Torino, 22 novembre 2000

Automi cellulari invertibili

Autore: Pierre Blanc

Gli automi cellulari nascono dalle ricerche di von Neumann e Ulam, poi sviluppate da Wolfram.

La proprietà fondamentale degli automi cellulari è che la trasformazione globale associata può sempre essere localizzata, e questo è utile dal punto di vista computazionale: per ottenere un risultato veloce con il calcolatore è sufficiente far eseguire in parallelo le trasformazioni locali.

Le applicazioni più frequenti sono per la crittografia, ma gli automi cellulari si usano spesso anche in simulazioni di gas. E' noto dalla termodinamica che le trasformazioni che entrano in gioco sono microscopicamente reversibili ma macroscopicamente irreversibili. Per simulare il comportamento di un gas con gli automi cellulari bisogna trovare un'appropriata trasformazione reversibile e applicarla ripetutamente alla griglia dell'automa.

In questa sede verranno analizzate le trasformazioni invertibili di automa cellulare, che formano un gruppo, limitandosi agli automi 1-dimensionali di lunghezza finita.

Le caratteristiche fondamentali degli automi cellulari sono: località, omogeneità, parallelismo, tempo discreto. Le unità fondamentali degli automi sono le celle (o cellule).

Località: data una cella con un intorno contenente altre celle, questa scambia informazioni solo con le celle dell'intorno.

Omogeneità: la cella si evolve con la legge di transizione locale f nel tempo

$t=0,1,2,\ldots, \in \mathbf{N}^{\,t \mapsto t+1}$

Al tempo t, la cella C è in uno stato C(t) e passa allo stato $C(t+1)=f(D_0(t), D_1(t), \ldots, D_s(t))$, dove $D_0, D_1, \ldots, D_s$ sono le celle dell'intorno di C.

C'è una struttura topologica data dagli intorni. Chiamo *I* la funzione d'intorno.
$\forall C \in C \; \exists I(C) \subseteq C$

L'insieme degli stati è *A* con | *A* |=q. $\forall t \in N \; \exists C(t) \in A$

La funzione di transizione locale f è tale che $C(t+1) = f(D_0(t),\ldots,D_s(t))$ dove *I*(C)=$\{D_j\}$

Parallelismo: passando da t a t+1 si aggiornano simultaneamente gli stati di tutte le celle.

Una legge locale è una funzione tra l'insieme di tutte le configurazioni locali e *A*.
Esistono $|A|^{|\text{conf loc}|} = q^{q^{|I(C)|}}$ leggi locali.

ES.: Automi unidimensionali finiti. Ho un insieme di n celle:

□ □ □ □ □
1 ··· i−1 i i+1 ··· n

Definiamo un intorno. Il più semplice è quello di raggio 1. Se numeriamo le celle (c_i è la cella i-esima) allora l'intorno di raggio 1 di c_i è:

$$I(c_i) = \{c_{i-1}, c_i, c_{i+1}\}$$

Quindi la legge di transizione locale ha solo 3 argomenti:

$$c_i(t+1) = f(c_{i-1}(t), c_i(t), c_{i+1}(t))$$

Se $A = Z_2 = \{0,1\}$ abbiamo gli automi binari.

In questo caso le configurazioni locali, e quinidi i possibili intorni, sono $q^{|I(c)|} = 2^3 = 8$

Una legge assegna il valore della cella al tempo t+1 a seconda del suo intorno. Per esempio (legge 90 di Wolfram):

n_I	7	6	5	4	3	2	1	0
$I(c_i)$	111	110	101	100	011	010	001	000
$c_i(t+1)$	0	1	0	1	1	0	1	0

Gli intorni, scritti come nella tabella, possono essere visti come numeri in base q=2 tra 0 e $2^3 - 1$=7. A loro volta le leggi vengono numerate tra 0 e $2^{2^3} - 1$=255 con la formula:

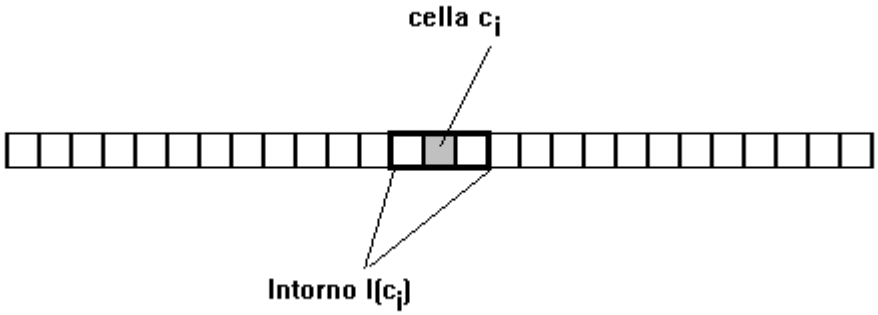
$$\text{numero della legge} = \sum_{I \in I} 2^{n_I} \cdot c_i(t+1)$$

