Teoria dei Codici

AlpT (@freaknet.org)
http://freaknet.org/alpt

May 6, 2009

Abstract

Questo testo e' una rielaborazione personale degli appunti presi durante il corso di Teoria dei Codici, tenuto dal Prof. Re Riccardo presso il dipartimento di Matematica, Catania, A.A. 2008/2009.
Saro' ben lieto di correggere ogni eventuale errore che mi comunicherai.
Buon lettura.

^_^

Copyright ©2008 Andrea Lo Pumo aka AlpT <alpt@freaknet.org>. All rights reserved.

This document is free; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this document; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Contents

1 Introduzione **1**

2 Varie **1**

3 MDS **2**

4 BCH e Reed Solomon **5**

4.0.1 Trasformata di Fourier 10

4.0.2 Decodifica 13

5 Appendice A **18**

6 Appendice B **18**

7 * **19**

1 Introduzione

Questi appunti digitali fanno riferimento a i relativi appunti cartacei che sono stati acquisiti e inclusi nell'appendice.
Notazione:

1. [QUA,OssX.Y.Z,pg.123] e' un riferimento alla proposizione OssX.Y.Z che trovate nell'appendice B, a pagina 123.
2. [RE,OssX.Y.Z,pg.123] e' un riferimento all'appendice A.
3. [AC,4.7,pg.72] e' un riferimento agli appunti di Complementi di Algebra (vedi gli altri appunti su).
4. [AL,7.13,pg.46] e' un riferimento agli appunti di Algebra Lineare.

2 Varie

Lemma 2.1. *Sia $\beta \in U_n$, con U_n gruppo delle radici n-esime dell'unita', allora*

$$\beta \neq 1 \Rightarrow \beta^0 + \beta^1 + \cdots + \beta^{n-1} = 0$$

Proof:

$$x^n - 1 = (x-1)(1 + x + x^2 + \cdots + x^{n-1}) \quad (1)$$
$$\beta \in U_n \Leftrightarrow \beta^n - 1 = 0 \underbrace{\Leftrightarrow}_{(1),\ \beta \neq 1} 1 + \beta + \cdots + \beta^{n-1} = 0$$

□

Proposition 2.2. *Sia $G \in k \times n$ la matrice generatrice del codice lineare $C \subseteq K^n$, $\dim C = k$. Sia $H \in n-k \times n$, con $\rho(H) = n-k$,*

$$H \text{ e' una matrice di controllo per } C \Leftrightarrow H \cdot G^t = 0$$

Inoltre, se i vettori colonna $h_1, \ldots, h_s$ sono una base dello spazio vettoriale $\{x \in K^n \mid Gx = 0\}$, allora

$$H = \begin{pmatrix} {h_1}^t \\ {h_2}^t \\ \vdots \\ {h_s}^t \end{pmatrix}$$

e' una matrice di controllo di C (nota[1]).
Nota: questa proposizione e' utile per calcolare H a partire da G.

Proof:

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \text{ generatrice di } C \Rightarrow \{g_1, \ldots, g_k\} \text{ base di } C \quad (1)$$

⟨1⟩

$$H \text{ e' una matrice di controllo per } C \Leftrightarrow H \cdot G^t = 0$$

[1] e si ha $s = n - k$

infatti,
$\rho(H) = n-k \Rightarrow$ le righe di H, $H_1, \ldots, H_{n-k}$, sono l.i. (2)
H di controllo per C $\underbrace{\Leftrightarrow}_{\text{[QUA,prop3.3.1,pg.4]}}$ H generatrice per $C^\perp \underbrace{\Leftrightarrow}_{(1)} \{H_1, \ldots, H_{n-k}\}$ indipendenti, , $H_i g_j = 0 \ \forall i,j <$
$\underbrace{\Leftrightarrow}_{(2)} H_i g_j = 0 \ \forall i,j \Leftrightarrow HG^t = 0$

$\langle 2 \rangle$ Dim 2.

$$x \in C^\perp \Leftrightarrow x \cdot g_i = 0 \forall i \Leftrightarrow Gx = 0 \Leftrightarrow x \in \{x \in K^n \mid Gx = 0\}$$
$$\Rightarrow C^\perp = \{x \in K^n \mid Gx = 0\} \quad (2)$$

Siano le colonne $h_1, \ldots, h_s$ una base di $C^\perp$ e sia

$$H = \begin{pmatrix} {h_1}^t \\ \vdots \\ {h_s}^t \end{pmatrix}$$

allora

$$(2) \Rightarrow {h_i}^t \cdot g_j = 0 \ \forall i,j \Leftrightarrow HG^t = 0$$
$$\dim C^\perp = n - \dim C = n-k \Rightarrow s = n-k$$
$$\{h_1, \ldots, h_{n-k}\} \text{ base } \Rightarrow \{h_1, \ldots, h_{n-k}\} \text{ l.i.}$$
$$\underbrace{\Rightarrow}_{\text{passo 1}} H \text{ e' di controllo per } C$$

□

3 MDS

Proposition 3.1. *Costruzione di codici MDS.*
Sia $S = [\gamma_1, \ldots, \gamma_n] \subseteq F_q$, $|S| = n$, *e sia* $k \leq n$, *allora il codice lineare*

$$C = \{(f(\gamma_1), \ldots, f(\gamma_n)) \mid f \in F_q[x]_{k-1}\}$$

e' un codice MDS con $\dim C = k$.

Proof: Sia $\overline{f} = (f(\gamma_1), \ldots, f(\gamma_n))$. Si ha:

$$f \in F_q[x]_{k-1} \Rightarrow \deg f \leq k-1 \vee f \equiv 0 \quad (1)$$
$$f \neq 0 \underbrace{\Rightarrow}_{(1)} f \text{ puo' avere al piu' } k-1 \text{ radici} \quad (1.1)$$

$\langle 1 \rangle$ C e' lineare e $\dim C = k$
Consideriamo l'applicazione:

$$\varphi : F_q[x]_{k-1} \longrightarrow C$$
$$f \mapsto \overline{f}$$

φ e' lineare perche' la valutazione di polinomi e' un omomorfismo di anelli. E' surriettiva per definizione di C.

$$\operatorname{Im}\varphi = C, \ \varphi \text{ lineare } \Rightarrow C \text{ spazio vett.}$$

E' iniettiva:

$$\ker\varphi = \{f \mid f(\gamma_i) = 0 \ \forall i = 1, \ldots, n\} \underbrace{=}_{(1.1)} = \{0\} \Rightarrow \varphi \text{ iniettiva}$$

$$\varphi \text{ isomorfismo } \Rightarrow \dim F_q[x]_{k-1} = \dim \operatorname{Im} f = \dim C \Leftrightarrow \dim C = k$$

(1.1) $\Rightarrow$ al piu' si annullano $k-1$ coordinate di $\overline{f} \Rightarrow n - w(\overline{f}) \leq k-1 \Leftrightarrow w(\overline{f}) \geq n-k+1$ (2)

(2) $\Rightarrow d(C) \underbrace{=}_{\text{[QUA,Oss3.1,pg.1]}} \min w(C^*) \geq n-k+1$ (3)

$d(C) \underbrace{\leq}_{\text{[QUA,Prop3.3,pg.1]}} n - \dim C + 1 = n-k+1$

$\Rightarrow d(C) = n-k+1 \Leftrightarrow C$ e' MDS

□

Proposition 3.2. *Sia $C \subseteq F_q^n$ un codice lineare e sia*

$$\pi : C \longrightarrow C' = \pi(C)$$
$$(c_1, \ldots, c_n) \mapsto (c_1, \ldots, c_m)$$

la proiezione che tronca le ultime $n-m$ componenti.
Se $n - m < d(C)$, allora,

0. *π e' un isomorfismo vettoriale*
1. *$C' \subseteq F_q^m$ e' un codice con $\dim C = \dim C'$*
2. *$d(C') \geq d(C) - (n-m)$*
3. *C MDS $\Rightarrow C'$ MDS*

Nota: la 2. vale per un codice C qualsiasi

Proof:

⟨1⟩

π e' surriettiva (per definizione), ma e' anche iniettiva, basta infatti applicare la dimostrazione di [QUA,prop3.3,pg.1], sostituendo $d-1$ con $n-m$.

