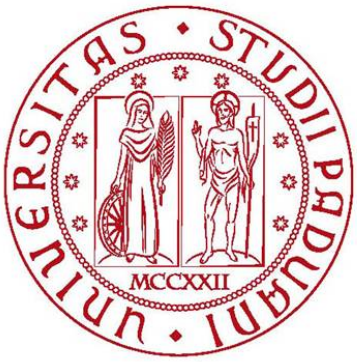

UNIVERSITA' DEGLI STUDI DI PADOVA

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea Magistrale in Matematica

LA PROBABILITA' DI GENERARE I SOTTOGRUPPI MASSIMALI DEI GRUPPI ALTERNI E SIMMETRICI

Relatore:
Prof. Andrea Lucchini

Laureanda:
Ilaria Rigovacca
Matricola 1179926

Anno accademico 2018-2019

5 Luglio 2019

Indice

Introduzione

Questo studio si apre introducendo e descrivendo oggetti e risultati inerenti ai gruppi di permutazione. Un gruppo di permutazione non è altro che un sottogruppo del gruppo simmetrico $Sym(\Omega)$, con Ω un qualsiasi insieme di elementi; in particolare, se Ω è un insieme finito di n elementi, scriveremo semplicemente Sym_n piuttosto che $Sym(\Omega)$.
Il sottogruppo di Sym_n contenente tutte le permutazioni pari prende il nome di gruppo alterno e viene indicato con Alt_n.
Lo scopo del capitolo 1 è quello di presentare e comprendere il Teorema di O'Nan-Scott, di cui non verrà fornita la dimostrazione in quanto non strettamente necessaria ai fini di questo lavoro. Tale teorema rappresenta un risultato fondamentale nello studio dei gruppi di permutazione, in quanto permette di classificare in 5 tipologie differenti i sottogruppi massimali del gruppo di permutazione $G \in \{Alt_n, Sym_n\}$. Nel dettaglio, un sottogruppo massimale di tale G può essere di tipo intransitivo, imprimitivo, affine, diagonale o almost simple: ecco quindi che per capire queste diverse tipologie risulta indispensabile introdurre concetti quali la transitività, la primitività ed il prodotto semidiretto, necessario per sviluppare il prodotto intrecciato e quindi per costruire i sottogruppi imprimitivi. Verranno poi descritti e costruiti i vari tipi di sottogruppi menzionati nel teorema di O'Nan-Scott.

Grazie ad un teorema provato nel 2018 da Lucchini, Marion e Tracey è noto che tali sottogruppi massimali possono essere generati al più da 4 elementi: lo scopo finale di questa tesi sarà quello di determinare asintoticamente con quanta probabilità è possibile generare tali sottogruppi con 4 elementi casuali.
Per fare questo si rende indispensabile la "Teoria delle Corone", sviluppata nel 2003 da Lucchini e Detomi ed affrontata nel secondo capitolo di questa tesi.
Dato un gruppo finito G indichiamo con $P_G(t)$ la probabilità che t elementi casuali appartenenti a G generino G stesso. Chiaramente, affinchè $P_G(t) > 0$, deve verificarsi la condizione $t \geq d(G)$, dove $d(G)$ indica il minor numero di elementi richiesti per generare G.
Nel calcolo di tale probabilità i sottogruppi normali di G giocano un ruolo fondamentale; se N è un sottogruppo normale di G e $P_{G,N}(t)$ è la probabilità di generare

G con t elementi posto che essi generino N, infatti:

$$P_G(t) = P_{G/N}(t)P_{G,N}(t).$$

Nel 1959 Gaschütz dimostrò una formula in grado di calcolare $P_{G,N}(t)$ (e di conseguenza $P_G(t)$) nel caso in cui G fosse un gruppo risolubile, cioè nel caso in cui fosse possibile trovare una serie principale di G in cui ogni fattore principale risultasse abeliano. In particolare, evidenziò come tale probabilità fosse indipendente dalla scelta della serie principale.

Successivamente Lucchini e Detomi svilupparono la "Teoria delle Corone", grazie alla quale riuscirono a generalizzare il risultato di Gaschütz al caso in cui G fosse un generico gruppo finito.

Nel secondo capitolo di questa tesi percorreremo quindi inizialmente i risultati di Gaschütz per poi introdurre gli oggetti necessari per affrontare la Teoria delle Corone.

Prima di applicare i risultati appena citati per studiare la probabilità di generare i sottogruppi massimali di $G \in \{Sym_n, Alt_n\}$, nel terzo capitolo vedremo un'applicazione della teoria delle Corone in un caso interessante ed indipendente dai gruppi di permutazione. Studieremo, infatti, il valore asintotico di $P_G(t)$ nel caso in cui G sia un gruppo almost simple, cioè tale che $S \leq G \leq Aut(S)$, con S gruppo semplice non abeliano. Giungeremo quindi a confrontare tale valore con quello che si ottiene per generare un gruppo semplice: mentre quest'ultima probabilità tende asintoticamente ad 1, la prima coinvolge la funzione Zeta di Riemann e risulta essere asintoticamente pari a $\frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\left(1-\frac{4}{2^s}\right)$.

Nel quarto capitolo, infine, sfrutteremo la Teoria delle Corone per studiare la probabilità asintotica $P_H(4)$ al variare di H tra i sottogruppi massimali di Sym_n e di Alt_n, classificati nel teorema di O'Nan-Scott. Non solo: dal risultato già precedentemente richiamato di Lucchini, Marion e Tracey emerge come i sottogruppi massimali di tipo intransitivo, imprimitivo e affine siano in realtà 2-generati; per queste tre tipologie sarà quindi interessante studiare anche l'andamento asintotico di $P_H(2)$.
In definitiva, risulterà possibile confrontare le probabilità ottenute nelle diverse tipologie di sottogruppi massimali di permutazione e determinare infine quale sia il caso peggiore. In altre parole, sarà possibile individuare quale tipologia di sottogruppi massimali di $G \in \{Sym_n, Alt_n\}$ ha la probabilità minore di essere generata da 4 elementi casuali.

Capitolo 1

Sottogruppi massimali di Sym_n

I sottogruppi massimali di Sym_n e di Alt_n sono stati classificati da O'Nan-Scott e sono di cinque diverse tipologie. Riporteremo tale risultato in seguito, dopo aver introdotto gli strumenti necessari alla comprensione dello stesso.

Sia Ω un insieme. Il *gruppo simmetrico* su Ω, indicato con $Sym(\Omega)$, è l'insieme di tutte le permutazioni di Ω: tale insieme forma un gruppo con l'operazione di composizione. Se Ω è un insieme finito di n elementi, scriviamo Sym_n per indicare il gruppo simmetrico su Ω.
Un *gruppo di permutazione* su Ω è un sottogruppo di $Sym(\Omega)$.
Il sottogruppo di Sym_n formato dalle permutazioni pari prende il nome di *gruppo alterno* e si indica con Alt_n o A_n.
Sia G un gruppo. Un' *azione* di G su Ω può essere vista come un omomorfismo $\phi : G \longrightarrow Sym(\Omega)$: ecco quindi che l'immagine di un'azione di G su Ω è un gruppo di permutazione, chiamato *gruppo di permutazione indotto da G su Ω* ed indicato con G^{Ω}.
Definiamo *grado di un gruppo di permutazione* la cardinalità dell'insieme Ω.
Un'azione si dice *fedele* se il suo kernel è l'identità. Osserviamo dunque che se un'azione è fedele, G è isomorfo a G^{Ω}.

Definizione 1.1. (Orbita di un punto)
Sia G un gruppo di permutazioni su un insieme Ω. Per ogni $\omega \in \Omega$ consideriamo l'insieme $orb_G(\omega) = \{\phi(\omega) | \phi \in G\} \subseteq \Omega$. Tale insieme prende il nome di orbita di ω sotto l'azione di G.

Osservazione 1.1. *Le orbite di ω, al variare di ω, formano una partizione dell'insieme Ω.*
Infatti, sia G un gruppo di trasformazioni che agisce sull'insieme Ω. Allora G definisce una relazione di equivalenza su Ω, data dalla regola $x \sim_G y$ se $y = \phi(x)$ per

qualche $\phi \in G$. La classe di equivalenza determinata da un elemento ω è l'insieme $G\omega = \{\phi(\omega)|\phi \in G\} = orb_G(\omega)$.

L'azione di G su Ω si dice *transitiva* se c'è solamente un'orbita.

Vediamo un teorema di struttura per i gruppi di permutazione.
Sia G un gruppo di permutazione su Ω con orbite Ω_i, dove $i \in I$ e I è un insieme di indici. G agisce su ogni insieme Ω_i, dunque induce dei gruppi di permutazioni transitivi G^{Ω_i}, chiamati i *costituenti transitivi di G*.

Teorema 1.1. *Ogni gruppo di permutazioni è un prodotto subcartesiano dei suoi costituenti transitivi.*

Definizione 1.2. (Stabilizzatore di un punto)
Sia G un gruppo di permutazioni di un insieme Ω. Per ogni $\omega \in \Omega$ consideriamo l'insieme $stab_G(\omega) = \{\phi \in G|\phi(\omega) = \omega\} \subseteq G$. Tale insieme prende il nome di stabilizzatore di ω in G.

1.1 Regolarità, transitività e primitività

Definizione 1.3. (Gruppi di permutazione semiregolari e regolari)
Un gruppo di permutazioni G si dice semiregolare *se solo l'identità ha un punto fissato, cioè se $stab_G(\omega) = 1\ \forall \omega \in \Omega$.*
G si dice regolare *se è transitivo e semiregolare.*

Definizione 1.4. (Transitività multipla)
Sia k un intero positivo minore di $|\Omega|$. Diremo che G è k-transitivo su Ω *se agisce transitivamente sull'insieme di tutte le k-uple di diversi elementi di Ω, dove l'azione è componente per componente, cioè $g((\alpha_1, \alpha_2, ..., \alpha_k)) = (g(\alpha_1), g(\alpha_2), ..., g(\alpha_k))$.*
Se tale azione invece è regolare, diremo che G è semplicemente k-transitivo su Ω.

Per $k > 1$, G è k-transitivo su Ω se e solo se:

- G è transitivo su Ω e
- $Stab_G(\alpha)$ è $(k-1)$-transitivo su $\Omega \setminus \{\alpha\}$

S_n è (semplicemente) n-transitivo, mentre A_n è $(n-2)$-transitivo (infatti ci sono esattamente 2 permutazioni in S_n che mappano una data $(n-2)$-upla in un'altra e differiscono per una trasposizione dei 2 elementi rimanenti, dunque una è pari e l'altra è dispari).

Definizione 1.5. (Blocchi e congruenza)
Sia G transitivo su Ω. Una congruenza *è una relazione di equivalenza su Ω G-invariante. Un* blocco *è un sottoinsieme Δ di Ω tale che $g(\Delta) = \Delta$ o $g(\Delta) \cap \Delta = \emptyset$, $\forall g \in G$.*

Banalmente, ogni classe di congruenza è un blocco, ed ogni blocco non vuoto è una classe di equivalenza in quanto viene mandato da G in un altro blocco disgiunto da quello di partenza (dalla definizione di blocco).
Esistono due relazioni di congruenza triviali per ogni gruppo G: la relazione di uguaglianza, in cui i blocchi sono i singoletti e la relazione universale, in cui $\alpha \sim \beta$ $\forall \alpha, \beta$, in cui c'è un unico blocco.

Definizione 1.6. (Primitività)
Diremo che G è imprimitivo *se ha una relazione di congruenza non triviale,* primitivo *altrimenti.*

Le uniche tipologie di blocco per un gruppo primitivo dunque sono il blocco totale o blocchi formati da singoli elementi.
Osserviamo poi che solamente un gruppo transitivo può avere la proprietà di essere primitivo.

Teorema 1.2. *Valgono le seguenti affermazioni:*

1. *Un gruppo 2-transitivo è primitivo.*
2. *Un sottogruppo normale di un gruppo primitivo è transitivo.*
3. *Un gruppo G transitivo su Ω è primitivo se e solo se $Stab_G(\alpha)$ è un sottogruppo massimale di G*
4. *Un gruppo è primitivo se esiste un sottogruppo massimale con cuore normale triviale.*

1.2 Prodotto semidiretto e prodotto intrecciato

Introduciamo infine i concetti di prodotto semidiretto ed intrecciato.

Proposizione 1.1. (Vedi [6], Lemma 3.1)
Siano G, G_0 due gruppi e supponiamo che $N \lhd G$ sia complementato da H e $N_0 \lhd G_0$ sia complementato da H_0.
Assumiamo $N \cong N_0$ e $H \cong H_0$, in cui ogni isomorfismo è denotato con $(\ )_0$, e supponiamo poi che $(n^h)_0 = (n_0)^{h_0}$, $\forall n \in N, h \in H$. Allora esiste ed è unico l'isomorfismo da G e G_0 che estende l'isomorfismo $N \longrightarrow N_0$ e $H \longrightarrow H_0$.

Teorema 1.3. *Siano H ed N due gruppi, e supponiamo che H agisca su N tramite automorfismo.*
Allora esiste un gruppo G contenente un sottogruppo normale $N_0 \cong N$, complementato da un sottogruppo $H_0 \cong H$, e tale che $\forall n \in N$ e $h \in H$, si abbia:

$$(n^h)_0 = (n_0)^{h_0}.$$

Qui, $n^h \in N$ è il risultato della data azione di h su n, mentre $(n_0)^{h_0} \in N_0$ è il risultato della coniugazione di n_0 tramite h_0 in G.

Dalla proposizione 1.1 segue che il gruppo G del teorema 1.3 è unicamente determinato da N, H, e dalla data azione tramite automorfismo di H su N: viene chiamato *prodotto semidiretto* di N tramite H rispetto all'azione data.
Inoltre, sempre dalla proposizione 1.1, ogni gruppo G con un sottogruppo normale N ed un complemento H è isomorfo al prodotto semidiretto di N tramite H. Indicheremo il prodotto semidiretto con $G = N \rtimes H$, specificando l'azione utilizzata che, come abbiamo visto, è essenziale nella definizione del prodotto semidiretto.
Osserviamo poi che il prodotto semidiretto risulta essere un prodotto diretto se e solo se $H_0 \lhd G$ e questo accade esattamente quando l'azione di coniugio di H_0 su N_0 è triviale, o equivalentemente, quando l'azione originale di H su N è triviale.
Identificheremo spesso N con N_0 e H con H_0 tramite l'isomorfismo $x \longmapsto x_0$, dunque scrivendo $G = N \rtimes H$ intendiamo $N \lhd G$, $G = NH$, $N \cap H = 1$ e come azione tramite automorfismo di H su N il coniugio.
Il prodotto semidiretto è utile per comprendere la nozione di prodotto intrecciato, che ora andremo ad introdurre.
Siano G, H due gruppi e sia Ω un insieme su cui agisce G. Sia B l'insieme di tutte le funzioni da Ω in H, e definiamo un'operazione su B in modo che sia un gruppo: se $f, g \in B$ allora fg è definito da $(fg)(\alpha) = f(\alpha)g(\alpha)$, con $\alpha \in \Omega$. E' facile vedere che B è un gruppo e in realtà coincide con il prodotto diretto esterno di $|\Omega|$ copie di H.
L'azione di G su Ω induce un azione tramite automorfismo di G su B: se vediamo B come prodotto diretto, possiamo descrivere l'azione di G su B come una semplice permutazione delle coordinate.
Vediamolo in un modo più preciso. Data $f \in B$ e $x \in G$, la funzione f^x su Ω è definita in modo tale che $f^x(\alpha \cdot x) = f(\alpha)$ o, equivalentemente, $f^x(\alpha) = f(\alpha \cdot x^{-1})$.
Definiamo ora $W = B \rtimes G$ con l'azione appena definita: W prende il nome di *prodotto intrecciato* di H con G e B, visto come sottogruppo di W, viene detto il *gruppo base* del prodotto intrecciato.
Solitamente il prodotto intrecciato di H con G viene indicato con $W = H \wr G$, ma tale notazione non menziona l'insieme Ω e l'azione di G su tale insieme.

Costruiamo ora il prodotto intrecciato di due gruppi di permutazione.[2]
Siano H e K due gruppi di permutazione sugli insiemi Γ e Δ rispettivamente e sia $\Omega = \Gamma \times \Delta$. Possiamo pensare ad Ω come ad un fascio di fibre costruite sull'insieme Δ, con la mappa di proiezione $(\gamma, \delta) \longmapsto \delta$: ogni fibra $\Gamma_\delta = \{(\gamma, \delta) : \gamma \in \Gamma\}$, per δ fissato, è in biiezione con Γ.
Sia poi B il prodotto cartesiano di $|\Delta|$ copie di H, in cui ogni copia agisce su ogni fibra così come H agisce su Γ. In questo modo B è l'insieme delle funzioni da Δ in H, con le operazioni definite punto a punto come sopra. L'azione è data da: $f \cdot (\gamma, \delta) = ((f(\delta))(\gamma), \delta)$ (notiamo che è ben definita in quanto $f(\delta) \in H$, e $h(\gamma) \in \Gamma$).
Sia poi T una copia di K, che permuta le fibre di Ω: $k \cdot (\gamma, \delta) = (\gamma, k \cdot \delta)$.
Il prodotto $B \rtimes T$ è il prodotto intrecciato di H e K, cioè $H \wr K = B \rtimes T$.
Osserviamo due proprietà di tale prodotto intrecciato:

- Se H e K sono transitivi su Γ e Δ rispettivamente, allora $H \wr K$ è transitivo su $\Omega = H \times K$.
- Se $|\Gamma|, |\Delta| > 1$, allora $H \wr K$ è imprimitivo. Possiamo vedere tale risultato in due modi: o identifichiamo le fibre come i blocchi, oppure definiamo una relazione di congruenza non triviale, cioè $(\gamma, \delta) \sim (\gamma', \delta')$ se e solo se $\delta = \delta'$.

E' possibile definire un'altra azione (diversa quindi dalla permutazione delle fibre e generalmente non imprimitiva) del prodotto intrecciato: definiamo l'*azione prodotto* sull'insieme delle sezioni globali del fascio di fibre, dove per *sezione globale* si intende un sottoinsieme contenente un punto per ogni fibra.
Formalmente, $H \wr K$ agisce sull'insieme delle funzioni da Δ in Γ, indicato con Γ^Δ; il gruppo base B (cioè l'insieme delle funzioni da Δ in H) agisce coordinata per coordinata e il gruppo T isomorfo a K permuta gli argomenti delle funzioni. In sostanza quindi, per $\phi \in \Gamma^\Delta$, $f \in B = H^\Delta$, poniamo $(f \cdot \phi)(\delta) = \phi(\delta) f(\delta)$, e per $k \in K$ poniamo $(k \cdot \phi)(\delta) = \phi(k^{-1}(\delta))$.
Si può dimostrare che l'azione prodotto di $H \wr K$ è primitiva se e solo se H è primitivo e non regolare su Γ, Δ è finito e K è transitivo su Δ.

1.3 Gruppi affini e gruppi diagonali

Sia V uno spazio vettoriale su un campo K.
Per ogni $a \in V$, la traslazione $t_a : x \longmapsto x + a$ è chiaramente una permutazione di V: le traslazioni formano dunque un sottogruppo di $Sym(V)$ isomorfo a V.
Le trasformazioni lineari $x \longmapsto Ax$, con $A \in GL(d, K)$, sono anch'esse permutazioni di V.

Definizione 1.7. (Gruppo affine)
Il sottogruppo di $Sym(V)$ generato da tutte le traslazioni e da tutte le trasformazioni lineari invertibili prende il nome di gruppo affine *e si indica con $AGL(d,K) \cong GL(d,K) \ltimes V$, dove l'azione di $GL(d,K)$ su V è quella naturale:*

$$(Bt_b)(At_a) = (BAt_{b+Ba})$$

Se il campo K ha ordine primo p, allora scriviamo $AGL(d,K) = AGL(d,p) = AGL_d(p)$.

