UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

L'enumerazione dei gruppi finiti.

Relatore: Prof. Andrea Lucchini
Laureando: Elena Tomasella
Matricola: 2002964

Anno Accademico 2022/2023

21 luglio 2023

Indice

Capitolo 1

Introduzione

In questa parte di mondo c'è qualcosa che nella vita facciamo continuamente: scegliere. Non tutte le scelte hanno lo stesso peso, non tutte le scelte sono naturali. Io sono solita fare un'analisi attenta di vantaggi e svantaggi, per educare un'emotività cosciente che trova sempre modo di farmi capire quale direzione prendere, dove rivolgere lo sguardo. Quando ho dovuto scegliere su cosa scrivere la mia tesi triennale, si trattava di capire a cosa volessi dedicare il mio tempo. L'ultima lezione del corso di Algebra 2 è stata un colloquio coi miei sentimenti. Avrei voluto ricominciare il corso il giorno dopo. I primi mesi di teoria dei gruppi sono stati una faticaccia, non riuscivo a vedere. I matematici o futuri matematici sorrideranno nel leggere "vedere", perché è uno dei verbi più sfruttati dai professori nelle loro locuzioni poi citate dagli studenti. In soldoni: studiare studiare studiare senza riuscire a cogliere l'insieme, lo schema, il senso. Con una pazienza che non mi appartiene al di fuori della carriera scolastica ho continuato a studiare affidandomi alla speranza che tempo e dedizione avrebbero portato a qualcosa. In effetti ad un qualche punto qualcosa è successo - l'amore succede. In teoria dei gruppi ho trovato delle idee che mi hanno ispirata e realizzata. La materia mi ha restituito quello che cercavo nel percorso di Laurea Triennale: conoscenze trasversali. Così, al momento di scegliere l'argomento della tesi, ho fatto un po' di colloqui, ma poi il sorriso giusto è affiorato nell'ufficio del prof. Lucchini, e non ci sono stati più dubbi. Mi sono sentita nel posto giusto e questo non è da razionalizzare: è una sensazione di epifania. A proposito del mio relatore Andrea Lucchini: vorrei ringraziarlo subito per l'estrema disponibilità, per la pratica celerità, per l'attenta comprensione. Mi sono sentita seguita: questo gli fa grande onore. Nonostante la sua posizione e la sua profondità scientifica mi ha fatto percepire d'avere uno spazio prioritario nell'organizzazione dei suoi impegni ordinari. Qui si conclude la storia di questa tesi, che ora mi accingo a introdurre sotto un punto di vista tecnico.

Questo lavoro di tesi triennale riguarda l'enumerazione dei gruppi finiti, ovvero la questione di valutare quanti siano i gruppi finiti di ordine n fissato. È divisa in due parti: nella prima troverete in modo dettagliato il caso in cui n sia potenza di un numero primo p, nella seconda un'idea della dimostrazione di Pyber (con annesso panorama di prerequisiti) che racconta cosa succede per un generico n naturale.

Per la lettura sono richieste delle nozioni di teoria dei gruppi che si studiano nel corso triennale di Algebra 2. Altri oggetti che discendono dal programma del corso saranno introdotti mano a mano, dove ci sarà necessità. Il mio intento è quello di fornire gli

strumenti tecnici per riuscire a seguire le dimostrazioni e per comprendere la profondità dei risultati.

Vi lascio alla lettura con un'ultima postilla. Questa tesi è la conclusione di un percorso di Laurea Triennale in Matematica durante il quale ho scritto moltissimo: appunti delle lezioni, quaderni di esercizi, taccuini personali. Scrivere è per me istintivo e necessario. È una forma di espressione che spesso dichiaro ma non molto spesso condivido, perché, come tutte le forme di espressione, la sua trasparenza comporta una delicata vulnerabilità. In questa occasione avrei potuto scegliere un tono meno creativo, ma sarebbe stato sterile: non ho voluto forzare un processo di scrittura che non mi appartiene. Da un lato temevo fosse fuori luogo scegliere un tipo di narrazione più personale, ma dall'altro non volevo fosse altrimenti. Vorrei la scrittura nella mia vita come gli effetti di luce nei quadri di Vermeer. È un sogno, e i sogni hanno bisogno di spazio. La verità è che non vedevo l'ora di scrivere questa tesi.

Capitolo 2

Storia

Per la mia personale esperienza scolastica, credo che i programmi didattici italiani siano fortemente impregnati di storia: si tende a preferire un susseguirsi cronologico nella presentazione dei contenuti. Ho sempre apprezzato questo approccio sia perché penso che completare con un quadro storico gli argomenti tecnici sia uno stimolo per l'educazione di uno spirito critico, sia perché credo che la graduale comprensione storica possa essere da guida per la graduale comprensione da parte degli studenti. In questo lavoro di tesi seguirò effettivamente lo sviluppo cronologico dei risultati, che si sono migliorati e complicati tecnicamente nel tempo. Inoltre, dato che tratterò di ricerche riconducibili principalmente a tre matematici, riporterò per sommi capi le loro biografie.

Concentriamoci sulla semplicità della formulazione della domanda: quanti gruppi di ordine n esistono? Originale: "How many groups of order n are there?". Questo è proprio il titolo di alcune Lectures a più voci tenute ad Oxford negli anni '90. I protagonisti furono Graham Higman, Simon R. Blackburn e Peter M. Neumann. Se volessimo essere davvero curiosi sull'origine della questione, dovremmo considerare che per certi casi speciali o per gruppi di ordine piccolo delle stime e dei calcoli erano già stati fatti prima di avere il risultato di Graham Higman. Si era notato che all'aumento della cardinalità fissata si ottiene un aumento considerevole del numero di gruppi di tale cardinalità. L'obiettivo dalla ricerca si è allora spostato dal calcolo esplicito alla miglior stima possibile. L'americano Charles Sims ebbe l'idea di implementare il procedimento dimostrativo utilizzato da Graham Higman sui p-gruppi per fornire effettivamente un risultato ottimale. In tempi recenti l'ungherese Pyber si è occupato del caso di generica cardinalità n naturale, andando dunque ad ampliare l'ambiente algebrico di lavoro.

2.1 Graham Higman

Matematico inglese, Graham Higman passò l'infanzia a Plymouth prima di vincere una borsa di studio al Balliol College di Oxford, dove già suo fratello era studente. Scelse la matematica per differenziarsi da questo fratello maggiore, che si dedicava invece alla chimica. All'epoca la scelta dei corsi di matematica era spesso complementare ad altri interessi prioritari, ma questo non era il caso di Graham Higman, come intuì il suo tutor Henry Whitehead. Fondò uno società di matematici non ancora laureati lì ad Oxford, e in questo modo Graham coltivò la sua conoscenza riguardo la teoria dei gruppi. Si laureò e dottorò ad Oxford, per poi proseguire con un anno a Cambridge dove conobbe Philip Hall e Max Newman, contatti di fondamentale importanza. Durante la Seconda Guerra Mondiale lavorò in un Ufficio Metereologico, nel quale fece richiesta, al termine del conflitto, per un posto indeterminato. In quel periodo, durante un'intervista gli chiesero perché non avesse accettato un posto accademico. A quel punto lui rifiutò l'offerta di lavoro all'Ufficio Metereologico per aspirare ad una carriera accademica. La prima proposta arrivò dall'Università di Durham: la declinò perché voleva collaborare con Newman a Manchester. Nel 1946 l'offerta giunse anche da Manchester, e stavolta la accettò. Ottenne in seguito anche una cattedra e fu nominato membro della Royal Society di Londra, oltre che membro Senior al suo vecchio college. Per i floridi anni di carriera che seguirono, vinse il Berwick Prize dalla London Mathematical Society nel '62, la medaglia De Morgan nel '74, e la medaglia Sylvester nel '79.

2.2 Charles Sims

Charles Sims è stato un matematico americano, nato in Indiana nel 1937 e recentemente morto in Florida nel 2017. Gli piaceva essere chiamato Charlie. I primi anni della sua istruzione scolastica li passò in Indiana, ma dopo essersi diplomato si trasferì in Michigan per frequentare l'università. Dopo la laurea cominciò a fare ricerca ad Harvard, e fu proprio questo il periodo in cui prese a cuore lo studio dell'enumerazione dei gruppi finiti. In un articolo basato sulla sua tesi venne citato non tanto il risultato conclusivo ottenuto, quanto il fatto che la dimostazione per la limitazione dall'alto fosse basata su una serie di proposizioni molto interessanti. Finito il dottorato, durante il quale conobbe anche Annette, diventata poi sua moglie, passò qualche anno lavorando al "Massachusetts Institute of Technology". Si spostò poi alla Rutgers University in New Jersey. Sims dedicò le sue ricerche alla teoria di gruppi e fu protagonista di floride collaborazioni, tra cui per esempio quella con Higman. Scrisse diversi articoli riguardo alla rivoluzione che la didattica stava subendo in quegli anni per la diffusione del Word Wide Web. Nel 2012 fu scelto per la "Inaugural Class of Fellows" della American Mathematical Society, con la seguente motivazione: "[...] since he was one of the most influential figures in computational group theory, but was much more besides".

2.3 Lázló Pyber

Lázló Pyber è un matematico ungherese, nato nel 1960 e attualmente ricercatore presso il centro "Alfréd Renyi Institute of Mathematics" di Budapest. È famoso per aver risolto svariate congetture di teoria dei grafi, come per esempio la congettura di Erdös-Gallai "i rami di qualsiasi grafo semplice di n vertici possono essere ricoperti con al più $n-1$ cicli e archi" e la congettura di Erdös "un grafo con n vertici e il suo complementare possono essere ricoperti con $n^2/4+2$ cricche (cliques)". Si è occupato anche dell'enumerazione dei gruppi finiti, per il caso di cardinalità n generica. Nel 2007 ha vinto il premio "Academic Prize of the Hungarian Academic of Sciences", e nel 2017 è stato insignito di un ERC Advanced Grant.

Parte I

Gruppi di ordine p^n

Capitolo 3

Nozioni preliminari

Vedremo alcune definizioni e alcuni teoremi, più o meno sofisticati, che ci serviranno per gli argomenti che affronteremo. Il nostro ambiente di lavoro sarà sempre quello dei gruppi finiti.

3.1 Gruppi

Definizione 3.1.1. *Siano G un gruppo, X un insieme non vuoto, e $\sigma : X \to F$ una funzione. F (più propriamente (F, σ)) è un gruppo libero su X se e solo se ad ogni funzione α dall'insieme X al gruppo G corrisponde un unico omomorfismo $\beta : F \to G$ tale che $\alpha = \sigma\beta$. Un gruppo che risulta essere libero per qualche insieme non vuoto X si chiama gruppo libero.*

Da questa definizione segue sia che la funzione σ è necessariamente inettiva, sia che G è generato dall'immagine di σ.

Proposizione 3.1.2. *Se un gruppo F_r contiene un sottoinsieme S per cui ogni elemento x di F_r si scrive in modo unico nella forma $x = x_1^{l_1} \dots x_r^{l_r}$ con $x_i \in S$ e $x_i \neq x_{i+1}$ per tutti gli i, r intero positivo e $l_i \neq 0$ per ogni i, allora il gruppo F_r è libero su S.*

Proposizione 3.1.3. *Sia G un gruppo generato da un suo sottoinsieme X, e sia F un gruppo libero su Y. Se la mappa $\alpha : Y \to X$ è suriettiva, si può estendere ad un epimorfismo da F in G. In particolare ogni gruppo è immagine di un gruppo libero.*

Dato un gruppo finito G, generabile con d elementi, esiste allora un omomorfismo suriettivo $\alpha : F \to G$, essendo F il gruppo libero sull'insieme $Y = \{y_1, \dots, y_d\}$. Il nucleo $\ker \alpha$ è un sottogruppo di F finitamente generato; in particolare si può descrivere $\ker \alpha$ assegnando un insieme finito R di elementi di F (che quindi si possono scrivere come parole nei generatori $y_1, \dots, y_d$), tale che $\ker \alpha$ sia il più piccolo sottogruppo normale di G contentente R. La conoscenza di Y e di R è quindi sufficiente per descrivere il gruppo G: la coppia (Y, R) determina quella che viene chiamata una *presentazione* di G. Si usa per tale presentazione la notazione $G = \langle Y | R \rangle$.

3.2 Commutatori

Curiosità generale prima delle definizioni tecniche: i commutatori sono uno strumento fondamentale quando si lavora computazionalmente coi p-gruppi.

Definizione 3.2.1. *Dato un gruppo G, e considerati due suoi elementi $x, y \in G$, indichiamo con $[x, y]$ il commutatore di x e y, dove*

$$[x, y] = x^{-1}y^{-1}xy.$$

Inoltre definiamo anche $[x, y, z] = [[x, y], z]$, per $x, y, z \in G$. Con la notazione x^y si intende il prodotto $y^{-1}xy$.

Faccio notare che il commutatore di due elementi x, y ci indica quanto xy sia diverso da yx, infatti $[x, y] = 1$ se e solo se i due elementi commutano tra loro. Equivalentemente possiamo pensare che il commutatore ci dica qual è la differenza tra x e il suo coniugato sotto y.

Lemma 3.2.2. *Per ogni $x, y, z \in G$*

$$\begin{aligned}
&[x, y] = [y, x]^{-1},\\
&[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z],\\
&[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z],\\
&[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y] = 1.
\end{aligned}$$

Le uguaglianze del lemma 3.2.2 si ottengono applicando la definizione di commutatore. Sostituendo opportunamente gli elementi nelle espressioni del lemma 3.2.2 segue il risultato del corollario che ora enuncio.

Corollario 3.2.3. *Per ogni $x, y, z \in G$ abbiamo che*

$$\begin{aligned}
[x^{-1}, y] &= ([x, y]^{-1})^{x^{-1}} = [x, y, x^{-1}]^{-1}[x, y]^{-1},\\
[x, y^{-1}] &= ([x, y]^{-1})^{y^{-1}} = [x, y, y^{-1}]^{-1}[x, y]^{-1}.
\end{aligned}$$

Lemma 3.2.4. *Supponiamo che sia x che y commutino con $[x, y]$, dove x e y sono due elementi del gruppo G. Allora per ogni n naturale si ha che*

$$\begin{aligned}
[y, x^n] = [y^n, x] &= [y, x]^n,\\
(xy)^n &= x^n y^n [y, x]^{\frac{1}{2}n(n-1)}.
\end{aligned}$$

Dimostrazione. La prima delle due equazioni si dimostra per induzione su n, usando il lemma 3.2.2 per il passo induttivo. La seconda equazione si dimostra sfruttando $y^i x = xy^i[y^i, x]$. □

Ora anziché lavorare con elementi di G, considero i suoi sottogruppi. È opportuno allora dare le definizioni di commutatore tra sottogruppi e di sottogruppo derivato.

Definizione 3.2.5. *Siano H e K sottogruppi di G. Allora diciamo che il loro commutatore è*

$$[H, K] = \langle \{[h, k] : h \in H, k \in K\} \rangle,$$

ovvero il sottogruppo generato dall'insieme di tutti i commutatori di elementi rispettivamente del primo e del secondo sottogruppo.

Vorrei stressare il fatto che il commutatore sia il sottogruppo generato dall'insieme dei commutatori: preso l'insieme dei commutatori questo non necessariamente ha struttura di gruppo. In particolare se prendiamo $[G, G]$ questo può contenere non commutatori.

Definizione 3.2.6. *Dato un gruppo G diciamo che il suo derivato, indicato convenzionalmente con G', è $G' = [G, G]$.*

Il derivato di un gruppo è triviale (cioè coincide con l'unità del gruppo) solamente nel caso in cui sia un gruppo abeliano.

Lemma 3.2.7. *Siano K, L, M tre sottogruppi di G. Allora*

$$[K, L, M] \leq [M, K, L][L, M, K]$$

quando $[M, K, L]$ e $[L, M, K]$ sono sottogruppi normali di G.

La definizione di serie centrale può essere data anche senza usare la nozione di commutatore, ma ci sarà utile esprimerla anche in questi termini.

