# Pebble Exchange Group of Graphs 

Tatsuoki Kato ${ }^{1}$<br>Yamagata University<br>2-2-2 Iida-Nishi, Yamagata 990-9585, Japan

Tomoki Nakamigawa ${ }^{2}$<br>Department of Information Science<br>Shonan Institute of Technology<br>1-1-25 Tsujido-Nishikaigan, Fujisawa 251-8511, Japan<br>Tadashi Sakuma 3<br>Faculty of Science<br>Yamagata University<br>1-4-12 Kojirakawa, Yamagata 990-8560, Japan


#### Abstract

A graph puzzle $\operatorname{Puz}(G)$ of a graph $G$ is defined as follows. A configuration of $\operatorname{Puz}(G)$ is a bijection from the set of vertices of a board graph to the set of vertices of a pebble graph, both graphs being isomorphic to some input graph $G$. A move of pebbles is defined as exchanging two pebbles which are adjacent on both a board graph and a pebble graph. For a pair of configurations $f$ and $g$, we say that $f$ is equivalent to $g$ if $f$ can be transformed into $g$ by a finite sequence of moves.

Let $\operatorname{Aut}(G)$ be the automorphism group of $G$, and let $1_{G}$ be the unit element of $\operatorname{Aut}(G)$. The pebble exchange group of $G$, denoted by


[^0]$\operatorname{Peb}(G)$, is defined as the set of all automorphisms $f$ of $G$ such that $1_{G}$ and $f$ are equivalent to each other.

In this paper, some basic properties of $\operatorname{Peb}(G)$ are studied. Among other results, it is shown that for any connected graph $G$, all automorphisms of $G$ are contained in $\operatorname{Peb}\left(G^{2}\right)$, where $G^{2}$ is a square graph of $G$.
keywords: pebble motion, motion planning, graph puzzle, automorphism

## 1 Introduction

Let $G$ be a finite and undirected graph with no multiple edge or loop. The vertex set of $G$ and the edge set of $G$ are denoted by $V(G)$ and $E(G)$, respectively. Let $P=\{1, \ldots, k\}$ be a set of pebbles with $k<|V(G)|$. An arrangement of $P$ on $G$ is defined as a function $f$ from $V(G)$ to $\{0,1, \ldots, k\}$ with $\left|f^{-1}(i)\right|=1$ for $1 \leq i \leq k$, where $f^{-1}(i)$ is a vertex occupied with the $i$ th pebble for $1 \leq i \leq k$ and $f^{-1}(0)$ is a set of unoccupied vertices. A move is defined as shifting a pebble from a vertex to some unoccupied neighbour. The pebble motion problem on the pair $(G, P)$ is to decide whether a given arrangement of pebbles reachable from another by executing a sequence of moves. The well-known puzzle named "15-puzzle" due to Loyd [10] is a typical example of this problem where the graph $G$ is a $4 \times 4$-grid.

The pebble motion problem is studied intensively [1 55, $8,9,11-14$, because of its considerable theoretical interest as well as its wide range of applications for computer science and robotics, such as management of indivisible packets of data moving on wide-area communication network and motion planning of independent robots. In 1974, Wilson [14] solved completely the feasibility problem (i.e. the problem of determining whether all the configurations of the puzzle are rearrangeable from one another or not) for the case of $\left|f^{-1}(0)\right|=1$ on general graphs, and it followed by the result of Kornhauser, Miller and Spirakis (FOCS '84) 9 for the case of $\left|f^{-1}(0)\right| \geq 2$. Papadimitriou, Raghavan, Sudan and Tamaki (FOCS '94) [11] consider the case that there exists a single special pebble ("robot") and that the other pebbles ("obstacles") are indistinguishable. They focus on the time complexity problems for optimal number of moves from an arbitrary given arrangement of the pebbles to a proper goal arrangement in which the robot is on the desired vertex. In 2012, Fujita, Nakamigawa and Sakuma [5] generalized the problem to the case of "colored pebbles", where each pebble of $P$ is distinguished by its color. They
also completely solved the feasibility problem for their model.
In 2015, Fujita, Nakamigawa and Sakuma [6] generalized the pebble motion problem as follows: For two graphs $G$ and $H$ with a common number of vertices, let us consider a puzzle $\operatorname{Puz}(G, H)$, where $G$ is a board graph and $H$ is a pebble graph. We call a bijection $f$ from $V(G)$ to $V(H)$ a configuration of $\operatorname{Puz}(G, H)$, and we denote the set of all configurations of $\operatorname{Puz}(G, H)$ by $\mathcal{C}(G, H)$. Given a configuration $f$, if $f(x)=y$, we consider that the vertex $x$ of the board is occupied by the pebble $y$. In $\operatorname{Puz}(G, H)$, two pebbles $y_{1}=f\left(x_{1}\right)$ and $y_{2}=f\left(x_{2}\right)$ can be exchanged if $x_{1} x_{2} \in E(G)$ and $y_{1} y_{2} \in E(H)$. Then the resultant configuration $g$ satisfies that $g\left(x_{1}\right)=y_{2}$, $g\left(x_{2}\right)=y_{1}$ and $g(x)=f(x)$ for any $x \in V(G) \backslash\left\{x_{1}, x_{2}\right\}$. We call the operation a move. If a configuration $f$ is transformed into another configuration $g$ with a finite sequence of moves, we say that $f$ and $g$ are equivalent, denoted by $f \sim g . \operatorname{Puz}(G, H)$ is called feasible if all the configurations of the puzzle are equivalent to each other.

In [6], the above mentioned graph puzzle was formally introduced and some more necessary/sufficient conditions of the feasibility of the puzzle was studied. This model has again a wide range of real world applications, especially for robot motion planning problems and facility relocation problems. Please see [6] for details.

In this paper, we will shed light on some algebraic property of the puzzle, which is of not only theoretical interest, but also practical importance, as will be discussed later.

In the following, we only consider the case where a board graph and a pebble graph are the same, and we denote $\mathcal{C}(G, G)$ and $\operatorname{Puz}(G, G)$ simply by $\mathcal{C}(G)$ and $\operatorname{Puz}(G)$, respectively.

The automorphism group of a graph $G$, denoted by $\operatorname{Aut}(G)$, is the group which consists of all bijections $f$ from $V(G)$ to $V(G)$ such that $f\left(x_{1}\right) f\left(x_{2}\right) \in$ $E(G)$ if and only if $x_{1} x_{2} \in E(G)$. Let $1_{G}$, or simply 1 , denote the identity element of $\operatorname{Aut}(G)$. Let us introduce the pebble exchange group of $G$, denoted by $\operatorname{Peb}(G)$, as the group which consists of all automorphisms $f$ of $G$ such that $1_{G}$ and $f$ are equivalent in $\operatorname{Puz}(G)$.

In application, when a graph $G$ represents some system, an automorphism $f$ of $G$ corresponds to a rearrangement of possible arrangements of the system. If $f$ is contained in $\operatorname{Peb}(G)$, the corresponding rearrangement is realizable with a sequence of local changes step by step. Hence if we
can show the equation $\operatorname{Peb}(G)=\operatorname{Aut}(G)$ here, it means that practically all the necessary and sufficient arrangements are mutually reachable from one another.

However, it seems to be a highly nontrivial and difficult problem to characterize completely the graphs whose pebble exchange groups are equal to their automorphism groups. Hence, before to attack this problem directly, in this paper we will show that the class of graphs $G$ satisfying $\operatorname{Peb}(G)=\operatorname{Aut}(G)$ is considerably large. Especially, we prove (Theorem 12) that, for any connected graph $G$, the pebble exchange group of the square $G^{2}$ of $G$ contains a subgroup isomorphic to the automorphism group of $G$. Since the maximum degree of $G^{2}$ is no more than the square of the maximum degree of $G$, if the maximum degree of $G$ is a small constant and the order of $G$ is sufficiently large, then not only $G$ but also $G^{2}$ are sparse graphs, and the puzzle $\operatorname{Puz}\left(G^{2}\right)$ is also far from feasible in general. In spite of this, somewhat surprisingly, by using Theorem 12, for example, we can show that, for any connected graph $G$, if we 2-subdivide all the edges of $G$, and if we take its square, the resulting graph $H$ satisfies the equation $\operatorname{Peb}(H)=\operatorname{Aut}(H)$.

## 2 Preliminaries

Pebble motion problems on graphs have been extensively studied. In the following, let us introduce previously proven theorems closely related to this paper, by using the concept of $\operatorname{Puz}(G, H)$.

