Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea in Matematica

Tesi di laurea

Applicazioni della teoria estremale dei grafi a problemi in teoria dei gruppi

Laureanda:
Jessica Anzanello
Matricola 1224775

Relatore:
Prof. Andrea Lucchini

Anno Accademico 2021–2022
23 Settembre 2022

Indice

0.1 Introduzione e risultati

Siano m, n due interi positivi e sia $\mathfrak{X}$ una classe di gruppi. Diciamo che un gruppo G soddisfa la condizione $\mathfrak{X}(m,n)$ se comunque si scelgano due sottoinsiemi di G, M e N, di cardinalità rispettivamente m e n, esistono $x \in M$ e $y \in N$ tali che $\langle x, y\rangle \in \mathfrak{X}$. Se G soddisfa la condizione $\mathfrak{X}(m,n)$, diciamo che $G \in \mathfrak{X}(m,n)$ o che G è un $\mathfrak{X}(m,n)$-gruppo.

Nel 2001, Bernard H. Neumann in [16] formulò la seguente domanda:

Quesito 1. *"Sia G un gruppo finito e supponiamo che comunque si scelgano un insieme M di m elementi e un insieme N di n elementi di G, almeno un elemento di M commuti con almeno un elemento di N. Quali relazioni tra* $|G|$*, m e n garantiscono che G sia abeliano?"*

Chiamiamo $\mathfrak{A}$ la classe dei gruppi abeliani. Utilizzando la proprietà sopra introdotta, possiamo riformulare la domanda di B. H. Neumann nel seguente modo: sia G un gruppo finito non abeliano tale che $G \in \mathfrak{A}(m,n)$, esiste un limite (dipendente solo da m e n) per l'ordine di G? Osserveremo che un gruppo infinito $G \in \mathfrak{A}(m,n)$ per qualche m e n è abeliano (si vedano i dettagli nella sezione 1.3). Pertanto, nel considerare gruppi non abeliani che soddisfano la condizione $\mathfrak{A}(m,n)$, ci interessano solo i casi finiti.

Una risposta parziale alla domanda in questione fu data da A. Abdollahi, A. Azad, A. Mohammadi Hassanabadi e M. Zarrin in [1] come segue. Sia G un $\mathfrak{A}(m,n)$-gruppo non abeliano, allora $|G| \leq c^{m+n} max\{m,n\}$, dove c è una costante che compare nel seguente teorema, dimostrato da Lacy Pyber nel 1987 [17]: se un gruppo finito G contiene al più n coppie di elementi che non commutano, allora $|G/Z(G)| \leq c^n$.

Un'elementare soluzione alternativa, con una migliore stima per l'ordine di G, è stata ottenuta da A. Lucchini come corollario del seguente teorema:

Teorema 1.1. *Sia* $\mathfrak{X}$ *una classe di gruppi e supponiamo che esista un reale positivo* γ *con la seguente proprietà: se* X *è un gruppo finito e la probabilità che due elementi di* X *scelti casualmente generino un gruppo in* $\mathfrak{X}$ *è maggiore di* γ*, allora* $X \in \mathfrak{X}$*. Se* $m \leq n$ *e* $G \in \mathfrak{X}(m,n) \setminus \mathfrak{X}$ *allora*

$$|G| \leq \left(\frac{2}{1-\gamma}\right)^m (n-1).$$

Corollario 1.1.1. *Se* $m \leq n$ *e* G *è un gruppo finito in* $\mathfrak{A}(m,n) \setminus \mathfrak{A}$*, allora*

$$|G| \leq \left(\frac{16}{3}\right)^m (n-1).$$

Obiettivo di questa tesi è anzitutto, nel primo capitolo, quello di illustrare questa risposta di A. Lucchini alla domanda di B. H. Neumann. Per fare questo, useremo un rilevante risultato di *teoria estremale dei grafi*, il teorema di Kővári-Sós-Turán, che afferma che se s e t sono due interi positivi, allora un grafo con n vertici e almeno $\frac{(t-1)^{\frac{1}{s}}n^{2-\frac{1}{s}}+(s-1)n}{2}$ archi contiene una copia del grafo completo bipartito $K_{s,t}$, e un famoso risultato di W. H. Gustafson, che asserisce che, in un gruppo finito non abeliano, la probabilità che due elementi commutino è al più 5/8. Continueremo questo capitolo osservando che un gruppo infinito $G \in \mathfrak{A}(m,n)$, per qualche m e n, è abeliano e concluderemo vedendo brevemente com'è possibile applicare il teorema 1.1 ad altre classi di gruppi, oltre a quella dei gruppi abeliani finiti, in particolare a ogni classe di gruppi chiusa per sottogruppi, gruppi quoziente ed estensioni.

Il secondo capitolo è dedicato alla dimostrazione del teorema di Kővári-Sós-Turán, che vedremo in tre versioni: per grafi non orientati, per grafi non orientati bipartiti e per grafi orientati. Quest'ultimo sarà utlizzato nel terzo capitolo, dove vedremo inoltre un risultato analogo, ma nel caso degli ipergrafi.

Nel terzo capitolo lavoreremo con *parole* invece che con *classi di gruppi* e inizieremo pertanto ricordando i concetti di parola e di gruppo libero. Definiremo una proprietà analoga a $\mathfrak{X}(m,n)$, che chiameremo $w(m,n)$, per parole in F_2 e vedremo che, essenzialmente con gli stessi argomenti, è possibile provare un risultato simile al teorema 1.1, ma che riguarda appunto parole (in F_2) in luogo di classi di gruppi, che fornisce, come corollario, un argomento alternativo per mostrare che la risposta alla domanda di Neumann è positiva e che può essere inoltre applicato alla *parola di 2-Engel* in luogo della parola *commutatore*. Lavoreremo sempre con parole che soddisfano un gap di probabilità, ovvero parole $w \in F_r$ tali per cui esiste una costante $\gamma_w < 1$ con la proprietà che, per ogni gruppo finito G, se la probabilità che $w(g_1,...,g_r) = 1$ in G è almeno γ_w, allora w è un'identità in G. Daremo quindi una generalizzazione della proprietà $w(m,n)$ per parole in F_r, dicendo che un gruppo G ha la proprietà w_t se comunque si scelgano r sottoinsiemi $X_1,...,X_r$ di G con $|X_1| = ... = |X_r| = t$, esiste $(g_1,...,g_r) \in X_1 \times ... \times X_r$ tale che $w(g_1,...,g_r) = 1$. Proveremo che se w soddisfa un gap di probabilità, allora per ogni intero positivo t esiste una costante c_t tale che se un gruppo finito G soddisfa la proprietà w_t, allora $|G| \leq c_t$ o w è un'identità in G. Applicheremo questo risultato ad alcune parole che sono naturali generalizzazioni del commutatore e in particolare questo ci permetterà di definire una proprietà per i gruppi metabeliani e una per i gruppi con classe di nilpotenza al più t. Concluderemo il capitolo con la dimostrazione di un risultato di Erfanian et al. che generalizza il teorema dei 5/8 di Gustafson.

Capitolo 1

Una domanda di B. H. Neumann

Quesito 1 (B. H. Neumann)**.** *Sia G un gruppo finito non abeliano tale che $G \in \mathfrak{A}(m,n)$. Esiste un limite (dipendente solo da m e n) per l'ordine di G?*

Obiettivo di questo capitolo è quello di provare il teorema 1.1, da cui, come corollario, ricaveremo una risposta alla domanda di B. H. Neumann in questione. Per fare questo, useremo il teorema di Kővári-Sós-Turán, rimandandone la dimostrazione al secondo capitolo, e dimostreremo il cosiddetto *teorema dei 5/8* di W. H. Gustafson. Nelle sezioni 1.1 e 1.2 indicheremo sempre con G un gruppo finito. Considereremo il caso dei gruppi infiniti nella sezione 1.3, osservando che se un gruppo infinito appartiene a $\mathfrak{A}(m,n)$ per qualche m e n, allora è abeliano. Concluderemo il capitolo considerando altre applicazioni del teorema 1.1.
Ci sono utili alcuni richiami sulle azioni di gruppo:

Definizione 1.1 (Azione di gruppo)**.** Siano G un gruppo finito e Ω un insieme finito non vuoto. Un'*azione* di G su Ω è una mappa

$$\circ : G \times \Omega \to \Omega; (g,\omega) \mapsto g \circ \omega,$$

tale che per ogni $\omega \in \Omega$ e per ogni $g, h \in G$:

- $1 \circ \omega = \omega$;
- $(gh) \circ \omega = g \circ (h \circ \omega)$.

