13.12.2023

$f \in \mathrm{End}_{\mathbb{R}}(V)$

$\lambda \in \mathbb{R}$ eigenvalue if $\exists\, v \in V \setminus \{0\}$ s.t.

$f(v) = \lambda v$, v is called an eigenvalue

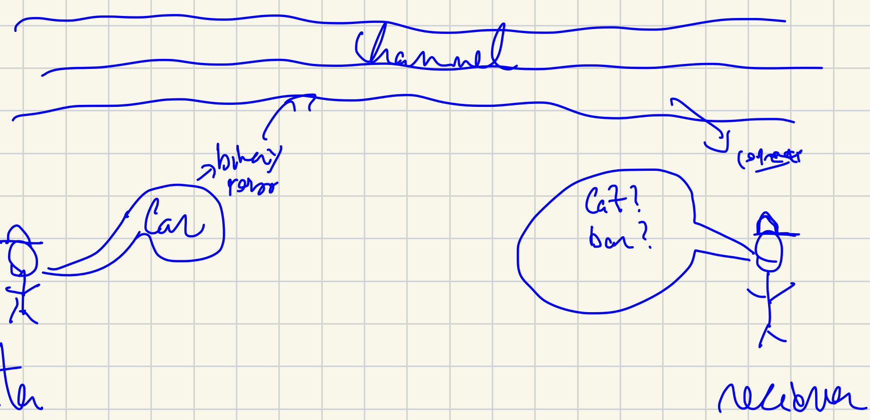
λ eigenvalue $\Leftrightarrow$ λ root of $P_f(x)$

$P_f(x) = \det([f]_B - X I_n)$

Eigenspace:

$$S(\lambda) = \{ v \in V \mid \underbrace{f(v) = \lambda v}_{\Leftrightarrow\ [f]_B \cdot [v]_B = \lambda \cdot [v]_B} \}$$

Codes



$n-k$ bits	k bits
check digits	message

$\to$ (n, k) code $(n > k)$

$\mathbb{Z}_2 = \{0, 1\}$ field

1+1 = 0 not 10 !

$\gamma : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$

encoder

linear code $\to$ γ linear map

$\hookrightarrow$ $\operatorname{Im}\gamma \leq \mathbb{Z}_2^n$

$\operatorname{Im}\gamma = \mathcal{C}$ = the set of codewords

$$[\gamma]_{E,E'} = \left[\, \gamma(e_1)_{E'} \; \ldots\ldots \; \gamma(e_k)_{E'} \,\right]$$

$\hookrightarrow$ generator matrix of the code $= G$

To encode $m \in \mathbb{Z}_2^k$ we do $G \cdot [m]_E$

$$G = \left(\frac{P}{I_k} \right) \in M_{n,k}(\mathbb{Z}_2)$$

$H = (I_{n-k} \mid P) \in M_{n-k,n}(\mathbb{Z}_2)$

↳ parity check matrix

If $v \in \mathbb{Z}_2^n$ then $v \in \mathcal{C} \implies H \cdot [v] = 0$

<u>Hamming distance between two vectors</u>

$d_H(v, v')$ = # of positions on which v and v' disagree

$= w(v, v')$

↳ # of 1's

$d_H(\underline{1}0\underline{0}10, \underline{0}0\underline{1}10) = 2$

$w(\underline{1}0\underline{1}00) = 2$

↳ $v + v'$

$d(\mathcal{C}) = \min d_H(v, v')$

↳ min hamming distance

We can detect at most $d(\mathcal{C}) - 1$ errors.

We can correct at most $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ errors. $\rightarrow$ floor value.

$d(\mathcal{C})$ = min # col in H that add up to a zero column.

5. Determine the minimum Hamming distance between the code words of the code with generator matrix $G = \left(\frac{P}{I_4}\right) \in M_{9,4}(\mathbb{Z}_2)$, where:

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Discuss the error-detecting and error-correcting capabilities of this code, and write down the parity check matrix.

6. Encode the following messages using the generator matrix of the (9,4)-code of Exercise **5.**: 1101, 0111, 0000, 1000.

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} = (I_{n-k} \mid P)$$

no zero-column $\Rightarrow d(\mathcal{C}) \geq 1$

$d(\mathcal{C}) \geq 2$ (no identical column)

$d(\mathcal{C}) = 3$ $(\mathcal{C}_3 + \mathcal{C}_5 + \mathcal{C}_6 = 0)$ $\Rightarrow$

$\Rightarrow$ we can detect 2 errors and we can correct 1.