π e' chiaramente lineare.

π lineare, biettiva $\Rightarrow \pi$ isomorfismo vettoriale $\Rightarrow \dim C' = \dim C$

⟨2⟩

Sia $c \in C$,

$d(C) \underbrace{=}_{\text{[QUA,oss3.1,pg.1]}} \min w(C^*) = w(\overline{x})$ (1)

$d(C') = \min w(C'^*) = w(\pi(y))$ (2)

$w(\pi(c)) = w(c) - |\{i \mid c_i \neq 0, \ \ i = m+1, \ldots, n\}| \underbrace{\geq}_{(1)} d(C) - |\{i \mid c_i \neq 0, \ \ i = m+1, \ldots, n\}| \geq d(C) - (n-m) =$

$\underbrace{\Rightarrow}_{(2)} d(C') \geq d(C) - (n-m)$ (3)

⟨3⟩

C MDS $\Rightarrow d(C) = n - \dim C + 1 \underbrace{=}_{1.} n - \dim C' + 1$ (4)

$d(C') \underbrace{\geq}_{(3)} d(C) - (n-m) \underbrace{=}_{(4)} n - \dim C' + 1 - n + m = m - \dim C' + 1$

$d(C') \underbrace{\leq}_{\text{[QUA,prop3.3,pg.1]}} m - \dim C' + 1$

$\Rightarrow d(C') = m - \dim C' + 1 \Rightarrow C'$ MDS

□

Definition 3.3. Sia $C \subseteq F_q^n$ codice lineare, $m \leq n$, e sia

$$\overline{C} = \{c \in C \mid c_{m+1} = c_{m+2} = \cdots = c_n = 0\}$$

sia data la proiezione

$$\begin{aligned} &\pi : \overline{C} \longrightarrow \pi(\overline{C}) \\ &(c_1, \ldots, c_n) \mapsto (c_1, \ldots, c_m) \end{aligned}$$

allora, la funzione

$$\begin{aligned} &\overline{\pi} : \mathcal{P}(F_q^n) \longrightarrow \mathcal{P}(F_q^m) \\ &C \mapsto \pi(\overline{C}) \end{aligned}$$

viene chiamata *operazione di shortening*. $\pi(\overline{C})$ viene chiamato m-shortening di C.

Proposition 3.4. *Sia $C \subseteq F_q^n$ codice lineare e sia $C' = \pi(\overline{C})$ lo m-shortening di C.*
Se $n - m \leq k$, allora

1. *$H = (h_1, \ldots, h_n)$ matrice di controlo di $C \Rightarrow H' = (h_1, \ldots, h_m)$ di controllo di C', (h_i colonna)*
2. *C MDS di tipo $[n, k] \Rightarrow C'$ MDS di tipo $[m, k - (n - m)]$*

Proof: E' chiaro che π e' un isomorfismo vettoriale, quindi

$$\pi \text{ isomorfismo } \Rightarrow \dim C' = \dim \overline{C} \quad (0)$$

Sia $H = (h_1, \ldots, h_n)$ una matrice di controllo di C, con h_i colonna.
$\langle 1 \rangle$ $H' = (h_1, \ldots, h_n)$ e' di controllo per C'

$$(x_1, \ldots, x_m) \in C' \underbrace{\Leftrightarrow}_{\text{def di } \pi} (x_1, \ldots, x_m, 0, 0, \ldots, 0) \in \overline{C} \Leftrightarrow H \cdot (x_1, \dot{s}, x_m, 0, 0, \ldots, 0)^t = 0 \Leftrightarrow$$

$$x_1 h_1 + \cdots + x_m h_m = 0 \Leftrightarrow H' \cdot (x_1, \ldots, x_m) = 0$$

C MDS $\Rightarrow d(C) = n - k + 1$, $k = \dim C \underbrace{\Rightarrow}_{\text{[QUA,prop3.2,pg.1]}} s = n - k$, ogni insieme di $\leq s$ colonne di H e' l.i. $(1) \Rightarrow$

$\underbrace{\Rightarrow}_{H' = (h_1, \ldots, h_m)}$ ogni insieme di $\leq s = n - k$ colonne di H' e' l.i. (2)

(2) $\underbrace{\Rightarrow}_{m \geq n-k \text{ per Hp}}$ $n - k$ colonne di H' sono *l.i.* (2.1)

H di controllo $\Rightarrow H \in n - k \times n \Rightarrow H' \in n - k \times m$ (3)

(2), (3) $\Rightarrow \rho(H') = n - k \Rightarrow \dim C' = m - (n - k) = k - (n - m)$ (4)

$d(C') = s' + 1 \underbrace{=}_{(2)} n - k + 1 \underbrace{=}_{(4)} n - (\dim C' + (n - m)) + 1 = m - \dim C' + 1 \Rightarrow C'$ MDS

□

Proposition 3.5. *TODO/Domanda: conoscendo H matrice di controllo di C, qual'e' la matrice di controllo di C' ottenuto tramite puncturing? (Hint: usare H in forma standard).*

4 BCH e Reed Solomon

NOTA: in questa sezione supponiamo sempre $(n, p) = 1$.

Definition 4.1.

$$C \text{ e' un codice BCH} \overset{\text{def}}{\Leftrightarrow} C = \left\{c(x) \in F_q[x]_{n-1} \mid c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+\delta-2}) = 0\right\}$$

dove $U_n = \langle\alpha\rangle = \left\{1, \alpha, \alpha^2, \ldots, \alpha^n\right\}$, $b, \delta > 0$, $\delta \leq n$.

Lemma 4.2. *Sia C un BCH, allora*

$$\alpha^b,\ \alpha^{b+1},\ \ldots,\ \alpha^{b+\delta-2}$$

sono tutte distinte fra loro

Proof: Sia $0 \leq i < j \leq \delta - 2$

$0 \leq i < j \leq \delta - 2 < \delta \leq n \Rightarrow i < j < n \Rightarrow j - i < j < n$ (1)

$$\alpha^{b+j} = \alpha^{b+i} \underbrace{\Leftrightarrow}_{n=|U_n|=o(\alpha)} b + j = b + i \ \mathbb{Z}_n \Leftrightarrow i = j \ \mathbb{Z}_n \Leftrightarrow n \Big/ j - i \underbrace{\Leftrightarrow}_{j-i<n} j - i = 0 \Leftrightarrow j = i$$

□

Proposition 4.3. *Sia C un codice BCH, allora*

1. *C e' ciclico*
2. *$d(C) \geq \delta$*

Proof:

⟨1⟩ Dim 1.

Basta applicare la [RE,Prop4.6,pg.24] alla definizione, considerando che

$$\alpha \in U_n \Rightarrow \alpha^i \in U_n$$

⟨2⟩ Dim 2.

