Math 137B Professor: Padraic Bartlett

Lecture 2: Cayley Graphs

Week 3 *UCSB 2014*

(Relevant source material: Section VIII.1 of Bollobas's Modern Graph Theory; 3.7 of Godsil and Royle's Algebraic Graph Theory; various papers I've read and cannot remember.)

This week's lecture, as well as next week's lecture, are all about the interplay of **graph theory** and **algebra**. Specifically, we are going to develop **Cayley graphs** and **Schreier diagrams** to study various kinds of groups, and to prove some very deep and surprising theorems from abstract algebra!

Because this course does not count group theory as a prerequisite, we should first, um, **define** what groups are:

1 Group Theory: Examples

If you've made it to this class, you've worked with groups before! However, you may have never seen them actually **defined**. Let's fix that:

Definition. A **group** is a set G along with some operation $\cdot$ that takes in two elements and outputs another element of our group, such that we satisfy the following properties:

- **Identity**: there is some identity element $e \in G$ such that for any other $g \in G$, we have $e \cdot g = g$.

  In other words, combining any group element g with the identity via our group operation does not change g! You know many objects like this: if we work with the real numbers $\mathbb{R}$ and think of addition as our group operation, then 0 is our identity, as $0 + x = x$ for any x. Similarly, if we consider the real numbers again but take our operation to be multiplication, then 1 is our identity, as $1 \cdot x = x$ for any x.

- **Inverses**: for any $g \in G$, there is some g^{-1} such that $g \cdot g^{-1} = e$.

  In other words, if we start at any group element g, we can always find something to combine with g using our group operation to get back to the identity! Again, you know several objects like this: with $\mathbb{R}$ and addition, the inverse of any number x is just its negative $-x$, while if we consider the set of nonzero real numbers and multiplication, the inverse for any x is just $1/x$.

- **Associativity**: for any three $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

  In other words, the order in which we group combinations together doesn't matter, as long as the sequence that we have those objects grouped together in does not change! I.e. we can combine a with $b \cdot c$, or first find $a \cdot b$ and then combine that with c. Again, most of the natural operations you're familiar with (addition, multiplication) are associative: it is perhaps more interesting to point out some things that are

nonassociative. For example, exponentiation is a nonassociative operation: $2^{(3^4)} = 2^{81} \approx 2.41 \cdot 10^{24}$, while $(2^3)^4 = 8^4 = 4096$.

It bears noting that this does not say that $a \cdot b = b \cdot a$: that is a different property, called **commutativity**, and is not a property that groups need to have (as we will show in the examples!) Groups that are commutative are called **abelian groups**, after the mathematician Niels Henrik Abel.

We list a number of examples of groups, as well as some nonexamples:

Example. As noted above, the real numbers with respect to addition, which we denote as $\langle \mathbb{R}, + \rangle$, is a group: it has the identity 0, any element x has an inverse $-x$, and it satisfies associativity.

Nonexample. The real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}, \cdot \rangle$, is **not** a group: the element $0 \in \mathbb{R}$ has no inverse, as there is nothing we can multiply 0 by to get to 1!

Example. The nonzero real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}^\times, \cdot \rangle$, is a group! The identity in this group is 1, every element x has an inverse $1/x$ such that $x \cdot (1/x) = 1$, and this group satisfies associativity.

Example. The integers with respect to addition, $\langle \mathbb{Z}, + \rangle$ form a group!

Nonexample. The integers with respect to multiplication, $\langle \mathbb{Z}, \cdot \rangle$ do not form a group: for example, there is no integer we can multiply 2 by to get to 1.

