Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Daniele A. Gewurz

Sui vettori di Parker e concetti correlati

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **3-A**—*La Matematica nella Società e nella Cultura* (2000), n.1S, p. 85–88.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2000_8_3A_1S_85_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2000.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. III-A, Supplemento ad Aprile 2000, 85-88

Sui vettori di Parker e concetti correlati.

DANIELE A. GEWURZ

Non domandarci la formula che mondi possa aprirti,
sì qualche storta sillaba e secca come un ramo.
Eugenio Montale

La mia tesi parla dei vettori di Parker. Il vettore di Parker di un gruppo di permutazioni finito G è una sequenza finita di interi non negativi collegata con l'azione mediante coniugazione di G sull'insieme dei cicli che compaiono nei suoi elementi.

I temi principali di questa tesi consistono nel comprendere quali informazioni sul gruppo possano essere recuperate da dati così esigui e nell'ottenere più o meno esplicitamente i vettori di Parker di varie importanti classi di gruppi.

Cominciamo dando, a mo' di motivazione per il loro studio, l'applicazione nell'ambito della teoria computazionale di Galois da cui nacquero.

In tale contesto, possiamo essere in grado di calcolare (o approssimare) i vettori di Parker del gruppo di Galois di un polinomio, così che è interessante comprendere quanta informazione esso ci dia sul gruppo stesso.

Più precisamente, sia f un polinomio di grado n a coefficienti in $\mathbf{Q}$ o, senza ledere la generalità, in $\mathbf{Z}$. Consideriamo il problema di determinare G, il gruppo di Galois di f su $\mathbf{Q}$ (cioè il gruppo di Galois di un campo di spezzamento di f, visto come estensione di $\mathbf{Q}$). Questo gruppo permuta le radici di f; così esso è isomorfo ad un sottogruppo di S_n.

Consideriamo un primo p «sufficientemente grande» (così che esso non divida il discriminante e il coefficiente direttore di f). Riduciamo f modulo p, ottenendo un polinomio $\overline{f} \in GF(p)[x]$. Sia $K = GF(p^k)$ il campo di spezzamento di $\overline{f}$ e $\vartheta : a \mapsto a^p$ il suo automorfismo di Frobenius. Allora ϑ permuta le radici di $\overline{f}$ e le lunghezze dei cicli di ϑ sono i gradi dei fattori irriducibili di $\overline{f}$ (su $GF(p)$); infatti, se $\overline{g}$ è un fattore irriducibile di grado d di $\overline{f}$ e α è una delle sue radici, allora le altre sono α^p, α^{p^2}, …, $\alpha^{p^{d-1}}$.

Perciò fattorizzando $\overline{f}$ e sollevando ϑ ad un elemento di G, otteniamo le lunghezze dei cicli di un elemento del gruppo di Galois.

Il teorema di densità di Cebotarev garantisce che l'insieme dei primi che, mediante questa procedura, dànno un fissato elemento di G ha densità tale che ogni classe di coniugio di elementi è equiprobabile quando si sceglie casualmente un primo p.

Quindi, ripetendo quanto precede per «molti» primi, si può ottenere abbastanza informazione da essere in grado di dare una stima sulla distribuzione

delle lunghezze dei cicli degli elementi di G. Il lemma di Parker collega direttamente tali lunghezze con il vettore di Parker di G.

Riassumendo, ridurre f modulo p per «molti» p ci dà le lunghezze dei cicli di «molti» elementi di G, il che a sua volta ci consente di dare una stima del vettore di Parker di G.

Diamo poi la definizione e il risultato fondamentale, il lemma di Parker, che lega il vettore di Parker di un gruppo alla struttura ciclica dei suoi elementi.

Sia G un gruppo di permutazioni di grado n. Lo possiamo identificare con un sottogruppo di S_n, il gruppo simmetrico su n punti. Definiamo $\mathcal{C}_i$ come l'insieme di tutti i cicli di lunghezza i che appaiono negli elementi di G, scritti come prodotti di cicli disgiunti, e poniamo $\mathcal{C} := \bigcup_{i=1}^{n} \mathcal{C}_i$. Ovviamente, questo insieme non è vuoto perché, per ogni G, $\mathcal{C}_1 = \{(1), (2), \ldots, (n)\}$, dato che questi cicli appaiono nell'elemento identità.