Supponiamo per assurdo che $d(C) < \delta$,

$$d(C) < \delta \underbrace{\Leftrightarrow}_{\text{[QUA,Oss3.1,pg.1]}} \exists c(x) \in C \setminus \{0\} : \ w(c(x)) < \delta \ (1)$$

Si ha
$c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in C \underbrace{\Leftrightarrow}_{\text{def.}} c(\alpha^i) = 0 \ \ \forall i = b, b+1, \ldots, b+\delta-2 \Leftrightarrow$

$$\Leftrightarrow \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots, & \alpha^{(n-1)b} \\ 1 & \alpha^{(b+1)} & \alpha^{2(b+1)} & \ldots, & \alpha^{(n-1)(b+1)} \\ \vdots & & & & \\ 1 & \alpha^{(b+\delta-2)} & \alpha^{2(b+\delta-2)} & \ldots, & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = 0 \quad (2)$$

$w(c(x)) < \delta \Leftrightarrow$ esistono al piu' $\delta - 1$ componenti non nulle, $c_{i_1}, \ldots, c_{i_{d-1}}$ di $c(x)$ (3)

(2) $\underbrace{\Leftrightarrow}_{H_i \text{ colonna}}$ $c_0 H_1 + c_1 H_2 + \cdots + c_{n-1} H_n = 0 \underbrace{\Leftrightarrow}_{(3)} c_{i_1} H_{i_1+1} + c_{i_2} H_{i_2+1} + \cdots + c_{i_{\delta-1}} H_{i_{\delta-1}+1} = 0 \Leftrightarrow$

$$\Leftrightarrow \begin{bmatrix} \alpha^{i_1 b} & \alpha^{i_2 b} & \alpha^{i_3 b} & \ldots & \alpha^{i_{\delta-1} b} \\ \alpha^{i_1(b+1)} & \alpha^{i_2(b+1)} & \alpha^{i_3(b+1)} & \ldots & \alpha^{i_{\delta-1}(b+1)} \\ \vdots & & & & \\ \alpha^{i_1(b+\delta-2))} & \alpha^{i_2(b+\delta-2)} & \alpha^{i_3(b+\delta-2)} & \ldots & \alpha^{i_{\delta-1}(b+\delta-2)} \end{bmatrix} \begin{bmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_{\delta-1}} \end{bmatrix} = 0 \quad (4)$$

Sia A l'ultima matrice, si ha:

$$\det A \underbrace{=}_{\text{mettendo in evidenza dalle colonne}} \alpha^{i_1 b}\alpha^{i_2 b} \ldots \alpha^{i_{\delta-1} b} \det \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \alpha^{i_3} & \ldots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \alpha^{2i_3} & \ldots & \alpha^{2i_{\delta-1}} \\ \vdots & & & & \\ \alpha^{(\delta-2)i_1} & \alpha^{(\delta-2)i_2} & \alpha^{(\delta-2)i_3} & \ldots & \alpha^{(\delta-2)i_{\delta-1}} \end{bmatrix} =$$

$$\underbrace{=}_{\text{Vandermonde}} \alpha^{i_1 b}\alpha^{i_2 b} \ldots \alpha^{i_{\delta-1} b} \prod_{1 \le j < h \le \delta-1} (\alpha^{i_j} - \alpha^{i_h}) \quad (5)$$

$\det A \neq 0 \underbrace{\Leftrightarrow}_{(5)} \alpha^{i_j} \neq \alpha^{i_h} \ \ \forall j \neq h$ questo e' vero per la [4.2,pg.5]

$\Rightarrow A$ e' invertibile $\underbrace{\Rightarrow}_{(4)} c_{i_1} = \cdots = c_{i_{\delta-1}} = 0 \underbrace{\Leftrightarrow}_{(3)} c(x) = 0$

ma questo e' assurdo contro $c(x) \in C \setminus \{0\}$

□

Definition 4.4. C e' RS (Reed-Solomon) $\Leftrightarrow$ C e' BCH e inoltre $n \Big/ q-1$

Proposition 4.5. *Sia C di Reed-Solomon, allora*

1. $U_n = \langle \alpha \rangle \subseteq F_q$
2. $P_{min}\left(\alpha^i, F_q\right) = x - \alpha^i$
3. *C e' generato da* $g(x) = \prod_{i=b}^{b+\delta-2} x - \alpha^i \in F_q[x]$, *ovvero:*

$$C = \{q(x)g(x) \mid q(x) \in F_q[x], \ \deg q(x) + \deg g(x) \le n-1 \text{ oppure } q(x) = 0\}$$

4. $d(C) = \delta$, $\dim C = n - \delta + 1$, $\deg g(x) = \delta - 1$
   ovvero C e' MDS di tipo $[n, n-\delta+1, \delta]$

Proof:
⟨1⟩ Dim 1.

$$C \text{ RS } \Rightarrow n \Big/ q-1 \underbrace{\Rightarrow}_{\text{[QUA,Oss4.4.1,pg.18]}} U_n \subseteq F_q$$

$\langle 2 \rangle$ Dim 2.

$$\alpha^i \in U_n \subseteq F_q \Rightarrow P_{\min}\left(\alpha^i, F_q\right) = x - \alpha^i$$

$\langle 3 \rangle$ Dim 3.

Per la [RE,Prop4.6,pg.24] si ha

$$g(x) = \operatorname{mcm}\left(P_{\min}\left(\alpha^i, F_q\right) \mid i = b, b+1, \ldots, b+\delta-2\right) \underbrace{=}_{2.} \operatorname{mcm}\left(x - \alpha^i \mid i = b, b+1, \ldots, b+\delta-2\right) \quad (1)$$

$\left\{\alpha^i\right\}$ distinte per la [4.2,pg.5], $\deg x - \alpha^i = 1 \Rightarrow \left\{x - \alpha^i\right\}$ coprimi fra loro $\Rightarrow$ mcm e' il prodotto

$\langle 4 \rangle$ Dim. 4.

Si ha

$$\deg g(x) \underbrace{=}_{3.,\ [4.2,\text{pg.}5]} \delta - 1 \underbrace{\Rightarrow}_{\text{[RE,Prop4.3,pg.21]}} \dim C = n - \deg g(x) = n - \delta + 1 \quad (1)$$

Inoltre,

$$n - \delta + 1 \underbrace{=}_{(1)} \dim C \underbrace{\leq}_{\text{[QUA,Prop3.3,pg.1]}} n - d(C) + 1 \underbrace{\leq}_{[4.3,\text{pg.}5]} n - \delta + 1 \Rightarrow \begin{cases} \dim C = n - \delta + 1 \\ \delta = d(c) \end{cases}$$

□

Proposition 4.6. *Sotto le ipotesi di [4.5,pg.6], sia $g(x) = g_0 + g_1 x + \cdots + g_{\delta-1}x^{\delta-1}$ il generatore di C, allora*

1. $\left\{\lambda x^i g(x) \mid i \geq 0, \ \ \lambda \in F_q^*\right\} \subseteq \{c(x) \in C \mid w(c(x)) = d(C)\}$

   Cioe', gli elementi di $\lambda x^i g(x)$ hanno peso minimo. Domanda: vale $\supseteq$?
2. $g_{\delta-1} = 1, \ \ g_h = (-1)^{\delta-1-h} \displaystyle\sum_{i_1 < i_2 < \cdots < i_{\delta-1-h}} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_{\delta-1-h}} \ \ \forall h = 0, \ldots, \delta-2$

   dove: $\{\alpha_1, \ldots, \alpha_{\delta-1}\} = \left\{\alpha^i \mid i = b, b+1, \ldots, b+\delta-2\right\}$
3. $g_i \neq 0 \ \ \forall i$

Proof:

$\langle 1 \rangle$ Dim. 1., 3.

