Űrkommunikáció
Space Communication
2023/8.

Galois field, GF($q = p^m$)

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

The elements of the field (symbols, not numbers as usual):

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

Representation of Elements:

- m dimensional p-ary vectors:

$$\{\underbrace{0\ 0\ \cdots 0}_{\text{m}},\ \underbrace{0\ 0\ \cdots 1}_{\text{m}},\ \cdots, \underbrace{(p-2)\ (p-1)\ \cdots (p-1)}_{\text{m}}\ \underbrace{(p-1)\ (p-1)\ \cdots (p-1)}_{\text{m}}\}$$

Null-element, Unit-element, ….., other elements

Example $GF(2^2 = 4) = \{00 \quad 01 \quad 10 \quad 11\}$

- P-ary polynomials of maximum degree = m-1:

$$\{\underbrace{0,\ 1,\ \cdots,\ (p-1),}_{\text{0 degree}}\ \underbrace{x,\ x+1,\ \cdots,\ x+(p-1),\ 2x,\ \cdots\ (p-1)x+(p-1),}_{\text{1. degree}}$$

$$\underbrace{x^2,\ x^2+x,\ x^2+1,\ x^2+x+1, \cdots,\ (p-1)x^2+(p-1)x+(p-1),}_{\text{2. degree}}\ \cdots,$$

$$\underbrace{x^{m-1},\ x^{m-1}+1,\ \cdots,\ (p-1)x^{m-1}+(p-1)x^{m-2}+\cdots+(p-1)x+(p-1)}_{\text{(m-1)-th degree}}\}$$

Example $GF(2^2 = 4) = \{0 \quad 1 \quad x \quad x+1\}$

Galois field, GF($q = p^m$)

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

The elements of the field (symbols, not numbers as usual):

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

The operations applied over GF(q=p) are not appropriate:

Example $GF(2^2 = 4) = \{0, 1, 2, 3\}$; 1+1 (mod 4)=2=3+3 (mod 4)

Operations, $a, b \epsilon GF(q = p^m)$:

Addition a ⊕ b

- Sum of the values modulo p at each coordinates of the vectors

Example $GF(2^2 = 4) = \{00 \quad 01 \quad 10 \quad 11\}$; 10 ⊕ 11 = 01

- Sum of the coefficients modulo p of the members same degree

Example $GF(2^2 = 4) = \{0 \quad 1 \quad x \quad x + 1\}$; x ⊕ x+1 = 1

Multiplication a(x) ∗ b(x)

$$c(x) = a(x) \cdot b(x) \ \ Mod\ p(x)$$

Product of the polynomials modulo p(x) irreducible polynomial degree of m, and coefficients modulo p. Irreducible polynomial can't be product of polynomials lower degree.

Example $GF(2^2 = 4) = \{0 \quad 1 \quad x \quad x + 1\}$; p(x)=$x^2 + x + 1$;

x ∗ (x+1) mod p(x) = $x^2 + x \ \ mod\ p(x) = 1 \cdot p(x) + 1\ mod\ p(x) = 1$

Galois field, GF$(q = p^m)$

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

$$GF(2^2 = 4) = \{0, 1,2,3\} = \{00 \quad 01 \quad 10 \quad 11\} = \{0 \quad 1 \quad x \quad x + 1\}$$

Field elements by *symbols* *vectors* *polynomials*

$a, b \in GF(q = p^m)$

Addition a $\oplus$ b
modulo p at each coordinates

a $\oplus$ b		00	01	10	11
		0	1	2	3
00	0	0	1	2	3
01	1	1	0	3	2
10	2	2	3	0	1
11	3	3	2	1	0

Multiplication a(x) $*$ b(x)
$c(x) = a(x) \cdot b(x)\ mod$ p(x)=$x^2 + x + 1$

a(x) $*$ b(x)		0	1	x	x+1
		0	1	2	3
0	0	0	0	0	0
1	1	0	1	2	3
x	2	0	2	3	1
x+1	3	0	3	1	2

Example: Systematic, MDS, Hamming (N=q+1=5,K=q-1=3,q=$2^2 = 4$) code

$GF(4)=\{0, 1, 2, 3\}$; $t_{corr} = 1$;

