Dr. Maurice Cochand
Assistant: Jan Volec

# Problem sheet 4

**1.** Suppose your receive a word $w'$ in code BHC $[15, 7, 5]$. Recall that we considered $GF_2[X]/(X^4+X+1)$ as a vector space with basis $\{1, x, x^2, x^3\}$ and the decoding procedure was done by applying $w' \in \{0,1\}^{15}$ to the $8 \times 15$-matrix

$$B = \begin{bmatrix} x^0 & x^1 & \dots & x^{14} \\ x^{3\cdot 0} & x^{3\cdot 1} & \dots & x^{3\cdot 14} \end{bmatrix}.$$

If $Bw' = (S_1, S_3) \neq 0$ the message has been corrupted by one or two bit flips. Let us assume $Bw' = (1, 1, 0, 0, 1, 1, 0, 1)$.

**a)** Write $S_1$ and $S_3$ as polynomials and show that there are two errors, i.e., $S_3 \neq S_1^3$.

**b)** Invert $S_1$ and calculate $S_1^{-3} S_3$.

**c)** Give the two faulty bit positions (see handout [EC4]).

**2.** In order to construct a family of expander graphs explicitly, we will make use of so-called $LD_{p,t}$-graphs which are defined in algebraic means. Let $p$ be a prime and $t$ an integer so that $t < p$. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the finite field of $p$ elements and $V(LD_{p,t}) = \mathbb{F}_p^{t+1}$ the $t+1$ dimensional vector space over $\mathbb{F}_p$. For every vertex $a \in \mathbb{F}_p^{t+1}$, we index the set of the edges incident to $a$ edges by $\mathbb{F}_p^2$. Specifically, we define the edge set $E(LD_{p,t})$ to be

$$\{(a, a + \beta(1, \alpha, \alpha^2, \dots, \alpha^t)) : a \in \mathbb{F}^{t+1}, (\alpha, \beta) \in \mathbb{F}_p^2)\}.$$

Note that a vertex $a$ has exactly $p^2$ edges connected to it (and $p$ of them are loops). In order to study the spectral properties of the adjacency matrix of this graph, it will be useful to construct a good basis of eigenvectors: For $a \in \mathbb{F}_p^{t+1}$, define the vector $v_a = (v_a(b))_{b \in \mathbb{F}_p^{t+1}} \in l^2(\mathbb{C}_p^{t+1})$ coordinate-wise by

$$v_a(b) = \omega^{\sum_j a_j b_j}$$

where $\omega = e^{2\pi i/p}$ is a primitive $p$th root of unity. Prove that the set $\{v_a \ : \ a \in \mathbb{F}_p^{t+1}\}$ is an orthogonal system with respect to the standard inner product $\langle v, w \rangle = \sum_j v_j \overline{w}_j$.

*Hint: Recall that* $\sum_{k=0}^{p-1} \omega^k = 0$.

**Please turn over!**

**3.** Use the notation from the notes [Z1-Z3] on the Zig-Zag product and prove that

$$\|(\tilde{A}x^{\|})^{\|}\| \leq \overline{\lambda}_G \|x^{\|}\|.$$

**4.** The $n$ citizens of the "Land of Make Believe" have elected a new president among two candidates. The electronic voting system claimed that the winner got at least 3/4 of the votes, however, unfortunately it forgets who the winner is! Since time is money, it has been decided to not go through all the votes again but choose the president as follows:

Let $G(V, E)$ be a $d$-regular $\lambda$-expander with $|V| = n$.

- Identify the citizens with the node set $V$.
- Chose a citizen $v$ at random.
- The candidate getting the majority of votes in $N(v)$, the set of the $d$ neighbors of $v$, will be the new president!

Prove that the probability of choosing the wrong candidate can be upper bounded by $4\left(\frac{\lambda}{d}\right)^2$.

For any questions concerning the exercises, you can write an email to Jan Volec, `jan@ucw.cz`.