For two graphs $G$ and $H$, let $G \times H$ denote a Cartesian product of $G$ and $H$, where $V(G \times H)=V(G) \times V(H)$ and $E(G \times H)=\left\{\left(u_{1}, v_{1}\right)\left(u_{2}, v_{2}\right) \in\right.$ $V(G \times H)^{2}: u_{1} u_{2} \in E(G)$ and $v_{1}=v_{2}$, or $u_{1}=u_{2}$ and $\left.v_{1} v_{2} \in E(H)\right\}$. Let $P_{k}$ be the path with $k$ vertices, and let $K_{1, \ell}$ be the star with $\ell$ pendant vertices.

Theorem 1 (W. W. Johnson [8], W. E. Story [13]) $\operatorname{Puz}\left(P_{4} \times P_{4}, K_{1,15}\right)$ corresponds to the 15-puzzle, by considering that the center $z$ of $K_{1,15}$ corresponds to the unoccupied space of the 15-puzzle. For two configurations $f, g \in \mathcal{C}\left(P_{4} \times P_{4}, K_{1,15}\right)$ with $f^{-1}(z)=g^{-1}(z), f$ is equivalent to $g$ if and only if $g^{-1} \circ f$ is an even permutation on $V(G)$.

We will show some more examples, from Theorem 2 to Theorem 5, which are considered as generalizations of Theorem 1. Suppose that both $G$ and $H$


Figure 1: The graph $\theta(1,2,2)$
are bipartite graphs with at least three vertices. It is not difficult to see that $\operatorname{Puz}(G, H)$ is not feasible because of the parity of configurations (cf. [6]).

Let $\theta(1,2,2)$ be a graph such that $V(\theta(1,2,2))=\left\{v_{i}: 1 \leq i \leq 7\right\}$ and $E(\theta(1,2,2))=\left\{v_{1} v_{2}, v_{2} v_{3}, v_{3} v_{4}, v_{4} v_{5}, v_{5} v_{6}, v_{6} v_{1}, v_{1} v_{7}, v_{4} v_{7}\right\}$. See Figure [1]

Theorem 2 (R. M. Wilson [14]) Let $G$ be a 2 -connected non-bipartite graph with $n$ vertices. If $G$ is not a cycle or $\theta(1,2,2)$, then $\operatorname{Puz}\left(G, K_{1, n-1}\right)$ is feasible.

For a positive integer $k$, a path $P=v_{1} v_{2} \cdots v_{k}$ of a graph $G$ is called a $k$-isthmus if (1) every edge of $P$ is a bridge of $G$, (2) every vertex of $P$ is a cut-vertex of $G$, and (3) $\operatorname{deg}_{G}\left(v_{i}\right)=2$ for $1<i<k$. For two graphs $G$ and $H$, the join $G+H$ is defined as $V(G+H)=V(G) \cup V(H)$, $E(G+H)=E(G) \cup E(H) \cup\{u v: u \in V(G), v \in V(H)\}$.

We remark that an isthmus is intuitively "a path connecting two blocks", and we cannot drop any one of conditions (1), (2) and (3) in the definition. For example, let $G$ be a graph such that $V(G)=\left\{v_{i}: 1 \leq i \leq 6\right\}, E(G)=$ $\left\{v_{i} v_{i+1}: 1 \leq i \leq 4\right\} \cup\left\{v_{3} v_{6}\right\}$ and let $P=v_{2} v_{3} v_{4}$. Then $P$ satisfies (1) and (2), but $P$ is not called an isthmus. Next, let $G$ be a graph such that $V(G)=\left\{v_{i}: 1 \leq i \leq 5\right\}, E(G)=\left\{v_{i} v_{i+1}: 1 \leq i \leq 4\right\} \cup\left\{v_{2} v_{4}\right\}$ and let $P=v_{2} v_{4}$. Then $P$ satisfies (2) and (3), but $P$ is not called an isthmus. Finally, let $G$ be a path of 3 vertices and let $P=G$. Then $P$ satisfies (3) and (1), but $P$ is not called an isthmus.

Let $K_{n}$ denote a complete graph with $n$ vertices, and let $K_{m, n}$ denote a complete bipartite graph on $m$ and $n$ vertices. For a graph $G$, let $\bar{G}$ be the complement of $G$. A set of pebbles is called labeled if we can distinguish them from one another. Otherwise we call the set of pebbles unlabeled.

Theorem 3 (D. Kohnhauser, G. Miller, and P. Spirakis [9]) Let $2 \leq$ $k \leq n$. A pebble graph $K_{k}+\overline{K_{n-k}}$ is considered as a set of $n-k$ labeled pebbles and $k$ unlabeled pebbles, in which two labeled pebbles cannot directly exchange their positions with each other. Let $G$ be a connected graph with $n$ vertices except a cycle. Then $\operatorname{Puz}\left(G, K_{k}+\overline{K_{n-k}}\right)$ is feasible if and only if $G$ has no $k$-isthmus.

Theorem 4 (S. Fujita, T. Nakamigawa, and T. Sakuma [5]) Let $2 \leq$ $k \leq n / 2$. Let $G$ be a graph with $n$ vertices. Then $\operatorname{Puz}\left(G, K_{k, n-k}\right)$ is feasible if and only if (1) $G$ is not a cycle, and (2) $G$ is not bipartite, and (3) $G$ has no $k$-isthmus.

Theorem 5 (S. Fujita, T. Nakamigawa, and T. Sakuma [5]) Let $r \geq$ 3 and let $2 \leq n_{1} \leq \ldots \leq n_{r}$. Let $G$ be a graph with $n=n_{1}+n_{2}+\cdots+n_{r}$ vertices. Then $\operatorname{Puz}\left(G, K_{n_{1}, n_{2}, \ldots, n_{r}}\right)$ is feasible if and only if (1) $G$ is not a cycle, and (2) $G$ has no $\left(n-n_{r}\right)$-isthmus.

Now we show that $\operatorname{Peb}(G)$ is a group, more precisely, a normal subgroup of $\operatorname{Aut}(G)$, first we prepare the following lemma.

Lemma 6 For $\varphi_{1}, \varphi_{2}, \alpha, \beta \in \operatorname{Aut}(G)$, if $\varphi_{1} \sim \varphi_{2}$, then we have $\beta \circ \varphi_{1} \circ \alpha \sim$ $\beta \circ \varphi_{2} \circ \alpha$.

Proof. Since $\varphi_{1} \sim \varphi_{2}$, there exists a finite sequence of transpositions $\sigma_{1}, \sigma_{2}, \ldots, \sigma_{s}$ on $V(G)$ corresponding to moves from $f_{0}=\varphi_{1}$ to $f_{s}=\varphi_{2}$ such that $f_{i}=\sigma_{i} \circ f_{i-1}$ for $1 \leq i \leq s$. By the definition of a move in $\operatorname{Puz}(G)$, for $1 \leq i \leq s$, we have a pair of vertices $x_{i}$ and $y_{i}$ satisfying $\left(x_{i}, y_{i}\right) \in E(G)$, $\left(f_{i-1}\left(x_{i}\right), f_{i-1}\left(y_{i}\right)\right) \in E(G)$ and $\sigma_{i}$ exchanges $f_{i-1}\left(x_{i}\right)$ and $f_{i-1}\left(y_{i}\right)$.

Put $\varphi_{j}^{\prime}=\beta \circ \varphi_{j} \circ \alpha$ for $1 \leq j \leq 2$. Let us define a sequence of configurations $g_{i}=\beta \circ f_{i} \circ \alpha$ for $0 \leq i \leq s$ and let us define a sequence of transpositions $\tau_{i}=\beta \circ \sigma_{i} \circ \beta^{-1}$ for $1 \leq i \leq s$. Furthermore, let us define $u_{i}=\alpha^{-1}\left(x_{i}\right)$ and $v_{i}=\alpha^{-1}\left(y_{i}\right)$. Then we have $g_{i}=\beta \circ\left(\sigma_{i} \circ f_{i-1}\right) \circ \alpha=\left(\beta \circ \sigma_{i} \circ \beta^{-1}\right) \circ\left(\beta \circ f_{i-1} \circ \alpha\right)=$ $\tau_{i} \circ g_{i-1}$ for $1 \leq i \leq s$.