Osserviamo dunque che un elemento del gruppo affine è completamente determinato una volta fissati la matrice invertibile $A \in GL(d,K)$ e il vettore di traslazione $a \in V$.
Ragioniamo sull'ordine del gruppo affine $AGL_d(p)$ nel caso in cui il campo K abbia ordine primo p:

- Caso $d = 1$: la matrice A in questo caso ha una sola entrata e l'unico vincolo è che sia diversa da 0 (dovendo essere invertibile). Abbiamo dunque $(p-1)$ scelte per fissare tale matrice. Il vettore di traslazione a invece può essere qualsiasi: abbiamo quindi p scelte per fissarlo.
  Ecco quindi che $|AGL_1(p)| = (p-1)p$

- Caso $d = 2$: la matrice A presenta due colonne. La prima colonna deve essere diversa da $(0,0)$ (si hanno quindi p^2-1 possibilità); la seconda colonna, affinchè la matrice sia invertibile, deve essere diversa da un multiplo della prima colonna (si hanno quindi p^2-p possibilità). Il vettore di traslazione a invece non ha vincoli: si hanno p^2 scelte per esso.
  Risulta quindi $|AGL_2(p)| = p^2(p^2-p)(p^2-1)$.

- Caso generale d: la matrice presenta d colonne, dunque seguendo la logica dei casi precedenti si hanno $\prod_{k=0}^{d-1}(p^d - p^k)$ possibilità, mentre per il vettore di traslazione si hanno p^d scelte.
  In definitiva dunque $|AGL_d(p)| = p^d \prod_{k=0}^{d-1}(p^d - p^k)$.

Possiamo dunque concludere che $AGL_d(p)$ risulta essere un sottogruppo di $Sym(p^d)$.

Definizione 1.8. (Gruppo semplice e gruppo almost simple)
Un gruppo G si dice semplice *se i suoi unici sottogruppi normali sono il sottogruppo banale e il gruppo G stesso.*
Un gruppo G si dice almost simple *se contiene un gruppo S semplice e non abeliano ed è contenuto nel gruppo degli automorfismi di S. In simboli: $S \leq G \leq Aut(S)$ con S gruppo semplice non abeliano.*

Sia ora S un gruppo semplice e consideriamo il gruppo $X = AutS \wr Sym(k) \cong Aut(S^k)$: tale isomorfismo è dato dal fatto che un elemento di $Aut(S^k)$ può agire sui singoli fattori (ottenendo così una base del prodotto intrecciato) o permutarli.
La base B di tale prodotto intrecciato è $Aut(S)^k$, quindi l'insieme delle k-uple $\{(\alpha_1, \alpha_2, ..., \alpha_k) | \alpha_i \in Aut(S)\}$.
Consideriamo ora l'insieme $B^* = \{(\alpha_1, \alpha_2, ..., \alpha_k) | \alpha_1 = \alpha_2 = ... = \alpha_k \text{ mod } S\}$: ogni elemento di tale insieme lo si può scrivere come $(\alpha s_1, \alpha s_2, ..., \alpha s_k)$ con $s_i \in S, \alpha \in \Sigma$, essendo Σ un fissato trasversale di S in $Aut(S)$.
Definiamo poi $Out(S) = Aut(S)/S$, dove abbiamo identificato S con $Inn(S)$: data la precedente osservazione, la cardinalità di B^* risulta essere $|B^*| = |S^k||Out(S)|$.
In secondo luogo osserviamo che l'insieme B^* viene preservato dall'azione di $Sym(k)$ su B: in altre parole, notiamo che se permutiamo le coordinate di un elemento di B^* fissato, viene chiaramente preservata la proprietà "$\alpha_1 = ... = \alpha_k$ mod S".
E' dunque possibile considerare il nuovo gruppo $Y = B^* \rtimes Sym(k)$.

Notiamo immediatamente che S^k è un sottogruppo di B^*; inoltre S^k risulta essere un sottogruppo normale di Y: essendo un elemento di S^k una k-upla di elementi del gruppo semplice S, infatti, se si permutano le coordinate (sotto l'azione di $Sym(k)$) ogni entrata continua ad appartenere ad S e lo stesso accade sotto l'azione di elementi di B^* in quanto $S \trianglelefteq Aut(S)$.
Ecco quindi che possiamo quozientare Y con S^k ottenendo così

$$Y/S^k = B^*/S^k \rtimes Sym(k)S^k/S^k = B^*/S^k \rtimes Sym(k).$$

Gli elementi di B^*/S^k li possiamo scrivere come k-uple $(\alpha S, \alpha S, ..., \alpha S)$ e se permutiamo tali coordinate agendo tramite $Sym(k)$ otteniamo lo stesso elemento: possiamo quindi scrivere Y/S^k come prodotto diretto

$$Y/S^k = B^*/S^k \times Sym(k) \cong Out(S) \times Sym(k).$$

Definizione 1.9. (Gruppo diagonale)
L'estensione $Y = S^k.(Out(S) \times Sym(k))$ *prende il nome di* gruppo diagonale*, dove* $S^k \trianglelefteq Y$ *e* $Y/S^k = Out(S) \times Sym(k)$.

Consideriamo ora il sottogruppo $M = \langle(\alpha, \alpha, ..., \alpha)\sigma\rangle$, con $\alpha \in Aut(S)$ e $\sigma \in Sym(k)$ e l'azione di Y sui laterali di M in Y.
Chiaramente $|M| = |Aut(S)||Sym(k)|$ e $|Y| = |S^k||Out(S)||Sym(k)|$ e di conseguenza

$$|Y/M| = \frac{|S^k||Out(S)||Sym(k)|}{|Aut(S)||Sym(k)|} = \frac{|S^k||Out(S)||Sym(k)|}{|S||Out(S)||Sym(k)|} = |S|^{k-1}$$

Vediamo poi che Y è un gruppo primitivo dimostrando la massimalità di M (punto

4, teorema 1.2).
Sia $\tau = (t_1, t_2, ..., t_{k-1}, 1)$ un elemento di $Y \setminus M$, ove $t_i \in S$: quanto vogliamo dimostrare è che, detto Z il gruppo generato da M e da τ, vale $Z = \langle M, \tau \rangle = Y$.
Per mostrare questo richiamiamo prima il concetto di prodotto sottodiretto e un risultato sulla costruzione di quest'ultimo nel caso dei gruppi semplici:

Definizione 1.10. (Prodotto sottodiretto)
$H \leq S^k = S_1 \times ... \times S_k$ *si dice* prodotto sottodiretto *di* S^k *se ogni proiezione è suriettiva, cioè* $\pi_i(H) = S_i \ \forall i$.

Proposizione 1.2. *Se* H *è un prodotto sottodiretto di gruppi semplici* $S_1 \times ... \times S_k$, *allora* H *si può scrivere come prodotto diretto di diagonali generalizzate* $\Delta_1 \times ... \times \Delta_u$, *dove* u *è il numero di blocchi della partizione di* k *e su ogni blocco le entrate sono legate da automorfismi di* S *(ad esempio se si ha un blocco di dimensione 3, la prima entrata* x *viene scelta arbitrariamente, la seconda entrata è l'immagine tramite* α_1 *di* x *e la terza è l'immagine tramite* α_2 *di* x, *ove* $x \in S$, $\alpha_1, \alpha_2 \in Aut(S)$*).*

Torniamo alla dimostrazione della massimalità di M in Y.
Consideriamo l'intersezione R di Z con S^k, $R = Z \cap S^k$. Ora in R è contenuta la diagonale con tutti gli elementi uguali (che chiameremo D): R risulta quindi essere un prodotto sottodiretto di S^k, in quanto contenendo la diagonale D tutte le proiezioni risultano essere suriettive. Attraverso la proposizione 1.2 riusciamo a scrivere R come prodotto di diagonali generalizzate: $R = \Delta_1 \times ... \times \Delta_u$. Tale prodotto di diagonali generalizzate però deve contenere la diagonale D e dunque gli automorfismi dei vari blocchi Δ_i non possono che essere l'identità: abbiamo così ottenuto un raffinamento della diagonale D contenuta in R.
Osserviamo ora che $Z \cap S^k \trianglelefteq Z$: quando si agisce con un qualsiasi elemento di M dunque si normalizza R (e ricordiamo che M contiene tutte le possibili permutazioni). Da una parte quindi si ha un prodotto raffinato di diagonali che viene fissato da qualsiasi permutazione, dall'altro, per la transitività, si riesce sempre a trovare una permutazione di $Sym(k)$ che non rispetti la partizione fissata: l'unico modo per non giungere ad un assurdo dunque è che $M = Y$.

1.4 Teorema di O'Nan-Scott

Dopo aver appreso tali nozioni siamo quindi pronti a comprendere le 5 tipologie di sottogruppi massimali di Sym_n o di Alt_n, descritte nel teorema di O'Nan-Scott.

Teorema 1.4. *(O'Nan-Scott)(vedi [9], Teorema 5.5)*
Sia $G = Sym_n$ *o* $G = Alt_n$, *con* $n \geq 5$. *Sia* H *un sottogruppo massimale di* G. *Allora vale una delle seguenti asserzioni:*

1. *H è intransitivo: $H = (Sym_k \times Sym_{n-k}) \cap G$ con $1 \leq k < n/2$.*

2. *H è affine: $H = AGL_d(p) \cap G$ dove $n = p^d$, p è un numero primo e $d \geq 1$.*

3. *H è imprimitivo o di tipo intrecciato: $H = (S_k \wr S_t) \cap G$, dove $n = kt$ o $n = k^t$ per qualche $t > 1$.*

4. *H è di tipo diagonale: $H = (S^k.(Out(S) \times Sym_k)) \cap G$, dove S è semplice e non abeliano e $n = |S|^{k-1}$ per qualche $k > 1$.*

5. *H è almost simple.*

Osservazione 1.2.
Osserviamo che la tipologia 3 comprende entrambe le azioni del prodotto intrecciato che abbiamo visto. Considerando l'azione di permutazione delle fibre, si ottiene H imprimitivo con $n = kt$, considerando invece l'azione prodotto si ottiene il caso $n = k^t$.

Nel capitolo 4 saremo interessati a comprendere la parità di H, in modo da determinare se H è un sottogruppo massimale di Alt_n o di Sym_n. In alcuni casi, infatti, pur considerando $G = Sym_n$, il sottogruppo H è contenuto nel gruppo alterno ed è quindi un sottogruppo massimale di quest'ultimo.

Capitolo 2

Corone e probabilità di generare un gruppo finito

In questo capitolo introduciamo le nozioni che saranno alla base dei risultati successivi e che permetteranno di calcolare le probabilità cui siamo interessati.

Sia G un gruppo finito e sia t un intero non negativo. Indichiamo con $P_G(t)$ la probabilità che t elementi casuali generino G.
Come richiamato in [3], tale probabilità si può scrivere come una serie di Dirichlet finita $\sum_{n\in\mathbb{N}} a_n n^{-t}$, dove $a_n \in \mathbb{Z}$ e $a_n = 0$ se n divide $|G|$; si può dunque parlare di $P_G(s)$ per ogni numero complesso s.
Il fatto che si possa scrivere come una tale serie di Dirichlet è interessante, in quanto l'anello delle serie di Dirichlet finite a coefficienti in $\mathbb{Z}$ ha la proprietà di avere unica fattorizzazione: è proprio a questo proposito che i sottogruppi normali di G giocano un ruolo fondamentale.
Sia quindi N un sottogruppo normale di G e sia t un intero soddisfacente $t \geq d(G/N)$, definiamo

$$P_{G,N}(t) := \frac{P_G(t)}{P_{G/N}(t)}.$$

Come si può evincere dalla formula, $P_{G,N}(t)$ rappresenta la probabilità che t elementi generino G, posto che generino G/N.
Osserviamo che $P_{G,N}(t)$ è definita solo per interi positivi sufficientemente grandi. In realtà esiste una funzione $P_{G,N}(s)$, $s \in \mathbb{C}$, che interpola i valori $P_{G,N}(t)$ e che può essere scritta come serie di Dirichlet finita a coefficienti interi. Notiamo poi che se una serie di Dirichlet finita f è nulla se calcolata su interi sufficientemente grandi, allora $f(s) = 0$ per ogni $s \in \mathbb{C}$: in questo modo si ha l'unicità della serie $P_{G,N}(s)$ che interpola $P_{G,N}(t)$.
Di conseguenza tutte le fattorizzazioni che vedremo che coinvolgeranno oggetti co-

me $P_{G,N}$ e $P_G = P_{G,G}$ valgono e sono provate per interi sufficientemente grandi (in particolare $t \geq d(G)$), ma restano valide anche per ogni numero complesso s.

Alla luce di quanto appena visto, possiamo dunque fattorizzare $P_G(s)$ (o, indifferentemente $P_{G,G}(s)$)) come segue:

$$P_G(s) = P_{G/N}(s)P_{G,N}(s) \tag{2.1}$$

Consideriamo ora la serie principale di un gruppo finito G, cioè:

$$1 = N_0 < N_1 < ... < N_l = G$$

con $N_i \trianglelefteq G$ t.c. $\frac{N_{i+1}}{N_i} \underset{min}{\trianglelefteq} \frac{G}{N_i}$.

Iterando la formula 2.1 otteniamo un'espressione per $P_G(s)$ come prodotto indicizzato sui fattori principali della serie:

$$P_G(s) = \prod_i P_{G/N_{i-1},N_i/N_{i-1}}(s) \tag{2.2}$$

Osserviamo poi che se $N \leq Frat(G)$ (ricordiamo che $Frat(G) := \bigcap M$ con $M \leq_{max} G$), allora $P_{G,N}(s) = 1$ per ogni s: ecco quindi che il prodotto in 2.2 è in realtà indicizzato sui fattori principali non-Frattini della serie.
Riporteremo in seguito un risultato presente in [3], che afferma che i fattori presenti nell'espressione 2.2 di $P_G(s)$ sono indipendenti dalla scelta della serie principale del gruppo G preso in considerazione.

Per studiare $P_G(s)$ risulta quindi di fondamentale importanza riuscire a calcolare $P_{G,N}(s)$ quando N è un sottogruppo normale minimale di G.

2.1 Caso particolare: G risolubile

Nel caso in cui N è un gruppo abeliano, è sufficiente sfruttare la seguente proposizione per calcolare $P_{G,N}(s)$:

Proposizione 2.1. *[citata in [3]]*
Sia N un sottogruppo abeliano, minimale e normale di un gruppo G finito e sia $t \geq d(G/N)$. Sia $c(N)$ il numero dei complementi di N in G.

- *Se $N \leq Frat(G)$, allora $P_{G,N}(t) = 1$*
- *Se $N \not\leq Frat(G)$, allora $P_{G,N}(t) = 1 - \frac{c(N)}{|N|^t}$*

Come conseguenza della proposizione 2.1 e della formula 2.2 si ha un'espressione diretta per $P_G(s)$ nel caso in cui si prenda G gruppo risolubile (cioè G tale che esiste una serie $1 = N_0 \lhd N_1 \lhd ... \lhd N_l = G$ t.c. $\frac{N_{i+1}}{N_i}$ siano abeliani):

$$P_G(s) = \prod_{1 \leq i \leq l} P_{G/N_{i-1}, N_i/N_{i-1}}(s) = \prod_{1 \leq i \leq l} 1 - \frac{c(N_i/N_{i-1})}{|N_i/N_{i-1}|^s} \tag{2.3}$$

In realtà Gaschütz è riuscito ad ottenere, dopo aver calcolato il valore esatto del numero dei complementi $c(N_i/N_{i-1})$, una formula per $P_G(s)$ dipendente solamente dai fattori principali di G visti come G-moduli.
Richiamiamo la nozione di G-modulo e di omomorfismo di G-moduli che, come vedremo, sarà utile in seguito.

Definizione 2.1. (G-modulo)
Un G-modulo *A è un gruppo abeliano A insieme ad un'azione di G su A compatibile con la struttura di A come gruppo abeliano, cioè una mappa*

$$\begin{aligned} G \times A &\longrightarrow A \\ (g, a) &\longmapsto g \cdot a \end{aligned}$$

tale che:

1. $1 \cdot a = a, \quad \forall a \in A$
2. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a, \quad \forall a \in A,\ g_1, g_2 \in G$
3. $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2, \quad \forall a_1, a_2 \in A,\ g \in G$

Un G-modulo è triviale *se $g \cdot a = a\ \forall a \in A, \forall g \in G$. In altre parole, cioè, se l'azione di G su A è triviale.*

Definizione 2.2. (omomorfismo di G-moduli)
Un omomorfismo di G-moduli *$\phi : A \longrightarrow B$, con A e B G-moduli, è un omomorfismo di gruppi abeliani soddisfacente la condizione $\phi(g \cdot a) = g \cdot \phi(a)$.*
L'inisieme di tali omomorfismi viene indicato con la notazione $Hom_G(A, B)$.

Siamo quindi in grado di comprendere tutti gli oggetti introdotti nella formula di Gaschütz per $P_G(s)$, ove G è un gruppo risolubile.

Teorema 2.1. *Sia G un gruppo risolubile finito. Allora*

$$P_G(s) = \prod_M \Bigg(\prod_{0 \leq i \leq \delta_G(M)-1} 1 - \frac{|End_G(M)|^i |M|^{\theta_G(M)}}{|M|^s} \Bigg),$$

dove M è un G-modulo irriducibile G-isomorfo ad un fattore principale di G complementato, $\delta_G(M)$ è il numero di fattori principali G-isomorfi ad M, $\theta_G(M) = 0$ se M è triviale come G-modulo e $\theta_G(M) = 1$ altrimenti.
Inoltre, tale fattorizzazione di $P_G(s)$ è indipendente dalla scelta della serie principale.

Per ottenere tale formula, è necessario osservare che, com'è noto, il numero $c(N)$ di complementi coincide con la cardinalità dell'insieme $Der(G/N, N)$ delle derivazioni da G/N in N, che può essere calcolato utilizzando il teorema 2 presente in [3]. Combinando la proposizione 2.1 con tale teorema segue che, detto

$$\chi = \{i | 1 \leq i \leq l \text{ e } N_i/N_{i-1} \cong_G M\},$$

allora

$$\prod_{i \in \chi} P_{G/N_{i-1}, N_i/N_{i-1}}(t) = \prod_{0 \leq i \leq \delta_G(M)-1} 1 - \frac{|End_G M|^i |Der(G/C_G(M), M)|}{|M|^t} \qquad (2.4)$$

indipendentemente dalla scelta della serie principale.
Se poi G è risolubile allora $|Der(G/C_G(M), M)| = |M|^{\theta_G(M)}$, da cui segue immediatamente il teorema 2.1.

2.2 Caso generale

Al fine di indagare il caso in cui in cui i fattori principali non siano abeliani, introduciamo il concetto di corona, passando attraverso altre definizioni.

2.2.1 G-gruppi

Definizione 2.3. (G-gruppo)
Un G-gruppo *A è un gruppo A con un omomorfismo $\theta : G \longrightarrow Aut(A)$ (dunque è un gruppo A su cui agisce il gruppo G).*
Come notazione scriveremo $a^g := a^{\theta(g)}$, con $a \in A$, $g \in G$.

- *Un G-gruppo si dice* irriducibile *se non è possibile trovare alcun sottogruppo proprio invariante rispetto l'azione.*
- *Dato un $G-$gruppo si ha il prodotto semidiretto GA corrispondente, dove la moltiplicazione è data da $g_1a_1 \cdot g_2a_2 = g_1g_2a_1{}^{g_2}a_2$, ove $g_i \in G$, $a_i \in A$.*

E' immediato osservare che $ker(\theta) = C_G(A)$, infatti $ker(\theta) = \{g \in G | \theta(g) = id\} = \{g \in G | a^g = a \ \forall a \in A\}$.

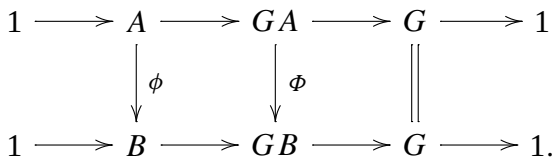

Figura 2.1: Diagramma gruppi G-equivalenti

Definizione 2.4. (G-isomorfismo)
Due G-gruppi A e B sono detti G-isomorfi *(e scriveremo $A \cong_G B$) se esiste un isomorfismo $\phi : A \longrightarrow B$ t.c. $a^{g\phi} = a^{\phi g}$, con $a \in A$, $g \in G$.*
ϕ è detto G-isomorfismo.