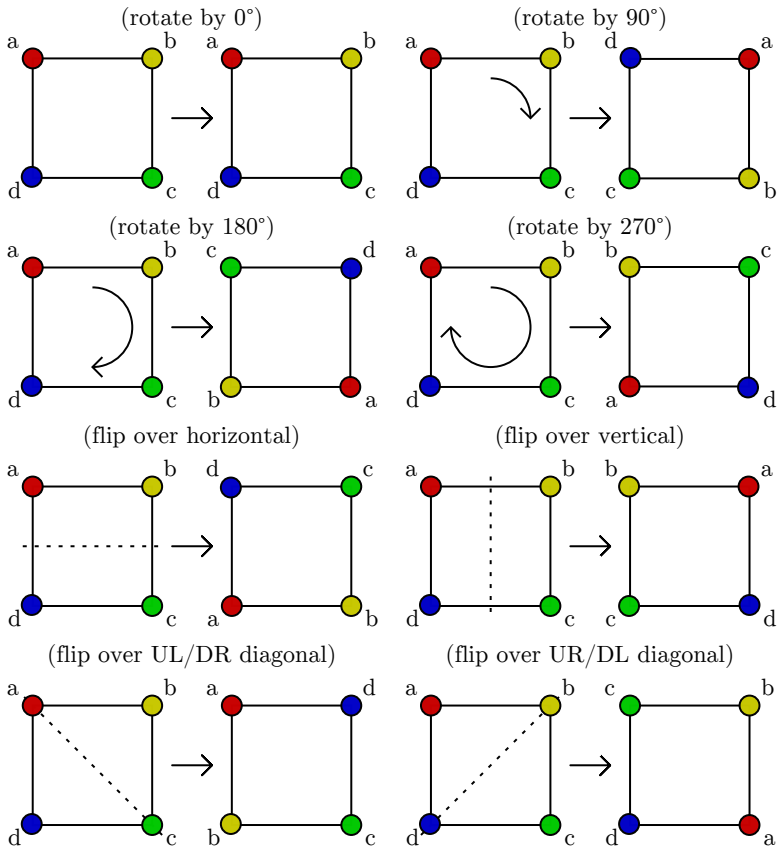
Nonexample. The natural numbers $\mathbb{N}$ are not a group with respect to either addition or multiplication. For example: in addition, there is no element $-1 \in \mathbb{N}$ that we can add to 1 to get to 0, and in multiplication there is no natural number we can multiply 2 by to get to 1.

Example. $GL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices, is a group under the operation of matrix multiplication. Notice that this group is an example of a **nonabelian** group, as there are many matrices for which $AB \neq BA$: consider $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ versus $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

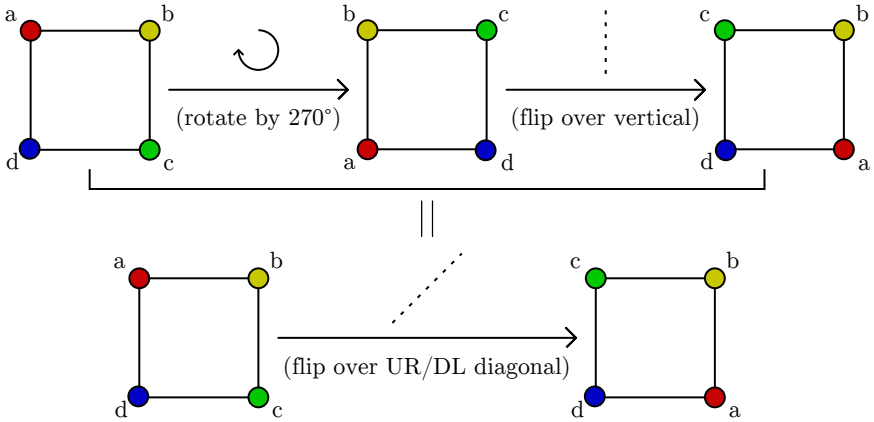
Example. $SL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices with determinant 1, is also a group under the operation of matrix multiplication; this is because the property of being determinant 1 is preserved under taking inverses and multiplication for matrices.

Example. $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots n-1\}$ is a group with respect to the operation of addition mod n: the identity in this group is 0, every element x has an inverse $n - x$ (because $x + (n - x) = n \equiv 0 \mod n$,) and addition is associative.

