Università degli Studi di Padova

DIPARTIMENTO MATEMATICA

Corso di Laurea in Matematica

Dipartimento di Matematica "Tullio Levi-Civita"

Il numero atteso di elementi casuali necessari per generare un gruppo finito

Relatore:
Prof. Andrea Lucchini

Candidato:
Marco Pizzati
Matricola 2109074

Anno accademico 2025/2026 - 17.07.2026

Indice

Introduzione

Dato un gruppo finito G, la conoscenza di un suo insieme di generatori può fornire molte informazioni circa la struttura del gruppo. Un modo efficace per minimizzare le informazioni necessarie per conoscere e descrivere un gruppo è quindi quello di trovare un insieme di generatori la cui cardinalità sia la più piccola possibile.

In questa tesi studieremo una versione probabilistica di questo problema. In particolare, dato un qualsiasi gruppo finito G, vogliamo cercare di calcolare il numero atteso di elementi del gruppo estratti casualmente e non necessariamente distinti che occorrono per formare un insieme di generatori per il gruppo stesso. Indichiamo questo valore atteso con $\mathcal{E}(G)$.

Nel Capitolo 1 daremo una definizione rigorosa del problema e ricaveremo una formula per il calcolo di $\mathcal{E}(G)$. A questo scopo introdurremo la probabilità $P_G(n)$ che n elementi scelti casualmente generino G. Vedremo che queste due quantità sono collegate: conoscendo il valore di $P_G(n)$ per ogni $n \in \mathbb{N}$ possiamo ricavare il valore di $\mathcal{E}(G)$. É inoltre possibile calcolare $P_G(n)$ attraverso la funzione di Möbius μ associata al reticolo dei sottogruppi di G: unendo queste due osservazioni possiamo ricavare la formula cercata.

Tale formula è però spesso difficile da utilizzare, in quanto richiede la conoscenza dell'intero reticolo dei sottogruppi di G: un problema che rischia di essere addirittura più complicato del problema stesso che vogliamo affrontare. Per questo motivo nel Capitolo 2 cercheremo di dare una stima di $\mathcal{E}(G)$ basandoci sulla conoscenza solo dei suoi sottogruppi massimali. Questa scelta è naturale: un insieme di elementi non genera G precisamente quando è contenuto in un sottogruppo proprio, e quindi in un sottogruppo massimale. Per poter arrivare a questo risultato sarà necessario lavorare con gli invarianti $\mathcal{M}(G)$ e $\mathcal{V}_\eta(G)$: il primo indica il tasso di crescita dei sottogruppi massimali di G all'aumentare del loro indice, mentre il secondo si riferisce al primo intero positivo k tale per cui $P_G(k) > \eta$, dove $0 < \eta < 1$.

Nel Capitolo 3 vedremo un'applicazione dei risultati trovati in precedenza. L'obiettivo è sapere quando per un gruppo finito G bastano k suoi elementi, con k sufficientemente grande ma comunque limitato dall'alto e piccolo rispetto a $|G|$, per generarlo con una buona probabilità. Dobbiamo quindi trovare una stima dall'alto di $\mathcal{V}_\eta(G)$. Per trovare una tale stima ci appoggeremo all'invariante $d(G)$, il quale si riferisce alla minima cardinalità di un insieme di generatori per G. Vedremo poi che per i gruppi nilpotenti e risolubili basta solo la conoscenza di $d(G)$ per ottenere la stima cercata, mentre per i gruppi finiti qualsiasi serve almeno un'altra informazione

sul gruppo G, ovvero il suo ordine $|G|$.

Nel Capitolo 4 infine vedremo una versione probabilistica di un teorema dimostrato in [7] secondo cui

$$d(G) \leq \max_p d_p(G) + 1,$$

dove $d_p(G)$ indica il minimo numero di generatori di un p-sottogruppo di Sylow di G. In particolare, otterremo una stima analoga per $\mathcal{E}(G)$.

Capitolo 1

Una prima formula

Il problema che affronteremo in questa tesi riguarda la generazione di gruppi finiti. In particolare siamo interessati a rispondere alla seguente domanda: qual è il valore atteso del numero di elementi di un gruppo finito G, scelti in maniera casuale e uniforme, necessari affinché essi generino tutto il gruppo?

Per dare una definizione più rigorosa del problema dobbiamo appoggiarci al linguaggio della teoria della probabilità. Sia G un gruppo finito non banale e sia $x = (x_n)_{n\in\mathbb{N}}$ una successione di variabili aleatorie a valori in G indipendenti e distribuite uniformemente. Definiamo inoltre la variabile aleatoria τ_G, che è un tempo d'attesa, come:

$$\tau_G := \min\{n \geq 1 | \langle x_1, \dots, x_n \rangle = G\}.$$

Allora possiamo definire $\mathcal{E}(G)$ come il valore atteso di τ_G, ovvero $\mathcal{E}(G) = \mathbb{E}(\tau_G)$. Il nostro obbiettivo è quindi quello di riuscire a calcolare, o almeno stimare, $\mathcal{E}(G)$.

Vediamo subito un caso semplice: sia C_p un gruppo ciclico di ordine p primo. Allora è evidente che la variabile τ_G è una variabile geometrica, con parametro $\frac{p-1}{p}$. Quindi $\mathcal{E}(G) = \mathbb{E}(\tau_G) = \frac{p}{p-1}$.

Ci si accorge presto però che, ad eccezione di alcuni casi semplici come nel caso del gruppo ciclico, il calcolo di $\mathcal{E}(G)$ può diventare estremamente complesso. Abbiamo quindi bisogno di alcuni aiuti per poter svolgere questo calcolo più facilmente.

1.1 Calcolo di $P_G(d)$

Definizione 1.1.1. Siano G un gruppo finito e $d \in \mathbb{N}$. Indichiamo con $\phi_G(d)$ il valore della d-esima *funzione di Eulero del gruppo* G, ovvero il numero di sequenze ordinate $(g_1, \dots, g_d) \in G^d$ tali che $\langle g_1, \dots, g_d \rangle = G$. Definiamo poi $P_G(d)$ come

$$P_G(d) = \frac{\phi_G(d)}{|G|^d}.$$

A partire da questa definizione segue subito che $P_G(d)$ può essere interpretato, nel linguaggio della probabilità, come la probabilità che una sequenza ordinata di d

elementi di G, non per forza distinti e scelti in maniera casuale e uniforme, generi tutto G.

Per calcolare $P_G(d)$, che ci permetterà poi di calcolare agilmente $\mathcal{E}(G)$, è necessario introdurre la funzione di Möbius.

Definizione 1.1.2. Sia $\mathcal{P}$ un insieme parzialmente ordinato. La *funzione di Möbius* di $\mathcal{P}$ è la mappa $\mu_{\mathcal{P}} : \mathcal{P} \times \mathcal{P} \to \mathbb{Z}$ tale che $\mu_{\mathcal{P}}(x, y) = 0$ se $x \not\leq y$, altrimenti è definita ricorsivamente dalle equazioni

$$\mu_{\mathcal{P}}(x, x) = 1 \text{ e } \sum_{x \leq z \leq y} \mu_{\mathcal{P}}(x, z) = 0 \text{ se } x < y$$

Il nostro obbiettivo in questa prima sezione è quello di dimostrare il seguente teorema.

Teorema 1.1.3. *Siano G è un gruppo finito e $d \in \mathbb{N}$. Allora vale*

$$P_G(d) = \sum_{H \leq G} \frac{\mu(H, G)|H|^d}{|G|^d},$$

dove $\mu(\cdot, \cdot)$ è la funzione di Möbius definita sul reticolo dei sottogruppi di G.

Prima della dimostrazione servono però dei risultati preliminari sulla funzione di Möbius.

Lemma 1.1.4. *Sia $\mathcal{P}$ un insieme finito e parzialmente ordinato e siano $x, y \in \mathcal{P}$, con $x < y$. Allora vale*

$$\sum_{x \leq z \leq y} \mu_{\mathcal{P}}(z, y) = 0.$$

Dimostrazione. Siano dati $x, y \in \mathcal{P}$ come nell'enunciato. Siano inoltre $x_1 = x, x_2, \ldots, x_n \in \mathcal{P}$ tutti e soli gli elementi distinti di $\mathcal{P}$ tali che $x \leq x_i \leq y \ \forall i \in \{1, \ldots n\}$. Definiamo due matrici quadrate $n \times n$: $A = (a_{ij})_{i,j=1,\ldots,n}$ e $B = (b_{ij})_{i,j=1,\ldots,n}$ tali che $a_{ij} = \mu_{\mathcal{P}}(x_i, x_j)$ e $b_{ij} = \gamma(x_i, x_j)$, con

$$\gamma(x_i, x_j) = \begin{cases} 1 & \text{se } x_i \leq x_j \\ 0 & \text{altrimenti} \end{cases}.$$

Moltiplicando le due matrici si ottiene la matrice $C = AB = (c_{ij})_{i,j=1,\ldots,n}$, con

$$c_{ij} = \sum_{x \leq z \leq y} \mu_{\mathcal{P}}(x_i, z)\gamma(z, x_j).$$

Dalla definizione della funzione di Möbius e per costruzione di $\gamma(z, x_j)$, sappiamo che $\mu_{\mathcal{P}}(x_i, z) = 0$ o che $\gamma(z, x_j) = 0$ a meno che non si abbia $x_i \leq z$ e $z \leq x_j$. Quindi, per le proprietà di $\mu_{\mathcal{P}}$ abbiamo che:

$$c_{ij} = \sum_{x_i \leq z \leq x_j} \mu_{\mathcal{P}}(x_i, z) = \delta_{x_i, x_j}.$$

Abbiamo quindi dimostrato che $AB = \mathbf{1}_n$, e ciò implica che anche $BA = \mathbf{1}_n$. Sappiamo dunque che $D = BA = (d_{ij})_{i,j=1,\dots,n} = (\delta_{i,j})_{i,j=1,\dots,n}$. Dalle definizioni di A e B, e con un ragionamento analogo al precedente, segue anche che:

$$\delta_{i,j} = d_{ij} = \sum_{x \le z \le y} \gamma(x_i, z)\mu_{\mathcal{P}}(z, x_j) = \sum_{x_i \le z \le x_j} \mu_{\mathcal{P}}(z, x_j).$$

Perciò, prendendo $x_i = x$ e $x_j = y$, abbiamo che

$$\sum_{x \le z \le y} \mu_{\mathcal{P}}(z, y) = 0.$$

□

Il prossimo risultato che vediamo è detto *formula di inversione di Möbius*.

Proposizione 1.1.5. *Siano $\mathcal{P}$ un insieme finito e parzialmente ordinato, $f : \mathcal{P} \to \mathbb{N}$ una funzione e $a \in \mathcal{P}$ fissato. Definiamo*

$$F(b) = \sum_{a \le x \le b} f(x).$$

Allora per ogni $b \ge a$ vale che

$$f(b) = \sum_{a \le x \le b} \mu_{\mathcal{P}}(x, b)F(x).$$

Dimostrazione. Dato $b \ge a$ fissato possiamo calcolare:

$$\sum_{a \le x \le b} \mu_{\mathcal{P}}(x, b)F(x) = \sum_{a \le x \le b} \mu_{\mathcal{P}}(x, b) \left(\sum_{a \le y \le x} f(y) \right) = \sum_{a \le y \le b} f(y) \left(\sum_{y \le x \le b} \mu_{\mathcal{P}}(x, b) \right).$$

Dal Lemma 1.1.4 abbiamo che

$$\sum_{y \le x \le b} \mu_{\mathcal{P}}(x, b) = \delta_{y,b}$$

da cui segue

$$\sum_{a \le x \le b} \mu_{\mathcal{P}}(x, b)F(x) = \sum_{a \le y \le b} f(y)\delta_{y,b} = f(b).$$

□

Abbiamo ora tutti gli strumenti per dimostrare il Teorema 1.1.3.

Dimostrazione. Dalla definizione di $P_G(d)$ osserviamo che basta dimostrare il seguente risultato equivalente:

$$\phi_G(d) = \sum_{H \le G} \mu(H, G)|H|^d. \tag{1.1}$$

Sia $K \leq G$ un sottogruppo di G. Possiamo osservare che dati $(k_1, \ldots, k_d) \in K^d$ abbiamo che $\langle k_1, \ldots, k_d \rangle = H \leq K$, ovvero ogni sequenza ordinata di elementi di K genera un sottogruppo di K. Da questa semplice osservazione, e ricordando la definizione di funzione di Eulero, possiamo ricavare che:

$$\sum_{H \leq K} \phi_H(d) = |K|^d.$$

Ora sia $\mathcal{P}_K$ il reticolo dei sottogruppi di K, e $f : \mathcal{P}_K \to \mathbb{N}$ una funzione tale che $f(H) = \phi_H(d)$, $\forall H \leq K$. Dalla formula di inversione di Möbius otteniamo, ponendo $a = \{1\}$ e $b = K$:

$$\phi_K(d) = \sum_{H \leq K} \mu(H, K)|H|^d.$$

Ponendo G in luogo di K si ottiene la 1.1, e dunque, dividendo per $|G|^d$, la tesi. □

1.2 Un primo calcolo di $\mathcal{E}(G)$

L'obbiettivo di questa sezione è quello di trovare una formula per $\mathcal{E}(G)$ sfruttando quanto visto in precedenza.

Iniziamo subito con un'osservazione fondamentale che collega il concetto di $P_G(d)$ con quello di $\mathcal{E}(G)$.