Definizione 2.5. (G-equivalenza)
Due G-gruppi A e B sono detti G-equivalenti *(e scriveremo $A \sim_G B$) se esiste un isomorfismo $\Phi : GA \longrightarrow GB$ t.c. il diagramma in figura 2.1 commuti.*

La G-equivalenza è una relazione di equivalenza e vale il fatto che due G-gruppi G-isomorfi sono G-equivalenti (infatti se $\phi : A \longrightarrow B$ è un isomorfismo, allora $(ga)^{\Phi} = ga^{\phi}$ definisce un isomorfismo $\Phi : GA \longrightarrow GB$ che fa commutare il diagramma); il viceversa vale solamente in caso di G-gruppi abeliani.

Ricordiamo che un gruppo è *primitivo* se ha un sottogruppo massimale con cuore triviale (Teorema 1.2, punto 4).
Se G è un gruppo primitivo, allora $soc(G)$ può essere di tre diversi tipi:

- sottogruppo normale minimale abeliano (I);
- sottogruppo normale minimale non-abeliano (II);
- prodotto di due sottogruppi normali minimali non-abeliani (III).

Definizione 2.6. *G è* primitivo di tipo I, II, III *in base al tipo di $soc(G)$.*
Nei primi due casi diremo che G è monolitico.

Definizione 2.7. (G-relazione)
Due fattori principali di un gruppo finito G si dicono G-relazionati *se sono G-isomorfi tra loro oppure se sono G-isomorfi ai due sottogruppi normali minimali di un'immagine epimorfa primitiva di tipo III di G.*

Come menzionato in [3], dato che due fattori principali sono G-relazionati se e solo se essi sono G-equivalenti come G-gruppi, due fattori principali G-equivalenti

risultano essere o G-isomorfi tra loro o a due fattori principali di G aventi un complemento comune (che è un sottogruppo massimale di G).

Si ricordi infine che il gruppo Frattini $Frat(G)$ di un gruppo G finito non triviale è nilpotente. La seguente terminologia sarà usata frequentemente nel seguito e nei capitoli successivi.

Definizione 2.8. (Fattore principale Frattini e complementato)
Sia G un gruppo finito non triviale e sia H/K un fattore principale di G.

1. *Diremo che H/K è* Frattini *se $H/K \leq Frat(G/K)$.*

2. *Diremo che H/K è* complementato *se esiste un sottogruppo U di G tale che $UH = G$ e $U \cap H = K$. Il gruppo U viene detto* complemento *di H/K in G.*

Dal momento che il sottogruppo $Frat(G)$ di un gruppo G è nilpotente e che l'unico complemento di $Frat(G)$ è G stesso, ne segue immediatamente la seguente proposizione:

Proposizione 2.2. *(vedi [9], Lemma 2.4)*
Sia G un gruppo finito non triviale e sia $A = H/K$ un fattore principale di G.

1. *Se A è abeliano allora A è non-Frattini se e solo se A è complementato;*

2. *Se A è non abeliano, allora A è non-Frattini.*

2.2.2 Corone

Grazie alla terminologia appena introdotta possiamo avvicinarci al concetto di corona.

Definizione 2.9. (A-corona)
Sia A un G-gruppo irriducibile. Poniamo

$$\begin{aligned} I_G(A) &= \{g \in G | g \text{ induce un automorfismo interno in } A\} \\ &= \{g \in G | \exists a \in A \text{ tale che } x^g = x^a \quad \forall x \in A\} \end{aligned}$$

e

$$R_G(A) = \bigcap \{R \leq I_G(A) \mid R \trianglelefteq G,\ I_G(A)/R_G(A) \sim_G A,\ I_G(A)/R \text{ non-Frattini}\}$$

se l'intersezione non è vuota, altrimenti poniamo $I_G(A) = R_G(A)$.
Il gruppo quoziente $I_G(A)/R_G(A)$ prende il nome di A-corona di G.

Osservazione 2.1. *Notiamo subito che se due G-gruppi A e B sono G-equivalenti, si ha*

$$I_G(A) = I_G(B) \text{ e } R_G(A) = R_G(B);$$

di conseguenza A e B definiscono la stessa corona.

Nella proposizione seguente elenchiamo alcune proprietà delle corone.

Proposizione 2.3. *(Vedi [3])*
Sia A un G-gruppo irriducibile e sia $I/R := I_G(A)/R_G(A)$ la A-corona. Allora:
1. $R = I$, e in questo caso poniamo $\delta_G(A) = 0$, oppure $I/R = soc(G/R)$ ed è il prodotto diretto di $\delta_G(A)$ sottogruppi normali minimali G-equivalenti ad A;
2. Ogni serie principale di G contiene esattamente $\delta_G(A)$ fattori principali non-Frattini G-equivalenti ad A;
3. Se A è abeliano allora I/R ha un complemento in G/R;
4. Due diversi sottogruppi normali minimali di una corona hanno un complemento in comune;
5. Due fattori principali di G non-Frattini sono G-relazionati se e solo se essi definiscono la stessa corona.

Corollario 2.1. *Gli unici fattori principali non-Frattini di una serie passante per $I_G(A)$ e $R_G(A)$, G-equivalenti ad A sono quelli tra $R_G(A)$ e $I_G(A)$.*
In particolare, sia H/K un fattore principale di G non-Frattini, allora $H/K \sim_G A$ se e solo se $KR_G(A) \leq HR_G(A) \leq I_G(A)$.

Proseguiamo ora col dare altre definizioni, al fine di capire al meglio la natura di $G/R_G(A)$.

Definizione 2.10. (Crown-based power)
Sia L un gruppo primitivo monolitico (quindi primitivo di tipo I o II) e sia A il suo unico sottogruppo normale minimale. Sia k un intero positivo e L^k il prodotto diretto k-dimensionale di L.
Il sottogruppo L_k definito da

$$L_k := \{(l_1, ..., l_k) \in L^k | l_1 \equiv ... \equiv l_k \ mod\ A\ \} \leq L^k$$

viene detto la crown-based power di L di dimensione k.

Banalmente, $soc(L_k) = A^k$, $L_k/soc(L_k) \cong L/soc(L)$ ed il gruppo quoziente di L_k su un qualsiasi sottogruppo normale minimale è isomorfo a L_{k-1}, con $k > 1$.

Osserviamo poi che, se prendiamo L un gruppo primitivo monolitico con $A := soc(L)$, allora in L_k ogni sottogruppo normale minimale è L_k-equivalente ad A, la A-corona risulta essere $soc(L_k)$ e $\delta_{L_k}(A) = k$.

Definizione 2.11. (Gruppo primitivo monolitico associato)
Sia A un G-gruppo irriducibile con $\delta_G(A) \neq 0$. Sia poi $\rho : G \longrightarrow Aut(A)$ definita da $g \longmapsto g^\rho$, con $g^\rho : a \longmapsto a^g \ \forall a \in A$.
Il gruppo primitivo monolitico associato ad A *è definito come*

$$L_A = \begin{cases} G^\rho A \cong (G/C_G(A))A & \text{se } A \text{ abeliano} \\ G^\rho \cong (G/C_G(A)) & \text{altrimenti} \end{cases}$$

Osserviamo che due G-gruppi possono avere gruppi primitivi monolitici associati isomorfi, nonostante possano avere centralizzatori differenti.
Come mostrato in [3] (vedi Proposizione 9), se A è un fattore principale non-Frattini di G e $I_G(A)/R_G(A)$ è la sua corona, allora il gruppo $G/R_G(A)$ è isomorfo alla crown-based power di L_A di dimensione $\delta_G(A)$.
Dalla proposizione 2.3, poi, sappiamo che se A è un G-gruppo irriducibile e $\delta_G(A) \neq 0$, allora $I_G(A)/R_G(A) = soc(G/R_G(A))$; ma per quanto appena richiamato, $G/R_G(A)$ è la crown-based power di dimensione $\delta_G(A)$ del gruppo primitivo monolitico L_A.
Sfruttando quindi un'osservazione precedente, possiamo affermare che *soc*(crown-based power) è una corona.
Abbiamo dunque stabilito una corrispondenza tra le corone e le crown-based powers.

Definizione 2.12. (Crown-based image)
Diremo che $G/R_G(A)$ è la A-crown-based image *di G.*

Vale infine il seguente fatto [3]:

Proposizione 2.4. *L'immagine omomorfa G/N di un gruppo G è una crown-based power se e solo se $R_G(A) \leq N < I_G(A)$, ove A è un sottogruppo normale minimale di G/N.*

Oppure, più in generale:

Proposizione 2.5. *Sia L un'immagine omomorfa, primitiva, monolitica di G e sia $A := soc(L)$. Sia N un sottogruppo normale di G.*
Allora $R_G(A) \leq N < I_G(A)$ se e solo se G/N è isomorfo a una crown-based power di L e i sottogruppi normali minimali di G/N sono G-relazionati ad A.

2.2.3 Fattorizzazione di $P_G(s)$

Vediamo ora alcuni risultati circa la fattorizzazione di $P_G(s)$, che sfruttano gli oggetti appena introdotti.

Proposizione 2.6. *Sia N un prodotto diretto di alcuni sottogruppi normali minimali di G, ognuno G-equivalente a un G-gruppo A fissato. Allora valgono le due espressioni equivalenti:*

$$P_{G,N}(s)P_{G,R_G(A)}(s) = P_{G,NR_G(A)}(s) \tag{2.5}$$

$$P_{G,N}(s) = P_{G/R_G(A),NR_G(A)/R_G(A)}(s) \tag{2.6}$$

Facciamo subito un paio di osservazioni sulla proposizione 2.6 appena vista:

- Per dimostrare l'espressione 2.5 (vedi [3]) si fa uso di un risultato di Gaschütz, secondo cui se $M \trianglelefteq G$ allora la cardinalità dell'insieme

  $$\Omega_{g_1,...,g_t,M} := \{(m_1, ..., m_t) \in M^t | \langle g_1 m_1, ..., g_t m_t \rangle = G\}$$

  è indipendente dalla scelta dei t elementi $g_1, ..., g_t$; tale insieme poi, come si vede facilmente, ha cardinalità pari a $P_{G,M}(t)|M|^t$. Per dimostrare l'espressione dunque è sufficiente mostrare, tramite la costruzione di una biiezione, che $|\Omega_{g_1,...,g_t,N}||\Omega_{g_1,...,g_t,R}| = |\Omega_{g_1,...,g_t,NR}|$.

- Per dimostrare l'espressione 2.6, a partire dalla 2.5 è sufficiente questa serie di uguaglianze:

  $$P_{G,N}(t) \underset{(2.5)}{=} \frac{P_{G,NR}(t)}{P_{G,R}(t)} = \frac{P_G(t)}{P_{G/NR}(t)} \frac{P_{G/R}(t)}{P_G(t)} = \frac{P_{G/R}(t)}{P_{G/NR}(t)} = P_{G/R,NR/R}(t)$$

Vediamo ora come $P_G(s)$ può essere scritto come prodotto indicizzato su G-gruppi irriducibili; in particolare, il contributo dato da una classe di G-equivalenza dipende solamente dalla relativa crown-based image, come si può vedere nel teorema seguente ([3]):

Teorema 2.2. *Sia G un gruppo finito. Allora*

$$P_G(s) = \prod_A P_{G/R_G(A),I_G(A)/R_G(A)}(s)$$

dove A è un G-gruppo irriducibile G-equivalente ad un fattore principale non-Frattini di G.

Come diretta conseguenza del teorema 2.2 si ha il seguente risultato:

Corollario 2.2. *Un gruppo G finito può essere generato con d elementi se e solo se ogni immagine epimorfa di G che è una crown-based power può essere generata da d elementi.*

Osserviamo dunque che al fine di avere una stima per $P_G(s)$ abbiamo bisogno di conoscere il numero delle classi di equivalenza dei fattori principali non-Frattini di G e, per ogni fattore principale A, una stima di $P_{G/R_G(A),I_G(A)/R_G(A)}(s) = P_{L_{\delta_G(A)},A^{\delta_G(A)}}(s)$.
In particolare, dobbiamo studiare $P_{L_{\delta_G(A)},A^{\delta_G(A)}}$ quando L è un gruppo primitivo monolitico e $A = soc(L)$.

Vediamo infine una serie di risultati che ci permetteranno di esprimere $P_G(s)$ come un prodotto dipendente da $\delta_G(A)$ e da L_A, dove A varia nell'insieme dei G-gruppi irriducibili G-equivalenti a dei fattori principali non-Frattini di G.
Esplicitiamo innanzitutto il contributo dato a $P_G(s)$ da un sottogruppo normale minimale:

Proposizione 2.7. *(Vedi [3])*
Sia N un sottogruppo normale minimale di G t.c. $N \not\leq FratG$; sia L_N il gruppo primitivo monolitico associato ad N. Siano poi

$$\gamma_N := |C_{Aut(soc(L_N))}(L_N/soc(L_N))|$$

$$q_N := \begin{cases} |End_{L_N} N| & \text{se } \delta_G(N) = 1 \\ 1 & \text{altrimenti} \end{cases}$$

Allora

$$P_{G,N}(s) = \begin{cases} P_{L_N,soc(L_N)}(s) & \text{se } \delta_G(N) = 1 \\ P_{L_N,soc(L_N)}(s) - (1 + q_N + ... + q_N^{\delta_G(N)-2})\gamma_N/|N|^t & \text{altrimenti} \end{cases}$$

Grazie alla notazione che ora andremo ad introdurre è possibile esprimere in modo più sintetico l'enunciato della proposizione 2.7.
Sia dunque L un gruppo primitivo monolitico e sia $N = soc(L)$; definiamo

$$\begin{cases} \widetilde{P}_{L,1}(s) = P_{L,N}(s) \\ \widetilde{P}_{L,i}(s) = P_{L,N}(s) - (1 + q_N + ... + q_N^{i-2})\gamma_N/|N|^t & \text{con } i > 1 \end{cases}$$

dove γ_N e q_N sono definiti come nell'enunciato precedente.
Ecco dunque che, con la notazione appena introdotta, la proposizione 2.7 diventa:

$$P_{G,N}(s) = \widetilde{P}_{L_N,\delta_G(N)}(s) \tag{2.7}$$

Nel caso in cui $G = L_k$, ed N_1 è un suo sottogruppo normale minimale, allora $P_{L_k,N_1}(s) = \widetilde{P}_{L,k}(s)$ (infatti abbiamo già osservato che, se L è un gruppo primitivo monolitico e $A = soc(L)$, ogni sottogruppo normale minimale di L_k risulta essere

L_k-equivalente ad A e $\delta_{L_k}(A) = k$; il gruppo primitivo monolitico associato a N_1 (e dunque ad A dato che sono L_k-equivalenti) non può quindi che essere L stesso).
Se poi $N_2 \neq N_1$ è un altro sottogruppo normale minimale di L_k allora $P_{L_k/N_1,N_2N_1/N_1}(s) = \widetilde{P}_{L,k-1}(s)$ (ricordiamo infatti che L_k quozientato con un qualsiasi suo sottogruppo normale minimale è isomorfo a L_{k-1}).
Ora $soc(L_k)$ è il prodotto diretto di k sottogruppi normali minimali L_k-relazionati (dunque si ha una serie principale di lunghezza k in cui ogni fattore è L_k-relazionato ad N), iterando quanto visto nelle righe precedenti si ha:

$$P_{L_k,soc(L_k)}(s) = \prod_{1\leq i\leq k} \widetilde{P}_{L,i}(s) \tag{2.8}$$

Arriviamo dunque ai due teoremi finali:

Teorema 2.3. *Sia $H/K \sim_G A$ un fattore principale non-Frattini di un gruppo finito G. Allora*

$$P_{G/K,H/K}(s) = \widetilde{P}_{L_A,i}(s), \tag{2.9}$$

dove $i = \delta_{G/K}(A)$ è il numero di fattori principali G/K-equivalenti, dunque anche G-equivalenti, ad A in una data serie principale di G/K.

Dimostrazione. Il teorema 2.3 non è altro che un ulteriore modo per esprimere la proposizione 2.7.
Osserviamo infatti che se H/K è G-equivalente ad un G-gruppo A, allora $L_{H/K} \cong L_A$, $q_{H/K} = q_A$, $\gamma_{H/K} = \gamma_A$ e $|H/K| = |A|$. Ora da 2.7 si ha

$$P_{G/K,H/K}(s) = \widetilde{P}_{L_{H/K},\delta_{G/K}(H/K)}(s),$$

ma per quanto appena osservato vale

$$\widetilde{P}_{L_{H/K},\delta_{G/K}(H/K)}(s) = \widetilde{P}_{L_A,\delta_{G/K}(A)}(s).$$

Questo conclude la dimostrazione. □

In ogni serie principale di G il numero dei fattori principali non-Frattini G-equivalenti ad A è esattamente $\delta_G(A)$ (proprietà 2 delle corone, proposizione 2.3): il contributo che tali fattori danno a $P_G(s)$ è dunque esattamente $\prod_{1\leq i\leq \delta_G(A)} \widetilde{P}_{L_A,i}(s)$.
Se $1 = N_0 < N_1 < ... < N_l = G$ è una serie principale di G, unendo quanto visto finora e raggruppando i fattori principali G-equivalenti ad A otteniamo:

$$\begin{aligned} P_G(s) &\underset{(2.2)}{=} \prod_{1\leq i\leq l} P_{G/N_{i-1},N_i/N_{i-1}}(s) = \prod_{N_i/N_{i-1}\,\text{non-Frattini}} P_{G/N_{i-1},N_i/N_{i-1}}(s) \\ &= \prod_A \Bigg(\prod_{N_i/N_{i-1}\sim_G A} P_{G/N_{i-1},N_i/N_{i-1}}(s) \Bigg) = \prod_A \Bigg(\prod_{1\leq i\leq \delta_G(A)} \widetilde{P}_{L_A,i}(s) \Bigg), \end{aligned} \tag{2.10}$$

dove A appartiene all'insieme dei G-gruppi irriducibili G-equivalenti ad un fattore principale non-Frattini di G.
A questo punto possiamo quindi affermare che, indipendentemente dalla serie principale considerata, abbiamo la fattorizzazione seguente:

Teorema 2.4. *Sia G un gruppo finito. Vale*

$$P_G(s) = \prod_A \Big(\prod_{1 \leq i \leq \delta_G(A)} \widetilde{P}_{L_A,i}(s) \Big), \tag{2.11}$$

dove A appartiene all'insieme dei G-gruppi irriducibili G-equivalenti ad un fattore principale non-Frattini di G e L_A è il gruppo primitivo monolitico associato ad A.

Generare con buona probabilità

Nei capitoli seguenti verrà applicata la teoria svolta in questo capitolo in diversi casi: in linea generale, infatti, saremo interessati a studiare la probabilità asintotica di generare determinati tipi di gruppi.
A tal fine risulterà molto spesso utile il seguente teorema:

Teorema 2.5. *[Morini, AL 2001]*
Sia L un gruppo primitivo monolitico, $A = soc(L)$ e $d = max\{2, d(L/A)\}$.
Allora

$$P_{L,A}(d) \longrightarrow 1 \quad se\ |A| \longrightarrow \infty.$$

Capitolo 3

Risultati sui gruppi almost simple

In questo capitolo vedremo una serie di risultati riguardanti i gruppi almost simple: in particolare, indagheremo sulla probabilità asintotica di generare un gruppo almost simple G a partire da $d(G)$ elementi. Tale probabilità, come abbiamo visto nel capitolo precedente, verrà indicata con $P_G(d(G))$.
I risultati che troveremo, oltre ad essere utili per il capitolo 4, ci permetteranno di confrontare la probabilità asintotica di generare un gruppo semplice con quella che otterremo per generare un gruppo almost simple.

