ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

IL CYCLIC SIEVING PHENOMENON

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
Fabrizio Caselli

Presentata da:
Giuditta Bellosi

Sessione Unica
Anno Accademico 2018-2019

Alla mia famiglia,
di sangue e non …

Introduzione

In questa tesi ci siamo riproposti di presentare quello che è noto in letteratura come *fenomeno del setaccio ciclico*, in inglese *cyclic sieving phenomenon* (da cui l'acronimo CSP), che si verifica nell'azione di un gruppo ciclico G su un insieme finito: esso consiste nel fatto che il numero di elementi dell'insieme fissati da ogni sottogruppo di G corrisponde alla valutazione di un polinomio a coefficienti interi in una radice primitiva dell'unità di ordine corrispondente a quello del sottogruppo considerato. Il nostro obbiettivo è quindi di studiare il CSP in determinati contesti algebrici.
Nel primo capitolo richiameremo brevemente la nozione di azione di un gruppo su un insieme e di radice dell'unità, mentre nel secondo presenteremo il CSP e le sue caratteristiche fondamentali.
Nel terzo capitolo analizzeremo tale fenomeno nella teoria dei multinsiemi: nella prima parte descriveremo l'ambiente dei multinsiemi e le loro proprietà, soffermandoci in particolare sull'azione del gruppo simmetrico su di essi, mentre nella seconda daremo la definizione di polinomio gaussiano e metteremo in luce alcune sue proprietà. Il CSP mostrato in questo capitolo è di particolare importanza in quanto verrà ripreso e dimostrato, con nuovi contesti e strumenti, nei due capitoli successivi.
Nel quarto capitolo ci occupiamo di studiare il fenomeno del setaccio ciclico nel contesto della Teoria della Rappresentazione. Inizieremo introducendo le nozioni base di tale teoria passando poi, nella seconda parte, a mostrare come tale fenomeno possa essere visto come il cambiamento di base all'interno di un G-modulo. Nella parte successiva, abbiamo raccolto alcuni risultati

della Teoria della Rappresentazione che ci permetteranno di enunciare il teorema che garantisce la presenza del CSP in una terna generica sfruttando esclusivamente l'isomorfismo tra G-moduli. Nell'ultima sezione definiremo i tensori simmetrici e li utilizzeremo per fornire un'ulteriore dimostrazione al CSP enunciato nel caso dei multinsiemi.
Nel quinto capitolo ci focalizzeremo sullo studio del fenomeno nel contesto dei gruppi generati da riflessioni complesse, sfruttando l'azione libera dei gruppi. L'intento principale è quello di fornire una visione più complessa del cyclic sieving phenomenon e di dimostrare come questa si possa ricondurre, in determinati contesti, al CSP mostrato nel caso dei multinsiemi. Per prima cosa introduciamo le azioni libere e semi libere di gruppi ciclici collegandole, attraverso il concetto di regolarità, ai gruppi generati dalle riflessioni complesse. Poi definiremo due importanti algebre, l'algebra gruppo e l'algebra dei coinvarianti, di cui dimostreremo alcune proprietà. Tali algebre sono necessarie per enunciare un importante teorema sul CSP che mette in relazione gli elementi precedentemente citati. Questo teorema può essere utilizzato per dimostrare il CSP nel caso dei multinsiemi, attraverso i gruppi di Coxeter. Nella terza sezione infatti, presenteremo i gruppi di Coxeter ed alcune loro importanti caratteristiche, come la funzione *inversione*. Ci soffermeremo soprattuto sul gruppo simmetrico visto come gruppo di Coxeter e sulle conseguenze di questo fatto. Concluderemo dimostrando il CSP enunciato nel terzo capitolo con le nozioni acquisite.
Alcuni dei risultati presentati in questa tesi sono particolarmente complessi e vi è una vasta letteratura a riguardo; per questo in determinati casi abbiamo preferito accennare soltanto alla dimostrazione, privilegiando la visione di insieme e la comprensione profonda dei concetti.

Indice

Capitolo 1

Premesse

L'intento di questo capitolo è quello di presentare i concetti necessari ad una completa affermazione del fenomeno analizzato in questa tesi.

1.1 Nozioni sui Gruppi

Per prima cosa consideriamo un gruppo ciclico **finito**.

Definizione 1.1. Un gruppo G si dice *finito* se è costituito da un numero finito di elementi.

Definizione 1.2. Un gruppo G si dice *ciclico* se esiste un elemento $g \in G$ tale che

$$G = \{g^n : n \in \mathbb{Z}\}. \tag{1.1}$$

Definizione 1.3. Sia G un gruppo, e l'elemento neutro di G e $g \in G$. Si dice *ordine* di g e si indica con *o(g)* il più piccolo $n \in \mathbb{N}$ tale che:

$$g^n = e. \tag{1.2}$$

Definiamo, ora, l'azione di un gruppo su un insieme.

Definizione 1.4. Sia X un insieme e C un gruppo. L'*azione di C su X* è una funzione definita nel seguente modo:

$$\begin{aligned} C \times X &\longrightarrow X \\ (\sigma, x) &\longmapsto \sigma \cdot x, \end{aligned} \tag{1.3}$$

tale che valgano le seguenti proprietà:

1. $1_C \cdot x = x$ $\quad \forall x \in X,$
2. $g \cdot (h \cdot x) = (gh) \cdot x$ $\quad \forall g, h \in$ C e $\forall x \in X.$

Definizione 1.5. Sia X un insieme finito, C gruppo ciclico e sia $g \in C$. L'*insieme dei punti fissi di* X è il seguente:

$$X^g = \{y \in X : gy = y\}. \tag{1.4}$$

1.2 Le radici n-esime dell'unità

Presentiamo le radici n-esime primitive dell'unità.

Definizione 1.6. Chiamiamo *radici n-esime dell'unità*, le soluzioni complesse dell'equazione:

$$x^n = 1. \tag{1.5}$$

Definizione 1.7. Chiamiamo Ω il gruppo delle radici n-esime complesse dell'unità.

Definizione 1.8. Le radici n-esime *primitive* dell'unità sono tutte le radici n-esime complesse dell'unità che generano Ω.

Capitolo 2

Il cyclic sieving phenomenon

In questo capitolo presentiamo l'oggetto del nostro studio.

Definizione 2.1. Sia una terna *(X, C, f(q))* con X un insieme finito, C un gruppo ciclico finito che agisce su X ed *f(q)* $\in \mathbb{N}[q]$ associato a X.
Diciamo che la terna *(X, C, f(q))* presenta il *cyclic sieving phenomenon* se $\forall\, g \in C$ si verifica che:

$$\#X^g = f(\omega_{o(g)}). \tag{2.1}$$

Da questa prima definizione possiamo osservare che:

Osservazione 1. La radice *o(g)*-esima primitiva dell'unita sulla quale valutiamo il polinomio, non è scelta in modo univoco. Vale il seguente risultato.
Sia $f(q) \in \mathbb{C}[q]$ un polinomio complesso che valutato nelle radici n-esime dell'unità dà come risultato un numero razionale.
Siano ora *u,v* due radici primitive d-esime dell'unità, con $d|n$. Poichè u e v hanno lo stesso polinomio minimo, il d-esimo polinomio ciclotomico, esiste un isomorfismo di campi:

$$\begin{aligned} \phi : \mathbb{Q}[u] &\longrightarrow \mathbb{Q}[v] \\ u &\longmapsto v \\ a &\longmapsto a, \end{aligned} \tag{2.2}$$

per ogni $a \in \mathbb{Q}$.
Di conseguenza $f(u) = \phi(f(u)) = f(\phi(u)) = f(v)$. Il polinomio f assume

quindi lo stesso valore su ogni radice primitiva d-esima dell'unità.
Questo risultato è fondamentale in quanto ci permetterà di valutare il polinomio in una qualsiasi radice primitiva *o(g)*-esima dell'unità.

Osservazione 2. Inizialmente, potrebbe sembrare strano come, valutando un polinomio a coefficienti interi in un numero complesso, si ottenga un numero intero che vada effettivamente a contare qualcosa. Dimostreremo però, contesto per contesto, come la scelta di questo polinomio renda effettivamente possibile il fenomeno.

Osservazione 3. Inoltre, si fa riferimento al polinomio scelto come un polinomio *naturalmente associato* in quanto si deve verificare che, nel caso in cui $g = e$:

$$f(1) = \#X. \tag{2.3}$$

Ovvero si deve verificare che il polinomio valutato nell'unità sia esattamente la cardinalità dell'insieme di partenza.

Capitolo 3

CSP sui multinsiemi

L'intento di questo capitolo è quello di studiare il *cyclic sieving phenomenon* nell'ambiente dei multinsiemi. La scelta di questo contesto è conveniente per varie ragioni. Da un lato, fornisce una verifica abbastanza semplice del CSP. Dall'altro, questo risultato può essere ottenuto anche in contesti più complessi, come vedremo nei capitoli successivi.

3.1 I multinsiemi

Presentiamo i multinsiemi e le loro proprietà.

Definizione 3.1. Sia $n \in \mathbb{N}$ e sia $[n]= \{1,2,\ldots\}$. Si dice *multinsieme* su $[n]$ e si indica con M la seguente famiglia:

$$M = \{i_1 i_2 \ldots i_k \ \text{ t .c } \ 1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n \ \text{ e } \ k \in \mathbb{N}\}. \tag{3.1}$$

Pertanto, un multinsieme su $[n]$ è una lista ordinata in modo crescente di numeri naturali minori di n.
Possiamo, inoltre, dare una definizione di multinsieme che tenga conto della molteplicità dei singoli numeri nella lista.

Definizione 3.2. Sia $n \in \mathbb{N}$ e sia $[n]= \{1,2,\ldots\}$. Si dice *multinsieme* su $[n]$ e si indica con M la seguente famiglia:

$$M = \{1^{m_1}, 2^{m_2}, \ldots, n^{m_n}\}, \tag{3.2}$$

dove m_i è la molteplicità del numero i in M.
La *cardinalità* di un multinsieme è la somma delle molteplicità dei suoi numeri:

$$\# M = \sum_{i=1}^{n} m_i. \tag{3.3}$$

Esempio 3.1. $M = 222344555 = \{2^3, 3, 4^2, 5^3\}$.

Definiamo l'unione disgiunta di multinsiemi.

Definizione 3.3. Siano L ed M due multinsiemi tali che: L=$\{ 1^{l_1}, 2^{l_2}, \ldots, n^{l_n}\}$ ed M=$\{ 1^{m_1}, 2^{m_2}, \ldots, n^{m_n}\}$. Si definisce *unione disgiunta di multinsiemi*:

$$L \sqcup M = \{1^{l_1+m_1}, 2^{l_2+m_2}, \ldots, n^{l_n+m_n}\}. \tag{3.4}$$

Definiamo l'insieme finito che consideriamo nel CSP di questo capitolo:

$$X = \left(\binom{[n]}{k}\right) = \{M : \text{è un multinsieme di } [n] \text{ di cardinalità } k\}. \tag{3.5}$$

Vediamo un semplice esempio per capire come è costituito questo insieme.

Esempio 3.2. Sia n= 3 e k= 2 allora $X = \{11, 22, 33, 44, 12, 13, 23\}$.

Il secondo elemento necessario nella terna è un gruppo ciclico finito.

Definizione 3.4. Un *n-ciclo* di $\mathbb{N}$ è una permutazione di n elementi. Ogni *n-ciclo* ha quindi ordine n.

Il gruppo ciclico finito che prendiamo in considerazione è gruppo generato da un n-ciclo:

$$C_n = \big\langle (1, 2, \ldots, n) \big\rangle. \tag{3.6}$$

Mostriamo ora l'azione di C_n su M.

Definizione 3.5. Sia $g \in C_n$ e $M = \{i_1 i_2 \dots i_k\}$; g agisce su M nel seguente modo:

$$gM = g(i_1)g(i_2)\cdots g(i_k), \tag{3.7}$$

riscrivendo in ordine crescente la parte destra dell'equazione.

Riprendiamo l'esempio 3.2.
Consideriamo il gruppo ciclico $C_3 = \{$ e, (1,2,3),(1,3,2)$\}$ e l'elemento g=(1,2,3), g agisce su X nel seguente modo:

$$\begin{array}{ccc} (1,2,3)\mathbf{11} = \mathbf{22} & (1,2,3)\mathbf{22} = \mathbf{33} & (1,2,3)\mathbf{33} = \mathbf{11} \\ (1,2,3)\mathbf{12} = \mathbf{23} & (1,2,3)\mathbf{13} = \mathbf{12} & (1,2,3)\mathbf{23} = \mathbf{13}. \end{array} \tag{3.8}$$

Giunti a questo punto è necessario calcolare $\#X^g$.
Per fare ciò utilizziamo il gruppo delle permutazioni di $[n]$ che indichiamo con $\mathfrak{S}_n$.

Osservazione 4. Si può osservare come l'azione (3.7) resti valida sui multinsiemi per qualsiasi $g \in \mathfrak{S}_n$.

Osservazione 5. Inoltre, possiamo applicare l'unione disgiunta di multinsiemi, definita in (3.3), direttamente ai cicli di $\mathfrak{S}_n$. E' sufficiente considerare ogni ciclo come un insieme, ovvero come un multinsieme in cui le uniche molteplicità presenti sono 1 o 0.

