Sul periodo delle matrici di permutazione

G. Campanini - A. Di Porto
Fondazione Ugo Bordoni, Roma, Italia

Introduzione

Dopo un breve richiamo alla definizione di *matrici di permutazione* e ad alcune loro proprietà, si affronta lo studio del *periodo* delle suddette matrici. In particolare si analizza il massimo periodo ammissibile e si fornisce il numero delle matrici aventi un prefissato periodo T.

Matrici di permutazione

Sia n un intero positivo. Consideriamo l'insieme $\mathcal{M}(n, \mathbb{Z}_2)$ delle matrici quadrate di ordine n i cui elementi, a_{ij} $(i, j = 1, 2,..., n)$, appartengono al campo di Galois $GF(2)=\mathbb{Z}_2=\{0,1\}$. Per ogni matrice $A \in \mathcal{M}(n,\mathbb{Z}_2)$ indichiamo con $|A_{(1)}|$ il numero degli elementi a_{ij} il cui valore sia 1, $0 \le |A_{(1)}| \le n^2$.

Prendiamo adesso in considerazione il sottoinsieme $\mathcal{G}_{(n)}$ di $\mathcal{M}(n, \mathbb{Z}_2)$ così definito:

$$\mathcal{G}_{(n)} = \{A : |A_{(1)}| = n ;\ a_{sk} = 1 \Rightarrow a_{ik} = 0, \forall i \neq s \ \ \& \ \ a_{sj} = 0, \forall j \neq k \}.$$

Nel seguito indicheremo con le lettere A, B, C le matrici, dette anche *matrici di permutazione* [1], appartenenti all'insieme $\mathcal{G}_{(n)}$, e con le lettere a_{ij}, b_{ij}, c_{ij}, $(i, j = 1, 2,..., n)$, i rispettivi elementi; la notazione $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ indica, quindi, una matrice definita dai suoi elementi.

Si osservi che le matrici di $\mathcal{G}_{(n)}$ sono tutte *non singolari*, ovvero a *determinante non nullo*, poiché, per ogni A in $\mathcal{G}_{(n)}$, un solo *prodotto associato* ad A è diverso da zero ed è uguale a ± 1 [2].

Proposizione 1: L'insieme $\mathcal{G}_{(n)}$ dotato dell'operazione prodotto righe per colonne è un *gruppo non commutativo* [3].

Dimostrazione : L'operazione definita in $\mathcal{G}_{(n)}$ è l'usuale *prodotto righe per colonne tra matrici* [2]. Tale operazione è binaria [3] e definita su tutto $\mathcal{G}_{(n)}$. Infatti è immediato verificare che, comunque si prendano A e B in $\mathcal{G}_{(n)}$, risulta

Lavoro eseguito nell'ambito della Convenzione in atto tra l'Amministrazione delle Poste e delle Telecomunicazioni e la Fondazione Ugo Bordoni

$$A \times B = C \in \mathcal{G}_{(n)} \quad ,$$

e quindi:

- l'*insieme* $\mathcal{G}_{(n)}$ *è chiuso* rispetto all'operazione su esso definita;
- la *legge associativa* è rispettata in $\mathcal{G}_{(n)}$, poiché $\mathcal{G}_{(n)}$ è un s. i. dell'insieme $\mathcal{M}(n, \mathbb{R})$ delle matrici quadrate di ordine n a elementi reali [3];
- la matrice $I \in \mathcal{G}_{(n)}$ che ha tutti gli elementi non nulli sulla diagonale principale è l'unico *elemento neutro* rispetto al prodotto tra matrici sopra definito;
- per ogni $A = (a_{ij}) \in \mathcal{G}_{(n)}$ la matrice $A^{-1} = (a'_{ij}) \in \mathcal{G}_{(n)}$ i cui elementi sono tali che

$$a'_{sh} = 1 \quad \text{se} \quad a_{hs} = 1 \quad ,$$

è la *matrice inversa* di A e risulta

$$A^{-1} \times A = A \times A^{-1} = I \quad .$$

Si noti che, tenendo conto del fatto che le matrici di $\mathcal{G}_{(n)}$ sono *non singolari*, la definizione sopra data di A^{-1} coincide con l'usuale definizione di matrice inversa, inoltre è sempre $A^{-1} = \overline{A}$, dove con $\overline{A}$ si indica la *matrice trasposta* di A [2].

