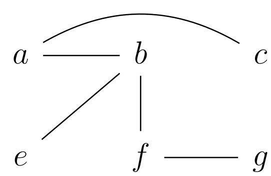
THE GRAPH ISOMORPHISM PROBLEM

MATH 410 (FALL 2019)
PROF. MAZEL-GEE

Abstract. This document is simultaneously a mathematical text and a menu of homework problems, which explains how to use group theory to solve the graph isomorphism problem.

0. Introduction

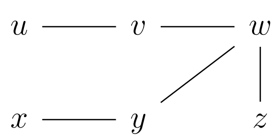
0.1. **The graph isomorphism problem.** A *graph* is a simple mathematical object consisting of vertices and edges. Here is an example of a graph with six vertices and four edges:



.

Graphs are defined more carefully and precisely in §1.

It is not very difficult to count the number of graphs with a fixed vertex set. A much more difficult problem is to count the number of graphs "up to isomorphism": this is the *graph isomorphism problem.* For example, the above graph is isomorphic to the following graph:



.[1]

For any natural number $n \in \mathbb{N}$, we will write $|\Gamma_n|$ for the number of isomorphism classes of graphs with n vertices: then, the graph isomorphism problem is to determine the natural number $|\Gamma_n|$.

As it turns out, it is not so hard to solve the graph isomorphism problem "by hand" – that is, without using group theory – for small values of n. More specifically, it is a simple matter to compute $|\Gamma_n|$ for $n \leq 3$, and it is not so difficult to compute $|\Gamma_4|$, but it is extremely difficult to compute $|\Gamma_n|$ by hand for any $n \geq 5$. The reason for this phenomenon is that as n increases, the following quantities both grow very rapidly: the number of graphs with n vertices, and the number of isomorphisms between graphs with n vertices. In fact, this rapid growth causes the graph isomorphism problem to quickly become intractable as n grows, even with the use of a computer.

---

last updated: December 5, 2019 at 8am.

[1] In fact, these two graphs are isomorphic in two different ways.

As we will see, the use of group theory makes the graph isomorphism problem substantially easier. More precisely, we will reduce the computation of $|\Gamma_n|$ to a computation regarding the symmetric group S_n, which we will be able to solve for all $n \leq 5$. However, it remains a difficult open problem to find a closed-form solution of the graph isomorphism problem, i.e. a formula for $|\Gamma_n|$ as a function of n involving only the standard operations of arithmetic.

Group theory applies to the graph isomorphism problem as follows. As the notation suggests, the natural number $|\Gamma_n|$ is the cardinality of a set Γ_n of isomorphism classes of graphs with n vertices. This set can be obtained as the *quotient set* of a certain *group action*; these notions are defined in §2. In §3 we introduce *Burnside's lemma*, which gives a formula for the cardinality of the quotient set of a group action. In §4 we assemble the results necessary to apply Burnside's lemma to compute $|\Gamma_n|$ for $n \leq 5$.

0.2. **The problems.** The problems in this menu/text are separated into two types: "prix fixe" problems and "side dish" problems. You are required to solve the former (namely Problems 19-21), and you must spend at least 15 points on the latter. Many of the side dish problems are either directly or indirectly relevant to the graph isomorphism problem, so you might consider them whether or not you write up your solutions.

Whether or not you solve a particular problem, you may use it in your solutions to other problems.

To ease your typographical burden, instead of drawing graphs (or other diagrams) in LaTeX you may submit photos of hand-drawn graphs either embedded in your homework document or as a separate email attachment. If you pursue the latter route, please label your pictures clearly with figure numbers and refer to those labels in your homework.

1. The graph isomorphism problem

Notation 1.1. Given a set X, we write

$$\mathcal{P}(X) := \{Y \subseteq X\}$$

for its power set, i.e. the set of all of its subsets.

Problem 1 (side dish, 2 points)**.** For a finite set X with $|X| = n$, find $|\mathcal{P}(X)|$.