Esempio 3.3. $(1,3,4) \sqcup (1,4,5) \sqcup (4,5,6) = \{1^2, 3, 4^3, 5^2, 6\}$.

Vediamo ora un lemma fondamentale per il proseguo della dimostrazione.

Lemma 3.1.1. *Sia $g \in \mathfrak{S}_n$ con la seguente decomposizione in cicli disgiunti $g = c_1 c_2 \dots c_t$.*
Allora gM=M se e solo se M può essere scritto come:

$$M = c_{r_1} \sqcup c_{r_2} \sqcup \dots c_{r_r} \quad t.c. \quad r_i \in \{1, \dots, t\}, \tag{3.9}$$

in cui i cicli nell'unione disgiunta non devono essere distinti per forza.

Dimostrazione. ($\Leftarrow$) Sia c un ciclo di g. Abbiamo visto che possiamo considerare un ciclo come un insieme nell'Osservazione 5. Sia quindi $\bar{c}$ l'insieme corrispondente a c. Poichè g agisce su $\bar{c}$ permutando tra loro i suoi elementi, abbiamo che $g\bar{c} = \bar{c}$. g fissa dunque ogni singolo insieme, e quindi ogni singolo ciclo. Di conseguenza g fissa le unioni disgiunte di questi cicli.
($\Rightarrow$) Dimostriamo questo lato dell'implicazione per assurdo.
Supponiamo che M non sia scritto come unione disgiunta di cicli. Vi sarà dunque un ciclo c di g e due indici i e $j \in [n]$ tali che *c(i)=j*. Tuttavia i e j hanno molteplicità diverse in *M*. Di conseguenza avremo che $gM \neq M$ contraddicendo le ipotesi. □

Vediamo ora un esempio del lemma.

Esempio 3.4. Sia g= (1,2,4)(3,5). I multinsiemi di cardinalità al massimo 5 fissati da g sono $\{3,5\}, \{1,2,4\}, \{3^2,5^2\}, \{1,2,3,4,5\}$.

Il Lemma resta valido nel caso in cui restringiamo il campo al gruppo ciclico C_n. Possiamo dare perciò una valutazione effettiva di $\#X^g$.

Definizione 3.6. Siano d e $k \in \mathbb{N}$. Se d divide k scriviamo $d|k$.

Corollario 3.1.2. *Se* $X = \left(\!\!\binom{[n]}{k}\!\!\right)$ *e* $g \in C_n$ *con o(g)=d. Allora:*

$$\#X^g = \begin{cases} \binom{n/d+k/d-1}{k/d} & \text{se } d|k \\ 0 & \text{altrimenti.} \end{cases} \tag{3.10}$$

Dimostrazione. Poichè $g \in C_n$ con *o(g)=* d la sua scomposizione in cicli disgiunti consiste in $\frac{n}{d}$ cicli di lunghezza d.
Studiamo i due casi differenti. Se d non divide k allora nessun multinsieme M di cardinalità k può essere scritto come unione disgiunta di cicli di g. Di conseguenza, per il Lemma 3.1.1 non vi sono punti fissi e questo giustifica il secondo caso del corollario.
Se invece $d|k$, i punti fissati da g sono i multinsiemi ottenuti scegliendo $\frac{k}{d}$ tra gli $\frac{n}{d}$ cicli di g, contati con ripetizione. Il problema si riconduce quindi al

contare in quanti modi posso scegliere $\frac{k}{d}$ posizioni in una lista con $\frac{n}{d} + \frac{k}{d} - 1$ spazi. Questo è esattamente il coefficiente binomiale ottenuto nel primo caso del teorema. $\square$

3.2 Polinomi Gaussiani

Andiamo ora a presentare il polinomio a coefficienti interi che consideriamo nella terna.

Definizione 3.7. Sia $n \in \mathbb{N}$ e $[n] = \{1, 2, \dots\}$. Si definisce *q-analogo di n* il polinomio

$$[n]_q = 1 + q + q^2 + \cdots + q^{n-1}. \tag{3.11}$$

Osservazione 6. Si può notare come ponendo q= 1 si ottiene $[n]_1 = n$.

Definizione 3.8. Definiamo il *polinomio Gaussiano* o il *coefficiente q-binomiale* come:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}, \tag{3.12}$$

per ogni $0 \leq k \leq n$ con $[n]_q! = [1]_q[2]_q \dots [n]_q$.

Poichè $\#\left(\left(\begin{smallmatrix} [n] \\ k \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} n \\ k \end{smallmatrix}\right)$ e deve rimanere valida la condizione (2.3), una scelta naturale per il nostro polinomio è:

$$f(q) = \begin{bmatrix} n\text{+}k\text{-}1 \\ k \end{bmatrix}_q. \tag{3.13}$$

Osservazione 7. Per il coefficiente q-binomiale vale la seguente formula ricorsiva, analoga alla formula di Stiefel per i coefficienti binomiali:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n\text{-}1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n\text{-}1 \\ k\text{-}1 \end{bmatrix}_q. \tag{3.14}$$

Questa formula ci permette di dimostrare che il polinomio Gaussiano sia effettivamente un polinomio a coefficienti interi.

Teorema 3.2.1. *Il polinomio gaussiano è un polinomio a coefficienti interi.*

Dimostrazione. Procediamo per induzione su n sfruttando la formula (3.14).
Sia n=1, allora $\begin{bmatrix} 1 \\ k \end{bmatrix}_q = 1$ per definizione.
Supponiamo sia verificata per *n-1*.
Verifichiamo che valga per n. Per la (3.14) sappiamo che $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n\text{-}1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n\text{-}1 \\ k\text{-}1 \end{bmatrix}_q$.
Inoltre, $\begin{bmatrix} n\text{-}1 \\ k \end{bmatrix}_q \in \mathbb{N}[q]$ per ipotesi induttiva e q^{n-k} è un monomio con coefficiente *1* che moltiplica $\begin{bmatrix} n\text{-}1 \\ k\text{-}1 \end{bmatrix}_q$ che appartiene a $\mathbb{N}[q]$ anch'esso per ipotesi induttiva. La tesi è quindi dimostrata. □

Il polinomio scelto, pertanto, soddisfa le ipotesi del CSP.

Teorema 3.2.2. *Il cyclic sieving phenomenon è verificato da:*

$$\left(\left(\binom{[n]}{k} \right), \langle (1, 2, \ldots, n) \rangle, \begin{bmatrix} n+k\text{-}1 \\ k \end{bmatrix}_q \right). \tag{3.15}$$

Abbiamo mostrato in (3.1.2) come calcolare $\#X^g$. Dobbiamo dunque valutare $f(\omega_{o(g)})$. Per fare ciò sono necessari i seguenti lemmi.

Lemma 3.2.3. *Sia* $\omega = \omega_d$*, allora:*

$$1 + \omega + \omega^2 + \cdots + \omega^{d-1} = 0. \tag{3.16}$$

Dimostrazione. Sappiamo che ω è una radice d-esima primitiva dell'unità, quindi per definizione $1 - \omega^d = 0$. Possiamo scomporre $(1 - \omega^d)$ nel sequente modo:
$(1 - \omega^d) = (1 - \omega)(1 + \omega + \omega^2 + \cdots + \omega^{d-1}) = 0$.
$(1 - \omega) \neq 0$ per definizione di radice d-esima primitiva. Di conseguenza, per la legge dell'annullamento del prodotto, $1 + \omega + \omega^2 + \cdots + \omega^{d-1} = 0$ □

Lemma 3.2.4. *Siano* $m, n \in \mathbb{N}$ *tali che* $m \equiv n$ *(mod d) e sia* $\omega = \omega_d$*, allora:*

$$\lim_{q \to \omega} \frac{[m]_q}{[n]_q} = \begin{cases} \frac{m}{n} & \textit{se } n \equiv 0 \textit{ (mod d)} \\ 1 & \textit{altrimenti.} \end{cases} \tag{3.17}$$

Dimostrazione. Sia $m \equiv n \equiv r \pmod{d}$ con $0 \leq r < d$.
Sappiamo dal Lemma 3.2.3 che $1+\omega+\omega^2+\cdots+\omega^{d-1} = 0$, e dalla Definizione 3.7 otteniamo che: $[m]_\omega = 1+\omega+\omega^2+\ldots\omega^{r-1} = [n]_\omega$. Abbiamo quindi due casi possibili.
Se $r \neq 0$, allora $[m]_\omega \neq 0$ e $[n]_\omega \neq 0$, di conseguenza $\frac{[m]_\omega}{[n]_\omega} = 1$ come nel secondo caso del teorema.
Se $r = 0$, allora $\exists\ l,k \in \mathbb{N}$ tali per cui posso scrivere $n = ld$ ed $m = kd$. Pertanto si ha che:

$$\frac{[m]_q}{[n]_q} = \frac{(1+q+q^2+\cdots+q^{d-1})(1+q^d+q^{2d}+\cdots+q^{(k-1)d})}{(1+q+q^2+\cdots+q^{d-1})(1+q^d+q^{2d}+\cdots+q^{(l-1)d})}. \tag{3.18}$$

Possiamo notare come il fattore $(1+q+q^2+\cdots+q^{d-1})$ si semplifica nell'espressione. Andiamo dunque a calcolare il limite ricordandoci che $\omega^d = 1$ per definizione.

$$\lim_{q\to\omega} \frac{[m]_q}{[n]_q} = \frac{k}{l} = \frac{m}{n}. \tag{3.19}$$

□

Prima di enunciare il lemma conclusivo ricordiamo il seguente teorema della Teoria dei Gruppi.

Teorema 3.2.5 (Teorema di Lagrange)**.** *Un sottogruppo di un gruppo finito ha ordine che divide l'ordine del gruppo.*

Corollario 3.2.6. *Se G è un gruppo finito, allora l'ordine di ogni suo elemento divide l'ordine di G.*

Per tale motivo se *o(g)=* d e $g \in C_n$, allora $d|n$.
Enunciamo ora l'ultimo lemma.

Corollario 3.2.7. *Sia* $\omega = \omega_d$ *e* $d|n$*, allora:*

$$\begin{bmatrix} n\text{+}k\text{-}1 \\ k \end{bmatrix}_\omega = \begin{cases} \binom{n/d+k/d-1}{k/d} & \textit{se } d|k \\ 0 & \textit{altrimenti.} \end{cases} \tag{3.20}$$

Dimostrazione. Dalla Definizione 3.8 sappiamo che:

$$\begin{bmatrix} n{+}k{-}1 \\ k \end{bmatrix}_\omega = \frac{[n{+}k{-}1]_\omega!}{[k]_\omega![n-1]_\omega!} = \frac{[n{-}1]_\omega![n]_\omega \dots [n+k-1]_\omega}{[k]_\omega![n-1]_q!} = \frac{[n]_\omega \dots [n+k-1]_\omega}{[k]_\omega[k-1]_\omega \dots [1]_\omega}. \tag{3.21}$$

Studiamo i due casi possibili.
Supponiamo che d non divida k. Poichè $d|n$, il primo fattore del numeratore della frazione è zero, come dimostra il Lemma 3.2.3. Per la stessa motivazione, ogni successivo d-esimo fattore risulta zero, mentre i fattori restanti sono non nulli. Lo stesso discorso è applicabile al denominatore: anch'esso è di periodo d ma con i primi d-1 fattori non nulli. Possiamo quindi concludere che il numero di zeri presenti nel numeratore è sempre maggiore del numero di zeri presenti nel denominatore. Di conseguenza è dimostrato il secondo caso del teorema.
Supponiamo ora che $d|k$. Riordinando l'equazione (3.21) otteniamo che:

$$\begin{bmatrix} n{+}k{-}1 \\ k \end{bmatrix}_\omega = \lim_{q\to\omega} \left(\frac{[n]_q}{[k]_q} \cdot \frac{[n+1]_q}{[1]_q} \cdot \frac{[n+2]_q}{[2]_q} \dots \frac{[n+k-1]_q}{[k-1]_q} \right). \tag{3.22}$$

Possiamo notare come ogni fattore del prodotto sia nella forma $\frac{[m]_q}{[n]_q}$ con $m \equiv n$ (mod d). Di conseguenza, applicando il Lemma 3.2.4, abbiamo che tutti i fattori valgono 1, tranne i casi in cui n è un multiplo di d. Poichè $d|k$, anche k è multiplo di d. L'equazione precedente può essere quindi riscritta nel seguente modo:

$$\begin{aligned} \begin{bmatrix} n{+}k{-}1 \\ k \end{bmatrix}_\omega &= \frac{n}{k} \cdot 1 \dots 1 \cdot \frac{n+d}{d} \cdot 1 \dots 1 \cdot \frac{n+2d}{2} \cdot 1 \dots \\ &\text{divido per d} \\ &= \frac{n/d}{k/d} \cdot \frac{n/d+1}{1} \cdot \frac{n/d+2}{2} \dots \\ &= \binom{n/d+k/d-1}{k/d}. \end{aligned} \tag{3.23}$$

□

Per concludere, confrontando la valutazione di in $\#X^g$ vista in 3.1.2 con la valutazione di $f(\omega_{o(g)})$ vista in 3.2.7, abbiamo dimostrato il Teorema 3.2.2 e, quindi, il cyclic sieving phenomenon per il multinsiemi.

