# Distinguishing labellings of group action on vector spaces and graphs 

Sandi Klavžar ${ }^{\text {a,1 }}$, Tsai-Lien Wong ${ }^{\text {b,c, }, * 2}$, Xuding Zhu ${ }^{\text {b,c, } 3}$<br>${ }^{\text {a }}$ Department of Mathematics and Computer Science, PeF, University of Maribor, Koroška cesta 160, 2000 Maribor, Slovenia<br>${ }^{\mathrm{b}}$ Department of Applied Mathematics, National Sun Yat-sen University, Kaohsiung, Taiwan 80424, Taiwan<br>${ }^{c}$ National Center for Theoretical Sciences, Taiwan

Received 11 April 2005
Available online 13 March 2006
Communicated by Gerhard Hiss


#### Abstract

Suppose $\Gamma$ is a group acting on a set $X$. A $k$-labeling of $X$ is a mapping $c: X \rightarrow\{1,2, \ldots, k\}$. A labeling $c$ of $X$ is distinguishing (with respect to the action of $\Gamma$ ) if for any $g \in \Gamma, g \neq \mathrm{id}_{X}$, there exists an element $x \in X$ such that $c(x) \neq c(g(x))$. The distinguishing number, $D_{\Gamma}(X)$, of the action of $\Gamma$ on $X$ is the minimum $k$ for which there is a $k$-labeling which is distinguishing. This paper studies the distinguishing number of the linear group $G L_{n}(K)$ over a field $K$ acting on the vector space $K^{n}$ and the distinguishing number of the automorphism group $\operatorname{Aut}(G)$ of a graph $G$ acting on $V(G)$. The latter is called the distinguishing number of the graph $G$ and is denoted by $D(G)$. We determine the value of $D_{G L_{n}(K)}\left(K^{n}\right)$ for all fields $K$ and integers $n$. For the distinguishing number of graphs, we study the possible value of the distinguishing number of a graph in terms of its automorphism group, its maximum degree, and other structure properties. It is proved that if $\operatorname{Aut}(G)=S_{n}$ and each orbit of $\operatorname{Aut}(G)$ has size less than $\binom{n}{2}$, then $D(G)=\left\lceil n^{1 / k}\right\rceil$ for some positive integer $k$. A Brooks type theorem for the distinguishing number is obtained: for any graph $G, D(G) \leqslant \Delta(G)$, unless $G$


[^0]is a complete graph, regular complete bipartite graph, or $C_{5}$. We introduce the notion of uniquely distinguishable graphs and study the distinguishing number of disconnected graphs. © 2006 Elsevier Inc. All rights reserved.

Keywords: Distinguishing number; Group; General linear group; Vector space; Graph; Graph automorphism; Distinguishing set

## 1. Introduction

Let $\Gamma$ be a group acting on a set $X$. For a positive integer $k$, a $k$-labeling of $X$ is a mapping $c: X \rightarrow\{1,2, \ldots, k\}$. We say $c$ is a distinguishing labeling (with respect to the action of $\Gamma$ ) if for any $g \in \Gamma$, if $g$ is not the identity, then there is an element $x \in X$ such that $c(x) \neq c(g(x))$. The distinguishing number $D_{\Gamma}(X)$ of the action of $\Gamma$ on $X$ is the minimum number $k$ for which there is a $k$-labeling $c$ which is a distinguishing labeling.

The distinguishing number was first defined by Albertson and Collins [1] for graphs. Let $G$ be a graph and $\ell$ a vertex labeling of $G$. We say $(G, \ell)$ is a labeled graph. By an automorphism of $(G, \ell)$ we mean an automorphism $\varphi$ of $G$ that in addition preserves vertex labels, i.e., $\ell(\varphi(v))=\ell(v)$ for every vertex $v$. A distinguishing labeling of $G$ is a labeling $\ell$ of $G$ such that $(G, \ell)$ has only the trivial automorphism. In other words, for a graph $G$, the distinguishing number of $G$ is the distinguishing number of the action of the automorphism group $\operatorname{Aut}(G)$ on $V(G)$, i.e., $D(G)=D_{\operatorname{Aut}(G)}(V(G))$. In the seminal paper [1] it was proved, among others, that if $\operatorname{Aut}(G)=S_{4}$, then $D(G)=2$ or 4, and for each group $\Gamma$ there exists a graph $G$ such that $\operatorname{Aut}(G) \cong \Gamma$ and $D(G)=2$. In addition, $D(G) \leqslant 2$ whenever $\operatorname{Aut}(G)$ is abelian, and $D(G) \leqslant 3$ whenever $\operatorname{Aut}(G)$ is dihedral. Bogstad and Cowen [3] determined the distinguishing number of hypercubes and their squares. For hypercubes they proved $D\left(Q_{2}\right)=D\left(Q_{3}\right)=3$ and $D\left(Q_{d}\right)=2$ for $d \geqslant 4$. Their work on hypercubes powers was completed in [4] where it is proved that $D\left(Q_{n}^{p}\right)=2$ for each $n \geqslant 4$ and $2<p<n-1$. (Here $Q_{n}^{p}$ denotes the graph that is obtained from $Q_{n}$ by making adjacent any pair of vertices at distance at most $p$.) For the computational complexity of the $d$-distinguishability problem see [11].

Tymoczko [12] generalized the notion of the distinguishing number to group actions on sets. It was proved in [12] that if a general group $\Gamma$ acts on itself by translation, or the symmetric group $S_{n}$ acts on itself by conjugation, then the distinguishing number is 2 . An example was given in [12] to show that there is a faithful $S_{4}$-action with distinguishing number 3, in contrast to the fact that there is no graph $G$ with $\operatorname{Aut}(G)=S_{4}$ and with $D(G)=3$. This shows that not all faithful group actions are realized as actions of the automorphism groups of a graph on its vertex set. In [6], Chan studied the distinguishing number of the wreath product of two groups on the Cartesian product of their sets, the distinguishing number of the direct product of two groups on the direct product of their sets. In [5], Chan proved that if $\Gamma$ is nilpotent of class $c$ or supersolvable of length $c$, then $\Gamma$ acts with distinguishing number at most $c+1$. In particular, if $\Gamma$ is an abelian group then $\Gamma$ acts with distinguishing number at most 2 , if $\Gamma$ is a dihedral group, then $\Gamma$ acts with distinguishing number at most 3 . It was also proved in [5] that the distinguishing number of the action of the linear group $G L_{n}(K)$ over a field $K$ on the vector space $K^{n}$ is equal to 2 if $K$ is infinite or $|K|>n+1$.

In this paper, we answer a question of Chan, by determining the distinguishing number of the linear group $G L_{n}(K)$ over a field $K$ on the vector space $K^{n}$ for all fields $K$ and for all integers $n$. Then we study the distinguishing number of graphs. We determine the distinguishing number of graphs $G$ with $\operatorname{Aut}(G)=S_{n}$ and for which each orbit of $\operatorname{Aut}(G)$ has size less than $\binom{n}{2}$. We prove a Brooks type theorem for the distinguishing number of graphs. Namely, for a connected graph $G$ its distinguishing number is bounded by the largest degree, unless $G$ is either $K_{n}, n \geqslant 1, K_{n, n}, n \geqslant 1$, or $C_{5}$. We also introduce the notion of uniquely distinguishable graphs, and use the concept to the study of the distinguishing number of disjoint unions of connected graphs.

## 2. The distinguishing number of the linear group $G L_{n}(K)$

In this and the next section, we discuss the distinguishing number of the action of the linear group $G L_{n}(K)$ over a field $K$ on the vector space $K^{n}$. Here $G L_{n}(K)$ is the group of $n \times n$ invertible matrices over a field $K$, and the action of $G L_{n}(K)$ on $K^{n}$ is through the left multiplication defined as $v \rightarrow A v$ for $A \in G L_{n}(K)$ and $v \in K^{n}$.

This problem was first studied by Chan [5]. It was proved in [5] that if $K$ is infinite or $K$ is finite but $|K|>n+1$, then $D_{G L_{n}(K)}\left(K^{n}\right)=2$. Then Chan posed the following problem:

Problem 2.1. Compute $D_{G L_{n}(K)}\left(K^{n}\right)$ for $n \geqslant 3$ and $|K| \leqslant n+1$.
We solve this problem and determine the value of $D_{G L_{n}(K)}\left(K^{n}\right)$ for all $n$ and all $K$. This section is devoted to the case that $|K| \geqslant 3$. The case $|K|=2$ is left to the next section. In the following, we assume that $K$ is finite, and $\alpha$ is a generator of the multiplicative group $K^{\times}$, and the order of $\alpha$ is $o(\alpha)=k=|K|-1$. We shall denote by $e_{1}, e_{2}, \ldots, e_{n}$ a basis of $K^{n}$.

