$. Each B_i is called a *block* of H. Note that since an imprimitive subgroup H is transitive, the blocks of H have the same cardinality k for some integer $1 < k < n$.

In this section, we prove that Conjecture 4.3 is true if the subgroup H is intransitive.

Theorem 5.1 *Suppose $n > 6$. If H is an intransitive subgroup of S_n and $H \neq A_{n-1}, S_{n-1}$, then H is 2-distinguishing.*

Proof. Suppose H is an intransitive subgroup of S_n and $H \neq A_{n-1}, S_{n-1}$. Then there are at least 2 orbits of H on $\{1, 2, \cdots, n\}$. We consider two cases.

Case 1. There is an orbit of H on $\{1, 2, \cdots, n\}$ of cardinality 1.

Without loss of generality, we assume that n is fixed by all the elements of H, i.e., H is a subgroup of S_{n-1} (we view an element $\sigma \in S_n$ which fixes n as an element of S_{n-1}, as S_{n-1} is viewed as a subgroup of S_n). Since $H \neq A_{n-1}, S_{n-1}$, the index $[S_{n-1} : H]$ is at least $n-1$ (as $n-1 \neq 4$). Let $T_1, T_2, \cdots, T_m$ be the cosets of H in S_{n-1}, where $m \geq n-1$. Since S_{n-1} has n cosets in S_n, namely $(1n)S_{n-1}, (2n)S_{n-1}, \cdots, (n-1n)S_{n-1}, S_{n-1}$, the cosets of H in S_n are

$$(1n)T_1, \cdots, (1n)T_m, (2n)T_1, \cdots, (2n)T_m, \cdots, (n-1n)T_1, \cdots, (n-1n)T_m, T_1, \cdots, T_m.$$

For $j = 1, 2, \cdots, n-1$, let $\mathcal{B}_j = \{(jn)T_1, (jn)T_2, \cdots, (jn)T_m\}$ and let $\mathcal{B}_n = \{T_1, T_2, \cdots, T_m\}$. For $\tau \in S_n$, define $\tau(\mathcal{B}_n)$ as

$$\tau(\mathcal{B}_n) = \{\tau(T_1), \tau(T_2), \cdots, \tau(T_m)\}.$$

Observe that $\mathcal{B}_j = (jn)\mathcal{B}_n$ and if $\tau \in S_{n-1}$, i.e., if $\tau(n) = n$, then $\tau(\mathcal{B}_n) = \mathcal{B}_n$.

Suppose $\tau \in S_n$. For any $j \neq n$, $(\tau(j)n)\ \tau\ (jn) \in S_{n-1}$. This implies that

$$\tau(\mathcal{B}_j) = (\tau(j)n)\ (\tau(j)n)\ \tau\ (jn)\mathcal{B}_n = \mathcal{B}_{\tau(j)}.$$

Let f be the 2-labeling of the cosets of H in S_n in such a way that $\mathcal{B}_j$ contains exactly $j-1$ cosets of label 1. As $m \geq n-1$, this is possible. If $\tau \in S_n$ is label preserving, then $\mathcal{B}_j$ and $\mathcal{B}_{\tau(j)}$ have the same number of cosets of label 1. Hence $\tau(j) = j$ for all j and $\tau = id$. So f is a distinguishing labeling.

Case 2. Each orbit of H on $\{1, 2, \cdots, n\}$ has cardinality at least 2.

Then there is an orbit Q of H on $\{1, 2, \cdots, n\}$ such that $2 \leq |Q| \leq n/2$. Without loss of generality, assume that $Q = \{1, 2, \cdots, q\}$, where $2 \leq q \leq n/2$.

Let $\sigma = (1\ 2\ 3\ \cdots\ n)$, and let $\psi = (1\ (q+1))(3\ (q+2))$. Let $Z = \{\psi, \sigma^j : j = 0, 1, \cdots, n-q\}$. Let f be the 2-labeling which labels cosets ϕH by label 1 for $\phi \in Z$ and label other cosets of H by label 2.

Consider the hypergraph $\mathcal{G}$ with vertex set $\{1, 2, \cdots, n\}$, in which E is a hyperedge if and only if $E = \phi(\{1, 2, \cdots, q\})$ for some $\phi \in Z$. In other words, the hyperedges of $\mathcal{G}$ are $\{1, 2, \cdots, q\}, \{2, 3, \cdots, q+1\}, \cdots, \{n-q+1, n-q+2, \cdots, n\}$ and $\{2, 4, 5, \cdots, q+2\}$.

Suppose $\tau \in S_n$ preserves the labeling f. We claim that τ is an automorphism of the hypergraph $\mathcal{G}$. Let E be an hyperedge of $\mathcal{G}$. Then $E = \phi(\{1, 2, \cdots, q\})$, where $\phi \in Z$.