Capitolo 4

CSP nella Teoria della Rappresentazione

Lo scopo di questo capitolo è quello di presentare il *cyclic sieving phenomenon* dal punto di vista della Teoria della Rappresentazione, mettendo in luce aspetti differenti e in alcuni casi più intuitivi rispetto al contesto dei multinsiemi. Enunceremo infine un paradigma che permette di verificare il CSP per una terna generica.

4.1 Nozioni sulla Teoria della Rappresentazione

Iniziamo introducendo alcune nozioni base sulla teoria della rappresentazione che sfrutteremo successivamente.

Definizione 4.1. Sia G un gruppo, chiamiamo *G-modulo* o *modulo per G* uno spazio vettoriale V su $\mathbb{C}$ sul quale G agisce attraverso trasformazioni lineari invertibili.

Stiamo dunque chiedendo che ogni elemento di G agisca in modo "compatibile" sullo spazio vettoriale.

Definizione 4.2. Sia G un gruppo, un G-modulo si chiama *modulo sinistro* se G agisce su V a sinistra. Viceversa un G-modulo si chiama *modulo destro* se G agisce su V a destra.

Diamo ora la definizione di rappresentazione di un gruppo.

Definizione 4.3. Sia $GL(V)$ il gruppo generale lineare delle trasformazioni linerari invertibili di V. Se V è un G-modulo, chiamiamo *rappresentazione di G* la seguente mappa:

$$\begin{aligned} \rho : G &\longrightarrow GL(V) \\ g &\longmapsto [g]. \end{aligned} \tag{4.1}$$

Con $[g]$ indichiamo una mappa lineare invertibile in $GL(V)$.

Si può dare la definizione di rappresentazione di un gruppo anche partendo da uno spazio vettoriale e sfruttando l'omomorfismo di gruppi.

Definizione 4.4. Sia V uno spazio vettoriale, allora la *rappresentazione di un gruppo G* è l'omomorfismo tra gruppi indicato da $\rho : G \longrightarrow GL(V)$.

Definizione 4.5. Sia G un gruppo che agisce su un insieme X, chiamiamo $\mathbb{C}X$ il *modulo di permutazione* corrispondente ad X.

Definizione 4.6. Sia V un G-modulo, si definisce *dimensione di V* la dimensione di V considerato come spazio vettoriale.

Definizione 4.7. Sia A una matrice quadrata, si definisce *traccia della matrice* la somma di tutti gli elementi che stanno sulla sua diagonale:

$$tr(A) = \sum_{i=1}^{n} a_{ii}. \tag{4.2}$$

Osservazione 8. La traccia è additiva in quanto: $tr(A+B) = tr(A)+tr(B)$. Vale inoltre, per il prodotto di scalare : $tr(c \cdot A) = c \cdot tr(A)$. Di conseguenza, l'operazione di calcolare la traccia di una matrice è una trasformazione lineare.

Osservazione 9. Nel nostro caso, $[g]$ è una mappa lineare invertibile ed ad essa sarà quindi associata una matrice quadrata invertibile. Possiamo dunque indicare con *tr[g]* la traccia della matrice associata a $[g]$.

Giunti a questo punto presentiamo il *carattere* di un G-modulo.

Definizione 4.8. Sia V un G-modulo, il *carattere* di G su V è la funzione così definita:

$$\begin{aligned} \chi : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \chi(g) = tr[g]. \end{aligned} \tag{4.3}$$

Osservazione 10. La definizione sopra è ben posta: infatti due matrici simili hanno la stessa traccia, quindi la traccia di una trasformazione lineare è indipendente dalla scelta della base.

Vediamo ora l'isomorfismo tra *G-moduli.*

Definizione 4.9. Due G-moduli V, W si dicono *G-isomorfi* o *G-equivalenti*, e si indicano con $V \cong W$, se e solo se esiste una biezione lineare $\phi : V \longrightarrow W$ tale che preservi l'azione del gruppo G:

$$\forall g \in G, \ \forall \ v \in V \quad \text{si verifica che} \quad \phi(gv) = g\phi(v). \tag{4.4}$$

4.2 CSP come cambiamento di base

Dopo questa introduzione abbiamo già abbastanza elementi per poter mostrare una semplice interpretazione del CSP.

Per prima cosa costruiamo un $\mathbb{C}$-spazio vettoriale a partire da un insieme X.

Definizione 4.10. Sia X un insieme, indichiamo con $V = \mathbb{C}X$ lo spazio vettoriale complesso ottenuto considerando gli elementi di X come una base e le loro combinazioni lineari a coefficienti complessi come elementi. Ovvero, se $X = \{s_1, s_2, \ldots, s_k\}$ allora:

$$\mathbb{C}X = \{c_1s_1 + c_2s_2 + \cdots + c_ksk : c_i \in \mathbb{C} \ \text{ per ogni } i\}. \tag{4.5}$$

Osservazione 11. Se G è un gruppo che agisce su X, allora G agisce anche su $\mathbb{C}X$.

Associamo ora ad ogni elemento g di G, con G gruppo che agisce su X, una mappa lineare invertibile che indichiamo con $[g]$.
Sia B una base di V, indichiamo con $[g]_B$ la matrice associata a $[g]$ rispetto alla base B.
Possiamo inoltre considerare l'insieme X stesso come base. A questo punto, la matrice associata $[g]_X$ non è altro che la matrice che permuta gli elementi di X secondo l'azione di g.

Osservazione 12. Indicheremo in grassetto gli elementi di X quando li consideriamo come vettori.

Vediamo ora un esempio.

Esempio 4.1. Sia $X = \{1, 2, 3\}$. Costruiamo $\mathbb{C}X$:

$$\mathbb{C}X = \{c_1\mathbf{1} + c_2\mathbf{2} + c_3\mathbf{3} \ : c_1, c_2, c_3 \in \mathbb{C}\}. \tag{4.6}$$

Sia G= $\langle(1, 2, 3)\rangle$ che agisce su X e quindi su $\mathbb{C}X$.
Consideriamo g=(1,2,3) elemento di G. La sua azione su X, visto come base, è:

$$(1, 2, 3)\mathbf{1} = \mathbf{2} \qquad (1, 2, 3)\mathbf{2} = \mathbf{3} \qquad (1, 2, 3)\mathbf{3} = \mathbf{1}. \tag{4.7}$$

La matrice che otteniamo è la seguente:

$$[(1, 2, 3)]_X = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}. \tag{4.8}$$

Come possiamo notare essa è esattamente una matrice di permutazione.

Abbiamo mostrato in (4.5) che $\mathbb{C}X$ può essere visto come un G-modulo. Di conseguenza, per la Definizione 4.8, si ha che:

$$\chi(g) = tr[g]_X = \#X^g. \tag{4.9}$$

Per mostrare il CSP è necessario un polinomio a coefficienti interi.
Sia *f(q)*=$\sum_{i=0}^{l} m_i q^i$ con $m_i \in \mathbb{N}$ per ogni i.
Per l'Osservazione 16, che dimostreremo nella sezione successiva, sappiamo che esiste una base B per $\mathbb{C}X$ tale che, per ogni $g \in C$, la matrice associata alla trasformazione lineare invertibile è rappresentata da una matrice diagonale così costituita:

$$[g]_B = diag(\underbrace{1, \ldots, 1}_{m_0}, \underbrace{\omega, \ldots, \omega}_{m_1}, \ldots, \underbrace{\omega^l, \ldots \omega^l}_{m_l}), \tag{4.10}$$

con $\omega = \omega_{o(g)}$. Di conseguenza calcolando il carattere di g si ottiene che:

$$\chi(g) = tr[g]_B = \sum_{i=0}^{l} m_i \omega^i = f(q). \tag{4.11}$$

Uguagliando i caratteri in (4.9) e in (4.11) abbiamo verificato il CSP per la terna:

$$\Big(X, G, f(q)\Big), \tag{4.12}$$

secondo le definizioni precedenti.
Abbiamo mostrato che il *cyclic sieving phenomenon* in questo caso è un cambiamento di base in un C-modulo.

4.3 Un paradigma per la Teoria della Rappresentazione

In questa sezione vengono raccolti alcuni risultati standard della Teoria della Rappresentazione, introducendo concetti quali la *riducibilità* e la *decomponibilità*. Enunceremo infine il paradigma che permette di verificare il CSP data una terna generica attraverso l'isomorfismo tra C-moduli.

Definizione 4.11. Sia V un G-modulo, diciamo che W è un *sottomodulo di* G se è un sottospazio di V invariante rispetto all'azione di G, ovvero: $g\mathbf{w} \in W$ per ogni $g \in G, \mathbf{w} \in W$.

Osservazione 13. Chiamiamo *moduli banali* il sottospazio zero, ovvero quello generato dallo 0: $(0) := \{0\}$, e V stesso.

Definizione 4.12. Un G-modulo V si dice *riducibile* se ha sottomoduli non banali; in caso contrario si dice *irriducibile*.

Definizione 4.13. Un G-modulo V si dice *decomponibile* se può essere scritto come somma diretta di n sottomoduli non nulli con $n \in \mathbb{N}$.

Osservazione 14. E' necessario soffermarsi su queste due definizioni per sottolineare un'importante differenza tra gli spazi vettoriali e i moduli. Quando si parla di spazi vettoriali, l'essere *riducibile* equivale all'essere *decomponibile*: uno spazio vettoriale è riducibile se può essere scritto come somma diretta di un numero finito di sottospazi. D'altro canto invece, quando si trattano i moduli, i due concetti sono ben distinti. Possono esistere infatti moduli riducibili non decomponibili: è sufficiente che essi abbiano un sottomodulo non banale che non ammetta un complementare.

Il seguente teorema, che racchiude tre risultati standard della Teoria della Rappresentazione, dimostra che se si ha un gruppo finito G e un suo modulo su $\mathbb{C}$, i concetti di riducibilità e decomponibilità effettivamente coincidono.

Teorema 4.3.1. *Sia G un gruppo finito e si considerino i G-moduli che sono spazi vettoriali su $\mathbb{C}$, allora si verificano le seguenti istanze:*

(a) Il numero dei G-moduli irriducibili e a due a due non isomorfi è finito ed uguale al numero delle classi coniugio di G.

(b) (Teorema di Maschke) Ogni G-modulo può essere scritto come somma diretta di G-moduli irriducibili.

(c) Due G-moduli sono equivalenti se e solo se hanno lo stesso carattere.

Di seguito riporteremo solo la dimostrazione del punto (b) data l'importanza del Teorema di Maschke nella Teoria della Rappresentazione. Per la dimostrazione delle altre due proposizioni si veda la Proposizione 1.10.1 e il Corollario 1.9.4 in [6].

Dimostrazione. (b) Si vuole dimostrare che V, G-modulo di G, con G gruppo finito può essere scritto come:

$$V = \sum_{i=1}^{n} \oplus W^{(i)}, \tag{4.13}$$

con $W^{(i)}$ G-modulo irriducibile $\forall i \in \{1, \ldots, n\}$.
Procediamo per induzione su $d = \dim V$.
Se $d = 1$, allora $V = W^{(1)}$, che è irriducibile per definizione; dunque V è irriducibile.
Supponiamo ora $d > 1$. Abbiamo due possibilità: o V è irriducibile e quindi la proprietà è dimostrata; oppure V è riducibile e quindi ammette un G-sottomodulo non banale che indicheremo con W. La dimostrazione ora procede con la costruzione del complementare di W.
Sia $\mathbf{B}= \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ una qualsiasi base di V e consideriamo il prodotto interno definito nel seguente modo: $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \delta_{ij}$ per ogni $\mathbf{v}_i, \mathbf{v}_j \in \mathbf{B}$. Questo prodotto può però non essere G-invariante; quindi andiamo a definire il seguente prodotto interno:

$$\langle \mathbf{v}, \mathbf{w} \rangle' = \sum_{g \in G} \langle g\mathbf{v}, g\mathbf{w} \rangle.$$

Verificare che esso sia effettivamente un prodotto interno è banale. Passiamo invece a dimostrare che sia invariante rispetto all'azione di G. Il nostro scopo è quindi dimostrare che

$$\langle h\mathbf{v}, h\mathbf{w} \rangle' = \langle \mathbf{v}, \mathbf{w} \rangle',$$

per ogni $h \in G$ e $\mathbf{v}$, $\mathbf{w} \in V$. Il procedimento è una semplice applicazione delle definizioni:

$$\begin{aligned} \langle h\mathbf{v}, h\mathbf{w} \rangle' &= \sum_{g \in G} \langle gh\mathbf{v}, gh\mathbf{w} \rangle \quad \text{per definizione di } \langle \cdot, \cdot \rangle', \\ &= \sum_{f \in G} \langle f\mathbf{v}, f\mathbf{w} \rangle \quad g \text{ varia in } G, \text{ anche } f = gh \text{ varia in } G, \\ &= \langle \mathbf{v}, \mathbf{w} \rangle' \quad \text{per definizione.} \end{aligned} \tag{4.14}$$

Sia ora $W^\perp = \{\mathbf{v} \in V \ \text{ t.c. } \ \langle \mathbf{v}, \mathbf{w} \rangle' = 0\}$. Il fatto che W è un sottomodulo di G, come anche che $W^\perp$ è un sottomodulo di G, è facilmente dimostrabile. Possiamo dunque scrivere V come:

$$V = W \oplus W^\perp.$$

A questo punto, poichè $\dim W < d$ e $\dim W^\perp < d$, possiamo applicare l'ipotesi induttiva e scrivere sia W che $W^\perp$ come somma di irriducibili. Essendo V la loro somma diretta, il teorema è dimostrato. □

Osservazione 15. Per quanto riguarda il punto (c), mentre l'implicazione diretta risulta abbastanza intuitiva, l'implicazione inversa è da considerarsi un risultato importante in quanto permette di caratterizzare completamente i G-moduli utilizzando esclusivamente la traccia.