## Theorem 2.2. Suppose $K$ is a finite field.

(1) If $|K| \geqslant 3$ and $n \geqslant 3$, then $D_{G L_{n}(K)}\left(K^{n}\right)=2$.
(2) If $|K| \geqslant 4$, then $D_{G L_{n}(K)}\left(K^{n}\right)=2$.
(3) If $|K|=3$ and $n=2$, then $D_{G L_{n}(K)}\left(K^{n}\right)=3$.

Proof. The case $|K|=3$ and $n=2$ was settled in [5]. We only need to prove (1) and (2). It is obvious that $D_{G L_{n}(K)}\left(K^{n}\right) \geqslant 2$ provided that $n \geqslant 2$ or $|K| \geqslant 3$. Thus we only need to exhibit a distinguishing 2-labeling when $|K| \geqslant 4$ or $|K|=3$ and $n \geqslant 3$.

Assume $|K| \geqslant 3$ and $n \geqslant 3$. Then $k \geqslant 2$. Let

$$
\begin{aligned}
X_{1}= & \left\{e_{1}\right\} \cup\left\{\alpha^{i} e_{j}: i=0,1, \ldots, k-1, j=2,3, \ldots, n\right\} \\
& \cup\left\{\alpha e_{i}+e_{i+1}: i=1,2, \ldots, n-1\right\} \\
& \cup\left\{-\alpha e_{1}-(\alpha+1)\left(e_{2}+e_{3}+\cdots+e_{n-1}\right)-e_{n}\right\}, \\
X_{2}= & K^{n} \backslash X_{1} .
\end{aligned}
$$

Let $c$ be the 2-labeling which labels the elements of $X_{i}$ by label $i$ for $i=1,2$. We shall prove that $c$ is a distinguishing labeling. Let $\phi \in G L_{n}(K)$ be an invertible linear transformation of $K^{n}$ which preserves the labels. We shall prove that for each $i \in\{1,2, \ldots, n\}$, $\phi\left(e_{i}\right)=e_{i}$. This implies that $\phi=\mathrm{id}_{K^{n}}$.

First of all, since $e_{1}=\sum_{x \in X_{1}} x$ and $\phi\left(X_{1}\right)=X_{1}$, we have

$$
\phi\left(e_{1}\right)=\phi\left(\sum_{x \in X_{1}} x\right)=\sum_{x \in X_{1}} \phi(x)=\sum_{x \in X_{1}} x=e_{1} .
$$

Assume that $2 \leqslant i \leqslant n$ and each of $e_{1}, e_{2}, \ldots, e_{i-1}$ is fixed by $\phi$. This implies that $\phi$ fixes each of the elements in the set $X^{\prime}=\left\{e_{1}\right\} \cup\left\{\alpha^{s} e_{j}: s=0,1, \ldots, k-1, j=2,3, \ldots\right.$, $i-1\} \cup\left\{\alpha e_{j}+e_{j+1}: j=1,2, \ldots, i-2\right\}$.

We shall prove that $e_{i}$ is also fixed by $\phi$. As $\alpha e_{i-1}+e_{i} \in X_{1} \backslash X^{\prime}$, we have $\phi\left(\alpha e_{i-1}+\right.$ $\left.e_{i}\right)=\alpha e_{i-1}+\phi\left(e_{i}\right) \in X_{1} \backslash X^{\prime}$. On the other hand, $e_{i}, \alpha e_{i} \in X_{1} \backslash X^{\prime}$ implies that $\phi\left(e_{i}\right) \in$ $X_{1} \backslash X^{\prime}$, and $\phi\left(\alpha e_{i}\right)=\alpha \phi\left(e_{i}\right) \in X_{1} \backslash X^{\prime}$. This implies that $\phi\left(e_{i}\right)=\alpha^{j} e_{t}$ for some $j \in$ $\{0,1, \ldots, k-1\}$ and $t \in\{i, i+1, \ldots, n\}$, for otherwise, we would have $\phi\left(e_{i}\right)=-\alpha e_{1}-$ $(\alpha+1)\left(e_{2}+e_{3}+\cdots+e_{n-1}\right)-e_{n}$, but then, because $k \geqslant 2$,

$$
\alpha \phi\left(e_{i}\right)=\alpha\left(-\alpha e_{1}-(\alpha+1)\left(e_{2}+e_{3}+\cdots+e_{n-1}\right)-e_{n}\right) \notin X_{1},
$$

which is a contradiction.
Thus $\phi\left(\alpha e_{i-1}+e_{i}\right)=\alpha e_{i-1}+\alpha^{j} e_{t}$. If $i \geqslant 3$, then since $\alpha e_{i-1}+\alpha^{j} e_{t} \in X_{1}$ and $t \geqslant i$ we must have $t=i$ and $j=0$. If $i=2$, then it is also easy to see that either $\phi\left(e_{2}\right)=e_{2}$, or $\alpha e_{i-1}+\alpha^{j} e_{t}=-\alpha e_{1}-(\alpha+1)\left(e_{2}+e_{3}+\cdots+e_{n-1}\right)-e_{n}$. However, $\alpha e_{i-1}+\alpha^{j} e_{t}=$ $-\alpha e_{1}-(\alpha+1)\left(e_{2}+e_{3}+\cdots+e_{n-1}\right)-e_{n}$ implies that $\alpha=-\alpha$ which means that $K$ has characteristic 2 , and $\alpha+1=0$ (since $n \geqslant 3$ ), which means that $\alpha=1$ and hence $|K|=2$, a contradiction.

It remains to prove that if $|K| \geqslant 4$ and $n=2$, then $D_{G L_{n}(K)}\left(K^{n}\right)=2$. Let $e_{1}, e_{2}$ be a basis of $K^{2}$. Let

$$
\begin{aligned}
& X_{1}=\left\{\alpha^{i} e_{2}: i=1,2, \ldots, k-1\right\} \cup\left\{e_{1}+e_{2}\right\} \\
& X_{2}=K^{2} \backslash X_{1}
\end{aligned}
$$

Let $c$ be the 2-labeling which labels the elements of $X_{i}$ by label $i$ for $i=1,2$. Let $\phi$ be a label preserving invertible linear transformation of $K^{2}$. As $\sum_{x \in X_{1}} x=e_{1}$ and $\phi\left(X_{1}\right)=X_{1}$, we conclude that $\phi\left(e_{1}\right)=e_{1}$.

Since $\alpha^{j}\left(e_{1}+e_{2}\right) \notin X_{1}$ for $j=1,2$, we infer that $\alpha^{j} \phi\left(e_{1}+e_{2}\right) \notin X_{1}$ for $j=1,2$. Moreover, $e_{1}+e_{2}$ is the only element of $X_{1}$ for which $\alpha\left(e_{1}+e_{2}\right) \notin X_{1}$ and $\alpha^{2}\left(e_{1}+e_{2}\right) \notin X_{1}$, therefore $\phi\left(e_{1}+e_{2}\right)=e_{1}+e_{2}$. Here we used the condition that $k=|K|-1 \geqslant 3$. We conclude that $\phi\left(e_{2}\right)=e_{2}$ and so $\phi$ is the identify.

## 3. The case $|K|=2$

This section discusses the case $|K|=2$. The exact value of $D_{G L_{n}(K)}\left(K^{n}\right)$ is determined for all $n \geqslant 2$.

Theorem 3.1. Suppose $K$ is the field $G F(2)$, i.e., $|K|=2$. Then

$$
D_{G L_{n}(K)}\left(K^{n}\right)= \begin{cases}2, & \text { if } n \geqslant 5 \\ 3, & \text { if } n=2,4 \\ 4, & \text { if } n=3\end{cases}
$$

The case $n=2$ is solved in [5], so we need to prove the cases $n \geqslant 3$. The proof of Theorem 3.1 is a little bit complicated, hence we divide it into four lemmas according to the value of $n$.

Lemma 3.2. Suppose $K$ is the field $G F(2)$. If $n \geqslant 6$, then $D_{G L_{n}(K)}\left(K^{n}\right)=2$.
Proof. Assume $n \geqslant 6$. Let $X_{1}=\left\{e_{1}, e_{2}, \ldots, e_{n}, e_{1}+e_{2}, e_{1}+e_{2}+e_{3}, \ldots, e_{1}+e_{2}+\cdots+\right.$ $\left.e_{n}, u, v\right\}$, where $u, v$ are defined as follows:

If $n$ is even then

$$
u=e_{2}+e_{3}+e_{n}, \quad v=e_{1}+e_{2}+\left(e_{5}+e_{7}+e_{9}+\cdots+e_{n-1}\right)+e_{n}
$$

If $n$ is odd, then

$$
u=e_{1}+e_{4}+e_{n}, \quad v=e_{1}+e_{2}+\left(e_{6}+e_{8}+e_{10}+\cdots+e_{n-1}\right)+e_{n}
$$

Observe that if $n$ is even, then $u+v=e_{1}+e_{3}+e_{5}+\cdots+e_{n-1}$. If $n$ is odd, then $u+v=e_{2}+e_{4}+e_{6}+\cdots+e_{n-1}$.