Ad ogni azione possiamo associare un morfismo di gruppi $\gamma : G \to Sym(\Omega)$ che manda un elemento $g \in G$ nella permutazione $w \mapsto g \circ \omega$ di Ω.
L'insieme $G \circ \omega = \{g \circ \omega : g \in G\}$ è detto l'*orbita* di $\omega \in \Omega$. L'insieme $Stab_G(\omega) = \{g \in G : g \circ \omega = \omega\}$ è detto lo *stabilizzatore* di un elemento $\omega \in \Omega$ ed è legato alla cardinalità dell'orbita dalla seguente proprietà:

$$[G : Stab_G(\Omega)] = |G \circ \omega|.$$

L'azione di gruppo che useremo in questo capitolo è quella di *coniugio* di un gruppo G su se stesso: $g \circ x = gxg^{-1}$. In questo caso $Stab_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_G(x)$ è il *centralizzante* di x in G. Le orbite sono chiamate *classi di coniugio*. Ricordiamo infine che per l'azione di coniugio vale *l'equazione delle classi*: $|G| = |Z(G)| + |C_1| + ... + |C_t|$, dove $C_1, ..., C_t$ sono le classi di coniugio non banali.

1.1 Teorema di A. Lucchini per classi di gruppi

Definizione 1.2 (Grafo bipartito)**.** Un *grafo bipartito* $\Gamma = (U, V, E)$ consiste di due insiemi disgiunti di vertici U e V, e di un insieme E di archi, ciascuno dei quali collega un vertice di U con un vertice di V.

Definizione 1.3 (Grafo completo bipartito)**.** Un *grafo completo bipartito* è un grafo bipartito in cui $\forall u \in U$ e $\forall v \in V$ u e v sono collegati da un arco. Un grafo completo bipartito in cui U ha s vertici e V ha t vertici è denotato con $K_{s,t}$.

L'argomento centrale per provare il teorema1.1 è il seguente teorema (per la dimostrazione si veda il capitolo 2):

Teorema 2.3 (Kővári-Sós-Turán, 1954)**.** *Se s e t sono due interi positivi, allora un grafo con n vertici e almeno $\frac{(t-1)^{\frac{1}{s}} n^{2-\frac{1}{s}} + (s-1)n}{2}$ archi contiene una copia del grafo completo bipartito $K_{s,t}$.*

Teorema 1.1 (A. Lucchini, 2020 [9])**.** *Sia $\mathfrak{X}$ una classe di gruppi e supponiamo che esista un reale positivo γ con la seguente proprietà: se X è un gruppo finito e la probabilità che due elementi di X scelti casualmente generino un gruppo in $\mathfrak{X}$ è maggiore di γ, allora $X \in \mathfrak{X}$. Se $m \leq n$ e $G \in \mathfrak{X}(m, n) \setminus \mathfrak{X}$ allora*

$$|G| \leq \left(\frac{2}{1-\gamma}\right)^m (n-1).$$

Dimostrazione. Sia $G \in \mathfrak{X}(m, n) \setminus \mathfrak{X}$ un gruppo finito. Consideriamo il grafo $\Gamma_{\mathfrak{X}}(G)$ i cui vertici sono gli elementi di G e tale che due vertici x e y sono collegati da un arco se e solo se $\langle x, y\rangle \notin \mathfrak{X}$. Sia η il numero di archi di $\Gamma_{\mathfrak{X}}(G)$. Poiché $G \notin \mathfrak{X}$, allora la probabilità che due vertici di $\Gamma_{\mathfrak{X}}(G)$ siano collegati da un arco è almeno $1 - \gamma$. Quindi abbiamo

$$\eta \geq \frac{(1-\gamma)|G|^2}{2}. \tag{1.1}$$

Poiché $G \in \mathfrak{X}(m, n)$, $\Gamma_{\mathfrak{X}}(G)$ non può contenere il grafo completo bipartito $K_{m,n}$ come sottografo. Per il teorema di Kővári-Sós-Turán,

$$\eta \leq \frac{(n-1)^{1/m}|G|^{2-1/m} + (m-1)|G|}{2}. \tag{1.2}$$

Combinando 1.1 e 1.2 deduciamo che

$$1-\gamma \leq \left(\frac{n-1}{|G|}\right)^{1/m} + \frac{m-1}{|G|} \leq \left(\frac{n-1}{|G|}\right)^{1/m} + \frac{n-1}{|G|}. \tag{1.3}$$

Possiamo assumere $|G| \geq n-1$. Questo implica che $\left(\frac{n-1}{|G|}\right)^{1/m} \geq \frac{n-1}{|G|}$ e pertanto segue da 1.3 che

$$1-\gamma \leq 2\left(\frac{n-1}{|G|}\right)^{1/m}.$$

E quindi

$$|G| \leq \left(\frac{2}{1-\gamma}\right)^m (n-1).$$

□

Se $\mathfrak{X} = \mathfrak{A}$, possiamo stimare γ con il seguente risultato:

Teorema 1.2 (W. H. Gustafson, 1973 [7])**.** *Se G è un gruppo non abeliano finito, allora la probabilità che due elementi di G scelti casualmente commutino è al più $\frac{5}{8}$.*

Corollario 1.1.1 (A. Lucchini, 2022 [10])**.** *Se $m \leq n$ e G è un gruppo finito in $\mathfrak{A}(m,n) \setminus \mathfrak{A}$, allora*

$$|G| \leq \left(\frac{2}{1-\frac{5}{8}}\right)^m (n-1) = \left(\frac{16}{3}\right)^m (n-1).$$

1.2 Il teorema dei 5/8

In questa sezione proviamo il teorema di W. H. Gustafson 1.2 . È un elegante e in qualche modo sorprendente risultato quello che la probabilità che due elementi scelti casualmente commutino, in un gruppo finito non abeliano, non possa essere arbitrariamente vicina a 1. Per essere più precisi tale probabilità non può appartenere all'intervallo $(\frac{5}{8}, 1]$ e pertanto c'è un *gap* nei possibili valori di probabilità, concetto che approfondiremo nel capitolo 3. Cominciamo questa sezione con alcuni lemmi preliminari.

Sia G un gruppo finito. La probabilità $P(G)$ che due elementi di G scelti casualmente commutino è $|C|/|G|^2$, dove $C = \{(a,b) \in G \times G : ab = ba\}$. Vale il seguente

Lemma 1.3.

$$P(G) = \frac{K(G)}{|G|},$$

dove $K(G)$ è il numero di classi di coniugio di G.

Dimostrazione. Al fine di contare gli elementi di C, osserviamo che fissato un elemento $a \in G$, il numero di elementi di C della forma (a, b) è $|C_G(a)|$. Dunque abbiamo
$$|C| = \sum_{a \in G} |C_G(a)|.$$
Dette $C_1, ..., C_t$ le classi di coniugio di G, consideriamo $\forall i, x_i \in C_i$. Quindi $C_i = G \circ x_i$. Possiamo quindi banalmente scrivere
$$\sum_{a \in G} |C_G(a)| = \sum_{i=1}^{t} \sum_{a \in G \circ x_i} |C_G(a)|.$$
Se $a \in G \circ x_i$, allora $a = g x_i g^{-1}$ $\exists g \in G$. Quindi $C_G(a) = g C_G(x_i) g^{-1}$ e pertanto $|C_G(a)| = |C_G(x_i)|$. Ricordando anche che $[G : C_G(x_i)] = |G \circ x_i|$ otteniamo
$$|C| = \sum_{i=1}^{t} \sum_{a \in G \circ x_i} |C_G(x_i)| = \sum_{i=1}^{t} [G : C_G(x_i)] \cdot |C_G(x_i)| = t \cdot |G| = K(G) \cdot |G|.$$
Da cui segue la conclusione. □

Lemma 1.4. *Sia G un gruppo. Se $G/Z(G)$ è ciclico, allora G è abeliano.*

Dimostrazione. Sia $G/Z(G)$ gruppo ciclico. Allora $\exists gZ(G) \in G/Z(G)$ tale che $G/Z(G) = \langle gZ(G) \rangle$. Sia $h \in G$, allora $hZ(G) \in G/Z(G)$. Quindi $\exists n \in \mathbb{Z}$ tale che $hZ(G) = (gZ(G))^n = g^n Z(G)$. Dunque $(g^n)^{-1} h \in Z(G)$. Quindi $\exists i \in Z(G)$ tale che $i = (g^n)^{-1} h$, così $h = g^n i$. Allora $\forall h \in G$ $\exists n \in \mathbb{Z}$ e $i \in Z(G)$ tali che $h = g^n i$.
Siano $h_1, h_2 \in G$. Allora $h_1 = g^{n_1} i_1, h_2 = g^{n_2} i_2$, $\exists n_1, n_2 \in \mathbb{Z}, i_1, i_2 \in Z(G)$. Quindi $h_1 h_2 = (g^{n_1} i_1)(g^{n_2} i_2)$. Poiché $i_1, i_2 \in Z(G)$ abbiamo che
$h_1 h_2 = (g^{n_1} i_1)(g^{n_2} i_2) = g^{n_1+n_2} i_1 i_2 = g^{n_2+n_1} i_1 i_2 = g^{n_2} g^{n_1} i_1 i_2 = g^{n_2} g^{n_1} i_2 i_1 = g^{n_2} i_2 g^{n_1} i_1 = h_2 h_1$. Poiché questo è vero $\forall h_1, h_2 \in G$, G è abeliano. □

Lemma 1.5. *Se G è un gruppo finito non abeliano, allora $|Z(G)| \leq |G|/4$.*

Dimostrazione. Sia G un gruppo finito non abeliano e supponiamo per assurdo che $|Z(G)| > |G|/4$. Poiché $Z(G)$ è un sottogruppo di G, per il teorema di Lagrange $|Z(G)| \big| |G|$. Quindi $|Z(G)| = |G|/n$ $\exists n \in \mathbb{N}$. Poiché $|Z(G)| > |G|/4$, allora $|G|/n > |G|/4$. Questo implica $n < 4$, ovvero $n \in \{1, 2, 3\}$. Pertanto
$$|G/Z(G)| = \frac{|G|}{|Z(G)|} \in \{1, 2, 3\}.$$
Se $|G/Z(G)| = 1$, allora G è abeliano, assurdo. Pertanto si deve avere $|G/Z(G)| \in \{2, 3\}$, ovvero $|G/Z(G)|$ è un numero primo e ciò implica che $G/Z(G)$ è un gruppo ciclico. Per il lemma precedente, segue che G è abeliano, assurdo. □

Possiamo dimostrare ora il teorema di Gustafson.

