CODICI E GRAFI

Stefano Bertorelli

Dottorato in Ingegneria dell'Informazione

XVIII ciclo

Anno Accademico 2003/2004

Corso di Matematica Discreta

Riassunto

In questo lavoro si mostra come sia possibile generare codici binari a partire dalla matrice di adiacenza di determinati grafi [1]. In particolare, ponendo alcune condizioni cui i grafi devono sottostare, si può assicurare che il codice risultante possegga specifiche proprietà. Questo metodo viene usato per la costruzione di tutti i codici binari auto-duali doppiamente pari di lunghezza minore o uguale a 24.

1 Introduzione

In questa relazione è descritta la tecnica che permette di generare codici dai grafi ed è mostrato come, imponendo varie condizioni sui grafi di partenza, si possa ottenere un codice che abbia determinate caratteristiche. In particolare, si possono produrre tutti i codici binari auto-duali e doppiamente pari di lunghezza 8, 12 e 24 semplicemente ricercando un insieme di grafi che soddisfino a particolari condizioni.

E' degno di nota il fatto che questo metodo ha molti e importanti vantaggi. Si ottiene non solamente una base naturale per il codice, insieme con un sistema semplice per ricordarne la matrice generatrice, ma anche una descrizione di tutte le parole di codice. Questo permette di calcolare la distanza minima del codice direttamente dal grafo e di scrivere immediatamente tutte le parole di codice (compatibilmente con la lunghezza di queste ultime). Inoltre, si possono sfruttare le simmetrie del grafo (che equivalgono a simmetrie del codice) per facilitare il calcolo dell'alfabeto del codice nei casi più complessi.

2 Codici auto-duali doppiamente pari

Sia F un campo finito e F^n lo spazio vettoriale delle n-ple di elementi di F. Un codice lineare C è un sottospazio di F^n, ed i vettori che lo compongono sono chiamati parole di codice. La lunghezza delle parole di informazione è detta *dimensione del codice*; se tale valore è pari k, si dice che il codice è di tipo [n,k] e n viene detta la lunghezza del codice.

Se $a = (a_1, a_2, ..., a_n)$ e $b = (b_1, b_2, ..., b_n)$ sono parole di codice di C, allora si definisce come *distanza di Hamming d(a,b)* tra a e b il numero di posizioni in cui tali parole differiscono. Il *peso di Hamming wt(a)* di una parola di codice a è il numero di elementi di a diversi da zero. Vale la relazione:

$$d(a,b) = wt(a-b) \qquad \textbf{(1)}$$

Uno dei parametri più importanti di un codice correttore di errori è la sua *distanza minima di Hamming*, definita come:

$$\min_{a \neq b} wt(a-b) \tag{2}$$

dal momento che a partire da questo numero è possibile sapere quanti errori possono essere corretti dal codice. Un codice di lunghezza n, dimensione k e distanza minima d si definisce codice di tipo [n,k,d]. E' da notare come essendo C chiuso ripetto alla differenza, la minima distanza d è pari al peso minimo delle sue parole di codice diverse da zero.

Si definisce prodotto interno naturale nello spazio vettoriale F^n come:

$$a \cdot b = \sum_i a_i b_i \tag{3}$$

e se $a \cdot b = 0$, allora a e b sono ortogonali.

Dato un codice lineare C, si definisce *codice duale* $C^\perp$ l'insieme dei vettori che sono ortogonali a tutte le parole di codice di C, ovvero:

$$C^\perp = \left\{ u \middle| u \cdot v = 0, \quad for \quad all \quad v \in C \right\} \tag{4}$$

Ovviamente, $C^\perp$ è un codice lineare, e se C è del tipo [n,k], allora $C^\perp$ è del tipo [n,n-k]. Se $C = C^\perp$, allora C si dice autoduale e n = 2k.

Si definisce *polinomio numeratore dei pesi di Hamming* di C il polinomio:

$$W_c(x,y) = \sum_i A_i x^{n-i} y^i = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \tag{5}$$

dove A_i è il numero di parole di codice di C con peso i.

Un codice si definisce *binario* se l'ordine del campo F su cui è definito è pari a due.

