

Polinomio generale locatore d'errore per codici ciclici binari con lunghezza $n < 63$ e capacità di correzione d'errore $t \leq 2$

Elisa Signori

11 maggio 2009

Sommario

- 1 **Parte prima**
 - **Conoscenze preliminari**
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 **Parte seconda**
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - Conclusione
- 3 **Parte terza**
 - La classificazione è completa!
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

Conoscenze preliminari

Daremo, in questa sezione, alcuni importanti concetti e definizioni basilari che ci serviranno a capire meglio il senso e lo scopo di questo seminario.

Definizione (codice lineare a blocchi)

Sia \mathbb{F}_q il campo finito con q elementi e siano $k, n \in \mathbb{N}$ tali che $k \leq n$. Sia C un sottospazio vettoriale di $(\mathbb{F}_q)^n$ di dimensione k . Allora C è un codice lineare a blocchi su \mathbb{F}_q di dimensione k e lunghezza n .

Conoscenze preliminari

Daremo, in questa sezione, alcuni importanti concetti e definizioni basilari che ci serviranno a capire meglio il senso e lo scopo di questo seminario.

Definizione (codice lineare a blocchi)

Sia \mathbb{F}_q il campo finito con q elementi e siano $k, n \in \mathbb{N}$ tali che $k \leq n$. Sia C un sottospazio vettoriale di $(\mathbb{F}_q)^n$ di dimensione k . Allora C è un codice lineare a blocchi su \mathbb{F}_q di dimensione k e lunghezza n .

Conoscenze preliminari

Definizione (distanza di un codice lineare)

Sia C un codice lineare. Definiamo la distanza d di C come la minima distanza (qui intendiamo distanza di Hamming, ma potremmo darne delle altre) tra due diverse parole in C , cioè:

$$d = \min_{c, c' \in C, c \neq c'} d(c, c').$$

Equivalentemente, d è il peso minimo tra i pesi delle parole codice diverse da 0.

Conoscenze preliminari

Definizione (distanza di un codice lineare)

Sia C un codice lineare. Definiamo la distanza d di C come la minima distanza (qui intendiamo distanza di Hamming, ma potremmo darne delle altre) tra due diverse parole in C , cioè:

$$d = \min_{c, c' \in C, c \neq c'} d(c, c').$$

Equivalentemente, d è il peso minimo tra i pesi delle parole codice diverse da 0.

Conoscenze preliminari

Definizione (distanza di un codice lineare)

Sia C un codice lineare. Definiamo la distanza d di C come la minima distanza (qui intendiamo distanza di Hamming, ma potremmo darne delle altre) tra due diverse parole in C , cioè:

$$d = \min_{c, c' \in C, c \neq c'} d(c, c').$$

Equivalentemente, d è il peso minimo tra i pesi delle parole codice diverse da 0.

Conoscenze preliminari

Definizione (capacità di correzione d'errore)

Chiamiamo t la capacità di correzione d'errore di un codice lineare C , cioè il numero di errori che tale codice può correggere.

Teorema (stima della capacità di correzione d'errore)

Un codice C di parametri $[n, k, d]$ sul campo \mathbb{F}_q ha capacità di rilevazione d'errore $z = d - 1$ e capacità di correzione d'errore $t = \lfloor \frac{d-1}{2} \rfloor$.

Conoscenze preliminari

Definizione (capacità di correzione d'errore)

Chiamiamo t la capacità di correzione d'errore di un codice lineare C , cioè il numero di errori che tale codice può correggere.

Teorema (stima della capacità di correzione d'errore)

Un codice C di parametri $[n, k, d]$ sul campo \mathbb{F}_q ha capacità di rilevazione d'errore $z = d - 1$ e capacità di correzione d'errore $t = \lfloor \frac{d-1}{2} \rfloor$.

Conoscenze preliminari

Definizione (equivalenza tra codici)

Per ogni permutazione $\rho \in S_n$, denotiamo con $\tilde{\rho}$ la sua azione, associata al cambio di coordinate in $(\mathbb{F}_q)^n$:

$\tilde{\rho} : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$. Sia π una permutazione in \mathbb{F}_q ottenuta come:

- moltiplicazione per un elemento di \mathbb{F}_q diverso da 0;*
- automorfismo del campo;*
- combinazione dei due casi precedenti.*

Siano ora C_1 e C_2 due codici con la stessa lunghezza n .

Diciamo che C_1 e C_2 sono equivalenti se esiste una permutazione σ di $(\mathbb{F}_q)^n$ del tipo:

$\sigma : (v_1 \ \cdots \ v_n) \rightarrow \tilde{\rho} (\pi_1(v_1) \ \cdots \ \pi_n(v_n))$ tale che $\rho \in S_n$, $(\pi_i)_{i=1\dots n}$ come sopra e $\sigma(C_1) = C_2$.

Conoscenze preliminari

Definizione (equivalenza tra codici)

Per ogni permutazione $\rho \in S_n$, denotiamo con $\tilde{\rho}$ la sua azione, associata al cambio di coordinate in $(\mathbb{F}_q)^n$:

$\tilde{\rho} : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$. Sia π una permutazione in \mathbb{F}_q ottenuta come:

- moltiplicazione per un elemento di \mathbb{F}_q diverso da 0;*
- automorfismo del campo;*
- combinazione dei due casi precedenti.*

Siano ora C_1 e C_2 due codici con la stessa lunghezza n .

Diciamo che C_1 e C_2 sono equivalenti se esiste una permutazione σ di $(\mathbb{F}_q)^n$ del tipo:

$\sigma : (v_1 \ \cdots \ v_n) \rightarrow \tilde{\rho} (\pi_1(v_1) \ \cdots \ \pi_n(v_n))$ tale che $\rho \in S_n$, $(\pi_i)_{i=1\dots n}$ come sopra e $\sigma(C_1) = C_2$.

Conoscenze preliminari

Definizione (equivalenza tra codici)

Per ogni permutazione $\rho \in S_n$, denotiamo con $\tilde{\rho}$ la sua azione, associata al cambio di coordinate in $(\mathbb{F}_q)^n$:

$\tilde{\rho} : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$. Sia π una permutazione in \mathbb{F}_q ottenuta come:

- *moltiplicazione per un elemento di \mathbb{F}_q diverso da 0;*
- *automorfismo del campo;*
- *combinazione dei due casi precedenti.*

Siano ora C_1 e C_2 due codici con la stessa lunghezza n .

Diciamo che C_1 e C_2 sono equivalenti se esiste una permutazione σ di $(\mathbb{F}_q)^n$ del tipo:

$\sigma : (v_1 \ \cdots \ v_n) \rightarrow \tilde{\rho} (\pi_1(v_1) \ \cdots \ \pi_n(v_n))$ tale che $\rho \in S_n$, $(\pi_i)_{i=1\dots n}$ come sopra e $\sigma(C_1) = C_2$.

Conoscenze preliminari

Definizione (equivalenza tra codici)

Per ogni permutazione $\rho \in S_n$, denotiamo con $\tilde{\rho}$ la sua azione, associata al cambio di coordinate in $(\mathbb{F}_q)^n$:

$\tilde{\rho} : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$. Sia π una permutazione in \mathbb{F}_q ottenuta come:

- *moltiplicazione per un elemento di \mathbb{F}_q diverso da 0;*
- *automorfismo del campo;*
- *combinazione dei due casi precedenti.*

Siano ora C_1 e C_2 due codici con la stessa lunghezza n .

Diciamo che C_1 e C_2 sono equivalenti se esiste una permutazione σ di $(\mathbb{F}_q)^n$ del tipo:

$\sigma : (v_1 \ \cdots \ v_n) \rightarrow \tilde{\rho} (\pi_1(v_1) \ \cdots \ \pi_n(v_n))$ tale che $\rho \in S_n$, $(\pi_i)_{i=1 \dots n}$ come sopra e $\sigma(C_1) = C_2$.

Conoscenze preliminari

Definizione (equivalenza tra codici)

Per ogni permutazione $\rho \in S_n$, denotiamo con $\tilde{\rho}$ la sua azione, associata al cambio di coordinate in $(\mathbb{F}_q)^n$:

$\tilde{\rho} : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$. Sia π una permutazione in \mathbb{F}_q ottenuta come:

- *moltiplicazione per un elemento di \mathbb{F}_q diverso da 0;*
- *automorfismo del campo;*
- *combinazione dei due casi precedenti.*

Siano ora C_1 e C_2 due codici con la stessa lunghezza n .

Diciamo che C_1 e C_2 sono equivalenti se esiste una permutazione σ di $(\mathbb{F}_q)^n$ del tipo:

$\sigma : (v_1 \ \cdots \ v_n) \rightarrow \tilde{\rho} (\pi_1(v_1) \ \cdots \ \pi_n(v_n))$ tale che $\rho \in S_n$, $(\pi_i)_{i=1\dots n}$ come sopra e $\sigma(C_1) = C_2$.

Conoscenze preliminari

Definizione (equivalenza tra codici)

Per ogni permutazione $\rho \in S_n$, denotiamo con $\tilde{\rho}$ la sua azione, associata al cambio di coordinate in $(\mathbb{F}_q)^n$:

$\tilde{\rho} : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$. Sia π una permutazione in \mathbb{F}_q ottenuta come:

- *moltiplicazione per un elemento di \mathbb{F}_q diverso da 0;*
- *automorfismo del campo;*
- *combinazione dei due casi precedenti.*

Siano ora C_1 e C_2 due codici con la stessa lunghezza n .

Diciamo che C_1 e C_2 sono equivalenti se esiste una permutazione σ di $(\mathbb{F}_q)^n$ del tipo:

$\sigma : (v_1 \ \cdots \ v_n) \rightarrow \tilde{\rho} (\pi_1(v_1) \ \cdots \ \pi_n(v_n))$ tale che $\rho \in S_n$, $(\pi_i)_{i=1\dots n}$ come sopra e $\sigma(C_1) = C_2$.

Conoscenze preliminari

Un'importante insieme di codici è quello dei codici ciclici, di cui tratteremo diffusamente in questo seminario.

Definizione (codice ciclico)

Dato un n -vettore $c = (c_0 \ \cdots \ c_{n-1})$ possiamo considerare il suo shift:

$sh(c) = (c_{n-1} \ c_0 \ \cdots \ c_{n-2})$ che è ancora un n -vettore con lo stesso campo di coefficienti.

Sia C un codice di parametri $[n, k, d]$ sul campo

\mathbb{F}_q tale che $\forall c \in C, sh(c) \in C$. Diciamo allora che C è ciclico.

Conoscenze preliminari

Un'importante insieme di codici è quello dei codici ciclici, di cui tratteremo diffusamente in questo seminario.

Definizione (codice ciclico)

Dato un n -vettore $c = (c_0 \ \cdots \ c_{n-1})$ possiamo considerare il suo shift:

$sh(c) = (c_{n-1} \ c_0 \ \cdots \ c_{n-2})$ che è ancora un n -vettore con lo stesso campo di coefficienti.

Sia C un codice di parametri $[n, k, d]$ sul campo

\mathbb{F}_q tale che $\forall c \in C, sh(c) \in C$. Diciamo allora che C è ciclico.

Conoscenze preliminari

Osservazione

Le parole di C si prestano molto bene ad essere rappresentate come polinomi e questo può portare grandi vantaggi nell'operare con codici ciclici; infatti se $c = (c_0 \ \cdots \ c_{n-1})$:

$$pol_c(x) = c_0 + c_1 * x + \cdots + c_{n-1} * x^{n-1} \in \mathbb{F}_q[X].$$

Conoscenze preliminari

Osservazione

Notiamo anche che $\deg(pol_C) \leq (n-1) \Rightarrow pol_C \in \mathbb{F}_q[x]/(x^n-1)$.
E' noto che, se C è un codice di parametri $[n, k, d]$ ciclico, allora C , visto come sottoanello di $\mathbb{F}_q[x]/(x^n-1)$, è un ideale.

Poiché $\mathbb{F}_q[x]/(x^n-1)$ è un anello a ideali principali, esiste una classe di polinomi equivalenti $[g] \in \mathbb{F}_q[x]/(x^n-1)$ che genera C . Tale classe ammette un unico rappresentante $g \in \mathbb{F}_q[x]$ di grado minimo. Tale g è detto polinomio generatore di C e $\deg(g) = n - k, g|(x^n - 1)$.

Conoscenze preliminari

Osservazione

Notiamo anche che $\deg(pol_C) \leq (n-1) \Rightarrow pol_C \in \mathbb{F}_q[x]/(x^n-1)$.
E' noto che, se C è un codice di parametri $[n, k, d]$ ciclico, allora C , visto come sottoanello di $\mathbb{F}_q[x]/(x^n-1)$, è un ideale.

Poiché $\mathbb{F}_q[x]/(x^n-1)$ è un anello a ideali principali, esiste una classe di polinomi equivalenti $[g] \in \mathbb{F}_q[x]/(x^n-1)$ che genera C . Tale classe ammette un unico rappresentante $g \in \mathbb{F}_q[x]$ di grado minimo. Tale g è detto polinomio generatore di C e $\deg(g) = n - k, g|(x^n - 1)$.

Conoscenze preliminari

Definizione (complete defining set)

Sia g il generatore di un codice ciclico C di parametri $[n, k, d]$ e sia α una radice n -esima primitiva dell'unità nel campo di spezzamento di $x^n - 1$.

Definiamo S_C l'insieme:

$$S_C = \{i_1, \dots, i_{n-k} \mid g(\alpha^{i_j}) = 0, \forall j \in 1, 2, \dots, (n-k)\}.$$

S_C è detto complete defining set di C .

Conoscenze preliminari

Definizione (defining set)

L'insieme S'_C è un defining set per C se

- 1 $S'_C \subset S_C$;
- 2 $\forall f \in \mathbb{F}_q[x]$ vale: $f(\alpha^{i'}) = 0, \forall i' \in S'_C \Rightarrow f(\alpha^i) = 0, \forall i \in S_C$.

Poiché ogni codice ciclico è completamente determinato dalle radici del suo generatore g , una matrice di controllo di parità per C , \mathcal{H} , è data dal teorema seguente.

Conoscenze preliminari

Definizione (defining set)

L'insieme S'_C è un defining set per C se

- 1 $S'_C \subset S_C$;
- 2 $\forall f \in \mathbb{F}_q[x]$ vale: $f(\alpha^{i'}) = 0, \forall i' \in S'_C \Rightarrow f(\alpha^i) = 0, \forall i \in S_C$.

Poiché ogni codice ciclico è completamente determinato dalle radici del suo generatore g , una matrice di controllo di parità per C , \mathcal{H} , è data dal teorema seguente.

Conoscenze preliminari

Definizione (defining set)

L'insieme S'_C è un defining set per C se

- 1 $S'_C \subset S_C$;
- 2 $\forall f \in \mathbb{F}_q[x]$ vale: $f(\alpha^{i'}) = 0, \forall i' \in S'_C \Rightarrow f(\alpha^i) = 0, \forall i \in S_C$.

Poiché ogni codice ciclico è completamente determinato dalle radici del suo generatore g , una matrice di controllo di parità per C , \mathcal{H} , è data dal teorema seguente.

Conoscenze preliminari

Definizione (defining set)

L'insieme S'_C è un defining set per C se

- 1 $S'_C \subset S_C$;
- 2 $\forall f \in \mathbb{F}_q[x]$ vale: $f(\alpha^{i'}) = 0, \forall i' \in S'_C \Rightarrow f(\alpha^i) = 0, \forall i \in S_C$.