What remains to be necessary to check is that $g_{i}$ 's are corresponding to moves. We have $\left(u_{i}, v_{i}\right) \in E(G)$ and $\left(g_{i-1}\left(u_{i}\right), g_{i-1}\left(v_{i}\right)\right)=\left(\beta \circ f_{i-1} \circ\right.$ $\left.\alpha\left(u_{i}\right), \beta \circ f_{i-1} \circ \alpha\left(v_{i}\right)\right)=\left(\beta \circ f_{i-1}\left(x_{i}\right), \beta \circ f_{i-1}\left(y_{i}\right)\right) \in E(G)$. Finally, $\tau_{i}$ is a transposition exchanging $\beta\left(f_{i-1}\left(x_{i}\right)\right)$ and $\beta\left(f_{i-1}\left(y_{i}\right)\right)$, namely $g_{i-1}\left(u_{i}\right)$ and $g_{i-1}\left(v_{i}\right)$, as required.

Proposition $7 \operatorname{Peb}(G)$ is a normal subgroup of $\operatorname{Aut}(G)$.

Proof. Firstly, let $f, g \in \operatorname{Peb}(G)$. Since $1_{G} \sim g$, by Lemma 6, we have $f=1_{G} \circ 1_{G} \circ f \sim 1_{G} \circ g \circ f=g \circ f$. Hence, we have $1_{G} \sim f \sim g \circ f$. It follows that $g \circ f \in \operatorname{Peb}(G)$. Secondly, By definition, $1_{G}$ is contained in $\operatorname{Peb}(G)$. Therefore, $\operatorname{Peb}(G)$ is a subgroup of $\operatorname{Aut}(G)$. In order to show that $\operatorname{Peb}(G)$ is a normal subgroup of $\operatorname{Aut}(G)$, what we need to show is that for $f \in \operatorname{Peb}(G)$ and $g \in \operatorname{Aut}(G)$, we have $g \circ f \circ g^{-1} \in \operatorname{Peb}(G)$. Since $1_{G} \sim f$, by Lemma 6, we have $1_{G}=g \circ 1_{G} \circ g^{-1} \sim g \circ f \circ g^{-1}$. Hence, we have $g \circ f \circ g^{-1} \in \operatorname{Peb}(G)$, as required.

## 3 Main Results

It is known that for any finite group $\Gamma$, there exists a graph $G$ such that $\operatorname{Aut}(G) \simeq \Gamma$ (cf. [7]). By using this fact, we have the following result.

Proposition 8 For any finite group $\Gamma$, there exists a graph $G$ such that $\operatorname{Peb}(G) \simeq \Gamma$.

Proof. Let us take a graph $H$ such that $\operatorname{Aut}(H) \simeq \Gamma$. Since at least one of $H$ and $\bar{H}$ is connected, and $\operatorname{Aut}(H) \simeq \operatorname{Aut}(\bar{H})$, by replacing $H$ with $\bar{H}$, if necessary, we may assume $H$ is connected.

Let us build a new graph $H^{\prime}$ from $H$ as follows; $V\left(H^{\prime}\right)=V(H) \cup\left\{x_{u v}^{i}\right.$ : $u v \in E(H), 1 \leq i \leq 3\}, E\left(H^{\prime}\right)=\left\{u x_{u v}^{1}, v x_{u v}^{1}, x_{u v}^{1} x_{u v}^{2}, x_{u v}^{2} x_{u v}^{3}: u v \in E(H)\right\}$. Intuitively, $H^{\prime}$ is obtained by adding a pendant path to the middle of each edge of $H$.

Claim 1. $\operatorname{Aut}\left(H^{\prime}\right) \simeq \operatorname{Aut}(H)$.
For $f \in \operatorname{Aut}(H)$, let us define a bijection $f^{\prime}$ on $V\left(H^{\prime}\right)$ such that $f^{\prime}(v)=f(v)$ for $v \in V(H)$ and $f^{\prime}\left(x_{u v}^{i}\right)=x_{f(u) f(v)}^{i}$. Then we have $f^{\prime} \in \operatorname{Aut}\left(H^{\prime}\right)$, and by this correspondence, we have $\operatorname{Aut}(H) \subset \operatorname{Aut}\left(H^{\prime}\right)$.

Conversely, we will show that $\operatorname{Aut}\left(H^{\prime}\right) \subset \operatorname{Aut}(H)$. Let $g \in \operatorname{Aut}\left(H^{\prime}\right)$. For $u v \in V(H), x_{u v}^{1} x_{u v}^{2} x_{u v}^{3}$, denoted by $P_{u v}$ is a pendant path of length two contained in $H^{\prime}$. Since $H^{\prime}$ contains no pendant path of length two other than $P_{u v}$ for some $u v \in E(H)$, we have $g\left(P_{u v}\right)=P_{g(u) g(v)}$. It follows that an
automorphism $g$ of $H^{\prime}$ restricted on $V(H)$ induces an automorphism of $H$. Therefore, we have $\operatorname{Aut}\left(H^{\prime}\right) \subset \operatorname{Aut}(H)$.

Now, let us consider $G=H^{\prime}+z$ with $n$ vertices, which is the join of $H^{\prime}$ and an additional vertex $z$.
Claim 2. $\operatorname{Aut}(G) \simeq \operatorname{Aut}\left(H^{\prime}\right)$.
For $f \in \operatorname{Aut}\left(H^{\prime}\right)$, let $f^{\prime}$ be a bijection on $V(G)$ such that $f^{\prime}(z)=z$ and $f^{\prime}(v)=f(v)$ for $v \in V\left(H^{\prime}\right)$. Then we have $f^{\prime} \in \operatorname{Aut}(G)$, and by this correspondence, we have $\operatorname{Aut}\left(H^{\prime}\right) \subset \operatorname{Aut}(G)$. Conversely, for $g \in \operatorname{Aut}(G)$, we have $g(z)=z$, because $z$ is the unique vertex of degree $|V(G)|-1$ in $G$. Hence, $g$ restricted on $V\left(H^{\prime}\right)$ induces an automorphism of $H^{\prime}$. Hence, we have $\operatorname{Aut}(G) \subset \operatorname{Aut}\left(H^{\prime}\right)$, as required.

Since $G$ is a non-bipartite 2-connected graph containing $K_{1, n-1}$ as a spanning subgraph, by Theorem $2, \operatorname{Puz}(G)$ is feasible. Therefore, we have $\operatorname{Peb}(G)=\operatorname{Aut}(G)$. Since $\operatorname{Aut}(G) \simeq \operatorname{Aut}\left(H^{\prime}\right) \simeq \operatorname{Aut}(H) \simeq \Gamma$, we have $\operatorname{Peb}(G) \simeq \Gamma$, as required.

Second, we note a simple observation about $\operatorname{Peb}(G)$, where $G$ contains no small cycle. For a graph $G$, the girth of $G$, denoted by $\operatorname{girth}(G)$, is the order of a smallest cycle contained in $G$. If $G$ contains no cycle, $\operatorname{girth}(G)$ is defined as $\infty$. A matching of a graph $G$ is a set of independent edges of $G$. For a matching $M$ of a graph $G$, let $f(M)$ be a configuration of $\operatorname{Puz}(G)$ such that for all $x \in V(M), f(x)=y$, where $x y \in E(M)$, and $f(x)=x$ for all $x \notin V(M)$. Let $\mathcal{M}(G)=\{f(M): M$ is a matching of $G\}$.

Proposition 9 Let $G$ be a connected graph with at least three vertices. If $\operatorname{girth}(G) \geq 5$, then $\operatorname{Peb}(G) \simeq\left\{1_{G}\right\}$.

Proof. It is sufficient to show that if $f \in \mathcal{C}(G) \backslash\left\{1_{G}\right\}$ satisfies $1_{G} \sim f$, then $f$ is not an automorphism of $G$.

Claim. Let $f$ be a configuration of $G$. Then $f \sim 1_{G}$ if and only if $f \in \mathcal{M}(G)$.

First, suppose that $f=f(M) \in \mathcal{M}(G)$, where $M$ is a matching of $G$. Starting from $1_{G}$, by exchanging all pairs of pebbles $u$ and $v$ satisfying $u v \in$ $E(M)$, we have $f(M) \sim 1_{G}$.