Si osservi, infine, che il gruppo $\mathcal{G}_{(n)}$ *non è commutativo*, per $n > 2$. Ad esempio, per $n = 4$, si considerino le matrici A e B definite rispettivamente dai seguenti elementi

$$A : a_{12} = a_{23} = a_{31} = a_{44} = 1$$

$$B : b_{13} = b_{24} = b_{31} = b_{42} = 1 \quad ,$$

risulta allora

$$C = A \times B \neq B \times A = C' \quad ,$$

si ha, infatti, $c_{14} = 1$ e $c'_{11} = 1$.◆

Inoltre, il gruppo $\mathcal{G}_{(n)}$ è isomorfo al *gruppo totale* $\mathcal{S}_n$(*) *delle sostituzioni* su n elementi ; di conseguenza l'*ordine* (o *cardinalità*) di $\mathcal{G}_{(n)}$ [3] è finito ed è uguale a $n!$.

Relazione d'equivalenza associata a una matrice di $\mathcal{G}_{(n)}$

Al fine di caratterizzare il *periodo* di un elemento di $\mathcal{G}_{(n)}$, risulta utile ricordare la definizione generale di *periodo di un elemento di un gruppo* .

(*) $\mathcal{S}_n$ è detto anche *gruppo simmetrico* di grado n [1].

Un elemento x di un gruppo ha periodo e finito(**) se risulta:

$$x^e = u \quad ; \quad x^h \neq u \quad , \quad 0 < h < e,$$

dove u indica l'unità del gruppo.

Per il gruppo $\mathcal{G}_{(n)}$ valgono inoltre le seguenti proposizioni:

Proposizione 2 : $\mathcal{G}_{(n)}$ non è un gruppo ciclico.
Proposizione 3 : Ogni elemento di $\mathcal{G}_{(n)}$ ha periodo finito.
Proposizione 4 : Se $A \in \mathcal{G}_{(n)}$ ha periodo e allora

$$A^s = I \Rightarrow s \equiv 0 \pmod{e} \; ; \quad A^s = A^r \Rightarrow s \equiv r \pmod{e},$$

e, inoltre, l'insieme

$$\mathcal{A} = \{A, A^2, \ldots, A^e = I\}$$

è sottogruppo ciclico di $\mathcal{G}_{(n)}$; $\mathcal{A}$ è quindi commutativo e viene brevemente indicato con il nome di *gruppo generato da* A [3].

Per quel che riguarda le proposizioni 2, 3 si tenga rispettivamente presente che $\mathcal{G}_{(n)}$ è non commutativo e che $\mathcal{G}_{(n)}$ è un gruppo finito; per la proposizione 4 si ricordino le definizioni di periodicità di un elemento e di gruppo ciclico [3].◆

Indichiamo con $a_{ij}^{(t)}$ gli elementi della matrice A^t (potenza t-esima di $A \in \mathcal{G}_{(n)}$). Fissata una qualunque riga di A, e sia essa la i-esima, definiamo *periodo della riga i-esima* di A il più piccolo esponente $t > 0$ tale che $a_{ii}^{(t)} = 1$.

Al fine di chiarire la precedente definizione mostriamo un esempio in $\mathcal{G}_{(6)}$.

Esempio 1 : Sia $A \in \mathcal{G}_{(6)}$ definita dai seguenti elementi

$$A : a_{13} = a_{25} = a_{34} = a_{41} = a_{52} = a_{66} = 1,$$

la riga 6 ha periodo 1;

$$A^2 : a_{14}^{(2)} = a_{22}^{(2)} = a_{31}^{(2)} = a_{43}^{(2)} = a_{55}^{(2)} = a_{66}^{(2)} = 1,$$

le righe 2 e 5 hanno periodo 2;

$$A^3 : a_{11}^{(3)} = a_{25}^{(3)} = a_{33}^{(3)} = a_{44}^{(3)} = a_{52}^{(3)} = a_{66}^{(3)} = 1,$$

le righe 1, 3 e 4 hanno periodo 3.
È immediato vedere che il periodo di A è uguale a 6.

(**) In letteratura sono spesso usate le parole *ordine* ed *esponente* come sinonimi di periodo finito.