Poiché ogni codice ciclico è completamente determinato dalle radici del suo generatore g , una matrice di controllo di parità per C , \mathcal{H} , è data dal teorema seguente.

Conoscenze preliminari

Teorema

Sia C un codice ciclico con $(n, q) = 1$. Sia $S_C = \{i_1, \dots, i_{n-k}\}$ il suo defining set e sia α una radice n -esima primitiva dell'unità nel campo di spezzamento di $x^n - 1$ su \mathbb{F}_q .

Allora una matrice di controllo di parità per C è data da:

$$\mathcal{H} = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

Tale matrice \mathcal{H} è detta matrice di controllo di parità standard per C .

Conoscenze preliminari

Teorema

Sia C un codice ciclico con $(n, q) = 1$. Sia $S_C = \{i_1, \dots, i_{n-k}\}$ il suo defining set e sia α una radice n -esima primitiva dell'unità nel campo di spezzamento di $x^n - 1$ su \mathbb{F}_q .

Allora una matrice di controllo di parità per C è data da:

$$\mathcal{H} = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

Tale matrice \mathcal{H} è detta matrice di controllo di parità standard per C .

Conoscenze preliminari

Teorema

Sia C un codice ciclico con $(n, q) = 1$. Sia $S_C = \{i_1, \dots, i_{n-k}\}$ il suo defining set e sia α una radice n -esima primitiva dell'unità nel campo di spezzamento di $x^n - 1$ su \mathbb{F}_q .

Allora una matrice di controllo di parità per C è data da:

$$\mathcal{H} = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}.$$

Tale matrice \mathcal{H} è detta matrice di controllo di parità standard per C .

Conoscenze preliminari

Decodifica con le sindromi

Supponiamo di trasmettere una parola codice $\hat{c} \in C$. Sia y il vettore ricevuto ed e il vettore errore. Abbiamo che:

$$y = \hat{c} + e \Rightarrow e = y - \hat{c}.$$

Se applichiamo \mathcal{H} (matrice di controllo di parità) a y abbiamo:

$$\mathcal{H}y = \mathcal{H}(\hat{c} + e) = \mathcal{H}\hat{c} + \mathcal{H}e = 0 + \mathcal{H}e = s.$$

L' $(n - k)$ -vettore s è detto sindrome associata a y .

N.B. La sindrome dipende soltanto dall'errore, non dalla parola che viene trasmessa, quindi per convenzione porremo

$$\hat{c} = 0 \Rightarrow y = e.$$

Conoscenze preliminari

Decodifica con le sindromi

Supponiamo di trasmettere una parola codice $\hat{c} \in C$. Sia y il vettore ricevuto ed e il vettore errore. Abbiamo che:

$$y = \hat{c} + e \Rightarrow e = y - \hat{c}.$$

Se applichiamo \mathcal{H} (matrice di controllo di parità) a y abbiamo:

$$\mathcal{H}y = \mathcal{H}(\hat{c} + e) = \mathcal{H}\hat{c} + \mathcal{H}e = 0 + \mathcal{H}e = s.$$

L' $(n - k)$ -vettore s è detto sindrome associata a y .

N.B. La sindrome dipende soltanto dall'errore, non dalla parola che viene trasmessa, quindi per convenzione porremo

$$\hat{c} = 0 \Rightarrow y = e.$$

Conoscenze preliminari

Decodifica con le sindromi

Supponiamo di trasmettere una parola codice $\hat{c} \in C$. Sia y il vettore ricevuto ed e il vettore errore. Abbiamo che:

$$y = \hat{c} + e \Rightarrow e = y - \hat{c}.$$

Se applichiamo \mathcal{H} (matrice di controllo di parità) a y abbiamo:

$$\mathcal{H}y = \mathcal{H}(\hat{c} + e) = \mathcal{H}\hat{c} + \mathcal{H}e = 0 + \mathcal{H}e = s.$$

L' $(n - k)$ -vettore s è detto sindrome associata a y .

N.B. La sindrome dipende soltanto dall'errore, non dalla parola che viene trasmessa, quindi per convenzione porremo

$$\hat{c} = 0 \Rightarrow y = e.$$

Conoscenze preliminari

Decodifica con le sindromi

Supponiamo di trasmettere una parola codice $\hat{c} \in C$. Sia y il vettore ricevuto ed e il vettore errore. Abbiamo che:

$$y = \hat{c} + e \Rightarrow e = y - \hat{c}.$$

Se applichiamo \mathcal{H} (matrice di controllo di parità) a y abbiamo:

$$\mathcal{H}y = \mathcal{H}(\hat{c} + e) = \mathcal{H}\hat{c} + \mathcal{H}e = 0 + \mathcal{H}e = s.$$

L' $(n - k)$ -vettore s è detto sindrome associata a y .

N.B. La sindrome dipende soltanto dall'errore, non dalla parola che viene trasmessa, quindi per convenzione porremo

$$\hat{c} = 0 \Rightarrow y = e.$$

Conoscenze preliminari

Decodifica con le sindromi

Supponiamo di trasmettere una parola codice $\hat{c} \in C$. Sia y il vettore ricevuto ed e il vettore errore. Abbiamo che:

$$y = \hat{c} + e \Rightarrow e = y - \hat{c}.$$

Se applichiamo \mathcal{H} (matrice di controllo di parità) a y abbiamo:

$$\mathcal{H}y = \mathcal{H}(\hat{c} + e) = \mathcal{H}\hat{c} + \mathcal{H}e = 0 + \mathcal{H}e = s.$$

L' $(n - k)$ -vettore s è detto sindrome associata a y .

N.B. La sindrome dipende soltanto dall'errore, non dalla parola che viene trasmessa, quindi per convenzione porremo

$$\hat{c} = 0 \Rightarrow y = e.$$

Conoscenze preliminari

In particolare, nel caso binario, se abbiamo errori alle locazioni $(i_1 \ i_2 \ \dots \ i_m)$ sarà:

$$y = e = (0 \ \dots \ 0 \ i_1 \ 0 \ \dots \ i_m \ 0 \ \dots \ 0)$$

quindi la sindrome si esprime come somma delle colonne di \mathcal{H} corrispondenti alle locazioni d'errore, cioè:

$$s = \mathcal{H}_{i_1} + \dots + \mathcal{H}_{i_m}.$$

Conoscenze preliminari

In particolare, nel caso binario, se abbiamo errori alle locazioni $(i_1 \ i_2 \ \dots \ i_m)$ sarà:

$$y = e = (0 \ \dots \ 0 \ i_1 \ 0 \ \dots \ i_m \ 0 \ \dots \ 0)$$

quindi la sindrome si esprime come somma delle colonne di \mathcal{H} corrispondenti alle locazioni d'errore, cioè:

$$s = \mathcal{H}_{i_1} + \dots + \mathcal{H}_{i_m}.$$

Conoscenze preliminari

In particolare, nel caso binario, se abbiamo errori alle locazioni $(i_1 \ i_2 \ \dots \ i_m)$ sarà:

$$y = e = (0 \ \dots \ 0 \ i_1 \ 0 \ \dots \ i_m \ 0 \ \dots \ 0)$$

quindi la sindrome si esprime come somma delle colonne di \mathcal{H} corrispondenti alle locazioni d'errore, cioè:

$$s = \mathcal{H}_{i_1} + \dots + \mathcal{H}_{i_m}.$$

Conoscenze preliminari

Definizione (coset)

Sia C un codice di parametri $[n, k, d]$ sul campo \mathbb{F}_q e sia $a \in (\mathbb{F}_q)^n$. Denotiamo con $a + C$ l'insieme $\{a + c \mid c \in C\}$. Gli insiemi del tipo $a + C$ sono detti coset del codice.

Si verifica che, se C è un codice come sopra, due n -vettori stanno nello stesso coset di C se e solo se corrispondono alla stessa sindrome.

Conoscenze preliminari

Definizione (coset)

Sia C un codice di parametri $[n, k, d]$ sul campo \mathbb{F}_q e sia $a \in (\mathbb{F}_q)^n$. Denotiamo con $a + C$ l'insieme $\{a + c \mid c \in C\}$. Gli insiemi del tipo $a + C$ sono detti coset del codice.

Si verifica che, se C è un codice come sopra, due n -vettori stanno nello stesso coset di C se e solo se corrispondono alla stessa sindrome.

Conoscenze preliminari

Definizione (coset leader)

Per ogni coset $a + C$ e ogni vettore $v \in (a + C)$, diciamo che v è un coset leader se è un elemento di peso minimo nel coset.

Definizione (sindrome correggibile)

Se una sindrome s è associata ad un coset con un solo coset leader, allora s è detta sindrome correggibile (essendoci un unico coset leader la correzione dell'errore può avvenire senza ambiguità). In altre parole, è una sindrome associata a un errore di peso $\mu \leq t$.

Conoscenze preliminari

Definizione (coset leader)

Per ogni coset $a + C$ e ogni vettore $v \in (a + C)$, diciamo che v è un coset leader se è un elemento di peso minimo nel coset.

Definizione (sindrome correggibile)

Se una sindrome s è associata ad un coset con un solo coset leader, allora s è detta sindrome correggibile (essendoci un unico coset leader la correzione dell'errore può avvenire senza ambiguità). In altre parole, è una sindrome associata a un errore di peso $\mu \leq t$.

Conoscenze preliminari

Definizione (polinomio locatore d'errore)

*Sia C un codice tale che $(n, q) = 1$. Se durante una trasmissione occorrono μ errori ($\mu \leq t$), denotiamo con $L_e(z)$ (dove e rappresenta l'errore) il **polinomio locatore d'errore**, cioè un polinomio di grado μ le cui radici rappresentano le locazioni d'errore.*

Conoscenze preliminari

Definizione (locazioni d'errore)

Se \mathbf{e} è il vettore errore, abbiamo:

$$\mathbf{e} = (\underbrace{0, \dots, 0}_{k_1-1}, \overset{\uparrow}{1}_{k_1}, 0, \dots, 0, \overset{\uparrow}{1}_{k_l}, 0, \dots, 0, \overset{\uparrow}{1}_{k_\mu}, \underbrace{0, \dots, 0}_{n-1-k_\mu});$$

allora k_1, \dots, k_μ sono le locazioni d'errore, perciò:

$$L_e(z) = \prod_{l=1}^{\mu} (z - \alpha^{k_l}).$$

Conoscenze preliminari

Definizione (polinomio generale locatore d'errore)

Il **polinomio generale locatore d'errore** per un codice C è un polinomio $\mathcal{L} \in \mathbb{F}_q[X, z]$, dove $X = (x_1, \dots, x_{n-k})$, tale che:

- 1 $\mathcal{L}(X, z) = z^t + a_{t-1}(X)z^{t-1} + \dots + a_0(X)$, con $a_j(X) \in \mathbb{F}_q[X]$, $0 \leq j \leq (t-1)$;
- 2 data una sindrome correggibile $\mathbf{s} = (s_1, \dots, s_{n-k})$, se valutiamo le X variabili in \mathbf{s} abbiamo che le t radici di $\mathcal{L}(\mathbf{s}, z)$ sono le μ locazioni d'errore più lo zero con molteplicità $(t - \mu)$.

N.B. $\mathcal{L}(\mathbf{s}, z) = z^{t-\mu} L_e(z)$.

Conoscenze preliminari

Definizione (polinomio generale locatore d'errore)

Il **polinomio generale locatore d'errore** per un codice C è un polinomio $\mathcal{L} \in \mathbb{F}_q[X, z]$, dove $X = (x_1, \dots, x_{n-k})$, tale che:

- 1 $\mathcal{L}(X, z) = z^t + a_{t-1}(X)z^{t-1} + \dots + a_0(X)$, con $a_j(X) \in \mathbb{F}_q[X]$, $0 \leq j \leq (t-1)$;
- 2 data una sindrome correggibile $\mathbf{s} = (s_1, \dots, s_{n-k})$, se valutiamo le X variabili in \mathbf{s} abbiamo che le t radici di $\mathcal{L}(\mathbf{s}, z)$ sono le μ locazioni d'errore più lo zero con molteplicità $(t - \mu)$.

N.B. $\mathcal{L}(\mathbf{s}, z) = z^{t-\mu} L_e(z)$.

Conoscenze preliminari

Definizione (polinomio generale locatore d'errore)

Il **polinomio generale locatore d'errore** per un codice C è un polinomio $\mathcal{L} \in \mathbb{F}_q[X, z]$, dove $X = (x_1, \dots, x_{n-k})$, tale che:

- 1 $\mathcal{L}(X, z) = z^t + a_{t-1}(X)z^{t-1} + \dots + a_0(X)$, con $a_j(X) \in \mathbb{F}_q[X]$, $0 \leq j \leq (t-1)$;
- 2 data una sindrome correggibile $\mathbf{s} = (s_1, \dots, s_{n-k})$, se valutiamo le X variabili in \mathbf{s} abbiamo che le t radici di $\mathcal{L}(\mathbf{s}, z)$ sono le μ locazioni d'errore più lo zero con molteplicità $(t - \mu)$.

N.B. $\mathcal{L}(\mathbf{s}, z) = z^{t-\mu}L_e(z)$.

Conoscenze preliminari

Definizione (polinomio generale locatore d'errore)

Il **polinomio generale locatore d'errore** per un codice C è un polinomio $\mathcal{L} \in \mathbb{F}_q[X, z]$, dove $X = (x_1, \dots, x_{n-k})$, tale che:

- 1 $\mathcal{L}(X, z) = z^t + a_{t-1}(X)z^{t-1} + \dots + a_0(X)$, con $a_j(X) \in \mathbb{F}_q[X]$, $0 \leq j \leq (t-1)$;
- 2 data una sindrome correggibile $\mathbf{s} = (s_1, \dots, s_{n-k})$, se valutiamo le X variabili in \mathbf{s} abbiamo che le t radici di $\mathcal{L}(\mathbf{s}, z)$ sono le μ locazioni d'errore più lo zero con molteplicità $(t - \mu)$.

N.B. $\mathcal{L}(\mathbf{s}, z) = z^{t-\mu} L_e(z)$.

Sommario

1 Parte prima

- Conoscenze preliminari
- **Alcuni risultati di rilievo**
- Teoremi sulla struttura di alcuni codici

2 Parte seconda

- Codici con $t \leq 1$ e $n < 63$
- Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
- Caso $t = 2$ e $S = \{1, n - 1, l\}$
- Una nuova famiglia di codici
- Conclusione

3 Parte terza

- La classificazione è completa!
- Qualche teorema utile
- Casi 2 e 5 in dettaglio

Alcuni risultati di rilievo

Per un generico codice lineare C , non è dato sapere quando \mathcal{L} esiste e se esiste lo denoteremo con \mathcal{L}_C ; tuttavia sappiamo che **ogni codice ciclico ammette un polinomio generale locatore d'errore**. Dalla definizione di \mathcal{L}_C , abbiamo immediatamente il seguente algoritmo di decodifica:

```

Input  $\mathbf{s} = (s_1, \dots, s_{n-k})$ 
 $\mu = t$ 
While  $a_{t-\mu}(s_1, \dots, s_{n-k}) = 0$  do
Output  $\mu, L_e(z)$ 
  
```

dove $L_e(z) = \frac{\mathcal{L}_C(z)}{z^{t-\mu}}$.

