SUI CODICI UNIDIREZIONALI

Luca TALLINI

Oltre ad una breve descrizione della problematica sui codici Unidirezionali è quì data la dimostrazione di una congettura di S. Al-Bassan e B. Bose che interviene nella teoria dei suddetti autori, sulla costruzione di codici ottimali nella classe dei codici bilanciati che si ottengono con il metodo della complementazione di Knuth.

1 INTRODUZIONE.

Durante la trasmissione dei dati su un canale è inevitabile che avvengano degli errori. Nel caso binario si possono classificare tre tipi di errori:

1. **errori simmetrici**: il tipo di errore è detto simmetrico quando durante la trasmissione si possono avere sia errori $0 \rightarrow 1$ che errori $1 \rightarrow 0$. I canali caratterizzati da questo tipo di errori sono i Canali Binari Simmetrici (BSC).

2. **errori asimmetrici**: il tipo di errore è detto asimmetrico quando durante la trasmissione si possono avere solo errori $1(0) \rightarrow 0(1)$ e mai errori $0(1) \rightarrow 1(0)$. I canali caratterizzati da questo tipo di errori sono i Canali Asimmetrici ($ZC(\overline{Z}C)$).

3. **errori unidirezionali**: il tipo di errore è detto unidirezionale quando durante la trasmissione si possono avere sia errori $0 \rightarrow 1$

che errori $1 \rightarrow 0$, ma mai simultaneamente nella stessa parola di dati. I canali caratterizzati da questo tipo di errori sono i Canali Unidirezionali (UC).

Mentre sono ben noti alla letteratura esempi di BSC, esempi di canali fisici che obbediscono propriamente al modello di errore asimmetrico e/o unidirezionale sono: le Fibre Ottiche, i Dischi ottici, le PROMs (Programmable Read Only Memories), le Semiconductor memories, i circuiti e le memorie VLSI dei computers.

Il problema è quello di ottenere una trasmissione affidabile di dati sui canali su menzionati, codificando l'informazione con codici efficienti che correggano o almeno riconoscano errori, ovvero garantiscano la correttezza del dato ricevuto.

Piú precisamente ci si propone di risolvere i seguenti due tipi di problemi:

1. **Riconoscimento degli errori (Error Detection)**: questo problema si propone di stabilire se, nella parola di dati ricevuta sono stati commessi o meno errori.

2. **Correzione degli errori (Error Correction)**: questo problema si propone di correggere gli eventuali errori della parola di dati ricevuta.

I codici efficienti che offrono i servizi di correzione e riconoscimento di errori sui canali Asimmetrici e/o Unidirezionali sono detti codici Unidirezionali.

In seguito parleremo di codici binari a lunghezza fissa.

Nell'ambito dei codici riconoscitori di errori su UC e/o ZC, fino ad oggi, sono state studiate le seguenti quatro classi di codici:

1. **AUED** (All Unidirectional Error Detecting): è l'insieme dei codici che incondizionatamente riconoscono se la parola di dati in output al canale è affetta da errori unidirezionali o meno.

2. **t-UED** (t-Unidirectional Error Detecting): è l'insieme dei codici che riconoscono se la parola di dati in output al canale è affetta da errori unidirezionali, sotto l'ipotesi che il numero di bit errati è minore od uguale a t [4].

3. **b-BUED** (b-Burst Unidirectional Error Detecting): è l'insieme dei codici che riconoscono se nella parola di dati in output al canale è avvenuto un burst di errori unidirezionali di lunghezza minore od uguale a b, *sotto l'ipotesi che sia avvenuto un burst di errori* unidirezionali di lunghezza minore od uguale a b (Data una parola di dati in output X, si dice che è avvenuto un burst di errori di lunghezza b, se i bit erronei di X sono confinati in b bit consecutivi dei quali il primo e l'ultimo sono in errore) [2].

4. **t-UBED** (t-Unidirectional Byte Error Detecting): Si dice che sono avvenuti degli errori unidirezionali di byte in una parola di m byte di b bit se sono avvenuti degli errori unidirezionali in alcuni byte della parola. t-UBED è l'insieme dei codici che riconoscono se nella parola di dati in output al canale sono avvenuti degli errori unidirezionali di byte, sotto l'ipotesi che il numero di byte errati è minore od uguale a t [5].

2 METODO DI KNUTH PER I CODICI BILANCIATI.

Diamo la seguente:

Definizione 2.1 *Un codice $\mathcal{C}$ si dice bilanciato se ogni parola di $\mathcal{C}$ ha lunghezza n e peso $\left\lceil \frac{n}{2} \right\rceil \left(\left\lfloor \frac{n}{2} \right\rfloor \right)$. $\mathcal{C}$ si dice bilanciato con k bit di informazione e r bit di controllo se:*

1. $|\mathcal{C}| = 2^k$,
2. *Ogni parola di $\mathcal{C}$ ha lunghezza $k+r$ e peso $\left\lceil \frac{k+r}{2} \right\rceil \left(\left\lfloor \frac{k+r}{2} \right\rfloor \right)$.*

I codici bilanciati sono particolari codici AUED. Infatti, se una parola di codice è affetta da errori unidirezionali, il peso necessariamente deve cambiare, di modo che, se il codice è bilanciato, il decodificatore, contando il numero degli 1 della parola ricevuta, riesce a stabilire se sono stati commessi errori o meno.