Teorema 1.2 (W. H. Gustafson, 1973)**.** *Se G è un gruppo non abeliano finito, allora la probabilità che due elementi di G scelti casualmente commutino è al più $\frac{5}{8}$.*

Dimostrazione. Sia $P(G)$ la probabilità che due elementi di G commutino. Per il lemma 1.3, $P(G) = K(G)/|G|$, dove $K(G)$ è il numero di classi di coniugio di G. L'equazione delle classi ci dice che: $|G| = |Z(G)| + |C_1| + ... + |C_t|$, dove $C_1, ..., C_t$ sono le classi di coniugio non triviali. Abbiamo $|C_i| \geq 2 \; \forall i = 1, ..., t$. Da cui

$$\frac{|G| - |Z(G)|}{2} \geq t.$$

Pertanto

$$K(G) = |Z(G)| + t \leq |Z(G)| + \frac{|G| - |Z(G)|}{2} \leq \frac{|G| + |Z(G)|}{2}.$$

Poiché G non è abeliano, allora, per il lemma 1.5, $|Z(G)| \leq |G|/4$. E ciò permette di concludere che

$$P(G) \leq \frac{5}{8}.$$

$\square$

Osservazione 1.1. Il teorema di Gustafson fornisce il miglior limite superiore possibile per $P(G)$. Si consideri infatti, per esempio, il gruppo diedrale di ordine 8, ovvero il gruppo delle simmetrie del quadrato:

$$D_8 = \langle r, s : r^4 = s^2 = 1, sr = rs^{-1} \rangle.$$

Le classi di coniugio di D_8 sono 5: $\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}$ e $\{sr, sr^3\}$. E pertanto $P(D_8) = 5/8$.

1.3 $\mathfrak{A}(m, n)$-gruppi infiniti

Consideriamo ora gli $\mathfrak{A}(m, n)$-gruppi *infiniti*.
Presentiamo brevemente il risultato centrale, ottenuto da B. H. Neumann, di cui avremo bisogno.

Definizione 1.4 (PE-gruppi)**.** Sia G un gruppo (non necessariamente finito) e associamo a G un grafo $\Gamma = \Gamma_{\mathfrak{A}}(G)$ come nella dimostrazione del teorema 1.1, ovvero: i vertici di Γ sono gli elementi di G, e due vertici g e h di Γ sono collegati da un arco se e solo se g e h non commutano come elementi di G. Chiamiamo *PE-gruppi*, da Paul Erdős, la classe dei gruppi il cui grafo non contiene un sottografo completo infinito.

Tale definizione porta il nome di Paul Erdős, poiché, nel 1975, Erdős pose il seguente problema:

> Sia G un gruppo tale che Γ non contiene un sottografo completo infinito: c'è un limite finito sulla cardinalità dei sottografi completi di Γ?

A questa domanda Neumann rispose con la seguente caratterizzazione dei PE-gruppi:

Teorema 1.6 (B. H. Neumann, 1976 [15]). *Un gruppo G è un PE-gruppo se e solo se ha centro di indice finito.*

Proposizione 1.7. *Se un gruppo infinito $G \in \mathfrak{A}(m,n)$, allora G è abeliano.*

Dimostrazione. Sia $G \in \mathfrak{A}(m,n)$ gruppo infinito. Allora ogni sottoinsieme infinito di G contiene due elementi che commutano tra loro. Quindi G è un PE-gruppo. Dal teorema di Neumann 1.6, $G/Z(G)$ è finito, in particolare $Z(G)$ è infinito. Siano M e N due sottoinsiemi di $Z(G)$ di cardinalità m e n rispettivamente. Allora $\forall x, y \in G$, esistono $xz_1 \in xM$ e $yz_2 \in yN$ tali che $xz_1yz_2 = yz_2xz_1$, e dunque $xy = yx$. $\square$

1.4 Altri corollari del teorema 1.1

Sebbene l'obiettivo principale di questo capitolo sia stato quello di considerare la classe $\mathfrak{A}$ dei gruppi abeliani, è possibile applicare il teorema 1.1 ad altre classi di gruppi. Nel 2012, infatti, Zarrin, in [18], generalizzò la domanda di Neumann sugli $\mathfrak{A}(m,n)$-gruppi finiti nel seguente modo:

Quesito 2. *Sia $\mathfrak{X}$ una classe di gruppi e sia G un gruppo finito, tale che $G \notin \mathfrak{X}$. Esiste un limite (che dipenda solo da m e n) per l'ordine di G, se G soddisfa la condizione $\mathfrak{X}(m,n)$?*

Zarrin, in [18], diede una risposta per la classe dei gruppi nilpotenti, e in un precedente lavoro di Bryce [2] si può trovare una soluzione positiva per il caso dei gruppi supersolubili, nel caso in cui $m = n$. Grazie al teorema 1.1, A. Lucchini ha migliorato il risultato di Zarrin [[18], teorema 3.6] e ottenuto altri risultati. Infatti, in [9], il teorema 1.1 viene applicato alle seguenti classi di gruppi, per cui abbiamo una stima della costante γ:

- ogni classe di gruppi finiti chiusa per sottogruppi, gruppi quoziente ed estensioni;
- la classe dei gruppi nilpotenti finiti;
- la classe dei gruppi risolubili finiti;
- la classe dei gruppi finiti di ordine dispari.

Consideriamo quindi i seguenti interessanti risultati.

R. M. Guralnick e J. S. Wilson, usando la classificazione dei gruppi finiti semplici (ovvero i gruppi i cui unici sottogruppi normali sono il gruppo triviale e il gruppo stesso), hanno provato il seguente risultato:

Teorema 1.8 (R. M. Guralnick and J. S. Wilson, 2000 [6])**.** *Esiste un numero reale k, strettamente compreso tra 0 e 1, con la seguente proprietà: sia $\mathfrak{X}$ una classe di gruppi finiti chiusa per sottogruppi, gruppi quoziente ed estensioni, e sia G un gruppo finito; se la probabilità che due elementi di G scelti casualmente generino un gruppo in $\mathfrak{X}$ è maggiore di k, allora G è in $\mathfrak{X}$.*

Combinando [[6], proposizione 5] con [[12], teorema 1.1] si può dedurre che è possibile prendere $k = \frac{37}{90} = max(1 - \frac{53}{90}, \frac{5}{18})$. Il risultato principale ottenuto da A. Lucchini in [9] è il seguente

Corollario 1.1.2 (A. Lucchini, 2020)**.** *Sia $\mathfrak{X}$ una classe di gruppi finiti chiusa per sottogruppi, gruppi quoziente ed estensioni, e sia G un gruppo finito. Se $m \leq n$ sono interi positivi e $G \in \mathfrak{X}(m, n) \setminus \mathfrak{X}$, allora*

$$|G| \leq \left(\frac{180}{53}\right)^m (n-1).$$

Per concludere, consideriamo le classi dei gruppi risolubili, nilpotenti e di ordine dispari.

Definizione 1.5 (Gruppo risolubile)**.** Un *gruppo risolubile* è un gruppo G che ammette una *serie normale abeliana*, ovvero tale che esiste una catena di sottogruppi

$$\{1\} \lhd H_1 \lhd H_2 \lhd ... \lhd H_{n-1} \lhd H_n = G$$

in cui ogni H_i è normale in H_{i+1} e il quoziente H_{i+1}/H_i è abeliano.

Definizione 1.6 (Gruppo nilpotente)**.** Un *gruppo nilpotente* è un gruppo G che ammette una *serie centrale*, ovvero tale che esiste una catena di sottogruppi

$$\{1\} \lhd H_1 \lhd H_2 \lhd ... \lhd H_{n-1} \lhd H_n = G$$

in cui ogni H_i è normale in H_{i+1} e il quoziente H_{i+1}/H_i è contenuto nel centro di G/H_i. Il minimo n per cui G ammette una serie centrale di lunghezza n è detto *indice (o classe) di nilpotenza* di G.

Teorema 1.9 (R. M. Guralnick e J. S. Wilson, 2000 [6])**.** *Sia G un gruppo finito.*

- *Se la probabilità che due elementi di G scelti casualmente generino un gruppo risolubile è maggiore di $\frac{11}{30}$, allora G è risolubile.*

- *Se la probabilità che due elementi di G scelti casualmente generino un gruppo nilpotente è maggiore di $\frac{1}{2}$, allora G è nilpotente.*
- *Se la probabilità che due elementi di G scelti casualmente generino un gruppo di ordine dispari è maggiore di $\frac{1}{4}$, allora G ha ordine dispari.*

Inoltre, le costanti sono ottimali in ciascun caso.