Alcuni risultati di rilievo

Per un generico codice lineare C , non è dato sapere quando \mathcal{L} esiste e se esiste lo denoteremo con \mathcal{L}_C ; tuttavia sappiamo che **ogni codice ciclico ammette un polinomio generale locatore d'errore**. Dalla definizione di \mathcal{L}_C , abbiamo immediatamente il seguente algoritmo di decodifica:

```

Input  $\mathbf{s} = (s_1, \dots, s_{n-k})$ 
 $\mu = t$ 
While  $a_{t-\mu}(s_1, \dots, s_{n-k}) = 0$  do
Output  $\mu, L_e(z)$ 
  
```

dove $L_e(z) = \frac{\mathcal{L}_C(z)}{z^{t-\mu}}$.

Alcuni risultati di rilievo

Per un generico codice lineare C , non è dato sapere quando \mathcal{L} esiste e se esiste lo denoteremo con \mathcal{L}_C ; tuttavia sappiamo che **ogni codice ciclico ammette un polinomio generale locatore d'errore**. Dalla definizione di \mathcal{L}_C , abbiamo immediatamente il seguente algoritmo di decodifica:

```

Input  $\mathbf{s} = (s_1, \dots, s_{n-k})$ 
 $\mu = t$ 
While  $a_{t-\mu}(s_1, \dots, s_{n-k}) = 0$  do
Output  $\mu, L_e(z)$ 
  
```

dove $L_e(z) = \frac{\mathcal{L}_C(z)}{z^{t-\mu}}$.

Alcuni risultati di rilievo

Per un generico codice lineare C , non è dato sapere quando \mathcal{L} esiste e se esiste lo denoteremo con \mathcal{L}_C ; tuttavia sappiamo che **ogni codice ciclico ammette un polinomio generale locatore d'errore**. Dalla definizione di \mathcal{L}_C , abbiamo immediatamente il seguente algoritmo di decodifica:

```

Input  $\mathbf{s} = (s_1, \dots, s_{n-k})$ 
 $\mu = t$ 
While  $a_{t-\mu}(s_1, \dots, s_{n-k}) = 0$  do
Output  $\mu, L_e(z)$ 
  
```

dove $L_e(z) = \frac{\mathcal{L}_C(z)}{z^{t-\mu}}$.

Alcuni risultati di rilievo

Per un generico codice lineare C , non è dato sapere quando \mathcal{L} esiste e se esiste lo denoteremo con \mathcal{L}_C ; tuttavia sappiamo che **ogni codice ciclico ammette un polinomio generale locatore d'errore**. Dalla definizione di \mathcal{L}_C , abbiamo immediatamente il seguente algoritmo di decodifica:

```

Input  $\mathbf{s} = (s_1, \dots, s_{n-k})$ 
 $\mu = t$ 
While  $a_{t-\mu}(s_1, \dots, s_{n-k}) = 0$  do
Output  $\mu, L_e(z)$ 
  
```

dove $L_e(z) = \frac{\mathcal{L}_C(z)}{z^{t-\mu}}$.

Alcuni risultati di rilievo

D'ora in poi ci focalizzeremo su codici lineari ciclici e binari, cioè definiti su $\mathbb{F}_q = \mathbb{F}_2$. Sia t , come già detto in precedenza, la capacità di correzione d'errore. Allora vediamo che quando $t = 2$ o $t = 1$, il polinomio generale locatore d'errore assume una forma particolare, come spiegheremo nel teorema seguente.

Alcuni risultati di rilievo

D'ora in poi ci focalizzeremo su codici lineari ciclici e binari, cioè definiti su $\mathbb{F}_q = \mathbb{F}_2$. Sia t , come già detto in precedenza, la capacità di correzione d'errore. Allora vediamo che quando $t = 2$ o $t = 1$, il polinomio generale locatore d'errore assume una forma particolare, come spiegheremo nel teorema seguente.

Alcuni risultati di rilievo

Teorema

Sia C un codice con capacità di correzione d'errore $t = 1$ e sia \bar{s} una sindrome correggibile. Allora il polinomio generale locatore d'errore per C è $\mathcal{L}_C(X, z) = z + a$, dove $a \in \mathbb{F}_2[x]$.

Inoltre, c'è un errore $\Leftrightarrow a(\bar{s}) \neq 0$ e in tal caso la locazione d'errore è $a(\bar{s})$.

Sia ora C un codice con $t = 2$, \bar{s} una sindrome correggibile e \bar{z}_1, \bar{z}_2 le locazioni d'errore. Allora $\mathcal{L}_C(X, z) = z^2 + az + b$, dove $a, b \in \mathbb{F}_2[x]$ e $b(\bar{s}) = \bar{z}_1 \bar{z}_2$, $a(\bar{s}) = \bar{z}_1 + \bar{z}_2$.

Inoltre, ci sono due errori $\Leftrightarrow b(\bar{s}) \neq 0$ e c'è un errore soltanto $\Leftrightarrow b(\bar{s}) = 0$ e $a(\bar{s}) \neq 0$.

Alcuni risultati di rilievo

Teorema

Sia C un codice con capacità di correzione d'errore $t = 1$ e sia \bar{s} una sindrome correggibile. Allora il polinomio generale locatore d'errore per C è $\mathcal{L}_C(X, z) = z + a$, dove $a \in \mathbb{F}_2[x]$. Inoltre, c'è un errore $\Leftrightarrow a(\bar{s}) \neq 0$ e in tal caso la locazione d'errore è $a(\bar{s})$.

Sia ora C un codice con $t = 2$, \bar{s} una sindrome correggibile e \bar{z}_1, \bar{z}_2 le locazioni d'errore. Allora $\mathcal{L}_C(X, z) = z^2 + az + b$, dove $a, b \in \mathbb{F}_2[x]$ e $b(\bar{s}) = \bar{z}_1\bar{z}_2$, $a(\bar{s}) = \bar{z}_1 + \bar{z}_2$. Inoltre, ci sono due errori $\Leftrightarrow b(\bar{s}) \neq 0$ e c'è un errore soltanto $\Leftrightarrow b(\bar{s}) = 0$ e $a(\bar{s}) \neq 0$.

Alcuni risultati di rilievo

Teorema

Sia C un codice con capacità di correzione d'errore $t = 1$ e sia \bar{s} una sindrome correggibile. Allora il polinomio generale locatore d'errore per C è $\mathcal{L}_C(X, z) = z + a$, dove $a \in \mathbb{F}_2[x]$. Inoltre, c'è un errore $\Leftrightarrow a(\bar{s}) \neq 0$ e in tal caso la locazione d'errore è $a(\bar{s})$.

Sia ora C un codice con $t = 2$, \bar{s} una sindrome correggibile e \bar{z}_1, \bar{z}_2 le locazioni d'errore. Allora $\mathcal{L}_C(X, z) = z^2 + az + b$, dove $a, b \in \mathbb{F}_2[x]$ e $b(\bar{s}) = \bar{z}_1\bar{z}_2$, $a(\bar{s}) = \bar{z}_1 + \bar{z}_2$.

Inoltre, ci sono due errori $\Leftrightarrow b(\bar{s}) \neq 0$ e c'è un errore soltanto $\Leftrightarrow b(\bar{s}) = 0$ e $a(\bar{s}) \neq 0$.

Alcuni risultati di rilievo

Teorema

Sia C un codice con capacità di correzione d'errore $t = 1$ e sia \bar{s} una sindrome correggibile. Allora il polinomio generale locatore d'errore per C è $\mathcal{L}_C(X, z) = z + a$, dove $a \in \mathbb{F}_2[x]$. Inoltre, c'è un errore $\Leftrightarrow a(\bar{s}) \neq 0$ e in tal caso la locazione d'errore è $a(\bar{s})$.

Sia ora C un codice con $t = 2$, \bar{s} una sindrome correggibile e \bar{z}_1, \bar{z}_2 le locazioni d'errore. Allora $\mathcal{L}_C(X, z) = z^2 + az + b$, dove $a, b \in \mathbb{F}_2[x]$ e $b(\bar{s}) = \bar{z}_1 \bar{z}_2$, $a(\bar{s}) = \bar{z}_1 + \bar{z}_2$. Inoltre, ci sono due errori $\Leftrightarrow b(\bar{s}) \neq 0$ e c'è un errore soltanto $\Leftrightarrow b(\bar{s}) = 0$ e $a(\bar{s}) \neq 0$.

Alcuni risultati di rilievo

I codici che prendiamo in considerazione hanno lunghezza n tale che $n \leq 61$, n dispari e sono, come già detto sopra, ciclici e binari (cioè abbiamo $\mathbb{F}_q = \mathbb{F}_2$ e $(n, q) = 1$). Enunceremo ora un teorema che dà delle relazioni tra i polinomi locatori d'errore di codici equivalenti e tra sottocodici di un codice dato.

Alcuni risultati di rilievo

I codici che prendiamo in considerazione hanno lunghezza n tale che $n \leq 61$, n dispari e sono, come già detto sopra, ciclici e binari (cioè abbiamo $\mathbb{F}_q = \mathbb{F}_2$ e $(n, q) = 1$). Enunceremo ora un teorema che dà delle relazioni tra i polinomi locatori d'errore di codici equivalenti e tra sottocodici di un codice dato.

Alcuni risultati di rilievo

Teorema

Siano C , C' , C'' tre codici aventi stessa lunghezza e stessa capacità di correzione d'errore t . Siano \mathcal{L}_C , $\mathcal{L}_{C'}$, $\mathcal{L}_{C''}$ i loro rispettivi polinomi generali locatori d'errore.

Se C è un sottocodice di C' , allora possiamo assumere $\mathcal{L}_C = \mathcal{L}_{C'}$.

Se C è equivalente a C'' tramite la permutazione $\phi : (\mathbb{F}_2)^n \mapsto (\mathbb{F}_2)^n$, allora possiamo decodificare C usando $\mathcal{L}_{C''}$ (tramite ϕ).

Alcuni risultati di rilievo

Teorema

Siano C , C' , C'' tre codici aventi stessa lunghezza e stessa capacità di correzione d'errore t . Siano \mathcal{L}_C , $\mathcal{L}_{C'}$, $\mathcal{L}_{C''}$ i loro rispettivi polinomi generali locatori d'errore.

Se C è un sottocodice di C' , allora possiamo assumere $\mathcal{L}_C = \mathcal{L}_{C'}$.

Se C è equivalente a C'' tramite la permutazione $\phi : (\mathbb{F}_2)^n \mapsto (\mathbb{F}_2)^n$, allora possiamo decodificare C usando $\mathcal{L}_{C''}$ (tramite ϕ).

Alcuni risultati di rilievo

Teorema

Siano C , C' , C'' tre codici aventi stessa lunghezza e stessa capacità di correzione d'errore t . Siano \mathcal{L}_C , $\mathcal{L}_{C'}$, $\mathcal{L}_{C''}$ i loro rispettivi polinomi generali locatori d'errore.

Se C è un sottocodice di C' , allora possiamo assumere $\mathcal{L}_C = \mathcal{L}_{C'}$.

Se C è equivalente a C'' tramite la permutazione

$\phi : (\mathbb{F}_2)^n \mapsto (\mathbb{F}_2)^n$, allora possiamo decodificare C usando $\mathcal{L}_{C''}$ (tramite ϕ).

Alcuni risultati di rilievo

Definizione

Siano $0 \leq j \leq n$ e $1 \leq \mu \leq n$ numeri interi. Denotiamo con $J_{j,\mu}^X$ l'ideale in $\mathbb{F}_2[z_1, \dots, z_\mu, x]$ generato da :

$$\left\{ \sum_{l=1}^{\mu} z_l^j - x, x^{2^m} - x \right\}$$

$$\cup \{z_l^n - 1 \mid 1 \leq l \leq \mu\} \cup \{p(n, z_{\tilde{l}}, z_l) \mid 1 \leq \tilde{l} \leq l \leq \mu\}.$$

N.B. Notiamo che la varietà di un ideale del tipo $J_{j,\mu}^X$ corrisponde a errori di peso esattamente μ , rispetto a una sola sindrome.

Alcuni risultati di rilievo

Definizione

Siano $0 \leq j \leq n$ e $1 \leq \mu \leq n$ numeri interi. Denotiamo con $J_{j,\mu}^X$ l'ideale in $\mathbb{F}_2[z_1, \dots, z_\mu, x]$ generato da :

$$\left\{ \sum_{l=1}^{\mu} z_l^j - x, x^{2^m} - x \right\}$$

$$\cup \{z_l^n - 1 \mid 1 \leq l \leq \mu\} \cup \{p(n, z_{\tilde{l}}, z_l) \mid 1 \leq \tilde{l} \leq l \leq \mu\}.$$

N.B. Notiamo che la varietà di un ideale del tipo $J_{j,\mu}^X$ corrisponde a errori di peso esattamente μ , rispetto a una sola sindrome.

Alcuni risultati di rilievo

Quando $\mu = 2$, abbiamo $\mathcal{V}\left(\mathcal{J}_{j;2}^X \cap \mathbb{F}_2[z_1, z_2]\right) \subset T$, dove:

$T = \{(\beta_1, \beta_2) \in R^2 \mid \beta_1 \neq \beta_2\}$ e $R = \{\beta \in \mathbb{F} \mid \beta^n = 1\}$.

Nella notazione sopra, denotiamo con $\mathcal{V}(I)$ la varietà di un ideale I .

Dalle proprietà della varietà delle sindromi, abbiamo la proposizione che segue.

Alcuni risultati di rilievo

Quando $\mu = 2$, abbiamo $\mathcal{V}\left(J_{j,2}^X \cap \mathbb{F}_2[z_1, z_2]\right) \subset T$, dove:

$$T = \{(\beta_1, \beta_2) \in R^2 \mid \beta_1 \neq \beta_2\} \text{ e } R = \{\beta \in \mathbb{F} \mid \beta^n = 1\}.$$

Nella notazione sopra, denotiamo con $\mathcal{V}(I)$ la varietà di un ideale I .

Dalle proprietà della varietà delle sindromi, abbiamo la proposizione che segue.

Alcuni risultati di rilievo

Quando $\mu = 2$, abbiamo $\mathcal{V}\left(J_{j,2}^X \cap \mathbb{F}_2[z_1, z_2]\right) \subset T$, dove:

$T = \{(\beta_1, \beta_2) \in R^2 \mid \beta_1 \neq \beta_2\}$ e $R = \{\beta \in \mathbb{F} \mid \beta^n = 1\}$.

Nella notazione sopra, denotiamo con $\mathcal{V}(I)$ la varietà di un ideale I .

Dalle proprietà della varietà delle sindromi, abbiamo la proposizione che segue.

Alcuni risultati di rilievo

Quando $\mu = 2$, abbiamo $\mathcal{V}\left(J_{j,2}^X \cap \mathbb{F}_2[z_1, z_2]\right) \subset T$, dove:

$$T = \{(\beta_1, \beta_2) \in R^2 \mid \beta_1 \neq \beta_2\} \text{ e } R = \{\beta \in \mathbb{F} \mid \beta^n = 1\}.$$

Nella notazione sopra, denotiamo con $\mathcal{V}(I)$ la varietà di un ideale I .

Dalle proprietà della varietà delle sindromi, abbiamo la proposizione che segue.