Let $X_{2}=K^{n} \backslash X_{1}$ and let $c$ be the 2-labeling which labels the elements of $X_{i}$ by label $i$ for $i=1,2$. We shall prove that $c$ is a distinguishing labeling. Let $\phi \in G L_{n}(K)$ be a linear transformation of $K^{n}$ which preserves the labels. We shall prove that $\phi\left(e_{i}\right)=e_{i}$ for $i=1,2, \ldots, n$, which implies that $\phi$ is the identity. It is easy to verify that $\sum_{x \in X_{1}} x=e_{1}$. Since $\phi$ is invertible and preserves the labels (that is, $\phi\left(X_{1}\right)=X_{1}$ ), we have

$$
\phi\left(e_{1}\right)=\phi\left(\sum_{x \in X_{1}} x\right)=\sum_{x \in X_{1}} \phi(x)=\sum_{x \in X_{1}} x=e_{1} .
$$

Assume that $i \geqslant 2$ and $\phi\left(e_{j}\right)=e_{j}$ for $j=1,2, \ldots, i-1$. We shall prove that $\phi\left(e_{i}\right)=e_{i}$. Let

$$
\begin{aligned}
& x=\phi\left(e_{i}\right) \\
& y=\phi\left(e_{1}+e_{2}+\cdots+e_{i}\right)=e_{1}+e_{2}+\cdots+e_{i-1}+\phi\left(e_{i}\right)
\end{aligned}
$$

As $e_{i}, e_{1}+e_{2}+\cdots+e_{i} \in X_{1}$, we have $x, y \in X_{1}$. Moreover, $x+y=e_{1}+e_{2}+\cdots+e_{i-1}$. It is straightforward to verify that (using the fact that $n \geqslant 6$ ), $e_{i}$ and $e_{1}+e_{2}+\cdots+e_{i}$ are the only two elements of $X_{1}$ whose sum is equal to $e_{1}+e_{2}+\cdots+e_{i-1}$. Therefore $\{x, y\}=\left\{e_{i}, e_{1}+e_{2}+\cdots+e_{i}\right\}$. It remains to show that $x \neq e_{1}+e_{2}+\cdots+e_{i}$. Assume to the contrary that $x=e_{1}+e_{2}+\cdots+e_{i}$. We consider two cases.

Case 1. $i \leqslant n-1$.
Let

$$
\begin{aligned}
w & =\phi\left(e_{i+1}\right) \\
z & =\phi\left(e_{1}+e_{2}+\cdots+e_{i+1}\right)=e_{1}+e_{2}+\cdots+e_{i-1}+\phi\left(e_{i}\right)+\phi\left(e_{i+1}\right)=e_{i}+w
\end{aligned}
$$

Then $w, z \in X_{1}$ and $w+z=e_{i}$. Again it is easy to verify that $e_{1}+e_{2}+\cdots+e_{i}$ and $e_{1}+e_{2}+\cdots+e_{i-1}$ are the only two elements of $X_{1}$ whose sum is $e_{i}$. This implies that $\{w, z\}=\left\{e_{1}+e_{2}+\cdots+e_{i}, e_{1}+e_{2}+\cdots+e_{i-1}\right\}$. But $e_{1}+e_{2}+\cdots+e_{i-1}=\phi\left(e_{1}+e_{2}+\right.$ $\left.\cdots+e_{i-1}\right)$, in contrary to the fact that $\phi$ is one-to-one. Therefore $x=e_{i}$, i.e., $\phi\left(e_{i}\right)=e_{i}$.

Case 2. $i=n$.
If $n$ is even, then

$$
\begin{aligned}
\phi(u) & =\phi\left(e_{2}+e_{3}+e_{n}\right) \\
& =e_{2}+e_{3}+e_{1}+e_{2}+\cdots+e_{n} \\
& =e_{1}+e_{4}+e_{5}+\cdots+e_{n} \notin X_{1},
\end{aligned}
$$

which is a contradiction. If $n$ is odd, then

$$
\begin{aligned}
\phi(u) & =\phi\left(e_{1}+e_{4}+e_{n}\right) \\
& =e_{1}+e_{4}+e_{1}+e_{2}+\cdots+e_{n} \\
& =e_{2}+e_{3}+e_{5}+e_{6}+\cdots+e_{n} \notin X_{1},
\end{aligned}
$$

which is again a contradiction.
Lemma 3.3. Suppose $K$ is the field $G F(2)$. If $n=5$, then $D_{G L_{n}(K)}\left(K^{n}\right)=2$.
Proof. Let $X_{1}=\left\{e_{1}, e_{2}, e_{3}, e_{4}, e_{5}, e_{1}+e_{2}, e_{1}+e_{3}, e_{1}+e_{4}, e_{1}+e_{5}, e_{2}+e_{3}, e_{2}+e_{4}, e_{2}+\right.$ $\left.e_{3}+e_{5}, e_{2}+e_{3}+e_{4}+e_{5}\right\}$. Let $X_{2}=K^{n} \backslash X_{1}$. Let $c$ be the 2-labeling which labels the elements of $X_{i}$ by label $i$ for $i=1,2$. We shall prove that $c$ is a distinguishing labeling. Let $\phi \in G L_{n}(K)$ be a linear transformation of $K^{n}$ which preserves the labels.

For $i=1,2,3,4$, let $Y_{i} \subseteq X_{1}$ be the subset of $X_{1}$ consisting of all the elements $u$ of $X_{1}$ such that there exist exactly $i$ 2-element sets $\{x, y\}$ with $x, y \in X_{1}$ and $u=x+y$. Then a straightforward but tedious calculation shows that

$$
\begin{aligned}
& Y_{1}=\left\{e_{1}+e_{5}, e_{2}+e_{3}+e_{4}+e_{5}\right\} \\
& Y_{2}=\left\{e_{3}, e_{5}, e_{1}+e_{3}, e_{1}+e_{4}, e_{2}+e_{4}, e_{2}+e_{3}+e_{5}\right\} \\
& Y_{3}=\left\{e_{2}, e_{4}, e_{1}+e_{2}, e_{2}+e_{3}\right\}, \\
& Y_{4}=\left\{e_{1}\right\} .
\end{aligned}
$$

For example, we have $e_{1} \in Y_{4}$, because $e_{1} \in X_{1}$ and

$$
e_{1}=e_{2}+\left(e_{1}+e_{2}\right)=e_{3}+\left(e_{1}+e_{3}\right)=e_{4}+\left(e_{1}+e_{4}\right)=e_{5}+\left(e_{1}+e_{5}\right)
$$

where $e_{2}, e_{1}+e_{2}, e_{3}, e_{1}+e_{3}, e_{4}, e_{1}+e_{4}, e_{5}, e_{1}+e_{5} \in X_{1}$. Moreover, there is no other two elements $x, y \in X_{1}$ with $x+y=e_{1}$.

If $x, y, u \in X_{1}$ and $x+y=u$, then we have $\phi(x), \phi(y), \phi(u) \in X_{1}$ and $\phi(x)+\phi(y)=$ $\phi(u)$. Therefore $\phi\left(Y_{i}\right)=Y_{i}$ for $i=1,2,3,4$. This implies that $\phi\left(\sum_{x \in Y_{i}} x\right)=\sum_{x \in Y_{i}} x$, for $i=1,2,3,4$. As $\sum_{x \in Y_{1}} x=e_{1}+e_{2}+e_{3}+e_{4}, \sum_{x \in Y_{2}} x=e_{3}, \sum_{x \in Y_{3}} x=e_{1}+e_{2}+e_{3}+e_{4}$ and $\sum_{x \in Y_{4}} x=e_{1}$, we conclude that $\phi$ fixes each of $e_{1}, e_{3}, e_{2}+e_{4}$. Now $e_{5}$ is the only element of $Y_{2}$ which is the sum of an element of $Y_{1}$ and an element of $Y_{4}$, and $e_{4}$ is the only element of $Y_{3}$ which is the sum of an element of $Y_{1}$ and an element of $Y_{2}$. So $\phi$ fixes each of $e_{5}$ and $e_{4}$. Therefore $\phi$ is the identity.