Teorema di MacWilliams per codici binari lineari – Se C è un codice binario lineare e $C^\perp$ è il suo codice duale, allora

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y) \tag{6}$$

dove $|C| = 2^k$ è il numero di parole di codice in C. Analogamente, si ha:

$$\sum_{k=0}^{n} A_k' x^{n-k} y^k = \frac{1}{|C|} \sum_{i=0}^{n} A_i (x+y)^{n-i} (x-y)^i \tag{7}$$

oppure anche:

$$\sum_{u\in C^{\perp}} x^{n-wt(u)} y^{wt(u)} = \frac{1}{|C|}\sum_{u\in C}(x+y)^{n-wt(u)}(x-y)^{wt(u)} \quad \textbf{(8)}$$

dove A_i' identifica il numero di parole di codice di peso i in $C^{\perp}$.

Le (6), (7) e (8) sono chiamate le *identità di MacWilliams*. Una dimostrazione del teorema sopra enunciato si può trovare in [2], capitolo 5.

2.1 Teoria dell'invarianza

Un codice *C* è *doppiamente pari* se, per ogni a in *C*, *wt(a)* è divisibile per 4. Se C è un codice auto-duale doppiamente pari di lunghezza n, dalle identità di MacWilliams segue che:

$$W_c(x,y) = \frac{1}{2^{n/2}} W_c(x+y, x-y) = W_c\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \quad \textbf{(9)}$$

Inoltre, poiché $W_c(x,y)$ coinvolge solo potenze di y^4, si ha che:

$$W_c(x,y) = W_c(x,iy) \quad \textbf{(10)}$$

Vogliamo ora trovare il numero di tutti i polinomi $W_c(x,y)$ che soddisfano la (9) e la (10).

Le due equazioni (9) e (10) mostrano che $W_c(x,y)$ è invariante se si operano le sostituzioni (trasformazioni lineari):

$$\mathrm{T}_1\colon (x,y) \to \left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \text{ e } \mathrm{T}_2\colon (x,y) \to (x,iy) \quad \textbf{(11)}$$

o, in notazione matriciale:

$$\mathrm{T}_1\colon \begin{pmatrix} x \\ y \end{pmatrix} \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \text{ e } \mathrm{T}_2\colon \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \quad \textbf{(12)}$$

$W_c(x,y)$ deve essere invariante anche per ogni combinazione (ad es. T_1^2, T_1T_2, $T_1T_2T_1$ ecc.) di queste trasformazioni. Le matrici $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ e $\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$, moltiplicate fra di loro in tutti i modi possibili, danno origine a un gruppo G_1 che contiene 192 matrici, ovvero il polinomio $W_c(x,y)$ è invariante sotto il gruppo:

$$G_1 = \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix} \right\rangle \qquad \textbf{(13)}$$

il cui ordine è 192.

Ora il nostro obiettivo è di trovare il numero dei polinomi $W_c(x,y)$ che sono invarianti per tutte le trasformazioni individuate dalle 192 matrici in G_1. Limitiamo il nostro studio agli invarianti omogenei (in cui tutti i termini hanno lo stesso grado) per semplificare il calcolo. Ricordando che se f e g sono invarianti, lo sono anche cf (con c costante moltiplicativa), f + g, f - g, fg, ecc., la domanda da porsi diventa: *quanti invarianti linearmente indipendenti omogenei ci sono per ogni grado d?* Denotiamo tale numero a_d. Un modo conveniente per rappresentare questi numeri è di combinarli in una serie di potenze:

$$\Phi(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 + \ldots \qquad \textbf{(14)}$$

A questo punto si invoca il *Teorema di Molien*, la cui dimostrazione può essere trovata in [2], capitolo 19.

Teorema di Molien – Per ogni gruppo finito G di matrici complesse m x m, $\Phi(\lambda)$ è dato da:

$$\Phi(\lambda) = \frac{1}{|G|}\sum_{A\in G}\frac{1}{\det(I - \lambda A)} \qquad \textbf{(15)}$$

dove $|G|$ è la cardinalità di G.

