Finding generating sets of finite groups using their Cayley graphs

Presented by
Tanakorn Udomworarat

Advisor
Teerapong Suksumran

Department of Mathematics, Faculty of Science,
Chiang Mai University, Thailand

Semigroups and Groups, Automata, Logics
Politecnico di Milano, Cremona
10-13 June 2019

Outline

1 Introduction
- Cayley graphs

2 Main Results
- Equivalence relation and components of Cayley graphs
- Connections between components and cosets
- Construction generating sets of groups
- Finding minimal generating sets of finite groups

Cayley graphs

Cayley digraph $\overrightarrow{\mathrm{Cay}}(G, A)$

- G is a group
- $A \subseteq G$
- Vertex set is G
- Arc set is $\{(g, ga) : g \in G, a \in A\}$

Cayley color digraph $\overrightarrow{\mathrm{Cay}}_c(G, A)$

- Arc (g, ga) is given color a

Cayley graph $\mathrm{Cay}(G, A)$

- Underlying graph of $\overrightarrow{\mathrm{Cay}}(G, A)$
- $\{u, v\}$ is an edge if and only if $u = va$ or $v = ua$ for some $a \in A$
- $\{u, v\}$ is an edge in $\mathrm{Cay}(G, A)$ if and only if (u, v) or (v, u) is an arc in $\overrightarrow{\mathrm{Cay}}(G, A)$

Equivalence relation and components of Cayley graphs

Definition 1

The **equivalence relation** $\mathfrak{p}$ on G is defined by $u \, \mathfrak{p} \, v$ if and only if either $u = v$ or there is a path from u to v in $\mathrm{Cay}(G, A)$.

Definition 2

C is a **component** of $\mathrm{Cay}\,(G, A)$ if and only if there is an equivalence class X of the relation $\mathfrak{p}$ such that C is the subgraph of $\mathrm{Cay}\,(G, A)$ induced by X, that is, $C = \mathrm{Cay}\,(G, A)[X]$.

Remark 3

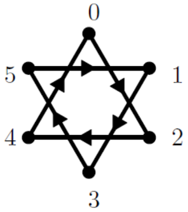
- $u \, \mathfrak{p} \, v$ if and only if u and v are in the same component of $\mathrm{Cay}\,(G, A)$.

Relations between components and cosets

Theorem 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 $\mathrm{Cay}(G, A)$.

Example In $\mathbb{Z}_6$, $\langle 2 \rangle = \{0, 2, 4\}$.
Cosets of $\langle 2 \rangle$ in $\mathbb{Z}_6$ are $0 + \langle 2 \rangle = \{0, 2, 4\}$ and $1 + \langle 2 \rangle = \{1, 3, 5\}$.



$\overrightarrow{\mathrm{Cay}}\,(\mathbb{Z}_6, \{2\})$

Connections between components and cosets

Corollary 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 6

Let G be a group and let $A \subseteq G$. Any component of $\mathrm{Cay}(G, A)$ is of the form

$$\mathrm{Cay}(G, A)[g\langle A \rangle]$$

for some $g \in G$.

Corollary 7

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

Construction generating sets of groups

Generating set of a group G is a subset such that each element of the group can be expressed as the combination (under the group operation) of finitely many elements of the subset and their inverses.

Theorem 8 (Well-known Result)

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

Theorem 9

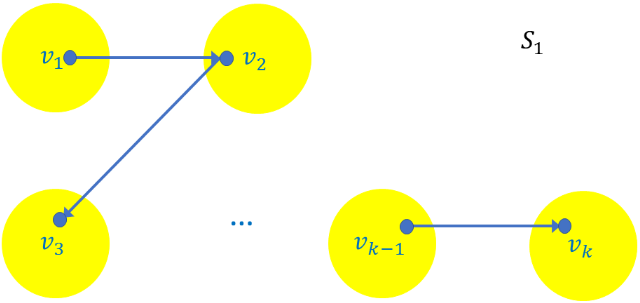
If $\mathrm{Cay}\,(G, A)$ has finitely many components and if $v_1, v_2, \ldots, v_k$ are representative vertices in all the components of $\mathrm{Cay}\,(G, A)$, then

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

form generating sets of G.