Per quanto segue abbiamo bisogno delle seguenti notazioni:

1. $\mathcal{I} \stackrel{\text{def}}{=} \mathbb{Z}_2^k$ è l'insieme delle parole di informazione.
2. $\mathcal{A} \stackrel{\text{def}}{=} \mathbb{Z}_2^r$ è l'insieme delle parole di controllo.
3. Data $X \in \mathbb{Z}_2^k$, $w(X)$ è il peso di X.
4. Data $X \in \mathcal{I}$, $X^{(i)}$ è la parola X complementata dei primi i bit.

Se $X \in \mathcal{I}$, l'insieme:

$$\{(0, w(X^{(0)})), (1, w(X^{(1)})), (2, w(X^{(2)})), \ldots, (k, w(X^{(k)}))\},$$

descrive una passeggiata aleatoria da $w(X)$ a $k - w(X)$. Poiche:

$$\forall X \in \mathcal{I} \quad \left\lceil \frac{k}{2} \right\rceil \left(\left\lfloor \frac{k}{2} \right\rfloor \right) \in [w(X), k - w(X)],$$

per ogni X esiste sicuramente un indice i tale che:

$$w(X^{(i)}) = \left\lceil \frac{k}{2} \right\rceil \left(\left\lfloor \frac{k}{2} \right\rfloor \right).$$

A partire da questa osservazione è possibile codificare la generica parola $X \in \mathcal{I}$ al seguente modo. Sia $i \in [0, k]$ il piú piccolo indice per cui $w(X^{(i)}) = \left\lfloor \frac{k}{2} \right\rfloor$, codificando i con una parola di controllo Y bilanciata, ovvero tale che $w(Y) = \left\lceil \frac{r}{2} \right\rceil$, possiamo far corrispondere a X la parola bilanciata $YX^{(i)}$.

Il codice appena proposto è un semplice esempio, certamente non ottimale, di come applicare il metodo di Knuth [6]. In generale si dovrà colmare lo sbilanciamento di $X^{(i)}$ con un opportuno sbilanciamento del check Y.

3 TEORIA DI AL-BASSAN E BOSE.

Nel 1989 Al-Bassam e Bose in [1] hanno costruito una teoria generale per lo schema su proposto, proggettando un codice bilanciato ottimale, nella classe di tutti i codici bilanciati che si ottengono con il metodo della complementazione di Knuth e hanno decodifica sequenziale (la decodifica si dice parallela se basta un solo confronto del check Y per decodificare, altrimenti si dice sequenziale). Cominciamo ad esporre la teoria generale su detta.

Sia $\mathcal{S}_i$ l'insieme di tutte le stringhe binarie di lunghezza k e peso i. Dati $Y \in \mathcal{A}$, $w_1, w_2, \ldots, w_q, v \in \{0, \ldots, k\}$, con la notazione:

$$Y :: \mathcal{S}_{w_1} \cup \mathcal{S}_{w_2} \cup \ldots \cup \mathcal{S}_{w_q} \longrightarrow \mathcal{S}_v, \tag{3.1}$$

intenderemo che ogni parola di peso $w_1, w_2 \ldots$, o w_q (ovvero ogni parola in $\mathcal{S}_{w_1} \cup \mathcal{S}_{w_2} \cup \ldots \cup \mathcal{S}_{w_q}$), è codificata, complementando un bit alla volta, fino a che il peso sia v, e quindi appendendo, ad essa, la parola di controllo Y. Il codice che così si ottiene è bilanciato se $v = \left\lceil \frac{k+r}{2} \right\rceil - w(Y)$, per ogni parola di controllo $Y \in \mathcal{A}$. Il decodificatore, leggendo Y, il quale codifica $w_1, w_2 \ldots, w_q$, complementa il resto della parola di codice un bit alla volta, fino a che è ottenuto uno dei pesi $w_1, w_2 \ldots, w_q$. Ovviamente la mappa (3.1) deve essere ben definita e iniettiva affinché lo schema sia corretto.

D'ora in poi, in (3.1), supporremo, senza perdita di generalità, che $w_1 < w_2 < \ldots < w_q$.

Se $q = 1$, chiameremo la funzione (3.1), mappa singola, se $q = 2$, mappa doppia, e così via. Il seguente Teorema da delle condizioni necessarie e sufficienti perche una mappa singola sia ben definita e iniettiva.

Teorema 3.1 *La mappa singola* $Y :: \mathcal{S}_a \longrightarrow \mathcal{S}_v$ *è ben definita e iniettiva se, e solo se* $\min\{a, k-a\} \leq v \leq \max\{a, k-a\}$.

Per riferirci ad una mappa doppia, scriveremo:

$$Y :: \mathcal{S}_a \cup \mathcal{S}_b \longrightarrow \mathcal{S}_v,$$

essendo $b > a$. Si ha il seguente:

Teorema 3.2 *La mappa doppia* $Y :: \mathcal{S}_a \cup \mathcal{S}_b \longrightarrow \mathcal{S}_v$ *(dove* $b > a$*) è ben definita e iniettiva se, e solo se:*

$$b - a \geq \max\{v, k-v\}.$$

Per quanto riguarda le mappe triple, quadruple, ecc., notiamo che dal Teorema appena enunciato segue che se una mappa (3.1), per $q \geq 3$, è ben

definita e iniettiva allora

$$\forall i, j \in [1, q] \qquad |w_i - w_j| > \max\{v, k - v\} \geq \left\lceil \frac{k}{2} \right\rceil,$$

che, dovendo risultare $0 \leq w_i \leq k$, è impossibile.

Il problema è quindi ricondotto a trovare la miglior combinazione di mappe singole soddisfacenti il Teorema 3.1 e di mappe doppie soddisfacenti il Teorema 3.2.

