Matematica, Cultura e Società

Rivista dell'Unione Matematica Italiana

Andrea Lucchini

Un approccio asintotico alla teoria dei gruppi finiti

Matematica, Cultura e Società. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **10** (2025), n.2, p. 187–197.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RUMI_2025_1_10_2_187_0>

Matematica, Cultura e Società. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2025.

Matematica, Cultura e Società – Rivista dell'Unione Matematica Italiana
Serie I, Vol. 10, N. 2, agosto 2025, 187-197

Un approccio asintotico alla teoria dei gruppi finiti

Andrea Lucchini
Università degli Studi di Padova
E-mail: lucchini@math.unipd.it

Sommario: *Nella letteratura dedicata allo studio dei gruppi finiti appare sempre più frequentemente la denominazione "asymptotic group theory". Questa denominazione, un po' generica, si riferisce a tutte quelle situazioni in cui si considera un invariante numerico associato allo studio dei gruppi finiti e ci si chiede se, escluse le oscillazioni anche notevoli che si osservano nell'insieme dei valori assunti dall'invariante in questione se si considera solo una porzione molto limitata di gruppi finiti, emerge un andamento più regolare e in qualche modo descrivibile se si allarga l'orizzonte a famiglie sempre più grandi. In altri termini si studia l'andamento asintotico dell'invariante in questione. In questa esposizione ci proponiamo di analizzare una serie di situazioni di questo tipo, concentrandoci su esempi che possono essere introdotti e descritti usando solo le nozioni più elementari della teoria dei gruppi.*

Abstract: *In the literature dedicated to the study of finite groups, the term 'asymptotic group theory' appears increasingly frequently. This somewhat generic term refers to all those situations where a numerical invariant associated with the study of finite groups is considered, and one wonders if, excluding the sometimes significant fluctuations observed in the set of values assumed by the invariant when considering only a very limited portion of finite groups, a more regular and somewhat describable pattern emerges when the horizon is broadened to increasingly larger families. In other words, the asymptotic behavior of the invariant in question is studied. In this exposition, we aim to analyze a series of situations of this type, focusing on examples that can be introduced and described using only the most elementary notions of group theory.*

1. – Introduzione

Negli ultimi anni si parla sempre più frequentemente di "teoria asintotica dei gruppi". È una denominazione un po' vaga, che include situazioni e problematiche anche abbastanza diverse. In questa esposizione presterò particolare attenzione all'approccio asintotico alla teoria dei gruppi finiti, che si presta, a mio parere, a essere illustrato senza bisogno di troppe nozioni tecniche. In particolare vorrei concentrarmi su esempi che possono essere raccontati usando soltanto le nozioni di teoria dei gruppi che vengono impartite ai nostri studenti nei primi anni della laurea triennale in matematica.

Accettato: 9 giugno 2025.

L'idea di base è considerare un qualche invariante numerico collegato allo studio dei gruppi finiti, ad esempio il numero di sottogruppi di un gruppo finito, il numero di gruppi finiti di ordine assegnato, l'ordine medio di un elemento nel gruppo simmetrico. Se si considera solo un gruppo particolare, o una famiglia di pochi gruppi finiti, il valore assunto da quell'invariante appare in genere caotico e privo di particolare significato. Ma se ci si colloca a una opportuna distanza, osservando una porzione più ampia di gruppi, molto spesso si scopre una certa regolarità nel comportamento di quel particolare invariante. Può succedere che l'invariante considerato cambi fortemente, senza nessuna evidente regolarità. Però in molto casi, un'indagine più accurata rivela l'esistenza di limitazioni inferiori e superiori asintoticamente ottimali e in diversi casi si

osserva una maggiore regolarità se si considerano opportune sottofamiglie della famiglia dei gruppi presi in considerazione.

L'attenzione a risultati di questo tipo non è nuova. Incontreremo nei diversi esempi che prenderemo in considerazioni contributi databili all'inizio del secolo scorso, ma indubbiamente la ricerca in questa direzione è stata fortemente stimolata dallo sviluppo della "teoria computazionale dei gruppi". Nell'ideazione e implementazione di algoritmi che permettano di studiare i gruppi finiti con l'ausilio dei computer è molto importante avere stime asintotiche per poter analizzare l'efficienza di tali algoritmi.

Anche se concentrerò la mia attenzione su questioni collegate ai gruppi finiti, vorrei menzionare che i metodi e risultati descritti si applicano anche allo studio di gruppi infiniti, ad esempio collegando le proprietà strutturali di un gruppo infinito al comportamento asintotico di invarianti calcolati nella famiglia dei gruppi finiti che ne compaiono come immagini epimorfe.

2. – L'enumerazione dei gruppi finiti

1. Dato un numero intero positivo n, indichiamo con $f(n)$ il numero di gruppi di ordine n (contati a meno di isomorfismo). È naturale chiedersi se ci sia un qualche tipo di regolarità nell'andamento della successione $\{f(n)\}_{n\in\mathbb{N}}$. Un esercizio alla portata di uno studente dei primi anni di un corso di studi in matematica è determinare i primi 15 valori di questa successione: si ha $f(n)=1$ se $n\in\{1,2,3,5,7,11,13,15\}$, $f(n)=2$ se $n\in\{4,6,9,10,14\}$, $f(n)=5$ se $n\in\{8,12\}$. Questi primi valori non permettono di fare grandi previsioni sull'andamento della successione, ma anche chi non ha alcuna familiarità con la teoria dei gruppi è portato a congetturare che $f(n)$ sia uguale ad 1 se n è un numero primo, come di fatto insegnamo ai nostri studenti. Determinare invece $f(16)$ è un esercizio troppo difficile. Furono Otto Hölder [21] e Jacob Young [49], nel 1893, i primi a provare che $f(16)=14$.

Negli ultimi anni si è notevolmente sviluppata la teoria computazionale dei gruppi, che permette di studiare proprietà dei gruppi finiti per mezzo di un computer. Tra i risultati di maggior rilievo ottenuti c'è la costruzione, dovuta a Hans Ulrich Besche, Bettina Eick e Eamon O'Brien [2] della completa libreria dei gruppi di ordine minore o uguale a 2.000. Possiamo pertanto usare questa libreria per determinare i primi 2.000 valori nella nostra successione. Evidenziamo i fatti seguenti: ci sono quasi 50 miliardi di gruppi di ordine minore o uguale a 2.000 (esattamente 49.910.531.351). D'altra parte, se analizziamo i valori ottenuti da $f(n)$ per $n\leq 2.000$, scopriamo che in 1.490 casi otteniamo valori inferiori a 10, in 1.863 valori inferiori a 100, in 1.952 valori inferiori a 1.000, in 1.992 valori inferiori a 10.000. Solo in 6 casi risulta $f(n)\geq 1.000.000$. Chi sono questi 6 valori? Eccoli:

$$\begin{aligned} f(2^8\cdot 7) &= 1.083.553,\\ f(2^8\cdot 3) &= 1.090.235,\\ f(2^8\cdot 5) &= 1.116.461,\\ f(2^9) &= 10.494.213,\\ f(2^9\cdot 3) &= 408.641.062,\\ f(2^{10}) &= 49.487.367.289. \end{aligned}$$

Da tutti questi valori si ricava soprattutto la seguente impressionante osservazione: più del 99% dei gruppi di ordine minore o uguale di 2.000 ha ordine 2^{10}.