Second, suppose that $f \sim 1_{G}$. Let $f_{0}=1_{G}, f_{1}, f_{2}, \ldots, f_{s-1}, f_{s}=f$ be a sequence of configurations, where $f_{i}$ is generated from $f_{i-1}$ by a move for all
$1 \leq i \leq s$. By induction, we may assume $f_{s-1}=f(M) \in \mathcal{M}(G)$. Let us assume we have $f$ from $f_{s-1}$ by a move, in which two pebbles $u$ and $v$ are exchanged. What we need to show is that $f \in \mathcal{M}(G)$.
Case 1. Both $u$ and $v$ are contained in $V(M)$ and $u v \in E(M)$.
In this case, we have $f=f\left(M^{\prime}\right)$, where $M^{\prime}=M \backslash\{u v\}$.
Case 2. Both $u$ and $v$ are contained in $V(M)$ and $u v \notin E(M)$.
Suppose that $u x \in E(M)$ and $v y \in E(M)$. In order to exchange $u=f_{s-1}(x)$ and $v=f_{s-1}(y)$, we have $u v \in E(G)$ and $x y \in E(G)$. Hence, uxyv forms a cycle of length 4 , a contradiction.
Case 3. Exactly one of $u$ and $v$ is contained in $V(M)$.
We may assume $u \in V(M)$ and $v \notin V(M)$. Suppose that $u x \in E(M)$. In order to exchange $u=f_{s-1}(x)$ and $v=f_{s-1}(v)$, we have $u v \in E(G)$ and $v x \in E(G)$. Hence, $u x v$ forms a cycle of length 3, a contradiction.

Case 4. Neither $u$ nor $v$ is contained in $V(M)$.
In this case, we have $f=f\left(M^{\prime}\right)$, where $M^{\prime}=M \cup\{u v\}$. Suppose, for contradiction, that there exists an automorphism $f$ of $G$ with $f \sim 1_{G}$ and $f \neq 1_{G}$. By the above claim, we have a matching $M$ of $G$ such that $f=f(M)$. Since $f \neq 1_{G}$, we have $E(M) \neq \emptyset$. Let $u v \in E(M)$. Because $|V(G)|$ is at least 3 and $G$ is connected, we may assume there exists a vertex $x \in V(G) \backslash\{u, v\}$ such that $u x \in E(G)$. If $x \in V(M)$, there exists an edge $x y \in E(M)$. Since $f$ is an automorphism of $G$, we have $f(u) f(x)=v y \in E(G)$. Hence, uvyx forms a cycle of length 4 , a contradiction. If $x \notin V(M)$, since $f$ is an automorphism of $G$, we have $f(u) f(x)=v x \in E(G)$. Hence, uvx forms a cycle of length 3 , a contradiction.

The next result is about the pebble exchange group of a product of graphs.
For two graphs $G_{1}$ and $G_{2}$, the Cartesian product of $G_{1}$ and $G_{2}$, denoted by $G_{1} \times G_{2}$, is a graph such that its vertices are ordered pairs of elements $\left(x_{1}, x_{2}\right)$, where $x_{i} \in V\left(G_{i}\right)$ for $1 \leq i \leq 2$, and two vertices $\left(x_{1}, x_{2}\right)$ and $\left(y_{1}, y_{2}\right)$ of $G_{1} \times G_{2}$ are adjacent if and only if either $x_{1}=y_{1}$ and $x_{2} y_{2}$ is an edge of $G_{2}$ or $x_{2}=y_{2}$ and $x_{1} y_{1}$ is an edge of $G_{1}$. For two groups $\Gamma_{1}$ and $\Gamma_{2}$, the direct product of $\Gamma_{1}$ and $\Gamma_{2}$, denoted by $\Gamma_{1} \times \Gamma_{2}$, is a group such that its elements are ordered pairs of elements $\left(\alpha_{1}, \alpha_{2}\right)$, where $\alpha_{i} \in \Gamma_{i}$ for $1 \leq i \leq 2$, and its multiplication $\circ$ is defined as $\left(\alpha_{1}, \alpha_{2}\right) \circ\left(\beta_{1}, \beta_{2}\right)=\left(\alpha_{1} \circ_{1} \beta_{1}, \alpha_{2} \circ_{2} \beta_{2}\right)$, where $\circ_{i}$ is the multiplication of $\Gamma_{i}$ for $1 \leq i \leq 2$.

Theorem 10 For any two connected graphs $G_{1}$ and $G_{2}, \operatorname{Peb}\left(G_{1} \times G_{2}\right) \simeq$ $\operatorname{Peb}\left(G_{1}\right) \times \operatorname{Peb}\left(G_{2}\right)$.

The proof of Theorem 10 will be given in Section 3.
Let $Q_{n}$ be the $n$-dimensional hypercubic graph. Since $Q_{n}=P_{2}^{n}$ and $\operatorname{Peb}\left(P_{2}\right) \simeq \mathbb{Z}_{2}$, we have the following corollary as an immediate consequence of Theorem 10.

Corollary 11 For $n \geq 1, \operatorname{Peb}\left(Q_{n}\right) \simeq\left(\mathbb{Z}_{2}\right)^{n}$.

As a graph $G$ becomes sparse, the number of possible moves on $G$ decreases. Hence, it is interesting to show the existence of graphs $G$ such that $\operatorname{Peb}(G)$ has a rich structure and $|E(G)|=O(|V(G)|)$.

For two vertices $u, v$ of a graph $G$, let $d_{G}(u, v)$ denote the distance between $u$ and $v$ in $G$. Furthermore, for two subsets $X, Y$ of the vertex set $V(G)$, let us define $d_{G}(X, Y):=\min \left\{d_{G}(u, v) \mid u \in X, v \in Y\right\}$. We abbreviate $d_{G}(\{u\}, Y)$ (resp. $\left.d_{G}(X,\{v\})\right)$ to $d_{G}(u, Y)$ (resp. $\left.d_{G}(X, v)\right)$.

The square graph $G^{2}$ of $G$ is defined as $V\left(G^{2}\right)=V(G)$ and $E\left(G^{2}\right)=$ $\left\{u v \in V(G)^{2}: d_{G}(u, v)=1\right.$ or 2$\}$.

The main result of the paper is the following theorem.

Theorem 12 For any connected graph $G, \operatorname{Peb}\left(G^{2}\right) \supset \operatorname{Aut}(G)$.

In order to prove Theorem [12, we first deal with the simplest but the most important case, where $G$ is a path.

Lemma 13 For $n \geq 2, \operatorname{Peb}\left(P_{n}^{2}\right) \supset \operatorname{Aut}\left(P_{n}\right)$.
The proof of Lemma 13 will be given in Section 4.
Second, let us introduce a new operation, path flip, for a configuration $f \in \mathcal{C}(G)$. Let $P=v_{0} v_{1} \ldots v_{n}$ be a path of $G$. If $f\left(v_{0}\right) f\left(v_{1}\right) \ldots f\left(v_{n}\right)$ is also a path of $G$, by a path flip, $f$ can be replaced with $g \in \mathcal{C}(G)$ such that $g\left(v_{i}\right)=f\left(v_{n-i}\right)$ for $0 \leq i \leq n$, and $g(x)=f(x)$ for all $x \in V(G) \backslash V(P)$.

The following lemma may be of independent interest apart from pebble exchange puzzles.

Lemma 14 For a connected graph $G$, and for any two configurations $f$, $g \in \operatorname{Aut}(G), f$ can be transformed into $g$ by a finite sequence of path flips.

The proof of Lemma 14 will be given in Section 5.
By Lemma 13, any path flip can be achieved with a sequence of pebble exchanges in $\operatorname{Puz}\left(G^{2}\right)$. Hence, by Lemma 14, Theorem 12 follows.

## 4 Proof of Theorem 10

First, we will show that $\operatorname{Peb}\left(G_{1}\right) \times \operatorname{Peb}\left(G_{2}\right) \subset \operatorname{Peb}\left(G_{1} \times G_{2}\right)$. For $\sigma \in \operatorname{Peb}\left(G_{1}\right)$ and $\tau \in \operatorname{Peb}\left(G_{2}\right)$, it suffices to show that $(\sigma, \tau) \in \operatorname{Peb}\left(G_{1} \times G_{2}\right)$. In the first part of moves, we process a sequence of moves corresponding to $\sigma$ on all copies of $G_{1}$ in parallel. In the second part of moves, we process a sequence of moves corresponding to $\tau$ on all copies of $G_{2}$ in parallel. The sequence of all moves yields $(\sigma, \tau)$.

Second, we will show that $\operatorname{Peb}\left(G_{1} \times G_{2}\right) \subset \operatorname{Peb}\left(G_{1}\right) \times \operatorname{Peb}\left(G_{2}\right)$.
Claim 1. Let $f \in \mathcal{C}\left(G_{1} \times G_{2}\right)$ such that $1_{G_{1} \times G_{2}} \sim f$. For two pebbles $x$ and $y$, if $f^{-1}(x)$ and $f^{-1}(y)$ are in a common copy of $G_{i}$ for some $i=1,2$, then $x$ and $y$ are not in a common copy of $G_{3-i}$.

