Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

INTRODUZIONE ALLA TEORIA DEI Q-ANALOGHI IN COMBINATORIA

Tesi di Laurea in Matematica

Relatore:
Chiar.ma Prof.ssa
Marilena Barnabei

Presentata da:
Gregorio Galeotti

Anno Accademico 2021-2022

Mathematics is the art
of giving the same name
to different things.

Henri Poincaré

Introduzione

Lo scopo di questo lavoro è quello di fornire un'introduzione alla teoria dei q-analoghi e alle sue applicazioni nello studio di problemi legati a successioni numeriche. Vedremo in particolare come sia possibile, generalizzando con successioni polinomiali il conteggio di alcune classi di oggetti, ricavare su questi ultimi informazioni e proprietà aggiuntive.

Nel primo capitolo, dopo una breve introduzione sul concetto di funzione generatrice, di fondamentale importanza nello studio delle successioni numeriche, sono definiti i primi q-analoghi di oggetti combinatori. In particolare vengono introdotti i q-analoghi dei fattoriali, i coefficienti gaussiani e i coefficienti multinomiali. Vedremo come i q-fattoriali sono in modo naturale la funzione generatrice per le permutazioni contate secondo il numero di inversioni e come i coefficienti gaussiani permettano di contare i sottospazi vettoriali di uno spazio vettoriale finito.

Il capitolo 2 è dedicato allo studio delle partizioni di interi e ai loro diagrammi di Young. Dopo averne ricavato la funzione generatrice mostreremo come da essa è possibile ricavare numerose proprietà. Studieremo inoltre un'interessante connessione fra le partizioni con determinate restrizioni e i coefficienti gaussiani definiti nel capitolo 1.

Nel terzo ed ultimo capitolo sono presentati i risultati principali legati ai cammini di Dyck e ai numeri di Catalan. È inoltre proposta una generalizzazione dei numeri di Catalan attraverso i polinomi di Narayana: mostreremo come questi polinomi permettono di contare i cammini di Dyck secondo il numero di picchi e siano quindi un possibile q-analogo dei numeri di Catalan.

Indice

Capitolo 1

Funzioni Generatrici e Coefficienti Gaussiani

1.1 Funzioni Generatrici

Supponiamo di avere un problema la cui risposta è una successione di numeri $a_0, a_1, a_2 \ldots$; il nostro obiettivo è quello di ottenere più informazioni possibili di questa successione. Chiaramente una formula esplicita per calcolare a_n sarebbe il risultato più auspicabile, e ci permetterebbe di affermare con certezza di aver risposto al problema. Purtroppo però non è sempre possibile aspettarsi che un'espressione esplicita per a_n sia di facile formulazione, né tantomeno siamo sicuri che tale espressione esista.
Consideriamo ad esempio la successione $2, 3, 5, 7, 11, 13, 17, 19, \ldots$, ovvero la successione il cui termine a_n è l'n-esimo numero primo. In questo caso, aspettarsi di riuscire a dare un'espressione esplicita per a_n non è, a meno di scoperte eccezionali, molto ragionevole.
In molti casi, anche se definire esplicitamente a_n risulta particolarmente complicato, è invece più semplice definire una serie formale i cui coefficienti sono gli elementi $a_0, a_1, a_2 \ldots$ della successione cercata.

Definizione 1.1.1. *Data una successione* $\{a_n\}_{n\in\mathbb{N}}$*, si dice funzione genera-*

trice di $\{a_n\}$ la serie formale S tale che

$$S = \sum_{n=0}^{\infty} a_n x^n$$

Osservazione. Nonostante vengano chiamate *funzioni generatrici*, è bene ricordare che esse sono definite come serie formali e per questo è possibile manipolarle come oggetti puramente algebrici, spesso non considerando le loro proprietà analitiche in quanto funzione e in particolare senza considerare se la funzione associata alla serie sia in generale ben definita.

Esempio 1. La serie $S = \sum_{n=0}^{\infty} n!x^n = 1 + x + 2x^2 + 6x^3 + \cdots + n!x^n + \cdots$ ha perfettamente senso nel contesto delle serie formali nonostante non converga per alcun valore di x tranne nel caso $x = 0$. Allo stesso modo ha senso considerare la sua derivata formale $S' = \sum_{n=1}^{\infty} n!nx^{n-1} = \sum_{n=0}^{\infty} (n+1)!(n+1)x^n$.

Allo scopo di semplificare in futuro la notazione, introduciamo il seguente simbolo:

Definizione 1.1.2. *Data una serie formale S, indichiamo con $[x^n]S$ il coefficiente di x^n in S.*

Esempio 2. $[x^n]e^x = [x^n] \sum_{n=0}^{\infty} \frac{1}{n!} x^n = \frac{1}{n!}$.

Una volta individuata la funzione generatrice S di una successione, essa **potrebbe** portare alla soluzione esatta del problema. Indipendentemente dal fatto che questo sia possibile o meno, ecco alcune cose che la funzione generatrice potrebbe aiutare a fare:

- **Trovare una formula di ricorrenza:** in molti casi, il processo di ricerca della funzione generatrice ha proprio inizio da una regola di ricorrenza. Ciò nonostante, è spesso possibile scoprire dalla funzione generatrice S nuove formule di ricorrenza per $\{a_n\}$.

- **Trovare una formula asintotica:** quando il problema consiste nella ricerca di una successione particolarmente complicata è utile cercare, invece della formula esatta per a_n, una soluzione approssimata. Tornando all'esempio sulla successione dei numeri primi, non conosciamo una formula esatta per a_n ma è un fatto dimostrato (dal Teorema dei Numeri Primi) che, per n sufficientemente grande, $\pi(n) \sim \frac{n}{log(n)}$, dove $\pi(n) = |\{x < n : x \text{ è } primo\}|$.

- **Dimostrare alcune proprietà della successione,** quali ad esempio alcune importanti identità legate alla successione studiata. Siccome l'associazione *successione-funzione generatrice* è biunivoca, mostrare l'uguaglianza di due funzioni generatrici equivale a dimostrare che le due successioni associate coincidono. Inoltre, le funzioni generatrici offrono talvolta un metodo piuttosto veloce per studiare proprietà statistiche e probabilistiche della successione.

- **Altro?** Se c'è qualcos'altro di interesse riguardo la nostra successione, la funzione generatrice è un buon punto di partenza. Potremmo ad esempio voler cercare alcune proprietà di congruenza in modulo dei coefficienti. Potremmo notare, una volta determinata la serie S, una somiglianza con una funzione generatrice già nota e questo potrebbe portare a dedurre che la soluzione del problema in questione è strettamente legata alla soluzione di un problema già studiato.

È bene osservare che si può parlare di funzione generatrice anche nel caso in cui si stia trattando, invece che di una successione di numeri, di una k-pla di numeri $\{b_0, b_1, \ldots, b_{k-1}\}$ siccome quest'ultima può essere identificata con la successione definita da

$$a_n = \begin{cases} b_n & \text{se } n \leq k-1 \\ 0 & \text{se } n > k-1 \end{cases}.$$

La funzione generatrice associata sarà quindi la serie formale $S = \sum_{n \geq 0} a_n x^n$ che può essere vista anche come il polinomio $b_0 + b_1 x + \cdots + b_{k-1} x^{k-1}$.

Nel corso del lavoro ci troveremo spesso a considerare la funzione generatrice in quanto non avremo a disposizione un modo per calcolare i valori espliciti di una successione; vediamo ora un primo esempio semplice di funzione generatrice derivante da una proprietà di ricorsione.

1.1.1 Un esempio di ricorsione

Problema. *Supponiamo di dover trovare la successione* $a_0, a_1, a_2 \dots$ *definita per ricorrenza come*

$$a_0 = 0, \qquad a_{n+1} = 2a_n + 1 \quad \forall n \in \mathbb{N}.$$

Calcolando i primi termini della successione $(0, 1, 3, 7, 15, 31...)$ potrebbe saltare subito all'occhio che sono esattamente 1 in meno delle potenze di 2. Potremmo supporre quindi che $a_n = 2^n - 1\ \forall n \geq 0$ e dimostrarlo velocemente per induzione.
Decidiamo però di dimenticarci per un attimo di tutto questo e di affrontare il problema attraverso lo studio della funzione generatrice. Questa potrebbe apparire come un'inutile complicazione (e per un problema di questo tipo indubbiamente lo è) ma già dalla prossima sezione vedremo dei problemi in cui questo approccio risulterà fondamentale.
Il nostro obiettivo è quindi quello di determinare la serie $A(x) = \sum_{n \geq 0} a_n x^n$. Per fare questo, moltiplichiamo entrambi i membri della ricorrenza di partenza per x^n e sommiamo sui valori di n per cui tale ricorrenza è valida, ovvero per $n \geq 0$. Ricordando che $a_0 = 0$, al primo membro otteniamo

$$\begin{aligned}\sum_{n \geq 0} a_{n+1} x^n &= a_1 + a_2 x + a_3 x^2 + \dots \\ &= \frac{(a_0 + a_1 x + a_2 x^2 + \dots) - a_0}{x} = \frac{A(x)}{x}.\end{aligned}$$

Ripetendo gli stessi passaggi al secondo membro, si ottiene

$$\begin{aligned}\sum_{n \geq 0} (2a_n + 1) x^n &= 2A(x) + \sum_{n \geq 0} x^n \\ &= 2A(x) + \frac{1}{1-x}.\end{aligned}$$

Avendo usato per la serie geometrica la relazione $\sum_{n\geq 0} x^n = \frac{1}{1-x}$. Uguagliando le due espressioni trovate abbiamo quindi

$$\frac{A(x)}{x} = 2A(x) + \frac{1}{1-x},$$

che possiamo risolvere come equazione di primo grado nella variabile $A(x)$ e ottenere quindi $A(x)$ nella forma

$$A(x) = \sum_{n\geq 0} a_n x^n = \frac{x}{(1-x)(1-2x)}.$$

Questa è quindi la funzione generatrice del problema, i cui coefficienti $a_0, a_1, a_2, \ldots$ sono gli elementi della successione cercata. A questo punto potremmo comunque voler determinare una formula esplicita per il coefficiente a_n. Per fare questo, non ci resta che sviluppare la serie $A(x)$:

$$\begin{aligned}\frac{x}{(1-x)(1-2x)} &= x\left(\frac{2}{1-2x} - \frac{1}{1-x}\right) \\ &= (2x + 2^2x^2 + 2^3x^3 + \ldots) - (x + x^2 + x^3 + \ldots) \\ &= (2-1)x + (2^2-1)x^2 + (2^3-1)x^3 + \ldots \\ &= \sum_{n\geq 0}(2^n - 1)x^n.\end{aligned}$$

1.2 q-analoghi: prime definizioni

La teoria dei *q-analoghi* ha come scopo quello di generalizzare, attraverso l'utilizzo di un parametro q, un concetto o un oggetto matematico già esistente. Si parlerà quindi di q-analogo di un numero, di una successione, di un teorema ecc.. La natura generica di questa teoria le permette di trovare applicazioni in diversi ambiti della matematica; nel corso di questo lavoro ci limiteremo ad analizzare alcuni q-analoghi polinomiali in combinatoria ma notabili sono anche gli sviluppi di teorie analoghe in campo algebrico e nell'analisi, dove si parla ad esempio di q-analogo del concetto di derivata.
È uno dei rari casi in matematica in cui la definizione non cattura appieno il concetto, ma possiamo prenderla come un punto di partenza.

