Algebraic Structures and Their Applications Vol. 8 No. 2 (2021) pp 131-143.

Research Paper

AN ALGORITHM FOR FINDING MINIMAL GENERATING SETS OF FINITE GROUPS[†]

TANAKORN UDOMWORARAT AND TEERAPONG SUKSUMRAN*

Abstract. In this article, we study connections between components of the Cayley graph $\mathrm{Cay}(G, A)$, where A is an arbitrary subset of a group G, and cosets of the subgroup of G generated by A. In particular, we show how to construct generating sets of G if $\mathrm{Cay}(G, A)$ has finitely many components. Furthermore, we provide an algorithm for finding minimal generating sets of finite groups using their Cayley graphs.

1. Introduction

The problem of determining (minimal) generating sets of groups has been studied widely; see, for instance, [2, 4, 6, 15, 18–20]. Although the existence of a generating set of a certain group is known, it might be a difficult task to explore it. In fact, there is no general effective

DOI: 10.29252/as.2021.2029

MSC(2010): Primary 05C25; Secondary 20F05, 20D99.

Keywords: Cayley graph, Connected graph, Coset, Generating set, Graph component.

Received: 05 December 2020, Accepted: 24 March 2021.

[†]Part of this work was presented at the conference *Semigroups and Groups, Automata, Logics* (SandGAL 2019), Cremona, Italy, June 10-13, 2019.

*Corresponding author.

method to determine a generating set of a given group. From a complexity point of view, MIN-GEN—finding a minimum size generating set—for groups is in DSPACE$(\log^2 n)$; see Proposition 3 of [1].

Cayley graphs prove useful in studying various mathematical structures [3,8–10,12,16,17,21] and have many applications in several fields [7, 11, 14, 22, 23]. It is clear that a Cayley graph of any group G encodes a large amount of information about algebraic, combinatorial, and geometric structures of G. In addition, Cayley graphs allow us to visualize groups and then to examine properties of groups in a convenient way. Often, a Cayley graph of a (finite) group G relative to A is drawn with the condition that A be a generating set of G (and even if $A = A^{-1}$; e.g. in geometric group theory). In this case, the Cayley graph is strongly connected. In fact, it is a standard result in the literature that a Cayley graph $\mathrm{Cay}\,(G, A)$ is connected if and only if A generates G. In the present article, we investigate Cayley graphs in a more general setting by relaxing the requirement that A be a generating set of G. In particular, we count the number of components of a Cayley graph in terms of the index of a subgroup. As a consequence of this result, we are able to construct a generating set of a certain group whenever its Cayley graph has finitely many components. This leads to an algorithm for finding some minimal generating sets of finite groups. We remark that some results presented in the next section are known in algebraic graph theory; see, for instance, [9, Lemma 5.1], [13, p.1], and [16, pp. 302–303].

2. Main results

2.1. **Definitions and basic properties.** Let $G = (V, E)$ be a graph. The equivalence relation $\mathfrak{p}$ on V is defined by $u\,\mathfrak{p}\,v$ if and only if either $u = v$ or there is a path from u to v in G. We say that C is a component of G if and only if there is an equivalence class X of the relation $\mathfrak{p}$ such that C is the subgraph of G induced by X, that is, $C = G[X]$. Note that $u\,\mathfrak{p}\,v$ if and only if u and v are in the same component of G.

Let G be a (finite or infinite) group and let A be an arbitrary subset of G. Recall that the *Cayley digraph* of G with respect to A, denoted by $\overrightarrow{\mathrm{Cay}}\,(G, A)$, is a directed graph with the vertex set G and the arc set $\{(g, ga) \colon g \in G, a \in A \text{ and } a \neq e\}$. Remark that we exclude the identity e in order to avoid loops in Cayley digraphs. The (undirected) *Cayley graph* of G with respect to A, denoted by $\mathrm{Cay}\,(G, A)$, is defined as a graph with the vertex set G such that $\{u, v\}$ is an edge if and only if $u = va$ or $v = ua$ for some $a \in A \setminus \{e\}$. It is not difficult to check that $\mathrm{Cay}\,(G, A)$ is the underlying graph of $\overrightarrow{\mathrm{Cay}}\,(G, A)$; that is, the vertex sets of $\mathrm{Cay}\,(G, A)$ and $\overrightarrow{\mathrm{Cay}}\,(G, A)$ coincide and $\{u, v\}$ is an edge in $\mathrm{Cay}\,(G, A)$ if and only if (u, v) or (v, u) is an arc in $\overrightarrow{\mathrm{Cay}}\,(G, A)$. To nonidentity elements of A, we can associate distinct colors, labeled by their names. The *Cayley color digraph* of G with respect to A, denoted by $\overrightarrow{\mathrm{Cay}}_c\,(G, A)$, consists of the digraph $\overrightarrow{\mathrm{Cay}}\,(G, A)$ in which any arc (g, ga) is given color a for all $a \in A \setminus \{e\}$.

