Seminar 12

(3,2)-party check code is a 2-digits message, with a 3-digits code, where the first digit is the sum of the 2 digits of the message, computed modulo 2.

(3,1)-repeating code is a 1-digit message, with a 3-digits code, where the first and the second digits repeat the code.

$p \in \mathbb{Z}_2[X]$ of degree $n-k$ is a generator of a polynomial code (n,k), whose words are polynomials of degree less then n, divisible by p.

For a (n,k) polynomial code, we have 2^k code words. For a message m, we transform it as $m \cdot X^{n-k} = qp + r$, where $degree(r) < degree(p) = n-k$. And we code it as $v = r + m \cdot X^{n-k}$.

A **party check matrix** looks like $H = (I_{n-k} \mid P)$. And a vector $u \in M_{n,1}(\mathbb{Z}_2)$ is a code vector $\iff H \cdot u = 0$.

Hamming distance: u, v of the same length $\Rightarrow$ the number of positions in which they differ. We denote it by $d(u,v)$, which is a metric on $\mathbb{Z}_2^n$.

A code detects all erros $\leq t \iff min(d(u,v)) \geq t+1$. And it can correct all errors $\leq t \iff min(d(u,v)) \geq 2t+1$.

An **enconder** is $\gamma : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ with $[\gamma]_{EE'} = G$.

1. (i) $110 \to 1 = (1+0) \pmod 2$. This is true, so it does not have detectable errors.

   $010 \to 0 = (1+0) \pmod 2$. This is not true, so it contains a detectable error.

   The same goes for all, so the words with detectable errors are :$010, 001, 111$.

   (ii) $111 \to 11$ repeat the message 1.

   $011 \to 01$ repeat the message 1.

   The same for all, except the last one $001 \to 00$ does not repeat the message 1.

2. Let $f = X^7 + X^6 + X^4 + X^3 + 1$ and $g = X^6 + X^3 + X^2 + X$.

   We have the code $(8,4)$, so $n = 8$ and $k = 4$.

   We compute $f : p$, which gives us the quotient $X^3 + X$ and the reminder $X^3 + X + 1$. So f is not divisible by p, hence f is not a code word.

   We compute $g : p$, which gives us the quotient $X^2 + X$ and no reminder. So $p \mid g$, hence g is a code word.

3. For the code $(6,3)$ we have $n=6$ and $k=3$.

   We have $2^k = 2^3 = 8$ words $\Rightarrow$ The messages are $\{000, 001, 010, 100, 011, 101, 110, 111\}$.

   We take the first word $000 = m$. We compute $m = 0 \cdot X^0 + 0 \cdot X^1 + 0 \cdot X^2 = 0$. So $m \cdot X^{n-k} = 0$.

   Now, we compute $r = m \cdot X^{n-k} \pmod p \Rightarrow r = 0$.

   And, in the end $v = r + m \cdot X^{n-k} \Rightarrow v = 0 \Rightarrow 000000$ (the same number of digits as n).

   We do this for all words and we get:

   $001 \to m = 0 \cdot X^0 + 0 \cdot X^1 + 1 \cdot X^2 \to mX^{n-k} = X^5 \to r = X + 1 \to v = 1 + X + X^5 \to 110001$

   $010 \to mX^{n-k} = X^4 \to r = X^2 + X + 1 \to v = 1 + X + X^2 + X^4 \to 111010$

   $100 \to mX^{n-k} = X^3 \to r = X^2 + 1 \to v = 1 + X^2 + X^3 \to 111000$

   $011 \to mX^{n-k} = X^4 + X^5 \to r = X + 1 \to v = X^5 + X + 1 \to 110001$

   $101 \to mX^{n-k} = X^3 + X^5 \to r = X^2 + X \to v = X + X^2 + X^3 + X^5 \to 011101$

   $110 \to mX^{n-k} = X^3 + X^4 \to r = X \to v = X + X^3 + X^4 \to 010110$

   $111 \to mX^{n-k} = X^3 + X^4 + X^5 \to r = 1 \to v = 1 + X^3 + X^4 + X^5 \to 100111$

4. We have $n=5$ and $k=3$ and $H = (I_{n-k} \mid P) \Rightarrow H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$.

   For a vector $u = (u_1, u_2, u_3, u_4, u_5)$ we need to solve the system $H \cdot u = O_2$.