Cosa abbiamo imparato a questo punto sulla nostra successione? In realtà ancora abbastanza poco, ma ci siamo resi conto che il valore $f(n)$ è particolarmente elevato quando c'è un primo che divide n con molteplicità elevata. Ci viene voglia di studiare una successione diversa. Fissiamo un primo p e vediamo come cresce la successione $\{f(p^m)\}_{m\in\mathbb{N}}$.

Per $p=2$ disponiamo dei seguenti primi valori:

$$\begin{gathered} f(2)=1, f(2^2)=2, f(2^3)=8, f(2^4)=14, f(2^5)=51,\\ f(2^6)=267, f(2^7)=2.328, f(2^8)=56.092,\\ f(2^9)=10.494.213, f(2^{10})=49.487.367.289. \end{gathered}$$

Per $p=3$, i valori noti sono i sequenti:

$$\begin{gathered} f(3)=1, f(3^2)=2, f(3^3)=5, f(3^4)=15,\\ f(3^5)=67, f(3^6)=504, f(3^7)=9.310. \end{gathered}$$

In base a questi dati, per quanto limitati, ci si può aspettare che, comunque si fissi il primo p, la successione $\{f(p^m)\}_{m\in\mathbb{N}}$ tenda all'infinito molto velocemente. Ma quanto velocemente?

Una prima risposta la diede Graham Higman [20] nel 1960, dimostrando che, per ogni primo p e ogni

intero positivo m risulta

$$f(p^m) \geq p^{\frac{2}{27}(m^3-6m^2)}. \tag{2.1}$$

Pochi anni dopo, nel 1965, Charles Sims [47] diede una limitazione superiore al valore di $f(p^m)$ dimostrando

$$p^{\frac{2}{27}(m^3+O(m^{\frac{8}{3}}))} \geq f(p^m). \tag{2.2}$$

Le due disuguaglianze (2.1) e (2.2) si possono conglobare in un unico enunciato, che fornisce una indicazione molto precisa sull'andamento asintotico della successione $\{f(p^m)\}_{m\in\mathbb{N}}$:

$$f(p^m) = p^{\frac{2}{27}m^3(1+o(1))}. \tag{2.3}$$

La precedente formula stimola la domanda: perchè proprio $2/27$? Non è molto difficile scoprirlo. Un ruolo chiave nello studio dei p-gruppi finiti è svolto dal loro sottogruppo di Frattini. Il sottogruppo di Frattini di un gruppo finito G è l'intersezione dei sottogruppi massimali di G. Nella sua dimostrazione, Higman prova che, fissati due interi positivi a, b con $a+b=m$, il numero di gruppi di ordine p^m il cui sottogruppo di Frattini ha indice p^a e ordine p^b è all'incirca $p^{\frac{a^2b}{2}}$: la funzione $\dfrac{a^2b}{2}$, soggetta al vincolo $a+b=m$, assume il suo massimo per $a=\dfrac{2}{3}m$ e questo massimo è per l'appunto $\dfrac{2}{27}m^3$.

Abbiamo visto così che la successione $\{f(n)\}_{n\in\mathbb{N}}$ ha un andamento asintotico ben determinato quando viene ristretta ai numeri interi positivi che sono potenza di primo. Ma cosa succede per i rimanenti valori?

Per affrontare questa questione dobbiamo richiamare la teoria di Sylow. Supponiamo $n = p_1^{a_1}\cdots p_k^{a_k}$ con $p_1,\ldots,p_k$ primi distinti. I teoremi di Sylow ci garantiscono che un gruppo G di ordine n contiene un sottogruppo P_i di ordine $p_i^{a_i}$ per ogni $1\leq i\leq k$ e tale P_i è univocamente determinato a meno di isomorfismo.

Consideriamo allora $P_1,\ldots,P_k$ di ordini, rispettivamente, $p_1^{a_1},\ldots,p_t^{a_k}$. Quanti sono i gruppi di ordine n che hanno i sottogruppi di Sylow isomorfi a $P_1,\ldots,P_k$? La risposta è stata fornita da László Pyber [42] nel 1993.

Sia $\mu = \max_{1\leq i\leq k} a_i$ e siano $P_1,\ldots,P_k$ gruppi di ordine $p_1^{a_1},\ldots p^{a_k}$. Il numero di gruppi di ordine $n = p_1^{a_1}\cdots p_k^{a_k}$ con sottogruppi di Sylow isomorfi a $P_1,\ldots,P_k$ è al più $n^{75\mu+16}$. Combinando questo risultato, la cui dimostrazione è particolarmente profonda e coinvolge in diversi passaggi la classificazione dei gruppi semplici finiti, con i risultati di Higman e Sims, si ottiene infine una stima asintotica dell'andamento della successione $\{f(n)\}_{n\in\mathbb{N}}$.

$$f(n) \leq n^{\left(\frac{2}{27}+o(1)\right)\mu^2} \text{ per} \mu\to\infty. \tag{2.4}$$

Nonostante questo risultato di Pyber sia molto preciso e significativo, restano aperte affascinanti questioni. Per esempio abbiamo osservato prima che più del 99% dei gruppi di ordine ≤ 2.000 ha ordine 2^{10}. Questo suggerisce la seguente domanda, che non ha ancora trovato risposta: possiamo dire che il numero di gruppi di ordine al più n è "dominato" da $f(2^m)$ essendo 2^m la più grande potenza di 2 minore o uguale ad n?