Ci sono 2^r mappe corrispondenti alle 2^r parole di controllo disponibili. Se d parole di controllo sono usate per le mappe singole e $2^r - d$ per le mappe doppie, il numero di pesi differenti che possiamo riconoscere negli algoritmi di codifica e decodifica è $2(2^r - d) + d = 2^{r+1} - d$. Siccome dobbiamo riconoscere $k + 1$ pesi differenti, si deve avere:

$$k + 1 = 2^{r+1} - d \iff k = 2^{r+1} - d - 1.$$

È quindi chiaro che per massimizzare k dobbiamo minimizzare il numero delle mappe singole d. Nella costruzione di Bose, data in [3] d era uguale a $r + 1$, per cui in seguito supporremo $d \leq r + 1$.

Cerchiamo di caratterizzare qual'è la scelta ottimale per la combinazione di mappe. Diamo il seguente:

Teorema 3.3 *Dato $d \leq r + 1$, se esiste una combinazione di mappe:*

$$\begin{aligned}
&Y_1 :: S_{a_1} \longrightarrow S_{v_1}, \\
&Y_2 :: S_{a_2} \longrightarrow S_{v_2}, \\
&\vdots \\
&Y_d :: S_{a_d} \longrightarrow S_{v_d}, \\
&Y_{d+1} :: S_{a_{d+1}} \cup S_{b_{d+1}} \longrightarrow S_{v_{d+1}}, \\
&Y_{d+2} :: S_{a_{d+2}} \cup S_{b_{d+2}} \longrightarrow S_{v_{d+2}}, \\
&\vdots \\
&Y_{2^r} :: S_{a_{2^r}} \cup S_{b_{2^r}} \longrightarrow S_{v_{2^r}},
\end{aligned} \tag{3.2}$$

con $b_i > a_i$, per $i = d+1, \ldots, 2^r$, tale che:

$$\begin{gathered} \min\{a_i, k-a_i\} \leq v_i \leq \max\{a_i, k-a_i\} \quad \forall i \in [1,d], \\ b_i - a_i > \max\{v_i, k-v_i\} \quad \forall i \in [d+1, 2^r], \\ \{a_1 \ldots, a_{2^r}, b_{d+1}, \ldots, b_{2^r}\} = \{0, \ldots, k\}, \\ w(Y_i) = \left\lceil \tfrac{k+r}{2} \right\rceil - v_i \quad \forall i \in [1, 2^r], \end{gathered} \tag{3.3}$$

allora esiste anche una combinazione di mappe per cui valgono le (3.3) e:

$$\begin{cases} a_i \geq \left\lceil \frac{k}{2} \right\rceil \Longrightarrow v_i \geq \left\lceil \frac{k}{2} \right\rceil \\ a_i \leq \left\lfloor \frac{k}{2} \right\rfloor \Longrightarrow v_i \leq \left\lfloor \frac{k}{2} \right\rfloor \end{cases} \quad \forall i \in [1,d], \tag{3.4}$$

oppure:

$$\begin{cases} \begin{cases} a_i \geq \left\lceil \frac{k}{2} \right\rceil \Longrightarrow v_i \geq \left\lceil \frac{k}{2} \right\rceil \\ a_i \leq \left\lfloor \frac{k}{2} \right\rfloor \Longrightarrow v_i \leq \left\lfloor \frac{k}{2} \right\rfloor \end{cases} & \text{se } a_i \neq \left\lceil \frac{k+r}{2} \right\rceil + 1, \\ v_i = \left\lceil \frac{k-r}{2} \right\rceil & \text{se } a_i = \left\lceil \frac{k+r}{2} \right\rceil + 1. \end{cases} \tag{3.5}$$

Dimostrazione: Posto:

$$\begin{cases} v' \stackrel{\text{def}}{=} \left\lceil \frac{k-r}{2} \right\rceil \\ v'' \stackrel{\text{def}}{=} \left\lceil \frac{k+r}{2} \right\rceil \end{cases},$$

notiamo che, poiché:

$$\forall v, w \in [0,k] \quad \left| \left\lfloor \frac{k}{2} \right\rfloor - w \right| \leq \left\lceil \frac{k}{2} \right\rceil \leq \max\{v, k-v\},$$

e:

$$\forall v, w \in [0,k] \quad \left| \left\lceil \frac{k}{2} \right\rceil - w \right| \leq \left\lceil \frac{k}{2} \right\rceil \leq \max\{v, k-v\},$$

nella combinazione (3.2), dovendo valere le (3.3), si ha:

$$\left\lfloor \frac{k}{2} \right\rfloor, \left\lceil \frac{k}{2} \right\rceil \in \{a_1, \ldots, a_d\}.$$

Poiché:

$$|\{w \in \{a_i, b_i\}_{1=d+1,\ldots,2^r} : w < \left\lfloor \frac{k}{2} \right\rfloor\}| =$$

$$|\{w \in \{a_i, b_i\}_{1=d+1,\ldots,2^r} : w > \left\lceil \frac{k}{2} \right\rceil\}| = 2^r - d,$$

si ha:

$$|\{a \in \{a_i\}_{1=1,\ldots,d} : a < \left\lfloor \frac{k}{2} \right\rfloor\}| = |\{a \in \{a_i\}_{1=1,\ldots,d} : a > \left\lceil \frac{k}{2} \right\rceil\}| = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Notiamo inoltre che, se è possibile la mappa singola:

$$Y :: S_a \longrightarrow S_v,$$

poiché vale la prima relazione delle (3.3), si ha:

