Űrkommunikáció
Space Communication
2023/7.

Linear block codes
Algebraic code construction; definitions

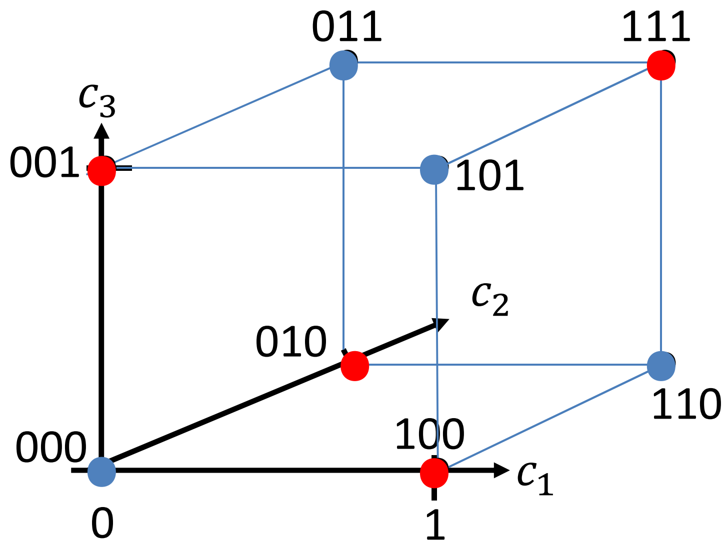
Linear vector space $\vec{V}$: The space is <u>closed</u> for linear operations (addition, multiplication).

$$\overline{v_i} + \overline{v_j} = \overline{v_k}\,; \quad \forall\ \overline{v_i}, \overline{v_j}, \overline{v_k}\ \epsilon\ \vec{V}$$

Code space $\vec{C}$, called Code: The valid code vectors are constituent parts of a linear subspace within a linear vector space.

$$\forall i:\ \overline{c_i}\ \epsilon\ \vec{C}\ \subset\ \vec{V}$$

E.g. ● Vectors yes, but ● vectors not



Linear independent part of a space:

$$\sum_i \overline{c_i} \neq \overline{0}\,;$$

E.g. every two but not three ●, except $\overline{0}$

101+011=110, de 101+011+110=000

Base of $\vec{C}$: A such set of linear independent $\overline{g_i}$ vectors, of which ones linear combination (weighted sum, weighted with the message symbols) generates every valid code vectors.

Linear block codes
Algebraic code construction; definitions

Base of $\vec{C}$; *Base of a Code*; *Generator matrix* $\bar{\bar{G}}$:

$$\overline{c_i} = \sum_{k=1}^{K} u_{i_k} \cdot \overline{g_k} = \overline{u_i} \cdot \begin{bmatrix} \overline{g_1} \\ \overline{g_2} \\ \vdots \\ \overline{g_K} \end{bmatrix} = \overline{u_i} \cdot \bar{\bar{G}}$$

Basis vectors: $\overline{g_i}$; The Generator matrix $\bar{\bar{G}}$ is the column vector of the basis vectors.

Because the space should be <u>closed</u> we need such linear arithmetic operations that not points out from the finite vector space. SO we need a finite mathematical field.

Évariste Galois

Galois Field, GF(q), finite q number of elements (symbols).

The size of the field is q either a prime number or power of prime.

GF(q), q=p or p^m

Galois Field, GF(q)

The elements of the field (symbols such as Arabic symbols for numbers):

$$GF(q) = \{0, 1, 2, \dots, q-1\}$$

Arithmetic operations over **prime**-size GF(q=p) Galois field:

Operations, $a, b \in GF(q)$:

Addition	Multiplication
$a \oplus b = a+b \bmod q$	$a * b = a \cdot b \bmod q$

Properties of operations:

Closed:	$a \oplus b = c \in GF(q)$	$a * b = c \in GF(q)$
Commutative:	$a \oplus b = b \oplus a$	$a * b = b * a$
Associative:	$(a \oplus b) \oplus c = a \oplus (b \oplus c)$	distributive: $(a*b)*c = a*(b*c)$
∃ null-element, 0:	$a \oplus 0 = a$	∃ unit-element, 1: $a * 1 = a$
Invers:	$a \oplus b = 0$; $a = -b$	$a * b = 1$; $a = 1/b$

The order of an element $a \neq 0 \in GF(q)$ is the smallest x, which $a^x = \underbrace{a * a * \cdots * a}_{x} = 1$

Primitive element α, which order x=q-1, thus $\alpha^{q-1} = 1$.

There exist at least one primitive element for every GF(q).