Hamming bound, perfect: $1 + N \cdot (q-1) = 1 + (q+1) \cdot (q-1) = q^2 = q^{N-K}$;

a ⊕ b		00	01	10	11
		0	1	2	3
00	0	0	1	2	3
01	1	1	0	3	2
10	2	2	3	0	1
11	3	3	2	1	0

$$\bar{\bar{H}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{bmatrix}$$

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

a(x) * b(x)		0	1	x	x+1
		0	1	2	3
0	0	0	0	0	0
1	1	0	1	2	3
x	2	0	2	3	1
x+1	3	0	3	1	2

$$\bar{u} = [1 \quad 2 \quad 3]$$

$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [1 \quad 2 \quad 3 \quad 0 \quad 0]$$

$$\bar{e} = [0 \quad 3 \quad 0 \quad 0 \quad 0]$$

$$\bar{v} = \bar{c} + \bar{e} = [1 \quad 1 \quad 3 \quad 0 \quad 0]$$

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = e_i \cdot \bar{h}_i^T = \begin{bmatrix} e_i \cdot h_{1,i} \\ e_i \cdot h_{2,i} \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}; \qquad e_i = 3; \quad \frac{\bar{s}^T}{3} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \bar{h}_i^T; \quad i=2$$

$$\hat{\bar{e}} = [0 \quad 3 \quad 0 \quad 0 \quad 0]$$

$$\hat{\bar{c}} = [1 \quad 2 \quad 3 \quad 0 \quad 0]$$

$$\hat{\bar{u}} = [1 \quad 2 \quad 3]$$

Example: Systematic, MDS, Hamming (N=q+1=5,K=q-1=3,q=$2^2 = 4$) code

$a \oplus b$		00	01	10	11
		0	1	2	3
00	0	0	1	2	3
01	1	1	0	3	2
10	2	2	3	0	1
11	3	3	2	1	0

$$\bar{\bar{H}} = \begin{bmatrix} 1\ 1\ 1\ 1\ 0 \\ 1\ 2\ 3\ 0\ 1 \end{bmatrix}$$

$$\bar{\bar{G}} = \begin{bmatrix} 1\ 0\ 0\ 1\ 1 \\ 0\ 1\ 0\ 1\ 2 \\ 0\ 0\ 1\ 1\ 3 \end{bmatrix}$$

$a(x) * b(x)$		0	1	x	x+1
		0	1	2	3
0	0	0	0	0	0
1	1	0	1	2	3
x	2	0	2	3	1
x+1	3	0	3	1	2

$$\bar{u} = [\qquad\qquad]$$

$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [\qquad\qquad\qquad]$$

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

$$\bar{v} = \bar{c} + \bar{e} = [\qquad\qquad\qquad]$$

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = e_i \cdot \bar{h}_i^T = \begin{bmatrix} e_i \cdot h_{1,i} \\ e_i \cdot h_{2,i} \end{bmatrix} = \begin{bmatrix} \ \\ \ \end{bmatrix}; \qquad e_i =; \qquad \frac{\bar{s}^T}{e_i} = \begin{bmatrix} \ \\ \ \end{bmatrix} = \bar{h}_i^T; \ \ i=$$