Definizione 1.2.1. *Il q-analogo di una proposizione o di un'espressione P è una proposizione o un'espressione P_q, dipendente dal parametro q, tale che*

$$\lim_{q\to 1} P_q = P.$$

Ad esempio, dato un numero naturale n, si può dire che n^q sia un q-analogo di n poiché, sostituendo per $q = 1$ in questa espressione si ottiene n. Allo stesso modo, $2q + (n-2)q^2$ è un q-analogo di n. Un altro esempio di q-analogo di n (sul quale ritorneremo in dettaglio) potrebbe essere

$$\frac{1-q^n}{1-q}$$

dato che, calcolando il limite con il teorema di de l'Hôpital, si ha

$$\lim_{q\to 1} \frac{1-q^n}{1-q} \overset{H}{=} \lim_{q\to 1} \frac{-nq^{n-1}}{-1} = n$$

A questo punto dovrebbe apparire evidente che vi sono infiniti modi di definire il q-analogo di un intero n e resta quindi da dare una definizione che sia utile e coerente con la teoria che si vuole sviluppare. Non esiste una definizione standard di q-analogo *buono* o *utile* ma, per ciò che concerne gli argomenti trattati in questo lavoro, possiamo tentare di dare un'idea di questo concetto; cercheremo, nel corso di questo lavoro, q-analoghi P_q che soddisfino le seguenti proprietà:

- P_q può essere espresso come somma o prodotto (al più infinito) di funzioni razionali in q.

- P_q ha proprietà analoghe a P.

- P_q ci permette studiare più nel dettaglio e di ottenere informazioni più approfondite su ciò che è descritto da P.

Queste ultime due richieste corrispondono in un certo senso a chiedere che P_q sia a tutti gli effetti una generalizzazione di P.

1.2.1 q-numeri

La teoria dei q-analoghi comincia dalla definizione di q-analogo di un intero positivo n. L'uguaglianza

$$\lim_{q\to 1}\frac{1-q^n}{1-q}=n$$

mostrata precedentemente ci suggerisce una possibile definizione.

Definizione 1.2.2. *Il q-analogo di un intero n, detto anche $q-numero$, si indica con $[n]_q$ ed è definito come*

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

Di per sé la scelta di questa definizione potrebbe sembrare piuttosto arbitraria ma vedremo presto che questa espressione appare in modo naturale in numerosi contesti e che permette di costruire su questa base il resto della teoria che andremo a studiare.
Inoltre possiamo subito verificare che questa generalizzazione preserva in un certo senso una delle proprietà fondamentali dei numeri naturali: la primalità. Per arrivare a dimostrare questo fatto richiamiamo alcuni risultati sui polinomi ciclotomici, dei quali ricordiamo la definizione.

Definizione 1.2.3. *Dato $n\in\mathbb{N}$, si indica con $\Phi_n(x)$ l'n-esimo polinomio ciclotomico definito come*

$$\Phi_n(x)=\prod_{\substack{k\leqslant n\\(k,n)=1}}(x-e^{2i\pi\frac{k}{n}}).$$

Ovvero $\Phi_n(x)$ è il polinomio monico che ha come radici tutte e sole le radici primitive n-esime dell'unità.

Lemma 1.2.4. *$\forall n\in\mathbb{N}$,*

$$x^n-1=\prod_{d|n}\Phi_d(x)$$

Dimostrazione.

$$\begin{aligned}
x^n - 1 &= \prod_{1 \leqslant k \leqslant n} \left(x - e^{2i\pi \frac{k}{n}} \right) \\
&= \prod_{d|n} \prod_{\substack{1 \leqslant k \leqslant n \\ (k,n)=d}} \left(x - e^{2i\pi \frac{k}{n}} \right) \\
&= \prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x).
\end{aligned}$$

□

Lemma 1.2.5. *$\forall n \in \mathbb{N}$, $\Phi_n(x) \in \mathbb{Z}[x]$ e $\Phi_n(x)$ è irriducibile in $\mathbb{Z}[x]$.*

La dimostrazione di quest'ultimo fatto e uno studio più dettagliato delle proprietà di questi polinomi sono disponibili in [13].
Siamo quindi pronti ad enunciare e dimostrare il seguente teorema che lega la primalità di n all'irriducibilità di $[n]_q$.

Teorema 1.2.6. *$\forall n \in \mathbb{N}$, n è primo se e solo se $[n]_q$ è irriducibile in $\mathbb{Z}[q]$.*

Dimostrazione. Sia n primo. Allora, $\forall k \in \{1, 2, \dots, n\}$, $(k, n) = 1$. Quindi, per il lemma 1.2.4,

$$q^n - 1 = \Phi_1(q)\Phi_n(q).$$

Da cui segue che

$$\Phi_n(q) = \frac{q^n - 1}{\Phi_1(q)} = \frac{q^n - 1}{q - 1} = [n]_q.$$

Per il lemma 1.2.5, $\Phi_n(q)$ è irriducibile in $\mathbb{Z}[x]$ da cui l'irriducibilità di $[n]_q$.
Mostriamo ora che se $n \in \mathbb{N}$ è composto, allora $[n]_q$ è riducibile.
Per il lemma 1.2.4,

$$q^n - 1 = \prod_{d|n} \Phi_d(q) = (q - 1) \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(q).$$

Quindi, dividendo ambo i membri per $q - 1$ si ottiene:

$$[n]_q = \frac{q^n - 1}{q - 1} = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(q).$$

Poiché n non è primo, n ha almeno un fattore proprio a e quindi $[n]_q$ è divisibile per $\Phi_a(q)$ e per $\Phi_{\frac{n}{a}}(q)$. $\square$

Avendo definito $[n]_q$ in questo modo, è possibile definire in modo naturale il q-analogo del fattoriale nel modo seguente:

Definizione 1.2.7.

$$[n]_q! = \prod_{k=1}^{n}[k]_q = 1 \cdot (1+q) \cdot (1+q+q^2) \cdots (1+q+q^2 \cdots + q^{n-1})$$

Osservazione. Dal fatto che $\lim_{q \to 1}[n]_q = n$ risulta immediatamente che

$$\lim_{q \to 1}[n]_q! = n!.$$

In ambito combinatorio, l'importanza di $n!$ è strettamente legata al conteggio delle permutazioni di n elementi. Vediamo ora in che modo $[n]_q!$ generalizza questa proprietà e permette di ottenere informazioni aggiuntive sulle permutazioni di $\{1, 2, \ldots, n\}$.

1.2.2 Inversioni

Una prima applicazione diretta dei $q-$fattoriali si può trovare nel conteggio delle permutazioni secondo il numero di *inversioni*.

Definizione 1.2.8. *Sia $p = p_1p_2 \cdots p_n$ una permutazione. Diciamo che la coppia (p_i, p_j) è un'inversione di p se $i < j$ ma $p_i > p_j$. Denotiamo il numero di inversioni di una permutazione p con $i(p)$.*

Esempio 3. Data la permutazione $p = 213645$, si ha $i(p) = 3$. Nello specifico, le 3 inversioni sono: $(2, 1)$, $(6, 4)$ e $(6, 5)$.

Come prima osservazione, risulta evidente che $0 \leq i(p) \leq \binom{n}{2}$ per ogni permutazione di n elementi e che i due valori estremi si ottengono rispettivamente con $p_1 = 12 \cdots n$ e $p_2 = n(n-1) \cdots 1$.
Andiamo ora ad analizzare la funzione generatrice associata alle permutazioni di n elementi con k inversioni. Denotato $b(n, k)$ il numero di permutazioni di n elementi con k inversioni, vale il seguente risultato.

Teorema 1.2.9. *Per ogni intero $n \geq 2$, si ha*

$$I_n(q) = \sum_{k=0}^{\binom{n}{2}} b(n,k)q^k = (1+q)(1+q+q^2)\cdots(1+q+q^2+\cdots+q^{n-1}) = [n]_q!$$

Dimostrazione. Come osservato precedentemente, $\forall n \in \mathbb{N}$ esiste una sola permutazione, $12\cdots n$, che abbia zero inversioni; ovvero $b(n,0) = 1$. In particolare, $b(1,0) = 1 = I_1(q)$. La formula data è quindi valida per $n = 1$, procediamo ora per induzione. Consideriamo una permutazione di $n-1$ nella quale inseriamo l'elemento n scegliendo arbitrariamente la posizione di inserimento j. Poiché n è maggiore di ogni elemento in $\{1, 2, \cdots, n-1\}$, l'inserimento di n nella $j-$esima posizione dà origine a $n-j$ nuove inversioni, *non* modifica le inversioni già presenti nella permutazione e non dipende da quante inversioni siano presenti nella permutazione di partenza. La funzione generatrice del numero di inversioni aggiunte è quindi $1+q+q^2+\cdots+q^{n-1} = [n]_q$ e le inversioni aggiunte sono indipendenti da quelle già presenti; vale quindi la seguente relazione tra $I_{n-1}(q)$ e $I_n(q)$

$$I_n(q) = (1+q+q^2+\cdots+q^{n-1})I_{n-1}(q) = [n]_q I_{n-1}(q),$$

da cui per induzione segue la tesi. $\square$

Esempio 4. Per n=3, vale

$$I_3(q) = (1+q+q^2)(1+q) = 1+2q^2+2q^3+q^4.$$

I coefficienti del polinomio corrispondono alle permutazioni di S_3 ordinate in base al loro numero di inversioni: 123, 132, 213, 312, 231, 321.

$[n]_q!$ generalizza quindi $n!$ in quanto conta ancora gli elementi di S_n ma tenendo conto del numero di inversioni di ogni permutazione. Nella figura 1.1 sono mostrati i primi valori di $b(n,k)$. Mostriamo ora un risultato di tipo ricorsivo per questi numeri.