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

ADD

$$G \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 0_{91} \; ; \quad G \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$G \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The (n,k) polynomial code generated by

$P \in \mathbb{Z}/_2[x]$

If $\deg P = n-k$ $\Rightarrow$ this is a linear code.

ex $n=5$ $k=3$ $P = x^2 + x$

Step 1: write the message as a polynomial

$m = a_0 a_1 \dots a_{k-1} \rightarrow P_m = a_0 + a_1 x + \dots + a_{k-1} x^{k-1}$

ex 101

$\rightarrow 1 + x^2$

Step 2: Multiply P_m by x^{n-k}

$F_m = x^{n-k} \cdot P_m$

ex $x^2(1+x^2) = x^4 + x^2$

Step 3 Divide F_m by P (Euclidean division)

$F_m = P \cdot q + R_m$

$$
\begin{array}{l|l}
x^4 + x^2 & x^2 + x \\
\hline
x^4 + x^3 & x^2 + x \\
\cline{1-1}
x^3 + x^2 & \\
x^3 + x^2 & \\
\cline{1-1}
/ &
\end{array}
$$

Step 4 : Add F_m to R_m $\Rightarrow$ encoded polynomial.

$$F_m + R_m = x^4 + x^2 + 0$$

Step 5 : Convert the poly to a vector

$$x^4 + x^2 = 0\;0\;\boxed{1\;0\;1} \rightarrow$$ message with which we started with.

8. The (7,3)-code generated by $p = 1 + X^2 + X^3 + X^4 \in \mathbb{Z}_2[X]$.

$$G = [\gamma]_{E,E'} = [\gamma(e_1)_{E'}, \gamma(e_2)_{E'}, \gamma(e_3)_{E'}]$$

$e_1 = 100$

$e_2 = 010$

$e_3 = 001$

Determine G and H, $d(\mathcal{C})$ and the detection / correction capabilities of the [7, 3] code generated by $p = 1 + x^2 + x^3 + x^4 \in \mathbb{Z}/_2[x]$

• $m = e_1 = 100 \to \ell_m = 1$

$$F_m = x^{\overset{7-3}{4}} \cdot 1 = x^4$$

$$F_m = x^{n-k} \cdot \ell_m$$

shifting m-k digits to make room for the check digits.

$$\begin{array}{l|l} x^4 & x^4 + x^3 + x^2 + 1 \\ \cline{2-2} \underline{x^4 + x^3 + x^2 + 1} & 1 \\ x^3 + x^2 + 1 & \end{array}$$

$R_m = x^3 + x^2 + 1$

$R_m + F_m = x^4 + x^3 + x^2 + 1 \longrightarrow 1011\boxed{100}$

• $m = 010 \Rightarrow \ell_m = x$

$$F_m = x^4 \cdot x = x^5$$

$$\begin{array}{l|l} x^5 & x^4 + x^3 + x^2 + 1 \\ \cline{2-2} \underline{x^5 + x^4 + x^3 + x} & x + 1 \\ x^4 + x^3 + x & \\ \underline{x^4 + x^3 + x^2 + 1} & \\ x^2 + x + 1 & \end{array}$$

$R_m = x^2 + x + 1$

$$R_m + F_m = 1 + x + x^2 + x^5 \to 1110\boxed{010}$$

$$m = 001 \Rightarrow l_m = x^2$$

$$F_m = x^4 \cdot x^2 = x^6$$

$$
\begin{array}{l|l}
x^6 & x^4 + x^3 + x^2 + 1 \\
\hline
x^6 + x^5 + x^4 + x^2 & x^2 + x \\
\hline
x^5 + x^4 + x^2 & \\
x^5 + x^4 + x^3 + x & \\
\hline
x^3 + x^2 + x = R_m &
\end{array}
$$

$$R_m + F_m = x^6 + x^3 + x^2 + x$$

$$0111\boxed{001}$$

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

we have no zero-columns $\Rightarrow d(\mathcal{C}) > 1$

we have no 2 identical columns $\Rightarrow d(\mathcal{C}) > 2$

$C_5 + C_1 + C_3 + C_4 = 0 \Rightarrow d(\mathcal{C}) \leq 4$

$d(\mathcal{C}) = 4$

detection $= 3$

correction $= 1$