FUNZIONI DI WARING

$$S_d = \sum_{i=1}^{\nu} x_i^d$$

$$S(z) = \sum_{d=1}^{\infty} S_d z^d = \sum_{d=1}^{\infty} \sum_{i=1}^{\nu} x_i^d z^d =$$

$$= \sum_{i=1}^{\nu} \sum_{d=1}^{\infty} (x_i z)^d =$$

$$= \sum_{i=1}^{\nu} \frac{x_i z}{1 - x_i z}$$

$$L(z) = \prod_{i=1}^{\nu} (1 - x_i z) = 1 + \sum_{j=1}^{\nu} (-1)^j \sigma_j(\bar{x}) z^j$$

$$L(z) \cdot S(z) = \sum_{i=1}^{\nu} \frac{x_i z}{1 - x_i z} \prod_{j=1}^{\nu} (1 - x_j z) =$$

$$= \sum_{i=1}^{\nu} x_i z \prod_{\substack{j=1 \\ j \neq i}}^{\nu} (1 - x_j z)$$

$$= -z L'(z)$$

$$\boxed{z L'(z) + L(z) \sum_{d=1}^{\infty} S_d z^d = 0}$$

$f \in K[X]$ irriducibile $\quad n = \deg(f)$

$K = K[X]/f(X) = K(\xi) \quad [K:K] = n = \deg f$

$\xi = \xi_1 \dots \xi_n$ coniugati

$$f = \prod_{i=1}^{n} (X - \xi_i) = a_0 X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n$$

IL DISCRIMINANTE DI f È LA FUNZIONE SIMMETRICA

$$\mathrm{Disc}(f) = a_0^{2n-2} \prod_{i<j} (\xi_i - \xi_j)^2$$

$$= a_0^{-1} \, \mathrm{Res}(f, f')$$

$a_0 = 1$

$$\mathrm{Disc}(f) = \prod_{i \neq j} (\xi_i - \xi_j)^2 = \prod f'(\xi_i) = N(f'(\xi))$$

$$= \begin{vmatrix} \mathrm{Tr}(\xi_1 \cdot \xi_1) & \mathrm{Tr}(\xi_1 \cdot \xi_2) & \cdots & \mathrm{Tr}(\xi_1 \cdot \xi_n) \\ \mathrm{Tr}(\xi_2 \cdot \xi_1) & & & \\ & & \mathrm{Tr}(\xi_i \cdot \xi_j) & \\ \mathrm{Tr}(\xi_n \cdot \xi_1) & & & \mathrm{Tr}(\xi_n \cdot \xi_n) \end{vmatrix}$$

$$= \begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & & & \\ \vdots & & & \\ s_{n-1} & & & s_{2n-2} \end{vmatrix}$$

$$V = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1^2 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3 & \cdots & x_n^2 \\ \vdots & & & & \\ x_1^{n-1} & x_2^{n-1} & x_i^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

$$\begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & & & \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{vmatrix} = V \quad V^c$$

CODICE BCH "NARROW SENSE"

LE RADICI DEL POLINOMIO GENERATORE SONO

$\alpha, \ldots, \alpha^{2t-1}$ NEL CASO BINARIO APPUNTO 2^t

A DISTANZA DESIGNATA $\delta = 2t$ $\delta = 2t+1$

BCH BOUND

IL CODICE BCH A DISTANZA DESIGNATA δ HA DISTANZA $\boxed{d \geq \delta}$

SE $d \geq 2t+1$ BCH BINARIO NARROW SENSE CON DISTANZA DESIGNATA $2t$

OGNI ERRORE DI PESO $\leq t$ È CORREGGIBILE

$$e(x) = \sum_{i=1}^{\nu} B_i X^{j_i} \qquad \gamma_i := \alpha^{j_i}$$

$$\Lambda(z) = \prod_{i=1}^{\nu} (1 - \gamma_i z)$$ ERROR LOCATOR POLYNOMIAL

$$\boxed{S_k = e(\alpha^k) = e(\alpha^k) = \sum_{i=1}^{\nu} B_i \alpha^{k j_i} = \sum_{i=1}^{\nu} B_i \gamma_i^k}$$

j_i ERROR POSITION

B_i ERROR VALUE

γ_i ERROR LOCATOR

BOSE RAY-CHAUDURY MARZO 60] BCH
HOCQUENGHEM SETT. 59] BINARY

PETERSON SETT. 60

DECODIFICA BCH BINARIO

FORMULA DI NEWTON PER

1) VALUTARE IL PESO DELL'ERROR

2) VALUTARE L'ERROR LOCATOR

GORENSTEIN-ZIERLER GIUGNO 61

ESTENSIONE A BCH SU $GF(p^m)$

LEMMA DI NEWTON

SOLUZIONE DIVERSA PER 1) E 2)