Iniziamo dunque la costruzione delle rappresentazioni irriducibili di un generico *gruppo ciclico* C con $\#C = n$.
In primo luogo mostriamo come si presentano i moduli di dimensione 1 di un gruppo ciclico mettendoli in relazione con i moduli di dimensione 1 di un gruppo finito G. Questi, per il teorema precedente, sono irriducibili.
Sia g un generatore di C, g ha quindi ordine n. Volendo un C-modulo di dimensione 1, consideriamo $V = \mathbb{C}\{\mathbf{v}\}$ per un certo vettore $\mathbf{v}$.
Dalla definizione di modulo si ottiene: $g\mathbf{v} = c\mathbf{v}$ per un certo $c \in \mathbb{C}$.
Inoltre si verifica che:

$$\mathbf{v} = e\mathbf{v} = g^n\mathbf{v} = c^n\mathbf{v}.$$

Di conseguenza $c^n = 1$, e quindi c è una radice n-esima dell'unità.
Per ogni radice n-esima dell'unità ω possiamo creare la seguente mappa:

$$\begin{aligned} \rho : C &\longrightarrow GL(V) \\ g^j &\longmapsto [\omega^j], \end{aligned} \tag{4.15}$$

con $j \in \mathbb{N}$.
Tale mappa è una rappresentazione di gruppi, stiamo infatti mandando la radice ω in una sua potenza.

Abbiamo dunque trovato n G-moduli irriducibili distinti di C che indicheremo con $V^{(0)}, V^{(1)}, \ldots, V^{(n-1)}$. Tali moduli sono irriducibili perchè hanno tutti dimensione 1 e sono distinti per il punto *(c)* del Teorema 4.3.1. In aggiunta, poichè hanno tutti caratteri differenti e trattandosi di matrici di dimensione 1, la traccia della matrice è il numero stesso.
Inoltre, i gruppi ciclici sono abeliani e di conseguenza C ha un numero di classi coniugio pari alla sua cardinalità. Dunque la parte *(a)* del Teorema 4.3.1 ci assicura che non vi siano altre rappresentazioni irriducibili.

Sia ora un qualsiasi C-modulo V, esso può essere scritto per la parte *(b)* del Teorema 4.3.1 come somma diretta di G-moduli irrudicibili. Abbiamo quindi il seguente isomorfismo tra moduli:

$$V \cong \bigoplus_{i=0}^{n-1} a_i V^{(i)}, \tag{4.16}$$

dove con $a_i V^{(i)}$ indichiamo la somma diretta di a_i copie di $V^{(i)}$.

Osservazione 16. Ogni addendo della sommatoria è unidimensionale; pertanto vi sarà una base B che diagonalizza simultaneamente le matrici associate alle trasformazioni lineari $[g]$ per ogni $g \in C$.

Osservazione 17. E' possibile inoltre estendere la definizione dei $V^{(i)}$, e quindi della sommatoria diretta (4.16), a tutti gli interi sfruttando la congruenza modulo n:

$$V^{(i)} = V^{(j)} \quad \text{se} \quad i \equiv j \mod n.$$

Giunti a questo punto, prima di enunciare il paradigma che caratterizza il CSP, mostriamo come si possa associare ad un polinomio, un modulo specifico.

Definizione 4.14. Sia $f(q) = \sum_{i \geq 0} m_i q^i$ tale che $m_i \in \mathbb{N}^*$. Definiamo il suo *C-modulo corrispondente* nel seguente modo:

$$V_f = \bigoplus_{i \geq 0} m_i V^{(i)}. \tag{4.17}$$

Possiamo dunque enunciare il seguente teorema.

Teorema 4.3.2. *Il cyclic sieving phenomenon è verificato in (X,C, f(q) se e solo se si ha che* $\mathbb{C}X \cong V_f$ *come C-moduli.*

Dimostrazione. Per prima cosa notiamo che $\#X^g$ è il carattere di $\mathbb{C}X$. Gli elementi fissati da g in $\mathbb{C}X$ sono quelli che hanno 1 sulla diagonale nelle rispettive colonne della matrice associata.
Contare il numero di elementi fissi equivale perciò a contare il numero di *1* sulla diagonale, e quindi al carattere di $\mathbb{C}X$.
Dimostriamo, ora, che $f(\omega_{o(g)})$ è il carattere di V_f.
Il generatore g di C agisce su $V^{(i)}$ come moltiplicazione per ω^i. Il carattere di g è $\chi(g) = \sum_{i \geq 0} m_i \omega^i$ che è esattamente $f(\omega_{o(g)})$.
Consideriamo un elemento diverso dal generatore. Sia $h = g^j$; h agisce su $V^{(i)}$ come ω^{ij}. Il carattere di h è $\chi(g^i) = \sum_{i \geq 0} m_i \omega^{ij} = f(\omega^j)$. L'Osservazione 1 conclude.
La doppia implicazione è verificata dal punto *(*c) del Teorema 4.3.1. □

Questo teorema è fondamentale in quanto ci permette di capire a priori se nella terna che stiamo considerando si verifica il CSP.

4.4 CSP nei tensori simmetrici

In questa sezione introduciamo i tensori simmetrici e forniamo un'ulteriore prova al CSP nel caso dei multinsiemi.
Abbiamo visto che, per punto *(c)* del Teorema 4.3.1, due G-moduli isomorfi hanno la stessa traccia. Per ottenere dunque *f(ω)* come traccia, come visto in (4.11), possiamo considerare un qualsiasi modulo isomorfo a $\mathbb{C}X$.

Introduciamo ora gli strumenti necessari per la costruzione del nostro modulo, partendo innanzitutto dal prodotto tensoriale di spazi vettoriali.

Definizione 4.15. Siano V e W due spazi vettoriali sullo stesso campo $\mathbb{K}$; consideriamo lo spazio vettoriale libero $\mathcal{L}(V, W)$, cioè l'insieme delle combinazioni lineari formali finite di elemnti di $V \times W$ a coefficienti in $\mathbb{K}$ e sia poi B il sottospazio vettoriale generato da $\{(\alpha_1 v_1 + \alpha_2 v_2, w) - \alpha_1(v_1, w) - \alpha_2(v_2, w),\ (v, \beta_1 w_1 + \beta_2 w_2) - \beta_1(v, w_1) - \beta_2(v, w_2),\ \text{con } v, v_i \in V,\ w, w_i \in W,\ \alpha_i, \beta_i \in \mathbb{K}\}$; si definisce prodotto tensore di V e W

$$V \otimes W = \frac{\mathcal{L}(V, W)}{B}.$$

In questo spazio quoziente, la classe della coppia (v, w) si indica con $v \otimes w$.

Osservazione 18. Innanzitutto è immediato che la somma è data dalla somma delle componenti e il prodotto per uno scalare sia dato da:

$$a(v \otimes w) = (av) \otimes w = v \otimes (aw).$$

Inoltre, il quoziente che viene fatto nella precedente definizione equivale a rendere bilineare il simbolo $\otimes$. In particolare sono date $B = \{v_i | i \in I \subset \mathbb{N}\}$ base di V e $B' = \{w_j | j \in J \subset \mathbb{N}\}$ base di W,

$$v \otimes w = \Big(\sum_{i \in I} \alpha_i v_i\Big) \otimes \Big(\sum_{j \in J} \beta_j w_j\Big) = \Big(\sum_{i \in I, j \in J} \alpha_i \beta_i v_i \times w_j\Big),$$

e quindi

$$\{v_i \otimes w_j, v_i \in B,\ w_j \in B'\},$$

è una base di $V \otimes W$ per cui $\dim(V \otimes W) = \dim(V) \cdot \dim(W)$. Sebbene sarebbe stato più semplice e intuitivo definire il prodotto tensore a partire da basi assegnate ciò non sarebbe stato corretto perchè così esso sarebbe stato dipendente dalla scelta di queste ultime.

Definizione 4.16. Sia V spazio vettoriale, definiamo l'*n-esima potenza tensoriale* di V il tensore n-volte prodotto di V con se stesso:

$$V^{\otimes n} = \underbrace{V \otimes V \otimes \cdots \otimes V}_{n}.$$

Consideriamo lo spazio vettoriale V=$\mathbb{C}[n]$ con base B=$\{\mathbf{i} : 1 \leq i \leq n\}$.
Sia $V^{\otimes k}$ la k-esima potenza tensoriale di V.
Questo avrà come base:

$$\{\mathbf{i}_1 \otimes \ \mathbf{i}_2 \cdots \otimes \mathbf{i}_k : \mathbf{i}_j \in B \, \forall \ \ 1 \leq j \leq k\}.$$

Definiamo ora il tensore sul quale andremo effettivamente a lavorare.

Definizione 4.17. Sia $V = \mathbb{C}[n]$ e $V^{\otimes k}$ la sua k-esima potenza tensoriale. Definiamo $Sym_k(n)$ come il quoziente di $V^{\otimes k}$ rispetto al sottospazio generato da:

$$\mathbf{i}_1 \otimes \ \mathbf{i}_2 \cdots \otimes \mathbf{i}_k - \mathbf{i}_{g(1)} \otimes \ \mathbf{i}_{g(2)} \cdots \otimes \mathbf{i}_{g(k)},$$

per ogni $g \in \mathfrak{S}_n$ (3.1) e per ogni $\mathbf{i}_1 \otimes \ \mathbf{i}_2 \cdots \otimes \mathbf{i}_k$ tensore.

Osservazione 19. E' sufficente considerare le differenze tra i tensori prodotto della base, ed estendere per linearità alle differenze tra tutti i tensori.

Indichiamo dunque con $\mathbf{i}_1 \ \mathbf{i}_2 \dots \mathbf{i}_k$ la classe di equivalenza del tensore $\mathbf{i}_1 \otimes \ \mathbf{i}_2 \cdots \otimes \mathbf{i}_k$. Tali classi sono indicizzate dai multinsiemi di k elementi di [n] e formano una base per $Sym_k(n)$.
Sia $C_n = \langle (1, 2, \dots, n) \rangle$ il gruppo ciclico che agisce su V.
C_n induce un'azione su $Sym_k(n)$ nel seguente modo:

$$g(\mathbf{i}_1 \ \mathbf{i}_2 \dots \mathbf{i}_k) = g(\mathbf{i}_1)g(\ \mathbf{i}_2) \dots g(\mathbf{i}_k).$$

Osservazione 20. E' necessario sottolineare, per non confondersi, la differente azione di g in (4.17) e in (4.4). Nel primo caso infatti g agisce sugli indici degli elementi della base, permutandoli; nel secondo caso, invece, g agisce direttamente sugli elementi della base.

Osservazione 21. Possiamo notare come l'azione in (3.7) sia la stessa di (4.4): otteniamo così un isomorfismo di C_n-moduli tra $\mathbb{C}\left(\left(\begin{smallmatrix} [n] \\ k \end{smallmatrix}\right)\right)$ e $Sym_k(n)$.

Possiamo dunque dimostrare il CSP del Teorema 3.2.2 attraverso $Sym_k(n)$.

Sia $g \in C_n$; indichiamo con $[g]$ la trasformazione lineare associata a g in $\mathbb{C}[n]$ e con $[g]$' la trasformazione lineare associata a g in $Sym_k(n)$.
Indicheremo con χ il carattere di C_n quando agisce su $\mathbb{C}[n]$, e con χ' il carattere di C_n quando agisce su $Sym_k(n)$.

Vediamo ora quali relazioni intercorrono tra le loro basi.
Per prima cosa supponiamo che esista una base B=$\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ per $\mathbb{C}[n]$ che diagonalizzi $[g]$. Ovvero possiamo considerare:

$$[g]_B = diag(x_1, x_2, \dots, x_n).$$

Come abbiamo detto nella precedente costruzione, B genera una base per $Sym_k(n)$ nel seguente modo:

$$B' = \{\mathbf{b}_{i_1}\mathbf{b}_{i_2} \dots \ \mathbf{b}_{i_k} : 1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n\}.$$

Inoltre poichè B è una base per $\mathbb{C}[n]$, ogni suo elemento è un autovettore per $[g]$, e ugualmente ogni elemento di B' è un autovettore di $[g]$':

$$g(\mathbf{b}_{i_1}\mathbf{b}_{i_2} \dots \ \mathbf{b}_{i_k}) = g(\mathbf{b}_{i_1})g(\mathbf{b}_{i_2}) \dots g(\ \mathbf{b}_{i_k}) = x_{i_1}x_{i_2} \dots x_{i_k}\mathbf{b}_{i_1}\mathbf{b}_{i_2} \dots \ \mathbf{b}_{i_k}.$$

Ne consegue che

$$[g]'_{B'} = diag(x_{i_1}x_{i_2} \dots x_{i_k} : 1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n),$$

e quindi

$$\chi'(g) = \sum_{1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n} x_{i_1}x_{i_2} \dots x_{i_k}.$$

Questo polinomio è chiamato *polinomio simmetrico completamente omogeneo* e si indica con $h_k(x_1, x_2, \dots, x_n)$.

