Topics in Algebra: Cryptography - Blatt 8

11.30-12:15, Seminarraum 9, Oskar-Morgenstern-Platz 1, 2.Stock

http://www.mat.univie.ac.at/~gagt/crypto2018

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1. Is the Hamming distance indeed a distance?

Question 2. Given a linear code C, is its generating matrix uniquely defined?

Question 3. Is the complete graph $K_{3,3}$ a bipartite expander?

Question 4. Let Y be a non-bipartite expander with expansion parameter λ. What is the expansion parameter of the bipartite expander X constructed from Y (constructed in the lecture notes)? What about the diameter and the girth of X (supposing we know the diameter and the girth of Y)?

2 Exercises

Question 5. Let X be a finite d-regular graph with girth $g \geq 3$. Prove that

$$|X| \geq d(d-1)^{\lfloor (g-3)/2 \rfloor}.$$

Question 6. Let $\{X_i\}$ be a d-regular expander family. Show that $d > 2$.

Question 7. What's the difference between the interior and exterior boundaries of a subset of vertices? Can we measure one in terms of the other?

Question 8. Let X be a finite graph of cardinality n, and let A be the matrix with entries a_{xy} =number of edges between $x, y \in V(X)$.

i) Show that A^k has entries that count the number of walks of length k in X.

ii) Let D be the diagonal matrix with entries $D_{xx} = \mathrm{deg}(x)$ for each $x \in V(X)$ and let $\Delta = D - A$. Show that X is connected if and only if the multiplicity of the eigenvalue 0 is 1. Can you generalise this to the situation where X has k connected components?

The goal of question 8 is to show how graphs and their properties can be encoded in linear algebra. The matrix A is called the *adjacency matrix*, D the *degree matrix* and Δ the *graph laplacian*. The operator Δ encodes what happens to neighbours - if we feed into this the characteristic functions of subsets of vertices with size less than $|V(X)/2|$, we can connect this matrix to the boundary of a set defined in the class. In this way, we can link geometric expansion to the spectrum of eigenvalues of Δ. We'll talk more about this in the class.