$\langle 1.1 \rangle$ $w(g(x)) = d(C)$

$$\deg g(x) \underbrace{=}_{[4.5,\text{pg.}6]} \delta - 1 \Rightarrow g(x) = g_0 + g_1 x + \cdots + g_{\delta-1}x^{\delta-1} \quad (1)$$

$$w(g(x)) = |\{i \mid g_i \neq 0\}| \underbrace{\leq}_{(1)} \delta$$

$$d(C) \underbrace{=}_{[4.5,\text{pg.}6]} \delta, \ \ g(x) \in C \Rightarrow w(g(x)) \geq d(C) = \delta$$

$$\Rightarrow w(g(x)) = \delta = d(C) \quad (2)$$

Inoltre, $x^i g(x)$ e' $g(x)$ "spostato", ovvero,

$$g(x) \simeq (g_0, g_1, \ldots, g_{\delta-1}, 0, 0, \ldots, 0) \Rightarrow x^i g(x) \simeq (g_i, g_{i+1}, \ldots,)$$

e poiche' C e' ciclico, $x^i g(x) \in C$.
Infine,

$$(2) \Rightarrow g_i \neq 0 \ \ \forall i \ \ (3)$$
$$\lambda g_i = 0 \underbrace{\Leftrightarrow}_{g_i \neq 0} \lambda = 0$$

$\langle 2 \rangle$ Dim. 2.

$$g(x) \text{ monico } \Rightarrow g_{\delta-1} = 1$$

Gli altri coefficienti si ricavano applicando le formule di Viete' (vedi [AC,4.7,pg.72]) alla [4.5,pg.6]

□

Proposition 4.7. *Sia π la proiezione che tronca le ultime $n-m$ componenti:*

$$\pi : {F_q}^n \longrightarrow {F_q}^m, \ \ m < n$$
$$(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_m)$$

Se C e' RS, si ha

$$\pi(C) \text{ e' un codice MDS di tipo } [m, n-\delta+1, \delta-(n-m)], \text{ ovvero:}$$
$$\dim \pi(C) = \dim C = n-\delta+1, \ \ d(\pi(C)) = \delta-(n-m)$$

Questa proposizione permette di costruire codici MDS a partire dai codici MDS di Reed-Solomon.

Proof: Nota: questa proposizione e' una diretta conseguenza di [3.2,pg.3]. Diamo qui di seguito una dim. alternativa.
Sia $C' = \pi(C)$
$\langle 1 \rangle$ π e' surriettiva e lineare

$\langle 2 \rangle$ Dim. che $d(C') = \delta - (n-m)$
Per la [3.2,pg.3] si ha

$$d(C') \geq d(C) - (n-m)$$

Sia $g(x) \simeq (g_0, g_1, \ldots, g_{\delta-1}, 0, 0, \ldots, 0)$ il generatore di C (vedi [4.5,pg.6]),
$g(x) \in C \underbrace{\Rightarrow}_{C \text{ ciclico}} x^{n-d} g(x) \in C$
$x^{n-d} g(x) = (0, 0, \ldots, 0, g_0, g_1, \ldots, g_{\delta-1}) =$ $g(x)$ spostato negli ultimi posti
$\pi(x^{n-d} g(x)) = (0, 0, \ldots, 0, g_0, g_1, \ldots, g_{\delta-1-(n-m)})$ (1)
$g_i \neq 0 \ \ \forall i$ vedi [4.6,pg.7] (2)
(1), (2) $\Rightarrow w(\pi(x^{n-d} g(x))) = (\delta - 1 - (n-m)) + 1 \Rightarrow d(C') = \min w(C'^*) \leq \delta - (n-m) \Rightarrow$
$\underbrace{\Rightarrow}_{\text{passo ??}}$ $d(C') = \delta - (n-m)$ (3)

$\langle 3 \rangle$ $\dim C' = \dim C$
Per la [4.5,pg.6], $\dim C = n - \delta + 1$.

Per la [RE,prop4.3,pg.21], una matrice generatrice per C e'

$$G = \begin{bmatrix} g_0 & g_1 & \dots, & g_{\delta-1} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots, & g_{\delta-1} & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & \dots, & g_{\delta-1} & 0 & \dots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots, & g_{\delta-1} \end{bmatrix} \in n-\delta+1 \times n$$

G generatrice per C $\underbrace{\Rightarrow}_{\text{[QUA,prop3.3.1,pg.4]}}$ G di controllo per $C^\perp$

C RS $\underbrace{\Rightarrow}_{\text{[4.5,pg.6]}}$ C MDS $d(C) = \delta$ $\underbrace{\Rightarrow}_{\text{[QUA,prop3.4,pg.2]}}$ $C^\perp$ MDS $d(C^\perp) = n - d(C) + 2 = n - \delta + 2$ (4)

$d(C^\perp) \underbrace{=}_{\text{[QUA,prop3.2,pg.1]}} s+1 \underbrace{\Rightarrow}_{(4)} s = n-\delta+1 \Rightarrow$ qualsiasi insieme di s colonne di G e' l.i. $\Rightarrow$

$\Rightarrow$ qualsiasi minore di ordine $n-\delta+1$ e' invertibile (5)

$$G = \begin{bmatrix} G_1 \\ G_2 \\ \vdots \\ G_{n-\delta+1} \end{bmatrix}, \quad G_i \text{ riga}$$

$$G' = \pi(G) = \begin{bmatrix} \pi(G_1) \\ \vdots \\ \pi(G_{n-\delta+1}) \end{bmatrix} \in n-\delta+1 \times m \quad (6)$$

$$\begin{cases} (5) \\ (6) \\ n-\delta+1 \le m \end{cases} \Rightarrow \text{ le righe di G' } \textit{sonol.i.} \underbrace{\Rightarrow}_{\pi(G_i) \in C'} \dim C' \ge \dim C$$

π lineare e surriettiva $\Rightarrow \dim C' \le \dim C$

$\Rightarrow \dim C' = \dim C$

□

Example 4.8. Vogliamo costruire un codice con $n = 8$ (parole di 8 caratteri), $e = 2$ (correzione di due errori), MDS.

$$\frac{d-1}{2} \underbrace{=}_{\text{[RE,prop2.1,pg.10]}} e = 2 \Rightarrow d = 5$$

$$MDS \Rightarrow k = n - d + 1 = 8 - 5 + 1 = 4$$

Quindi cerchiamo un codice di tipo $[8, 4, 5]$.
Come campo scegliamo F_9. Costruiamo un RS con $b = 1$

$RS \Rightarrow d = \delta = \deg g(x) + 1$

$F_9 = F_{3^2} \simeq \dfrac{F_3[x]}{(x^2+1)} \simeq F_3[i] = \{a + ib \mid a, b \in F_3\}$

F_9^* ciclico , $|F_9^*| = 8 \underbrace{\Rightarrow}_{\text{biezione tra i divisori di } |G| \text{ e i sottogruppi}}$ $\exists!$ sottogruppo di ordine 4 ed e' $\langle i \rangle = \{1, i, -1, -i\}$

L'unico sottogruppo di ordine $2e'$ $\{1, -1\} \subseteq \langle i \rangle$

$1 + i \notin \langle i \rangle$, $1 + i \neq 1 \Rightarrow o(1+i) = 8 \Rightarrow F_9^* = \langle 1 \rangle + i$

Sia $\alpha = 1 + i$

$o(\alpha) = 8 \Rightarrow U_8 = \langle \alpha \rangle$

$\deg g(x) \underbrace{=}_{[4.5,\text{pg.6}]} \delta - 1 = 5 - 1 = 4 \underbrace{\Rightarrow}_{[4.5,\text{pg.6}]} g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) =$