Osservazione 22. Tale polinomio si chiama *completamente omogeneo* poichè è la somma di tutti i monomi di grado k nelle variabili x_i. Inoltre $h_k(x_1, x_2, \dots, x_n)$ è un polinomio simmetrico in quanto è invariante per le permutazioni degli indici delle variabili.

Per proseguire con la nostra dimostrazione è necessario mettere in relazione $h_k(x_1, x_2, \dots, x_n)$ con i coefficienti q-binomiali.
Per fare ciò imponiamo che $x_i = q^{i-1}$ per ogni i.
Dimostriamo dunque il seguente lemma.

Lemma 4.4.1. *Sia $n \geq 1$ e $k \geq 0$; si verifica che:*

$$h_k(1, q, q^2, \dots, q^{n-1}) = \begin{bmatrix} n+k\text{-}1 \\ k \end{bmatrix}_q . \tag{4.18}$$

Dimostrazione. Procediamo con una doppia induzione su n e k.
Se $n = 1$ abbiamo che $h_k(1) = x_1^k|_{x_1=1} = 1$.
Se $k = 0$ entrambi i lati danno 1.
Consideriamo il caso in cui $n \geq 2$ e $k \geq 1$.
Ciò che vogliamo ora dimostrare è che il polinomio $h_k(1, q, q^2, \dots, q^{n-1})$ verifica la ricorsione (3.14) che caratterizza i polinomi Gaussiani.
Per prima cosa, separiamo la sommatoria di $h_k(1, q, q^2, \dots, q^{n-1})$ in termini che non contengono x_n e in termini che lo contengono. Nel primo caso si ha il polinomio simmetrico completamente omogeneo in una variabile in meno, ovvero $h_k(x_1, x_2, \dots, x_{n-1})$.
Nei termini che rimangono è sempre presente x_n e posso quindi raccoglierlo.
Ciò che rimane ha grado diminuito di 1, e quindi *k-1*. Pertanto, si verifica che:

$$h_k(x_1, x_2, \dots, x_n) = h_k(x_1, x_2, \dots, x_{n-1}) + x_n h_{k-1}(x_1, x_2, \dots, x_{n-1}).$$

Applico (4.4) e ottengo:

$$h_k(1, q, q^2, \dots, q^{n-1}) = h_k(1, q, q^2, \dots, q^{n-2}) + q^{n-1} h_{k-1}(1, q, q^2, \dots, q^{n-1}).$$

$h_k(1, q, q^2, \dots, q^{n-2})$ e $h_{k-1}(1, q, q^2, \dots, q^{n-2})$ verificano l'uguaglianza (4.18) per ipotesi induttiva. Di conseguenza, sostituendo n con *n+k-1* abbiamo verificato la proprieà (3.14). Il lemma è quindi dimostrato. □

A questo punto possiamo fornire la dimostrazione del CSP di 3.2.2.

Dimostrazione. Sia $\mathbb{C}[n]$ l'insieme che consideriamo e C_n il gruppo ciclico che agisce su di esso. Consideriamo l'elemento $h = (1, 2, \ldots, n) \in C_n$, dove [h] è la matrice associata alla trasformazione lineare da $\mathbb{C}[n]$ in se stesso. Tale matrice ha come polinomio caratteristico $x^n - 1$ con radici $1, \omega_n, \omega_n^2, \ldots \omega_n^{n-1}$, dove ω_n è una radice primitiva n-esima dell'unità.
Tutte queste radici sono distinte. Esiste quindi una base B di $\mathbb{C}[n]$ che diagonalizza la matrice associata $[h]$:

$$[h]_B = diag(1, \omega_n, \omega_n^2, \ldots \omega_n^{n-1}).$$

Mettiamo ora in relazione questo risultato con le *o(g)*-esime radici primitive dell'unità, con g elemento generico di C_n.
Poichè h è il generatore di C_n, ogni altro elemento di C_n sarà nella forma $g = (1, 2, \ldots, n)^i$ per un qualche i.
Di conseguenza, sfruttando la rappresentazione diagonale precedentemente dimostrata si ottiene:

$$[g]_B = diag(1^i, \omega_n^i, \omega_n^{2i}, \ldots \omega_n^{(n-1)i}) = diag(1, \omega, \omega^2, \ldots \omega^{n-1}),$$

dove $\omega = \omega_n^i$ è una radice primitiva $o(g)$-esima dell'unità. Seguendo il procedimento precedentemente esposto ed il Lemma 4.18 si ottiene che:

$$\chi'(g) = h_k(1, \omega, \omega^2, \ldots \omega^{n-1}) = \begin{bmatrix} n+k\text{-}1 \\ k \end{bmatrix}_w. \tag{4.19}$$

Dall'Osservazione 21 sappiamo che $Sym_k(n) \cong \mathbb{C}\left(\left(\binom{[n]}{k}\right)\right)$. Dal punto *(c)* del Teorema 4.3.1 questi hanno lo stesso carattere, di conseguenza dal risultato in (4.9) si ottiene che:

$$\chi'(g) = \#\left(\binom{[n]}{k}\right)^g.$$

Confrontando gli ultimi due risultati il CSP è dimostrato. □

Capitolo 5

CSP in un gruppo di riflessioni complesse

L'intento di questo capitolo è di presentare il *cyclic sieving phenomenon* dal punto di vista delle azioni libere e semi libere di gruppi ciclici, considerando come insieme di partenza un gruppo generato dalle riflessioni complesse. Questo ci permette di fornire un'ulteriore dimostrazione del Teorema 3.2.2 che racchiuda i risultati raggiunti fino ad ora. Per fare ciò, utilizzeremo i gruppi di Coxeter ed alcune loro proprietà peculiari.

5.1 L'azione libera e i gruppi di riflessioni complesse

L'intento della sezione è di presentare il CSP nel contesto dei gruppi generati dalle riflessioni complesse sfruttando l'azione libera e semi libera di gruppi.

Presentiamo come prima cosa l'azione libera e semi libera di gruppi.

Definizione 5.1. Sia $[N]$ definito in 3.1 e $g \in \mathfrak{S}_N$ con ordine $o(g) = n$. Diciamo che g agisce in modo *libero* su $[N]$, se tutti i cicli di g sono di lunghezza n.

Osservazione 23. Chiedere che tutti i cicli di g abbiano lunghezza n, ovvero il suo ordine, implica chiedere che $n|N$.

Esempio 5.1. Sia $N = 6$ e $g = (1,2)(3,4)(5,6)$; g agisce in modo libero su $[6]$.

Definizione 5.2. Sia $[N]$ definito in 3.1 e $g \in \mathfrak{S}_N$ con ordine $o(g) = n$. Diciamo che g agisce in modo *semi-libero* su $[N]$, se agisce in modo libero su $[N]$, oppure tutti i suoi cicli sono di lunghezza n tranne uno, il quale è un elemento singolo.

Osservazione 24. In questo caso chiedere che tutti i cicli di g siano di lunghezza n tranne uno, il quale deve essere un elemento singolo, implica chiedere che $n|N-1$.

Esempio 5.2. Sia $N = 7$ e $g = (1,2)(3,4)(5,6)(7)$; allora g agisce in modo semi libero su $[7]$.

Poniamo ora queste definizioni in relazione con i gruppi ciclici.

Definizione 5.3. Sia $[N]$ come definito in 3.1, C un gruppo ciclico e g il suo generatore. Diciamo che C agisce in modo *libero* o *semi-libero* su $[N]$ se g agisce rispettivamente in modo libero o semi-libero su $[N]$.

Indichiamo con:

$$\binom{[N]}{k} = \{S : S \text{ è un sottoinsieme di } [N] \text{ con } k \text{ elementi}\}.$$

Si può dimostrare, Teorema 1.1 di [2], il seguente risultato.

Teorema 5.1.1. *Sia C un gruppo ciclico che agisce in modo semi-libero su [N]. Allora le seguenti terne*

$$\left(\left(\binom{[N]}{k}\right), C, \begin{bmatrix} N+k-1 \\ k \end{bmatrix}_q\right), \tag{5.1}$$

$$\left(\binom{[N]}{k}, C, \begin{bmatrix} N \\ k \end{bmatrix}_q\right), \tag{5.2}$$

esibiscono il cyclic sieving phenomenon.

Il gruppo ciclico $C = \langle(1, 2, \ldots, N)\rangle$ agisce in modo libero, e in particolare semi libero, su $[N]$ per definizione. Otteniamo, dunque, un primo importante risultato. Il Teorema 3.2.2 può essere infatti visto come un caso particolare della terna (5.2) del teorema sopra enunciato.
Per avere tuttavia una visione più chiara del fenomeno è necessario analizzare alcuni aspetti.
In primo luogo, mostriamo in che modo la richiesta di un'azione semi libera su C sia opportuna e necessaria per la dimostrazione.
Per fare ciò dobbiamo introdurre i *gruppi di riflessioni complesse* che noi considereremo sempre nel caso finito.

Definizione 5.4. Sia $GL_N(\mathbb{C})$ il gruppo delle matrici invertibili $N \times N$ a valori in $\mathbb{C}$. Una *riflessione complessa* è un elemento di $GL_N(\mathbb{C})$ tale che fissi un unico iperpiano di $\mathbb{C}^N$ ed abbia ordine finito.

Definizione 5.5. Un *gruppo di riflessioni complesse* è un gruppo generato da riflessioni complesse.

Osservazione 25. Le riflessioni complesse generalizzano il concetto delle riflessioni reali che definiremo in 5.14. D'altro canto, le riflessioni reali possono essere considerate complesse attraverso un'estensione di campi. Dimostreremo inoltre nell'Esempio 5.3 come il gruppo simmetrico possa essere realizzato come un gruppo generato da riflessioni reali.

Definizione 5.6. Un gruppo generato da riflessioni complesse si dice *irriducibile* se non è isomorfo ad un prodotto diretto di altri gruppi di riflessioni complesse non banali.

Definizione 5.7. Sia W un gruppo generato da riflessioni complesse finito e sia $g \in W$. Diciamo che g è un elemento *regolare* se possiede un autovettore che non giace su alcun iperpiano riflettente di W.
L'autovalore relativo a tale autovettore è anch'esso chiamato *regolare*.

Mostriamo dunque come nel caso in cui W sia il gruppo simmetrico, ipotesi plausibile per l'Osservazione 25, la regolarità degli elementi sia in relazione con l'azione semi libera su $[N]$.

Proposizione 5.1.2. *Sia $W = \mathfrak{S}_N$. Allora $g \in W$ è regolare se e solo se g agisce in modo semi libero su [N].*

Dimostrazione. ($\Leftarrow$) Supponiamo che $o(g) = n$ e che g agisca semi liberamente su $[N]$. Dalla Definizione 5.2 di azione semi libera vi sono due casi possibili da considerare.
Supponiamo che $n|N$; g è il prodotto di più cicli di lunghezza n:

$$g = (1, 2, \dots, n)(n + 1, n + 2, \dots, 2n) \dots.$$

Consideriamo l'azione del primo ciclo $(1, 2, \dots, n)$ su $\mathbb{C}^n$. La matrice associata $[(1, 2, \dots, n)]$ è del tipo:

$$\begin{bmatrix} 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \cdots & 0 \end{bmatrix}, \tag{5.3}$$

di dimensione $n \times n$.
Il polinomio caratteristico è $(1 - t^n)$ e gli autovalori sono le radici n-esime dell'unità. Poichè l'insieme delle radici n-esime dell'unità e l'insieme delle loro inverse coincidono, possiamo considerare l'autovalore $\omega = \omega_n^{-1}$ e il suo relativo autovettore , $[\omega, \omega^2, \dots, \omega^n]^t$, in cui ogni componente è distinta.
Tale ragionamento può essere svolto per ogni n-ciclo di g.
Di conseguenza, l'autovettore $\mathbf{v}$ di $[g]$ sarà:

$$\mathbf{v} = [\omega, \omega^2, \dots, \omega^n, 2\omega, 2\omega^2, \dots, 2\omega^n, \dots].$$