In questo caso 90=64+16+8+2

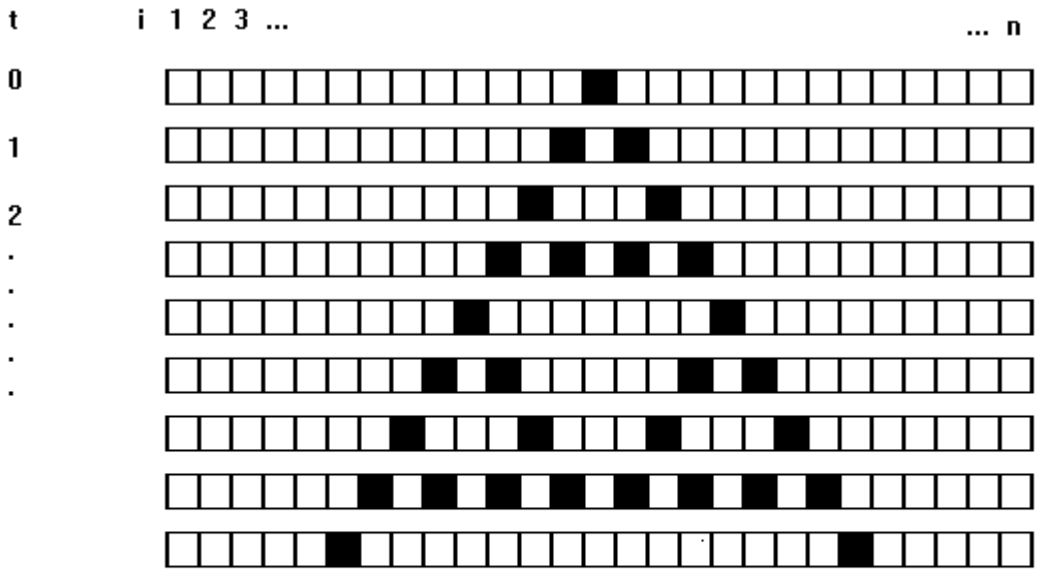
Esempio:

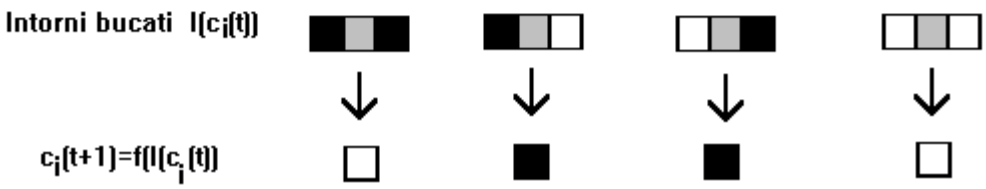
Automa unidimensionale con 2 colori di lunghezza n

Intorno di raggio 1



Evoluzione con legge 90 di Wolfram:





Wolfram ha classificato quattro tipi di evoluzione per automi cellulari finiti:

1) l'automa arriva sempre ad uno stato stazionario a partire da qualsiasi condizione iniziale.

2) l'automa giunge ad un ciclo, che può essere diverso a seconda della condizione iniziale.

3) l'automa è caotico. Per qualsiasi condizione iniziale arriva a ripetere stati dove certe condizioni appaiono distribuite a caso.

4) l'automa è sensibile alle condizioni iniziali e giunge a situazioni che presentano un alto grado di ordine e al tempo stesso complessità.

Sia K un anello. Dato un automa cellulare (CA) di lunghezza n con coefficienti in K consideriamo il gruppo $S_{K^n}:\left\{\sigma: K^n \to K^n\right\}$ con σ biettiva. Sono leggi di transizione globali di automa cellulare solo quelle $\sigma \in S_{K^n}$ indotte da una legge locale. Consideriamo il gruppo delle leggi globali di CA invertibili $A_n(K) \leq S_{K^n}$. Il nostro scopo è determinare A_n.

Sia T il morfismo

$$\begin{cases} T: G \to S_X \\ T: g \mapsto T(g) \end{cases}$$

$$\begin{cases} T(g): X \to X \\ T(g): a \mapsto T(g)(a) \end{cases}$$

Si ha $T(G) \leq S_X$; inoltre le T(g) sono biezioni. T(G) è quindi una rappresentazione permutazionale di G.

$G \cong T(G) \Leftrightarrow T \text{ è iniettiva} \Leftrightarrow \operatorname{Ker} T = \left\{1_G\right\}$. Si dice anche che T è fedele. Studiamo in dettaglio l'azione T.

1) L'orbita di $a \in X$ è $O_T(a) = O(a) := \left\{T(g)(a): g \in G\right\} \subseteq X$

2) Lo stabilizzatore di $a \in X$ è $\operatorname{Stab}_T(a) = \operatorname{Stab}(a) := \left\{g \in G: T(g)(a) = a\right\} \subseteq G$

3) Il fissato da $g \in G$ è $\operatorname{Fix}_T(g) = \operatorname{Fix}(g) := \left\{a \in X: T(g)(a) = a\right\} \subseteq X$

PROP.: $\operatorname{Stab}(a) \leq G$

$a \sim_T b \Leftrightarrow \exists g \in G : T(g)(a) = b \ (b \in O_T(a))$

PROP.: $\sim_T$ è una relazione di equivalenza.