Riportiamo come prima cosa la seguente proposizione, dalla quale emerge come i gruppi almost simple siano in realtà 2 o 3-generati:

Proposizione 3.1. *(vedi [9], proposizione 3.16)*
Sia G un gruppo finito almost simple e sia $G_0 = soc(G)$. Allora $d(G) \in \{2, 3\}$. Inoltre $d(G) = 3$ se e solo se G ha un fattore principale centrale non-Frattini $A \cong C_2$ con $\delta_G(A) = 3$. Inoltre se $d(G) > 2$ allora $G_0 = PSL_n(q)$ dove $q = p^f$, $n \geq 4$ è pari, p è dispari e f è pari, o $G_0 = O^\epsilon(q)$ dove $\epsilon \in \{\pm\}$, p è dispari e f è pari.

Sia dunque G un gruppo almost simple, $s \in \{2, 3\}$: dalla teoria sviluppata nel capitolo 2 emerge che, per studiare $P_G(s)$, è necessario in primo luogo costruire una serie principale di G e, in secondo luogo, indagare sul contributo dato da ogni fattore principale.
Dato che per definizione $S \leq G \leq Aut(S)$ con S semplice, l'ultimo fattore principale di G sarà isomorfo a S. Ora S è un gruppo semplice e quindi il suo contributo al calcolo di $P_G(s)$, per il teorema 2.5, tende ad 1.
Possiamo dunque affermare che, asintoticamente,

$$P_G(s) = P_{G/S}(s),$$

dove G/S è un sottogruppo del gruppo degli automorfismi esterni $Out(S)$ di S.

Osservazione 3.1. *Dalla proposizione 3.1 si ha che anche* $d(Out(S)) \in \{2, 3\}$. *Nello specifico,* $d(Out(S)) = 3$ *se e solo se* $Out(S)$ *ha un fattore principale centrale non-Frattini* $A \cong C_2$ *con* $\delta_{Out(S)}(A) = 3$.

Dopo aver richiamato il teorema di Dirichlet e la definizione della funzione Zeta di Riemann, strumenti che d'ora in avanti saranno molto utili, enunciamo e dimostriamo un'importante proposizione che individua un bound inferiore per $P_{H \leq Out(S)}(s)$.

Teorema 3.1. *(Dirichlet, 1837)*
Siano $a, m \in \mathbb{Z}^+$ *tali che* $MCD(a, m) = 1$.
Allora esistono infiniti numeri primi p *tali che* $p \equiv a \mod m$.

Definizione 3.1. (Zeta di Riemann) *La funzione* ζ *definita da*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

prende il nome di funzione Zeta di Riemann.

Ricordando anche la formula del prodotto di Eulero

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{q \text{ primo}} \frac{1}{\left(1 - \frac{1}{q^s}\right)},$$

si ottiene l'uguaglianza seguente, che useremo in svariate occasioni:

$$\prod_{q \text{ primo}} \left(1 - \frac{1}{q^s}\right) = \frac{1}{\zeta(s)}. \tag{3.1}$$

Procediamo dunque con l'enunciare la seguente importante

Proposizione 3.2. *Sia* S *un gruppo semplice finito e* $Out(S) = Aut(S)/S$ *il suo gruppo di automorfismi esterni. Allora vale*

$$P_H(s) \geq \frac{1}{\zeta(s)} \frac{1}{\zeta(s-1)} \left(1 - \frac{4}{2^s}\right), \qquad \forall H \leq Out(S). \tag{3.2}$$

G_0	$\mathrm{Out}(G_0)$	Remarks
Alt_n, $n \geq 5$	$\begin{cases} Z_2 \\ Z_2 \times Z_2 \end{cases}$	$\begin{cases} \text{if } n \neq 6 \\ \text{if } n = 6 \end{cases}$
$\mathbf{L}_n(q)$	$\begin{cases} Z_{(n,q-1)} : Z_f : Z_2 \\ Z_{(2,q-1)} \times Z_f \end{cases}$	$\begin{cases} \text{if } n \geq 3 \\ \text{if } n = 2 \end{cases}$
$\mathbf{U}_n(q)$	$Z_{(n,q+1)} : Z_{2f}$	
$\mathbf{S}_{2m}(q)$	$\begin{cases} Z_2 \times Z_f \\ Z_f \\ Z_{2f} \end{cases}$	$\begin{cases} \text{if } q \text{ odd} \\ \text{if } m \geq 3 \text{ and } q \text{ even} \\ \text{if } m = 2 \text{ and } q \text{ even} \end{cases}$
$\mathbf{O}^0_{2m+1}(q)$, q odd	$Z_2 \times Z_f$	
$\mathbf{O}^+_8(q)$	$\begin{cases} \mathrm{Sym}_4 \times Z_f \\ \mathrm{Sym}_3 \times Z_f \end{cases}$	$\begin{cases} \text{if } q \text{ odd} \\ \text{if } q \text{ even} \end{cases}$
$\mathbf{O}^+_{2m}(q)$, $m > 4$	$\begin{cases} D_8 \times Z_f \\ Z_2 \times Z_2 \times Z_f \\ Z_2 \times Z_f \end{cases}$	$\begin{cases} \text{if } q \text{ odd and } D(Q) \text{ square} \\ \text{if } q \text{ odd and } D(Q) \text{ non-square} \\ \text{if } q \text{ even} \end{cases}$
$\mathbf{O}^-_{2m}(q)$	$\begin{cases} D_8 \times Z_f \\ Z_2 \times Z_{2f} \\ Z_{2f} \end{cases}$	$\begin{cases} \text{if } q \text{ odd and } D(Q) \text{ square} \\ \text{if } q \text{ odd and } D(Q) \text{ non-square} \\ \text{if } q \text{ even} \end{cases}$
$G_2(q)$	$\begin{cases} Z_f \\ Z_f : Z_2 \end{cases}$	$\begin{cases} \text{if } p \neq 3 \\ \text{if } p = 3 \end{cases}$
$F_4(q)$	$\begin{cases} Z_f \\ Z_f : Z_2 \end{cases}$	$\begin{cases} \text{if } p \neq 2 \\ \text{if } p = 2 \end{cases}$
$E_6(q)$	$Z_{(3,q-1)} : Z_f : Z_2$	
$E_7(q)$	$Z_{(2,q-1)} \times Z_f$	
$E_8(q)$	Z_f	
${}^2B_2(q)$, $q = 2^{2m+1}$	Z_f	
${}^2G_2(q)$, $q = 3^{2m+1}$	Z_f	
${}^2F_4(q)$, $q = 2^{2m+1}$	Z_f	
${}^3D_4(q)$	Z_{3f}	
${}^2E_6(q)$	$Z_{(3,q+1):Z_{2f}}$	
M_{11}, M_{23}, M_{24}, J_1, J_4, Ru Ly, Co_1, Co_2, Co_3, Fi_{23}, Th, BM, M	1	
M_{12}, M_{22}, J_2, J_3, HS, Suz, McL, He, O'N, Fi_{22}, Fi'_{24}, HN	Z_2	

Figura 3.1: Il gruppo degli automorfismi esterni di un gruppo finito semplice

Dimostrazione. Dimostriamo come prima cosa il caso in cui $H = Out(S)$.

Nella tabella in figura 3.1 (riportata da [9]) vi è una lista di tutti i gruppi semplici finiti e del loro corrispondente gruppo degli automorfismi esterni. Per ogni gruppo $Out(S)$ presente nella tabella è possibile calcolare $P_{Out(S)}(s)$ sfruttando la teoria sviluppata nel capitolo 2: andremo dunque a calcolare i contributi dati dai fattori principali non-Frattini di $Out(S)$.

Occupiamoci come prima cosa dei casi in cui $S \in \{PSL_n(q), E_6(q)\}$: dalla tabella in figura 3.1 si vede che $Out(S)$ è del tipo $C_a \rtimes C_b \times C_2 \cong D_{2a} \times C_b$.
Focalizziamoci intanto sul contributo dato dal fattore principale C_b, per poi occuparci dei fattori C_a e C_2.
Osserviamo innanzitutto che, in generale, $Frat(C_b) \neq 1$: ciò che realmente contribuisce al calcolo di $P_H(s)$ è quindi $C_b/Frat(C_b)$. Tale quoziente risulta essere un gruppo ciclico ed è possibile verificare che il suo ordine è pari al prodotto dei numeri primi che dividono b: grazie al teorema di struttura dei gruppi abeliani finiti, secondo cui ogni gruppo abeliano finito è isomorfo al prodotto diretto di ciclici di ordine potenza di primi, si ottiene

$$C_b/Frat(C_b) \cong \prod_{r_i|b,\ r_i \text{ primo}} C_{r_i}.$$

Dalla formula 2.4 si ricava immediatamente che il contributo del fattore ciclico C_b non è altro che $\prod_i \left(1 - \frac{1}{r_i^s}\right)$.
Occupiamoci ora del fattore principale ciclico C_a.
Anche in questo caso, chiaramente, $Frat(C_a) \neq 1$ e $C_a/Frat(C_a) \cong \prod_j C_{r_j}$, dove i vari r_j sono i numeri primi coinvolti in a.
Sia dunque r uno degli r_j. Possono esserci tre casi:

- Il fattore relativo a r è non centrale: dalla formula 2.4 il suo contributo al calcolo di $P_H(s)$ è pari a $\left(1 - \frac{r}{r^s}\right)$;
- Il fattore relativo a r è centrale, ma uguale a uno di quelli coinvolti in C_b: il suo contributo quindi è di nuovo pari a $\left(1 - \frac{r}{r^s}\right)$;
- Il fattore relativo a r è centrale e diverso da quelli coinvolti in C_b: il suo contributo, applicando ancora una volta la formula 2.4, risulta essere pari a $\left(1 - \frac{1}{r^s}\right)$.

I fattori principali C_a e C_b dunque portano un contributo a $P_H(s)$ maggiore o uguale a $\prod_{r<t} \left(1 - \frac{1}{r^s}\right)\left(1 - \frac{r}{r^s}\right)$, con t abbastanza grande.
In particolare, il contributo dato a $P_H(s)$ dai fattori dispari di a e b risulta essere maggiore o uguale a $\prod_{r<t} \left(1 - \frac{1}{r^s}\right)\left(1 - \frac{r}{r^s}\right)$, con t abbastanza grande e r primo

dispari; quello dato dal fattore 2, invece, data la presenza del fattore ciclico C_2 tra i fattori principali di $Out(S)$, risulta essere un divisore di $\Big(1-\frac{1}{2^s}\Big)\Big(1-\frac{2}{2^s}\Big)\Big(1-\frac{4}{2^s}\Big)$. Osserviamo che se il contributo dato dal fattore 2 è pari alla quantità appena scritta, allora $s \geq 3$: in questo caso particolare, infatti, $Out(S)$ ha un fattore principale non-Frattini $A \cong C_2$ con $\delta_{Out(S)}(A) = 3$.
In definitiva possiamo concludere, grazie alla formula 3.1, che asintoticamente

$$P_H(s) \geq \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big),$$

dove $S \in \{PSL_n(q), E_6(q)\}$.

E' poi immediato calcolare $P_H(s)$ in tutti gli altri casi descritti nella tabella 3.1 e vedere che

$$P_{H(S)}(s) > \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big),$$

dove ricordiamo che $H = Out(S)$.
Nel dettaglio, infatti, analizzando la tabella caso per caso, si ha:

- se $S = Alt_n$, con $n \geq 5$ allora

  $P_{Out(S)}(s) \geq \Big(1-\frac{1}{2^s}\Big)\Big(1-\frac{2}{2^s}\Big) > \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big)$;

- se $S \in \{U_n(q), E_7(q), {}^2E_6(q)\}$ allora

  $P_{Out(S)}(s) \geq \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)} > \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big)$;

- se $S \in \{S_{2m}(q), O^0_{2m+1}(q)$ con q dispari$, G_2(q), F_4(q)\}$ allora

  $P_{Out(S)}(s) \geq \frac{1}{\zeta(s)}\Big(1-\frac{2}{2^s}\Big) > \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big)$;

- se $S \in \{E_8(q), {}^2B_2(q)$ con $q = 2^{2m+1}, {}^2G_2(q)$ con $q = 3^{2m+1}, {}^2F_4(q)$ con $q = 2^{2m+1}, {}^3D_4(q)\}$ allora

  $P_{Out(S)}(s) \geq \frac{1}{\zeta(s)} > \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big)$;

- se $S = O^+_8(q)$ allora il caso peggiore si ha quando q è dispari e quindi $Out(S) = Sym_4 \times C_f$. In questo caso si ha

  $P_{Out(S)}(s) \geq \frac{1}{\zeta(s)}\Big(1-\frac{2}{2^s}\Big)\Big(1-\frac{3}{3^s}\Big)\Big(1-\frac{4}{4^s}\Big)$.

  Ora, dato che $\Big(1-\frac{4}{4^s}\Big) > \Big(1-\frac{4}{2^s}\Big)$, anche in questo caso si conclude.

- Se $S \in \{O^+_{2m}(q), O^-_{2m}(q)\}$, si ha:

  $P_{Out(S)}(s) \geq \frac{1}{\zeta(s)}\Big(1 - \frac{4}{4^s}\Big)\Big(1 - \frac{2}{2^s}\Big)$. Tale quantità risulta essere maggiore di quella ottenuta nel caso precedente, e quindi si riesce a concludere.

- Se poi $S \in \{M_{11}, M_{23}, M_{24}, J_1, J_4, Ru\ Ly, Co_1, Co_2, Co_3, Fi_{23}, Th, BM, M\}$, essendo $Out(S) = 1$, banalmente si avrà $P_{Out(S)}(s) = 1$;

- Infine, se $S \in \{M_{12}, M_{22}, J_2, J_3, HS, Suz, McL, He, O'N, Fi_{22}, Fi'_{24}, HN\}$, allora

  $P_{Out(S)}(s) = \Big(1 - \dfrac{1}{2^s}\Big) > \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1 - \frac{4}{2^s}\Big)$.

Per concludere la dimostrazione resta da analizzare il caso $H < Out(S)$, che risulta essere del tutto analogo a quanto visto sopra: nel peggiore dei casi (cioè nel caso in cui $S \in \{PSL_n(q), E_6(q)\}$), infatti, il sottogruppo H sarà della forma $C_c \rtimes C_d$ o, eventualmente, $C_c \rtimes C_d \times C_2$, con $C_c \leq C_a$ e $C_d \leq C_b$. Con argomenti analoghi a quelli utilizzati nel caso $H = Out(S)$ si conclude velocemente. □

Osservazione 3.2. *Il bound inferiore per $P_{H \leq Out(S)}(s)$ della proposizione 3.2 non è migliorabile: esiste una famiglia infinita Ω di gruppi finiti semplici tali che*

$$\inf_{T \leq \Omega} P_{Out(T)}(s) = \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1 - \frac{4}{2^s}\Big). \tag{3.3}$$

Dimostrazione. Vogliamo costruire una famiglia di gruppi semplici finiti per cui valga 3.3.
Consideriamo una famiglia $\{r_1, r_2, ..., r_m\}$ dei numeri primi strettamente minori di un certo q fissato.
Applichiamo ora il teorema di Dirichlet richiamato precedentemente (vedi teorema 3.1) con $a = 1$ e $m = r_1 r_2 ... r_m$: esistono quindi infiniti numeri primi p tali che $p \equiv 1 \mod r_1 r_2 ... r_m$. Preso un primo p di questo tipo, dunque, sappiamo che il prodotto $r_1 r_2 ... r_m$ divide $(p-1)$; di conseguenza ogni singolo primo r_i della famiglia sopra considerata divide $(p-1)$.
Definiamo ora t il prodotto $t = \prod_{i \in \{1,...,m\}} r_i$.
Chiaramente, per come abbiamo appena definito t, quest'ultimo è diviso da ogni primo r_i ed inoltre per ogni r_i vale

$$p^t \equiv 1 \mod r_i.$$

Definito quindi $\tilde{q} = p^t$, consideriamo il gruppo semplice

$$T = PSL_{\tilde{q}-1}(\tilde{q}) :$$

dalla tabella in figura 3.1, poichè $(\tilde{q}-1, \tilde{q}-1) = \tilde{q}-1$, si ottiene che il suo gruppo degli automorfismi esterni è pari a

$$Out(T) = C_u \rtimes C_t \times C_2 \cong D_{2u} \times C_t,$$

con $u = \tilde{q} - 1$.
Dal momento che, per quanto visto nelle righe precedenti, sia t che u sono divisibili per tutti i primi r_i, si ottiene:

$$P_{Out(T)}(s) \leq \Big(1 - \frac{4}{2^s}\Big) \prod_{r_i < q} \Big(1 - \frac{1}{r_i^s}\Big)\Big(1 - \frac{r_i}{r_i^s}\Big). \tag{3.4}$$

Facendo tendere q all'infinito e combinando quanto appena ottenuto con l'equazione 3.2, si ottiene l'uguaglianza desiderata.

□

Grazie ai risultati appena visti e al teorema 2.5 giungiamo alla seguente

Proposizione 3.3. *Sia G un gruppo almost simple di ordine n. Allora*

$$\limsup_{n\to\infty} P_G(s) = \frac{1}{\zeta(s)} \frac{1}{\zeta(s-1)} \Big(1 - \frac{4}{2^s}\Big). \tag{3.5}$$

In particolare, se $G = Aut(S)$:

$$\limsup_{n\to\infty} P_{Aut(S)}(s) = \frac{1}{\zeta(s)} \frac{1}{\zeta(s-1)} \Big(1 - \frac{4}{2^s}\Big).$$

E' dunque possibile confrontare la probabilità asintotica di generare un gruppo semplice con quella di generare un almost simple: mentre la prima tende a 1, la seconda è asintoticamente pari a $\frac{1}{\zeta(s)} \frac{1}{\zeta(s-1)} \Big(1 - \frac{4}{2^s}\Big)$.

Capitolo 4

Sulla probabilità asintotica di generare i sottogruppi massimali di Sym_n e di Alt_n

In questo capitolo ci proponiamo di studiare l'andamento asintotico di $P_H(d(H))$ al variare di H tra i sottogruppi massimali di Sym_n e di Alt_n, classificati nel capitolo 1 grazie al teorema di O'Nan-Scott.
Come emerge dalla proposizione seguente vale che $d(H) \leq 4$ per ogni H sottogruppo massimale di Sym_n o di Alt_n: studieremo quindi l'andamento asintotico di $P_H(4)$.

Proposizione 4.1. *([9], Proposition 5.1)*
Si supponga che $G_0 \leq G \leq Aut(G_0)$, dove $G_0 = Alt_n$ è un gruppo alternante di grado $n \geq 5$. Se H è un sottogruppo massimale di G, allora $d(H) \leq 4$.
In particolare, $d(H) = 4$ se e solo se $G \in \{Alt_n, Sym_n\}$, $H = (T^k.(Out(T) \times Sym_k)) \cap G$ è di tipo diagonale, $Sym_k \leq H$ e $d(Out(T) \cap H/T^k) = 3$.

Per generare qualsiasi sottogruppo massimale di Sym_n o di Alt_n, quindi, sono sufficienti 4 elementi. In particolare, andando a vedere la dimostrazione di tale proposizione, si scopre che i sottogruppi massimali di tipo intransitivo, imprimitivo e affine sono in realtà generati da 2 elementi soltanto; i sottogruppi massimali almost simple sono 2 o 3 generati, mentre i sottogruppi di tipo diagonale possono essere 4-generati.

4.1 Caso intransitivo: $H = (Sym_a \times Sym_{n-a}) \cap G$

Occupiamoci come prima cosa dei sottogruppi massimali $H = (Sym_a \times Sym_{n-a}) \cap G$ di $G \in \{Sym_n, Alt_n\}$, cioè di quelli intransitivi.

Osserviamo subito che $Sym_a \times Sym_{n-a} \not\leq Alt_n$, in quanto contiene un elemento dispari: ciò significa che, se $G = Sym_n$, il sottogruppo $H = Sym_a \times Sym_{n-a}$ è un sottogruppo massimale di Sym_n.
Iniziamo l'analisi nel caso $G = Sym_n$, per poi occuparci del caso $G = Alt_n$.