Alcuni risultati di rilievo

Proposizione

Sia C un codice tale che $S = S_C = \{j_1, \dots, j_r\}$. Allora:

$$\mathcal{V}(I_C) = \bigcup_{0 \leq \mu \leq t} \mathcal{V}(J_{S, \mu}^{x_1, \dots, x_r}).$$

Alcuni risultati di rilievo

Nel caso $t = 2$, abbiamo:

$$\mathcal{V}(I_C) = \mathcal{V}(J_{S,0}) \sqcup \mathcal{V}(J_{S,1}) \sqcup \mathcal{V}(J_{S,2})$$

e quindi

$$\mathcal{V}(I_C^X) = \mathcal{V}(J_{S,0}^X) \sqcup \mathcal{V}(J_{S,1}^X) \sqcup \mathcal{V}(J_{S,2}^X)$$

dove A^X significa $A \cap \mathbb{F}_2[X]$, per ogni ideale $A \in \mathbb{F}_2[X, Z]$.

Cioè, $\mathcal{V}(J_{S,0}^X)$ rappresenta l'ideale delle sindromi di peso 0 (e la stessa cosa vale per le sindromi di peso 1 e 2). Quindi è chiaro che:

$$\mathcal{V}(J_{S,0}^X) = \{(0, \dots, 0) \in (\mathbb{F}_2)^r\}.$$

Alcuni risultati di rilievo

Nel caso $t = 2$, abbiamo:

$$\mathcal{V}(I_C) = \mathcal{V}(J_{S,0}) \sqcup \mathcal{V}(J_{S,1}) \sqcup \mathcal{V}(J_{S,2})$$

e quindi

$$\mathcal{V}(I_C^X) = \mathcal{V}(J_{S,0}^X) \sqcup \mathcal{V}(J_{S,1}^X) \sqcup \mathcal{V}(J_{S,2}^X)$$

dove A^X significa $A \cap \mathbb{F}_2[X]$, per ogni ideale $A \in \mathbb{F}_2[X, Z]$.

Cioè, $\mathcal{V}(J_{S,0}^X)$ rappresenta l'ideale delle sindromi di peso 0 (e la stessa cosa vale per le sindromi di peso 1 e 2). Quindi è chiaro che:

$$\mathcal{V}(J_{S,0}^X) = \{(0, \dots, 0) \in (\mathbb{F}_2)^r\}.$$

Alcuni risultati di rilievo

Nel caso $t = 2$, abbiamo:

$$\mathcal{V}(I_C) = \mathcal{V}(J_{S,0}) \sqcup \mathcal{V}(J_{S,1}) \sqcup \mathcal{V}(J_{S,2})$$

e quindi

$$\mathcal{V}(I_C^X) = \mathcal{V}(J_{S,0}^X) \sqcup \mathcal{V}(J_{S,1}^X) \sqcup \mathcal{V}(J_{S,2}^X)$$

dove A^X significa $A \cap \mathbb{F}_2[X]$, per ogni ideale $A \in \mathbb{F}_2[X, Z]$.

Cioè, $\mathcal{V}(J_{S,0}^X)$ rappresenta l'ideale delle sindromi di peso 0 (e la stessa cosa vale per le sindromi di peso 1 e 2). Quindi è chiaro che:

$$\mathcal{V}(J_{S,0}^X) = \{(0, \dots, 0) \in (\mathbb{F}_2)^r\}.$$

Alcuni risultati di rilievo

Definizione (bordering polynomial)

Con le notazioni date nelle precedenti definizioni, diciamo che $h \in \mathbb{F}_2[x_1, \dots, x_r]$ è un **bordering polynomial** se:

$$h(\mathcal{V}(J_{S,0}^X)) = h(\mathcal{V}(J_{S,1}^X)) = 0 \text{ e } h(\mathcal{V}(J_{S,2}^X)) = 1.$$

Sommario

1 Parte prima

- Conoscenze preliminari
- Alcuni risultati di rilievo
- **Teoremi sulla struttura di alcuni codici**

2 Parte seconda

- Codici con $t \leq 1$ e $n < 63$
- Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
- Caso $t = 2$ e $S = \{1, n - 1, l\}$
- Una nuova famiglia di codici
- Conclusione

3 Parte terza

- La classificazione è completa!
- Qualche teorema utile
- Casi 2 e 5 in dettaglio

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice con $n \leq 61$ e $d \in \{3, 4\}$ (cioè $t = 1$). Allora ci sono solo quattro casi possibili:

- 1 *C ha un defining set del tipo $S = \{m\}$, con $(n, m) = 1$;*
- 2 *C ha un defining set del tipo $S = \{m, h\}$, con $(m, h) = 1$;*
- 3 *C è sottocodice di un codice del tipo tra quelli sopra elencati;*
- 4 *C è equivalente a un codice del tipo tra quelli sopra elencati.*

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice con $n \leq 61$ e $d \in \{3, 4\}$ (cioè $t = 1$). Allora ci sono solo quattro casi possibili:

- 1 *C ha un defining set del tipo $S = \{m\}$, con $(n, m) = 1$;*
- 2 *C ha un defining set del tipo $S = \{m, h\}$, con $(m, h) = 1$;*
- 3 *C è sottocodice di un codice del tipo tra quelli sopra elencati;*
- 4 *C è equivalente a un codice del tipo tra quelli sopra elencati.*

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice con $n \leq 61$ e $d \in \{3, 4\}$ (cioè $t = 1$). Allora ci sono solo quattro casi possibili:

- 1 *C ha un defining set del tipo $S = \{m\}$, con $(n, m) = 1$;*
- 2 *C ha un defining set del tipo $S = \{m, h\}$, con $(m, h) = 1$;*
- 3 *C è sottocodice di un codice del tipo tra quelli sopra elencati;*
- 4 *C è equivalente a un codice del tipo tra quelli sopra elencati.*

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice con $n \leq 61$ e $d \in \{3, 4\}$ (cioè $t = 1$). Allora ci sono solo quattro casi possibili:

- 1 *C ha un defining set del tipo $S = \{m\}$, con $(n, m) = 1$;*
- 2 *C ha un defining set del tipo $S = \{m, h\}$, con $(m, h) = 1$;*
- 3 *C è sottocodice di un codice del tipo tra quelli sopra elencati;*
- 4 *C è equivalente a un codice del tipo tra quelli sopra elencati.*

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice con $n \leq 61$ e $d \in \{3, 4\}$ (cioè $t = 1$). Allora ci sono solo quattro casi possibili:

- 1 *C ha un defining set del tipo $S = \{m\}$, con $(n, m) = 1$;*
- 2 *C ha un defining set del tipo $S = \{m, h\}$, con $(m, h) = 1$;*
- 3 *C è sottocodice di un codice del tipo tra quelli sopra elencati;*
- 4 *C è equivalente a un codice del tipo tra quelli sopra elencati.*

Teoremi sulla struttura di alcuni codici

Il teorema appena visto e gli altri che seguiranno sono stati ottenuti tramite un metodo computazionale di ricerca diretto (il programma che ha svolto tali calcoli si chiama MAGMA ed è stato appositamente richiesto dagli autori di tali risultati).

Teorema

Sia C un codice con lunghezza $n \leq 125$ ($n \neq 105$) e distanza $d \in \{5, 6\}$. Allora C è equivalente ad un codice D tale che $1 \in S_D$.

Teoremi sulla struttura di alcuni codici

Il teorema appena visto e gli altri che seguiranno sono stati ottenuti tramite un metodo computazionale di ricerca diretto (il programma che ha svolto tali calcoli si chiama MAGMA ed è stato appositamente richiesto dagli autori di tali risultati).

Teorema

Sia C un codice con lunghezza $n \leq 125$ ($n \neq 105$) e distanza $d \in \{5, 6\}$. Allora C è equivalente ad un codice D tale che $1 \in S_D$.

Teoremi sulla struttura di alcuni codici

Riprendiamo ora un teorema sui codici BCH.

Teorema

Per ogni $m \geq 2$ ed ogni $1 \leq h \leq m$, sia C un codice BCH binario primitivo di lunghezza $n = 2^m - 1$ e distanza designata $\delta = 2^h - 1$.

Teoremi sulla struttura di alcuni codici

Riprendiamo ora un teorema sui codici BCH.

Teorema

Per ogni $m \geq 2$ ed ogni $1 \leq h \leq m$, sia C un codice BCH binario primitivo di lunghezza $n = 2^m - 1$ e distanza designata $\delta = 2^h - 1$.

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice con lunghezza $n \leq 125$, ($n \neq 105$) e distanza $d \in \{5, 6\}$. Allora C è equivalente a un codice D tale che $1, l \in S_D$, con l numero dispari, $l \geq 3$.

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono soltanto tre casi possibili:

1 C è uno dei codici seguenti:

$n = 9, S_C = \{0, 1\}; n = 15, S_C = \{1, 3\}, \{0, 1, 7\}; n = 17, S_C = \{1\}; n = 21, S_C = \{1, 3\}, \{0, 1, 5\}; n = 25, S_C = \{1\}; n = 27, S_C = \{0, 1\}, \{1, 9\}; n = 31, S_C = \{1, 15\}, \{1, 5\}, \{1, 3\}; n = 33, S_C = \{0, 1\}; n = 35, S_C = \{1, 3\}, \{1, 5\}; n = 39, S_C = \{0, 1\}; n = 43, S_C = \{1\}; n = 45, S_C = \{1, 3\}, \{1, 21\}, \{1, 9\}, \{0, 1, 7\}, \{1, 7, 15\}; n = 51, S_C = \{1, 3\}, \{1, 9\}, \{0, 1, 19\}, \{0, 1, 5\}; n = 55, S_C = \{1\}; n = 57, S_C = \{0, 1\};$

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono soltanto tre casi possibili:

1 C è uno dei codici seguenti:

$n = 9, S_C = \{0, 1\}; n = 15, S_C = \{1, 3\}, \{0, 1, 7\}; n =$
 $17, S_C = \{1\}; n = 21, S_C = \{1, 3\}, \{0, 1, 5\}; n =$
 $25, S_C = \{1\}; n = 27, S_C = \{0, 1\}, \{1, 9\}; n = 31, S_C =$
 $\{1, 15\}, \{1, 5\}, \{1, 3\}; n = 33, S_C = \{0, 1\}; n = 35, S_C =$
 $\{1, 3\}, \{1, 5\}; n = 39, S_C = \{0, 1\}; n = 43, S_C = \{1\}; n =$
 $45, S_C = \{1, 3\}, \{1, 21\}, \{1, 9\}, \{0, 1, 7\}, \{1, 7, 15\}; n =$
 $51, S_C = \{1, 3\}, \{1, 9\}, \{0, 1, 19\}, \{0, 1, 5\}; n = 55, S_C =$
 $\{1\}; n = 57, S_C = \{0, 1\};$

Teoremi sulla struttura di alcuni codici

- 2 C è un sottocodice di un codice tra quelli sopra elencati;
- 3 C è equivalente a un codice tra quelli dei due casi sopra.

Teoremi sulla struttura di alcuni codici

- 2 C è un sottocodice di un codice tra quelli sopra elencati;
- 3 C è equivalente a un codice tra quelli dei due casi sopra.

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono solo sette casi possibili:

- 1 n è tale che il codice con insieme di definizione $\{0, 1\}$ abbia distanza d almeno 5;
- 2 C è un codice BCH, cioè $S_C = \{1, 3\}$;
- 3 C ammette un insieme di definizione del tipo $S_C = \{1, n-1, l\}$, dove $l \in \{0, \frac{n}{3}\}$;
- 4 C ammette un insieme di definizione del tipo $S_C = \{1, \frac{n}{7}\}$, per qualche $l \geq 3$;

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono solo sette casi possibili:

- 1 n è tale che il codice con insieme di definizione $\{0, 1\}$ abbia distanza d almeno 5;
- 2 C è un codice BCH, cioè $S_C = \{1, 3\}$;
- 3 C ammette un insieme di definizione del tipo $S_C = \{1, n-1, l\}$, dove $l \in \{0, \frac{n}{3}\}$;
- 4 C ammette un insieme di definizione del tipo $S_C = \{1, \frac{n}{7}\}$, per qualche $l \geq 3$;

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono solo sette casi possibili:

- 1 n è tale che il codice con insieme di definizione $\{0, 1\}$ abbia distanza d almeno 5;
- 2 C è un codice BCH, cioè $S_C = \{1, 3\}$;
- 3 C ammette un insieme di definizione del tipo $S_C = \{1, n-1, l\}$, dove $l \in \{0, \frac{n}{3}\}$;
- 4 C ammette un insieme di definizione del tipo $S_C = \{1, \frac{n}{7}\}$, per qualche $l \geq 3$;

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono solo sette casi possibili:

- 1 n è tale che il codice con insieme di definizione $\{0, 1\}$ abbia distanza d almeno 5;
- 2 C è un codice BCH, cioè $S_C = \{1, 3\}$;
- 3 C ammette un insieme di definizione del tipo $S_C = \{1, n-1, l\}$, dove $l \in \{0, \frac{n}{3}\}$;
- 4 C ammette un insieme di definizione del tipo $S_C = \{1, \frac{n}{7}\}$, per qualche $l \geq 3$;

Teoremi sulla struttura di alcuni codici

Teorema

Sia C un codice $[n, k, d]$ con distanza $d \in \{5, 6\}$ ($t = 2$) e $7 \leq n \leq 63$ (n dispari). Allora ci sono solo sette casi possibili:

- 1 n è tale che il codice con insieme di definizione $\{0, 1\}$ abbia distanza d almeno 5;
- 2 C è un codice BCH, cioè $S_C = \{1, 3\}$;
- 3 C ammette un insieme di definizione del tipo $S_C = \{1, n-1, l\}$, dove $l \in \{0, \frac{n}{3}\}$;
- 4 C ammette un insieme di definizione del tipo $S_C = \{1, \frac{n}{7}\}$, per qualche $l \geq 3$;

Teoremi sulla struttura di alcuni codici

5 C è uno dei seguenti:

- $n = 31$, $S_C = \{1, 15\}$;
- $n = 31$, $S_C = \{1, 5\}$;
- $n = 45$, $S_C = \{1, 21\}$;
- $n = 51$, $S_C = \{1, 9\}$;
- $n = 51$, $S_C = \{0, 1, 5\}$;

6 C è un sottocodice dei codici sopra elencati;

7 C è un codice equivalente a uno dei casi precedenti.

Teoremi sulla struttura di alcuni codici

5 C è uno dei seguenti:

- $n = 31$, $S_C = \{1, 15\}$;
- $n = 31$, $S_C = \{1, 5\}$;
- $n = 45$, $S_C = \{1, 21\}$;
- $n = 51$, $S_C = \{1, 9\}$;
- $n = 51$, $S_C = \{0, 1, 5\}$;

6 C è un sottocodice dei codici sopra elencati;

7 C è un codice equivalente a uno dei casi precedenti.

Teoremi sulla struttura di alcuni codici

5 C è uno dei seguenti:

- $n = 31$, $S_C = \{1, 15\}$;
- $n = 31$, $S_C = \{1, 5\}$;
- $n = 45$, $S_C = \{1, 21\}$;
- $n = 51$, $S_C = \{1, 9\}$;
- $n = 51$, $S_C = \{0, 1, 5\}$;

6 C è un sottocodice dei codici sopra elencati;

7 C è un codice equivalente a uno dei casi precedenti.

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - **Codici con $t \leq 1$ e $n < 63$**
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - Conclusione
- 3 Parte terza
 - La classificazione è completa!
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

Codici con $t \leq 1$ e $n < 63$

In questa sezione, consideriamo **tutti i codici con $t \leq 1$ e $n \leq 61$** . Ci interessa esibire un polinomio locatore generale d'errore per ognuno di essi.