3) VALUTAZIONE DELL'ERROR MAGNITUDE

ALGORITMO DI DECODIFICA PGZ

BERLEKAMP 1967

ALGORITMO ALTERNATIVO

MASSEY 1969

APPLICAZIONE A LFSR

: NOTEVOLI MIGLIORIE

FORNEY SETT. 65

ADATTATO PER LA ERASURE

ALGORITMO DI DECODIFICA BM

SUGIYAMA ET AL. 1975

APPLICABILITÀ DELL'ALGORITMO

EUCLIDEO AI CODICI DI GOPPA

SAKATA

GENERALIZZAZIONE AL CASO MULTIVARIATE

ALGORITMO DI DECODIFICA DI SUGIYAMA

SUDAN 1997

DECODIFICA DI $[n, k, d]$ RS con $e > \left\lfloor \frac{n-1}{2} \right\rfloor$

GURUSWAMI-SUDAN 1996

ULTERIORI RESTRIZIONI

ALGORITMO DI DECODIFICA SUDAN-GURUSWAMI

$$\zeta_1 - \sigma_1 = 0$$

$$\zeta_2 - \zeta_1 \sigma_1 + 2\sigma_2 = 0$$

$$\zeta_3 - \zeta_2 \sigma_1 + \zeta_1 \sigma_2 - 3\sigma_3 = 0$$

$$\zeta_4 - \zeta_3 \sigma_1 + \zeta_2 \sigma_2 - \zeta_1 \sigma_3 + 4\sigma_4 = 0$$

NEL CASO BINARIO

$$\zeta_2 - \zeta_1 \sigma_1 = \zeta_1 (\zeta_1 - \sigma_1) = 0$$

$$0 = \left(\zeta_2 + \zeta_1 \sigma_1\right)^2 + \sigma_1 \left(\zeta_3 + \zeta_2 \sigma_1 + \zeta_1 \sigma_2 + \sigma_3\right) =$$

$$\zeta_4 + \zeta_2 \sigma_1^2 + \zeta_3 \sigma_1 + \zeta_2 \sigma_1^2 + \zeta_1^2 \sigma_2 + \zeta_1 \sigma_3$$

$$= \zeta_4 + \zeta_3 \sigma_1 + \zeta_2 \sigma_2 + \zeta_1 \sigma_3$$

PETERSON

1) $$\begin{vmatrix} 1 & 0 & 0 & 0 & 0 & \cdots \\ S_2 & S_1 & 1 & 0 & 0 & \cdots \\ S_4 & S_3 & S_2 & S_1 & 1 & \cdots \\ \vdots & & & & & \\ S_{2K-4} & S_{2K-3} & S_{2K-6} & S_{2K-2} & \cdots & S_{K-3} \\ S_{2K-2} & S_{2K-1} & S_{2K-4} & S_{2K-5} & \cdots & S_{K-1} \end{vmatrix} = M_K$$

A) # ERRORI $< K-1 \Rightarrow \det(M_K) = 0$

B) $S_i = \sum_{j=1}^{K} X_j^i \Rightarrow \det(M) = \prod_{i<j} (X_i - X_j)$

2) RISOLVERE

$$\begin{cases} S_1 + \sigma_1 = 0 \\ S_3 + S_2\sigma_1 + S_1\sigma_2 + \sigma_3 = 0 \\ \cdots \\ S_{2\nu+1} + S_{2\nu}\sigma_1 + \cdots + S_{\nu+1}\sigma_\nu = 0 \end{cases}$$

1A) $(0, 1, \sigma_1, \cdots, \sigma_{K-2})^T$ E' UNA SOLUZIONE

1B) $X_i = X_j \Rightarrow$ SOLO $K-2$ ELEMENTI DELLA COLONNA $\Rightarrow \det(M_K) = 0$