Example. Consider a regular n-gon. There are a number of geometric transformations, or **similarities**, that we can apply that send this n-gon to "itself:" i.e. there are several rotations and reflections that when applied to a n-gon do not change the n-gon. For example, given a square, we can rotate the plane by $0°, 90°, 180°$, or $270°$, or flip over one of the horizontal, vertical, top-left/bottom-right, or the top-right/bottom-left axes:



Given two such transformations f, g, we can compose them to get a new transformation $f \circ g$. Notice that because these two transformations each individually send the n-gon to itself, their composition also sends the n-gon to itself! Therefore composition is a well-defined operation that we can use to combine two transformations.



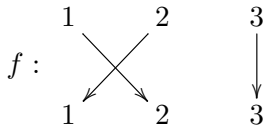
Notice that the trivial rotation by 0°, when composed with any other map, does not change that map: so, under the operation of composition, rotation by 0° is an **identity**! Similarly, notice that performing the same flip twice in a row returns us back to the identity, so every flip has an **inverse** given by itself! (I.e. if f is a flip, $f \circ f = id$: i.e. $f = f^{-1}$.) As well, if we rotate by k degrees, rotating by $360 - k$ degrees results in a total rotation by 360: i.e. rotation by 0°. So all rotations have inverses as well!

Finally, notice that because function composition is associative, this operation is **associative** as well: consequently, the collection of all symmetries of a regular n-gon forms a group under the operation of function composition!

Example. $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \dots p-1\}$ is a group with respect to the operation of multiplication mod p whenever p is a prime; check this if you don't see why!

Example. The **symmetric group** S_n is the collection of all of the permutations on the set $\{1, \dots n\}$, where our group operation is composition. In case you haven't seen this before:

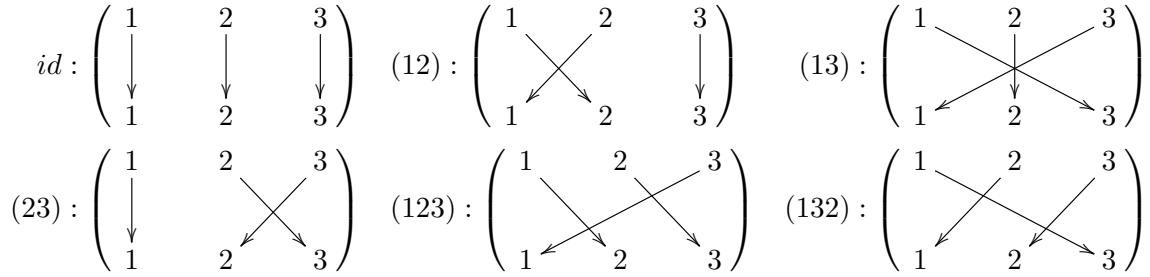
- A **permutation** of a set is just a bijective function on that set. For example, one bijection on the set $\{1, 2, 3\}$ could be the map f that sends 1 to 2, 2 to 1, and 3 to 3.
- One way that people often denote functions and bijections is via "arrow" notation: i.e. to describe the map f that we gave above, we could write



- This, however, is not the most space-friendly way to write out a permutation. A much more condensed way to write down a permutation is using something called **cycle notation**. In particular: suppose that we want to denote the permutation that sends $a_1 \to a_2$, $a_2 \to a_3$, $\dots a_{n-1} \to a_n$, $a_n \to a_1$, and does not change any of the other elements (i.e. keeps them all the same.) In this case, we would denote this permutation using cycle notation as the permutation

$$(a_1 a_2 a_3 \dots a_n).$$

To illustrate this notation, we describe all of the six possible permutations on $\{1, 2, 3\}$ using both the arrow and the cycle notations:



Because the composition of any two bijections is still a bijection, we have in particular that the composition of any two permutations is another permutation: so our group operation does indeed combine group elements into new group elements. Composing any map f with the identity map $id(x) = x$ does not change the map f, so $id(x)$ is an identity element; moreover, any bijection f has an inverse function f^{-1} such that $f \circ f^{-1}$ is the identity map. Therefore, this forms a group!