$$\begin{aligned} &\min\{a, k-a\} = \min\{k-a, a\} \leq \min\{v, k-v\} \leq \\ &\max\{v, k-v\} \leq \max\{k-a, a\} = \max\{a, k-a\}, \end{aligned} \tag{3.6}$$

e allora sono possibili anche le mappe:

$$\begin{aligned} &Y' :: S_a \longrightarrow S_{k-v}, \\ &Y'' :: S_{k-a} \longrightarrow S_v, \\ &Y''' :: S_{k-a} \longrightarrow S_{k-v}, \end{aligned}$$

se invece è possibile la mappa doppia:

$$Y :: S_a \cup S_b \longrightarrow S_v,$$

poiché vale la seconda relazione delle (3.3), si ha:

$$(k-a) - (k-b) = b - a > \max\{v, k-v\} = \max\{k-v, v\}, \tag{3.7}$$

e allora sono possibili anche le mappe:

$$\begin{aligned} &Y' :: S_a \cup S_b \longrightarrow S_{k-v}, \\ &Y'' :: S_{k-b} \cup S_{k-a} \longrightarrow S_v, \\ &Y''' :: S_{k-b} \cup S_{k-a} \longrightarrow S_{k-v}. \end{aligned}$$

Effettuiamo degli scambi, nelle mappe (3.2), tra elementi dell'insieme $\{S_{a_1}, \ldots, S_{a_{2^r}}, S_{b_{d+1}}, \ldots, S_{2^r}\}$, al modo che segue. Per $i \in [1,d]$, se $Y_i :: S_{a_i} \longrightarrow S_{v_i}$ è tale che $a_i \geq \left\lceil \frac{k}{2} \right\rceil$ distinguiamo i seguenti casi:

1. $v_i \in \left[\left\lceil \frac{k}{2} \right\rceil, v'' \right]$: Non effettuiamo nessuno scambio.

2. $v_i \in \left[v', \left\lfloor \frac{k}{2} \right\rfloor \right]$ ed esiste una mappa singola $Y_j :: S_{a_j} \longrightarrow S_{v_j} = S_{k-v_i}$ con $a_j \leq \left\lfloor \frac{k}{2} \right\rfloor$: In questo caso poniamo:

$$Y_i :: S_{a_j} \longrightarrow S_{v_i} \text{ e } Y_j :: S_{a_i} \longrightarrow S_{v_j}.$$

   Per la (3.6) è possibile fare ciò.

3. $v_i \in \left[v', \left\lfloor \frac{k}{2} \right\rfloor \right]$ e non esiste nessuna mappa come in 2.: Si distinguono i seguenti sottocasi:

   (a) $v_i \neq v'$: In questo caso, poiché $d \leq r+1$, esiste sicuramente una mappa doppia $Y_j :: S_{a_j} \cup S_{b_j} \longrightarrow S_{v_j} = S_{k-v_i}$. Allora poniamo:

$$Y_i :: S_{a_j} \cup S_{b_j} \longrightarrow S_{v_i} \text{ e } Y_j :: S_{a_i} \longrightarrow S_{v_j}.$$

   Per le (3.6) e (3.7) è possibile fare ciò.

   (b) $v_i = v'$: In questo caso, se è possibile rifarsi ai casi precedenti, allora è possibile far si che:

$$a_i \geq \left\lceil \frac{k}{2} \right\rceil \Longrightarrow v_i \geq \left\lceil \frac{k}{2} \right\rceil \text{ con } i \in [1,d].$$

   Se invece l'unica mappa $Y_j :: S_{a_j} \longrightarrow S_{v_j}$ con $v_j = k - v_i = v''$ è tale che $a_j \geq \left\lceil \frac{k}{2} \right\rceil$, allora è possibile solo fare in modo che:

$$\begin{cases} a_i \geq \left\lceil \frac{k}{2} \right\rceil \Longrightarrow v_i \geq \left\lceil \frac{k}{2} \right\rceil & \text{se } a_i \neq v'' + 1 \\ v_i = v' & \text{se } a_i = v'' + 1 \end{cases} \quad \text{con } i \in [1,d].$$

Se $a_i \leq \left\lceil \frac{k}{2} \right\rceil$ con ragionamenti analoghi si perviene ad analoghi risultati. Per avere il Teorema basta notare che se esiste una combinazione di mappe del tipo (3.2) per cui valgono le (3.3), poiché $\binom{r}{i} = \binom{r}{r-i}$ e valgono le (3.6) e (3.7), esiste anche la combinazione di mappe simmetrica, cioè quella che si ottiene scambiando tutti i pesi da w a $k - w$. ∎

Posto, $\forall v \in [v', v'']$:

$$h_v \stackrel{\text{def}}{=} \max\{v, k - v\} - (2^r - 1),$$

$$\bar{x}_v \stackrel{\text{def}}{=} \begin{cases} 0 & \text{se } v \notin [2^r - d, 2^r - 1] \\ 1 & \text{se } v \in [2^r - d, 2^r - 1], \end{cases} \tag{3.8}$$

e:

$$g_v = \binom{r}{v'' - v},$$

sia:

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} \stackrel{\text{def}}{=} \sum_{v=v'}^{v''} (g_v - \bar{x}_v) h_v.$$

Si ha il seguente:

Teorema 3.4 *Dato $d \leq r + 1$, per ogni combinazione di mappe (3.2) per cui valgono le (3.3), e la (3.4) o la (3.5) si ha:*

$$\sum_{i=d+1}^{2^r} [\max\{v_i, k - v_i\} + 1 - (b_i - a_i)] \geq (\mathbf{g} - \bar{\mathbf{x}})\mathbf{h}, \tag{3.9}$$

e l'uguale vale se, e solo se:

$$a_i = v_i \in [v', v''] \quad \forall i \in [i, d]. \tag{3.10}$$

Dimostrazione: Notiamo che per ogni $\mathbf{x} = (x_{v'}, \ldots, x_{v''}) \in \mathbb{N}^{r+1}$, tale che $\sum_{v=v'}^{v''} x_v = d$, si ha:

$$(\mathbf{g} - \mathbf{x})\mathbf{h} = \sum_{v=v'}^{v''} (g_v - x_v) h_v = \sum_{v=v'}^{v''} (g_v - x_v)(\max\{v, k - v\} + 1 - 2^r) =$$

$$\sum_{v=v'}^{v''}(g_v - x_v)(\max\{v, k-v\}+1) - 2^r \sum_{v=v'}^{v''}(g_v - x_v) =$$

$$\sum_{v=v'}^{v''}(g_v - x_v)(\max\{v, k-v\}+1) - 2^r(2^r - d),$$

ovvero:

$$(\mathbf{g} - \mathbf{x})\mathbf{h} = \sum_{v=v'}^{v''}(g_v - x_v)(\max\{v, k-v\}+1) - 2^r(2^r - d). \qquad (3.11)$$

Si ha:

$$\sum_{i=d+1}^{2^r} b_i + \sum_{a_i \geq \lceil \frac{k}{2} \rceil : i \in [1,d]} a_i = \sum_{v=\lceil \frac{k}{2} \rceil}^{k} v = \sum_{v=2^r}^{k} v + \sum_{v=\lceil \frac{k}{2} \rceil}^{2^r-1} v,$$

e:

$$\sum_{i=d+1}^{2^r} a_i + \sum_{a_i \leq \lceil \frac{k}{2} \rceil - 1 : i \in [1,d]} a_i = \sum_{v=0}^{\lceil \frac{k}{2} \rceil - 1} v = \sum_{v=0}^{2^r-d-1} v + \sum_{v=2^r-d}^{\lceil \frac{k}{2} \rceil - 1} v,$$

da cui rispettivamente segue che:

$$\sum_{i=d+1}^{2^r} b_i = \sum_{v=2^r}^{k} v - \Big(\sum_{a_i \geq \lceil \frac{k}{2} \rceil : i \in [1,d]} a_i - \sum_{v=\lceil \frac{k}{2} \rceil}^{2^r-1} v \Big) = \sum_{v=2^r}^{k} v - \Delta_b \qquad (3.12)$$

e:

$$\sum_{i=d+1}^{2^r} a_i = \sum_{v=0}^{2^r-d-1} v + \Big(\sum_{v=2^r-d}^{\lceil \frac{k}{2} \rceil - 1} v - \sum_{a_i \leq \lceil \frac{k}{2} \rceil - 1 : i \in [1,d]} a_i \Big) = \sum_{v=0}^{2^r-d-1} v + \Delta_a, \qquad (3.13)$$

dove:

$$\Delta_b \stackrel{\text{def}}{=} \sum_{a_i \geq \lceil \frac{k}{2} \rceil : i \in [1,d]} a_i - \sum_{v=\lceil \frac{k}{2} \rceil}^{2^r-1} v \geq 0$$

e:

$$\Delta_a \stackrel{\text{def}}{=} \sum_{v=2^r-d}^{\lceil \frac{k}{2} \rceil - 1} v - \sum_{a_i \leq \lceil \frac{k}{2} \rceil - 1 : i \in [1,d]} a_i \geq 0.$$

Dalle (3.12) e (3.13), segue che:

$$\sum_{i=d+1}^{2^r} b_i - a_i = \sum_{v=2^r}^{k} v - \sum_{v=0}^{2^r-d-1} v - \Delta_b - \Delta_a = 2^r(2^r-d) - \Delta_b - \Delta_a. \quad (3.14)$$

Posto:

$$x_v \stackrel{\text{def}}{=} \begin{cases} 0 & \text{se } v \notin \{v_i\}_{i\in[1,d]} \\ 1 & \text{se } v \in \{v_i\}_{i\in[1,d]}, \end{cases} \quad (3.15)$$

si ha:

$$\sum_{i=d+1}^{2^r} [\max\{v_i, k-v_i\} + 1 - (b_i - a_i)] =$$

$$\sum_{i=d+1}^{2^r} (\max\{v_i, k-v_i\} + 1) - \sum_{i=d+1}^{2^r} (b_i - a_i) =$$

$$\sum_{v=v'}^{v''} (g_v - x_v)(\max\{v, k-v\} + 1) - \sum_{i=d+1}^{2^r} (b_i - a_i) \stackrel{(3.11)}{=}$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} - \sum_{v=v'}^{v''} (g_v - \bar{x}_v)(\max\{v, k-v\} + 1) + 2^r(2^r - d) +$$

$$\sum_{v=v'}^{v''} (g_v - x_v)(\max\{v, k-v\} + 1) - \sum_{i=d+1}^{2^r} (b_i - a_i) \stackrel{(3.14)}{=}$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} + \sum_{v=v'}^{v''} (g_v - x_v - g_v + \bar{x}_v)(\max\{v, k-v\} + 1) + \Delta_b + \Delta_a =$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} + \sum_{v=v'}^{v''} (\bar{x}_v - x_v) \max\{v, k-v\} + \not{g} - \not{g} + \Delta_b + \Delta_a =$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} + \sum_{v=v'}^{\lceil \frac{k}{2} \rceil - 1} (\bar{x}_v - x_v)(k-v) + \sum_{v=\lceil \frac{k}{2} \rceil}^{v''} (\bar{x}_v - x_v)v + \Delta_b + \Delta_a =$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} + \sum_{v=v'}^{\lceil \frac{k}{2} \rceil - 1} \bar{x}_v(k-v) - \sum_{v=v'}^{\lceil \frac{k}{2} \rceil - 1} x_v(k-v) + \sum_{v=\lceil \frac{k}{2} \rceil}^{v''} \bar{x}_v v - \sum_{v=\lceil \frac{k}{2} \rceil}^{v''} x_v v + \Delta_b + \Delta_a =$$