Next, we mention some basic properties of Cayley graphs and Cayley digraphs.

Theorem 2.1. *Let G be a group and let A be a finite subset of G. Then*

$$\operatorname{indeg} v = \operatorname{outdeg} v = \begin{cases} |A| & \text{if } e \notin A; \\ |A| - 1 & \text{if } e \in A \end{cases}$$

for all vertices v in $\overrightarrow{\mathrm{Cay}}\,(G, A)$. Therefore, $\overrightarrow{\mathrm{Cay}}\,(G, A)$ is regular.

Proof. Note that $va = vb$ if and only if $a = b$ for all $u, v \in G, a, b \in A$. In the case when $e \notin A$, we obtain

$$\operatorname{outdeg} v = |\{va : a \in A\}| = |A|$$

and

$$\operatorname{indeg} v = |\{va^{-1} : a \in A\}| = |\{a^{-1} : a \in A\}| = |A|.$$

In the case when $e \in A$, we obtain

$$\operatorname{outdeg} v = |\{va : a \in A - \{e\}\}| = |A - \{e\}| = |A| - 1$$

and

$$\operatorname{indeg} v = |\{va^{-1} : a \in A - \{e\}\}| = |\{a^{-1} : a \in A - \{e\}\}| = |A - \{e\}| = |A| - 1.$$

□

Theorem 2.2. *Let G be a group and let A be a finite subset of G not containing e. Then*

$$\deg v = 2|A| - |A \cap A^{-1}|, \tag{2.1}$$

where $A^{-1} = \{a^{-1} : a \in A\}$, for all vertices v in $\mathrm{Cay}\,(G, A)$. Therefore, $\mathrm{Cay}\,(G, A)$ is regular.

Proof. Suppose that $vA = \{va : a \in A\}$ and $vA^{-1} = \{va^{-1} : a \in A\}$. Then $vA \cap vA^{-1} = v(A \cap A^{-1})$. Note that

$$\begin{aligned} \{u, v\} \in E(\mathrm{Cay}\,(G, A)) \quad &\Leftrightarrow \quad (u, v) \in E(\overrightarrow{\mathrm{Cay}}\,(G, A)) \text{ or } (v, u) \in E(\overrightarrow{\mathrm{Cay}}\,(G, A)) \\ &\Leftrightarrow \quad u = va^{-1} \text{ for some } a \in A \text{ or } u = va \text{ for some } a \in A. \end{aligned}$$

Hence,

$$\begin{aligned}\deg v &= |\{u \in G : \{u, v\} \in E(\mathrm{Cay}\,(G, A))\}|\\ &= |vA \cup vA^{-1}|\\ &= |vA| + |vA^{-1}| - |vA \cap vA^{-1}|\\ &= |vA| + |vA^{-1}| - |v(A \cap A^{-1})|\\ &= 2|A| - |A \cap A^{-1}|.\end{aligned}$$

□

The following lemma gives a characterization of the existence of paths in Cayley graphs, which is quite well known in the literature.

Lemma 2.3 (See, e.g., Lemma 5.1 of [9]). *Let g and h be distinct elements in a group G and let $A \subseteq G$. Then there is a path from g to h in* $\mathrm{Cay}\,(G, A)$ *if and only if $g^{-1}h = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ for some $a_1, a_2, \ldots, a_n \in A$, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{\pm 1\}$.*

2.2. **Components of Cayley graphs and Cayley digraphs.** In what follows, if A is a subset of a group G, then $\langle A \rangle$ denotes the subgroup of G generated by A. That is, $\langle A \rangle$ is the smallest subgroup of G containing A. Henceforward, A is a subset of a (finite or infinite) group G unless stated otherwise.