   So, we get the system $\begin{cases} u_1 + u_5 = 0 \\ u_2 + u_3 + u_4 + u_5 = 0 \end{cases}$

   $\Rightarrow u = (u_2 + u_3 + u_4, u_2, u_3, u_4, u_2 + u_3 + u_4)$

   $\Rightarrow \{(0,0,0,0,0), (1,1,0,0,1), (1,0,1,0,1), (1,0,0,1,1), (0,1,1,0,0,), (0,0,1,1,0), (0,1,0,1,0), (1,1,1,1,1)\}$.

5. We compute $H = (I_5 \mid P) \Rightarrow H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$.

For a vector $u = (u_1, u_2, \ldots, u_9)$, we compute $H \cdot u = O_9$ and we solve the system that forms.

In the end, we get the vector:

$u = (u_8, u_7 + u_9, u_6 + u_8 + u_9, u_7, u_6 + u_9, u_6, u_7, u_8, u_9)$.

$\Rightarrow \{000000000, 001011000, 010100100, 101000010, 011010001, 011111100, 100011010, 010001001, 111100110, 001110101, 110010011, 110111110, 000101101, 111001011, 100110111\}$.

Now, for the Hamming distance we need $min(d(u_i, u_j))$. For that, we must compute $min(d(u_1, u_i)) = min(d(u_2, u_i)) = \cdots = min(d(u_9, u_i)) = 3$.

As $min(d(u_i, u_j)) = 3 \geq t + 1 \Rightarrow t \leq 2 \Rightarrow$ the code detects 2 errors.

And, as $min(d(u_i, u_j)) = 3 \geq 2t + 1 \Rightarrow t \leq 1 \Rightarrow$ the code can correct 1 error.

6. From $G = [\gamma]_{EE'} \Rightarrow \begin{cases} \gamma(e_1) = 001011000, e_1 = 1000 \\ \gamma(e_2) = 010100100, e_2 = 0100 \\ \gamma(e_3) = 101000010, e_3 = 0010 \\ \gamma(e_4) = 011010001, e_4 = 0001 \end{cases}$

   For $1101 = e_1 + e_2 + e_4 \Rightarrow \gamma(1101) = \gamma(e_1) + \gamma(e_2) + \gamma(e_4) = 001011000 + 010100100 + 011010001 = 000101101$.

   For $0111 = e_2 + e_3 + e_4 \Rightarrow \gamma(0111) = \gamma(e_2) + \gamma(e_3) + \gamma(e_4) = 100110111$.

   For $0000 = e_1 + e_2 \Rightarrow \gamma(0000) = \gamma(e_1) + \gamma(e_2) = 000000000$.

   For $1000 = e_1 \Rightarrow \gamma(1000) = \gamma(e_1) = 001011000$.

7. We have $\gamma : \mathbb{Z}_2^1 \to \mathbb{Z}_2^4$, with $[\gamma]_{EE'} = G$, where $E = (e_1) = 1$ and $E' = (e'_1, e'_2, e'_3, e'_4)$.

   For $e_1 = 1 \Rightarrow m = 1 \Rightarrow mX^{n-k} = X^3 \Rightarrow r = X^2 + X + 1 \Rightarrow v = 1 + X + X^2 + X^3 \Rightarrow 1111$.

   Hence, $G = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} P \\ I_k \end{bmatrix} \Rightarrow P = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$.

   Now, $H = (I_{n-k} \mid P) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$.

8. We have $\gamma : \mathbb{Z}_2^3 \to \mathbb{Z}_2^7$, with $[\gamma]_{EE'} = G$, where $E = (e_1, e_2, e_3)$ and $E' = (e'_1, e'_2, e'_3, e'_4, e'_5, e'_6, e'_7)$.

   For $e_1 = (1,0,0) \Rightarrow 100 \Rightarrow m = 1 \Rightarrow mX^{n-k} = X^4 \Rightarrow r = 1 + X^2 + X^3 \Rightarrow v = 1 + X^2 + X^3 + X^4 \Rightarrow 1011100$.

   For $e_2 = (0,1,0) \Rightarrow 010 \Rightarrow m = X \Rightarrow mX^{n-k} = X^5 \Rightarrow r = 1 + X^2 \Rightarrow v = 1 + X + X^2 + X^5 \Rightarrow 1110010$.

   For $e_3 = (0,0,1) \Rightarrow 001 \Rightarrow m = X^2 \Rightarrow mX^{n-k} = X^6 \Rightarrow r = X + X^2 + X^3 \Rightarrow v = X + X^2 + X^3 + X^6 \Rightarrow 0111001$.

   Hene, $G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$