Poichè ogni componente è distinta, $\mathbf{v}$ non giace in alcun iperpiano di equazione $x_i = x_j$.
Supponiamo invece che $n|N + 1$; g è il prodotto di più cicli di lunghezza *n-1* e di un unico elemento fissato.
Per quanto riguarda gli (*n-1*) cicli, si porta avanti il procedimento del caso precedente. Il singolo elemento, invece, rimane fisso. Perciò l'unico autovettore possibile è un autovettore che abbia zero nella coordinata della sua

posizione. L'autovettore $\mathbf{v}$ di $[g]$ quindi ha tutte le componenti distinte, uno zero nella componente relativa al singolo elemento, e non giace in alcun iperpiano di equazione $x_i = x_j$.
In entrambi i casi g risulta essere un elemento regolare.
($\Rightarrow$) Supponiamo che g non agisca in modo semi libero.
Consideriamo il caso in cui g è costituito da cicli di lunghezza differente, k ed l, tali che: $k, l \geq 2$ e $k \neq l$. Possiamo supporre che $k < l$. L'elemento g è così costituito:

$$g = (1, 2, \dots, k)(k + 1, k + 2, \dots, k + l) \dots .$$

Supponiamo che $\mathbf{v}$=$[a_1, a_2, \dots, a_N]^t$ sia un autovettore regolare di g. Per essere un autovettore di g deve verificarsi una delle seguenti ipotesi: o $[a_1, a_2, \dots, a_k]^t$ è un autovettore per $g' = (1, 2, \dots, k)$; oppure $[a_1, a_2, \dots, a_k]^t$ è il vettore nullo.
Quest'ultimo caso è da escludere poichè il vettore ha almeno due componenti, in quanto $k \geq 2$, ed ogni componente è nulla, contraddicendo la regolarità $\mathbf{v}$.
Consideriamo quindi il primo caso. Gli autovettori di g' sono nella forma $[\omega_k^i, \omega_k^{2i}, \dots, \omega_k^{ki}]^t$ con autovalore corrispondente ω_k^{-i} per $1 \leq i \leq k$.
Il ragionamento svolto finora è applicabile anche a $g'' = (k+1, k+2, \dots, k+l)$ e al relativo autovettore $[a_{k+1}, a_{k+2}, \dots, a_{k+l}]^t$.
Di conseguenza, l'autovalore ω di g deve essere una radice dell'unità di ordine che divide $MCD(k, l)$. Tuttavia, poichè $MDC(k, l) \leq k < l$, l'autovettore di g'' avrà almeno due componenti uguali, contraddicendo la regolarità di $\mathbf{v}$.
L'elemento g non può essere dunque costituito da cicli di lunghezza differente, maggiore di uno.
L'ultimo caso da escludere è quello in cui g possiede almeno due punti fissi. Ad ogni punto fisso corrisponde infatti uno zero nella relativa componente dell'autovettore $\mathbf{v}$; si hanno così più componenti uguali contraddicendo la regolarità di $\mathbf{v}$.
Abbiamo quindi dimostrato che l'elemento g possa essere scritto unicamente come un elemento che agisce semi liberamente. $\square$

In conclusione, abbiamo dimostrato che, nel caso in cui consideriamo il gruppo simmetrico $\mathfrak{S}_N$, chiedere che un elemento agisca semi liberamente equivale a chiedere che tale elemento sia regolare.

5.2 L'algebra gruppo e l'algebra delle coinvarianti

L' intento di questa sezione è di presentare due algebre particolari: il modulo di permutazione $\mathbb{C}[W]$ e l'algebra dei coinvarianti di W. Queste algebre ci permettono di enunciare e dimostrare un importante risultato per il cyclic sieving phenomenon che mette in relazione gli elementi presentati fino ad ora.
Iniziamo ricordando alcune proprietà importanti.

Lemma 5.2.1. *Sia V un G-modulo:*

1. *Se $W \subseteq V$ è un G-modulo allora anche lo spazio quoziente V/W è un G-modulo.*
2. *Se $H \leq G$ è un sottogruppo, allora V è anche un H-modulo.*

Definizione 5.8. Sia V un G-modulo. Chiamiamo *invarianti* di G in V:

$$V^G = \{\mathbf{v} \in V : g\mathbf{v} = \mathbf{v} \quad \text{per ogni} \quad g \in G\}.$$

Presentiamo le due algebre.
Sia G un gruppo, studiamo $\mathbb{C}[G]$.
Per prima cosa, un gruppo G agisce su se stesso attraverso la moltiplicazione a sinistra. $\mathbb{C}[G]$ è il modulo di permutazione corrispondente a G secondo la Definizione 4.5. $\mathbb{C}[G]$ è un'algebra, nello specifico un'*algebra gruppo*, in quanto si comporta sia come uno spazio vettoriale, per la Definizione 4.10, sia come un anello, poichè si possono moltiplicare tra loro combinazioni lineari di elementi, sfruttando il fatto che l'insieme sia un gruppo. Inoltre, quest'algebra contiente tutte le rappresentazioni irriducibili di G.

A tale proposito, $\mathbb{C}[G]$ può essere scritta come somma diretta dei sottomoduli irriducibili di G contati con molteplicità.
Il teorema seguente permette di mettere in relazione l'algebra gruppo con le dimensioni dei sottomoduli irriducibili di G.

Teorema 5.2.2. *Sia G un gruppo finito e siano $V^{(1)}, V^{(2)}, \dots, V^{(k)}$ i suoi sottomoduli irriducibili. Scriviamo $\mathbb{C}[G] = \oplus_i m_i V^{(i)}$. Allora, per ogni i, si verifica che:*

$$m_i = \dim V^{(i)},$$

ovvero ogni sottomodulo irriducibile è presente nella sommatoria un numero di volte pari al suo grado. Si ottiene inoltre che:

$$\sum_{i=1}^{k} (\dim V^{(i)})^2 = \#G.$$

Osservazione 26. La seconda parte del teorema è l'interpretazione dal punto di vista dimensionale del punto precedente. Gli elementi di G sono una base per $\mathbb{C}[G]$. Pertanto, $\dim \mathbb{C}[G] = \#G$. Applicando la prima parte del teorema si ottiene che:

$$\dim \mathbb{C}[G] = \sum_{i=1}^{k} m_i \dim V^{(i)} = \sum_{i=1}^{k} (\dim V^{(i)})^2 = \#G.$$

La seconda algebra che consideriamo è definita per qualunque sottogruppo $W \leq GL_N(\mathbb{C})$. Per la nostra tesi possiamo limitarci a considerare il caso in cui W sia $\mathfrak{S}_n$. Tuttavia i risultati successivi restano validi considerando un qualunque W della tipologia sopra definita.
Sia ora $S = \mathbb{C}[x_1, x_2, \dots, x_n]$ l'algebra dei polinomi a coefficienti complessi in N variabili, considerando $x_1, x_2, \dots, x_n$ come le coordinate di $\mathbb{C}^N$.
W agisce su S permutando tra loro le variabili.
Definiamo, dunque, l'algebra dei coinvarianti:

Definizione 5.9. Sia $W \leq GL_N(\mathbb{C})$ e sia $S = \mathbb{C}[x_1, x_2, \dots, x_n]$. Definiamo l'*algebra dei coinvarianti di W* il quoziente:

$$A = S/S_+^W, \tag{5.4}$$

dove con S_+^W si indica l'ideale generato dagli invarianti di W su S, ovvero l'ideale generato dai polinomi omogenei di grado positivo.

Osservazione 27. Possiamo notare come $S_+^W \subseteq S$ ed è per costruzione un W-sottomodulo. Per il punto (1) del Lemma 5.2.1, W agisce su A.

Consideriamo g un elemento regolare di W di ordine n . Sia C il gruppo ciclico generato da g : $C = \langle g \rangle$.
Sia sempre $\omega = \omega_n$.
Il passo successivo è mostrare come il prodotto di gruppi $W \times C$ agisce sulle due algebre.
Per quanto riguarda l'algebra gruppo, l'azione è definita nel modo seguente: $(w, c) \in W \times C$ manda $\left(\sum_\sigma a_\sigma \sigma\right)$ in $w\left(\sum_\sigma a_\sigma \sigma\right)c$, con $a_\sigma \in \mathbb{C}$ e $\sigma \in W$.

Osservazione 28. W agisce per motiplicazione a sinistra e C per moltiplicazione a destra su elementi di $\mathbb{C}[W]$ che sono combinazioni di elementi di W; l'azione è quindi definita dalla moltiplicazione interna al gruppo. Tali azioni commutano per la proprietà associativa nei gruppi.

L'azione sull' algebra dei coinvarianti è invece così definita: $(w, c) \in W \times C$ manda a in wac.
In questa azione, W permuta le variabili degli elementi di A, come visto in precedenza, e C agisce moltiplicando ogni variabile per la radice primitiva n-esima dell'unità:

$$g(x_i) = \omega x_i, \tag{5.5}$$

per ogni $i \in [N]$.
Il teorema seguente, dimostrato in [3], dimostra che le due algebre sono due moduli isomorfi nel contesto in cui ci siamo posti.

Teorema 5.2.3. *Sia $W = \mathfrak{S}_n$, sia A la sua algebra dei coinvarianti e sia $C \leq W$ il sottogruppo ciclico generato da un elemento regolare di W. Allora $\mathbb{C}[W]$ e A sono $W \times C$-moduli isomorfi.*

Il risultato più importante di questo Teorema è quello di permetterci di considerare l'algebra dei coinvarianti A, come un'algebra graduata.

Definizione 5.10. Un'algebra A è un'algebra graduata se esiste una famiglia di sottospazi vettoriali $\{A_i\}_{i\in\mathbb{N}}$ che decompongono A in una somma diretta:

$$A = \oplus_i A_i,$$

in modo tale che sia soddisfatta la seguente proprietà:

$$A_s A_k \subseteq A_{s+k},$$

per ogni $r, s \in \mathbb{N}$.

Nel nostro caso, A può essere scritta come sommatoria diretta degli elementi omogenei di grado d, A_d.

$$A = \oplus_{d\geq 0} A_d.$$

Inoltre, poichè A è un'algebra graduata su $\mathbb{C}$, essa possiede la seguente *Serie di Hilbert*

$$\text{Hilb(A;q)} = \sum_{d\geq 0} \dim_{\mathbb{C}} A_d q^d. \tag{5.6}$$

Giunti a questo punto, abbiamo tutti gli strumenti necessari per poter enunciare, dimostrare e comprendere il seguente importante teorema.

Teorema 5.2.4. *Sia* $W = \mathfrak{S}_n$ *, sia* A *la sua algebra dei coinvarianti e sia* $C \leq W$ *il sottogruppo ciclico generato da un elemento regolare di* W*. Si consideri un qualsiasi sottogruppo* $W' \leq W$ *e la rispettiva algebra dei coinvarianti* $A^{W'}$*. Allora il cyclic sieving phenomenon è verificato dalla seguente terna:*

$$\Big(W/W', C, Hilb(A^{W'}; q)\Big).$$

Dimostrazione. In primo luogo il Teorema 5.2.3 afferma che A e $\mathbb{C}[W]$ sono $W \times C$-moduli isomorfi attraverso un isomorfismo che indichiamo con $\phi : A \longrightarrow \mathbb{C}[W]$.
Poichè C è un sottogruppo di $W \times C$, per il punto (2) del Lemma 5.2.1, A e $\mathbb{C}[W]$ sono isomorfi anche come C-moduli.
Abbiamo precedentemente osservato che le azioni di W e C commutano. Di

conseguenza anche le azioni di W' e C commutano. $A^{W'}$ e $\mathbb{C}[W]^{W'}$ sono C-moduli e, restringendo ϕ, si ha ancora un isomorfismo di C-moduli tra loro. Procediamo ora con lo studio dell'azione di C.
Per osservare l'azione del generatore g su $A^{W'}$, sfruttiamo il fatto che A sia un'algebra graduata. Studiamo dunque l'azione di g sulle sue componenti di grado d.
Per definizione (5.5) $g(x_i) = \omega x_i$, con $\omega = \omega_n$, di conseguenza $g(x_i^d) = (g(x_i))^d = \omega^d x_i^d$. g moltiplica quindi ogni componente d-esima di $A^{W'}$ per ω^d.
Sia ora $V_{Hilb(A^{W'})} = \bigoplus_{d \geq o} \dim_{\mathbb{C}} A_d^{W'} V^{(d)}$ il C-modulo corrispondente alla funzione $Hilb(A^{W'})$ secondo la Definizione data in (4.17). Possiamo osservare come l'azione di g sul d-esimo addendo di $V_{Hilb(A^{W'})}$, definita da (4.15), sia anch'essa la moltiplicazione per ω^d. Ne consegue che $A^{W'} \cong V_{Hilb(A^{W'})}$ come C-moduli.
Per quanto riguarda $\mathbb{C}[W]^{W'}$, consideriamo l'insieme delle classi laterali destre $W \backslash W'$.
Un elemento generico $\sum_i c_i g_i \in \mathbb{C}[W]$ è invariante per W' se e solo se i suoi coefficienti sono constanti in ogni classe, in caso contrario infatti non potrebbe essere mandato in se stesso dagli elementi di W'.
Sia ora $C(W \backslash W')$ il C-modulo di permutazione di $W \backslash W'$. Questo ha per base le classi $W'w$; quando vado ad applicare $g \in C$, con C che agisce sulla destra, si verifica che $W'wg = W'(wg) = W'h$ con $h = wg \in W$, per definizione di gruppo. L'azione di C su $C(W \backslash W')$ non è altro che una permutazione di classi laterali destre. Tale azione coincide con l'azione di C su $\mathbb{C}[W]^{W'}$ in quanto g permuta esclusivamente i g_i tra gli elementi di W'. Di conseguenza, $\mathbb{C}[W]^{W'} \cong C(W \backslash W')$ come C-moduli.
Poichè ogni gruppo ciclico è abeliano, $C(W \backslash W') \cong C(W/W')$, dove W/W' è l'insieme delle classi laterali sinistre e C agisce sulla sinistra.
Abbiamo mostrato dunque la seguente catena di isomorfismi di C-moduli:

$$C(W/W') \cong C(W \backslash W') \cong \mathbb{C}[W]^{W'} \cong A^{W'} \cong V_{Hilb(A^{W'})}.$$

Questa soddisfa le ipotesi del Teorema 4.3.2, e ciò conclude la nostra dimostrazione. □

Osservazione 29. Da questa dimostrazione possiamo notare come il teorema sia piuttoso profondo ed in parte complesso. Essa, infatti, ha fatto uso di diverse teorie: la Teoria della Rappresentazione, la Teoria dei Gruppi e la Teoria dei Moduli.