La serie $\Phi(\lambda)$ è detta *serie di Molien di G*. Per il gruppo G_1 precedentemente definito, dal teorema di Molien si ottiene:

$$\Phi(\lambda) = \frac{1}{192}\left\{\frac{1}{(1-\lambda)^2} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)(1-i\lambda)} + \ldots\right\} \qquad \textbf{(16)}$$

Se si calcolano tutti i termini della (16) si ottiene un risultato sorprendente:

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} \tag{17}$$

ovvero:

$$\Phi(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 + ... = (1+\lambda^8+\lambda^{16}+\lambda^{24}+...)(1+\lambda^{24}+\lambda^{48}+...) \tag{18}$$

Perciò si ha che $a_j = 0$ per tutti i j non multipli di 8; ovvero, il grado di un invariante omogeneo deve essere multiplo di 8. Inoltre, il risultato mostrato nella (18) è quello che si avrebbe se ci fossero due invarianti di base, di grado 8 e 24, tali che tutti gli altri si possano ottenere tramite somme e prodotti dei due.

In altre parole, il numero di polinomi omogenei linearmente indipendenti di ciascun grado è ottenuto per combinazione di due soli polinomi, uno di grado 8 e l'altro di grado 24. Il primo deriva dal codice di Hamming esteso H di tipo [8, 4, 4] con numeratore di pesi pari a:

$$W_H(x,y) = x^8 + 14x^4y^4 + y^8 \tag{19}$$

ed il secondo dal codice di Golay G di tipo [24, 12, 8] con numeratore di pesi:

$$W_G(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24} \tag{20}$$

L'importanza di questi due codici è dimostrata dal *teorema di Gleason*:

Teorema - Il polinomio numeratore di ogni codice auto-duale doppiamente pari binario è un polinomio in $W_H(x,y)$ e in $W_G(x,y)$

Anche in questo caso, la dimostrazione può essere trovata in [2], capitolo 19.

3 Costruzione di codici binari da grafi

Sia *G* un grafo privo di lati multipli (anche se può contenere anelli) e il suo insieme di nodi sia $S = \{1,\ 2,\ 3,\ ...n\}$; sia poi *C = c(i,j)* la sua matrice di adiacenza. Ricordiamo che la matrice di adiacenza di un grafo *G*, avente $\{v_1,\ v_2,\ ...\ v_n\}$ come insieme di nodi, si definisce come la matrice *A(G) = a(i,j)* dove:

$$a_{ij} = \begin{cases} 1, & \text{se } v_i \text{ e } v_j \text{ sono adiacenti} \\ 0, & \text{altrimenti} \end{cases} \qquad \textbf{(21)}$$

Denotiamo con *V(S)* lo spazio vettoriale n-dimensionale su *GF(2)* (campo di Galois di ordine 2) con base $B = \{v_i : i \in S\}$ e interpretiamo *C* come la matrice che descrive una trasformazione lineare da *V* a *V* rispetto a questa base. Si identifica ogni vettore in *V* con il sottoinsieme dei nodi di *G* al quale corrisponde. Siamo particolarmente interessati agli autospazi $V^{(\lambda)}$ di *C*, per $\lambda \in GF(2)$; $V^{(0)}$ corrisponde agli insiemi di nodi *X* per i quali ogni nodo di *G* è adiacente ad un numero pari di nodi in *X*, mentre $V^{(1)}$ consiste negli insiemi *X* per cui ogni nodo non in *X* è adiacente a un numero pari di nodi in *X* e ogni nodo di *X* è adiacente a un numero dispari di nodi in *X*.

Si definisce ora un grafo bipartito $\hat{G}$ che abbia il doppio dei nodi di *G* come segue:

1) I nodi sono 1, 2, …, n, $\bar{1}$, $\bar{2}$, …, $\bar{n}$;

2) i è connesso a $\bar{j}$ se e solo se i è adiacente a j in *G*, e queste sono le uniche adiacenze nel grafo.