Il caso $t = 0$ è banale.

Se invece $t = 1$, possiamo distinguere i casi seguenti, in accordo con un teorema visto in precedenza.

Codici con $t \leq 1$ e $n < 63$

In questa sezione, consideriamo **tutti i codici con $t \leq 1$ e $n \leq 61$** . Ci interessa esibire un polinomio locatore generale d'errore per ognuno di essi.

Il caso $t = 0$ è banale.

Se invece $t = 1$, possiamo distinguere i casi seguenti, in accordo con un teorema visto in precedenza.

Codici con $t \leq 1$ e $n < 63$

In questa sezione, consideriamo **tutti i codici con $t \leq 1$ e $n \leq 61$** . Ci interessa esibire un polinomio locatore generale d'errore per ognuno di essi.

Il caso $t = 0$ è banale.

Se invece $t = 1$, possiamo distinguere i casi seguenti, in accordo con un teorema visto in precedenza.

Codici con $t \leq 1$ e $n < 63$

- 1) $S = \{m\}$, con $(n, m) = 1$; in questo caso, il codice C è equivalente al codice BCH con $t = 1$ e $S' = \{1\}$. Dato che $z_1^m = x_1$, $z_1^{n+1} = z_1$ e $(n, m) = 1$, possiamo applicare il lemma di Bezout per trovare un intero k tale che: $mk \equiv 1 \pmod{(n)}$. Ciò significa che

$$(z_1^m)^k = z_1 \Rightarrow x_1^k = z_1.$$

In altre parole, possiamo dire che

$$\mathcal{L}_C = z_1 + x_1^k.$$

Codici con $t \leq 1$ e $n < 63$

- 1) $S = \{m\}$, con $(n, m) = 1$; in questo caso, il codice C è equivalente al codice BCH con $t = 1$ e $S' = \{1\}$. Dato che $z_1^m = x_1$, $z_1^{n+1} = z_1$ e $(n, m) = 1$, possiamo applicare il lemma di Bezout per trovare un intero k tale che: $mk \equiv 1 \pmod{(n)}$. Ciò significa che

$$(z_1^m)^k = z_1 \Rightarrow x_1^k = z_1.$$

In altre parole, possiamo dire che

$$\mathcal{L}_C = z_1 + x_1^k.$$

Codici con $t \leq 1$ e $n < 63$

- 1) $S = \{m\}$, con $(n, m) = 1$; in questo caso, il codice C è equivalente al codice BCH con $t = 1$ e $S' = \{1\}$. Dato che $z_1^m = x_1$, $z_1^{n+1} = z_1$ e $(n, m) = 1$, possiamo applicare il lemma di Bezout per trovare un intero k tale che: $mk \equiv 1 \pmod{(n)}$. Ciò significa che

$$(z_1^m)^k = z_1 \Rightarrow x_1^k = z_1.$$

In altre parole, possiamo dire che

$$\mathcal{L}_C = z_1 + x_1^k.$$

Codici con $t \leq 1$ e $n < 63$

- 1) $S = \{m\}$, con $(n, m) = 1$; in questo caso, il codice C è equivalente al codice BCH con $t = 1$ e $S' = \{1\}$. Dato che $z_1^m = x_1$, $z_1^{n+1} = z_1$ e $(n, m) = 1$, possiamo applicare il lemma di Bezout per trovare un intero k tale che: $mk \equiv 1 \pmod{(n)}$. Ciò significa che

$$(z_1^m)^k = z_1 \Rightarrow x_1^k = z_1.$$

In altre parole, possiamo dire che

$$\mathcal{L}_C = z_1 + x_1^k.$$

Codici con $t \leq 1$ e $n < 63$ **2) $S = \{m, h\}$, con $(m, h) = 1$.**

Abbiamo che $z_1^m = x_1$ e $z_1^h = x_2$. Dal lemma di Bezout abbiamo che esistono due interi m' e h' tali che

$mm' + hh' = 1$ quindi $(z_1^m)^{m'} (z_1^h)^{h'} = z_1^{mm'+hh'} = z_1$ e $x_1^{m'} x_2^{h'} = z_1$. Dunque, concludendo:

$$\mathcal{L}_C = z_1 + x_1^{m'} x_2^{h'}.$$

Codici con $t \leq 1$ e $n < 63$

2) $S = \{m, h\}$, con $(m, h) = 1$.

Abbiamo che $z_1^m = x_1$ e $z_1^h = x_2$. Dal lemma di Bezout abbiamo che esistono due interi m' e h' tali che

$mm' + hh' = 1$ quindi $(z_1^m)^{m'} (z_1^h)^{h'} = z_1^{mm'+hh'} = z_1$ e $x_1^{m'} x_2^{h'} = z_1$. Dunque, concludendo:

$$\mathcal{L}_C = z_1 + x_1^{m'} x_2^{h'}.$$

Codici con $t \leq 1$ e $n < 63$

2) $S = \{m, h\}$, con $(m, h) = 1$.

Abbiamo che $z_1^m = x_1$ e $z_1^h = x_2$. Dal lemma di Bezout abbiamo che esistono due interi m' e h' tali che

$mm' + hh' = 1$ quindi $(z_1^m)^{m'} (z_1^h)^{h'} = z_1^{mm'+hh'} = z_1$ e $x_1^{m'} x_2^{h'} = z_1$. Dunque, concludendo:

$$\mathcal{L}_C = z_1 + x_1^{m'} x_2^{h'}.$$

Codici con $t \leq 1$ e $n < 63$

- 3)** C è un sottocodice di un codice C' del tipo 1) o 2) e in tal caso possiamo usare per C il polinomio locatore di C' , come già visto in un teorema precedente;
- 4)** C è equivalente a un codice appartenente ai casi 1), 2) o 3); anche in questo caso è possibile decodificare utilizzando il polinomio locatore del codice equivalente.

Codici con $t \leq 1$ e $n < 63$

- 3) C è un sottocodice di un codice C' del tipo 1) o 2) e in tal caso possiamo usare per C il polinomio locatore di C' , come già visto in un teorema precedente;
- 4) C è equivalente a un codice appartenente ai casi 1), 2) o 3); anche in questo caso è possibile decodificare utilizzando il polinomio locatore del codice equivalente.

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - **Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$**
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - Conclusione
- 3 Parte terza
 - La classificazione è completa!
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

Parte seconda

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Per quanto già visto, sappiamo che ogni codice con $t = 2$ e $n < 125$, $n \neq 105$ soddisfa l'ipotesi che $\{1, 2i + 1\} \subset S_C$. Vedremo che, per quanto riguarda il polinomio locatore, possiamo descrivere facilmente a , ma sfortunatamente possiamo avere soltanto una rappresentazione implicita per b .

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Teorema

Sia C un codice con $t = 2$ e $\{1, 2i + 1\} \subset S$, per qualche $i \geq 1$. Siano x_1 e x_2 le x -variabili corrispondenti a $1 \in S_C$ e a $(2i + 1)$ rispettivamente. Allora il polinomio generale locatore d'errore per C sarà:

$$\mathcal{L}_C(x_1, x_2, \dots, x_r, z) = z^2 + x_1 z + b,$$

dove $b \in \mathbb{F}_2[X]$; inoltre esiste $P \in \mathbb{F}_2[x_1, x_2, y]$ tale che

$$P(\overline{x}_1, \overline{x}_2, b(\mathbf{s})) = 0,$$

per ogni sindrome correggibile $\mathbf{s} = (\overline{x}_1, \overline{x}_2, \dots, \overline{x}_r)$.

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Teorema

Sia C un codice con $t = 2$ e $\{1, 2i + 1\} \subset S$, per qualche $i \geq 1$. Siano x_1 e x_2 le x -variabili corrispondenti a $1 \in S_C$ e a $(2i + 1)$ rispettivamente. Allora il polinomio generale locatore d'errore per C sarà:

$$\mathcal{L}_C(x_1, x_2, \dots, x_r, z) = z^2 + x_1 z + b,$$

dove $b \in \mathbb{F}_2[X]$; inoltre esiste $P \in \mathbb{F}_2[x_1, x_2, y]$ tale che

$$P(\bar{x}_1, \bar{x}_2, b(\mathbf{s})) = 0,$$

per ogni sindrome correggibile $\mathbf{s} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_r)$.

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Teorema

Sia C un codice con $t = 2$ e $\{1, 2i + 1\} \subset S$, per qualche $i \geq 1$. Siano x_1 e x_2 le x -variabili corrispondenti a $1 \in S_C$ e a $(2i + 1)$ rispettivamente. Allora il polinomio generale locatore d'errore per C sarà:

$$\mathcal{L}_C(x_1, x_2, \dots, x_r, z) = z^2 + x_1 z + b,$$

dove $b \in \mathbb{F}_2[X]$; inoltre esiste $P \in \mathbb{F}_2[x_1, x_2, y]$ tale che

$$P(\bar{x}_1, \bar{x}_2, b(\mathbf{s})) = 0,$$

per ogni sindrome correggibile $\mathbf{s} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_r)$.

Parte seconda

Caso generale per $t = 2: \{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2: \{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Abbiamo anche che $\deg_{y_3}(P) \leq i$ e P dipende solo da i e non dagli altri elementi di S .

Dimostrazione.

Come abbiamo già visto, $\mathcal{L}_C(X, z) = z^2 + az + b$, dove $a, b \in \mathbb{F}_2[X]$ e $b(\mathbf{s}) = \overline{z_1} \overline{z_2}$, $a(\mathbf{s}) = \overline{z_1} + \overline{z_2}$. Per quanto riguarda a , dal momento che $1 \in S_C$, abbiamo che $z_1 + z_2 = x_1$ e quindi $a = x_1$.

Per quanto riguarda b , abbiamo bisogno di alcuni lemmi che non vedremo in questo contesto. □

Parte seconda

Caso generale per $t = 2: \{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2: \{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Abbiamo anche che $\deg_{y_3}(P) \leq i$ e P dipende solo da i e non dagli altri elementi di S .

Dimostrazione.

Come abbiamo già visto, $\mathcal{L}_C(X, z) = z^2 + az + b$, dove $a, b \in \mathbb{F}_2[X]$ e $b(\mathbf{s}) = \overline{z_1} \overline{z_2}$, $a(\mathbf{s}) = \overline{z_1} + \overline{z_2}$. Per quanto riguarda a , dal momento che $1 \in S_C$, abbiamo che $z_1 + z_2 = x_1$ e quindi $a = x_1$.

Per quanto riguarda b , abbiamo bisogno di alcuni lemmi che non vedremo in questo contesto. □

Parte seconda

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Esempio

Sia C un codice con $S = \{1, 3\}$ e $t = 2$ (C in questo caso è un BCH).

Allora abbiamo che $z_1 + z_2 = x_1$ e $z_1^3 + z_2^3 = x_2$; quindi:

$$\mathcal{L}_C = z^2 + x_1 z + b.$$

Allora:

$$z_1^3 + z_2^3 = (z_1 + z_2)^3 + z_1 z_2 (z_1 + z_2) \Leftrightarrow b x_1 + x_2 + x_1^3 = 0.$$

Parte seconda

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Esempio

Sia C un codice con $S = \{1, 3\}$ e $t = 2$ (C in questo caso è un BCH).

Allora abbiamo che $z_1 + z_2 = x_1$ e $z_1^3 + z_2^3 = x_2$; quindi:

$$\mathcal{L}_C = z^2 + x_1 z + b.$$

Allora:

$$z_1^3 + z_2^3 = (z_1 + z_2)^3 + z_1 z_2 (z_1 + z_2) \Leftrightarrow b x_1 + x_2 + x_1^3 = 0.$$

Parte seconda

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Esempio

Sia C un codice con $S = \{1, 3\}$ e $t = 2$ (C in questo caso è un BCH).

Allora abbiamo che $z_1 + z_2 = x_1$ e $z_1^3 + z_2^3 = x_2$; quindi:

$$\mathcal{L}_C = z^2 + x_1 z + b.$$

Allora:

$$z_1^3 + z_2^3 = (z_1 + z_2)^3 + z_1 z_2 (z_1 + z_2) \Leftrightarrow b x_1 + x_2 + x_1^3 = 0.$$

Parte seconda

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$

Esempio

Sia C un codice con $S = \{1, 3\}$ e $t = 2$. Abbiamo allora $z_1 + z_2 = x_1$, $z_1^5 + z_2^5 = x_2$ e

$$\mathcal{L}_C = z^2 + x_1 z + b.$$

Quindi, facendo tutti i calcoli risulterà:

$$b^2 x_1 + b x_1^3 + x_2 + x_1^5 = 0.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - **Caso $t = 2$ e $S = \{1, n-1, l\}$**
 - Una nuova famiglia di codici
 - Conclusione
- 3 Parte terza
 - La classificazione è completa!
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Consideriamo ora un codice C con $t = 2$ e $S = \{1, n-1, l\}$.
 In tal caso, possiamo considerare le tre sindromi $\{x_1, x_2, x_3\}$ tali
 che:

$$z_1 + z_2 = x_1,$$

$$z_1^{n-1} + z_2^{n-1} = x_2,$$

$$z_1^l + z_2^l = x_3.$$

Sappiamo anche che $z_1^{n+1} = z_1$ e $z_2^{n+1} = z_2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Consideriamo ora un codice C con $t = 2$ e $S = \{1, n-1, l\}$.
 In tal caso, possiamo considerare le tre sindromi $\{x_1, x_2, x_3\}$ tali
 che:

$$z_1 + z_2 = x_1,$$

$$z_1^{n-1} + z_2^{n-1} = x_2,$$

$$z_1^l + z_2^l = x_3.$$

Sappiamo anche che $z_1^{n+1} = z_1$ e $z_2^{n+1} = z_2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Consideriamo ora un codice C con $t = 2$ e $S = \{1, n-1, l\}$.
 In tal caso, possiamo considerare le tre sindromi $\{x_1, x_2, x_3\}$ tali
 che:

$$z_1 + z_2 = x_1,$$

$$z_1^{n-1} + z_2^{n-1} = x_2,$$

$$z_1^l + z_2^l = x_3.$$

Sappiamo anche che $z_1^{n+1} = z_1$ e $z_2^{n+1} = z_2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Il polinomio generale locatore d'errore di C è del tipo

$$\mathcal{L}_C = z^2 + x_1 z + b(x_1, x_2, x_3)$$

dove $b(\overline{x}_1, \overline{x}_2, \overline{x}_3) = \overline{z}_1 \overline{z}_2$ per ogni sindrome correggibile $\mathbf{s} = (\overline{x}_1, \overline{x}_2, \overline{x}_3)$ corrispondente agli errori di locazioni $\overline{z}_1, \overline{z}_2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Il polinomio generale locatore d'errore di C è del tipo

$$\mathcal{L}_C = z^2 + x_1 z + b(x_1, x_2, x_3)$$

dove $b(\overline{x}_1, \overline{x}_2, \overline{x}_3) = \overline{z}_1 \overline{z}_2$ per ogni sindrome correggibile $\mathbf{s} = (\overline{x}_1, \overline{x}_2, \overline{x}_3)$ corrispondente agli errori di locazioni $\overline{z}_1, \overline{z}_2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Il polinomio generale locatore d'errore di C è del tipo

$$\mathcal{L}_C = z^2 + x_1 z + b(x_1, x_2, x_3)$$

dove $b(\overline{x_1}, \overline{x_2}, \overline{x_3}) = \overline{z_1} \overline{z_2}$ per ogni sindrome correggibile $\mathbf{s} = (\overline{x_1}, \overline{x_2}, \overline{x_3})$ corrispondente agli errori di locazioni $\overline{z_1}, \overline{z_2}$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Per studiare il caso in cui ci sono esattamente due errori ($\mu = 2$), ci bastano le prime due sindromi, come vedremo nel caso A di questa sezione. Per estendere al caso in cui c'è solo un errore, abbiamo bisogno anche della terza sindrome (che si usa per determinare un bordering polynomial \mathbf{h}), come vedremo nei casi B e C.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