In ultimo, per poter utilizzare questo teorema per fornire una dimostrazione differente del Teorema 3.2.2 è necessario sfruttare i gruppi di Coxeter.

5.3 I gruppi di Coxeter

In questa sezione presentiamo i gruppi di Coxeter e alcune delle loro principali proprietà.
Per prima cosa, occorre dare la definizione di gruppi di Coxeter.

Definizione 5.11. Un *gruppo di Coxeter finito*, W, è un gruppo finito con questa presentazione: sia S l'insieme dei generatori soggetto alle seguenti relazioni:
Siano $s, s' \in S$:

$$(ss')^{m(s,s')} = e,$$

con *m(s,s')* numeri interi positivi che soddisfano:

$$\begin{aligned} m(s,s') &= m(s,s'), \\ m(s,s') &= 1 \Leftrightarrow s = s'. \end{aligned} \tag{5.7}$$

Osservazione 30. Dalla definizione degli $m(s,s')$ possiamo notare due cose. In primo luogo, vale la proprietà simmetrica. In secondo luogo, gli elementi di S sono involuzioni, poichè $m(s,s) = 1$ di conseguenza $ss = e$ e quindi $s^2 = e$. Inoltre portando metà dei fattori nella parte destra dell'equazione in 5.11 si ottiene:

$$\underbrace{ss'ss'\dots}_{m(s,s')} = \underbrace{s'ss's\dots}_{m(s,s')}.$$

Osservazione 31. Un gruppo generico W può avere differenti presentazioni che si comportano secondo le relazioni precedentemente definite; normalmente l'insieme dei generatori a cui si fa riferimento è implicitamente assegnato. Tuttavia se si volesse esplicitare, si parlerà di *sistema di Coxeter* e si indicherà con *(W,S)*.

Uno dei gruppi di Coxeter più famosi e più utilizzati è il gruppo simmetrico che indichiamo con $\mathfrak{S}_n$.
Consideriamo come insieme di generatori l'insieme delle trasposizioni adiacenti: $S = \{s_1, s_2, \ldots, s_{n-1}\}$, dove $s_i = (i, i+1)$.
In questo caso le relazioni tra le coppie di elementi di S si traducono in questo modo:

$$\begin{aligned} &s_i^2 = 1, \\ &s_i s_j = s_j s_i \quad |i-j| \geq 2, \\ &s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \quad 1 \leq i \leq n-1 \text{ (relazione treccia)}. \end{aligned} \tag{5.8}$$

Osservazione 32. Il poter considerare il gruppo simmetrico come un particolare gruppo di Coxeter ci permetterà, attraverso alcune proprietà che mostriamo nella sezione successiva, di dimostrare il Teorema 3.2.2.

Diamo ora qualche definizione utile per lavorare con gruppi di Coxeter:

Definizione 5.12. Un gruppo di Coxeter W si dice *irriducibile* se non è isomorfo ad un prodotto diretto di altri gruppi di Coxeter non banali.

Definizione 5.13. Il *rango* di un gruppo di Coxeter, indicato con *rk W*, è la cardinalità di S. I suoi elementi sono chiamati *riflessioni semplici*.

Osservazione 33. Il gruppo di Coxeter può essere inoltre messo in relazione con il gruppo delle simmetrie di un politopo regolare, in base alla struttura del suo grafo. Quest'ultimo si costruisce nel seguente modo:
si considerano gli elementi di S come vertici e si collegano tra loro da un arco etichettato con *m(s,s')* se $s \neq s'$. Per convenzione, se *m(s,s')* $= 2$, ovvero s ed *s'* commutano, si omette l'arco, e se *m(s,s')* $= 3$, vi è l'arco senza etichetta. Il gruppo di Coxeter può essere realizzato come il gruppo delle simmetrie di

un politopo regolare se e solo se i vertici del suo grafo hanno grado uno o due.

Esiste inoltre, differentemente dall'osservazione precedente, un'interpretazione geometrica che vale per tutti i gruppi di Coxeter.

Definizione 5.14. Una *riflessione* su $\mathbb{R}^n$ è una trasformazione lineare r_H che fissa un iperpiano H punto per punto, e che manda ogni vettore perpendicolare ad H nel suo opposto rispetto ad H.

Definizione 5.15. Il *gruppo di riflessioni reali* è un gruppo generato da riflessioni reali.

I gruppi finiti generati dalle riflessioni reali coincidono con i gruppi di Coxeter finiti.
Nel seguente esempio mostriamo questo risultato considerando $\mathfrak{S}_n$.

Esempio 5.3. Mostriamo come realizzare $\mathfrak{S}_n$ come un gruppo di riflessioni reali.
Si considerino gli iperpiani riflettenti $H_{i,j}$ di equazione $x_i = x_j$.
Sia $r_{i,j}$ la riflessione corrispondente, $r_{i,j}(x_1, x_2, \ldots, x_n)$ è dunque il punto ottenuto scambiando la i-esima e la j-esima coordinata. Di conseguenza la riflessione $r_{i,j}$ corrisponde alla trasposizione $(i, j) \in \mathfrak{S}_n$.
Poichè $\mathfrak{S}_n$ è generato dal gruppo delle trasposizioni, abbiamo concluso la dimostrazione.

5.3.1 L'inversione e i sottogruppi parabolici

Andiamo ora a presentare la funzione *inversione* sui gruppi di Coxeter. Tale funzione ci permette di mettere in relazione il gruppo simmetrico, come gruppo di Coxeter, e i coefficienti q-binomiali.

Definizione 5.16. Sia W un gruppo di Coxeter ed S il suo insieme dei generatori; sia $w \in W$. Per definizione di gruppo di Coxeter esso può essere scritto come:

$$w = s_1 s_2 \dots s_k,$$

dove $s_i \in S$ è considerato come elemento generico e non come i-esimo generatore.

Osservazione 34. Tale scrittura non è unica poichè ogni elemento può essere scritto come prodotto di un numero diverso di fattori, basti solo pensare all'identità scritta come prodotto di una trasposizione per la sua inversa.

Definizione 5.17. Questa espressione viene detta *ridotta* se k è il minimo numero tra tutte le espressioni che generano w. Il valore k è chiamato *lunghezza* di w e si indica con $l(w) = k$.

Studiamo il caso in cui W è $\mathfrak{S}_n$.
Consideriamo ora w con la seguente notazione:

$$w = w_1 w_2 \dots w_n \qquad \text{con} \quad w_i = w(i) \quad i \in [n].$$

Definizione 5.18. Definiamo l'*insieme delle inversioni di* w nel modo segente:

$$\text{Inv}\, w = \{(i,j) : i < j \quad \text{e} \quad w_i > w_j\}.$$

Il *numero di inversione* di w è inv $w = \#\text{Inv}\, w$.

Esempio 5.4. $w = w_1 w_2 \dots w_n = 31524$, allora $\text{Inv}\, w = \{(1,2),(1,4),(3,4),(3,5)\}$ e di conseguenza inv $w = 4$.

Nell'esempio precedente, w scritto in forma ridotta, risulta essere $w = (2,3)(1,2)(4,5)(3,4) = s_2 s_1 s_4 s_3$, in questo caso s_i indica l'i-esimo generatore.
Si verifica quindi che *l(w)*= inv w.
Mostriamo come quest'ultima proprietà sia sempre valida.

Proposizione 5.3.1. *Sia* $\mathfrak{S}_n$ *e* $w \in \mathfrak{S}_n$. *Allora:*

$$l(w) = inv\, w.$$

Dimostrazione. In primo luogo mostriamo che inv $w \leq$ *l(w)*.
La verifica è semplice: per definizione ogni w si costruisce come prodotto di trasposizioni ed, ad ogni nuova moltiplicazione s_i, si hanno due casi possibili. Nel primo caso, $w(i) > w(i+1)$, ovvero gli elementi erano già invertiti ed applicando s_i ciò si annulla. Oppure $w(i) < w(i+1)$, e parallelamente all'aumento della lunghezza, aumenta anche il numero di inversioni di 1.
Di conseguenza si ha che il numero delle inversioni, inv w, è al massimo pari alla lunghezza *l(w)*.
Mostriamo ora che $l(w) \leq$ inv w.
Sia inv $w = k$. Abbiamo due possibilità: o w è l'identità, oppure $k \geq 1$ e quindi vi sono almeno due numeri consecutivi, al posto i e $i+1$, invertiti. Nel primo caso è immediatamente verificata l'ipotesi in quanto si considera $l(id)=0$. Nel secondo caso si procede nel seguente modo:
Consideriamo l'elemento ws_i; allora inv (ws_i) = (inv w) -1, per quanto precedentemente detto.
Procediamo per induzione su inv w.
Supponiamo $l(ws_i) \leq$ inv ws_i; di conseguenza abbiamo che $ws_i = s_{i_1}s_{i_2}\dots s_{i_h}$ con $h \leq k-1$. Componendo per s_i a destra ed a sinistra, si ottiene che $w = s_{i_1}s_{i_2}\dots s_{i_h}s_i$. w è quindi prodotto di $h+1$ generatori. Si verifica pertanto che $l(w) \leq h+1 \leq k-1+1$ ovvero $l(w) \leq$ inv w. □

Introduciamo dunque il concetto di sottogruppo parabolico e mostriamo come, restringendoci al caso in cui si considera $\mathfrak{S}_n$ come gruppo di Coxeter, vi siano le prime analogie con il CSP.

Definizione 5.19. Sia *(W,S)* un sistema di Coxeter e $J \subset S$. Chiamiamo *sottogruppo parabolico* W_J, il sottogruppo di W generato da J.

Siano wW_J una classe laterale destra. Ogni classe laterale possiede un unico rappresentante di lunghezza minima; sia W^J l'unione dei rappresentanti di lunghezza minima. Definiamo dunque il seguente polinomio:

$$W^J(q) = \sum_{w \in W^J} q^{l(w)}. \tag{5.9}$$

Osservazione 35. Questo polinomio è la *weight generating function* della statistica *inv*. Una *statistica* su un insieme finito X è una funzione $st : X \longrightarrow \mathbb{N}$. Ad ogni statistica è associata una *weight generating function*

$$f^{st}(X) = f^{st}(X; q) = \sum_{y \in X} q^{sty}.$$

La cosa interessante di questo polinomio è che in determinate condizioni esso si comporta esattamente come il coefficiente q-binomiale definito in 3.8.

Proposizione 5.3.2. *Sia* $W = \mathfrak{S}_n$ *e* $J = S \backslash \{s_k\}$*, allora:*

$$W^J(q) = \begin{bmatrix} n \\ k \end{bmatrix}_q, \tag{5.10}$$

per ogni $0 \leq k \leq n$ *in cui con* $k = 0$ *o* $k = n$ *si ha che* $J = S$.

Prima di fornire la dimostrazione analizziamo il contesto.
Sia $W = \mathfrak{S}_n$, ed $S = \{s_1, s_2, \ldots, s_{n-1}\}$ il suo insieme dei generatori. Si consideri l'insieme J come nell'enunciato della proposizione. L'insieme J non è altro che l'insieme S meno una trasposizione, nello specifico quella che manda k in $k + 1$.
Quando dunque moltiplichiamo a destra un generico $w \in \mathfrak{S}_n$ per un elemento di $(\mathfrak{S}_n)_J$ non facciamo altro che permutare tra loro $\{w_1, w_2, \ldots, w_k\}$ e $\{w_{k+1}, w_{k+2}, \ldots, w_n\}$, separatamente.
Perciò:

$$(\mathfrak{S}_n)_J \cong \mathfrak{S}_k \times \mathfrak{S}_{n-k},$$

dove $\mathfrak{S}_k$ è il gruppo delle permutazioni degli elementi dell'insieme $\{1, 2, \ldots, k\}$ e $\mathfrak{S}_{n-k}$ è il gruppo delle permutazioni degli elementi dell'insieme $\{k + 1, k + 2, \ldots, n\}$.
Si consideri ora $(\mathfrak{S}_n)^J$: per definizione esso è l'insieme dei rappresentanti di lunghezza minima delle classi.
Abbiamo inoltre dimostrato nella Proposizione 5.3.1 come la lunghezza di w sia uguale al suo numero di inversioni. Di conseguenza, gli elementi di

lunghezza minima di $\mathfrak{S}_n$ saranno quelli i cui elementi sono ordinati in senso crescente fino al k-esimo elemento e dal *k+1*-esimo in poi:

$$(\mathfrak{S}_n)^J = \{w \in \mathfrak{S}_n : w_1 < w_2 < \dots w_k \text{ e } w_{k+1} < w_{k+2} < \dots w_n\}.$$

Presentiamo dunque la dimostrazione della Proposizione 5.3.2.

