UNIVERSITÀ DEGLI STUDI DI PISA
ISTITUTO DI SCIENZE DELL'INFORMAZIONE

Su alcune proprietà delle sequenze binarie

SERGIO FRASCA - PIETRO PIRAM

NOTE SCIENTIFICHE
S - 74 - 4
MARZO 1974

Università degli Studi di Pisa
ISTITUTO DI SCIENZE DELL'INFORMAZIONE

SU ALCUNE PROPRIETA' DELLE SEQUENZE BINARIE

Sergio Frasca* - Pietro Piram

Nota Scientifica S-74-4
(Marzo 1974)

---

* Specializzando in "Calcolo Automatico" presso l'Istituto di Elaborazione dell'Informazione del C.N.R. - Pisa.

SU ALCUNE PROPRIETA' DELLE SEQUENZE BINARIE

Riassunto.

In questa nota si studiano le proprietà di un operatore lineare O che opera su sequenze di data lunghezza, di elementi di GF(2).

L'operatore O e il suo inverso presentano analogie con l'integrale e la derivata dell'analisi classica, ove le sequenze binarie siano viste come funzioni reali di variabile reale.

L'operatore O e le sue potenze vengono utilizzati per mettere in luce particolari proprietà delle sequenze binarie. In particolare viene ricavato uno sviluppo formalmente analogo a quello di Taylor e una procedura per ricavare particolari insiemi di vettori linearmente indipendenti.

Premessa.

Le sequenze binarie di lunghezze n saranno considerate anche come vettori dello spazio a n dimensioni i cui versori sono le sequenze (100...0)(010..0) etc

Le sequenze saranno indicate come lettere minuscole e gli elementi delle sequenze con lettere minuscole con indice in basso.

Le matrici saranno indicate con lettere maiuscole.

Ulteriori notazioni saranno definite all'occorrenza.

Si supporrà, infine, che, per tutte le sequenze, gli elementi con indice negativo siano nulli (cioè tutte le sequenze sono precedute da infiniti zeri).

Sia $s^{(k)}$ una sequenza binaria di lunghezza k il cui generico simbolo sarà indicato son s_i. Definiamo i seguenti operatori O^{-1} e O^{1}

$$O^{-1}[s_i] = s_{i-1} + s_i$$

$$O^{1}[s_i] = \sum_{j=1}^{i} s_j$$

per $1 \leq i \leq k$.

L'operatore O^{-1} mostra una proprietà locale della sequenza e cioè se c'è o no variazione, l'operatore O^{1} mostra invece una proprietà totale e cioè se nei primi i simboli si ha un numero di uno pari o dispari.

Definiamo

$$O^{-n}(s_i) = O^{-(n-1)}(s_i) + O^{-(n-1)}(s_{i-1})$$

per $n \geq 2$

e, analogamente

$$O^{n}(s_i) = \sum_{j=1}^{i} O^{(n-1)}(s_i)$$

Teorema 1.1

$$O^{-1}[s_i+g_i] = O^{-1}[s_i] + O^{-1}[g_i]$$

Teorema 1.2

$$O^{1}[s_i+g_i] = O^{1}[s_i] + O^{1}[g_i]$$

Entrambi i teoremi sono facilmente dimostrabili.

O^1 e O^{-1} possono essere visti anche come operatori che operano sull'intera sequenza lunga k producendo una nuova sequenza della stessa lunghezza. Dalla linearità di O^1 e O^{-1} si deduce che ad essi può essere associata una matrice $k \times k$.

Per l'operatore O^{-1} si ha la seguente matrice

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & . & . \\ 1 & 1 & 0 & 0 & . & . \\ 0 & 1 & 1 & 0 & . & . \\ 0 & 0 & 1 & 1 & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

mentre per O^1 si ha

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & . & . & 0 \\ 1 & 1 & 0 & 0 & . & . & 0 \\ 1 & 1 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 1 & 1 & 1 & . & . & 1 & 1 \end{pmatrix}$$

Teorema 1.3

$$A.B = I$$

dove I è la matrice identità $k \times k$.