Definizione 3.2.8. *Una catena di sottogruppi di G*

$$\{1\} = H_0 \subseteq H_1 \subseteq H_2 \cdots \subseteq H_r = G$$

si dice una serie centrale per G se $H_i \triangleleft G$ e $H_i/H_{i-1} \subseteq Z(G/H_{i-1})$ per ogni $i \in \{1, \ldots, r\}$, dove $Z(G/H_{i-1})$ è il centro di G/H_{i-1}.

L'ultima condizione della definizione si può sostituire, usando il linguaggio dei commutatori, chiedendo che $[H_i, G] \subseteq H_{i-1}$. Per lunghezza della serie intendiamo il numero di contenimenti, ovvero quante volte dobbiamo usare il simbolo $\subseteq$ per scrivere la serie.

Definizione 3.2.9. *La serie centrale discendente $G_1, G_2, G_3, \ldots$ di un gruppo G è definita ricorsivamente, ponendo $G_1 = G$ e $G_{i+1} = [G_i, G]$ per ogni i intero positivo.*

Facciamo notare che il termine *centrale* trova senso se si osserva che G_i/G_{i+1} è centrale in G/G_{i+1}.

3.3 Nilpotenza

Nel corso di Teoria di Galois ho conosciuto i gruppi risolubili come possibile generalizzazione dei gruppi abeliani. In quel frangente la necessità di lavorare con gruppi risolubili era legata al secondo teorema fondamentale di Galois, in cui viene enunciata la relazione tra equazioni risolubili per radicali e risolubilià del gruppo di Galois associato all'equazione. Qui invece l'attenzione si deve focalizzare sui gruppi nilpotenti (che sono particolari gruppi risolubili): sono effettivamente la più naturale generalizzazione dei gruppi abeliali.

Definizione 3.3.1. *Diciamo che un gruppo è nilpotente quando $G_r = \{1\}$ per qualche intero r. Il più piccolo intero positivo r per cui $G_{r+1} = \{1\}$ è la classe di nilpotenza di G.*

In termini più discorsivi traduciamo la definizione proposta dal [8] : un gruppo si dice nilpotente se possiede una serie centrale, e la sua classe di nilpotenza è la lunghezza della sua più corta serie centrale. Ricordiamo il seguente risultato: un gruppo finito è nilpotente se e solo se è prodotto diretto dei suoi sottogruppi di Sylow; in particolare tutti i p-gruppi sono nilpotenti. Quando scriverò che un p-gruppo ha $\Phi-$classe 2, sarà da intendere che nella più corta serie centrale del gruppo ci sono solo due gradini.

Proposizione 3.3.2. *Siano i un intero positivo, G il gruppo generato dall'insieme S, T un sottogruppo di G_i la cui immagine in G_i/G_{i+1} genera G_i/G_{i+1}. Con queste condizioni si ha che*

$$G_{i+1}/G_{i+2} = \langle [t,s]G_{i+2} : t \in T, s \in S \rangle.$$

Proposizione 3.3.3. *Preso G un gruppo nilpotente, e detto $H < G$, abbiamo che se $H_2G_3 = G_2$ allora $H_i = G_i$ per ogni $i \geq 2$.*

3.4 Il gruppo di Frattini

Definizione 3.4.1. *Il gruppo di Frattini di un gruppo G si indica con $\Phi(G)$ ed è l'intersezione di tutti i sottogruppi massimali del gruppo G. Nel caso sfortunato in cui G non abbia sottogruppi massimali (e tali gruppi esistono, si veda ad esempio il gruppo di Prüfer), per convenzione si prende $\Phi(G) = G$.*

Lemma 3.4.2. *Preso un sottoinsieme X del gruppo G, vale la seguente:*

$$\langle X, \Phi(G) \rangle = G \text{ se e solo se } \langle X \rangle = G.$$

Il lemma appena enunciato può essere interpretato così: il gruppo di Frattini di G è l'insieme degli elementi non generatori del gruppo. Ricordiamo che il nostro studio per i risultati che verranno si restringe in un primo momento ai gruppi di cardinalità una potenza di p primo. Vediamo un lemma che ci indica come mettersi in questo caso sia fonte di grande semplificazione per lo studio del gruppo di Frattini.

Corollario 3.4.3. *Se G è un p-gruppo finito allora ogni suo sottogruppo massimale M è normale e $[G : M] = p$.*

Lemma 3.4.4. *Sia G un gruppo finito di ordine potenza di primo p. Il gruppo $G/\Phi(G)$ è allora un gruppo abeliano elementare di ordine p^d, dove d è il minimo numero di generatori di G. Inoltre, $\Phi(G) = G^pG'$, con G^p il sottogruppo di G generato dall'insieme $\{x^p : x \in G\}$.*

3.5 Algebra lineare

Questa sezione sarà utile per la comprensione del capitolo 6. Rimando anzitutto alla definizione di spazio vettoriale: è bene averla sempre chiara per proseguire la lettura di questo paragrafo. Utilizzerò la notazione q per intendere un numero primo, e $\mathbb{F}_q$ per per il campo finito di q elementi.

Proposizione 3.5.1. *Sia V spazio vettoriale su $\mathbb{F}_q$. Ci sono allora*

$$(q^d - 1)(q^d - q) \dots (q^d - q^{k-1})$$

scelte di k vettori linearmente indipendenti di V.

Questa proposizione ci permette di calcolare il numero $n_{d,k}$ di sottospazi di dimensione k di uno spazio vettoriale di dimensione d:

$$n_{d,k} = \frac{(q^d - 1)(q^d - q) \dots (q^d - q^{d-1})}{(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})}.$$

Corollario 3.5.2. *Sia p un numero primo e sia P un gruppo abeliano elementare di ordine p^d. Allora P ha esattamente $n_{d,k}$ sottogruppi di ordine p^k, dove*

$$n_{d,k} = \frac{(p^d - 1)(p^d - p) \dots (p^d - p^{k-1})}{(p^k - 1)(p^k - p) \dots (p^k - p^{k-1})}.$$

Definizione 3.5.3. *Dati V e W due spazi vettoriali su un campo F diciamo che $\Phi : V \times V \to W$ è una forma bilineare se è lineare su ogni entrata. La forma bilineare si dice essere alternante se e solo se $\Phi(v, v) = 0$ per ogni $v \in V$.*

Definizione 3.5.4. *Dato $U \leq V$ sottospazio e Φ forma alternante, lo spazio ortogonale di U è:*

$$U^\perp = \{v \in V : \Phi(u, v) = 0 \ \forall u \in U\}.$$

Capitolo 4

Stime non ottimali

Prendiamo un numero naturale n: d'ora in poi con $f(n)$ intenderò il numero di gruppi (a meno di isomorfismo) di cardinalità n. Una curiosità: quando parlerò dei p-gruppi scriverò $f(p^n)$, dove p^n sarà allora la cardinalità del p-gruppo per qualche n, e questa scelta di notazione è concorde a quella degli autori in [1], ma si discosta da quella delle Lectures originali di Higman del 1959, dove viene utilizzata invece $f(n, p)$.

4.1 Piccoli gruppi

I gruppi di ordine n per $1 \leq n \leq 16$ sono stati classificati più di un secolo fa e quindi si può conoscere esattamente $f(n)$ per questi casi base. Riporto una tabella presente in [1] che esplicita quanto appena dichiarato.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14

Vorrei fare qualche commento. Notiamo che per tutti i numeri primi abbiamo una sola classe di isomorfismo dei gruppi di cardinalità corrispondente: sono i gruppi ciclici di ordine primo, tutti semplici. Non è comunque una condizione necessaria questa struttura di gruppo, infatti anche $f(15) = 1$, senza che 15 sia primo. Per questi piccoli n naturali troviamo per esempio gruppi che sono prodotti diretti (ad esempio $C_6 \cong C_2 \times C_3$), prodotti semidiretti (ad esempio $D_3 \cong C_3 \rtimes C_2$), quaternioni ($Q_8$, più piccolo gruppo hamiltoniano: ha tutti i sottogruppi normali pur non essendo abeliano): una gamma già variegata di strutture da poter studiare.

Aprendo un buon libro di matematica è praticamente certo (e di solito non serve neanche attendere molto) arrivare al momento di generalizzare. Durante il mio studio triennale ho voluto vivere questo approccio alla generalizzazione come uno dei valori che ispirassero il mio studio. È un concetto affascinante. Una volta colto nella sua forma purissima, quella matematica, è, a parer mio, assolutamente trasversale. Nell'argomento che sto trattando l'approccio alla generalizzazione si traduce nella curiosità: cosa accade per numeri oltre il 16, per generici $n \in \mathbb{N}$? L'idea di continuare a contare affidandoci alla classificazione risulta inapprodabile, ed ecco che vediamo affiorare l'intento di cercare delle stime ottimali.

4.2 Stime dall'alto

Vorrei mostrare un paio di possibili stime dall'alto per $f(n)$. La prima riguarderà il caso di un generico n naturale, la seconda invece le potenze di primi, avvicinandoci ai capitoli che verranno.

Proposizione 4.2.1. *Vale la seguente stima dall'alto per il numero di gruppi di ordine n: $f(n) \leq n^{n \log n}$.*

Dimostrazione. Sia G un gruppo di ordine n. Definiamo

$$d(G) = \min\{k | \exists g_1, \dots, g_k \in G,\ G = \langle g_1, \dots, g_k \rangle\}.$$

Dimostriamo intanto che $d(G) \leq \log n$. Prendiamo una catena massimale di sottogruppi di G:

$$\{1\} = G_0 < G_1 < \cdots < G_r = G.$$

Scegliamo $g_i \in G_i \setminus G_{i-1} \forall i \in \{1, \dots, r\}$. Il teorema di Lagrange ci dice che

$$|G| = \prod_{i=0}^{r} |G_i : G_{i-1}| \geq 2^r.$$

Avremo allora $r = d(G) \leq \log n$, da cui $r \leq \lfloor \log n \rfloor$, essendo r un intero.

Dal teorema di Cayley per i gruppi sappiamo che $G \leq Sym(n)$, dunque valgono le seguenti disuguaglianze:

$$\begin{aligned} f(n) &\leq |\{H \leq Sym(n) \text{ } con \text{ } |H| = n\}| \\ &\leq |\{H \leq Sym(n) \text{ } generati \text{ } da \text{ } \lfloor \log n \rfloor \text{ } elementi\}| \\ &\leq |\{H \subseteq Sym(n) \text{ } composti \text{ } da \text{ } \lfloor \log n \rfloor \text{ } elementi\}| \\ &\leq (n!)^{\log n} \\ &\leq n^{n \log n}. \end{aligned}$$

□

Come anticipato, ragioniamo ora in termini di p-gruppi. Nel prossimo capitolo vi parlerò di Higman per il suo risultato sulla limitazione dal basso per $f(n)$, mentre ora ve lo presento come autore di una limitazione dall'alto, anche se non ottimale. In realtà Higman fornisce nella stessa Lecture un risultato più preciso di quello che esporrò qui, ma lui stesso mette l'accento su quanto quest'altro procedimento articolato e complesso porti poi ad una stima molto vicina a quella che si riesce ad ottenere con strumenti più maneggevoli. Farò riferimento al teorema che sto per enunciare e dimostrare anche nel capitolo 6, perché l'idea dimostrativa è la stessa.

Teorema 4.2.2. *Con le notazioni utilizzate finora vale la seguente stima per ogni $m \geq 1$:*

$$f(p^m) \leq p^{\frac{1}{6}(m^3 - m)}$$

Dimostrazione. Cerco di dare un'idea dimostrativa prima di scrivere tecnicamente il procedimento. Graham Higman ha voluto fornire questa stima dall'alto spostando il problema sullo studio delle possibili presentazioni di un gruppo di cardinalità p^m. Ci saranno quindi due gradini per arrivare a concludere: prima vedere che per i p-gruppi ci si può restringere ad un particolare tipo di presentazioni, e poi stimare dall'alto il numero di tali presentazioni.

Consideriamo una serie normale massimale per un gruppo G di ordine p^m

$$G = G_0 \lhd \cdots \lhd G_{m-1} = \{1\}.$$

Abbiamo allora che per ogni $1 \leq i \leq m$ il quoziente G_i/G_{i-1} è gruppo ciclico di ordine p e che, definendo gli indici come indicato, G_i è sottogruppo normale di G, di indice p^i. Prendiamo un elemento $g_i \in G_{i-1} \setminus G_i$. Potremo quindi scrivere, per $\alpha_1, \ldots, \alpha_m \in \{1, \ldots, p-1\}$, ogni elemento del gruppo come

$$g = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_m^{\alpha_m}.$$

Siccome ogni termine della serie ha indice p nel precendente, si ha $g_i^p \in G_i$. Questo ci permette di scrivere, per $\beta_{i,i+1}, \ldots, \beta_{i,m} \in \{0, \ldots, p-1\}$ e per ogni g_i con $1 \leq i \leq m$:

$$g_i^p = g_{i+1}^{\beta_{i,i+1}} \ldots g_m^{\beta_{i,m}}, \tag{4.1}$$

Ora: $g_i G_i$ sta nel centro di G/G_i infatti quest'ultimo è un p-gruppo e come tale ha tutti i propri sottogruppi normali minimi contenuti nel centro. Questo significa che tutti i commutatori $[g_j, g_i]$ stanno in G_i per $1 \leq j < i \leq m$. Si possono trovare degli interi $\gamma_{j,i,k} \in \{0, \ldots, p-1\}$ per scrivere

$$[g_j, g_i] = g_{i+1}^{\gamma_{j,i,i+1}} \ldots g_m^{\gamma_{j,i,m}}. \tag{4.2}$$

Ora, omettendo la dimostrazione, diciamo che gli elementi scelti $g_1, \ldots, g_m$ assieme alle due tipologie di relazioni tra essi messe in evidenza in (4.1) e in (4.2) forniscono una presentazione di G. La classe di isomorfismo di G sarà determinabile attraverso la conoscenza dei $\beta_{j,i}$ per $1 \leq j < i \leq m$ e dei $\gamma_{j,i,k}$ per $1 \leq j < i < k \leq m$. Per ognuno di questi valori abbiamo p scelte possibili, e contandoli ci accorgiamo che sono $\frac{1}{6}(m^3 - m)$. Concludiamo che ci saranno allora $p^{\frac{1}{6}(m^3-m)}$ classi di isomorfismo per un gruppo G di ordine p^m, e questa è proprio la stima dall'alto che stavamo cercando. □

Capitolo 5

Limitazione dal basso

5.1 Idea di dimostrazione

Giungiamo al cuore della questione: il risultato di Graham Higman sulla limitazione dal basso per il numero di p-gruppi. L'idea della dimostrazione è quella di passare per la corrispondenza con un altro oggetto, come molto spesso capita di fare in matematica e specialmente in algebra. Studieremo alcune biezioni le cui protagoniste saranno le orbite ottenute dall'azione degli automorfismi di G sull'insieme dei sottogruppi di $\Phi(G)$. Servono alcuni lemmi preparatori.

5.2 Lemmi preparatori

Ricordo che la Φ-classe di un p-gruppo G è la lunghezza minima di una sua catena normale in cui tutti i quozienti sono centrali e abeliani elementari. Se un p-gruppo G ha Φ-classe 2 allora esiste un sottogruppo abeliano H di esponente p, contenuto nel centro di G, tale che il quoziente G/H sia ancora abeliano di esponente p.

Introduco delle scelte notazionali e definisco alcuni oggetti che utilizzerò uniformemente nei risultati di questo capitolo. Sia p un numero primo fissato. Preso un gruppo libero F_r di rango r generato da $x_1, \dots, x_r$, diciamo che G_r sia il quoziente F_r/N, dove N è il sottogruppo generato da tutte le parole del tipo $x^{p^2}, [x,y]^p, [x,y,z]$, per opportuni $x, y, z \in F_r$. Mostreremo nel lemma 5.2.2 che G_r è un p-gruppo finito. Il p-gruppo G_r è di Φ-classe 2. Identifico gli elementi x_i con la loro immagine in G_r: tali elementi possiamo dire che siano quindi generatori di G_r.