Examples for GF(q=p)

The elements of the field are the power of the primitive element

$$GF(q) = \{0, 1, 2, \ldots, q-1\} = \{\alpha^{-\infty}, \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\}$$

Remark: $\alpha^{q-1} = \alpha^0 = 1$

E.g. $GF(q = 7) = \{0, 1, 2, 3, 4, 5, 6\}$

Is 2 a primitive element? $\alpha = 2$?

$2^{-\infty} = 0;\quad 2^0 = 1;\quad 2^1 = 2;\quad 2^2 = 4;\quad 2^3 = 1;\quad 2^4 = 2^3 \cdot 2 = 2;\quad 2^5 = 4$, ... NO!

$\alpha = 3$?

$3^{-\infty} = 0;\quad 3^0 = 1;\quad 3^1 = 3;\quad 3^2 = 2;\quad 3^3 = 6;\quad 3^4 = 4;\quad 3^5 = 5$ YES!

Therefore:

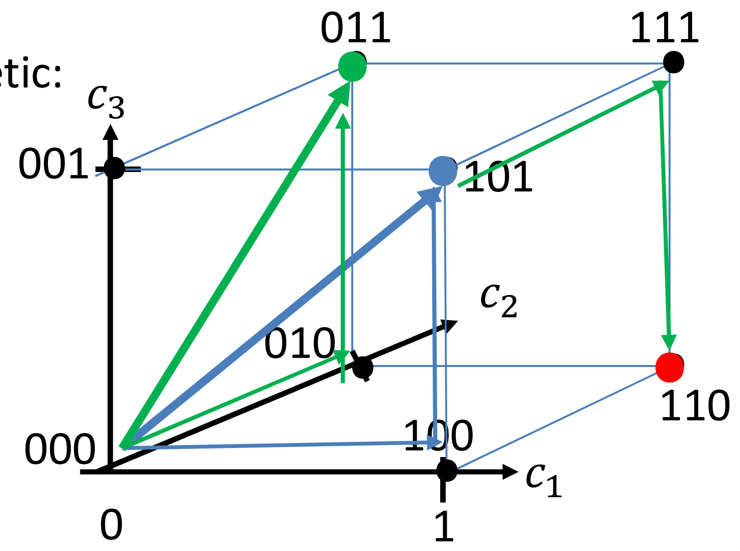
$$GF(q = 7) = \{\alpha^{-\infty}, \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\} = \{0, 1, 3, 2, 6, 4, 5\}$$

We already known GF(q=2), that is the binary arithmetic:

Sum of binary vectors

Modulo 2 addition of the coordinates:

101+011=110



Procedure of Code generation

- Define (N, K, q) parameter set for the required correction capability $t_{corr} = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ according the construction rules.
- Appropriate choice of the basis vectors in the N dimensional space that constitutes the generator matrix $\bar{\bar{G}}$ with the size of KxN to generate the valid code vectors of the Code $\vec{C}$

Defining the Base:

$$\bar{\bar{G}} = \begin{bmatrix} \overline{g_1} \\ \overline{g_2} \\ \vdots \\ \overline{g_K} \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & g_{1N} \\ g_{21} & g_{22} \cdots & g_{2N} \\ \vdots & \vdots & \vdots \\ g_{K1} & \cdots\cdots & g_{KN} \end{bmatrix}$$

Generating the code vectors:

$$\overline{c_i} = \sum_{k=1}^{K} u_{i_k} \cdot \overline{g_k} = \overline{u_i} \cdot \begin{bmatrix} \overline{g_1} \\ \overline{g_2} \\ \vdots \\ \overline{g_K} \end{bmatrix} = \overline{u_i} \cdot \bar{\bar{G}}$$