COROLL.: Poiché O(a) è la classe di equivalenza [a] , l'insieme delle orbite è una partizione di X.

PROP.: |O(a)|=[G:Stab(a)]

PROP.: T è un'azione di H su A

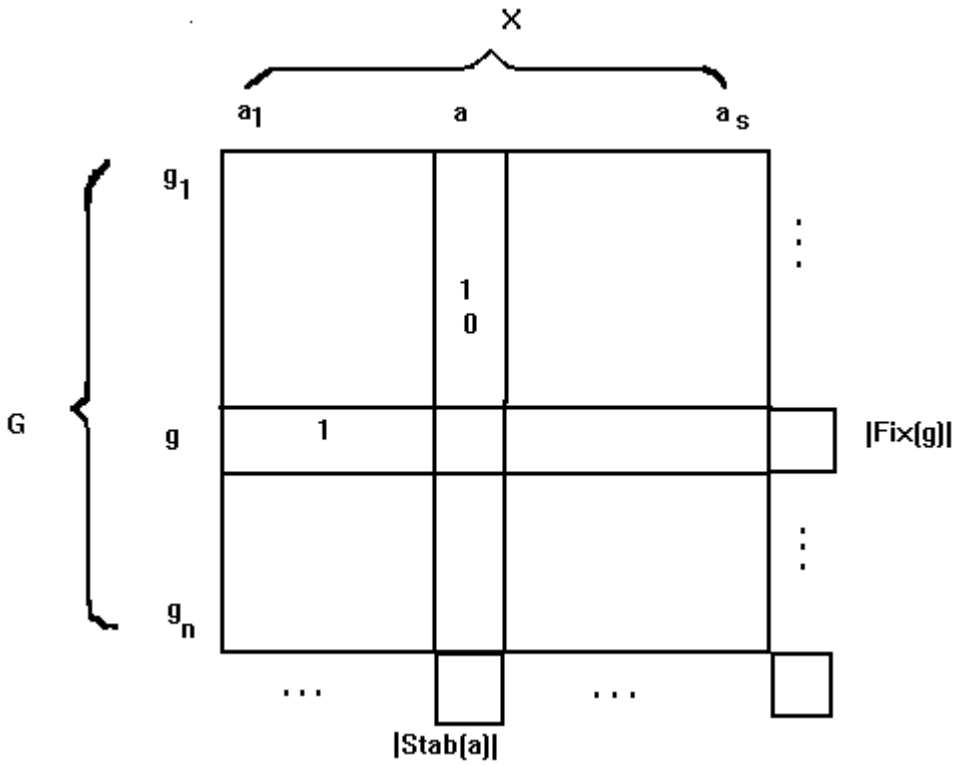
Dim.:

PROP.: Nell'azione di $a \in X$ ci sono $\tau(n)$ orbite, dove $\tau(n)$ è il numero dei divisori di n.

Dim.: Dato d|n , $O(d)=\{a \in Z_n | (a,n) = d\}$. $b \in O(a) \Rightarrow \exists h \in Z_n^* | ha = b$, ma (ha,n)=(a,n), quindi (a,n)=(b,n).

LEMMA DI BURNSIDE: Sia T un'azione di G su X. Allora il numero delle orbite= $\frac{1}{|G|}\sum_{g \in G}|Fix(g)|$

Dim.:



La tabella è stata costruita in modo che si trovi 1 se T(g)(a)=a, altrimenti si trova 0. Sommando gli elementi della colonna corrispondente ad a si ottiene |Stab(a)|, mentre sommando gli elementi della riga corrispondente a g si ottiene |Fix(g)|.

Si ha:

$$N=\sum_{a\in X}|\mathrm{Stab}(a)|=\sum_{g\in G}|\mathrm{Fix}(g)|$$

dove N è il numero di 1 nella tabella.

Usiamo la proprietà $|O(a)|=[G:\mathrm{Stab}(a)]=\frac{|G|}{|\mathrm{Stab}(a)|}$, segue

$$\sum_{a\in X}\frac{|G|}{|O(a)|}=\sum_{g\in G}|\mathrm{Fix}(g)| \quad \text{quindi} \quad \sum_{a\in X}\frac{1}{|O(a)|}=\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

Ma il primo termine è proprio il numero delle orbite, quindi si ottiene l'enunciato.

TEOR. (KESAVA-MENON): $\tau(n)\varphi(n)=\sum_{(h,n)=1}(h-1,n)$

Dim.: Usiamo il lemma di Burnside: $\tau(n)=\frac{1}{|H|}\sum_{h\in H}|\mathrm{Fix}(h)|$ con $H=Z_n^*$. $|Z_n^*|=\varphi(n)$.

$h\in Z_n^* \Leftrightarrow (h,n)=1$. $\mathrm{Fix}(h)=\{a\in Z_n^* | ha=a\}$ ma

$ha=a \bmod n \Leftrightarrow ha-a=0 \bmod n \Leftrightarrow a(h-1)=0 \bmod n$ congruenza lineare modulo n che ha

(h-1, n) soluzioni. Quindi |Fix(h)|=(h-1,n), sostituendo nel lemma di Burnside si ottiene l'enunciato.