An equivalence class of the relation $\mathfrak{p}$ induced by the Cayley graph $\mathrm{Cay}\,(G, A)$, defined in the beginning of Section 2.1, turns out to be a coset of $\langle A \rangle$ in G, as shown in the following theorem.

Theorem 2.4. *Let $u, v \in G$. Then u and v are in the same coset of $\langle A \rangle$ in G if and only if $u \,\mathfrak{p}\, v$, where $\mathfrak{p}$ is the equivalence relation induced by* $\mathrm{Cay}\,(G, A)$.

Proof. ($\Rightarrow$) Let X be a coset of $\langle A \rangle$ in G. Then $X = g\langle A \rangle$ for some $g \in G$. Let $u, v \in X$. Then $u = g a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ and $v = g b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$, where $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in A$ and $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n, \delta_1, \delta_2, \ldots, \delta_m \in \{\pm 1\}$. In the case when $u \neq v$,

$$u^{-1}v = a_n^{-\varepsilon_n} \cdots a_2^{-\varepsilon_2} a_1^{-\varepsilon_1} b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$$

implies that there is a path from u to v by Lemma 2.3. Thus $u \,\mathfrak{p}\, v$.

($\Leftarrow$) Let $u, v \in G$ and suppose that $u \,\mathfrak{p}\, v$. If there exists a path from u to v in $\mathrm{Cay}\,(G, A)$, then $u^{-1}v = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$, where $a_1, a_2, \ldots, a_n \in A, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{\pm 1\}$. Suppose that $u \in g\langle A \rangle$ for some $g \in G$. Then $u = g b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$ with $b_1, b_2, \ldots, b_m \in A$, $\delta_1, \delta_2, \ldots, \delta_m \in \{\pm 1\}$. Thus $v = g b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m} a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \in g\langle A \rangle$. □

Corollary 2.5. *Let $X \subseteq G$. Then X is an equivalence class of the relation $\mathfrak{p}$ induced by* $\mathrm{Cay}\,(G, A)$ *if and only if X is a coset of $\langle A\rangle$ in G.*

Corollary 2.6. *Let G be a group and let $A \subseteq G$.*

(1) *C is a component of* $\mathrm{Cay}\,(G, A)$ *if and only if there is a unique coset X of $\langle A\rangle$ such that* $C = \mathrm{Cay}\,(G, A)[X]$.

(2) *C is a component of* $\overrightarrow{\mathrm{Cay}}\,(G, A)$ *if and only if there is a unique coset X of $\langle A\rangle$ such that* $C = \overrightarrow{\mathrm{Cay}}\,(G, A)[X]$.

In general, finding the subgroup of G generated by A might be a complicated and tedious task. Corollary 2.6 enables us to find this subgroup by looking at the component of $\mathrm{Cay}\,(G, A)$ that contains the identity of G (see Theorem 2.7). Furthermore, it indicates that another component of $\mathrm{Cay}\,(G, A)$ is simply a left translation of the identity component (see the proof of Theorem 2.8). We remark that part of Corollary 2.6 (1) is known in the literature; see, for instance, [13, p. 1].

Theorem 2.7. *The subgroup $\langle A\rangle$ is equal to the set of vertices in the component of* $\mathrm{Cay}\,(G, A)$ *containing the identity of G. In general, C is a component of* $\mathrm{Cay}\,(G, A)$ *containing a vertex v if and only if the vertex set of C equals $v\langle A\rangle$.*

Proof. Let C be the component of $\mathrm{Cay}\,(G, A)$ containing the identity of G. By Corollary 2.6, $C = \mathrm{Cay}\,(G, A)[g\langle A\rangle]$ for some $g \in G$. Since C contains the identity of G, that is, $e \in g\langle A\rangle$, it follows that $g \in \langle A\rangle$ and so $g\langle A\rangle = \langle A\rangle$. The remaining statement can be proved in a similar fashion. □

Theorem 2.8. *If B and C are components of* $\mathrm{Cay}\,(G, A)$*, then B and C are isomorphic as graphs.*

Proof. Suppose that B and C are components of $\mathrm{Cay}\,(G, A)$. From Corollary 2.6, we obtain $B = \mathrm{Cay}\,(G, A)[g_1\langle A\rangle]$ and $C = \mathrm{Cay}\,(G, A)[g_2\langle A\rangle]$ for some $g_1, g_2 \in G$. Let φ be a map defined by $\varphi(x) = g_2 g_1^{-1} x$ for all $x \in g_1\langle A\rangle$. It is straightforward to check that φ is a graph isomorphism from B to C. So B and C are isomorphic. □

Another application of Corollary 2.6 reveals a geometric aspect of Cayley digraphs and Cayley graphs: they are disjoint unions of smaller Cayley digraphs (or graphs).

