
La Matematica nella Società e nella Cultura

RIVISTA DELL'UNIONE MATEMATICA ITALIANA

VALENTINA COLOMBO

Alcune proprietà della funzione di Möbius nel reticolo dei sottogruppi dei gruppi Alterni e Simmetrici

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. 4 (2011), n.1 (Fascicolo Tesi di Dottorato), p. 39–42.

Unione Matematica Italiana

[<http://www.bdim.eu/item?id=RIUMI_2011_1_4_1_39_0>](http://www.bdim.eu/item?id=RIUMI_2011_1_4_1_39_0)

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Alcune proprietà della funzione di Möbius nel reticolo dei sottogruppi dei gruppi Alterni e Simmetrici

VALENTINA COLOMBO

Nel lavoro di tesi ci siamo occupati di analizzare alcune proprietà della funzione di Möbius μ definita nel reticolo dei sottogruppi di un gruppo finito; in particolare abbiamo considerato i gruppi Alterni e Simmetrici. Si sono ottenuti risultati riguardanti due distinti problemi.

1. – Primo problema

Sia G un gruppo profinito finitamente generato; definiamo la funzione di Möbius $\mu(H, G)$ nel reticolo dei sottogruppi aperti di G in questo modo: $\mu(G, G) = 1$ e $\sum_{K \geq H} \mu(K, G) = 0$ se $H < G$. In [4] Mann ha proposto di studiare le seguenti questioni:

- 1) Quali sono i gruppi per cui $|\mu(H, G)|$ cresce polinomialmente in termini dell'indice di H ?
- 2) Quali sono i gruppi per cui il numero $b_n(G)$ dei sottogruppi H di indice n , tali che $\mu(H, G) \neq 0$, cresce al massimo polinomialmente in n ?

L'interesse per questi quesiti è legato allo studio della funzione $P_G(t)$, che esprime la probabilità che t elementi di G scelti a caso generino topologicamente G (la probabilità viene definita mediante la misura di Haar normalizzata su G). Come è stato provato da Mann in [4], i gruppi per i quali $|\mu(H, G)|$ e $b_n(G)$ crescono polinomialmente, in termini rispettivamente di $|G : H|$ e n , sono quelli per i quali la somma infinita

$$\sum_{H <_o G} \frac{\mu(H, G)}{|G : H|^s}$$

è assolutamente convergente in qualche semipiano del piano complesso. Quando ciò si verifica, questa somma infinita rappresenta, nel dominio di convergenza, una funzione analitica che assume precisamente il valore $P_G(t)$ per ogni intero positivo t grande abbastanza. Poiché $\mu(M, G) = -1$, per ogni sottogruppo massimale M di G , si ottiene $m_n(G) \leq b_n(G)$ (dove $m_n(G)$ denota il numero dei sottogruppi massimali di G di indice n). In particolare, se $b_n(G)$ cresce polinomialmente, allora G ha crescita polinomiale per i sottogruppi massimali (PMSG). Un risultato di Mann e Shalev ([5]) identifica i gruppi PMSG con i gruppi positivamente finitamente generati (PFG), cioè tali che $P_G(t) > 0$ per qualche scelta di t . Mann ha dunque congetturato la validità di una sorta di proposizione inversa:

Congettura 1 (Mann). Se G è un gruppo PFG, allora $|\mu(H, G)|$ è limitato polinomialmente in $|G : H|$, e $b_n(G)$ ha crescita al massimo polinomiale in n .

Sia $\mathcal{A}(G)$ l'insieme dei gruppi monolitici finiti con zoccolo non abeliano, che sono immagini epimorfe di G ; per ogni $L \in \mathcal{A}(G)$ denotiamo con X_L il gruppo almost simple associato a L , e con $b_n^*(X_L)$ il numero dei sottogruppi K di X_L con $|X_L : K| = n$, $K \text{soc} X_L = X_L$ e $\mu(K, X_L) \neq 0$. Recentemente Lucchini ha dimostrato che per stabilire se un gruppo PFG soddisfa o meno la congettura di Mann, è sufficiente studiare il comportamento della funzione di Möbius dei gruppi almost simple associati agli elementi di $\mathcal{A}(G)$. Più precisamente, ha provato il seguente enunciato ([2]): esistono due costanti γ_1 e γ_2 tali che $b_n(G) \leq n^{\gamma_1}$ e $|\mu(H, G)| \leq |G : H|^{\gamma_2}$, per ogni $n \in \mathbb{N}$ e per ogni sottogruppo aperto H di G , se e solo se esistono due costanti c_1 e c_2 tali che $b_n^*(X_L) \leq n^{c_1}$ e $|\mu(Y, X_L)| \leq |X_L : Y|^{c_2}$, per ogni $L \in \mathcal{A}(G)$, ogni $n \in \mathbb{N}$ ed ogni $Y \leq X_L$ con $Y \text{soc} X_L = X_L$.