Osservazione 1.2.1. A partire da $P_G(d)$ è facile calcolare $\mathcal{E}(G)$: osserviamo innanzitutto che $\tau_G > d$ se e solo se $\langle x_1, \ldots, x_d \rangle \lneq G$. Da ciò segue che

$$P(\tau_G > d) = 1 - P(\tau_G \leq d) = 1 - P_G(d).$$

Quindi abbiamo che:

$$\begin{aligned}\mathcal{E}(G) =& \mathbb{E}(\tau_G) = \mathbb{E}\left(\sum_{k=1}^{\infty} \mathbf{1}_{\{\tau_G \geq k\}}\right) = \sum_{k=1}^{\infty} \mathbb{E}\left(\mathbf{1}_{\{\tau_G \geq k\}}\right) \\ =& \sum_{k=1}^{\infty} P(\tau_G \geq k) = \sum_{k=0}^{\infty} P(\tau_G > k) = \sum_{k=0}^{\infty} (1 - P_G(k)).\end{aligned}$$

Siamo quindi riusciti a ricavare $\mathcal{E}(G)$ a meno di conoscere $P_G(d)$ per ogni $d \in \mathbb{N}$. Possiamo ora dimostrare il seguente teorema.

Teorema 1.2.2. *Se G è un gruppo finito non banale, allora*

$$\mathcal{E}(G) = -\sum_{H < G} \frac{\mu(H, G)|G|}{|G| - |H|}.$$

Dimostrazione. Dall'Osservazione 1.2.1 (1), dal Teorema 1.1.3 (2), dalla convergenza delle serie geometriche (3) e dal fatto (4) che

$$\frac{\mu(G, G)}{|G : G|^k} = 1 \ \forall k \in \mathbb{N}$$

segue che:

$$\begin{aligned}\mathcal{E}(G) =&\mathbb{E}(\tau_G) \overset{(1)}{=} \sum_{k=0}^{\infty}(1 - P_G(k)) \overset{(2)}{=} \sum_{k=0}^{\infty}\left(1 - \sum_{H\leq G}\frac{\mu(H,G)}{|G:H|^k}\right)\\ \overset{(4)}{=}& -\sum_{k=0}^{\infty}\left(\sum_{H<G}\frac{\mu(H,G)}{|G:H|^k}\right) = -\sum_{H<G}\left(\sum_{k=0}^{\infty}\frac{\mu(H,G)}{|G:H|^k}\right)\\ \overset{(3)}{=}& -\sum_{H<G}\frac{\mu(H,G)|G|}{|G|-|H|}.\end{aligned}$$

□

Vediamo ora un esempio di applicazione della formula che abbiamo appena ricavato.

Esempio 1.2.3. Consideriamo il gruppo diedrale D_{2p}, con p un primo dispari. Per calcolare $\mathcal{E}(D_{2p})$ possiamo procedere in due modi.

1. Proviamo innanzitutto a ragionare sulla struttura di D_{2p}. Sappiamo che $D_{2p} = \langle\rho\rangle \rtimes \langle\sigma\rangle$ con $\langle\rho\rangle \cong C_p$ e $\langle\sigma\rangle \cong C_2$. Dunque $D_{2p} = \langle g_1, \dots, g_n\rangle$ se e solo se esistono $1 \leq i < j \leq n$ tali che $g_i \neq 1$ e $g_j \notin \langle g_i\rangle$. Come per il gruppo ciclico C_p, il numero di "estrazioni" (indipendenti) di elementi di D_{2p} che dobbiamo fare per ottenere un elemento non banale g_i è descritto da una variabile aleatoria geometrica di parametro $\frac{2p-1}{2p}$. Il suo valore atteso vale dunque $E_0 = \frac{2p}{2p-1}$. Ora con probabilità $p_1 = \frac{p}{2p-1}$ l'elemento non banale g_i ha ordine 2: in questo caso il numero di "estrazioni" necessarie per trovare un elemento g_j tale che $g_j \notin \langle g_i\rangle$ è descritto da una variabile aleatoria geometrica di parametro $\frac{2p-2}{2p}$ e dunque valore atteso $E_1 = \frac{2p}{2p-2} = \frac{p}{p-1}$. Con probabilità $p_2 = \frac{p-1}{2p-1}$ invece g_i ha ordine p: in questo caso il numero di "estrazioni" necessarie per trovare un elemento g_j tale che $g_j \notin \langle g_i\rangle$ è descritto da una variabile aleatoria geometrica di parametro $\frac{2p-p}{2p} = 0.5$ e dunque valore atteso $E_2 = 2$. Mettendo tutto insieme otteniamo:

$$\begin{aligned}\mathcal{E}(D_{2p}) =& E_0 + p_1E_1 + p_2E_2\\ =&\frac{2p}{2p-1} + \frac{p}{2p-1}\frac{p}{p-1} + 2\frac{p-1}{2p-1}\\ =&\frac{1}{2p-1}\left(2p + \frac{p^2}{p-1} + 2p - 2\right)\\ =&\frac{1}{2p-1}\left(\frac{p^2}{p-1} + 2(2p-1)\right)\\ =&\frac{p^2}{(2p-1)(p-1)} + 2.\end{aligned}$$

2. Proviamo ora a calcolare $\mathcal{E}(D_{2p})$ usando il Teorema 1.2.2. Sappiamo che D_{2p} contiene esattamente i seguenti sottogruppi: sé stesso; un sottogruppo massimale di ordine p; p sottogruppi massimali di ordine 2; il sottogruppo banale.

Ora se $M \leq G$ è un suo sottogruppo massimale allora, dal Lemma 1.1.4 vale che

$$\sum_{M \leq H \leq G} \mu(H, G) = \mu(M, G) + \mu(G, G) = 0.$$

Siccome poi $\mu(G, G) = 1$ si ricava che $\mu(M, G) = -1$. Inoltre possiamo calcolare che

$$\begin{aligned}\sum_{H \leq G} \mu(H, G) =& \mu(\{1\}, G) + \left(\sum_{\{1\} \neq H < G} \mu(H, G) \right) + \mu(G, G) \\ =& \mu(\{1\}, G) + (p+1)(-1) + 1 = 0,\end{aligned}$$

da cui segue che $\mu(\{1\}, G) = p$. Applicando il Teorema 1.2.2 otteniamo dunque che

$$\mathcal{E}(D_{2p}) = -\frac{2p^2}{2p-1} + p\frac{2p}{2p-2} + \frac{2p}{2p-p} = 2 + \frac{p^2}{(2p-1)(p-1)},$$

come visto al punto precedente.

Capitolo 2

Stima attraverso i sottogruppi massimali

Dall'esempio proposto alla fine del Capitolo 1, vediamo che per applicare la formula che abbiamo ricavato, e quindi per poter calcolare $\mathcal{E}(G)$, è necessario conoscere l'intero reticolo dei sottogruppi di G.

Adottiamo quindi un altro approccio, che ci permetterà di ottenere una stima abbastanza accurata di $\mathcal{E}(G)$ semplicemente conoscendo i sottogruppi massimali di G, una richiesta molto più debole rispetto a quella di conoscere l'intero reticolo dei sottogruppi. In particolare ci appoggeremo alla seguente definizione.

Definizione 2.0.1. Dato $n \in \mathbb{N}$ indichiamo con $m_n(G)$ il numero dei sottogruppi massimali di G con indice n. Indichiamo infine con $\mathcal{M}(G)$ il valore:

$$\mathcal{M}(G) = \max_{n \geq 2} \frac{\log m_n(G)}{\log n}.$$

Osservazione 2.0.2. Si può interpretare l'invariante $\mathcal{M}(G)$ come il "grado polinomiale" del tasso di crescita $m_n(G)$. Infatti applicando le proprietà dei logaritmi si ottiene banalmente che

$$m_n(G) \leq n^{\mathcal{M}(G)}.$$

2.1 Stima di $\mathcal{E}(G)$ dall'alto

A partire dalla definizione appena data possiamo ottenere una stima dall'alto di $\mathcal{E}(G)$ a partire da $\mathcal{M}(G)$. Prima però abbiamo bisogno del seguente lemma.

Lemma 2.1.1. *Sia G un gruppo finito e $d \in \mathbb{N}$. Allora vale*

$$1 - P_G(d) \leq \sum_{n=2}^{\infty} \frac{m_n(G)}{n^d}.$$

Dimostrazione. Iniziamo con due osservazioni preliminari. Innanzitutto osserviamo che, siccome G è finito, dalla definizione di $m_n(G)$ abbiamo che

$$\sum_{M \leq_{max} G} \frac{|M|^d}{|G|^d} = \sum_{M \leq_{max} G} \frac{1}{|G:M|^d} = \sum_{n=2}^{\infty} \frac{m_n(G)}{n^d}. \tag{2.1}$$

Inoltre possiamo vedere che, se $g_1, \ldots, g_d$ sono elementi di G, allora $\langle g_1, \ldots, g_d \rangle = G$ se e solo se non esiste un sottogruppo massimale $M \leq G$ tale che $(g_1, \ldots, g_d) \in M^d$. Quindi abbiamo che:

$$\phi_G(d) = |G|^d - \left| \bigcup_{M \leq_{max} G} M^d \right|. \tag{2.2}$$

Mettendo tutto insieme otteniamo:

$$1 - P_G(d) = 1 - \frac{\phi_G(d)}{|G|^d} \overset{(2.2)}{=} \frac{\left| \bigcup_{M \leq_{max} G} M^d \right|}{|G|^d} \leq \sum_{M \leq_{max} G} \frac{|M|^d}{|G|^d} \overset{(2.1)}{=} \sum_{n=2}^{\infty} \frac{m_n(G)}{n^d}.$$

□

Proposizione 2.1.2. *Sia G un gruppo finito. Allora vale $\mathcal{E}(G) \leq \lceil \mathcal{M}(G) \rceil + 3$.*

Dimostrazione. Siano $m = \lceil \mathcal{M}(G) \rceil$ e $d = m + k$ con $k \in \mathbb{N}$. Dall'Osservazione 2.0.2 e dal Lemma 2.1.1 otteniamo:

$$1 - P_G(d) \leq \sum_{n=2}^{\infty} \frac{m_n(G)}{n^d} \leq \sum_{n=2}^{\infty} \frac{n^{\mathcal{M}(G)}}{n^d} \leq \sum_{n=2}^{\infty} \frac{n^m}{n^d} \leq \sum_{n=2}^{\infty} \frac{1}{n^k}.$$

Mettendo insieme questo risultato appena trovato con l'Osservazione 1.2.1 segue che:

$$\begin{aligned}
\mathcal{E}(G) &= \sum_{d=0}^{\infty} (1 - P_G(d)) \leq m + 2 + \sum_{d=m+2}^{\infty} (1 - P_G(d)) \\
&\leq m + 2 + \sum_{k=2}^{\infty} \left(\sum_{n=2}^{\infty} \frac{1}{n^k} \right) = m + 2 + \sum_{n=2}^{\infty} \left(\sum_{k=2}^{\infty} \frac{1}{n^k} \right) \\
&= m + 2 + \sum_{n=2}^{\infty} \frac{n}{n^2(n-1)} = m + 2 + \sum_{n=1}^{\infty} \frac{1}{n(n+1)} = m + 3.
\end{aligned}$$

□

2.2 Stima di $\mathcal{E}(G)$ dal basso

In questa sezione cercheremo di dare una stima dal basso di $\mathcal{E}(G)$, sempre attraverso l'utilizzo di $\mathcal{M}(G)$. Il lavoro richiesto per arrivare ad una stima del genere è però essenzialmente più difficile di quello fatto per la stima dall'alto. Per questo dobbiamo introdurre un'ulteriore importante definizione.

Definizione 2.2.1. Sia G un gruppo finito, e $0 < \eta < 1$ un numero reale. Allora chiamiamo

$$\mathcal{V}_\eta(G) = \min\{k \in \mathbb{N} : P_G(k) \geq \eta\}$$

Cerchiamo ora di collegare le due quantità $\mathcal{E}(G)$ e $\mathcal{V}_\eta(G)$. Per farlo abbiamo bisogno del seguente lemma, oltre che della disuguaglianza di Markov.

Lemma 2.2.2. *Siano $a, b \in \mathbb{N}$. Allora vale*

$$1 - P_G(a+b) \leq (1 - P_G(a))(1 - P_G(b)).$$

Dimostrazione. Definiamo i tre insiemi

$$\begin{aligned}
&\Phi_{a+b}(G) = \{(g_1, \ldots, g_{a+b}) \in G^{a+b} : \langle g_1, \ldots, g_{a+b}\rangle = G\}\\
&A = \{(x_1, \ldots, x_a, y_1, \ldots, y_b) \in G^{a+b} : \langle x_1, \ldots, x_a\rangle = G\}\\
&B = \{(x_1, \ldots, x_a, y_1, \ldots, y_b) \in G^{a+b} : \langle x_1, \ldots, x_a\rangle \neq G, \langle y_1, \ldots, y_b\rangle = G\}.
\end{aligned}$$

Allora è evidente che, siccome $A \cap B = \emptyset$, $A \cup B \subseteq \Phi_{a+b}(G)$ e che $|\Phi_{a+b}(G)| = \phi_G(a+b)$, si ha:

$$\begin{aligned}
P_G(a+b) = \frac{\phi_G(a+b)}{|G|^{a+b}} &= \frac{|\Phi_{a+b}(G)|}{|G|^{a+b}}\\
&\geq \frac{|A| + |B|}{|G|^{a+b}} = P_G(a) + (1 - P_G(a))P_G(b)\\
&= P_G(a) + P_G(b) - P_G(a)P_G(b).
\end{aligned}$$

Da ciò si ottiene:

$$1 - P_G(a+b) \leq 1 - P_G(a) - P_G(b) + P_G(a)P_G(b) = (1 - P_G(a))(1 - P_G(b)).$$

□

Teorema 2.2.3 (Disuguaglianza di Markov)**.** *Sia γ una variabile aleatoria non negativa e $k > 0$ un numero reale. Allora vale*

$$P(\gamma \geq c) \leq \frac{\mathbb{E}(\gamma)}{c}$$

Proposizione 2.2.4. *Sia G un gruppo finito e $\eta \in \mathbb{R}$ tale che $0 < \eta < 1$. Allora vale*

$$\eta\mathcal{E}(G) \leq \mathcal{V}_\eta(G) \leq \frac{\mathcal{E}(G)}{1-\eta}.$$