Example. The **free group** on n generators $a_1, \dots a_n$, denoted

$$\langle a_1, \dots a_n \rangle,$$

is the following group:

- The elements of the group are all of the strings of the form

  $$a_{i_1}^{k_1} a_{i_2}^{k_2} \dots a_{i_l}^{k_l},$$

  where the indices $i_1, \dots i_l$ are all valid indices for the $a_1, \dots a_n$ and the $k_1, \dots k_l$ are all integers.

- We also throw in an identity element e, which corresponds to the "empty string" that contains no elements.

- Given two strings s_1, s_2, we can **concatenate** these two strings into the word $s_1 s_2$ by simply writing the string that consists of the string s_1 followed by the string s_2.

- Whenever we have a^k in a string, we think of this as being $\overbrace{a \cdot a \cdot \dots a}^{k \text{ copies}}$, i.e. k copies of a. If we have multiple consecutive strings of a's, we can combine them together into one such a^k: for example, the word $a^3 a a^2$ is the same thing as the word a^6.

- Finally, if we ever have an aa^{-1} or an $a^{-1}a$ occurring next to each other in a string, we can simply replace this pairing with the empty string e.

For example, the free group on two generators $\langle a, b \rangle$ contains strings like

$$a^6 b^4 a^{-2} b^3 a^1, b^{12}, a^{-1} b^{-2} a^4 b, \dots$$

As described earlier, we concatenate strings by simply placing one after the other: i.e.

$$a^2 b^{-2} a^3 b a^3 \cdot a^{-3} b^{-1} a^1 b^3 = a^2 b^{-2} a^3 b a^3 a^{-3} b^{-1} a^1 b^3.$$

As described above, we typically simplify this right-hand string by canceling out terms and their inverses, and grouping together common powers of our generators:

$$a^2 b^{-2} a^3 b a^3 \cdot a^{-3} b^{-1} a^1 b^3 = a^2 b^{-2} a^3 \cancel{b} \cancel{a^3} \cancel{a^{-3}} \cancel{b^{-1}} a^1 b^3 = a^2 b^{-2} a^4 b^3$$

This is a group! In particular, concatenation is associative, the empty string e is clearly an identity, and we can "invert" any word $a_{i_1}^{k_1} a_{i_2}^{k_2} \dots a_{i_l}^{k_l}$ by simply reversing it and switching the signs on the k_i's: i.e.

$$\cancel{a_{i_1}^{k_1}} \cancel{a_{i_2}^{k_2}} \dots \cancel{a_{i_l}^{k_l}} \cdot \cancel{a_{i_l}^{-k_l}} \dots \cancel{a_{i_2}^{-k_2}} \cancel{a_{i_1}^{-k_1}} = e$$

2 Group Theory: Additional Definitions

When we work with groups, a few concepts are particularly useful to think about:

Definition. Given a group G with an operation $\cdot$ a **subgroup** of G is a subset S of G such that S is a group in its own right using the operation $\cdot$ from G. Note that this means that combining any two elements in S must remain in S, the inverse to any element in S must lie in S, and the identity element of G must be in S.

