REU 2006 · Discrete Math · Lecture 5

Instructor: László Babai
Scribe: Megan Guichard
Editors: Duru Türkoğlu and Megan Guichard

June 30, 2006. Last updated July 3, 2006 at 11:30pm.

1 Review

Recall the definitions of **tree**, **graph**, **spanning tree**, etc. Notice that **vertex** is the singular, **vertices** is the plural form. We may use **vxs** as a shorthand for "vertices."

We were looking at the spanning trees of K_n, the complete graph on n vertices. We sketched proofs of Cayley's Formula: The number of spanning trees of K_n is n^{n-2}. The second proof established a bijection between trees and strings of length $(n-2)$ on an alphabet of n letters.

We also started the first proof: We claimed that, given natural numbers $d_1, d_2, \ldots, d_n$ representing the degrees of labeled vertices in a tree, there are exactly

$$\frac{(n-2)!}{\prod_{i=1}^{n}(d_i-1)!}$$

trees such that vertex i has degree d_i, for each $i = 1, 2, \ldots, n$.

We claimed that Cayley's theorem follows from this result in one line.

Proof. By the multinomial theorem from last time,

$$(1+1+\cdots+1)^{n-2} = \sum \frac{(n-2)!}{(d_i-1)!}$$

where the sum is over n-tuples $(d_1, \ldots, d_n)$ such that $d_i - 1 \geq 0$ and $\sum(d_i - 1) = n-2$. The left-hand side is n^{n-2}, and the right-hand side counts all trees on n vertices. □

2 Some more graph theory

Definition 1. Two graphs G_1 and G_2 are **isomorphic** if there exists a function

$$f : V(G_1) \to V(G_2)$$

such that $x \sim_{G_1} y$ if and only if $f(x) \sim_{G_2} f(y)$. Here $V(G)$ is the set of vertices of the graph G, and $x \sim_G y$ means x and y are adjacent vertices in G.
Such a function f is called an **isomorphism**.

Definition 2. See the handout for the definition of **planar**.

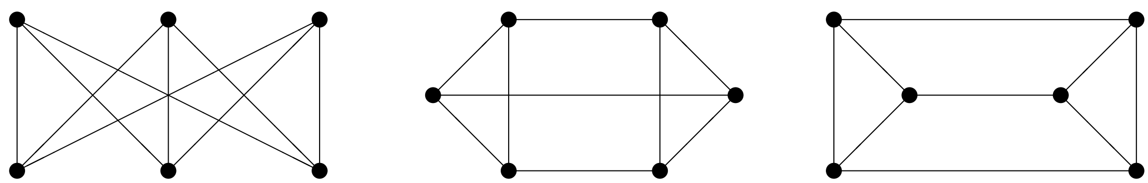


Figure 1: Three graphs

Example 3. Question: Are the above graphs isomorphic to each other?
Answer: The graphs in the middle and the right are isomorphic, while the graph on the left ($K_{3,3}$) is not isomorphic to others.

You can see the isomorphism between second and third graphs by simply moving the outside nodes of the second graph inside the rectangle. The transformed graph is the third graph.

For non-isomorphism, see that given any three points of the non-$K_{3,3}$ graphs, an edge connects two of them. Why? Use the pigeonhole principle; the vertices of the second graph are all in one of two triangles, so of any three vertices, at least two will be in the same triangle, hence adjacent. Alternately, $K_{3,3}$ is 2-colorable, but the second graph is not, because any graph with triangles is not 2-colorable.

Since isomorphism is transitive, just proving that the second graph is not isomorphic to $K_{3,3}$ would prove the same for the third graph.

There is a famous graph in graph theory, called **Petersen's graph**, which is a counterexample to many false conjectures. Petersen's graph appears in Figure **??**.

Exercise 4. Are the two graphs in Figure **??** isomorphic? Note the first has 5-fold symmetry, the second has 3-fold symmetry.

Definition 5. The **complement** of a graph G is a graph $\overline{G}$ such that $V(\overline{G}) = V(G)$ and $x \sim_{\overline{G}} y$ if and only if $x \not\sim_G y$.