Definition 1.2. Given a set X, we define ***X-choose-2*** to be the subset

$$\binom{X}{2} := \{Y \in \mathcal{P}(X) : |Y| = 2\} \subseteq \mathcal{P}(X)$$

of its power set consisting of its cardinality-2 subsets.

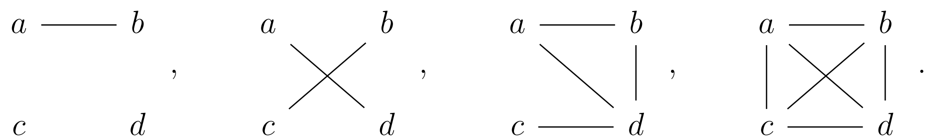
Problem 2 (side dish, 2 points)**.** List the elements of $\binom{X}{2}$ in the following cases: $X = \emptyset$, $X = \{a\}$, $X = \{a, b\}$, $X = \{a, b, c\}$, $X = \{a, b, c, d\}$.

Problem 3 (side dish, 2 points)**.** For a finite set X with $|X| = n \in \mathbb{N}$, find $|\binom{X}{2}|$.

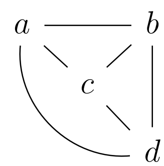
Definition 1.3. A ***graph*** consists of the following data:

- a set V, whose elements are called ***vertices*** of the graph;
- a subset $E \subseteq \binom{V}{2}$, whose elements are called ***edges*** of the graph.

Example 1.4. Although graphs are defined abstractly, they may be thought of in more concrete visual terms, as indicated in §0. For instance, a few graphs with vertex set $V = \{a, b, c, d\}$ may be depicted as follows:



However, note that a number of features of these pictures are not mathematically relevant, e.g. the placement of the vertices and the intersection point between the edges $a - d$ and $b - c$ (when both of those edges are present). For instance, the last graph above may also be equivalently depicted as



.[2]

Remark 1.5. Many variants of Definition 1.3 are possible. For example, one could allow for multiple edges between two vertices (instead of just 0 or 1), or edges that start and end at the same vertex, or directed edges (whose vertices are distinguished as the *source* and *target* of the edge). The techniques used here can also be used to address the corresponding graph isomorphism problems.

Problem 4 (side dish, 3 points)**.** For a finite set V with $|V| = n \in \mathbb{N}$, give a formula for the number of graphs with vertex set V. (*Hint*: The set of edges of such a graph can be any subset of $\binom{V}{2}$.)

Observation 1.6. A bijection $V \xrightarrow{\varphi} V'$ determines a bijection $\binom{V}{2} \xrightarrow{\tilde{\varphi}} \binom{V'}{2}$ given by the formula $\tilde{\varphi}(\{v, w\}) = \{\varphi(v), \varphi(w)\}$.

Definition 1.7. Let (V, E) and (V', E') be graphs. An ***isomorphism*** from (V, E) to (V', E') is a bijection $V \xrightarrow{\varphi} V'$ such that $\tilde{\varphi}(E) = E'$.

Notation 1.8. Given a natural number $n \in \mathbb{N}$, we write $|\Gamma_n| \in \mathbb{N}$ for the number of isomorphism classes of graphs with exactly n vertices.

Notation 1.9. For any natural number $n \in \mathbb{N}$, we write $\underline{n} := \{1, \dots, n\}$. (So $|\underline{n}| = n$, and in particular $\underline{0} = \emptyset$.)

---

[2]It is a separate and interesting question which graphs are *planar*, i.e. can be drawn in the plane without any edges crossing each other.

Problem 5 (side dish, 2 points)**.** Prove that every graph with n vertices is isomorphic to a graph with vertex set $\underline{n}$. (*Hint*: Use Observation 1.6.)

Problem 6 (side dish, 3 points)**.** Find $|\Gamma_0|$, $|\Gamma_1|$, $|\Gamma_2|$, and $|\Gamma_3|$ by hand.

Problem 7 (side dish, 4 points)**.** Find $|\Gamma_4|$ by hand.