$$(\mathbf{g}-\bar{\mathbf{x}})\mathbf{h}+\left\{\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}\bar{x}_v k-\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}x_v k\right\}+\left\{\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}x_v v-\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}\bar{x}_v v\right\}+$$

$$\left\{\sum_{v=\lceil\frac{k}{2}\rceil}^{v''}\bar{x}_v v-\sum_{v=\lceil\frac{k}{2}\rceil}^{v''}x_v v\right\}+\Delta_b+\Delta_a \overset{(3.8),(3.15)}{=}$$

$$(\mathbf{g}-\bar{\mathbf{x}})\mathbf{h}+\left\{\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}\bar{x}_v k-\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}x_v k\right\}+\left\{\sum_{v_i\le\lceil\frac{k}{2}\rceil-1:i\in[1,d]}v_i-\sum_{v=2^r-d}^{\lceil\frac{k}{2}\rceil-1}v\right\}+$$

$$\left\{\sum_{v=\lceil\frac{k}{2}\rceil}^{2^r-1}v-\sum_{v_i\ge\lceil\frac{k}{2}\rceil:i\in[1,d]}v_i\right\}+\Delta_b+\Delta_a=$$

$$(\mathbf{g}-\bar{\mathbf{x}})\mathbf{h}+\left\{\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}\bar{x}_v k-\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}x_v k\right\}+\left\{\sum_{a_i\le\lceil\frac{k}{2}\rceil-1:i\in[1,d]}a_i-\sum_{v=2^r-d}^{\lceil\frac{k}{2}\rceil-1}v\right\}+$$

$$\left\{\sum_{v_i\le\lceil\frac{k}{2}\rceil-1:i\in[1,d]}v_i-\sum_{a_i\le\lceil\frac{k}{2}\rceil-1:i\in[1,d]}a_i\right\}+\left\{\sum_{v=\lceil\frac{k}{2}\rceil}^{2^r-1}v-\sum_{a_i\ge\lceil\frac{k}{2}\rceil:i\in[1,d]}a_i\right\}+$$

$$\left\{\sum_{a_i\ge\lceil\frac{k}{2}\rceil:i\in[1,d]}a_i-\sum_{v_i\ge\lceil\frac{k}{2}\rceil:i\in[1,d]}v_i\right\}++\Delta_b+\Delta_a.$$

Se vale la (3.4), poiché:

$$\left\{\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}\bar{x}_v k-\sum_{v=v'}^{\lceil\frac{k}{2}\rceil-1}x_v k\right\}=0,$$

$$p_a \overset{\text{def}}{=} \left\{\sum_{v_i\le\lceil\frac{k}{2}\rceil-1:i\in[1,d]}v_i-\sum_{a_i\le\lceil\frac{k}{2}\rceil-1:i\in[1,d]}a_i\right\}\ge 0,$$

e:

$$p_b \overset{\text{def}}{=} \left\{\sum_{a_i\ge\lceil\frac{k}{2}\rceil:i\in[1,d]}a_i-\sum_{v_i\ge\lceil\frac{k}{2}\rceil:i\in[1,d]}v_i\right\}\ge 0,$$

si ha:

$$\sum_{i=d+1}^{2^r} [\max\{v_i, k - v_i\} + 1 - (b_i - a_i)] =$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} - \not\Delta_a + p_a - \not\Delta_b + p_b + \not\Delta_b + \not\Delta_a \geq (\mathbf{g} - \bar{\mathbf{x}})\mathbf{h},$$

e il segno di uguaglianza vale se, e solo se:

$$p_a, p_b = 0 \iff (3.10).$$

Se vale la (3.5), poiché:

$$\left\{ \sum_{v=v'}^{\lceil \frac{k}{2} \rceil - 1} \bar{x}_v k - \sum_{v=v'}^{\lceil \frac{k}{2} \rceil - 1} x_v k \right\} = -k,$$

$$p'_a \stackrel{\text{def}}{=} \left\{ \left[\sum_{v_i \leq \lceil \frac{k}{2} \rceil - 1 : i \in [1,d]} v_i - v' \right] - \sum_{a_i \leq \lceil \frac{k}{2} \rceil - 1 : i \in [1,d]} a_i \right\} \geq 0,$$

e:

$$p'_b \stackrel{\text{def}}{=} \left\{ \left[\sum_{a_i \geq \lceil \frac{k}{2} \rceil : i \in [1,d]} a_i - (v'' + 1) \right] - \sum_{v_i \geq \lceil \frac{k}{2} \rceil : i \in [1,d]} v_i \right\} \geq 0,$$

si ha:

$$\sum_{i=d+1}^{2^r} [\max\{v_i, k - v_i\} + 1 - (b_i - a_i)] =$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} - k - \not\Delta_a + p'_a + v' - \not\Delta_b + p'_b + v'' + 1 + \not\Delta_b + \not\Delta_a =$$