Suppose, for contradiction, that there exists a pair of pebbles $x$ and $y$ and a configuration $f$ with $1 \sim f$ such that $f^{-1}(x)$ and $f^{-1}(y)$ are in a common copy of $G_{i}$, and $x$ and $y$ are in a common copy of $G_{3-i}$. We may assume that $f$ can be reached from 1 with the minimum number $s$ of moves until at least one of such counterexamples $(x, y)$ occurs. We may assume that $y$ is exchanged with a pebble $z$ in the $s$-th move.

Case 1. $f^{-1}(y)$ and $f^{-1}(z)$ are in a common copy of $G_{3-i}$.
In this case, by the minimality of $s, y$ and $z$ are in a common copy of $G_{3-i}$. Since $x$ and $y$ are in a common copy of $G_{3-i}, x$ and $z$ are in a common copy of $G_{3-i}$. Then the pair $(x, z)$ becomes our counterexample just after the $(s-1)$-th steps. This contradicts the minimality of $s$.

Case 2. $f^{-1}(y)$ and $f^{-1}(z)$ are in a common copy of $G_{i}$.
In this case, the pair $(x, y)$ is already our counterexample after the $(s-1)$-th steps. This contradicts the minimality of $s$.

Claim 2. Let $f$ be an automorphism of $G_{1} \times G_{2}$ such that $1_{G_{1} \times G_{2}} \sim f$. For
two pebbles $x$ and $y$, if $f^{-1}(x)$ and $f^{-1}(y)$ are in a common copy of $G_{i}$ for some $i=1,2$, then $x$ and $y$ are in a common copy of $G_{i}$.
Let us assume that $f^{-1}(x)$ and $f^{-1}(y)$ are in a common copy of $G_{i}$. Since $f$ is an automorphism of $G_{1} \times G_{2}$, there exists a path $P$ from $x$ to $y$ such that a path $f^{-1}(V(P))$ is in a common copy of $G_{i}$. By Claim 1, all pairs of vertices in $V(P)$ are in a mutually different copy of $G_{3-i}$. Hence, any pair of adjacent vertices in $V(P)$ are in a common copy of $G_{i}$. Therefore, $x$ and $y$ are in a common copy of $G_{i}$.

By Claim 2, $f$ induces a permutation $\tilde{\sigma}_{i}$ on the set of all copies of $G_{3-i}$ for $i=1,2$, where $\tilde{\sigma}_{i}$ naturally corresponds to $\sigma_{i} \in \operatorname{Aut}\left(G_{i}\right)$. Then, we have $f=\left(\sigma_{1}, \sigma_{2}\right) \in \operatorname{Aut}\left(G_{1}\right) \times \operatorname{Aut}\left(G_{2}\right)$. Furthermore, by Claim 1, if two pebbles $x$ and $y$ are in a common copy of $G_{i}, x$ and $y$ can be exchanged only if they occupy a common edge of a common copy of $G_{i}$. Hence, we have $\sigma_{i} \in \operatorname{Peb}\left(G_{i}\right)$ for $i=1,2$. Therefore, we have $f \in \operatorname{Peb}\left(G_{1}\right) \times \operatorname{Peb}\left(G_{2}\right)$.

## 5 Proof of Lemma 13

It is not difficult to see that $\operatorname{Puz}\left(P_{n}^{2}\right)$ is feasible for $n \leq 5$. Hence, in this case, we have $\operatorname{Peb}\left(P_{n}^{2}\right)=\operatorname{Aut}\left(P_{n}^{2}\right) \supset \operatorname{Aut}\left(P_{n}\right)$. Suppose that $n \geq 6$. In this case, since $\operatorname{Aut}\left(P_{n}^{2}\right)=\operatorname{Aut}\left(P_{n}\right) \simeq \mathbb{Z}_{2}$, it suffices to prove $\operatorname{Peb}\left(P_{n}^{2}\right) \simeq \mathbb{Z}_{2}$. Let us label the vertices of $P_{n}$ as $V\left(P_{n}\right)=\{1,2, \ldots, n\}$ and $E\left(P_{n}\right)=\{i j$ : $j-i=1\}$. Note that $\operatorname{Aut}\left(P_{n}^{2}\right)=\left\{1_{n}, \alpha_{n}\right\}$, where $1_{n}(i)=i$ for $1 \leq i \leq n$ and $\alpha_{n}(i)=n-i+1$ for $1 \leq i \leq n$. It suffices to show that $1_{n} \sim \alpha_{n}$ in $\operatorname{Puz}\left(P_{n}^{2}\right)$.

In the following, besides $\operatorname{Puz}\left(P_{n}^{2}\right)$, we consider two additional puzzles $\operatorname{Puz}\left(P_{n+1}^{2} \backslash\{n\}, P_{n}^{2}\right)$ and $\operatorname{Puz}\left(P_{n}^{2}, P_{n+1}^{2} \backslash\{n\}\right)$. For configurations $f \in \mathcal{C}\left(P_{n}^{2}, P_{n}^{2}\right)$, $g \in \mathcal{C}\left(P_{n+1}^{2} \backslash\{n\}, P_{n}^{2}\right)$ and $h \in \mathcal{C}\left(P_{n}^{2}, P_{n+1}^{2} \backslash\{n\}\right)$, we will use notations as

$$
\begin{aligned}
f & =(f(1), f(2), \ldots, f(n-1), f(n)), \\
g & =(g(1), g(2), \ldots, g(n-1), *, g(n+1)), \\
h & =(h(1), h(2), \ldots, h(n-1), h(n)) .
\end{aligned}
$$

By using this notation, $1_{n}$ and $\alpha_{n}$ is expressed as

$$
1_{n}=(1,2, \ldots, n-1, n), \quad \alpha_{n}=(n, n-1, \ldots, 2,1) .
$$

Let us define $1_{n}^{\prime}$ and $\beta_{n} \in \mathcal{C}\left(P_{n+1}^{2} \backslash\{n\}, P_{n}^{2}\right)$ as

$$
1_{n}^{\prime}=(1,2, \ldots, n-1, *, n), \quad \beta_{n}=(n, n-1, \ldots, 2, *, 1),
$$

and let us define $1_{n}^{\prime \prime}$ and $\gamma_{n} \in \mathcal{C}\left(P_{n}^{2}, P_{n+1}^{2} \backslash\{n\}\right)$ as

$$
1_{n}^{\prime \prime}=(1,2, \ldots, n-1, n+1), \quad \gamma_{n}=(n+1, n-1, \ldots, 2,1) .
$$

What we want to show is that $1_{n} \sim \alpha_{n}, 1_{n}^{\prime} \sim \beta_{n}, 1_{n}^{\prime \prime} \sim \gamma_{n}$ for all $n \geq 1$. Note that $P_{n+1}^{2} \backslash\{n\}$ is naturally considered as a subgraph of $P_{n}^{2}$. Hence, if $1_{n}^{\prime} \sim \beta_{n}$, by using the same sequence of moves from $1_{n}^{\prime}$ to $\beta_{n}$, we have a sequence of moves from $1_{n}$ to $\alpha_{n}$. Therefore, $1_{n}^{\prime} \sim \beta_{n}$ implies that $1_{n} \sim \alpha_{n}$. Furthermore, $\operatorname{Puz}\left(P_{n+1}^{2} \backslash\{n\}, P_{n}^{2}\right)$ and $\operatorname{Puz}\left(P_{n}^{2}, P_{n+1}^{2} \backslash\{n\}\right)$ are isomorphic as puzzles, since these puzzles can be switched to each other by interchanging the roles of a board graph and a pebble graph, and $1_{n}^{\prime}$ and $\beta_{n}$ are corresponding to $1_{n}^{\prime \prime}$ and $\gamma_{n}$, respectively. Hence, $1_{n}^{\prime} \sim \beta_{n}$ holds if and only if $1_{n}^{\prime \prime} \sim \gamma_{n}$ holds.

We proceed by induction on $n$. For $n \leq 2$, it is not difficult to see that the conclusion holds. Let $n \geq 3$. It suffices to show that $1_{n}^{\prime} \sim \beta_{n}$ by using the inductive assumptions $1_{k} \sim \alpha_{k}, 1_{k}^{\prime} \sim \beta_{k}, 1_{k}^{\prime \prime} \sim \gamma_{k}$ for $2 \leq k \leq n-1$. We have

$$
\begin{aligned}
1_{n}^{\prime} & =(1,2, \ldots, n-2, n-1, *, n) \\
& \sim(1, n, \ldots, 4,3, *, 2) \quad \text { by } 1_{n-1}^{\prime} \sim \beta_{n-1} \\
& \sim(1,3, \ldots, n-1, n, *, 2) \text { by } 1_{n-2} \sim \alpha_{n-2} \\
& \sim(n, n-1, \ldots, 3,1, *, 2) \text { by } 1_{n-1}^{\prime \prime} \sim \gamma_{n-1} \\
& \sim(n, n-1, \ldots, 3,2, *, 1) \text { by the exchange of } 1 \text { and } 2 \\
& =\beta_{n},
\end{aligned}
$$

as required.