$= (x - i - 1)(x - 2i)(x - 1 - 2i)(x + 1)$

$C(x) = \{q(x)g(x) \mid q(x) \in F_9[x],\ \deg q(x) \leq 3 \text{ oppure } q(x) = 0\}$

4.0.1 Trasformata di Fourier

Definition 4.9. Trasformata di Fourier finita.
Sia $U_n = \langle \beta \rangle$, supponiamo sempre $(n, p) = 1$, , con $p = \operatorname{char} F_q$, e inoltre che $U_n \subseteq F_q \Leftrightarrow n \Big/ q - 1$.
La trasformata di Fourier finita, relativa a β, e' la seguente applicazione:

$$\mathfrak{F}_\beta : F_q[x]_{n-1} \longrightarrow F_q[x]_{n-1}$$
$$v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} \mapsto v^*(x) = v(\beta^0) + v(\beta^1)x + \cdots + v(\beta^{n-1})x^{n-1}$$

Nota[2] In termini vettoriali:

$$\mathfrak{F}_\beta : F_q^n \longrightarrow F_q^n$$
$$v = (v_0, \ldots, v_{n-1}) \mapsto v^* = (v(\beta^0), \ldots, v(\beta^{n-1}))$$
$$\text{dove } v(\beta^j) = v \cdot ((\beta^j)^0, (\beta^j)^1, (\beta^j)^2, \ldots, (\beta^j)^{n-1}) = v \cdot (\beta^0, \beta^j, \beta^{2j}, \ldots, \beta^{(n-1)j})$$

Notazione:

$$v^* \overset{\text{def}}{=} \mathfrak{F}(v)$$
$$v_* \overset{\text{def}}{=} \mathfrak{F}^{-1}(v)$$

Proposition 4.10.

1. *Fourier e' un isomorfismo vettoriale.*

[2] Se il campo in cui operiamo e' $\mathbb{C}$, allora

$$\beta = e^{i\frac{2\pi}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

per questo motivo l'applicazione sopra definita si chiama Trasformata di Fourier Finita

2. *La matrice associata e' la matrice di Vandermonde*

$$A_{ij} = \beta^{ij} \quad \forall i,j = 0,\dots,n-1$$
$$A \in n\times n$$

(in questo caso numeriamo gli elementi di A a partire da 0.

$$v^* = Av, \quad \textit{dove } v^*, v \textit{ si intendono come colonne}$$

3. *L'inversa di $\mathfrak{F}$ e':*

1. $(\mathfrak{F}_\beta)^{-1} = \frac{1}{n}\mathfrak{F}_{\beta^{-1}}$
2. $w_* \overset{def}{=} \mathfrak{F}_{\beta^{-1}}(w) = (w(\beta^0), w(\beta^{-1}), w(\beta^{-2}), \dots, w(\beta^{-(n-1)})) = (w(\beta^{n-n}), w(\beta^{n-1}), w(\beta^{n-2}), \dots, w(\beta^1))$
3. $(A^{-1})_{ij} = \frac{1}{n}\beta^{-ij}$

Nota[3].

Proof:
$\langle 1\rangle$ Dimostriamo che $\mathfrak{F}$ e' lineare ed invertibile
Calcolare un polinomio $v(x)$ in un elemento $v(\alpha)$ equivale a effettuare un prodotto scalare.
Per questo motivo possiamo esprimere $\mathfrak{F}$ direttamente con una matrice:

$$v^* \underbrace{=}_{\text{def. di } \mathfrak{F}} \begin{pmatrix} v(\beta^0) \\ v(\beta^1) \\ v(\beta^2) \\ \vdots \\ v(\beta^{n-1}) \end{pmatrix} =$$

$$= \begin{pmatrix} (\beta^0, \beta^0, \beta^0, \dots, \beta^0)\cdot v \\ (\beta^0, \beta^1, \beta^2, \dots, \beta^{(n-1)})\cdot v \\ (\beta^0, (\beta^1)^2, \left(\beta^2\right)^2, \dots, \left(\beta^{(n-1)}\right)^2)\cdot v \\ \vdots \\ (\beta^0, \beta^j, \beta^{2j}, \dots, \beta^{(n-1)j})\cdot v \\ \vdots \\ (\beta^1, \beta^{n-1}, \beta^{2(n-1)}, \dots, \beta^{(n-1)(n-1)})\cdot v \end{pmatrix} = \begin{pmatrix} \beta^0 & \beta^0 & \beta^0 & \dots, & \beta^0 \\ \beta^0 & \beta^1 & \beta^2 & \dots, & \beta^{(n-1)} \\ \vdots & & & & \\ \beta^0 & \beta^j & \beta^{2j} & \dots, & \beta^{(n-1)j} \\ \vdots & & & & \\ \beta^1 & \beta^{n-1} & \beta^{2(n-1)} & \dots, & \beta^{(n-1)(n-1)} \end{pmatrix} v$$

Sia A l'ultima matrice. A e' una matrice di Vandermonde formata sulle radici $\left\{\beta^0, \beta^1, \dots, \beta^{n-1}\right\} = U_n$. Quindi e' invertibile.
$\langle 2\rangle$ Calcoliamo $\mathfrak{F}^{-1}$
$\langle 2.1\rangle$ Dim. che $(\mathfrak{F}_\beta)^{-1} = \frac{1}{n}\mathfrak{F}_{\beta^{-1}}$

[3] la 3. da' esplicitamente l'inversa della matrice di Vandermonde A

$v^* = \mathfrak{F}_\beta(v) = (v(\beta^0), \dots, v(\beta^{n-1}))$ (1)

$\mathfrak{F}_{\beta^{-1}}(v^*) = (v^*(\beta^0),\ v^*(\beta^{-1}),\ \dots,\ v^*(\beta^{-(n-1)}))$ (2)

Poniamo $\overline{\alpha} \stackrel{\text{def}}{=} (\alpha^0, \alpha, \dots, \alpha^{n-1})$

$$v^*(\beta^{-i}) = v^* \cdot \overline{\beta}^{-i} \underbrace{=}_{(1)} \sum_{j=0}^{n-1} v(\beta^j)\beta^{-ij} = \sum_{j=0}^{n-1}(v \cdot \overline{\beta}^j)\beta^{-ij} = \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} v_k \beta^{jk}\beta^{-ij} = \sum_{k=0}^{n-1} v_k \sum_{j=0}^{n-1} \beta^{j(k-i)} \quad (3)$$

$$\sum_{j=0}^{n-1} \beta^{j(k-i)} = \sum_{j=0}^{n-1} \left(\beta^{(k-i)}\right)^j =$$

$$\beta^{k-i} = 1 \Leftrightarrow k = i\ \ (\mathbb{Z}_n) \underbrace{\Leftrightarrow}_{0 \le i,k \le n-1} k = i\ \ (*)$$

$$\underbrace{=}_{[2.1,\text{pg.}1],\ (*)} \begin{cases} n & k = i \Leftrightarrow \beta^{(k-i)} = 1 \\ 0 & k \neq i \end{cases} = n\delta_{ik} \quad (4)$$

$$(3), (4) \Rightarrow v^*(\beta^{-i}) = \sum_{k=0}^{n-1} v_k n \delta_{ik} = n v_i \quad (5)$$

$$\mathfrak{F}_{\beta^{-1}}(v^*) \underbrace{=}_{(2),(5)} n(v_0, v_1, \dots, v_{n-1}) \Rightarrow \frac{1}{n}\mathfrak{F}_{\beta^{-1}}(v^*) = v \quad (6)$$