Lemma 3.4. Suppose $K$ is the field $G F(2)$. If $n=3$, then $D_{G L_{n}(K)}\left(K^{n}\right)=4$.
Proof. Assume $n=3$. Label $e_{i}$ by label $i$ for $i=1,2,3$, and label the remaining elements by label 4 , the result is certainly a distinguishing labeling. So $D_{G L_{3}(K)}\left(K^{3}\right) \leqslant 4$. It remains to show that for any 3-labeling $c$ of $K^{3}$, there is an invertible linear transformation which is not the identity and which preserves the labels. Note that to define an invertible linear transformation $\phi$, it suffices to define the value of $\phi(u), \phi(v), \phi(w)$ for any three linearly independent vectors $u, v, w$ so that $\phi(u), \phi(v), \phi(w)$ are also linearly independent. There are 7 nonzero elements in $K^{3}$. Let $X_{i}=c^{-1}(i) \backslash\{0\}$. Assume that $t_{i}=\left|X_{i}\right|$ and $t_{1} \leqslant t_{2} \leqslant t_{3}$. We divide the discussion into a few cases.

Case 1. $\left(t_{1}, t_{2}, t_{3}\right)=(1,1,5)$.
Assume $X_{1}=\{u\}, X_{2}=\{v\}$. Let $w, w^{\prime} \in X_{3}, w \neq w^{\prime}$ and $w, w^{\prime} \neq u+v$. Then $\phi(u)=u, \phi(v)=v$ and $\phi(w)=w^{\prime}$ defines a linear transformation which preserves the labels.

Case 2. $\left(t_{1}, t_{2}, t_{3}\right)=(1,2,4)$.
Assume that $X_{1}=\{u\}$, and $v \in X_{2}$. The other element of $X_{2}$ is either equal to $u+v$, or is independent of $u, v$. In either case, the mapping which fixes $u$ and interchanges the two elements of $X_{2}$ defines (or can be extended to) a linear transformation which preserves the labels.

Case 3. $\left(t_{1}, t_{2}, t_{3}\right)=(1,3,3)$.
Assume $X_{1}=\{u\}$. If $\sum_{x \in X_{2}} x=0$, then $\sum_{x \in X_{3}}=u$. It follows that $X_{2}=\{v, w, v+w\}$ and $X_{3}=\{u+v, u+w, u+v+w\}$. Let $\phi(u)=u, \phi(v)=w, \phi(w)=v$. Then $\phi$ preserves the labels. The case $\sum_{x \in X_{3}}=0$ is symmetric. Assume $\sum_{x \in X_{2}} x=v \neq 0$ and $\sum_{x \in X_{3}} x=$
$u+v \neq 0$. Then $X_{2}=\{u+v, w+v, w+u+v\}$ and $X_{3}=\{v, w, u+w\}$, where $u, v, w$ are independent. Let $\phi(u)=u, \phi(v)=v, \phi(w)=u+w$. Then $\phi$ preserves the labels.

Case 4. $\left(t_{1}, t_{2}, t_{3}\right)=(2,2,3)$.
Assume first that $\sum_{x \in X_{3}} x=0$. Then $X_{3}=\{u, v, u+v\}$. Without loss of generality, we may assume that $X_{2}=\{w, w+u\}$, where $w, u, v$ are linearly independent. Then $X_{1}=$ $\{w+u+v, w+v\}$. Let $\phi(u)=u, \phi(w)=w, \phi(v)=u+v$. Then $\phi$ preserves the labels.

Assume $\sum_{x \in X_{3}} x=v \neq 0$. Then $X_{3}=\{v+u, v+w, v+u+w\}$, where $u, v, w$ are linearly independent. Without loss of generality, we may assume that $X_{2}=\{v, u\}$ and $X_{1}=\{w, u+w\}$. Let $\phi(v)=v, \phi(u)=u, \phi(w)=u+w$. Then $\phi$ preserves the labels.

Lemma 3.5. Suppose $K$ is the field $G F(2)$. If $n=4$, then $D_{G L_{n}(K)}\left(K^{n}\right)=3$.
Proof. First we prove that $D_{G L_{n}(K)}\left(K^{n}\right) \leqslant 3$. Let $X_{1}=\left\{e_{2}, e_{3}, e_{4}, e_{1}+e_{2}+e_{3}+e_{4}\right\}$, $X_{2}=\left\{e_{1}, e_{1}+e_{2}, e_{2}+e_{3}, e_{3}+e_{4}\right\}$, and $X_{3}=K^{n} \backslash\left(X_{1} \cup X_{2}\right)$. Let $c$ be the 3-labeling which labels the elements of $X_{i}$ by label $i$ for $i=1,2,3$. It suffices to prove that $c$ is a distinguishing labeling. Let $\phi \in G L_{n}(K)$ be a linear transformation of $K^{n}$ which preserves the labels. Similarly as before, we have $\phi\left(e_{1}\right)=e_{1}$, because $\sum_{x \in X_{1}} x=e_{1}$. Assume $i \geqslant 2$ and we have proved that $\phi\left(e_{j}\right)=e_{j}$ for $j \leqslant i-1$. Then

$$
\phi\left(e_{i}\right)=\phi\left(e_{i-1}+e_{i-1}+e_{i}\right)=e_{i-1}+\phi\left(e_{i-1}+e_{i}\right)
$$

Note that $\phi\left(e_{i-1}+e_{i}\right) \in X_{2}$. As $\phi\left(e_{1}\right)=e_{1}$, so $\phi\left(e_{i-1}+e_{i}\right) \neq e_{1}$. Hence $\phi\left(e_{i-1}+e_{i}\right)=$ $e_{s}+e_{s+1}$ for some $s \in\{1,2,3\}$. On the other hand, $\phi\left(e_{i}\right) \in X_{1}$. So

$$
\phi\left(e_{i}\right)=e_{i-1}+e_{s}+e_{s+1} \in X_{1}
$$

By comparing to each element of $X_{1}$, we conclude that $s=i-2$ or $i-1$. If $s=i-2$, then $\phi\left(e_{i}\right)=e_{i-2}$, in contrary to the fact that $\phi\left(e_{i-2}\right)=e_{i-2}$. Therefore $s=i-1$ and $\phi\left(e_{i}\right)=e_{i}$. Thus $\phi$ is the identity.

It remains to prove that $D_{G L_{n}(K)}\left(K^{n}\right) \neq 2$. Let $c$ be an arbitrary 2-labeling of $K^{n}$. Let $X_{i}=c^{-1}(i) \backslash\{0\}$ for $i=1,2$. As $\left|K^{4}\right|=16$, we may assume that $\left|X_{1}\right| \leqslant 7$. Furthermore, we assume that either $\sum_{x \in X_{1}} x=0$ or $\sum_{x \in X_{1}} x=e_{4}$ (because if $\sum_{x \in X_{1}} x=u \neq 0$, then $u$ can be extended into a basis of $K^{4}$ ). We shall construct a linear transformation $\phi \in G L_{4}(K)$ which is not identity and which preserves the labeling $c$.

We denote by $Q$ the subspace of $K^{4}$ generated by $\left\{e_{1}, e_{2}, e_{3}\right\}$. Let $Y_{1}=Q \cap X_{1}$ and let $Y_{2}=\left\{u \in Q: u+e_{4} \in X_{1}\right\}$. By our assumption, $\sum_{x \in X_{1}} x=0$ or $e_{4}$. This implies that $\sum_{x \in Y_{1}} x+\sum_{x \in Y_{2}} x=0$.

Claim 3.6. For any subsets $Y_{1}, Y_{2}$ of $Q \backslash\{0\}$ such that $\sum_{x \in Y_{1}} x+\sum_{x \in Y_{2}} x=0$, there is a linear transformation $\phi$ of $Q$ which is not identity, and $\phi\left(Y_{i}\right)=Y_{i}$ for $i=1,2$.

Proof. By symmetry, we may assume that $\left|Y_{1}\right| \leqslant\left|Y_{2}\right|$.
If $Y_{1} \cap Y_{2}=\emptyset$ or $Y_{1} \subseteq Y_{2}$, then $Y_{1}, Y_{2} \backslash Y_{1}, Q \backslash\left(Y_{1} \cup Y_{2}\right)$ induces a 3-labeling of $Q$. By Lemma 3.4, the required linear transformation $\phi$ exists.

Thus we assume that $D=Y_{1} \cap Y_{2} \neq \emptyset, Y_{i}^{\prime}=Y_{i} \backslash D \neq \emptyset$ for $i=1$, 2. Our task is to construct a linear transformation $\phi$ of $Q$ such that $\phi(D)=D, \phi\left(Y_{i}^{\prime}\right)=Y_{i}^{\prime}$ for $i=1,2$.

Note that $2|D|+\left|Y_{1}^{\prime}\right|+\left|Y_{2}^{\prime}\right|=\left|X_{1}\right| \leqslant 7$. As each element of $D$ occurs twice in the summation $\sum_{x \in Y_{1}} x+\sum_{x \in Y_{2}} x$, the assumption $\sum_{x \in Y_{1}} x+\sum_{x \in Y_{2}} x=0$ implies that $\sum_{x \in Y_{1}^{\prime} \cup Y_{2}^{\prime}} x=0$. This implies that $\left|Y_{1}^{\prime}\right|+\left|Y_{2}^{\prime}\right|=3$ or 4 .