Essendo

$$A_{hj} = 1 \quad \text{per} \quad j = h, \quad j = h-s$$

e zero altrimenti,

$$B_{jm} = 1 \quad \text{per} \quad j \geq m$$

risulta

$$(A.B)_{hm} = \Sigma_j \; A_{hj} \; B_{jm} = \begin{cases} 0 \text{ per } & h \neq m \\ 1 \text{ per } & h = m \end{cases}$$

da cui il teorema.

Osserviamo che gli operatori 0^{-1} e 0^{1} sono analoghi agli operatori "derivata" e "integrale" dell'analisi classica, qualora si intenda l'indice della sequenza come "variabile indipendente".

Il teorema 1.3 in questa prospettiva è l'analogo di quello di Torricelli-Barrow. Ciò giustifica la notazione adottata, alla quale possiamo aggiungere anche l'operatore "identità" 0°.

Si verifica che valgono le proprietà formali degli esponenti e cioè

$$0^{m} * 0^{n} = 0^{m+n}$$

essendo l'* il prodotto operatorio e m e n interi relativi.

Essendo A la matrice relativa all'operatore 0^{i}, la matrice A^{n} risulta associata all'operatore $0^{i.n}$.

Teorema 1.4

$$0^{m}[s_{i}] = 0^{m-1}[s_{i}] + 0^{m}[s_{i-1}]$$

Si ricava dalla 3 ponendo $n=-m+1$.
D'ora in poi identificheremo queste due notazioni

$$0^{m}[s_{i}] \equiv s_{i}^{m}$$

Teorema 1.5

$$0^{n}[s_{i}] = 0^{n-2^{k}}[s_{i}] + 0^{n}[s_{i-2^{k}}] \quad \text{ovvero} \quad s_{i}^{m} = s_{i}^{m-2^{k}} + s_{i-2^{k}}^{m}$$

Si ricava iterando k volte il teorema 1.4.

Corollario 1.6

$$s_i^m = s_i^{m+2^k} + s_{i-2^k}^{m+2^k}$$

Si ricava da 1.5 ponendo $m=n-2^k$.

Teorema 1.7

I primi 2^k elementi di s_i^m sono uguali ai primi 2^k elementi di $s_i^{m+j\times 2^k}$ con j intero qualsiasi.

Si dimostra, per $j=-1$, osservando che il secondo elemento del secondo termine del Teorema 1.5 è nullo per $i<2^k$. Per j qualunque, transitivamente.

Corollario 1.8

$$s_1^n = s_1^m$$

per ogni m,n.
Si deduce banalmente da 1.7.

Definiamo un insieme di funzioni che chiamiamo monomie. Esse saranno indicate con x_i^0, x_i^1, $\ldots, x_i^n$

$x_i^0 = 1$ per qualsiasi i e $x_i^k = 0^k[x_i^0]$

x^0	1 1 1 1 1 1 1 1 1 ...
x^1	1 0 1 0 1 0 1 0 1 ...
x^2	1 1 0 0 1 1 0 0 1 ...
x^3	1 0 0 0 1 0 0 0 1 ...
x^4	1 1 1 1 0 0 0 0 1 ...
x^5	1 0 1 0 0 0 0 0 1 ...
x^6	1 1 0 0 0 0 0 0 1 ...
x^7	1 0 0 0 0 0 0 0 1 ...
x^8	1 1 1 1 1 1 1 1 0 ...

Tali funzioni sono particolarmente interessanti per le loro proprietà (importanti sono talune analogie con le potenze di x come variabile reale).

Sia X la matrice quadrata $2^k \times 2^k$ costituita dalle prime 2^k funzioni monomie fino alla lunghezza 2^k. x_i^k è l'elemento che giace sulla (k-1)esima riga e i-esima colonna di X.

<u>Teorema 2.1</u>

$$x_i^n = x_i^0 + x_{i-1}^1 + x_{i-1}^2 \ldots x_{i-1}^n = x_{i-1}^0 + x_{i-1}^1 \ldots x_{i-1}^n \quad \text{per} \quad i>1.$$

La prima uguaglianza si deduce dal Teorema 2.4 con iterazioni opportune.