2. Invece di enumerare tutti i gruppi di ordine n, si possono contare solo i gruppi di ordine n che soddisfano a qualche ulteriore proprietà. Un contributo significativo in questa direzione è dovuto a Derek Holt [22]. Ricordiamo che un gruppo G è detto perfetto se non contiene nessun sottogruppo normale proprio N tale che G/N sia abeliano. Holt ha fornito una stima asintotica per il numero $h_{\text{perf}}(n)$ dei gruppi perfetti di ordine minore o uguale ad n, dimostrando che

$$n^{\frac{(\log_2(n))^2}{108}-\frac{13\log_2(n)}{36}} \leq h_{\text{perf}}(n) \leq n^{\frac{(\log_2(n))^2}{48}+\log_2(n)}. \tag{2.5}$$

Utilizzando i risultati di Higman e Sims per stimare $h(n)=\sum_{m\leq n} f(m)$, Holt prova anche

$$\lim_{n\to\infty}\frac{h_{\text{perf}}(n)}{h(n)} = 0,$$

in altre parole, parafrasando la battuta in un celebre film, "quasi nessun gruppo finito è perfetto". Anche in questo caso, i recenti sviluppi della teoria dei gruppi computazionali ci permettono di disporre di verifiche sperimentali di questo risultato: ci sono soltanto 15.768 gruppi perfetti di ordine al più 2.000.0000 [23]. Vale anche la pena di osservare che

circa il 46% di questi gruppi perfetti ha ordine $1.966.080 = 2^{17} \cdot 3 \cdot 5$.

3. Un gruppo finito di ordine n può essere generato con $[\log_2(n)]$ elementi, ma molto spesso basta un numero decisamente più basso di elementi. Ad esempio 2.149 dei 2.328 gruppi di ordine 2^7 possono essere generati con 4 elementi. È quindi interessante, fissato $d \in \mathbb{N}$, considerare il numero $f(n,d)$ di gruppi di ordine n generabili con d elementi e studiare l'andamento asintotico della successione $\{f(n,d)\}_{n\in\mathbb{N}}$. In [40] si prova che, per ogni primo p,

$$f(p^m,d) \leq p^{\frac{(d+1)m^2}{2}+O(m)}. \tag{2.6}$$

Nel 2001 Alex Lubotzky [34] ha generalizzato questo risultato, provando che esiste una costante c tale che

$$f(n,d) \leq n^{cd\log_2(n)}$$

per ogni $n, d \in \mathbb{N}$. Questa stima è del corretto ordine di grandezza. Infatti Avinoam Mann [38] ha provato che per ogni $d > 1$ esiste una costante positiva c_d tale che $f(p^m,d) \geq p^{c_d m^2}$ per ogni potenza di primo p^m.

3. – Sottogruppi e classi di coniugio

1. Denotiamo con $\sigma(G)$ il numero di sottogruppi di un assegnato gruppo G. Recentemente, rendendo più preciso un risultato contenuto in [3], Marco Fusari e Pablo Spiga [17] hanno dimostrato che, per ogni gruppo finito G, risulta

$$\sigma(G) \leq c|G|^{\frac{\log_2(|G|)}{4}}$$

essendo

$$c = \prod_{i\geq 1} \frac{1}{1-\frac{1}{2^i}} \left(-1+2\sum_{k=0}^{\infty}\frac{1}{2^{k^2}}\right) \sim 7.37197.$$

Questa stima è asintoticamente ottimale. Infatti se indichiamo con P_n il prodotto diretto di n gruppi ciclici di ordine 2 allora

$$\lim_{n\to\infty} \frac{\sigma(|P_n|)}{|P_n|^{\frac{\log_2(|P_n|)}{4}}} = c.$$

Cosa possiamo dire se, invece di considerare tutti i sottogruppi di un gruppo finito, consideriamo solo quelli massimali? Nel 1961 Tim Wall [48] congetturò che il numero di sottogruppi massimali di un gruppo finito G fosse al più $|G|-1$ (questa sarebbe una stima ottimale, perchè il prodotto diretto di n gruppi ciclici di ordine 2 ha ordine 2^n e contiene esattamente 2^n-1 sottogruppi massimali). Lo stesso Wall provò che la congettura è vera per ogni gruppo finito risolubile. Nel 2007 Liebeck, Pyber e Shalev [32] provarono un enunciato più debole (esiste una costante c tale che ogni gruppo finito G contiene al più $2c|G|^{\frac{3}{2}}$ sottogruppi massimali) ma nello stesso lavoro dimostrarono anche che i gruppi semplici finiti, tranne un numero finito di possibili eccezioni, soddisfano alla congettura di Wall. Un inaspettato colpo di scena si verificò nel 2012. Per renderne conto, devo qui essere un po' più tecnico che nel resto di questa esposizione. Il lettore che abbia meno familiarità con le nozioni che sto per usare non si spaventi. È una breve parentesi che mi permetto, con la giustificazione che quello che sto descrivendo è stato uno degli eventi più significativi tra gli approcci asintotici alla teoria dei gruppi degli ultimi anni. Successivamente tornerò a utilizzare solo nozioni assolutamente di base. Scommettendo che la congettura fosse vera per tutti i gruppi semplici, il caso critico che si prospettava era quello del prodotto semidiretto di uno spazio vettoriale V con un gruppo semplice G che agisce su V irriducibilmente e fedelmente. Il conto del numero di sottogruppi massimali di tale prodotto semidiretto richiede il calcolo della dimensione del primo gruppo di coomologia $\mathrm{H}^1(G,V)$. Nel 1986 Bob Guralnick aveva congetturato che tale dimensione fosse limitata da una costante assoluta valida in tutti i casi. In realtà, ai fini della congettura di Wall, quello che basta, e che è in ogni caso necessario, è limitare la dimensione di $\mathrm{H}^1(G,V)$ in funzione del rango di Lie di G nel caso in cui G sia un gruppo semplice di tipo Lie. Nel giugno del 2012 fu organizzato, presso l'American Institute of Mathematics (San Jose, California), un workshop intitolato "Cohomology bounds and growth rates", dedicato a recenti sviluppi che sembravano prospettare un'imminente dimostrazione della congettura di Guralnick. Il terzo giorno del workshop Leonard Scott, uno degli organizzatori, riferì di alcune evidenze computazionali ottenute da un suo studente, Tim Sprowl, che prospettavano l'esistenza di esempi in cui la dimensione di $\mathrm{H}^1(G,V)$ assumesse valori non

contrari alla congettura di Guralnick ma comunque superiori alle aspettative. Uno dei partecipanti al workshop, Frank Luebeck, era un esperto di teoria dei gruppi computazionale, e riuscì a far girare durante la notte un programma da lui implementato per effettuare computazioni proibitive che nessuno finora era riuscito a completare. Tra gli esempi che Luebeck riuscì a testare, se ne presentarono alcuni che smentirono sia la congettura di Guralnick che la congettura di Wall. Nei giorni successivi questo approccio portò a concludere che non solo la congettura di Wall era falsa, ma che si potevano esibire infiniti controesempi. È curioso tuttavia osservare che in tutti i controesempi noti, il numero di sottogruppi massimali di G è comunque inferiore a $|G|^{1+a}$, con $a < 1/1000$. Quindi seppur falsa, la congettura predice un numero di sottogruppi massimali di pochissimo inferiore a quello che in realtà sembra potersi verificare.