Dimostrazione. Ricordando la definizione del tempo di attesa τ_G, dalla disuguaglianza di Markov (Teorema 2.2.3) segue che, posti $c = \mathcal{E}(G)/(1-\eta)$ e $k = \lfloor c \rfloor$:

$$P(\tau_G > k) = P(\tau_G > c) < \frac{\mathbb{E}(\tau_G)}{c} = \frac{\mathcal{E}(G)}{c} = 1 - \eta.$$

Inoltre dall'Osservazione 1.2.1 si ricava che

$$P_G(k) = 1 - P(\tau_G > k) < 1 - (1 - \eta) = \eta,$$

da cui si deriva banalmente che

$$\mathcal{V}_\eta(G) \leq \frac{\mathcal{E}(G)}{1-\eta}.$$

Ci manca quindi ora da dimostrare l'altra disuguaglianza. Per farlo osserviamo innanzitutto che se abbiamo $k, m, j \in \mathbb{N}$ tali che $mk \leq j < (m+1)k$, allora dal Lemma 2.2.2 segue che

$$1 - P_G(j) \leq 1 - P_G(mk) \leq (1 - P_G(k))^m.$$

Dall'Osservazione 1.2.1,fissato $k \in \mathbb{N}$, ricaviamo quindi che

$$\begin{aligned}\mathcal{E}(G) &= \sum_{d=0}^{\infty}(1 - P_G(d)) = \sum_{m=0}^{\infty}\left(\sum_{j=mk}^{(m+1)k}(1 - P_G(j))\right) \\ &\leq \sum_{m=0}^{\infty}\left(\sum_{j=mk}^{(m+1)k}(1 - P_G(k))^m\right) = \sum_{m=0}^{\infty} k(1 - P_G(k))^m = \frac{k}{P_G(k)}.\end{aligned}$$

In particolare se $k \leq \eta\mathcal{E}(G) < k+1$ (in questo caso possiamo porre anche $k \neq 0$, in quanto se $\eta\mathcal{E}(G) < 1$ la disuguaglianza è banalmente vera), si ottiene che

$$P_G(k) \leq \frac{k}{\mathcal{E}(G)} < \eta,$$

da cui si deriva che $\mathcal{V}_\eta(G) \geq \eta\mathcal{E}(G)$. □

Abbiamo dunque confrontato $\mathcal{V}_\eta(G)$ con $\mathcal{E}(G)$. Per poter arrivare a una stima dal basso di $\mathcal{E}(G)$ in funzione di $\mathcal{M}(G)$ ci basta dunque stimare $\mathcal{V}_\eta(G)$ con $\mathcal{M}(G)$. Mettendo poi tutto insieme troveremo la stima cercata.

Per iniziare abbiamo bisogno della seguente definizione.

Definizione 2.2.5. Sia G un gruppo e $H \leq G$ un suo sottogruppo. Definiamo il cuore normale di H come $\mathrm{Core}_G(H) = \bigcap_{g\in G} gHg^{-1}$. Si dice che un sottogruppo H è core-free se il suo cuore normale è banale, ovvero $\mathrm{Core}_G(H) = \bigcap_{g\in G} gHg^{-1} = \{1\}$.

Osservazione 2.2.6. Il cuore normale di un sottogruppo $H \leq G$ è il più grande sottogruppo normale di G contenuto in H.

Attraverso il Teorema di classificazione dei gruppi semplici finiti si può dimostrare il seguente teorema ([6], Teorema 1.3) che ci permette di stimare il numero di sottogruppi massimali di un gruppo finito G.

Teorema 2.2.7. *Esiste una costante b tale che per ogni gruppo finito G e per ogni $n \in \mathbb{N}$, $n \geq 2$, G ha al più n^b sottogruppi massimali core-free di indice n.*

Dimostriamo ora alcuni risultati che mettono in relazione la Teoria della probabilità con la Teoria dei gruppi. Senza alcuna sorpresa, la misura probabilità uniforme P definita su un gruppo G è data da $P(E) = \frac{|E|}{|G|}$, dove $E \subseteq G$. In particolare possiamo osservare che se G è finito e $E \leq G$ vale che

$$P(E) = \frac{1}{|G : E|}.$$

Ricordiamo la nota disuguaglianza di Chebyshev.

Teorema 2.2.8 (Disuguaglianza di Chebyshev)**.** *Sia γ una variabile aleatoria con media e varianza finita e $c > 0$ un numero reale. Allora vale*

$$P(|\gamma - \mathbb{E}(\gamma)| \geq c) \leq \frac{\mathrm{Var}(\gamma)}{c^2}.$$

Per proseguire è necessario anche dimostrare la seguente importante proposizione.

Proposizione 2.2.9. *Sia X uno spazio di probabilità finito e siano $X_1, \ldots, X_n$ eventi a due a due indipendenti. Allora vale*

$$\sum_{i=1}^{n} P(X_i) \leq \frac{1}{P(\cap_{1 \leq i \leq n}(X \smallsetminus X_i))}.$$

Dimostrazione. Per comodità chiamiamo $p_k = P(X_k)$ e poniamo α_k, con $1 \leq k \leq n$, la funzione caratteristica di X_k, ovvero $\alpha_k : X \to \{0, 1\}$ con

$$\alpha_k(x) = \begin{cases} 1 & \text{se } x \in X_k \\ 0 & \text{altrimenti.} \end{cases}$$

Definiamo inoltre

$$\alpha(x) = \sum_{k=1}^{n} (\alpha_k(x) - p_k).$$

Si vede subito che

$$\mathbb{E}(\alpha) = \mathbb{E}\left(\sum_{k=1}^{n} (\alpha_k - p_k)\right) = \sum_{k=1}^{n} (\mathbb{E}(\alpha_k) - p_k) = 0.$$

Quindi

$$\begin{aligned} \mathrm{Var}(\alpha) =& \mathbb{E}(\alpha^2) - \mathbb{E}(\alpha)^2 = \sum_{x \in X} \left(\sum_{k=1}^{n} (\alpha_k(x) - p_k)\right)^2 P(x) \\ =& \sum_{k=1}^{n} \left(\sum_{x \in X} (\alpha_k(x) - p_k)^2 P(x) + \sum_{l \neq k} \sum_{x \in X} (\alpha_k(x) - p_k)(\alpha_l(x) - p_l) P(x)\right). \end{aligned}$$

Dalla definizione di α_k segue che

$$\sum_{x\in X}(\alpha_k(x)-p_k)^2P(x) = (1-p_k)^2p_k + p_k^2(1-p_k) = (1-p_k)p_k.$$

Similmente, per $l \neq k$ abbiamo che

$$(\alpha_k(x)-p_k)(\alpha_l(x)-p_l) = \begin{cases} -(1-p_k)p_l & \text{se } x \in X_k \smallsetminus X_l, \\ -p_k(1-p_l) & \text{se } x \in X_l \smallsetminus X_k, \\ (1-p_k)(1-p_l) & \text{se } x \in X_k \cap X_l, \\ p_kp_l & \text{se } x \in X \smallsetminus (X_k \cup X_l). \end{cases}$$

Siccome gli eventi $X_1, \ldots, X_n$ sono a due a due indipendenti, possiamo calcolare le probabilità

$$\begin{aligned} &P(X_k \smallsetminus X_l) = P(X_k \cap (X \smallsetminus X_l)) = P(X_k)P(X \smallsetminus X_l) = p_k(1-p_l), \\ &P(X_l \smallsetminus X_k) = P(X_l \cap (X \smallsetminus X_k)) = P(X_l)P(X \smallsetminus X_k) = p_l(1-p_k), \\ &P(X_k \cap X_l) = P(X_k)P(X_l) = p_kp_l, \\ &P(X \smallsetminus (X_k \cup X_l)) = P((X \smallsetminus X_k) \cap (X \smallsetminus X_l)) = P(X \smallsetminus X_k)P(X \smallsetminus X_l) = p_kp_l. \end{aligned}$$

Quindi calcoliamo

$$\sum_{x\in X}(\alpha_k(x)-p_k)(\alpha_l(x)-p_l)P(x) = 2p_lp_k(1-p_l)(1-p_k) - 2p_lp_k(1-p_l)(1-p_k)$$

che si annulla. Mettendo tutto insieme risulta dunque che

$$\mathrm{Var}(\alpha) = \sum_{k=1}^{n} p_k(1-p_k).$$

Usando la disuguaglianza di Chebyshev (Teorema 2.2.8) con $c = \sum_{1\leq k\leq n} p_k$ ricaviamo che

$$\begin{aligned} P\left(\bigcap_{k=1}^{n}(X \smallsetminus X_k)\right) = P\left(\alpha = -\sum_{k=1}^{n} p_k\right) &\leq P\left(|\alpha| \leq \sum_{k=1}^{n} p_k\right) \\ &\leq \frac{\mathrm{Var}(\alpha)}{(\sum_{1\leq k\leq n} p_k)^2} = \frac{\sum_{1\leq k\leq n} p_k(1-p_k)}{(\sum_{1\leq k\leq n} p_k)^2} \\ &\leq \frac{1}{\sum_{1\leq k\leq n} p_k}. \end{aligned}$$

Passando ai reciproci si ottiene dunque la tesi. □

Lemma 2.2.10. *Siano G un gruppo finito e $k \in \mathbb{N}$, $k > 0$. Consideriamo in G^k la distribuzione uniforme. Se A e B sono sottogruppi massimali di G con $\mathrm{Core}_G(A) \neq \mathrm{Core}_G(B)$, allora A^k e B^k sono eventi indipendenti.*

Dimostrazione. Vogliamo dimostrare che $P(A^k \cap B^k) = P(A^k)P(B^k)$, con $P(E^k) = \frac{|E|^k}{|G|^k}$ in quanto stiamo considerando la probabilità uniforme. Siano ora $A_0 = \mathrm{Core}_G(A)$ e $B_0 = \mathrm{Core}_G(B)$. Ora, anche se fosse $A_0 \leq B_0$ (si procede in maniera analoga se $B_0 \leq A_0$) si avrebbe comunque che $A_0 \leq B$ e che $B_0 \nleq A_0$ da cui $B_0 \nleq A$ (altrimenti ci sarebbe in A un sottogruppo normale più grande del cuore normale di A stesso, il che è assurdo). Per la massimalità di A, ciò implica che $AB_0 = G$ e quindi anche $AB = G$. Quindi abbiamo che

$$1 = |G : AB| = \frac{|G : A||G : B|}{|G : A \cap B|} \Rightarrow |G : A \cap B| = |G : A||G : B|.$$

Possiamo quindi concludere che

$$P(A^k \cap B^k) = |G : A \cap B|^{-k} = |G : A|^{-k}|G : B|^{-k} = P(A^k)P(B^k).$$

□

Abbiamo ora tutti gli strumenti per poter confrontare $\mathcal{V}_\eta(G)$ con $\mathcal{M}(G)$.

Proposizione 2.2.11. *Sia $0 < \eta < 1$ un numero reale. Allora*

$$\mathcal{V}_\eta(G) \geq \mathcal{M}(G) - b + \log_2 \eta,$$

dove b è la costante che appare nel Teorema 2.2.7.

Dimostrazione. Sia $\mathcal{N} = \{N_1, \ldots, N_u\}$ l'insieme di tutti i cuori normali dei sottogruppi massimali di G. Per ogni $N_i \in \mathcal{N}$ sia M_i uno dei sottogruppi massimali tali che $N_i = \mathrm{Core}_G(M_i)$. Sia $c_n(G)$ il numero dei sottogruppi massimali di indice n ottenuti in questo modo. Sia $\Phi_G(k) = \{(g_1, \ldots, g_k) \in G^k | \langle g_1, \ldots, g_k \rangle = G\}$. Per $1 \leq i \leq u$, se $(g_1, \ldots, g_k) \in M_i^k$, allora $(g_1, \ldots, g_k) \notin \Phi_G(k)$, e dunque

$$\Phi_G(k) \subseteq \bigcap_{1 \leq i \leq u} (G^k \setminus M_i^k).$$

Dal Lemma 2.2.10 si ricava che, in quanto $N_i \neq N_j$ per $1 \leq i, j \leq u$, con $i \neq j$, gli eventi $M_1^k, \ldots, M_u^k$ sono in G^k a due a due indipendenti e quindi dalla Proposizione 2.2.9 si ottiene che

$$\sum_{n \geq 1} \frac{c_n(G)}{n^k} = \sum_{1 \leq i \leq u} P(M_i^k) \leq \frac{1}{P(\cap_{1 \leq i \leq u}(G^k \setminus M_i^k))} \leq \frac{1}{P(\Phi_k(G))} = \frac{1}{P_G(k)}.$$

In particolare abbiamo che

$$c_n(G) \leq \frac{n^k}{P_G(k)}.$$

Posto $k = \mathcal{V}_\eta(G)$ otteniamo che

$$c_n(G) \leq \frac{n^{\mathcal{V}_\eta(G)}}{\eta}.$$

Infine, una volta noto il cuore normale, dal Teorema 2.2.7 sappiamo che ci sono al più n^b sottogruppi massimali con un tale cuore normale. Si ricava quindi che

$$m_n(G) \leq c_n(G)n^b,$$

che implica che

$$m_n(G) \leq \eta^{-1} n^{\mathcal{V}_\eta(G)+b}.$$

Si può dunque concludere che

$$\mathcal{M}(G) = \sup_{n\geq 2} \frac{\log m_n(G)}{\log n} = \sup_{n\geq 2} \frac{\log_2 m_n(G)}{\log_2 n} \leq \mathcal{V}_\eta(G) + b - \log_2 \eta.$$

□

Per completezza vediamo anche il seguente risultato, che ci tornerà più utile nei successivi capitoli.