Lemma 1.2.10. *Sia $n \geq k$. Allora vale*

$$b(n+1,k) = b(n+1,k-1) + b(n,k) \tag{1.1}$$

Dimostrazione. Sia $p = p_1 p_2 \cdots p_{n+1}$ una permutazione di $(n+1)$ elementi con k inversioni, $k \leq n$.
Se $p_{n+1} = n+1$, possiamo rimuovere l'entrata $n+1$ alla permutazione p senza alterare il numero di inversioni, e ottenere così una permutazione di n elementi con ancora k inversioni, contata quindi da $b(n,k)$.
Se invece $p_i = n+1$ per un qualche intero $i \leq n$, possiamo scambiare l'entrata $n+1$ con quella successiva. Questa operazione dà come risultato una permutazione di $n+1$ elementi con $k-1$ inversioni in cui l'entrata $n+1$ non è nella prima posizione. Tuttavia, tutte le permutazioni di $n+1$ elementi con $k-1$ inversioni hanno questa proprietà poiché mettere $n+1$ come prima entrata genererebbe almeno $n \geq k > k-1$ inversioni. Queste ultime sono quindi contate dal termine $b(n+1,k-1)$.
Questo completa la dimostrazione e mostra inoltre la necessarietà della condizione $n \geq k$. □

n \ k	0	1	2	3	4	5	6	7	8	9	10
1	1										
2	1	1									
3	1	2	2	1							
4	1	3	5	6	5	3	1				
5	1	4	9	15	20	22	20	15	9	4	1

Figura 1.1: I valori di $b(n,k)$ per $n \leq 5$

Osservazione. Questo risultato non è vero nel caso generale. Ad esempio, se $k > \binom{n}{2}/2$ allora $b(n+1,k) < b(n+1,k-1)$ e la relazione (1.1) è falsa poiché $b(n,k) > 0$. Dalla figura 1.1 si può vedere come questa formula ricorsiva non valga per $n = 4$ e $k = 7$.

Trovare una formula esplicita per i $b(n,k)$ è significativamente più difficile, anche restringendosi al caso $n \geq k$, e va oltre gli scopi di questo lavoro. Una trattazione più completa dell'argomento richiede l'utilizzo dei concetti di *partizione* e *scomposizione* di interi, ed è presente in [10].

1.2.3 Coefficienti Gaussiani

Conseguentemente a quanto appena visto per il fattoriale, è possibile definire il q-analogo del coefficiente binomiale.

Definizione 1.2.11. *Dati due interi non negativi n, k con $k \leq n$, si definisce coefficiente gaussiano o q-coefficiente binomiale e si indica con $\binom{n}{k}_q$ la quantità*

$$\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q![k]_q!} = \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q)(1-q^2)\cdots(1-q^k)} = \prod_{i=1}^{k} \frac{1-q^{n-i+1}}{1-q^i}$$

Per $k=0$ il prodotto è vuoto e si pone per convenzione $\binom{n}{k}_q = 1$. Per $k > n$, $\binom{n}{k}_q = 0$.

Esempio 5. Per $n = 4$, $k = 2$, si ha

$$\binom{4}{2}_q = \frac{(1-q^4)(1-q^3)}{(1-q)(1-q^2)} = (1+q^2)(1+q+q^2) = 1+q+2q^2+q^3+q^4.$$

Come è auspicabile nella teoria dei q-analoghi, la generalizzazione dei coefficienti binomiali ai coefficienti gaussiani preserva buona parte delle loro proprietà, in molti casi con $[n]_q$ giocante il ruolo di n nelle formule del caso base. Andiamo ora a mostrarne le principali:

- I coefficienti gaussiani sono simmetrici rispetto a n: $\binom{n}{k}_q = \binom{n}{n-k}_q$

  In particolare, $\binom{n}{0}_q = \binom{n}{n}_q = 1$

$$\binom{n}{1}_q = \binom{n}{n-1}_q = \frac{1-q^n}{1-q} = 1+q+\cdots+q^{n-1} = [n]_q$$

- I coefficienti gaussiani sono q-analoghi leciti dei coefficienti binomiali, ovvero:
$$\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$$

Dimostrazione.

$$\lim_{q\to 1}\binom{n}{k}_q = \lim_{q\to 1}\frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q^k)(1-q^{k-1})\cdots(1-q)} = \lim_{q\to 1}\prod_{i=0}^{k-1}\frac{1-q^{n-i}}{1-q^{k-i}} \overset{H}{=}$$
$$\overset{H}{=} \lim_{q\to 1}\prod_{i=0}^{k-1}\frac{(n-i)q^{n-i-1}}{(k-i)q^{k-i-1}} = \prod_{i=0}^{k-1}\frac{n-i}{k-i} = \binom{n}{k}$$

dove $\overset{H}{=}$ indica l'applicazione del teorema di de l'Hôspital. □

- Per $k < n$ vale un analogo della formula ricorsiva di Pascal, in due formulazioni equivalenti:

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q$$
$$\binom{n}{k}_q = q^k\binom{n-1}{k}_q + \binom{n-1}{k-1}_q$$

Dimostrazione. Osserviamo che la seconda uguaglianza segue in modo diretto dalla prima applicando la sostituzione $k \to n-k$, ricordando che $\binom{n}{k}_q = \binom{n}{n-k}_q$. Ci concentriamo quindi sul dimostrare la prima. Dalla definizione di coefficiente gaussiano seguono le seguenti relazioni:

$$\binom{m}{r}_q = \frac{1-q^m}{1-q^{m-r}}\binom{m-1}{r}_q \qquad (1)$$

$$\frac{1-q^r}{1-q^{m-r}}\binom{m-1}{r}_q = \binom{m-1}{r-1}_q \qquad (2)$$

Inoltre, abbiamo

$$\frac{1-q^m}{1-q^{m-r}} = \frac{1-q^r+q^r-q^m}{1-q^{m-r}} = q^r + \frac{1-q^r}{1-q^{m-r}}$$

Sostituendo quest'ultimo fatto in (1) otteniamo

$$\binom{m}{r}_q = q^r \binom{m-1}{r}_q + \frac{1-q^r}{1-q^{m-r}} \binom{m-1}{r}_q$$

Sostituendo ora (2) all'ultimo termine, otteniamo $\binom{m-1}{r-1}_q$ e quindi la tesi. $\square$

Osservazione. La ricorrenza appena dimostrata permette, per ogni n fissato, di calcolare i valori di $\binom{n}{k}_q$ partendo dai valori iniziali

$$\binom{n}{n} = \binom{n}{0} = 1.$$

e ricordando che $\binom{n}{n}_q = 1$, $\forall n \in \mathbb{N}$.
La formula mostra anche qualcosa di più profondo sulla natura di questi oggetti: i coefficienti gaussiani, che fino ad ora sono stati definiti come funzioni razionali in q, sono in realtà **polinomi** nella variabile q.

Vedremo nel corso di questo lavoro diverse applicazioni dei coefficienti in ambito combinatorio. Ne diamo ora un'interpretazione di tipo geometrico che spicca per rilevanza: è un risultato noto che i coefficienti binomiali $\binom{n}{k}$ contano i sottoinsiemi di cardinalità k di un insieme con n elementi, mostreremo come i coefficienti gaussiani generalizzano questa proprietà agli spazi vettoriali.

1.2.4 Sottospazi Vettoriali su Campi Finiti

Analizziamo ora un'interessante connessione tra i coefficienti gaussiani e un classico problema di algebra lineare. Questa applicazione è così importante nello studio di questi oggetti che talvolta essa è proprio il punto di partenza per la definizione di $\binom{n}{k}_q$. Il nostro obiettivo è quello di mostrare che il polinomio $\binom{n}{k}_q$ offre un modo diretto per contare i sottospazi di dimensione k di un determinato $\mathbb{K}$-spazio vettoriale V di dimensione n, sostituendo alla variabile q la cardinalità del campo $\mathbb{K}$.

Chiaramente, perché il problema abbia senso, ci restringeremo al caso in cui $\mathbb{K}$ sia un campo finito (ovvero $\mathbb{K} = \mathbb{F}_{p^n}$) e V abbia dimensione finita su $\mathbb{K}$, altrimenti tali sottospazi sono infiniti a meno dei casi banali. L'idea chiave del risultato che andiamo a mostrare è di contare il numero totale di basi dei sottospazi di dimensione k e capire poi quante di queste basi individuino lo stesso sottospazio W.

Proposizione 1.2.12. *Se V è uno spazio vettoriale di dimensione n su $\mathbb{F}_q$, allora $|V| = q^n$.*

Dato questo fatto preliminare, che segue in maniera diretta identificando canonicamente V con $\mathbb{F}_{q^n}$, siamo pronti ad enunciare il teorema centrale di questa sezione.

Teorema 1.2.13. *Sia $p \in \mathbb{N}$ un numero primo e sia $q = p^m$ per un certo intero positivo m. Sia $\mathbb{F}_q$ il campo finito di cardinalità di q e V uno spazio vettoriale di dimensione n su $\mathbb{F}_q$.*
Allora il coefficiente gaussiano $\binom{n}{k}_q$ è uguale al numero di sottospazi vettoriali di dimensione k di V.

Dimostrazione. Per prima cosa, ci proponiamo di contare quante sono le basi totali dei sottospazi di V di dimensione k. Una base $\{v_1, \dots, v_k\}$ di un sottospazio vettoriale di questo tipo corrisponde alla scelta di k vettori di V linearmente indipendenti. L'unica condizione da imporre sulla scelta di v_1 è che esso sia diverso dal vettore nullo; vi sono quindi $(q^n - 1)$ modi di scegliere v_1. Ad ogni passo successivo, per la scelta di v_i va impone la condizione che esso non appartenga a $span\{v_1, \dots, v_{i-1}\}$ che ha dimensione $i - 1$ e quindi, per la proposizione precedente, ha cardinalità q^{i-1}. Vi sono quindi $(q^n - q^{i-1})$ scelte possibili per ogni v_i. Procedendo in questo modo per la scelta di k vettori linearmente indipendenti otteniamo che il numero di basi diverse è

$$\prod_{i=0}^{k-1} (q^n - q^i) = \prod_{i=0}^{k-1} q^i (q^{n-i} - 1). \qquad (1)$$

Verifichiamo ora quante di queste basi individuano lo stesso sottospazio o, analogamente, quante sono le basi di ognuno di questi sottospazi. Possiamo contarle in modo analogo al punto precedente: fissato un sottospazio W di dimensione k, per determinare una sua base $\{v_1, \ldots, v_k\}$ abbiamo $(q^k - 1)$ scelte per v_1, $(q^k - q)$ per v_2 ecc. fino a $(q^k - q^{k-1})$ per v_k. Il numero di basi di W è quindi

$$\prod_{i=0}^{k-1}(q^k - q^i) = \prod_{i=0}^{k-1} q^i(q^{k-i} - 1). \qquad (2)$$

Dividendo la (1) per la (2) otteniamo che il numero di sottospazi cercati è

$$\frac{\prod_{i=0}^{k-1}(q^{n-i} - 1)}{\prod_{i=0}^{k-1}(q^{k-i} - 1)} = \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-k+1})}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1)} = \binom{n}{k}_q.$$

□

Facendo uso di questa interpretazione geometrica dei coefficienti gaussiani è possibile dare una dimostrazione alternativa della formula ricorsiva di Pascal. Questa dimostrazione è più profonda delle semplici manipolazioni algebriche con le quali l'abbiamo mostrata in precedenza e, sebbene sia più complessa, la presentiamo ora in quanto può essere utile a capire a fondo questo collegamento con l'algebra lineare. Ricordiamo la formula in questione per $k < n$

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q.$$

Dimostrazione. Sia W un iperpiano di V (ovvero un sottospazio vettoriale di dimensione $n-1$). I sottospazi vettoriali di V dimensione k possono essere due tipi: quelli contenuti in W e quelli che intersecano W in un sottospazio di dimensione $k-1$.