LEMMA: $\sum_{j=0}^{v}(-1)^j\binom{v}{j}=0$

Dim.: E' la formula del binomio per $(1-1)^v=0$

DEF.: Funzione μ di Moebius.

$\mu(1)=1$,

n>1, $n=p_1^{k_1}\dots p_s^{k_s}$, $\begin{cases}\text{se } \exists j: k_j>1 \Rightarrow \mu(n)=0 \text{ (non è square free)}\\ \text{se } \forall j\ k_j=1 \Rightarrow \mu(n)=(-1)^s\end{cases}$

PROP.: $\sum_{d|m}\mu(d)=0$

TEOR.: Legge di inversione di Moebius.

Date f,g definite sui naturali positivi $\forall m, g(m)=\sum_{d|m}f(d) \Leftrightarrow \forall m, f(m)=\sum_{d|m}\mu(d)g\left(\frac{m}{d}\right)$

Dim.: $\Rightarrow$) Utilizziamo la seguente osservazione:

OSS.: $d|m \wedge e|\frac{m}{d} \Leftrightarrow e|m \wedge d|\frac{m}{e}$

Dim.: $\Rightarrow$) $\frac{m}{d}=he \Rightarrow m=hed \Rightarrow e|m \Rightarrow \frac{m}{e}=hd \Rightarrow d|\frac{m}{e}$

$\Leftarrow$) Il viceversa si ottiene scambiando e con d.

$$\sum_{d|m}\mu(d)g\left(\frac{m}{d}\right)=\sum_{d|m}\mu(d)\sum_{e|\frac{m}{d}}f(e)=\sum_{d|m}\sum_{e|\frac{m}{d}}\mu(d)f(e)=\sum_{e|m}\sum_{d|\frac{m}{e}}\mu(d)f(e)$$

Ora, per n>1 è sempre $\sum_{d|m}\mu(d)=0$, quindi è sempre $\sum_{d|\frac{m}{e}}\mu(d)$ =0, tranne che nel caso $\frac{m}{e}=1$ cioè m=e, dove vale 1. Dunque rimane solo il termine $1\cdot f(m)=f(m)$

Studiamo l'azione dello shift sugli anelli con n elementi.

$|<\rho>|=n$, $<\rho> \cong C_n = \text{gruppo moltiplicativo} = \{\rho, \rho^2, \ldots, \rho^n = 1\} \cong Z_n$

Vogliamo calcolare quante orbite ci sono con un certo numero di elementi: $\begin{cases} C_n \to Z_n \\ \rho^k \mapsto [k]_n \end{cases}$

Consideriamo l'azione di C_n su X. Allora l'orbita $O((c_1,\ldots,c_n)) := \{\rho^k(c_1,\ldots,c_n)\}_k$

Se ho 2 colori si ritrovano gli automi cellulari binari.

Posto $\tau = (c_1,\ldots,c_n)$ si può verificare che $|O(\tau)| \mid n$. Infatti, data una azione T di G su X:

$\forall x \in X$, $|O(x)|=[G:\text{stab}(x)]=\frac{|G|}{|\text{stab}(x)|} \Rightarrow |O(x)| \mid |G|=n$ (infatti $G=C_n$).

Inoltre dato d | n, allora c'è sempre almeno un'orbita che contiene d collane: sia $q \geq 2$; (10...010...0.....10....0) d blocchi lunghi n/d. Se faccio uno shift ho che tutti i blocchi si trasformano nello stesso modo e dopo d passi si torna al punto di partenza. In questa orbita ci sono d collane.

DEF.: $\omega(d)$:=numero di orbite con d elementi

Allora ogni collana è in una sola orbita (partizione).

Si consideri $\sum_{d|n} d\omega(d) = q^n$.

Usando la formula di inversione di Moebius dove $g(m)=q^m$ e $f(n)=n\omega(n)$:

$$n\omega(n) = \sum_{d|n} \mu(d) q^{n/d} \Rightarrow \omega(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$$

Il numero totale delle orbite è $\sum_{d|n} \omega(d) = \sum_{d|n} \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e}$

Le trasformazioni globali appartengono all'insieme $\{F: K^n \to K^n\} = K^{n K^n}$

mentre le trasformazioni locali all'insieme $\{F: K^n \to K\}$

Consideriamo intorni completi di lunghezza n. Le leggi vanno estese a questo caso con la

relazione

num. legge nuovo= $F_n = \text{num.legge} \cdot (2^{2^n} + 1)$

I è l'operatore di intorno; data la configurazione $a = (a_0,\ldots,a_{n-1})$

I(a_0)=$a = (a_0,\ldots,a_{n-1})$, $I(a_1) = (a_1,\ldots,a_{n-1},a_0) = \alpha \cdot a$ (α è lo shift)

$I(a_2) = \alpha^2 a,\ldots,I(\alpha_k) = \alpha^k a$

Una F globale $F:K^n \to K^n$ è una legge di automa cellulare se $\exists f \text{locale } f\ K^n \to K$:
$\forall a \in K^n\ F(a) = (f(I(a_0),f(I(a_1),\ldots,f(I(a_{n-1}))$ cioè (*) $\forall a\ F(a) = (f(a),f(\alpha a),\ldots,f(\alpha^{n-1}a))$