Theorem 2.9. *Let G be a group and let $A \subseteq G$. If $C_i, i \in I$, are all the components of* $\overrightarrow{\mathrm{Cay}}\,(G, A)$ *and if v_i is a vertex in C_i for all $i \in I$, then*

$$\overrightarrow{\mathrm{Cay}}\,(G, A) = \dot{\bigcup_{i\in I}} \overrightarrow{\mathrm{Cay}}\,(G, A)[v_i\langle A\rangle],$$

where the dot notation indicates that the union is disjoint.

Corollary 2.10. *Let G be a group and let $A \subseteq G$. If $C_i, i \in I$, are all the components of* $\mathrm{Cay}\,(G, A)$ *and if v_i is a vertex in C_i for all $i \in I$, then*

$$\mathrm{Cay}\,(G, A) = \dot{\bigcup_{i\in I}} \mathrm{Cay}\,(G, A)[v_i\langle A\rangle].$$

Next, we show that the number of components of $\mathrm{Cay}\,(G, A)$ is indeed the number of cosets of $\langle A\rangle$ in G. This result refines the well known fact that the Cayley graph $\mathrm{Cay}\,(G, A)$ is connected if and only if A generates G.

Lemma 2.11. *The numbers of components of* $\mathrm{Cay}\,(G, A)$ *and* $\mathrm{Cay}\,(G, \langle A\rangle)$ *are equal.*

Proof. Set $E = \{X : X \text{ is a coset of } \langle A\rangle\}$, $S = \{C : C \text{ is a component of } \mathrm{Cay}\,(G, A)\}$, and $T = \{C : C \text{ is a component of } \mathrm{Cay}\,(G, \langle A\rangle)\}$. By Corollary 2.6, $|S| = |E| = |T|$. □

Theorem 2.12. *The number of components of* $\mathrm{Cay}\,(G, A)$ *equals $[G : \langle A\rangle]$, the index of $\langle A\rangle$ in G.*

Proof. The theorem follows directly from Corollary 2.6 and Lemma 2.11. □

As a consequence of Theorem 2.12, we immediately obtain a few properties of Cayley graphs related to algebraic properties of groups.

Corollary 2.13. *If G is a finite group, then the number of components of* $\mathrm{Cay}\,(G, A)$ *divides* $|G|$.

Proof. This follows from Theorem 2.12 and the fact that $[G : \langle A\rangle]$ divides $|G|$. □

Corollary 2.14. *The Cayley graph* $\mathrm{Cay}\,(G, A)$ *is connected if and only if $G = \langle A\rangle$.*

Proof. This follows from the fact that $[G : \langle A\rangle] = 1$ if and only if $\langle A\rangle = G$. □

Corollary 2.15. *Let G be a group. Then G is cyclic if and only if there exists an element $a \in G$ such that* $\mathrm{Cay}\,(G, \{a\})$ *is connected.*

Among other things, we obtain a graph-theoretic version of the famous Lagrange theorem in abstract algebra, as shown in the following theorem.

Theorem 2.16. *Let G be a group and let H be a subgroup of G. Then the following hold:*

(1) *Each component of* $\mathrm{Cay}\,(G, H)$ *has a left coset of* H *as its vertex set and is the complete graph* $K_{|H|}$*. In particular, there is a one-to-one correspondence between the vertex sets of components of* $\mathrm{Cay}\,(G, H)$ *and the left cosets of* H *in* G*.*

(2) *The Cayley graph* $\mathrm{Cay}\,(G, H)$ *has* $[G\colon H]$ *components. Hence, if* H *is proper in* G*, then* $\mathrm{Cay}\,(G, H)$ *is disconnected.*

In view of Theorem 2.16, the index formula $|G| = [G\colon H]|H|$ can be recovered by counting the number of vertices of $\mathrm{Cay}\,(G, H)$ in the case when G is finite. Moreover, a simple application of Theorem 2.16 shows that 2 always divides $|G|(|H| - 1)$ for any subgroup H of a finite group G. In fact, the result is trivial when $H = \{e\}$. Therefore, we assume that $H \neq \{e\}$. Let C be a component of $\mathrm{Cay}\,(G, H)$. Then C is the complete graph $K_{|H|}$ and so there are $\binom{|H|}{2} = \frac{|H|(|H|-1)}{2}$ edges in C. Hence, the total number of edges in $\mathrm{Cay}\,(G, H)$ equals

$$\frac{|H|(|H| - 1)}{2}[G\colon H] = \frac{|G|(|H| - 1)}{2}.$$

This shows that $\frac{|G|(|H|-1)}{2}$ must be an integer.