Lemma 5.2.1. *Sia dato H un p-gruppo di Φ-classe 2. Allora presi $y_1, \dots, y_r \in H$ esiste un automorfismo $\Phi : G_r \to H$, tale che $\Phi(x_i) = y_i$ per $i \in \{1, \dots, r\}$.*

Dimostrazione. Il gruppo F_r è un gruppo libero e quindi esiste un omomorfismo $\Psi : F_r \to H$ per cui $\Psi(x_i) = y_i$, per $i \in \{1, \dots, r\}$. Per ipotesi H è un p-gruppo di Φ-classe 2 (si faccia attenzione ai generatori di N), quindi $N \leq \ker \Psi$. Avevamo definito $G_r = F_r/N$ e ora sappiamo che N sta nel nucleo di Ψ, quindi concludiamo che Ψ induce l'automorfismo $\Phi : G_r \to H$ tale che $\Phi(x_i) = y_i$, sempre per $i \in \{1, \dots, r\}$. Questo è quello che stavamo cercando. □

Lemma 5.2.2. *Il gruppo G_r è un p-gruppo e il suo gruppo di Frattini $\Phi(G_r)$ è un sottogruppo centrale di ordine $p^{\frac{1}{2}r(r+1)}$ e di indice p^r. Inoltre, per ogni automorfismo $\alpha \in Aut(G_r)$ che induce l'identità su $G_r/\Phi(G_r)$, questo coincide con l'identità su $\Phi(G_r)$.*

Dimostrazione. Con riferimento a 3.2.4 ricordo che $[x^p, y] \in N$, da cui segue che le p-esime potenze stanno nel centro di G.

Qualunque commutatore o p-esima potenza è nel centro di G_r ed ha ordine p, quindi $G_r^p G_r'$ è un p-gruppo elementare abeliano contenuto nel centro di G. Siccome anche $G_r/G_r^p G_r'$ è un p-gruppo elementare abeliano, concludiamo che G_r è un p-gruppo. Dunque $\Phi(G_r) = G_r^p G_r' \leq Z(G_r)$. Vediamo ora che $\Phi(G_r)$ è generato dagli elementi delle potenze p-esime $x_1^p, \ldots, x_r^p$ e dai commutatori $[x_i, x_j]$ con $1 \leq i < j \leq r$, e che questi sono proprio un insieme di generatori minimale. Prendiamo un gruppo H ciclico di ordine p^2, generato da h: sarà quindi di Φ-classe 2. Sono allora valide le ipotesi del lemma 5.2.1: esiste per ogni $1 \leq k \leq r$ un omomorfismo $\Psi : G_r \to H$ tale che

$$\Psi_k(x_i) = \begin{cases} h & \text{per } i = k \\ 1 & \text{per } i \neq k. \end{cases}$$

Ora supponiamo che esistano $a_i \in \{0, \ldots, p-1\}$ con $1 \leq i \leq r$ e $b_{i,j} \in \{0, \ldots, p-1\}$ con $1 \leq i < j \leq r$ tali che

$$\prod_{i=1}^{r} (x_i^p)^{a_i} \prod_{1 \leq i < j \leq r} [x_i, x_j]^{b_{i,j}} = 1.$$

Applicando Ψ_k a questa equazione per ogni $1 \leq k \leq r$ si deduce $(h^p)^{a_k} = 1$, e quindi $a_k = 0$. Con un procedimento simile si può dimostrare che anche i $b_{i,j} = 0$. Si considera il gruppo H delle matrici 3x3 unitriangolari superiori su $\mathbb{F}_p$ e l'omomorfismo $\Phi_{i,j}$ che associa ai generatori x_i e x_j rispettivamente

$$h_i = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ e } h_j = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

e $h_k = \Phi_{i,j}(x_k) = 1$ per ogni $1 \leq k \leq r$ con $k \neq i$ e $k \neq j$. Applicando $\Phi_{i,j}$ all'equazione (5.2.2) si ottiene $[h_i, h_j]^{b_{i,j}} = 1$, da cui segue $b_{i,j} = 0$. Visto che l'insieme scelto di generatori per G_r è minimale, possiamo dire che $|\Phi(G_r)| = p^{r + \frac{1}{2}r(r-1)}$.

Sappiamo che $G_r/\phi(G_r)$ è abeliano elementare con insieme minimo di generatori $x_1, \ldots, x_r$: $\Phi(G)$ ha indice p^r. Ci manca da dimostrare la seconda asserzione. Come da ipotesi, consideriamo un automorfismo $\alpha \in Aut(G)$ che induce l'identità sul quoziente $G/\Phi(G_r)$. Esisteranno allora r elementi $h_1, \ldots, h_r$ di $\Phi(G_r)$ tali che $\alpha(x_i) = x_i h_i$, al variare di $i \in \{1, \ldots, r\}$. Il gruppo di Frattini è centrale ed è di esponente p, quindi:

$$\alpha(x_i^p) = \alpha(x_i)^p = (x_i h_i)^p = x_i^p \tag{5.1}$$

$$\alpha([x_j, x_i]) = [\alpha(x_j), \alpha(x_i)] = [x_j h_j, x_i h_i] = [x_j, x_i]. \tag{5.2}$$

Morale: l'automorfismo α fissa il gruppo di Frattini $\Phi(G_r)$, come afferma la tesi. □

Lemma 5.2.3. *Siano $N_1, N_2 \leq \Phi(G_r)$. Allora $G_r/N_1 \cong G_r/N_2$ se e solo se esiste un automorfismo $\alpha \in Aut(G_r)$ per cui $\alpha(N_1) = N_2$.*

Dimostrazione. I quozienti G_r/N_1 e G_r/N_2 sono ben definiti perché $\Phi(G_r) \leq Z(G_r)$. Ogni automorfismo $\alpha \in Aut(G_r)$ che manda N_1 in N_2 ne induce uno del tipo $\alpha' : G_r/N_1 \to G_r/N_2$. Dobbiamo dimostrare che vale anche il viceversa.

Prendiamo un automorfismo $\alpha' : G_r/N_1 \to G_r/N_2$, e degli elementi $y_1,\ldots,y_r \in G_r$ che soddisfino $\alpha'(x_iN_1) = y_iN_2$. Anche in questa dimostazione stiamo assumendo per ipotesi che G_r sia un p-gruppo di Φ-classe 2 e perciò possiamo sfruttare il lemma 5.2.1: esiste un omomorfismo $\alpha : G_r \to G_r$ tale che $\alpha(x_i) = y_i$. Sappiamo che α' è un automorfismo, quindi N_2 e $y_1, \ldots, y_r$ generano G_r. Ricordando che $N_2 \leq \Phi(G_r)$ possiamo dire che anche gli elementi $y_1, \ldots, y_r$ assieme a $\Phi(G_r)$ generano G_r. Ora fidiamoci, si può dimostrare: queste condizioni garantiscono che G_r sia generato da $y_1, \ldots, y_r$.

Mettiamo assieme i tasselli: sappiamo che gli y_i stanno nell'immagine di α e che generano G_r, quindi l'automorfismo α' è suriettivo. Ci basta ricordare che G_r è un gruppo finito per concludere che $\alpha' \in Aut(G_r)$. Quel che ci manca per arrivare alla tesi è far vedere che $\alpha(N_1) = N_2$, ovvero che l'immagine di α sia effettivamente quella che desideriamo. Per come è stata scelta la definizione di α si ha che $\alpha(x)N_2 = \alpha'(xN_1)$ con x uno qualunque tra i generatori di G_r, e comunque per qualunque elemento di G_r vale la relazione $\alpha(x)N_2 = \alpha'(xN_1)$. Dunque per commutatività del diagramma

$$\begin{array}{ccc} G_r & \xrightarrow{\alpha} & G_r \\ \downarrow & & \downarrow \\ G_r/N_1 & \xrightarrow{\alpha'} & G_r/N_2 \end{array}$$

si ha che $\alpha(N_1) = N_2$. □

5.3 Miglior limitazione dal basso

Proposizione 5.3.1. *Dati r e s interi tali che $1 \leq s \leq \frac{1}{2}r(r+1)$, esistono almeno $p^{\frac{1}{2}rs(r+1)-r^2-s^2}$ classi di isomorfismo di gruppi di ordine p^{r+s}.*

Dimostrazione. Riprendiamo in mano il gruppo G_r, e sia poi X l'insieme dei sottogruppi $N \leq \Phi(G_r)$ di indice p^s in $\Phi(G_r)$. Da ogni elemento di X possiamo ottenere i quozienti G_r/N di ordine p^{r+s}, al variare di N. Per il lemma 5.2.3 l'insieme delle classi di isomorfismo di questi quozienti è in corrispondenza biunivoca con l'insieme delle orbite degli automorfismi di $Aut(G_r)$ che agiscono su X.

Sia θ il naturale automorfismo da $Aut(G_r)$ in $Aut(G_r/\Phi(G_r))$. Sfruttando il lemma 5.2.2, ogni automorfismo $\alpha \in \ker\theta$ coincide con l'identità su $\Phi(G_r)$, agendo così in modo triviale sull'insieme X. Questo vuol dire che $\ker\theta$ è contenuto nello stabilizzatore di ogni elemento di X, cosicché la lunghezza di ogni orbita ottenuta dall'azione di $Aut(G_r)$ su X ha cardinalità al più $|Aut(G_r)|/|\ker\theta| \leq |Aut(G_r/\Phi(G_r))|$. Cambiamo punto di vista, guardando a $G_r/\Phi(G_r)$ come ad uno spazio vettoriale su $\mathbb{F}_p$, dove il gruppo di automorfismi di $G_r/\Phi(G_r)$ corrisponde alle trasformazioni lineari invertibili. Possiamo

sfruttare la stima $|Aut(G_r/\Phi(G_r))| = |GL(r,p)| \leq p^{r^2}$. Per quel che si è detto finora, ogni orbita di X ha cardinalità al massimo p^{r^2}. Il risultato presentato nel corollario 3.5.2 fornisce la seguente disequazione: $|X| \geq p^{(\frac{1}{2}r(r+1)-s)s}$. Basta incastrare queste ultime considerazioni per concludere: ci sono al più

$$p^{(\frac{1}{2}r(r+1)-s)s}/p^{r^2} = p^{(\frac{1}{2}rs(r+1))-s^2-r^2}$$

orbite di $Aut(G_r)$ su X, ovvero classi di isomorfismo di gruppi di ordine p^{r+s}. □

Teorema di Graham Higman 5.3.2. *Con la notazione introdotta predecentemente per $f(p^m)$, vale la seguente stima dal basso:*

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

Dimostrazione. Per $m \leq 6$ vediamo che la stima è banalmente vera. Per completezza dell'argomento svolgiamo il conto per questi primi sei casi.

$$m = 1 : f(p) \geq p^{-\frac{10}{27}} \tag{5.3}$$
$$m = 2 : f(p^2) \geq p^{\frac{-32}{27}} \tag{5.4}$$
$$m = 3 : f(p^3) \geq p^{-2} \tag{5.5}$$
$$m = 4 : f(p^4) \geq p^{-\frac{64}{27}} \tag{5.6}$$
$$m = 5 : f(p^5) \geq p^{-\frac{50}{27}} \tag{5.7}$$
$$m = 6 : f(p^6) \geq 1. \tag{5.8}$$

Tutti i membri di destra nelle disequazioni sovrastanti sono quantità inferiori o al più uguali a uno, mentre a sinistra la quantità è di certo maggiore o uguale a uno perché troviamo almeno il gruppo ciclico di p^m elementi. Per $m > 6$, scegliamo l'intero s come di seguito:

$$s = \begin{cases} \frac{1}{3}m, & \text{se } m \equiv 0 \bmod 3 \\ \frac{1}{3}(m+2), & \text{se } m \equiv 1 \bmod 3 \\ \frac{1}{3}(m+1), & \text{se } m \equiv 2 \bmod 3. \end{cases}$$

Sia $r = m - s$: per come lo sto definendo r è una quantità positiva. Sono valide le ipotesi della 5.3.1, e dalla sua tesi troviamo la stima cercata:

$$f(p^m) \geq p^{\frac{1}{2}rs(r+1)-r^2-s^2} \geq p^{\frac{2}{27}m^2(m-6)}.$$ □

La stima di Graham Higman ha un curioso fattore 2/27. Ancora più curioso è il modo in cui viene spiegato questo numero in [1], dove gli autori scrivono che il teorema sul miglior lower bound *gives us an indication* riguardo l'apparizione di 2/27, ed in letteralmente poco più di due righe risolvono il fatto. Il numero sembra spuntare come un fungo, e non sto usando questo lessico senza cognizione di causa, ora ve lo contestualizzo. Le colline di casa e le piogge di settembre mi hanno insegnato come fanno capolino i chiodini, e vi posso quindi assicurare che il paragone calza a pennello! Al di là della personale esperienza bucolica, non sono la prima ad affiancare questa immagine. In un articolo pubblicato su [4], cui parte del titolo è proprio *Funghi matematici*, gli autori fanno riferimento ad

un'immagine di Arnol'd: la matematica come collezione di funghi nella loro interezza, con il corpo fruttifero che rappresenta definizioni e risultati, e il micelio il labirintico intreccio di problemi, congetture, idee, errori. Credo che la struttura dei miceti si sposi bene col raccontare anche un altro aspetto della matematica. Capita spesso di ritrovarsi di fronte ad apparenti coincidenze, che nascondono interessanti grovigli di radici. Nel nostro cammino abbiamo trovato questo simpatico 2/27 nel mezzo della via, e non vogliamo calpestarlo: qual è il suo micelio?

Facciamo un passo indietro e torniamo alla 5.3.1: possiamo reinterpretarla dicendo che ci sono approssimativamente $p^{\frac{1}{2}a^2bm^3}$ gruppi aventi sottogruppo di Frattini di indice p^{am} e di ordine p^{bm}. Detto G generico gruppo di ordine p^m, siccome $\Phi(G) \leq G$, dal teorema di Lagrange:

$$|G| = |G : \Phi(G)||\Phi(G)| \Rightarrow p^m = p^{am}p^{bm} = p^{(a+b)m} \Rightarrow a + b = 1.$$

Il massimo (assunto per $a = 2/3$) della funzione $h(a, b) = \frac{1}{2}a^2b$ soggetta al vincolo $a+b = 1$ vale proprio 2/27. Si può proprio svolgere il conto come problema di massimo vincolato.

Come ho fatto vedere esplicitamente il nosto vincolo è $g(a, b) = a + b - 1 = 0$, quindi il moltiplicatore di Lagrange è $\nabla g = (1, 1)$. Possiamo scriverci la Lagrangiana

$$L(a, b, \lambda) = \frac{1}{2}a^2b + \lambda(a + b - 1)$$

e di conseguenza il sistema per la ricerca del massimo di questo sistema vincolato è il seguente:

$$\begin{cases} L_a = 0 \\ L_b = 0 \\ L_\lambda = 0 \end{cases} \Rightarrow \begin{cases} ab + \lambda = 0 \\ \frac{1}{2}a^2 + \lambda = 0 \\ a + b - 1 = 0 \end{cases} \Rightarrow \begin{cases} a(1 - a) - \frac{a^2}{2} = 0 \\ \lambda = -\frac{1}{2}a^2 \\ b = 1 - a \end{cases} \tag{5.9}$$

Dalla prima equazione troviamo $3a^2 - 2a = 0$, le cui soluzioni sono $a = 0$ e $a = 2/3$. Alla seconda corrisponde il massimo della funzione h sul vincolo imposto. Et voilà: $h(2/3, 1/3) = 2/27$!

Capitolo 6

Limitazione dall'alto

6.1 Idea di dimostrazione

Presenterò ora un risultato dovuto a Charles Sims. La strada sarà un po' più tortuosa rispetto a quella percorsa da Graham Higman nello studiare il lower bound. Premetto che a volte non mi accerterò della piena percorribilità a piedi, e farò quindi qualche piccolo balzo per superare dei torrenti potenzialmente fastidiosi. Ad ogni modo, quando arriverà il momento, sarò molto chiara sul grado di fiducia da riporre su risultati che non dimostrerò in questa sede. Prima di iniziare questo capitolo, vi invito a rileggere la stima dall'alto del teorema 4.2.2 facendo attenzione all'argomento che si usa per concludere. Come ha fatto Higman in quel caso, anche Sims fonda la sua dimostrazione sulla ricerca di presentazioni per il p-gruppo G, cercando di minimizzare la quantità di strumenti necessari per una presentazione di p-gruppo. L'approccio di Sims è quello di linearizzare il problema, vedremo in che termini.