Corollario 1.1.3 (A. Lucchini, 2020)**.** *Siano $m \leq n$ interi positivi e sia G un gruppo finito.*

1. *Se $\mathfrak{N}$ è la classe dei gruppi nilpotenti e $G \in \mathfrak{N}(m,n) \setminus \mathfrak{N}$, allora*
$$|G| \leq 4^m(n-1).$$
2. *Se $\mathfrak{R}$ è la classe dei gruppi risolubili e $G \in \mathfrak{R}(m,n) \setminus \mathfrak{R}$, allora*
$$|G| \leq \left(\frac{60}{19}\right)^m (n-1).$$
3. *Se $\mathfrak{D}$ è la classe dei gruppi di ordine dispari e $G \in \mathfrak{D}(m,n) \setminus \mathfrak{D}$, allora*
$$|G| \leq \left(\frac{8}{3}\right)^m (n-1).$$

Nonostante questi risultati, la domanda di Zarrin ha risposta negativa per alcune rilevanti classi di gruppi. Per esempio, consideriamo la classe $\mathfrak{M}$ dei gruppi metabeliani, di cui ricordiamo la definizione:

Definizione 1.7. Un gruppo G si dice *metabeliano* se il suo *sottogruppo derivato* $[G, G]$, cioè il sottogruppo generato dai commutatori, è abeliano.

Dati $g, h \in G$, il *commutatore* di g e h si definisce come $[g, h] = g^{-1}h^{-1}gh$. Sia $S = \{[g, h] : g, h \in G\}$ l'insieme dei commutatori di G. Il derivato di G $[G, G]$ è dunque il sottogruppo generato da S, ovvero il più piccolo sottogruppo di G che contiene S.

Teorema 1.10 (B. H. Neumann, 1956 [14])**.** *Esistono (infiniti) gruppi finiti che non sono metabeliani, ma tali per cui ogni sottogruppo 2-generato è metabeliano.*

Pertanto, la risposta al quesito di Zarrin è negativa per la classe $\mathfrak{M}$ dei gruppi metabeliani. Più in generale, la risposta è certamente negativa per ogni classe $\mathfrak{X}$ che non è *2-riconoscibile*, cioè per cui esistono gruppi finiti che non sono in $\mathfrak{X}$, ma tali per cui tutti i sottogruppi 2-generati lo sono. Un'altra importante classe di gruppi che non sono 2-riconoscibili è quella dei gruppi con classe di nilpotenza al più due. Nel terzo capitolo proporremo pertanto una variazione del problema di Zarrin considerando parole e non più classi di gruppi, che ha risposta affermativa, tra gli altri, nei sopramenzionati casi dei gruppi metabeliani e gruppi con classe di nilpotenza al più 2.

Capitolo 2

Il teorema di Kővári-Sós-Turán

Questo capitolo è dedicato alla dimostrazione del teorema di Kővári-Sós-Turán [8], che denoteremo d'ora in avanti con KST per brevità. Il teorema dà un limite superiore alla soluzione del *problema di Zarankiewicz*, tutt'oggi insoluto, che chiede quale sia il massimo numero di archi in un grafo bipartito che ha un dato numero di vertici e non ha sottografi completi bipartiti di una certa dimensione. Tale problema prende il nome dal matematico polacco Kazimierz Zarankiewicz, che propose alcuni casi speciali del problema nel 1951. Il teorema di KST è stato dimostrato da Tamás Kővári, Vera T. Sós e Pál Turán poco dopo che il problema fu posto.

Il problema di Zarankiewicz è un esempio di un tipo di problemi che costituiscono quella che viene chiamata *teoria estremale* dei grafi. Naturalmente, non vi è una definizione precisa di che cosa consista la teoria estremale; tipici problemi di cui si occupa possono essere formulati come problemi di ottimizzazione: fissata una certa proprietà $\mathcal{P}$ dei grafi (come l'esistenza di particolare sottografi), cosa si può dire dei grafi che hanno il massimo (o, a volte, minimo) numero di archi tra quelli che (con lo stesso numero di vertici) soddisfano la proprietà $\mathcal{P}$? I grafi che sono una soluzione ottimale per tali problemi di ottimizzazione vengono detti *grafi estremali*.

Ricordiamo che denotiamo con $K_{s,t}$ un grafo completo bipartito $\Gamma = (U, V, E)$ in cui U ha s vertici e V ha t vertici. $\forall s \geq 1$, $K_{s,1}$ è chiamato *s-stella*. Ovvero una s-stella è un albero con un nodo interno e s foglie. Inoltre, denoteremo con $x \sim y$ un arco non orientato tra due vertici x e y di un grafo Γ, mentre con $x \mapsto y$ un arco orientato da x a y, vertici di un grafo diretto $\vec{\Gamma}$.

Per la dimostrazione del teorema di KST, ci sono utili alcuni richiami sulle funzioni convesse.

Definizione 2.1. Una funzione reale $\phi(x)$ definita su un intervallo I si dice *funzione convessa* sull'intervallo I se, comunque si considerino due punti $x_1, x_2 \in I$, con $x_1 < x_2$, risulta che

$$\phi(tx_1 + (1-t)x_2) \leq t\phi(x_1) + (1-t)\phi(x_2) \ \forall t \in [0,1].$$

Teorema 2.1. *Sia $\phi(x)$ una funzione due volte derivabile su un intervallo I. Se $\phi''(x) > 0 \ \forall x \in I$, allora ϕ è convessa su I.*

Useremo un caso particolare della disuguaglianza di Jensen in forma discreta, con pesi tutti uguali a $\frac{1}{n}$:

Teorema 2.2 (Jensen, 1906)**.** *Sia $\phi : I \to \mathbb{R}$ una funzione convessa reale, $x_1, ..., x_n \in I$, allora*

$$\phi(\frac{\sum_{i=1}^n x_i}{n}) \leq \frac{\sum_{i=1}^n \phi(x_i)}{n}.$$

Osservazione 2.1. La funzione $\phi(x) = \binom{x}{s}$, dove $\binom{x}{s} = \frac{x(x-1)...(x-s+1)}{s!}$, è convessa per $x \geq s$. Infatti, per la regola del prodotto, abbiamo

$$\phi''(x) = \frac{2}{s!} \sum_{0 \leq i < j \leq s-1} \prod_{l=0}^{s-1} \frac{x-l}{(x-i)(x-j)} > 0 \ \forall x \geq s.$$

Teorema 2.3 (KST per grafi non orientati)**.** *Se s e t sono due interi positivi, allora un grafo con n vertici e almeno $\frac{(t-1)^{\frac{1}{s}} n^{2-\frac{1}{s}} + (s-1)n}{2}$ archi contiene una copia del grafo completo bipartito $K_{s,t}$.*

La dimostrazione di 2.3 seguirà come corollario del teorema di KST nel caso dei *grafi orientati*, che useremo nel terzo capitolo; prima di considerare quest'ultimo, abbiamo bisogno di una versione del teorema di KST per *grafi non orientati bipartiti*:

Teorema 2.4 (KST per grafi non orientati bipartiti)**.** *Sia $\Gamma = (U, V, E)$ un grafo bipartito con $|U| = |V| = n$ e tale che non vi siano sottografi del tipo $K_{s,t}$, con s vertici in U e t vertici in V. Allora*

$$|E| \leq (t-1)^{1/s} n^{2-1/s} + (s-1)n.$$

Dimostrazione. Sia Σ l'insieme dei sottografi di Γ del tipo s-stella, con centro $v \in V$ e s vertici $u_1, ..., u_s \in U$. Chiamiamo $\sigma := |\Sigma|$. Allora

$$\sigma \leq (t-1)\binom{n}{s}. \tag{2.1}$$

Infatti, al più, possiamo scegliere le s foglie di una s-stella (tra gli n vertici di U) in $\binom{n}{s}$ modi. Dunque, fissate le s foglie, se avessimo t modi per scegliere il nodo centrale $v \in V$, avremmo un $K_{s,t}$-sottografo di Γ. Quindi, al più, vi sono $t-1$ modi per scegliere il nodo centrale della s-stella.