Perciò $\hat{C}$, matrice di adiacenza di $\hat{G}$, ha la forma:

$$\hat{C} = \begin{pmatrix} 0 & C \\ C & 0 \end{pmatrix} \qquad \textbf{(22)}$$

I codici ai quali siamo particolarmente interessati sono quelli definiti dagli autospazi di $\hat{C}$ corrispondenti all'autovalore 1. Ovvero, cerchiamo i kernel di matrici che hanno la forma:

$$\hat{C} + I = \begin{pmatrix} I & C \\ C & I \end{pmatrix} \qquad \textbf{(23)}$$

Dal momento che C è simmetrica, si hanno le seguenti proprietà (denotando con ~ l'equivalenza delle righe):

$$\begin{aligned} rango(\hat{C}+I)=n \quad &\Leftrightarrow \quad (I \mid C) \approx (C \mid I) \\ &\Leftrightarrow \quad (C^{-1} \mid I) \approx (C \mid I) \\ &\Leftrightarrow \quad C^{-1}=C \\ &\Leftrightarrow \quad C^2=I \\ &\Leftrightarrow \quad CC^T=I \\ &\Leftrightarrow \quad (\hat{C}+I)(\hat{C}+I)^T=0 \end{aligned} \qquad \textbf{(24)}$$

Dalla teoria dei grafi la condizione $C^2 = I$ implica che:

(P1) *per ogni coppia di nodi di G, il numero di nodi adiacenti ad entrambi è pari, ed ogni nodo ha grado dispari*;

Perciò ogni grafo con questa proprietà dà origine a un codice binario auto-duale. Per assicurare che il codice risultante sia anche doppiamente pari, si richiede:

(P2) *ogni vertice di G ha grado congruente a 3 modulo 4*.

Esempio 1

Si consideri il grafo $G=K_4$. Ogni nodo ha grado 3 e ogni coppia di nodi ha solo due adiacenti in comune, perciò le proprietà P1 e P2 sono soddisfatte. In Figura 1 è mostrata la costruzione di $\hat{G}$ a patire da G.

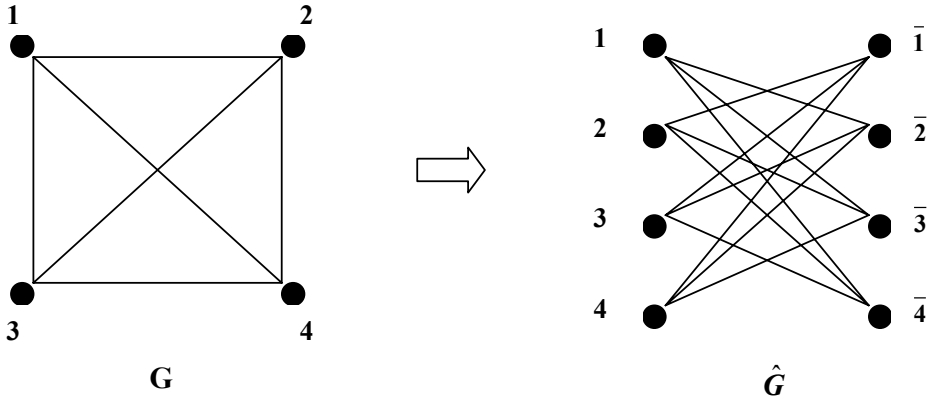


Figura 1 – Grafo G=K$_4$ e grafo corrispondente $\hat{G}$

Il codice risultante sarà binario, auto-duale e doppiamente pari; le parole di codice saranno del tipo: $\{i, j, k, l, \bar{i}, \bar{j}, \bar{k}, \bar{l}\}$ dove ogni elemento rappresenta un nodo di $\hat{G}$ e può assumere, naturalmente, valori pari a zero o uno.

In particolare, i bit pari ad uno delle parole di codice saranno dati dagli insiemi di nodi del tipo $\{X \mid \overline{Y}\}$, con X pari a un qualunque sottoinsieme di nodi di G e $\overline{Y}$ pari all'insieme dei nodi di $\hat{G}$ connessi ad un numero dispari di nodi di X. Come detto in precedenza, questo corrisponde a cercare gli autospazi della matrice di adiacenza di $\hat{G}$ corrispondenti all'autovalore 1 (sottoinsiemi di nodi X tali per cui ogni nodo non in X è adiacente a un numero pari di nodi in X e ogni nodo in X è adiacente a un numero dispari di nodi in X).