Teorema 2.2.12. *Dato $0 < \eta < 1$ esistono due costanti positive α_η, β_η tali che, per ogni gruppo finito G,*

$$\mathcal{M}(G) - \alpha_\eta \leq \mathcal{V}_\eta(G) \leq \mathcal{M}(G) + \beta_\eta.$$

Dimostrazione. Dalla Proposizione 2.2.11 sappiamo che possiamo porre $\alpha_\eta = 2 - \log_2 \eta$. Per quanto riguarda β_η, dalle osservazioni fatte nelle dimostrazioni della Proposizione 2.2.11 (1) e del Lemma 2.1.1 (2) e dall'Osservazione 2.0.2 (3) segue che

$$\begin{aligned} 1 - P_G(k) &\overset{(1)}{=} P\left(\bigcup_{M\leq_{max} G} M^k\right) \leq \sum_{M\leq_{max} G} P(M^k) \\ &= \sum_{M\leq_{max} G} \frac{1}{|G:M|^k} \overset{(2)}{=} \sum_{n=2}^{\infty} \frac{m_n(G)}{n^k} \overset{(3)}{=} \sum_{n=2}^{\infty} \frac{1}{n^{k-\mathcal{M}(G)}}. \end{aligned}$$

Sia ora β_η tale che

$$\sum_{n=2}^{\infty} \frac{1}{n^{\beta_\eta}} \leq 1 - \eta.$$

Per $k = \mathcal{M}(G) + \beta_\eta$ si ha

$$P_G(k) \geq 1 - \sum_{n=2}^{\infty} \frac{1}{n^{k-\mathcal{M}(G)}} = 1 - \sum_{n=2}^{\infty} \frac{1}{n^{\beta_\eta}} \geq \eta,$$

da cui abbiamo $\mathcal{V}_\eta(G) \leq k = \mathcal{M}(G) + \beta_\eta$. □

Mettendo insieme tutti i risultati visti in questo capitolo, possiamo ora dimostrare facilmente il seguente teorema.

Teorema 2.2.13. *Sia G un gruppo finito. Allora vale*

$$\lceil \mathcal{M}(G) \rceil - b - 2 \leq \mathcal{E}(G) \leq \lceil \mathcal{M}(G) \rceil + 3,$$

dove b è la costante che appare nel Teorema 2.2.7.

Dimostrazione. Abbiamo già dimostrato la Proposizione 2.1.2, quindi basta solo dimostrare la prima disuguaglianza. Prima di tutto possiamo vedere che dalla Proposizione 2.2.11 segue che, per ogni intero positivo i

$$\mathcal{V}_{2^{-i}}(G) \geq \mathcal{M}(G) - b + \log_2(2^{-i}) \geq \mathcal{M}(G) - b - i.$$

Sia ora $m = \lceil \mathcal{M}(G) \rceil$. Allora dall'osservazione appena fatta vediamo che posto $k = m - b - 1 - i$ si ottiene che $P_G(k) < 2^{-i}$. Possiamo inoltre assumere che $m \geq b + 2$, altrimenti $\mathcal{E}(G) \geq 0 \geq m - b - 2$. Quindi otteniamo

$$\begin{aligned} \mathcal{E}(G) &\geq \sum_{k=0}^{m-b-2} (1 - P_G(k)) \geq \sum_{k=0}^{m-b-2} \left(1 - 2^{k-(m-b-1)}\right) \\ &= m - b - 1 - \sum_{j=1}^{m-3} 2^{-j} \geq m - b - 1 - \sum_{j=1}^{\infty} 2^{-j} = m - b - 2. \end{aligned}$$

□

Capitolo 3

Generare con buona probabilità

In questo capitolo vogliamo capire come generare un gruppo con una buona probabilità, ovvero vogliamo stabilire un numero intero positivo k tale per cui presi k elementi del gruppo in maniera casuale essi lo generino buona probabilità.

Confrontandoci con i risultati visti fino ad ora, il problema che vogliamo affrontare non è altro che una stima dall'alto di $\mathcal{V}_\eta(G)$. Per una tale stima ci affideremo all'invariante $d(G)$, così definito:

Definizione 3.0.1. Sia G un gruppo finito. Allora denotiamo con $d(G)$ la minima cardinalità di un sottoinsieme $X \subseteq G$ che genera tutto il gruppo, ovvero

$$d(G) = \min_{X \subseteq G, \langle X \rangle = G} |X|.$$

Osservazione 3.0.2. Se $N \trianglelefteq G$, con $G = \langle g_1, \dots, g_n \rangle$, allora $G/N = \langle g_1 N, \dots, g_n N \rangle$, dunque $d(G/N) \leq d(G)$.

Dai risultati ottenuti nel Capitolo 2, in particolare dai Teoremi 2.2.12 e 2.2.13 possiamo osservare che studiare la quantità $\mathcal{V}_\eta(G) - d(G)$ non è poi così diverso dallo studio delle quantità $\mathcal{M}(G) - d(G)$ e $\mathcal{E}(G) - d(G)$.

Concentriamoci dunque sullo studio di tali differenze, innanzitutto per i gruppi nilpotenti e risolubili.

3.1 Stima di $\mathcal{V}_\eta(G)$ per gruppi nilpotenti e risolubili

Il primo a studiare la differenza $\mathcal{E}(G) - d(G)$ fu Carl Pomerance, il quale si concentrò sul caso in cui G è un gruppo abeliano elementare finito. In realtà vedremo che i suoi risultati possono essere estesi anche alla classe più generale di gruppi nilpotenti.

Definizione 3.1.1. Un gruppo G si dice *nilpotente* se ammette una *serie centrale*, ovvero una catena normale finita del tipo

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G,$$

tale che per ogni $i \in \{1, \dots, n\}$, vale

$$H_i / H_{i-1} \leq Z\left(G/H_{i-1}\right). \tag{3.1}$$

Osservazione 3.1.2. I p-gruppi finiti, con p un intero primo, sono nilpotenti. Infatti per ogni p-gruppo P è noto che $Z(P) \neq \{1\}$ e $P/Z(P)$ è ancora un p-gruppo. Ora, se $Z(P) = P$ allora abbiamo la serie centrale

$$\{1\} \trianglelefteq Z(P) = P.$$

Se invece $Z(P) < P$ allora abbiamo che $Z(P/Z(P)) = Z_2/Z(P)$, per un unico $Z(P) < Z_2 \trianglelefteq P$. Abbiamo dunque che

$$\{1\} \trianglelefteq Z_1 = Z(P) \trianglelefteq Z_2 \trianglelefteq P,$$

con $Z_2/Z_1 = Z(P/Z_1)$. Iterando l'argomento otteniamo una catena normale di sottogruppi di P del tipo

$$\{1\} \trianglelefteq Z(P) \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_n = P,$$

con i quozienti $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. Dunque P è nilpotente.

La condizione (3.1) si può esprimere anche attraverso l'utilizzo dei commutatori:

Definizione 3.1.3. Sia G un gruppo e $a, b \in G$. Definiamo il *commutatore* di a e b l'elemento

$$[a, b] = a^{-1}b^{-1}ab.$$

Dati due sottogruppi A e B di G definiamo il commutatore di A e B il sottogruppo

$$[A, B] = \langle [a, b] | a \in A,\ b \in B \rangle.$$

Osservazione 3.1.4. Possiamo vedere, guardando alla definizione di serie centrale, che la condizione $H_i/H_{i-1} \leq Z\left(G/H_{i-1}\right)$ è equivalente alla condizione che $[H_i, G] \leq H_{i-1}$. Infatti il quoziente H_i/H_{i-1} è contenuto in $Z(G/H_{i-1})$ se e solo se per ogni $h \in H_i,\ g \in G$, vale

$$hgH_{i-1} = (hH_{i-1})(gH_{i-1}) = (gH_{i-1})(hH_{i-1}) = hgH_{i-1}.$$

Ma questo è equivalente a chiedere che

$$\forall h \in H_i,\ \forall g \in G,\ (gh)^{-1}hg = [h, g] \in H_{i-1},$$

ovvero che $[H_i, G] \leq H_{i-1}$.

I commutatori sono importanti per lo studio della struttura del gruppo G, in particolare ci permettono di capire quando un quoziente G/N è abeliano. Vale infatti il seguente lemma.

Lemma 3.1.5. *Sia $N \trianglelefteq G$ un sottogruppo normale. Allora $G' \stackrel{def}{=} [G, G] \leq N$ se e solo se il quoziente G/N è abeliano.*

Dimostrazione. Sappiamo che, dati $a, b \in G$, vale

$$abN = (aN)(bN) = (bN)(aN) = baN$$

se e solo se $(ba)^{-1}ab = a^{-1}b^{-1}ab = [a, b] \in N$. Allora se $G' \leq N$ abbiamo che per ogni $a, b \in G$ vale $[a, b] \in N$, dunque G/N è abeliano. Viceversa, se G/N è abeliano abbiamo che, dati $a, b \in G$ qualsiasi, $abN = baN$, e dunque $[a, b] \in N$. Possiamo concludere quindi che $G' \leq N$. □

Vediamo ora alcune delle caratteristiche principali dei gruppi finiti nilpotenti (per la dimostrazione: [4], pag. 274).

Teorema 3.1.6. *Sia G un gruppo finito. Allora sono equivalenti:*

(a) G è nilpotente;

(b) ogni sottogruppo massimale di G è normale in G;

(c) ogni sottogruppo di Sylow di G è normale in G;

(d) G si decompone come il prodotto diretto dei suoi sottogruppi di Sylow.

Prima di iniziare a studiare la differenza $\mathcal{E}(G) - d(G)$ per i gruppi finiti nilpotenti, abbiamo bisogno di dare un'ultima definizione e dimostrare un lemma.

Definizione 3.1.7. Sia G un gruppo finito non banale. Allora definiamo il *sottogruppo di Frattini* di G il sottogruppo formato dall'intersezione di tutti i sottogruppi massimali di G, ovvero

$$\mathrm{Frat}(G) = \bigcap_{M \leq_{max} G} M.$$

Osservazione 3.1.8. Il sottogruppo di Frattini ha la proprietà che se $H \leq G$ è tale per cui $H \,\mathrm{Frat}(G) = G$, allora si deve avere che $H = G$. Infatti se per assurdo $H \neq G$, allora H è contenuto in almeno un sottogruppo massimale di G, per esempio M, e dunque si avrebbe $H \,\mathrm{Frat}(G) \leq M < G$, il che è assurdo.

A partire da questa proprietà vediamo che si può considerare il sottogruppo $\mathrm{Frat}(G)$ come l'insieme dei non-generatori di G, ovvero degli $x \in G$ tali che $G = \langle x, X\rangle$ implica che $G = \langle X\rangle$. Infatti se $x \in G$ è un non-generatore allora si può vedere che per ogni sottogruppo massimale M di G, $M \leq \langle x, M\rangle < G$, e dunque $M = \langle x, M\rangle$ da cui $x \in M$. Quindi siccome x sta in tutti i sottogruppi massimali ne segue che $x \in \mathrm{Frat}(G)$. Se invece $x \in \mathrm{Frat}(G)$, allora con un ragionamento analogo a quello fatto in precedenza ne segue che x è un non-generatore.

Grazie a questa intuizione possiamo fare un'ultima osservazione, che ci servirà in seguito. Il sottogruppo di Frattini gode della proprietà che

$$\langle g_1, \ldots, g_k\rangle = G \iff \langle \mathrm{Frat}(G)g_1, \ldots, \mathrm{Frat}(G)g_k\rangle = G/\,\mathrm{Frat}(G).$$

Infatti se $\langle \mathrm{Frat}(G)g_1, \ldots, \mathrm{Frat}(G)g_k\rangle = G/\,\mathrm{Frat}(G)$, allora posto $H = \langle g_1, \ldots, g_k\rangle$ si ha che $G = H \,\mathrm{Frat}(G)$ e dunque $G = H = \langle g_1, \ldots, g_k\rangle$.

Questo ci permette di concludere che $\forall k \in \mathbb{N}$, $P_G(k) = P_{G/\,\mathrm{Frat}(G)}(k)$ e dunque $\mathcal{E}(G) = \mathcal{E}(G/\,\mathrm{Frat}(G))$.

Lemma 3.1.9. *Siano G un gruppo finito nilpotente d-generato e p un fattore primo di $|G|$ e sia N_p è il sottogruppo normale dato dall'intersezione di tutti i sottogruppi massimali di indice p. Allora G/N_p è un p-gruppo abeliano elementare tale che $d(G/N_p) \leq d$.*

Dimostrazione. Siccome G è nilpotente, per il Teorema 3.1.6 abbiamo che

$$G = P_p \times \prod_{q \neq p} P_q := P \times H,$$

dove con P_q si intende il q-sottogruppo di Sylow di G. Ora sia M un sottogruppo massimale di G di indice p. Allora $H \leq M$: se esistesse $x \in H \setminus M$ si avrebbe che p non divide $|x|$. Però il quoziente G/M è un p-gruppo, dunque ogni suo elemento ha ordine potenza di p. Quindi un tale x non può esistere. Quindi i sottogruppi massimali di indice p sono del tipo $M = M_p \times H$, con M_p un sottogruppo massimale di P tale che $|P : M_p| = p$. In realtà in P i sottogruppi massimali M hanno tutti indice p, in quanto $M \trianglelefteq P$ (perché i p-gruppi sono nilpotenti) e P/M è un gruppo semplice senza sottogruppi propri (per il Teorema di corrispondenza), dunque un gruppo ciclico di ordine p. Quindi abbiamo che

$$N_p = \left(\bigcap_{M \leq_{max} P} M \right) \times H = \mathrm{Frat}(P) \times H$$

e dunque

$$G/N_p \cong P/\mathrm{Frat}(P).$$

Ci basta dunque dimostrare la tesi per il p-gruppo P. Per l'osservazione fatta in precedenza, per ogni sottogruppo massimale M di P vale che P/M è abeliano (è ciclico) e dunque $P' \leq M$ per il Lemma 3.1.5. Quindi $P' \leq \mathrm{Frat}(P)$ e, sempre dal Lemma 3.1.5, ricaviamo che $P/\mathrm{Frat}(P)$ è abeliano. Dobbiamo ora dimostrare che $x^p \in \mathrm{Frat}(P)$ $\forall x \in P$, ovvero che ogni elemento ha ordine p in $P/\mathrm{Frat}(P)$. Questo deriva da un ragionamento analogo a quello fatto in precedenza: sia M un sottogruppo massimale di P, allora P/M è ciclico di ordine p, dunque $M = (xM)^p = x^p M$ per ogni $x \in P$. Ma allora $x^p \in M$ per ogni sottogruppo massimale M, dunque $x^p \in \mathrm{Frat}(P)$.
Infine, grazie all'Osservazione 3.0.2 abbiamo che $d(P/\mathrm{Frat}(P)) \leq d(P)$ e abbiamo dunque dimostrato la tesi. □

Abbiamo ora tutti gli elementi per studiare la differenza $\mathcal{E}(G) - d(G)$. Come accennato in precedenza Carl Pomerance dimostrò i suoi risultati per i gruppi finiti abeliani elementari. L'Osservazione 3.1.8 e la dimostrazione del Lemma 3.1.9 ci permettono però di estendere i suoi risultati alla più vasta classe dei gruppi finiti nilpotenti.