## 6 Proof of Lemma 14

In the following, for a configuration $f \in \mathcal{C}(G)$, we say that $f$ is realizable by path flips, if $f$ can be transformed from $1_{G}$ by a finite sequence of path flips. Note that, in general, if two automorphisms $\sigma$ and $\tau$ of $G$ are realizable by path flips, their composition $\tau \circ \sigma$ is also realizable by path flips. (This fact for path flips can be proved in the same way as in the proof of Proposition 7 for pebble exchanges, which are "edge flips", that is, flips of paths of length 1.)

Suppose, for contradiction, that there exists a pair $(G, \sigma)$ of a graph $G$ and an automorphism $\sigma \in \operatorname{Aut}(G)$ such that $\sigma$ is not realizable by path
flips. Note that the order of an automorphism $\sigma \in \operatorname{Aut}(G)$ is the smallest integer $k$ such that $\sigma^{k}=1_{G}$. Let $(G, \sigma)$ be a counterexample such that (1) $|V(G)|$ is minimum, and (2) the order of $\sigma$ is minimum subject to (1). Let $n$ be the order of $\sigma$. First, we claim that $n$ is a prime power. Indeed, if $n$ is not a prime power, there exist two relatively prime integers $r \geq 2$ and $s \geq 2$ with $n=r s$. Since the order of $\sigma^{r}$ is $s<n$ and the order of $\sigma^{s}$ is $r<n$, by the choice of $n$, both $\sigma^{r}$ and $\sigma^{s}$ are realizable by path flips. Since $r$ and $s$ are relatively prime, there exist two positive integers $x$ and $y$ such that $r x+s y \equiv 1(\bmod n)$. Hence, we have $\sigma=\left(\sigma^{r}\right)^{x}\left(\sigma^{s}\right)^{y}$ and so $\sigma$ is also realizable by path flips.

Let $n=p^{\alpha}$, where $p$ is a prime and $\alpha$ is a positive integer. Let $C(\sigma)$ denote the cyclic subgroup of $\operatorname{Aut}(G)$ generated by $\sigma$. If $\sigma^{\prime}$ is another generator of $C(\sigma), \sigma^{\prime}$ is realizable by path flips if and only if $\sigma$ is realizable by path flips. For a vertex $x$ of $G$, let us denote the orbit of $x$ in $C(\sigma)$ by $C(\sigma) \cdot x$. Let us choose a pair ( $\sigma^{\prime}, x$ ), where $\sigma^{\prime}$ is a generator of $C(\sigma)$ and $x$ is a vertex of $G$ such that (1) the distance $d_{G}\left(x, \sigma^{\prime}(x)\right)$ is minimum, and (2) $|C(\sigma) \cdot x|$ is minimum subject to (1).

We redefine $\sigma$ as a chosen element $\sigma^{\prime}$, and put $d=d_{G}(x, \sigma(x))$ and $m=|C(\sigma) \cdot x|$. Note that $m$ is a power of $p$, since $m$ divides $n=p^{\alpha}$. First, we deal with the case, where $d=0$.

Case 1. $d=0$.
In this case, we have $C(\sigma) \cdot x=\{x\}$ and $m=1$. Let $G^{\prime}=G-x$. Then there exists a vertex partition $V\left(G^{\prime}\right)=V_{1} \cup V_{2} \cup \cdots \cup V_{s}$ with a positive integer $s$, where $G\left[V_{i}\right]$ is a connected component of $G^{\prime}$ for all $1 \leq i \leq s$.

Note that if two vertices $u$ and $v$ are contained in a common $V_{i}$ for some $i$, then there exists a $u v$-path $P$ not passing through $x$. Since $\sigma$ is an automorphism with $\sigma(x)=x, \sigma(P)$ is a path not passing through $x$. Hence, $\sigma(u)$ and $\sigma(v)$ are also contained in a common $V_{j}$ for some $j$. Therefore, $\sigma$ induces a permutation $\tilde{\sigma}$ on $\{1, \ldots, s\}$ such that $\sigma\left(V_{i}\right)=V_{\tilde{\sigma}(i)}$ for all $1 \leq i \leq s$. Furthermore, if $j$ is contained in $C(\tilde{\sigma}) \cdot i, G\left[V_{i}\right]$ and $G\left[V_{j}\right]$ are isomorphic to each other.

Let us denote $\tilde{\sigma}$ as a product of transpositions such that $\tilde{\sigma}=\tilde{\sigma}_{t} \circ \cdots \circ \tilde{\sigma}_{2} \circ \tilde{\sigma}_{1}$ with $\tilde{\sigma}_{k}\left(\ell_{k}\right)=m_{k}, \tilde{\sigma}_{k}\left(m_{k}\right)=\ell_{k}$ for some indices $\ell_{k}$ and $m_{k}$ for all $1 \leq k \leq t$. Then we have a sequence of automorphisms $\sigma_{1}, \sigma_{2}, \ldots, \sigma_{t}, \tau$ of $G$ such that $\sigma_{k}\left(V_{\ell_{k}}\right)=V_{m_{k}}, \sigma_{k}\left(V_{m_{k}}\right)=V_{\ell_{k}}, \sigma_{k}^{2}(v)=v$ for $v \in V_{\ell_{k}} \cup V_{m_{k}}$ and $\sigma_{k}(v)=v$ for $v \notin V_{\ell_{k}} \cup V_{m_{k}}$ for $1 \leq k \leq t$, and $\tau\left(V_{i}\right)=V_{i}$ for all $1 \leq i \leq s$. Since $\left.\tau\right|_{G\left[V_{i}\right]}$, i.e. the restriction of $\tau$ to $G\left[V_{i}\right]$, is realizable by path flips for each
$i$ by the inductive hypothesis, $\tau$ is also realizable by path flips. What we need to show is that each $\sigma_{k}$ is realizable by path flips. Hence, it suffices to prove the assertion under the condition where $V\left(G^{\prime}\right)=V_{1} \cup V_{2}, \sigma\left(V_{1}\right)=V_{2}$, $\sigma\left(V_{2}\right)=V_{1}$ and $\sigma^{2}(v)=v$ for all $v \in V\left(G^{\prime}\right)$. In this case, let us take $v_{1} \in V_{1}$ such that $d_{G}\left(x, v_{1}\right)$ is maximum, and let $v_{2}=\sigma\left(v_{1}\right)$. Then we have $v_{i} \in V_{i}$ for $i=1,2, \sigma\left(v_{1}\right)=v_{2}$ and $\sigma\left(v_{2}\right)=v_{1}$.

Let $P$ be a path of $G$ from $v_{1}$ to $v_{2}$, and set a path $P^{\prime}=P \backslash\left\{v_{1}, v_{2}\right\}$. Now, let us flip $P$ with a bijection $\tau$ on $V(G)$, and let us flip $P^{\prime}$ with a bijection $\tau^{\prime}$ on $V(G)$ subsequently. Then we have $\left(\tau^{\prime} \circ \tau\right)\left(v_{i}\right)=v_{3-i}=\sigma\left(v_{i}\right)$ for $1 \leq i \leq 2$, and $\left(\tau^{\prime} \circ \tau\right)(v)=v$ for all $v \notin\left\{v_{1}, v_{2}\right\}$. Set $H=G \backslash\left\{v_{1}, v_{2}\right\}$. Since $\sigma(V(H))=V(H)$, we have $\left.\sigma\right|_{H} \in \operatorname{Aut}(H)$. By the choice of $v_{1}$ and $v_{2}, H$ is connected. Hence, by the inductive hypothesis, $\left.\sigma\right|_{H}$ is realizable by path flips. Therefore, $\sigma$, which is $\left.\sigma\right|_{H} \circ \tau^{\prime} \circ \tau$, is also realizable by path flips, as required.