Case 1. $|D|=1$, say $D=\{u\}$.
If $\left|Y_{1}^{\prime}\right|=1$, say $Y_{1}^{\prime}=\{v\}$, then $\left|Y_{2}^{\prime}\right|=2$ or 3. Assume $\left|Y_{2}^{\prime}\right|=2$. Then $Y_{2}^{\prime}=\{v+w, w\}$ for some $w$ such that $u, v, w$ are linearly independent. Then the mapping $\phi$ which fixes $u, v$ and interchanges the two elements of $Y_{2}^{\prime}$ is the required linear transformation. If $\left|Y_{2}^{\prime}\right|=3$, then $Y_{2}^{\prime}=\{v+u, w+v, w+u+v\}$, where $u, v, w$ are linearly independent. Then the mapping $\phi$ which fixes $u, v$ and $\phi(w)=w+u$ is the required linear transformation.

If $\left|Y_{1}^{\prime}\right|=2$, then $\left|Y_{2}^{\prime}\right|=2$. If $Y_{1}^{\prime}=\{w, v\}$, where $u, v, w$ are independent, then $Y_{2}^{\prime}=$ $\{u+v, u+w\}$. In this case, the mapping $\phi$ which fixes $u$ and interchanges $v$ and $w$ is the required linear transformation. If $Y_{1}^{\prime}=\{v, v+u\}$, then $Y_{2}^{\prime}=\{w, w+u\}$. In this case, the mapping $\phi$ which fixes $u$ and $v$ and interchanges $w+u$ and $w$ is the required linear transformation.

Case 2. $|D|=2$, say $D=\{u, v\}$.
Then $\left|Y_{1}^{\prime}\right|=1$ and $\left|Y_{2}^{\prime}\right|=2$. Thus either $Y_{1}^{\prime}=\{w\}$, where $u, v, w$ are independent, or $Y_{1}^{\prime}=\{u+v\}$. In any case, the mapping $\phi$ which interchanges $u$ and $v$ and fixes $w$ (where $u, v, w$ are independent) is the required linear transformation. This completes the proof of Claim 3.6.

Now we extend $\phi$ constructed in the proof of Claim 3.6 to a linear transformation of $K^{4}$ by letting $\phi\left(e_{4}\right)=e_{4}$. It is easy to verify that such an extension of $\phi$ preserves the labeling $c$.

## 4. Graphs with a symmetric group as their automorphism group

Given a group $\Gamma$, a graph $G$ is said to realize $\Gamma$ if $\operatorname{Aut}(G)=\Gamma$. Albertson and Collins [8] defined the distinguishing set of $\Gamma$ as

$$
D(\Gamma)=\{D(G): G \text { realizes } \Gamma\}
$$

In [1], it was proved that $D\left(S_{4}\right)=\{2,4\}$ and conjectured that $n-1 \notin D\left(S_{n}\right)$. In this section, we prove that if $G$ realizes $S_{n}$ and each orbit of $\operatorname{Aut}(G)$ has size less than $\binom{n}{2}$ then $D(G)=$ $\left\lceil n^{1 / k}\right\rceil$ for some positive integer $k$. Moreover, for each $k \geqslant 1$, there is a graph $G$ which realizes $S_{n}$, with each orbit of size less than $\binom{n}{2}$ and with $D(G)=\left\lceil n^{1 / k}\right\rceil$.

First we need a lemma proved by Liebeck [10] concerning the structure of graphs $G$ with $\operatorname{Aut}(G)=S_{n}$.

Lemma 4.1. [10] Let $G=(V, E)$ be a graph which realizes $S_{n}$, where $n>6$. If each orbit of $\operatorname{Aut}(G)$ on $V(G)$ has size less than $\binom{n}{2}$, then all the orbits have size 1 or $n$.

In the following, we denote the set $\{1,2, \ldots, n\}$ by $I$. Each automorphism $\tau$ of $G$ is also viewed as a permutation of $I$. So $\tau$ is viewed to act on the set $V(G) \cup I$.

Theorem 4.2. Let $G=(V, E)$ be a graph which realizes $S_{n}$ and $n>6$. If each orbit of $\operatorname{Aut}(G)$ on $V(G)$ has size less than $\binom{n}{2}$, then $D(G)=\left\lceil n^{1 / k}\right\rceil$ for some positive integer $k$.

Proof. By Lemma 4.1, each orbit of $\operatorname{Aut}(G)$ has size 1 or $n$. Let $X_{i}=\left\{x_{i, 1}, x_{i, 2}, \ldots, x_{i, n}\right\}$ $(i=1,2, \ldots, k)$ be the orbits of $\operatorname{Aut}(G)$ on $V(G)$ of size $n$. We have $k \geqslant 1$, for otherwise each orbit of $\operatorname{Aut}(G)$ has size 1, which implies that $\operatorname{Aut}(G)=\left\{\mathrm{id}_{V}\right\}$, consists of the single identity permutation on the vertex set $V$, in contrary to our assumption.

For any $\varphi \in \operatorname{Aut}(G)$, for any $i \in\{1,2, \ldots, k\}$, let $\left.\varphi\right|_{X_{i}}$ be the restriction of $\varphi$ to $X_{i}$. First we show that if $\varphi, \psi \in \operatorname{Aut}(G)$ and $\left.\varphi\right|_{X_{i}}=\left.\psi\right|_{X_{i}}$, then $\varphi=\psi$. For $x \in V$, let $H_{x}=\{\tau \in \operatorname{Aut}(G): \tau(x)=x\}$. Let $x^{*}$ be an arbitrary vertex in $X_{i}$. Then $\bigcap_{x \in X_{i}} H_{x}=$ $\bigcap_{\tau \in \operatorname{Aut}(G)} \tau H_{x^{*}} \tau^{-1}$ is a normal subgroup of $\operatorname{Aut}(G)$ with index at least $n$ (as $H_{x^{*}}$ has index $n$ ). As the only nontrivial normal subgroup of $S_{n}$ is $A_{n}$ for $n \geqslant 5$, we conclude that $\bigcap_{\tau \in \operatorname{Aut}(G)} \tau H_{x} \tau^{-1}=\left\{\mathrm{id}_{V}\right\}$. Since $\varphi^{-1} \psi \in \bigcap_{x \in X_{i}} H_{x}$, we have $\varphi^{-1} \psi=\operatorname{id}_{V}$, i.e., $\varphi=\psi$.

It follows from the paragraph above that the set $\left\{\left.\varphi\right|_{X_{i}}: \varphi \in \operatorname{Aut}(G)\right\}$ consists of all the permutations of $X_{i}$. In other words, the mapping $f_{i}$ defined as $f_{i}(\varphi)=\left.\varphi\right|_{X_{i}}$ is an automorphism of $S_{n}$. It is well known that for $n \geqslant 3$ and $n \neq 6$, $\operatorname{Aut}\left(S_{n}\right)=\operatorname{Inn}\left(S_{n}\right)$. This implies that, for each $i \in\{1,2, \ldots, k\}$, after identifying $x_{i, j}$ with $j$, there is a permutation $\tau_{i} \in S_{n}$ such that for any $\varphi \in S_{n}, f_{i}(\varphi)=\tau_{i} \varphi \tau_{i}^{-1}$. In other words, $\varphi\left(x_{i, j}\right)=x_{i, \tau_{i} \varphi \tau_{i}^{-1}(j)}$. For $j=1,2, \ldots, n$, let $A_{j}$ be the sequence $\left(x_{1, \tau_{1}(j)}, x_{2, \tau_{2}(j)}, \ldots, x_{k, \tau_{k}(j)}\right)$. Then each $\varphi \in$ $\operatorname{Aut}(G)$ induces a permutation on the set $\left\{A_{1}, A_{2}, \ldots, A_{n}\right\}$. Conversely, any permutation on the set $\left\{A_{1}, A_{2}, \ldots, A_{n}\right\}$ corresponds to an automorphism of $G$.

Now we show that $D(G)=\left\lceil n^{1 / k}\right\rceil$. Let $s=\left\lceil n^{1 / k}\right\rceil$ and let $C=\{1,2, \ldots, s\}$. For a labeling $\ell$ of the vertices of $G$ by labels from $C$, let $\ell\left(A_{i}\right)$ be the sequence $\left(\ell\left(x_{1, \tau_{1}(i)}\right), \ell\left(x_{2, \tau_{2}(i)}\right), \ldots, \ell\left(x_{k, \tau_{k}(i)}\right)\right)$. Since $s^{k} \geqslant n$, there is a labeling $\ell$ of the vertices of $G$ by labels from $C$ so that all the sequences $\ell\left(A_{1}\right), \ell\left(A_{2}\right), \ldots, \ell\left(A_{n}\right)$ are distinct. If $\varphi$ is an automorphism of $G$ for which $\ell(\varphi(v))=\ell(v)$ for all $v \in V$, then we have $\ell\left(\varphi\left(A_{i}\right)\right)=\ell\left(A_{i}\right)$. As $\ell\left(A_{i}\right) \neq \ell\left(A_{j}\right)$ for any $i \neq j$, this implies that $\sigma\left(A_{i}\right)=A_{i}$. So $\sigma$ is the identity permutation. Therefore $\ell$ is a distinguishing labeling of $G$, and hence $D(G) \leqslant s=\left\lceil n^{1 / k}\right\rceil$.