Considerando dunque il grafo $\hat{G}$ di Figura 1, gli insiemi di vertici corrispondenti agli uni delle parole di codice sono i seguenti (si utilizza la notazione $\{i, \ j, \ k, \ l\} = \{1, \ 2, \ 3, \ 4\}$):

$$\mathbf{0},$$
$$\{i, \ j, \ k, \ l, \ \bar{i}, \ \bar{j}, \ \bar{k}, \ \bar{l}\},$$
$$\{i, \ \bar{j}, \ \bar{k}, \ \bar{l}\} \text{ (e altri tre analoghi)},$$
$$\{j, \ k, \ l, \ \bar{i}\} \text{ (e altri tre analoghi)},$$
$$\{i, \ j, \ \bar{i}, \ \bar{j}\} \text{ (e altri cinque analoghi)}.$$

Se si utilizza la consueta notazione per i codici, l'alfabeto del codice risultante sarà dunque formato dalle seguenti parole:

$$\begin{bmatrix}0&0&0&0&0&0&0&0\end{bmatrix}$$
$$\begin{bmatrix}1&1&1&1&1&1&1&1\end{bmatrix}$$
$$\begin{bmatrix}1&0&0&0&0&1&1&1\end{bmatrix}$$
$$\begin{bmatrix}0&1&0&0&1&0&1&1\end{bmatrix}$$
$$\begin{bmatrix}0&0&1&0&1&1&0&1\end{bmatrix}$$
$$\begin{bmatrix}0&0&0&1&1&1&1&0\end{bmatrix}$$
$$\begin{bmatrix}0&1&1&1&1&0&0&0\end{bmatrix}$$
$$\begin{bmatrix}1&0&1&1&0&1&0&0\end{bmatrix}$$
$$\begin{bmatrix}1&1&0&1&0&0&1&0\end{bmatrix}$$
$$\begin{bmatrix}1&1&1&0&0&0&0&1\end{bmatrix}$$
$$\begin{bmatrix}1&1&0&0&1&1&0&0\end{bmatrix}$$
$$\begin{bmatrix}1&0&1&0&1&0&1&0\end{bmatrix}$$
$$\begin{bmatrix}1&0&0&1&1&0&0&1\end{bmatrix}$$
$$\begin{bmatrix}0&1&1&0&0&1&1&0\end{bmatrix}$$
$$\begin{bmatrix}0&1&0&1&0&1&0&1\end{bmatrix}$$
$$\begin{bmatrix}0&0&1&1&0&0&1&1\end{bmatrix}$$

Il codice risultante è il codice di Hamming esteso del tipo [8,4], che si ottiene dal consueto codice di Hamming [7,4] aggiungendo un bit di parità "totale". L'Hamming [7,4] è un codice sistematico in cui i primi quattro bit delle parole di codice sono uguali ai bit di informazione e le tre cifre di parità si ottengono da questi ultimi con le regole seguenti [5] (notazione: p sta per parità, i per informazione):

$$\begin{aligned} p_1 &= i_2 + i_3 + i_4 \\ p_2 &= i_1 + i_3 + i_4 \\ p_3 &= i_1 + i_2 + i_4 \end{aligned} \qquad \textbf{(25)}$$

Perciò si può interpretare il grafo bipartito $\hat{G}$ come segue. I nodi di destra rappresentano i bit di informazione; i nodi di sinistra rappresentano invece i bit di parità. I lati indicano il modo in cui le cifre di parità dipendono dai bit di informazione, ed infatti ricalcano le regole definite in (25); è da notare come il quarto bit di parità, oltre che come bit di parità totale, possa essere trovato secondo la regola:

$$p_4 = i_1 + i_2 + i_3 \qquad \textbf{(26)}$$

Esempio 2.

Sia ora G il grafo dell'icosaedro, mostrato in Figura 2.

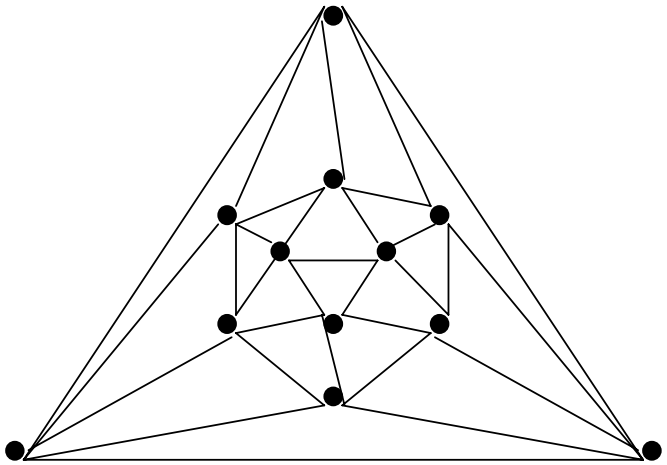


Figura 2 – Grafo planare dell'icosaedro.