D'altra parte, abbiamo anche che

$$\sigma = \sum_{v \in V} \binom{deg(v)}{s}. \tag{2.2}$$

Infatti, fissato un vertice $v \in V$, il numero di sottografi del tipo s-stella di Γ di centro v è esattamente il numero di modi con cui possiamo scegliere s nodi incidenti a v tra i $deg(v)$ nodi totali di U incidenti v, ovvero $\binom{deg(v)}{s}$. Otteniamo quindi, combinando 2.1 e 2.2 e dividendo per n:

$$\frac{\sigma}{n} = \frac{\sum_{v \in V} \binom{deg(v)}{s}}{n} \leq \frac{(t-1)\binom{n}{s}}{n}. \tag{2.3}$$

Applichiamo la disuguaglianza di Jensen alla funzione $\phi(x) = \binom{x}{s}$, valutata sugli n vertici $v \in V$:

$$\frac{\sum_{v \in V} \binom{deg(v)}{s}}{n} \geq \binom{\frac{\sum_{v \in V} deg(v)}{n}}{s}. \tag{2.4}$$

Sia $e = |E|$. Ricordando il cosiddetto *(bipartite) handshaking lemma*: $\sum_{u \in U} deg(u) = \sum_{v \in V} deg(v) = e$, abbiamo

$$\binom{\frac{\sum_{v \in V} deg(v)}{n}}{s} = \binom{\frac{e}{n}}{s} \geq \frac{(\frac{e}{n} - s + 1)^s}{s!}. \tag{2.5}$$

Combinando 2.3, 2.4 e 2.5 otteniamo

$$\frac{(\frac{e}{n} - s + 1)^s}{s!} \leq \frac{\sigma}{n} \leq \frac{(t-1)\binom{n}{s}}{n}.$$

Da cui si conclude che

$$e \leq (t-1)^{\frac{1}{s}} n^{2-\frac{1}{s}} + (s-1)n.$$

□

Passiamo ora a considerare ora il caso dei *grafi orientati*.

Definizione 2.2. Chiamiamo $\vec{K}_{s,t}$ il grafo completo bipartito orientato in cui l'insieme dei vertici è un'unione disgiunta $A \cup B$, con $|A| = s$ e $|B| = t$, e un arco è diretto da ogni vertice di A a ogni vertice di B.

Teorema 2.5 (KST per grafi orientati). *Sia $\vec{\Gamma} = (V, \vec{E})$ un grafo orientato con $|V| = n$ vertici. Supponiamo che $\vec{\Gamma}$ non contenga una copia di $\vec{K}_{s,t}$. Allora*

$$|\vec{E}| \leq (t-1)^{1/s} n^{2-1/s} + (s-1)n.$$

Dimostrazione. Definiamo un nuovo grafo $\tilde{\Gamma}$, non orientato e bipartito, con parti V_1 e V_2, dove $V_1 = V_2 = V$, in modo che $x \in V_1$ sia collegato con un arco a $y \in V_2$ se e solo se $x \mapsto y$ è un arco orientato di $\vec{\Gamma}$.
In questo modo, $\tilde{\Gamma}$ e $\vec{\Gamma}$ hanno lo stesso numero di archi. Inoltre, $\vec{\Gamma}$ non contiene una copia del sottografo completo bipartito orientato $\vec{K}_{s,t}$ se e solo se $\tilde{\Gamma}$ non contiene una copia del sottografo completo bipartito non orientato $K_{s,t}$. Concludiamo quindi per il teorema di KST, nel caso dei grafi non orientati bipartiti 2.4, che

$$|\vec{E}| \leq (t-1)^{1/s} n^{2-1/s} + (s-1)n.$$

□

Possiamo quindi dimostrare il teorema 2.3:

Dimostrazione. Sia $\Gamma = (V, E)$ un grafo con n vertici, che non contiene una copia del grafo completo bipartito $K_{s,t}$. Definiamo un nuovo grafo $\vec{\Gamma}$, orientato, con gli stessi vertici V di Γ, e bidirezionando gli archi di Γ, ovvero in modo che $x \sim y$ è un arco di Γ se e solo se $x \mapsto y$ e $y \mapsto x$ sono archi orientati di $\vec{\Gamma}$. Pertanto, $\vec{\Gamma}$ ha $2|E|$ archi, e Γ contiene una copia di $K_{s,t}$ se e solo se $\vec{\Gamma}$ contiene una copia di $\vec{K}_{s,t}$. Quindi, per 2.5:

$$2|E| \leq (t-1)^{1/s} n^{2-1/s} + (s-1)n,$$

e si ha la conclusione. □

Il lettore potrebbe a questo punto chiedersi se valgano dei risultati analoghi anche per gli *ipergrafi*. La risposta è affermativa e, a riguardo, vedremo un teorema di Paul Erdős nel prossimo capitolo.

Capitolo 3

Sulle parole che soddisfano un gap di probabilità

In questo capitolo lavoreremo con *parole* invece che con *classi di gruppi* e inizieremo pertanto ricordando i concetti di *parola* e *gruppo libero* nella sezione 3.1. Proseguiremo dimostrando un risultato di A. Lucchini simile al teorema 1.1, ma che riguarda appunto parole (in F_2) in luogo di classi di gruppi. Lavoreremo con parole che soddisfano un *gap di probabilità*, concetto che definiremo nella sezione 3.3, e proporremo una variazione del problema di Zarrin 2 in termini di parole che soddisfano un gap di probabilità, che generalizza il teorema di Lucchini a parole in un numero arbitrario di variabili. Concluderemo il capitolo con la dimostrazione di un risultato di A. Erfanian, R. Rezaei e P. Lescot che generalizza il teorema dei 5/8 di Gustafson.

3.1 Parole e gruppi liberi

Definizione 3.1 (Parola)**.** Dato un insieme X, possiamo definire un nuovo insieme X^{-1}, costituito dagli "inversi formali" degli elementi di X. Cioè, definiamo un insieme di nuovi simboli, uno per ogni elemento $x \in X$, che denotiamo con x^{-1}, quindi:

$$X^{-1} = \{x^{-1} \mid x \in X\}.$$

Una *parola* w in X è una sequenza finita di simboli di $X \cup X^{-1}$, che denotiamo come:

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_r^{\epsilon_r},$$

dove $x_i \in X$, $\epsilon_i = \pm 1$, $r \geq 0$: se $r = 0$, la sequenza è vuota e w è la *parola vuota*, che denotiamo con 1. Diciamo che r è la lunghezza della parola w. Diciamo che w è una *parola ridotta* se è priva delle sottosequenze del tipo xx^{-1} e $x^{-1}x$ per ogni $x \in X$.

Per gli scopi di questo capitolo ci limitiamo a presentare brevemente un modo per costruire un *gruppo libero* a partire da un insieme $X \neq \emptyset$.

Teorema 3.1 (Gruppo libero)**.** *Sia dato un insieme di n elementi $X = \{t_1, ..., t_n\}$. Denotiamo con W_n l'insieme delle parole di lunghezza n su X. L'insieme $W = \cup_{n\in\mathbb{N}} W_n$ è un monoide, con identità la parola vuota, rispetto all'operazione $*$ di giustapposizione definita da $(x_1...x_s) * (y_1...y_t) = x_1...x_s y_1...y_t$.*
Consideriamo la relazione di equivalenza $\sim$ sul monoide W generata dalle relazioni $xx^{-1} \sim 1$, $x^{-1}x \sim 1$ per ogni $x \in X$. L'insieme $W/\sim$ è un gruppo, detto gruppo libero generato da X, denotato come $F(X)$, oppure $F\langle t_1, ..., t_n\rangle$, dove l'inverso di $w = x_1^{\epsilon_1}...x_r^{\epsilon_r}$ è $w^{-1} = x_r^{-\epsilon_r}...x_1^{-\epsilon_1}$. Chiamiamo gli elementi di X generatori del gruppo libero.

In seguito denoteremo un gruppo libero su un insieme di n elementi anche semplicemente con F_n, senza indicare esplicitamente una scelta di n generatori. Viceversa, quando vorremo specificare una scelta di n generatori $\{x_1, x_2, ..., x_n\}$, scriveremo anche $w = w(x_1, x_2, ..., x_n)$. Inoltre, con $w \in F_n$ intendiamo $[w]_\sim \in F_n$. In particolare possiamo assumere che w sia una parola ridotta.

Per ogni gruppo G, sia $G^{(n)}$ il prodotto diretto di n copie di G e sia $w = w(x_1, ..., x_n)$ una parola in F_n.
Allora, abbiamo sempre una *funzione parola*:

$$w : G^{(n)} \to G; (g_1, ..., g_n) \mapsto w(g_1, ..., g_n)$$

indotta per sostituzione dalla parola w.

Definizione 3.2. Sia $w = w(x_1, ..., x_d)$ una parola in F_d. Diciamo che w è un'identità in G e scriviamo $w \equiv 1$ se:

$$w(g_1, ..., g_d) = 1$$

per ogni $g_1, ..., g_d \in G$.

3.2 Teorema di A. Lucchini per parole in F_2

In questa sezione mostriamo che, essenzialmente con gli stessi argomenti, è possibile provare un risultato simile al teorema 1.1, ma che riguarda parole in F_2 invece di classi di gruppi.

Consideriamo la seguente proprietà per parole in F_2, nello stesso ordine di idee della proprietà $\mathfrak{X}(m, n)$ per classi di gruppi che abbiamo utilizzato nel primo capitolo:

Definizione 3.3. Sia $w \in F_2$ una parola e siano m e n due interi positivi. Diciamo che un gruppo finito G ha la proprietà $w_{m,n}$ o che G è un $w_{m,n}-$gruppo se comunque si scelgano due sottoinsiemi di G, M e N, di cardinalità rispettivamente m e n, esistono $x \in M$ e $y \in N$ tali che $w(x, y) = 1$.