Possiamo definire in modo naturale un'azione di G sull'insieme $\mathcal{C}$: dato $g \in G$ e $(a_1, a_2, \ldots, a_k) \in \mathcal{C}$, poniamo

$$(a_1, a_2, \ldots, a_k)^g := (a_1^g, a_2^g, \ldots, a_k^g).$$

Equivalentemente, possiamo dire che l'azione è definita mediante coniugazione (in S_n, visto che un singolo ciclo non è in generale un elemento di G).

È ovvio dalla definizione e da elementari proprietà della coniugazione in S_n che ogni orbita di questa azione deve essere contenuta in uno dei $\mathcal{C}_i$. Chiamiamo $p_i(G)$ (o semplicemente p_i, quando non c'è possibilità di confusione) il numero di orbite di questa azione che sono contenute in $\mathcal{C}_i$, cioè il numero di orbite sugli i-cicli.

Allora la sequenza $\mathbf{p}(G) = (p_1(G), p_2(G), \ldots, p_n(G))$ è il *vettore di Parker* del gruppo G. Talvolta si considera $\mathbf{p}(G)$ come una successione infinita i cui termini sono definitivamente uguali a zero:

$$(p_1(G), p_2(G), \ldots, p_n(G), 0, 0, \ldots).$$

Inoltre, è chiaro che $p_1(G) = 1$ è equivalente al dire che G è transitivo, in quanto l'insieme $\mathcal{C}_1$ degli 1-cicli è (in bijezione con) l'insieme dei punti su cui agisce G. In generale, $p_1(G)$ è uguale al numero di orbite di G.

In alcuni casi, si calcola immediatamente il vettore di Parker di un gruppo: per esempio, sapendo che due cicli sono coniugati in S_n se, e solo se, essi hanno la stessa lunghezza, possiamo concludere che il vettore di Parker di S_n è $(1, 1, \ldots, 1)$ (n componenti).

Il principale risultato sui vettori di Parker è il seguente, dovuto a Richard A. Parker (egli diede la definizione e alcuni risultati sui vettori nel corso del convegno «Groups at St. Andrews» del 1996, ma non risulta che abbia pubblicato nulla in proposito; le definizioni e i risultati standard possono essere trovati in [1]).

TEOREMA 1 (Lemma di Parker). – *Siano G e $\mathcal{C}_i$ come sopra. Sia $c_k(g)$ il numero dei k-cicli dell'elemento $g \in G$. Allora il numero delle orbite di G su $\mathcal{C}_k$ è*

$$p_k(G) = \frac{1}{|G|} \sum_{g \in G} k c_k(g).$$

In particolare, la somma dei componenti del vettore di Parker è uguale al grado del gruppo.

Come prima elementare applicazione del lemma di Parker, possiamo calcolare il vettore di Parker di un gruppo ciclico di ordine primo p, C_p (nella sua azione naturale su p punti). In un gruppo siffatto, l'identità ha p 1-cicli, mentre ogni altro elemento ha esattamente un p-ciclo. Così troviamo $p_1(C_p) = 1$, $p_p(C_p) = p - 1$ e $p_k(C_p) = 0$ per gli altri valori di k. Perciò, in questo caso, p_k è uguale al numero di elementi di ordine k. Si può mostrare che ciò avviene in realtà per tutti i gruppi ciclici nella loro azione regolare e, più in generale, per tutti i gruppi regolari.

Per dare un altro esempio, consideriamo i gruppi alterni A_n. In questi gruppi compaiono cicli di tutte le lunghezze minori o uguali a $n - 2$. Se n è dispari un $(n-1)$-ciclo (con un 1-ciclo) è una permutazione di classe dispari, e quindi $p_{n-1}(A_n) = 0$ (n dispari), mentre ci sono almeno due classi di coniugio di n-cicli (in S_n, i cicli $(1\ 2 \ldots (n-2)(n-1)\ n)$ e $(1\ 2 \ldots (n-2)\ n(n-1))$ sono coniugati tramite una permutazione dispari). Così, $p_n(A_n) = 2$ (n dispari), e quindi $p(A_n) = (1, 1, \ldots, 1, 0, 2)$ (n dispari).

Se n è pari, un ragionamento analogo conduce a $p(A_n) = (1, 1, \ldots, 1, 2, 0)$ (n pari).