Since τ preserves the label f, we conclude that $\tau\phi H = \phi' H$ for some $\phi' \in Z$. This means that $\tau\phi = \phi' h$ for some $h \in H$. As $\{1, 2, \cdots, q\}$ is an orbit of H on $\{1, 2, \cdots, n\}$, we have $h(\{1, 2, \cdots, q\}) = \{1, 2, \cdots, q\}$. Therefore

$$\tau(E) = \tau\phi(\{1, 2, \cdots, q\}) = \phi'(\{1, 2, \cdots, q\})$$

is a hyperedge of $\mathcal{G}$. Thus τ is indeed an automorphism of $\mathcal{G}$. We claim that $\mathcal{G}$ is a rigid hypergraph, i.e., the only automorphism of $\mathcal{G}$ is the identity. For each vertex i of $\mathcal{G}$, the degree of i in $\mathcal{G}$, denoted by $d(i)$, is the number of hyperedges containing i. We say two vertices are *adjacent* if there is a hyperedge containing both vertices. It is easy to verify that $1, n$ are the only two vertices of degree 1. So for any automorphism ϕ of $\mathcal{G}$, we must have $\phi(\{1, n\}) = (\{1, n\})$. If $q \geq 3$, then $n - 1$ is the only vertex of degree 2. Thus n is adjacent to $n - 1$, which is a vertex of degree 2, and since $n > 6$ and $q \leq n/2$, 1 is not adjacent to any vertex of degree 2. Therefore any automorphism must fixes each of 1 and n. If $q = 2$, then 1 is adjacent to 2, which is a vertex of degree 3, and n is not adjacent to any vertex of degree 3. So again, any automorphism must fixes each of 1 and n. Now $n - 1$ is the only vertex in $\mathcal{G} - \{n\}$ which has degree 1 and distinct from 1. Thus any automorphism of $\mathcal{G}$ must fix $n - 1$. Repeat this argument, one can show that any automorphism of $\mathcal{G}$ must fix j for $j = n-2, n-3, \cdots, q+3$. On the other hand, 2 is the only vertex such that there are two edges E_1, E_2 containing 2, with $1 \in E_1$ and $|E_1 \cap E_2| = q - 1$. So any automorphism of $\mathcal{G}$ must fix 2. By considering the subgraph of $\mathcal{G}$ obtained by deleting $1, 2$, we conclude that 3 is fixed by any automorphism of $\mathcal{H}$. Repeat this argument, one can show that any automorphism of $\mathcal{G}$ must fix j for $j = 3, 4, \cdots, n - q + 1 \geq q + 1$. Thus $\mathcal{H}$ is a rigid hypergraph, and f is a distinguishing labeling. □

6 Imprimitive subgroups

In this section, we prove that Conjecture 4.3 is true if the subgroup H is imprimitive.

Theorem 6.1 *Assume $n > 6$. If H is a subgroup of S_n which is imprimitive, then H is 2-distinguishing.*

Proof. Suppose H is a subgroup of S_n which is imprimitive. Let $B_1, B_2, \cdots, B_m$ be the blocks of H, where $m \geq 2$, and each block has cardinality $k \geq 2$. Without loss of generality, we assume $B_i = \{(i-1)k + 1, (i-1)k + 2, \cdots, ik\}$ for $i = 1, 2, \cdots, m$. Let

$$\mathcal{B} = \{B_1, B_2, \cdots, B_m\}.$$

For $\phi \in S_n$, let

$$\phi(\mathcal{B}) = \{\phi(B_1), \phi(B_2), \cdots, \phi(B_m)\}.$$

The sets $\phi(B_1), \phi(B_2), \cdots, \phi(B_m)$ are the *blocks* of ϕ. For an element $i \in \{1, 2, \cdots, n\}$ and for $\phi \in S_n$, we denote by $[i]_\phi$ the block of ϕ containing i. For a subset T of S_n, the *T-block containing i* is defined as

$$[i]_T = \cap_{\phi \in T}[i]_\phi.$$

We define the *T-degree of i* as

$$d_T(i) = |[i]_T|.$$

In the remainder of the proof, Z is a subset of S_n, and f is a 2-labeling of the cosets of H which labels ϕH by label 1 if $\phi \in Z$, and labels other cosets of H by label 2. Let $\psi \in S_n$ be an arbitrary permutation such that for any $\phi \in Z$, $\psi\phi H = \phi' H$ for some $\phi' \in Z$, i.e., ψ preserves the labels. We shall prove that for an appropriately chosen Z, the labeling f is a distinguishing labeling. In other words, we shall prove that $\psi = id$. The proof is divided into three cases. In each case, the choice of Z is different. However, in each case, the proof is divided into two steps.

The first step is to prove that $\psi\phi(\mathcal{B}) = \phi(\mathcal{B})$ for each $\phi \in Z$. This implies that for any $j \in \{1, 2, \cdots, n\}$, for any $\phi \in Z$,

$$\psi([j]_\phi) = [\psi(j)]_\phi.$$

This implies the following statement:

(*) For any subset T of Z, for any $j \in \{1, 2, \cdots, n\}$, $d_T(j) = d_T(\psi(j))$.

The second step is, by using Property (*), to prove that $\psi(j) = j$ for each $j \in \{1, 2, \cdots, n\}$.