Proposizione 3.1.10. *Sia G è un gruppo finito nilpotente d-generato, allora $\mathcal{M}(G) \leq d$.*

Dimostrazione. Sia N_p l'intersezione di tutti i sottogruppi massimali di indice p. Dal Lemma 3.1.9 segue che G/N_p è un p-gruppo abeliano elementare con $r = d(G/N_p) \leq d(G) \leq d$. Quindi abbiamo che $G/N_p \cong \mathbb{F}_p^r$, che si può vedere come uno spazio vettoriale di dimensione r su $\mathbb{F}_p$. Abbiamo quindi che $m_p(G/N_p)$ corrisponde al numero di iperpiani di $\mathbb{F}_p^r$. Sappiamo che ogni iperpiano è determinato da un vettore nello spazio duale, (è individuato dall'equazione lineare omogenea $a_1x_1 + \cdots + a_nx_n$) quindi il loro numero coincide con il numero dei vettori non nulli di $\mathbb{F}_p^r$ a meno di proporzionalità (vettori proporzionali "identificano" lo stesso iperpiano), quindi abbiamo che

$$m_p(G/N_p) = \frac{p^r - 1}{p - 1}.$$

Inoltre, per il Teorema di corrispondenza abbiamo che $m_p(G) = m_p(G/N_p)$ in quanto i sottogruppi massimali di G di indice p sono tutti e soli quelli che contengono N_p. Mettendo tutto insieme otteniamo

$$m_p(G) = m_p(G/N_p) = \frac{p^r - 1}{p - 1} \leq \frac{p^d - 1}{p - 1}.$$

Quindi, per ogni $n \geq 2$,

$$\frac{\log m_n(G)}{\log n} \leq d,$$

da cui la tesi. □

Grazie al Teorema 2.2.13 possiamo quindi concludere che:

Teorema 3.1.11. *Sia G è un gruppo finito nilpotente, allora $\mathcal{E}(G) - d(G) \leq 3$.*

In realtà, con un ragionamento molto più laborioso, Carl Pomerance (in [13]) ottenne una stima più fine: per ogni gruppo finito nilpotente G,

$$\mathcal{E}(G) - d(G) \leq 1 + \sum_{j=2}^{\infty} \left(1 - \prod_{t=2}^{\infty} \zeta(t)^{-1} \prod_{l=2}^{j-1} \zeta(l) \right) \sim 2.11845$$

con $\zeta(s) = \sum_n 1/n^s$ la funzione zeta di Riemann. Con un calcolo simile Igor Pak (in [11]) dimostrò che se G è un gruppo finito nilpotente, allora $\mathcal{V}_{1/e}(G) \leq d(G) + 1$.

Vediamo ora il caso dei gruppi risolubili. Enunciamo solo i risultati principali senza entrare nei dettagli delle dimostrazioni.

Definizione 3.1.12. Un gruppo G è detto *risolubile* se esiste una catena normale finita

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

tale che ogni quoziente H_i/H_{i-1} è abeliano per $i \in \{1, \ldots, n\}$.

Introduciamo anche il numero

$$\gamma = \log_9(48 \cdot 24^{1/3}) \sim 2.24399,$$

chiamato la *costante di Palfy-Wolf*, che sarà fondamentale in questi risultati. Questa costante è stata trovata indipendentemente da Palfy (in [12]) e Wolf (in [16]), i quali hanno dimostrato che se G è un sottogruppo risolubile di $GL(V)$ che non stabilizza alcun sottogruppo proprio di V, allora $|G| \leq |V|^\gamma$. A partire dal loro risultato, è stato dimostrato (in [10]) il seguente teorema.

Teorema 3.1.13. *Sia G è un gruppo risolubile finito e d-generato, allora, per n abbastanza grande, vale*

$$m_n(G) \leq n^{\gamma d+3}.$$

Dal Teorema 2.2.12 segue subito il seguente Corollario.

Corollario 3.1.14. *Dato $0 < \eta < 1$ esiste una costante positiva c_η tale che, per ogni gruppo finito risolubile G,*

$$\mathcal{V}_\eta(G) \leq \gamma d(G) + c_\eta.$$

3.2 Stima di $\mathcal{V}_\eta(G)$ per i gruppi finiti

Il comportamento di $\mathcal{V}_\eta(G)$ quando G è nilpotente o risolubile ci suggerisce che potrebbe esistere una funzione $\rho_\eta : \mathbb{N} \to \mathbb{N}$ tale che, per ogni gruppo finito G, valga $\mathcal{V}_\eta(G) \leq \rho_\eta(d(G))$.

In realtà questa intuizione è errata. Vale infatti il seguente teorema (per una dimostrazione più completa: [5]).

Teorema 3.2.1. *Per ogni intero positivo n, esiste un gruppo finito di-generato tale che $\mathcal{E}(G) \geq n$.*

Prima della dimostrazione, abbiamo bisogno della seguente osservazione.

Osservazione 3.2.2. Sia S un gruppo semplice non abeliano. Cerchiamo di capire quanto vale $d(S^t)$, con $t \in \mathbb{N}$. Siano $s_1, s_2 \in S$ tali che $\langle s_1, s_2 \rangle = S$ (grazie al Teorema di classificazione dei gruppi semplici sappiamo infatti che S è 2-generato) e definiamo

$$g_1 = (s_{1,1}, \ldots, s_{1,t}),\ g_2 = (s_{2,1}, \ldots, s_{2,t}) \in S^t.$$

Cerchiamo di capire quando essi generano S^t. Per $1 \leq i \leq t$ consideriamo le proiezioni canoniche sull'i-esima coordinata $\pi^i : L_t \to L$ che mappano $(s_1, \ldots, s_t)$ in s_i. Osserviamo quindi le coordinate di g_1 e g_2 producono t coppie in S^2. Ora se vogliamo che $\langle g_1, g_2 \rangle = S^t$, allora per $1 \leq i \leq t$ si deve avere che $\langle s_{1,i}, s_{2,i} \rangle = \langle g_1^{\pi_i}, g_2^{\pi_i} \rangle = G^{\pi_i} = S$, ovvero che ciascuna delle t coppie generi S, perché le proiezioni sono degli epimorfismi e dunque mandano sottoinsiemi generatori in sottoinsiemi generatori. In particolare abbiamo che ciascuna delle coppie deve stare in

$$\Omega = \{(s_1, s_2) \in S^2 | \langle s_1, s_2 \rangle = S\}.$$

Questo insieme, ricordando la definizione 1.1.1, ha cardinalità $|\Omega| = |S|^2 P_S(2)$.

Non basta però che le t coppie stiano in Ω affinché $\langle g_1, g_2 \rangle = S^t$. Infatti se esistono $\gamma \in \mathrm{Aut}(S)$ e $1 \leq i < j \leq t$ tali che $(s_{1,j}, s_{2,j}) = ((s_{1,i})^\gamma, (s_{2,i})^\gamma)$, allora $\langle g_1, g_2 \rangle$ è

contenuto nel sottogruppo di S^t che consiste degli elementi $(s_1, \dots, s_t)$ con $s_j = s_i^\gamma$, e dunque $\langle g_1, g_2 \rangle \lneq S^t$. Per evitare questa possibilità si deve dunque avere che le t coppie appartengono ad orbite distinte sotto l'azione di $\mathrm{Aut}(S)$ su Ω. Ora se $\omega = (s_1, s_2) \in \Omega$ e $\alpha \in \mathrm{Stab}_{\mathrm{Aut}(S)}(\omega)$, allora $(s_i)^\alpha = s_i$ per $i \in \{1, 2\}$. Siccome $\langle s_1, s_2 \rangle = S$, allora l'automorfismo α fissa tutto S, dunque si ha $\alpha = 1$. Quindi $\mathrm{Stab}_{\mathrm{Aut}(S)}(\omega) = \{1\}$ per ogni $\omega \in \Omega$, e dunque, per la biezione tra $\mathrm{Aut}(S)/\mathrm{Stab}_{\mathrm{Aut}(S)}(\omega)$ (l'insieme delle classi laterali) e l'orbita di ω sotto l'azione di $\mathrm{Aut}(S)$, abbiamo che la cardinalità di ogni orbita è $|\mathrm{Aut}(S)|$. Dunque vi sono $|\Omega|/|\mathrm{Aut}(S)|$ distinte orbite dell'azione di $\mathrm{Aut}(S)$ sull'insieme Ω.

Abbiamo in sintesi dimostrato che

$$d(S^t) \leq 2 \iff t \leq \frac{|\Omega|}{|\mathrm{Aut}(S)|} = \frac{|S|^2 P_S(2)}{|\mathrm{Aut}(S)|}.$$

Siamo ora pronti per la dimostrazione.

Dimostrazione. Per ogni intero positivo $n \geq 7$ definiamo $G_n = \mathrm{Alt}(n)^{\frac{n!}{8}}$. Siccome $n \geq 7$, allora $\mathrm{Aut}(\mathrm{Alt}(n)) \cong \mathrm{Sym}(n)$. Si può inoltre dimostrare che $P_{\mathrm{Alt}(n)}(2) \geq 53/90 > 1/2$. Ora, dall'Osservazione 3.2.2, siccome

$$\frac{|\mathrm{Alt}(n)|^2 P_{\mathrm{Alt}(n)}(2)}{|\mathrm{Aut}(\mathrm{Alt}(n))|} \geq \frac{(n!/2)^2(1/2)}{n!} = \frac{n!}{8},$$

allora $d(G_n) = d(\mathrm{Alt}(n)^{\frac{n!}{8}}) = 2$.

Ora G_n contiene $n!/8$ sottogruppi normali N tali che $G_n/N \cong \mathrm{Alt}(n)$. Sappiamo che $m_n(\mathrm{Alt}(n)) = n$, quindi $m_n(G_n) \geq n \cdot n!/8$. Dal Teorema 2.2.13 segue

$$\mathcal{E}(G_n) \geq \mathcal{M}(G_n) - b - 2 \geq \frac{\log(n \cdot n!/8)}{\log(n)} - b - 2,$$

e si conclude osservando che

$$\lim_{n \to \infty} \frac{\log(n \cdot n!/8)}{\log(n)} = \infty.$$

□

Il fallimento della nostra intuizione ci porta dunque a concludere che per un generico gruppo finito la quantità $d(G)$ non basta a stimare $\mathcal{V}_\eta(G)$: sono dunque necessarie altre informazioni sul gruppo per trovare la stima cercata.

Risultati preliminari

Per poter raggiungere il nostro obbiettivo abbiamo però prima bisogno di introdurre alcuni concetti, come ad esempio il concetto di G-gruppo e di fattore principale, e alcuni risultati di base su questi argomenti.

Prima di addentrarci in questi concetti diamo un po' di definizioni generali.

Definizione 3.2.3. Dato un gruppo G il suo *zoccolo*, $\mathrm{soc}(G)$, è il sottogruppo generato dai sottogruppi normali minimali. Un gruppo G si dice *monolitico* se contiene un unico sottogruppo minimale N. In questo caso è chiaro che $\mathrm{soc}(G) = N$. Un gruppo monolitico G si dice *primitivo* se $\mathrm{soc}(G) \not\leq \mathrm{Frat}(G)$.

Definizione 3.2.4. Sia L un gruppo monolitico primitivo e $N = \mathrm{soc}(L)$. Allora definiamo

$$\mathrm{End}_L(N) = \{\phi \in \mathrm{End}(N) | (x^g)^\phi = (x^\phi)^g \ \forall x \in N, \forall g \in G\}.$$

Definiamo inoltre la quantità

$$q_L = \begin{cases} |\mathrm{End}_L(N)| & \text{se } N \text{ é abeliano,} \\ 1 & \text{altrimenti.} \end{cases}$$

Ricordiamo che, se N è abeliano, $\mathrm{End}_L(N)$ è un anello con divisione per il Lemma di Schur ([14], 8.1.4) e, siccome è finito, è un campo per il Teorema di Wedderburn.

Definizione 3.2.5. Sia G un gruppo di permutazioni che agisce su insieme Ω. Un sottoinsieme $B \subseteq \Omega$ è detto *blocco per* G se, per ogni $g \in G$, $B^g = B$ oppure $B^g \cap B = \emptyset$. Un gruppo di permutazioni G si dice *primitivo* se agisce su un insieme Ω transitivamente, ovvero dati $\omega, \alpha \in \Omega$ esiste $g \in G$ tale che $\omega^g = \alpha$, e non preservandone alcuna partizione non banale, quindi se non esistono blocchi non banali di Ω per G.

Vediamo subito due risultati sulla struttura dei gruppi primitivi che saranno necessari in futuro.

Osservazione 3.2.6. Sia G un gruppo finito e M un suo sottogruppo massimale. Indichiamo con G/M l'insieme delle classi laterali sinistre di M in G e consideriamo l'azione naturale di G su G/M, tale per cui $(xM)^g = gxM$ per ogni $g \in G$, $xM \in G/M$. Si può facilmente osservare che tale azione è ben definita, ovvero non dipende dal rappresentante xM scelto. Inoltre è chiaro che una tale azione è transitiva, in quanto, dati $xM, yM \in G/M$ posto $g = yx^{-1}$ si ha che $(xM)^g = yM$.