La seconda uguaglianza deriva dal fatto che $x_i^0 = x_{i-1}^0 = 1$ per $i>1$.

Teorema 2.2

La matrice X è simmetrica.

Si deduce dal teorema precedente poichè esso implica che, essendo la prima riga e la prima colonna identiche, la seconda colonna sia uguale alla seconda riga e così via.

Data una matrice quadrata $A^{(n)}$ di dimensione n(pari) la esprimiamo mediante sottomatrici come segue:

$$A^{(n)} = \begin{pmatrix} A_{11}^{(\frac{n}{2})} & A_{12}^{(\frac{n}{2})} \\ \\ A_{21}^{(\frac{n}{2})} & A_{22}^{(\frac{n}{2})} \end{pmatrix} .$$

Teorema 2.3

La sottomatrice $X_{22}^{(2^{k-1})}$ è composta da soli zero, per ogni k.

Infatti per il teorema 1.7 i primi 2^{k-1} elementi di x_{2^k} sono tutti uguali a 1. Per il teorema 1.5 i secondi 2^{k-1} elementi di x_{2^k}, che sono gli elementi della prima riga di $X_{22}^{(2^{k-1})}$ sono nulli. Per il teorema 3.2 sono nulli anche gli elementi della prima colonna di $X_{22}^{(2^{k-1})}$. Per il teorema 1.4 sono nulli anche il secondo, il terzo etc. elemento della seconda riga di $X_{22}^{(2^{k-1})}$, e analogamente per le righe successive.

Teorema 2.4

Le prime 2^k funzioni sono periodiche di periodo 2^k.

Si dimostra dalla simmetria della X e per il teorema 1.7.

Il periodo minimo della funzione n-esima è 2^{k_n} essendo $2^{k_n-1} < n \leq 2^{k_n}$.

Osserviamo che tutte le matrici costituite da sequenze binarie legate dall'operatore $O^{\pm 1}$ sono periodiche "verticalmente". Se le sequenze binarie sono quelle monomie, allora la matrice è periodica anche "orizzontalmente".

Teorema 2.5

La matrice $X^{(2^k)}$ contiene un numero pari di uno per riga e per colonna, eccetto che per la riga e la colonna 2^k che contengono un solo uno.

La x^{2^k-1} è costituita da (100...0) e ciò perchè i primi 2^k elementi di x^{2^k} debbono essere uguali a 1 per il teorema 1.7. Dal teorema 2.1 si deduce che il numero di uno per colonna è pari (esclusa l'ultima colonna). Per la simmetria, ciò è vero anche per le righe.

Teorema 2.6

La matrice $X^{(2^k)}$ è triangolare e la diagonale secondaria è composta da tutti uno.

L'ultima riga è composta da (100...0). Per il teorema 1.3 la n-esima riga è ottenuta dalla (n+1)-esima tramite l'operatore O^{-1}.

Quindi $x_2^{2^k-2} = 1$ e $x_i^{2^k-2} = 0$ per $i>2$.

Iterando per $x_3^{2^k-3}$ etc. si ha l'asserto.

Teorema 2.7

Il determinante della matrice X è uguale a 1.

Si deduce dal teorema 2.6.

Osservazione.

La matrice $X^{(2^k)}$ è costituita ricorsivamente nel seguente modo

$$X^{(2^k)} = \begin{pmatrix} X^{(2^{k-1})} & X^{(2^{k-1})} \\ X^{(2^{k-1})} & 0 \end{pmatrix}$$

$X^{(2^0)} = 1.$

Osservazione.

Dal Teorema 2.7 si deduce che le prime 2^k sequenze x^i_j $1 \leq j \leq 2^k$ sono linearmente indipendenti e quindi costituiscono una base per i vettori con 2^k componenti.