Proposizione 5: Fissata una qualunque matrice $A \in \mathcal{G}_{(n)}$ ad essa è associata una *relazione d'equivalenza* (indicata con il simbolo $\approx$) tra le sue righe, così definita: la riga i-esima è equivalente alla riga j-esima se e solo se $a_{ij}^{(r)} = 1$ per qualche intero $r \neq 0$, ovvero, indicando le righe di A con il loro indice

$$i \approx j \iff \exists\, r \gtrless 0 \text{ tale che } a_{ij}^{(r)} = 1.$$

Dimostrazione: La relazione così definita tra le righe di A è una relazione d'equivalenza [3]. Infatti, essa

- è *riflessiva*, $i \approx i$, poiché $a_{ii}^{(t)} = 1$, dove t è il periodo della riga i;
- è *simmetrica*, $i \approx j \iff j \approx i$, poiché, tenendo conto dell'uguaglianza $(a_{hk}^{(-r)}) = A^{-r} = \overline{A}^{r}$, si hanno le seguenti successive implicazioni
$$i \approx j \Rightarrow a_{ij}^{(r)} = 1 \Rightarrow a_{ji}^{(-r)} = 1 \Rightarrow j \approx i;$$
- è *transitiva*, $i \approx j$ e $j \approx k \Rightarrow i \approx k$, poiché
$$i \approx j \Rightarrow a_{ij}^{(r)} = 1. \text{ e } j \approx k \Rightarrow a_{jk}^{(s)} = 1,$$
e le due ultime uguaglianze implicano
$$a_{ik}^{(r+s)} = 1 \Rightarrow i \approx k. \quad \blacklozenge$$

Dalla proposizione 5 possiamo dedurre le seguenti proposizioni:

Proposizione 6: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$, essa definisce una relazione d'equivalenza che induce una partizione nell'insieme delle righe di A in sottoinsiemi disgiunti ovvero in *classi d'equivalenza* (***).

Proposizione 7: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$, il periodo massimo ammissibile di una riga di A è uguale a n.

Proposizione 8: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$, le righe di A appartenenti ad una stessa classe di equivalenza $\mathbf{c}$ hanno tutte lo stesso periodo, quest'ultimo è uguale al numero degli elementi contenuti in $\mathbf{c}$. Siano $\mathbf{c}_{n_s}$, $(s = 1, 2,\ldots,r)$ le classi di equivalenza della partizione indotta da A; n_s indica il periodo e il numero delle righe fra loro equivalenti contenute in $\mathbf{c}_{n_s}$ e si ha:

$$1 \leq r \leq n \;;\; \sum_{s=1}^{r} n_s = n \;;\; 0 < n_1 \leq n_2 \leq \ldots \leq n_r \leq n \;.$$

(***) La definizione di classe d'equivalenza definita da una matrice di permutazione non differisce, "mutatis mutandis", dalla definizione di *orbita di un elemento* $s \in S = \{1, 2,\ldots, n\}$ sotto l'azione di una permutazione $\sigma \in \mathcal{S}_n$, dove $\mathcal{S}_n$ è il gruppo simmetrico di grado n [1].

Prima di proseguire nella trattazione illustriamo quanto detto con un esempio:

Esempio 2 : Sia $A \in \mathcal{G}_{(8)}$ definita dai seguenti elementi

$$A : a_{13}= a_{22}= a_{35}= a_{46}= a_{51}= a_{64}= a_{78}= a_{87}= 1,$$

le classi d'equivalenza associate alla matrice di permutazione A sono le seguenti:

$$\mathbf{c}_{n_1} = \{2\} \ ; \ \mathbf{c}_{n_2} = \{4, 6\} \ ; \ \mathbf{c}_{n_3} = \{7, 8\} \ ; \ \mathbf{c}_{n_4} = \{1, 3, 5\}.$$

Periodo delle matrici di permutazione

Da quanto esposto in precedenza (in particolare dalla proposizione 8), si possono enunciare le due seguenti proposizioni:

Proposizione 9: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$ essa definisce una relazione d'equivalenza tra le sue righe; il periodo T di $A \in \mathcal{G}_{(n)}$ è allora uguale al minimo comune multiplo (mcm) tra le cardinalità delle classi disgiunte associate alla relazione di equivalenza indotta da A: $T = \text{mcm}\ (n_1, n_2,\ldots,n_r)$.

Proposizione 10: I periodi ammissibili sono quegli interi T tali che:

$$T = \prod_{i=1}^{\infty} p_i^{\alpha^i} \qquad \text{con la condizione} \qquad \sum_{\substack{i=1 \\ i\,:\,\alpha^i > 0}}^{\infty} p_i^{\alpha^i} \le n$$

dove p_i rappresenta l'i-esimo primo, essendo $p_1 = 2$.