2. Ricordo che due elementi g_1, g_2 di un gruppo G si dicono coniugati in G se esiste $x \in G$ tali che $g_2 = x^{-1}g_1x$. La relazione di coniugazione è una relazione di equivalenza e le classi di equivalenza vengono dette classi di coniugazione. Indichiamo con $\kappa(G)$ il numero di classi di coniugazione di un dato gruppo G. Chiaramente $\kappa(G) \leq |G|$, e vale l'uguaglianza se e solo se G è un gruppo abeliano. Ma quanto più piccolo può essere $\kappa(G)$ rispetto a $|G|$? Una prima rilevante osservazione relativamente a questa domanda la si può trovare in un lavoro di Edmund Landau [30] del 1903. Rispondendo a un quesito proposto da Frobenius, Landau dimostra che, per ogni intero positivo t, esiste solo un numero finito di gruppi finiti G con $k(G) = t$. Come osservato da Richard Brauer, l'argomento usato da Landau permette di dimostrare che, per ogni gruppo finito G, risulta

$$\kappa(G) \geq \log_2(\log_2(|G|)).$$

Val la pena di osservare che, contrariamente a quanto si può essere portati a congetturare in base a questo risultato, esistono gruppi infiniti in cui tutti gli elementi diversi dall'identità sono tra loro coniugati.

In una sua famosa raccolta di problemi aperti, Brauer [4] propose di cercare una stima inferiore sostanzialmente più fine. Segue da un classico risultato di Philip Hall che $\kappa(G) \geq \log_2(|G|)$ per ogni gruppo G finito e nilpotente, mentre Mark Cartwright [6] dimostrò che esiste una costante positiva a tale che, per ogni gruppo finito risolubile G, si ha $\kappa(G) \geq a(\log_2 |G|)^b$, con $b \sim 0.00347$. D'altra parte László Kovács e Charles Leedham-Green [28] hanno provato che per ogni primo dispari p esiste un gruppo P di ordine p^p con $\kappa(P) = (p^3 - p^2 + p + 1)/2$. Quindi esistono gruppi con ordine n arbitrariamente grande, ma con meno di $(\log_2(n))^3$ classi di coniugazione.

La migliore risposta alla questione proposta da Brauer è al momento quella data da Thomas Keller [27] nel 2011: esiste una costante $\epsilon > 0$, esplicitamente computabile, tale che per ogni gruppo G di ordine $n \geq 4$, risulta

$$k(G) \geq \frac{\epsilon \log_2 n}{(\log_2 \log_2 n)^7}.$$

3. Concludiamo questa sezione con un'altra domanda piuttosto naturale e concreta. Quanto è lontano un gruppo finito dall'essere abeliano? Formalizziamo meglio la domanda. Ogni gruppo finito G contiene sottogruppi abeliani (ad esempio tutti i suoi sottogruppi ciclici). Si può dire che almeno uno di questi sottogruppi abeliani ha ordine "grande" in funzione dell'ordine del gruppo G?

Lo studio di questa questione comincia con un contributo di Paul Erdös e Ernst Gabor Straus [9] che nel 1976 hanno dimostrato che ogni gruppo di ordine n contiene un sottogruppo abeliano di ordine approssimativamente uguale a $\log_2 n$. Questo risultato è stato perfezionato da Pyber [43], dimostrando che esiste $\epsilon > 0$ tale che ogni gruppo di ordine n contiene un sottogruppo abeliano di ordine almeno $2^{\epsilon\sqrt{\log_2 n}}$.

Merita di essere menzionato un altro risultato asintotico contenuto in [9]. Denotiamo con $\alpha_t(G)$ il numero di t-uple ordinate di elementi di G che commutano a due a due. Risulta che $\dfrac{\alpha_t(G)}{\alpha_{t-1}(G)}$ tende all'infinito con il crescere dell'ordine di $|G|$.

4. – Il gruppo simmetrico

Riconsideriamo adesso alcune delle questioni proposte nella sezione precedente nel caso particolare del

gruppo simmetrico $\mathrm{Sym}(n)$, ossia il gruppo delle permutazioni dell'insieme $\{1,\dots,n\}$.

1. È ben noto che il numero di classi di coniugazione $\kappa(\mathrm{Sym}(n))$ del gruppo simmetrico di grado n coincide con il numero di partizioni di n, ossia con il numero $p(n)$ di modi di scrivere n come somma di interi positivi, senza tener conto dell'ordine degli addendi. Determinare l'andamento asintotico di $\kappa(\mathrm{Sym}(n))$ al crescere di n si riduce quindi a un problema di teoria dei numeri (qual è l'andamento asintotico della funzione di partizione?), a cui hanno dato soluzione Ramanujan e Hardy nel 1918. Ricordiamo anche un risultato di Kovács e Robinson [29], in base al quale $\kappa(G) \leq 5^{n-1}$ per ogni $G \leq \mathrm{Sym}(n)$.

Cosa succede invece se consideriamo il numero $\sigma(\mathrm{Sym}(n))$ dei sottogruppi di $\mathrm{Sym}(n)$? Utilizzando un computer possiamo ricavare alcuni dati sperimentali, per farci una vaga idea della rapidità con cui cresce $\sigma(\mathrm{Sym}(n))$ all'aumentare del valore di n. Nella seconda colonna della tabella successiva sono indicati i valori di $\sigma(\mathrm{Sym}(n))$ al variare di n tra 1 e 12. Molti di questi sottogruppi sono tra di loro isomorfi, così nella terza colonna viene riportato il numero di sottogruppi di $\mathrm{Sym}(n)$, contati a meno di isomorfismo.

1	1	1
2	2	2
3	6	4
4	30	9
5	156	16
6	1455	29
7	11300	55
8	151221	137
9	1694723	241
10	25594446	453
11	404126228	894
12	10594925360	2065

Come in altre situazioni descritte prima, ci si rende conto che $\sigma(\mathrm{Sym}(n))$ cresce molto rapidamente. Una descrizione alquanto precisa dell'andamento asintotico della successione $\{\sigma(\mathrm{Sym}(n))\}_{n\in\mathbb{N}}$ è stata ottenuta solo recentemente da Colva Roney-Dougal e Gareth Tracey [45], che hanno provato il seguente risultato: esistono due costanti $\alpha > 0$ e β tali che, per ogni $n > 1$, risulta

$$2^{\frac{n^2}{16}+\alpha n \log n} \leq \sigma(\mathrm{Sym}(n)) \leq 2^{\frac{n^2}{16}+\beta n^{\frac{3}{2}}}. \tag{4.1}$$

In [26] invece si dimostra che il numero di sottogruppi di $\mathrm{Sym}(n)$, contati a meno di isomorfismo, è almeno $2^{\frac{n^2}{36}-o(n^2)}$. Si può calcolare che circa il 42% dei sottogruppi di $\mathrm{Sym}(12)$ ha ordine potenza di 2. Si congettura che questa proporzione si avvicini ad 1 al crescere di n, ma manca ancora la dimostrazione di un risultato di questo tipo.