Si può subito notare come non soddisfi alla proprietà (P2); tuttavia, è facilmente verificabile che, per ogni coppia di nodi, ci sono o esattamente due nodi adiacenti a entrambi oppure non ve ne è nessuno. Perciò la proprietà (P1) è verificata; a partire da

questo grafo è possibile ricavare un codice binario auto-duale, anche se non doppiamente pari.

Il codice *C* risultante ha 2×12 parole di peso 6, che corrispondono, seguendo lo stesso criterio dell'esempio precedente e con la notazione $S = \{1, \ 2, \ \ldots \ 12\}$, $\overline{S} = \{\overline{1}, \ \overline{2}, \ \ldots \ \overline{12}\}$, ad un nodo di S (o di $\overline{S}$) e ai cinque nodi di $\overline{S}$ (o di S) ad esso adiacenti in $\hat{G}$. Inoltre, ci sono altre 20×2 parole di peso 6, che corrispondono a tre nodi formanti un triangolo T da un lato e ai tre nodi adiacenti ad uno solo di T dall'altro. Si può dimostrare che queste 64 parole di codice sono le uniche di peso 6 e che non ve ne sono altre.

Come già detto, questo grafo non dà origine ad un codice doppiamente pari, dal momento che i nodi hanno grado 5. Peraltro, il grafo complementare di *G* soddisfa entrambe le proprietà (P1) e (P2) e quindi il codice risultante è auto-duale e doppiamente pari. Ricordiamo che il grafo complementare $\overline{G}$ di *G* è il grafo avente lo stesso insieme di nodi di *G* ma nel quale due nodi sono adiacenti solo se non lo sono nel grafo di partenza. Il complementare del grafo dell'icosaedro, in particolare, origina il codice di Golay di cui si è parlato in precedenza.

4 Enumerazione dei codici derivanti da grafi

Da quanto esposto fino ad ora si può evincere come alcuni dei codici binari auto-duali doppiamente pari più interessanti si possono ricavare da grafi con determinate caratteristiche; inoltre, quando questa possibilità è verificata, essa rappresenta un modo molto semplice e conveniente di studiare il codice.

Peraltro, sembra naturale chiedersi se questo metodo sia o meno applicabile alla maggior parte dei codici auto-duali doppiamente pari; in altre parole, ci si domanda se esiste un metodo che consenta di valutare se un determinato codice è ottenibile da un grafo nel modo sopra descritto oppure no. La risposta a questa domanda è data dal seguente teorema, nel quale, con il termine *involuzione* si intende una permutazione senza punti fissi che scambia gli elementi a due a due. Ricordiamo inoltre che un automorfismo di un grafo *G* è una funzione bijettiva ϕ dall'insieme dei nodi *V(G)* in se stesso tale che, dati due nodi v e w, $\phi(v)$ e $\phi(w)$ sono adiacenti se e solo se lo sono v e w. Gli automorfismi di *G* formano un gruppo detto il *gruppo di automorfismi di G*, $\Gamma(G)$.

Teorema - Un codice binario auto-duale è equivalente (tramite permutazione dei vettori che compongono la sua base) ad uno ottenuto da un grafo (secondo quanto esposto sopra) se e solo se il suo gruppo di automorfismi contiene una involuzione.

La dimostrazione che segue si trova in [1] e la sua generalizzazione al caso non binario in [3].

Dimostrazione – Supponiamo che il codice C abbia una matrice generatrice della forma (**I** | **C**) dove **C** è simmetrica e $\mathbf{C}^2 = \mathbf{I}$. Allora si ha:

$$(\mathbf{I} \mid \mathbf{C}) \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = (\mathbf{C} \mid \mathbf{I}) \sim (\mathbf{I} \mid \mathbf{C}^{-1}) \sim (\mathbf{I} \mid \mathbf{C}) \tag{27}$$

Perciò la matrice preserva il codice e corrisponde ad una permutazione senza punti fissi dei vettori base.