I sottospazi del primo tipo sono $\binom{n-1}{k}_q$ per il teorema precedente.

Tutti gli altri sono identificati da un sottospazio di dimensione $k-1$ di W e da un vettore $w \in V \smallsetminus W$. I sottospazi di dimensione $k-1$ sono $\binom{n-1}{k-1}_q$

mentre i vettori in $V \setminus W$ sono $(q^n - q^{n-1})$. Tra questi vettori, $(q^k - q^{k-1})$ identificano però lo stesso sottospazio. Il numero totale dei sottospazi del secondo tipo è quindi

$$\frac{(q^n - q^{n-1})}{(q^k - q^{k-1})}\binom{n-1}{k-1}_q = q^{n-k}\binom{n-1}{k-1}_q$$

Sommando le due quantità calcolate si ottiene quindi la tesi. □

Osservazione. All'apparenza la dimostrazione appena completata dimostra la validità della formula di Pascal solo per i valori di q che sono potenze di un numero primo, in quanto solo in tal caso ha senso l'interpretazione geometrica che abbiamo dato dei coefficienti gaussiani. Abbiamo però mostrato che entrambi i membri dell'equazione sono funzioni razionali in q (senza aver dimostrato la formula di Pascal non sappiamo ancora che i coefficienti gaussiani sono polinomi) uguali in infiniti punti. Allora devono coincidere su tutto il loro dominio, $\mathbb{R} \setminus \{1\}$. Si può pensare di estendere la funzione $q \to \binom{n}{k}_q$ in $q = 1$ per continuità ponendo $\binom{n}{k}_1 = \binom{n}{k}$; in tal caso per $q = 1$ si ottiene la formula classica di Pascal per i coefficienti binomiali. L'uguaglianza è quindi verificata su tutto $\mathbb{R}$.

1.2.5 Coefficienti Multinomiali e Multiinsiemi

Proseguendo in modo naturale dai coefficienti gaussiani, diamo la definizione di *q-coefficiente multinomiale.* Vedremo in questa sezione come questi siano uno strumento efficace per studiare le permutazioni di multiinsiemi.

Definizione 1.2.14. *Sia $n \in \mathbb{N}$ e siano $a_1, a_2, \cdots, a_k$ interi positivi tali che $\sum_{i=1}^k a_i = n$, si definisce*

$$\binom{n}{a_1, a_2, \ldots, a_k}_q = \frac{[n]_q!}{[a_1]_q![a_2]_q! \cdots [a_k]_q!}$$

$\binom{n}{a_1,a_2,\ldots,a_k}_q$ *prende il nome di $(a_1, a_2, \ldots, a_k)$-coefficiente gaussiano o $q-$coefficiente multinomiale.*

Invece di considerare le permutazioni dell'insieme $\{1, 2, \ldots, n\}$, in questa sezione studieremo le permutazioni di multiinsiemi. Un *multiinsieme* è un oggetto matematico che generalizza in maniera immediata il concetto di insieme, semplicemente permettendo di avere al suo interno più copie di uno stesso elemento. La definizione formale è la seguente.

Definizione 1.2.15. *La coppia $K = (A, m)$ viene detta multiinsieme se:*

1. *A è un insieme*

2. *$m : A \to \mathbb{N}$ è una funzione a valori interi positivi*

Si definisce cardinalità di un multiinsieme K la quantità

$$|K| = \sum_{a \in A} m(a)$$

Osservazione. Poiché la funzione m assume valori in $\mathbb{N}$,

$$|K| = +\infty \iff |A| = +\infty.$$

A viene detto **sostegno** del multiinsieme, m viene detta **molteplicità** del multiinsieme e indica quante copie di ogni elemento sono presenti nel multiinsieme. Un metodo utile per visualizzare i multiinsiemi è pensarli come il grafico della funzione m, ovvero l'insieme delle coppie $\{(a, m(a)) : a \in A\}$.

Esempio 6. Sia $K = (A, m)$ un multiinsieme tale che:

- $A = \{a, b, c\}$

- $m(a) = 3, m(b) = 1, m(c) = 3$

Allora K si può vedere come l'insieme di coppie $\{(a, 3), (b, 1), (c, 2)\}$.
Inoltre abbiamo che $|K| = 3 + 1 + 2 = 6$.

Nella trattazione dei prossimi risultati, useremo la seguente notazione: indichiamo con

$$K = \{\eta_1^{a_1}, \eta_2^{a_2}, \ldots, \eta_k^{a_k}\} \qquad n = |K| = a_1 + a_2 + \cdots + a_k$$

il multiinsieme di cardinalità n contenente a_i copie dell'elemento η_i.
La nozione di multiinsieme può apparire inutilmente complicata ma essa emerge in modo naturale in numerosi contesti, ed è molto utile nello studio della combinatoria. Diamo ora due esempi elementari in cui l'introduzione del concetto di multiinsieme chiarisce alcune ambiguità notazionali e vedremo nel prossimo capitolo anche come questa notazione si presti a descrivere le partizioni di un intero.

Esempio 7. L'anello dei numeri interi $\mathbb{Z}$ è un dominio a fattorizzazione unica, nel senso che ogni numero si può scrivere in modo unico (a meno di un segno) come prodotto di fattori primi. Per evitare fraintendimenti, la fattorizzazione di un numero naturale n si può quindi vedere come il multiinsieme contenente i suoi fattori primi, considerati rispetto a quante volte essi compaiono nella fattorizzazione. In questo modo si ha che il multiinsieme dei fattori primi di 60 è $\{2^2, 3, 5\}$ e quello di 18 è $\{2, 3^2\}$.

Esempio 8. Sia $p(x)$ un polinomio di grado n, siano $\alpha_1, \alpha_2 \dots, \alpha_k$ le sue radici e denotiamo con $m(\alpha_1), m(\alpha_2), \dots, m(\alpha_k)$ le loro molteplicità algebriche. Allora le radici di p possono essere viste come il multiinsieme $\{\alpha_1^{m(\alpha_1)}, \alpha_2^{m(\alpha_2)}, \dots, \alpha_k^{m(\alpha_k)}\}$. Con questa notazione, le radici del polinomio $x^3 - 3x + 2$ sono $\{1^2, -2\}$.

In questa sezione ci occuperemo di estendere i risultati sulle inversioni visti in precedenza al multiinsieme $K = \{1^{a_1}, 2^{a_2} \dots, k^{a_k}\}$. Una *permutazione* di un multiinsieme K è un modo di elencare i suoi elementi (considerati con le relative molteplicità). Indichiamo con S_K l'insieme di tutte le permutazioni dell'insieme K.

Esempio 9. Sia $K = \{1^2, 2^2\}$.
Allora $S_K = \{1122, 1212, 1221, 2112, 2121, 2211\}$.

Enunciamo ora un risultato che nella combinatoria classica è noto perché legato al conteggio delle permutazioni con ripetizione che, dato un multiinsieme K, lega la cardinalità di S_K ai coefficienti multinomiali.

Teorema 1.2.16. *Sia $K = \{e_1^{a_1}, e_2^{a_2}, \dots, e_k^{a_k}\}$, un multiinsieme con $|K| = n$. Allora*

$$|S_K| = \frac{n!}{a_1!a_2!\cdots a_k!} = \binom{n}{a_1, a_2, \dots, a_k}$$

Abbiamo visto che il $q-$fattoriale di un intero offre un modo per contare le permutazioni in base al numero di inversioni; allo stesso modo i $q-$coefficienti multinomiali possono essere usati per generalizzare il risultato appena enunciato e studiare le inversioni nelle permutazioni di multiinsiemi.
Un'inversione in una permutazione $p = p_1p_2...p_n$ di un multiinsieme $K = \{1^{a_1}, 2^{a_2} \dots, k^{a_k}\}$ è definita in modo analogo al caso dell'insieme $\{1, 2, \dots, n\}$, con l'unica differenza di usare l'indice di posizione nell'indicarla invece dell'entrata corrispondente al fine di evitare ambiguità.

Definizione 1.2.17. *Data una permutazione $p = p_1p_2...p_n$ di un multiinsieme K, la coppia di indici (i, j) si dice inversione di p se $i < j$ e $p_i > p_j$.*

Esempio 10. La permutazione $p = 13242$ ha 3 inversioni: $(2, 3)$, $(2, 5)$ e $(4, 5)$.

Il nostro obiettivo è ora quello di generalizzare il teorema 1.2.9 alle permutazioni di multiinsiemi, ovvero trovare un risultato che permetta di contare le permutazioni di un multiinsieme K in base al numero di inversioni. Naturalmente, ci aspettiamo una formula più complessa di quella dimostrata nel teorema 1.2.9 in quanto l'espressione da trovare dipenderà, oltre che dalla cardinalità n del nostro multiinsieme, anche da ognuno dei valori a_i delle molteplicità dei singoli elementi.

Prima di enunciare il teorema, osserviamo che i $q-$coefficienti multinomiali soddisfano, in modo analogo ai coefficienti multinomiali, la seguente identità

$$\binom{n}{a_1, a_2, \dots, a_k}_q = \binom{n}{a_1}_q \binom{n-a_1}{a_2}_q \binom{n-a_1-a_2}{a_3}_q \cdots \binom{a_k}{a_k}_q.$$

Denotato $i(p)$ il numero di inversioni di p, quello che vogliamo trovare è quindi un'espressione ben definita per la somma

$$\sum_{p\in S_K} q^{i(p)}.$$

Teorema 1.2.18. *Sia $K = \{1^{a_1}, 2^{a_2}, \dots, k^{a_k}\}$ un multiinsieme tale che $\sum_{i=1}^k a_i = n$. Allora*

$$\sum_{p\in S_K} q^{i(p)} = \binom{n}{a_1, a_2, \cdots, a_k}_q.$$

Dimostrazione. Per prima cosa dimostriamo il teorema nel caso $k = 2$, ovvero per $K' = \{1^{a_1}, 2^{a_2}\}$ con $a_1 + a_2 = n$. Mostriamo per induzione su n che

$$\sum_{p\in S_{K'}} q^{i(p)} = \binom{n}{a_1}_q.$$

Per $n = 1$ si ha $a_1 = 0 \vee a_1 = 1$ e il risultato è ovvio poiché $\binom{1}{0}_q = \binom{1}{1}_q = 1$. Assumiamo ora vera la tesi per $n-1$. Una permutazione del multiinsieme K' può avere come ultima entrata un 1 o un 2. Nel primo caso l'ultima entrata dà luogo a $a_2 = n - a_1$ inversioni, altrimenti non è coinvolta in nessuna inversione. Per ipotesi induttiva questo significa che

$$\sum_{p\in S_{K'}} q^{i(p)} = \binom{n-1}{a_1}_q + q^{n-a_1}\binom{n-1}{a_1-1}_q = \binom{n}{a_1}_q.$$