The next theorem shows how to construct a generating set of G from an arbitrary subset A of G whenever $\mathrm{Cay}\,(G, A)$ has a finite number of components (e.g., G is finite or G has a subgroup of finite index).

Theorem 2.17. *If* $\mathrm{Cay}\,(G, A)$ *has finitely many components* $C_1, C_2, \ldots, C_k$ *and if* v_i *is a vertex in* C_i *for all* $i = 1, 2, \ldots, k$*, then*

$$S_1 = A \cup \{v_1^{-1}v_2, v_2^{-1}v_3, \ldots, v_{k-1}^{-1}v_k\} \quad \textit{and} \quad S_2 = A \cup \{v_1^{-1}v_2, v_1^{-1}v_3, \ldots, v_1^{-1}v_k\}$$

form generating sets of G*.*

Proof. First, we will show that $\mathrm{Cay}\,(G, S_1)$ is connected. Let u and v be distinct vertices in $\mathrm{Cay}\,(G, S_1)$. If u and v are in the same component of $\mathrm{Cay}\,(G, A)$, then there is a path from u to v in $\mathrm{Cay}\,(G, A)$. Since $\mathrm{Cay}\,(G, A)$ is a subgraph of $\mathrm{Cay}\,(G, S_1)$, there is a path from u to v in $\mathrm{Cay}\,(G, S_1)$. Therefore, we may suppose that u and v are in distinct components of $\mathrm{Cay}\,(G, A)$, namely the i^{th} and j^{th} components, respectively. Hence, $u\,\mathfrak{p}_1\,v_i$ and $v\,\mathfrak{p}_1\,v_j$, where $\mathfrak{p}_1$ is the equivalence relation induced by $\mathrm{Cay}\,(G, A)$. It follows that $u\,\mathfrak{p}_2\,v_i$ and $v\,\mathfrak{p}_2\,v_j$, where $\mathfrak{p}_2$ is the equivalence relation induced by $\mathrm{Cay}\,(G, S_1)$. Since $v_{i+1} = v_i(v_i^{-1}v_{i+1})$ and $v_i^{-1}v_{i+1} \neq e$ for all $i = 1, 2, \ldots, k-1$, we obtain that $\{v_i, v_{i+1}\}$ is an edge in $\mathrm{Cay}\,(G, S_1)$ for all $i = 1, 2, \ldots, k-1$. This implies that $v_i\,\mathfrak{p}_2\,v_j$. By symmetry and transitivity, $u\,\mathfrak{p}_2\,v$ and so there is a path from u to v in $\mathrm{Cay}\,(G, S_1)$. Thus $\mathrm{Cay}\,(G, S_1)$ is connected. The verification that S_2 is a generating set of G is similar to the case of S_1. $\square$

Theorem 2.18. *Let A be a finite subset of a group G not containing e. If* $\mathrm{Cay}\,(G, A)$ *has k components, where $k \in \mathbb{N}$, then G is generated by $|A| + k - 1$ elements and so*

$$\mathrm{rank}(G) \leq |A| + k - 1.$$

Proof. Let S_2 be the set defined in Theorem 2.17. We claim that $|S_2| = |A| + k - 1$. Let $B = \{v_1^{-1}v_2, v_1^{-1}v_3, \ldots, v_1^{-1}v_k\}$. By the left cancellation law, the elements in B are all distinct. So $|B| = k-1$. Next, we show that $A \cap B = \emptyset$. If there is an element $a \in A \cap B$, then $a = v_1^{-1}v_i$ for some $i \in \{2, 3, \ldots, k\}$. Since $v_i = v_1(v_1^{-1}v_i) = v_1 a$ and $a \in A \setminus \{e\}$, there is an edge from v_1 to v_i, a contradiction. Thus $A \cap B = \emptyset$. Hence,

$$|S_2| = |A \cup B| = |A| + |B| - |A \cap B| = |A| + k - 1.$$

By Theorem 2.17, G is generated by S_2. By definition,

$$\mathrm{rank}(G) = \min\{|X| \colon X \subseteq G \text{ and } \langle X \rangle = G\} \leq |A| + k - 1,$$

which completes the proof. □

Corollary 2.19. *Let G be a group and let $a \in G \setminus \{e\}$. If* $\mathrm{Cay}\,(G, \{a\})$ *has k components, where $k \in \mathbb{N}$, then G is generated by k elements and so* $\mathrm{rank}(G) \leq k$.