4.1.1 Caso $G = Sym_n$

Dal momento che il sottogruppo $H = Sym_a \times Sym_{n-a}$, come detto sopra, è 2-generato, ha senso chiedersi quanto vale $P_H(2)$, oltre che $P_H(4)$: nel capitolo 1 abbiamo visto come, per calcolare tali probabilità, sia necessario costruire una serie principale di H e indagare poi sui contributi dati da ogni fattore principale, ricordando che se il fattore principale è abeliano possiamo utilizzare l'approccio di Gaschütz.

A tal proposito osserviamo preliminarmente che il gruppo ciclico di ordine due, C_2, visto come G-modulo con G gruppo di permutazione, risulta essere triviale. Imponendo la compatibilità dell'azione di G su $C_2 = \langle x \rangle$ con la struttura di gruppo abeliano, infatti, si vede che comunque si prenda $g \in G$, $g \cdot x$ deve essere un elemento di C_2 di ordine 2. Necessariamente dunque si ha che $g \cdot x = x$.
Come conseguenza diretta di questo fatto, con le notazioni del capitolo 2, si ha che $\theta_G(C_2) = 0$.

Analizziamo, come prima cosa, i casi con $a \in \{2, 3, 4\}$.
Possiamo subito osservare che se $a \in \{3, 4\}$, allora i fattori principali di H di ordine diverso da 2 sono H-moduli non triviali. Di conseguenza la funzione θ_H calcolata su tali fattori principali vale 1.

- Sia $a = 2$, dunque consideriamo il sottogruppo $H = Sym_2 \times Sym_{n-2} = C_2 \times Sym_{n-2}$.
  I suoi fattori principali risultano essere C_2, C_2 e Alt_{n-2}.
  Dal teorema 2.5, poichè stiamo studiando la probabilità asintotica (quindi con $n \longrightarrow \infty$), emerge che il contributo dato dal fattore Alt_{n-2} per il calcolo di $P_H(s)$ tende a 1. Resta quindi il contributo dei due fattori ciclici e, dato che asintoticamente H è risolubile, utilizzando la formula di Gaschütz (teorema 2.1) con $\theta_H(C_2) = 0$ e $\delta_H(C_2) = 2$, otteniamo che:

  - $P_{Sym_2 \times Sym_{n-2}}(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{2}\right) = \frac{3}{4}\frac{1}{2} = \frac{3}{8} \approx 0,375$
  - $P_{Sym_2 \times Sym_{n-2}}(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right) = \frac{15}{16}\frac{7}{8} = \frac{105}{128} \approx 0,82$

- Sia ora $a = 3$, dunque $H = Sym_3 \times Sym_{n-3}$: i suoi fattori principali sono C_2, C_2, C_3 e Alt_{n-3}.
  Asintoticamente il contributo dato dall'ultimo fattore principale, come nel caso precedente, tende a 1. Restano così solo i contributi dati dai fattori principali ciclici ed utilizzando la formula di Gaschütz (con $\theta_H(C_2) = 0$, $\delta_H(C_2) = 2$, $\theta_H(C_3) = 1$ e $\delta_H(C_3) = 1$) si ottiene che per $n \longrightarrow \infty$:
  - $P_{Sym_3 \times Sym_{n-3}}(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{2}\right)\left(1 - \frac{3}{9}\right) = \frac{3}{4}\frac{1}{2}\frac{2}{3} = \frac{1}{4} = 0,25$
  - $P_{Sym_3 \times Sym_{n-3}}(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right)\left(1 - \frac{3}{81}\right) = \frac{15}{16}\frac{7}{8}\frac{26}{27} = \frac{455}{576} \approx 0,79$

- Sia infine $a = 4$ ed $H = Sym_4 \times Sym_{n-4}$. Dal momento che la serie principale di Sym_4 è Sym_4-Alt_4-K-1 (dove K è il gruppo di Klein), ne segue che i fattori principali di H sono C_2, C_2, C_3, K, Alt_{n-4}.
  Osserviamo che tali fattori principali, tranne Alt_{n-4} (il cui contributo asintoticamente tende ad 1), sono abeliani: è possibile utilizzare quindi la formula di Gaschütz, ricordando che C_3 e K non sono H-moduli triviali. Si ottiene quindi:
  - $P_{Sym_4 \times Sym_{n-4}}(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{2}\right)\left(1 - \frac{3}{9}\right)\left(1 - \frac{4}{16}\right) = \frac{3}{4}\frac{1}{2}\frac{2}{3}\frac{3}{4} \approx 0,188$
  - $P_{Sym_4 \times Sym_{n-4}}(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right)\left(1 - \frac{3}{81}\right)\left(1 - \frac{4}{256}\right) = \frac{15}{16}\frac{7}{8}\frac{26}{27}\frac{63}{64} \approx 0,778$

Analizziamo ora il caso in cui $a \geq 5$.
In questo caso i fattori principali sono C_2, C_2, Alt_a e Alt_{n-a} poichè, essendo $a \geq 5$, Alt_a e Alt_{n-a} sono semplici. Sfruttando sempre il teorema 2.5, come nei casi precedenti, possiamo concludere che il contributo dato dal fattore Alt_{n-a} per il calcolo di $P_H(s)$ tende a 1. Resta quindi da determinare il contributo dato dagli altri tre fattori.

Grazie alla formula 2.4 e alle osservazioni preliminari riusciamo a determinare il contributo dato dai due ciclici, che risulta essere quindi pari a $\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{2}{2^s}\right)$, dove s è il numero di generatori (nei casi in esame $s \in \{2, 4\}$). Resta da calcolare il contributo del fattore principale Alt_a, cioè $P_{H,Alt_a}(s)$.
Osserviamo innanzitutto che $P_{H,Alt_a}(s) = P_{Sym_a,Alt_a}(s)$.

Nel caso in cui $s = 2$, da [10] emerge che per quasi tutti i valori di a si ha $P_{Sym_a,Alt_a}(2) \geq \frac{9}{10}$ e che il caso peggiore si verifica con $a = 6$, in cui $P_{Sym_6,Alt_6}(2) = \frac{53}{90}$. Di conseguenza, quindi, asintoticamente si ha:

- $P_{Sym_a \times Sym_{n-a}}(2) \geq \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{2}\right)\frac{53}{90} = \frac{3}{4}\frac{1}{2}\frac{53}{90} \approx 0,22$, con caso peggiore per $a = 6$

Considerando i risultati ottenuti con 2 elementi generatori (quindi con $s = 2$) per i diversi valori di a, emerge che la probabilità minore la si ha per generare $H = Sym_4 \times Sym_{n-4}$.
Dimostriamo ora che vale lo stesso nel momento in cui si abbiano 4 elementi generatori.

Sia dunque $s = 4$. Ricordiamo che $P_{H,Alt_a}(4) = P_{Sym_a,Alt_a}(4)$ e dimostriamo quindi che $P_{Sym_a,Alt_a}(4) > P_{Sym_4,Alt_4}(4) = \frac{637}{768}$.
Per fare questo, dopo aver ricordato un risultato di Gaschütz, dimostriamo la seguente disuguaglianza:

$$P_{Sym_a,Alt_a}(4) \geq 1 - (1 - P_{Sym_a,Alt_a}(2))^2 \tag{4.1}$$

Teorema 4.1. *(di Gaschütz)*
Sia G un gruppo finito, $d(G) \leq d$.
Sia $N \trianglelefteq G$ e si supponga esistano $g_1, ..., g_d \in G$ tali che $G = \langle g_1, ..., g_d \rangle N$.
Allora la cardinalità $\phi_{G,N}(d)$ dell'insieme $\{(n_1, ..., n_d) \in N^d | G = \langle g_1 n_1, ..., g_d n_d \rangle\}$ è positiva e non dipende dalla scelta di $g_1, ..., g_d$.

Dimostrazione. (della disuguaglianza 4.1)
Sia $\{x_1, x_2, x_3, x_4\}$, $x_i \in Sym_a$, un insieme di quattro generatori di Sym_a/Alt_a, cioè tali che $\langle x_1, x_2, x_3, x_4 \rangle Alt_a = Sym_a$. Per il teorema 4.1 di Gaschütz appena richiamato, sappiamo che esistono $n_1, n_2, n_3, n_4 \in Alt_a$ tali che $\langle x_1 n_1, x_2 n_2, x_3 n_3, x_4 n_4 \rangle = Sym_a$.
Detto $\phi_{Sym_a,Alt_a}(4) = |\{(n_1, n_2, n_3, n_4) \in Alt_a | \langle x_1 n_1, x_2 n_2, x_3 n_3, x_4 n_4 \rangle = Sym_a\}|$, si ha:

$$P_{Sym_a,Alt_a}(4) = \frac{\phi_{Sym_a,Alt_a}(4)}{|Alt_a|^4}.$$

Ora, ancora per il teorema 4.1, $\phi_{Sym_a,Alt_a}(4)$ non dipende dalla particolare scelta dei generatori $x_1, x_2, x_3, x_4 \in Sym_a$: dato che Sym_a/Alt_a è in realtà 2-generato, possiamo considerare come generatori gli elementi x_1, x_2, x_1, x_2, dove $\langle x_1, x_2 \rangle Alt_a = Sym_a$.
Per ottenere la disuguaglianza 4.1, indaghiamo sul numero di 4-uple (n_1, n_2, n_3, n_4) tali che $\langle x_1 n_1, x_2 n_2, x_1 n_3, x_2 n_4 \rangle = Sym_a$. Chiaramente, se $\langle x_1 n_1, x_2 n_2 \rangle = Sym_a$, tutte le 4-uple del tipo $(n_1, n_2, *, *)$ e $(*, *, n_1, n_2)$ appartengono a $\phi_{Sym_a,Alt_a}(4)$.
Ragionando sulla probabilità complementare, quindi, si ottiene:

$$P_{Sym_a,Alt_a}(4) \geq 1 - (1 - P_{Sym_a,Alt_a}(2))(1 - P_{Sym_a,Alt_a}(2)).$$

□

Utilizzando la disuguaglianza 4.1 appena dimostrata, si ha che per i valori di a per cui $P_{Sym_a,Alt_a}(2) \geq \frac{9}{10}$ (cioè per quasi tutti i valori di a), vale:

$$P_{Sym_a,Alt_a}(4) \geq 1 - (1 - P_{Sym_a,Alt_a}(2))^2 \geq 1 - \left(\frac{1}{10}\right)^2 = \frac{99}{100} > \frac{637}{768}.$$

Per i restanti valori di a, poi, si può verificare che il caso peggiore lo si ha per $a = 5$, per cui vale $P_{Sym_5,Alt_5}(4) = \frac{106549}{108000}$; anche in questo caso, comunque, $P_{Sym_5,Alt_5}(4) \geq P_{Sym_4,Alt_4}(4)$.

Dall'analisi sopra effettuata si ottiene, quindi, la seguente proposizione:

Proposizione 4.2. *Sia Ω_n l'insieme dei massimali intransitivi di Sym_n. Allora:*

$$\lim_{n\to\infty}\left(\min_{H\in\Omega_n} P_H(2)\right) = \lim_{n\to\infty} P_{Sym_4\times Sym_{n-4}}(2) = \frac{3}{16} \approx 0,188; \tag{4.2}$$

$$\lim_{n\to\infty}\left(\min_{H\in\Omega_n} P_H(4)\right) = \lim_{n\to\infty} P_{Sym_4\times Sym_{n-4}}(4) = \frac{3185}{4096} \approx 0,778. \tag{4.3}$$

4.1.2 Caso $G = Alt_n$

Sia ora $G = Alt_n$: i suoi massimali di tipo intransitivo, dal teorema di O'Nan-Scott (capitolo 1), sono della forma $H = (Sym_a \times Sym_{n-a}) \cap Alt_n$.
Come emerge dalla dimostrazione del teorema 5.5 in [9], poi, si ha che H è un sottogruppo di indice 2 del sottogruppo massimale $Sym_a \times Sym_{n-a}$ di Sym_n: ciò comporta che tra i fattori principali di H ci sia un fattore ciclico C_2 in meno rispetto ai fattori principali di $Sym_a \times Sym_{n-a}$. Questo fatto porta ad avere un fattore $\left(1 - \frac{2}{2^s}\right)$ in meno nel calcolo di $P_H(s)$ rispetto a quanto visto nel caso di $P_{Sym_a\times Sym_{n-a}}(s)$.

Nel caso $a \geq 5$, poi, è presente un'ulteriore differenza: mentre precedentemente si aveva $P_{H,Alt_a}(s) = P_{Sym_a,Alt_a}(s)$, ora si ha $P_{H,Alt_a}(s) = P_{Alt_a,Alt_a}(s) = P_{Alt_a}(s)$. In realtà, a livello di calcoli, questo non porta con sè alcuna differenza: i casi peggiori rimangono gli stessi ed è possibile verificare che $P_{Sym_6,Alt_6}(2) = P_{Alt_6}(2)$ e che $P_{Sym_5,Alt_5}(4) = P_{Alt_5}(4)$.

In definitiva, dalla proposizione 4.2 e da quanto appena osservato, si giunge alle seguente

Proposizione 4.3. *Sia Ω_n l'insieme dei massimali intransitivi di Alt_n. Allora:*

$$\lim_{n\to\infty}\Big(\min_{H\in\Omega_n} P_H(2)\Big) = \lim_{n\to\infty} P_{(Sym_4\times Sym_{n-4})\cap Alt_n}(2) = \frac{\frac{3}{16}}{\frac{1}{2}} \approx 0,375; \tag{4.4}$$

$$\lim_{n\to\infty}\Big(\min_{H\in\Omega_n} P_H(4)\Big) = \lim_{n\to\infty} P_{(Sym_4\times Sym_{n-4})\cap Alt_n}(4) = \frac{\frac{3185}{4096}}{\frac{7}{8}} = \frac{455}{512} \approx 0,889. \tag{4.5}$$

4.2 Caso imprimitivo o intrecciato: $H = (Sym_a \wr Sym_b) \cap G$

Prendiamo ora in considerazione i sottogruppi massimali di $G \in \{Sym_n, Alt_n\}$ di tipo imprimitivo o intrecciato: sono il terzo tipo di sottogruppi massimali del teorema di O'Nan-Scott e sono della forma $H = (Sym_a \wr Sym_b) \cap G$ dove $n = ab$ o $n = a^b$ per qualche $b > 1$, $a > 1$.
Ricordiamo che $Sym_a \wr Sym_b = (Sym_a)^b \rtimes Sym_b$.
L'obiettivo, analogo al caso intransitivo, è quello di studiare asintoticamente $P_H(2)$ e $P_H(4)$: per fare questo costruiamo delle serie principali di H, che saranno differenti a seconda dei casi considerati.

Osserviamo innanzitutto che $Sym_a \wr Sym_b \not\leq Alt_n$: in questo modo tale sottogruppo è un sottogruppo massimale del gruppo simmetrico Sym_n.
Effettueremo prima lo studio asintotico di $P_H(2)$ e $P_H(4)$ nel caso $G = Sym_n$ e solo successivamente affronteremo il caso $G = Alt_n$, i cui sottogruppi massimali di tipo imprimitivo o intrecciato saranno del tipo $H = (Sym_a \wr Sym_b) \cap Alt_n$.

Prima di cominciare lo studio dettagliato, diamo delle definizioni che ci saranno utili per costruire le serie principali nei vari casi.

Definizione 4.1. *(vedi [7], p.185-186)*
Sia $n \geq 5$, sia p un numero primo e Sym_n agisca sul modulo di permutazione F_p^n permutandone le coordinate. Definiamo i seguenti sottomoduli di F_p^n:

$$U = \{(a_1, ..., a_n) | \sum_{i=1}^{n} a_i = 0,\ a_i \in F_p\}; \tag{4.6}$$

$$D = \{(a, ..., a) | a \in F_p\}. \tag{4.7}$$

Lo spazio $(n-1)$-dimensionale U prende il nome di "deleted permutation module" per Sym_n.
Definiamo inoltre

$$W = \frac{U}{U \cap D}, \tag{4.8}$$

che prende il nome di "fully deleted permutation module" per Sym_n su F_p.

Osserviamo innanzitutto che U e D sono invarianti per l'azione di Sym_n: entrambi i moduli vengono infatti preservati se vengono permutate le coordinate dei loro elementi. Come enunciato in [7], poi, è possibile dimostrare che sono gli unici sottomoduli propri di F_p^n Sym_n-invarianti.

Si può notare inoltre che D è contenuto in U se e solo se p divide n. Se p non divide n, $U \cap D = \{0\}$ e dunque $W = U$: in questo caso il fully deleted permutation module coincide con il deleted permutation module.
Se p divide n, invece, $U \cap D = D$ e quindi in questo caso $W = U/D$.
Possiamo dunque affermare che

$$dim(W) = \begin{cases} n-1 & \text{se } p \text{ non divide } n \\ n-2 & \text{se } p \text{ divide } n \end{cases}$$

Come è dimostrato in [7], poi, W è irriducibile.

Osservazione 4.1. *Nella trattazione che andremo a fare, avremo $p = 2$ e $n = b$. F_p^n dunque sarà C_2^b.*
Se b è un numero dispari (quindi 2 non divide b), la dimensione di W sarà $(b-1)$, in quanto l'intersezione di D con U è vuota. Se b è un numero pari, invece, la dimensione di W sarà $(b-2)$ e sia W che D saranno moduli irriducibili.

Osservazione 4.2. *E' possibile definire il "deleted permutation module" e il "fully deleted permutation module" anche per Alt_n su F_p, seguendo fedelmente la costruzione fatta sopra.*

Proposizione 4.4. *Il sottogruppo $N := (Alt_a)^b$ di $(Sym_a)^b$, con $a \geq 5$, è un sottogruppo normale minimale.*

Dimostrazione. Il sottogruppo N considerato è chiaramente un sottogruppo normale di $(Sym_a)^b$, poichè $Alt_a \trianglelefteq Sym_a$. Si tratta quindi di dimostrarne la minimalità.
Sia $(x_1, ..., x_b)$ un elemento di N non identico, dunque $x_i \in Alt_a$ e $\exists i$ t.c. $x_i \neq 1$.
Notiamo che, essendo N normale in $(Sym_a)^b$, se vengono permutate le coordinate di

$(x_1, ..., x_b)$ si ottiene necessariamente un altro elemento di N: non è quindi restrittivo supporre che la coordinata x_1 sia diversa da 1.

Consideriamo ora un elemento $y \in Alt_a$ che non commuti con x_1 e costruiamo la b-upla $(y, x_2, ..., x_b)$.

Il commutatore tra $(x_1, x_2, ...x_b)$ e $(y, x_2, ..., x_b)$ risulta quindi essere la b-upla $(z, 1, ..., 1)$, ove $z := [x_1, y] \neq 1$. Notiamo che necessariamente $(z, 1, ..., 1) \in N$.
Possiamo poi coniugare $(z, 1, ..., 1)$ con qualsiasi elemento di Alt_a: N contiene allora il sottogruppo generato dagli elementi $(z^t, 1, ..., 1)$, al variare di t in Alt_a ed essendo Alt_a un gruppo semplice, ne segue che N contiene tutto il sottogruppo $A_1 = \{(a, 1, ..., 1) | a \in Alt_a\}$.

Permutando le coordinate (tramite l'azione di Sym_b) si riesce quindi ad ottenere un insieme di generatori per N: ecco quindi che un sottogruppo normale contenuto in $(Alt_a)^b$ è $(Alt_a)^b$ stesso. □

4.2.1 Caso b dispari

Cominciamo l'analisi fissando b e imponendo che sia *dispari*.
Al fine di studiare il comportamento asintotico, necessariamente a deve tendere a infinito, dunque $a \longrightarrow \infty$. In particolare, $a \geq 5$.
Distinguiamo ora i casi $b \geq 5$ e $b < 5$ nel costruire le serie principali di $Sym_a \wr Sym_b = (Sym_a)^b \rtimes Sym_b$.