TEOR.:Una $F \in K^{n^{K^n}}$ è legge di CA $\Leftrightarrow \alpha \circ F = F \circ \alpha$ (commuta con l'operatore di shift)

Dim.: $\Rightarrow$) Per ipotesi esiste una funzione locale f tale che vale (*). Allora
$\alpha \circ F(a) = \alpha\left(f(a),f(\alpha a),\ldots,f(\alpha^{n-1}a)\right) = \left(f(\alpha a),f(\alpha^2 a),\ldots,f(\alpha^{n+1}a),f(a)\right) =$
$= F(a_1a_2\ldots a_{n-1}a_0) = F(\alpha a) = F \circ \alpha(a)$

$\Leftarrow$) La F si può sempre scrivere così $F(a) = \left(F_0(a),F_1(a),\ldots,F_{n-1}(a)\right)$ dove le F_i sono le trasformazioni locali $F_i : K^n \to K$

$$K^n \xrightarrow{F} K^n \xrightarrow{\Pi_i} K$$

Prendo $a \in K^n$ $\alpha(F_0(a),F_1(a),\ldots,F_{n-1}(a)) = F \circ \alpha(a) = F(\alpha a) = \left(F_0(\alpha a),F_1(\alpha a),\ldots,F_{n-1}(\alpha a)\right)$

$F_1(a) = F_0(\alpha a)$ $F_2(a) = F_1(\alpha a) = F_0(\alpha(\alpha a)) = F_0(\alpha^2 a)$ e in genere

$F_k(a) = F_0(\alpha^k a)$

$F_0(a) = F_{n-1}(\alpha a) \Rightarrow F_0(\alpha^{n-1}a) = F_{n-1}(a)$ $F(a) = \left(F_0(a),F_0(\alpha a),\ldots,F_0(\alpha^{n-1}a)\right)$

E' vera la tesi con $f = F_0$.

PROP.:CA(n) è chiuso rispetto al composto.

PROP.: $\forall F \in CA(n),\forall a \in K^n, F(O(a)) \subseteq O(F(a))$

(CA(n),°) è un monoide. $(CA(n)^*,\circ) = G_n$ gruppo degli invertibili.

COROLL.: se $F \in G_n \Rightarrow F(O(\bar{a})) = O(F(\bar{a}))$ (immediato)

OSS.: F manda un'orbita di lunghezza d in un'altra di lunghezza d $\Rightarrow$ E' una permutazione sulle orbite di lunghezza d.

Consideriamo un automa cellulare con q simboli, di lunghezza n. Ci sono in tutto q^n configurazioni globali. L'insieme dei simboli in Z_q è $\{0,1,..,q-1\}$. Indichiamo con a il contenuto di una cella, con a preso tra i q simboli. Una configurazione globale si può rappresentare con un numero tra 0 e q^n -1, scritto in base $q \geq 2$: $a_0 + a_1 q + a_2 q^2 + ... + a_{n-1} q^{n-1}$

Studiamo ora l'azione di <q> su Z_{q^n-1}.

$$R_{q^n-1} = Z[x] \Big/ (x^{q^n-1} - 1)$$

L'effetto dello shift corrisponde all'effetto della moltiplicazione per x in R_{q^n-1}.

Infatti:

$$qc \bmod q^n - 1 = q(a_0 + a_1 q + ... + a_{n-1} q^{n-1}) \bmod q^n - 1 =$$
$$= a_0 q + a_1 q^2 + ... + a_{n-2} q^{n-1} + a_{n-1} q^n \bmod q^n - 1 =$$
$$= a_{n-1} + a_0 q + ... + a_{n-2} q^{n-1}$$

Il risultato è il numero che corrisponde alla configurazione $a_{n-1} a_0 \cdots a_{n-2}$, cioè esattamente la configurazione di partenza shiftata di 1.

Le orbite dello shift nell'insieme X delle configurazioni globali con q simboli e lunghezza n sono i laterali ciclotomici (più uno).

OSS.: In X queste orbite sono distinte: (00...0)$\rightarrow$ 0

(11...1)$\rightarrow$ $q^n - 1$

Invece 0=$q^n - 1$ mod $q^n - 1$, quindi due orbite distinte corrispondono allo stesso elemento in R_{q^n-1}.

$\Rightarrow$ num. orbite = num. laterali +1

Studiamo ora l'azione di <q> su Z_{q^n-1}.

Se $H \le Z_m^*$ agisce su $Z_m \Rightarrow$ n° orbite=$\frac{1}{|H|}\sum_{h\in H}(h-1,m)$

Applicandolo abbiamo <q>=

$H \le Z_{q^n-1} \Rightarrow n°\text{lat.ciclot.} = \frac{1}{n}\sum_{k=0}^{n-1}(q^k-1,q^n-1)$ $(H=\{q^0,q^1,\dots,q^{n-1}\})$ $\Rightarrow$ n° di orbite dello shift= $\frac{1}{n}\sum_{k=0}^{n-1}(q^k-1,q^n-1)+1$

Sia ora $G_n(q)$ il gruppo delle trasformazioni globali invertibili con q simboli e lunghezza n.