Abbiamo cosi' dimostrato che:

$$\left(\frac{1}{n}\mathfrak{F}_{\beta^{-1}}\right) \circ \mathfrak{F}_\beta(v) = v \Rightarrow \left(\frac{1}{n}\mathfrak{F}_{\beta^{-1}}\right)\mathfrak{F}_\beta = \text{id} \underbrace{\Rightarrow}_{\mathfrak{F}_\beta \text{ invertibile}} \left(\frac{1}{n}\mathfrak{F}_{\beta^{-1}}\right)\mathfrak{F}_\beta(\mathfrak{F}_\beta)^{-1} = (\mathfrak{F}_\beta)^{-1} \Leftrightarrow \frac{1}{n}\mathfrak{F}_{\beta^{-1}} = (\mathfrak{F}_\beta)^{-1}$$

□

Proposition 4.11. *I codici di Reed-Solomon, con $b = 1$, si ottengono dalla costruzione [3.1,pg.2] scegliendo $S = U_n$ e $k - 1 = n - \delta$. (nota[4])*

Remark 4.1. La costruzione [3.1,pg.2] fornisce un metodo per costruire codici MDS. Tuttavia, conviene usare i codici di Reed-Solomon, perche' esistono algoritmi di decodifica molto efficienti.

Proof: Sia $U_n = \langle\beta\rangle$.

⟨1⟩ Dimostriamo che il codice

$$D = \left\{(f(\beta^0), \dots, f(\beta^{n-1})) \mid f \in F_q[x]_{n-\delta}\right\}$$

e' isomorfo al codice di RS definito da β, scegliendo $b = 1$.

C e' MDS definito da β, con $b = 1 \Leftrightarrow$

$$\underbrace{\Leftrightarrow}_{def.} (n, p) = 1,\ n \Big/ q - 1,\ \ C = \left\{c(x) \in F_q[x]_{n-1} \mid c(\beta^i) = 0\ \ \forall i = 1, \dots, \delta - 1\right\} \quad (1)$$

dove $U_n = \langle\beta\rangle$

[4] quindi questa proposizione e' una dimostrazione alternativa del fatto che i codice RS sono MDS

Poiche' $(n,p)=1,\ n \Big/ q-1$, possiamo considerare le trasformate di Fourier dei $c(x)$, secondo β^{-1}:

$\mathfrak{F}_{\beta^{-1}}(c(x)) = c^*(x) = c(1) + c(\beta^{-1})x + c(\beta^{-2})x^2 + \cdots + c(\beta^{-(n-1)})x^{n-1} =$

$= c(1) + c(\beta^{n-1})x + c(\beta^{n-2})x^2 + \cdots + c(\beta^1)x^{n-1} \underbrace{=}_{(1)} c(1) + c(\beta^{n-1})x + c(\beta^{n-2})x^2 + \cdots + c(\beta^\delta)x^{n-\delta}$ (2)

Sia $C' = \mathfrak{F}_{\beta^{-1}}(C)$

(2) $\Rightarrow C' \subseteq F_q[x]_{n-\delta}$ (3)

$\mathfrak{F}_{\beta^{-1}}$ isomorfismo (vedi [4.10,pg.10]) $\Rightarrow \dim C' = \dim C \underbrace{=}_{[4.5,\text{pg.}6]} n-\delta+1 = \dim F_q[x]_{n-\delta}$ (3.1)

(3), (3.1) $\Rightarrow C' = F_q[x]_{n-\delta}$ (4)

C si ottiene con l'inversa di $\mathfrak{F}_{\beta^{-1}}$:

$$(\mathfrak{F}_{\beta^{-1}})^{-1} \underbrace{=}_{[4.10,\text{pg.}10]} \frac{1}{n}\mathfrak{F}_\beta \Rightarrow C = \frac{1}{n}\mathfrak{F}_\beta(C')$$

$$c(x) \in C \Leftrightarrow c(x) = \frac{1}{n}\sum_{i=0}^{n-1} c^*(\beta^i)x^i \leftrightarrow \big(c^*(\beta^0), \ldots, c^*(\beta^{n-1})\big) \underbrace{\in}_{(3)} D$$

$$\Rightarrow C \simeq D$$

□

4.0.2 Decodifica

Definition 4.12. Sia $C \subseteq F_q^n$ un codice RS, su $U_n = \langle\beta\rangle$, con $b=1$, $\dim C = k$, $d(C) = \delta$.
Sia $c(x)$ la parola trasmessa e $d(x) = c(x) + e(x)$ la parola ricevuta, con $e(x)$ errore.
Supponiamo che l'errore si possa correggere, ovvero (vedi [RE,Prop2.1,pg.10])

$$w = w(e(x)) \leq t = \lfloor \frac{\delta - 1}{2} \rfloor$$

Definiamo i seguenti oggetti:

$\overline{b} = (b_1, \ldots, b_w) = (e_{i_1}, \ldots, e_{i_w})$ vettore dei coefficienti non nulli di $e(x)$, con $0 \leq i_1 < \cdots < i_w \leq n-1$

$\overline{a} = (a_1, \ldots, a_w) = (\beta^{i_1}, \ldots, \beta^{i_w})$ vettore di posizione dei coefficienti $\overline{b}$

nota[5]

L'*error locator polynomial* e':

$$\sigma(x) = \prod_{i=1}^{w} x - a_i$$

Le *sindromi generalizzate* sono:

$$s_j = d(\beta^j) \ \ \forall j = 1, \ldots, \delta - 1$$

[5] esiste una corrispondenza biunivoca tra $\{\beta^{i_j} \mid j = 1, \ldots, w\}$ e $\{i_j \mid j = 1, \ldots, w\}$. Per questo motivo conoscere $\overline{a}$ equivale a conoscere $(i_1, \ldots, i_w)$

Proposition 4.13. *Sotto le ipotesi di [4.12,pg.13], si ha*

1. $e_j \neq 0 \Rightarrow \sigma(\beta^j) = 0 \ \ \forall j = 1, \ldots, n-1$
2. $s_j = d(\beta^j) = e(\beta^j) \ \ \forall j = 1, \ldots, \delta - 1$
3. $s_j\sigma_0 + s_{j+1}\sigma_1 + \cdots + s_{j+w}\sigma_w = 0 \ \ \forall j = 1, \ldots, w$
4. $\overline{b}$ *e' soluzione del sistema* $A \begin{pmatrix} b_1 \\ \vdots \\ b_w \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_w \end{pmatrix}$, *dove dove* A *e' la matrice* $A = (a^i_j)_{i=1,\ldots,w;\ j=1,\ldots,w}$

   la soluzione esiste ed e' unica
5. $(\sigma_0, \ldots, \sigma_{w-1})$ *e' soluzione di* $M_w \begin{pmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_{w-1} \end{pmatrix} = - \begin{pmatrix} s_{w+1} \\ s_{w+2} \\ \vdots \\ s_{2w} \end{pmatrix}$, *dove* $M_h = (s_{i+j-1})_{i=1,\ldots,h;\ j=1,\ldots,h}$

   la soluzione esiste ed e' unica
6. $w = \rho(M_t)$

Proof:
⟨1⟩

$$e_j \neq 0 \Rightarrow e_j \text{ e' un coefficiente di } e(x) \text{ non nullo } \Rightarrow \exists k : \ j = i_k \underbrace{\Leftrightarrow}_{\text{def di } \sigma(x)} \beta^{i_k} \text{ radice di } \sigma(x) \Leftrightarrow \sigma(\beta^j) = 0$$

⟨2⟩

$$1 \leq j \leq \delta - 1, \ c(x) \in C \text{ ReedSolomon} \Rightarrow c(\beta^j) = 0 \ \ (1)$$
$$s_j \underbrace{=}_{\text{def}} d(\beta^j) = c(\beta^j) + e(\beta^j) \underbrace{=}_{(1)} = e(\beta^j) \ \ \forall j = 1, \ldots, \delta - 1$$

⟨3⟩

⟨3.1⟩ Dimostrazione 1

Per definizione di $\overline{b}$:

$$e(x) = b_1 x^{i_1} + \cdots + b_w x^{i_w}$$
$$e(\beta^j) = b_1 \beta^{j i_1} + \cdots + b_w \beta^{j i_w} \underbrace{=}_{\text{def di } \overline{a}} b_1 a_1^j + \cdots + b_w a_w^j \ \ (1.1)$$
$$s_j \underbrace{=}_{2.} e(\beta^j) \underbrace{=}_{(1.1)} b_1 a_1^j + \cdots + b_w a_w^j \ \ \forall j = 1, \ldots, \delta - 1 \ \ (1.2)$$

Poniamo $b_i = a_i = 0 \ \ \forall w < i \leq t$.