2. Group actions

Definition 2.1. Let G be a group and let X be a set. An ***action*** of G on X is a function

$$G \times X \xrightarrow{\alpha} X$$

that satisfies the following conditions:

- *unitality*: for all $x \in X$, $\alpha(1_G, x) = x$;
- *associativity*: for all $g, h \in G$ and for all $x \in X$, $\alpha(g, \alpha(h, x)) = \alpha(g \cdot h, x)$.

We will generally simply write $g \star x := \alpha(g, x)$ for a group action; then, the above conditions may be rewritten as the requirements that $1_G \star x = x$ and that $g \star (h \star x) = (g \cdot h) \star x$.

Example 2.2. For any $n \in \mathbb{N}$, the function $S_n \times \underline{n} \to \underline{n}$ given by the formula $\sigma \star i := \sigma(i)$ defines an action of the symmetric group S_n on the set $\underline{n}$, called the *fundamental action* of S_n. More generally, for any set X, the formula $\sigma \star x := \sigma(x)$ defines an action on X of its permutation group S_X.

Example 2.3. Let G be a group, and let us write $U(G)$ for its underlying set.

(1) The group G acts on the set $U(G)$ by left multiplication: $g \star h := g \cdot h$.
(2) The group G acts on the set $U(G)$ by conjugation: $g \star h := g \cdot h \cdot g^{-1}$.

Example 2.4. Given an action of a group G on a set X and a subgroup $H \subseteq G$, the group H acts on the set X via the same formula. More precisely, the composite function

$$H \times X \longrightarrow G \times X \xrightarrow{\alpha} X$$

(in which the first function is the inclusion) defines an action of H on X.

Example 2.5. Suppose that a group G acts on a set X, and suppose that the subset $Y \subseteq X$ is *invariant* under the action, i.e. that for any $g \in G$ and any $y \in Y$ we have $g \star y \in Y$. Then, G acts on the set Y by the same formula. More precisely, the condition that the subset $Y \subseteq X$ is G-invariant implies that we have a factorization

$$\begin{array}{ccc} G \times Y & \dashrightarrow & Y \\ \downarrow & & \downarrow \\ G \times X & \longrightarrow & X \end{array}$$

(where the downwards functions are the inclusions) which defines an action of G on Y.

Problem 8 (side dish, 5 points)**.** For a group G and a set X, construct a bijection

$$\{\text{actions of } G \text{ on } X\} \longrightarrow \hom(G, S_X)$$

from the set of actions of G on X to the set of homomorphisms from G to the permutation group S_X of X. How do Examples 2.2 and 2.4 interact with this bijection?

Problem 9 (side dish, 3 points)**.** Let G be a group and let $H \subseteq G$ be a subgroup. Show that the formula $g \star (aH) := (g \cdot a)H$ gives a well-defined action of G on the set G/H of left cosets of H.

Problem 10 (side dish, 4 points)**.** Give an example of a group G, a set X, and a function $G \times X \to X$ which is associative but not unital.

Notation 2.6. Given a natural number $n \in \mathbb{N}$, we write $\tilde{\Gamma}_n$ for the set of graphs with vertex set $\underline{n}$.

Observation 2.7. By the hint from Problem 4, we have a natural isomorphism $\tilde{\Gamma}_n \cong \mathcal{P}(\binom{\underline{n}}{2})$: a graph with vertex set $\underline{n}$ is completely specified by its set $E \subseteq \binom{\underline{n}}{2}$ of edges.

Problem 11 (side dish, 3 points)**.** Suppose that a group G acts on a set X. Prove that G also acts on $\mathcal{P}(X)$ according to the formula $g \star Y := \{g \star y : y \in Y\}$.