Definizione 3.4. Sia G un gruppo finito e $w \in F_n$ una parola. Chiamiamo $P_{w=1}(G)$ la probabilità che $w(g_1, g_2, ..., g_n) = 1$ in G, dove $g_1, g_2, ..., g_n$ sono scelti indipendentemente in accordo con la distribuzione uniforme di probabilità in G.

Proviamo ora il seguente risultato.

Teorema 3.2 (A. Lucchini, 2022 [10]). *Supponiamo che una parola $w \in F_2$ abbia la seguente proprietà: esiste un reale positivo $\gamma < 1$ tale che se w non è un'identità in un gruppo finito X, allora $P_{w=1}(X) \leq \gamma$. Se $m \leq n$ e un gruppo finito G ha la proprietà $w_{m,n}$, allora w è un'identità in G oppure:*

$$|G| \leq \left(\frac{2}{1-\gamma}\right)^m (n-1).$$

Dimostrazione. Sia G sia un $w_{m,n}-$gruppo finito. Consideriamo il grafo orientato $\vec{\Gamma}_w(G)$, i cui vertici sono gli elementi di G, e in cui c'è un arco $x_1 \mapsto x_2$ se e solo se $w(x_1, x_2) \neq 1$. Se w non è un'identità in G, allora la probabilità che due vertici di $\vec{\Gamma}_w(G)$ siano collegati da un arco è almeno $1 - \gamma$. Quindi abbiamo:

$$\eta \geq (1-\gamma)|G|^2. \tag{3.1}$$

D'altra parte, poiché G è un $w_{m,n}-$gruppo, il grafo $\vec{\Gamma}_w(G)$ non può contenere il grafo completo bipartito orientato $\vec{K}_{m,n}$ come sottografo. Per il teorema di KST per i grafi orientati 2.5:

$$\eta \leq (n-1)^{1/m}|G|^{2-1/m} + (m-1)|G|. \tag{3.2}$$

A questo punto concludiamo come nel teorema 1.1. Combinando 3.1 e 3.2 deduciamo che

$$1-\gamma \leq \left(\frac{n-1}{|G|}\right)^{1/m} + \frac{m-1}{|G|} \leq \left(\frac{n-1}{|G|}\right)^{1/m} + \frac{n-1}{|G|}. \tag{3.3}$$

Possiamo assumere $|G| \geq n-1$. Questo implica $\left(\frac{n-1}{|G|}\right)^{1/m} \geq \frac{n-1}{|G|}$ e pertanto segue da 3.3 che

$$1-\gamma \leq 2\left(\frac{n-1}{|G|}\right)^{1/m}.$$

Da cui:

$$|G| \leq \left(\frac{2}{1-\gamma}\right)^m (n-1).$$

□

Vedremo alcuni corollari di questo teorema nella prossima sezione.

3.3 Parole t-limitate

Nel teorema 3.2 abbiamo considerato parole $w \in F_2$ tali per cui esiste un reale positivo $\gamma < 1$ con la proprietà che ogni gruppo finito G soddisfa $w \equiv 1$ oppure $P_{w=1}(G) \leq \gamma$. Ad oggi, è un problema aperto quello di chiedersi se data una parola $w \in F_r$ esista una costante $\gamma = \gamma(w) < 1$ con la proprietà descritta. Nel prosieguo del capitolo considereremo alcune parole con tale proprietà e diremo che queste parole soddisfano un *gap di probabilità*. Fissiamo pertanto la seguente definizione:

Definizione 3.5. Diciamo che una parola $w = w(x_1, ..., x_r) \in F_r$ soddisfa un *gap di probabilità* se esiste una costante $\gamma = \gamma_w < 1$ tale che, per ogni gruppo finito G, se $P_{w=1}(G) > \gamma$, allora $w \equiv 1$.

Vedremo che le seguenti parole, il commutatore e sue naturali generalizzazioni, soddisfano un gap di probabilità:

- *commutatore*: $[x, y] \in F_2$;
- *parola di 2-Engel*: $[[x, y], y] \in F_2$;
- *parola metabeliana*: $[[x_1, x_2], [x_3, x_4]] \in F_4$;
- *commutatore lungo*: $[x_1, [x_2, [..., x_d]]] \in F_d$;
- ogni parola della forma $\tilde{w}(x_1, x_2, ..., x_d) = [x_1, w(x_2, ..., x_d)] \in F_d$, con $w \in F_{d-1}$ che soddisfa un gap di probabilità.

Abbiamo concluso il primo capitolo osservando che la domanda di Zarrin 2 ha risposta negativa per alcune rilevanti classi di gruppi, tra le quali quella dei gruppi metabeliani e quella dei gruppi con classe di nilpotenza al più 2. Proponiamo quindi ora una variazione di questo problema che ha risposta positiva, tra le altre, per le classi di gruppi in questione. Per fare questo, abbiamo bisogno di dare una prima generalizzazione della proprietà 3.3, che abbiamo definito per parole in F_2, per parole in F_r con r qualsiasi:

Definizione 3.6. Sia $w = w(x_1, ..., x_r)$ una parola in F_r e sia t un intero positivo. Diciamo che un gruppo finito G ha la *proprietà* w_t se comunque si scelgano r sottoinsiemi $X_1, ..., X_r$ di G con $|X_1| = ... = |X_r| = t$, esiste una r-upla $(g_1, ..., g_r) \in X_1 \times ... \times X_r$ tale che $w(g_1, ..., g_r) = 1$. Inoltre, diciamo che w è una *parola t-limitata* se esiste una costante c_t tale che se un gruppo finito G soddisfa la proprietà w_t, allora $|G| \leq c_t$ o $w \equiv 1$ in G.

Il risultato centrale di questa parte finale è il seguente

Teorema 3.3. *Se una parola w soddisfa un gap di probabilità, allora w è una parola t-limitata per ogni intero positivo t.*

Osserviamo che, grazie al teorema 3.2, questo risultato è provato nel caso particolare in cui $w \in F_2$. Prima di passare a dimostrarlo in generale, soffermiamoci a considerare due importanti parole di F_2 a cui possiamo applicare il teorema 3.2: il *commutatore* e la *parola di 2-Engel*.

3.3.1 Commutatore

Consideriamo $w = [x, y] \in F_2$.
Ricordiamo che dato un gruppo finito G, abbiamo definito $P(G)$ come la probabilità che due elementi di G scelti casualmente commutino. Allora: $P(G) = P_{[x,y]=1}(G)$. Inoltre, G è un $\mathfrak{A}(m, n)$-gruppo se e solo se è un $w(m, n)$-gruppo. Il commutatore soddisfa un gap di probabilità per il teorema di Gustafson, e quindi applicando il teorema 3.2 a $w = [x, y]$ riotteniamo il corollario 1.1.1 e abbiamo pertanto un argomento alternativo per provare che la risposta alla domanda di B. H. Neumann è positiva.

3.3.2 Parola di 2-Engel

Definizione 3.7 (parola di 2-Engel)**.** La parola di 2-Engel è $w := [[x, y], y] = [x, y, y] \in F\langle x, y\rangle$. In forma estesa, questa è:

$$w = y^{-1}x^{-1}yxy^{-1}x^{-1}y^{-1}xyy.$$

Un gruppo G è detto di 2-Engel se $[x, y, y] \equiv 1$ in G. La parola di 2-Engel soddisfa un gap di probabilità per il seguente

Teorema 3.4 (C. Delizia, U. Jezerenik, P. Moravec, C. Nicotera, 2020 [3])**.** *Sia $w = [x, y, y]$ la parola di 2-Engel. Esiste una costante $\delta < 1$ tale che se w non è un identità in un gruppo finito G, allora $P_{w=1}(G) \leq \delta$.*

Possiamo quindi applicare il teorema di Lucchini 3.2 a $w = [x, y, y]$ e ottenere il seguente

Corollario 3.2.1 (A. Lucchini, 2022)**.** *Sia $w = [x, y, y]$ la parola di 2-Engel. Esiste una costante τ tale che se $m \leq n$ e G soddisfa la proprietà $w_{m,n}$, allora o w è un'identità in G o $|G| \leq \tau^m(n - 1)$.*

Dimostrazione. Per 3.4, la parola di 2-Engel soddisfa un gap di probabilità per una certa costante $\delta < 1$. Per 3.2, possiamo prendere $\tau = \frac{2}{1-\delta}$. □

Questi risultati ci dicono in particolare che il commutatore e la parola di 2-Engel sono t-limitate. Per dimostrare il teorema 3.3 in generale abbiamo bisogno di un teorema di Paul Erdős sugli *ipergrafi*. Iniziamo quindi dando le seguenti definizioni.

3.3.3 Dimostrazione del teorema 3.3

Definizione 3.8 (ipergrafo)**.** Un *ipergrafo* è un grafo in cui un arco può essere collegato a un qualunque numero di vertici. Formalmente, un ipergrafo H è una coppia $H = (V, E)$ dove V è un insieme di elementi chiamati *nodi* oppure *vertici*, ed E è un insieme formato da sottoinsiemi non vuoti di V chiamati *iperarchi* oppure *archi*.