Alcune proprietà dei gruppi di permutazioni possono essere «lette» direttamente nei loro vettori di Parker. Esistono semplici condizioni sufficienti sul vettore di Parker di un gruppo G che garantiscono la transitività, o la n-transitività di G; esse generalizzano le ovvie considerazioni per cui G è transitivo se $p_1(G) = 1$ (ha una sola orbita) o se $p_{deg(G)} > 0$ (ha un ciclo di lunghezza massima).

A partire da queste condizioni, e con altre considerazioni di carattere per lo più aritmetico, si arriva a caratterizzare i gruppi simmetrici e alterni in base ai loro vettori di Parker, con un'unica eccezione. Più precisamente:

TEOREMA 2. – *Se G è un gruppo di permutazioni di grado n e $p_1(G) = p_2(G) = \ldots = p_n(G) = 1$, allora, se $n \neq 6$, $G \cong S_n$ con l'azione naturale. Quando $n = 6$, G è isomorfo o a S_6 o a $PGL(2, 5)$ (nella sua azione su 6 simboli, quale si ottiene per esempio con la presentazione* $\langle (12345), (16)(23)(45) \rangle$).

Quando il gruppo da studiare è dotato di proprietà o strutture particolari, ciò può tradursi in corrispondenti peculiarità del vettore di Parker, rendendo più facile il ricavarlo e, in alcuni casi, permettendo di identificare le proprietà o il gruppo stesso a partire dal vettore di Parker. Ad esempio, si è già accennato ai gruppi regolari, mentre per i gruppi di Frobenius si può dire qualcosa di preciso sui lega-

mi tra il vettore di Parker di un gruppo G e quello del suo stabilizzatore G_α (vincoli meno stretti fra questi due vettori si possono ottenere anche per G qualsiasi):

PROPOSIZIONE 1. – *Sia G un gruppo di Frobenius di grado m che agisce su Ω. Se il vettore di Parker di G_α è $\mathbf{p} = (p_1, p_2, \ldots, p_{m-1})$ e il vettore di Parker del nucleo di Frobenius K è $\mathbf{p}'$, allora il vettore di Parker di G è $\mathbf{p}'' := \mathbf{p} + \mathbf{p}'/|G_\alpha|$, ma con 1 al posto della prima componente.*

Isolando una delle proprietà dei gruppi di Frobenius, il fatto che possiedono un sottogruppo normale regolare, è possibile indagare che cosa si può dire in generale sui gruppi di permutazioni che ammettono un tale sottogruppo.

Si è poi studiato come l'indice dei cicli di un gruppo di permutazioni (concetto centrale nella teoria dell'enumerazione di Pólya, per la quale si veda ad esempio [2]) sia uno strumento molto potente quando si studiano i vettori di Parker. Un risultato chiave collega l'indice dei cicli di un gruppo di permutazioni al suo vettore di Parker, consentendoci di far uso dei risultati standard sul primo per ottenere una miglior comprensione del secondo, come ad esempio il suo comportamento rispetto al prodotto diretto e al prodotto corona. È stata anche introdotta una possibile estensione ai gruppi lineari del concetto di vettore di Parker, che fa seguito ad un'analoga estensione degli indici dei cicli.

I gruppi affini generali sono casi particolari della classe dei gruppi con un sottogruppo normale regolare. Il problema di determinare i loro vettori di Parker, così come quelli dei gruppi lineari generali e speciali, è affrontato e risolto nell'ultimo capitolo della tesi, dove vengono anche esibiti esplicitamente rappresentanti delle orbite contate dai vettori. Il lavoro su questo aspetto prosegue tuttora.

Parte del contenuto della tesi è alla base di due articoli ([3] e [4]) dell'autore.

BIBLIOGRAFIA

[1] PETER J. CAMERON, *Permutation Groups* (Cambridge University Press, 1999).
[2] N. G. DE BRUIJN, *Pólya's Theory of Counting*, Applied Combinatorial Mathematics (ed. Edwin F. Beckenbach) (John Wiley, New York, 1964), 144-184.
[3] DANIELE A. GEWURZ, *Reconstruction of permutation groups from their Parker vectors*, Journal of Group Theory (to appear).
[4] DANIELE A. GEWURZ, *Parker vectors and cycle indices of permutation groups*, Journal of Algebraic Combinatorics (submitted).

Dipartimento di Matematica, Università di Roma «La Sapienza»
e-mail: gewurz@mat.uniroma1.it
Dottorato in Matematica (sede amministrativa: Roma) - Ciclo X
Direttore di ricerca: Prof. Peter J. Cameron, Università di Londra
Queen Mary & Westfield College