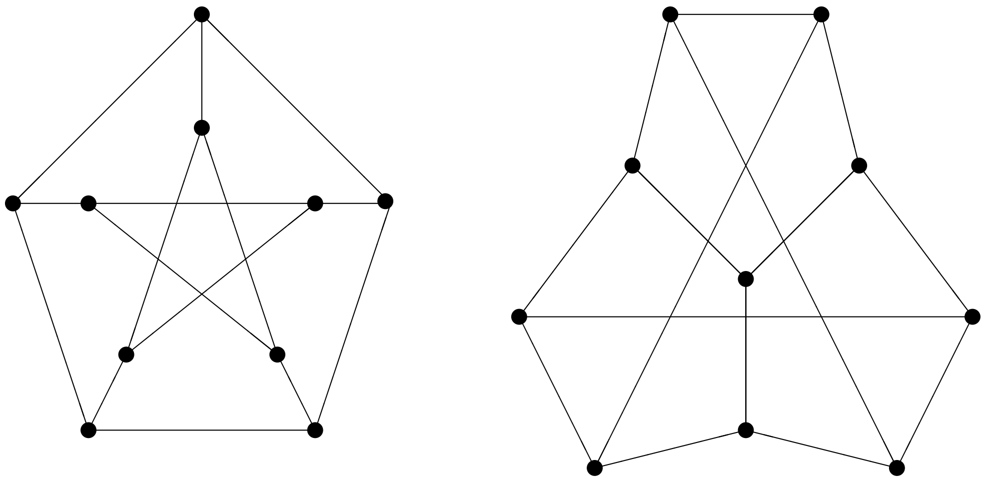


Figure 2: Petersen's graph (left) and another graph which may be isomorphic

Question. Is it possible that $G \cong \overline{G}$?
Yes; for example, P_0, the path of length zero, i.e. the graph with one vertex and no edges. Also, C_5, the cycle of length 5, has complement which is again a C_5. Another example for self-complementary graphs is P_3, the path of length 3.

Exercise 6. If $G \cong \overline{G}$, then the number of vertices n of G satisfies $n \equiv 0$ or $1 \pmod 4$.

Exercise 7. If $n \equiv 0, 1 \pmod 4$, then there exists a self-complementary graph G with n vertices.

Definition 8. An **automorphism** of a graph G is an isomorphism $G \to G$.

It is interesting to count the number of automorphisms of a graph.

Example 9. Show that:

- $|\mathrm{Aut}(K_n)| = n!$.
- $|\mathrm{Aut}(P_{n-1})| = 2$ if $n \geq 1$.
- $|\mathrm{Aut}(C_n)| = 2n$.

Exercise 10. Prove that the number of automorphisms of the cube (as a graph) is 48.

What about the number of automorphisms of the dodecahedron? There are 20 vertices. Pick a vertex; there are 20 choices of where to send it. Then there are three ways of rotating

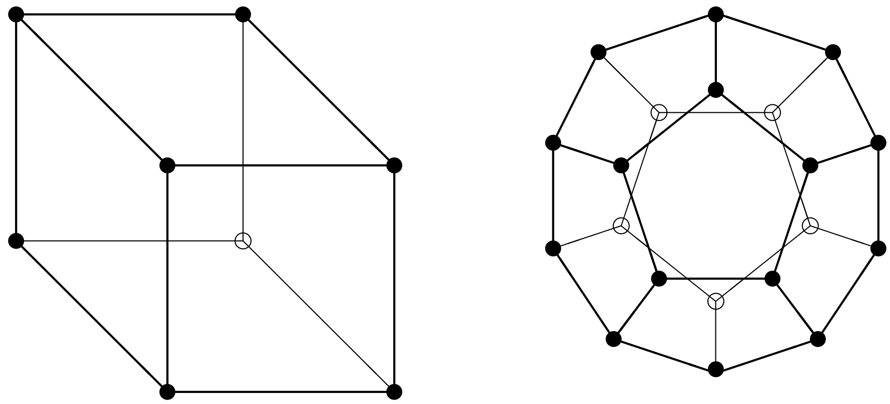


Figure 3: Graphs of a 3-cube and dodecahedron

the dodecahedron which still give an automorphism. Finally, given any edge, there is a reflection of the dodecahedron fixing that edge. So altogether there are 120 automorphisms of the dodecahedron.

Exercise 11. Find the number of automorphisms of Petersen's graph. (Hint: from the defining diagram, we know it has at least 10, coming from the symmetries of the pentagon. If you prove that the diagram with 3-fold symmetry is isomorphic, then the number is at least 30, because the automorphisms form a group—use Lagrange's theorem. In fact the number of automorphisms is 120.)

This leads us to the realization that $\mathrm{Aut}(G)$ is a group; in particular, it is a subgroup of the symmetric group on the set of vertices $V(G)$.