If $s<\left\lceil n^{1 / k}\right\rceil$, then $s^{k}<n$. For any labeling $\ell$ of $V$ with $s$ labels, there exist $j \neq j^{\prime}$ such that $\ell\left(A_{j}\right)=\ell\left(A_{j^{\prime}}\right)$. The automorphism $\sigma$ of $G$ which fixes all the other vertices of $G$ and interchanges $A_{j}$ and $A_{j^{\prime}}$ preserves the labeling $\ell$. So $\ell$ is not a distinguishing labeling of $G$. Therefore $D(G)=\left\lceil n^{1 / k}\right\rceil$.

It is very likely that the condition "each orbit of $\operatorname{Aut}(G)$ on $V(G)$ has size less than $\binom{n}{2}$ " in Theorem 4.2 can be removed. This guess is supported by the following observation.

Suppose $n>6$ and $G$ is a graph with $\operatorname{Aut}(G)=S_{n}$. Let $H$ be the complete bipartite graph with $V(G)$ and $I$ as the two partite sets. Define an equivalence relation $\simeq$ on the edge set of $H$ as follows: $x i \simeq y j$ if and only if there is an automorphism $\tau \in \operatorname{Aut}(G)=S_{n}$ such that $\tau(x)=y$ and $\tau(i)=j$. Denote by $E_{1}, E_{2}, \ldots, E_{m}$ the equivalence classes of $\simeq$, and for each vertex $x$ of $G$, let $E_{i}(x)=\left\{e \in E_{i}: e\right.$ is incident to $\left.x\right\}$.

Lemma 4.3. If there is a vertex $x$ and an index $i$ (or two indices $i, i^{\prime}$ ) such that $2 \leqslant\left|E_{i}(x)\right| \leqslant n / 2\left(\right.$ or $\left.2 \leqslant\left|E_{i}(x) \cup E_{i^{\prime}}(x)\right| \leqslant n / 2\right)$, then $D(G)=2$.

Proof. Assume that $x$ is a vertex for which there is an index $i$ with $2 \leqslant\left|E_{i}(x)\right| \leqslant n / 2$. With a change of names, if necessary, we may assume that $E_{i}(x)=\{x 1, x 2, \ldots, x t\}$. (In case there are two indices $i, i^{\prime}$ with $2 \leqslant\left|E_{i}(x) \cup E_{i^{\prime}}(x)\right| \leqslant n / 2$, assume that $E_{i}(x) \cup E_{i^{\prime}}(x)=$ $\{x 1, x 2, \ldots, x t\})$. Let $\tau$ be the cyclic permutation $(12 \cdots n)$, and let $\pi$ be any (fixed) permutation for which $\pi(1)=2, \pi(i)=i+2$ for $i=2,3, \ldots, t$. For $i=0,1,2, \ldots, n-t$, let $x_{i}=\tau^{i}(x)$, and let $x_{n-t+1}=\pi(x)$. Let $X=\left\{x_{0}, x_{1}, \ldots, x_{n-t+1}\right\}$. Let $H^{\prime}$ be the subgraph of $H$ with vertex set $V^{\prime}=X \cup I$, and with edge set $E^{\prime}=\bigcup_{j=1}^{t}\left(\left(\bigcup_{i=0}^{n-t} \tau^{i}(x) \tau^{i}(j)\right) \cup\right.$ $\pi(x) \pi(j))$.

Now we show that $H^{\prime}$ is a rigid graph. As $H^{\prime}$ is connected and the two partite sets have different cardinality, any automorphism $\phi$ of $H^{\prime}$ preserves the partite sets, i.e., $\phi(X)=X$ and $\phi(I)=I$. Observe that in $H^{\prime}$, each vertex $x_{i} \in X$ has degree $t$. Vertices of $I$ have different degrees. For example, it is easy to verify that each of vertices 1 and $n$ has degree 1 , vertex 2 has degree 3 , vertex $n-1$ has degree 2 (because $n>6$ ), and every other vertex has degree at least $\min \{3, t\}$. For each vertex $x_{i}$, let $S\left(x_{i}\right)$ be the multiset of degrees of neighbors of $x_{i}$ in $H^{\prime}$, i.e., $S\left(x_{i}\right)=\left\{d_{H^{\prime}}(j): x_{i} j \in E^{\prime}\right\}$. If $\phi$ is an automorphism of $H^{\prime}$, then for any $x_{i} \in X, S\left(x_{i}\right)=S\left(\phi\left(x_{i}\right)\right)$. Since $S\left(x_{n-t}\right)$ and $S\left(x_{0}\right)$ are the only multisets that contains 1 , and since $S\left(x_{n-t}\right) \neq S\left(x_{0}\right)$, it follows that both $x_{0}$ and $x_{n-t}$ are fixed by $\phi$. Observe that $x_{1}$ is the only vertex which shares $t-1$ neighbors with $x_{0}$, so $\phi$ fixes $x_{1}$. For $i=n-t-1, n-t-2, \ldots, 4,3, x_{i}$ is the only vertex of $X$ which shares $t-1$ neighbors with $x_{i+1}$. So $\phi$ fixes $x_{n-t-1}, x_{n-t-2}, \ldots, x_{3}$. So $\phi$ fixes every vertex of the set $X^{\prime}=$ $X \backslash\left\{x_{2}, x_{n-t+1}\right\}$. For $i, j \in\{1,2, \ldots, n\}$, it is easy to verify that if $i \neq j$, then $N_{H^{\prime}}(i) \cap X^{\prime} \neq$ $N_{H^{\prime}}(j) \cap X^{\prime}$. Therefore $\phi$ fixes all the vertices of $I$, and hence fixes each of $x_{2}$ and $x_{n-t+1}$ as well. So $H^{\prime}$ is a rigid graph.

Let $\ell(v)=1$ for $v \in X$ and $\ell(y)=2$ for all other vertices $y$ of $G$. Suppose $\sigma \in \operatorname{Aut}(G)$ is an automorphism of $G$ which preserves the labels. Then $\sigma(X)=X$ and $\sigma(I)=I$. If $x i$ is an edge of $H^{\prime}$, then $\sigma(x) \sigma(i) \simeq x i$ and hence $\sigma(x) \sigma(i)$ is an edge of $H^{\prime}$. (By the definition of $H^{\prime}$, if $x, y \in X, i, j \in I, x i$ is an edge of $H^{\prime}$ and $y j$ is not an edge of $H^{\prime}$, then $x i \nsim y j$.) So $\sigma$ is an automorphism of $H^{\prime}$. As $H^{\prime}$ is a rigid graph, we conclude that $\sigma$ is the identity. So $\ell$ is a distinguishing labeling, and hence $D(G)=2$.

Lemma 4.4. If there are vertices $x_{1}, x_{2}, \ldots, x_{k}$ such that each lies in a distinct orbit, and each has $\left|E_{i_{1}}\left(x_{i}\right)\right|=1$ and $\left|E_{i_{2}}\left(x_{i}\right)\right|=n-1$ for some indices $i_{1}, i_{2}$, then $D(G) \leqslant$ $\left\lceil n^{1 / k}\right\rceil+1$.

Proof. By choosing different vertices in the orbit of $x_{i}$, if necessary, we may assume that $E_{i_{1}}\left(x_{i}\right)=\left\{x_{i} 1\right\}$. Let $\tau=(12 \cdots n)$ be the cyclic permutation. For $i=1,2, \ldots, k$, for $j=$ $0,1, \ldots, n-1$, let $x_{i, j}=\tau^{j}\left(x_{i}\right)$. Let $A_{j}$ denote the sequence $\left(x_{1, j}, x_{2, j}, \ldots, x_{k, j}\right)$. Label the vertices of $G$ so that labels $1,2, \ldots,\left\lceil n^{1 / k}\right\rceil$ are used to label vertices $x_{i, j}$ in such a way that $\ell\left(A_{j}\right) \neq \ell\left(A_{j^{\prime}}\right)$ for $j \neq j^{\prime}$, and label the other vertices of $G$ with an extra label $\left\lceil n^{1 / k}\right\rceil+1$. Similarly to the proof of Theorem 4.2, the labeling is a distinguishing labeling. So $D(G) \leqslant\left\lceil n^{1 / k}\right\rceil+1$.