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} + (v' + v'' + 1 - k) + p'_a + p'_b > (\mathbf{g} - \bar{\mathbf{x}})\mathbf{h}.$$

Onde l'asserto. ∎

Diamo ancora il seguente:

Teorema 3.5 *Dato $d \leq r+1$, condizione necessaria e sufficiente affinché esista una combinazione di mappe (3.2) per cui valgono le (3.3) e risulti:*

$$Y_i :: \mathcal{S}_{v_i} \longrightarrow \mathcal{S}_{v_i} \quad \forall i \in [1, d], \tag{3.16}$$

con i v_i scelti in mezzo all'intervallo $[0,k]$, ovvero tali che:

$$v_i \in [2^r - d, 2^r - 1] \iff v_i \stackrel{\text{def}}{=} 2^r - d - 1 + i \quad \forall i \in [1,d], \qquad (3.17)$$

è che sia:

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} \leq 0.$$

Dimostrazione: Se le (3.2) sono una combinazone di mappe per cui valgono le (3.3), la (3.16) e la (3.17), allora, per il Teorema precedente e le (3.3), si ha:

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} = \sum_{i=d+1}^{2^r} [\max\{v_i, k - v_i\} + 1 - (b_i - a_i)] \leq 0.$$

Per quanto riguarda la restante parte della dimostrazione, notiamo che se disponessimo di tutti check Y_i tali che $v_i = \left\lceil \frac{k+r}{2} \right\rceil - w(Y_i) \leq 2^r - 1$ allora definire le mappe doppie sarebbe semplice, in quanto per ogni $i = d+1, \ldots, 2^r$ si potrebbe porre $Y_i :: \mathcal{S}_{i-(d+1)} \cup \mathcal{S}_{i-(d+1)+2^r} \longrightarrow \mathcal{S}_{v_i}$. Ma così non è. $\forall t \in [1, -\min_{v \in [v',v'']} h_v]$, è però possibile associare a t mappe di check Y_i tali che $h_{v_i} > 0$, h_{v_i} mappe di check Y_j per cui $h_{v_j} = -t$.

Si ha:

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} = \sum_{v=v'}^{v''} (g_v - \bar{x}_v)h_v = \sum_{h_v > 0} (g_v - \bar{x}_v)h_v + \sum_{h_v < 0} (g_v - \bar{x}_v)h_v \leq 0,$$

per cui:

$$\sum_{h_v > 0} (g_v - \bar{x}_v)h_v \leq \sum_{h_v < 0} (g_v - \bar{x}_v)|h_v|,$$

e quindi, posto $M = max_{v \in [v',v'']} h_v$ e $m = -min_{v \in [v',v'']} h_v$, ponendo:

$$\sum_{h_v > 0} (g_v - \bar{x}_v)h_v \stackrel{\text{def}}{=} \sum_{h=1}^{M} t_h^+ h$$

e:

$$\sum_{h_v < 0} (g_v - \bar{x}_v)|h_v| \stackrel{\text{def}}{=} \sum_{h=1}^{m} t_h^- h,$$

si ha:

$$\sum_{h=1}^{M} t_h^+ h \leq \sum_{h=1}^{m} t_h^- h = t_1^- 1 + t_2^- 2 + \ldots t_m^- m.$$

Suddividiamo la prima sommatoria della precedente relazione, al seguente modo:

$$\sum_{h=1}^{M} t_h^+ h = (\sum_{h=h_1+1}^{M} t_h^+ h + t_{h_1}^{+'} h_1) + (t_{h_1}^{+''} h_1 + \sum_{h=h_2+1}^{h_1-1} t_h^+ h + t_{h_2}^{+'} h_2) + \ldots$$

$$\ldots + (t_{h_{m-1}}^{+''} h_{m-1} + \sum_{h=1}^{h_{m-1}-1} t_h^+ h),$$

in modo che si abbia:

$$(\sum_{h=h_1+1}^{M} t_h^+ h + t_{h_1}^{+'} h_1) = t_1^- 1,$$

$$\forall l = 2, \ldots, m-1 \quad (t_{h_{l-1}}^{+''} h_{l-1} + \sum_{h=h_l+1}^{h_{l-1}-1} t_h^+ h + t_{h_l}^{+'} h_l) = t_l^- l,$$

e:

$$(t_{h_{m-1}}^{+''} h_{m-1} + \sum_{h=1}^{h_{m-1}-1} t_h^+ h) \leq t_m^- m,$$

ovvero:

$$(\sum_{h=h_1+1}^{M} t_h^+ h + t_{h_1}^{+'} h_1) = t_1^-,$$

$$\forall l = 2, \ldots, m-1 \quad \left(\frac{t_{h_{l-1}}^{+''} h_{l-1}}{l} + \sum_{h=h_l+1}^{h_{l-1}-1} \frac{t_h^+ h}{l} + \frac{t_{h_l}^{+'} h_l}{l}\right) = t_l^-,$$

e:

$$\left(\frac{t_{h_{m-1}}^{+''} h_{m-1}}{m} + \sum_{h=1}^{h_{m-1}-1} \frac{t_h^+ h}{m}\right) \leq t_m^-.$$

Sfruttando le ultime tre relazioni scritte è possibile, associando a l mappe di livello $h > 0$ h mappe di livello $-l$, costruire una combinazione di mappe soddisfacente le (3.3).