$a_j = \beta^{i_j} \neq 0 \Rightarrow e_{i_j} \neq 0 \underbrace{\Rightarrow}_{1.} \sigma(a_j) = 0$

$a_i = 0 \Leftrightarrow i > w$

$\Rightarrow b_i a_i^j \sigma(a_i) = 0 \ \ \forall i = 1, \ldots, t \ \ (1.3)$

$(1.3) \Rightarrow \sum_{i=1}^{t} b_i a_i^j \sigma(a_i) = 0 \ \ (1.4)$

$$\sum_{i=1}^{t} b_i a_i^j \sigma(a_i) = \sum_{i=1}^{t} b_i a_i^j \left(\sigma_0 + \sigma_1 a_i + \cdots + \sigma_w a_i^w\right) = \sigma_0 \left(\sum_{i=1}^{t} b_i a_i^j\right) + \sigma_1 \left(\sum_{i=1}^{t} b_i a_i^{j+1}\right) + \cdots + \sigma_w \left(\sum_{i=1}^{t} b_i a_i^{j+w}\right) =$$

$$\sum_{i=1}^{t} b_i a_i^{j+h} \underbrace{=}_{(1.2),\ a_i = 0 \ \forall i > w} s_{j+h} \ \ \forall j = 1, \ldots, \delta - 1 - h (*)$$

$$\underbrace{=}_{(*)} \sigma_0 s_j + \sigma_1 s_{j+1} + \cdots + \sigma_w s_{j+w} \ \ (1.5)$$

$(1.4),\ (1.5) \Rightarrow \sigma_0 s_j + \sigma_1 s_{j+1} + \cdots + \sigma_w s_{j+w} = 0 \ \ \forall j = \delta - 1 - w \ \ (**)$

In particolare, poiche' $2w \leq 2t \leq \delta - 1 \Rightarrow w \leq \delta - 1 - w$, la $(**)$ vale per $j = 1, \ldots, w$.

$\langle 3.2 \rangle$ Dimostrazione alternativa 2

Diamo solo una bozza di dimostrazione.

$$\mathfrak{F}_{\beta^{-1}}(e(x)) = e^*(x) = \sum_{i=0}^{n-1} e(\beta^{n-i}) x^i \ \ (1)$$

$$e(x) = \left(\mathfrak{F}_{\beta^{-1}}\right)^{-1}(e^*(x)) = \frac{1}{n} \mathfrak{F}_{\beta}(e^*(x)) = \frac{1}{n} \sum_{i=1}^{n-1} e^*(\beta^i) x^i \ \ (2)$$

$e_k \Rightarrow e_k \sigma(\beta^k) = 0; \ \ e_k \neq 0 \underbrace{\Rightarrow}_{1.} e_k \sigma(\beta^k) = 0$

$$\Rightarrow e_k \sigma(\beta^k) \underbrace{=}_{1.} 0 \ \ \forall k = 1, \ldots, n-1 \ \ (3)$$

$(3) \underbrace{\Leftrightarrow}_{(2)} e^*(\beta^k) \sigma(\beta^k) = 0 \ \ \forall k = 1, \ldots, n-1 \Leftrightarrow \forall \beta^k \in U_n$ e' una radice di $e^*(x)\sigma(x) \Leftrightarrow x^n - 1 \Big/ e^*(x)\sigma(x) \ \ (4)$

$\deg e^*(x) \leq n-1, \ \deg \sigma(x) = w \Rightarrow \deg e^*(x)\sigma(x) \leq n + w - 1 \ \ (5) \Rightarrow$

$\underbrace{\Rightarrow}_{(4),(5)} e^*(x)\sigma(x) = (x^n - 1)(h_0 + h_1 x + \cdots + h_{w-1} x^{w-1}) \ \ (6) \Rightarrow$

$\Rightarrow$ in $e^*(x)\sigma(x)$ non sono presenti i termini di grado $r: \ w \leq r \leq n-1 \ \Rightarrow$ i loro coefficienti sono nulli (7)

calcoliamo i coefficienti sviluppando il prodotto e usando la (1):

$$(7) \Leftrightarrow \sum_{i=0}^{r} \sigma_{r-i} e(\beta^{n-i}) = 0 \ \ \forall r = w, w+1, \ldots, n-1$$

Utilizzando la 2., con un'opportuno cambio di variabili e un'opportuna scelta di β si ottiene la tesi.

$\langle 4 \rangle$

(1.2) $\underbrace{\Rightarrow}_{w\le t=\lfloor \delta-1/2\rfloor <\delta-1}$ $s_j = b_1 a_1^j + \cdots + b_w a_w^j \ \ \forall j = 1,\ldots,w \Leftrightarrow$

$$\Leftrightarrow \begin{pmatrix} a_1 & \ldots & a_w \\ a_1^2 & \ldots & a_w^2 \\ \vdots & & \\ a_1^w & \ldots & a_w^w \end{pmatrix} \overline{b} = \begin{pmatrix} s_1 \\ \vdots \\ s_w \end{pmatrix}$$

mettendo in evidenza nelle colonne di A: $\det A = a_1 \cdots a_w \begin{vmatrix} 1 & \ldots & 1 \\ a_1 & \ldots & a_w \\ \vdots & & \\ a_1^{w-1} & \ldots & a_w^{w-1} \end{vmatrix} \underbrace{=}_{\text{Vandermonde}} a_1 \cdots a_w \prod_{i<j}(a_i - a_j)$

Poiche'

$$a_i \neq a_j \ \ \forall i \neq j, \ \ a_i \neq 0 \ \ \forall i \Rightarrow \det A \neq 0 \ \ (9.2)$$

il sistema ammette un'unica soluzione.

$\langle 5 \rangle$

$\sigma(x)$ e' monico $\Rightarrow \sigma_w = 1 \underbrace{\Rightarrow}_{3.} -s_{j+w} = s_j\sigma_0 + s_{j+1}\sigma_1 + \cdots + s_{j+w-1}\sigma_{w-1} = 0 \ \ \forall j = 1,\ldots,w \Leftrightarrow$

$$\Leftrightarrow \begin{pmatrix} s_1 & s_2 & \ldots & s_{1+w-1} \\ s_2 & s_3 & \ldots & s_{2+w-1} \\ \vdots & & & \\ s_j & s_{j+1} & \ldots & s_{j+w-1} \\ \vdots & & & \\ s_w & s_{w+1} & \ldots & s_{2w-1} \end{pmatrix} \begin{pmatrix} \sigma_0 \\ \vdots \\ \sigma_{w-1} \end{pmatrix} = - \begin{pmatrix} \sigma_{w+1} \\ \vdots \\ \sigma_{2w} \end{pmatrix} \Leftrightarrow M_w \begin{pmatrix} \sigma_0 \\ \vdots \\ \sigma_{w-1} \end{pmatrix} = - \begin{pmatrix} \sigma_{w+1} \\ \vdots \\ \sigma_{2w} \end{pmatrix}$$

Resta da dimostrare che la soluzione esiste ed e' unica.