It is very likely that if $x$ is a vertex for which there are indices $i_{1}, i_{2}$ with $\left|E_{i_{1}}(x)\right|=1$ and $\left|E_{i_{2}}(x)\right|=n-1$, then $x$ lies in an orbit of size $n$. We also believe that if $x$ is a vertex for which there is an index $i$ with $\left|E_{i}(x)\right|=n$, then $x$ lies in an orbit of size 1, i.e., $x$ is fixed by every automorphism of $G$. If this is the case then the extra color used in the proof of Lemma 4.4 is not needed, and we have the conclusion that $D(G)=\left\lceil n^{1 / k}\right\rceil$. We state it as a conjecture:

Conjecture 4.5. If $G=(V, E)$ is a graph which realizes $S_{n}$ and $n \geqslant 6$, then $D(G)=$ $\left\lceil n^{1 / k}\right\rceil$ for some positive integer $k$.

## 5. A Brooks type results on $D(G)$

Albertson and Collins [1] proved that for a connected graph $G, D(G) \leqslant \Delta(G)+1$, where $\Delta(G)$ denotes the maximum degree of $G$. (In [2] the result is mentioned for the case of regular graphs.) Moreover, the result for the case of trees appears in [12, Theorem 4.1]. In this section we prove that $D(G) \leqslant \Delta(G)$, unless $G$ is a complete graph, complete bipartite graph, or $C_{5}$. (Just before the print of this paper, we learned that this result is proved independently by Collins and Trenk [9].) We begin with the following observation. For a vertex $x$ of a graph $G, N_{G}(x)$ denote the set of vertices adjacent to $x$.

Lemma 5.1. Let $(G, \ell)$ be a connected, labeled graph and let every vertex of $X \subseteq V(G)$ be fixed by every automorphism of $(G, \ell)$. Let $x \in X$ and set $S=N_{G}(x) \backslash X$. If $\ell(u) \neq \ell(v)$ holds for any different vertices $u$ and $v$ of $S$, then every vertex of $S$ is fixed by every automorphism of $(G, \ell)$.

Proof. Let $\varphi$ be an automorphism of $(G, \ell)$. By assumption, every vertex of $X \subseteq V$ is fixed by $\varphi$. In particular, $\varphi(x)=x$. This implies that $\varphi(S)=S$. Since $\ell(v) \neq \ell(u)$ for any $u, v \in S$ with $u \neq v$ we conclude that $\varphi$ fixes every vertex of $S$.

Theorem 5.2. Let $G$ be a connected graph. Then $D(G) \leqslant \Delta(G)$ unless $G$ is either $K_{n}$, $n \geqslant 1, K_{n, n}, n \geqslant 1$, or $C_{5}$. In these cases $D(G)=\Delta(G)+1$.

Proof. It is easy to verify that for $n \geqslant 1, D\left(K_{n}\right)=n=\Delta\left(K_{n}\right)+1, D\left(K_{n, n}\right)=n+1=$ $\Delta\left(K_{n, n}\right)+1$, and that $D\left(C_{5}\right)=3=\Delta\left(C_{5}\right)+1$.

Assume $G \notin\left\{K_{n}, K_{n, n}, C_{5}\right\}$. We shall prove that $D(G) \leqslant \Delta(G)$.
Suppose that $G$ is not regular. Let $u$ be a vertex of $G$ with $d(u)<\Delta(G)$ and set $\ell(u)=\Delta(G)$. No other vertex but $u$ will receive label $\Delta(G)$, thus $u$ will be fixed by every automorphism of $(G, \ell)$. Arrange the remaining vertices in a breadth-first search (BFS) order with $u$ as the root, and proceed as follows. Let $v$ be a vertex considered in this order and suppose that some of its neighbors are not yet labeled. Then label the unlabeled neighbors of $v$ with different labels from $\{1,2, \ldots, \Delta(G)-1\}$. By an inductive application of Lemma 5.1 we easily infer that $\ell$ is a $\Delta(G)$-distinguishing labeling of $G$.

Assume that $G$ is regular. Since $D\left(C_{n}\right)=2$ for $n \geqslant 6$, cf. [1], we may assume in the rest that $\Delta(G) \geqslant 3$. Take an arbitrary shortest cycle $C$ and let $u, v, w$ be three consecutive
vertices of $C$. If $\left(N_{G}(u) \backslash C\right) \neq\left(N_{G}(w) \backslash C\right)$ then let $x \in N_{G}(u) \backslash\left(C \cup N_{G}(w)\right)$. Then we set $\ell(z)=\Delta(G)$ for all $z \in C \backslash v, \ell(x)=\ell(v)=1$. No other vertex will receive label $\Delta(G)$ and no other neighbor of $u$ or of $w$ will receive label 1. It follows that $u$ and $w$ will be fixed by every automorphism of $G$ since the neighborhood of $u$ contains two vertices of label 1 while the neighborhood of $w$ contains only one such vertex. Recall that $x$ is not adjacent to $w$ and note that $x$ is cannot be adjacent to any other vertex of $C$ labeled with $\Delta$ since $C$ is a shortest cycle. It follows that the vertices $x$ and $v$ are distinguishable because $x$ is adjacent to only one vertex of label $\Delta$ but $v$ is adjacent to two such vertices. By the BFS method started in vertex $v$ we can extend $\ell$ to a $\Delta(G)$-distinguishing labeling of $G$.

Thus we assume that for any three consecutive vertices $u, v, w$ of a shortest cycle $C$ we have $\left(N_{G}(u) \backslash C\right)=\left(N_{G}(w) \backslash C\right)$. Since $\left|N_{G}(u)\right|=\Delta \geqslant 3$, we conclude that $G$ has girth at most 4. If $G$ has a triangle, then $u$ is adjacent to $w$, and hence for every $x \in N_{G}(u)$, $u, w, x$ are three consecutive vertices of a shortest cycle $C^{\prime}$ (which is a triangle), and hence $\left(N_{G}(u) \backslash C^{\prime}\right)=\left(N_{G}(x) \backslash C^{\prime}\right)$. This implies that $G$ is a complete graph, in contrary to our assumption. If $G$ has no triangle, then $G$ has girth 4 , and hence $N_{G}(u) \cap C=N_{G}(w) \cap C$. Therefore $N_{G}(u)=N_{G}(w)$. Moreover, for any two vertices $x, y \in N_{G}(u), x, u, y$ are three consecutive vertices of a 4-cycle $(x, u, y, w)$, and hence $N_{G}(x)=N_{G}(y)$. This implies that any two nonadjacent vertices lies in a 4-cycle and hence have the same neighbors. So $G$ is a regular complete bipartite graph, again in contrary to our assumption.

In some cases Theorem 5.2 can be further improved. For instance:
Proposition 5.3. Let $G$ be a connected graph and let $H$ be a subgraph of $G$ invariant under every automorphism of $G$. If $H$ has at least one edge and $D(H)<\Delta(G)$ then $D(G)<\Delta(G)$.

Proof. We proceed similarly as in the proof of Theorem 5.2. First label vertices of $H$ with $D(H)$ labels so that $H$ is eventually fixed by an arbitrary automorphism of $(H, \ell)$. Since $H$ is invariant under every automorphism of $G$ this implies that $H$ will be point-wise fixed by automorphisms of ( $G, \ell^{\prime}$ ), where $\ell^{\prime}$ is any extension of $\ell$. Let $v$ be a vertex of $H$ which has a neighbor in $H$ and construct a BFS tree with $v$ as a root. Then follow the BFS order and whenever we reach a vertex with unlabeled neighbors, label its unlabeled neighbors with different labels. By the BFS construction, we can always use labels from $\{1,2, \ldots, \Delta-1\}$. Lemma 5.1 completes the proof.

As we already mentioned, Theorem 5.2 is proved in [12] for the case of trees. (If a tree $T$ has at least two edges, then $D(T) \leqslant \Delta(T)$.) On the other hand, Cheng [7] showed that the distinguishing number of a tree can be computed efficiently. The main ideas are to reduce the problem to rooted trees whose centers consist of a single vertex and then to count different $d$-distinguishing labelings starting from the leaves. Based on this approach the following result easily follows.

Proposition 5.4. Let $T$ be a tree, $T_{0}$ the set of its leaves, and for $i \geqslant 1$ let $T_{i}=\{x \notin$ $\left.T_{0} \cup \cdots \cup T_{i-1}: \exists y \in T_{i-1}, x \sim y\right\}$. Set $d_{i}(x)=\left|N_{G}(x) \cap T_{i}\right|$. Then

$$
D(T) \leqslant \max \left\{\left\lceil d_{i}(x)^{1 /(i+1)}\right\rceil: x \in V(T), i \geqslant 0\right\} .
$$



Fig. 1. The tree $T_{3}$.

