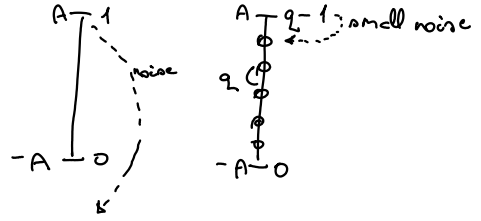
2016. október 5., szerda 16:21

"t" → $\underset{z}{H}$ "21" linearly independent vectors

Binary codes → q-ary codes

$u_i, c_i, v_i \in \{0,1\}$ $\quad u_i, v_i, c_i \in \{0,1,\dots q\}$



Data speed $[\mathrm{Id}(q) = \log_2(q)] \Longleftrightarrow B \in \mathbb{R}$ (bit error rate)

Finite Algebra → Galois Field

Galois Field:

$GF(q) = \{0,1,\dots q-1\}$, "+", "*"

"+"	"*"
Closed: $\forall \alpha,\beta \in GF(q) \to (\alpha+\beta) \in GF(q)$	Closed: $\forall \alpha,\beta \in GF(q) \to (\alpha\cdot\beta) \in GF(q)$
Symmetric: $\alpha+\beta = \beta+\alpha \;:\; \forall \alpha,\beta \in GF(q)$	Symmetric: $\alpha\cdot\beta = \beta\cdot\alpha \;:\; \forall \alpha,\beta \in GF(q)$
Associative: $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma) : \forall \alpha,\beta,\gamma$	Associative: $(\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma) : \forall \alpha,\beta,\gamma$

$\forall \alpha \in GF(q)\setminus\{0\} \to \alpha^{q-1} = 1$

Proof:

$\alpha_1\cdot\alpha_2\cdot\dots\alpha_{q-1} = \alpha\cdot\alpha_1\cdot\alpha\cdot\alpha_2\cdot\alpha\cdot\alpha_3\cdot\dots\alpha\cdot\alpha_N$

Power Table over GF(7):

all of the element can be produced by power of 3 or of 5

element	power 1	2	3	4	5	6	order
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6 ← element primitive
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

$2^3 = 8 = 1\cdot 7 + \underline{1}$

$3^3 = 27 = 3\cdot 7 + \underline{6}$

$3^3 = 3^4\cdot 3^2 = 3\cdot 2 = 6$

$3^4 = 3^2\cdot 3^2 = 2\cdot 2 = 4$

Statement: Every Galois Field have at least one element prime

Polinoms over GF(q):

$a(x) = a_0 + a_1 x + a_2 x^2 + \dots a_n x^n \;:\; a_0, a_1, \dots a_n, x \in GF(q)$

$\deg(a(x)) = n$ ← degree

$b(x) = b_0 + b_1 x + b_2 x^2 + \dots b_m x^m \;:\; b_0, b_1, \dots b_n, x \in GF(q)$

$c(x) = a(x) + b(x) = (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + \dots + (a_k+b_k)^k \;:\; k = \max\{n,m\}$

$d(x) = a(x)\cdot b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \underbrace{\left(\sum_{j=0}^{\min\{i,\deg(a(x))\}} b_{i-j} a_j\right)}_{c_i} x^i + \dots$

$a(x) \overset{X}{\longleftrightarrow} \underline{a} = (a_0, a_1, \dots a_n)$

polinom | vector

$c(x)=a(x)+b(x)$	$\underline{c} = \underline{a} + \underline{b}$
$d(x)=a(x)\cdot b(x)$	$\underline{d} = \underline{a} * \underline{b}$ ← convolution

Given: $a(x), d(x)$

$\deg(a(x))=n \;>\; \deg(d(x))=k$

$\exists\, q(x), r(x) : \; a(x) = q(x)\,d(x) + r(x)$ ← remainder polinom

↑ quotient polinom

? ? ?

Basic law of algebra:

$a(x) \quad \exists x_i : a(x_i)=0$

$a(x) = b(x)(x-x_i)$

$\deg(a(x)) > \deg(b(x))$

$a(x)\big|_{x=x_i} = \underbrace{b(x)(x-x_i)\big|_{x=x_i}}_{0} + \underbrace{r}_{r=0} = 0$

$\exists x_j : b(x_j)=0 \;\rightarrow\; b(x) = c(x)(x-x_j) \;\Rightarrow\; a(x) = c(x)(x-x_i)(x-x_j)$

# of roots $<$ $\deg(a(x))$