Ad esempio per $d = 6$ e $r = 27$, $k = 2^{r+1} - d - 1 = 268435449$, posto $* = 1342177$, si ha $v' = *11$, $v'' = *38$, $\left\lfloor \frac{k}{2} \right\rfloor = *24$, $\left\lceil \frac{k}{2} \right\rceil = *25$, $2^r - d = *22$ e $2^r - 1 = *27$. Si ha $M = 11$, $m = 2$ e:

$$t_{11}^+ = \binom{27}{0} + \binom{27}{27} = 2 \cdot 1 = 2,$$
$$t_{10}^+ = \binom{27}{1} + \binom{27}{26} = 2 \cdot 27 = 54,$$
$$t_9^+ = \binom{27}{2} + \binom{27}{25} = 2 \cdot 351 = 702,$$
$$t_8^+ = \binom{27}{3} + \binom{27}{24} = 2 \cdot 2925 = 5850,$$
$$t_7^+ = \binom{27}{4} + \binom{27}{23} = 2 \cdot 17550 = 35100,$$
$$t_6^+ = \binom{27}{5} + \binom{27}{22} = 2 \cdot 80730 = 161460,$$
$$t_5^+ = \binom{27}{6} + \binom{27}{21} = 2 \cdot 296010 = 592020,$$
$$t_4^+ = \binom{27}{7} + \binom{27}{20} = 2 \cdot 888030 = 1776060,$$
$$t_3^+ = \binom{27}{8} + \binom{27}{19} = 2 \cdot 2220075 = 4440150,$$
$$t_2^+ = \binom{27}{9} + \binom{27}{18} = 2 \cdot 4686825 = 9373650,$$
$$t_1^+ = \binom{27}{10} + \binom{27}{17} = 2 \cdot 8436285 = 16872570,$$

$$t_1^- = \binom{27}{12} + \binom{27}{15} - 2 = 2 \cdot 17383859 = 34767718,$$
$$t_2^- = \binom{27}{13} + \binom{27}{14} - 2 = 2 \cdot 20058299 = 40116598.$$

Si ha $t_2^{+'} = \frac{t_1^- - \sum_{h=3}^{11} t_h^+ h}{2} = 5057394$ e $t_2^{+''} = t_2^+ - t_2^{+'} = 4316256$, per cui una combinazione di mappe può essere costruita associando ad una mappa di livello h, h mappe di livello -1, ciò per ogni $h = 11, \ldots, 2$, per $\sum_{h=3}^{11} t_h^+ + t_2^{+'}$ volte, dopodiché si associano a due mappe di livello h, h mappe di livello -2, ciò per $h = 1, 2$, per $t_2^{+''} + t_1^+$ volte. Infine si definiscono le mappe doppie che accoppiano i pesi q e $q + 2^r$, per ogni q, fino ad esaurire i check. Ciò si può fare perché i check rimasti sono tali che $\max\{v, k - v\} \leq 2^r - 1$.

È facile vedere che quanto abbiamo fatto si può fare, con qualche accortezza, in generale. ∎

La caratterizzazione della scelta ottimale per la combinazione di mappe è data dal seguente:

Teorema 3.6 *Il piú piccolo d per cui esiste una combinazione di mappe (3.2) per cui valgono le (3.3), è il piú piccolo d per cui risulta:*

$$(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} \leq 0.$$

Per tale scelta di d è possibile supporre che:

$$Y_i :: \mathcal{S}_{v_i} \longrightarrow \mathcal{S}_{v_i} \quad \forall i \in [1, d],$$

con i v_i scelti in mezzo all'intervallo $[0, k]$, ovvero tali che:

$$v_i \in [2^r - d, 2^r - 1] \quad \Longleftrightarrow \quad v_i \stackrel{\text{def}}{=} 2^r - d - 1 + i \quad \forall i \in [1, d],$$

Inoltre si ha:

$$d \geq 1 + 0.8\sqrt{r},$$

e quindi:

$$k \simeq 2^{r+1} - 0.8\sqrt{r} - 2.$$

Dimostrazione: Sia d il piú piccolo intero tale che (3.2) è una combinazione di mappe per cui valgono le (3.3), allora:

1. Per il Teorema 3.3 esiste una combinazione di mappe (3.2) per cui valgono le (3.3) e la (3.4) o la (3.5).
2. Per il Teorema 3.4 si ha $(\mathbf{g} - \bar{\mathbf{x}})\mathbf{h} \leq 0$.
3. Per il Teorema 3.5 esiste una combinazione di mappe (3.2) per cui valgono le (3.3), la (3.16) e la (3.17).

Per la restante parte del Teorema rimandiamo a [1]. ∎

Bibliografia

[1] S. Al-Bassam and B. Bose, *Design of Efficient Balanced Codes*, in Proc. IEEE 19th Int. Symp. Fault Tolerant Computing, June 1989.

[2] B. Bose, *Burst Unidirectional Error-Detecting Codes*, IEEE Trans. Comput. vol. c-35, pp. 350–353, April 1986.

[3] B. Bose, *On Unordered Codes*, in Proc. IEEE 17th Int. Symp. Fault Tolerant Computing, pp. 102–107, July 1987

[4] B. Bose and D. J. Lin, *Systematic Unidirectional Error-Detecting Codes*, IEEE Trans. Comput. vol. c-34, pp.1026–1032, Nov. 1985.

[5] L. A. Dunnin, G. Dial and M. R. Varnasi, *Unidirectional Byte Error Detecting Codes for computer Memory System*, IEEE Trans. Comput, vol. c-39, pp. 592–595, April 1990.

[6] D. E. Knuth, *Efficient Balanced Codes*, IEEE Trans. Inform. Theory, vol. IT-32, pp. 51–53, Jan. 1986.

Luca TALLINI
Viale Ippocrate n. 97
Roma, ITALIA,
cap. 00161.