## Case 2. $d \geq 1$.

Let us take a shortest path $P=y_{0} y_{1} \ldots y_{d-1} \sigma(x)$ from $x$ to $\sigma(x)$, where we set $x=y_{0}$. Let $Y=V(P) \backslash\{\sigma(x)\}$.
Claim 1. If $0 \leq i<j \leq d-1$, then $\sigma^{s}\left(y_{i}\right) \neq \sigma^{t}\left(y_{j}\right)$ for all integers $s$ and $t$.
Suppose, for contradiction, that $\sigma^{s}\left(y_{i}\right)=\sigma^{t}\left(y_{j}\right)$ for some $s$ and $t$. We have $y_{i}=\sigma^{k}\left(y_{j}\right)$, where $k=t-s$. Since $d\left(y_{i}, \sigma^{k}\left(y_{i}\right)\right)=d\left(\sigma^{k}\left(y_{j}\right), \sigma^{k}\left(y_{i}\right)\right)=$ $d\left(y_{j}, y_{i}\right)<d$, by the choice of $d$, $\sigma^{k}$ is not a generator of $C(\sigma)$. Since $C(\sigma)$ is a cyclic group of the order $n=p^{\alpha}$, we have $k \equiv 0(\bmod p)$. Furthermore, we have $d\left(y_{i}, \sigma^{k+1}\left(y_{i}\right)\right)=d\left(\sigma^{k}\left(y_{j}\right), \sigma^{k+1}\left(y_{i}\right)\right)=d\left(y_{j}, \sigma\left(y_{i}\right)\right) \leq d\left(y_{j}, \sigma(x)\right)+$ $d\left(\sigma(x), \sigma\left(y_{i}\right)\right)=d-j+i<d$. Therefore, we have $k+1 \equiv 0(\bmod p)$, a contradiction.
Claim 2. For all $0 \leq i \leq d-1$, if $s \not \equiv t(\bmod m)$, then $\sigma^{s}\left(y_{i}\right) \neq \sigma^{t}\left(y_{i}\right)$.
Suppose, for contradiction, that $\sigma^{s}\left(y_{i}\right)=\sigma^{t}\left(y_{i}\right)$ for some $s$ and $t$ with $s \not \equiv t$ $(\bmod m)$. We have $y_{i}=\sigma^{k}\left(y_{i}\right)$ with some $k \not \equiv 0(\bmod m)$. Since $y_{i}=\sigma^{n}\left(y_{i}\right)$ also holds, we have $\left|C(\sigma) \cdot y_{i}\right| \leq \operatorname{gcd}(k, n)<m$, because $n$ is a power of $p$ and $k \not \equiv 0(\bmod m)$. With the fact $d\left(y_{i}, \sigma\left(y_{i}\right)\right) \leq d$, this contradicts the choice of $x$.

For $0 \leq k \leq m-1$, let us define $X_{k}=\cup_{0 \leq i \leq n-1 ~ a n d ~}^{i \equiv k(\bmod m)} \sigma^{i}(V(P))$, and $X_{k}^{\prime}=X_{k}-\left\{\sigma^{k}(x)\right\}$. Then we have $\sigma\left(X_{k}\right)=X_{k+1}$ for $0 \leq k \leq m-2$, and $\sigma\left(X_{m-1}\right)=X_{0}$. Furthermore, by Claim 1 and Claim 2, $X_{k}^{\prime} \cap X_{\ell}^{\prime}=\emptyset$ for $k \neq \ell$.

Let us define a subgraph $H$ of $G$ such that $V(H)=\cup_{0 \leq k \leq m-1} X_{k}$ and $E(H)=\cup_{0 \leq i \leq n-1}$ and $i \equiv k(\bmod m) \sigma^{i}(E(P))$. Since $\sigma(V(H))=V(H)$ and
$\sigma(E(H))=E(H),\left.\sigma\right|_{H}$ is an automorphism of $H$.
Claim 3. $\left.\sigma\right|_{H}$ is realizable by path flips on $H$.
For $0 \leq k \leq m-1$, let $H_{k}=H\left[X_{k}\right]$. If $m=n$, by definition of $X_{k}$ and $H_{k}$, we have $V\left(H_{k}\right)=X_{k}=\sigma^{k}(V(P))$, and $E\left(H_{k}\right)=\sigma^{k}(E(P))$. Hence, $H_{k}$ is simply a path $\sigma^{k}(P)$ for $0 \leq k \leq m-1$, and $H$ is a cycle. Hence, $\operatorname{Aut}(H)$ is isomorphic to a dihedral group, which is generated by a pair of reflections of cycles. Since a reflection is realizable by a path flip, the claim is proved. In the following, we assume that $m<n$. Let us define a configuration $\tau \in \mathcal{C}(H)$ such that $\tau(v)=\sigma(v)$ for $v \in V(H) \backslash X_{m-1}$ and $\tau(v)=\sigma^{1-m}(v)$ for $v \in X_{m-1}$.

We claim that $\tau$ is an automorphism of $H$, because for $0 \leq k \leq n-1,\left.\sigma\right|_{H_{k}}$ is an isomorphism from $H_{k}$ to $H_{k+1}$ and $\left.\sigma^{1-m}\right|_{H_{m-1}}$ is an isomorphism from $H_{m-1}$ to $H_{0}$. Furthermore, by definition, the order of $\tau$ is $m$. Since $m<n$, by the minimality of $n, \tau$ is realizable by path flips. On the other hand, $\left.\sigma^{m}\right|_{H_{0}}$ is an automorphism of $H_{0}$. Since the order of $\left.\sigma^{m}\right|_{H_{0}}=n / m<n$, by the minimality of $n,\left.\sigma^{m}\right|_{H_{0}}$ is realizable by path flips. Since $\sigma$ is a composition of $\tau$ and $\left.\sigma^{m}\right|_{H_{0}}, \sigma$ is also realizable by path flips.

We may assume $V(G) \backslash V(H) \neq \emptyset$. Choose a vertex $z \in V(G) \backslash V(H)$ such that $d_{G}(z, V(H))$ is maximum. Let $Q$ be a shortest path from $z$ to $V(H)$, and let $y \in V(Q) \cap V(H)$ be the end vertex of $Q$. Then $y$ is contained in $\sigma^{i}(Y)$ for some $i$, where $0 \leq i \leq n-1$. Since we have $d_{G}\left(\sigma^{-i}(z), V(H)\right)$ $=d_{G}\left(z, \sigma^{i}(V(H))\right)=d_{G}(z, V(H))$, by replacing $V(Q)$ with $\sigma^{-i}(V(Q))$ if necessary, we may assume $y$ is contained in $Y$ from the beginning. Let us define a subgraph $F$ of $G$ such that $V(F)=V(H) \cup \cup_{0 \leq i \leq n-1} \sigma^{i}(V(Q))$ and $E(F)=E(H) \cup \cup_{0 \leq i \leq n-1} \sigma^{i}(E(Q))$. Since $\sigma(V(F))=V(F)$ and $\sigma(E(F))=$ $E(F),\left.\sigma\right|_{F}$ is an automorphism of $F$.

Case 2.1. $V(F) \neq V(G)$.
In this case, by the minimality of $|V(G)|,\left.\sigma\right|_{F}$ is realizable by path flips. Let us define two more subgraphs $F^{\prime}=F-C(\sigma) \cdot z$ and $G^{\prime}=G-C(\sigma) \cdot z$. By the maximality of $d_{G}(z, V(H))$, both $F^{\prime}$ and $G^{\prime}$ are connected, and $\sigma\left(V\left(F^{\prime}\right)\right)=$ $V\left(F^{\prime}\right), \sigma\left(V\left(G^{\prime}\right)\right)=V\left(G^{\prime}\right)$. Hence, $\left.\sigma\right|_{F^{\prime}}$ and $\left.\sigma\right|_{G^{\prime}}$ are automorphisms of $F^{\prime}$ and $G^{\prime}$, respectively. Again by the minimality of $|V(G)|,\left.\sigma\right|_{F^{\prime}}$ and $\left.\sigma\right|_{G^{\prime}}$ are realizable by path flips. Since $\sigma$ is a composition of $\left.\sigma\right|_{F},\left.\sigma^{-1}\right|_{F^{\prime}}$ and $\left.\sigma\right|_{G^{\prime}}, \sigma$ is realizable by path flips.
Case 2.2. $V(F)=V(G)$.
For $0 \leq k \leq m-1$, let us define $W_{k}=\cup_{0 \leq i \leq n-1}$ and $i \equiv k(\bmod m) \sigma^{i}(V(Q))$. Note that $W_{k}$ 's are not necessarily disjoint to each other. Let us define a configuration $\tau \in \mathcal{C}(F)$ such that $\tau(v)=\sigma(v)$ for $v \in V(H) \backslash\left(X_{m-1}^{\prime} \cup W_{m-1}\right)$
and $\tau(v)=\sigma^{1-m}(v)$ for $v \in X_{m-1}^{\prime} \cup W_{m-1}$. We need to check that $\tau$ is well-defined. Suppose that there exists a vertex $v \in V(F)$ such that $v \in$ $\left(X_{m-1}^{\prime} \cup W_{m-1}\right) \cap\left(X_{k}^{\prime} \cup W_{k}\right)$ for some $k$ with $0 \leq k \leq m-2$. Suppose that there exists a vertex $v \in V(F)$ such that $v \in\left(X_{m-1}^{\prime} \cup W_{m-1}\right) \cap\left(X_{k}^{\prime} \cup W_{k}\right)$ for some $k$ with $0 \leq k \leq m-2$. Then there exists a positive integer $i$ such that $\sigma^{i}(v)=v$ and $i$ is not divisible by $m$. Let $j$ be a greatest common divisor of $n$ and $i$. Then we have $\sigma^{j}(v)=v$ and $j$ is not divisible by $m$. Since both $j$ and $m$ are divisors of $n$, a prime power, $j$ is a divisor of $m$. Hence, we have $\sigma^{m}(v)=v$, which implies $\sigma(v)=\sigma^{1-m}(v)$.