Now, the dodecahedron and Petersen's graph both have automorphism groups with 120 elements. This naturally leads to the question:

Exercise 12. Are the automorphism groups of Petersen's graph and the dodecahedron isomorphic? (This is *not* the same as asking whether the graphs are isomorphic!)

Let Q_k be the k-dimensional cube. The one-dimensional cube has two vertices; the two-dimensional cube has 4, the three-dimensional cube has 8, and in general the k-dimensional cube has 2^k vertices. Proof: the $(k+1)$-dimensional cube can be defined by taking two copies of the k-dimensional cube and connecting all corresponding vertices. The number of edges is $k \cdot 2^{k-1}$—sum the degrees of the vertices and divide by two.

We can make this more explicit as follows. Label the vertices of the 1-cube 0 and 1. Then to get the 2-cube we take two copies of the 1-cube, which we denote by prefixing the vertices of one cube with 0s and the other with 1s. So the vertices are 00, 01, 10, and 11. In general, the k-cube will have vertices which are strings of 0s and 1s of length k. The edges

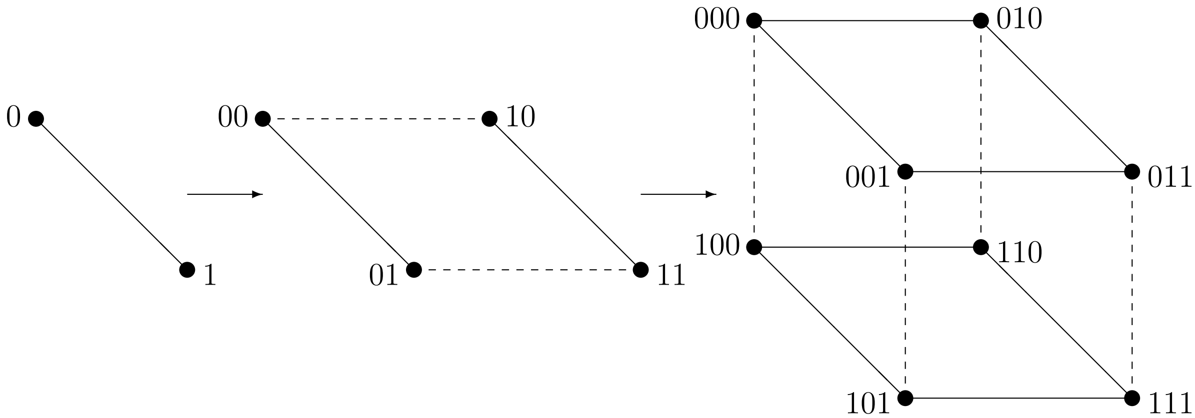


Figure 4: A 1-cube, 2-cube, and 3-cube, with vertices labeled

connect vertices whose strings differ in exactly one place.

So, what is $|\mathrm{Aut}(Q_k)|$? There are several symmetries which are immediately apparent. First of all, we can permute the coordinates of the strings, giving $k!$ automorphisms. Also, we can toggle the digits in a specified location in the strings. This is geometrically represented by a reflection through the k^{th} median. So there are at least $k! \cdot 2^k$ automorphisms.

Exercise 13. Prove that there are exactly $k! \cdot 2^k$ automorphisms of Q_k.

3 Automorphisms of trees

We are interested in another proof of Cayley's formula. Look at the number of trees on n vertices. We can divide them into classes by looking at the maximum distance between any two vertices.

For example, if $n = 5$, there are only three different types of trees, shown in Figure **??**.

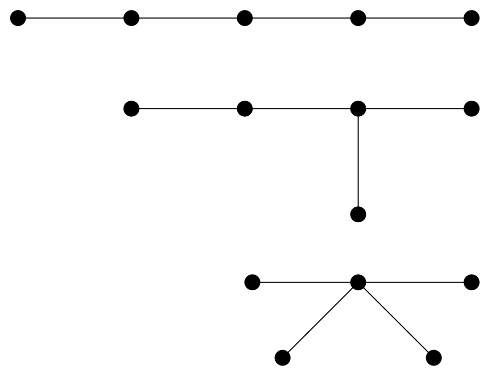
Now, how many trees are there of each of these types?

The line P_4 has two automorphisms, so there are $\frac{5!}{2} = 60$ trees of this type, which we see by counting the number of ways of ordering $1, 2, 3, 4, 5$ and dividing by two to correct for the overcount.

There are also $\frac{5!}{2}$ trees of the second type. More generally,

Lemma 14. The number of ways to place a graph G on a set of n vertices is $\frac{n!}{|\mathrm{Aut}(G)|}$.