$F\in G_n(q)$: 1) F permuta tra loro le orbite della stessa lunghezza d (d | n)

2) F commuta con lo shift (α) (si deve determinare l'immagine tramite F di un elemento di un orbita per ogni orbita)

Una matrice P di permutazione è una matrice quadrata a coefficienti in Z_2 che contiene uno e un solo 1 per ogni riga e per ogni colonna: P rappresenta la permutazione che manda i in j dove i è la i-esima riga e j la j-esima colonna tali che P(i,j)=1.

$P=\{P \mid P \text{ è di permutazione nxn}\}$ con il prodotto di matrici è isomorfo a S_n.

Per definire $F\in G_n$ devo decidere una permutazione tra le orbite e per ogni orbita devo scegliere l'immagine del rappresentante. La matrice P è rappresentata da sottomatrici circolanti e diagonali a blocchi.

$G_n(q)$: sono fondamentali i divisori d|n. Abbiamo ω (d) orbite di lunghezza d. Se $F\in G_n(q) \Rightarrow$ F è una permutazione delle q^n configurazioni globali che si rappresentano con numeri interi tra 0 e q^n-1 scritti in base q. Ogni orbita è rappresentata dal suo minimo. Gli elementi dell'orbita O(s) sono nell'ordine s=min O(s), qs $\bmod(q^n-1)$, q^2s $\bmod(q^n-1)$, ..., q^{d-1}s $\bmod(q^n-1)$ (|O(s)|=d).

Le orbite sono ordinate secondo la grandezza del rappresentante (tra quelle con la stessa lunghezza). F è rappresentata da una matrice permutazionale $q^n \times q^n$ dove le colonne e le righe seguono l'ordine detto. I blocchi delle orbite di lunghezza d sono ordinati secondo d crescente.

I blocchi delle orbite di lunghezza d formano una sottomatrice C (dω (d)xdω (d)).

C ha una "forma" che è una matrice di permutazione ω (d)xω (d), cioè al posto i,j

$1 \le i, j \le \omega(d)$ c'è 1 se la i-esima orbita va nella j-esima.

Ogni orbita ha una sottomatrice A di F circolante corrispondente al posto i,j della forma di C. A è dxd e si rappresenta con un x^k, $0 \le k \le d-1$ (shift di k posti).

Quindi C è determinata da una forma (individua una permutazione tra le orbite di lunghezza d) e un elenco di shift: ci sono ω (d) orbite e per ciascuna va specificata la matrice circolante.

Chiamo $G_d(d|n)$ il gruppo formato da tutte le componenti dω (d)xdω (d)

$|G_d| = \omega(d)!\, d^{\omega(d)}$

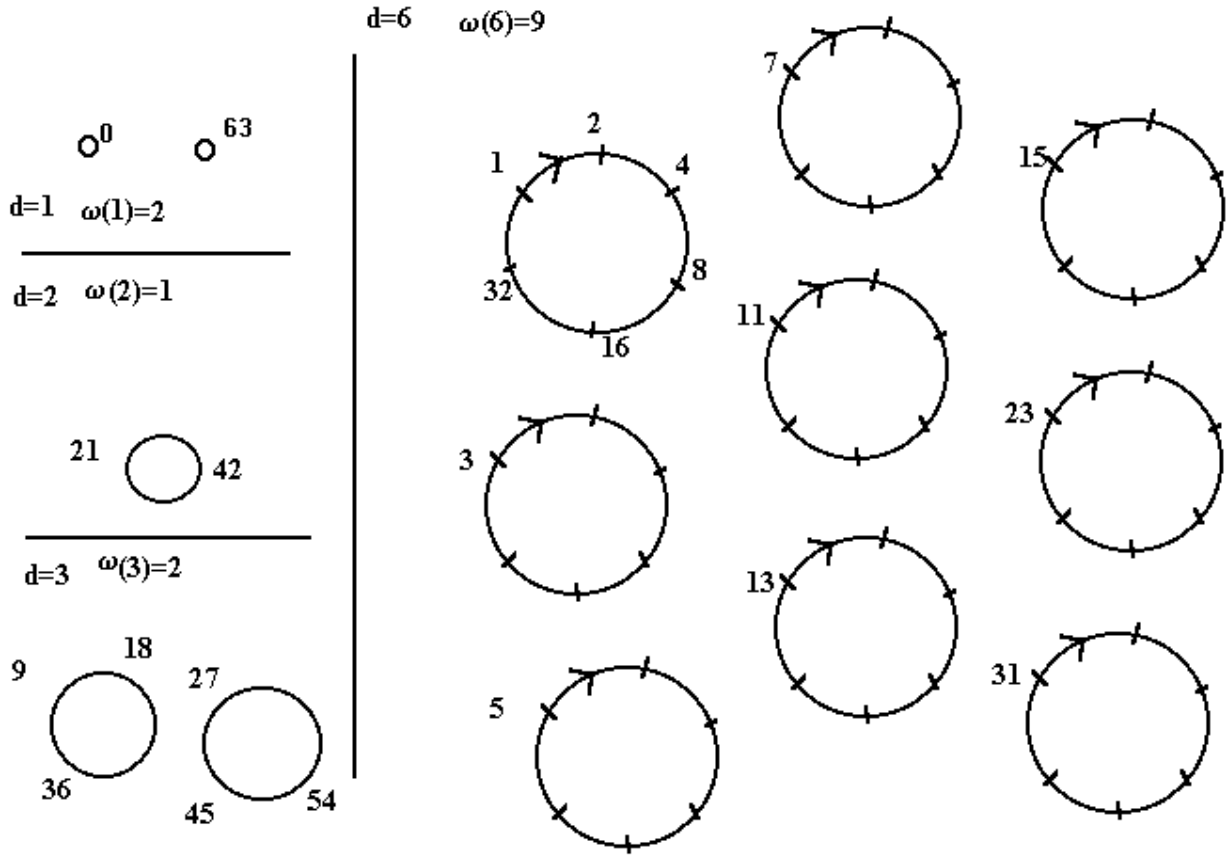
$C = \left(\sigma, \left(x^{k_1}, x^{k_2}, \ldots, x^{k_{\omega(d)}}\right)\right)$

