Maths 190 Lecture 23

- **Topic for today**: Secret sharing and zero knowledge proofs
- **Question of the day 1**: Can you tell two people a secret so that neither of them know it?
- **Question of the day 2**: Can you convince someone that you know the solution to a problem without telling them the answer?

Nothing from today's lecture is in the textbook, or will be in the exam.

Secret Sharing

- Suppose I have a secret, which is the answer ‘yes’ or ‘no’ to some question.
- How can I tell the answer to two people so that:
  - Neither of them knows the answer;
  - Together, they know the answer.

Secret Sharing

Is it possible for:

- A question with three possible answers.
- A question with a ‘yes’ or ‘no’ answer and I want to tell it to three people so that none of them know the answer, no pair of them know the answer, but all 3 of them know the answer.

Secret Sharing

General method:

- Suppose I have a secret s which can be encoded as a number between 0 and $n-1$.
- Suppose I want to share the secret with t people.
- Then I generate $t-1$ random numbers $s_1, s_2, \ldots, s_{t-1}$ between 0 and $n-1$.
- Set $s_t = s - s_1 - s_2 - \cdots - s_{t-1} \mod n$.
- Give person i share s_i.

Secret Sharing

- There is even a way to give $m > t$ people shares, so that any t of them can know the secret, but any $t - 1$ (or fewer) of them do not!
- These ideas have important applications in information security.
- For example, some critical computer systems require a collection of authorized users to enter passwords together before certain operations can be performed.

Zero knowledge proofs

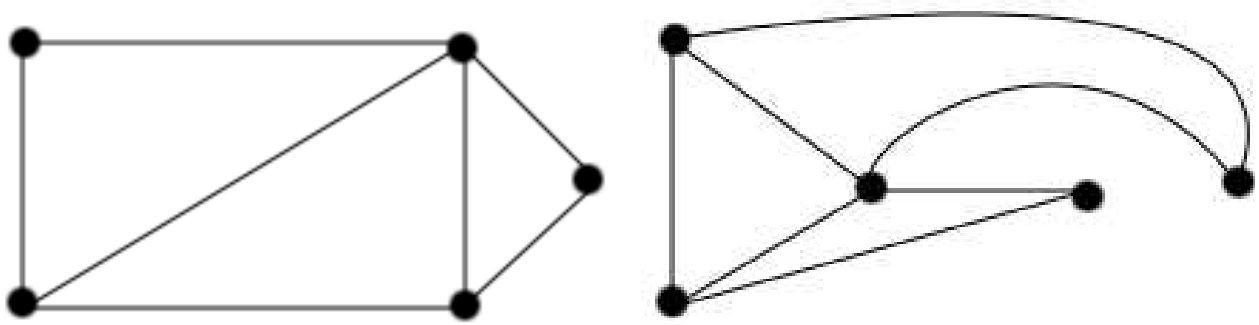
Can you convince someone that you know the solution to a problem without telling them the answer?

Example: Where's Wally?