Definition. Given a group G, we say that it is **generated** by some collection of elements $a_1, \dots a_n \in G$ if we can create any element in G via some combination of the elements $a_1, \dots a_n$ and their inverses. Note that some groups have multiple different sets of generators: i.e. $\langle \mathbb{Z}, + \rangle$ is generated both by the single element 1 and also by the pair of elements $\{2, 3\}$

Definition. In our above discussion, we have primarily defined groups by giving a set and an operation on that set. There are other ways of defining a group, though! A **group presentation** is a collection of n generators $a_1, \dots a_n$ and m words $R_1, \dots R_m$ from the free group $\langle a_1, \dots a_n \rangle$, which we write as

$$\langle a_1, \dots a_n \mid R_1, \dots R_m \rangle.$$

We associate this presentation with the group defined as follows:

- Start off with the free group $\langle a_1, \dots a_n \rangle$.
- Now, declare that within this free group, the words $R_1, \dots R_m$ are all equal to the empty string: i.e. if we have any words that contain some R_i as a substring, we can simply "delete" this R_i from the word.

You have actually seen some groups defined via a presentation before:

Example. Consider the group with presentation

$$\langle a \mid a^n \rangle.$$

This is the collection of all words written with one symbol a, where we regard $a^n = e$: i.e. it's just

$$e, a, a^2, a^3, \dots a^{n-1}.$$

This is because given any string $a^k \in \langle a \rangle$, we have $a^k = a^l$ for any $k \equiv l \mod n$. This is because we can simply concatenate copies of the strings a^n, a^{-n} as many times as we want without changing a string, as $a^n = e$!

You have seen this group before: this is just $\mathbb{Z}/n\mathbb{Z}$ with respect to addition, if you replace a with 1 and think of $\overbrace{11\dots1}^{k \text{ times}}$ as k.

Often, we will give a group with a presentation in the form

$$\langle a_1, \dots a_n \mid R_1 = R_2, R_3 = R_4, \dots, \dots R_{m-1} = R_m \rangle,$$

because it is easier sometimes to think of saying that certain kinds of words are equal rather than other kinds of words are the identity; this is equivalent to the group presentation

$$\langle a_1, \dots a_n \mid R_1(R_2)^{-1}, R_3(R_4)^{-1}, \dots, \dots R_{m-1}(R_m)^{-1} \rangle.$$

With these definitions set down, we can actually start to do some graph theory:

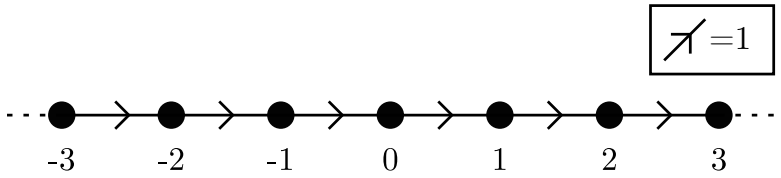
3 Cayley Graphs and Groups

Definition. Take any group A along with a generating set S. We define the **Cayley graph** $G_{A,S}$ associated to A as the following directed graph:

- Vertices: the vertices of G_A are precisely the elements of A.
- Edges: for two vertices x, y, create the oriented edge (x, y) if and only if there is some generator $s \in S$ such that $x \cdot s = y$. If this happens, we decorate the edge (x, y) with this generator s, so that we can keep track of how we have formed our connections.

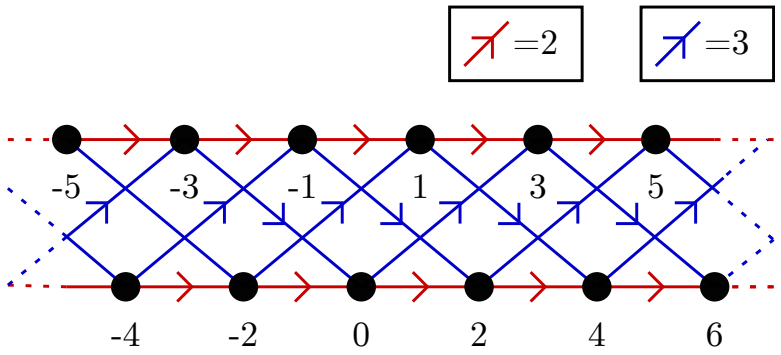
We consider a few examples here:

Example. The integers $\mathbb{Z}$ with the generator 1 have the following very simple Cayley graph:



This is not hard to see: we have one vertex for every element in our group (i.e. every integer,) and an edge (x, y) for each pair x, y such that $x = y + 1$, by definition. Because this is a Cayley graph, we label each of these edges with the generator that created that edge: for this graph, because there's only one generator this is pretty simple (we just label every edge with a 1.)