- Sia b dispari, $b \geq 5$, $a \longrightarrow \infty$.
  Per la proposizione 4.4 e l'osservazione 4.1 possiamo concludere che i fattori principali di $Sym_a \wr Sym_b$ in questo caso sono: C_2, Alt_b (che è semplice), $D \cong C_2$ centrale e complementato, W e $N = (Alt_a)^b$.
  Capiamo ora i contributi che questi fattori danno al calcolo di $P_H(s)$, con $s \in \{2, 4\}$ per quanto osservato a inizio capitolo.

  Dal momento che $|N| = |(Alt_a)^b| \longrightarrow \infty$, per il teorema 2.5 si ha che $P_{H,N}(s) \longrightarrow 1$. Asintoticamente, quindi, $Sym_a \wr Sym_b$ si comporta come $C_2 \wr Sym_b$.

  I due fattori ciclici C_2 di ordine 2, poi, essendo abeliani, danno un contributo a $P_H(s)$ di $\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{2}{2^s}\right)$. Al fine di indicare tale contributo con la notazione appropriata, osserviamo che H/N ha un sottogruppo normale M/N isomorfo a $W \times Alt_b$ e $H/M \cong C_2 \times C_2$: il contributo dei fattori principali ciclici appena menzionato sarà quindi $P_{H,M} = \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{2}{2^s}\right)$.

  Occupiamoci ora del contributo dato da W, quindi di $P_{H/N,W}(s)$ (osserviamo infatti che $H/N \cong C_2 \wr Sym_b$ ha un sottogruppo normale isomorfo a W ed ha quindi senso la scrittura $P_{H/N,W}$). Essendo W abeliano, dalla proposizione 2.1 sappiamo che il contributo che esso dà a $P_H(s)$ è pari a $\left(1 - \frac{c}{(2^{b-1})^s}\right)$, dove c è

il numero di complementi di W: per determinare tale c, è necessario fare una piccola digressione sulla coomologia.

E' noto che $c = |Der(Sym_b, W)|$, dove con $Der(Sym_b, W)$ indichiamo il gruppo dato dall'insieme delle funzioni $\delta : Sym_b \longrightarrow W$ tali che $(xy)^\delta \mapsto (x^\delta)^y + y^\delta$ con l'operazione di composizione (notiamo che è stata usata una notazione additiva).
Un sottogruppo delle derivazioni è composto dalle derivazioni interne indicate con $IDer(Sym_b, W)$, quindi dalle funzioni $\delta_w : Sym_b \longrightarrow W$ tali che $x \mapsto [x, w] = w - w^x$, per $w \in W$ fissato.
Dalla definizione appena data è immediato osservare che vale il seguente isomorfismo:

$$IDer(Sym_b, W) \cong W. \tag{4.9}$$

Definizione 4.2. *Viene detto* primo gruppo di coomologia *e viene indicato con* $H^1(Sym_b, W)$ *il quoziente tra il gruppo delle derivazioni e quello delle derivazioni interne:*

$$H^1(Sym_b, W) = \frac{Der(Sym_b, W)}{IDer(Sym_b, W)}.$$

E' possibile dimostrare (vedi [8], 5.8) che, per b dispari, si ha $H^1(Sym_b, W) = 1$: sfruttando l'isomorfismo 4.9 è quindi immediato concludere che, in questo caso particolare,

$$c = |W|.$$

A questo punto possiamo quindi determinare in modo preciso $P_{H/N,W}(s)$, che risulta essere così pari a $P_{H/N,W}(s) = \big(1 - \frac{|W|}{(2^{b-1})^s}\big) = \big(1 - \frac{2^{b-1}}{(2^{b-1})^s}\big)$.

Resta ora da determinare il contributo di Alt_b, quindi $P_{H/(Sym_a)^b, Alt_b}(s)$. Tale contributo è già stato discusso nel caso dei sottogruppi massimali intransitivi: nella discussione di questo caso era emerso come, per quasi tutti i valori di b, $P_{Sym_b, Alt_b}(2) \geq \frac{9}{10}$ e $P_{Sym_b, Alt_b}(4) \geq \frac{99}{100}$.

Riassumendo, dunque:

- $P_{H,M}(s) = \big(1 - \frac{1}{2^s}\big)\big(1 - \frac{2}{2^s}\big)$;
- $P_{H,N}(s) \longrightarrow 1$;
- $P_{H/N,W}(s) = \big(1 - \frac{1}{(2^{b-1})^{s-1}}\big)$;
- $P_{H/(Sym_a)^b, Alt_b}(s) = \frac{P_{Sym_b, Alt_b}(s)}{P_{C_2}(s)}$.
  In particolare, per quasi tutti i valori di b, valgono: $P_{Sym_b, Alt_b}(2) \geq \frac{9}{10}$ e $P_{Sym_b, Alt_b}(4) \geq \frac{99}{100}$.

Da quanto appena scritto si vede come solo gli ultimi due contributi dipendano in realtà da b. Possiamo subito notare che, se $b \longrightarrow \infty$, tali contributi tendono a 1: gli unici fattori principali che, di fatto, contribuiscono alla probabilità $P_H(s)$ in questo caso sono i due ciclici C_2.
Si possono infine determinare i casi peggiori, cioè i casi in cui la probabilità di generare $P_H(s)$ è minore: si verificano in corrispondenza di $b = 5$ sia nel caso in cui $s = 2$, che nel caso in cui $s = 4$.
In conclusione, quindi:

- $P_H(2) \geq \left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right)\left(1 - \frac{1}{16}\right)\frac{19}{30} = \frac{3}{4}\frac{1}{2}\frac{15}{16}\frac{19}{30} = \frac{57}{256} \approx 0,2227$, con caso peggiore per $b = 5$;
- $P_H(4) \geq \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right)\left(1 - \frac{1}{4096}\right)\frac{106549}{108000} = \frac{15}{16}\frac{7}{8}\frac{4095}{4096}\frac{106549}{108000} = \frac{67871713}{83886080} \approx 0,8091$, con caso peggiore per $b = 5$;

- Sia b dispari, $b < 5$ (cioè $b = 3$); $a \longrightarrow \infty$.
Questo caso è molto simile al precedente: l'unica differenza è che, al posto di avere il fattore principale Alt_b, ora si ha un C_3. I fattori principali di $H = Sym_a \wr Sym_3$, con $a \longrightarrow \infty$ dunque sono: C_2, C_3, $D \cong C_2$, W, $N = (Alt_a)^3$.
Asintoticamente, dunque, vale:
  - $P_H(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right)\left(1 - \frac{3}{9}\right)\left(1 - \frac{1}{4}\right) = \frac{3}{4}\frac{1}{2}\frac{2}{3}\frac{3}{4} = \frac{3}{16} \approx 0,188$
  - $P_H(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right)\left(1 - \frac{3}{81}\right)\left(1 - \frac{1}{64}\right) = \frac{15}{16}\frac{7}{8}\frac{26}{27}\frac{63}{64} = \frac{3185}{4096} \approx 0,778$

Riassumendo, otteniamo quindi la seguente

Osservazione 4.3. *Nel caso in cui b sia un fissato numero dispari e $a \longrightarrow \infty$, la probabilità minore di generare un sottogruppo massimale di tipo imprimitivo o intrecciato di Sym_n si verifica con $b = 3$. Per questo valore di b, la probabilità di generare $Sym_a \wr Sym_3$ con 2 generatori è asintoticamente pari a 0,188, mentre quella di generarlo con 4 elementi sale asintoticamente a 0,778.*

Proseguiamo ora la nostra analisi imponendo ancora una volta la condizione che b sia *dispari*, ma studiando il caso in cui b tenda ad infinito e a sia un numero fissato. Notiamo innanzitutto che il caso in cui $a \geq 5$ e $b \longrightarrow \infty$ lo abbiamo in realtà già studiato sopra: gli unici fattori che contribuivano al calcolo di $P_H(s)$ erano i due ciclici C_2 di ordine 2. Nel seguito vedremo che anche nel caso in cui $a \in \{2, 3, 4\}$ si ottiene lo stesso risultato.

- Sia $a = 4$, dunque $H = Sym_4 \wr Sym_b$ con $b \longrightarrow \infty$.
Dal momento che la serie principale di Sym_4 è $Sym_4 - Alt_4 - K - 1$, ne risulta che i fattori principali di $H = Sym_4 \wr Sym_b$ sono: C_2, Alt_b, $D \cong C_2$, W, $W_1 = (C_3)^b$ e $W_2 = (K)^b$ ed è possibile verificare l'irriducibilità dei W_i.

Il contributo dato dai due fattori principali W_i, essendo abeliani (e potendo quindi applicare la proposizione 2.1), è pari a $P_{H/N,W_i}(s) = \left(1 - \frac{c}{|W_i|^s}\right)$.

E' poi possibile dimostrare (vedi [4], teorema 1) che $c \leq |W_i|^{\frac{3}{2}}$, quindi $\left(1 - \frac{c}{|W_i|^s}\right) \geq \left(1 - \frac{|W_i|^{\frac{3}{2}}}{|W_i|^s}\right) = \left(1 - \frac{1}{|W_i|^{s-\frac{3}{2}}}\right)$. Ora $b \longrightarrow \infty$, quindi $|W_i| \longrightarrow \infty$: il contributo dei fattori prinicipali $|W_i|$, così, tende a 1. In altre parole, cioè, $P_{H/N,W_i}(s) \longrightarrow 1$ asintoticamente.

Per quanto visto nei casi precedenti, poi, $P_{H/N,W}(s) \longrightarrow 1$ e, per il teorema 2.5, anche $P_{H/(Sym_a)^b,Alt_b}(s) \longrightarrow 1$.

Di conseguenza gli unici fattori principali che asintoticamente contribuiscono al calcolo di $P_H(s)$ sono i fattori ciclici C_2.

Possiamo quindi concludere che:

- $P_H(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right) = \frac{3}{4}\frac{1}{2} = \frac{3}{8} \approx 0,375.$
- $P_H(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right) = \frac{15}{16}\frac{7}{8} = \frac{105}{128} \approx 0,82.$

- Sia $a = 3$, dunque $H = Sym_3 \wr Sym_b$ con $b \longrightarrow \infty$.
  In questo caso i fattori principali di $H = Sym_3 \wr Sym_b$ sono C_2, Alt_b, $D \cong C_2$, W e $(C_3)^b$. In modo analogo al caso precedente, si può vedere che gli unici contributi al calcolo di $P_H(s)$, asintoticamente, sono dati dai fattori C_2. Dunque:
  - $P_H(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right) = \frac{3}{4}\frac{1}{2} = \frac{3}{8} \approx 0,375.$
  - $P_H(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right) = \frac{15}{16}\frac{7}{8} = \frac{105}{128} \approx 0,82.$

- Sia $a = 2$, dunque $H = Sym_2 \wr Sym_b$ con $b \longrightarrow \infty$.
  In questo caso i fattori principali di $H = Sym_2 \wr Sym_b$ sono C_2, Alt_b, $D \cong C_2$, W. In modo analogo ai casi precedenti, gli unici contributi al calcolo di $P_H(s)$, asintoticamente, sono dati dai fattori C_2. Dunque:
  - $P_H(2) \longrightarrow \left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right) = \frac{3}{4}\frac{1}{2} = \frac{3}{8} \approx 0,375.$
  - $P_H(4) \longrightarrow \left(1 - \frac{1}{16}\right)\left(1 - \frac{2}{16}\right) = \frac{15}{16}\frac{7}{8} = \frac{105}{128} \approx 0,82.$

Riassumendo si ottiene quindi la seguente

Osservazione 4.4. *Nel caso in cui a sia un numero fissato, $b \longrightarrow \infty$ e b dispari, indipendentemente dal valore di a, la probabilità di generare il sottogruppo massimale di tipo intrecciato o imprimitivo di Sym_n asintoticamente tende a 0,375 nel caso in cui si considerino 2 generatori, mentre sale a 0,82 nel caso in cui si abbiano 4 generatori.*

4.2.2 Caso b pari

Per concludere l'analisi della probabilità di generare i sottogruppi massimali di tipo imprimitivo rimane da considerare il caso in cui b sia un numero *pari* fissato e $a \longrightarrow \infty$ (quindi in particolare $a \geq 5$).
Ciò che cambia dai casi visti precedentemente è che ora, essendo b pari, la diagonale D di $(C_2)^b$ è contenuta nel deleted permutation module U: come abbiamo visto nell'osservazione 4.1, in questo caso il fully deleted permutation module $W = U/D$ ha ordine 2^{b-2}. Osserviamo inoltre che in questo caso è presente anche un fattore principale isomorfo a D, centrale, di ordine 2 e non complementato: se D fosse complementato in H/N, infatti, lo sarebbe come H-modulo in U; ma dato che gli unici sottomoduli di U sono U,W,D e 0, non è possibile trovare un complemento di D in U (poichè $D \subseteq W$). Tale fattore, essendo non complementato, non contribuisce quindi al calcolo di $P_H(s)$.

I moduli irriducibili di $(C_2)^b$, per quanto appena detto, risultano essere quindi un C_2 centrale, W, e $D \cong C_2$ centrale e non complementato; gli altri fattori principali di $H = Sym_a \wr Sym_b$, invece, sono analoghi ai casi precedenti.

Costruiamo ora caso per caso, come in precedenza, le serie principali al fine di capire i contributi dati da ogni singolo fattore.

- Sia $b \geq 5$, b pari e $a \longrightarrow \infty$.
  Per quanto osservato nelle righe precedenti i fattori principali di $H = Sym_a \wr Sym_b$ risultano essere: C_2, Alt_b, C_2 centrale, $W_1 = W$, $W_2 = D \cong C_2$ non complementato e $N = (Alt_a)^b$.

  Ora il fattore W_2, dato che non è complementato, non dà contributi a $P_H(s)$; resta da capire come contribuisce il fattore W_1, che è l'unico fattore diverso rispetto al caso b dispari.
  Tale fattore ha ordine 2^{b-2} ed è abeliano: utilizzando la proposizione 2.1, il contributo che esso dà a $P_H(s)$ è pari a $\left(1 - \frac{c}{|W_1|^s}\right)$ e, poichè $c \leq |W_1|^{\frac{3}{2}}$ (vedi [4],teorema 1), si ottiene: $P_{H,W_1}(s) = \left(1 - \frac{c}{|W_1|^s}\right) \geq \left(1 - \frac{|W_1|^{\frac{3}{2}}}{|W_1|^s}\right)$.
  Osserviamo che più b è grande, più questo contributo si avvicina a 1.
  Il contributo degli altri fattori lo abbiamo già discusso più volte in precedenza.
  In definitiva, otteniamo asintoticamente:

- $P_H(2) \geq \left(1-\frac{1}{4}\right)\left(1-\frac{2}{4}\right)\left(\frac{53}{90}\right)\left(1-\frac{1}{4}\right) = \frac{3}{4}\frac{1}{2}\frac{53}{90}\frac{3}{4} = \frac{53}{320} \approx 0,166$, con caso peggiore per $b = 6$;
- $P_H(4) \geq \left(1-\frac{1}{16}\right)\left(1-\frac{2}{16}\right)\left(\frac{1661598}{1679616}\right)\left(1-\frac{1}{2^{10}}\right) = \frac{15}{16}\frac{7}{8}\frac{1661598}{1679616}\frac{1023}{1024} \approx 0,811$, con caso peggiore per $b = 6$.

- Sia ora $b < 5$, b pari, $a \longrightarrow \infty$.
  Nel caso $b = 4$ la serie principale di $H = Sym_a \wr Sym_4$ sarà composta dai fattori: C_2, C_3, $K \cong C_2 \times C_2$, C_2 centrale, $W_1 = W \cong C_2 \times C_2$, $W_2 = D \cong C_2$ centrale non complementato e, infine, $N = (Alt_a)^4$.

  Partiamo innanzitutto con l'osservare che il modulo irriducibile $C_2 \times C_2$ compare due volte come fattore principale di H, quindi si sarebbe portati a pensare che $\delta_H(C_2 \times C_2) = 2$. In realtà, però, i due moduli $C_2 \times C_2$ non sono H-isomorfi, poichè non hanno lo stesso centralizzante in H: sono moduli irriducibili diversi, entrambi aventi $\delta_H(C_2 \times C_2) = 1$.
  Vediamo ora i contributi dei singoli fattori (con le notazioni usate precedentemente):

  - $P_{H,M}(s) = \left(1-\frac{1}{2^s}\right)\left(1-\frac{2}{2^s}\right)$;
  - $P_{H/(Sym_a)^4,C_3}(s) = \left(1-\frac{3}{3^s}\right)$;
  - $P_{H/(Sym_a)^4,K\cong C_2\times C_2}(s) = \left(1-\frac{4}{4^s}\right)$;
  - $P_{H/N,W_1\cong C_2\times C_2}(s) = \left(1-\frac{c}{4^s}\right) = \left(1-\frac{4}{4^s}\right)$;
  - $P_{H/N,W_2}(s)$, essendo non-complementato, non dà contributi;
  - $P_{H,(Alt_a)^4}(s) \longrightarrow 1$ per il teorema 2.5.

  Per i primi tre contibuti è stata semplicemente applicata la formula 2.4; per il contributo $P_{H/N,W_1}$, invece, si è utilizzata la proposizione 2.1 unita al fatto che la coomologia di un modulo fedele e irriducibile per un gruppo risolubile è nulla, dunque in questo caso $c = |W_1| = 4$.
  Moltiplicando tali contributi otteniamo $P_H(s)$:

  - $P_H(2) \longrightarrow \frac{3}{4}\frac{1}{2}\frac{2}{3}\frac{3}{4}\frac{3}{4} = \frac{9}{64} \approx 0,141$;
  - $P_H(4) \longrightarrow \frac{15}{16}\frac{7}{8}\frac{26}{27}\frac{63}{64}\frac{63}{64} = \frac{200655}{262144} \approx 0,765$.

  Nel caso $b = 2$, poi, i fattori principali di $H = Sym_a \wr C_2$ sono semplicemente C_2, C_2 centrale, $W_2 \cong C_2$ non complementato e $(Alt_a)^2$: gli unici fattori che asintoticamente danno un contributo al calcolo di $P_H(s)$ sono i due ciclici complementati. Si ha quindi:

– $P_{Sym_a \wr C_2}(2) \longrightarrow \frac{3}{4}\frac{1}{2} = \frac{3}{8} \approx 0,375$;
– $P_{Sym_a \wr C_2}(4) \longrightarrow \frac{15}{16}\frac{7}{8} = \frac{105}{128} \approx 0,82$.

In conclusione, quindi, ciò che si ottiene è la seguente

Osservazione 4.5. *Se b è un numero pari fissato e $a \longrightarrow \infty$, la probabilità minore di generare un sottogruppo massimale imprimitivo di Sym_n del tipo $Sym_a \wr Sym_b$ si verifica per $b = 4$.*
La probabilità di generare questo tipo di sottogruppo a partire da due elementi dello stesso, risulta tendere asintoticamente a $0,141$; a partire da quattro elementi, invece, tende asintoticamente a $0,765$. Per tutti gli altri valori di b si hanno probabilità maggiori di generare sia con 2 che con 4 elementi.

Resterebbe da analizzare solo il caso in cui a sia un numero fissato e $b \longrightarrow \infty$, con b pari. Tale caso, però, è sostanzialmente analogo al caso visto sopra con $b \longrightarrow \infty$ e b dispari.

Dopo aver analizzato tutti i casi possibili, si giunge quindi ad enunciare:

Proposizione 4.5. *Sia Ω_n l'insieme dei massimali di tipo imprimitivo o intrecciato di Sym_n. Allora:*

$$\lim_{n\to\infty} \Big(\min_{H\in\Omega_n} P_H(2) \Big) = \lim_{a\to\infty} P_{Sym_a \wr Sym_4}(2) = \frac{9}{64} \approx 0,141; \tag{4.10}$$

$$\lim_{n\to\infty} \Big(\min_{H\in\Omega_n} P_H(4) \Big) = \lim_{a\to\infty} P_{Sym_a \wr Sym_4}(4) = \frac{200655}{262144} \approx 0,765. \tag{4.11}$$

Occupiamoci ora del caso $G = Alt_n$, quindi $H = (Sym_a \wr Sym_b) \cap Alt_n$. Come avveniva per i sottogruppi massimali intransitivi precedentemente studiati, il sottogruppo H appena scritto è un sottogruppo di $Sym_a \wr Sym_b$ di indice 2: ancora una volta quindi si perde il contributo di un fattore ciclico C_2 nel calcolo di $P_H(s)$ rispetto ai casi visti sopra.
Per il resto, invece, si procede in modo del tutto analogo al caso $G = Sym_n$ appena analizzato.