A: $\mu = 2$

Supponiamo ci siano esattamente due errori. Ciò è equivalente a $\bar{z}_1 \neq 0, \bar{z}_2 \neq 0$. Sotto tali ipotesi abbiamo che:

$$(x_1 x_2) = (z_1 + z_2)(z_1^{n-1} + z_2^{n-1}) = z_1 z_2 (z_1^{n-2} + z_2^{n-2})$$

e $x_2^2 = (z_1^{n-1} + z_2^{n-1})^2 = z_1^{n-2} + z_2^{n-2}$. Quindi:

$$(x_1 x_2) = z_1 z_2 x_2^2, \text{ cioè } b = z_1 z_2 = \frac{x_1 x_2}{x_2^2} = \frac{x_1}{x_2}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

A: $\mu = 2$

Supponiamo ci siano esattamente due errori. Ciò è equivalente a $\bar{z}_1 \neq 0, \bar{z}_2 \neq 0$. Sotto tali ipotesi abbiamo che:

$$(x_1 x_2) = (z_1 + z_2)(z_1^{n-1} + z_2^{n-1}) = z_1 z_2 (z_1^{n-2} + z_2^{n-2})$$

e $x_2^2 = (z_1^{n-1} + z_2^{n-1})^2 = z_1^{n-2} + z_2^{n-2}$. Quindi:

$$(x_1 x_2) = z_1 z_2 x_2^2, \text{ cioè } b = z_1 z_2 = \frac{x_1 x_2}{x_2^2} = \frac{x_1}{x_2}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **A:** $\mu = 2$

Supponiamo ci siano esattamente due errori. Ciò è equivalente a $\bar{z}_1 \neq 0, \bar{z}_2 \neq 0$. Sotto tali ipotesi abbiamo che:

$$(x_1 x_2) = (z_1 + z_2)(z_1^{n-1} + z_2^{n-1}) = z_1 z_2 (z_1^{n-2} + z_2^{n-2})$$

e $x_2^2 = (z_1^{n-1} + z_2^{n-1})^2 = z_1^{n-2} + z_2^{n-2}$. Quindi:

$$(x_1 x_2) = z_1 z_2 x_2^2, \text{ cioè } b = z_1 z_2 = \frac{x_1 x_2}{x_2^2} = \frac{x_1}{x_2}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **A:** $\mu = 2$

Supponiamo ci siano esattamente due errori. Ciò è equivalente a $\bar{z}_1 \neq 0, \bar{z}_2 \neq 0$. Sotto tali ipotesi abbiamo che:

$$(x_1 x_2) = (z_1 + z_2)(z_1^{n-1} + z_2^{n-1}) = z_1 z_2 (z_1^{n-2} + z_2^{n-2})$$

e $x_2^2 = (z_1^{n-1} + z_2^{n-1})^2 = z_1^{n-2} + z_2^{n-2}$. Quindi:

$$(x_1 x_2) = z_1 z_2 x_2^2, \text{ cioè } b = z_1 z_2 = \frac{x_1 x_2}{x_2^2} = \frac{x_1}{x_2}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Abbiamo un caso particolare se $S' = \{0, 1\}$ è un insieme di definizione per C . Infatti, in tal caso, per le ipotesi fatte su S_C , affinché 1 generi 1 e $n-1 \equiv -1$, 1 e -1 devono stare nella stessa classe ciclotomica quindi, per qualche δ tale che $1 \leq \delta(n-1)$ avremo:

$$2^\delta \equiv -1 \pmod{n} \Rightarrow$$

$$1 \equiv -2^\delta \pmod{n}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Abbiamo un caso particolare se $S' = \{0, 1\}$ è un insieme di definizione per C . Infatti, in tal caso, per le ipotesi fatte su S_C , affinché 1 e $n-1 \equiv -1$, 1 e -1 devono stare nella stessa classe ciclotomica quindi, per qualche δ tale che $1 \leq \delta(n-1)$ avremo:

$$2^\delta \equiv -1 \pmod{n} \Rightarrow$$

$$1 \equiv -2^\delta \pmod{n}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Abbiamo un caso particolare se $S' = \{0, 1\}$ è un insieme di definizione per C . Infatti, in tal caso, per le ipotesi fatte su S_C , affinché 1 generi 1 e $n-1 \equiv -1$, 1 e -1 devono stare nella stessa classe ciclotomica quindi, per qualche δ tale che $1 \leq \delta(n-1)$ avremo:

$$2^\delta \equiv -1 \pmod{n} \Rightarrow$$

$$1 \equiv -2^\delta \pmod{n}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Abbiamo un caso particolare se $S' = \{0, 1\}$ è un insieme di definizione per C . Infatti, in tal caso, per le ipotesi fatte su S_C , affinché 1 generi 1 e $n-1 \equiv -1$, 1 e -1 devono stare nella stessa classe ciclotomica quindi, per qualche δ tale che $1 \leq \delta(n-1)$ avremo:

$$2^\delta \equiv -1 \pmod{n} \Rightarrow$$

$$1 \equiv -2^\delta \pmod{n}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Abbiamo un caso particolare se $S' = \{0, 1\}$ è un insieme di definizione per C . Infatti, in tal caso, per le ipotesi fatte su S_C , affinché 1 generi 1 e $n-1 \equiv -1$, 1 e -1 devono stare nella stessa classe ciclotomica quindi, per qualche δ tale che $1 \leq \delta(n-1)$ avremo:

$$2^\delta \equiv -1 \pmod{n} \Rightarrow$$

$$1 \equiv -2^\delta \pmod{n}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre:

$$\begin{aligned} z_1 &= z_1^{n+1} = z_1^{n-2^\delta} = \left(z_1^{n-2^\delta}\right) \left(z_1^n\right)^{2^\delta-1} = \\ &= z_1^{n-2^\delta+n(2^\delta-1)} = z_1^{n2^\delta-2^\delta} = z_1^{(n-1)2^\delta}. \end{aligned}$$

Ciò significa che:

$$x_2^{2^\delta} = \left(z_1^{n-1} + z_2^{n-1}\right)^{2^\delta} = z_1 + z_2 = x_1$$

quindi

$$b = \frac{x_1}{x_2} = \frac{x_2^{2^\delta}}{x_2} = x_2^{2^\delta-1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre:

$$\begin{aligned} z_1 &= z_1^{n+1} = z_1^{n-2^\delta} = \left(z_1^{n-2^\delta}\right) (z_1^n)^{2^\delta-1} = \\ &= z_1^{n-2^\delta+n(2^\delta-1)} = z_1^{n2^\delta-2^\delta} = z_1^{(n-1)2^\delta}. \end{aligned}$$

Ciò significa che:

$$x_2^{2^\delta} = \left(z_1^{n-1} + z_2^{n-1}\right)^{2^\delta} = z_1 + z_2 = x_1$$

quindi

$$b = \frac{x_1}{x_2} = \frac{x_2^{2^\delta}}{x_2} = x_2^{2^\delta-1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre:

$$\begin{aligned} z_1 &= z_1^{n+1} = z_1^{n-2^\delta} = \left(z_1^{n-2^\delta}\right) (z_1^n)^{2^\delta-1} = \\ &= z_1^{n-2^\delta+n(2^\delta-1)} = z_1^{n2^\delta-2^\delta} = z_1^{(n-1)2^\delta}. \end{aligned}$$

Ciò significa che:

$$x_2^{2^\delta} = \left(z_1^{n-1} + z_2^{n-1}\right)^{2^\delta} = z_1 + z_2 = x_1$$

quindi

$$b = \frac{x_1}{x_2} = \frac{x_2^{2^\delta}}{x_2} = x_2^{2^\delta-1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre:

$$\begin{aligned} z_1 &= z_1^{n+1} = z_1^{n-2^\delta} = \left(z_1^{n-2^\delta}\right) \left(z_1^n\right)^{2^\delta-1} = \\ &= z_1^{n-2^\delta+n(2^\delta-1)} = z_1^{n2^\delta-2^\delta} = z_1^{(n-1)2^\delta}. \end{aligned}$$

Ciò significa che:

$$x_2^{2^\delta} = \left(z_1^{n-1} + z_2^{n-1}\right)^{2^\delta} = z_1 + z_2 = x_1$$

quindi

$$b = \frac{x_1}{x_2} = \frac{x_2^{2^\delta}}{x_2} = x_2^{2^\delta-1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

B: $\mu = 1$ e $l = 0$

Dato che $l = 0$, trattiamo qui il caso in cui $S = \{0, 1, n-1\}$; l'ipotesi $\mu = 1$ significa che esattamente uno tra $\{z_1, z_2\}$ è 0. In particolare, se c'è un solo errore il prodotto $z_1 z_2$ dà 0.

Sfortunatamente la frazione $\frac{x-1}{x_2}$ diventa $\frac{z_1}{z_1^{-1}} = z_1^2$ e non può essere usata come b in questo caso.

Dobbiamo dunque moltiplicare per un bordering polynomial $h \in \mathbb{F}_2[x_1, x_2, x_3]$. Tale h assicura che il prodotto

$$\frac{x_1}{x_2} h(x_1, x_2, x_3)$$

assume il valore $\overline{z_1 z_2}$ sia quando $\mu = 1$ sia quando $\mu = 2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **B:** $\mu = 1$ e $l = 0$

Dato che $l = 0$, trattiamo qui il caso in cui $S = \{0, 1, n-1\}$; l'ipotesi $\mu = 1$ significa che esattamente uno tra $\{z_1, z_2\}$ è 0. In particolare, se c'è un solo errore il prodotto $z_1 z_2$ dà 0.

Sfortunatamente la frazione $\frac{x-1}{x_2}$ diventa $\frac{z_1}{z_1^{-1}} = z_1^2$ e non può essere usata come b in questo caso.

Dobbiamo dunque moltiplicare per un bordering polynomial $h \in \mathbb{F}_2[x_1, x_2, x_3]$. Tale h assicura che il prodotto

$$\frac{x_1}{x_2} h(x_1, x_2, x_3)$$

assume il valore $\overline{z_1 z_2}$ sia quando $\mu = 1$ sia quando $\mu = 2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **B:** $\mu = 1$ e $l = 0$

Dato che $l = 0$, trattiamo qui il caso in cui $S = \{0, 1, n-1\}$; l'ipotesi $\mu = 1$ significa che esattamente uno tra $\{z_1, z_2\}$ è 0. In particolare, se c'è un solo errore il prodotto $z_1 z_2$ dà 0.

Sfortunatamente la frazione $\frac{x-1}{x_2}$ diventa $\frac{z_1}{z_1^{-1}} = z_1^2$ e non può essere usata come b in questo caso.

Dobbiamo dunque moltiplicare per un bordering polynomial $h \in \mathbb{F}_2[x_1, x_2, x_3]$. Tale h assicura che il prodotto

$$\frac{x_1}{x_2} h(x_1, x_2, x_3)$$

assume il valore $\overline{z_1 z_2}$ sia quando $\mu = 1$ sia quando $\mu = 2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **B:** $\mu = 1$ e $l = 0$

Dato che $l = 0$, trattiamo qui il caso in cui $S = \{0, 1, n-1\}$; l'ipotesi $\mu = 1$ significa che esattamente uno tra $\{z_1, z_2\}$ è 0. In particolare, se c'è un solo errore il prodotto $z_1 z_2$ dà 0.

Sfortunatamente la frazione $\frac{x-1}{x_2}$ diventa $\frac{z_1}{z_1^{-1}} = z_1^2$ e non può essere usata come b in questo caso.

Dobbiamo dunque moltiplicare per un bordering polynomial $h \in \mathbb{F}_2[x_1, x_2, x_3]$. Tale h assicura che il prodotto

$$\frac{x_1}{x_2} h(x_1, x_2, x_3)$$

assume il valore $\overline{z_1 z_2}$ sia quando $\mu = 1$ sia quando $\mu = 2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **B:** $\mu = 1$ e $l = 0$

Dato che $l = 0$, trattiamo qui il caso in cui $S = \{0, 1, n-1\}$; l'ipotesi $\mu = 1$ significa che esattamente uno tra $\{z_1, z_2\}$ è 0. In particolare, se c'è un solo errore il prodotto $z_1 z_2$ dà 0.

Sfortunatamente la frazione $\frac{x-1}{x_2}$ diventa $\frac{z_1}{z_1^{-1}} = z_1^2$ e non può essere usata come b in questo caso.

Dobbiamo dunque moltiplicare per un bordering polynomial $h \in \mathbb{F}_2[x_1, x_2, x_3]$. Tale h assicura che il prodotto

$$\frac{x_1}{x_2} h(x_1, x_2, x_3)$$

assume il valore $\overline{z_1 z_2}$ sia quando $\mu = 1$ sia quando $\mu = 2$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Inoltre, poichè x_2^{-1} equivale praticamente a x_2^{n-1} , il prodotto suddetto vale 0 quando $\mu = 0$. Per costruire un h siffatto, usiamo la terza sindrome. Quando $l = 0$ abbiamo che

$$z_1^l + z_2^l = x_3 \Rightarrow z_1^n + z_2^n = x_3.$$

Dato che $z_1^n = 1 \Leftrightarrow z_1 \neq 0$, abbiamo che:

- $z_1^n + z_2^n = 1 + 1 = 0$, se $\mu = 2$;
- $z_1^n + z_2^n = 1$, se $\mu = 1$;
- $z_1^n + z_2^n = 0 + 0 = 0$, se $\mu = 0$.

Cioè, possiamo prendere

$$h = (1 + x_3).$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

C: $\mu = 1$ e $l = n/3$

Questo caso si sviluppa più o meno allo stesso modo del precedente, con l'unica differenza che, avendo $l = n/3$ otterremo un h diverso.

Otterremo, facendo i calcoli, che:

$$h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **C:** $\mu = 1$ e $l = n/3$

Questo caso si sviluppa più o meno allo stesso modo del precedente, con l'unica differenza che, avendo $l = n/3$ otterremo un h diverso.

Otterremo, facendo i calcoli, che:

$$h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$ **C:** $\mu = 1$ e $l = n/3$

Questo caso si sviluppa più o meno allo stesso modo del precedente, con l'unica differenza che, avendo $l = n/3$ otterremo un h diverso.