$\Rightarrow (X_i - X_j) \mid \det(M_K) \Rightarrow \prod (X_i - X_j) \mid \det(M_K)$

$$\deg(\det M_K) = \frac{K(K-1)}{2} = \deg\left(\prod (X_i - X_j)\right)$$

GORAN STEFANONI

FUNZIONI DI WARING

$$s_d = \sum_{i=1}^{\nu} \beta_i x_i^d$$

$$S(z) = \sum_{d=1}^{\infty} s_d z^d = \sum_{d=1}^{\infty} \sum_{i=1}^{\nu} \beta_i x_i^d z^d =$$

$$= \sum_{i=1}^{\nu} \beta_i \sum_{d=1}^{\infty} (x_i z)^d =$$

$$= \sum_{i=1}^{\nu} \beta_i \frac{x_i z}{1 - x_i z}$$

$$L(z) = \prod_{i=1}^{\nu} (1 - x_i z) = 1 + \sum_{j=1}^{\nu} (-1)^j \sigma_j(\vec{x}) z^j$$

$$L(z) \cdot S(z) = \sum_{i=1}^{\nu} \beta_i \frac{x_i z}{1 - x_i z} \prod_{j=1}^{\nu} (1 - x_j z) = \quad)$$

$$= \sum_{i=1}^{\nu} \beta_i x_i z \prod_{\substack{j=1 \\ j \neq i}}^{\nu} (1 - x_j z) = w(z)$$

$$= -z L'(z)$$

$$\boxed{z L'(z) + L(z) \sum_{d=1}^{\infty} s_d z^d = 0}$$

$$s_j + \sum_{\lambda=1}^{j-1} (-1)^{\lambda} s_{j-\lambda} \sigma_{\lambda} + (-1)^j j \sigma_j = 0 \qquad j < \nu$$

$$s_j + \sum_{\lambda=1}^{\nu} (-1)^{\lambda} s_{j-\lambda} \sigma_{\lambda} = 0 \qquad j \geq \nu$$

$$L(z) \cdot S(z) = w(z) = \sum_{i=1}^{\nu} \beta_i x_i z \prod_{\substack{j=1 \\ j \neq i}}^{\nu} (1 - x_j z)$$

$$V = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1^2 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3 & \cdots & x_n^2 \\ \vdots & & & & \\ x_1^{n-1} & x_2^{n-1} & x_i^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

$$\begin{vmatrix} s_{0,1} & s_{1,2} & \cdots & s_{n,n} \\ s_{1,2} & s_{2,3} & \cdots & s_{n,n} \\ \vdots & & & \\ s_{n,1} & s_{n,n} & \cdots & s_{2n-2} \end{vmatrix} = V \Delta V^T$$

$$\Delta = \begin{vmatrix} \beta_1 x_1 & & & \\ & \beta_2 x_2 & & \\ & & \ddots & \\ & & & \beta_n x_n \end{vmatrix}$$

GORENSTEIN-ZIERLER

1) DETERMINARE IL MASSIMO VALORE μ PER CUI

$$\det \begin{vmatrix} S_1 & S_2 & \cdots & S_\mu & S_{\mu+1} \\ S_2 & S_3 & \cdots & S_{\mu+1} & S_{\mu+2} \\ \vdots & & & & \\ S_\mu & S_{\mu+1} & \cdots & S_{2\mu-1} & S_{2\mu} \end{vmatrix} \neq 0$$

(colonne: c_1 c_2 $\cdots$ c_μ $c_{\mu+1}$)

IL NUMERO DEGLI ERRORI È $\boxed{e = \mu}$

(2) ABBIAMO TROVATO IL VALORE $\mu = e$ PER CUI

(*) I VETTORI COLONNA

$\{c_1, \dots, c_e\}$ SONO LINEARMENTE INDIPENDENTI

(*) $c_{e+1} \in \langle c_1, \dots, c_e \rangle$

$\Rightarrow c_{e+1} = \sigma_e c_1 + \sigma_{e-1} c_2 + \cdots + \sigma_2 c_{e-1} + \sigma_1 c_e$

* $\sigma(X) = 1 + \sum_{i=1}^{e} \sigma_i X^i$

SE LA RIDUZIONE È GAUSS PER COLONNE [E LA MEMORIZZIAMO PER APPLICARLA SULL'ULTIMA RIGA] IL RISULTATO È GRATIS

ERROR $\sum_{i \in I} e_i X_i^d$

ERASUR $\sum_{j \in J} \boxed{d_j} X_j^d$ $\quad d_j = r_j - c_j$

DOVE r_j È IL VALORE STIMATO

d_j QUINDI PUÒ ESSERE VISTO COME UN ERRORE IN LOCATION j E MAGNITUDE d_j [$d_j = 0$ AMMISSIBILE]