Dimostrazione. Procediamo per induzione doppia su n e k.
Se k=0, allora $J = \mathfrak{S}_n$ e $(\mathfrak{S}_n)^J = \{w \in \mathfrak{S}_n : w_1 < w_2 < \dots w_k < w_{k+1} < w_{k+2} < \dots w_n\}$. $(\mathfrak{S}_n)^J$ possiede dunque un unico elemento che non ha inversioni; utilizzando la Definizione (5.9) otteniamo che $W^J(q) = 1 = \begin{bmatrix} n \\ 0 \end{bmatrix}_q$.
Se n=1, $\mathfrak{S}_n$ contiene esclusivamente l'elemento 1, che non ha quindi inversioni e di conseguenza $W^J(q) = 1 = \begin{bmatrix} 0 \\ k \end{bmatrix}_q$.
Consideriamo ora il caso in cui $n \geq 2$ e $k \geq 1$.
Vogliamo dimostrare che si verifica la proprietà (3.14) che caratterizza i coefficienti q-binomiali.
Sia $(\mathfrak{S}_n)^J$ definito come in 5.3.1. Questo lo possiamo vedere come unione di due differenti insiemi: uno che fissa n e uno in cui n non è fissato.
Nel primo caso, essendo n fissato, per definizione di $(\mathfrak{S}_n)^J$ l'unica posizione in cui w possa trovarsi è l'n-esima. Ne consegue che possiamo vederlo come l'insieme delle permutazioni di *n-1* elementi ordinati in senso crescente fino alla k-esima posizione e dalla *k+1*-esima in poi, ovvero $(\mathfrak{S}_{n-1})^J$.
Nel secondo caso, dovendo sempre essere un sottoinsieme di $(\mathfrak{S}_n)^J$, l'unica posizione in cui possa trovarsi n è la k-esima. Ne consegue che: in primo luogo, stiamo considerando permutazioni di *n-1* elementi in cui nello specifico si permutano rispettivamente i primi *k-1* elementi tra loro e i successivi *n-k* elementi, lavorando quindi con $J' = S \backslash \{s_{k-1}\}$.
In secondo luogo, ogni elemento dell'insieme possiede esattamente *n-k* inversioni che coinvolgono n, in quanto n è maggiore degli *n-k* elementi successivi. Sfruttando sempre 5.3.1, possiamo raccogliere q^{n-k} nel polinomio.

Riconducendoci all'espressione polinomiale si ottiene che:

$$\begin{aligned}\mathfrak{S}_n^J(q) &= \sum_{w\in\mathfrak{S}_{n-1}^J} q^{l(w)} + q^{n-k}\sum_{w\in\mathfrak{S}_{n-1}^{J'}} q^{l(w)},\\ &= \begin{bmatrix} n\text{-}1 \\ k \end{bmatrix}_q + q^{n-k}\begin{bmatrix} n\text{-}1 \\ k\text{-}1 \end{bmatrix}_q.\end{aligned} \tag{5.11}$$

Abbiamo dimostrato la proprietà (3.14) e quindi il teorema. □

In conclusione, se consideriamo il gruppo simmetrico $\mathfrak{S}_n$ come gruppo di Coxeter abbiamo dimostrato un'altra possibile definizione per il coefficente q-binomiale. Il polinomio naturalmente associato può essere infatti visto come la funzione generatrice $W^J(q)$.

5.4 Conclusioni

Abbiamo ora tutti gli strumenti necessari per dimostrare il CSP nel caso dei multinsiemi sfruttando il Teorema 5.2.4.
Questo teorema può infatti essere applicato ai gruppi di Coxeter appena presentati, sfruttando il fatto che $W^J(q) = Hilb(A^{W_J}; q)$.
Pertanto possiamo enunciare il seguente corollario.

Corollario 5.4.1. *Sia (W, S) un sistema di Coxeter finito e sia $J \subseteq S$. Sia $C \leq W$ il gruppo ciclico generato da un elemento regolare g di W. Allora la terna*

$$\Big(W/W_J, C, W^J(q)\Big),$$

soddisfa il cyclic sieving phenomenon.

Abbiamo visto nelle sezioni precedenti che il caso in cui $W = \mathfrak{S}_N$ e $J = S\backslash\{s_k\}$, soddisfa le ipotesi del corollario.
Applichiamo il corollario e facciamo le seguenti considerazioni. In primis, abbiamo dimostrato nella Proposizione 5.1.2 che per un elemento g l'essere regolare equivale all'agire in modo semi libero.
L'azione di C su $\mathfrak{S}_N/(\mathfrak{S}_N)_J$ equivale all'azione di C su $\left(\!\binom{[n]}{k}\!\right)$.

In ultimo, abbiamo dimostratato nella Proposizione 5.3.2 che $W^J(q)$ è una funzione generatrice e si comporta esattamente come il coefficente q-binomiale. In conclusione, attraverso queste considerazioni, abbiamo dimostrato il CSP presentato nel Teorema 3.2.2 partendo da un gruppo generato dalle riflessioni complesse e facendo uso delle azioni semi libere di gruppi. L'obbiettivo del nostro capitolo è quindi raggiunto.

Bibliografia

[1] Bruce E. Sagan. The cyclic sieving phenomenon: a survey. Pre print : arXiv:1008.0790.

[2] Reiner, V., Stanton, D., and White, D. The cyclic sieving phenomenon. J. Combin. Theory Ser. A 108, 1 (2004), 17–50.

[3] Springer, T. A. Regular elements of finite reflection groups. Invent. Math. 25 (1974), 159–198.

[4] Bjo ̈rner A., and Brenti, F. Combinatorics of Coxeter groups, vol. 231 of Graduate Texts in Mathematics. Springer, New York, 2005.

[5] Westbury, B. Invariant theory and the cyclic sieving phenomenon. Preprint arXiv:0912.1512.

[6] Sagan, B. E. The symmetric group: Representations, combinatorial algo- rithms, and symmetric functions, second ed., vol. 203 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2001.

Ringraziamenti

Siamo giunti infine a quello che è l'ultimo capitolo di questa tesi ma il primo capitolo ad essere stato scritto nella mia testa. Le persone che hanno contribuito a questo risultato sono molteplici, motivo per cui questi ringraziamenti non saranno brevi. In primo luogo desidero ringraziare il Professor Fabrizio Caselli che ha permesso a questa studentessa un po' particolare di crescere e le è stato vicino sia professionalmente che umanamente. Il secondo ringraziamento va alla mia famiglia. So che qualunque traduzione in parole di quello che provi e quanto vi sia grata, risulterà riduttivo, tuttavia faccio un tentativo. Ringrazio quindi mia madre, colei che mi ha gestisto emotivamente e fisicamente in questi anni, istante per istante; mio padre, fonte di serenità e pragmaticità e le mie fantastiche sorelle, Agata ed Erminia, che mi hanno sostenuto, badato, fatto da mangiare e gestito nei momenti di disagio tra video, balletti trash e coccole. Ringrazio i miei zii, per il supporto costante e gli impegni di famiglia spostati in base ai miei impegni universitari e le mie cuginette per gli audio di incoraggiamento e i pomeriggi passati insieme scaricando la tensione. Ringrazio infine la più importante, la mia nonna, che mi ha sostenuto con cibo carezze e preghiere, e che ha reso la sua casa un rifugio sicuro in cui poter studiare prima di ogni esame. (Nonna, ormai ti sei laureata un po' anche te!) Ringrazio dunque due persone che sono state fondamentali nella mia crescita, come persona, come studente e come matematica. In primis, il mio (ex-)professore di pianoforte Walter Orsigner che mi ha insegnato a credere in me stessa e ad apprezzare e ricercare la bellezza, soprattutto quando la strada è complicata e faticosa, come nella matematica. Il secondo ringraziamento va alla Dott.ssa Romanelli, senza la quale avrei interrotto il mio percorso di studi molto tempo fa. Le sono grata per tutto quello che ha fatto in questi anni, per la sua presenza costante, i consigli, i racconti dei suoi magnifici viaggi e la gestione della mia persona, mi ha realmente cambiato un po' la vita. Passiamo dunque agli amici, ovvero quei pochi individui che mi siano rimasti dopo tre anni di intenso studio, servizio, lavoro, mal di testa e pacchi all'ultimo. Ringrazio Francesca, con la quale condivido ormai da tanti anni gioie e fallimenti della vita, in particolare quella universitaria. Ci tengo a ringraziarla soprattuto per la pazienza che ha avuto ogni volta che tornava nel continente ed io puntualmente avevo un esame, per le cene sulla scrivania e i saluti con i minuti contati. Ringrazio Cristian, compagno di biblioteca, di letture, di panchine e di sogni. Ringrazio Lorenzo, ottimo ascoltatore delle mie lamentele e sfortune e dispensatore di consigli sinceri. Ringrazio Giacomo, presenza costante nella mia vita, che più di tutti ha dovuto gestire le mie ansie, i miei silenzi, e i miei sbalzi d'umore. Ogni esame dato è stato dato un po' insieme, ma del resto è la mia la scienza pura, dove andremo a finire. Un ringraziamento speciale va alle Little Princesses Elena e Matilde (e la MYSS) che tra vinello, chiacchiere, pessimi outfit, concerti, ricerche spasmodiche di oggetti di cancelleria e sclerate hanno accompagnato questi ultimi anni. Estendo il ringraziamento ai Colori Pastello rimanenti: Luca, che nonostante la mia natura da ammazzabalotte e la mia scelta universitaria, continua a propormi serate cariche; Alessandro, che mi permette (e apprezza) di spiegargli i versi salienti di ogni canzone; Andrea, che mi regala grandi risate e grandi momenti d'affetto e infine Mattia, che tra tutti gestisce la mia disorganizzazione cronica, i miei spostamenti e attacchi di sonno e con il quale posso finalmente ascoltare buona musica. Grazie, siete per una seconda famiglia. A proposito di famiglia, non posso non ringraziare gli scout, persone ed esperienze che mi hanno accompagnato, impegnato e distratto in questi anni di studio. Ringrazio Francesco che ha vissuto quest'ultimo anno e questa laurea un po' con me e ha spesso fatto il grosso del lavoro. Ringrazio infine i più importanti, i miei bambini: Marta, Cristina, Benedetta, Daria, Chiara, Chiara, Tommaso, Massimiliano, Mattia, Vassili, Jack, Giec e Matteo. Vi ringrazio per aver vissuto con me questo anno, esame per esame, per avermi messo in difficoltà, per avermi fatto crescere, per aver accettato la mia testa tra le nuvole, il mio ripetere teoremi e l'essere sempre incasinata per l'università; per i sassi negli zaini, le camminate sotto la pioggia e i confronti sinceri; per aver vissuto con me questa laurea e, cosa più importante, avermi fatto usare una marea di tempo: grazie! Tornando a noi, ringrazio Sofia, che anche dall'Inghilterra mi sostiene con videochiamate skype infinite, merende rigorosamente suddivise, e che mi insegna sempre ad essere un po' più intraprendente, anche nel mio nuovo percorso di studi. Ringrazio Caterina, che mi è sempre stata accanto, anche nei momenti più bui, con la quale condivido libri, passioni, caffè, intense sessioni di studio e di chiacchiere. Un grande abbraccio va ai mitici I Più simpi, per gli audio prima degli esami, le cene, le partite a taboo, le vancanze ancora da organizzare e questa lenta ma costante crescita insieme. Ringrazio Andrea e Francesco per avermi accompagnato e rasserenato da qualche anno a questa parte: grazie per le cene etniche (che comunque il più buono è il greco), per l'affrontare le sessioni insieme ai nostri Mac e per Taylor. Ringrazio Michele che accetta ancora di vedermi una volta ogni mille mesi per colpa dello studio e mi ricorda sempre che non sono l'unica persona con dei disagi. Ringrazio infine i miei fondamentali compagni matematici. Davide, fornitore ufficiale di appunti e analista insostituibile, con il quale ho vissuto letteralmente ogni momento di questo percorso,tesi inclusa, dalle pause ai cibi smezzati del Metà, dalle corse ai viaggi in treno sul senso della vita, il tutto coronato da un "Giudi ridi un po'!". Laura con cui ho condiviso ansie, evidenziatori, occhiaie, lamentele e gossip. Fabio, compagno di sfortune e giornate storte, sempre in grado di farmi vedere il lato positivo. Federico e Eleonora che mi hanno accolto e supportato, tra consigli di aule studio (che poi non sono mai realmente andata al Paleotti), discorsi filosofici ed esami impossibili. Davide (il blastatore) che mi ha allietato nelle sessioni di studio più intense e mi ricorda sempre che prima della matematica viene la satira politica. Infine Titta che ha gestito le mie chiamate disperate per appunti, esami non verbalizzati e disagi Bolognesi. Ci tengo in ultimo a ringraziare le mie nuove compagne di collegio Sofia, Sara, Elisabetta e Rebecca, perchè in questo unico mese sono riuscite a farmi sentire a casa e mi hanno sostenuto in tutti modi nella stesura finale della tesi. Un grazie finale a tutti quelli che mi sono scordata, ma la mia sbadataggine mi precede: grazie di essere sul mio cammino, davvero!