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

$$\hat{\bar{c}} = [\qquad\qquad\qquad]$$

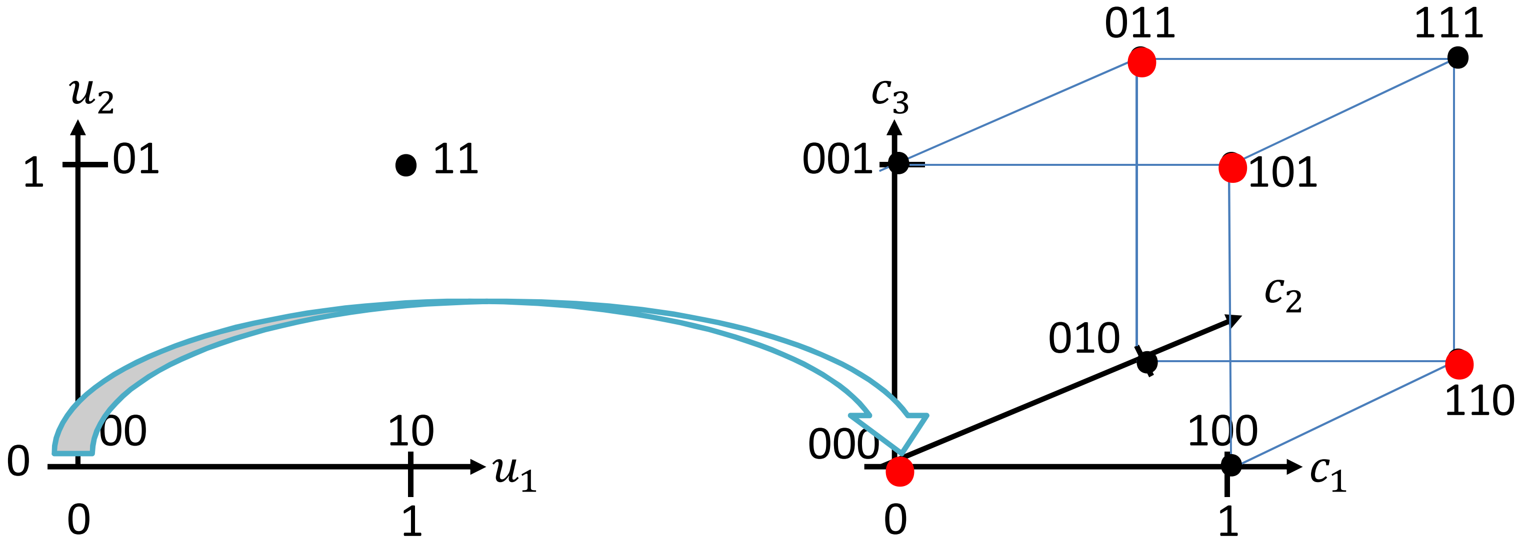
$$\hat{\bar{u}} = [\qquad\qquad]$$

Cyclic block codes

Definition: The cyclic shift of every valid code vector results in also valid code

If $\overline{c_i} = [c_1, c_2, \ldots, c_{N-1}, c_N]$ valid, then $\overline{c_j} = [c_N, c_1, \ldots, c_{N-2}, c_{N-1}]$ also.

Remark: Heuristically we already designed a cyclic code



Message vectors	
0	0
1	0
0	1
1	1

Code vectors		
0	0	0
1	0	1
0	1	1
1	1	0

Cyklic (N,K,q) block codes

Representing code words with code polynomials (instead of vectors)
Remark: coefficients of the polynomials are elements of and operations over GF(q)

The N dimensional $\bar{c}$ vector corresponds to c(x) polynomial, $\max\{\deg(c(x))\} = N-1$:
Indexing from 0,

$$\bar{c} = [c_0, c_1, \dots, c_{N-2}, c_{N-1}] \Leftrightarrow c(x) = c_0 \cdot x^0 + c_1 \cdot x^1 + \dots + c_{N-2} \cdot x^{N-2} + c_{N-1} \cdot x^{N-1}$$

Cyclic shift:

- Shift with one position: multiply with x

$$x \cdot c(x) = c_0 \cdot x^1 + c_1 \cdot x^2 + \dots + c_{N-2} \cdot x^{N-1} + c_{N-1} \cdot x^N$$

- Adding zero:

$$x \cdot c(x) = c_0 \cdot x^1 + c_1 \cdot x^2 + \dots + c_{N-2} \cdot x^{N-1} + c_{N-1} \cdot x^N \pm c_{N-1}$$

$$x \cdot c(x) = c_{N-1} + c_0 \cdot x^1 + c_1 \cdot x^2 + \dots + c_{N-2} \cdot x^{N-1} + c_{N-1} \cdot (x^N - 1)$$

- Make it cyclic: $mod\ with\ (x^N - 1)$ polynomial

$$x \cdot c(x)\ mod\ (x^N - 1) = c_{N-1} + c_0 \cdot x^1 + c_1 \cdot x^2 + \dots + c_{N-2} \cdot x^{N-1}$$

Deriving other code polynomials in general: If c(x) is a valid code, then $c_i(x)$ is also a valid code polynomial of degree $\max\{\deg(c_i(x))\} = N-1$

$$c_i(x) = x^i \cdot c(x)\ mod\ (x^N - 1)$$

Generating Cyclic (N,K,q) block codes

(One possible method – there are also others):
Theorem:
Any g(x) polynomial of degree N-K that divides the $(x^N - 1)$ polynomial is appropriate for code generation.