Sia ora B un blocco di G/M per G con $M \in B$ e sia $H = \mathrm{Stab}_G(B) = \{g \in G | B^g = gB = B\}$. Ora è chiaro che $H \leq G$, ma si vede anche che $M \leq H$, in quanto dato $m \in M$ abbiamo che $mB = B$. In quanto M è massimale abbiamo dunque che $H = M$ o $H = G$.

Nel primo caso si deve avere $B = M/M = \{M\}$, mentre nel secondo si deve avere che $B = G/M$. Quindi l'azione di G su G/M preserva solo i blocchi banali.

Tale azione non è però sempre fedele. Infatti $g \in G$ sta nel nucleo dell'azione se e solo se

$$(xM)^g = xM \ \forall x \in G \Leftrightarrow x^{-1}gx \in M \ \forall x \in G \Leftrightarrow g \in \bigcap_{x \in G} xMx^{-1} \Leftrightarrow g \in \mathrm{Core}_G(M).$$

Dunque il nucleo dell'azione coincide con $\mathrm{Core}_G(M)$. Possiamo osservare ora che considerando l'azione di $G/\mathrm{Core}_G(M)$ su G/M definita come sopra a meno di passaggio al quoziente, le proprietà di tale azione non cambiano, ovvero tale azione è comunque primitiva. Infatti abbiamo che dato $g, h \in G$ allora abbiamo che

$$g\,\mathrm{Core}_G(M) = h\,\mathrm{Core}_G(M) \Leftrightarrow h^{-1}g \in \mathrm{Core}_G(M),$$

e dunque $h^{-1}g$ fissa tutti gli elementi di G/M.

Abbiamo quindi in sintesi dimostrato che se M è un sottogruppo massimale di G allora $G/\mathrm{Core}_G(M)$ è un gruppo primitivo.

Lemma 3.2.7. *Sia G un gruppo primitivo e siano Ω l'insieme su cui G agisce in maniera primitiva e N un sottogruppo normale di G non banale. Allora N agisce transitivamente su Ω.*

Dimostrazione. Possiamo subito osservare che le orbite dell'azione di N su Ω costituiscono una partizione di Ω, perché la relazione che associa due elementi a, b di Ω se e solo se esiste un n tale che $a^n = b$ è di equivalenza. Abbiamo quindi $\Omega = \bigsqcup O_i$, con O_i le varie orbite. Siano ora O_j un orbita e $g \in G$. Allora anche $(O_j)^g$ è un'orbita sotto l'azione di N, ovvero esiste un k tale che $O_j = O_k$. Infatti, per la normalità di N, abbiamo che

$$(O_j)^g = (\omega^N)^g = \{(\omega^n)^g | n \in N\} = \{\omega^{ng} | n \in N\} = \{\omega^{gn_1} | n_1 \in N\} = (\omega^g)^N.$$

Abbiamo quindi dimostrato che l'insieme delle orbite di Ω sotto l'azione di N è una partizione di Ω che viene preservata dall'azione di G. Dunque per la primitività di G abbiamo che questa partizione deve essere banale. Dunque siamo nel caso in cui le orbite sono i singoletti (che implica che $N = \{1\}$) oppure nel caso in cui vi è una sola orbita, che vuol dire che N agisce transitivamente su Ω. □

A partire da questo lemma possiamo dimostrare la seguente proposizione.

Proposizione 3.2.8. *Sia G un gruppo di permutazioni primitivo finito. Allora G ha al massimo due sottogruppi normali minimali. Nel caso G ammetta due sottogruppi normali minimali, allora essi non sono abeliani.*

Dimostrazione. Siano N_1 e N_2 due sottogruppi normali minimali di G. Dalla definizione di commutatori discende allora subito che anche $[N_1, N_2]$ è normale e vale $[N_1, N_2] \leq N_1 \cap N_2$. Siccome però N_1 e N_2 sono minimali allora $N_1 \cap N_2 = \{1\}$, in quanto è un sottogruppo normale. Abbiamo quindi che $[N_1, N_2] = \{1\}$, che implica $N_2 \leq C_G(N_1)$, con $C_G(H) \stackrel{def}{=} \{g \in G | h^g = h\ \forall h \in H\}$ il centralizzante di H in G.

Facciamo ora un'osservazione sull'azione di $C = C_G(N_1)$ su Ω. Supponiamo che esistano $c \in C$ e $\omega \in \Omega$ tali che $\omega^c = \omega$. Sia ora $\alpha \in \Omega$ qualsiasi. Dal Lemma 3.2.7 abbiamo che N_1 è transitivo, ovvero esiste $n \in N_1$ tale che $\omega^n = \alpha$. Ma allora, siccome $c \in C$, abbiamo $\alpha = \omega^n = (\omega^c)^n = (\omega^n)^c = \alpha^c$, ovvero c fissa ogni punto di Ω, quindi $c = 1$ perché G è un gruppo di permutazioni e dunque l'azione è fedele. Da questa osservazione possiamo osservare che $|C| \leq |\Omega|$, in quanto la applicazione che,

fissato un elemento $\omega \in \Omega$, manda ogni elemento $c \in C$ nell'elemento $\alpha \in \Omega$ tale che $\omega^c = \alpha$ è iniettiva. Infatti, dati $c_1, c_2 \in C$ tali che $\omega^{c_1} = \omega^{c_2} = \alpha$ allora avremmo che $(\omega^{c_1})^{c_2^{-1}} = (\omega^{c_2})^{c_2^{-1}} = \omega$, e per quanto sopra osservato si ottiene $c_1 c_2^{-1} = 1$, ovvero $c_1 = c_2$.

Dimostriamo ora che $N_2 = C$. Iniziamo osservando che, in quanto anche N_2 è normale, allora anche l'azione di N_2 è transitiva. In realtà, come sopra osservato, siccome $N_2 \leq C$, abbiamo che l'azione è più forte: vale che dati $\omega, \alpha \in \Omega$ esiste un unico $n \in N_2$ tale che $\omega^n = \alpha$. Da questo ricaviamo che $|N_2| = |\Omega|$, in quanto fissato $\omega \in \Omega$ esiste una biiezione che manda ogni elemento $\alpha \in \Omega$ nell'unico elemento $n \in N_2$ tale che $\omega^n = \alpha$. Ma allora $N_2 \leq C$ e $|C| \leq |\Omega| = |N_2|$, da cui $N_2 = C_G(N_1)$. Scambiando i ruoli di N_1 e N_2 si ottiene che anche $N_1 = C_G(N_2)$.

Sia ora $N_3 \trianglelefteq G$ un terzo sottogruppo normale minimale. Ripetendo lo stesso ragionamento allora avremmo che $N_3 = C_G(N_1)$, e dunque $N_3 = N_2$.

Abbiamo quindi trovato che se il gruppo G ammette due sottogruppi normali minimali distinti $N_1 \neq N_2$ allora $C_G(N_1) = N_2$ e $C_G(N_1) = N_2$. Possiamo quindi concludere che, siccome $N_1 \cap N_2 = \{1\}$, i due sottogruppi normali minimali non sono abeliani, in quanto $N_1 \not\leq C_G(N_1) = N_2$ e $N_2 \not\leq C_G(N_2) = N_1$. □

Osservazione 3.2.9. Sia G un gruppo primitivo su Ω che ammette due sottogruppi normali minimali distinti N_1 e N_2. Sia $\omega \in \Omega$ un punto e $H = \mathrm{Stab}_G(\omega)$. Dalla dimostrazione precedente segue che $H \cap N_1 = \{1\} = H \cap N_2$. Sia ora $g \in G$. Dalla transitività dell'azione di N_1 su Ω abbiamo che $\omega^g = \alpha = \omega^n$ per un qualche $n \in N_1$. In particolare abbiamo dunque che $\omega^{gn^{-1}} = \omega$ e dunque $gn^{-1} \in H$. Vale quindi che $G = HN_1$ e analogamente $G = HN_2$. Abbiamo quindi dimostrato che lo stabilizzatore di un punto è un complemento comune a tutti e due i sottogruppi normali minimali.

Possiamo ora iniziare a introdurre i primi concetti. Partiamo con ordine dalla definizione di G-gruppo, G-isomorfismo e G-equivalenza.

Definizione 3.2.10. Dato un gruppo G diciamo che il gruppo A è un *G-gruppo* se G agisce su A tramite automorfismi. Se G non stabilizza alcun sottogruppo proprio non banale di A diremo che A è un G-gruppo *irriducibile*.

Definizione 3.2.11. Due G-gruppi A e B di dicono *G-isomorfi*, e scriveremo $A \cong_G B$, se esiste un isomorfismo di gruppi $\phi : A \to B$ tale che $\forall a \in A,\ \forall g \in G,\ (a^g)^\phi = (a^\phi)^g$.

Definizione 3.2.12. Due G-gruppi A e B di dicono *G-equivalenti*, e scriveremo $A \equiv_G B$, se esistono due isomorfismi $\phi : A \to B$ e $\Phi : A \rtimes G \to B \rtimes G$ che commutano il seguente diagramma:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Phi} & & \| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1. \end{array} \tag{3.2}$$

Vediamo ora cosa sono i fattori principali di un gruppo G e come il concetto di G-isomorfismo ci permetterà di definire una relazione di equivalenza tra i fattori principali di G.

Definizione 3.2.13. Siano X e Y sottogruppi normali di un gruppo finito G tali che $Y \leq X$. Diciamo che X/Y è un *fattore principale* di G se è un sottogruppo normale minimale di G/Y. Indichiamo con $\mathcal{CF}(G)$ l'insieme dei fattori principali di G.

Possiamo osservare che ogni fattore principale X/Y di G è un G-gruppo. Infatti, in quanto $X, Y \trianglelefteq G$, possiamo considerare l'azione $\rho : G \to \mathrm{Aut}(X/Y)$ tale che $g^\rho : xY \mapsto x^g Y$ per ogni $x \in X$. A partire da ciò diamo la seguente osservazione.

Definizione 3.2.14. Siano $X_1/Y_1,\ X_2/Y_2 \in \mathcal{CF}(G)$. Diciamo che X_1/Y_1 e X_2/Y_2 sono in *G-relazione* se si ha che o $X_1/Y_1 \cong_G X_2/Y_2$ o esiste un sottogruppo normale $N \trianglelefteq G$ tale che

1. G/N è un gruppo di permutazioni primitivo, che contiene due sottogruppi normali minimali distinti: M_1/N e M_2/N;
2. Esiste un sottogruppo $N \leq U \leq G$ tale che U/N è un complemento sia di M_1/N che di M_2/N in G/N;
3. $X_1/Y_1 \cong_G M_1/N$ e $X_2/Y_2 \cong_G M_2/N$.

Proposizione 3.2.15. *Siano $X_1/Y_1,\ X_2/Y_2 \in \mathcal{CF}(G)$. Allora $X_1/Y_1 \equiv_G X_2/Y_2$ se e solo se X_1/Y_1 e X_2/Y_2 sono in G-relazione.*

Definizione 3.2.16. Diciamo che un fattore principale X/Y di G è *di Frattini* se vale che $X/Y \leq \mathrm{Frat}(G/Y)$.

Osservazione 3.2.17. Se X/Y è un fattore principale non di Frattini di G, allora esiste un sottogruppo massimale M di G tale che $G = XM$ e $M \cap X = Y$. Infatti se X/Y non è di Frattini, ovvero $X/Y \not\leq \mathrm{Frat}(G/Y)$, allora esiste un massimale M/Y di G/Y tale che $X/Y \not\leq M/Y$. In particolare dobbiamo avere $X \not\leq M$ in G e, dalla massimalità di M segue che $G = XM$. Inoltre si ha che $Y \leq X \cap M \leq X$ e $X \cap M \trianglelefteq G$, e dunque dalla minimalità di X/Y segue che $X \cap M = Y$.

Definizione 3.2.18. Sia A un fattore principale di G. Allora, considerando l'azione ρ definita in precedenza, si definisce il *gruppo monolitico primitivo associato ad A* come

$$L_G(A) = \begin{cases} G^\rho A \cong A \rtimes (G/C_G(A)) & \text{se } A \text{ è abeliano,} \\ G^\rho \cong G/C_G(A) & \text{altrimenti.} \end{cases}$$

Ad ogni gruppo finito G e ogni fattore principale A di G è associato un intero positivo $\delta_G(A)$. Tale numero risulta essere molto utile nello studio dei fattori principali di G. Si può per esempio dimostrare il seguente teorema (per la dimostrazione: [9]).

Teorema 3.2.19. *Ogni serie principale di G contiene esattamente $\delta_G(A)$ fattori principali che sono non di Frattini e sono G-equivalenti ad A.*

Stima per i gruppi finiti

Abbiamo ora tutti gli elementi per trovare una stima di $\mathcal{V}_\eta(G)$ per tutti i gruppi finiti. Per ottenerla partiamo dalla seguente definizione.