Per la (1.2), la matrice M_w si puo' cosi' decomporre:

$$M_w = A'_w \mathrm{diag}(b_1a_1, \ldots, b_wa_w)(A'_w)^t \quad (10)$$

$$\text{dove } A'_w = \begin{pmatrix} 1 & \ldots & 1 \\ a_1 & \ldots & a_w \\ \vdots & & \\ a_1^{w-1} & \ldots & a_w^{w-1} \end{pmatrix}$$

infatti:

$$\mathrm{diag}(b_1a_1, \ldots, b_wa_w)(A'_w)^t = \begin{pmatrix} b_1a_1(1, a_1, \ldots, a_1^{w-1}) \\ b_2a_2(1, a_2, \ldots, a_2^{w-1}) \\ \vdots \\ b_wa_w(1, a_w, \ldots, a_w^{w-1}) \end{pmatrix}$$

$$\left(A'_w \mathrm{diag}(b_1a_1, \ldots, b_wa_w)(A'_w)^t\right)_{ij} = (A_{w'})_i (\mathrm{diag}(b_1a_1, \ldots, b_wa_w)(A'_w)^t)^j = \begin{pmatrix} a_1^{i-1} & \ldots & a_w^{i-1} \end{pmatrix} \begin{pmatrix} b_1a_1a_1^{j-1} \\ b_2a_2a_2^{j-1} \\ \vdots \\ b_wa_wa_w^{j-1} \end{pmatrix} =$$

$$= b_1a_1a_1^{j-1}a_1^{i-1} + \cdots + b_wa_wa_w^{j-1}a_w^{i-1} = b_1a_1^{i+j-1} + \cdots + b_wa_w^{i+j-1} \underbrace{=}_{(1.2)} s_{i+j-1} \underbrace{=}_{\text{def. di } M_w} (M_w)_{ij} \quad (10.1)$$

Quindi,
$\det M_w = (\det A_w)^2 \det(\mathrm{diag}(b_1a_1, \ldots, b_wa_w)) = b_1a_1 \cdots b_wa_w(\det A_w)^2 \underbrace{\neq}_{b_i \neq 0 \text{ per def di } \overline{b},\ (9.2)} 0$

⟨6⟩
Estendiamo il vettore $\overline{b}$ ponendo $b_i = 0 \quad \forall i > w$ e scegliamo $a_{w+1}, \ldots, a_t$ in modo che $\{a_1, \ldots, a_t\}$ siano tutti distinti fra loro[6]. Si ha:

$$M_h = M_h = A'_h \mathrm{diag}(b_1a_1, \ldots, b_ha_h)(A'_h)^t \quad \forall w \leq h \leq t \quad (11)$$

infatti, basta rileggere la (10.1) considerando che $b_i = 0 \ \forall i > w$.

$\{a_1, \ldots, a_t\}$ distinti fra loro $\underbrace{\Rightarrow}_{A_h \text{ matrice di Vandermonde}}$ A'_h invertibile $\forall w \leq h \leq t \quad (11.1)$

$h = t$ e' il massimo indice che possiamo prendere perche':

$$(M_t)_{t,t} = s_{2t-1}$$
$$\text{gli } s_j \text{ sono } s_1, \ldots, s_{\delta-1}$$
$$2t - 1 \underbrace{\leq}_{t=\lfloor \delta - 1/2 \rfloor} \delta - 1$$

Quindi,

$$(11),\ (11.1) \underbrace{\Rightarrow}_{\text{[AL,7.13,pg.46]}} \rho(M_t) = \rho(\mathrm{diag}(b_ia_i \mid 1 \leq i \leq t)) =$$
$$= t - |\{1 \leq i \leq t \mid a_i = 0\}| = t - |\{1 \leq i \leq t \mid b_i = 0\}| = w$$

□

Proposition 4.14. *Algoritmo di decodifica.*
Sotto le ipotesi di [4.12,pg.13], si puo' utilizzare il seguente algoritmo per calcolare $c(x)$ a partire dalla parola ricevuta $w(x)$.

1. *Sia $t = \lfloor \delta - 1/2 \rfloor$*
2. *Calcola $s_j = w(\beta^j) \ \forall j = 1, \ldots, \delta - 1$*
3. *Calcola il rango $w = \rho(M_t)$, dove M_t e' la matrice $M_t = (s_{i+j-1})_{i=1,\ldots,t;\ j=1,\ldots,t}$*
4. *Risolvi il sistema:*

$$M_w \begin{pmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_{w-1} \end{pmatrix} = - \begin{pmatrix} s_{w+1} \\ s_{w+2} \\ \vdots \\ s_{2w} \end{pmatrix}$$

5. *Trova le radici $\overline{a} = (a_1, \ldots, a_w)$ di*

$$\sigma(x) = \sum_i \sigma_i x^i$$

   L'unico metodo generale noto per trovarle e' procedere per forza bruta sostituendo tutti i possibili elementi di F_q.

6. *Da $\overline{a}$ ricava il vettore $(i_1, \ldots, i_w)$ tale che $\beta^{i_j} = a_j$.*

[6] $\{a_1, \ldots, a_w\}$ sono gia' distinti fra loro

7. *Risolvi il sistema*

$$A \begin{pmatrix} b_1 \\ \vdots \\ b_w \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_w \end{pmatrix}$$

dove A *e' la matrice* $A = (a^i_j)_{i=1,\dots,w;\ j=1,\dots,w}$

8. $e(x)$ *e' il polinomio*

$$e(x) = b_1 x^{i_1} + \cdots + b_w x^{i_w}$$

9. *Correggi la parola* $w(x)$*:*

$$c(x) = w(x) - e(x)$$

$c(x)$ *e' la parola corretta*

Nota: un altro algoritmo di decodifica, piu' efficiente di questo, e' il "Berlekamp-Massey Algorithm".

Proof: La correttezza di questo algoritmo deriva dalla [4.13,pg.13] □

5 Appendice A

Qui di seguito vengono inclusi gli appunti cartacei appunti forniti dal professore Re Riccardo. Sono stati modificati con l'aggiunta di alcune annotazioni.
. . . TODO: da scannerizzare

6 Appendice B

Qui di seguito vengono inclusi i miei appunti cartacei.
. . . TODO: da scannerizzare

7 *

Index
*, 19

AlphaNDistinte, 5
Appendice A, 18
Appendice B, 18

BCH e Reed Solomon, 5
BCH-DistanzaDelta, 5

CostruzioneDiRSconFourier, 12
CostruzioneMDS, 2

Decodifica, 13
DefBCH, 5
DefRSDecodifica, 13
DefShortening, 4

error locator polynomial, 13

Fourier, 10

Introduzione, 1

MDS, 2

operazione di shortening, 4

PropFourier, 10
PropRSDecodifica, 14

RS-Coeffg(x), 7
RS-OssVarie, 6
RS-Proiezione, 8

ShortMDSestMDS, 4
sindromi generalizzate, 13
SommaDiUnita, 1

Trasformata di Fourier, 10
TroncatMDSestMDS, 3
TrovaHdaG, 1

Varie, 1