Per i contenuti che espongo faccio tacito riferimento notazionale al capitolo introduttivo, se non specificato altrimenti. Ricordo in particolare che la serie centrale discendente per un gruppo G si definisce come $G = G_1 \geq G_2 \geq \dots$ dove $G_{i+1} = [G_i, G]$. Un qualsiasi p-gruppo può essere associato ad una mappa bilinare alternante grazie alla mappa naturale $\phi : G \times G \to G_2/G_3\Phi(G_2)$ che manda la coppia $(x, y) \in G \times G$ in $[x, y]G_3\Phi(G_2)$. Infatti, siccome $[G_2, G_1] = G_3$ e $[g^p, h] = [g, h]^p \mod G_3$ per qualsiasi $g, h \in G$, se si moltiplicano x e y per un elemento di $\Phi(G)$ l'immagine sarà comunque $\phi(x, y)$. Per questo la ϕ induce la mappa bilineare alternante $[,] : G/\Phi(G) \times G/\Phi(G) \to G_2/G_3\Phi(G_2)$. I due quozienti $G/\Phi(G)$ e $G_2/G_3\Phi(G_2)$ sono p-gruppi abeliani elementari: possiamo vederli anche come spazi vettoriali V e W su $\mathbb{F}_p$. Si può dimostrare che $[,] : V \times V \to W$ è bilineare con $[x, x] = 0$ per ogni $x \in V$, quindi alternante.

Definizione 6.1.1. *Dato un gruppo G diciamo che il rango di Sims $s(G)$ è il più piccolo intero non negativo s per cui esiste un sottogrupppo $H \leq G$ che abbia s generatori e sia $G_2 = H_2G_3$.*

Il rango di Sims di G è s se e solo se esiste un sottospazio $U \leq V$ con $\dim U = s$ che sia minimale rispetto alla dimensione e tale che $[U, U] = W$. Questo è vero perché un sottogruppo $H \leq G$ gode della proprietà $H_2G_3 = G_2$ se e solo se l'immagine $U = \phi(H)$

è tale che $[U,U] = W$. Vedremo che quando un p-gruppo G ha rango di Sims piccolo ci saranno poche possibilità per G una volta fissato G/G_3; se invece G ha rango di Sims grande allora ci saranno poche scelte per G/G_3.

La dimostrazione della stima di Sims sarà divisa in tre fasi che sfruttano le proprietà appena accennate. In un primo momento guarderemo qual è il massimo numero possibile di G/G_3 una volta fissato s, e per farlo lavoreremo linearizzando il problema di trovare quante sono le possibili strutture commutative di G/G_3 una volta fissato il rango di Sims s. Il secondo step sarà scegliere tra tutte le presentazioni di G quelle con delle particolari caratteristiche, ed è questo il passaggio in cui si migliora la stima del teorema 4.2.2 di Graham Higman. Il passo finale sarà proprio quello di dare una stima dall'alto al numero di queste speciali presentazioni di G.

6.2 Primo step: linearizzare il problema

Proposizione 6.2.1. *Consideriamo due spazi vettoriali V e W e prendiamo uno forma bilineare alternante $[,] : V \times V \to W$ con $\dim W > 0$. Supponiamo di avere $[V,V] = W$ e prendiamo U sottospazio minimale rispetto alla dimensione per cui si abbia $[U,U] = W$. Allora esistono degli elementi $x_1, \dots, x_s$ per cui, detto $V_i = \langle x_1, \dots, x_i \rangle$ con $i \in \{1, \dots, s-1\}$, si ha $[x_i, x_{i+1}] \notin [V_i, V_i]$.*

Da questa proposizione seguono i due corollari seguenti.

Corollario 6.2.2. *Consideriamo due spazi vettoriali V e W e prendiamo una forma bilineare alternante $[,] : V \times V \to W$ con $[V,V] = W$. Esiste allora un sottospazio $U \leq V$ con $[U,U] = W$ e $\dim U \leq \dim W + 1$.*

Dimostrazione. Quando $\dim W = 0$, il corollario diventa triviale (si prenda $U = \{0\}$), quindi assumiamo che $\dim W > 0$. Consideriamo U di dimensione minimale per cui $[U,U] = W$. Dalla proposizione 6.2.1 sappiamo che U ha una base $x_1, \dots, x_s$ con gli $s-1$ vettori $[x_1, x_2], [x_2, x_3], \dots, [x_{s-1}, x_s]$ linearmente indipendenti come sottoinsieme di W. Dunque $\dim U - 1 \leq \dim W$, da cui $\dim U \leq \dim W + 1$. □

Corollario 6.2.3. *Consideriamo due spazi vettoriali V e W e prendiamo uno forma bilineare alternante $[,] : V \times V \to W$ con $[V,V] = W$. Detto s il più piccolo intero tale che esista un sottospazio s-dimensionale $U \leq V$ per cui $[U,U] = W$, comunque si scelga un sottospazio $K \leq V$ si ha*

$$\dim[K,K] \leq \dim K + \dim W + 1 - s.$$

Dimostrazione. La mappa $[,]$ induce una mappa bilineare alternante $[,]' : V \times V \to W/[K,K]$. Siccome $[V,V]' = W/[K,K]$, il corollario 6.2.3 ci assicura che esiste un sottospazio $L \leq V$ tale che $\dim L \leq \dim(W/[K,K]) + 1$ con $[L,L]' = W/[K,K]$. È anche vero che $[K+L, K+L] = W$. Usando le formule per le dimensioni di spazi vettoriali quozienti e di somma di spazi vettoriali si ha la catena di disuglianze $s \leq \dim(K+L) \leq \dim K + \dim L \leq \dim K + \dim W - \dim[K,K] + 1$, da cui $\dim[K,K] \leq \dim K + \dim W + 1 - s$. □

L'idea della proposizione che segue, quella di sfruttare delle limitazioni superiori sul numero di mappe alternanti, è il contributo di Newman e Seeley al risultato di Sims.

Proposizione 6.2.4. *Prendiamo s un intero positivo e due spazi vettoriali V, W su $\mathbb{F}_p$, di dimensioni rispettivamente r_1 e r_2. Consideriamo le mappe bilineari alternanti $[,] : V \times V \to W$ e definiamo $N_p(r_1, r_2, s)$ tale che $p^{N_p(r_1,r_2,s)} \in \mathbb{R}$ sia il numero di tali forme bilineari alternanti per cui esista un sottospazio s-dimensionale $U \leq V$ con $[U, U] = W$, senza che ne esista uno di dimensione $s-1$ con la stessa proprietà. Allora:*

$$N_p(r_1, r_2, s) \leq \frac{1}{2} r_1^2 (r_2 - (s-1)) + O((r_1 + r_2)^{\frac{8}{3}}) \tag{6.1}$$

$$N_p(r_1, r_2, s) \leq \frac{1}{2} r_1^2 (r_2 - (s-1)) + \frac{1}{2} r_1 r_2 (s-1) + O((r_1 + r_2)^{\frac{5}{2}}) \tag{6.2}$$

Dimostrazione. Inizio dalla dimostrazione della (6.1). Siano $f = \lfloor r_1^{2/3} \rfloor$ e $g = \lfloor r_1 / f \rfloor$. Scegliamo una base $x_1, \ldots, x_{r_1}$ di V. La mappa bilineare alternante $[,]$ sarà determinata dai valori di $[x_k, x_l]$ per $1 \leq k < l \leq r_1$. Siccome ci sono al più p^{r_2} scelte per l'immagine di ogni vettore $[x_k, x_l]$, le mappe bilinari saranno al più $p^{\binom{r_1}{2} r_2}$. Se $s < 2r_1^{2/3} + 2$, otteniamo la (6.1), infatti si avrebbe

$$N_p(r_1, r_2, s) \leq \binom{r_1}{2} r_2 = \frac{1}{2}(r_1^2 r_2 - r_1 r_2) \leq \frac{1}{2} r_1^2 (r_2 - (s-1)) + O((r_1 + r_2)^{\frac{8}{3}}).$$

Assumiamo quindi $s \geq 2r_1^{2/3} + 2$. Definiamo i sottospazi $V_1, \ldots, V_g$ di V come

$$V_i = \langle x_{(i-1)f+1}, x_{(i-1)f+2}, \ldots, x_{(i-1)f+f} \rangle$$

per $i \in \{1, \ldots, g-1\}$ e poi

$$V_g = \langle x_{(g-1)f+1}, \ldots, x_{r_1} \rangle.$$

Per tutti gli interi i e j in $1 \leq i < j \leq g$ abbiamo $\dim(V_i + V_j) \leq \dim V_i + \dim V_j \leq 2f$. Il corollario 6.2.3 ci fa concludere che

$$\dim[V_i + V_j, V_i + V_j] \leq 2f + r_2 + 1 - s < r_2.$$

Per ogni $1 \leq i < j \leq g$, prendiamo un sottospazio di W che sia di dimensione $2f + r_2 + 1 - s$ e che contenga $[V_i + V_j, V_i + V_j]$: chiamiamo W_{ij} tale sottospazio. Facendo un conteggio come mostrato nella proposizione 3.5.1 sappiamo che ci sono al più $p^{r_2^2 \binom{g}{2}}$ possibili scelte per W_{ij}, e per ogni tale W_{ij} ci sono $p^{2f + r_2 + 1 - s}$ scelte per l'immagine di ogni $[x_k, x_l]$ perché $x_k, x_l \in V_i + V_j$ per qualche $1 \leq i < j \leq g$ e quindi $[x_k, x_l] \in W_{ij}$. In definitiva una volta fissato il sottospazio W_{ij} ci sono al più $p^{\binom{r_1}{2}(2f + r_2 + 1 - s)}$ possibili mappe bilineari alternanti $[,]$. Notando che $f = r_1^{2/3} + O(1)$ e $g = r_1^{1/3} + O(1)$, si ha

$$p^{N_p(r_1,r_2,s)} \leq p^{\binom{r_1}{2}(2f + r_2 + 1 - s) + r_2^2 \binom{g}{2}} = p^{\binom{r_1}{2}(r_2 - (s-1)) + O(r_1 + r_2)^{8/3}},$$

da cui si ricava la (6.1) sviluppando il coefficiente binomiale.

Passiamo alla dimostrazione della (6.2). Notiamo che anche qui la limitazione superiore è subito verificata per alcuni s, ovvero per $s \leq 2r_1^{1/2}+2$. Supponiamo allora che $s > 2r_1^{1/2}+2$. Diciamo $f = \lfloor r_1^{1/2} \rfloor$ e $g = \lfloor r_1/f \rfloor$. Scegliamo la base $x_1, \dots, x_{r_1}$ per definire V_i e W_{ij} tali e quali a quelli della dimostrazione per (6.1). Anche con queste nuove scelte di f e di g il sottospazio W_{ij} rimane ben definito perché $r_2 - s + 1 + 2f < r_2$. Analogamente a prima, per la proposizione 3.5.1 sappiamo che ci sono al più $p^{\binom{g}{2}(r_2-(r_2-s+1+2f)+1)(r_2-s+1+2f)} = p^{\binom{g}{2}(r_2-s+1+2f)(s-2f)}$ sottospazi W_{ij} di W, con $p^{r_2-s+1+2f}$ scelte per l'immagine di ogni $[x_k, x_l]$. Morale:

$$N_p(r_1, r_2, s) \leq p^{\binom{g}{2}(s-2f)(r_2-s+1+2f)+\binom{r_1}{2}(r_2-s+1+2f)}.$$

Sostituendo $f = r_1^{1/2} + O(1)$ e $g = r_1^{1/2} + O(1)$, si trova proprio (6.2). □

6.3 Secondo step: ottimalizzare la scelta dei casi

Come anticipato, in questo step intermedio si scelgono delle particolari presentazioni per il gruppo G di modo da abbassare la stima dall'alto che avevamo visto con il metodo di Graham Higman nel teorema 4.2.2. All'inizio mostrerò una serie di relazioni valide per gli elementi di G, per poi verificare che individuino una presentazione del gruppo. Consideriamo G di cardinalità p^n, e la sua serie centrale discendente $G = G_1 \geq G_2 \geq G_3 \geq G_4 \geq \cdots \geq G_c \geq G_{c+1} = \{1\}$. Per $1 \leq i \leq c$ sia r_i il rango di G_i/G_{i+1}. Poniamo poi $V = G/\Phi(G)$ e $W = G_2/G_3\Phi(G_2)$. Dal lemma 3.4.4, per il gruppo di Frattini $\Phi(G)$ di un p-gruppo sappiamo che $\dim V = r_1$ e $\dim W = r_2$. Costruiamo due basi $x_1, \dots, x_{r_1}$ e $y_1, \dots, y_{r_2}$ rispettivamente di V e di W nel modo seguente. Il processo di formare dei commutatori in G induce una mappa bilineare alternante $[,] : V \times V \to W$. Sia s il rango di Sims di G e sia $U \leq V$ di dimensione minimale affinché $[U, U] = W$, quindi un sottospazio U s-dimensionale. Dal corollario 6.2.2 si ha $s \leq r_2 + 1$, e dalla proposizione 6.2.1 sappiamo che esiste una base $x_1, \dots, x_s$ per U, con $V_i = \langle x_1, \dots, x_i \rangle$ per $i \in \{1, \dots, s-1\}$ e $[x_i, x_{i+1}] \notin [V_i, V_i]$. Poniamo $W_i = [V_i, V_i]$ e $d_i = \dim(W_i)$. Allora $0 < d_1 < \cdots < d_s = r_2$. Definiamo inoltre $d_0 = 0$. Prendiamo una base $y_1, \dots, y_{r_2}$ per W di modo da avere $W_i = \langle y_1, \dots, y_{d_i} \rangle$ per ogni $i \in \{2, 3, \dots, s\}$. Ora

$$W_i = \langle W_{i-1}, [x_1, x_i], \dots, [x_{i-1}, x_i] \rangle,$$

quindi possiamo scegliere gli elementi y_j per cui esistano $f(1), \dots, f(r_2)$ in $\mathbb{Z}$ tali che $y_j = [x_{f(j)}, x_i]$ con $1 \leq f(j) < i$ per ogni $d_{i-1} < j \leq d_i$. Per ottenere una base di V, estendiamo $x_1, \dots, x_s$ a $x_1, \dots, x_{r_1}$. Per $1 \leq i \leq r_1$ sia x_i tale che $x_i = g_{1i}\Phi(G)$, e definiamo per $d_{i-1} < j \leq d_i$ gli oggetti

$$g_{2j} = [g_{1f(j)}, g_{1i}]. \tag{6.3}$$

Infine prendiamo $H = \langle g_{11}, \dots, g_{1s} \rangle \leq G$.

Il gruppo H_2 contiene tutti gli elementi g_{2j} e $G_2/G_3\Phi(G_2)$ è generato da $y_1, \dots, y_{r_2}$, quindi si conclude che $H_3G_3 = G_2$. Per la proposizione 6.2.4 otteniamo che $H_i = G_i$ per ogni $i \geq 2$.