This also tells us that the number of different ways of labeling the vertices of the last tree is $\frac{5!}{4!} = 5$.



$\frac{5!}{2} =$ 60 ways to label vertices

$\frac{5!}{2} =$ 60

$\frac{5!}{4!} =$ 5

125

Figure 5: Trees on 5 vertices

So the total number of trees in this case is $60 + 60 + 5 = 125 = 5^3$, verifying Cayley's formula.

4 Probability

If you fix n and pick a random graph on n vertices, what is the expected number of automorphisms? Picking a random graph means flipping a coin for each pair of vertices in order to determine whether that edge will be in the graph. Thus a random graph on n vertices is determined by $\binom{n}{2}$ coin flips.

Exercise* 15. Pr(a random graph has a nontrivial automorphism) $\to 0$ as $n \to \infty$.

Some discussion of the above exercise: Let $V = \{1, 2, \ldots, n\}$. What is the number of graphs on this set of vertices? We saw that it was $2^{\binom{n}{2}}$. We can also think of this as the number of **spanning subgraphs** of K_n, that is, the number of subgraphs of K_n on all the n vertices.

What is the number of spanning subgraphs of a graph G? It will be 2^m, where m is the number of edges. (A spanning subgraph is different from a subgraph, because general subgraphs are allowed to delete vertices.)

5 Counting graphs

Let g_n be the number of nonisomorphic graphs on n vertices.

We can establish some bounds on g_n. Clearly $2^{\binom{n}{2}}$ is an upper bound. Also $\frac{1}{n!} \cdot 2^{\binom{n}{2}}$ is a lower bound, because any given graph has at most $n!$ automorphisms.

To give a detailed proof of the lower bound, we know there are $2^{\binom{n}{2}}$ graphs on n vertices. If we divide these up into equivalence classes of isomorphic graphs and count the number of equivalence classes, then we get the number of graphs on this set of vertices. Now we know that each class has at most $n!$ graphs in it, thus the lower bound follows. Then we have the following easy fact

$$\log_2 g_n \sim \binom{n}{2} \sim \frac{n^2}{2} \tag{5.0.1}$$

A harder theorem is

Theorem 16. $g_n \sim \frac{1}{n!} 2^{\binom{n}{2}}$.

This is related to the fact that, as $n \to \infty$, the probability of a graph having a nontrivial automorphism goes to 0. In fact,

Theorem 17. $E(|\mathrm{Aut}(G)|) \to 1$ as $n \to \infty$.

Theorem 18. $\Pr(|\mathrm{Aut}(G)| \geq 2) \to 0$ as $n \to \infty$.

What is the relationship between these three theorems?

Exercise 19. Prove that

- Theorem **??** implies Theorem **??**.
- Theorem **??** is equivalent to Theorem **??**.

Exercise 20.** Prove Theorem **??**.

6 Symmetric Groups

Definition 21. A_5 is the group of even permutations of 5 points. $|A_5| = 60$.

Exercise 22. Prove that the group of orientation-preserving symmetries of the dodecahedron is isomorphic to A_5. (There are 120 symmetries total, but half of them are orientation-reversing.)

Exercise 23. The group of automorphisms of the dodecahedron is *not* isomorphic to S_5.

Exercise 24. The group of automorphisms of Petersen's graph is isomorphic to S_5. (Hint: this is an ah-ha! proof.)

Exercise 25. The group of orientation-preserving automorphisms of the cube is S_4. (Try this before you try to prove anything about the dodecahedron!)

7 Rubik's Cube

What is the number of configurations of the Rubik's cube?

An easier question: suppose you are allowed to pull the Rubik's cube apart and then put it back together in any way, leaving each center cube untouched. (You are not allowed to peel off the labels.) In this setting there are more configurations. What is the number of different arrangements you can get?

How can we form a Rubik's cube configuration? Corners can only switch places with corners, and so on. There are 12 edge cubies and 8 corner cubies. Each edge cubie can be flipped, giving 2^{12} possibilities for each fixed permutation. Also, there are 12! permutations, so $12! \cdot 2^{12}$ possibilities. Each corner can be rotated in 3 ways, so there are $8! \cdot 3^8$ arrangements. These symmetries form a group, which gives the Rubik's cube "supergroup," $\hat{G}$. The size of this group is

$$|\hat{G}| = 2^{12} \cdot 3^8 \cdot 12! \cdot 8!$$

The question is, how much smaller is the group G of actual configurations of the Rubik's cube? Well, for example, you cannot flip just one edge; you must flip an even number. This takes out a factor of 2. Also, if you sum the rotations of the corners, you must get a number which is $0 \pmod 3$. Finally, you can't just switch two edges; if you want to switch two edges, you must also switch either another pair of edges or a pair of corners.