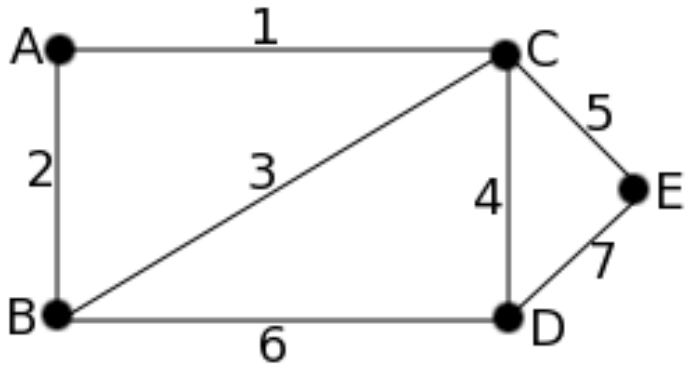
Graph isomorphism problem

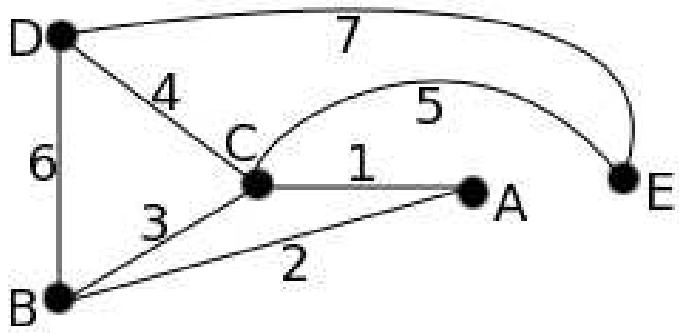
Two graphs are **isomorphic** if there is a one-to-one correspondence between the vertices of each graph and a corresponding one-to-one correspondence between the edges of each graph.

Are these graphs isomorphic?

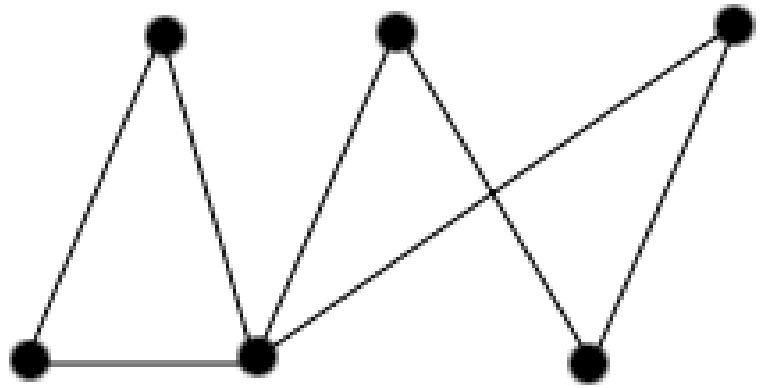


Isomorphic graphs





Draw a graph isomorphic to this



Proving I know an isomorphism

- It is a hard computational problem to find an isomorphism between two graphs (at least, when the number of vertices and edges is very large).
- Given a graph, it is easy to construct a "random" isomorphic graph, together with the isomorphism between them.
- Suppose I give you two graphs, for which I know an isomorphism between them.
  How can I convince you that I know an isomorphism between them without telling you the answer?

Proving I know an isomorphism

- Let G_1 and G_2 be the graphs.
- I can construct a graph G_3 which is isomorphic to G_2, together with the isomorphism between them.
  I therefore also know the isomorphism from G_1 to G_3 by composing the isomorphism from G_1 to G_2 with the isomorphism from G_2 to G_3.
- I tell you G_3.
- You flip a coin, and ask me to show that G_3 is isomorphic to either G_1 or G_2 (but not both!)
- We repeat this several times.

Zero knowledge proofs

- The above idea is called a **zero knowledge proof**.
  It convinces you that I know an isomorphism from G_1 to G_2.
- The proof does not tell you an isomorphism between G_1 and G_2.
  Indeed, the proof does not help you find the isomorphism in any way.
- If I don't know the isomorphism then I can construct a graph G_3 which is isomorphic to either G_1 or G_2, but I will only be able to correctly respond to your challenge (coin flip) with probability $1/2$.

Zero knowledge proofs

- There are zero knowledge proofs for solutions to "most" problems.
  (**Theorem:** All problems in NP have zero-knowledge proofs.)
- These ideas are used in cryptography (the study of secret communication and authentic communication).
  In particular, they can be used for authentication schemes which are much better than passwords.

Important ideas from today

Mathematical ideas can be used to construct methods to solve problems you might not have thought were possible.

In particular, we discussed sharing secrets, and proving knowledge of something without revealing the answer.

Nothing from today's lecture is in the textbook, or will be in the exam.

Wednesday's lecture will be a revision lecture, and I will go over the assignment solution.

There are no tutorials this week.