Case 1. $k \geq 3$ and $(m, k) \neq (2, 4)$.

Let $\sigma_0 = id$ and for $j = 1, 2, \cdots, k-1$, let

$$\sigma_j = (j\ (k{+}j)\ (2k{+}j)\ \cdots\ ((m{-}1)k{+}j))((j{+}1)\ (k{+}j{+}1)\ (2k{+}j{+}1)\ \cdots\ ((m{-}1)k{+}j{+}1)),$$

let

$$\tau = (1\ (k+2))$$

and let

$$Z = \{\sigma_i : i = 0, 1, 2, \cdots, k-1\} \cup \{\tau\}.$$

Straightforward calculation shows that the blocks of σ_j and τ are as follows:

$$\begin{aligned}
\sigma_0(\mathcal{B}) &= \{\{1, 2, \cdots, k\}, \{k+1, k+2, \cdots, 2k\}, \cdots, \{(m-1)k+1, (m-1)k+2, \cdots, mk\}\}. \\
\sigma_1(\mathcal{B}) &= \{\{k+1, k+2, 3, \cdots, k\}, \{2k+1, 2k+2, k+3, \cdots, 2k\}, \\
&\quad \cdots, \{1, 2, (m-1)k+3, \cdots, mk\}\}. \\
\sigma_2(\mathcal{B}) &= \{\{1, k+2, k+3, 4, \cdots, k\}, \{k+1, 2k+2, 2k+3, k+4, \cdots, 2k\}, \\
&\quad \cdots, \{(m-1)k+1, 2, 3, (m-1)k+4, \cdots, mk\}\}. \\
&\quad \cdots\cdots \\
\sigma_{k-1}(\mathcal{B}) &= \{\{1, 2, \cdots, k-2, k+(k-1), k+k\}, \{k+1, k+2, \cdots, k+(k-2), 2k+(k-1),
\end{aligned}$$

$$
\begin{aligned}
& 2k+k\},\cdots,\{(m-1)k+1,(m-1)k+2,\cdots,(m-1)k+(k-2),k-1,k\}\}.\\
\tau(\mathcal{B}) \;=\; & \{\{k+2,2,3,\cdots,k\},\{k+1,1,k+3,\cdots,2k\},\{2k+1,2k+2,\cdots,3k\},\\
& \cdots,\{(m-1)k+1,(m-1)k+2,\cdots,mk\}\}.
\end{aligned}
$$

As $(m,k)\neq(2,4)$, it follows that if $\phi,\phi'\in Z$ and $\phi\neq\phi'$, then $\phi(\mathcal{B})\neq\phi'(\mathcal{B})$. So all the cosets in the set $\{\phi H:\phi\in Z\}$ are distinct.

Construct an *edge colored graph* G whose vertex set is $V(G)=\{\phi(\mathcal{B}):\phi\in Z\}$, and in which

- $\phi(\mathcal{B})$ and $\phi'(\mathcal{B})$ are connected by a red edge if there is a permutation θ of $\{1,2,\cdots,m\}$ such that there are two indices i_1,i_2, $|\phi(B_i)\cap\phi'(B_{\theta(i)})|=k-1$ if $i\in\{i_1,i_2\}$, and $\phi(B_i)=\phi'(B_{\theta(i)})$ if $i\neq i_1,i_2$.

- $\phi(\mathcal{B})$ and $\phi'(\mathcal{B})$ are connected by a blue edge if there is a permutation θ of $\{1,2,\cdots,m\}$ such that $|\phi(B_i)\cap\phi'(B_{\theta(i)})|=k-2$ for all i.

It is easy to verify that G has only one red edge, joining $\sigma_0(\mathcal{B})$ and $\tau(\mathcal{B})$.

Let G' be the *blue graph* of G, i.e., G' is the graph consists of the blue edges. The structure of G' is as follows: First of all, G' contains a path $P=(\sigma_1(\mathcal{B}),\sigma_2(\mathcal{B}),\cdots,\sigma_{k-1}(\mathcal{B}))$, plus a vertex $\sigma_0(\mathcal{B})$ adjacent to every vertex of P. If $m\geq 3$, then $\tau(\mathcal{B})$ is an isolated vertex. If $m=2$, then $\tau(\mathcal{B})$ is adjacent to $\sigma_2(\mathcal{B})$. There are no other blue edges.

First we show that ψ induces a permutation of $V(G)$. Indeed, if $\phi\in Z$, then $\psi\phi H=\phi' H$ for some $\phi'\in Z$, because ψ preserves the labels. This implies that $\psi\phi=\phi' h$ for some $h\in H$. Hence

$$\psi\phi(\mathcal{B})=\phi' h(\mathcal{B}).$$

By definition of $\mathcal{B}$, we have $h(\mathcal{B})=\mathcal{B}$ for any $h\in H$. Therefore

$$\psi\phi(\mathcal{B})=\phi'(\mathcal{B})\in V(G).$$

Moreover, for any $\phi'\in Z$, there is a $\phi\in Z$ for which $\psi\phi H=\phi' H$, because ψ induces a permutation of $\{\phi H:\phi\in Z\}$. As $\psi\phi(\mathcal{B})=\phi'(\mathcal{B})$, the mapping induced by ψ from $V(G)$ to $V(G)$ is onto. So ψ induces a permutation of $V(G)$.