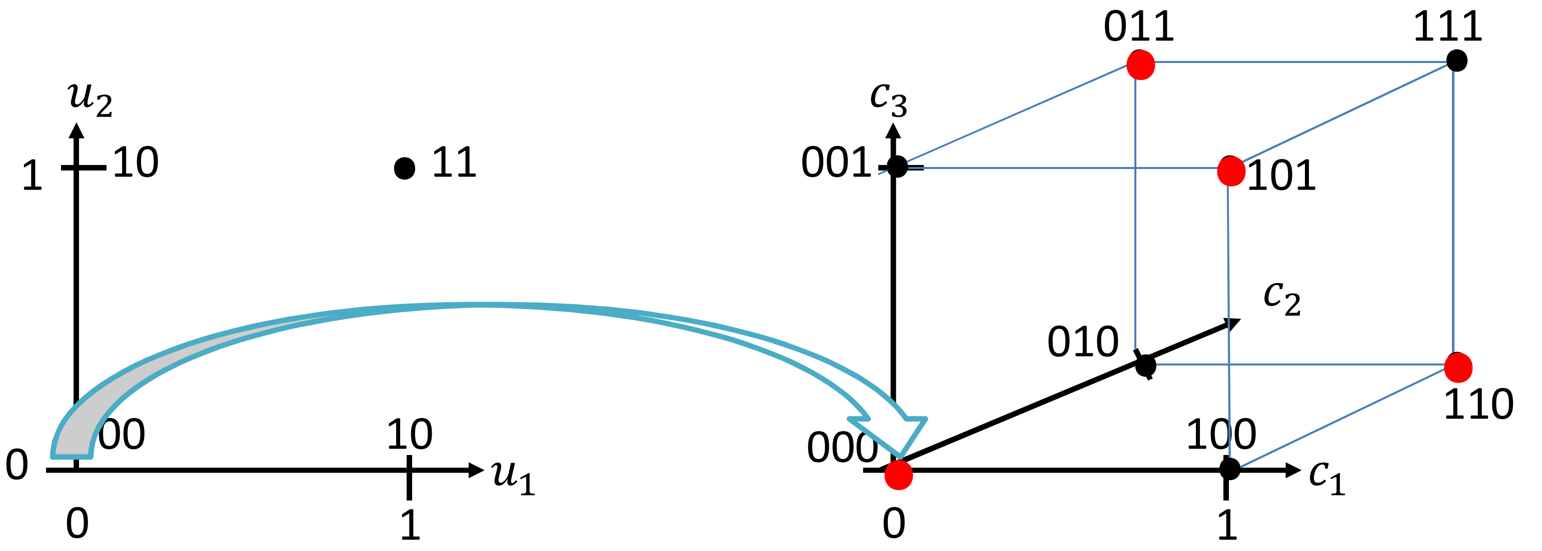
Systematic code; advantage by the 2. step of decoding, because the code vector contains the message vector:

$\bar{\bar{G}} = \left[\overline{\overline{I_{K,K}}} \quad \vdots \quad \overline{\overline{P_{K,N-K}}}\right]$ or $\bar{\bar{G}} = \left[\overline{\overline{P_{K,N-K}}} \quad \vdots \quad \overline{\overline{I_{K,K}}}\right]$ or

$$\bar{\bar{G}} = \left[\overline{\overline{P_{K,N-K-k}}} \quad \vdots \quad \overline{\overline{I_{K,K}}} \quad \vdots \quad \overline{\overline{P_{K,k}}}\right]$$

Example: Parity check code: (N=3, K=2, q=2)

Able to detect just one error: d_{min}=2, $t_{det} < d_{min}, t_{det_{max}} = d_{min} - 1 = 1$

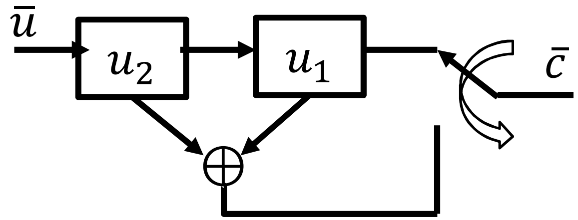


Message-vector		Code-vector		
0	0	0	0	0
1	0	1	0	1
0	1	0	1	1
1	1	1	1	0

Generator matrix

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Realization example



$\bar{c} = [c_1 = u_1, c_2 = u_2, c_3 = u_1 + u_2]$

Systematic, because contains the unity matrix;

Non systematic, but by changing rows or columns could be systematic

Processing of errors

There exists such a Parity check matrix $\bar{\bar{H}}$, that $\bar{\bar{G}} \cdot \bar{\bar{H}}^T = \bar{\bar{0}}$

E.g. for systematic $\bar{\bar{G}} = [\overline{\overline{I_{K,K}}} \quad \vdots \quad \overline{\overline{P_{K,N-K}}}]$ generator matrix:

$$\bar{\bar{H}}^T = \begin{bmatrix} -\bar{\bar{P}}_{K,N-K} \\ \dots \\ \bar{\bar{I}}_{N-K,N-K} \end{bmatrix} \underset{transponat}{\Longleftrightarrow} \bar{\bar{H}} = [-\bar{\bar{P}}^T_{K,N-K} = -\bar{\bar{P}}_{N-K,K} \quad \vdots \quad \bar{\bar{I}}_{N-K,N-K}]$$

Appropriate because:

$$\underbrace{\bar{u} \cdot \bar{\bar{G}}}_{\bar{c}} \cdot \bar{\bar{H}}^T = \bar{u} \cdot \bar{\bar{0}} = \bar{0} = \bar{c} \cdot \bar{\bar{H}}^T = \bar{\bar{H}} \cdot \bar{c}^T$$