Quando $i \in \{3, \dots, c\}$, definiamo $g_{i1}, \dots, g_{ir_i} \in G$ di modo da avere $G_i/G_{i+1} = \langle g_{i1}G_{i+1}, \dots, g_{1r_1}G_{i+1}\rangle$. Avendo appena visto che $G_i = H_i$ per ogni $i \leq 2$, è lecito prendere per la proposizione 6.2.1 $g_{ij} = [g_{(i-1)k}, g_{1l}]$ con $1 \leq k \leq r_{i-1}$ e $1 \leq l \leq s$. Quello che bisogna dimostrare è che se $i = 3$ si può scegliere $d_{l-1} < k$. È bastevole far vedere che l'insieme $\{[g_{2k}, g_{1l}] | 1 \leq l \leq s, 1 \leq k \leq r_2\}$ è contenuto nel sottogruppo L generato da G_4 e da $\{[g_{2k}, g_{1l}] | 1 \leq l \leq s, d_{l-1} < k \leq r_2\}$. La dimostrazione è induttiva. Consideriamo un intero $3 \leq a \leq s$ e come ipotesi induttiva assumiamo che $[g_{2k}, g_{1l}] \in L$ per ogni $1 \leq l < a$ e $1 \leq k \leq r_2$. Per $a = 3$ vale perché, come avevamo visto, $d_0 = d_1 = 0$. Ora dividiamo due casi da studiare al variare di k. Se vale $k > d_{a-1}$, per definizione di L siamo certi che $[g_{2k}, g_{1a}] \in L$. Ci interessa allora quando $1 \leq k \leq d_{a-1}$. Per la definizione data in (6.3) sappiamo che per tali k

$$[g_{2k}, g_{1a}] = [g_{1f(k)}, g_{1i}, g_{1a}] = [g_{1i}, g_{1a}, g_{1f(k)}]^{-1}[g_{1a}, g_{1f(k)}, g_{1i}]^{-1} \bmod G_4. \tag{6.4}$$

I commutatori $[g_{1i}, g_{1a}]$ e $[g_{1a}, g_{1f(k)}]$, sono prodotti di elementi g_{2j} modulo G_3. Per ipotesi induttiva, siccome $f(k) < a$ e $i < a$, ricaviamo che gli elementi in (6.4) stanno in L mod G_4, ma per definizione di $L \geq G_4$, quindi $[g_{2k}, g_{1a}] \in L$. Si conclude per induzione su a.

Avendo scelto dei particolari generatori di G, dobbiamo prendere un opportuno insieme di relazioni su di essi di modo da ottenere una presentazione del gruppo. Diamo alcune definizioni necessarie ad enunciare il prossimo teorema, utilizzando notazioni coerenti con quelle precedenti. Per $i \in \{1, \dots, c\}$ e $j \in \{1, \dots, r_i\}$:

$$a(i,j) = \min\{z \in \mathbb{N}^* | g_{ij}^{p^{a(i,j)}} \in \langle G_{i+1}, g_{i1}, \dots, g_{i(j-1)}\rangle\}. \tag{6.5}$$

Faccio delle considerazioni prima delle prossime due definizioni. Da (6.5) capiamo di poter scrivere gli elementi del gruppo G come

$$g = g_{11}^{e(1,1)} g_{12}^{e(1,2)} \cdots g_{1r_1}^{e(1,r_1)} g_{21}^{e(2,1)} \cdots g_{cr_2}^{e(c,r_2)} = \prod_{1 \leq i \leq c, 1 \leq j \leq r_i} g_{ij}^{e(i,j)}$$

dove $0 \leq e(i,j) < p^{a(i,j)}$. Condizione necessaria sufficiente affinché $g \in G_i$ è che $e(u,v) = 0$ per ogni $u < i$, per cui $|G_i| = p^{\sum_{u=i}^{c} \sum_{v=1}^{r_u} a(u,v)}$. Se prendiamo $i = 1$ nella prima sommatoria, l'esponente sarà m. Da questo e da (6.5) si ricava che per ogni $i \in \{1, \dots, c\}$ vale $\sum_{u=i+1}^{c} \sum_{v=1}^{r_u} a(u,v) \leq m - r_1 - \cdots - r_i$.

Per $i \in \{1, \dots, c\}$ e $j \in \{1, \dots, r_i\}$ sia $b(i,j,u,v) \in \mathbb{Z}$ tale che

$$g_{ij}^{p^{a(i,j)}} = \prod_{1 \leq u \leq c, 1 \leq v \leq r_u} g_{uv}^{b(i,j,u,v)}; \tag{6.6}$$

per $i \in \{1, \dots, c\}$, $j \in \{1, \dots, r_i\}$ e $k \in \{1, \dots, r_1\}$ sia $c(i,j,k,u,v) \in \mathbb{Z}$ tale che

$$[g_{ij}, g_{1k}] = \prod_{1 \leq u \leq c, 1 \leq v \leq r_u} g_{uv}^{c(i,j,k,u,v)}. \tag{6.7}$$

Faccio notare che $b(i,j,u,v) = 0$ se $u < i$ oppure se $u = i$ e $v \geq j$, mentre $c(i,j,k,u,v) = 0$ se $u \leq i$.

Teorema 6.3.1. *La classe di isomorfismo di G è univocamente determinata dagli interi $p, c, s, r_1, \ldots, r_c, d_0, \ldots, d_s$ assieme agli interi*

$$\begin{aligned}
&a(i,j), && 1 \le i \le c, 1 \le j \le r_i,\\
&b(i,j,u,v), && 1 \le i \le c, 1 \le j \le r_i, i \le u \le c, 1 \le v \le r_u,\\
&c(1,j,u,v), && 1 \le j < k \le r_1, 2 \le u \le c, 1 \le v \le r_u,\\
&c(2,j,k,u,v), && 1 \le k \le s, d_{k-1} < j \le r_2, 3 \le u \le c, 1 \le v \le r_u,\\
&c(i,j,k,u,v), && 3 \le i \le c, 1 \le j \le r_i, 1 \le k \le s, 1 < u \le c, 1 \le v \le r_u.
\end{aligned}$$

Dimostrazione. Per questo teorema non farò una dimostrazione completa, ma cercherò comunque di fornirvi alcuni spunti. Intanto ci si può ridurre a dimostrare qualcosa di equivalente alla tesi, ovvero: qualsiasi gruppo G di classe di nilpotenza al più c ha ordine al più p^m, se è generato dall'insieme $\{g_{ij} | 1 \le i \le c, 1 \le j \le r_i\}$, e se soddisfa (6.6) per $1 \le i \le c$ e $1 \le j \le r_i$, e se soddisfa (6.7) quando $i = 2$ con $1 \le k \le s$ e quando $3 \le i \le c$ con $1 \le j \le r_i$ e $1 \le k \le s$. Due gruppi L e M che abbiano la stessa collezione di interi di G, saranno entrambi isomorfi ad un quoziente di G. Siccome $\sum_{u=1}^{c} \sum_{v=1}^{r_u} a(u,v) = m$, i gruppi L e M hanno entrambi ordine p^m. Se il gruppo G ha massimo ordine p^m (ovvero quello che ci si riduce a dimostrare), saranno sia L che M isomorfi a G e dunque anche isomorfi tra loro per transizione.

È da controllare che il gruppo G abbia ordine al più p^m. Definiamo $H = \langle g_{11}, \ldots, g_{1s} \rangle$, $H_i = \langle g_{uv} | i \le u \le c, 1 \le v \le r_u \rangle$ quando $2 \le i \le c$, e $H_{c+1} = \{1\}$. Quando $u \le 2$, le relazioni di g_{uv} che abbiamo precedentemente studiato ci assicurano che l'elemento possa essere scritto come commutatore di lunghezza u in $g_{11}, \ldots, g_{1s}$. Si può dimostrare che la serie

$$H \ge H_2 \ge \cdots \ge H_c \ge H_{c+1} = \{1\}$$

è la serie centrale discendente di H, da cui in particolare si ricavano la normalità di H_c in H e la centralità di H_i/H_{i+1} in H/H_{i+1}. Dalle relazioni tra i commutatori che generano gli H_i segue che H/H_2 è abeliano, che H è normale in G, e che G/H è abeliano. Sono abeliani quindi i quozienti di due termini successivi della serie

$$G \ge H \ge H_2 \ge \cdots \ge H_c \ge 1.$$

Da (6.6) otteniamo le disuguaglianze che seguono:

$$\begin{aligned}
|H_i/H_{i+1}| &\le p^{\sum_{j=1}^{r_i} a(i,j)}\\
|H/H_2| &\le p^{\sum_{j=1}^{s} a(1,j)}\\
|G/H| &\le p^{\sum_{j=s+1}^{r_1} a(1,j)}.
\end{aligned}$$

Segue la tesi perché $|G| \le p^{\sum_{i=1}^{c} \sum_{j=1}^{r_i} a(i,j)} = p^m$, e questo basta, per quanto spiegato prima. □

6.4 Terzo step: miglior limitazione dall'alto

Come promesso, con la ponderata scelta di presentazioni per il gruppo G fatta nelle sezioni precedenti, cerchiamo una limitazione superiore al numero di classi di isomorfismo identificate da tali presentazioni.

Lemma 6.4.1. *Preso $n \in \mathbb{N}$, esistono esattamente 2^{n-1} partizioni ordinate di n.*

Dimostrazione. Per fare una partizione di n, immaginiamo di scriverlo come somma di n unità. Per intenderci:

$$\underbrace{1+1+\cdots+1+1}_{n \text{ volte}}.$$

Per scegliere una partizione di n dobbiamo decidere come raggruppare le unità della somma, ovvero quali e/o quante parantesi inserire. I segni sono proprio 2^{n-1}, tanti quanti le coppie di parentesi che si possono inserire $)+($ per formare delle partizioni di n. Concludiamo che esistono esattamente 2^{n-1} partizioni ordinate di n.

□

Corollario 6.4.2. *Le partizioni non ordinate di $n \in \mathbb{N}$ sono al più 2^{n-1}.*

Dimostrazione. Segue subito dal lemma 6.4.1. □

Ora leggerete due lemmi che riguardano dei problemi di estremo vincolato. Nel teorema conclusivo di questa sezione serviranno degli argomenti analitici per fornire la limitazione dall'alto sul numero di classi di isomorfismo di un gruppo G di ordine p^m. Questi lemmi anticipano i risultati necessari.

Lemma 6.4.3. *La funzione*

$$A(x,y,z,u) = \frac{1}{2}x^2(z+y-u) + \frac{1}{2}xyu + (uy - \frac{1}{2}u^2)z + \frac{1}{2}uz^2$$

assume valori minori uguali a $\frac{2}{27}$ per le variabili $y, z, u \geq 0$, $x \geq \frac{6}{10}$, $u \leq y$ soggette al vincolo $x+y+z=1$.

Dimostrazione. Questa dimostrazione farà uso della tecnica dei moltiplicatori di Lagrange per lo studio di estremi vincolati. Iniziamo quindi accertandoci che la funzione $A(x,y,z,u)$ non abbia punti critici interni:

$$\begin{aligned}
\frac{\partial A}{\partial x} &= x(z+y-u) + \frac{1}{2}yu; \\
\frac{\partial A}{\partial y} &= \frac{1}{2}x^2 + \frac{1}{2}xu + uz; \\
\frac{\partial A}{\partial z} &= \frac{1}{2}x^2 + uy - \frac{1}{2}u^2 + uz; \\
\frac{\partial A}{\partial u} &= -\frac{1}{2}x^2 + \frac{1}{2}xy + yz - uz + \frac{1}{2}z^2.
\end{aligned}$$

Per il teorema dei moltiplicatori di Lagrange, in un punto di estremo vincolato nell'interno della regione considerata devono valere $\frac{\partial A}{\partial x} = \frac{\partial A}{\partial y} = \frac{\partial A}{\partial z}$ e $\frac{\partial A}{\partial u} = 0$, da cui si trova

$$\frac{1}{2}xu = uy - \frac{1}{2}u^2.$$

Nell'interno della regione si ha $u > 0$, da cui $u = 2y - x$ e $2y > x$ su tutti gli eventuali punti critici interni. Dalla condizione di annullamento della derivata parziale rispetto a u e dato che $u = 2y - x$, si trova anche che

$$\frac{1}{2}x(y-z) + yz - 2yz + xz + \frac{1}{2}z^2 = 0,$$

per cui

$$z^2 = (x-y)(x-2z) \tag{6.8}$$

è un'altra uguaglianza valida negli eventuali punti critici interni. Siccome $x \geq \frac{6}{10}$, $z \geq 0$, ed è richiesto che $x+y+z = 1$, si ha $y \leq \frac{4}{10}$ e $x - y \geq \frac{2}{10}$ nella regione considerata. Prima si è mostato che $2y \geq x$, quindi $y \geq \frac{3}{10}$ e $z \leq \frac{1}{10}$. Dunque, $x - 2z \geq \frac{4}{10}$. L'equazione (6.8) vale al più $(\frac{1}{10})^2$ al membro di destra e almeno $\frac{2}{10}\frac{4}{10} = \frac{8}{100}$ al membro di sinistra. Questo è assurdo: non ci sono allora punti critici interni alla regione.

Bisogna studiare il comportamento della funzione $A(x, y, z, u)$ al bordo della regione. Iniziamo da $u = 0$: la funzione sarà $A(x, y, z, 0) = \frac{1}{2}x^2(y + z)$. Si può dimostrare che il massimo di $A(x, y, z, u)$ è assunto per $x = \frac{2}{3}$ e $y + z = \frac{1}{3}$, e vale $\frac{2}{27}$. Per $y = 0$ si ha che anche $u = 0$, quindi ci ritroviamo al caso appena valutato. Quando $z = 0$:

$$\begin{aligned} A(x, y, 0, u) &= \frac{1}{2}x^2(y-u) + \frac{1}{2}xyu \\ &= \frac{1}{2}x^2y + \frac{1}{2}xu(y-x) \\ &< \frac{1}{2}x^2y \\ &\leq \frac{2}{27}. \end{aligned}$$

Per completare lo studio al bordo ci mancano i casi $x = \frac{6}{10}$ e $u = y$. Per il primo si studia $A(\frac{6}{10}, y, z, u)$ con $y, z \geq 0$, $u \leq y$, sotto al vincolo $y + z = \frac{4}{10}$. Lo studio dei punti critici della funzione $A(x, y, z, u)$ non aveva coinvolto l'utilizzo della derivata parziale rispetto alla variabile x, quindi possiamo reciclare quella dimostrazione e concludere che $A(\frac{6}{10}, y, z, u)$ non ha punti critici interni e assume valore massimo $\frac{2}{27}$ qualora si annulli almeno uno tra y, z, u. Se $u = y$, possiamo sostituire $z = \frac{4}{10} - y$ e troviamo che

$$A(\frac{6}{10}, y, z, y) = \frac{18}{100}z + \frac{3}{10}y^2 + \frac{1}{2}y^2z + \frac{1}{2}yz^2 = \frac{72}{100} + \frac{1}{10}(y^2 - y),$$

funzione decrescente nella regione $0 \leq y \leq \frac{4}{10}$ che assume valore massimo pari a $\frac{72}{100} < \frac{2}{27}$ per $y = 0$.

Rimane solo da studiare il bordo $u = y$, in cui

$$A(x, y, z, y) = \frac{1}{2}x^2z + \frac{1}{2}xy^2 + \frac{1}{2}y^2z + \frac{1}{2}yz^2.$$

Il caso in cui $x = \frac{6}{10}$ è già stato valutato, e lo stesso vale per $y = 0$ e per $z = 0$. Basta verificare che la funzione $A(x, y, z, y)$ non abbia punti critici interni. Se esistessero, in tali punti si avrebbe che $\frac{\partial A(x,y,z,y)}{\partial y} = \frac{\partial A(x,y,z,y)}{\partial z}$, ovvero

$$xy + yz + \frac{1}{2}z^2 = \frac{1}{2}x^2 + \frac{1}{2}y^2 + yz,$$

da cui

$$z^2 = (x-y)^2.$$

Nella regione osservata entrambi i membri di questa uguaglianza sono quantità positive, allora $z = x - y$. Si può poi sostituire $y = 1 - x - z$ per trovare che $x = \frac{1}{2}$. Questo è assurdo perché $x \geq \frac{6}{10}$, quindi non ci sono punti critici (e in particolare massimi) nella ragione interna. Riassumendo: abbiamo mostrato che la funzione $A(x, y, z, u)$ non ha punti critici nell'interno della regione su cui la consideriamo, e che al bordo assume valori minori uguali a $\frac{2}{27}$, da cui segue la tesi. □

Lemma 6.4.4. *La funzione*

$$B(x, y, z, u) = \frac{1}{2}x^2(z + y - u) + (uy - \frac{1}{2}u^2)z + \frac{1}{2}uz^2$$

soddisfa $B(x, y, z, u) < \frac{72}{1000} \leq \frac{2}{27}$ *quando* $x, y, z, u \geq 0$, $u \leq \min(x, y)$, $x \leq \frac{6}{10}$, *soggetti al vincolo* $x + y + z = 1$.