Sia poi C un codice binario auto-duale di dimensione n e lunghezza $2n$, con base $\{v_1, \ v_2, \ \ldots \ v_{2n}\}$. Inoltre, sia α la trasformazione lineare dello spazio vettoriale indotta dalla permutazione $\pi = (1,2)(3,4)\ldots(2n\text{-}1,2n)$ che agisce sui vettori della base, e supponiamo che C sai preservato da α. Dobbiamo dimostrare che è possibile produrre un insieme di vettori $\{u_1, \ u_2, \ \ldots \ u_n\}$, con $u_i \in \{v_{2i-1}, \ v_{2i}\}$, tale che:

$$\langle u_1, \ u_2, \ \ldots \ u_n \rangle \cap C = 0 \tag{28}$$

(La (28) significa che è possibile assegnare zeri e uni casualmente nelle n posizioni considerate; vi è però una sola parola di codice corrispondente alla scelta effettuata. In particolare, c'è una unica parola di codice con un uno in posizione k e zeri nelle altre n-1 posizioni identificate dalla (28); il nodo k nel grafo $\hat{G}$ sarà adiacente ai nodi corrispondenti agli uni nelle altre n posizioni non comprese nella (28)).

Certamente $v_1 \notin C$ dal momento che $v_v \cdot v_1 = 1 \neq 0$, perciò scegliamo $u_1 = v_1$. Ora si suppone che si sia scelto $\{u_1, \ u_2, \ \ldots \ u_m\}$ tale che:

$$\langle u_1, \ u_2, \ \ldots \ u_m \rangle \cap C = 0 \tag{29}$$

ma che:

$$\langle u_1, \ u_2, \ \ldots \ u_m, \ v_{2m+1} \rangle \cap C \neq 0 \neq \langle u_1, \ u_2, \ \ldots \ u_m, \ v_{2m+2} \rangle \cap C \tag{30}$$

Sia:

$$u = \sum_{i=1}^{m} \lambda_i u_i + v_{2m+1} \in C; \qquad v = \sum_{j=1}^{m} \mu_j u_j + v_{2m+2} \in C \tag{31}$$

dove $\lambda_j, \mu_j \in F$ and $\alpha(v_{2m+1}) = v_{2m+2}$. Allora:

$$\alpha(u) \cdot v = v_{2m+2} \cdot v_{2m+2} = 1 \neq 0 \tag{32}$$

Questo contraddice il fatto che $\alpha(u)$ e v sono entrambi vettori del codice auto-duale *C*. perciò l'insieme di vettori linearmente indipendente può essere trovato e come base dello spazio vettoriale si sceglie:

$$\{u_1, \quad u_2, \quad \ldots \quad u_n, \quad \alpha(u_1), \quad \alpha(u_2), \quad \ldots \quad \alpha(u_n)\} \qquad \textbf{(33)}$$

che è semplicemente una permutazione della sua base originale.

Ora si sceglie una matrice generatrice del codice rispetto a questa base e la si riduce in modo da ottenere:

$$(\mathbf{I} \mid \mathbf{C}) \sim \alpha(\mathbf{I} \mid \mathbf{C}) \sim (\mathbf{C} \mid \mathbf{I}) \sim (\mathbf{C}^{-1} \mid \mathbf{I}) \qquad \textbf{(34)}$$

Ma essendo **C** auto-duale $\mathbf{C}\mathbf{C}^T = 1$, e quindi $\mathbf{C} = \mathbf{C}^{-1} = \mathbf{C}^T$. Perciò **C** è simmetrica, come richiesto. CVD

I codici auto-duali binari hanno generalmente grandi proprietà di simmetria, in modo particolare quando sono doppiamente pari, ed è stato dimostrato che tutti i codici di questo tipo di lunghezza non superiore a 24 posseggono un automorfismo del tipo sopra descritto. L'argomento è molto studiato e si è visto che questo è valido anche per quasi tutti i codici binari auto-duali doppiamente pari di lunghezza 32 [4].