Construction generating sets of groups

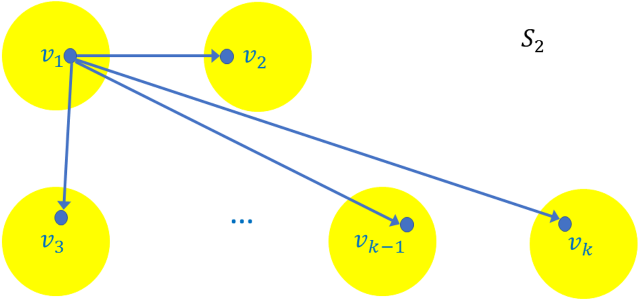
Idea of Theorem 9



Simple diagram of $\overrightarrow{\mathrm{Cay}}(G, S_1)$; $S_1 = A \cup \{v_1^{-1}v_2, v_2^{-1}v_3, \ldots, v_{k-1}^{-1}v_k\}$

Construction generating sets of groups

Idea of Theorem 9



Simple diagram of $\overrightarrow{\mathrm{Cay}}(G, S_2)$; $S_2 = A \cup \{v_1^{-1}v_2, v_1^{-1}v_3, \ldots, v_1^{-1}v_k\}$

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

1. Set $A = \{a_1\}$, where $a_1 \in G$ and $a_1 \neq e$.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

1. Set $A = \{a_1\}$, where $a_1 \in G$ and $a_1 \neq e$.
2. Set $v_1 = a_1, i = 1$.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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 $\mathrm{Cay}\,(G, A)$.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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 $A = A \cup \{a_i\}$.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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).

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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 $i = i - 1$.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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 $\mathrm{Cay}(G, A \backslash \{a_i\})$.

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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).

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.
Algorithm for finding minimal generating sets

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).

Finding minimal generating sets of finite groups

A generating set A of a group G is **minimal** if no proper subset of A generates G.

Let G be a finite group.

Algorithm for finding minimal generating sets

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).

When this algorithm stops, we have A is a minimal generating set of G.

Finding minimal generating sets of finite groups

Let G be the group defined by presentation

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

Its Cayley table is given by this table [1].

$\cdot$	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

Cayley table of the group G defined by (1).

1. The GAP Group, GAP - *groups, Algorithms, and Programming,* Version 4.10.0, 2018, http: //www.gap-system.org

Finding minimal generating sets of finite groups

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

1. Set $A = \{b\}, v_1 = b, i = 1$.
2. Draw $\mathrm{Cay}\,(G, \{b\})$.

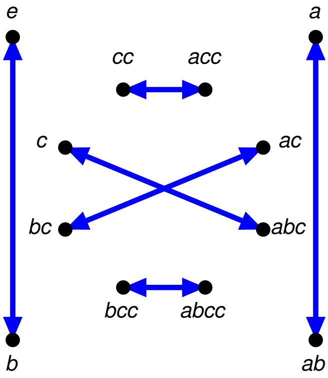


FIGURE – $\overrightarrow{\mathrm{Cay}}_c(G, \{b\})$; blue arcs are induced by b.

Finding minimal generating sets of finite groups

3. Since $\mathrm{Cay}\,(G, \{b\})$ is not connected, set $i = 2$ and $v_2 = ab$.
4. Set $a_2 = b^{-1}(ab) = a$ and $A = \{b, a\}$.
5. Draw $\mathrm{Cay}\,(G, \{b, a\})$.