Introduciamo un nuovo insieme di funzioni che chiameremo "locali" e indicheremo x^{-k} (con $k>0$ intero). Esse sono così definite

$$x_i^{-k} = 0^{-k}[x_i^0]$$

essendo $x_i^0 = 1$ per ogni i

x^0	1 1 1 1 1 1 1 1 ...
x^{-1}	1 0 0 0 0 0 0 0 ...
x^{-2}	1 1 0 0 0 0 0 0 ...
x^{-3}	1 0 1 0 0 0 0 0 ...
x^{-4}	1 1 1 1 0 0 0 0 ...
x^{-5}	1 0 0 0 1 0 0 0 ...
x^{-6}	1 1 0 0 1 1 0 0 ...
x^{-7}	1 0 1 0 1 0 1 0 ...
x^{-8}	1 1 1 1 1 1 1 1 ...

Sia Y la matrice quadrata $2^k \times 2^k$ costituita dalle prime 2^k funzioni locali fino alla lunghezza 2^k. Sia x_i^{-k} l'elemento che giace sulla (k-1)-esima riga e i-esima colonna di Y.

Teorema 2.8

La matrice Y è triangolare ed ha la diagonale composta da tutti uno. Infatti x^{-1} è costituita da (1000...). Quindi x^{-2} avrà un uno nella seconda posizione e zero di seguito, x^{-3} avrà un uno nella terza posizione e zero di seguito etc. Da ciò si deduce che il determinante di Y è 1.

Teorema 2.9

$$Y^{(2^k)} = \begin{pmatrix} Y^{(2^{k-1})} & 0 \\ Y^{(2^{k-1})} & Y^{(2^{k-1})} \end{pmatrix}$$

$Y^{(1)} = 1.$

Lo si può dimostrare dal fatto che $x_i^{-2^k} = 1$ per ogni $i \leq 2^k$ (Teorema 1.7) e dal Teorema 1.3 e dall'algoritmo di formazione della matrice X.

Dimostriamo una generalizzazione dei teoremi 2.7 e 2.8.

Teorema 2.10

Una matrice $X^{(n)}$ è non singolare qualunque sia n.

Sia k il massimo intero tale che $2^k < n$. La $X^{(n)}$ può essere schematizzata come

$$\left(\begin{array}{c|c} X^{(2^k)} & A \\ \hline A^T & 0 \end{array}\right)$$

A^T, di dimensioni $(n-2^k) \times 2^k$ è costituita dalle prime $n-2^k$ righe di $X^{(2^k)}$. Poichè $X^{(2^k)}$ è non singolare il rango di A^T è $n-2^k$.

Il teorema è vero se la matrice M costituita dalle prime $n-2^k$ righe di A è non singolare. Infatti in tal caso nessuna combinazione lineare di righe di $X^{(n)}$ è nulla.

Dimostriamo che M è non singolare. Si ha

$$M = X^{(n-2^k)}$$

che è una matrice del tipo $X^{(n)}$. Si può iterare il procedimento finchè M non sia del tipo X^{2^h} con h opportuno il che accade sempre, al peggio con h=0.

Teorema 2.11

Una matrice $Y^{(n)}$ è non singolare qualunque sia n. Si dimostra banalmente per la triangolarità di $Y^{(n)}$.

Chiamiamo una matrice quadrata M "di tipo MDD" (Matrice delle derivate) se la riga i-esima è la "derivata" della riga i-1 per ogni i 0 e l'elemento $M_{11} = 1$.

Chiamiamo invece una matrice quadrata N "di tipo MDI" se la riga i-esima è "l'integrale" della riga (i-1)-esima e $N_{11} = 1$.

Teorema 3.1

Data una qualsiasi matrice $A^{(n)}$ di tipo MDD, si ha, essendo a_{hk} il generico elemento di $A^{(n)}$,

$$(1) \qquad a_{hn} = \sum_{k=1}^{n} a_{1k} \times x_{n-k+1}^{-h}$$

Cioè il vettore colonna n-esima è determinato dalla suddetta legge dal vettore prima riga.

Per qualsiasi n, la 1 è vera per h=1 e anche per h=2.

Supponiamo che sia valida, per qualsiasi n, per h=r-1; dimostriamo che la (1) è vera per h=r.