By transmitting through BSC or more generally through DMC (discrete memoryless channel):

$$\bar{v} = \bar{c} + \bar{e}$$

Using the parity check matrix $\bar{\bar{H}}$ and the received vector $\bar{v}$ the decoder could calculate the so called syndrome vector:

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \bar{\bar{H}} \cdot [\bar{c} + \bar{e}]^T = \underbrace{\bar{\bar{H}} \cdot \bar{c}^T}_{\bar{0}} + \bar{\bar{H}} \cdot \bar{e}^T = \bar{\bar{H}} \cdot \bar{e}^T$$

Decision in the case of $\bar{s}^T = \bar{0}^T$:

- Trivial: $\bar{v} = \overline{c_i}$
- Unsolvable: $\bar{v} = \overline{c_j} \neq \overline{c_i}$ that we sent

Processing of errors

In the case of $\bar{s}^T \neq \bar{0}^T$ an equation system of N-K equations should be solved for $2 \cdot t_{corr}$ unknowns (each errors have two attributes: position and value)

$$\bar{s}^T = \bar{\bar{\bar{H}}} \cdot \bar{e}^T$$

The parity check matrix and the error vector:

$$\bar{\bar{\bar{H}}} = [\bar{h}_1^T \quad \bar{h}_2^T \quad \dots \quad \bar{h}_N^T]$$

The column vectors should be different and excluding $\bar{0}^T$, because they localizing the errors.

$$\bar{e} = \left[0, 0, \dots, e_i, \dots, e_j, \dots, 0, \dots, 0\right]$$

The syndrome vector:

$$\bar{s}^T = \sum_n e_n \cdot \bar{h}_n^T = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{N-K} \end{bmatrix} = \begin{bmatrix} e_i \cdot \bar{h}_{i_1}^T & + & e_j \cdot \bar{h}_{j_1}^T & + & \cdots \\ e_i \cdot \bar{h}_{i_2}^T & + & e_i \cdot \bar{h}_{j_2}^T & + & \cdots \\ \vdots & \vdots & \vdots & & \\ e_i \cdot \bar{h}_{i_{N-K}}^T & + & e_i \cdot \bar{h}_{j_{N-K}}^T & + & \cdots \end{bmatrix}$$

$$s_1 = e_i \cdot \bar{h}_{i_1}^T + e_j \cdot \bar{h}_{j_1}^T + e_k \cdot \bar{h}_{k_1}^T + \cdots$$
$$s_2 = e_i \cdot \bar{h}_{i_2}^T + e_j \cdot \bar{h}_{j_2}^T + e_k \cdot \bar{h}_{k_2}^T + \cdots$$

$$s_{N-K} = e_i \cdot \bar{h}_{i_{N-K}}^T + e_j \cdot \bar{h}_{j_{N-K}}^T + e_k \cdot \bar{h}_{k_{N-K}}^T + \cdots$$

Example: Binary Hamming (7,4,2)

Column in octal (e.g. 3=011)

$$\begin{array}{c c}
 & \begin{matrix} 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{matrix} \\
\bar{\bar{H}} = & \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}
\end{array}$$

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Message vector

$$\bar{u} = [1 \quad 1 \quad 0 \quad 1]$$

Code vector $\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0]$

$$[u_1, u_2, u_3, u_4, p_1 = u_1 + u_2 + u_4, p_2 = u_1 + u_3 + u_4, p_3 = u_2 + u_3 + u_4]$$

Received vector (One error on BSC)

$\bar{e} = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1]$

$\bar{v} = \bar{c} + \bar{e} = [1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1]$

Error correction:

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$\hat{\bar{e}} = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1]$

$\hat{\bar{c}} = [1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0]$

$\hat{\bar{u}} = [1 \quad 1 \quad 0 \quad 1]$

Received vector (Two errors on BSC)

$\bar{e} = [0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1]$

$\bar{v} = \bar{c} + \bar{e} = [1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1]$

Error detection, parity check:

$$p_{v1} \neq v_1 + v_2 + v_4 = 0, p_{v2} = 0, p_{v3} = 1$$

Example: Binary Hamming

(N=7, K=4, q=2)

$$\bar{\bar{H}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\bar{u} = [1 \quad 1 \quad 0 \quad 1]$$
$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0]$$
$$\bar{e} = [0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]$$
$$\bar{v} = \bar{c} + \bar{e} = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0]$$

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$
$$\hat{\bar{e}} = [0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]$$
$$\hat{\bar{c}} = [1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0]$$
$$\hat{\bar{u}} = [1 \quad 1 \quad 0 \quad 1]$$