Otterremo, facendo i calcoli, che:

$$h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}.$$

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$

Caso $t = 2$ e $S = \{1, n-1, l\}$

Riassumendo, abbiamo il seguente teorema:

Teorema

Sia C un codice di parametri $[n, k, d]$, con $t = 2$. Supponiamo che C abbia un insieme di definizione $S = \{1, n-1, l\}$, con $l \geq 3$ dispari. Allora

$$\mathcal{L}_C = z^2 + x_1 z + \frac{x_1}{x_2} h(x_1, x_2, x_3),$$

dove h è un bordering polynomial.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

Riassumendo, abbiamo il seguente teorema:

Teorema

Sia C un codice di parametri $[n, k, d]$, con $t = 2$. Supponiamo che C abbia un insieme di definizione $S = \{1, n-1, l\}$, con $l \geq 3$ dispari. Allora

$$\mathcal{L}_C = z^2 + x_1 z + \frac{x_1}{x_2} h(x_1, x_2, x_3),$$

dove h è un bordering polynomial.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

In particolare:

- se $l = 0$, $h = 1 + x_3$;
- se $l = n$, $h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}$.

Inoltre, se C ammette come insieme di definizione $S' = \{0, 1\}$ allora

$$\mathcal{L}_C = z^2 + x_1 z + x_2^{2^\delta - 1} h(x_1, x_2, x_3),$$

dove $1 \leq \delta \leq (n-1)$ è tale che $1 \equiv -2^\delta \pmod{n}$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

In particolare:

- se $l = 0$, $h = 1 + x_3$;
- se $l = n$, $h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}$.

Inoltre, se C ammette come insieme di definizione $S' = \{0, 1\}$ allora

$$\mathcal{L}_C = z^2 + x_1 z + x_2^{2^\delta - 1} h(x_1, x_2, x_3),$$

dove $1 \leq \delta \leq (n-1)$ è tale che $1 \equiv -2^\delta \pmod{n}$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

In particolare:

- se $l = 0$, $h = 1 + x_3$;
- se $l = n$, $h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}$.

Inoltre, se C ammette come insieme di definizione $S' = \{0, 1\}$ allora

$$\mathcal{L}_C = z^2 + x_1 z + x_2^{2^\delta - 1} h(x_1, x_2, x_3),$$

dove $1 \leq \delta \leq (n-1)$ è tale che $1 \equiv -2^\delta \pmod{n}$.

Parte seconda

Caso $t = 2$ e $S = \{1, n-1, l\}$ Caso $t = 2$ e $S = \{1, n-1, l\}$

In particolare:

- se $l = 0$, $h = 1 + x_3$;
- se $l = n$, $h = \frac{x_3^3 + 1}{x_1^{n/3} x_2^{2/3n} x_3 + 1}$.

Inoltre, se C ammette come insieme di definizione $S' = \{0, 1\}$ allora

$$\mathcal{L}_C = z^2 + x_1 z + x_2^{2^\delta - 1} h(x_1, x_2, x_3),$$

dove $1 \leq \delta \leq (n-1)$ è tale che $1 \equiv -2^\delta \pmod{n}$.

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - **Una nuova famiglia di codici**
 - Conclusione
- 3 Parte terza
 - La classificazione è completa!
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

Una nuova famiglia di codici

Definizione

*Sia C un codice; diciamo che C è un strictly two error correcting code (brevemente, **s2ec** code) se, una volta che sappiamo che sono avvenuti esattamente due errori, possiamo correggerli.*

Notiamo che ogni codice con distanza $d \geq 5$ è un s2ec code.

Definizione

Diciamo che n è s2ec se esiste un s2ec codice C avente lunghezza n e $S_C = \{1\}$.

Una nuova famiglia di codici

Definizione

*Sia C un codice; diciamo che C è un strictly two error correcting code (brevemente, **s2ec** code) se, una volta che sappiamo che sono avvenuti esattamente due errori, possiamo correggerli.*

Notiamo che ogni codice con distanza $d \geq 5$ è un s2ec code.

Definizione

Diciamo che n è s2ec se esiste un s2ec codice C avente lunghezza n e $S_C = \{1\}$.

Una nuova famiglia di codici

Definizione

*Sia C un codice; diciamo che C è un strictly two error correcting code (brevemente, **s2ec** code) se, una volta che sappiamo che sono avvenuti esattamente due errori, possiamo correggerli.*

Notiamo che ogni codice con distanza $d \geq 5$ è un s2ec code.

Definizione

Diciamo che n è s2ec se esiste un s2ec codice C avente lunghezza n e $S_C = \{1\}$.

Una nuova famiglia di codici

Diamo ora un importante lemma per capire la relazione tra distanza e s2ec:

Lemma

Sia C un codice con insieme di definizione $S_C = \{0, 1\}$ e distanza d . Le seguenti sono equivalenti:

- a) *C è un s2ec codice;*
- b) *$d \geq 5$.*

Esempio

Il codice con lunghezza $n = 9$ e $S_C = \{1\}$ è un s2ec codice, ma la sua distanza è soltanto $d = 3$.

Una nuova famiglia di codici

Diamo ora un importante lemma per capire la relazione tra distanza e s2ec:

Lemma

Sia C un codice con insieme di definizione $S_C = \{0, 1\}$ e distanza d . Le seguenti sono equivalenti:

- a) *C è un s2ec codice;*
- b) *$d \geq 5$.*

Esempio

Il codice con lunghezza $n = 9$ e $S_C = \{1\}$ è un s2ec codice, ma la sua distanza è soltanto $d = 3$.

Una nuova famiglia di codici

Diamo ora un importante lemma per capire la relazione tra distanza e s2ec:

Lemma

Sia C un codice con insieme di definizione $S_C = \{0, 1\}$ e distanza d . Le seguenti sono equivalenti:

- a) *C è un s2ec codice;*
- b) *$d \geq 5$.*

Esempio

Il codice con lunghezza $n = 9$ e $S_C = \{1\}$ è un s2ec codice, ma la sua distanza è soltanto $d = 3$.

Una nuova famiglia di codici

Diamo ora un importante lemma per capire la relazione tra distanza e s2ec:

Lemma

Sia C un codice con insieme di definizione $S_C = \{0, 1\}$ e distanza d . Le seguenti sono equivalenti:

- a) *C è un s2ec codice;*
- b) *$d \geq 5$.*

Esempio

Il codice con lunghezza $n = 9$ e $S_C = \{1\}$ è un s2ec codice, ma la sua distanza è soltanto $d = 3$.

Una nuova famiglia di codici

Diamo ora un importante lemma per capire la relazione tra distanza e s2ec:

Lemma

Sia C un codice con insieme di definizione $S_C = \{0, 1\}$ e distanza d . Le seguenti sono equivalenti:

- a) *C è un s2ec codice;*
- b) *$d \geq 5$.*

Esempio

Il codice con lunghezza $n = 9$ e $S_C = \{1\}$ è un s2ec codice, ma la sua distanza è soltanto $d = 3$.

Una nuova famiglia di codici

Diamo un'altro teorema ricavato per metodo di ricerca diretto:

Teorema

Ogni $n \leq 157$ è s2ec se e solo se

$n \in \{5, 9, 11, 13, 17, 19, 23, 25, 27, 29, 33, 37, 39, 41, 43, 47, 53,$
 $55, 57, 59, 61, 65, 67, 69, 71, 79, 81, 83, 87, 95, 97, 99, 101, 103,$
 $107, 109, 111, 113, 115, 121, 125, 129, 131, 137, 139, 141, 143,$
 $145, 149, 151\}.$

Una nuova famiglia di codici

Diamo un'altro teorema ricavato per metodo di ricerca diretto:

Teorema

Ogni $n \leq 157$ è s2ec se e solo se

$n \in \{5, 9, 11, 13, 17, 19, 23, 25, 27, 29, 33, 37, 39, 41, 43, 47, 53,$
 $55, 57, 59, 61, 65, 67, 69, 71, 79, 81, 83, 87, 95, 97, 99, 101, 103,$
 $107, 109, 111, 113, 115, 121, 125, 129, 131, 137, 139, 141, 143,$
 $145, 149, 151\}.$

Una nuova famiglia di codici

Ora enunciamo un teorema che ci dice come è fatto \mathcal{L} per i codici s2ec.

Teorema

Sia C un codice s2ec. Allora $\mathcal{L}_C = z^2 + x_1 z + b(X)$ è tale che

$$b = x_1^2 A(x_1^n) h,$$

dove $A \in \mathbb{F}[y]$ e h è un bordering polynomial.

Una nuova famiglia di codici

Ora enunciamo un teorema che ci dice come è fatto \mathcal{L} per i codici s2ec.

Teorema

Sia C un codice s2ec. Allora $\mathcal{L}_C = z^2 + x_1 z + b(X)$ è tale che

$$b = x_1^2 A(x_1^n) h,$$

dove $A \in \mathbb{F}[y]$ e h è un bordering polynomial.

Una nuova famiglia di codici

Una recente generalizzazione (dovuta a Chong-Dao Lee e Yao-Tsu Chang) del teorema sopra è la seguente:

Teorema

Sia C un codice binario ciclico con capacità di correzione d'errore t e $S_C = \{1\}$; sia x_1 la sindrome corrispondente a $1 \in S_C$. Allora il polinomio generale locatore d'errore per C è

$$\mathcal{L}_C = z^t + a_{t-1}(x_1)z^{t-1} + \cdots + a_0(x_1)$$

dove $a_i(x_1) = A(x_1^n) x_1^{t-i}$.

In particolare, per $t = 2$ abbiamo $b = a_0(x_1) = A(x_1^n) x_1^2$, che è quanto è stato scritto nel teorema precedente.

Una nuova famiglia di codici

Una recente generalizzazione (dovuta a Chong-Dao Lee e Yao-Tsu Chang) del teorema sopra è la seguente:

Teorema

Sia C un codice binario ciclico con capacità di correzione d'errore t e $S_C = \{1\}$; sia x_1 la sindrome corrispondente a $1 \in S_C$. Allora il polinomio generale locatore d'errore per C è

$$\mathcal{L}_C = z^t + a_{t-1}(x_1)z^{t-1} + \cdots + a_0(x_1)$$

dove $a_i(x_1) = A(x_1^n) x_1^{t-i}$.

In particolare, per $t = 2$ abbiamo $b = a_0(x_1) = A(x_1^n) x_1^2$, che è quanto è stato scritto nel teorema precedente.

Una nuova famiglia di codici

Una recente generalizzazione (dovuta a Chong-Dao Lee e Yao-Tsu Chang) del teorema sopra è la seguente:

Teorema

Sia C un codice binario ciclico con capacità di correzione d'errore t e $S_C = \{1\}$; sia x_1 la sindrome corrispondente a $1 \in S_C$. Allora il polinomio generale locatore d'errore per C è

$$\mathcal{L}_C = z^t + a_{t-1}(x_1)z^{t-1} + \dots + a_0(x_1)$$

dove $a_i(x_1) = A(x_1^n) x_1^{t-i}$.

In particolare, per $t = 2$ abbiamo $b = a_0(x_1) = A(x_1^n) x_1^2$, che è quanto è stato scritto nel teorema precedente.

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - **Conclusione**
- 3 Parte terza
 - La classificazione è completa!
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

Riassumendo...

CASO GENERALE: C con $t = 2$ e $n < 63$

Per concludere, se consideriamo un **qualsiasi codice C con $t = 2$ e $n < 63$ dispari**, il polinomio generale locatore d'errore è

$$\mathcal{L}_C = z^2 + x_1 z + b(X)$$

dove x_1 è la sindrome corrispondente a $1 \in S_C$ e b ha una rappresentazione esplicita che dipende dai casi specifici.

Riassumendo...

CASO GENERALE: C con $t = 2$ e $n < 63$

Per concludere, se consideriamo un **qualsiasi codice C con $t = 2$ e $n < 63$ dispari**, il polinomio generale locatore d'errore è

$$\mathcal{L}_C = z^2 + x_1 z + b(X)$$

dove x_1 è la sindrome corrispondente a $1 \in S_C$ e b ha una rappresentazione esplicita che dipende dai casi specifici.

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - Conclusione
- 3 Parte terza
 - **La classificazione è completa!**
 - Qualche teorema utile
 - Casi 2 e 5 in dettaglio

La classificazione è completa!

Il lavoro di questo seminario si basa sull'articolo *General Error Locator Polynomials for Binary Cyclic Codes with $t \leq 2$ e $n < 63$* di Emmauela Orsini e Massimiliano Sala; all'interno della categoria di codici presa in considerazione, si ritrovano alcuni (pochi) casi in cui la rappresentazione del polinomio locatore è implicita (in particolare, è implicita la rappresentazione di b).

Questi casi, che elenchiamo di seguito, sono stati studiati recentemente da Fabrizio Caruso e Massimiliano Sala e illustreremo di seguito una parte dei risultati di queste ricerche.

La classificazione è completa!

Il lavoro di questo seminario si basa sull'articolo *General Error Locator Polynomials for Binary Cyclic Codes with $t \leq 2$ e $n < 63$* di Emmauela Orsini e Massimiliano Sala; all'interno della categoria di codici presa in considerazione, si ritrovano alcuni (pochi) casi in cui la rappresentazione del polinomio locatore è implicita (in particolare, è implicita la rappresentazione di b).

Questi casi, che elenchiamo di seguito, sono stati studiati recentemente da Fabrizio Caruso e Massimiliano Sala e illustreremo di seguito una parte dei risultati di queste ricerche.

Parte terza

La classificazione è completa!

Casi rimanenti

CASI RIMANENTI

- 1 $n = 31, S_C = \{1, 15\};$
- 2 $n = 31, S_C = \{1, 5\};$
- 3 $n = 51, S_C = \{0, 1, 5\};$
- 4 $n = 51, S_C = \{1, 9\};$
- 5 $n = 45, S_C = \{1, 21\}.$

Parte terza

La classificazione è completa!

Casi rimanenti

CASI RIMANENTI

- 1 $n = 31, S_C = \{1, 15\};$
- 2 $n = 31, S_C = \{1, 5\};$
- 3 $n = 51, S_C = \{0, 1, 5\};$
- 4 $n = 51, S_C = \{1, 9\};$
- 5 $n = 45, S_C = \{1, 21\}.$

Parte terza

La classificazione è completa!

Casi rimanenti

CASI RIMANENTI

- 1 $n = 31, S_C = \{1, 15\};$
- 2 $n = 31, S_C = \{1, 5\};$
- 3 $n = 51, S_C = \{0, 1, 5\};$
- 4 $n = 51, S_C = \{1, 9\};$
- 5 $n = 45, S_C = \{1, 21\}.$

Parte terza

La classificazione è completa!

Casi rimanenti

CASI RIMANENTI

- 1 $n = 31, S_C = \{1, 15\};$
- 2 $n = 31, S_C = \{1, 5\};$
- 3 $n = 51, S_C = \{0, 1, 5\};$
- 4 $n = 51, S_C = \{1, 9\};$
- 5 $n = 45, S_C = \{1, 21\}.$

Casi rimanenti

CASI RIMANENTI

- 1 $n = 31, S_C = \{1, 15\};$
- 2 $n = 31, S_C = \{1, 5\};$
- 3 $n = 51, S_C = \{0, 1, 5\};$
- 4 $n = 51, S_C = \{1, 9\};$
- 5 $n = 45, S_C = \{1, 21\}.$

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - Conclusione
- 3 Parte terza
 - La classificazione è completa!
 - **Qualche teorema utile**
 - Casi 2 e 5 in dettaglio

Se $t = 2$...