$$(x^N - 1) = g(x) \cdot h(x) \Longleftrightarrow (x^N - 1) \; mod \; g(x) = 0$$

Generator polynomial, $\deg\big(g(x)\big) = N - K$:

$$g(x) = g_0 + g_1 \cdot x^1 + \ldots + g_{N-K} \cdot x^{N-K}$$

Parity check polynomial, $\deg\big(h(x)\big) = K$:

$$h(x) = h_0 + h_1 \cdot x^1 + \ldots + h_K \cdot x^K$$

Representing the message words of K message symbols (message vectors) with polynomials:
Message polynomial, $\max\left\{\deg\big(u(x)\big)\right\} = K - 1$:

$$u(x) = u_0 + u_1 \cdot x^1 + \ldots + u_{K-1} \cdot x^{K-1}$$

Generating codes: a code polynomial corresponds to a message polynomial applying the generator polynomial:

$$c_i(x) = u_i(x) \cdot g(x)$$

Generating Cyclic (N,K,q) block codes

Proof that $g(x) = g_0 + g_1 \cdot x^1 + \ldots + g_{N-K} \cdot x^{N-K}$ $\quad appropriate\ generator$

A valid message polynomial: $u_0 = u_1 = \cdots = u_{K-2} = 0, u_{K-1} = 1$:

$$u(x) = x^{K-1}$$

The corresponding code polynomial generated by g(x) according the theorem:

$$c(x) = u(x) \cdot g(x) = g_0 \cdot x^{K-1} + g_1 \cdot x^K + g_2 \cdot x^{K+1} + \ldots + g_{N-K} \cdot x^{N-1}$$

Cyclic shift:

$$x \cdot c(x) = g_0 \cdot x^K + g_1 \cdot x^{K+1} + \cdots + g_{N-K-1} \cdot x^{N-1} + g_{N-K} \cdot x^N \quad \pm g_{N-K} =$$
$$= g_{N-K} + g_0 \cdot x^K + g_1 \cdot x^{K+1} + \cdots + g_{N-K-1} \cdot x^{N-1} + g_{N-K} \cdot (x^N - 1)$$

$$c_1(x) = x \cdot c(x)\ mod\ (x^N - 1) = g_{N-K} + g_0 \cdot x^K + g_1 \cdot x^{K+1} + \cdots + g_{N-K-1} \cdot x^{N-1} =$$
$$= \underbrace{x^K \cdot g(x)}_{g(x)\ divides} - \underbrace{g_{N-K} \cdot (x^N - 1)}_{g(x) divides} = x^K \cdot g(x)\ mod(x^N - 1)$$

Therefore $c_1(x)$ *is also generated by g(x):*

$$c_1(x) = u_1(x) \cdot g(x)$$

Cyclic Redundancy Check, CRC

Generating codes:

$$c(x) = u(x) \cdot x^{N-K} - \underbrace{[(u(x) \cdot x^{N-K})\ mod\ g(x)]}_{r(x)}$$

The message polynomial u(x) shifted to the right with N-K positions and then subtracting the residuum polynomial r(x) of the division with g(x)

$\deg r(x) \leq N - K - 1$, because $\deg g(x) = N - K$

Representing with vectors:

$$\bar{u} = [u_0 \quad u_1 \quad u_2 \quad \cdots \quad u_{K-1}]$$

$$\bar{c} = \left[\underbrace{c_0 \quad \cdots \quad c_{N-K-1}}_{r(x)} \quad \underbrace{c_{N-K} \quad c_{N-K+1} \quad \cdots \quad c_{N-1}}_{Systematic}\right]$$

Because g(x) divides CRC codes, therefore CRC codes are generated by g(x).
CRC codes are systematic.

Cyclic binary Hamming (N,K,q)

Example: parameters of the block code: (N=7, K=4, q=2)

Choosing a generator polynomial:

$$\deg g(x) = N - K \text{ and } (x^N - 1) \text{ mod } g(x)=0$$

$$(x^7 - 1) = (x+1) \cdot (x^3 + x^2 + 1) \cdot (x^3 + x^1 + 1)$$

$$g(x) = (x^3 + x^2 + 1) \; or \; (x^3 + x^1 + 1)$$

Generating codes for the message u(x):

$$c(x) = u(x) \cdot g(x)$$

Processing of error with h(x) parity check polynomial:

$$\deg h(x) = K \text{ and } (x^N - 1) \text{ mod } h(x)=0$$

$$h(x) = (x+1)(x^3 + x^1 + 1) \;\; or \; (x+1)(x^3 + x^2 + 1)$$

A valid code polynomial multiplied with h(x) results 0

$$c(x) \cdot h(x) = \underbrace{u(x) \cdot g(x)}_{c(x)} \cdot h(x) = u(x) \cdot \underbrace{g(x) \cdot h(x)}_{(x^N - 1)} = u(x) \cdot (x^N - 1)$$

$$c(x) \cdot h(x) \;\; mod(x^N - 1) = 0$$

Cyclic binary Hamming (N,K,q)