Dimostrazione. La dimostrazione sarà analoga nell'impostazione a quella del lemma 6.4.3, infatti si sfrutterà il teorema dei moltiplicatori di Lagrange. Iniziamo verificando che la funzione $B(x, y, z, u)$ non abbia punti critici interni alla regione su cui la stiamo considerando. Calcoliamo le derivate parziali:

$$\begin{aligned}
\frac{\partial B}{\partial x} &= x(z + y - u);\\
\frac{\partial B}{\partial y} &= \frac{1}{2}x^2 + u;\\
\frac{\partial B}{\partial z} &= \frac{1}{2}x^2 + uy - \frac{1}{2}u^2 + uz;\\
\frac{\partial B}{\partial u} &= -\frac{1}{2}x^2 + yz - uz + \frac{1}{2}z^2.
\end{aligned}$$

Uguagliando le derivate parziali rispetto a y e z (ricordiamo che il vincolo è $x+y+z = 1$), si trova che $uy - \frac{1}{2}u^2 = 0$, da cui $2y = u$ nei punti critici della funzione $B(x, y, z, u)$. Questo è già un assurdo perché abbiamo anche che $u \leq y$ e $u > 0$: la funzione non ha punti critici interni. Cerchiamo il massimo valore che può assumere al bordo. Non si è fatto uso delle derivate parziali rispetto a x e ad u, quindi si può già dire che per $x = 0$ e $x = \frac{1}{6}$ la funzione non presenta punti critici. I casi che ci restano da studiare sono $z = 0$, $u = 0$, $y = 0$, $u = x$, $u = y$. Ne consideriamo uno alla volta.

Per $z = 0$, $x + y = 1$, e $0 \leq x \leq \frac{6}{10}$, troviamo che

$$B(x, y, 0, u) = \frac{1}{2}x^2(y - u) \leq \frac{1}{2}x^2 y,$$

funzione che assume massimo pari a $\frac{72}{1000}$ quando $x = \frac{6}{10}$ e $y = \frac{4}{10}$.

Per $u = 0$, $x + y + z = 1$, e $0 \leq x \leq \frac{6}{10}$, troviamo che

$$B(x, y, z, 0) = \frac{1}{2}x^2(z + y),$$

che assume massimo pari a $\frac{72}{1000}$ quando $x = \frac{6}{10}$ e $y + z = \frac{4}{10}$.

Se $y = 0$ allora anche $u = 0$, quindi ricadiamo nel caso appena discusso.

Per $u = x$, si ha $u \leq y$ e allora

$$B(x, y, z, x) = \frac{1}{2}x^2y - \frac{1}{2}x^3 + xyz + \frac{1}{2}xz^2.$$

Ricordiamo che la regione osservata è quella delle variabili non negative con $x+y+z = 1$, $x \leq y$: si trova così che $x \leq \frac{1}{2} < \frac{6}{10}$, perciò x soddisfa l'ulteriore condizione richiesta ovvero $x \leq \frac{6}{10}$. In tutti i punti critici interni, dove la variabile x è strettamente positiva, vale

$$\begin{aligned} \frac{\partial B(x, y, z, x)}{\partial y} &= \frac{\partial B(x, y, z, x)}{\partial z} \\ \frac{1}{2}x^2 + xz &= x(y + z) \\ x &= 2y. \end{aligned}$$

Avevamo però anche $x \leq y$, quindi dovrebbe essere $x = y = 0$, assurdo. La funzione $B(x, y, z, x)$ non ha punti critici interni. Se $x = 0$, la funzione $B(x, y, z, x)$ si annulla; dato che è una restrizione di $B(x, y, z, u)$, sappiamo anche che assume valori minori uguali a $\frac{72}{1000}$ quando $y = 0$ o $z = 0$. Quando invece $x = y$ troviamo

$$B(x, x, z, u) = x^2z + \frac{1}{2}xz^2,$$

con $x \geq 0, z \geq 0$, e $2x + z = 1$. Applicando il teorema dei moltiplicatori di Lagrange, abbiamo che in un eventuale punto critico interno di questa funzione ristretta deve valere che

$$\begin{aligned} \frac{\partial B(x, x, z, u)}{\partial x} &= 2\frac{\partial B(x, x, z, u)}{\partial z}; \\ 2xz + \frac{1}{2}z^2 &= 2x^2 + 2xz; \\ z^2 &= 4x^2, \end{aligned}$$

da cui $z = 2x$. Siccome $2x + z = 1$ esiste un unico punto critico interno, realizzato per $x = \frac{1}{4}$ e $z = \frac{1}{2}$, dove la funzione assume valore massimo $\frac{1}{16} \leq \frac{72}{1000}$. Al bordo $x = y = 0$ la funzione si annulla, quindi il valore $\frac{72}{1000}$ è proprio una limitazione superiore per $B(x, x, z, u)$.

Rimane da discutere il caso di $u = y$:

$$B(x, y, z, y) = \frac{1}{2}x^2z + \frac{1}{2}y^2z + \frac{1}{2}yz^2$$

sulla regione definita da $0 \leq x \leq \frac{6}{10}$, $y, z \geq 0$, $y \leq x$ e $x+y+z = 1$. Si tratta sempre di una restrizione di $B(x, y, z, u)$ anche se diversa da quelle già discusse, perciò sappiamo già che assume valore minore uguale a $\frac{72}{1000}$ quando $y = 0$ oppure $z = 0$, come pure per $x = 0$ visto

che allora si avrebbe anche $y = 0$. Se $y = x$ ci ritroviamo in $x = u$. L'unica questione ancora aperta riguarda quindi l'interno della regione su cui consideriamo $B(x, y, z, y)$. Calcoliamoci come usuale le derivate per cercare eventuali punti critici interni:

$$\begin{aligned}\frac{\partial B(x,y,z,y)}{\partial x} &= xz \\ \frac{\partial B(x,y,z,y)}{\partial y} &= yz + \frac{1}{2}z^2 \\ \frac{\partial B(x,y,z,x)}{\partial z} &= \frac{1}{2}x^2 + \frac{1}{2}y^2 + yz.\end{aligned}$$

Imponendo l'uguaglianza tra le derivate parziali rispetto a x e y troviamo $x = y + \frac{1}{2}z$ nei punti critici interni. Mettendo insieme il fatto che $x+y+z = 1$, abbiamo che $y = 3x-1$. Considerando invece le derivate parziali rispetto a y e z, la loro uguaglianza comporta che $z^2 = x^2 + y^2$ nei punti critici. Combinando con qualche passaggio algebrico queste condizioni si conclude che l'unico punto critico è

$$x = \frac{5-\sqrt{7}}{6}, y = \frac{3-\sqrt{7}}{2}, z = \frac{2\sqrt{7}-4}{3}.$$

La funzione $B(x, y, z, y)$ assume valore $\frac{7\sqrt{7}-17}{27} < \frac{72}{1000}$ nel suo unico punto critico. Per finire la dimostrazione bisogna accertarsi che nella regione di positività delle variabili y e z soggete a $y + z = \frac{4}{10}$ si abbia che

$$B\left(\frac{6}{10}, y, z, y\right) \leq \frac{72}{1000}.$$

In un punto critico interno, le derivate parziali rispetto a y e z di questa funzione si eguagliano, ovvero vale che

$$yz + \frac{1}{2}z^2 = \frac{18}{100} + \frac{1}{2}y^2 + yz.$$

Dato che stiamo studiando la funzione per $z \leq \frac{4}{10}$, in un suo punto critico si avrà che $y^2 = z^2 - \frac{36}{100} < 0$, che è assurdo. Non ci sono punti critici interni per la funzione $B(\frac{6}{10}, y, z, y)$, la quale si annulla per $z = 0$ e assume valore $\frac{72}{1000}$ per $y = 0$. Segue la tesi. □

Teorema 6.4.5. *Preso p un numero primo, si ha*

$$f(p^m) \leq p^{\frac{2}{27}m^3 + O(m^{\frac{5}{2}})}.$$

Dimostrazione. Siamo nelle ipotesi di avere un numero primo p e un intero m che sia fissato. Dal teorema 6.3.1 sappiamo che la classe di isomorfismo del gruppo G di ordine p^m è determinata da $c, s, r_i, a(i, j), b(i, j, u, v), c(i, j, k, u, v)$. Dando una limitazione superiore alla quantità di questi numeri interi si ottiene una stima dall'alto per numero di classi di isomorfismo di G. Sarà interessante vedere che quello che richiede più lavoro è $c(i, j, k, u, v)$, perché per gli altri interi non ci sono molte possibilità di scelta.

La somma $\sigma = r_1 + \cdots + r_c$ è compresa tra 1 e m, estremi inclusi. Con questa definizione otteniamo con gli r_i una partizione di σ in c parti. Una volta fissata σ, ci sono quindi al più $2^{\sigma-1}$ scelte per $c, r_1, \ldots, r_c$, ovvero tante quante le partizioni ordinate di σ, contate nel lemma 6.4.1. Siccome $\sigma \in \{1, \ldots, m\}$, ci sono al più $\sum_{\sigma=1}^{m} 2^{\sigma-1} \leq 2^m$ scelte per c e per $r_1, \ldots, r_c$.

Gli interi $d_2 - d_1, \ldots, d_s - d_{s-1}$ formano una partizione ordinata di r_2, in quanto i d_i sono strettamente crescenti al crescere di i. Ricordando che $d_0 = d_1 = 0$, gli interi d_i e s sono determinati da questa partizione ordinata di r_2. Utilizzando ancora il lemma 6.4.1 scopriamo così che le scelte per s e per $d_0, \ldots, d_s$ sono al più $2^{r_2-1} \leq 2^{m-1}$.

Gli interi $a(i,j)$ sono positivi e la loro somma è m, quindi sono al più il numero di partizioni ordinate di m che, sempre tornando al lemma 6.4.1, è 2^{m-1}.

Si ha poi $0 \leq b(i,j,u,v) < p^{a(u,v)}$: ci sono al più $p^{a(u,v)}$ scelte per $b(i,j,u,v)$. Una volta fissati i e j vale la seguente stima per il numero di scelte dei $b(i,j,u,v)$:

$$\prod_{u=i}^{c} \prod_{v=1}^{r_u} p^{a(u,v)} = p^{\sum_{u=i}^{c} \sum_{v=1}^{r_u} a(u,v)} \leq p^{\sum_{u=1}^{c} \sum_{v=1}^{r_u} a(u,v)} = p^m.$$

Per gli interi i ci sono al più m scelte e una volta fissato i ci sono r_i possibili j. Avendo $\sum_{i=1}^{c} r_i \leq m$, ci sono al più p^{m^2} scelte per gli interi $b(i,j,u,v)$. Finora possiamo dunque affermare che le possibili scelte per gli interi che definiscono la classe di isomorfismo di G esclusi i $c(i,j,k,u,v)$ sono al più

$$2^m 2^{m-1} 2^{m-1} p^{m^2} << p^{O(m^{5/2})}.$$

Ora supponiamo di fissare c, s, r_i, $a(i,j)$, $b(i,j,u,v)$: vediamo quante sono le scelte rimaste per $c(i,j,k,u,v)$.

Bisogna scegliere gli interi $c(i,j,k,u,v)$ in tre casi distinti: quando $i = 1$ e $1 \leq j < k \leq r_1$; quando $i = 2$, $1 \leq k \leq s$ e $d_{k-1} < j \leq r_2$; quando $3 \leq i \leq c$, $1 \leq j \leq r_i$ e $1 \leq k \leq s$. In tutti tre i casi si ha $i < u \leq c$, $1 \leq v \leq r_u$ e $0 \leq c(i,j,k,u,v) \leq p^{a(u,v)} - 1$. Gli interi $c(1,j,k,2,v) \mod p$ determinano la mappa $[,] : V \times V \to W$ che ritrovate definita e discussa nella sezione 6.2. Si possono quindi considerare gli interi $c(i,j,k,2,v)$ imponendo la condizione che s sia la minima dimensione per un sottospazio $U \leq V$ tale che $[U,U] = W$.

Con la notazione della proposizione 6.2.4, si può scrivere che ci sono $p^{N_p(r_1,r_2,s)}$ scelte per una mappa $[,] : V \times V \to W$ tale che s sia la minima dimensione di $U \leq V$ con $[U,U] = V$. Una volta scelta una di queste mappe, gli interi $c(1,j,k,2,v) \mod p$ sono determinati. Segue che, siccome ci sono al più $\binom{r_1}{2}$ scelte per j e k, il numero di possibili interi $c(1,j,k,2,v)$ è al più

$$p^{N_p(r_1,r_2,s)} \prod_{j=1}^{r_1} \prod_{k=j+1}^{r_1} \prod_{v=1}^{r_2} p^{a(2,v)-1} = p^{N_p(r_1,r_2,s)+\binom{r_1}{2}((\sum_{v=1}^{r_2} a(2,v))-r_2)}. \tag{6.9}$$

Per un ragionamento simile, quando $u \geq 3$ i possibili interi $c(1,j,k,u,v)$ sono al più

$$\prod_{j=1}^{r_1} \prod_{k=j+1}^{r_1} \prod_{u=3}^{c} \prod_{v=1}^{r_u} p^{a(u,v)} = p^{\binom{r_1}{2} \sum_{u=3}^{c} \sum_{v=1}^{r_u} a(u,v)}. \tag{6.10}$$

Mettendo assieme 6.9 e 6.10 appena scritte e l'osservazione $\sum_{u=2}^{c}\sum_{v=1}^{r_u} a(2,v) \leq m - r_1$ (ricavata dalle considerazioni dopo le definizioni (6.5)), si trova una limitazione superiore per $c(1,j,k,u,v)$:

$$p^{N_p(r_1,r_2,s)+\binom{r_1}{2}((\sum_{u=2}^{c}\sum_{v=1}^{r_u} a(u,v))-r_2)} \leq p^{N_p(r_1,r_2,s)+\binom{r_1}{2}(m-r_1-r_2)}.$$

Procediamo dando un numero massimo di scelte per $c(i,j,k,u,v)$ quando $i > 1$. Se i, j e k sono fissati, gli interi $c(i,j,k,u,v)$ sono al più

$$\prod_{u=i+1}^{c}\prod_{v=1}^{r_u} p^{a(u,v)} \leq p^{m-r_1-\cdots-r_i}.$$

Per $i \geq 3$ ci sono sr_i scelte per j e k quindi in particolare $p^{sr_i(m-r_1-\cdots-r_i)}$ possibili $c(i,j,k,u,v)$. Prendendo invece $i = 2$, ci sono $r_2 - d_{k-1}$ possibili scelte per j una volta che fissiamo k. Dato che $d_1, \ldots, d_s$ è una successione strettamente crescente e non negativa, per ogni $k \geq 2$ si avrà $d_{k-1} \geq k-2$. Ricordando che $d_0 = 0$, si trova che le scelte per j e k sono

$$\begin{aligned} sr_2 - \sum_{k=1}^{s} d_{k-1} &= sr_2 - \sum_{k=2}^{s} d_{k-1} \\ &\leq sr_2 - \sum_{k=2}^{s}(k-2) = sr_2 - \binom{s-1}{2}. \end{aligned}$$

Deduciamo che i possibili interi $c(2,j,k,u,v)$ sono al più $p^{(sr_2-\binom{s-1}{2})(m-r_1-r_2)}$. Il riassunto di queste considerazioni per le varie casistiche di i è che ci sono al più p^M interi $c(i,j,k,u,v)$, dove M è l'intero definito come

$$\begin{aligned} M = N_p(r_1,r_2,s) &+ \binom{r_1}{2}(m-r_1-r_2)+ \\ &+ (sr_2 - \binom{s-1}{2})(m-r_1-r_2)+ \\ &+ \sum_{i=3}^{c} sr_i(m-r_1-\cdots-r_i). \end{aligned}$$

Si nota che vale $r_i(m-r_1-\cdots-r_i) \leq \sum_{j=1}^{r_i} m-r_1-\cdots-r_{i-1}-j$, quindi

$$\begin{aligned} \sum_{i=3}^{c} sr_i(m-r_1-\cdots-r_i) &\leq s\sum_{i=3}^{c}\sum_{j=1}^{r_i}(m-r_1-\cdots-r_{i-1}-j) \\ &= s\sum_{k=1}^{r_3+\cdots+r_c}(m-r_1-r_2-k) \\ &\leq s\sum_{k=1}^{m-r_1-r_2}(m-r_1-r_2-k) \\ &= s\binom{m-r_1-r_2}{2}. \end{aligned}$$

Per limitare dall'alto M utilizzando questa stima scriviamo che

$$M \leq N_p(r_1, r_2, s) + \frac{1}{2}r_1^2(m - r_1 - r_2) + \tag{6.11}$$

$$+ \big((s-1)r_2 - \frac{1}{2}(s-1)^2\big)(m - r_1 - r_2) + \tag{6.12}$$

$$+ \frac{1}{2}(s-1)(s - r_1 - r_2)^2 + O(m^2). \tag{6.13}$$

Dobbiamo lavorare ancora sulla stima di M. Distinguiamo due casi. Prima consideriamo $r_1 \geq \frac{6}{10}m$: dalla stima (6.2) si ha

$$M \leq \frac{1}{2}r_1^2(m - r_1 - (s-1)) + \frac{1}{2}r_1 r_2(s-1) +$$
$$+ \big((s-1)r_2 - \frac{1}{2}(s-1)^2\big)(m - r_1 - r_2) +$$
$$+ \frac{1}{2}(s-1)(m - r_1 - r_2)^2 + O(m^{5/2}).$$

Per quanto dimostrato nel lemma 6.4.3, definite le variabili

$$x = \frac{r_1}{m}, y = \frac{r_2}{m}, z = \frac{m - r_1 - r_2}{m}, u = \frac{s-1}{m},$$

la funzione

$$A(x, y, z, u) = \frac{1}{2}x^2(z + y - u) + \frac{1}{2}xyu + \big(uy - \frac{1}{2}u^2\big)z + \frac{1}{2}uz^2,$$

assume massimo valore $\frac{2}{27}$ quando prendiamo x, y, z, u non negativi soggetti ai vincoli $x + y + x = 1$, $u \leq y$ e $x \geq \frac{6}{10}$.