Lemma

Per $t = 2$, tutte le potenze pari di sindromi non possono dare zero.

Dimostrazione

Assumiamo che per un dato intero pari s sia

$z_1^s + z_2^s = 0 \Rightarrow z_1^s = -z_2^s$. Dal momento che $z_1^n + z_2^n = 1$,

abbiamo che $z_1^{(n,s)} = z_2^{(n,s)} \Rightarrow z_1 = z_2$, che contraddice il fatto che $t = 2$.

Se $t = 2$...

Lemma

Per $t = 2$, tutte le potenze pari di sindromi non possono dare zero.

Dimostrazione

Assumiamo che per un dato intero pari s sia

$z_1^s + z_2^s = 0 \Rightarrow z_1^s = -z_2^s$. Dal momento che $z_1^n + z_2^n = 1$,

abbiamo che $z_1^{(n,s)} = -z_2^{(n,s)} \Rightarrow z_1 = -z_2$, che contraddice il fatto che $t = 2$.

Teorema da applicare ai casi 2 e 5

Teorema

Sia C un codice binario e ciclico con $\{l, s, s - l, s - 2l\} \subset S_C$, $t = 2$, $(s - 2l, n) = (l, n) = 1$. Siano x_1, x_2, x_3, x_4 le sindromi corrispondenti rispettivamente a $s, s - l, s - 2l, l$.

Allora:

$$b = b^* = \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{l^*},$$

dove l^ è l'inverso di l modulo n .*

Teorema da applicare ai casi 2 e 5

Teorema

Sia C un codice binario e ciclico con $\{l, s, s - l, s - 2l\} \subset S_C$, $t = 2$, $(s - 2l, n) = (l, n) = 1$. Siano x_1, x_2, x_3, x_4 le sindromi corrispondenti rispettivamente a $s, s - l, s - 2l, l$.

Allora:

$$b = b^* = \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{l^*},$$

dove l^ è l'inverso di l modulo n .*

Teorema da applicare ai casi 2 e 5

Teorema

Sia C un codice binario e ciclico con $\{l, s, s - l, s - 2l\} \subset S_C$, $t = 2$, $(s - 2l, n) = (l, n) = 1$. Siano x_1, x_2, x_3, x_4 le sindromi corrispondenti rispettivamente a $s, s - l, s - 2l, l$.

Allora:

$$b = b^* = \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{l^*},$$

dove l^ è l'inverso di l modulo n .*

Teorema da applicare ai casi 2 e 5

Dimostrazione

Consideriamo $x_2 x_4$:

$$\begin{aligned}
 x_2 x_4 &= (z_1^{s-l} + z_2^{s-l})(z_1^l + z_2^l) \\
 &= z_1^s + z_2^s + z_1^{s-l} z_2^l + z_1^l + z_2^{s-l} \\
 &= z_1^s + z_2^s + (z_1 z_2)^l (z_1^{s-2l} + z_2^{s-2l}) \\
 &= x_1 + (b^*)^l x_3.
 \end{aligned}$$

D'altronde abbiamo $(b^*)^l = (x_2 x_4 + x_1)/x_3$ e, per il fatto che $(l, n) = 1$ abbiamo $b^* = ((x_2 x_4 + x_1)/x_3)^{l^{-1}}$.

Per $t = 2$ abbiamo che $x_3 = z_1^{s-2l} + z_2^{s-2l}$ che non può dare zero perché $(s - 2l, n) = 1$. Abbiamo inoltre che $b^* = b$ perché per $t = 1$ abbiamo $x_1 x_3 + x_2 = z z^{s-1} + z^s = 0$.

Teorema da applicare ai casi 2 e 5

Dimostrazione

Consideriamo $x_2 x_4$:

$$\begin{aligned}
 x_2 x_4 &= (z_1^{s-l} + z_2^{s-l})(z_1^l + z_2^l) \\
 &= z_1^s + z_2^s + z_1^{s-l} z_2^l + z_1^l + z_2^{s-l} \\
 &= z_1^s + z_2^s + (z_1 z_2)^l (z_1^{s-2l} + z_2^{s-2l}) \\
 &= x_1 + (b^*)^l x_3.
 \end{aligned}$$

D'altronde abbiamo $(b^*)^l = (x_2 x_4 + x_1)/x_3$ e, per il fatto che $(l, n) = 1$ abbiamo $b^* = ((x_2 x_4 + x_1)/x_3)^{l^*}$.

Per $t = 2$ abbiamo che $x_3 = z_1^{s-2l} + z_2^{s-2l}$ che non può dare zero perché $(s - 2l, n) = 1$. Abbiamo inoltre che $b^* = b$ perché per $t = 1$ abbiamo $x_1 x_3 + x_2 = z z^{s-1} + z^s = 0$.

Teorema da applicare ai casi 2 e 5

Dimostrazione

Consideriamo x_2x_4 :

$$\begin{aligned}
 x_2x_4 &= (z_1^{s-l} + z_2^{s-l})(z_1^l + z_2^l) \\
 &= z_1^s + z_2^s + z_1^{s-l}z_2^l + z_1^l + z_2^{s-l} \\
 &= z_1^s + z_2^s + (z_1z_2)^l(z_1^{s-2l} + z_2^{s-2l}) \\
 &= x_1 + (b^*)^lx_3.
 \end{aligned}$$

D'altronde abbiamo $(b^*)^l = (x_2x_4 + x_1)/x_3$ e, per il fatto che $(l, n) = 1$ abbiamo $b^* = ((x_2x_4 + x_1)/x_3)^{l^*}$.

Per $t = 2$ abbiamo che $x_3 = z_1^{s-2l} + z_2^{s-2l}$ che non può dare zero perché $(s - 2l, n) = 1$. Abbiamo inoltre che $b^* = b$ perché per $t = 1$ abbiamo $x_1x_3 + x_2 = z_1z_2^{s-1} + z_2^s = 0$.

Teorema da applicare ai casi 2 e 5

Dimostrazione

Consideriamo x_2x_4 :

$$\begin{aligned}
 x_2x_4 &= (z_1^{s-l} + z_2^{s-l})(z_1^l + z_2^l) \\
 &= z_1^s + z_2^s + z_1^{s-l}z_2^l + z_1^l + z_2^{s-l} \\
 &= z_1^s + z_2^s + (z_1z_2)^l(z_1^{s-2l} + z_2^{s-2l}) \\
 &= x_1 + (b^*)^l x_3.
 \end{aligned}$$

D'altronde abbiamo $(b^*)^l = (x_2x_4 + x_1)/x_3$ e, per il fatto che $(l, n) = 1$ abbiamo $b^* = ((x_2x_4 + x_1)/x_3)^{l^*}$.

Per $t = 2$ abbiamo che $x_3 = z_1^{s-2l} + z_2^{s-2l}$ che non può dare zero perché $(s - 2l, n) = 1$. Abbiamo inoltre che $b^* = b$ perché per $t = 1$ abbiamo $x_1x_3 + x_2 = z z^{s-1} + z^s = 0$.

Teorema da applicare ai casi 2 e 5

Dimostrazione

Consideriamo $x_2 x_4$:

$$\begin{aligned}
 x_2 x_4 &= (z_1^{s-l} + z_2^{s-l})(z_1^l + z_2^l) \\
 &= z_1^s + z_2^s + z_1^{s-l} z_2^l + z_1^l + z_2^{s-l} \\
 &= z_1^s + z_2^s + (z_1 z_2)^l (z_1^{s-2l} + z_2^{s-2l}) \\
 &= x_1 + (b^*)^l x_3.
 \end{aligned}$$

D'altronde abbiamo $(b^*)^l = (x_2 x_4 + x_1)/x_3$ e, per il fatto che $(l, n) = 1$ abbiamo $b^* = ((x_2 x_4 + x_1)/x_3)^{l^*}$.

Per $t = 2$ abbiamo che $x_3 = z_1^{s-2l} + z_2^{s-2l}$ che non può dare zero perché $(s - 2l, n) = 1$. Abbiamo inoltre che $b^* = b$ perché per $t = 1$ abbiamo $x_1 x_3 + x_2 = z z^{s-1} + z^s = 0$.

Sommario

- 1 Parte prima
 - Conoscenze preliminari
 - Alcuni risultati di rilievo
 - Teoremi sulla struttura di alcuni codici
- 2 Parte seconda
 - Codici con $t \leq 1$ e $n < 63$
 - Caso generale per $t = 2$: $\{1, 2i + 1\} \subset S_C$, dove $i \geq 1$
 - Caso $t = 2$ e $S = \{1, n - 1, l\}$
 - Una nuova famiglia di codici
 - Conclusione
- 3 Parte terza
 - La classificazione è completa!
 - Qualche teorema utile
 - **Casi 2 e 5 in dettaglio**

Caso 2: $n = 31$ e $S_C = \{1, 5\}$

Quello che andiamo a considerare è un caso particolare del teorema appena visto. Effettivamente, C soddisfa le ipotesi del teorema per $l = 1$. Infatti, $S_C = \{1, 2, 4, 8, 16, 5, 10, 20, 9\}$ e dunque $s = 10$, $s - l = 9$, $s - 2l = 8$. Quindi abbiamo che il polinomio generale locatore d'errore per C è:

$$z^2 + x_1 z + \frac{x_1 x_3 + x_2}{x_4},$$

dove x_1, x_2, x_3, x_4 sono le sindromi associate rispettivamente a 10, 9, 8, 1.

Caso 2: $n = 31$ e $S_C = \{1, 5\}$

Quello che andiamo a considerare è un caso particolare del teorema appena visto. Effettivamente, C soddisfa le ipotesi del teorema per $l = 1$. Infatti, $S_C = \{1, 2, 4, 8, 16, 5, 10, 20, 9\}$ e dunque $s = 10$, $s - l = 9$, $s - 2l = 8$. Quindi abbiamo che il polinomio generale locatore d'errore per C è:

$$z^2 + x_1 z + \frac{x_1 x_3 + x_2}{x_4},$$

dove x_1, x_2, x_3, x_4 sono le sindromi associate rispettivamente a 10, 9, 8, 1.

Caso 2: $n = 31$ e $S_C = \{1, 5\}$

Quello che andiamo a considerare è un caso particolare del teorema appena visto. Effettivamente, C soddisfa le ipotesi del teorema per $l = 1$. Infatti, $S_C = \{1, 2, 4, 8, 16, 5, 10, 20, 9\}$ e dunque $s = 10$, $s - l = 9$, $s - 2l = 8$. Quindi abbiamo che il polinomio generale locatore d'errore per C è:

$$z^2 + x_1 z + \frac{x_1 x_3 + x_2}{x_4},$$

dove x_1, x_2, x_3, x_4 sono le sindromi associate rispettivamente a 10, 9, 8, 1.

Caso 2: $n = 31$ e $S_C = \{1, 5\}$

Quello che andiamo a considerare è un caso particolare del teorema appena visto. Effettivamente, C soddisfa le ipotesi del teorema per $l = 1$. Infatti, $S_C = \{1, 2, 4, 8, 16, 5, 10, 20, 9\}$ e dunque $s = 10$, $s - l = 9$, $s - 2l = 8$. Quindi abbiamo che il polinomio generale locatore d'errore per C è:

$$z^2 + x_1 z + \frac{x_1 x_3 + x_2}{x_4},$$

dove x_1, x_2, x_3, x_4 sono le sindromi associate rispettivamente a 10, 9, 8, 1.

Caso 2: $n = 31$ e $S_C = \{1, 5\}$

Quello che andiamo a considerare è un caso particolare del teorema appena visto. Effettivamente, C soddisfa le ipotesi del teorema per $l = 1$. Infatti, $S_C = \{1, 2, 4, 8, 16, 5, 10, 20, 9\}$ e dunque $s = 10$, $s - l = 9$, $s - 2l = 8$. Quindi abbiamo che il polinomio generale locatore d'errore per C è:

$$z^2 + x_1 z + \frac{x_1 x_3 + x_2}{x_4},$$

dove x_1, x_2, x_3, x_4 sono le sindromi associate rispettivamente a 10, 9, 8, 1.

Caso 5: $n = 45$ e $S_C = \{1, 21\}$

Anche questo è un caso particolare del teorema visto sopra.

Infatti,

$S_C = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23, 21, 42, 39, 33\}$ e,

se poniamo $l = 2$ possiamo avere $s = 23$, $s - l = 21$,

$s - 2l = 19$. Pertanto abbiamo che il polinomio generale

locatore per C è:

$$z^2 + x_5 z + \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{23},$$

dove x_1, x_2, x_3, x_4, x_5 sono le sindromi associate

rispettivamente a 23, 21, 19, 2, 1.

Questo è vero perché, applicando il teorema con i valori di l ed

s come scritto sopra abbiamo che $b^2 = \frac{x_1 x_3 + x_2}{x_4}$ e 23 è

l'inverso di 2 modulo 45.

Caso 5: $n = 45$ e $S_C = \{1, 21\}$

Anche questo è un caso particolare del teorema visto sopra. Infatti,

$S_C = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23, 21, 42, 39, 33\}$ e, se poniamo $l = 2$ possiamo avere $s = 23$, $s - l = 21$, $s - 2l = 19$. Pertanto abbiamo che il polinomio generale locatore per C è:

$$z^2 + x_5 z + \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{23},$$

dove x_1, x_2, x_3, x_4, x_5 sono le sindromi associate rispettivamente a 23, 21, 19, 2, 1.

Questo è vero perché, applicando il teorema con i valori di l ed s come scritto sopra abbiamo che $b^2 = \frac{x_1 x_3 + x_2}{x_4}$ e 23 è l'inverso di 2 modulo 45.

Caso 5: $n = 45$ e $S_C = \{1, 21\}$

Anche questo è un caso particolare del teorema visto sopra. Infatti,

$S_C = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23, 21, 42, 39, 33\}$ e, se poniamo $l = 2$ possiamo avere $s = 23$, $s - l = 21$, $s - 2l = 19$. Pertanto abbiamo che il polinomio generale locatore per C è:

$$z^2 + x_5 z + \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{23},$$

dove x_1, x_2, x_3, x_4, x_5 sono le sindromi associate rispettivamente a 23, 21, 19, 2, 1.

Questo è vero perché, applicando il teorema con i valori di l ed s come scritto sopra abbiamo che $b^2 = \frac{x_1 x_3 + x_2}{x_4}$ e 23 è l'inverso di 2 modulo 45.

Caso 5: $n = 45$ e $S_C = \{1, 21\}$

Anche questo è un caso particolare del teorema visto sopra. Infatti,

$S_C = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23, 21, 42, 39, 33\}$ e, se poniamo $l = 2$ possiamo avere $s = 23$, $s - l = 21$, $s - 2l = 19$. Pertanto abbiamo che il polinomio generale locatore per C è:

$$z^2 + x_5 z + \left(\frac{x_1 x_3 + x_2}{x_4} \right)^{23},$$

dove x_1, x_2, x_3, x_4, x_5 sono le sindromi associate rispettivamente a 23, 21, 19, 2, 1.

Questo è vero perché, applicando il teorema con i valori di l ed s come scritto sopra abbiamo che $b^2 = \frac{x_1 x_3 + x_2}{x_4}$ e 23 è l'inverso di 2 modulo 45.