In the case of ONE error represented by e(x) error polynomial :

$$v(x) = c(x) + e(x)$$

$$v(x) \cdot h(x) \;\; mod(x^N - 1) = \underbrace{c(x)h(x) \;\; mod(x^N - 1)}_{\equiv 0} + \underbrace{e(x)h(x) \; mod(x^N - 1)}_{\neq 0}$$

Detection of error:

$$v(x) \cdot h(x) \;\; mod(x^N - 1) \neq 0$$

ONE binary error at position i (i=0, 1, 2, …, N-1):

$$e(x) = x^i$$

Correction of error

- h(x) will be cyclically shifted by i positions to the right through multiplication with e(x)
- Decoder checks in which cyclic shift of h(x) match with $v(x) \cdot h(x) \;\; mod(x^N - 1)$

  => error position i => $\hat{e}(x)$ decided error polynomial
- decided code polynomial $\hat{c}(x) = v(x) - \hat{e}(x)$
- decided message polynomial $\hat{c}(x) \Rightarrow\!\!> \hat{u}(x)$

  Simple step if systematic, otherwise:

$$\hat{u}(x) = \hat{c}(x)/g(x)$$

Example: Cyclic binary Hamming (N,K,q)

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

$$(x^7 - 1) = (x + 1) \cdot (x^3 + x^2 + 1) \cdot (x^3 + x^1 + 1)$$

Choosing generator polynomial:

$$g(x) = (1 + x^2 + x^3)$$

Generating code for the message: $u(x) = 1 + x^3$

$$c(x) = u(x) \cdot g(x) = 1 + x^2 + x^3 + x^3 + x^5 + x^6 = 1 + x^2 + x^5 + x^6$$

Determining h(x) parity check polynomial:

$$h(x) = (x + 1)(x^3 + x^1 + 1) = 1 + x^2 + x^3 + x^4$$

ONE binary error at position i=3:

$$e(x) = x^3$$

Received polynomial:

$$v(x) = c(x) + e(x) = 1 + x^2 + x^3 + x^5 + x^6$$

Correction of error:

$$v(x) \cdot h(x) \;\; mod(x^N - 1) = 1 + x^3 + x^5 + x^6$$

$1 + x^3 + x^5 + x^6$ binary polynomial ⇔ binary vector [1 0 0 1 0 1 1]

$1 + x^2 + x^3 + x^4$ h(x) polynomial ⇔ binary vector: [1 0 1 1 1 0 0]

[1 0 0 1 0 1 1]

=> Error position i=3 => $\hat{e}(x) = x^3$ decided error polynomial

$$\hat{c}(x) = v(x) - \hat{e}(x)$$

Polynomials over GF(q)

Remark: The elements of the field (symbols, not numbers as usual):

$$GF(q) = \{0, 1, 2, \dots, q-1\}\ q = p\ or\ p^m$$

Arithmetic operations with field elements of GF(q) as usual.

Def.: *c(x)* is a polynomial over GF(q) with $\deg c(x) = N-1$ if

$$c(x) = c_0 \cdot x^0 + c_1 \cdot x^1 + \dots + c_{N-2} \cdot x^{N-2} + c_{N-1} \cdot x^{N-1}$$
$$c_i \epsilon GF(q), \qquad i = 0 \cdots N-1, c_{N-1} \neq 0.$$

Addition of polynomials:

$$c(x) = a(x) + b(x), c_i = a_i + b_i, \qquad \deg c(x) = max\{\deg a(x), \deg b(x)\}$$

e.g. for q=p: $c_i = a_i + b_i\ (mod\ q)$

Product of polynomials:

$$c(x) = a(x) \cdot b(x), \qquad \deg c(x) = \deg a(x) + \deg b(x)$$

$$c_i = \sum_{j=0}^{min\{i, \deg a(x)\}} a_j \cdot b_{i-j}$$

e.g. for q=p: $c_i = \sum_{j=0}^{min\{i, \deg a(x)\}} a_j \cdot b_{i-j}\ (mod\ q)$