3. An application to finding minimal generating sets

A generating set A of a (finite or infinite) group G is *minimal* if no proper subset of A generates G. It is clear that any finitely generated group has a minimal generating set, but finding one is quite difficult in certain circumstances. In this section, we provide an algorithm for finding minimal generating sets of finite groups as an application of Theorem 2.17. Let G be a finite group. A formal presentation of this algorithm is as follows.

(1) Set $A := \{a_1\}$, where $a_1 \in G$ and $a_1 \neq e$.
(2) Set $v_1 := a_1, i := 1$.
(3) Draw $\mathrm{Cay}\,(G, A)$.
(4) If $\mathrm{Cay}\,(G, A)$ is connected, skip to step (7). Otherwise, set $i := i + 1$ and $v_2 := b_i$, where b_i is an element of G not in the component of v_1.
(5) Set $a_i := v_1^{-1}v_2$ and $A := A \cup \{a_i\}$.
(6) Return to step (3).
(7) If $i = 1$, stop. Otherwise, set $i := i - 1$.
(8) Draw $\mathrm{Cay}\,(G, A\backslash\{a_i\})$.
(9) If $\mathrm{Cay}\,(G, A\backslash\{a_i\})$ is connected, set $A := A\backslash\{a_i\}$. Otherwise, go to step (10).
(10) Return to step (7).

Theorem 2.17 ensures that this algorithm must stop at some point and turns A into a minimal generating set of G. We illustrate how this algorithm works in the next example.

Example 3.1. Let G be the group defined by presentation

$$G = \langle a, b, c \colon a^2 = b^2 = (ab)^2 = c^3 = acabc^{-1} = abcbc^{-1} \rangle. \tag{3.1}$$

Its Cayley table is given by Table 1 (cf. [5]).

$\cdot$	e	a	b	ab	c	ac	bc	abc	cc	acc	bcc	$abcc$
e	e	a	b	ab	c	ac	bc	abc	cc	acc	bcc	$abcc$
a	a	e	ab	b	ac	c	abc	bc	acc	cc	$abcc$	bcc
b	b	ab	e	a	bc	abc	c	ac	bcc	$abcc$	cc	acc
ab	ab	b	a	e	abc	bc	ac	c	$abcc$	bcc	acc	cc
c	c	bc	abc	ac	cc	bcc	$abcc$	acc	e	b	ab	a
ac	ac	abc	bc	c	acc	$abcc$	bcc	cc	a	ab	b	e
bc	bc	c	ac	abc	bcc	cc	acc	$abcc$	b	e	a	ab
abc	abc	ac	c	bc	$abcc$	acc	cc	bcc	ab	a	e	b
cc	cc	$abcc$	acc	bcc	e	ab	a	b	c	abc	ac	bc
acc	acc	bcc	cc	$abcc$	a	b	e	ab	ac	bc	c	abc
bcc	bcc	acc	$abcc$	cc	b	a	ab	e	bc	ac	abc	c
$abcc$	$abcc$	cc	bcc	acc	ab	e	b	a	abc	c	bc	ac

TABLE 1. Cayley table of the group G defined by (3.1) (cf. [5]).

We can use the algorithm mentioned previously to find a minimal generating set of G as follows:

(1) Set $A := \{b\}$.
(2) Set $v_1 := b, i := 1$.
(3) Draw Cay $(G, \{b\})$, as shown in Figure 1.
(4) Since Cay $(G, \{b\})$ is not connected, set $i := 2$ and $v_2 := ab$.
(5) Set $a_2 := b^{-1}(ab) = a$ and $A := \{b, a\}$.
(6) Draw Cay $(G, \{b, a\})$, as shown in Figure 2.
(7) Since Cay $(G, \{b, a\})$ is not connected, set $i := 3$ and $v_2 := bc$.
(8) Set $a_3 := b^{-1}(bc) = c$ and $A := \{b, a, c\}$.
(9) Draw Cay $(G, \{b, a, c\})$, as shown in Figure 3.
(10) Since Cay $(G, \{b, a, c\})$ is connected and $i = 3$, set $i := 2$.
(11) Draw Cay $(G, \{b, c\})$, as shown in Figure 4.

