$n = 2^q - 1$

α n^{mo} RADICE PRIMIVA DI 1

ORDINE MOLTEPLICATIVO DI n MOD 2

È 2

$GF(2^q) : GF(2)^{(w)} = GF(2)[x] = GF(2)[x] / f(x)$

$f(x)$ FATTORE IRRIDUCIBILE DI $[x^n - 1]$

E DELL' n^{mo} POLYN. CYCLOTOMICO

DI GRADO 2

Es. GLI ELEMENTI DI $GF(2^3)^*$ SONO

- I POLINOMI DI $GF(2)[x]/p$ NON NULLI
- I VETTORI NON NULLI DI $GF(2)^3$
- LE RADICI n-ME DELL'UNITÀ

A MENO DI UNA PERMUTAZIONE

LA MATRICE DEL CODICE DI HAMMING È

$$H = (1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \dots \alpha^{n-1})$$

$$(c_0, \dots c_n) H^T = \sum c_i \alpha^i = c(\alpha)$$

BASTA INTERPRETARE

$(c_0, \dots, c_n)$ COME $\sum c_i X^i$

PER INTERPRETARE IL CODICE

DI HAMMING COME IL CODICE

CICLICO GENERATO DA UN FATTORE

IRRIDUCIBILE $f(x)$ DEL POLINOMIO

CICLOTOMICO, OSSIA IL

POLINOMIO MINIMO DELLA

RADICE α PRIMITIVA DELL'UNITÀ.

E LA SUO PARITY CHECK

LA VALUTAZIONE IN α

HAMMING ESTESO È GENERATO

DA $f(x)(X-1)$ E IL PARITY

CHECK DIVENTA

$$c(\alpha) = c(1) = 0$$

BASTA INTERPRETARE

$(c_0, \dots, c_n)$ COME $\sum c_i X^i$

PER INTERPRETARE IL CODICE

DI HAMMING COME IL CODICE

CICLICO GENERATO DA UN FATTORE

IRRIDUCIBILE $f(x)$ DEL POLINOMIO

CICLOTOMICO, OSSIA IL

POLINOMIO MINIMO DELLA

RADICE PRIMITIVA DELL'UNITÀ.

E LA SUA PARITY CHECK

LA VALUTAZIONE IN 2

HAMMING ESTESO È GENERATO

DA $f(x)(x-1)$ E IL PARITY

CHECK DIVENTA

$$c(2) = c(1) = 0$$

DECODIFICA DI HAMMING

$c(\alpha) = 0 \Rightarrow c$ è codice

$c(\alpha) = \alpha^e \Rightarrow c - X^e$ è codice

è la MLD-soluzione

corregge ogni errore di peso 1

DECODIFICA DI HAMMING ESTESO

$c(\alpha) = 0 \quad c(1) = 0 \Rightarrow c$ è codice

$c(\alpha) = \alpha^e \quad c(1) \neq 0 \Rightarrow c - X^e$ è codice

è la MLD-soluzione

$c(\alpha) = \alpha^e \quad c(1) \neq 0 \Rightarrow$ 2 o più errori

=

SI POSSONO USARE LE RADICI PER DECODIFICARE 2 ERRORI ?

SUPPONIAMO DI RICEVERE $C(x) + x^a + x^b$:

$\alpha \in F$ $\quad \sigma_1 := \tau(\alpha) = \alpha^a + \alpha^b$

$\sigma_2 := \tau(\alpha^2) = \alpha^{2a} + \alpha^{2b}$

MA $\sigma_2 = \alpha^{2a} + \alpha^{2b} = (\alpha^a + \alpha^b)^2 = \sigma_1^2$

NON SI RICAVA NULLA

SE PERÒ 3 È CICLO DI 1

α E α^3 SONO RADICI

$\sigma_1 := \tau(\alpha) = \alpha^a + \alpha^b$

$\sigma_2 := \tau(\alpha^2) = \alpha^{2a} + \alpha^{2b}$

$\sigma_3 := \tau(\alpha^3) = \alpha^{3a} + \alpha^{3b}$

SE C'È UN SOLO ERRORE $\sigma_3 = \sigma_1^3$

$\sigma_3 \neq \sigma_1^3 = \alpha^{3a} + 3\alpha^{a+b}(\alpha^{2a} + \alpha^{2b}) + \alpha^{3b}$

$= \sigma_3 + \alpha^{a+b}\sigma_1$

$\Leftrightarrow 0 \neq \alpha^{a+b}\sigma_1 \Leftrightarrow \alpha^a \neq \alpha^b$

42

RICEVO $r(x)$

CALCOLO $\sigma_1 = r(\alpha)$ $\sigma_3 = r(\alpha^3)$

0 ERRORI $\Rightarrow$ $\sigma_1 = \sigma_3 = 0$

1 ERRORE $\Rightarrow$ $\sigma_3 = \sigma_1^3 \; ; \; \sigma_1 \neq 0$

2 ERRORI $\Rightarrow$ $\sigma_3 \neq \sigma_1^3 \; ; \; \sigma_1 \neq 0$ (*)

NON ESISTONO $\Leftarrow$

NEL CASO (*) POSSO TROVARE I DUE ERRORI ?