Possiamo ora dimostrare il teorema nella sua forma generale per induzione su k, con il caso $k = 1$ banale e il caso $k = 2$ dimostrato sopra. Supponiamo quindi che il teorema sia valido per $K = \{1^{a_1}, 2^{a_2}, \dots, k^{a_k}\}$ e lo mostriamo per $K^+ = \{1^{a_1}, 2^{a_2}, \dots, k^{a_k}, (k+1)^{a_{k+1}}\}$.
Sia $n = |K^+| = \sum_{i=0}^{k+1} a_i$. Osserviamo che ogni permutazione di $p \in S_{K^+}$ è completamente determinata dalla coppia (p', p'') dove p' è la permutazione ottenuta da p sostituendo 1 ad ogni entrata minore di $k+1$ e p'' è ottenuta da p rimuovendo tutte le entrate uguali a $k+1$. Un esempio per $k = 3$: da (p', p'') è possibile risalire a p inserendo le entrate $k+1$ in p'' come indicato da p'.

$$p = 22431241 \in S_{K^+} \longleftrightarrow \begin{cases} p' = 11411141 \\ p'' = 223121 \end{cases}$$

Vale inoltre che

$$i(p) = i(p') + i(p'').$$

Determinare $\sum_{p'} q^{i(p')}$ è equivalente al caso $k = 2$ mostrato in precedenza e vale quindi $\sum_{p'} q^{i(p')} = \binom{n}{a_{k+1}}_q$.

Per determinare $\sum_{p''} q^{i(p'')}$, siccome sono state rimosse le entrate uguali a $k+1$, possiamo applicare l'ipotesi induttiva e otteniamo quindi

$$\sum_{p''} q^{i(p'')} = \binom{n - a_{k+1}}{a_1, a_2, \ldots, a_k}_q.$$

Poiché p' e p'' sono indipendenti l'una dall'altra e ogni p' (che contiene $a_1 + a_2 + \cdots + a_k$ copie di 1 e a_{k+1} copie di $k + 1$) può essere accoppiata con una qualsiasi p'' (data da a_i copie di i per $i \in 1, 2, \ldots, k$), segue che

$$\begin{aligned}
\sum_{p \in S_{K+}} q^{i(p)} &= \sum_{p'} q^{i(p')} \cdot \sum_{p''} q^{i(p'')} \\
&= \binom{n}{a_{k+1}}_q \binom{n - a_{k+1}}{a_1, a_2, \ldots, a_k}_q \\
&= \binom{n}{a_{k+1}}_q \binom{n - a_{k+1}}{a_1}_q \binom{n - a_{k+1} - a_1}{a_2}_q \cdots \binom{a_k}{a_k}_q \\
&= \binom{n}{a_1, a_2, \ldots, a_{k+1}}.
\end{aligned}$$

Questo completa la dimostrazione.

□

Capitolo 2

Partizioni di interi

2.1 La funzione generatrice

Dato $n \in \mathbb{N}$, una *partizione* di n è una combinazione di interi positivi, detti parti, la cui somma sia n, ovvero un'espressione del tipo

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k \qquad \textit{con } n \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k.$$

Analogamente le si può vedere come delle k-uple ordinate in modo decrescente $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$. Considerare solo le tuple ordinate in questo modo garantisce che due partizioni non vengano considerate distinte se esse differiscono solo per l'ordine degli addendi.
Tutte queste considerazioni sono riassunte formalmente nella seguente definizione che fa uso della notazione multiinsiemistica introdotta nel capitolo precedente. Nel corso di questo capitolo useremo in modo intercambiabile le notazioni date.

Definizione 2.1.1. *Dato un intero $n \in \mathbb{N}$, una partizione di n è un multiinsieme $\lambda = \{1^{\alpha_1}, 2^{\alpha_2}, \ldots, k^{\alpha_k}\}$ (si indica $\lambda \vdash n$) di numeri naturali che abbia somma degli elementi uguale a n, ovvero tale che $\sum_{i=1}^{k} k\alpha_k = n$.*
Gli elementi del multiinsieme vengono chiamate parti. Indichiamo con $p(n)$ il numero di partizioni distinte di n. Per convenzione, poniamo $p(0) = 1$.

Esempio 11. Le partizioni di 5 sono

$$
\begin{aligned}
(1,1,1,1,1) &= \{1^5\} \\
(2,1,1,1) &= \{1^3,2\} \\
(2,2,1) &= \{1,2^2\} \\
(3,1,1) &= \{1^2,3\} \\
(3,2) &= \{2,3\} \\
(4,1) &= \{1,4\} \\
(5) &= \{5\}.
\end{aligned}
$$

Vale quindi $p_5 = 7$.

Non vi è una formula esplicita per $p(n)$ ma possiamo determinarne la funzione generatrice $S(q)$, ovvero la serie S tale che $S = \sum_{n\geq 0} p(n)q^n$.

Teorema 2.1.2.

$$S(q) = \sum_{n\geq 0} p(n)q^n = \prod_{n\geq 0} \frac{1}{1-q^n} = \prod_{k\geq 0}\sum_{k\geq 0} q^{ik}. \tag{2.1}$$

Dimostrazione. Ogni partizione $\lambda = \{1^{\alpha_1}, 2^{\alpha_2}, \dots\}$ è univocamente determinata da $(\alpha_1, \alpha_2, \dots)$, ovvero da quante volte stiamo sommando parti uguali 1, uguali a 2, eccetera. Quindi, per determinare una generica partizione λ di n, decidiamo in maniera indipendente, per ogni intero positivo k, quante volte includere k fra le parti di n; ovvero scegliamo un valore da assegnare a α_k. Ogni scelta di α_k contribuisce per $k\alpha_k$ alla somma totale della partizione. La funzione generatrice per la scelta di α_k è quindi $(1 + q^k + q^{2k} + q^{3k} + \dots) = 1/(1-q^k)$. Moltiplicando su tutti i $k \in \mathbb{N}$ otteniamo la tesi:

$$S(q) = (1+q+q^2+\cdots)(1+q^2+q^4+\cdots)\cdots(1+q^k+q^{2k}+\cdots)\cdots = \prod_{k\geq 0}\sum_{i\geq 0} q^{ik}.$$

$\square$

Osservazione. Nonostante abbiamo scritto $S(q)$ come prodotto infinito, per quanto riguarda il calcolo di un particolare $p(n)$ non è necessario l'intero prodotto, né tantomeno sono necessari i fattori nella loro interezza, in quanto in ogni partizione di n non possono comparire parti maggiori di n né è possibile considerare più di $\left\lfloor \frac{n}{k} \right\rfloor$ parti uguali a k.
Per il calcolo di $p(n)$ è quindi sufficiente considerare il prodotto

$$S_n(q) = \prod_{k \leq n} \sum_{i \leq \frac{n}{k}} x^{ik}.$$

Riprendiamo come esempio il caso n=5:

$$\begin{aligned} p(5) = [x^5]S_q &= [x^5]S_n(q) \\ &= [x^5](1 + x + \cdots + x^5)(1 + x^2 + x^4)(1 + x^3)(1 + x^4)(1 + x^5) \\ &= 7. \end{aligned}$$

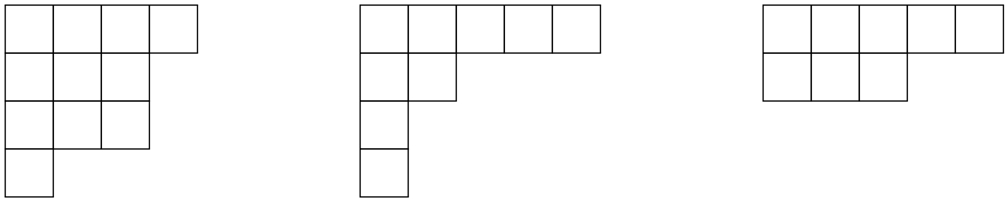
È possibile manipolare la funzione generatrice per considerare partizioni con determinate proprietà; ad esempio potremmo chiederci quante sono le partizioni di n in parti dispari, o con al più k parti. Prima di rispondere a domande di questo tipo introduciamo una rappresentazione grafica delle partizioni che permette di studiare meglio alcune proprietà.

2.2 I diagrammi di Young

Un'alternativa ai metodi già visti per la rappresentazione delle partizioni di un intero è quella dei *diagrammi di Young.* La partizione viene rappresentata da un insieme di celle quadrate di grandezza unitaria giustificate a sinistra, le cui righe sono ordinate per lunghezza in maniera decrescente, nel quale ogni riga rappresenta una delle parti della partizione. Analogamente, ad ogni diagramma di questo tipo si fa corrispondere una $(\lambda_1, \lambda_2, \dots, \lambda_k)$ dove λ_i è la lunghezza dell'$i-$esima riga del diagramma.

Esempio 12. Alcuni diagrammi di Young e le loro relative partizioni associate.

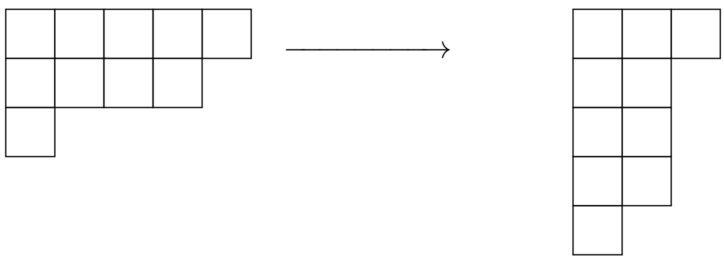
11=4+3+3+1 9=5+2+1+1 8=5+3



Osservazione. Questa rappresentazione può risultare utile anche per definire una relazione d'ordine sulle partizioni. Date $\lambda_1, \lambda \vdash n$, si può definire $\lambda_1 \leq \lambda_2 \iff$ il diagramma di Young di λ_1 è contenuto nel diagramma di Young di λ_2 (pensandoli come sottoinsiemi di $\mathbb{R}^2$). Non è negli scopi di questo lavoro ma lo studio del reticolo delle partizioni di n con questa o altre relazioni d'ordine permette di mostrare interessanti connessioni di tipo algebrico e geometrico [14].

Definizione 2.2.1. *Data $\lambda \vdash n$, si dice partizione coniugata o trasposta di λ la partizione associata al diagramma di Young ottenuto per simmetria rispetto alla diagonale principale, ovvero la partizione $\lambda^t = (\eta_1, \eta_2, \dots, \eta_j)$ dove η_i è la lunghezza dell'i$-$esima colonna del diagramma di Young di λ. Una partizione λ tale che $\lambda = \lambda^t$ si dice autoconiugata o autotrasposta.*

$\lambda = (5, 4, 1)$ $\qquad\qquad$ $\lambda^t = (3, 2, 2, 2, 1)$



Osservazione. Sia $P_n = \{\lambda \mid \lambda \vdash n\}$ l'insieme delle partizioni di n. Allora, data l'applicazione $T : P_n \longrightarrow P_n$ tale che $T(\lambda) = \lambda^t$, si ha che $T^{-1} = T$ poiché T corrisponde ad una simmetria. Quindi T è biunivoca e in particolare $\forall Q \subseteq P_n$ vale $|T(Q)| = |Q|$.

