Topics in Algebra: Cryptography - Blatt 5

http://www.mat.univie.ac.at/~gagt/crypto2019

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 k given in the example of the LFSR the period?

Question 2. Show that the matrix obtained from the linear equations of the Linear Feedback Shift register is invertible mod 2.

Question 3. Consider the LFSR as a bit generator. What are, in this case, the values of k and l for the definition of a bit generator?

Question 4. Is the Hamming distance indeed a distance?

Question 5. Given a linear code C, is its generating matrix uniquely defined?

Question 6. Is the complete graph $K_{3,3}$ a bipartite expander?

Question 7. 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 8. Suppose that Alice is using the ElGamal signature scheme. In order to save time in generating random numbers k such that are used to sign messages, Alice choses an initial random value k_0 and then signs the i^{th} message using the value $k_i = k_0 + 2i \mod p - 1$ (note that this means $k_i = k_{i-1} + 2 \mod p - 1$).

i) Suppose that Bob observes two consecutive signed messages

$$(x_i, \mathtt{sig}(x_i, k_i))$$

and

$$(x_{i+1}, \mathtt{sig}(x_{i+1}, k_{i+1})).$$

Describe how Bob can easily compute Alice's secret key a given this information without solving an instance of the discrete logarithm problem. Is this method independent of i?

ii) What if random values follow another recusive relation - would this still allow us to do as above?

iii) (Practical) Suppose that the parameters of the scheme are $p = 28703$ and $\alpha = 5, \beta = 11339$, and the two messages observed by Bob are:

$$x_i = 12000, \mathtt{sig}(x_i, k_i) = (26530, 19862)$$
$$x_{i+1} = 24567, \mathtt{sig}(x_{i+1}, k_{i+1}) = (3081, 7604).$$

Find the value of a using the attack from part i).

Question 9. Let f be a bit generator that only produces sequences in which exactly $l/2$ bits have value 0 and $l/2$ bits have value 1. Define the function **dst** by:

$$\mathbf{dst}(z_1, ..., z_l) = \begin{cases} 1 \text{ if } (z_1, ..., z_l) \text{ has exactly } l/2 \text{ bits equal to } 0 \\ 0 \text{ otherwise.} \end{cases}$$

i) Show that $E_{\mathbf{dst}}(p_u) = \frac{\binom{l}{l/2}}{2^l}$.

ii) Show also that $E_{\mathbf{dst}}(p_f) = 1$.

iii) Finally, show that for any fixed $\epsilon > 0$, that p_u and p_f are ϵ-distinguishable if l is sufficiently large.

Question 10. 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 11. Let $\{X_i\}$ be a d-regular expander family. Show that $d > 2$.

Question 12. 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 13. 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.