Tutti i grafi aventi un numero di nodi pari a 4, 8 o 12 che soddisfano le proprietà (P1) e (P2) sono stati elencati nel corso di uno studio (sono risultati 28 in tutto); le loro proprietà sono state tabulate e si sono indicati i codici componenti del codice risultante. Ricordiamo che è possibile costruire un codice avente un alfabeto più ampio a partire dalla somma di codici più semplici, detti codici componenti, e aggiungendo parole addizionali chiamate "*collante*".

5 Esempi di grafi con le proprietà desiderate

Nel seguito (Figura 5) verranno elencati i grafi aventi un numero di vertici pari a 4 e a 8 che soddisfano le proprietà (P1) e (P2). La notazione usata è la seguente: i cerchi più grandi rappresentano orbite del gruppo di automorfismi del grafo, con il numero dei nodi che contengono; le linee e i cerchi più piccoli rappresentano lati tra queste orbite.

Ad esempio, il grafo dell'icosaedro (Figura 2) è mostrato in Figura 3

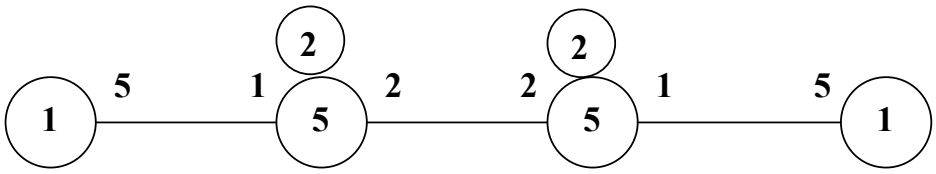


Figura 3 – Icosaedro

Analogamente, il grafo G_3 in Figura 5 rappresenta quello mostrato in Figura 4 ($3K_2*K_2$).

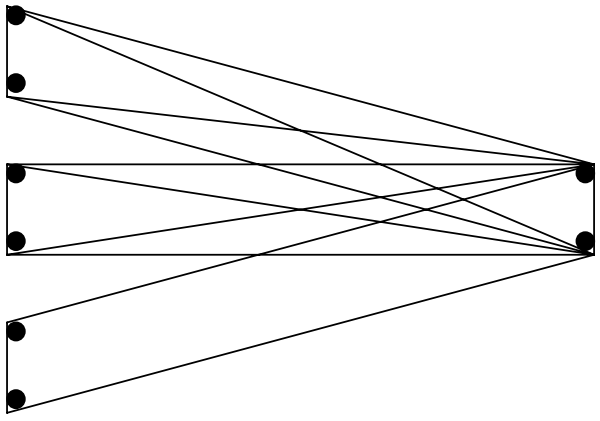
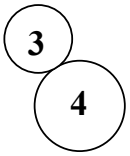
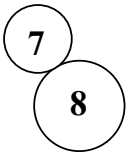


Figura 4 – Grafo 3K2*K2

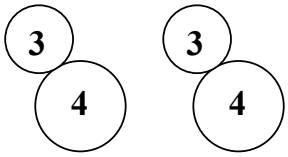


$G_1=K_4$

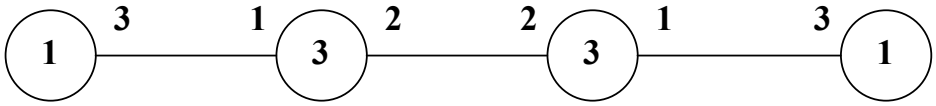


$G_2=K_8$

$G_3=3K_{2^*}\ K_2$



$G_4=2K_4$



G_5=the cube Q_3

Figura 5 – Grafi di 4 e 8 vertici che danno origine a codici binari auto-duali doppiamente pari di lunghezza 8 e 16.

Bibliografia

[1] L. Beineke, R. Wilson, *Graph Connections*, Oxford University Press, 1997.

[2] F. J. MacWilliams, N. J. A. Sloane*, The theory of error correcting codes*, North Holland, 1977.

[3] R. T. Curtis, *On graphs and codes*, Geom. Dedicata 41 (1992), 127-134.

[4] J. H. Conway, V. Pless, *On the enumeration of self-dual codes*, J. Combin. Theory (A) 28 (1980), 26-53.

[5] S. Bellini, *Teoria dell'informazione e codici*, to be published.