Dalla proposizione 4.5 e da quanto appena osservato, deduciamo la seguente

Proposizione 4.6. *Sia Ω_n l'insieme dei massimali di tipo imprimitivo o intrecciato di Alt_n. Allora:*

$$\lim_{n\to\infty}\Big(\min_{H\in\Omega_n} P_H(2)\Big) = \lim_{a\to\infty} P_{(Sym_a \wr Sym_4)\cap Alt_n}(2) = \frac{\frac{9}{64}}{\frac{1}{2}} \approx 0,28; \tag{4.12}$$

$$\lim_{n\to\infty}\Big(\min_{H\in\Omega_n} P_H(4)\Big) = \lim_{a\to\infty} P_{(Sym_a \wr Sym_4)\cap Alt_n}(4) = \frac{\frac{200655}{262144}}{\frac{7}{8}} \approx 0,875. \tag{4.13}$$

Prima di passare alla sezione successiva facciamo un'ultima osservazione.
Definiamo E l'insieme degli interi positivi n per cui esiste un gruppo di permutazione primitivo di grado n diverso da Alt_n e da Sym_n. In simboli, detto Ω_n l'insieme dei gruppi primitivi di permutazione di grado n:

$$E = \{n \in \mathbb{Z}^+ | \exists \omega_n \in \Omega_n \setminus \{Alt_n, Sym_n\}\}.$$

Tale insieme risulta avere densità zero (vedi [2], paragrafo 4.9): ciò significa che quasi tutti gli interi positivi n non appartengono all'insieme E.
Dalla definizione di E e dalle proposizioni 4.2, 4.3, 4.5 e 4.6 si ottiene la seguente

Proposizione 4.7. *Se $n \in \mathbb{Z}^+$, $n \notin E$, allora tutti i sottogruppi massimali di Sym_n e di Alt_n sono 2-generati.*
Inoltre valgono

$$\lim_{n\to\infty, n\notin E}\Big(\min_{H\leq_{max} Sym_n} P_H(2)\Big) = \frac{9}{64}.$$

$$\lim_{n\to\infty, n\notin E}\Big(\min_{H\leq_{max} Alt_n} P_H(2)\Big) = \frac{9}{32}.$$

4.3 Caso affine: $H = AGL_d(p) \cap G$

La tipologia di sottogruppo massimale H di $G \in \{Sym_n, Alt_n\}$ di cui ci occupiamo in questa sezione è il gruppo affine $AGL_d(p) \cap G$ che, come abbiamo visto nel capitolo 1, risulta essere isomorfo a $(GL_d(p) \ltimes C_p^d) \cap G$ (osserviamo che nel caso in cui il campo K abbia ordine primo p, lo spazio vettoriale V è isomorfo a C_p^d).

Occupiamoci come prima cosa di capire la parità del gruppo $AGL_d(p)$, in modo da comprendere se è un sottogruppo massimale di Sym_n o di Alt_n. A tal fine riportiamo la proposizione 3.8.1 presente in [1]:

Proposizione 4.8. *$AGL_d(p)$ è pari se e solo se p è pari, eccetto i casi in cui $(d, p) = (1, 2), (2, 2)$.*

Ora dal momento che p è un numero primo, se $p \neq 2$, esso risulta essere sicuramente un numero dispari: in questo caso il gruppo affine $AGL_d(p)$ è un sottogruppo massimale del gruppo simmetrico Sym_n e non è contenuto nel gruppo alterno Alt_n. Se, invece, $p = 2$ il gruppo affine $AGL_d(p)$ è un sottogruppo massimale del gruppo alterno Alt_n. Infatti, affinchè $n = p^d \to \infty$ con $p = 2$ fissato, necessariamente $d \to \infty$: facendo uno studio asintotico, quindi, i due casi eccezionali della proposizione 4.8 non si verificano mai.

4.3.1 Caso $G = Sym_n$

Sia p un primo dispari e studiamo, come fatto in precedenza, qual è la probabilità di generare il gruppo affine $AGL_d(p)$ di Sym_n con s elementi, ove $s \in \{2, 4\}$: per fare ciò dobbiamo innanzitutto scrivere una serie principale del gruppo $AGL_d(p) \cong GL_d(p) \ltimes C_p^d$.
Iniziamo con il trovare una serie principale del gruppo generale lineare $GL_d(p)$.
Consideriamo la funzione

$$det : GL_d(p) \longrightarrow K^*$$

$$A \longmapsto det(A)$$

che associa ad ogni matrice il suo determinante.
E' possibile verificare che tale funzione è un omomorfismo di gruppi (osserviamo che $K^* \cong GL_1(p)$) ed il suo kernel non è altro che il gruppo lineare speciale $SL_d(p)$, cioè il gruppo delle matrici $d \times d$ invertibili con determinante uguale a 1.
L'ordine di $SL_d(p)$ risulta essere quindi pari a $|SL_d(p)| = \frac{|GL_d(p)|}{(p-1)}$.
Il gruppo $SL_d(p)$ sarà il termine successivo a $GL_d(p)$ nella serie principale (dato che il gruppo speciale lineare coincide con il kernel dell'omomorfismo *det*, chiaramente $SL_d(p) \trianglelefteq GL_d(p)$) e il primo fattore di tale serie, per quanto abbiamo appena visto, quindi sarà $GL_d(p)/SL_d(p) \cong C_{p-1}$.

Il termine successivo della serie principale sarà poi il centro del gruppo lineare speciale, quindi $Z(SL_d(p))$, cioè il sottogruppo delle matrici scalari con determinante pari a 1.
Il fattore principale che ne deriva quindi sarà $SL_d(p)/Z(SL_d(p))$, nonchè il gruppo lineare speciale proiettivo $PSL_d(p)$.

L'ultimo fattore principale di $GL_d(p)$ dunque risulta essere $Z(SL_d(p))$.

In definitiva i fattori principali di $GL_d(p)$ sono: $C_{p-1} - PSL_d(p) - Z(SL_d(p))$.

Ora che siamo riusciti a scrivere i fattori principali di $GL_d(p)$, ricordando che $AGL_d(p) = GL_d(p) \ltimes C_p^d$ ed osservando che C_p^d è l'unico sottogruppo normale mini-

male di $AGL_d(p)$ (dimostrazione del teorema 5.5 in [9]), si ottengono immediatamente anche i fattori principali di $AGL_d(p)$, che risultano quindi essere C_{p-1}, $PSL_d(p)$, $Z(SL_d(p))$ e C_p^d.

Come nei casi già studiati dei sottogruppi massimali intransitivi e imprimitivi ciò che ci interessa fare è uno studio asintotico di $P_{AGL_d(p)}(s)$, quindi consideriamo $n = p^d \to \infty$.
Dal teorema 2.5 segue immediatamente che il contributo dato a $P_{AGL_d(p)}(s)$ dal fattore principale C_p^d tende asintoticamente a 1, così come quello dato dal fattore $PSL_d(p)$.
Osserviamo poi il seguente fatto:

Osservazione 4.6. *Il fattore $Z(SL_d(p))$ non è complementato e quindi non contribuisce al calcolo di $P_H(s)$.*
Se fosse complementato, infatti, si avrebbe che $SL_d(p) = PSL_d(p) \times Z(SL_d(p))$. Ciò però non è possibile, in quanto è noto che $SL_d(p)$ è un gruppo perfetto (cioè coincide con il suo derivato): se $SL_d(p)$ fosse uguale a $PSL_d(p) \times Z(SL_d(p))$ si dovrebbe avere la seguente serie di uguaglianze:

$$\begin{aligned} SL_d(p) = SL_d(p)^{(1)} = (PSL_d(p) \times Z(SL_d(p)))^{(1)} &= PSL_d(p)^{(1)} \times Z(SL_d(p))^{(1)} \\ &= PSL_d(p) \times 1, \end{aligned}$$

dove per l'ultima uguaglianza si è usata l'abelianità di $Z(SL_d(p))$ ed il fatto noto che $PSL_d(p)$ è un gruppo semplice.
Allo stesso tempo quindi si dovrebbe avere $SL_d(p) = PSL_d(p) \times Z(SL_d(p))$ e $SL_d(p) = PSL_d(p) \times 1$: si giunge così ad un assurdo, quindi $Z(SL_d(p))$ non può essere complementato.

Dall'analisi soprastante emerge quindi che l'unico fattore che asintoticamente contribuisce al calcolo di $P_{AGL_d(p)}(s)$ è il fattore ciclico C_{p-1}.
In generale, però, $Frat(C_{p-1}) \neq 1$: ciò che realmente contribuisce al calcolo di $P_H(s)$ dunque sarà $C_{p-1}/Frat(C_{p-1})$.
Abbiamo già visto nella dimostrazione della proposizione 3.2 che, grazie al teorema di struttura dei gruppi abeliani, si ottiene

$$C_{p-1}/Frat(C_{p-1}) \cong \prod_{q|p-1,\ q \text{ primo}} C_q.$$

Dalla formula 2.4 si ottiene che il contributo dato a $P_{AGL_d(p)}(s)$ da tale fattore principale non è altro che $\prod_{q|p-1} \left(1 - \frac{1}{q^s}\right)$, con q primo: dipende quindi dall'insieme dei fattori primi di $(p-1)$. Sfruttando poi il teorema di Dirichlet (vedi teorema 3.1), è possibile vedere che asintoticamente non ci sono limitazioni per tale insieme.

Sia infatti $\{p_1, ..., p_t\}$ una famiglia di numeri primi e applichiamo il teorema di Dirichlet con $a = 1$ e $m = p_1 p_2 ... p_t$.
Ne deduciamo immediatamente che esistono infiniti numeri primi p tali che $p \equiv 1 \pmod{p_1 ... p_t}$: preso quindi un primo p di questo tipo, $(p-1)$ risulta essere divisibile per tutti i numeri primi $p_1, ..., p_t$.
Ricordando poi l'uguaglianza 3.1 richiamata nel capitolo 3, possiamo concludere che il contributo dato dal fattore principale $C_{p-1}/Frat(C_{p-1})$ al calcolo di $P_{AGL_d(p)}(s)$ è pari al reciproco della funzione zeta di Riemann calcolata in s, quindi a $\frac{1}{\zeta(s)}$. In definitiva, quindi:

- $P_{AGL_d(p)}(2) \longrightarrow \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0,61$;
- $P_{AGL_d(p)}(4) \longrightarrow \frac{1}{\zeta(4)} = \frac{90}{\pi^4} \approx 0,92$.

Abbiamo così dimostrato la seguente

Proposizione 4.9. *Sia $AGL_d(p)$ un massimale di tipo affine di Sym_n. Allora:*

$$\lim_{n\to\infty} \left(\sup_{m \geq n} P_{AGL_d(p) \leq Sym_m}(2) \right) = \limsup_{n\to\infty} P_{AGL_d(p) \leq Sym_n}(2) = \frac{1}{\zeta(2)} \approx 0,61; \quad (4.14)$$

$$\lim_{n\to\infty} \left(\sup_{m \geq n} P_{AGL_d(p) \leq Sym_m}(4) \right) = \limsup_{n\to\infty} P_{AGL_d(p) \leq Sym_n}(4) = \frac{1}{\zeta(4)} \approx 0,92. \quad (4.15)$$

4.3.2 Caso $G = Alt_n$

Consideriamo ora il caso $G = Alt_n$: i suoi sottogruppi massimali di tipo affine saranno del tipo $H = AGL_d(p) \cap Alt_n$ se p è dispari, e $H = AGL_d(p)$ se p è pari.

Affrontiamo come prima cosa il caso $H = AGL_d(p) \cap Alt_n$ con p dispari.
Osserviamo innanzitutto che H è un sottogruppo di indice 2 del sottogruppo massimale $AGL_d(p)$ di Sym_n: il primo fattore principale di H (che abbiamo visto essere l'unico che asintoticamente contribuisce al calcolo della probabilità cui siamo interessati) sarà $C_{\frac{p-1}{2}}$ al posto di C_{p-1}.
Al fine di cogliere le differenze con il caso studiato sopra distinguiamo il caso in cui $\frac{p-1}{2}$ è dispari da quello in cui $\frac{p-1}{2}$ è pari:

- Caso $\frac{p-1}{2}$ dispari:
  in questo caso sicuramente il numero primo 2 non divide $\frac{p-1}{2}$: questo porta, a differenza di quanto accadeva per $AGL_d(p)$, a non avere il contributo $\left(1 - \frac{1}{2^s}\right)$ nel calcolo di $P_H(s)$.
  Di conseguenza per avere il valore di $P_H(s)$ in questo caso è sufficiente dividere $P_{AGL_d(p)}(s)$ per $\left(1 - \frac{1}{2^s}\right)$: così facendo $P_H(s) > P_{AGL_d(p)}(s)$.

- Caso $\frac{p-1}{2}$ pari:
  questo caso è del tutto analogo a quanto abbiamo visto per $AGL_d(p)$.
  Osserviamo che, affinchè si verifichi questo caso e quindi $\frac{p-1}{2}$ sia pari, necessariamente $p-1$ deve essere divisibile per 4: il teorema di Dirichlet, applicato con $a=1$ e $m=4p_1p_2...p_t$ ci assicura che un tale p esiste.

Si ha quindi una maggiore probabilità di generare il sottogruppo massimale affine H di Alt_n rispetto a quella di generare il sottogruppo massimale affine di Sym_n solo nel caso in cui $p-1$ non sia divisibile per 4: è sufficiente scegliere p in modo tale che $p-1$ sia divisibile per 4 affinchè la probabilità sia la stessa.

Osserviamo infine che lo studio dei sottogruppi massimali affini di Alt_n del tipo $H=AGL_d(p)$ con $p=2$ risulta superfluo al nostro scopo: vediamo ora nelle righe sottostanti che quanto abbiamo già dimostrato è sufficiente per concludere.
In generale, infatti, la probabilità di generare un sottogruppo massimale di tipo affine di Alt_n non può che essere maggiore o uguale alla probabilità di generare un sottogruppo massimale dello stesso tipo di Sym_n. Nelle righe precedenti, poi, abbiamo dimostrato l'esistenza di casi in cui si verifica l'uguaglianza: essendo interessati al valore minore che può assumere la probabilità nei vari casi, non è quindi necessario studiare $P_H(s)$ nel caso $H=AGL_d(p)$ con $p=2$.

Possiamo così generalizzare la proposizione 4.9:

Proposizione 4.10. *Sia H un massimale di tipo affine di $G \in \{Alt_n, Sym_n\}$. Allora*

$$\limsup_{n\to\infty} P_H(2) = \frac{1}{\zeta(2)} \approx 0,61; \tag{4.16}$$

$$\limsup_{n\to\infty} P_H(4) = \frac{1}{\zeta(4)} \approx 0,92; \tag{4.17}$$

4.4 Caso diagonale: $H = (S^k.(Out(S) \times Sym_k)) \cap G$

In questa sezione consideriamo i sottogruppi massimali diagonali H di $G \in \{Alt_n, Sym_n\}$, costruiti nel dettaglio nel capitolo 1. Sono la quarta tipologia di sottogruppi massimali del teorema di O'Nan-Scott e la loro forma è del tipo $H = (S^k.(Out(S) \times Sym_k)) \cap G$, dove S è un gruppo semplice finito.
Il primo obiettivo che ci proponiamo è quello di studiare asintoticamente $P_H(s)$, con $s=4$: come abbiamo fatto nelle sezioni precedenti, dobbiamo come prima cosa

costruire delle serie principali di H, differenti a seconda dei casi considerati.
Osserviamo subito che S^k è un sottogruppo normale minimo di H: per il teorema 2.5, asintoticamente, $P_H(s) = P_{(Out(S)\times Sym_k)\cap G}(s)$.

Consideriamo intanto il caso $k \geq 5$: sicuramente il gruppo $(Out(S) \times Sym_k) \cap G$ avrà tra i suoi fattori principali un ciclico C_2 e il gruppo semplice Alt_k provenienti dal termine Sym_k.
Applicando ancora una volta il teorema 2.5, asintoticamente si ha che il contributo del fattore principale Alt_k tende a 1.
Il fattore ciclico C_2 proveniente da Sym_k, poi, dà alla peggio un contributo pari a $\left(1 - \frac{8}{2^s}\right)$, in quanto nel peggiore dei casi $\delta_H(C_2) = 4$.
In formule, si avrà quindi asintoticamente:

$$P_H(s) \geq P_{Out(S)}(s)\left(1 - \frac{8}{2^s}\right) \geq \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\left(1 - \frac{4}{2^s}\right)\left(1 - \frac{8}{2^s}\right), \tag{4.18}$$

dove per l'ultima disuguaglianza si è usata la proposizione 3.2.
Osserviamo che è possibile avvicinarsi asintoticamente al bound inferiore appena trovato per $P_H(s)$: è infatti sufficiente prendere come gruppo semplice S un gruppo T appartenente alla famiglia Ω costruita nella dimostrazione dell'osservazione 3.2.

Consideriamo ora i casi $k < 5$.
Se $k = 3$ allora i fattori principali di $(Out(S) \times Sym_3) \cap G$ provenienti da Sym_3 sono un fattore ciclico C_2 di ordine 2 e un ciclico C_3 di ordine 3. Dal momento che, nel peggiore dei casi, $\delta_H(C_2) = 4$, si ottiene:

$$\begin{aligned} P_H(s) &\geq P_{Out(S)}(s)\left(1 - \frac{8}{2^s}\right)\left(1 - \frac{3}{3^s}\right) \\ &\geq \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\left(1 - \frac{4}{2^s}\right)\left(1 - \frac{8}{2^s}\right)\left(1 - \frac{3}{3^s}\right). \end{aligned} \tag{4.19}$$

Anche in questo caso ci si avvicina asintoticamente al bound inferiore nel caso in cui $S = T \in \Omega$.

Infine, se $k = 4$, oltre ai fattori principali presenti nel caso precedente (quindi se $k = 3$), vi è anche un fattore principale isomorfo al gruppo di Klein. Tale fattore dà un contributo al calcolo di $P_{(Out(S)\times Sym_3)\cap G}(s)$ pari a $\left(1 - \frac{4}{4^s}\right)$. In definitiva quindi, asintoticamente, si ottiene:

$$\begin{aligned} P_H(s) &\geq P_{Out(S)}(s)\left(1 - \frac{8}{2^s}\right)\left(1 - \frac{3}{3^s}\right)\left(1 - \frac{4}{4^s}\right) \\ &\geq \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\left(1 - \frac{4}{2^s}\right)\left(1 - \frac{8}{2^s}\right)\left(1 - \frac{3}{3^s}\right)\left(1 - \frac{4}{4^s}\right). \end{aligned} \tag{4.20}$$

Ancora una volta, prendendo come gruppo semplice S un gruppo $T \in \Omega$ costruito nella dimostrazione di 3.2, è possibile avvicinarsi asintoticamente al bound inferiore della disuguaglianza sopra scritta.
Confrontando le disuguaglianze 4.18, 4.19 e 4.20 ottenute per i diversi valori di k, emerge immediatamente che la probabilità minore si verifica nel caso in cui si pone $k = 4$ e $S = T \in \Omega$.