2. Ci si può anche chiedere con quale probabilità un sottogruppo casuale di $\mathrm{Sym}(n)$ soddisfi a determinate proprietà permutazionali. Ad esempio è interessante studiare il numero $f_{\mathrm{trans}}(n)$ di sottogruppi di $\mathrm{Sym}(n)$ che sono transitivi (ricordiamo che $G \leq \mathrm{Sym}(n)$ è transitivo se, per ogni $1 \leq i \leq j \leq n$, esiste $g \in G$ tale che $g(i) = j$). In [35] si dimostra che esiste una costante positiva β tale che

$$f_{\mathrm{trans}}(n) \leq 2^{\frac{\beta n^2}{\sqrt{\log n}}}. \tag{4.2}$$

Combinando (4.1) e (4.2), si deduce che la probabilità che un sottogruppo casuale di $\mathrm{Sym}(n)$ sia transitivo tende a zero quando n va all'infinito. A questo risultato si può collegare anche il seguente: con il tendere di n all'infinito tende a 1 la probabilità che un arbitrario elemento g di $\mathrm{Sym}(n)$ abbia la proprietà che gli unici sottogruppi transitivi di $\mathrm{Sym}(n)$ che lo contengono siano $\mathrm{Sym}(n)$ e il gruppo alterno $\mathrm{Alt}(n)$ [37].

3. Tra i sottogruppi transitivi di $\mathrm{Sym}(n)$, sono particolarmente importanti quelli primitivi. Ricordiamo che un sottogruppo transitivo G di $\mathrm{Sym}(n)$ è detto primitivo se le uniche partizioni di $\{1,\dots,n\}$ invarianti per l'azione di G sono quella che consiste degli n blocchi $\{1\},\dots,\{n\}$ e quella che consiste dell'unico blocco $\{1,\dots,n\}$. In tantissimi casi, la dimostrazione di un qualsiasi risultato riguardante i gruppi di permutazione transitivi si riduce al caso primitivo, quindi non sarebbe sbagliato affermare che i gruppi primitivi svolgono nell'ambito dello studio dei gruppi di permutazione un ruolo paragonabile a quello svolto dai gruppi semplici nello studio dei gruppi finiti. Per $n \geq 3$, $\mathrm{Sym}(n)$ e $\mathrm{Alt}(n)$ sono primitivi. Un altro esempio di gruppo primitivo lo si ottiene quando n è

una potenza di primo, e si considera il gruppo delle permutazioni sugli elementi di un campo $\mathbb{F}$ con n elementi che mandano $x \in \mathbb{F}$ in $ax + b$, dove a e b sono arbitrari elementi di $\mathbb{F}$, con $a \neq 0$. Un risultato molto importante di Peter Cameron, Peter Neumann e David Teague [5] afferma che l'insieme Λ dei numeri naturali n per i quali $\mathrm{Sym}(n)$ e $\mathrm{Alt}(n)$ sono gli unici sottogruppi primitivi di $\mathrm{Sym}(n)$ ha densità 1 nell'insieme $\mathbb{N}$ (ma attenzione, quello che succede per valori piccoli di n potrebbe trarre in inganno: 34 è il più piccolo elemento di Λ). Più precisamente, denotato con $\lambda(n)$ il numero degli interi positivi $m \leq n$ per i quali $\mathrm{Sym}(m)$ contiene sottogruppi primitivi diversi da $\mathrm{Sym}(m)$ e $\mathrm{Alt}(m)$, si ha $\lambda(n) \sim 2n/\log_2 n$. In ogni caso, i sottogruppi primitivi di $\mathrm{Sym}(n)$ sono comunque "pochi". Esiste infatti una costante assoluta c tale che $\mathrm{Sym}(n)$ contiene al più $n^{c \log n}$ classi di coniugio di sottogruppi primitivi [44]. Se n è un primo, allora tutti i sottogruppi transitivi di $\mathrm{Sym}(n)$ sono primitivi, ma utilizzando il risultato precedente si può dimostrare che, fissato un primo p, il rapporto tra sottogruppi primitivi e sottogruppi transitivi di $\mathrm{Sym}(p^u)$ tende a 0 quando u tende all'infinito.

Oltre che "pochi", i sottogruppi primitivi di $\mathrm{Sym}(n)$ sono anche "piccoli". Quello di stimare l'ordine dei sottogruppi primitivi di $\mathrm{Sym}(n)$ in funzione di n è stato uno dei problemi centrali della teoria dei gruppi nel diciannovesimo secolo, con contributi, tra gli altri, di Cauchy e Bertrand. Nel 1860 questo problema fu oggetto del Gran Premio dell'Accademia di Parigi. Il premio in quell'occasione non fu assegnato, sebbene tra i contendenti si annoveri anche Jordan. Utilizzando la classificazione dei gruppi semplici finiti, negli ultimi decenni sono stati dimostrati numerosi risultati significativi. Per esempio Cheryl Praeger e Jan Saxl [41] hanno dimostrato che un sottogruppo primitivo di $\mathrm{Sym}(n)$, diverso da $\mathrm{Alt}(n)$ e $\mathrm{Sym}(n)$, ha ordine al più 4^n.

4. Un altra domanda che ha stimolato diverse investigazioni è cosa si possa dire di un elemento casuale di $\mathrm{Sym}(n)$. Questioni di questo tipo rientrano in quella che si suole chiamare "teoria statistica dei gruppi". Ogni elemento del gruppo simmetrico si può scrivere come prodotto di cicli disgiunti e nel 1944 Goncharov [18] dimostrò che per quasi tutti i suoi elementi il numero di cicli coinvolti in questa decomposizione è all'incirca $\ln(n)$ (dove dicendo "quasi tutti" si intende che le eccezioni sono al più $o(n!)$). Ma in questo contesto vanno menzionati soprattutto una serie di contributi dovuti a Paul Erdös e Pál Turán, apparsi tra il 1965 e 1973, e dedicati al comportamento asintotico dell'ordine di un elemento casuale di $\mathrm{Sym}(n)$ [10], [11], [12], [13], [14], [15], [16]. Ad esempio, in questi lavori è dimostrato che l'ordine $\mathrm{ord}(x)$ di un elemento casuale x di $\mathrm{Sym}(n)$ è all'incirca $e^{\frac{(\ln(n))^2}{2}}$, che tale ordine è divisibile per tutti i primi minori di $\ln(n)/\ln(\ln(n))$ e che il suo più grande fattore primo è approssimativamente $n/e^{\sqrt{\ln(n)}}$. Più precisamente, la distribuzione di $\ln(\mathrm{ord}(x))$ è asintoticamente una distribuzione normale con mediana $\frac{1}{2}\ln^2 n$ e varianza $\frac{1}{3}\ln^2 n$. Questo contrasta fortemente con un classico risultato di Landau, in base al quale il massimo valore di $\ln(\mathrm{ord}(x))$ è $(1 + o(1))\sqrt{n \ln(n)}$.