Example over GF(q=2): $a(x) = 1 + x\ and\ b(x) = 1 + x + x^3$

$$a(x) + b(x) = x^3\ and\ a(x) \cdot b(x) = 1 + x^2 + x^3 + x^4$$

Polynomials over GF(q)

Division (Euclidean) of polynomials:
For $a(x)$ *and* $b(x) \neq 0$ polynomials $\exists$ $q(x)$ *quotient and* $r(x)$ *residuum polynomials*

$$a(x) = q(x) \cdot b(x) + r(x); \deg r(x) < \deg b(x)$$

b(x) is a divisor polynomial of a(x) if r(x)=0, and
r(x)=a(x) mod b(x) is the residuum

Def. Root of a polynomial: $c \epsilon GF(q)$, is a root of a(x) if a(c)=0.

Theorem: If c is a root, then a(x)=b(x) ·(x-c)
Proof: a(x)=b(x) · (x-c)+r(x); deg r(x)=0, because deg (x-c)=1
0=a(c)=b(c) · (c-c)+r=r

Theorem: An a(x) polynomial of deg a(x)=k have maximum k roots.
Proof:

$$a(x) = b(x) \cdot (x - c) \Rightarrow \deg b(x) = \deg a(x) - 1$$

$$b(x) = \dot{b}(x) \cdot (x - \dot{c}) \Rightarrow \deg \dot{b}(x) = \deg b(x) - 1$$

$$\dot{b}(x) = \ddot{b}(x) \cdot (x - \ddot{c}) \Rightarrow \deg \ddot{b}(x) = \deg \dot{b}(x) - 1$$

etc.

Reed-Solomon code

Reed-Solomon codes are non-binary, linear, maximum distance separable (MDS) block codes over GF(q) capable to correct more than one errors, Parameters (N,K,q,α)

Three equivalent code generation methods:

Method A: Coefficients of the code polynomial calculated from the message polynomial at different elements of the GF(q).

In general, let $\alpha_0, \alpha_1, \cdots, \alpha_{N-1}$ different $\exists\, GF(q), N \leq q$

and the message polynomial u(x), $\max\{\deg u(x)\} = K-1$ over GF(q)

$$u(x) = u_0 + u_1 \cdot x^1 + \ldots + u_{K-1} \cdot x^{K-1}$$

then the corresponding code polynomial c(x), $\max\{\deg c(x)\} = N-1$ over GF(q):

$$c(x) = c_0 + c_1 \cdot x^1 + \ldots + c_{N-1} \cdot x^{N-1}$$

With $c_0 = u(\alpha_0), c_1 = u(\alpha_1), c_2 = u(\alpha_2), \cdots, c_{N-1} = u(\alpha_{N-1})$

Theorem: Reed-Solomon codes are linear

Proof: For method A the corresponding generator matrix if using $\bar{c} = \bar{u} \cdot \bar{\bar{G}}$

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 1 & 1 & & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & & \alpha_{N-2} & \alpha_{N-1} \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \vdots\ \vdots & \alpha_{N-2}^2 & \alpha_{N-1}^2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \alpha_0^{K-1} & \alpha_1^{K-1} & \alpha_2^{K-1} & & \alpha_{N-2}^{K-1} & \alpha_{N-1}^{K-1} \end{bmatrix}$$

Reed-Solomon code

Theorem: Reed-Solomon codes are MDS codes

Remarks:

MDS code $M = q^{N-d_{min}+1}$ or equivalently: $K = N - d_{min} + 1$ or $d_{min} = N - K + 1$

Code weight: $w(\vec{C}) = \min_{\bar{c_i} \exists \vec{C} \setminus \bar{0}} \{\sum_{n=1}^{N} \chi\left(c_{i_n} \neq 0\right)\} = d_{min}$ for linear codes

Proof: $w(\vec{C}) = N - \langle 0\ coordinates\ of\ \bar{c} \rangle = N - \langle roots\ of\ u(x) \rangle \geq N - (K-1)$

and because Singleton: $w(\vec{C}) = d_{min} \leq N - K + 1 \xrightarrow{\text{yields}} d_{min} = N - K + 1$