Observation 2.8. Recall the fundamental action of S_n on $\underline{n}$ of Example 2.2. By Problem 11, this determines an action of S_n on the power set $\mathcal{P}(\underline{n})$. Because this action preserves the cardinalities of subsets of $\underline{n}$, the subset $\binom{\underline{n}}{2} \subseteq \mathcal{P}(\underline{n})$ is invariant under this action. Hence, by Example 2.5 we obtain an action of S_n on $\binom{\underline{n}}{2}$.[3] Applying Problem 11 again, we obtain an action of S_n on the set $\mathcal{P}(\binom{\underline{n}}{2}) \cong \tilde{\Gamma}_n$ (where the isomorphism is that of Observation 2.7).

3. Burnside's lemma

Definition 3.1. Given a group G acting on a set X, the ***orbit*** of an element $x \in X$ is the subset

$$Gx := \{g \star x \in X : g \in G\} \subseteq X \ .$$

Example 3.2. Let G be a group and let $H \subseteq G$ be a subgroup. Combining Examples 2.3(1) and 2.4, we obtain an action of the group H on the set $U(G)$ by left multiplication: $h \star g := h \cdot g$. The orbit of an element $g \in U(G)$ is the right coset

$$Hg = \{hg \in G : h \in H\} \subseteq U(G) \ .$$

Problem 12 (side dish, 4 points)**.** Given a group G acting on a set X, prove that the orbits

$$\{Gx \subseteq X : x \in X\} \subseteq \mathcal{P}(X)$$

define a partition of X.

[3] Using the notation of Observation 1.6, this action is given by the formula $\sigma \star \{x, y\} := \tilde{\sigma}(\{x, y\})$.

Notation 3.3. Given a group G acting on a set X, we write

$$G\backslash X := \{Gx \subseteq X : x \in X\} \subseteq \mathcal{P}(X)$$

for the quotient set of the equivalence relation corresponding to the partition of X by orbits of Problem 12. We write $[x] := Gx \in G\backslash X$ for the orbit generated by an element $x \in X$.

Notation 3.4. We write $\Gamma_n := S_n\backslash\tilde{\Gamma}_n$ for the quotient set of the action of the symmetric group S_n on the set $\tilde{\Gamma}_n$ of graphs with vertex set $\underline{n}$.[4]

Definition 3.5. Let G be a group acting on a set X. The ***fixed set*** of an element $g \in G$ is the subset

$$X^g := \{x \in X : g \star x = x\} \subseteq X\ .$$

Problem 13 (side dish, 3 points)**.** Find all fixed sets of the fundamental action of the symmetric group S_3 on the set $\underline{3}$ of Example 2.2.

Problem 14 (side dish, 3 points)**.** Let G be a group acting on a set X. Suppose that $h = aga^{-1}$ in G. Prove that action by a gives a well-defined bijection

$$X^g \xrightarrow{a\star -} X^h\ .$$

Theorem 3.6 (Burnside's lemma)**.** *Let G be a finite group acting on a finite set X. Then,*

$$|G\backslash X| = \frac{1}{|G|} \cdot \sum_{g\in G} |X^g|\ .$$

Lemma 3.7 (the orbit decomposition theorem)**.** *Let G be a finite group acting on a finite set X, and choose any $x \in X$.*

1. *The subset $G_x := \{g \in G : g \star x = x\} \subseteq G$ is a subgroup.*
2. *Suppose that $G\backslash X$ is a singleton. Then, $|G| = |X| \cdot |G_x|$. (In particular, $|G_y| = |G_x|$ for any $y \in X$.)*

Problem 15 (side dish, 10 points)**.** Prove the orbit decomposition theorem. (*Hint for part (2)*: Prove that the formula $gG_x \mapsto g \star x$ gives a well-defined bijection $G/G_x \to X$, and use Lagrange's theorem.)

Problem 16 (side dish, 10 points)**.** Prove Burnside's lemma by counting the number of elements of the set

$$F := \{(g, x) \in G \times X : g \star x = x\}$$

in two different ways, one of them using the orbit decomposition theorem.

Problem 17 (side dish, 3 points)**.** Verify Burnside's lemma for the fundamental action of the symmetric group S_3 on the set $\underline{3}$ of Example 2.2.