5. – La congettura di Netto

1. Quello che discuteremo in questa sezione è un problema che origina dal paragrafo seguente, contenuto in un classico testo scritto da Eugen Netto [39] nel 1892: *If we arbitrarily select two or more substitutions of n elements, it is to be regarded as extremely probable that the group of lowest order which contains these is the symmetric group, or at least the alternating group. In the case of two substitutions the probability in favor of the symmetric group may be taken as about 3/4, and in favor of the alternating, but not symmetric, group as about 1/4.*

Formuliamo meglio quello che sta congetturando Netto. Partiamo dalla facile osservazione che se prendiamo a caso una coppia ordinata (x, y) di elementi in $\mathrm{Sym}(n)$, con probabilità 1/4 entrambi questi elementi appartengono al sottogruppo $\mathrm{Alt}(n)$, mentre con probabilità 3/4 almeno uno dei due elementi non vi appartiene. Secondo Netto, nel primo caso è molto probabile che il sottogruppo di $\mathrm{Sym}(n)$ generato da x e y sia esattamente $\mathrm{Alt}(n)$, mentre nel secondo caso molto probabilmente x e y generano l'intero gruppo simmetrico $\mathrm{Sym}(n)$. Di conseguenza, quasi certamente il sottogruppo $\langle x, y\rangle$ generato da x e y coincide o con $\mathrm{Alt}(n)$ o con $\mathrm{Sym}(n)$. Definiamo dunque:

$$p_n := \frac{|\{(x, y) \in \mathrm{Sym}(n) \times \mathrm{Sym}(n) \mid \mathrm{Alt}(n) \leq \langle x, y\rangle\}|}{|\mathrm{Sym}(n)|^2}.$$

Anche in questo caso, possiamo usare un computer per determinare p_n quando n è piccolo. Nella tabella seguente vengono riportati i valori di p_n per $2 \leq n \leq 13$. I primissimi valori oscillano un po' e non rivelano ancora un preciso andamento, ma a partire da $n \geq 7$ la successione $\{p_n\}_{n\in\mathbb{N}}$ è crescente e già per $n \geq 12$ assume valori maggiori di 0.9.

2	0.750		8	0.795
3	0.722		9	0.859
4	0.542		10	0.875
5	0.633		11	0.894
6	0.588		12	0.903
7	0.794		13	0.913

Fu John Dixon [8] a confermare, nel 1969, la congettura di Netto, provando che $\lim_{n\to\infty} p_n = 1$. Più precisamente $p_n \geq 1 - 2/(\ln(\ln(n)))^2$.

2. Voglio evidenziare una conseguenza poco evidente di questo risultato, legata a una questione concreta che emerge nell'ambito della teoria dei gruppi computazionale. Supponiamo di voler identificare computazionalmente, per un assegnato gruppo G e un intero positivo t "non troppo grande" un insieme $g_1, \ldots, g_t$ di elementi di G tali che $G = \langle g_1, \ldots, g_t\rangle$ testando t-uple in G^t scelte casualmente. Chiaramente t deve essere maggiore o uguale della cardinalità minima, che denoteremo con $d(G)$, di un insieme di generatori per G. Denotiamo con $P(G,t)$ la probabilità che una t-upla ordinata $(g_1, \ldots, g_t) \in G^t$ generi G. Se $P(G,t)$ è troppo vicino a zero, la nostra ricerca di una t-upla di generatori fatta testando t-uple scelte casualmente ha scarse probabilità di avere successo. Quindi è importante scegliere t che sia sufficientemente grande per garantirci che $P(G,t)$ sia abbastanza elevato e nello stesso tempo il più piccolo possibile rispetto a $d(G)$. Fissato un numero reale positivo $\eta < 1$ la domanda che emerge è: *esiste una funzione $f_\eta : \mathbb{N} \to \mathbb{N}$ tale che $P(G, f_\eta(d(G))) \geq \eta$ per ogni gruppo finito G?* Il risultato di Dixon implica

$$\lim_{n\to\infty} P(\mathrm{Alt}(n), 2) = 1.$$

Inoltre è noto che per ogni $n \geq 5$,

$$P(\mathrm{Alt}(n), 2) \geq P(\mathrm{Alt}(6), 2) = 53/90.$$

Non è difficile dimostrare che, per $n \geq 5$, il prodotto diretto $(\mathrm{Alt}(n))^u$ di u copie di $\mathrm{Alt}(n)$ è generabile con 2 elementi se e solo se

$$u \leq \frac{P(\mathrm{Alt}(n), 2) \cdot n!}{a_n}$$

con $a_n = 8$ se $n = 6$, $a_n = 4$ altrimenti. Ad esempio, essendo $P(\mathrm{Alt}(5), 2) = \frac{19}{30}$, il prodotto diretto $(\mathrm{Alt}(5))^{19}$ di 19 copie di $\mathrm{Alt}(5)$ è generabile con 2 elementi. Ma si può anche dimostrare che la probabilità di generare con 2 elementi $(\mathrm{Alt}(5))^{19}$ è molto bassa. Infatti segue ad esempio da [25 Proposition 9] che

$$P((\mathrm{Alt}(5))^{19}, 2) = \frac{19!}{30^{19}} = \frac{2263261}{216243896484375000}.$$

Più in generale, da quanto detto sopra, segue che per $n \geq 7$ il gruppo $(\mathrm{Alt}(n))^{\frac{n!}{8}}$ è 2-generato ma la probabilità che una coppia di elementi lo generi è pressoché nulla. Ma è molto peggio di così: Alex Lubotzky e Bill Kantor [25] hanno provato infatti il fatto seguente:

$$\lim_{n\to\infty} P((\mathrm{Alt}(n))^{\frac{n!}{8}}, \lceil\sqrt{n}\rceil) = 0.$$

In particolare, fissato $k \in \mathbb{N}$, la probabilità che k elementi di $(\mathrm{Alt}(n))^{\frac{n!}{8}}$ lo generino tende a zero al crescere di n. Questo dimostra che per nessun numero reale positivo η può esistere una funzione f_η con le proprietà prima auspicate. Vale comunque un risultato più debole: per ogni $0 < \eta < 1$ esiste una costante c_η tale che, per ogni gruppo finito G, $P(G, d(G) + c_\eta \log_2 \log_2 |G|) \geq \eta$ [7].