Se consideriamo ad esempio $P_{n,k} = \{\lambda \in P_n \mid \lambda \textit{ ha prima parte uguale a } k\}$, ovvero l'insieme delle partizioni di n il cui diagramma di Young ha la prima riga di lunghezza k, allora $T(P_{n,k}) = P^t_{n,k} = \{\lambda \in P_n \mid \lambda \text{ ha } k \text{ parti}\}$. Vale quindi la seguente proprietà:

$\forall k \leq n$, il numero di partizioni di n in k parti è uguale al numero di partizioni di n con prima parte uguale a k.

Proprietà come queste ci permetteranno di dare formulazioni equivalenti di molte delle proprietà che andremo a vedere in seguito.

2.3 Alcune proprietà

In questa sezione vedremo alcuni dei risultati più importanti per quanto riguarda le partizioni di un intero, vedremo in particolare come sia possibile utilizzare la funzione generatrice dei p_n per studiare il numero di partizioni con imposte delle particolari restrizioni.

Teorema 2.3.1. *Siano $p_o(n)$ e $p_d(n)$ rispettivamente il numero di partizioni di n in parti dispari e in parti distinte. Allora $\forall n \in \mathbb{N}$, $p_o(n) = p_d(n)$.*

Esempio 13. Per n=8 si ha:

$$p_d(6) = 4 : \begin{cases} (6) \\ (5,1) \\ (4,2) \\ (3,2,1) \end{cases} \qquad \text{e} \qquad p_o(6) = 4 : \begin{cases} (5,1) \\ (3,3) \\ (3,1,1,1) \\ (1,1,1,1,1,1) \end{cases} .$$

Dimostrazione. Siano $S_d(q)$ e $S_o(q)$ le funzioni generatrici rispettivamente di $\{p_d(n)\}_{n\in\mathbb{N}}$ e $\{p_o(n)\}_{n\in\mathbb{N}}$. Per ottenere la tesi, ci basta quindi mostrare che $S_d(q) = S_o(q)$.
Dato che nella funzione generatrice di $\{p(n)\}_{n\in\mathbb{N}}$ (teorema 2.1.2), la scelta di un termine dal k-esimo fattore rappresenta quante volte l'intero k compare nella partizione, la funzione generatrice di $p_d(n)$ si ottiene considerando solo i primi due termini di ogni sommatoria; ogni fattore rappresenta quindi una scelta binaria di inclusione/esclusione dell'intero k dalla partizione. Per le

partizioni in parti dispari invece basta considerare solo i fattori corrispondenti a k dispari. Le due funzioni generatrici sono quindi:

$$S_d(q) = (1+q)(1+q^2)\cdots(1+q^k)\cdots = \prod_{n\geq 0}(1+q^n)$$

$$S_o(q) = \prod_{k\geq 0}\sum_{i\geq 0} q^{i(2k+1)} = \prod_{k\geq 0}\frac{1}{1-q^{2k+1}}.$$

Manipolando la prima formula otteniamo la seguente espressione

$$\begin{aligned} S_d(q) = \prod_{n\geq 0}(1+q^n) &= \prod_{n\geq 0}\frac{1-q^{2n}}{1-q^n} \\ &= \frac{1-q^2}{1-q}\cdot\frac{1-q^4}{1-q^2}\cdots\frac{1-q^{2k}}{1-q^k}\cdots\frac{1-q^{4k}}{1-q^{2k}}\cdots \end{aligned}$$

nella quale i termini di grado pari al denominatore si semplificano coi numeratori. Quindi

$$S_d(q) = \frac{1}{1-q}\cdot\frac{1}{1-q^3}\cdots = \prod_{k\geq 0}\frac{1}{1-q^{2k+1}} = S_o(q).$$

□

Consideriamo ora le partizioni di un intero n in parti distinte e potenze di 2. Per ogni n, esiste solo una partizione di questo tipo poiché essa corrisponde alla scrittura in binario del numero n. La funzione generatrice di queste partizioni sarà quindi $1+q+q^2+q^3+\cdots = \frac{1}{1-q}$. Allo stesso tempo, ragionando a partire della funzione generatrice per le partizioni generiche di n e considerando in quest'ultima solo i primi due termini dei fattori corrispondenti a $k = 2^j$, si ha che la funzione generatrice per le partizioni di questo tipo è $(1+q)(1+q^2)(1+q^4)\cdots$. Questo prova la seguente identità polinomiale:

Teorema 2.3.2.

$$\frac{1}{1-q} = \prod_{k\geq 0}(1+q^{2^k}) = (1+q)(1+q^2)(1+q^4)\cdots$$

Un discorso analogo si può fare considerando la scrittura di n rispetto a una qualsiasi base b e vale quindi una generalizzazione del fatto precedente:

Teorema 2.3.3. $\forall b \in \mathbb{N}$,

$$\frac{1}{1-q} = \prod_{k \geq 0} (1 + q^{b^k} + q^{2b^k} + \cdots q^{(b-1)b^k})$$

2.3.1 Partizioni in un rettangolo

In quest'ultima sezione sulle partizioni studieremo un'enumerazione che tenga conto di due vincoli: consideriamo le partizioni il cui diagramma di Young sia contenuto in un rettangolo $h \times k$, ovvero che abbia la prima riga lunga al più h e la prima colonna lunga al più k. Mostreremo come tali partizioni sono in corrispondenza biunivoca con i sottospazi vettoriali di dimensione k di uno spazio vettoriale finito di dimensione $h+k$ su $\mathbb{F}_q$ e sono quindi contate dal coefficiente gaussiano $\binom{h+k}{k}_q$ come visto nel teorema 1.2.13. Denotiamo $p_{h,k}(n)$ il numero di partizioni di n con diagramma di Young contenuto in un rettangolo $h \times k$.

Teorema 2.3.4. *Siano $h, k \in \mathbb{N}$. Allora*

$$\sum_{n \geq 0} p_{h,k}(n) q^n = \binom{h+k}{k}_q.$$

Ovvero il coefficiente gaussiano $\binom{h+k}{k}_q$ è la funzione generatrice delle partizioni contenute nel rettangolo $h \times k$.

Prima di procedere con la dimostrazione diamo la definizione di matrice a scala ridotta e un importante risultato che lega le matrici di questo tipo ai sottospazi di spazi vettoriali finiti.

Definizione 2.3.5. *Si dice pivot di una matrice a scala per righe il primo elemento non nullo di ogni riga. Una matrice M si dice a scala ridotta per righe se*

- *M è a scala per righe.*

- *Tutti i pivot di riga di M sono uguali a 1.*
- *Tutti gli altri elementi delle colonne contenenti i pivot di riga sono uguali a 0.*

Proposizione 2.3.6. *Ad ogni sottospazio vettoriale di dimensione k di un $\mathbb{K}$-spazio vettoriale V di dimensione n corrisponde una e una sola matrice $k \times n$ a scala ridotta a coefficienti in K.*

Quest'ultima proposizione, la cui dimostrazione segue da fatti di base di algebra lineare, ci dice in particolare che il numero di matrici $n \times k$ a scala ridotta a coefficienti in $\mathbb{F}_q$ è uguale al numero di sottospazi vettoriali di dimensione k di $\mathbb{F}_q^n$, ovvero $\binom{n}{k}_q$ per il teorema 1.2.13. Per dimostrare il teorema 2.3.4 ci è quindi sufficiente mostrare che legame c'è tra le partizioni contenute nel rettangolo $h \times k$ e le matrici a scala ridotta.

Dimostrazione. Sia $m = h + k$. Dato un vettore di interi $(a_1, a_2, \dots, a_k)$ con $1 < a_1 < a_2 < \dots < a_k \leq m$, questo identifica una famiglia di matrici ridotte a scala a coefficienti in $\mathbb{F}_q$ nelle quali il primo elemento non nullo di ogni riga i è alla posizione a_i. Ad esempio, per $m = 7$, $k = 4$ e $(a_1, a_2, a_3, a_4) = (1, 3, 4, 6)$ otteniamo le matrici della forma

$$\begin{bmatrix} 1 & \star & 0 & 0 & \star & 0 & \star \\ 0 & 0 & 1 & 0 & \star & 0 & \star \\ 0 & 0 & 0 & 1 & \star & 0 & \star \\ 0 & 0 & 0 & 0 & 0 & 1 & \star \end{bmatrix}$$

nelle quali il simbolo $\star$ rappresenta un elemento arbitrario di $\mathbb{F}_q$. Chiamando $\lambda_i = h - a_i + i$ il numero di $\star$ nella riga i, si ha che la k-upla $(\lambda_i, \lambda_2 \dots, \lambda_k) = \lambda$ definisce una partizione di un intero $n = \sum_{i=1}^{k} \lambda_i = |\lambda|$ in al più k parti e con prima parte lunga al più h. Il numero di matrici di questa forma, dati $a_1, a_2, \dots, a_k$, è $q^{|\lambda|}$. Viceversa, data una partizione $\lambda \vdash n = |\lambda|$ contenuta in un rettangolo $h \times k$, possiamo definire $a_i = h - \lambda_i + i$ e il vettore $(a_1, a_2, \dots, a_k)$ dà origine a $q^{|\lambda|}$ matrici seguendo la costruzione appena vista. Siccome il numero di matrici ridotte a scala di dimensione $k \times m$ è uguale al numero di sottospazi vettoriali di dimensione k di $\mathbb{F}_q^m$ con $m = h + k$, otteniamo la tesi

$$\binom{h+k}{k}_q = \sum_{\substack{\lambda \text{ contenuta nel} \\ \text{rettangolo } h\times k}} q^{|\lambda|} = \sum_{n\geq 0} p_{h,k}(n)q^n.$$

□

2.4 Un problema di conteggio

Vediamo ora un problema di conteggio di cui presentiamo la soluzione proposta da Titu Andreescu e Zuming Feng in [6]. Questo problema è un esempio significativo di come analizzare la funzione generatrice possa permettere di risolvere un problema la cui soluzione esplicita sarebbe altrimenti di difficile formulazione.

Problema. *Trovare il numero di sottoinsiemi di* $A = \{1, 2, 3, \ldots, 2000\}$ *la cui somma degli elementi sia divisibile per* 5.