$$S_d = \sum_{i \in I} e_i X_i^d + \sum_{j \in J} d_j X_j^d \quad (*)$$

NOTI X_i, X_j, S_d ALGEBRA LINEARE TROVIAMO e_i, d_j

$$r(z) = \prod_{j \in J} (z - X_j) = \sum_{k=0}^{\mu} r_k z^k$$

[OPPURE UNA VARIANTE DELLA FORMA DI FORNEY]

$$T_d = S_d r_0 + S_{d+1} r_1 + \dots + S_{d+\mu-1} r_{\mu-1} + S_{d+\mu}$$

$$= \sum_{i \in I} e_i X_i^d r(X_i) + \sum_{j \in J} d_j X_j^d r(X_j)$$

$$= \sum_{i \in I} E_i X_i^d \qquad E_i = e_i r(X_i)$$

$$\sigma(z) = \prod_{i \in I} (1 - X_i z) \qquad T(z) = \sum T_d X_i^d$$

QUESTO DETERMINA LA LOCATION DEGLI ERRORI

RESTA IL PROBLEMA DI DETERMINARE I VALORI DI ERRORI ED ERASURE

$$\omega(z) = \sum_{i=1}^{\nu} \beta_i x_i z \prod_{\substack{j=1 \\ j\neq i}}^{\nu} (1 - x_j z)$$

$$\sigma(z) = \prod_{i=1}^{\nu} (1 - x_i z)$$

$$\sigma'(z) = \sum_{j=1}^{\nu} -x_j \prod_{\substack{i=1 \\ i\neq j}}^{\nu} (1 - x_i z)$$

$$\omega(\gamma_j^{-1}) = \sum_{i=1}^{\nu} \beta_i \gamma_i \gamma_j^{-1} \prod_{\substack{j=1 \\ j\neq i}}^{\nu} (1 - \gamma_j \gamma_j^{-1})$$

$$= \beta_j \prod_{\substack{i=1 \\ i\neq j}}^{\nu} (1 - \gamma_i \gamma_j^{-1})$$

$$\sigma'(\gamma_j^{-1}) = \sum_{K=1}^{\nu} -\gamma_K \prod_{\substack{i=1 \\ K\neq i}}^{\nu} (1 - \gamma_i \gamma_j^{-1})$$

$$= -\gamma_j \prod_{\substack{i=1 \\ i\neq j}}^{\nu} (1 - \gamma_i \gamma_j^{-1})$$

$$-\gamma_j \omega(\gamma_j^{-1}) = -\gamma_j \beta_j \prod_{i\neq j} (1 - \gamma_i \gamma_j^{-1}) = \beta_j \sigma'(\gamma_j^{-1})$$

$$\beta_j = \frac{-\gamma_j \omega(\gamma_j^{-1})}{\sigma'(\gamma_j^{-1})}$$

BERLEKAMP : KEY EQUATION

K CORPO $\quad S(z) = \sum_{i=0}^{\infty} s_i z^i \in K[[z]] \quad s_0 \neq 0$

$t \in \mathbb{N}$ SE $d \geq 2t+1$ OGNI ERRORE DI PESO $\leq t$ È CORREGGIBILE

TROVARE:

- $\sigma(z) \in K[z] \quad DEG(\sigma) \leq t$
- $\omega(z) \in K[z] \quad DEG(\omega) \leq DEG(\sigma)$

CHE SODDISFANO LA

KEY - EQUATION

$$\sigma(z) \sum_{i=0}^{2t} s_i z^i \equiv \omega(z) \mod (z^{2t+1})$$

ITERATIVA CALCOLO $\forall K \leq 2t$ $\sigma^{(K)}(z)$, $\omega^{(K)}(z)$

$$\sigma^{(K)}(z)\, S(z) \equiv \omega^{(K)}(z) \mod z^{K+1}$$

$\sigma^{(K)}(0) =$

E DEI POLINOMI AUSILIARI $\tau^{(K)}(z)$, $\gamma^{(K)}(z)$

$$\tau^{(K)}(z)\, S(z) \equiv \gamma^{(K)} + z^{(K)} \mod z^{K+1}$$

$DEG\ \sigma^{(K)} + DEG\ \gamma^{(K)} \leq K$

$DEG\ \omega^{(K)} + DEG\ \tau^{(K)} \leq K$

DEI VALORI $D(K) \in K$; $B(K) \in \{0, 1\}$

IN OGNI ITERAZIONE IL COEFFICIENTE Δ DI z^{K+1} NELLA SERIE $\sigma^K S$

INSIEME AI VALORI $D(K)$, $B(K)$ [illegible]

