GRS kódok

$\underline{a}=(a_1,\dots,a_n)$, $\underline{b}=(b_1,\dots b_n)$ -re $\underline{a}\circ\underline{b}=(a_1b_1,\dots,a_nb_n)$

Mj. $\underline{a}\cdot\underline{b}=(\underline{a}\circ\underline{b})\cdot\underline{1}$

Def. $\underline{\alpha}=(\alpha_1,\dots,\alpha_n)$, $\alpha_i\in GF(q)$, $\alpha_i\neq\alpha_j$ (ha $i\neq j$)

$\underline{v}=(v_1,\dots,v_n)$, $v_i\neq 0$ $(i=1,\dots n)$

$V_{\underline{\alpha}}(f)\overset{def}{=}(f(\alpha_1),\dots,f(\alpha_n))$; $V_{\underline{\alpha}}: GF(q)[x]\to GF(q)^n$

$GRS_k(\underline{\alpha},\underline{v})\overset{def}{=}\{\underline{v}\circ V_{\underline{\alpha}}(f): f\in GF(q)[x], \deg(f)<k\}$

(n: hossz, k-dim.; k-dim.)

tétel. $GRS_k(\underline{\alpha},\underline{v})$ MDS kód, azaz $d=n-k+1$

Biz. Mit jelent $w(\underline{v}\circ V_{\underline{\alpha}}(f))\le n-k\ (<d)$? Azt, h. $V_{\underline{\alpha}}(f)$-nek, $\ge k$ db 0 koord.-ja van, azaz f-nek $\ge k$ gyöke. $\Rightarrow \deg(f)<k$

Tétel $\exists\underline{v}'$: $\forall k$-ra $GRS_k(\underline{\alpha},\underline{v})^{\perp}=GRS_{n-k}(\underline{\alpha},\underline{v}')$

Biz. I) $k=n-1$-re $GRS_{n-1}(\underline{\alpha},\underline{v})^{\perp}$ 1-dim. és MDS! $\Rightarrow\langle\underline{v}'\rangle$ $w(\underline{v}')=n$

II) Ez a $\underline{v}'$ $\forall k$-ra jó.

Ehhez kell: $(\underline{v}\circ V_{\underline{\alpha}}(f))\cdot(\underline{v}'\circ V_{\underline{\alpha}}(g))\overset{?}{=}0$, ha $\deg(f)<k$, $\deg(g)<n-k$

Tudjuk $(\underline{v}\circ V_{\underline{\alpha}}(h))\cdot\underline{v}'=0$, $\deg(h)<n-1$, $V_{\underline{\alpha}}(h)\in GRS_{n-1}$

$\Rightarrow (\underline{v}\circ\underline{v}'\circ V_{\underline{\alpha}}(h))\cdot\underline{1}=0$

$(\underline{v}\circ\underline{v}'\circ V_{\underline{\alpha}}(f)\circ V_{\underline{\alpha}}(g))\cdot\underline{1}$ $=V_{\underline{\alpha}}(fg)$, ahol $\deg(fg)\le n-1$

Mj. $\underline{v}=\underline{1}$-re RS REED–SOLOMON

$\underline{\alpha}=(1,\alpha,\alpha^2,\dots\alpha^{n-1})$, ahol α primitív $\sqrt[n]{1}$, (és $\underline{v}=\underline{1}$)

szűkebb ért. vett RS