Definizione 3.2.20. Sia $\mathcal{N}_G$ un insieme di rappresentanti delle classi di equivalenza di fattori principali di G non di Frattini. Possiamo allora definire i seguenti insiemi

$$\begin{aligned}
\mathcal{A}_G(n) &= \{A \in \mathcal{N}_G | A \text{ é abeliano e } |A| = n\};\\
\mathcal{B}_G(n) &= \{A \in \mathcal{N}_G | A \text{ non é abeliano e } |A| = n\};\\
\mathcal{C}_G(n) &= \{A \in \mathcal{N}_G | A \text{ non é abeliano e } L_G(A) \text{ contiene}\\
&\qquad\qquad \text{un sottogruppo massimale core-free di indice } n\};\\
\mathcal{D}_G(n) &= \{A \in \mathcal{N}_G | A \text{ non é abeliano e } n \big| |A|\};\\
\mathcal{N}_G(p) &= \{A \in \mathcal{N}_G | p \text{ divide } |A|\}.
\end{aligned}$$

Poniamo inoltre

$$\alpha_G(n) = |\mathcal{A}_G(n)|,\ \gamma_G(n) = \sum_{D \in \mathcal{D}_G(n)} \delta_G(D),\ \lambda_G(n) = \alpha_G(n) + \gamma_G(n).$$

Facciamo ora alcune considerazioni sui sottogruppi massimali di G. In particolare, dato $n \in \mathbb{N}$, proviamo a contare il numero dei sottogruppi massimali di G di indice n. Sia M uno di questi. Sappiamo dall'Osservazione 3.2.6 che $G/\operatorname{Core}_G(M)$ è un gruppo primitivo e dunque, dalla Proposizione 3.2.8, può avere al più due sottogruppi normali minimali. Vi sono dunque due casi: si può avere che $G/\operatorname{Core}_G(M) \cong L$, con L un gruppo monolitico primitivo oppure, come dimostrato in [2], $G/\operatorname{Core}_G(M) \cong L_2 \stackrel{def}{=} \{(l_1, l_2) \in L^2 | l_1 N = l_2 N\}$ con L un gruppo monolitico e $N = \operatorname{soc}(L)$ non abeliano.

Ora l'Osservazione 3.2.17 evidenzia uno stretto legame tra i sottogruppi massimali, in realtà tra i cuori normali di un sottogruppo massimale, e i fattori principali non di Frattini. In effetti, considerato $\overline{M} = M/\operatorname{Core}_G(M) \leq G/\operatorname{Core}_G(M)$ esso è un sottogruppo massimale core-free. Sia $\overline{N} = N/\operatorname{Core}_G(M)$ un sottogruppo normale minimale di $G/\operatorname{Core}_G(M)$: in quanto $\overline{M}$ non contiene alcun sottogruppo normale non banale si deve avere allora che $G/\operatorname{Core}_G(M) = \overline{M}\ \overline{N}$ e che $\overline{M} \cap \overline{N} = \{1\}$. Abbiamo allora che il fattore $N/\operatorname{Core}_G(M)$ è principale non di Frattini. Inoltre si ha che

$$|G| = \frac{|M||N|}{|\operatorname{Core}_G(M)|} \Rightarrow |G : M| = \frac{|G|}{|M|} = \frac{|N|}{|\operatorname{Core}_G(M)|}.$$

Ad ogni cuore normale di un sottogruppo massimale di indice n è quindi associato un fattore principale non di Frattini A con $|A| = n$. Tale fattore è del tipo $N/\operatorname{Core}_G(M)$. Per quanto osservato all'inizio sappiamo che $G/\operatorname{Core}_G(M)$ è di due tipi, e quindi il fattore principale associato a $\operatorname{Core}_G(M)$ può essere di tre tipi: (1) lo zoccolo abeliano di un gruppo monolitico (e quindi $A \in \mathcal{A}_G(n)$); (2) lo zoccolo non abeliano di un gruppo monolitico (e quindi $A \in \mathcal{C}_G(n)$); (3) un sottogruppo minimale di L_2 (e quindi $A \in \mathcal{B}_G(n)$).

Inoltre grazie a $\delta_G(A)$ possiamo contare quanti fattori di ogni tipo ci sono. In particolare abbiamo che vi sono al più: $\frac{q_L^{\delta_G(A)}-1}{q_L-1}$ cuori normali associati a fattori del primo tipo; $\delta_G(A)$ cuori normali associati a fattori del secondo tipo; $\frac{\delta_G(A)(\delta_G(A)-1)}{2}$ cuori normali associati a fattori del terzo tipo.

Infine, dato $\mathrm{Core}_G(M)$, dal Teorema 2.2.7, ci sono al più n^b sottogruppi massimali con tale cuore normale. Abbiamo dunque in sintesi dimostrato la seguente proposizione.

Proposizione 3.2.21. *Se G è un gruppo finito, allora dato $n \in \mathbb{N},\ n \geq 2$, vale che*

$$m_n(G) \leq \left(\sum_{A \in \mathcal{A}_G(n)} \frac{q_{L_G(A)}^{\delta_G(A)} - 1}{q_{L_G(A)} - 1} + \sum_{B \in \mathcal{B}_G(n)} \frac{\delta_G(B)(\delta_G(B)-1)}{2} + \sum_{C \in \mathcal{C}_G(n)} \delta_G(C) \right) n^b.$$

Grazie alle proprietà di $\delta_G(A)$ è inoltre possibile dimostrare il seguente lemma.

Lemma 3.2.22. *Sia $A \in \mathcal{A}_G(n)$, allora vale*

$$\frac{q_{L_G(A)}^{\delta_G(A)} - 1}{q_{L_G(A)} - 1} \leq n^{d(G)}.$$

Abbiamo finalmente tutti gli strumenti per dimostrare il seguente teorema.

Teorema 3.2.23. *Dato $0 < \eta < 1$ esiste una costante positiva c_η tale che, per ogni gruppo finito G,*

$$\mathcal{V}_\eta(G) \leq d(G) + 2\log_2 \log_2 |G| + c_\eta.$$

Dimostrazione. Dal Lemma 3.2.22 e dalla definizione 3.2.20 segue subito che

$$\sum_{A \in \mathcal{A}_G(n)} \frac{q_{L_G(A)}^{\delta_G(A)} - 1}{q_{L_G(A)} - 1} \leq \alpha_G(n) n^{d(G)}.$$

Inoltre, siccome $\mathcal{B}_G(n) \cup \mathcal{C}_G(n) \subseteq \mathcal{D}_G(n)$ vale che

$$\begin{aligned} \sum_{B \in \mathcal{B}_G(n)} \frac{\delta_G(B)(\delta_G(B)-1)}{2} + \sum_{C \in \mathcal{C}_G(n)} \delta_G(C) &\leq \sum_{D \in \mathcal{D}_G(n)} \frac{\delta_G(D)(\delta_G(D)-1)}{2} + \delta_G(D) \\ &\leq \sum_{D \in \mathcal{D}_G(n)} \frac{\delta_G(D)(\delta_G(D)+1)}{2} \\ &\leq \sum_{D \in \mathcal{D}_G(n)} \delta_G(D)^2 \leq \gamma_G(n)^2. \end{aligned}$$

Dalla Proposizione 3.2.21 segue dunque che

$$\begin{aligned} m_n(G) &\leq \left(\alpha_G(n) n^{d(G)} + \gamma_G(n)^2 \right) n^b \\ &\leq \left(\alpha_G(n) n^{d(G)} + \gamma_G(n)^2 + \alpha_G(n)^2 + 2\alpha_G(n)\gamma_G(n) + \gamma_G(n) n^{d(G)} \right) n^b \\ &= \lambda_G(n) \left(\lambda_G(n) + n^{d(G)} \right) n^b. \end{aligned}$$

Passando ai logaritmi si ottiene che

$$\begin{aligned}\frac{\log m_n(G)}{\log n} \leq & \frac{\log[\lambda_G(n)\left(\lambda_G(n)+n^{d(G)}\right)n^b]}{\log n}\\ = & \frac{\log\lambda_G(n)+\log\left(\lambda_G(n)+n^{d(G)}\right)+\log n^b}{\log n}\\ \leq & b+\frac{\log\lambda_G(n)}{\log n}+\frac{\log 2\max\{\lambda_G(n),n^{d(G)}\}}{\log n}\\ = & b+\frac{\log\lambda_G(n)}{\log n}+\frac{\log 2}{\log n}+\max\left\{\frac{\log\lambda_G(n)}{\log n},d(G)\right\}\\ \leq & b+\frac{\log\lambda_G(n)+1}{\log n}+\max\left\{\frac{\log\lambda_G(n)}{\log n},d(G)\right\},\end{aligned}$$

da cui

$$\mathcal{M}(G)\leq b+\max_{n\geq 2}\left\{\frac{\log\lambda_G(n)+1}{\log n}+\max\left\{\frac{\log\lambda_G(n)}{\log n},d(G)\right\}\right\}.$$

Ricordando la definizione 3.2.20, abbiamo che $\lambda_G(n)$ è al più il numero di fattori principali non di Frattini di G, quindi $\lambda_G(n)\leq\log_2|G|$. Abbiamo dunque

$$\mathcal{M}(G)\leq b+\log_2\log_2|G|+\frac{1}{\log 2}+\log_2\log_2|G|+d(G).$$

Confrontando questo risultato con il Teorema 2.2.12, ricaviamo la stima di $\mathcal{V}_\eta(G)$ cercata. □

Capitolo 4

Stima attraverso i sottogruppi di Sylow

In quest'ultimo capitolo vogliamo vedere una versione probabilistica del teorema dimostrato in [7], il quale afferma che, per ogni gruppo finito G, vale $d(G) \leq \max_p d_p(G)+1$, con $d_p(G) = d(P)$ e P un p-sottogruppo di Sylow di G. In particolare vogliamo dimostrare che esiste una stima simile anche per $\mathcal{E}(G)$.

Definizione 4.0.1. Un gruppo finito G è detto p-nilpotente, con $p \in \mathbb{N}$ primo, se G contiene un sottogruppo normale K tale che p non divide $|K|$ e G/K è un p-gruppo. Tale K è detto un p-complemento normale di G.

Osservazione 4.0.2. Se un tale sottogruppo normale K esiste, allora è unico: è il sottogruppo che contiene tutti gli elementi di G di ordine coprimo con p. Infatti se in K ci sono elementi di ordine p si ha che $p\big||K|$ (assurdo per ipotesi) e se $\exists g \in G \setminus K$ tale che p non divide $|g|$ allora si ha che G/K non è un p-gruppo (assurdo per ipotesi). Inoltre possiamo osservare che se P è un p-sottogruppo di Sylow di G, allora $G = PK,\ K \cap P = \{1\}$ e $G/K \cong P$, quindi K è un complemento dei p-sottogruppi di Sylow.

É stato inoltre dimostrato (in [15]) il seguente teorema.

Teorema 4.0.3. *Sia P un p-sottogruppo di Sylow di un gruppo finito G e sia $N \trianglelefteq G$ un sottogruppo normale di G tale che $N \cap P \leq \mathrm{Frat}(P)$. Allora N è p-nilpotente.*

Vogliamo ora dimostrare la seguente proposizione.

Proposizione 4.0.4. *Siano N un sottogruppo normale minimale di un gruppo finito G e $p \in \mathbb{N}$ un primo. Se $p\big||N|$ e $N \not\leq \mathrm{Frat}(G)$, allora $d_p(G) > d_p(G/N)$.*

Per la dimostrazione abbiamo però bisogno di alcuni lemmi preliminari.

Lemma 4.0.5. *Sia G un gruppo finito e $N \trianglelefteq G$ un suo sottogruppo normale. Allora vale*

$$\mathrm{Frat}(G)N/N \leq \mathrm{Frat}(G/N).$$

Inoltre se $N \leq \mathrm{Frat}(G)$ *allora vale*

$$\mathrm{Frat}(G/N) = \mathrm{Frat}(G)/N.$$

Dimostrazione. Ad ogni elemento $xN \in \mathrm{Frat}(G)N/N$ è associato un $x \in \mathrm{Frat}(G)N$. Abbiamo dunque $x = fn$ con $f \in \mathrm{Frat}(G)$ e $n \in N$. In particolare abbiamo allora che $xN = fN$. Ci basta dunque dimostrare che $fN \in \mathrm{Frat}(G/N)$ per ogni $f \in \mathrm{Frat}(G)$. Sia quindi $f \in \mathrm{Frat}(G)$ e M/N un sottogruppo massimale di G/N qualsiasi. Allora per il Teorema di corrispondenza abbiamo che M è massimale in G, e dunque per definizione $f \in M$. Passando al quoziente abbiamo dunque che $fN \in M/N$ per ogni massimale M/N, e quindi $fN \in \mathrm{Frat}(G/N)$.

Per la seconda tesi basta osservare che se $N \leq \mathrm{Frat}(G)$, allora $N \leq M$ per ogni M sottogruppo massimale di G. Quindi i sottogruppi massimali di G/N sono del tipo M/N, con M massimale in G. Allora vale

$$\mathrm{Frat}(G/N) = \bigcap_{M \leq_{max} G} M/N = \left(\bigcap_{M \leq_{max} G} M \right) /N = \mathrm{Frat}(G)/N.$$

□

Lemma 4.0.6. *Sia* G *un* p*-gruppo finito, allora* $\mathrm{Frat}(G) = G'G^p$ *con* $G^p = \langle g^p | g \in G \rangle$.

Dimostrazione. Dalla dimostrazione del Lemma 3.1.9 sappiamo che G' e G^p sono contenuti in $\mathrm{Frat}(G)$ e dunque abbiamo che anche il loro prodotto lo è. Abbiamo quindi che $N = G'G^p \leq \mathrm{Frat}(G)$.

Osserviamo inoltre che N è il prodotto di due sottogruppi caratteristici (perché dato $a \in \mathrm{Aut}(G)$, $[g,h]^a = [g^a, h^a]$ e $(g^p)^a = (g^a)^p$) e dunque è esso stesso caratteristico e in particolare è normale: è quindi ben definito il quoziente G/N. Osserviamo inoltre che esso è abeliano, in quanto $G' \leq N$, e elementare, in quanto $G^p \leq N$ e dunque $(gN)^p = g^p N = N$. Abbiamo dunque che $G/N \cong \mathbb{F}_p^d$, e quindi è un $\mathbb{F}_p$ spazio vettoriale. Come osservato nella dimostrazione della Proposizione 3.1.10, abbiamo che i sottogruppi massimali di G/N sono gli iperpiani di $\mathbb{F}_p^d$, i quali si intersecano solo nel vettore nullo: vale quindi $\mathrm{Frat}(G/N) = \{1\}$. Dal Lemma 4.0.5 abbiamo quindi che $\mathrm{Frat}(G)/N = \mathrm{Frat}(G/N) = \{1\}$, da cui la tesi. □

Lemma 4.0.7. *Sia* $G = A \times B$ *un* p*-gruppo finito. Allora* $d(G) = d(A) + d(B)$.