[4]So by Problem 5, the cardinality $|\Gamma_n|$ is indeed the number of isomorphism classes of graphs with exactly n vertices: Notation 3.4 is consistent with Notation 1.8.

Problem 18 (side dish, 4 points)**.** Verify Burnside's lemma for the action of the symmetric group S_3 on its underlying set $U(S_3)$ via conjugation of Example 2.3(2).

Definition 3.8. For a group G, we write $G\backslash G := G\backslash U(G)$ for the quotient set of the conjugation action of G on $U(G)$ of Example 2.3(2), and we refer to its elements as ***conjugacy classes***.

Observation 3.9. Let G be a finite group acting on a finite set X. We can compute $|G\backslash X|$ via the string of equalities

$$|G\backslash X| = \frac{1}{|G|}\cdot\sum_{g\in G}|X^g| = \frac{1}{|G|}\sum_{\alpha\in G\backslash G}\left(\sum_{g\in\alpha}|X^g|\right) = \frac{1}{|G|}\cdot\sum_{[g]\in G\backslash G}|[g]|\cdot|X^g| ,$$

where the first equality is Burnside's lemma, the second equality uses the fact that the elements of G are partitioned into conjugacy classes (i.e. Problem 12 applied to the conjugation action of G on itself), and the third equality follows from the fact that $|X^g| = |X^h|$ whenever g and h are conjugate (Problem 14). This formula is more efficient than Burnside's lemma, in that we only need to compute X^g once for each conjugacy class $[g]\in G\backslash G$ rather than computing X^g for every element $g\in G$. Of course, in exchange we must also compute the cardinality $|[g]|$ of each conjugacy class $[g]\in G\backslash G$.

4. The computation of $|\Gamma_n|$ for $n\leq 5$

Observation 4.1. Suppose that

$$\sigma = (a_1^1\ \cdots\ a_{i_1}^1)\ (a_1^2\ \cdots\ a_{i_2}^2)\ \cdots\ (a_1^j\ \cdots\ a_{i_j}^j)\in S_n$$

is a product of disjoint cycles. Recall that for any $\tau = S_n$,

$$\tau\sigma\tau^{-1} = (\tau(a_1^1)\ \cdots\ \tau(a_{i_1}^1))\ (\tau(a_1^2)\ \cdots\ \tau(a_{i_2}^2))\ \cdots\ (\tau(a_1^j)\ \cdots\ \tau(a_{i_j}^j)) .$$

Hence, two elements of S_n are conjugate if and only if they have the same cycle type (i.e. their cycle decompositions consist of cycles of the same length). Therefore, the sets of conjugacy classes of S_n for $0\leq n\leq 5$ are as follows:

$$\begin{aligned}
&S_0\backslash S_0 = \{\{\varepsilon\}\} ,\\
&S_1\backslash S_1 = \{\{\varepsilon\}\} ,\\
&S_2\backslash S_2 = \{\{\varepsilon\},\{(12)\}\} ,\\
&S_3\backslash S_3 = \{\{\varepsilon\},\{(12),(13),(23)\},\{(123),(132)\}\} = \{[\varepsilon],[(12)],[(123)]\} ,\\
&S_4\backslash S_4 = \{[\varepsilon],[(12)],[(12)(34)],[(123)],[(1234)]\} ,\\
&S_5\backslash S_5 = \{[\varepsilon],[(12)],[(12)(34)],[(123)],[(123)(45)],[(1234)],[(12345)]\} .
\end{aligned}$$

In the cases $n = 4$ and $n = 5$ where we have not explicitly enumerated the elements of each conjugacy class, their cardinalities are as follows:

element of $S_4 \backslash S_4$	$[\varepsilon]$	$[(12)]$	$[(12)(34)]$	$[(123)]$	$[(1234)]$
cardinality	1	6	3	8	6

,

element of $S_5 \backslash S_5$	$[\varepsilon]$	$[(12)]$	$[(12)(34)]$	$[(123)]$	$[(123)(45)]$	$[(1234)]$	$[(12345)]$
cardinality	1	10	15	20	20	30	24

.[5]

Remark 4.2. The following problems lead up to the computation of $|\Gamma_5|$, which is the main goal of this worksheet. However, as a warm-up exercise you may find it helpful to use this same technique to (re)compute $|\Gamma_n|$ for $0 \leq n \leq 4$. If you find yourself unable to do the $n = 5$ case, you may do a smaller case for partial credit (decreasing with the value of n).

