MATH 415

Modern Algebra I

Lecture 9: Cayley graphs (continued). Permutations.

Cayley graph

A finitely generated group G can be visualized via the **Cayley graph**. Suppose $a, b, \ldots, c$ is a finite list of generators for G. The Cayley graph is a directed graph (or digraph) with labeled edges where vertices are elements of G and edges show multiplication by generators. Namely, every edge is of the form $g \xrightarrow{s} gs$. Alternatively, one can assign colors to generators and think of the Cayley graph as a graph with colored edges.

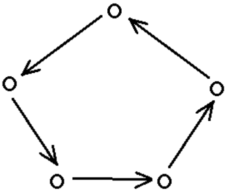
The Cayley graph can be used for computations in G. For example, let $h = a^2 b^{-1} c a^{-1}$. To compute gh, we need to find a path of the form (note the directions of edges)

$$g \xrightarrow{a} g_1 \xrightarrow{a} g_2 \xleftarrow{b} g_3 \xrightarrow{c} g_4 \xleftarrow{a} g_5.$$

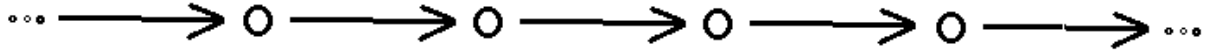
Such a path exists and is unique. Then $gh = g_5$.

Also, the Cayley graph can be used to find **relations** between generators, which are equalities of the form $g_1 g_2 \ldots g_k = 1$, where each g_i is a generator or the inverse of a generator. Any relation corresponds to a closed path in the graph.

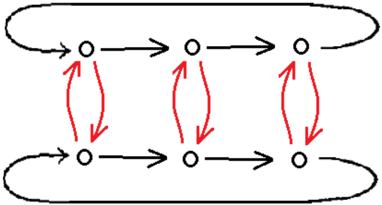
Examples of Cayley graphs



Group: $\mathbb{Z}_5$.
Generating set: $\{1\}$.



Group: $\mathbb{Z}$. Generating set: $\{1\}$.

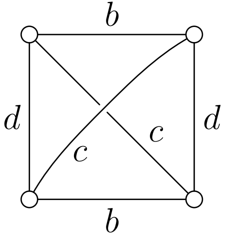


Group: $\mathbb{Z}_6$.
Generating set: $\{2, 3\}$.

Klein four-group

The **Klein four-group** $V = \{a, b, c, d\}$ is a group with the following Cayley table and Cayley graph:

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a



The group is abelian but not cyclic. The Cayley graph is relative to the generating set $\{b, c, d\}$ (a is the identity element). Since every generator is its own inverse, each directed edge $g \xrightarrow{s} gs$ is accompanied by another edge $g \xleftarrow{s} gs$. This allows to consider the Cayley graph as a graph with undirected edges.

Groups of permutations

Let X be a nonempty set. A **permutation** of X is a bijective function $f : X \to X$.

Given two permutations π and σ of X, the composition $\pi\sigma$, defined by $\pi\sigma(x) = \pi(\sigma(x))$, is called the **product** of these permutations. In general, $\pi\sigma \neq \sigma\pi$, i.e., multiplication of permutations is not commutative. However it is associative: $\pi(\sigma\tau) = (\pi\sigma)\tau$.

All permutations of a set X form a group called the **symmetric group** on X. *Notation:* S_X, Σ_X, $\mathrm{Sym}(X)$.

All permutations of $\{1, 2, \dots, n\}$ form a group called the **symmetric group on n symbols** and denoted S_n or $S(n)$.

Permutations of a finite set

The word "**permutation**" usually refers to transformations of finite sets.

Permutations are traditionally denoted by Greek letters (π, σ, τ, ρ,...).

Two-row notation. $\pi = \begin{pmatrix} a & b & c & \dots \\ \pi(a) & \pi(b) & \pi(c) & \dots \end{pmatrix}$,

where $a, b, c, \dots$ is a list of all elements in the domain of π. Rearrangement of columns does not change the permutation.

Example. The symmetric group S_3 consists of 6 permutations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Theorem The symmetric group S_n has $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ elements.

Traditional argument: The number of elements in S_n is the number of different rearrangements $x_1, x_2, \ldots, x_n$ of the list $1, 2, \ldots, n$. There are n possibilities to choose x_1. For any choice of x_1, there are $n-1$ possibilities to choose x_2. And so on...

Alternative argument: Any rearrangement of the list $1, 2, \ldots, n$ can be obtained as follows. We take a rearrangement of $1, 2, \ldots, n-1$ and then insert n into it. By the inductive assumption, there are $(n-1)!$ ways to choose a rearrangement of $1, 2, \ldots, n-1$. For any choice, there are n ways to insert n.

Product of permutations

Given two permutations π and σ, the composition $\pi\sigma$ is called the **product** of these permutations. Do not forget that the composition is evaluated from right to left: $(\pi\sigma)(x) = \pi(\sigma(x))$.

To find $\pi\sigma$, we write π underneath σ (in two-row notation), then reorder the columns so that the second row of σ matches the first row of π, then erase the matching rows.

Example. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

$$\begin{array}{l} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \\ \pi = \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \end{array} \implies \pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

To find π^{-1}, we simply exchange the upper and lower rows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Cycles

A permutation π of a set X is called a **cycle** (or **cyclic**) of length r if there exist r distinct elements $x_1, x_2, \ldots, x_r \in X$ such that

$$\pi(x_1) = x_2,\ \pi(x_2) = x_3, \ldots,\ \pi(x_{r-1}) = x_r,\ \pi(x_r) = x_1,$$

and $\pi(x) = x$ for any other $x \in X$.

Notation. $\pi = (x_1\ x_2\ \ldots\ x_r)$.

The identity function is (the only) cycle of length 1. Any cycle of length 2 is called a **transposition**.

The inverse of a cycle is also a cycle of the same length. Indeed, if $\pi = (x_1\ x_2\ \ldots\ x_r)$, then $\pi^{-1} = (x_r\ x_{r-1}\ \ldots\ x_2\ x_1)$.

Example. Any permutation of $\{1, 2, 3\}$ is a cycle.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3).$$