[illegible] DANNO I NUOVI VALORI PER $\sigma, \omega, \gamma, \tau, D, B$

FUNZIONI DI WARING

$$S_d = \sum_{i=1}^{\nu} X_i^d$$

$$S(z) = \sum_{d=0}^{\infty} S_d z^d = \sum_{d=0}^{\infty} \sum_{i=1}^{\nu} X_i^l X_i^d z^d =$$

$S_0 = 0$

$$= \sum_{i=1}^{\nu} X_i^l \sum_{d=0}^{\infty} (X_i z)^d =$$

$$S(z) = \sum_{d=0} S_{l+d}$$

$$= \sum_{i=1}^{\nu} X_i^l \frac{\cancel{X_i z}}{1 - X_i z}$$

$$L(z) = \prod_{i=1}^{\nu} (1 - X_i z) = 1 + \sum_{j=1}^{\nu} (-1)^j \sigma_j(\bar{x}) z^j$$

$$L(z) \cdot S(z) = \sum_{i=1}^{\nu} \frac{X_i z}{1 - X_i z} \prod_{j=1}^{\nu} (1 - X_j z) =$$

$$= \sum_{i=1}^{\nu} X_i z \prod_{\substack{j=1 \\ j \neq i}}^{\nu} (1 - X_j z)$$

$$= -z L'(z)$$

$$\boxed{z L'(z) + L(z) \sum_{d=1}^{\infty} S_d z^d = 0}$$

$$S_j + \sum_{\lambda=1}^{j-1} (-1)^{\lambda} S_{j-\lambda} \sigma_{\lambda} + (-1)^j j \sigma_j = 0 \qquad j < \nu$$

$$S_j + \sum_{\lambda=1}^{\nu} (-1)^{\lambda} S_{j-\lambda} \sigma_{\lambda} = 0 \qquad j \geq \nu$$

$$\ell \;/\!/\!/$$

$$DEG(\omega) < \nu$$

BERLEKAMP : KEY EQUATION — MASSEY

K CORPO $\quad S(z) = \sum_{i=0}^{\infty} s_i z^i \in K[[z]] \quad s_0 \neq 0 \quad \{s_i\}_{i=0}^{\infty}$ LINEARLY RECURRING SEQUENCE *

$t \in \mathbb{N}$ SE $d \geq 2t+1$ OGNI ERRORE DI PESO $\leq t$ È CORREGGIBILE

* CHE SI SUPPONE FINITA DI LUNGHEZZA $T+1$

TROVARE IL POLINOMIO MINIMALE

- $\sigma(z) \in K[z]$ $\quad \deg(\sigma) = L$ DELLA LRS
- $\omega(z) \in K[z]$ $\quad \deg(\omega) < \deg(\sigma) = L$

CHE SODDISFANO LA DEFINITO DALLA

KEY - EQUATION

$$\sigma(z) \sum_{i=0}^{2t-1} s_i z^i \equiv \omega(z) \mod (z^{2t+1})$$

DOVE L'ALGORITMA DI MOSTRA CHE IL MINIMO POLINOMIO σ $[L = \deg(\sigma)]$ DIPENDE SOLO DAI PRIMI $2t$ TERMINI PER CUI BASTA CONSIDERARE

$$\sigma(z) \sum_{i=0}^{2t-1} s_i z^i \equiv \omega(z) \mod (z^{2t})$$

SUGIYAMA

$\sigma(z)\,S(z) + \omega(z)\,z^{2t} = w(z)$

$DEG(\sigma) \le t \qquad DEG(\omega) \le t-1 \qquad S(z) = \sum_{i=0}^{2t-1} s_i z^i$

BERLEKAMP: $GCD(\sigma, \omega) = 1$

ALGORITMO EUCLIDEO: P_k, S_k, T_k

$P_k = S_k S + T_k z^{2t}$

$DEG(S_k) + DEG(P_{k-1}) = 2t$

SIA K: $DEG(P_k) \le t-1 < DEG(P_{k-1})$

$P_k \sigma \equiv S_k S \sigma \equiv S_k \omega \mod z^{2t}$

$DEG(P_k \sigma) \le t-1+t = 2t-1$

$DEG(S_k \omega) \le t-1+2t-DEG(P_{k-1}) < 2t$

$\Rightarrow P_k \sigma = S_k \omega \Rightarrow$ ↑ $\omega = c P_k$, $\sigma = c S_k$, $GCD(\sigma, \omega) = 1$

$\sigma(0) = 1 \Rightarrow c = S_k(0)^{-1}$

$\omega = S_k(0)^{-1} P_k$

$\sigma = S_k(0)^{-1} S_k$