To see that this bound is in a way best possible (and arbitrarily better than the $\Delta(T)$ bound) consider the following example. Let $k \geqslant 1$, take $2^{k}$ copies of the path $P_{k+1}$, select an end of each and identify the selected vertices. Denote the resulting graph $T_{k}$, see Fig. 1 for $T_{3}$. Then $\Delta\left(T_{k}\right)=2^{k}$, but by Proposition 5.4, $D\left(T_{k}\right) \leqslant 2$ and so $D\left(T_{k}\right)=2$.

## 6. Uniquely distinguishable graphs

Let $G$ and $H$ be connected graphs and let $G \cup H$ be the disjoint union of $G$ and $H$. Clearly, $D(G \cup H) \geqslant \max \{D(G), D(H)\}$. Moreover, if $G$ and $H$ are not isomorphic the equality holds. The remaining question is what is $D(G \cup G)$ ? (See [12] for such examples.) It is easy to note that $D(G \cup G) \leqslant D(G)+1$, hence $D(G \cup G)$ equals either $D(G)$ or $D(G)+1$. To classify graphs with respect to these two possibilities, we introduce the following definition.

A connected graph $G$ is uniquely distinguishable if for any $D(G)$-distinguishing labelings $\ell_{1}$ and $\ell_{2}$ of $G$ there exists an automorphism $\varphi$ of $G$ such that for any vertex $x \in V(G)$ we have $\ell_{1}(x)=\ell_{2}(\varphi(x))$. From this definition and by the above remarks we infer:

Proposition 6.1. Let $G$ be a connected graph. Then $D(G \cup G) \leqslant D(G)+1$, where the equality holds if and only if $G$ is uniquely distinguishable.

Note also that the definition immediately implies that the number of vertices of a uniquely $d$-distinguishable graph is a multiple of $d$.

A (connected) asymmetric graph is a uniquely 1 -distinguishable graph and $K_{n}$ is a uniquely $n$-distinguishable graph. The only uniquely 2 -distinguishable graph on four vertices is $K_{4}$ minus an edge. $C_{6}$ and the Cartesian product of $K_{3}$ with $K_{2}$ are uniquely 2-distinguishable graphs on six vertices.

Let $G$ and $H$ be graphs, let $V(G)=\left\{v_{1}, \ldots, v_{n}\right\}$, and let $H_{1}, \ldots, H_{n}$ be isomorphic copies of $H$. Take the disjoint union $G \cup H_{1} \cup \cdots \cup H_{n}$ and join by an edge every vertex of $H_{i}$ with $v_{i}, 1 \leqslant i \leqslant n$. Denote the resulting graph with $G^{\bullet H}$. In addition, let $D_{\leqslant d}(H)$ denote the number of nonequivalent distinguishable labelings of $H$ with at most $d$ labels.

Theorem 6.2. Let $d \geqslant 2$, let $H$ be a graph with $D(H) \leqslant d$, and let $n=d \cdot D_{\leqslant d}(H)$. Then $K_{n}^{\bullet H}$ is uniquely d-distinguishable.

Proof. Set $r=D_{\leqslant d}(H)$ and let $v_{1}, \ldots, v_{n}$ be the vertices of $K_{n}^{\bullet H}$ that correspond to $K_{n}$. The vertices of $K_{n}^{\bullet H}$ of the largest degree are $v_{1}, \ldots, v_{n}$, so any automorphism of $K_{n}^{\bullet H}$ will permute them. Let $\ell$ be a $d$-labeling of $K_{n}^{\bullet H}$ and suppose that at least $r+1$ vertices


Fig. 2. A uniquely 3-distinguishable graph.
among $v_{1}, \ldots, v_{n}$ receive the same label. Then there exist vertices $v_{i}, v_{j}$ such that $\ell\left(v_{i}\right)=$ $\ell\left(v_{j}\right)$ and such that the copies $H_{i}$ and $H_{j}$ of $H$ (in $K_{n}^{\bullet}{ }^{\bullet}$ ) have equivalent labelings $\ell_{i}$ and $\ell_{j}$, respectively. Let $\varphi_{i j}$ be an automorphism of $H$ such that $\ell_{i}=\ell_{j} \circ \varphi_{i j}$. Let $\varphi$ be the automorphism of $K_{n}^{\bullet H}$ with $\varphi\left(v_{i}\right)=v_{j}, \varphi\left(v_{j}\right)=v_{i}, \varphi\left(H_{i}\right)=\varphi_{i j}\left(H_{j}\right), \varphi\left(H_{j}\right)=\varphi_{i j}^{-1}\left(H_{i}\right)$, and fixed elsewhere. Since $\varphi$ is a nontrivial automorphism of $\left(K_{n}^{\bullet}{ }^{H}, \ell\right)$ it follows that $\ell$ is not a distinguishable labeling. An analogous argument also implies that $D\left(K_{n}^{\bullet H}\right) \geqslant$ $n / r=d$.

Let $\mathcal{H}_{1}=\left\{H_{1}, \ldots, H_{r}\right\}, \ldots, \mathcal{H}_{d}=\left\{H_{(d-1) r+1}, \ldots, H_{d r}\right\}$. We define a labeling $\ell$ as follows: $\ell\left(v_{1}\right)=\cdots=\ell\left(v_{r}\right)=1, \ldots, \ell\left(v_{(d-1) r+1}\right)=\cdots=\ell\left(v_{d r}\right)=d$. For each $1 \leqslant i \leqslant d$, label the graphs from $\mathcal{H}_{i}$ in such a way that no two graphs in $\mathcal{H}_{i}$ receive equivalent labelings. By the choice of $n$, such a labeling exists. It is easy to see that $\ell$ is a distinguishing labeling. On the other hand, if $\ell$ is a $d$-distinguishable labeling of $K_{n}^{\bullet H}$, then by the argument in the previous section, we may assume that $\ell\left(v_{1}\right)=\cdots=\ell\left(v_{r}\right)=1, \ldots$, $\ell\left(v_{(d-1) r+1}\right)=\cdots=\ell\left(v_{d r}\right)=d$, and moreover, any two of the graphs from $\mathcal{H}_{i}(1 \leqslant i \leqslant d)$ receive nonequivalent labelings. So we must use all the $r=D_{\leqslant d}(H)$ labelings to label the graphs from $\mathcal{H}_{i}$. Therefore $\ell$ defined above is the unique $d$-distinguishable labeling of $K_{n}^{\bullet H}$.

Theorem 6.2 is illustrated in Fig. 2 for the case $d=3$ and $H=K_{2}$.

## References

[1] M.O. Albertson, K.L. Collins, Symmetry breaking in graphs, Electron. J. Combin. 3 (1996) \#R18, 17 p.
[2] M.O. Albertson, K.L. Collins, An introduction to symmetry breaking in graphs, Graph Theory Notes N. Y. 30 (1996) 6-7.
[3] B. Bogstad, L.J. Cowen, The distinguishing number of the hypercube, Discrete Math. 283 (2004) 29-35.
[4] M. Chan, The distinguishing number of the augmented cube and hypercube powers, manuscript, August 2004.
[5] M. Chan, The maximum distinguishing number of a group, manuscript, September 2004.
[6] M. Chan, The distinguishing number of the direct and wreath product action, manuscript, Janurary 2005.
[7] C.T. Cheng, Three problems in graph labeling, PhD, The John Hopkins University, 1999.
[8] K.L. Collins, Symmetry breaking in graphs, Talk at the DIMACS Workshop on Discrete Mathematical Chemistry, DIMACS, Rutgers University, 23-25 March, 1998.
[9] K.L. Collins, A.N. Trenk, The distinguishing chromatic number, Electron. J. Combin. 13 (2006) \#R16, 19 p.
[10] M.W. Liebeck, Graphs whose full automorphism group is a symmetric group, J. Austral. Math. Soc. Ser. A 44 (1988) 46-63.
[11] A. Russell, R. Sundaram, A note on the asymptotics and computational complexity of graph distinguishability, Electron. J. Combin. 5 (1998) \#R23, 7 p.
[12] J. Tymoczko, Distinguishing numbers for graphs and groups, Electron. J. Combin. 11 (2004) \#R63, 13 p.


[^0]:    * Corresponding author.

    E-mail addresses: sandi.klavzar@uni-mb.si (S. Klavžar), tlwong@math.nsysu.edu.tw (T.-L. Wong), zhu@math.nsysu.edu.tw (X. Zhu).
    ${ }^{1}$ Supported in part by the Ministry of Science of Slovenia under the grant P1-0297. The work on the paper started during the visit of the author to the National Center for Theoretical Sciences of Taiwan.
    ${ }^{2}$ Supported in part by the National Science Council under grant NSC92-2115-M-110-010.
    ${ }^{3}$ Supported in part by the National Science Council under grant NSC92-2115-M-110-007.