Example. The integers $\mathbb{Z}$ with the generating set $\{2, 3\}$ have the following Cayley graph:

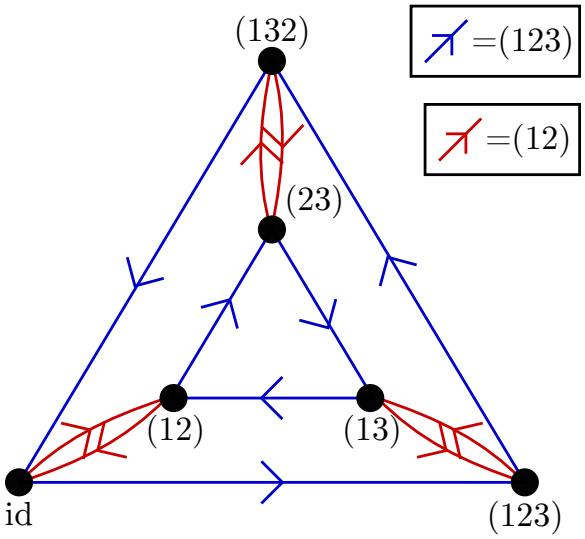


Again, our vertices are just the integers. However, this time we have two generators: the generator 2 connects any two integers that differ by 2, while the generator 3 connects any two integers that differ by 3. Notice that this graph is not the same as the graph above: in general, a group can have many markedly different Cayley graphs depending on the generators that you pick for it.

Example. Consider the symmetric group S_3 with generators $(12), (123)$. First, we calculate how these generators interact with our group elements when composed together:

group elt. $\circ$ generator	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(123)	(132)	(13)	(23)
(123)	(123)	(23)	(12)	(13)	(132)	(123)

We can use this table to create the Cayley graph for this group and generating set:



Example. Consider the group given by the presentation

$$\langle a, b \mid a^3 = b^2 = (ab)^2 = id \rangle.$$

Because we do not know all of the elements in this group ahead of time, it is not necessarily obvious how to create this group's Cayley graph; unlike in our earlier examples, we cannot simply write down all of the vertices and then draw edges corresponding to our generators.

Instead, to find the Cayley graph corresponding to this group, we can use the following procedure:

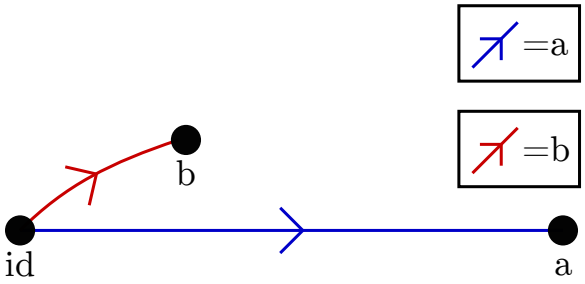
0. Start by placing one vertex that corresponds to the identity.

1. Take any vertex corresponding to a group element g that we currently have in our graph. Because our graph is a Cayley graph, it must have one edge leaving that vertex for each generator in our generating set. Add edges and vertices to our graph so that this property holds.