$$\sigma_1 = \alpha^a + \alpha^b$$

$$\sigma_1^3 = \sigma_3 + \alpha^a \alpha^b \sigma_1$$

$$\alpha^a \alpha^b = \frac{\sigma_1^3 - \sigma_3}{\sigma_1}$$

$$1 + \sigma_1 z + \frac{\sigma_1^3 - \sigma_3}{\sigma_1} z^2 =$$

$$1 + (\alpha^a + \alpha^b) z + \alpha^a \alpha^b z^2 =$$

$$= (1 + \alpha^a z)(1 + \alpha^b z)$$

$L(z) := 1$

IF $\sigma_1 \neq 0$ THEN

ALMENO 1 ERRORE

$L(z) := L(z) + \sigma_1 z$

IF $\sigma_1^3 \neq \sigma_3$ THEN

ALMENO 2 ERRORI

$L(z) := L(z) + \dfrac{\sigma_1^3 + \sigma_3}{\sigma_1^2} z^2$

$\sigma_1 = 0$ ERRORI $\sigma_1 \neq 0$ $L(z) = 1$ ...

HA RAGIONE

1 ERRORE α $\sigma_1 = \alpha^2 \neq 0; \sigma_1^3 \neq \sigma$

$L(z) = 1 - \alpha^2 z$

2 ERRORI α, β $\sigma_1 \neq 0; \sigma_1^3 \neq \sigma_3$

$L(z) = (1 - \alpha^2 z)(1 - \beta^2 z)$

SE 3 NON APPARTIENE AL CICLO DI 1
MA -1 CI APPARTIENE

$$\sigma_1 = 2(2)$$

$$\sigma_{-1} = 2(2^{-1})$$

0 ERRORI $\quad \sigma_1 = 0 \quad L(z) = 1$

1 ERRORE $\quad \alpha^a \quad \sigma_1 = \alpha^a \neq 0 \quad \sigma_1 = \sigma_{-1}^{-1}$

$$L(z) = (1 - \alpha^a z) = 1 - \sigma_1 z$$

2 ERRORI $\quad \alpha^a, \alpha^b \quad \sigma_1 = \alpha^a + \alpha^b \neq 0$

$$\sigma_{-1} = \frac{1}{\alpha^a} + \frac{1}{\alpha^b} = \frac{\alpha^a + \alpha^b}{\alpha^a \alpha^b} = \frac{\sigma_1}{\alpha^a \alpha^b} \neq \sigma_1$$

$$\alpha^a \alpha^b = \sigma_1 \sigma_{-1}^{-1}$$

$$L(z) = (1 - \alpha^a z)(1 - \alpha^b z) =$$

$$1 - \sigma_1 z + \sigma_1 \sigma_{-1}^{-1} z^2$$

$L(z) = 1$

IF $\sigma_1 \neq 0$ THEN

ALMENO 1 ERRORE

$L(z) = L(z) + \sigma_1 z$

IF $\sigma_2 \neq \sigma_{-1}^{-1}$ THEN

ALMENO 2 ERRORI

$L(z) = L(z) + \sigma_1 \sigma_{-1}^{-1} z^2$

SIA $\mathcal{C}$ UN CODICE CICLICO CHE ABBIA DISTANZA $2t+1$

SE RICEVIAMO UNA PAROLA $r(x)$ SAPPIAMO CHE ESISTE UNA PAROLA DI ERRORE $e(x)$ T.C.

- $r(x) - e(x) \in \mathcal{C}$
- $wt(e)$ È MINIMO

(*) SE $wt(e) \leq t$, $e(x)$ È MINIMA.

SE (*) È VERIFICATA VOGLIAMO POTER CALCOLARE $e(x)$

POSSIAMO SUPPORRE

$$e(x) = \sum_{i=0}^{e} a_i x^{j_i}$$

SIA $\gamma_i := \alpha^{j_i}$

$$L(z) = \prod_{i=1}^{e} (1 - \gamma_i z)$$

ERROR LOCATOR POLYNOMIAL

VOGLIO COME SCRIVERE $e \leq t$, $L(z)$

LA CONOSCENZA DI $L(z)$ PERMETTE DI CONOSCERE γ_i. L'ALGORITMO FORNISCE ANCHE STRUMENTI PER CALCOLARE a_i

SI SUPPONE CHE LE RADICI DEL POLINOMIO GENERATORE SIANO

$$\alpha^{l}, \alpha^{l+1}, \dots, \alpha^{l+2t-2} \quad (*)$$

LA DEFINIZIONE ORIGINALE SUPPONEVA $l=1$ "NARROW SENSE BCH"

QUESTO CODICE SI CHIAMA **BCH**

SE IL CORPO È $GF(2^m)$ SI CHIAMA **REED-SOLOMON** $n = 2^m - 1$

IN GENERALE BCH SU $GF(q)$ LUNGHEZZA $n = q-1$

PONIAMO $S_k := r(\alpha^{l+k}) = e(\alpha^{l+k})$

$$= \sum_{i=1}^{e} a_i \alpha^{(l+k)j_i} = \sum_{i=1}^{e} a_i \gamma_i^{l+k}$$

(*) COSA GARANTISCE CHE LA DISTANZA SIA $2t+1$?

ANZI: $> 2t$