Essendo

$$a_{rn} = a_{r-1,n-1} + a_{r-1,n}$$

per l'ipotesi fatta risulta

$$a_{rn} = \sum_{k=1}^{n-1} a_{1k}\, x_{n-k}^{-r+1} + \sum_{k=1}^{n} a_{1k}\, x_{n-k+1}^{-r+1} =$$

$$= \sum_{k=1}^{n-1} a_{1k} \left(x_{n-k}^{-r+1} + x_{n-k+1}^{-r+1}\right) + a_{1n}\, x_1^{-r+1} =$$

$$= \sum_{k=1}^{n-1} a_{1k}\, x_{n-k+1}^{-r} + a_{1n}\, x_1^{-r} = \sum_{k=1}^{n} a_{1k}\, x_{n-k+1}^{-r} \qquad \text{cdd.}$$

Esiste l'analogo del 3.1 per matrici di tipo MDI:

Teorema 3.2

Data una qualsiasi matrice $B^{(n)}$ di tipo MDI si ha

$$b_{hn} = \sum_{i=1}^{n} b_{1k} \cdot x_{n-k+1}^{h-2}$$

Si dimostra con procedimento induttivo analogo a quello del Teorema 3.1.

Dei Teoremi 3.1 e 3.2 si può dare la seguente interpretazione matriciale:

Teorema 3.1'

$$\begin{pmatrix} x_1^{-1} & x_2^{-1} & \dots & x_n^{-1} \\ x_1^{-2} & x_2^{-2} & \dots & x_n^{-2} \\ \vdots & & & \\ x_1^{-n} & \dots & \dots & x_n^{-n} \end{pmatrix} \cdot \begin{pmatrix} a_{1,n} \\ a_{1,n-1} \\ \vdots \\ a_{1,1} \end{pmatrix} = \begin{pmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ a_{n,n} \end{pmatrix}$$

Teorema 3.2'

$$\begin{pmatrix} x_1^{-1} & x_2^{-1} & \dots & x_n^{-1} \\ x_1^{0} & x_2^{0} & \dots & x_n^{0} \\ \vdots & & & \\ x_1^{n-2} & x_2^{n-2} & \dots & x_n^{n-2} \end{pmatrix} \cdot \begin{pmatrix} b_{1,n} \\ b_{1,n-1} \\ \vdots \\ b_{1,1} \end{pmatrix} = \begin{pmatrix} b_{1,n} \\ b_{2,n} \\ \vdots \\ b_{n,n} \end{pmatrix}$$

Da ciò si deduce che nell'ipotesi di non singolarità delle matrici relative ai Teoremi 3.1' e 3.2', si possono ricavare i teoremi inversi dei 3.1 e 3.2. In particolare, in base al Teorema 3.1 che afferma la non singolarità della matrice $Y^{(n)}$ relativa al Teorema 3.1', si può ottenere l'inverso del Teorema 3.1 che è analogo concettualmente al teorema dei Taylor dell'analisi classica. Per quanto riguarda l'inversione della matrice $Y^{(n)}$ si ha:

<u>Teorema 3.3</u>

$$Y = Y^{-1}$$

Per dimostrare il Teorema 3.3 dimostriamo il seguente

<u>Lemma 3.4</u>

$$Y^{(2^k)} = (Y^{(2^k)})^{-1}$$

La matrice $Y^{(2^k)}$ può essere schematizzata nel seguente modo

$$Y^{(2^k)} = \begin{pmatrix} Y^{(2^{k-1})} & 0 \\ Y^{(2^{k-1})} & Y^{(2^{k-1})} \end{pmatrix}$$

Risulta

$$(Y^{(2^k)})^2 = \begin{pmatrix} (Y^{(2^{k-1})})^2 & 0 \\ 0 & (Y^{(2^{k-1})})^2 \end{pmatrix}$$

quindi essendo $Y^1 = 1$ il lemma è facilmente dimostrabile per induzione.

Torniamo al teorema 3.3

La matrice $Y^{(n)}$ è l'inversa di se stessa, qualunque sia n.