Definizione 3.9 (r-grafo)**.** Un *r-grafo* $\Gamma = (V, E)$ è un ipergrafo r-uniforme, ovvero un ipergrafo in cui ciascun arco $e \in E$ ha esattamente r vertici.

Denotiamo con $K^{(r)}_{t,\dots,t}$ l'r-grafo completo r-partito con parti $V_1, ..., V_r$ di cardinalità t.

Definizione 3.10 (funzione di Turán)**.** Data una famiglia di k-grafi $\mathfrak{F}$, la *funzione di Turán* $ex_r(n, \mathfrak{F})$ è definita come $max_\Gamma e(\Gamma)$, su tutti gli r-grafi Γ di n vertici, che non hanno sottografi in $\mathfrak{F}$.

Dimostreremo il teorema 3.3 procedendo in modo analogo alla dimostrazione del teorema 3.2. Abbiamo però bisogno di un risultato similare al teorema di KST, ma nel caso degli ipergrafi. In questo, ci viene in aiuto il seguente teorema di Paul Erdős:

Teorema 3.5 (P. Erdős, 1964 [4])**.** *Dati due interi positivi r e t, esiste una costante $c(r, t)$ tale che, se $n \geq c(r, t)$, allora*

$$ex_r(n, K^{(r)}_{t,\dots,t}) \leq n^{r-\frac{1}{t^{r-1}}}.$$

Ora possiamo dimostrare il teorema 3.3:

Dimostrazione. Sia $w \in F_r$ e supponiamo che per ogni gruppo finito G se $P_{w=1}(G) > \gamma_w$, allora $w \equiv 1$. Supponiamo che G soddisfi la proprietà w_t ma che w non sia un'identità in G. Assumiamo inoltre che $|G| \geq c(r, t)$. Definiamo un r-grafo $\Gamma = (V, E)$ come segue: V è l'unione disgiunta di r copie $Y_1, ..., Y_r$ di G e $\{y_1, ..., y_r\} \in E$ se $y_i \in Y_i$ per $1 \leq i \leq r$ e $w(y_1, ..., y_r) \neq 1$. Poiché w non è un'identità in G,

$$|E| \geq (1 - \gamma)|G|^r. \tag{3.4}$$

D'altra parte, poiché G soddisfa la proprietà w_t, l'r-grafo Γ non può contenere $K^{(r)}_{t,\dots,t}$ come sottografo. Per il teorema 3.5:

$$|E| \leq (r|G|)^{r-\frac{1}{t^{r-1}}} \leq \frac{r^r|G|^r}{|G|^{\frac{1}{t^{r-1}}}}. \tag{3.5}$$

Combinando 3.4 e 3.5, deduciamo:

$$|G| \leq \left(\frac{r^r}{1 - \gamma_w}\right)^{t^{r-1}}.$$

$\square$

Applichiamo questo teorema alla *parola metabeliana* e al *commutatore lungo*.

3.3.4 Parola metabeliana

Definizione 3.11 (Parola metabeliana)**.** La *parola metabeliana* è la parola $[[x_1, x_2], [x_3, x_4]] \in F_4 = F\langle x_1, x_2, x_3, x_4\rangle$. In forma estesa, questa è:

$$x_2^{-1}x_1^{-1}x_2x_1x_4^{-1}x_3^{-1}x_4x_3x_1^{-1}x_2^{-1}x_1x_2x_3^{-1}x_4^{-1}x_3x_4.$$

Un gruppo G è metabeliano se $[[x_1, x_2], [x_3, x_4]] \equiv 1$ in G.
C. Delizia et al. in [3] hanno provato che anche la parola metabeliana, oltre alla parola di 2-Engel, soddisfa un gap di probabilità per una certa costante $\gamma < 1$. Otteniamo pertanto il seguente corollario di 3.3:

Corollario 3.3.1. *Diciamo che un gruppo finito G ha la proprietà t-metabeliana se, comunque si scelgano quattro sottoinsiemi X_1, X_2, X_3, X_4 di G di cardinalità t, esiste $(x_1, x_2, x_3, x_4) \in X_1 \times X_2 \times X_3 \times X_4$ tale che $[[x_1, x_2], [x_3, x_4]] = 1$. Per ogni intero positivo t esiste una costante k_t con la seguente proprietà: se un gruppo finito G soddisfa la proprietà t-metabeliana, allora G è metabeliano oppure $|G| \leq k_t$.*

Dimostrazione. Per la dimostrazione del teorema 3.3 possiamo prendere $k_t = \left(\frac{256}{1-\gamma}\right)^{t^3}$. □

3.3.5 Commutatore lungo

Definizione 3.12 (Commutatore lungo)**.** Il *commutatore lungo* è la parola $\gamma_d(x_1, ..., x_d) = [x_1, \gamma_{d-1}(x_2, ..., x_d)] = [x_1, [x_2, [..., x_d]]] \in F_d = F\langle x_1, ..., x_d\rangle$.

Un gruppo G è nilpotente con grado di nilpotenza al più d se $\gamma_{d+1} \equiv 1$ in G. γ_d soddisfa il seguente gap di probabilità:

Teorema 3.6 (A. Erfanian, R. Rezaei e P. Lescot, 2007 [5])**.** *Sia G un gruppo finito che non soddisfa $\gamma_d \equiv 1$. Allora*

$$P_{\gamma_d=1}(G) \leq 1 - \frac{3}{2^{d+1}}.$$

Tale limite superiore è ottimale.

Per la dimostrazione si veda la sezione 3.4. Otteniamo il seguente corollario di 3.3:

Corollario 3.3.2. *Diciamo che un gruppo finito G ha la proprietà di nilpotenza (r,t) se, comunque si scelgano $r+1$ sottoinisiemi $X_1, .., X_{r+1}$ di G di cardinalità t, esiste $(x_1, ..., x_{r+1}) \in X_1 \times ... \times X_{r+1}$ tale che $[x_1, [x_2, [..., x_{r+1}]]] = 1$. Per ogni intero positivo t esiste una costante $k_{r,t}$ con la seguente proprietà: se un gruppo finito G soddisfa la proprietà di nilpotenza (r, t), allora G è nilpotente con classe di nilpotenza al più r oppure $|G| \leq k_{r,t}$.*

Dimostrazione. Per la dimostrazione del teorema 3.3, e usando 3.6, possiamo prendere $k_{r,t} = \left(\frac{2(2r+2)^{r+1}}{3}\right)^{t^r}$. $\square$

In particolare abbiamo quindi una risposta per i gruppi nilpotenti con classe di nilpotenza al più 2, per i quali non era stato possibile ottenere un risultato in termini di classi di gruppi. Si ha $k_{2,t} = 144^{t^2}$.

3.3.6 Remark finale

Abbiamo definito la proprietà $\mathfrak{X}(m,n)$ per classi di gruppi e l'analoga proprietà $w(m,n)$ per parole 3.3 ammettendo che i sottoinsiemi M e N abbiano cardinalità diverse, m e n, e indagato un limite superiore per la cardinalità di G in termini di m e n. Quando abbiamo generalizzato la proprietà $w(m,n)$ a parole in F_r, definendo la proprietà w_t, abbiamo invece considerato sottoinsiemi $X_1, ..., X_r$ tutti della stessa cardinalità t. Possiamo generalizzare la proprietà w_t dicendo che se $w \in F_r$ e $s_1 \leq ... \leq s_r$ sono interi positivi, allora un gruppo finito G ha la proprietà $w_{s_1,...,s_r}$ se comunque si scelgano r sottoinsiemi $X_1, ..., X_r$ con $|X_1| = s_1, ..., |X_r| = s_r$, esiste $(g_1, ..., g_r) \in X_1 \times ... \times X_r$ tale che $w(g_1, ..., g_r) = 1$. Con questa notazione possiamo formulare una versione più forte del teorema 3.3:

Proposizione 3.7. *Sia $w \in F_r$ e supponiamo che esista una costante $\gamma_w < 1$ tale che, per ogni gruppo finito G, se $P_{w=1}(G) > \gamma_w$, allora $w \equiv 1$. Se un gruppo finito G soddisfa la proprietà $w_{s_1,...,s_r}$, allora w è un'identità in G oppure*

$$|G| \leq \left(\frac{r^r (s_r - 1)^{\frac{1}{s_1 \cdots s_{r-1}}} + o(1)}{1 - \gamma_w} \right)^{s_1 \dots s_{r-1}}$$

dove $o(1) \to 0$ quando $|G| \to \infty$.