Furthermore, since

$$|\psi\phi(B_i)\cap\psi\phi'(B_{\theta(i)})|=|\psi(\phi(B_i)\cap\phi'(B_{\theta(i)}))|,$$

we conclude that $\psi(\phi(\mathcal{B}))$ and $\psi(\phi'(\mathcal{B}))$ are connected by a red edge (respectively, a blue edge) if and only if $\phi(\mathcal{B})$ and $\phi'(\mathcal{B})$ are connected by a red edge (respectively, a blue edge). In other words, ψ induces an automorphism of the edge colored graph G.

Since $\sigma_0(\mathcal{B})$ is the only vertex incident to a red edge and at least 2 blue edges, ψ fixes $\sigma_0(\mathcal{B})$, and hence fixes $\tau(\mathcal{B})$, which is the only red neighbour of $\sigma_0(\mathcal{B})$.

The remaining vertices form a blue path P. So ψ either fixes each vertex of P, or ψ "flips" P, i.e., $\psi(\sigma_i(\mathcal{B}))=\sigma_{k-i}(\mathcal{B})$ for $i=1,2,\cdots,k-1$.

If $m = 2$, then $\sigma_2(\mathcal{B})$ is the only vertex of P connected to $\tau(\mathcal{B})$ by a blue edge, we conclude that ψ fixes $\sigma_2(\mathcal{B})$. As $k \neq 4$, ψ fixes each vertex of P.

If $m \geq 3$, then since $|\tau(B_1) \cap \sigma_1(B_1)| = k - 1$, and $|\tau(B_j) \cap \sigma_{k-1}(B_{j'})| \leq k - 2$ for any j, j', and since ψ fixes τ, we conclude that ψ cannot interchange $\sigma_1(\mathcal{B})$ and $\sigma_{k-1}(\mathcal{B})$. Hence ψ fixes each vertex of P.

So far we have proved that ψ fixes each vertex of G, i.e., $\psi\phi(\mathcal{B}) = \phi(\mathcal{B})$ for all $\phi \in Z$. Therefore for any $\phi \in Z$,

$$j \in [i]_\phi \Leftrightarrow \psi(j) \in [\psi(i)]_\phi,$$

and for any subset T of Z, for any $i \in \{1, 2, \cdots, n\}$,

$$\psi([i]_T) = [\psi(i)]_T, \text{ and } d_T(i) = d_T(\psi(i)).$$

We shall prove that $\psi = id$. First we shall prove that $\psi(1) = 1$.

Let $T = \{\sigma_0, \tau\}$. Straightforward calculation shows that 1 and $k + 2$ are the only two elements $i \in \{1, 2, \cdots, n\}$ with $d_T(i) = 1$. Therefore

$$\psi(\{1, k + 2\}) = \{1, k + 2\}.$$

Assume to the contrary that $\psi(1) \neq 1$. Then ψ interchanges 1 and $k + 2$.

As ψ preserves the blocks of $\sigma_0(\mathcal{B})$, we conclude that ψ interchanges the two sets $\{2, 3, \cdots, k\}$ and $\{k + 1, k + 3, \cdots, 2k\}$.

Note that

$$\begin{aligned} [1]_{\sigma_1} &= \{1, 2, (m-1)k + 3, (m-1)k + 4, \cdots, mk\}, \\ [k+2]_{\sigma_1} &= \{k + 1, k + 2, 3, 4, \cdots, k\}. \end{aligned}$$

As ψ interchanges 1 and $k + 2$, and $\psi(\sigma_1(\mathcal{B})) = \sigma_1(\mathcal{B})$, we conclude that ψ interchanges $[1]_{\sigma_1}$ and $[k + 2]_{\sigma_1}$. This is possible only if $m = 2$ and ψ interchanges 2 and $k + 1$, and interchanges the sets $\{3, 4, \cdots, k\}$ and $\{k + 3, k + 4, \cdots, 2k\}$.

As $[1]_{\sigma_2} = \{1, k + 2, k + 3, 4, \cdots, k\}$ and $\psi([1]_{\sigma_2})$ is a σ_2 block, we conclude that $\psi(\{1, k + 2, k + 3, 4, \cdots, k\}) = \{1, k + 2, k + 3, 4, \cdots, k\}$. However, this is impossible, as $k \geq 5$ and ψ interchanges the sets $\{3, 4, \cdots, k\}$ and $\{k + 3, k + 4, \cdots, 2k\}$. Therefore $\psi(1) = 1$.

For $j = 1, 2, \cdots, k - 1$, let $T_j = \{\sigma_0, \sigma_j\}$. Then $\{j, j + 1\}$ is a T_j block. As 1 is fixed by ψ, and as $\psi(\{j, j + 1\})$ must be a T_j block, we can easily prove, by induction on j, that ψ fixes each of j for $j = 1, 2, \cdots, k$.