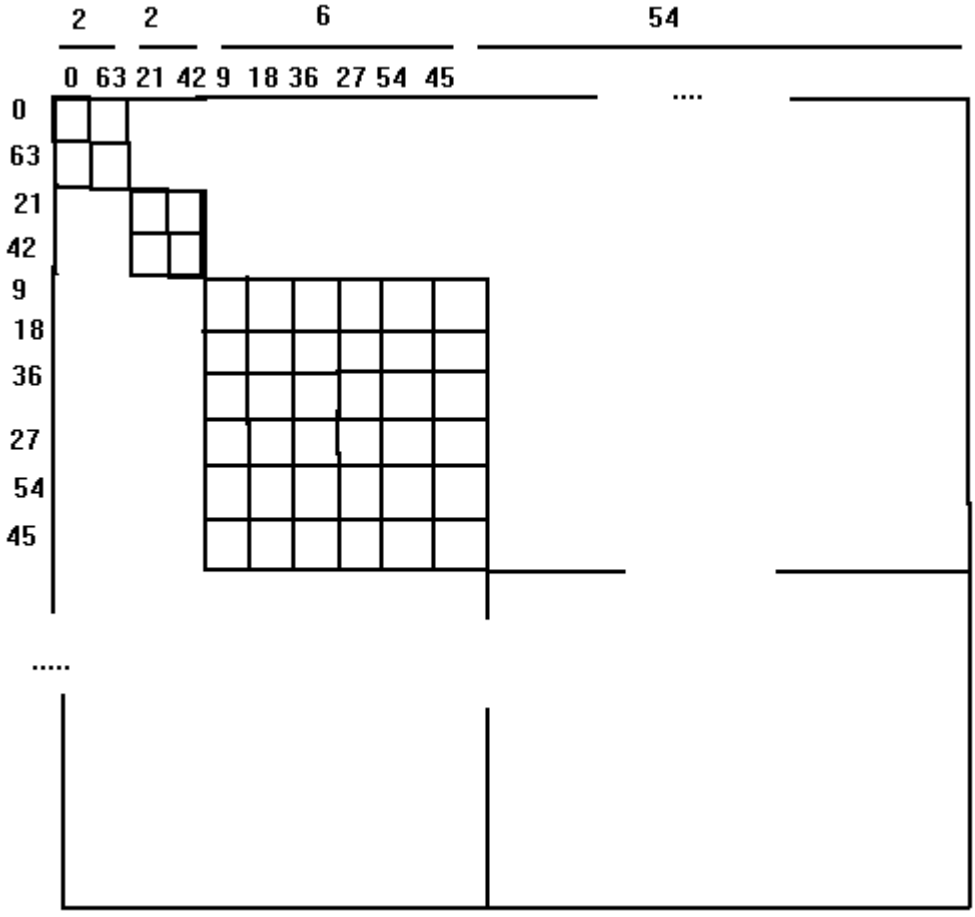
$G_n(q) = \bigoplus_{d|n} G_d \Rightarrow F = (C_1, \ldots, C_{\tau(n)})$ dove τ (n) è il numero dei divisori di n.

Per rappresentare C con forma data basta sostituire gli 1 con i relativi x^{k_i} dove gli x^{k_i} si moltiplicano così: $x^{k_i} x^{k_j} = x^{(k_i + k_j) \bmod d}$

Da tutto questo segue che $|G_n(q)| = \Pi |G_d|$

Orbite:


d=6 ω(6)=9
0
63
d=1 ω(1)=2
d=2 ω(2)=1
21
42
d=3 ω(3)=2
9
18
27
36
45
54
1
2
4
8
16
32
3
5
7
11
13
15
23
31


2
2
6
54
0 63 21 42 9 18 36 27 54 45
....
0
63
21
42
9
18
36
27
54
45
.....