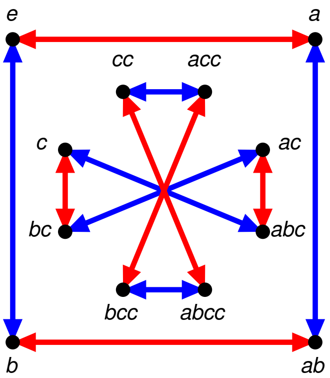


FIGURE – $\overrightarrow{\mathrm{Cay}}_c(G, \{b, a\})$; blue arcs are induced by b and red arcs are induced by a.

Finding minimal generating sets of finite groups

6. Since $\mathrm{Cay}\,(G, \{b, a\})$ is not connected, set $i = 3$ and $v_2 = bc$.
7. Set $a_3 = b^{-1}(bc) = c$ and $A = \{b, a, c\}$.
8. Draw $\mathrm{Cay}\,(G, \{b, a, c\})$.

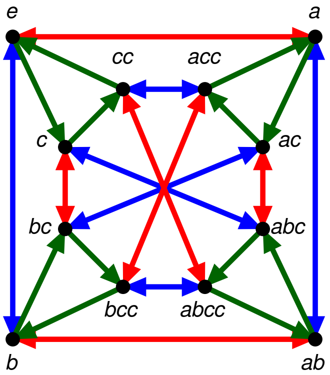


FIGURE – $\overrightarrow{\mathrm{Cay}}_c(G, \{b, a, c\})$; blue arcs are induced by b, red arcs are induced by a, and green arcs are induced by c.

Finding minimal generating sets of finite groups

9. Since $\mathrm{Cay}\,(G, \{b, a, c\})$ is connected and $i = 3$, set $i = 2$.
10. Draw $\mathrm{Cay}\,(G, \{b, c\})$.

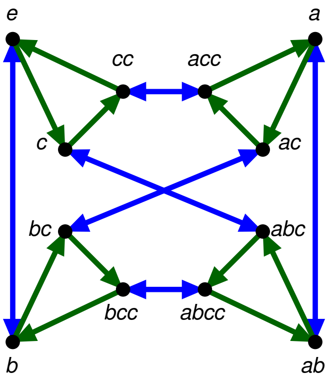


FIGURE – $\overrightarrow{\mathrm{Cay}}_c(G, \{b, c\})$; blue arcs are induced by b and green arcs are induced by c.

Finding minimal generating sets of finite groups

11. Since $\mathrm{Cay}\,(G, \{b, c\})$ is connected, set $A = \{b, c\}$.
12. Since $i = 2$, set $i = 1$.
13. Draw $\mathrm{Cay}\,(G, \{c\})$.

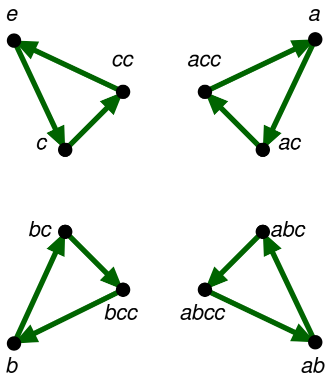


FIGURE – $\overrightarrow{\mathrm{Cay}}_c(G, \{c\})$; green arcs are induced by c.

Finding minimal generating sets of finite groups

14. Since $\mathrm{Cay}\,(G, \{c\})$ is not connected, go to the next step.
15. Since $i = 1$, stop.

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

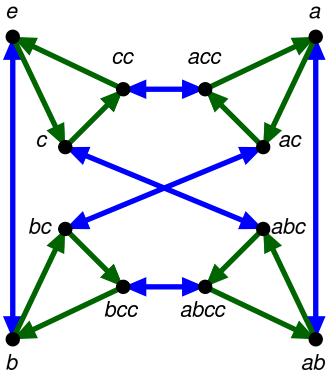


FIGURE – $\overrightarrow{\mathrm{Cay}}_c(G, \{b, c\})$; blue arcs are induced by b and green arcs are induced by c.

Acknowledgements

- Chiang Mai University, Thailand
- Development and Promotion of Science and Technology Talents Project (DPST)
- Institute for the Promotion of Teaching Science and Technology (IPST)