Problem 19 (prix fixe)**.** Choose a representative $\sigma \in S_5$ of each conjugacy class $[\sigma] \in S_5 \backslash S_5$ and compute the cardinality of the quotient set $\langle\sigma\rangle \backslash \binom{5}{2}$ of the action of the subgroup $\langle\sigma\rangle \subseteq S_5$ on the set $\binom{5}{2}$ of Example 2.4 and Observation 2.8. (*Hint*: It may be helpful to depict the action of the element σ on the set $\binom{n}{2}$ analogously to how we depicted the actions of elements of S_n on the set $\underline{n}$ when we first defined S_n.[6])

Problem 20 (prix fixe)**.** For any $\sigma \in S_n$, find a formula for the cardinality $|(\tilde{\Gamma}_n)^\sigma|$ of its fixed set with respect to the action of S_n on $\tilde{\Gamma}_n$ of Observation 2.8 in terms of the cardinality

---

[5]To give a sense of how these computations go, here are a few representative bits of reasoning.

- A transposition (i.e. 2-cycle) is entirely determined by the two numbers that appear, so the cardinality of $[(12)] \in S_n \backslash S_n$ is $\binom{n}{2}$.
- The n-cycles form the conjugacy class $[(123\ldots n)] \in S_n \backslash S_n$. An n-cycle in S_n is specified by an ordering of the elements of $\underline{n}$, of which there are $n!$, and each n-cycle can be written in n different ways (e.g. $(1234) = (2341) = (3412) = (4123)$), so this conjugacy class has cardinality $\frac{n!}{n} = (n-1)!$.
- More generally, for any $2 \leq k \leq n$ the k-cycles form the conjugacy class $[(123\ldots k)] \in S_n \backslash S_n$. It is a two-step process to specify a k-cycle in S_n: first we must choose k elements of $\underline{n}$, and then we must form a cycle out of them. Following the above reasoning, we see that this conjugacy class has cardinality $\binom{n}{k} \cdot (k-1)!$.
- An element of $[(12)(34)] \in S_4 \backslash S_4$ is entirely determined by which element 1 is paired with, so this conjugacy class has cardinality 3. Meanwhile, an element of $[(12)(34)] \in S_5 \backslash S_5$ is determined first by which element of $\underline{5}$ it fixes and then by how the remaining four elements are paired (of which as we have just seen there are three possibilities), so this conjugacy class has cardinality $5 \cdot 3 = 15$.
- When $n = 5$, there is a bijection $[(123)] \to [(123)(45)]$ given by composing a 3-cycle with the unique transposition that is disjoint from it.

[6]For instance, the element $(14)(23) \in S_4$ acts on the set $\binom{4}{2}$ as indicated in the diagram

$$\{1,2\} \rightleftarrows \{3,4\} \qquad \{1,3\} \rightleftarrows \{2,4\} \qquad \{1,4\} \circlearrowleft \qquad \{2,3\} \circlearrowleft \quad .$$

$|\langle\sigma\rangle\backslash\binom{n}{2}|$. (*Hint*: A graph $(\underline{n}, E)$ is fixed by σ if and only if each orbit of $\langle\sigma\rangle$ in $\binom{n}{2}$ (i.e. each element of the quotient set $\langle\sigma\rangle\backslash\binom{n}{2}$) is either entirely contained in E or disjoint from E.)

Problem 21 (prix fixe)**.** Compute $|\Gamma_5|$ by combining Observations 3.9 and 4.1 with your solutions to Problems 19 and 20.