ES.: Caso binario, n=6. d=1,2,3,6

Il numero di orbite di lunghezza d è rispettivamente:

ω (1)=2, ω (2)=1, ω (3)=2, ω (6)=9

Metto in ordine i rappresentanti di ogni orbita:

d = 1	d = 2	d = 3	d = 6
0,63	21	9,27	1,3,5,7,11,13,15,23,31

$G_6 = G_1 \times G_2 \times G_3 \times G_6$

$|C_d| = \omega(d)!\, d^{\omega(d)}$

d=1

$|C_1| = 2! = 2$

Ho solo 2 possibilità (permutazioni delle 2 orbite):

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

0 63 0 63

↓ ↓ e ↓ ↓

0 63 63 0

d=2

$|C_2| = \omega(2)!\, 2^{\omega(2)} = 2$

$O(21) = \{21,42\}$

Ho un orbita sola (quindi un'unica permutazione) ma 2 forme possibili:

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

(1,1) (1,x)

d=3

$|C_3| = \omega(3)!\,3^{\omega(3)} = 2!\,3^2 = 2 \cdot 9 = 18$

$O(9) = \{9,18,36\}$

$O(27) = \{27,54,45\}$

Ho 2 permutazioni e 9 forme possibili, per un totale di 18 elementi.

Ingrandiamo la forma nel caso di $\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, x, x^2\right)$:

	9	18	36	27	54	45
9	0	0	0	0	1	0
18	0	0	0	0	0	1
36	0	0	0	1	0	0
27	0	0	1	0	0	0
54	1	0	0	0	0	0
45	0	1	0	0	0	0

Consideriamo G_d: ci sono ω (d) orbite di lunghezza d. E' utile trovare una C | per C= dω (d). Se prendo C=((12... ω (d)),(1,1,...,x)) che manda il primo elemento di un'orbita nel primo della successiva, tranne per l'ultima orbita, in cui il primo elemento viene mandato nel secondo della prima orbita, e così via, si produce in G_n un elemento di periodo mcm $\{d\omega(d)\}$

Algoritmo per calcolare un'evoluzione di periodo massimo

q=2, n=6

$q^n - 1 = 63$

c è il numero della configurazione

c_0 è la configurazione iniziale inserita dall'utente

Attraverso i rappresentanti f[i] $(0 \le i \le 9)$ si individua la permutazione tra le orbite dello shift:

f[0]→ f[1] → ...→ f[8] → f[9]

dove f[9] è il secondo elemento della prima orbita.

k=0, r=0, i=0

$c=c_0$

do

{

stampa configurazione (c)

do

{

while (k<9)

{

if ($c=f[k]^{2^i \bmod 63}$) $r=f[k+1]^{2^i \bmod 63}$

k=k+1

}

i=i+1

k=0

}

while (r=0)

c=r

r=0

i=0

}

while ($c \neq c_0$)

Output

1 1 000001

2 3 000011

3 5 000101

4 7 000111

5 11 001011

6 13 001101

7 15 001111

8 23 010111

9 31 011111

10 2 000010

11 6 000110

12 10 001010

13 14 001110

14 22 010110

15 26 011010

16 30 011110

17 46 101110

18 62 111110

19 4 000100

20 12 001100

21 20 010100

22 28 011100

23 44 101100

24 52 110100

25 60 111100

26 29 011101

27 61 111101

28 8 001000

29 24 011000

30 40 101000

31 56 111000

32 25 011001

33 41 101001

34 57 111001

35 58 111010

36 59 111011

37 16 010000

38 48 110000

39 17 010001

40 49 110001

41 50 110010

42 19 010011

43 51 110011

44 53 110101

45 55 110111

46 32 100000

47 33 100001

48 34 100010

49 35 100011

50 37 100101

51 38 100110

52 39 100111

53 43 101011

54 47 101111

55 1 000001

Listato C

```
#include <stdio.h>

#include <math.h>

int pot(int , int );

void celle(int , int *);

void main (void)

{

int f[10],c0,c,i=0,a[6],r=0,k=0,p=1;

f[0]=1;f[1]=3;f[2]=5;f[3]=7;f[4]=11;f[5]=13;f[6]=15;f[7]=23;f[8]=31;f[9]=2;

printf("Inserire configurazione iniziale ");
```

```
scanf("%d",&c);
c0=c;
do
{
celle(c,a);
printf("%d %d %d%d%d%d%d%d\n",p,c,a[5],a[4],a[3],a[2],a[1],a[0]);
do {
while(k<9)
{
if (c==((f[k]*pot(2,i))%63))
r=((f[k+1]*pot(2,i))%63);
k++;
};
i++;k=0;
} while (r==0) ;
c=r; r=0;i=0;p++;
// if (p%3==0) printf("\n");
}
while (c!=c0);
}
int pot(int x, int i)
{
int k,r=1;
for (k=0;k<i;k++)
{
r=r*x;
}
return (r);
}
```

```
void celle(int c, int *a)

{

int j;

for(j=0;j<6;j++)

{

if (c%2==0)

{

a[j]=0;

} else a[j]=1;

c=c/2;

}

}
```

Home di Teutoburgo