Pertanto la congettura di Mann è vera se vale la seguente:

Congettura 2 (Lucchini). Esistono due costanti c_1 e c_2 tali che per ogni gruppo almost simple finito X si ha: $b_n^*(X) \leq n^{c_2}$ per ogni $n \in \mathbb{N}$, e $|\mu(Y, X)| \leq |X : Y|^{c_1}$ per ogni $Y \leq X$ con $Y \text{soc} X = X$.

Si è dimostrato che questa congettura è vera per tutti i gruppi Alterni e Simmetrici:

TEOREMA 1. — *Esiste una costante α tale che per ogni $n \in \mathbb{N}$, se $G \in \{\text{Alt}(n), \text{Sym}(n)\}$ e $m \in \mathbb{N}$, allora $b_m(G) \leq m^\alpha$.*

TEOREMA 2. — *Esiste una costante β tale che per ogni $n \in \mathbb{N}$, se $G \in \{\text{Alt}(n), \text{Sym}(n)\}$ e $H \leq G$, allora $|\mu(H, G)| \leq |G : H|^\beta$.*

Strumento fondamentale nelle dimostrazioni di questi teoremi è il teorema di chiusura di Crapo. Come conseguenza di tale teorema, risulta che se G è un gruppo di permutazione transitivo su un insieme Γ , al fine di limitare superiormente il numero dei sottogruppi H con $\mu(H, G) \neq 0$, e di stimare $|\mu(H, G)|$, è sufficiente ottenere:

- 1) limiti simili per il particolare caso in cui H sia transitivo;
- 2) stime sul numero dei sottogruppi di G che sono massimali rispetto alla proprietà di avere un certo insieme di orbite (sottogruppi Γ -chiusi), e limiti sul numero di orbite di un sottogruppo Γ -chiuso H , in termini dell'indice $|G : H|$.

Quando $G \in \{\text{Alt}(n), \text{Sym}(n)\}$, il punto 2) è facile, poiché un sottogruppo chiuso è coniugato a $(\text{Sym}(n_1) \times \cdots \times \text{Sym}(n_r)) \cap G$, con $n_1 + n_r = n$. Il punto 1) può essere risolto considerando l'azione di G sull'insieme $\mathcal{A}_n = \{(a, b) \mid 1 \leq a, b \leq n, a \neq b\}$. In tal modo è sufficiente avere informazioni sul numero di Möbius dei sottogruppi $\mathcal{A}_n$ -transitivi di G (ma questi sono precisamente i sottogruppi 2-transitivi di G), e calcolare quanti sottogruppi transitivi di G sono $\mathcal{A}_n$ -chiusi.

Si è inoltre dimostrato che il limite sul numero di Möbius di un sottogruppo H (Teorema 2) può essere migliorato se $G \in \{\text{Alt}(p), \text{Sym}(p)\}$, con p un primo “buono”; infatti vale il seguente teorema.

TEOREMA 3. – *Supponiamo p primo, con $p \neq 11, 23$ e $p \neq (q^d - 1)/(q - 1)$, per ogni coppia di numeri naturali (q, d) , con q potenza di primo e $q > 4$ se $d = 2$. Se $G \in \{\text{Alt}(p), \text{Sym}(p)\}$ e $H \leq G$, allora $|\mu(H, G)| \leq |G : H|$.*

Il risultato del Teorema 3 non vale per un generico grado $n \in \mathbb{N}$; ma ci induce a formulare la seguente congettura:

Congettura 3. Esiste una costante γ tale che $\forall n \in \mathbb{N}$, se $G \in \{\text{Alt}(n), \text{Sym}(n)\}$ e $H \leq G$, allora

$$|\mu(H, G)| \leq \gamma \cdot |G : H|.$$

2. – Secondo problema

Consideriamo ora un problema riguardante la funzione zeta probabilistica di un gruppo finito. Sia G un gruppo finito; denotiamo con $P_G(t)$ la probabilità che t elementi di G , scelti a caso, generino G stesso. La funzione intera $P_G(t)$ è interpolata da una funzione complessa $P_G(s)$, definita come:

$$P_G(s) := \sum_{|G:H|=n} \frac{\mu(H, G)}{n^s}$$

Chiamiamo funzione zeta probabilistica di G l'inverso moltiplicativo della funzione $P_G(s)$. In un recente lavoro (si veda [3]), Lucchini e Massa hanno provato che esistono espliciti criteri per stabilire se un gruppo quoziente $G/\text{Frat}(G)$ sia o meno isomorfo ad $\text{Alt}(n)$ (con $n \geq 5$) conoscendo solo i coefficienti di $P_G(s)$. Utilizzando questi risultati, sono poi stati in grado di dimostrare che se $P_G(s) = P_{\text{Sym}(n)}(s)$ ($n \geq 5$), allora o $G/\text{Frat}(G) \cong \text{Sym}(n)$ oppure $G/\text{Frat}(G) \cong \text{Alt}(n) \times C_2$. Ci occupiamo di determinare quali valori di n soddisfanno la seguente equazione:

$$(1) \quad P_{\text{Sym}(n)}(s) = P_{\text{Alt}(n) \times C_2}(s) = P_{\text{Alt}(n)}(s) \cdot P_{C_2}(s)$$

Equivalente a stabilire quando valga: $P_{\text{Sym}(n), \text{Alt}(n)}(s) = P_{\text{Alt}(n)}(s)$. Molti autori hanno studiato questo problema e, usando GAP, si conoscono già i valori di n , più piccoli di 12, che soddisfano l'uguaglianza (1). Boston e Mann in [1] hanno formulato la seguente congettura:

Congettura 4 (Boston, Mann). La validità di (1), per $n \geq 5$, riflette la non esistenza di sottogruppi massimali di $\text{Alt}(n)$ che coincidano col loro normalizzante in $\text{Sym}(n)$.