Ci rimane la valutazione del caso $r_1 \leq \frac{6}{10}m$. Dalle stime (6.1) e (6.11) otteniamo che

$$M \leq \frac{1}{2}r_1^2(m - r_1 - (s-1)) +$$
$$+ \big((s-1)r_2 - \frac{1}{2}(s-1)^2\big)(m - r_1 - r_2) +$$
$$+ \frac{1}{2}(s-1)(m - r_1 - r_2)^2 + O(m^{8/3}).$$

Con le stesse definizioni di prima per x, y, z, u, consideriamo la funzione

$$B(x, y, z, u) = \frac{1}{2}x^2(z + y - u) + (uy - \frac{1}{2}u^2)z + \frac{1}{2}uz^2.$$

Come dimostrato nel lemma 6.4.4 sulla regione delle $x, y, z, u \geq 0$ vincolate a $x+y+z = 1$, $u \leq \min(x, y)$ e $x \leq \frac{6}{10}$, la funzione $B(x, y, z, u)$ assume valore massimo μ strettamente inferiore a $\frac{2}{27}$. Possiamo dire che allora $M \leq \mu m^3 + O(m^{8/3}) \leq \frac{2}{27}m^3 + O(m^{5/2})$. Tirando le fila: per qualsiasi valore di r_1 abbiamo mostrato che $M \leq \frac{2}{27}m^3 + O(m^{5/2})$, da cui

$$f(p^m) \leq p^{\frac{2}{27}m^3 + O(m^{\frac{5}{2}})}.$$

□

Capitolo 7

Sincronia delle limitazioni

Teorema 7.1. *Preso p un numero primo abbiamo che*

$$f(p^m) = p^{\frac{2}{27}m^3+O(m^{\frac{5}{2}})}.$$

Dimostrazione. La limitazione dal basso di Graham Higman e la limitazione dell'alto di Charles Sims assicurano che

$$p^{\frac{2}{27}m^2(m-6)} \leq f(p^m) \leq p^{\frac{2}{27}m^3+O(m^{\frac{5}{2}})}.$$

Questo basta a concludere. □

Parte II

Gruppi di ordine n

Capitolo 8

Architettura dei gruppi finiti

Arrivata a mostrare la conclusione migliore a cui la ricerca ha portato per la stima del numero di gruppi di ordine p^n, vorrei fornire una panoramica riguardo al lavoro di Lázló Pyber, che non ha voluto restringere le sue stime alle sole potenze di primi. Cosa si riesce a dire per un generico n naturale scelto come cardinalità del gruppo? Come ci si può approciare al problema?

Passare dal caso particolare delle cardinalità che siano potenze di primo ad un generico n naturale è un salto che richiede la conoscenza di ulteriori tecniche di teoria dei gruppi. Se fin qui abbiamo camminato in salita per giungere ai risultati desiderati, ora dobbiamo armarci di funi e caschetto per arrampicarci in ferrata. Non svilupperò tutti i prerequisiti necessari alla dimostrazione di Pyber, ma cercherò comunque di restituire l'idea della ramificazione teorica sottostante il risultato.

Il lessico di "architettura di un gruppo finito" induce una certa ammirazione per la materia, suggerendo l'associazione di un'immagine a qualcosa che non è grafico per natura. Nella pratica è qualcosa di meno artistico: un approccio alla teoria di estrema potenzialità. La parola "architettura" chiarisce la modalità con cui la struttura dei gruppi finiti possa essere descritta da certi loro sottogruppi caratteristici dalla struttura più semplice. Un sottogruppo $H \leq G$ è caratteristico quando $\Phi(H) = H$ per ogni Φ automorfismo di G. In questo senso la conoscenza delle componenti costruttive ci permette di avere coscienza di cosa sia possibile edificare coi mezzi che abbiamo, ma anche, nel processo inverso, solida interpretazione del risultato finale oltre che un punto di partenza per iniziare a studiare il gruppo in questione. Questo approccio alla teoria dei gruppi si riconosce molto bene nella dimostrazione del teorema di Pyber. Iniziamo, come anticipato, dal dare delle nozioni preliminari. In particolare quelle di sottogruppo di Fitting e di Fitting generalizzato saranno, ora posso dirvelo, i nostri materiali di costruzione.

8.1 Fitting e Fitting generalizzato

Sia G un gruppo finito, e siano P e Q due p-gruppi che siano suoi sottogruppi normali. Allora PQ è un sottogruppo normale di G ed è anch'esso un p-gruppo. Se P e Q sono sottogruppi normali di G massimali rispetto all'essere p-gruppi, allora $P = Q = PQ$. Esiste

quindi un solo sottogruppo normale massimale di G che sia p-gruppo, che indicheremo con $O_p(G)$. Faccio notare che nel caso in cui G sia un p-gruppo si ha proprio che $O_p(G) = G$.

Definizione 8.1.1. *Sia G un gruppo finito. Con la notazione appena introdotta per $O_p(G)$, il sottogruppo Fitting di G è*

$$F(G) = \langle O_p(G) | p \text{ primo} \rangle.$$

Se p e q sono due primi distinti allora

$$[O_p(G), O_q(G)] \leq O_p(G) \cap O_q(G) = \{1\}.$$

Da questa osservazione segue che

$$F(G) = O_{p_1}(G) \times \cdots \times O_{p_k}(G)$$

dove $|G| = p_1^{a_1} \dots p_k^{a_k}$. Siccome $F(G)$ si può scrivere così, è nilpotente.

Teorema 8.1.2. *Per ogni gruppo finito G, il sottogruppo Fitting $F(G)$ è il sottogruppo nilpotente normale massimale per G.*

Teorema 8.1.3. *Dato un gruppo G finito si ha che $F(G/\Phi(G)) = F(G)/\Phi(G)$.*

Teorema 8.1.4. *Dato un gruppo finito e risolubile G, si che $C_G(F(G)) = Z(F(G))$.*

Per la dimostrazione del teorema di Pyber serve utilizzare il Fitting generalizzato, che estende la nozione ai gruppi non risolubili. Infatti, se prendiamo un gruppo G tale che $C_G(F(G))$ non sia contenuto in $F(G)$, allora $C_G(F(G))/Z(F(G))$ contiene un sottogruppo normale minimale non identico che è semplice ma non per forza abeliano (ricordo che il più piccolo esempio di gruppo semplice non abeliano è A_5, fondamentale in Teoria di Galois). Per introdurre il Fitting generalizzato è necessario conoscere i gruppi quasisemplici.

Definizione 8.1.5. *Un sottogruppo H di G è subnormale in G se e solo se esiste una catena di sottogruppi $G = H_1 > \cdots > H_k = H$ dove H_{i+1} è normale in H_i per ogni $i \in \{1, \dots, k-1\}$.*

Definizione 8.1.1. *Un gruppo G si dice essere quasi semplice se e solo se è perfetto (è perfetto quando coincide con il suo derivato G') e $G/Z(G)$ è isomorfo a un gruppo semplice.*

Definizione 8.1.6. *Un sottogruppo $C \leq G$ è detto una componente di G se è subnormale in G e quasisemplice. L'insieme delle componenti di un gruppo G si indica con $Comp(G)$, e si definisce inoltre $E(G) = \langle Comp(G) \rangle$ il sottogruppo di Bender di G.*

Definizione 8.1.7. *Coerentemente con le notazioni introdotte, il Fitting generalizzato di un gruppo finito G è il gruppo $F^*(G) = F(G)E(G)$.*

Proposizione 8.1.8. *Se G è un gruppo finito allora $Z(F(G)) = Z(F^*(G))$.*

Proposizione 8.1.9. *Se G è un gruppo finito allora $C_G(F^*(G)) = Z(F(G))$.*

8.2 A-gruppi

Definizione 8.2.1. *Dato un gruppo G questo è un A-gruppo se e solo se tutti i suoi sottogruppi nilpotenti sono abeliani.*

Enumerare gli A-gruppi finiti introduce la modalità di enumerazione per generici gruppi finiti. Si può dimostrare che se un gruppo è finito allora è un A-gruppo se e solo se i suoi sottogruppi di Sylow sono abeliani.

Lemma 8.2.2. *Sia G un gruppo di ordine $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Se M è un sottogruppo massimale risolubile di $A_i = Aut(O_{p_i}(G))$ e $|M| = p_i^{m_i} x_i$ con p_i che non divide x_i, allora $x_i \leq p_i^{3\alpha_i}$.*

Lemma 8.2.3. *Sia G un gruppo di ordine $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Siano poi $A_0 = E(G)$ e $A^* = A_0 \times A$, dove $A = Aut(F(G))$. Allora:*

1. *$|A^*| \leq n^{2\mu+1}$, con $\mu = \max\{\alpha_1, \dots, \alpha_k\}$;*
2. *se S è un sottogruppo risolubile di A_0, allora $|S| \leq n^3$;*
3. *ci sono al più $n^{\frac{41}{4}\mu + \frac{25}{2}}$ sottogruppi risolubili di A_0;*
4. *il numero di $|Mss(A^*)|$ di sottogruppi risolubili massimali di A^* è al più $n^{\frac{45}{4}\mu + 278\,847}$.*

Risulta necessario dare la definizione di estensione di gruppo. A onor dal vero per l'enumerazione degli A-gruppi sarebbe meglio conoscere la corrispondenza tra estensioni di gruppi e il secondo gruppo di comologia, ma per la consistente dimensione dell'argomento in rapporto alla sua marginalità in questa tesi preferisco procedere oltre.

8.3 Estensioni di gruppi

Definizione 8.3.1. *Sia E un gruppo e sia M un suo sottogruppo normale. L'estensione E di M tramite G è per definizione il quoziente $G = E/M$. C'è quindi la sequenza di mappe:*

$$1 \to M \to E \to G \to 1.$$

Definizione 8.3.2. *Due estensioni E ed E' sono dette equivalenti se esiste un omomorfismo $\Phi : E \to E'$ che renda commutativo il diagramma*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Capitolo 9

Caso dei gruppi risolubili

Prima di stimare dall'alto il numero di classi di isomorfismo per un gruppo G qualsiasi di ordine fissato n, è bene studiare quel che si può concludere con l'ipotesi aggiuntiva di risolubilità del gruppo. Questo non dovrebbe stupirci visto che ho già sottolineato come l'introduzione del Fitting generalizzato sia proprio legato alla gestione dei casi di gruppi non risolubili.

Sia $\mathcal{S}$ una famiglia di gruppi, in cui ogni elemento sia di ordine primo. Per limitare dall'alto il numero classi di isomorfismo di gruppi risolubili di ordine $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, cerchiamo di dare una limitazione dall'alto al numero di gruppi risolubili di ordine n che abbiano sottogruppi di Sylow isomorfi a quelli nell'insieme $\mathcal{S}$. Ci servono i seguenti oggetti, alcuni già definiti in precedenza e altri che introduco ora. Per $i \in \{1, \dots, k\}$:

$$\begin{aligned}
\mu &= \max\{\alpha_1, \dots, \alpha_k\};\\
F_i &= O_{p_i}(G);\\
F &= F(G) = F_1 \times \cdots \times F_k;\\
A_i &= Aut(F_i);\\
A &= Aut(F) = A_1 \times \cdots \times A_k;\\
B_i &= \{\sigma \in A_i | \sigma g = g \mod \Phi(F_i) \textit{ per ogni } g \in F_i\}.
\end{aligned}$$

Per ogni i, c'è un omomorfismo da A_i in $Aut(F_i/\Phi(F_i))$, e si può dimostrare che il kernel B_i di questo omomorfismo è un p_i-gruppo. Definiamo $d_i = d(F_i) = d(F_i/\Phi(F_i))$. Per il lemma 3.4.4, $Aut(F_i/\Phi(F_i))$ è isomorfo a $GL(d_i, p_i)$ e quindi A_i/B_i può essere visto come sottogruppo di $GL(d_i, p_i)$. Definiamo $Z = Z(F)$ e $Z_i = Z \cap F_i$. Notiamo che Z_i è il sottogruppo di Sylow di Z di ordine potenza di p_i. Siano poi $H = G/Z$ e $Q_i = P_i/Z_i$ dove P_i sono i p_i-sottogruppi di Sylow di G.

Lemma 9.1. *Con la notazione appena introdotta, supponiamo che Z e H siano dati. Il numero di gruppi G con sottogruppi di Sylow $P_1, \dots, P_k$ che sono estensioni di Z tramite H è al più $\prod_{i=1}^{k} p_i^{\alpha_i^2}$, ed è quindi al più n^{μ}.*

Il lemma appena enunciato si dimostra usando la corrispondenza tra estensioni e gruppi di comologia e in particolare fornendo stime all'ordine dei gruppi di comologia coinvolti. Siccome l'applicazione di questo risultato è di fondamentale importanza all'interno della dimostrazione del teorema di Pyber, da qui si capisce come davvero sia necessario

movimentare molte tecniche della teoria dei gruppi, tra cui quelle della coomologia, per ottenere un risultato generale sulla stima di gruppi di ordine n.