For $0 \leq k \leq m-1$, let $F_{k}=F\left[X_{k} \cup W_{k}\right]$. We claim that $\tau$ is an automorphism of $F$, because $\left.\sigma\right|_{F_{k}}$ is an isomorphism from $F_{k}$ to $F_{k+1}$ and $\left.\sigma^{1-m}\right|_{F_{m-1}}$ is an isomorphism from $F_{m-1}$ to $F_{0}$. Furthermore, by definition, the order of $\tau$ is $m$.

Case 2.2.1. $m<n$.
In this case, by the minimality of $n, \tau$ is realizable by path flips. Furthermore, $\left.\sigma^{m}\right|_{F_{0}}$ is an automorphism of $F_{0}$ and the order of $\left.\sigma^{m}\right|_{F_{0}}$ is $n / m$, which is less than $n$. Hence, by the minimality of $n,\left.\sigma^{m}\right|_{F_{0}}$ is realizable by path flips. Since $\sigma$ is a composition of $\tau$ and $\left.\sigma^{m}\right|_{F_{0}}, \sigma$ is realizable by path flips.
Case 2.2.2. $m=n$.
In this case, $H$ is a cycle of order $d n$. Put $r=d n$. We relabel the vertices of $F$ as follows: let us label $V(Q)$ as $Q=w_{0} w_{1} \ldots w_{s}$, where $w_{0}=z$ and $w_{s}=y$. For $0 \leq i \leq n-1$ and $0 \leq j \leq s$, let $w_{i, j}=\sigma^{i}\left(w_{j}\right)$. Note that $w_{i, j}$ may coincide with $w_{k, j}$ for some $i \neq k$. We also write $Q_{i}=w_{i, 0} w_{i, 1} \ldots w_{i, s}$ for $0 \leq i \leq n-1$. Let us label the vertices of $H$, which is a cycle of length $r$, as $H=z_{0} z_{1} \ldots z_{r}$, where $z_{r}=z_{0}$ and $z_{i d}=w_{i, s}$ for $0 \leq i \leq n-1$.

For a positive integer $N$ and for an integer $t$, let us define permutations $\pi(N, t)$ on $\{0,1, \ldots, N-1\}$ such that $\pi(N, t)(i) \equiv t-i(\bmod N)$ for $0 \leq$ $i \leq N-1$. For an integer $t$, let us define a bijection $\rho_{t}$ on $V(F)$ satisfying $\rho_{t}^{2}=1$, as follows:

$$
\rho_{t}\left(w_{i, j}\right)=w_{\pi(n, t)(i), j} \text { for } 0 \leq i \leq n-1 \text { and } 0 \leq j \leq s, \text { and } \rho_{t}\left(z_{i}\right)=z_{\pi(r, d t)(i)}
$$ for $0 \leq i \leq r-1$.

We need to check that $\rho_{t}$ is well-defined. If $w_{i, j}=w_{k, j}$ for some $i, k, j$ with $i \neq k$, we have $\sigma^{i}\left(w_{j}\right)=\sigma^{k}\left(w_{j}\right)$. For any integer $t$, since $\pi(n, t)(k)-$ $\pi(n, t)(i) \equiv i-k(\bmod n)$, we have $w_{\pi(n, t)(i), j}=\sigma^{\pi(n, t)(i)}\left(w_{j}\right)=\sigma^{\pi(n, t)(k)}\left(w_{j}\right)=$ $w_{\pi(n, t)(k), j}$, as claimed.

Let $H^{\prime}=F\left[\cup_{0 \leq i \leq n-1} Q_{i}\right]$. Since $\left.\rho_{t}\right|_{V\left(H^{\prime}\right)}$ is a permutation of $Q_{i}$ for $0 \leq$
$i \leq n-1$ and $\left.\rho_{t}\right|_{V(H)}$ is a reflection of $H, \rho_{t}$ is an automorphism of $F$.
Claim 4. $\rho_{t}$ is realizable by path flips on $F$.
For all $0 \leq i \leq n-1$ with $i<\pi(n, t)(i)$, let us choose a shortest path $R_{i}$ from $w_{i, 0}$ to $\rho_{t}\left(w_{i, 0}\right)=w_{\pi(n, t)(i), 0}$. By consecutive path flips of $R_{i}$ and $R_{i}-\left\{w_{i, 0}, \rho_{t}\left(w_{i, 0}\right)\right\}$, we can exchange $w_{i, 0}$ and $\rho_{t}\left(w_{i, 0}\right)$ for $0 \leq i \leq n-1$. In the remaining graph $F^{\prime}=F-C(\sigma) \cdot w_{0},\left.\rho\right|_{F^{\prime}}$ is realizable by path flips by the minimality of $|V(G)|$, as claimed.

Since $\sigma$ is a composition of $\rho_{1}$ and $\rho_{0}$, by Claim 4, it is realizable by path flips.

## References

[1] A. Archer, A modern treatment of the 15 puzzle, American Math. Monthly 106 (1999), 793-799.
[2] V. Auletta, A. Monti, M. Parente, and P. Persiano, A linear-time algorithm for the feasibility of pebble motion in trees, Algorithmica 23 (1999), 223-245.
[3] G. Calinescu, A. Dumitrescu, and J. Pach, Reconfigurations in Graphs and Grids, SIAM J. Discrete Math. 22 (2008), 124-138.
[4] A. Fink, R. Guy, Rick's tricky six puzzle: $S_{5}$ sits specially in $S_{6}$, Math. Magazine 82 (2009), 83-102.
[5] S. Fujita, T. Nakamigawa, and T. Sakuma, Colored Pebble Motion on Graphs, European J. of Combin. 33 (2012), 884-892.
[6] S. Fujita, T. Nakamigawa, and T. Sakuma, Pebble Exchange on Graphs, Disc. Appl. Math. 184 (2015), 281-287.
[7] R. Frucht, Graphs of degree three with a given abstract group, Canad. J. Math. 1 (1949), 365-378.
[8] W. W. Johnson, Notes on the 15 puzzle. I., American J. Math. 2 (1879), 397-399.
[9] D. Kohnhauser, G. Miller, and P. Spirakis, Coordinating pebble motion on graphs, the diameter of permutation groups, and applications, Proceedings of the 25 -th Symposium on Foundations of Computer Science, (FOCS '84), 241-250.
[10] S. Loyd, Mathematical Puzzles of Sam Loyd, Dover, New York, 1959.
[11] C. Papadimitriou, P. Raghavan, M. Sudan, and H. Tamaki, Motion planning on a graph, Proceedings of the 35 -th Symposium on Foundations of Computer Science, (FOCS '94), 511-520.
[12] D. Ratner and M. Warmuth, Finding a shortest solution for the $(N \times$ $N$ )-extension of the 15 -puzzle is intractable, J. Symbolic Computation 10 (1990), 111-137.
[13] W. E. Story, Notes on the 15 puzzle. II., American J. Math. 2 (1879), 399-404.
[14] R. M. Wilson, Graph puzzles, homotopy, and the alternating group, J. Combin. Theory Ser. B 16 (1974), 86-96.


[^0]:    ${ }^{1}$ Email: tatsuoki-k@jm.kj.yamagata-u.ac.jp
    ${ }^{2}$ This work was supported by JSPS KAKENHI Grant Number JP16K05260.
    Email: nakami@info.shonan-it.ac.jp
    ${ }^{3}$ This work was supported by JSPS KAKENHI Grant Number JP16K05260, JP26400185, JP18K03388.
    Email: sakuma@sci.kj.yamagata-u.ac.jp