3. Stime asintotiche sulla probabilità di generare un gruppo finito con un assegnato numero di elementi sono alla base di un algoritmo proposto in [36], per risolvere in tempo polinomiale il problema della generazione di un dato gruppo finito G, dove con "problema di generazione" si intende: determinare $d(G)$ e trovare un insieme di generatori di G di cardinalità $d(G)$. Più precisamente, chiamiamo "test di generazione" la verifica che un assegnato sottoinsieme di G lo generi. In [36] si dimostra che si può risolvere il problema di generazione per G effettuando al più $|G|^{13/5}$ test di generazione. Successivamente in [24] è stata presentata una variante stocastica dell'algoritmo proposto in [36] che permette di risolvere il problema di generazione per gruppi di permutazione di grado n con $O(n^2 \log n)$ test di generazione.

6. – Gruppi semplici

1. È ben noto che risale al 1984 il completamento della classificazione dei gruppi semplici finiti. Si tratta di un risultato chiave, si può dire il più rilevante, nell'ambito della teoria dei gruppi. D'altra parte la dimostrazione completa del teorema di classificazione è distribuita in circa 500 articoli, e riempie quasi 15.000 pagine a stampa. Sono in atto diversi progetti mirati a rivedere e migliorare la dimostrazione, ma finora nessuna sostanziale semplificazione è stata prodotta. Per questo, quando si dimostrano nuovi risultati in teoria dei gruppi, c'è sempre lo sforzo di usare con parsimonia (se possibile addirittura evitarla) la classificazione dei gruppi semplici. Ma è raro che si riescano a produrre risultati significativi senza far ricorso, in un modo o nell'altro, a proprietà dei gruppi semplici al momento dimostrabili solo usando la classificazione. Questo è ampiamente vero per la maggior parte dei risultati che ho esposto finora. Quasi tutti dipendono dalla classificazione, e alcuni di essi in maniera davvero pesante.

Sia come elemento base per dimostrare risultati più generali sia come argomento rilevante di per sé, il comportamento asintotico dei gruppi semplici finiti è stato ampiamente investigato.

2. Abbiamo visto nella sezione precedente che la probabilità di generare il gruppo alterno di grado n con due suoi elementi scelti a caso tende a 1 quando n tende all'infinito. Nel lavoro in cui lo dimostrò, Dixon congetturò che si trattasse del caso particolare di un risultato più generale. Una delle conseguenze della classificazione dei gruppi semplici è che ogni gruppo semplice può essere generato con 2 elementi. Quello che congetturò Dixon è che, facendo variare S nella famiglia dei gruppi semplici finiti, la probabilità che due elementi di S lo generino tende a 1 quando l'ordine di S va all'infinito. La congettura è vera e la dimostrazione viene dai risultati dimostrati in [25] e [33]. Val la pena di evidenziare un ingrediente fondamentale della dimostrazione. Se due elementi di S non lo generano, allora il sottogruppo che essi generano è contenuto in un sottogruppo massimale di S. Intuitivamente, più alto è il numero di sottogruppi massimali di S, più bassa è la probabilità di generarlo con 2 elementi. Questo ha suggerito di introdurre una funzione zeta che codifica la crescita del numero di sottogruppi massimali di S in funzione del loro indice. Precisamente, considerato $\mathcal{M}$ l'insieme dei sottogruppi massimali di S, per ogni $t \in \mathbb{R}$ definiamo

$$\zeta_S(t) = \sum_{M \in \mathcal{M}} |S : M|^{-t}.$$

In [31] è dimostrato che, fissato $t > 1$, $\zeta_S(t) \to 0$ per $|S| \to \infty$. La congettura di Dixon segue da questo risultato e dal fatto che $P(S,2) \geq 1 - \zeta_S(2)$.

Non sorprende che l'abbondanza in un gruppo semplice S di coppie di elementi che lo generano abbia come conseguenza che per ogni $1 \neq x \in S$ esiste $y \in S$ tale che $S = \langle x, y \rangle$. Bob Guralinck e Bill Kantor [19] hanno provato che vale un risultato ancora più preciso: ogni gruppo semplice S contiene una classe di coniugazione C con la proprietà che, per ogni $1 \neq x \in S$, C contiene molti elementi (più di un decimo della cardinalità di C) tali che $S = \langle x, y \rangle$.

3. Siano G un arbitrario gruppo finito e X un suo sottoinsieme. Denotiamo con $\delta(G,X)$ il più piccolo intero d tale che ogni elemento di G si può scrivere come prodotto di al più d elementi di $X \cup X^{-1}$. Un facile argomento di conteggio mostra che $\delta(G,X) \geq \log_{2|X|}(|G|)$. In [1] si dimostra che esiste una costante assoluta γ tale che ogni gruppo semplice non abeliano S contiene un insieme di generatori X di cardinalità al più 7 e tale che $\delta(S,X) \leq \gamma \log_2 |S|$. È curioso osservare che non vale un risultato analogo per i gruppi abeliani. Infatti se $G = \langle X \rangle$ è un gruppo abeliano finito, allora $\delta(G,X) \geq \frac{1}{2}\left(|G|^{\frac{1}{|X|}} - 1\right)$.

4. Tra i problemi ancora aperti nell'ambito dello studio dei gruppi semplici finiti c'è la conferma della seguente importante congettura di Thompson: ogni gruppo semplice finito non abeliano S contiene una classe di coniugio C tale che $S = C^2$, ossia ogni elemento di S può essere scritto come prodotto di due elementi di C. La congettura è stata verificata per diverse famiglie di gruppi semplici ma non ancora in generale. Nel 2007 Aner Shalev [46] dimostrò un risultato asintotico a supporto di tale congettura. Dato un numero reale positivo ϵ e un

gruppo semplice finito non abeliano S, denotiamo con $\pi_\epsilon(S)$ la probabilità che un elemento x scelto casualmente in S sia tale che $|C_x^2|/|S| \geq 1-\epsilon$, essendo C_x la classe di coniugazione che contiene x. Risulta che, per ogni ϵ, $\lim_{|S|\to\infty} \pi_\epsilon(S) = 1$.

RIFERIMENTI BIBLIOGRAFICI

[1] L. Babai, W. Kantor, A. Lubotzky, *Small-diameter Cayley graphs for finite simple groups*, European J. Combin. 10 (1989), no. **6**, 507-522.

[2] H. U. Besche, B. Eick, E. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. 12 (2002), no. **5**, 623-644.

[3] A. Borovik, L. Pyber, A. Shalev, *Maximal subgroups in finite and profinite groups*, Trans. Amer. Math. Soc. 348 (1996), no. **9**, 3745-3761.

[4] R. Brauer, *Representations of finite groups, Lectures on modern mathematics*, Vol. I (ed. T. L. Saaty; Wiley, New York, 1963)

[5] P. J. Cameron, P. M. Neumann, D. N. Teague, *On the degrees of primitive pennutation groups*, Math. Z. **180** (1982) 141-149.