Calcolando tale quantità per $s = 4$, si ottiene la seguente proposizione generale:

Proposizione 4.11. *Sia Ω_n l'insieme dei massimali di tipo diagonale di $G \in \{Sym_n, Alt_n\}$. Allora:*

$$\limsup_{n\to\infty} P_H(4) = \limsup_{n\to\infty} P_{(Out(T)\times Sym_4)\cap G}(4) = \frac{1}{\zeta(4)}\frac{1}{\zeta(3)}\frac{91}{256} \approx 0,273. \tag{4.21}$$

4.4.1 Parità del sottogruppo diagonale

Quanto fatto fino a questo momento non prende, però, in considerazione la parità di H, cioè non è al momento noto se H sia un sottogruppo massimale del gruppo alterno Alt_n o del simmetrico Sym_n: vediamo nelle righe seguenti cosa si può dire a riguardo.
Consideriamo a tal proposito la parte finale della dimostrazione del teorema 5.5 in [9], in cui viene dimostrato che se $k \neq 2$, allora $Sym_k \leq Alt_n$. In questo caso la parità del sottogruppo massimale H dipende solamente dalla parità di $Out(S)$ dato che $Sym_k \leq Alt_n$ e che S^k, essendo un prodotto di gruppi semplici, è contenuto in Alt_n.
Nelle righe seguenti dimostreremo che anche $Aut(S)$ (e di conseguenza $Out(S)$), è contenuto nel gruppo alterno.
Osserviamo subito che il gruppo alterno, avendo indice 2 nel simmetrico, contiene tutti gli elementi di ordine dispari: ciò implica che possiamo ridurci a dimostrare che tutti gli elementi di $Aut(S)$ di ordine potenza di 2 sono pari.
Sia quindi $\alpha \in Aut(S)$ tale che $|\alpha| = 2^r$, con $r \in \mathbb{N}$.
Per $0 \leq i \leq r$ definiamo

$$\Delta_i = C_S(\alpha^{2^{r-i}}).$$

In particolare si ha che

$$\begin{cases} \Delta_0 = C_S(\alpha^{2^r}) = C_S(1) = S \\ \Delta_r = C_S(\alpha) \end{cases} \tag{4.22}$$

Osserviamo poi che, per definizione di Δ_i, le orbite dell'azione di α sull'insieme $\Delta_i \setminus \Delta_{i+1}$ hanno tutte lunghezza pari a 2^{r-i}. Detta $\delta_i = |\Delta_i|$, quindi, si ottiene

$$\delta_i \equiv \delta_{i+1} \mod 2^{r-i}, \qquad 0 \leq i \leq r-1. \tag{4.23}$$

Sfruttando le relazioni sottolineate in 4.22, inoltre, otteniamo che δ_r indica il numero di punti fissi di α, mentre δ_0 non è altro che la cardinalità di S: essendo quest'ultimo un gruppo semplice, la sua cardinalità risulta essere un numero pari.
Scriviamo ora la relazione 4.23 con $i = 0$, ottenendo così $\delta_0 \equiv \delta_1 \mod 2^r$: dato che δ_0 per quanto appena osservato è pari, necessariamente lo è anche δ_1. Imponendo poi $i = 1$, otteniamo che anche δ_2 è pari, ma allora lo è anche δ_3 e via dicendo: in sostanza, $\delta_0, \delta_1, ..., \delta_{r-1}$ sono tutti numeri pari.

Consideriamo ora l'azione di $Aut(S)$ su $\Omega = S^k : diag(S)$. Osserviamo subito che gli elementi di Ω, per ogni classe laterale di $diag(S)$, sono del tipo $(1, s_1, s_2, ..., s_{k-1})$, con $s_i \in S$: ecco quindi che è possibile identificare Ω con S^t, essendo $t = k - 1$.
A questo punto l'azione di $Aut(S)$ su Ω è esattamente la seguente:

$$(s_1, ..., s_t)^\alpha = (s_1^\alpha, ..., s_t^\alpha).$$

Sia dunque $\alpha \in Aut(S)$ di ordine 2^r, con $r \neq 0$.
Per quanto precedentemente osservato α fissa tutti gli elementi di Δ_r^t, mentre su $\Delta_i^t \setminus \Delta_{i+1}^t$ agisce come prodotto di $\dfrac{\delta_i^t - \delta_{i+1}^t}{2^{r-i}}$ cicli di lunghezza 2^{r-i}.
Osservando poi che

$$\frac{\delta_i^t - \delta_{i+1}^t}{2^{r-i}} = \Big(\frac{\delta_i - \delta_{i+1}}{2^{r-i}}\Big)(\delta_i^{t-1} + \delta_i^{t-2}\delta_{i+1} + ... + \delta_{i+1}^{t-1}),$$

è possibile concludere che α è in realtà una permutazione pari. Grazie alla relazione 4.23, infatti, il termine $\Big(\dfrac{\delta_i - \delta_{i+1}}{2^{r-i}}\Big)$ è un numero intero ed il termine $(\delta_i^{t-1} + \delta_i^{t-2}\delta_{i+1} + ... + \delta_{i+1}^{t-1})$, essendo una somma di numeri pari, risulta essere a sua volta un numero pari.
A questo punto, quindi, α agisce come prodotto di un numero pari di cicli di lunghezza 2^{r-i}: ricordando la definizione del segno di una permutazione si ottiene che $sgn(\alpha) = 1$ e dunque α è una permutazione pari.
Come richiamato in precedenza, poi, il fatto che tutti gli elementi di $Aut(S)$ con ordine potenza di 2 siano pari implica che lo siano tutti gli elementi di $Aut(S)$: $Aut(S)$ è dunque contenuto in $Alt(\Omega)$.

Abbiamo così dimostrato che, se $k \neq 2$, il sottogruppo diagonale $H = S^k.(Out(S) \times Sym_k)$ è un sottogruppo massimale del gruppo alterno Alt_n.

Vediamo ora cosa si può dire nel caso rimanente, cioè nel caso $k = 2$.
Indagando ancora una volta la dimostrazione del teorema 5.5 in [9], emerge l'implicazione

$$N = \frac{|S| - i_2(S) - 1}{2} \quad \text{dispari} \Longrightarrow Alt_n \not\leq H, \tag{4.24}$$

dove con $i_2(S)$ si è indicato il numero delle involuzioni (cioè degli elementi di ordine 2) di S.
Se la quantità indicata con N è un numero dispari, quindi, il gruppo $H = S^2.(Out(S) \times Sym_2)$ risulta essere un sottogruppo massimale del gruppo simmetrico Sym_n.

Il teorema di Herzog (vedi [5]) sotto riportato, poi, classifica i gruppi semplici S con $i_2(S) \equiv 1 \mod 4$:

Teorema 4.2. *(Herzog)*
Sia S un gruppo semplice finito con $i_2(S)$ involuzioni e supponiamo $i_2(S) \equiv 1 \mod 4$. Allora vale una delle seguenti:

1. $i_2(S) = 1$ *e S è ciclico di ordine 2;*
2. $i_2(S) = 105$ *e $S \simeq A_7$;*
3. $i_2(S) = 165$ *e $S \simeq M_{11}$;*
4. $i_2(S) = \dfrac{q(q+\epsilon)}{2}$ *e $S \simeq PSL_2(q)$, dove $q = p^n > 3$ è una potenza di un primo dispari, $\epsilon = \pm 1$ e $q = \epsilon \mod 8$;*
5. $i_2(S) = q^2(q^2+q+1)$ *e $S \simeq PSL_3(q)$, dove $q = p^n$ è una potenza di un primo dispari e $q = -1 \mod 4$;*
6. $i_2(S) = q^2(q^2-q+1)$ *e $S \simeq PSU_3(q)$, dove $q = p^n$ è una potenza di un primo dispari e $q = 1 \mod 4$.*

Osserviamo ora il seguente fatto: essendo S un gruppo semplice, il suo ordine è sicuramente divisibile per 4; se inoltre lo stesso S compare nella lista del teorema di Herzog, allora $i_2(S) \equiv 1 \mod 4$ e dunque $i_2(S) \not\equiv -1 \mod 4$.
Ciò significa che in questo caso specifico N è un un numero dispari e dunque il sottogruppo $H = S^2.(Out(S) \times Sym_2)$ risulta essere un massimale del gruppo simmetrico.
E' così possibile indagare qual è la minor probabilità di generare un sottogruppo massimale diagonale di Sym_n di questo tipo.

Sfruttando ancora una volta la tabella in figura 3.1, vediamo che se S appartiene al quinto tipo del teorema di Herzog allora $Out(S) = C_{(3,q-1)} \rtimes C_n \times C_2$: prendendo quindi $q = 7^n$ con n dispari, dal momento che $7^n \equiv 1 \mod 3$, si ha $Out(S) = C_3 \rtimes C_n \times C_2$. Di conseguenza $H = S^2.(C_3 \rtimes C_n \times C_2 \times C_2)$.
Ragionando come in precedenza otteniamo che per $n \to \infty$, se $S \simeq PSL_3(q)$ con $q = 7^n$ e n dispari,

$$\limsup_{n\to\infty} P_H(s) = \frac{1}{\zeta(s)}\Big(1 - \frac{2}{2^s}\Big)\Big(1 - \frac{4}{2^s}\Big)\Big(1 - \frac{3}{3^s}\Big). \tag{4.25}$$

Vediamo (grazie alla tabella in figura 3.1) che questo valore, per S gruppo semplice tale che $i_2(S) \equiv 1 \mod 4$, risulta essere il più piccolo possibile.

- Se S è del primo o del terzo tipo del teorema di Herzog allora $Out(S) = 1$; di conseguenza $H = S^2.(C_2)$. Chiaramente

$$P_H(s) = \Big(1 - \frac{1}{2^s}\Big) > \frac{1}{\zeta(s)}\Big(1 - \frac{2}{2^s}\Big)\Big(1 - \frac{4}{2^s}\Big)\Big(1 - \frac{3}{3^s}\Big).$$

- Se S è del secondo tipo allora $Out(S) = C_2$, quindi $H = S^2.(C_2 \times C_2)$. Anche in questo caso è immediato vedere che $P_H(s)$ è strettamente maggiore del valore trovato in 4.25.

- Se S è del tipo 4 descritto nel teorema di Herzog allora $Out(S) = C_2 \times C_n$ (poichè $(2, q-1) = 2$); di conseguenza quindi

$$\limsup_{n\to\infty} P_H(s) = \frac{1}{\zeta(s)}\Big(1 - \frac{2}{2^s}\Big)\Big(1 - \frac{4}{2^s}\Big) > \frac{1}{\zeta(s)}\Big(1 - \frac{2}{2^s}\Big)\Big(1 - \frac{4}{2^s}\Big)\Big(1 - \frac{3}{3^s}\Big).$$

- Infine se S è di tipo 6, alla peggio (ad esempio scegliendo $p = 5$ e n dispari) si ottiene

$$\limsup_{n\to\infty} P_H(s) = \frac{1}{\zeta(s)}\Big(1 - \frac{3}{3^s}\Big)\Big(1 - \frac{2}{2^s}\Big) > \frac{1}{\zeta(s)}\Big(1 - \frac{2}{2^s}\Big)\Big(1 - \frac{4}{2^s}\Big)\Big(1 - \frac{3}{3^s}\Big).$$

Abbiamo quindi dimostrato la seguente

Proposizione 4.12. *Sia Ω_n l'insieme dei massimali di tipo diagonale di $G \in \{Alt_n, Sym_n\}$.*
Se $k \neq 2$ allora $\Omega_n \subset Alt_n$ e vale

$$\limsup_{n\to\infty} P_H(4) = \limsup_{n\to\infty} P_{(Out(T)\times Sym_4)\cap G}(4) = \frac{1}{\zeta(4)}\frac{1}{\zeta(3)}\frac{91}{256} \approx 0,273. \qquad (4.26)$$

Se $k = 2$ e S gruppo semplice tale che $i_2(S) \equiv 1 \mod 4$ allora i sottogruppi di tipo diagonale di Ω_n sono sottogruppi massimali di Sym_n. Inoltre vale

$$\limsup_{n\to\infty} P_H(4) = \frac{1}{\zeta(4)}\Big(1 - \frac{2}{2^4}\Big)\Big(1 - \frac{4}{2^4}\Big)\Big(1 - \frac{3}{3^4}\Big) \approx 0,584. \qquad (4.27)$$

4.5 Caso almost simple

Il quinto ed ultimo caso che rimane da indagare nel dettaglio è il caso dei sottogruppi massimali almost simple di $G \in \{Alt_n, Sym_n\}$.
Nel capitolo 3 abbiamo trattato nel dettaglio la probabilità di generare con s elementi un generico gruppo almost simple: applicando la proposizione 3.3 al sottogruppo massimale almost simple H di $G \in \{Alt_n, Sym_n\}$, si ha che

$$\limsup_{n\to\infty} P_H(s) = \frac{1}{\zeta(s)}\frac{1}{\zeta(s-1)}\Big(1-\frac{4}{2^s}\Big). \tag{4.28}$$

Osserviamo immediatamente che, per ogni valore di s, tale valore risulta essere strettamente superiore a quello che si ottiene nel caso peggiore dei sottogruppi massimali diagonali.
Purtroppo, la parità dei sottogruppi massimali di tipo almost simple è ostica da indagare. Ricordiamo, però, che siamo interessati ad identificare il caso peggiore in assoluto, quindi il valore più basso di $P_H(d(H))$ al variare di H tra i diversi sottogruppi massimali di $G \in \{Alt_n, Sym_n\}$: da quanto appena osservato segue che a tale scopo non è essenziale indagare sulla parità degli almost simple, potendo infatti ricondursi a studiare i sottogruppi massimali di tipo diagonale.

Conclusione

L'obiettivo che ha guidato la stesura di questa tesi è stato quello di capire, a livello asintotico, con quanta probabilità si riescono a generare i sottogruppi massimali di Sym_n o di Alt_n a partire da 4 elementi casuali.
Ripercorrendo il lavoro svolto nell'ultimo capitolo si evince come la probabilità asintotica minore si abbia con i sottogruppi massimali di $G \in \{Sym_n, Alt_n\}$ di tipo diagonale, ossia i sottogruppi della forma $S^k.(Out(S) \times Sym_k) \cap G$. Per tale tipologia di sottogruppi, però, l'analisi effettuata non ricopre tutte le varie casistiche nel caso in cui k risulti pari a 2: in questo caso abbiamo mostrato che, se le involuzioni del gruppo semplice S soddisfano la condizione $i_2(S) \equiv 1 \mod 4$, allora il sottogruppo massimale diagonale è un sottogruppo di Sym_n e la probabilità asintotica di generarlo con 4 elementi è approssimabile a 0,584. Tale valore, se confrontato con le probabilità ottenute per gli altri tipi di sottogruppi massimali di Sym_n, risulta in ogni caso essere quello minore e dunque non si è reso strettamente necessario studiare anche i casi in cui $i_2(S) \not\equiv 1 \mod 4$.
Se invece $k \neq 2$ il sottogruppo massimale diagonale è sottogruppo di Alt_n e la probabilità trovata risulta approssimabile a 0,273: tale valore è decisamente il minore in assoluto trovato.
In definitiva possiamo comunque affermare che, in linea generale, si ha una buona probabilità asintotica di generare i sottogruppi massimali di $G \in \{Sym_n, Alt_n\}$ con pochi elementi, soprattutto se si tiene conto del risultato visto nella proposizione 4.7.

In questo lavoro è emerso, inoltre, un risultato importante ed indipendente dai gruppi di permutazione: si è infatti trovato il valore della probabilità asintotica di generare un gruppo almost simple.

Ringraziamenti

Ebbene sì, siamo giunti al termine di questa avventura matematica! Arrivata finalmente a questo "Momento di Gloria" (Anna, Genny... quanto lo abbiamo desiderato?!) non posso fare altro che ringraziare le persone che mi hanno dato una mano, ed ogni tanto anche un braccio, per arrivare fino a qui.

Prima di tutto voglio ringraziare il mio relatore, il professore Andrea Lucchini. E' stato per me una guida costante ed estremamente efficiente: la sua disponibilità è stata davvero impagabile. La ringrazio per esserci stato sempre ed avermi accettata come tesista sia per la tesi triennale che per quella magistrale.
La parola "insegnante" deriva da "in-segnare", lasciare un segno: lei sicuramente nel mio percorso di studi questo segno l'ha lasciato, e non posso fare altro che ringraziarla.

In secondo luogo ringrazio con il cuore la mia famiglia. Sembra banale dire che senza il vostro sostegno probabilmente non ce l'avrei fatta (e non parlo "solo" di quello economico, papà!), ma è proprio così.
In tutto il mio percorso di studi non è mai mancata la vostra comprensione od una parola di conforto: devo riconoscere che in questi anni vi siete giocati tutte le carte possibili, compresa Nanù, per farmi tornare il sorriso quando le cose non andavano come avrei voluto. Ma finalmente la vostra "giovane Mennea" ce l'ha fatta!
Un grazie va anche a mio fratello Luca che, anche se fisicamente distante, ha trovato sempre il tempo per chiedermi come stavano andando le cose ed ha pazientato quando non potevo giocare a Pandemic perchè "devo studiare!".
Quindi grazie infinite a voi, che sicuramente più di tutti, mi avete supportata e, soprattutto, sopportata!
Con la famiglia voglio ringraziare anche tutti i miei parenti (e le preghiere della nonna), che hanno sempre fatto il tifo per me.

Devo poi ringraziare i miei amici: quelli vecchi, quelli nuovi e quelli che ormai sono una costante di vita. Ringrazio chi c'è stato nei primi anni difficili di questo percorso, e ringrazio quelli che mi hanno "raccolto" poi, a cammino iniziato.

Chiaramente non posso non fare il nome della mia amica Mery, che ha saputo capire che amicizia non è vedersi sempre ma esserci sempre; Ser, che si è sorbito qualsiasi sventura e che alla fine è venuto a studiare a Padova per condividere un altro pezzo di vita insieme ed infine la Giovy, dalla quale il sostegno non ha mai tardato a farsi sentire. Non nomino tutti gli altri di "SEUB" altrimenti non finisco più, ma vi ringrazio tutti per essere così come siete ed avermi accolta senza nessuna esitazione.

Voglio dedicare un paio di righe anche ai miei pazzi amici clown, senza i quali la mia vita avrebbe un colore decisamente più spento. Vi ringrazio per avermi portato fortuna ad ogni esame fatto il giorno dopo del servizio, ma soprattutto per i momenti profondi e le risate che abbiamo vissuto insieme.
E come dimenticare i miei amici matematici? Genny ed Anna, compagne fidate fin dal primo anno; Giovanni, il cui aiuto è stato spesso indispensabile ed infine Ale, che mi ha sempre incoraggiata. Non nomino anche tutti gli altri, ma i banchi della torre sono testimoni di quanto ci siamo aiutati in tutti questi anni. Grazie!

Ultimo, ma non meno importante, voglio ringraziare Enrico.
Fin dal primo momento hai sempre creduto in me e mi hai sostenuta, dandomi la serenità e l'appoggio per affrontare questi ultimi anni di università. Studiare insieme condividendo la fatica e poi la gioia dei nostri traguardi resterà uno dei miei ricordi migliori.
Grazie per esserci stato sempre.

Bibliografia

[1] Alberto Basile. *Second maximal subgroups of the finite alternating and symmetric groups*. PhD thesis, 01 2001.

[2] Peter J. Cameron. *Permutation Groups*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[3] E. Detomi and A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *Journal of Algebra*, 265(2):651 – 668, 2003.

[4] Robert M. Guralnick and Cornelius Hoffman. The first cohomology group and generation of simple groups. In Lino di Martino, William M. Kantor, Guglielmo Lunardon, Antonio Pasini, and Maria Clara Tamburini, editors, *Groups and Geometries*, pages 81–89, Basel, 1998. Birkhäuser Basel.

[5] Marcel Herzog. On the classification of finite simple groups by the number of involutions. *Proceedings of The American Mathematical Society - PROC AMER MATH SOC*, 77, 03 1979.

[6] I.M. Isaacs. *Finite Group Theory*. Graduate studies in mathematics. American Mathematical Society, 2008.

[7] Peter B. Kleidman and Martin W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1990.

[8] Andrea Lucchini. Generating wreath products and their augmentation ideals. *Rendiconti del Seminario Matematico della Università di Padova*, 98:67–87, 1997.

[9] Andrea Lucchini, Claude Marion, and Gareth Tracey. Generating maximal subgroups of finite almost simple groups, 07 2018.

[10] Nina E. Menezes, Martyn Quick, and Colva M. Roney-Dougal. The probability of generating a finite simple group. *Israel Journal of Mathematics*, 198(1):371–392, Nov 2013.