(12) Since Cay $(G, \{b, c\})$ is connected, set $A := \{b, c\}$.

(13) Since $i = 2$, set $i := 1$.

(14) Draw Cay $(G, \{c\})$, as shown in Figure 5.

(15) Since Cay $(G, \{c\})$ is not connected, go to the next step.

(16) Since $i = 1$, stop.

This shows that $A = \{b, c\}$ is a minimal generating set of G.

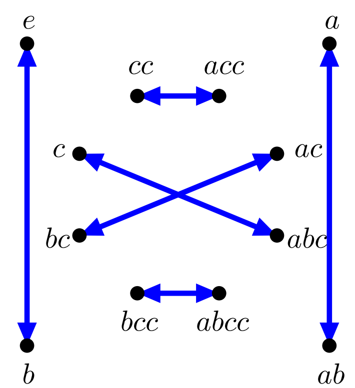

FIGURE 1. $\overrightarrow{\mathrm{Cay}}_c(G, \{b\})$; blue arcs are induced by b.

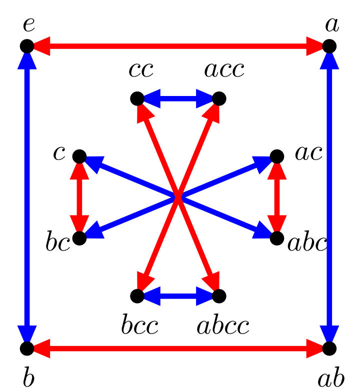

FIGURE 2. $\overrightarrow{\mathrm{Cay}}_c(G, \{b, a\})$; blue arcs are induced by b and red arcs are induced by a.

ACKNOWLEDGMENTS

The authors would like to express their special gratitude to Professor Milton Ferreira for his hospitality at the University of Aveiro, Aveiro, Portugal with financial support by Institute

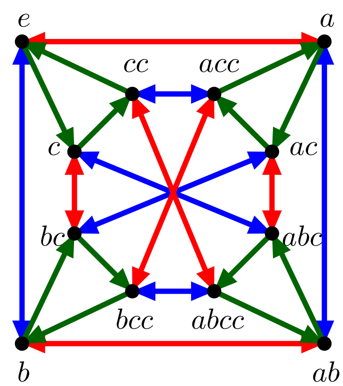

FIGURE 3. $\overrightarrow{\mathrm{Cay}}_c(G, \{b, a, c\})$; blue arcs are induced by b, red arcs are induced by a, and green arcs are induced by c.

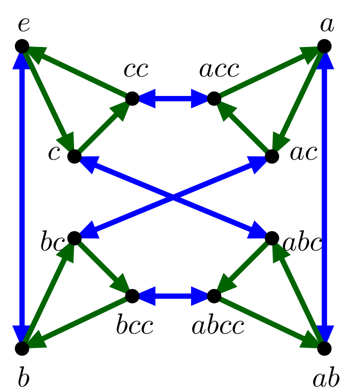

FIGURE 4. $\overrightarrow{\mathrm{Cay}}_c(G, \{b, c\})$; blue arcs are induced by b and green arcs are induced by c.

for Promotion of Teaching Science and Technology (IPST), Thailand, via Development and Promotion of Science and Technology Talents Project (DPST). This research was supported by Chiang Mai University. They would like to thank the referee for useful comments that improve the final version of the manuscript.

REFERENCES

[1] V. Arvind and J. Torán, *The complexity of quasigroup isomorphism and the minimum generating set problem*, Algorithms and computation, Lecture Notes in Computer Science, Springer, Berlin, **4288** (2006) 233-242.

[2] P. J. Cameron, A. Lucchini, and C. M. Roney-Dougal, *Generating sets of finite groups*, Trans. Amer. Math. Soc., **370** No. 9 (2018) 6751-6770.