Now we shall prove by induction on s that $\psi(sk+j) = sk+j$ for $j = 1, 2, \cdots, k$. We have already proved this is true for $s = 0$. Assume $0 \leq s \leq m-2$, and $\psi(sk+j) = sk+j$ for $j = 1, 2, \cdots, k$. As

$$\{(s + 1)k + 1, (s + 1)k + 2, sk + 3, \cdots, (s + 1)k\}$$

is a σ_1 block, and ψ fixes each of $sk + 3, \cdots, (s + 1)k$, we conclude that

$$\psi(\{(s + 1)k + 1, (s + 1)k + 2\}) = \{(s + 1)k + 1, (s + 1)k + 2\}.$$

Similarly, since

$$\{sk+1, (s+1)k+2, (s+1)k+3, sk+4, \cdots, (s+1)k\}$$

is a σ_2 block, and ψ fixes $sk+1, sk+4, \cdots, (s+1)k$, we have

$$\psi(\{(s+1)k+2, (s+1)k+3\}) = \{(s+1)k+2, (s+1)k+3\}.$$

Repeated this argument, we conclude that for $j = 1, 2, \cdots, k-1$,

$$\psi(\{(s+1)k+j, (s+1)k+j+1\}) = \{(s+1)k+j, (s+1)k+j+1\}.$$

Therefore ψ fixes each of $(s+1)k+j$ for $j = 1, 2, \cdots, k$. This implies that $\psi = id$.

Case 2. $m = 2$ and $k = 4$.

In this case $n = 8$. Let

$$\begin{aligned} \sigma_0 &= id,\ \sigma_1 = (1\ 5)(2\ 6),\ \sigma_2 = (2\ 6)(3\ 7), \\ \tau_1 &= (1\ 5),\ \tau_2 = (1\ 6),\ \tau_3 = (1\ 7),\ \tau_4 = (2\ 6). \end{aligned}$$

Let $Z = \{\sigma_0, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3, \tau_4\}$. The blocks of σ_j and τ_j are as follows:

$$\begin{aligned} \sigma_0(\mathcal{B}) &= \{\{1,2,3,4\},\{5,6,7,8\}\},\ \sigma_1(\mathcal{B}) = \{\{5,6,3,4\},\{1,2,7,8\}\}, \\ \sigma_2(\mathcal{B}) &= \{\{1,6,7,4\},\{5,2,3,8\}\},\ \tau_1(\mathcal{B}) = \{\{5,2,3,4\},\{1,6,7,8\}\}, \\ \tau_2(\mathcal{B}) &= \{\{6,2,3,4\},\{5,1,7,8\}\},\ \tau_3(\mathcal{B}) = \{\{7,2,3,4\},\{5,6,1,8\}\}, \\ \tau_4(\mathcal{B}) &= \{\{1,6,3,4\},\{5,2,7,8\}\}. \end{aligned}$$

Construct a graph G whose vertex set is $V(G) = \{\phi(\mathcal{B}) : \phi \in Z\}$, and in which $\phi(\mathcal{B})$ and $\phi'(\mathcal{B})$ are connected by an edge if there is a permutation θ of $\{1,2\}$ such that $|\phi(B_i) \cap \phi'(B_{\theta(i)})| = 2$ for all i. Then G is the graph as shown in Fig. 1, where $\sigma_i(\mathcal{B})$ is denoted by v_i, and $\tau_i(\mathcal{B})$ is denoted by u_i.

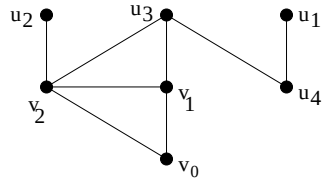

Figure 1: The graph G for Case 2

Similarly as in the proof of Case 1, ψ induces an automorphism of G. Since G is a rigid graph, we conclude that $\psi\phi(\mathcal{B}) = \phi(\mathcal{B})$ for all $\phi \in Z$. Let $T_i = \{\sigma_0, \tau_i\}$ for $i = 1, 2, 3, 4$. It is straightforward to verify that

- 1 and 5 are the only i with $d_{T_1}(i) = 1$.
- 1 and 6 are the only i with $d_{T_2}(i) = 1$.

- 1 and 7 are the only i with $d_{T_3}(i) = 1$.
- 2 and 6 are the only i with $d_{T_4}(i) = 1$.

As $d_{T_j}(i) = d_{T_j}(\psi(i))$ for any $j \in \{1, 2, 3, 4\}$ and $i \in \{1, 2, \cdots 8\}$, we conclude that ψ fixes each of $1, 2, 5, 6, 7$. Now $[8]_{\sigma_0} = \{5, 6, 7, 8\}$. As ψ fixes $5, 6, 7$, we must have $\psi(8) = 8$. As $[4]_{\sigma_2} = \{1, 6, 7, 4\}$ and ψ fixes $1, 6, 7$, we have $\psi(4) = 4$. This forces $\psi(3) = 3$, and hence $\psi = id$.

Case 3. $k = 2$.