Una prima intuizione potrebbe portare a dire che i sottoinsiemi cercati siano un quinto del totale, in quanto può essere ragionevole aspettarsi una distribuzione uniforme in modulo 5 dei valori cercati. Chiaramente $5 \nmid |\mathcal{P}(A)| = 2^{2000}$ quindi notiamo subito che questa intuizione andrà quanto meno rifinita. Vedremo che questa prima idea non si distacca di molto dalla risposta esatta al problema ma, per cominciare a chiarirci le idee, analizziamo prima cosa succede in un caso di dimensione ridotta: nella figura 2.1 sono presentati tutti i sottoinsiemi di $\{1, 2, 3, 4, 5\}$ raggruppati in base alla somma dei loro elementi.

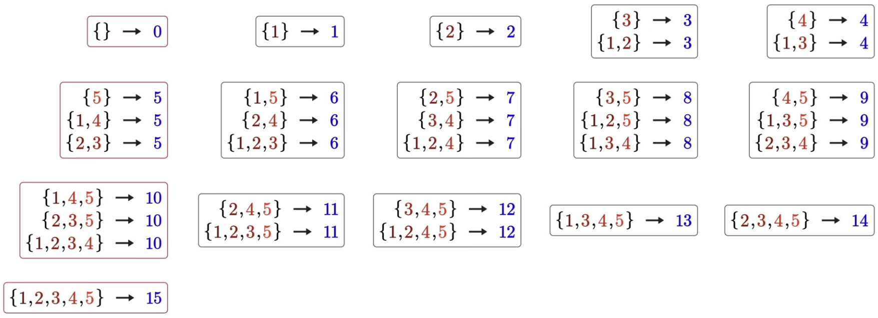


Figura 2.1: Una soluzione per $\{1, 2, 3, 4, 5\}$

Non abbiamo a disposizione una formula diretta e proviamo quindi a determinare la funzione generatrice dei sottoinsiemi di A rispetto alla loro somma; denominato a_n il numero di sottoinsiemi di A con somma n, cerchiamo un'espressione per $\sum_{n\geq 0} a_n q^n$.

L'intuizione alla base della soluzione del problema sta nella seguente proposizione, il resto saranno calcoli e manipolazioni della funzione generatrice trovata.

Proposizione 2.4.1. *Il numero di sottoinsiemi di $\{1, 2, 3..., k\}$ la cui somma degli elementi è uguale a n equivale al numero di partizioni di n in parti distinte tutte minori o uguali a k.*

Prendiamo un momento per convincerci di questa affermazione. Data una partizione di elementi distinti $\lambda \vdash n$, $\lambda = \{\lambda_1, \lambda_2, \dots, \lambda_j\}$ con $\lambda_i \leq k$ tale che $\sum_{i=1}^{j} \lambda_i = n$, questa può essere vista come un elemento di $\mathcal{P}(\{1, 2, 3, ...k\})$ la cui somma degli elementi sia n. Analogamente, dato $\{\lambda_1, \lambda_2, \dots, \lambda_j\} \subseteq \{1, 2, 3, ...k\}$ tale che $\sum_{i=1}^{j} \lambda_i = n$, questo identifica una partizione $\lambda \vdash n$ ottenuta riordinando in maniera decrescente i λ_i.

Tornando al nostro insieme $A = \{1, 2, 3..., 2000\}$, la funzione generatrice per le partizioni si otterrà considerando in (2.1) solo i primi 2000 fattori e solo i primi due termini di ognuno di essi come visto nel teorema 2.3.1:

$$S(q) = \prod_{i=1}^{2000} (1 + q^i) = (1 + q)(1 + q^2) \cdots (1 + q^{2000}) = \sum_{n\geq 0} a_n q^n.$$

Come ci aspettiamo, per $n > \frac{2000\cdot 20001}{2} = N$, $a_n = 0$: il sottoinsieme di somma massima è infatti A stesso, che corrisponde alla partizione $N = 2000 + \cdots + 2 + 1$. In un certo modo questa espressione in q può essere visto come un q-analogo della cardinalità di A. Infatti, per $q = 1$ vale $S(1) = \sum_{n\geq 0} a_n = 2^{2000} = |A|$ e $S(q)$ offre un conteggio più dettagliato dei sottoinsiemi di A, dividendoli in base alla loro somma.
Nonostante abbiamo un'espressione finita per il calcolo di a_n, la dimensione del problema non ci permette di sviluppare questo polinomio neanche utilizzando software dedicati. Ricordiamo che quello che stiamo cercando è il numero di sottoinsiemi che abbiano somma uguale a 0 in modulo 5, ovvero $a_0 + a_5 + a_{10} + \cdots + a_{5k} + \cdots + a_N$. $\forall j = 0, 1, 2, 3, 4$, chiamiamo c_j il numero di sottoinsiemi di A che abbiano somma j in modulo 5.
Sia $\zeta = e^{i\frac{2\pi}{5}}$ una radice quinta dell'unità. Per ζ vale la seguente proprietà: $\zeta^{5\alpha+\beta} = (\zeta^5)^\alpha\zeta^\beta = 1^\alpha\zeta^\beta = \zeta^\beta$. Diamo inoltre un altro risultato sulle radici primitive n-esime dell'unità che ci aiuterà nella risoluzione del problema.

Lemma 2.4.2. *Dato $n \in \mathbb{N}$, sia ζ una radice primitiva n-esima dell'unità, allora*

$$(1+\zeta)(1+\zeta^2)\cdots(1+\zeta^n) = \begin{cases} 2 & \textit{se } n \textit{ è dispari} \\ 0 & \textit{se } n \textit{ è pari} \end{cases}$$

Dimostrazione. Sia $p(x) = x^n - 1$, allora

$$p(x) = x^n - 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^n)$$

Sostituendo per $x = -1$ si ottiene

$$p(-1) = (-1-\zeta)(-1-\zeta^2)\cdots(-1-\zeta^n) = (-1)^n - 1,$$

ovvero

$$(1+\zeta)(1+\zeta^2)\cdots(1+\zeta^n) = 1 + (-1)^{n+1}$$

da cui la tesi.

$\square$

Valutiamo ora la funzione generatrice S in ζ in due modi differenti:

$$\begin{aligned}
S(\zeta) &= \prod_{i=1}^{2000}(1+\zeta^i) = ((1+\zeta)(1+\zeta^2)(1+\zeta^3)(1+\zeta^4)(1+\zeta^5))^{400} = 2^{400} \\
S(\zeta) &= \sum_{n\geq 0} a_n\zeta^n \quad = (a_0+a_5+\cdots)\zeta^0 + (a_1+a_6+\cdots)\zeta + (a_2+a_7+\cdots)\zeta^2 + \\
&\qquad\qquad\quad + (a_3+a_8+\cdots)\zeta^3 + (a_4+a_9+\cdots)\zeta^4 \\
&\qquad\qquad\quad = c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4.
\end{aligned}$$

Quindi uguagliando i due risultati ottenuti, abbiamo

$$(c_0 - 2^{400}) + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 = 0$$

cioè ζ è radice di $p(x) = (c_0-2^{400})+c_1x+c_2x^2+c_3+x^3+c_4x^4$. Questo significa che il polinomio minimo di ζ su $\mathbb{R}$ divide $p(x)$. ζ è una radice primitiva quinta dell'unità quindi il suo polinomio minimo è $q(x) = \frac{x^5-1}{x-1} = 1+x+x^2+x^3+x^4$. Poiché $q(x)$ è irriducibile in $\mathbb{R}$ e $p(x) \mid q(x)$, si ha necessariamente che $\exists\, c \in \mathbb{R}$ tale che

$$p(x) = cq(x) \implies c_0 - 2^{400} = c_1 = c_2 = c_3 = c_4.$$

Ricordando che $c_0 + c_1 + c_2 + c_3 + c_4 = \sum_{n\geq 0} a_n = 2^{2000}$, possiamo risolvere per c_0 e ottenere così il seguente risultato:

$$\begin{cases} c_0 = \dfrac{2^{2000} + 4\cdot 2^{400}}{5} \\ c_1 = c_2 = c_3 = c_4 = \dfrac{2^{2000} - 2^{400}}{5} \end{cases}.$$

Capitolo 3

q-numeri di Catalan

In quest'ultimo capitolo andremo a vedere una prima generalizzazione polinomiale dei numeri di Catalan attraverso i polinomi di Narayana. Daremo alcuni dei risultati principali e in particolare cercheremo di contestualizzare queste due successioni nell'ambito del conteggio dei cammini di Dyck, di cui diamo ora la definizione. Vi sono innumerevoli altre interpretazioni combinatorie di questi numeri e non è nelle intenzioni di questo lavoro parlare in dettaglio di molte di queste; maggiori approfondimenti si possono trovare in [2, 10, 11, 15].

3.1 Cammini di Dyck

Per gli scopi di questo lavoro, un *cammino* è semplicemente una serie di passi orizzontali, verticali o diagonali nel piano cartesiano. Ogni passo può essere identificato con una coppia $(i, j) \in \mathbb{Z}^2$ che rappresenta rispettivamente di quanto ci si stia spostando lungo l'asse x e lungo l'asse y.
Un *cammino di Dyck* è un cammino tutto contenuto nel primo quadrante con punto di partenza nell'origine e punto di arrivo in $(2n, 0)$ che consiste in passi di due tipi:

– I passi in direzione nord-est, corrispondenti alla coppia $(1, 1)$, detti *salite*.

– I passi in direzione sud-est, corrispondenti alla coppia $(1, -1)$, detti *discese*.

n viene detto *semilunghezza* del cammino e denotiamo $\mathscr{C}_n$ l'insieme dei cammini di Dyck di semilunghezza $2n$. Dato un cammino di questo tipo, possiamo codificare ogni salita con la lettera **U** (da *up*) e ogni discesa con la lettera **D** (da *down*). In questo modo ogni cammino di Dyck è univocamente determinato da una stringa di lunghezza $2n$ con n simboli **U** e n simboli **D** con la proprietà che, preso un qualunque segmento iniziale della stringa, questo non contiene più simboli **D** che simboli **U**; quest'ultima condizione garantisce che il cammino di Dyck considerato non scenda sotto l'asse y e sia quindi contenuto nel primo quadrante. Queste stringhe sono quindi una rappresentazione equivalente dei cammini di Dyck e vengono chiamate anche *parole di Dyck*. Nella figura 3.1 sono mostrati alcuni cammini di Dyck e le parole in **U** e **D** corrispondenti. Una definizione analoga e più comunemente usata descrive i cammini di Dyck come cammini con punto di partenza l'origine e punto di arrivo (n, n) e passi del tipo $(1, 0)$ e $(0, 1)$ che giacciano al di sotto, tuttalpiù toccandola, della diagonale principale. Le due definizioni sono intuitivamente analoghe e si ottengono l'una dall'altra ruotando e riscalando il reticolo in modo che i due punti di arrivo siano coincidenti.

Figura 3.1: I cammini di Dyck di semilunghezza 4 corrispondenti rispettivamente a UUDUUDDD e UUUDUDDD.

Nel corso di questo capitolo useremo principalmente la prima definizione allo scopo di rendere di più facile comprensione le dimostrazioni che seguiranno.