- Therefore: $t_{det} = d_{min} - 1 = N - K$, and $t_{corr} = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{N-K}{2} \right\rfloor$

Method B: $\bar{c} = \bar{u} \cdot \bar{\bar{G}}$, let $\alpha\ of\ order\ m \exists GF(q), N \leq m$

and $\alpha_0 = 1, \alpha_1 = \alpha, \alpha_2 = \alpha^2, \cdots, \alpha_{N-1} = \alpha^{N-1}$ different $\exists\ GF(q)$, then applying Method A becomes:

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 1 & 1 & & 1 & 1 \\ 1 & \alpha & \alpha^2 & & \alpha^{N-2} & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \vdots\ \vdots & \alpha^{2(N-2)} & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & \alpha^{K-1} & \alpha^{2(K-1)} & & \alpha^{(K-1)(N-2)} & \alpha^{(K-1)(N-1)} \end{bmatrix}$$

Reed-Solomon code

Method C: let α of $order$ $m \ni GF(q), N \leq m$

$Every\, c(x) = c_0 + c_1 \cdot x^1 + \ldots + c_{n-1} \cdot x^{n-1}$ $is\ valid,\ if\ \alpha^i\ are\ roots\ \forall\ i = 1,2,\cdots,N-K$

$$\vec{C} = \left\{c(x);\, if\ c\left(\alpha^i\right) = 0, \forall\, i = 1,2,\cdots,N-K\right\}$$

or equivalently:

$$\vec{C} = \left\{\bar{c};\, if\ \bar{\bar{\bar{H}}} \cdot \bar{c}^T = \bar{0}^T\right\}$$

where

$$\bar{\bar{\bar{H}}} = \begin{bmatrix} 1 & \alpha^1 & \alpha^{2\cdot 1} & \vdots\ \vdots & \alpha^{(N-2)\cdot 1} & \alpha^{(N-1)\cdot 1} \\ 1 & \alpha^2 & \alpha^{2\cdot 2} & & \alpha^{(N-2)\cdot 2} & \alpha^{(N-1)\cdot 2} \\ 1 & \alpha^3 & \alpha^{2\cdot 3} & & \alpha^{(N-2)\cdot 3} & \alpha^{(N-1)\cdot 3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & \alpha^{N-K} & \alpha^{2\cdot(N-K)} & & \alpha^{(N-2)\cdot(N-K)} & \alpha^{(N-1)\cdot(N-K)} \end{bmatrix}$$

Decoding of Reed-Solomon codes

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

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

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

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

Remark: Error processing in general

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)

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

The parity check matrix and the error vector:

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

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

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

Decoding of Reed-Solomon codes

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)

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{e}^T \text{ where } \bar{e} = [0, 0, \dots, e_i, \dots, e_j, \dots, 0, \dots, 0] \text{ and}$$

$$\bar{\bar{H}} = [\bar{h}_1^T \quad \bar{h}_2^T \quad \dots \quad \bar{h}_N^T] = \begin{bmatrix} 1 & \alpha^1 & \alpha^{2\cdot 1} & \vdots\vdots & h_i^1 & \vdots\vdots & h_j^1 & \vdots\vdots & \alpha^{(N-1)\cdot 1} \\ 1 & \alpha^2 & \alpha^{2\cdot 2} & & h_i^2 & & h_j^2 & & \alpha^{(N-1)\cdot 2} \\ 1 & \alpha^3 & \alpha^{2\cdot 3} & & h_i^3 & & h_j^3 & & \alpha^{(N-1)\cdot 3} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 1 & \alpha^{N-K} & \alpha^{2\cdot(N-K)} & & h_i^{(N-K)} & & h_j^{(N-K)} & & \alpha^{(N-1)\cdot(N-K)} \end{bmatrix}$$

The column vectors are different and excluding $\bar{0}^T$, therefore localizing the errors.
The syndrome vector:

$$\bar{s}^T = \sum_n e_n \cdot \bar{h}_n^T = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{N-K} \end{bmatrix}$$

Or the corresponding non-linear equation system of N-K equations:

$$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1 + e_k \cdot h_k^1 + \cdots$$

$$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2 + e_k \cdot h_k^2 + \cdots$$

$$s_{N-K} = e_i \cdot h_i^{(N-K)} + e_j \cdot h_j^{(N-K)} + e_k \cdot h_k^{(N-K)} + \cdots$$