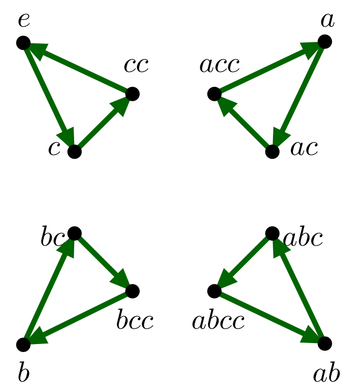

FIGURE 5. $\overrightarrow{\mathrm{Cay}}_c(G, \{c\})$; green arcs are induced by c.

[3] X. G. Fang, C. E. Praeger, and J. Wang, *On the automorphism groups of Cayley graphs of finite simple groups*, J. London Math. Soc., **66** No. 3 (2002) 563-578.

[4] C. D. Godsil, *Connectivity of minimal Cayley graphs*, Arch. Math. (Basel), **37** No. 5 (1981) 473-476.

[5] The GAP Group, GAP - *Groups, Algorithms, and Programming*, Version 4.10.0, 2018, http://www.gap-system.org.

[6] L. Halbeisen, M. Hamilton, and P. Růžička, *Minimal generating sets of groups, rings, and fields*, Quaest. Math., **30** No. 3 (2007) 355-363.

[7] A. V. Kelarev, *Labelled Cayley graphs and minimal automata*, Australas. J. Combin., **30** (2004) 95-101.

[8] ———, *On Cayley graphs of inverse semigroups*, Semigr. Forum, **72** No. 3 (2006) 411-418.

[9] A. V. Kelarev and C. E. Praeger, *On transitive Cayley graphs of groups and semigroups*, European J. Combin., **24** (2003) 59-72.

[10] A. V. Kelarev and S. J. Quinn, *A combinatorial property and Cayley graphs of semigroups*, Semigr. Forum, **66** (2003) 89-96.

[11] A. V. Kelarev, J. Ryan, and J. Yearwood, *Cayley graphs as classifiers for data mining: The influence of asymmetries*, Discrete Math., **309** No. 17 (2009) 5360-5369.

[12] B. Khosravi and M. Mahmoudi, *On Cayley graphs of rectangular groups*, Discrete Math., **310** No. 4 (2010) 804-811.

[13] W. Klotz and T. Sander, *Some properties of unitary Cayley graphs*, Electron. J. Combin., **14** (2007) Article R45, 12 pages.

[14] E. Konstantinova, *Some problems on Cayley graphs*, Linear Algebra Appl., **429** No. 11-12 (2008) 2754-2769.

[15] J. S. Leon, *On an algorithm for finding a base and a strong generating set for a group given by generating permutations*, Math. Comp., **35** No. 151 (1980) 941-974.

[16] C. H. Li, *On isomorphisms of finite Cayley graphs-a survey*, Discrete Math., **256** No. 1-2 (2002) 301-334.

[17] Z.-P. Lu and M.-Y. Xu, *On the normality of Cayley graphs of order pq*, Australas. J. Combin., **27** (2003) 81-93.

[18] A. Lucchini, *The largest size of a minimal generating set of a finite group*, Arch. Math. (Basel), **101** (2013) 1-8.

[19] A. Lucchini and F. Menegazzo, *Computing a set of generators of minimal cardinality in a solvable group*, J. Symbolic Comput., **17** No. 5 (1994) 409-420.

[20] F. Menegazzo, *The number of generators of a finite group*, Proceedings of the All Ireland Algebra Days, 2001 (Belfast), No. 50 (2003) 117-128.

[21] S. Panma, U. Knauer, and Sr. Arworn, *On transitive Cayley graphs of strong semilattices of right (left) groups*, Discrete Math., **309** No. 17 (2009) 5393-5403.

[22] J. Šiagiová and J. Širáň, *Approaching the Moore bound for diameter two by Cayley* graphs, J. Combin. Theory Ser. B, **102** No. 2 (2012) 470-473.

[23] W. Xiao and B. Parhami, *Cayley graphs as models of deterministic small-world networks*, Inform. Process. Lett., **97** No. 3 (2006) 115-117.

Tanakorn Udomworarat

Department of Mathematics

Faculty of Science, Chiang Mai University

Chiang Mai 50200, Thailand

tanakorn_u@cmu.ac.th

Teerapong Suksumran

Department of Mathematics

Faculty of Science, Chiang Mai University

Chiang Mai 50200, Thailand

teerapong.suksumran@cmu.ac.th