[6] M. Cartwright, *A bound on the number of conjugacy classes of a finite soluble group*, J. London Math. Soc. (2) **36** (1987) 229-244.

[7] E. Detomi, A. Lucchini, *Crowns and factorization of the probabilistic zeta function of a finite group*, J. Algebra 265 (2003), no. **2**, 651-668.

[8] J. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199-205.

[9] P. Erdös, E. G. Straus, *How abelian is a finite group?*, Linear and Multilinear Algebra 3 (1975/76), no. **4**, 307-312.

[10] P. Erdös, P. Turán, *On some problems of a statistical group-theory*. I, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **4** (1965), 175-186.

[11] P. Erdös, P. Turán, *On some problems of a statistical group-theory*. II, Acta Math. Acad. Sci. Hungar. **18** (1967), 151-163.

[12] P. Erdös, P. Turán, *On some problems of a statistical group-theory*. III, Acta Math. Acad. Sci. Hungar. **18** (1967), 309-320.

[13] P. Erdös, P. Turán, *On some problems of a statistical group-theory*. IV, Acta Math. Acad. Sci. Hungar. **19** (1968), 413-435.

[14] P. Erdös, P. Turán, *On some problems of a statistical group theory*. V, Period. Math. Hungar. 1 (1971), no. **1**, 5-13.

[15] P. Erdös, P. Turán, *On some problems of a statistical group theory*. VI, J. Indian Math. Soc. 34 (1970), no. 3-4, **3**, 175-192 (1971).

[16] P. Erdös, P. Turán, *On some problems of a statistical group theory*. VII, Period. Math. Hungar. **2** (1972), 149-163.

[17] M. Fusari, P. Spiga, *On the maximum number of subgroups of a finite group*, J. Algebra **635** (2023), 486-526.

[18] V. Goncharov, *Du domaine de l'analyse combinatoire*, (Russian) Bull. Acad. Sci. URSS. Sér. Math. [Izvestia Akad. Nauk SSSR] 8 (1944), 3-48.

[19] R. M. Guralnick, W. M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra 234 (2000), no. **2**, 743-792.

[20] G. Higman, *Enumerating p-groups*. I: Inequalities, Proc. London Math. Soc. (3) **10** (1960) 24-30.

[21] O. Hölder, *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. **43** (1893), 301-412.

[22] D. F. Holt, *Enumerating perfect groups*, J. London Math. Soc. (2) **39** (1989), no. 1, 67-78.

[23] A. Hulpke, *The perfect groups of order up to two million*, Math. Comp. 91 (2022), no. **334**, 1007-1017. Minimal sized generating sets of permutation groups

[24] D. F. Holt, G. Tracey, *Minimal sized generating sets of permutation groups*, arXiv:2404.03952 (2024).

[25] W. Kantor, A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata 36 (1990), no. **1**, 67-87.

[26] M. Kassabov, B. A. Tyburski, J. B. Wilson, *Subgroups of simple groups are as diverse as possible*, Bull. London Math. Soc. **54** (2022) 213-232.

[27] T. M. Keller, *Finite groups have even more conjugacy classes*, Israel J. Math. **181** (2011), 433-444.

[28] L. G. Kovács, C. R. Leedham-Green, *Some normally monomial p-groups of maximal class and large derived length*, Quart. J. Math. Oxford Ser. (2) 37 (1986), no. **145**, 49-54.

[29] L. G. Kovács, G. Robinson, *On the number of conjugacy classes of a finite group*, J. Algebra 160 (1993), no. **2**, 441-460.

[30] E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante*, Math. Ann. **56** (1903), 671-676.

[31] M. Liebeck, M. Benjamin, A. Shalev, *On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function*, Duke Math. J. 128 (2005), no. **3**, 541-557.

[32] M. Liebeck, L. Pyber, A. Shalev, On a conjecture of G. E. Wall, J. Algebra 317 (2007), no. 1, 184-197.

[33] M.W. Liebeck, A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103-113.

[34] A. Lubotzky, Enumerating boundedly generated finite groups, J. Algebra 238 (2001), no. 1, 194-199.

[35] A. Lucchini, F. Menegazzo, M. Morigi, *Asymptotic results for transitive permutation groups*, Bull. London Math. Soc. **32** (2000) 191-195.

[36] A. Lucchini, D. Thakkar, *The minimum generating set problem*, J. Algebra **640** (2024), 117-128.

[37] T. Luczak, L. Pyber, *On random generation of the symmetric group*, *Combin. Probab. Comput.* **2** (1993), 505-512.

[38] A. Mann, *Avinoam Enumerating finite groups and their defining relations*, J. Group Theory 1 (1998), no. **1**, 59-64.

[39] E. Netto, *Substitutionentheorie and ihre Anwendungen auf die Algebra*, Teubner, Leipzig, 1882, English transl. 1892, second ed., Chelsea, New York, 1964.

[40] P. M. Neumann, *An enumeration theorem for finite groups*, Quart. J. Math. Oxford (2), **20** (1969), 395-401.

[41] C. Praeger, J. Saxl, *On the orders of primitive permutation groups*, Bull. London Math. Soc. 12 (1980), no. **4**, 303-307.

[42] L. Pyber, *Enumerating finite groups of given order*, Ann. of Math. (2) 137 (1993), no. **1**, 203-220.

[43] L. Pyber, *How abelian is a finite group? The mathematics of Paul Erdö's*, I, 372-384, Algorithms Combin., **13**, Springer, Berlin, 1997.
[44] L. Pyber, A. Shalev, *Asymptotic results for primitive permutation groups*, J. Algebra 188 (1997), no. **1**, 103-124.
[45] C. M. Roney-Dougal, G. *Tracey, Subgroups of symmetric groups: enumeration and asymptotic properties*, arXiv:2503.05416 (2025).
[46] A. Shalev, *Mixing and generation in simple groups*, J. Algebra 319 (2008), no. **7**, 3075-3086.
[47] C. Sims, *Enumerating p-groups*, Proc. London Math. Soc. (3) **15** (1965), 151-166.
[48] G. E. Wall, *Some applications of the Eulerian functions of a finite group*, J. Aust. Math. Soc. **2** (1961) 35-59.
[49] J. Young, *On the determination of the groups whose order is a power of a prime*, Amer. J. Math. **15** (1893), 124-178.

Andrea Lucchini

Andrea Lucchini è professore ordinario di Algebra presso l'Università degli Studi di Padova. I suoi interessi scientifici riguardano la teoria dei gruppi, con particolare attenzione all'approccio probabilistico e a questioni di tipo combinatorio. Ha pubblicato circa duecento articoli su riviste internazionali ed è stato responsabile nazionale di diversi progetti PRIN.