Teorema 9.2. *Il numero di gruppi risolubili di ordine n con sottogruppi di Sylow $P_1, \ldots, P_k$ è al più $n^{8\mu+278\,833}$, a meno di isomorfismo.*

Dimostrazione. Considerato che la dimostrazione di questo teorema ha iter dimostrativo che è poi ripreso nella dimostrazione del teorema di Pyber, mi sembra importante schematizzare i passaggi caratterizzanti. Il gruppo G di ordine $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ agisce per coniugazione sul Fitting F, quindi c'è un omomorfismo Φ da G in A, con $ker(\Phi) = C_G(F)$. Usando l'ipotesi di risolubilità di G, si può anche dire grazie al lemma 8.1.4 che $C_G(F) \leq F$. Quindi $\ker(\Phi) = Z$ e si può vedere il quoziente $H = G/Z$ come un sottogruppo di A. Il gruppo G è un'estensione di Z tramite H. A questo punto dobbiamo fidarci del seguente fatto: G è determinato da H, Z, dall'azione di H su Z, e da un elemento di $H^2_{\mathcal{S}}(H, Z)$, dove $H^2_{\mathcal{S}}(H, Z)$ è l'insieme delle classi di equivalenza delle estensioni di Z tramite G con sottogruppi di Sylow $P_1, \ldots, P_k$. In particolare l'azione di H su Z è determinata dall'azione di H su F e una volta scelto F si conoscono di conseguenza anche Z e A. Le scelte possibili per F si possono capire velocemente ricordando che i sottogruppi di Sylow di G sono isomorfi ai P_i. Bisogna poi valutare quali siano le possibilità per H come sottogruppo di A. Dato che H è risolubile, sarà di certo contenuto in un sottogruppo massimale $M \leq A$. Per questo motivo è conveniente fissare un sottogruppo massimale M e poi contare le possibili scelte di H come suo sottogruppo. Si conclude poi con il lemma 9.1. □

Capitolo 10

Limitazione di Pyber

Per studiare un generico gruppo G, senza in particolare l'ipotesi di risolubilità, la notazione assunta sarà in coerente continuità con il capitolo 9. Fissiamo i sottogruppi di Sylow P_i di G di ordine p_i rispettivamente, dove $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Poi, per $i \in \{1, \dots, k\}$:

$$\begin{aligned} F_i &= O_{p_i}(G); \\ A_i &= Aut(F_i); \\ A &= Aut(F) = A_1 \times \cdots \times A_k; \\ A_0 &= Aut(E(G)); \\ A^* &= A_0 \times A. \end{aligned}$$

Il teorema di Pyber ha una dimostrazione che si articola in tre parti. Si prende l'ordine n di un gruppo e si scompone in potenze di fattori primi affinché siano chiari gli ordini dei p_i-Sylow del gruppo G. Quello che si cerca infatti è una limitazione superiore per un gruppo G che abbia determinati sottogruppi di Sylow. Inizialmente si conta il numero di scelte possibili per il Fitting generalizzato $F^*(G)$. Dopodiché si considera che il gruppo quoziente $G/Z(F(^*(G)))$ è un sottogruppo degli automorfismi del Fitting generalizzato. La naturale immersione di $Aut(F^*(G))$ in A^* fa vedere $G/Z(F^*(G))$ come sottogruppo di A^*. Data una limitazione dall'alto per il numero di tali possibili sottogruppi, si passa alla stima generale della tesi del teorema tramite il lemma 9.1. Vediamo tutto questo con maggior dettaglio tecnico.

Teorema di Pyber 10.1. *Il numero di gruppi G di ordine n, a meno di classi di isomorfismo, con gruppi di Sylow $P_1, \dots, P_k$ è al più $n^{\frac{97}{4}\mu + 278\,852}$.*

Dimostrazione. Proviamo intanto che ci sono al più $n^{2\mu+3}$ scelte per $F^*(G)$, a meno di isomorfismo. Per $n \leq 3$ è chiaro, perché per cardinalità del gruppo pari 1, 2 o 3 il Fitting generalizzato del gruppo coincide con il gruppo stesso ed esiste una sola classe di isomorfismo per tutte tre le cardinalità. Continuiamo quindi la dimostrazione prendendo $n \geq 4$. Siano $Comp(G) = \{C_1, \dots, C_t\}$ le componenti di G e $L_i = C_i/Z(C_i)$ per ogni $i \in \{1, \dots, t\}$. Si può dimostrare che $\prod_{i=1}^{t} |L_i|$ divide n e quindi $(|L_1|, \dots, |L_t|)$ è un partizione moltiplicativa di un divisore r di n. Per ogni r ci sono al più r^2 sue possibili

partizioni moltiplicative, e quindi il numero di scelte per t e per gli interi $|L_i|$ è limitato dall'alto da

$$\sum_{r|n} r^2 = \sum_{r|n} \left(\frac{n}{r}\right)^2 \leq n^2 \sum_{r=1}^{\infty} \frac{1}{r^2} < 2n^2.$$

La Classificazione (Classificazione dei gruppi semplici finiti, anche detto "Teorema enorme") ci assicura che esistono al più due gruppi semplici di ordine dato, e dunque ci sono al più 2^t scelte per le classi di isomorfismo dei gruppi L_i, una volta fissati i loro ordini. Un risultato che non riporto fornisce la stima $t \leq \mu/2$, da cui $2^t \leq 2^{\frac{1}{2}\mu} \leq 2^{\frac{1}{2}\log n} = \sqrt{n}$. Pertanto il numero di possibili classi di isomorfismo per i gruppi L_i è al più n^3, dato che $2n^2\sqrt{n} \leq n^3$.

Il fatto che ci siano al più n^μ possibili classi di isomorfismo di $F(G)$ si può dedurre dalla dimostrazione del teorema 9.2 che ho enunciato precedentemente. Sappiamo che il Fitting $F(G)$ è un prodotto diretto dei suoi sottogruppi di Sylow F_i di ordine p_i. Ogni F_i è isomorfo ad un sottogruppo di P_i. Ma $|P_i| = p_i^{\alpha_i}$, quindi ogni P_i ha al più $(p_i^{\alpha_i})^{\alpha_i} \leq (p_i^{\alpha_i})^\mu$ sottogruppi. Ci sono al più $\prod_{i=1}^k (p_i^{\alpha_i})^\mu = n^\mu$ possibilità per $F(G)$. Nel scegliere F_i come sottogruppo normale di P_i, determiniamo l'azione di P_i su F_i tramite coniugazione.

È necessaria una piccola digressione. G è il prodotto centrale dei suoi sottogruppi $H_1, \ldots, H_k$ se e solo se è generato dagli H_i, con $[H_i, H_j] = \{1\}$ per ogni i e j distinti tra 1 e k. Se definiamo $X = \prod_{i=1}^k H_i$, si può far vedere che G è un prodotto centrale di H_i se e solo se è isomorfo a un quoziente X/K dove $K \leq Z(X)$ che abbia intersezione banale con tutti i k fattori del prodotto diretto X. Si può dimostrare che ci sono al più $n^{\mu+3}$ possibili classi di isomorfismo per X. Per trovare la stima desiderata su $F^*(G)$, serve mostrare che ci sono al più n^μ scelte per K. Intanto, accettiamo (senza provarlo) che $|Z(L_i)|$ divide $|L_i|$. Siccome $|Z(F(G))|$ divide $|F(G)|$ e $Z(X) = Z(L_i) \times \cdots \times Z(L_t) \times Z(F(G))$, di certo $|Z(G)|$ divide n. Sappiamo che K è un sottogruppo del centro $Z(G)$, ed è quindi abeliano e di ordine che divide n: il gruppo K può essere generato da μ elementi. Ci sono quindi al più n^μ scelte per K, dato che $|Z(G)| \leq n$. Mettiamo insieme quanto sappiamo: ci sono al più n^μ classi di isomorfismo di $F(G)$, al più n^3 classi di isomorfismo dei gruppi L_i, e al più n^μ scelte per K. Segue che ci sono al più $n^{2\mu+3}$ scelte per il Fitting generalizzato $F^*(G)$, che era quanto volevamo dimostrare.

Sia $Z = Z(F^*(G))$. La proposizione 8.1.9 assicura che la coniugazione induce un'immersione di G/Z nel gruppo $Aut(F^*(G))$. Inoltre c'è un'altra immersione, questa naturale, di $Aut(F^*(G))$ in A^*. Esiste quindi una mappa $\Phi : G \to A^*$ tale che $\ker \Phi = Z$. La seconda parte della dimostrazione del teorema di Pyber si occupa di contare quante sono le possibili immagini $\Phi(G)$. Chiamo $H = \Phi(G)$. Si può dimostrare che dato un gruppo finito T esistono un suo sottogruppo risolubile S e un suo elemento $x \in T$ tali che T sia generato da S e da xSx^{-1}. Possiamo applicare questo risultato al gruppo H, quindi $H = \langle S, xSx^{-1} \rangle$ per qualche $S \leq H$ e $x \in H$. Dal primo punto del lemma 8.2.3 sappiamo che ci sono al più $n^{2\mu+1}$ possibili x, mentre dal quarto punto dello stesso lemma ricaviamo che ci son al più $n^{\frac{45}{4}\mu+278\,847}$ possibili sottogruppi risolubili massimali M che contengono S. Ora supponiamo di fissare un certo sottogruppo risolubile massimale M, e cerchiamo di capire quanti sottogruppi S può contenere al massimo. Sia $Q_1, \ldots, Q_k$ un sistema di Sylow per S. Con l'eventuale sostituzione del sottogruppo P_i con un suo coniugato, si può supporre che $Q_i \leq \Phi(P_i)$ per $i \in \{1, \ldots, k\}$. Si può dimostrare, e qui lo prenderò per

vero, che c'è una parte del sistema di Sylow $R_1, \dots, R_k$ per M tale che $Q_i = S \cap R_i$ per $i \in \{1, \dots, k\}$, e che ci sono $|M|$ possibilità per R_i. Ricordo che $|M| \leq |A^*| = n^{2\mu+1}$ e poi $A^* = A_0 \times \cdots \times A_k$. Per $j \in \{0, \dots, k\}$, prendiamo $\pi_j : A^* \to A_j$ la mappa naturale. Ora $M = M_0 \times \cdots \times M_k$, dove intendo $M_j = \pi_j(M)$. In particolare ogni M_j è sottogruppo risolubile massimale del rispettivo A_j. Per ogni $i \in \{1, \dots, k\}$, definisco

$$R_i = R_{i0} \times \cdots \times R_{ik},$$

dove $R_{ij} = \pi_j(R_i)$. Si ha quindi che R_{ij} è un p_i-sottogruppo di Sylow di M_j e che $\pi_j(Q_i) = \pi_j(S) \cap \pi_j(R_i) \leq R_{ij}$.

Prendiamo adesso un sistema di sottogruppi M e diamo la definizione di quasi-sistema di Sylow $T_1, \dots, T_k$ di M come di seguito. Chiamo $\Phi_i = \pi_i \circ \Phi$, che è la mappa da G in $Aut(F_i)$ indotta dalla coniugazione. Dato che $Q_i \leq \Phi(P_i)$, si ha che $\pi_i(Q_i) \leq \Phi_i(P_i)$. Per $i \in \{1, \dots, k\}$ e $j \in \{0, \dots, k\}$, definisco

$$T_{ij} = \begin{cases} R_{ij} & \text{se } i \neq j \\ \Phi_i(P_i) & \text{altrimenti.} \end{cases}$$

Il metodo utilizzato prima per contare i possbili $F^*(G)$ ha anche determinato l'azione di P_i sugli F_i, quindi possiamo considerare di conoscere $\Phi_i(P_i)$ per ogni $i \in \{1, \dots, k\}$: i sottogruppi T_{ij} sono determinati dal sistema di Sylow di M, una volta fissato M. Faccio notare che $T_i = T_{i0} \times \cdots \times T_{ik}$ è un p_i-gruppo, e che $Q_i \leq T_i$. Per ogni $j \in \{1, \dots, k\}$, definisco

$$X_j = \prod_{\substack{i=1 \\ i \neq j}}^{k} R_{ij}.$$

Siccome i sottogruppi R_i formano parte del quasi-sistema di Sylow di M, abbiamo che $R_{ij}R_{i'j'} = R_{i'j'}R_{ij}$ e quindi X_j è ben definito ed è un p_j-sottogruppo risolubile di A_j. Per il lemma 8.2.2 possiamo dire che $|X_j| \leq p_j^{3\alpha_j}$. Pertanto ho che

$$\begin{aligned} \prod_{i=1}^{k} |T_i| &= \prod_{i=1}^{k} |X_i| \prod_{i=1}^{k} |T_{ii}| \prod_{i=1}^{k} |T_{i0}| \\ &\leq \prod_{i=1}^{k} p_i^{3\alpha_i} \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k} |T_{i0} \\ &= n^4 \prod_{i=1}^{k} |T_{i0}| \\ &\leq n^4 |M_0| \\ &\leq n^7. \end{aligned}$$

Nell'introdurre $|M_0|$ nella stima si è dovuto usare il secondo risultato del teorema 8.2.3. Ora, ricordando che i $Q_i \leq T_i$, e che è generato da al più α_i elementi, ricaviamo che il numero di possibili Q_i, una volta fissato T_i, è al più $|T_i|^{\alpha_i}$. Siccome poi

$$\prod_{i=1}^{k} |T_i|^{\alpha_i} \leq \prod_{i=1}^{k} |T_i|^{\mu} \leq n^{7\mu},$$

ci sono al massimo $n^{7\mu}$ possibilità per i Q_i una volta che i T_i sono fissati.

Faccio un breve excursus di quello che abbiamo guadagnato fin qui. Sappiamo che $\Phi(G)$ è determinato da un sottogruppo risolubile S e da un elemento $x \in \Phi(G)$. Ci sono al più $n^{2\mu+1}$ scelte per x, al più $n^{\frac{45}{4}\mu+278\,847}$ scelte per M, al più $n^{2\mu+1}$ scelte per un sistema di Sylow R_i di M. È determinato il quasi-sistema di Sylow T_i. Ci sono al più $n^{7\mu}$ possibili Q_i, e quindi S è determinato. Una volta fissato il Fitting generalizzato $F^*(G)$, ci sono al più $n^{\frac{89}{4}\mu+278\,849}$ possibilità per $\Phi(G)$. Così si conclude la seconda parte della dimostrazione.

È il momento di richiamare il lemma 9.1. Sappiamo infatti che G è un'estensione di Z tramite G/Z. Una volta fissato il Fitting generalizzato, è completamente determinata la classe di isomorfismo di Z. Inoltre, una volta fissato $\Phi(G)$, la classe di isomorfismo di G/Z è determinata, come anche l'azione di G/Z su Z. Siamo dunque nelle condizioni di applicare il lemma 9.1 per concludere che ci sono al più n^{μ} scelte per G una volta che $F^*(G)$ e $\Phi(G)$ sono fissati. Per le stime dimostrate sulle possibili scelte di questi due oggetti, si conclude che le possibili classi di isomorfismo per G sono al più

$$n^{\frac{89}{4}\mu+278\,849} n^{2\mu+4} = n^{\frac{97}{4}\mu+278\,852}.$$

□

Ringraziamenti

I ringraziamenti da scrivere alla fine della tesi sono nella lista dei pensieri carichi di emotività a cui ci si dedica la sera per addormentarsi con l'idillica immagine di poter sorridere indossando la corona d'alloro a chi ha creduto in te più di quanto non riuscissi tu. Io non ho paura di parlare d'amore. Non voglio fare nomi in questi ringraziamenti: lo sai che ci sei, tra queste righe, te l'ho detto.

Bibliografia

[1] S.R. Blackburn, P.M. Neumann e G.Venkataraman. *Enumeration of finite groups*. Vol. 173. Cambridge tracts in Mathematics. Cambridge University Press, 2007.

[2] G. Higman. «Enumerating p-groups. I: inequalities». In: *Proceedings of the London Mathematical Society* 10 (1960), pp. 24–30.

[3] M. Isaacs. *Finite group theory*. Graduate Studies in Mathematics. American Mathematical Society, 2008.

[4] P.D. Lamberti, L. Provenzano e P. Toni. «Funghi matematici e Matematica come scienza semi-empirica». In: *Nuova Secondaria. Mensile di cultura, ricerca pedagogica e orientamenti didattici* (2021). URL: `https://www.edizionistudium.it/sites/default/files/sommario_444.pdf`.

[5] R. Monti. «Analisi Matematica 2B». In: 2022.

[6] L. Pyber. «Enumerating Finite Groups of Given Order». In: *The Annals of Mathematics* 137 (1993), pp. 203–220.

[7] L. Pyber. «Group Enumeration and Where It Leads Us». In: *Progress in Mathematics* 149 (1998), pp. 187–199.

[8] D.J.S. Robinson. *A course in the Theory of Groups*. Graduate Texts in Mathematics. Springer, 1996.