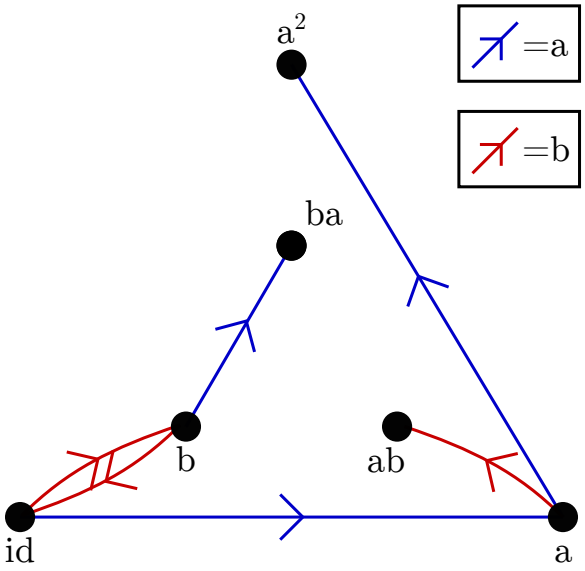
2. If some word R_i is a word that is equal to the identity in our group, then in our graph the path corresponding to that word must be a **cycle**: this is because if this word is the identity, then multiplying any element in our group by that word (i.e. taking the walk on our graph corresponding to that word) should not change that element (i.e. our walk should not take us somewhere new, and therefore should return to where it started!)

   Identify vertices only where absolutely necessary to insure that this property holds at every vertex. (This is the computationally "difficult" part of this algorithm. In general, finding the Cayley graph, or even more simply determining whether two arbitrary words in a presented graph are equal, is an **undecidable** problem: it is provable that no algorithm exists that will always solve this problem. Look up things like the halting problem if you want more examples of such things.)

So: if we do this here, we would start by drawing the following graph.



We add edge/vertex pairs to both of these added vertices a, b, that correspond to our generators. Notice that the relation $b^2 = id$ tells us that our b-edge leaving b must return to id, and that none of our other relations apply at this current stage (as they correspond to walks of length at least 3.)

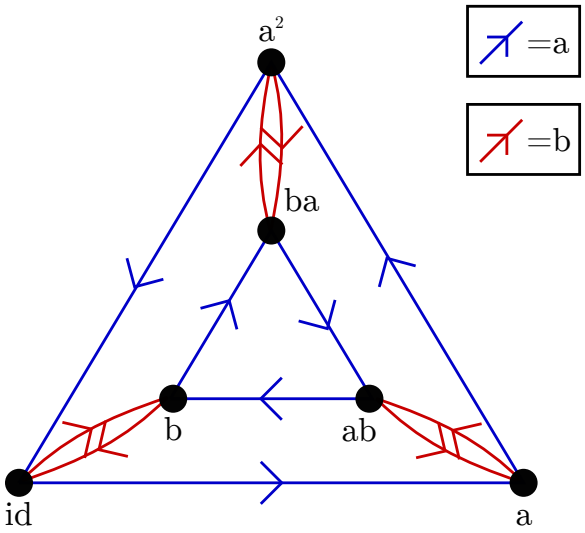


Now, we draw new edge from the vertices ab, ba, a^2. Notice that the relation $a^3 = id$ tells us that the a-edge leaving a^2 returns to the identity, and that the relation $b^2 = id$ tells us

that the b edge leaving ab returns to a. Furtheromre, the relation $abab = id$, along with the observations that $b^2 = id \Rightarrow b = b^{-1}, a^3 = id \Rightarrow a^2 = a^{-1}$ gives us a number of new relations:

- $abab = id \Rightarrow bab = a^{-1} = a^2$, and therefore the b-edge leaving ba goes to a^2. Furthermore, this also tells us that the b-edge leaving a^2 goes to ba, because the walk corresponding to b^2 starting from ba must return to ba.
- $abab = id \Rightarrow aba = b^{-1} = b$, and therefore that the a-edge leaving ab goes to b. Furthermore, this also tells us that the a-edge leaving ba goes to ab, because the walk corresponding to a^3 starting at ab must return to ab.

This gives us the following graph:



At this stage, we have satisfied our second property (that there is an edge leaving each vertex for each generator,) and we have only identified vertices when absolutely forced to do so by our relations. From visual inspection, it is clear that we satisfy the three relations $a^3 = b^2 = abab = id$ at every vertex; so this is the Cayley graph corresponding to our group!