DEPARTMENT OF MATHEMATICS

MATHS 190 Lecture 23 Summary

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, but together they know the answer?

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.

- 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 has applications in information security.

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

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.

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). But, given a graph, it is easy to construct a "random" isomorphic graph, together with the isomorphism between them.

If I have two graphs G_1 and G_2 and I know an isomorphism between them, then there is a zero knowledge proof which convinces you that I know an isomorphism from G_1 to G_2, but does not tells you what the isomorphism is.

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 using passwords.