Dim: $Y^{(n)}$ può essere schematizzata come segue

$$\begin{array}{|c|c|} \hline Y^{(2^k)} & 0 \\ \hline A & Y^{(n)} \\ \hline \end{array}$$

con k opportuno, $m<n$, ed $A = (Y^{(m)} \mid 0')$.

Facendo il prodotto a blocchi di $Y^{(n)}$ con se stessa si ha

$$(Y^{(n)})^2 = \left(\begin{array}{c|c} (Y^{(2^k)})^2 + 0.A & Y^{(2^k)}.0 + 0.Y^{(m)} \\ \hline A.Y^{(2^k)} + Y^{(m)}.A & A.0 + (Y^{(m)})^2 \end{array}\right)$$

Data la forma di A si può verificare che $A.Y^{(2^k)} = Y^{(m)}.A$ e quindi si ha

$$(Y^{(n)})^2 = \left(\begin{array}{c|c} (Y^{(2^k)})^2 & 0 \\ \hline 0 & (Y^{(m)})^2 \end{array}\right)$$

Poichè $(Y^{(2^k)})^2$ è diagonale, $(Y^{(n)})^2$ lo è se lo è $(Y^{(m)})^2$.

Essendo $m<n$ si può iterare il procedimento fino ad ottenere $m=2^h$ con h opportuno eventualmente nullo.

Ricaviamo quindi l'analogo del teorema di Taylor e cioè

<u>Teorema 3.5</u>

$$a_{1,h} = \sum_{k=1}^{n} a_{kn} \times x_{n-k+1}^{-h} \qquad 1 \leq h \leq n$$

dove a_{kn} rappresenta la "derivata" k-esima nel punto n della prima riga.

Vediamo come esprimere una sequenza s nella base costituita dalle funzioni locali x^{-k}.

<u>Teorema 3.6</u>

$$s^{(n)} = \sum_{k=1}^{n} \alpha_k \, x^{-k} \quad \text{con} \quad \vec{\alpha} = s^{(n)} \, Y^{(n)}$$

Infatti risulta

$$sYY = sYY$$

$$sI = \alpha\, Y$$

α può essere visto come il vettore "trasformato" di s secondo la base formata dalle funzioni locali.

Sia M una matrice del tipo MDD, di ordine 2^k, essendo D la matrice relativa all'operatore O^{-1}, si ha

Teorema 3.7

$$D.M^T = (PC.M)^T$$

dove

$$PC = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & . & . \\ 0 & 0 & 0 & 1 & . & . \\ 0 & . & . & . & . & . \\ . & . & . & . & . & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

cioè la matrice relativa all'operatore "permutazione ciclica" verso l'alto di un vettore colonna.

Il teorema si può verificare facilmente.

<u>Teorema 3.8</u>

Una matrice A di tipo MDD di ordine 2^k è non singolare.
L'asserto può essere dimostrato facendo vedere che è possibile ottenere tutti i versori come combinazioni lineari di righe della matrice.
Sommando la riga i-esima con la riga $(i+2^{k-1})$-esima, con $1 \le i < 2^{k-1}$, si ottie

ne una matrice di 2^{k-1} righe e 2^k colonne con le prime 2^{k-1} colonne identicamente nulle, mentre le rimanenti colonne formano una matrice B di tipo MDD, per la linearità dell'operatore O^{-1} e per il corollario 1.6.

Supponiamo di aver trovato un procedimento per costruire i versori di una matrice MDD di ordine 2^{k-1}; sapendo quindi come ottenere i versori della matrice B e cioè come ottenere gli ultimi 2^{k-1} versori della matrice A, possiamo portare la matrice A della forma

$$\begin{pmatrix} A' & A'' \\ A' & A''' \end{pmatrix}$$

alla forma

$$\begin{pmatrix} A' & 0 \\ A' & 0 \end{pmatrix}$$

A' è una MDD di ordine 2^{k-1} e quindi sappiamo ricavarne i versori, e quindi, i rimanenti versori di A. Iterando il procedimento per k-2,k-3 ..., il teorema risulta vero sapendo trovare i versori di una qualunque matrice MDD di ordine 2, il che si può ottenere banalmente.