Inoltre, per ogni periodo ammissibile, esiste almeno una matrice di permutazione avente quel fissato periodo. Si presenta quindi il problema di calcolare il numero di matrici $A \in \mathcal{G}_{(n)}$ aventi un fissato periodo T, dato un intero n maggiore di 1.

Sia T un periodo ammissibile per gli elementi di $\mathcal{G}_{(n)}$, allora avremo una o più *partizioni* [4] di n tali che il mcm tra i suoi addendi sia proprio T. Data una qualunque di tali partizioni,

$$(1) \qquad n = a +\ldots+ a + b +\ldots+ b +\ldots+c +\ldots+ c$$

con $k \ge 1$ addendi a, $h \ge 1$ addendi b e così via, $a > b >\ldots> c$, essa può essere associata a tutte quelle matrici $A \in \mathcal{G}_{(n)}$ che definiscono una relazione di equivalenza tra le loro righe che induce una partizione in k classi di equivalenza ciascuna di cardinalità a, in h classi di equivalenza ciascuna di cardinalità b, e così via; diremo allora che tutte queste matrici hanno la stessa *struttura ciclica* [1].

Dalla proposizione 9 è immediato concludere che le matrici aventi la stessa struttura ciclica hanno tutte lo stesso periodo T, mentre non si può affermare che tutte le matrici aventi lo stesso periodo T abbiano la stessa struttura ciclica.

Si noti che il numero delle strutture cicliche possibili è uguale al numero p(n) delle partizioni di n [1, 4].

Proposizione 11: Il numero N_{T_i} delle matrici con la stessa struttura ciclica definita dalla partizione (1) è dato dai seguenti prodotti:

$$N_{T_i} = \left(\frac{(n)!}{(n-ka)!\, a^k\, k!}\right)\left(\frac{(n-ka)!}{(n-ka-hb)!\, b^h\, h!}\right)\cdots\cdots\left(\frac{(tc)!}{(0)!\, c^t\, t!}\right) \tag{2}$$

Il numero delle matrici aventi un fissato periodo T è dato da ΣN_{T_i}, dove $1 \leq i <$ p(n) rappresenta il numero di partizioni di n i cui addendi hanno il minimo comune multiplo uguale a T.

Dimostrazione: È necessario chiarire come è stata ottenuta la (2) e, a questo proposito, è sufficiente giustificarne il primo fattore, poiché gli altri si ottengono di conseguenza. Data la partizione (1) si deve, innanzitutto, trovare il numero di combinazioni di classe ka di n elementi; per ciascuna di queste combinazioni si deve calcolare il numero di disposizioni di classe (a-1) di (ka-1) elementi; per ogni tale disposizione, il numero di disposizioni di classe (a-1) di (ka-a-1) elementi, e così via. Si ottiene quindi:

$$\binom{n}{ka}\prod_{i=1}^{k}\{[a(k+1-i)-1]\cdots\cdots[a(k-i)+1]\} = \binom{n}{ka}\frac{(ka-1)!}{\prod_{i=1}^{k-1} i\,a} = \binom{n}{ka}\frac{(ka-1)!}{a^{k-1}(k-1)!} =$$

$$= \frac{n!\,(ka)!}{(ka)!\,(n-ka)!\,ka\;a^{k-1}\,(k-1)!} = \frac{n!}{(n-ka)!\,a^k\,k!} \qquad \blacklozenge$$

Per trovare il massimo periodo ammissibile di un elemento $A \in \mathcal{G}_{(n)}$, $n > 1$, è sufficiente ricercare tra le p(n) partizioni di n le *partizioni migliori*, intendendo con questo termine quelle partizioni i cui addendi forniscono il mcm di valore più elevato.

Basandosi sulle proprietà di cui gode la successione dei numeri primi [5] e ricordando che, dati tre interi u, v e z risulta sempre:

$$(u+v) < uv \quad \text{per} \quad u \geq 2 \;\text{ e }\; v > 2\;,\; u > 2 \;\text{ e }\; v \geq 2$$
$$(u+z)v \gtreqless u(v+z) \Leftrightarrow v \gtreqless u,$$

si congettura il seguente algoritmo che fornisce una delle *migliori partizioni* di un fissato

intero n.

a) Si scriva n come somma di primi consecutivi p_i (i =1,2, .. , k ; p_1=2) più un eventuale resto R_1, $0 \le R_1 < p_{k+1}$:

(3) $$n = \sum_{i=1}^{k} p_i + R_1$$

b) Se risulta $R_1 = 0$ oppure $R_1 = 1$ la migliore partizione è data dalla (3), ad eccezione del solo caso $n = 3$ nel quale anche se risulta, secondo il passo a), $k = 1$, $p_k = 2$ e $R_1 = 1$, la migliore partizione non è (2+1) bensì 3.

c) Se il resto $R_1 \ge 2$, si ripartisca R_1 nella seguente somma

$$R_1 = \sum_{i=1}^{j} (p_i^2 - p_i) + R_2 \quad , 1 \le j < k \quad \text{e} \quad R_2 < p_{j+1}^2 - p_{j+1} ,$$

e si scriva

$$n = \sum_{i=1}^{j} p_i^2 + p_{j+1} + \ldots + p_k + R_2$$

d) Se il resto $R_2 \ge 2^2$, si operi come al punto c) con

$$R_2 = \sum_{i=1}^{s} (p_i^3 - p_i^2) + R_3 \quad , 1 \le s < j \quad \text{e} \quad R_3 < p_{s+1}^3 - p_{s+1}^2 ,$$

e si scriva

$$n = \sum_{i=1}^{s} p_i^3 + \sum_{i=s+1}^{j} p_i^2 + p_{j+1} + \ldots + p_k + R_3$$

e) Si continui ad operare sui resti successivi finché il t-esimo resto R_t, ottenuto dalla ripartizione $R_{t-1} = \Sigma (p_i^t - p_i^{t-1}) + R_t$, risulta minore di 2^t. Si scriva allora

(4) $$n = \sum_{i=1}^{k} p_i^{\alpha_i} + r_1 , \ \alpha_1 = t , \ \alpha_\nu > 1 \ (\nu \le j) \ \text{e} \ \alpha_\nu = 1 \ (\nu > j) , \ 0 \le r_1 = R_t < 2^{\alpha_1} .$$

f) Se risulta $r_1 = 0$ la migliore partizione è data dalla (4).

g) Se risulta $r_1 \ge 1$ si ricerchi, se esiste, il più piccolo valore $p_\mu^{\alpha_\mu}$ ($1 \le \mu \le k$) tale che $p_\mu^{\alpha_\mu} + a$ ($0 < a \le r_1$) sia uguale a p_{k+1}. Si scelga per n la seguente partizione:

(5) $$\sum_{\substack{i=1 \\ i \ne \mu}}^{k+1} p_i^{\alpha_i} + (r_1 - a)$$

Se $r_2 = r_1 - a = 0$, la (5) è la migliore partizione, altrimenti si continui ad operare su r_2 come fatto per r_1 e così via sino a che un resto r_t è uguale a zero oppure è tale che non esiste un valore $p_\tau^{\alpha_\tau}$ che permetta di ottenere $p_\tau^{\alpha_\tau} + d = p_{k+t}$, ($d \le r_t$).

A titolo d'esempio si applichi, per $n = 9$, l'algoritmo che permette di trovare il massimo periodo ammissibile T_{max} per gli elementi di $\mathcal{G}_{(9)}$:

- usando la (3) del punto a), si ha

$$n = \sum_{i=1}^{2} p_i + R_1$$

ovvero, $9 = 2 + 3 + 4$;

- essendo $R_1 = 4 > 2$, si ripartisca R_1 secondo quanto indicato al punto c)

$$R_1 = \sum_{i=1}^{1} (p_i^2 - p_i) + R_2$$

ovvero, $4 = 2 + 2$;

- si ripartisca n secondo il punto c)

$$n = p_1^2 + p_2 + R_2$$

ovvero, $9 = 4 + 3 + 2$;

- essendo $R_2 = 2$ $(1 < r_1 = R_2 < 2^2)$ si prosegue secondo il punto g) ottenendo, infine,

$$n = p_1^2 + (p_2 + r_1)$$

e quindi l'algoritmo termina poiché $r_2 = 0$. Si può infine scrivere: $9 = 4 + (3+2) = 4 + 5$.

Risulta allora: $T_{max} = \text{mcm}\ (4, 5) = 20$.

Periodo ammissibile T	Numero delle partizioni i	Numero delle matrici con periodo T ΣN_{T_i}
1	1	1
2	4	2.619
3	3	5.768
4	4	30.996
5	1	3.024
6	7	83.160
7	1	25.920
8	1	45.360
9	1	40.320
10	2	27.216
12	2	30.240
14	1	25.920
15	1	24.192
20	1	18.144
Totale	30	362.880 = 9!