Si verifica che questa congettura vale quando n è primo. Infatti se p è un primo “buono” (cioè $\text{Sym}(p)$ non contiene alcun sottogruppo transitivo di tipo almost simple) proviamo il seguente:

TEOREMA 4. – *Sia $p \geq 5$ primo, $p \neq 11, 23$ e $p \neq (q^d - 1)/(q - 1)$. Allora*

$$P_{\text{Sym}(p), \text{Alt}(p)}(s) = P_{\text{Alt}(p)}(s).$$

Altrimenti $\text{Alt}(p)$ possiede qualche sottogruppo massimale che coincide col suo normalizzante in $\text{Sym}(p)$; in tali casi proviamo il seguente teorema:

TEOREMA 5. – Se $p = 11$, $p = 23$ o $p = (q^d - 1)/(q - 1) > 5$, allora

$$P_{\text{Sym}(p), \text{Alt}(p)}(s) \neq P_{\text{Alt}(p)}(s).$$

Nelle dimostrazioni di questi teoremi usiamo spesso la formula esprimente la differenza tra $P_{\text{Sym}(n), \text{Alt}(n)}(s)$ e $P_{\text{Alt}(n)}(s)$; da questa formula si possono derivare alcune condizioni sufficienti (ma non necessarie) a garantire $P_{\text{Sym}(n), \text{Alt}(n)}(s) = P_{\text{Alt}(n)}(s)$.

La congettura di Boston e Mann non è vera in generale per $n \geq 5$: ad esempio quando $n = 21$ o $n = 62$ la congettura non vale. Non è facile stabilire se $\text{Sym}(n)$ soddisfi o meno tale congettura. In particolare è molto difficile studiare le intersezioni fra i sottogruppi imprimitivi: è possibile, ad esempio, che l'intersezione di alcuni (persino due) sottogruppi massimali imprimitivi di $\text{Sym}(n)$ sia già contenuta in $\text{Alt}(n)$ (è il caso di $n = 21$), e questo fatto potrebbe far fallire la congettura.

Concludiamo presentando una questione tuttora non risolta. Consideriamo i gruppi Simmetrici $\text{Sym}(n)$ che non contengono alcun sottogruppo proprio primitivo, diverso da $\text{Alt}(n)$. È noto che la famiglia $\overline{\mathcal{F}}$ di questi gruppi ha densità 1 nell'insieme di tutti i gruppi Simmetrici. È naturale chiedersi se $\text{Sym}(n) \in \overline{\mathcal{F}}$ soddisfi o meno la congettura di Boston e Mann, e se tutti i gruppi Simmetrici in $\overline{\mathcal{F}}$ abbiano lo stesso comportamento. Non abbiamo ancora ottenuto una risposta a questa domanda. La possibilità di esprimere sottogruppi del gruppo Alterno come intersezione di due (o più) sottogruppi massimali imprimitivi del gruppo Simmetrico, potrebbe implicare l'esistenza di un controesempio alla congettura anche tra i gruppi di $\overline{\mathcal{F}}$. Siamo però inclini a pensare che, se tale controesempio esiste, il grado debba essere scelto piuttosto grande.

BIBLIOGRAFIA

- [1] N. BOSTON, *A probabilistic generalization of the Riemann zeta function*, Analytic Number Theory vol. 1 (Allerton Park, IL, 1995) **138** (1996), 155-162.
- [2] A. LUCCHINI, *On the subgroups of a monolithic group with non trivial Möbius number*, in preparation.
- [3] A. LUCCHINI e M. MASSA, *The probabilistic zeta function of Alternating and Symmetric groups*, Algebra Colloquium **16** (2009), no. 2, 195-210.
- [4] A. MANN, *A probabilistic zeta function for arithmetic groups*, Internat. J. Algebra Comput. **15** (2005), no. 5-6, 1053-1059.
- [5] A. MANN e A. SHALEV, *Simple groups, maximal subgroups and probabilistic aspects of profinite groups*, Israel J. Math. **96** (1996), 449-468.

Dipartimento di Matematica Pura e Applicata, Università di Padova
e-mail: vcolombo@math.unipd.it

Scuola di Dottorato in Scienze Matematiche, Indirizzo Matematica
con sede presso l'Università di Padova – Ciclo XXII
Direttore di ricerca: Prof. Andrea Lucchini, Università di Padova