Dimostrazione. Dimostriamo innanzitutto che $\mathrm{Frat}(A) \times \mathrm{Frat}(B) = \mathrm{Frat}(G)$. Dal lemma precedente abbiamo che $\mathrm{Frat}(G) = G'G^p$, e siccome anche A e B, in quanto sottogruppi di G, sono p-gruppi allora vale anche $\mathrm{Frat}(A) = A'A^p$ e $\mathrm{Frat}(B) = B'B^p$. Mettendo tutto insieme, per le proprietà del prodotto diretto otteniamo che

$$\mathrm{Frat}(G) = (A \times B)'(A \times B)^p = A'A^p \times B'B^p = \mathrm{Frat}(A) \times \mathrm{Frat}(B).$$

Ora dalla dimostrazione della Proposizione 3.1.10 sappiamo che $G/\mathrm{Frat}(G) \cong (\mathbb{F}_p)^d$ con $d = d(G/\mathrm{Frat}(G)) = d(G)$ per l'Osservazione 3.1.8. Abbiamo dunque che

$d(G) = \dim_{\mathbb{F}_p}(G/\operatorname{Frat}(G))$. Siccome G è un p-gruppo allora anche A, B lo sono. In particolare abbiamo dunque che $A/\operatorname{Frat}(A)$ e $B/\operatorname{Frat}(B)$ sono spazi vettoriali come sopra e dunque, ricordando che la dimensione del prodotto diretto di due spazi vettoriali è la somma delle due dimensioni, abbiamo

$$\begin{aligned} d(G) &= \dim_{\mathbb{F}_p}(G/\operatorname{Frat}(G)) = \dim_{\mathbb{F}_p}((A \times B)/(\operatorname{Frat}(A) \times \operatorname{Frat}(B)) \\ &= \dim_{\mathbb{F}_p}(A/\operatorname{Frat}(A)) + \dim_{\mathbb{F}_p}(B/\operatorname{Frat}(B)) = d(A) + d(B). \end{aligned}$$

□

Lemma 4.0.8. *Sia G un p-gruppo finito, con $p \in \mathbb{N}$ primo. Supponiamo che*

$$G = (N_1 \times \cdots \times N_u) \rtimes H,$$

con $\{1\} \neq N_i \trianglelefteq G$ per $1 \leq i \leq u$. Allora $d(X) \geq u + d(H)$

Dimostrazione. Dimostriamolo per induzione sull'ordine di G. Osserviamo innanzitutto che se $|N_i| = p \ \forall i$ abbiamo che ogni $N_i \cong C_p$ e dunque è abeliano. Inoltre ogni N_i è normale per ipotesi e quindi il coniugio manda elementi di N_i in altri elementi di N_i. Quindi sui singoli N_i abbiamo che H agisce per coniugio come un sottogruppo di $\operatorname{Aut}(C_p)$. Siccome però $|\operatorname{Aut}(C_p)| = \varphi(p) = p - 1$ e H è un p-gruppo abbiamo che l'azione di H su ogni N_i è l'identità e dunque abbiamo che $G = C_p^u \times H$, da cui, per il Lemma 4.0.7, ricaviamo la tesi. Quindi possiamo ora assumere che, a meno di riordino degli indici, $|N_1| > p$. In questo caso allora N_1 contiene un sottogruppo M di ordine p e che è contenuto in $Z(G)$ e dunque è normale. Allora abbiamo per induzione che

$$d(X) \geq d(X/M) \geq u + d(H),$$

dove la prima disuguaglianza viene dall'Osservazione 3.0.2. □

Possiamo ora dimostrare la Proposizione 4.0.4

Dimostrazione. Sia P un p-sottogruppo di Sylow di G. Ci sono ora due casi:

1. N è abeliano: allora ammette un complemento H in G. Infatti siccome $N \not\leq \operatorname{Frat}(G)$ allora esiste H sottogruppo massimale tale che $N \not\leq H$. Tale H ha le proprietà che $G = NH$ e $N \cap H = \{1\}$. La prima deriva dalla massimalità di H e dal fatto che $N \not\leq \operatorname{Frat}(G)$. Invece $N \cap H = \{1\}$ viene dal fatto che N è abeliano. Infatti grazie a ciò sappiamo che $N \cap H \trianglelefteq N$ e questo unito al fatto che $N \cap H \trianglelefteq H$ (perché dato $h \in H$ vale: $h^{-1}(N \cap H)h = h^{-1}Nh \cap h^{-1}Hh = N \cap H$) ci permette di concludere che $N \cap H \trianglelefteq G$, in quanto $G = NH$. Infine, per la minimalità di N allora o $N \cap H = \{1\}$ oppure $N \cap H = N$, il che è assurdo in quanto $N \not\leq \operatorname{Frat}(G)$. Abbiamo dunque $G \cong N \rtimes H$, da cui $P \cong N \rtimes Y$ con Y un p-sottogruppo di Sylow di H. Allora dal Lemma 4.0.8 si ha

$$d_p(G) = d(P) \geq 1 + d(Y) = 1 + d_p(G/N),$$

da cui la tesi.

2. N non è abeliano: allora è isomorfo a un prodotto diretto di gruppi semplici non abeliani e siccome $p\big||N|$, allora N non può essere p-nilpotente. Quindi dal Teorema 4.0.3 segue che $N \cap P \not\leq \operatorname{Frat}(P)$ e quindi, applicando il Lemma 4.0.5

$$\left|\operatorname{Frat}\left(\frac{P}{P\cap N}\right)\right| \geq \left|\frac{(P\cap N)\operatorname{Frat}(P)}{P\cap N}\right| = \left|\frac{\operatorname{Frat}(P)}{\operatorname{Frat}(P)\cap N}\right| > \left|\frac{\operatorname{Frat}(P)}{P\cap N}\right|.$$

Dalla dimostrazione della Proposizione 3.1.10 sappiamo che per ogni p-gruppo Q vale che $Q/\operatorname{Frat}(Q)$ è uno spazio vettoriale sul campo finito $\mathbb{F}_p$ di dimensione $d(Q)$. Da $\frac{PN}{N} \cong \frac{P}{P\cap N}$, si ha che anche PN/N è un p-gruppo ed è un p-Sylow di G/N. Questo implica che

$$p^{d_p(G/N)} = \frac{|PN/N|}{|\operatorname{Frat}(PN/N)|} = \frac{|P/(P\cap N)|}{|\operatorname{Frat}(P/(P\cap N)|} < \frac{|P|}{|\operatorname{Frat}(P)|} = p^{d_p(G)},$$

da cui $d_p(G/N) < d_p(G)$. □

La Proposizione 4.0.4 ci dice che, fattorizzando G per un sottogruppo normale minimale N, con $p\big||N|$ e $N \not\leq \operatorname{Frat}(G)$, allora possiamo scendere almeno di 1 in d_p. Dal Teorema 3.2.19 sappiamo che $\delta_G(A)$ conta quante volte compare il fattore principale (quindi minimale) non di Frattini A. Ora gli elementi di $\mathcal{N}_G(p)$ sono proprio i fattori minimali che fanno diminuire d_p. Dunque ogni volta che quozientiamo per $A \in \mathcal{N}_G(p)$, che deve essere contato con molteplicità $\delta_G(A)$, abbiamo che $d_p(G/A) \leq d_p(G) - 1$. In sintesi abbiamo dunque dimostrato il seguente corollario.

Corollario 4.0.9.

$$\sum_{A\in\mathcal{N}_G(p)} \delta_G(A) \leq d_p(G).$$

Abbiamo ora tutti gli strumenti per enunciare e dimostrare la stima di $\mathcal{E}(G)$ cercata.

Teorema 4.0.10. *Esiste una costante c tale che*

$$\mathcal{E}(G) \leq \max_p d_p(G) + c$$

per ogni gruppo finito G.

Dimostrazione. Ripercorrendo le considerazioni che ci hanno portati alla Proposizione 3.2.21 cerchiamo di calcolare, per ogni $n \in \mathbb{N}$, $m_n(G)$. Supponiamo innanzitutto che n non sia del tipo q^a con $q \in \mathbb{N}$ un primo. Sia p un fattore primo di n. In questo caso sappiamo che se M è un sottogruppo massimale di G di indice n allora $\operatorname{soc}(G/\operatorname{Core}_G(M)) \cong A^\varepsilon$ con $\varepsilon \in \{1,2\}$ e $A \in \mathcal{D}_G(n)$ perché lo zoccolo non è abeliano. In particolare $n\big||A|$ e dunque $A \in \mathcal{N}_G(p)$. Guardando alla dimostrazione del Teorema 3.2.23 e sfruttando il Corollario 4.0.9 ricaviamo che

$$\begin{aligned} m_n(G) &\leq n^b \sum_{A\in\mathcal{D}_G(n)} \delta_G(A)^2 \leq n^b \sum_{A\in\mathcal{N}_G(p)} \delta_G(A)^2 \\ &\leq n^b \left(\sum_{A\in\mathcal{D}_G(n)} \delta_G(A)\right)^2 \leq n^b d_p(G)^2. \end{aligned}$$

Siccome n non è una potenza di un primo, allora $n \geq 6$ e dunque

$$\frac{\log m_n(G)}{\log n} \leq \frac{\log(n^b d_p(G)^2)}{\log n} \leq b + \frac{2\log d_p(G)}{\log 6} \leq b + d_p(G).$$

Ora assumiamo che $n = p^a$ con p un primo. Se M è un sottogruppo massimale di G di indice n, allora $\mathrm{soc}(G/\mathrm{Core}_G(M)) = A$ con $A \in \mathcal{A}_G(n) \cup \mathcal{C}_G(n)$ e dunque, sfruttando anche il Lemma 3.2.22, possiamo ricavare che

$$\begin{aligned} m_n(G) &\leq n^b \left(\sum_{A \in \mathcal{A}_G(n)} \frac{q_{L_G(A)}^{\delta_G(A)} - 1}{q_{L_G(A)} - 1} + \sum_{C \in \mathcal{C}_G(n)} \delta_G(C) \right) \\ &\leq n^b \left(\sum_{A \in \mathcal{A}_G(n)} n^{\delta_G(A)} + \sum_{C \in \mathcal{C}_G(n)} \delta_G(C) \right) \\ &\leq n^b \left(\sum_{A \in \mathcal{A}_G(n)} n^{\delta_G(A)} + \sum_{C \in \mathcal{C}_G(n)} n^{\delta_G(C)} \right) \\ &\leq n^b \sum_{A \in \mathcal{N}_G(p)} n^{\delta_G(A)} \leq n^b n^{\sum n^{\delta_G(A)}}, \end{aligned}$$

dove la seconda disuguaglianza deriva dal fatto che $q_{L_G(A)} \leq n$ per $A \in \mathcal{A}_G(n)$ con n potenza di primo. Possiamo dunque calcolare

$$\frac{\log m_n(G)}{\log n} \leq b + \sum_{A \in \mathcal{N}_G(p)} \delta_G(A) \leq b + d_p(G).$$

Mettendo tutto insieme ricaviamo che

$$\mathcal{M}(G) = \max_{n \geq 2} \frac{\log m_n(G)}{\log n} \leq \max_p d_p(G) + b.$$

Confrontando questo risultato con il Teorema 2.2.13 si ottiene la tesi. □

Bibliografia

[1] K. S. Brown. *The Coset Poset and Probabilistic Zeta Function of a Finite Group*. Vol. 225. 2. Journal of Algebra, 2000, pp. 989–1012.

[2] F. Dalla Volta A. Lucchini. *Finite groups that need more generators than any proper quotient*. Vol. 64. Journal of the Australian Mathematical Society, 1998, pp. 82–91.

[3] E. Detomi F. Morini A. Lucchini. *How many elemnts are needed to generate a finite group with good probability?* Israel Journal of Mathematics, pp. 29-44., 2002.

[4] B. Huppert C. A. Schroeder. *Finite Groups I*. 1st ed. 2025. Grundlehren der mathematischen Wissenschaften, A Series of Comprehensive Studies in Mathematics, 364. Springer Nature Switzerland, 2025.

[5] W. M. Kantor A. Lubotzky. *The probability of generating a finite classical group*. Vol. 36. Geometriae Dedicata, 1990, pp. 67–87.

[6] A. Lubotzky. *The expected number of random elements to generate a finite group*. Vol. 257. 2. Journal of Algebra, 2002, pp. 452–459.

[7] A. Lucchini. *A bound on the number of generators of a finite group*. Vol. 53(4). Arch. Math.(Basel), 1989, pp. 313–317.

[8] A. Lucchini. *The expected number of random elements to generate a finite group*. Vol. 181. Monatshefte für Mathematik, 2015.

[9] A. Lucchini. *Prefrattini subgroups and crowns*. Vol. 121. Arch. Math., 2023, pp. 469–483.

[10] A. Mann. *Positively finitely generated groups*. Vol. 8. 4. Forum mathematicum, 1996, pp. 429–460.

[11] I. Pak. *On Probability Of Generating A Finite Group*. Preprint, 1999. URL: `https://www.math.ucla.edu/~pak/papers/sim.pdf`.

[12] P.P Pálfy. *A polynomial bound for the orders of primitive solvable groups*. Vol. 77. Journal of Algebra, 1982, pp. 127–137.

[13] C. Pomerance M. Hill. *The expected number of random elements to generate a finite abelian group*. Vol. 43. Periodica Mathematica Hungarica, 2001, pp. 191–198.

[14] D. J. S. Robinson. *A course in the theory of groups*. Vol. 80 of Graduate Texts in Mathematics. Springer-Verlag, 1996.

[15] J. Tate. *Nilpotent quotient groups*. Vol. 3. Topology, 1964, pp. 109–111.

[16] T. R. Wolf. *Solvable and nilpotent subgroups of* $GL(n, q^m)$. Vol. 34. 5. Can. J. Math., 1982.