In fact, $|G| = \frac{1}{12}|\hat{G}|$. To prove this, we want to find some invariants. Claim: every legal move made with the Rubik's cube is an even permutation on the set of all cubies. Proof: rotating one side a quarter-turn gives a 4-cycle on the edges and a 4-cycle on the vertices. Thus every legal configuration differs from the solved position by an even permutation.

Exercise 26. Prove rigorously that $|G| = \frac{1}{12}|\hat{G}|$. The above methods can be used to show $\leq$; to also show $\geq$, you must find generators which enable you to achieve $\frac{1}{12}|\hat{G}|$ permutations. Or, you could show that $G \triangleleft \hat{G}$ and $\hat{G}/G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. (This is harder.)

Theorem 27 (Frucht, 1938). Every finite group H is isomorphic to the automorphism group of some finite graph G.

Theorem 28 (Babai). The quaternion group of order 8 is not isomorphic to the automorphism group of any planar graph.

8 Matchings

Definition 29. A **matching** in a graph is a set of disjoint edges. A **perfect matching** is a set of $n/2$ disjoint edges, where n is (as always) the number of vertices.

Definition 30. A **bipartite graph** is a 2-colorable graph. The **complete bipartite graph**

$K_{k,\ell}$ consists of k red vertices, ℓ blue vertices, and an edge connecting every pair of vertices of different colors.

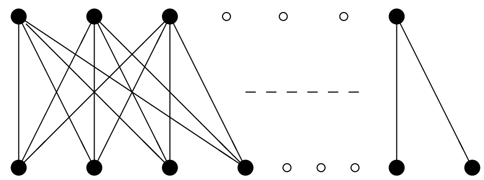


Figure 6: A complete bipartite graph.

So $K_{k,\ell}$ has $k + \ell$ vertices and $k\ell$ edges.

Suppose in a society each person wants to marry a person of the opposite gender, and each lists the people they are willing to marry in order of preference. Then if we find a perfect matching and marry off the corresponding couples, then everyone will have a spouse. However, this might not be a **stable** matching—it may be, for example, that a is married to A and b is married to B, but a prefers B to A, and B prefers a to b. (Here the notation is that females are uppercase and males are lowercase.) Therefore this matching can be improved by divorcing both couples and marrying a to B, then A and b will look for new spouses (possibly each other).

We define a notion of stable matching as the matching that nobody mutually prefers their spouse to somebody else as explained above. Note that there may be more than one stable matching given the preferences. Given the preferences is there a way to make everyone as happy as possible?

There is an algorithm, called “Man proposes algorithm”. The first man goes down his list until he finds a woman willing to marry him. Then the second man does the same, and so on. In this algorithm women accept the proposal if there is no better chance until that time, but still they might change their mind later, in the case that someone better shows up (ranked higher in their list.) In this case the divorced husband will keep proposing the next woman down in his list. Given that there are equal number of men and women, this algorithm is proven to yield a stable matching regardless of the preferences.

However, we can introduce a notion of a “better” stable matching. M_1 dominates another stable matching, M_2, if every person is at least as happy with their spouse in M_1 as they would be with the partner they are matched in M_2. It turns out that man proposes algorithm results in a stable matching which is optimal for men, and “pessimal” for women—that is, the worst stable matching from the women’s point of view.

In fact, it is another theorem which proves that the stable matchings favoring men and women are diametrically opposite. That is, there is a partial ordering of stable matchings from the men’s point of view, and another from the women’s point of view, and the women’s ordering is given by exactly flipping the partial ordering from the men's point of view. This is regardless of the individual preferences.

There is another version of this example, where $k \neq \ell$ and some people are allowed to have multiple partners (e.g. employer-employee relationships, or medical interns being assigned to hospitals, or ...). In fact, the American Medical Society has an algorithm that they use for assigning interns to hospitals. For many years they used an algorithm which assigned a hospital-optimal stable matching. But then mathematicians taught economists about this problem, and economists influenced the medical society, and so now an intern-optimal matching is reached. Similar algorithms are used in some states in assigning students to schools.

This was first published by Gale and Shapley in 1962. Less effective algorithms have been used by various organizations for a long time, but they often led to assignments which were not stable.