Let $\sigma_0 = id$ and for $i = 1, 2, \cdots, m-1$, let $\sigma_i = (1\ 3\ \cdots (2i+1))$. Let $\tau_1 = (1\ 4)$ and $\tau_2 = (1\ 4\ 6)$. Let $Z = \{\sigma_i : i = 0, 1, \cdots, m-1\} \cup \{\tau_1, \tau_2\}$. The blocks of σ_j and τ_j are as follows:

$$\begin{aligned}
\sigma_0(\mathcal{B}) &= \{\{1,2\},\{3,4\},\cdots,\{2m-1,2m\}\},\\
\sigma_1(\mathcal{B}) &= \{\{3,2\},\{1,4\},\{5,6\},\cdots,\{2m-1,2m\}\},\\
\sigma_2(\mathcal{B}) &= \{\{3,2\},\{5,4\},\{1,6\},\cdots,\{2m-1,2m\}\},\\
&\cdots\cdots\\
\sigma_{m-1}(\mathcal{B}) &= \{\{3,2\},\{5,4\},\cdots,\{2m-1,2m-2\},\{1,2m\}\},\\
\tau_1(\mathcal{B}) &= \{\{4,2\},\{3,1\},\{5,6\},\cdots,\{2m-1,2m\}\},\\
\tau_2(\mathcal{B}) &= \{\{4,2\},\{3,6\},\{5,1\},\{7,8\},\cdots,\{2m-1,2m\}\}.
\end{aligned}$$

Construct a graph G whose vertex set is $V(G) = \{\phi(\mathcal{B}) : \phi \in Z\}$, and in which $\phi(\mathcal{B})$ and $\phi'(\mathcal{B})$ are connected by an edge if there is a permutation θ of $\{1, 2, \cdots, m\}$ such that there are indices i_1, i_2 such that $|\phi(B_i) \cap \phi'(B_{\theta(i)})| = 1$ if $i \in \{i_1, i_2\}$ and $\phi(B_i) = \phi'(B_{\theta(i)})$ if $i \notin \{i_1, i_2\}$. Then G is the graph as shown in Fig. 2, where $\sigma_i(\mathcal{B})$ is denoted by v_i, and $\tau_i(\mathcal{B})$ is denoted by u_i.

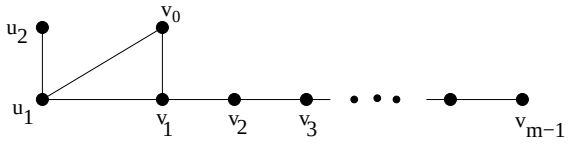

Figure 2: The graph G for Case 3

Similarly, ψ induces an automorphism of G. Since $m \geq 4$, G is a rigid graph. So $\psi\phi(\mathcal{B}) = \phi(\mathcal{B})$ for all $\phi \in Z$. For $i = 1, 2, \cdots, m-2$, let $T_i = \{\sigma_0, \sigma_i\}$. Let $X_i = \{2i+3, 2i+4, 2i+5, \cdots, 2m\}$. Then X_i consists of all the elements j with $d_{T_i}(j) = 2$. So $\psi(X_i) = X_i$ for $i = 1, 2, \cdots, m-2$. This implies that for $j = 3, 4, \cdots, m$,

$$\psi(\{2j-1, 2j\}) = \{2j-1, 2j\}. \tag{1}$$

For $i = 1, 2, \cdots, m-2$, let $R_i = \{\sigma_i, \sigma_{i+1}\}$, and let

$$Y_i = \{3, 2, 5, 4, 7, 6, \cdots, 2i+1, 2i\}.$$

Then $Y_i \cup X_{i+1}$ (where X_{m-1} is defined to be the empty set) consists of all the elements j with $d_{R_i}(j) = 2$. This implies that $\psi(Y_i) = Y_i$. Thus for $i = 1, 2, \cdots, m-2$,

$$\psi(\{2i+1, 2i\}) = \{2i+1, 2i\}. \tag{2}$$

The combination of (1) and (2) implies that $\psi(4) = 4$, $\psi(2j-1) = 2j-1, \psi(2j) = 2j$ for $j = 3, 4, \cdots, m-1$. As $\{3, 4\}$ is a σ_0 block, $\psi(4) = 4$ implies that $\psi(3) = 3$. As $\{3, 2\}$ is a σ_1 block, $\psi(3) = 3$ implies that $\psi(2) = 2$. As $\{1, 2\}$ is a σ_0 block, $\psi(2) = 2$ implies that $\psi(1) = 1$. As $\{1, 2m\}$ is a σ_{m-1} block, $\psi(1) = 1$ implies that $\psi(2m) = 2m$. As $\{2m-1, 2m\}$ is a σ_0 block, $\psi(2m) = 2m$ implies that $\psi(2m-1) = 2m-1$. Therefore $\psi = id$. □

7 Conclusions

In this section, we first prove that Theorem 5.1 and Theorem 6.1 implies that for almost all positive integers n, Conjecture 4.3 is true. We need the following result of Cameron and Teague [5] (see also [4]).