Data una sequenza s il cui generico elemento è s_i, chiamiamo $^{(k)}s$ la sequenza tale che

$$^{(k)}s_i = 0 \qquad i \leq k$$

$$^{(k)}s_i = s_{i-k} \qquad \text{per} \quad i>k$$

Teorema 4.1

Per una qualunque sequenza s di lunghezza n si ha

$$s = \sum_{k=1}^{n} s_k^{-1} \quad {}^{(k-1)}x^0$$

Si verifica banalmente.

Osserviamo che questo teorema equivale al Teorema 3.1. Il Teorema 4.1 sviluppa una qualunque sequenza s per "run".

Teorema 4.2

Per una qualunque sequenza s di lunghezza n si ha

$$s^{-k} = \sum_{i=1}^{n} s_i \cdot {}^{(i-1)}x^{-(k+1)}$$

Segue dal 4.1 e dalla linearità dell'operatore O^{-1}.

Considerando il peso di Hamming della sequenza s^{-1}, si ha che tale peso dà il numero totale di run in s.

La sequenza $s^{-1} \wedge s$, dove $\wedge$ indica il prodotto vettoriale o AND componente per componente, ha peso uguale al numero di run di uno.

Analogamente per le run di zeri la $s^{-1} \wedge \bar{s}$ dove $\bar{s}$ indica la sequenza complementata di s.

Se nella s^{-1} ci sono due uno vicini vuol dire che nella s esiste una run di lunghezza 1 in corrispondenza del primo uno di s^{-1}. In generale se ci sono n 1 consecutivi nella s^{-1}, vuol dire che nella s esistono n-1 run di lunghezza 1 consecutive. Quindi il prodotto $a=\overline{(s^{-2})}\wedge s^{-1}$ ha peso uguale al numero totale di run di lunghezza 1. a toglie un 1 all'inizio di ogni run di uno della s^{-1} e quindi gli uno di a sono sfasati di 1 rispetto alle run di lunghezza 1 di s.

Il prodotto $a\wedge {}^{(1)}s$ ha peso pari al numero di run di uno di lunghezza 1.

Per le run di zeri di lunghezza 1 si ha

$$\overline{s^{-2}} \wedge s^{-1} \wedge \overline{{}^{(1)}s} \qquad = \qquad a \wedge \overline{{}^{(1)}s}$$

Una run di lunghezza due in s dà luogo in s^{-1} ad una run di zeri di lunghezza uno, con lo zero posizionato sotto l'ultimo bit della run. Ci si riconduce quindi al ragionamento precedente per individuare le run di zeri di lunghezza uno. La formula è la seguente

$$\overline{s^{-3}} \wedge s^{-2} \wedge \overline{{}^{(1)}s^{-1}}$$

Per selezionare le run di uno di lunghezza due si fa

$$\overline{s^{-3}} \wedge s^{-2} \wedge \overline{{}^{(1)}s^{-1}} \wedge {}^{(1)}s$$

e analogamente per le run di zeri di lunghezza due

$$\overline{s^{-3}} \wedge s^{-2} \wedge \overline{{}^{(1)}s^{-1}} \wedge \overline{{}^{(1)}s} .$$

In generale una qualsiasi run di lunghezza n nella s dà luogo nella s^{-1} a una run di zeri di lunghezza n-1.

Possiamo quindi ricavare il seguente importante teorema:

<u>Teorema 4.3</u>

Il numero totale di run di lunghezza n nella s è dato dal peso della sequenza g(n)

$$g(n) = (\overline{s^{-(n+1)}} \wedge s^n) \wedge \bigwedge_{k=1}^{n-1} \overline{(1)_s{}^{-k}}$$

Abbiamo anche i seguenti due corollari

<u>Corollario 4.4</u>

Il numero di run di uno di lunghezza n è dato dal peso di

$$g(n,1) = g(n) \wedge (1)_s$$

<u>Corollario 4.5</u>

Il numero di run di zeri di lunghezza n è dato dal peso di

$$g(n,0) = g(n) \wedge \overline{(1)_s}$$