Dimostrazione. Denotiamo con $K^{(r)}_{s_1,...,s_r}$ l' r-grafo completo r-partito con parti di cardinalità $s_1, ..., s_r$. Allora $ex_r(n, K^{(r)}_{s_1,...,s_r}) \leq ((s_r - 1)^{\frac{1}{s_1 \cdots s_{r-1}}} + o(1))n^{r - \frac{1}{s_1 \cdots s_{r-1}}}$, dove $o(1) \to 0$ quando $n \to \infty$ (si veda il lemma 3.1 e il seguente remark in [11]). La tesi segue usando questo risultato al posto del teorema 3.5 nella dimostrazione del teorema 3.3. $\square$

3.4 Una generalizzazione del teorema dei 5/8

Nel primo capitolo abbiamo dimostrato il teorema di Gustafson 1.2, che alla luce delle notazioni introdotte in questo capitolo possiamo riscrivere come: $P_{\gamma_2=1}(G) \leq 5/8$, per ogni gruppo finito G non abeliano. Abbiamo visto che questo risultato si può generalizzare considerando il commutatore lungo: $P_{\gamma_d=1}(G) \leq 1 - \frac{3}{2^{d+1}}$. Concludiamo questo lavoro di tesi dando una dimostrazione di questo risultato, che è stato dimostrato per la prima volta da A. Erfanian, R. Rezaei e P. Lescot in [5] . Seguiamo il lavoro [3] di C. Delizia et al., che fornisce una dimostrazione alternativa, e iniziamo descrivendo un approccio generale per determinare una maggiorazione di $P_{w=1}(G)$, che è stato anche applicato in [3] per mostrare che la parola di 2-Engel e la parola metabeliana soddisfano un gap di probabilità, sotto assunzioni extra sulla struttura di G.

3.4.1 Un approccio generale: the GOOD and the BAD

Possiamo scrivere:

$$P_{w=1}(G) = \frac{1}{|G|^d} \sum_{g_2,...,g_d \in G} |\{g_1 \in G | w(g_1, ..., g_d) = 1\}|.$$

Denotiamo con $C_w(g_2, ..., g_d) := \{g_1 \in G | w(g_1, ..., g_d) = 1\}$. N.B. : $C_w(g_2, ..., g_d)$ è raramente un sottogruppo di G.
Supponiamo di definire un insieme $BAD \subseteq G^{d-1}$ con la proprietà che esistono due costanti assolute $0 < \delta_{GOOD}, \delta_{BAD} < 1$, che dipendono solo da w e non da G, tali che:

- $\forall (g_2, ..., g_d) \in GOOD$, $|C_w(g_2, ..., g_d)| \leq \delta_{GOOD} \cdot |G|$;
- $|BAD| \leq \delta_{BAD} \cdot |G|^{d-1}$;

dove $GOOD = G^{d-1} \setminus BAD$.
Allora, sommando separatamente su BAD e GOOD otteniamo facilmente che

$$P_{w=1}(G) \leq \delta_{GOOD} + (1 - \delta_{GOOD})\delta_{BAD},$$

che dà un limite superiore per $P_{w=1}(G)$.

3.4.2 Esempio di applicazione: il commutatore lungo

Consideriamo il commutatore lungo $\gamma_d(x_1, ..., x_d) = [x_1, \gamma_{d-1}(x_2, ..., x_d)] = [x_1, [x_2, [..., x_d]]]$.
Per il teorema di Gustafson, sappiamo che per un gruppo non abeliano finito G, $P_{\gamma_2=1}(G) \leq 5/8$. Dimostriamo ora il seguente

Teorema 3.6. *Sia G un gruppo finito che non soddisfa $\gamma_d \equiv 1$. Allora*

$$P_{\gamma_d=1}(G) \leq 1 - \frac{3}{2^{d+1}}.$$

Tale limite superiore è ottimale.

Dimostrazione. Procediamo per induzione su d. Sia G un gruppo che non soddisfa $\gamma_d \equiv 1$. Definiamo

$$\begin{aligned} BAD &:= \{(g_2,...,g_d) \in G^{d-1} | C_{\gamma_d}(g_2,...,g_d) = G\} \\ &= \{(g_2,...,g_d) \in G^{d-1} | \gamma_{d-1}(g_2,...,g_d) \in Z(G)\}. \end{aligned}$$

La cardinalità di quest'insieme è:

$$|BAD| = |\{(g_2,...,g_d) \in (G/Z(G))^{d-1} | \gamma_{d-1}(g_2,...,g_d) = 1\}| \cdot |Z(G)|^{d-1}.$$

Quindi $G/Z(G)$ non soddisfa $\gamma_{d-1} \equiv 1$. Per ipotesi induttiva esiste una costante δ_{d-1} tale che

$$|\{(g_2,...,g_d) \in (G/Z(G))^{d-1} | \gamma_{d-1}(g_2,...,g_d) = 1\}| \leq \delta_{d-1} \cdot |G/Z(G)|^{d-1}.$$

Dunque

$$|BAD| \leq \delta_{d-1} |G|^{d-1},$$

e quindi possiamo prendere $\delta_{BAD} = \delta_{d-1}$. Se $(g_2,...,g_d) \notin BAD$, abbiamo

$$C_{\gamma_d}(g_2,...,g_d) = C_G(\gamma_{d-1}(g_2,...,g_d)),$$

che è un sottogruppo proprio di G, e pertanto

$$|C_G(\gamma_{d-1}(g_2,...,g_d))| \leq \frac{1}{2}|G|.$$

Quindi possiamo prendere $\delta_{GOOD} = \frac{1}{2}$. Questo ci dà un limite superiore per la probabilità:

$$P_{\gamma_d=1}(G) \leq \frac{1}{2} + \frac{1}{2}\delta_{d-1} := \delta_d.$$

Poiché, per il teorema di Gustafson, $\delta_2 = \frac{5}{8}$, otteniamo $\delta_d = 1 - \frac{3}{2^{d+1}}$. Infine, si ottiene l'uguaglianza in $P_{\gamma_d=1}(G)$ per ogni d considerando il gruppo diedrale di ordine 2^{n+1}, i.e.,

$$D_{2^{n+1}} = \langle a, b : a^{2n} = b^2 = 1, bab = a^{-1} \rangle.$$

□

Il medesimo argomento funziona più in generale.

Proposizione 3.8 (P. Moravec, 2019 [13])**.** *Sia w una parola in $d-1$ variabili, e supponiamo che esista $\eta = \eta(w) < 1$ tale che, per ogni gruppo finito G, se $P_{w=1}(G) > \eta$, allora $w \equiv 1$. Sia*

$$\tilde{w}(x_1, x_2, ..., x_d) := [x_1, w(x_2, ..., x_d)].$$

Allora ogni gruppo finito G soddisfa $\tilde{w} \equiv 1$ oppure

$$P_{\tilde{w}=1}(G) \leq \frac{1}{2} + \frac{1}{2}\eta(w).$$

Abbiamo quindi ottenuto che ogni parola della forma $\tilde{w}$ soddisfa un gap di probabilità, e vi possiamo pertanto applicare il teorema 3.3.

Bibliografia

[1] A. Abdollahi, A. Azad, A. Mohammadi Hassanabadi, and M. Zarrin. B. H. Neumann's question on ensuring commutativity of finite groups. *Bull. Austral. Math. Soc.*, 74(1):121–132, 2006.

[2] R. A. Bryce. Ensuring a finite group is supersoluble. *Bull. Austral. Math. Soc.*, 74:219–226, 2006.

[3] C. Delizia, U. Jezernik, P. Moravec, and C. Nicotera. Gaps in probabilities of satisfying some commutator-like identities. *Israel J. Math.*, 237(1):115–140, 2020.

[4] P. Erdős. On extremal problems of graphs and generalized graphs. *Israel J. Math*, 2(3):183–190, 1964.

[5] A. Erfanian, R. Rezaei, and P. Lescot. On the relative commutativity degree of a subgroup of a finite group. *Comm. Algebra*, 35(12):4183–4197, 2007.

[6] R. M. Guralnick and J. S. Wilson. The probability of generating a finite soluble group. *Proc. London Math. Soc.*, 81(2):405–427, September 2000.

[7] W. H. Gustafson. What is the probability that two group elements commute? *Amer. Math. Month.*, 80(9):1031–1034, 1973.

[8] T. Kővári, V. T. Sós, and P. Turán. On a problem of Zarankiewicz. *Colloq. Math.*, 3(1):50–57, 1954.

[9] A. Lucchini. Applying the Kővári-Sós-Turán theorem to a question in group theory. *Comm. Algebra*, 48(11):4996–4998, 2020.

[10] A. Lucchini. A generalization of a question asked by B. H. Neumann. *Results Math.*, 77(5):181, July 2022.

[11] J. Ma, X. Yuan, and M. Zhang. Some extremal results on complete degenerate hypergraphs. *J. Combin. Theory Ser.*, A 154:598–609, 2018.

[12] N. E. Menezes, M. Quick, and C. M. Roney-Dougal. The probability of generating a finite simple group. *Israel J. Math.*, 198:371–392, 2013.

[13] P. Moravec. Gaps in probabilities of satisfying some commutator identities. In *SandGAL Cremona*, 2019.

[14] B. H. Neumann. On a conjecture of Hanna Neumann. *Proc. Glasgow Math. Assoc.*, 3:13–17, 1956.

[15] B. H. Neumann. A problem of Paul Erdős on groups. *J. Aust. Math. Soc.*, 21(4):467–472, 1976.

[16] B. H. Neumann. Ensuring commutativity of finite groups. *J. Aust. Math. Soc.*, 71(2):233–234, 2001.

[17] L. Pyber. The number of pairwise non-commuting elements and the index of the centre in a finite group. *J. London Math. Soc.*, 35(2):287–295, April 1987.

[18] M. Zarrin. Ensuring a group is weakly nilpotent. *Comm. Algebra*, 40(12):4739–4752, October 2012.