Theorem 7.1 *For almost all n, the only primitive group of degree n are S_n and A_n. More precisely, if*

$$\mathcal{E} = \{n : \text{ there exists a primitive group of degree } n, \text{ not } S_n \text{ or } A_n\},$$

and $e(x) = |\mathcal{E} \cap [1, x]|$, then

$$e(x) = 2\pi(x) + (1+\sqrt{2})x^{1/2} + O(x^{1/2}/\log x),$$

where $\pi(x)$ is the number of primes not exceeding x.

Theorem 7.2 *For almost all n, Conjecture 4.3 is true, and hence Conjecture 4.1 and Conjecture 1.3 are true.*

Proof. Let $\mathcal{E}$ be defined as in Theorem 7.1. Assume $n \notin \mathcal{E}$. It suffices to prove that for such an integer n, Conjecture 4.3 is true.

Let H be a subgroup of S_n and $H \neq A_n, S_{n-1}, A_{n-1}$. By the definition of $\mathcal{E}$, H is an intransitive or imprimitive subgroup of S_n. By Theorems 5.1 and 6.1, H is 2-distinguishing. Therefore $D_{S_n}(X) = 2$. □

Next we prove Conjecture 1.1 for $n \geq 9$. Our proof uses Bochert's Theorem (Theorem 14.2 of [20]):

Theorem 7.3 *(Bochert's Theorem) Let H be a primitive subgroup of S_n which is not S_n or A_n. Then*

$$[S_n : H] \geq \lfloor \frac{n+1}{2} \rfloor !.$$

Theorem 7.4 *Assume* $n! < \ell!\lfloor\frac{n+1}{2}\rfloor!$. *Then for any action* S_n *on* X, *either*

$$D_{S_n}(X) \in \{\lceil n^{1/k}\rceil : k \in Z^+\} \cup \{\lceil (n-1)^{1/k}\rceil : k \in Z^+\},$$

or $D_{S_n}(X) \leq \ell$. *Moreover, for any graph* G *with* $Aut(G) = S_n$, *either*

$$D(G) \in \{\lceil n^{1/k}\rceil : k \in Z^+\},$$

or $D(G) \leq \ell$.

Proof. If each orbit of S_n on X has cardinality less than $\binom{n}{2}$, then either $D_{S_n}(X) = \lceil n^{1/k}\rceil$ for some $k \geq 1$, or $D_{S_n}(X) = \lceil (n-1)^{1/k}\rceil$ for some $k \geq 1$. Assume there is an orbit O of cardinality at least $\binom{n}{2}$. Let H be the stabilizer of an element $x \in O$. If H is intransitive or imprimitive, then by Theorems 5.1 and 6.1, $D_{S_n}(X) = 2$. Assume H is primitive. By theorem 7.3, $[S_n : H] \geq \lfloor\frac{n+1}{2}\rfloor!$. So

$$|H| \leq \frac{n!}{\lfloor (n+1)/2\rfloor!}.$$

By our assumption, $|H| < \ell!$. It follows from a result of Tymoczko [19] that $D_H(O) \leq \ell - 1$. Let f be a $(\ell-1)$-distinguishing labeling of O (with respect to the action of H on O). Let $g(x) = \ell$ and let $g(y) = f(y)$ for $y \neq x$. Then if $\sigma \in S_n$ is label preserving, then $\sigma(x) = x$ and hence $\sigma \in H$. But since f is a distinguishing labeling of O with respect to the action of H on O, we conclude that $\sigma = id$. I.e., g is a distinguishing labeling of O. Therefore $D_{S_n}(X) \leq \ell$. This completes the proof of the first half of Theorem 7.4. The second half of Theorem 7.4 is proved similarly. □

Corollary 7.5 *Suppose* G *is a graph with* $Aut(G) = S_n$. *If* $n \geq 9$ *and* $D(G) \neq n$, *then* $D(G) \leq n - 2$.

Proof. If $n \geq 9$, then $n! < (n-2)!\lfloor\frac{n+1}{2}\rfloor!$. The conclusion follows from Theorem 7.4. □

Corollary 7.6 *For* $n \geq 13$, $n - 2 \notin D^*(S_n)$.

Proof. If $n \geq 13$, then $n! < (n-3)!\lfloor\frac{n+1}{2}\rfloor!$. The conclusion follows from Theorem 7.4. □

Bochert's Theorem is far from sharp when n is large. There are many improvements of Bochert's Theorem. The following result was proved by Maróti (Case (ii) of Corollary 1.1 in [16]):

Theorem 7.7 *If* H *is a primitive subgroup of* S_n *and* $H \neq S_n, A_n$, *then* $|H| < 50n^{\sqrt{n}}$.

Using Stirling formula, one can prove that if $n \geq 10$, then $50n^{\sqrt{n}} < \lceil (e\sqrt{n}) \rceil !$. Therefore we have the following corollary:

Corollary 7.8 *If G is a graph with $Aut(G) = S_n$ and $D(G) \neq n$, then $D(G) \leq \lceil e\sqrt{n} \rceil$. If S_n acts faithfully on X and $D_{S_n}(X) \neq n, n-1$, then $D_{S_n}(X) \leq \lceil e\sqrt{n} \rceil$.*

Proof. If $n \leq 9$, then $\lceil e\sqrt{n} \rceil \geq n-1$ and hence the conclusion follows. Otherwise, the conclusion follows from Theorems 7.4 and 7.7. □

It was conjectured by Albertson and Collins [1] that if G is a graph with $Aut(G) = S_n$ and $D(G) = n$, then G consists of K_n or its complement together with vertices in 1-orbits. This conjecture was confirmed by Tymoczko [19]. Indeed, Tymoczko proved that if S_n acts faithfully on X and $D_{S_n}(X) = n$, then X consists of exactly one n-orbit together with some 1-orbits. As an analogy of this result, we have the following:

Corollary 7.9 *Assume $n \geq 9$ and S_n acts faithfully on a set X. If $D_{S_n}(X) = n-1$, then X consists of exactly one n-orbit together with some (at least one) 2-orbits and some 1-orbits.*

Proof. The conclusion follows from Theorem 7.4 and Theorem 3.2. □

We remark that Corollary 7.9 is not true if n is small since there is a counterexample in Tymoczko's Theorem 3.1 (namely, $D_{S_4}(X) = 3$ but with one 6-orbit).

Although Conjecture 4.3 holds for almost all n, there are infinitely many n for which the conjecture remains open. To prove Conjecture 4.3 for these integers, one needs to consider primitive subgroups of S_n. The classification of the primitive subgroups of S_n is one of the oldest problems in group theory, and there is a rich source of literature on this topic (cf. [4]).

In the following, we show that to prove Conjecture 4.3, it suffices to consider maximal subgroups among those subgroups of S_n which is not equal to A_n.

Lemma 7.10 *Suppose H_1 is a subgroup of S_n and H_2 is a subgroup of H_1 (and hence also a subgroup of S_n). If H_1 is d-distinguishing, then H_2 is d-distinguishing.*

Proof. Suppose f is a distinguishing d-labeling of the cosets of H_1. Let f' be the d-labeling of the cosets of H_2 defined as $f'(gH_2) = f(gH_1)$. Then it is easy to verify that f' is a distinguishing labeling. □

References

[1] M. O. Albertson and K. L. Collins, *Symmetry breaking in graphs*, Electron. J. Combin. 3 (1996) #R18, 17pp.

[2] M. O. Albertson and K. L. Collins, *An introduction to symmetry breaking in graphs*, Graph Theory Notes N. Y. 30 (1996), 6–7.

[3] B. Bogstad and L. J. Cowen, *The distinguishing number of the hypercube*, Discrete Math. 283 (2004) 29–35.

[4] P. J. Cameron, *Permutation groups*, Handbook of Combinatorics, Edited by R. Graham, M. Grötschel and L. Lovász, 1995 Elsevier Science B.V., 612-645.

[5] P.J. Cameron and D.N. Teague, *On the degrees of primitive permutation groups*, Math. Z., 180(1982), 141-149.

[6] M. Chan, *The distinguishing number of the augmented cube and hypercube powers*, manuscript, August 2004.

[7] M. Chan, *The maximum distinguishing number of a group*, manuscript, September 2004.

[8] M. Chan, *The distinguishing number of the direct and wreath product action*, manuscript, Janurary, 2005.

[9] C. T. Cheng, *Three Problems in Graph Labeling*, Ph.D., The John Hopkins University, 1999.

[10] C. T. Cheng and L. J. Cowen, *On the local distinguishing numbers of cycles*, Discrete Math. 196 (1999) 97–108.

[11] K. L. Collins, *Symmetry breaking in graphs*, Talk at the DIMACS Workshop on Discrete Mathematical Chemistry, DIMACS, Rutgers University, March 23-25, 1998.

[12] S. Klavžar, T. Wong and X. Zhu, *Distinguishing labelings of group action on vector spaces and graphs*, manuscript, 2005.

[13] S. Klavžar and X. Zhu, *Cartesian powers of graphs can be distinguished with two labels*, manuscript, 2005.

[14] M. W. Liebeck, *Graphs whose full automorphism group is a symmetric group*, J. Austral. Math. Soc. Ser. A 44 (1988) 46–63.

[15] M. W. Liebeck and A. Shalev, *Maximal subgroups of symmetric groups*, J. Combin. Th. Ser. A, 75(1996), 341-352.

[16] A. Maróti, *On the orders of primitive groups*, J. Algebra, 258(2002), 631-640.

[17] F. Rubin, *Problem 729 in Journal of Recreational Mathematics*, Vol. 11 (1979), 128.

[18] A. Russell and R. Sundaram, *A note on the asymptotics and computational complexity of graph distinguishability*, Electron. J. Combin. 5 (1998) #R23, 7pp.

[19] J. Tymoczko, *Distinguishing numbers for graphs and groups*, Electron. J. Combin. 11 (2004) #R63, 13pp.

[20] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.