3.1.1 Numeri di Catalan

Enunciamo ora un primo risultato fondamentale sui cammini di Dyck.

Teorema 3.1.1. *Denotiamo con C_n il numero di cammini di Dyck di semilunghezza n. Allora vale la seguente formula:*

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{n!(n+1)!}.$$

Per convenzione consideriamo $C_0 = 1$, corrispondente all'unico cammino costante con punto di arrivo $(0,0)$. I C_n così definiti sono detti numeri di Catalan (A000108 in [1]) e sono una delle successioni numeriche più studiate in matematica. I primi numeri di questa successione sono

$$\begin{aligned} C_0 &= 1 \\ C_1 &= 1 \\ C_2 &= 2 \\ C_3 &= 5 \\ C_4 &= 12 \\ C_5 &= 42. \end{aligned}$$

Diamo ora una dimostrazione del teorema 3.1.1.

Dimostrazione. Sia A_n il numero di tutti i possibili cammini da $(0,0)$ in $(2n,0)$ di passi **U** e **D**, ovvero $A_n = \binom{2n}{n}$: A_n corrisponde al numero di scelte possibili per le posizioni delle n salite. Sia B_n il numero di cammini di questo tipo che non sono cammini di Dyck, ovvero i cammini da $(0,0)$ in $(2n,0)$ che scendono sotto l'asse $y = 0$. Allora abbiamo spostato il problema sul calcolo dei B_n poiché

$$C_n = A_n - B_n.$$

Un cammino in B_n è del tipo $\gamma = \alpha\mathbf{D}\beta$ dove α è un cammino di Dyck di semilunghezza k e β è un generico cammino di passi **U** e **D** con origine in

$(2k+1,-1)$ e punto finale in $(2n,0)$. La $\mathbf{D}$ messa in evidenza nella scrittura di γ rappresenta il primo passo in cui il cammino scende sotto l'asse $y=0$. Considero ora il cammino $\widetilde{\gamma}=\alpha\mathbf{D}\widetilde{\beta}$ ottenuto riflettendo β rispetto all'asse $y=-1$. $\widetilde{\gamma}$ è quindi un cammino con origine in $(0,0)$ e punto di arrivo in $(2n-2,0)$, ovvero un cammino con $n+1$ discese e $n-1$ salite.

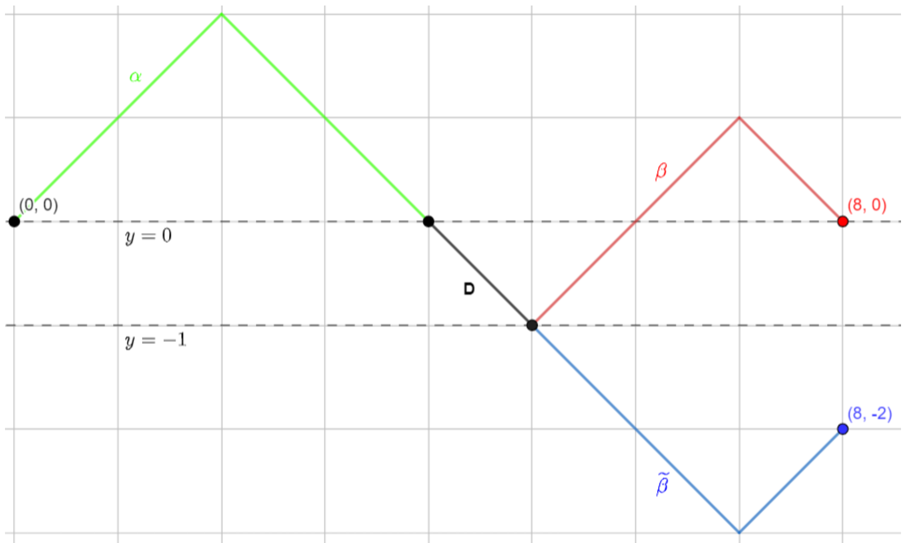


Figura 3.2: Un esempio per $n=4$ dell'operazione descritta nel teorema.

Siccome tutti i cammini da $(0,0)$ a $(2n-2,0)$ intersecano l'asse $y=-1$ e l'operazione di riflessione rispetto a tale asse è invertibile, l'applicazione $\gamma \longrightarrow \widetilde{\gamma}$ è una biezione. Possiamo quindi esprimere B_n come il numero di cammini con $n+1$ discese e $n-1$ salite, ovvero $B_n=\binom{2n}{n+1}$. Otteniamo quindi la tesi sviluppando l'espressione per C_n ottenuta:

$$\begin{aligned} C_n = A_n - B_n &= \binom{2n}{n} - \binom{2n}{n+1} \\ &= \frac{(2n)!}{n!n!} - \frac{(2n)!}{(n-1)!(n+1)!} \\ &= \frac{(2n)!(n+1) - (2n)!n}{n!(n+1)!} \\ &= \frac{1}{n+1}\frac{(2n)!}{n!n!} \\ &= \frac{1}{n+1}\binom{2n}{n}. \end{aligned}$$

□

Chiamiamo *ritorno* di un cammino di Dyck il primo punto del cammino, diverso da $(0,0)$, che sia sull'asse $y = 0$. Osserviamo che, dato $\gamma \in \mathscr{C}_n$ con primo ritorno al punto $(2k, 0)$, γ si può scomporre come $\gamma = \mathbf{U}\alpha_1\mathbf{D}\alpha_2$ con α_1 cammino di Dyck di semilunghezza $k-1$ e α_2 cammino di Dyck di semilunghezza $n-k$. Nel caso limite in cui γ abbia come unico ritorno il punto di arrivo $(2n, 0)$, α_2 coinciderà con il cammino costante in $(2n, 0)$. Questa decomposizione ci risulta utile per mostrare una formula di ricorsione per i C_n.

Teorema 3.1.2. *$\forall n \in \mathbb{N}$,*

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$$

Dimostrazione. Sia γ un cammino di Dyck di semilunghezza $n+1$, sia $2(k+1)$ la coordinata x del primo ritorno di γ, $k \leq n$. Allora γ si scompone come $\gamma = \mathbf{U}\alpha_1\mathbf{D}\alpha_2$ con $\alpha_1 \in \mathscr{C}_k$ e $\alpha_2 \in \mathscr{C}_{n-k}$. Il numero di cammini in $\mathscr{C}_{n+1}$ con primo ritorno in $(2(k+1), 0)$ è quindi $C_k C_{n-k}$; sommando su tutti i k da 0 a n si ha la tesi

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}.$$

□

Osservazione. Questa dimostrazione della formula di ricorsione non richiede di conoscere una formula esplicita per i C_n e permette, con la condizione iniziale $C_0 = 1$, di calcolare C_n per ogni $n \in \mathbb{N}$.

Da questa formula di ricorsione possiamo ricavare la funzione generatrice per i C_n.

Teorema 3.1.3.
$$c(x) = \sum_{n\geq 0} C_n x^n = \frac{1-\sqrt{1-4x}}{2x}.$$

Dimostrazione. Si procede in modo analogo a quanto visto nella sezione (1.1.1).

$$c(x) = \sum_{n\geq 0} C_n x^n \implies c^2(x) = \sum_{n\geq 0}\sum_{k=0}^{n} C_k C_{n-k} x^n = \sum_{n\geq 0} C_{n+1} x^n$$

Moltiplicando ambo i membri dell'ultima uguaglianza per x si ottiene

$$xc^2(x) = \sum_{n\geq 0} C_{n+1} x^{n+1} = c(x) - C_0 = c(x) - 1$$

Quindi $xc^2(x) - c(x) + 1 = 0$. Risolvendo per $c(x)$ si ottiene

$$c(x) = \frac{1+\sqrt{1-4x}}{2x} \qquad \vee \qquad c(x) = \frac{1-\sqrt{1-4x}}{2x}.$$

Poiché $\lim_{x\to 0} c(x) = C_0 = 1$, l'espressione cercata è $c(x) = \dfrac{1-\sqrt{1-4x}}{2x}$. □

3.1.2 Polinomi di Narayana

In questa sezione vediamo una prima generalizzazione polinomiale dei numeri di Catalan attraverso i polinomi di Narayana, così chiamati in onore del matematico canadese T. V. Narayana.
Definiamo, $\forall n \in \mathbb{N}$, i polinomi di Narayana come

$$\mathscr{N}_n(q) = \sum_{k=1}^{n} \frac{1}{n}\binom{n}{k-1}\binom{n}{k} q^k$$

con $\mathscr{N}_0(q) = 1$. I coefficienti di questi polinomi $N(n,k) = \frac{1}{n}\binom{n}{k-1}\binom{n}{k}$ sono detti numeri di Narayana (A001263 in [1]).

n						
1	1					
2	1	1				
3	1	3	1			
4	1	6	6	1		
5	1	10	20	10	1	
6	1	15	50	50	15	1
	1	2	3	4	5	6
	k					

Figura 3.3: I primi valori di $N(n,k)$. Sommando lungo le righe si ottengono i numeri di Catalan C_n.

Mostreremo in questa sezione in che modo i polinomi di Narayana possono essere visti come q-analoghi dei numeri di Catalan. Nella figura 3.3 sono mostrati i primi valori per $N(n,k)$; osserviamo che sommando per sui valori di k, ovvero calcolando $\mathscr{N}_n(1)$, si ottengono i primi numeri di Catalan C_n. Dato un cammino di Dyck, chiamiamo picco una salita immediatamente seguita da una discesa, ovvero un'istanza di **UD** nella scrittura del cammino; analogamente chiamiamo valle una discesa seguita da una salita, ovvero un'istanza di **DU**. Risulta evidente dalla rappresentazione grafica dei cammini di Dyck che dato un cammino γ, il numero di valli è uguale al numero di picchi meno uno. Mostreremo che questa relazione tra i numeri di Narayana e i numeri di Catalan è un risultato generale interpretando i numeri di Narayana $N(n,k)$ come il numero di cammini di Dyck di semilunghezza n con k picchi (o $k-1$ valli). I polinomi di Narayana $\mathscr{N}_n(q)$ sono quindi le funzioni generatrici dei cammini di Dyck di lunghezza n contati secondo questa proprietà. Indicando con $C_{n,k}$ il numero di cammini di Dyck di semilunghezza n con k picchi, vale il seguente risultato.

Teorema 3.1.4. *$\forall n \in \mathbb{N}$, $\forall k \leq n$,*

$$C_{n,k} = \frac{1}{n}\binom{n}{k-1}\binom{n}{k} = N(n,k).$$

Dimostrazione. Per la seguente dimostrazione sfrutteremo la definizione equivalente di cammini di Dyck data all'inizio del capitolo come cammini da $(0,0)$ in (n,n). Considerando i cammini in questo modo, il numero di picchi corrisponde al numero di passi orizzontali seguiti immediatamente da un passo verticale, viceversa per le valli. Osserviamo che un cammino da $(0,0)$ in (n,n) con passi orizzontali e verticali con k valli è univocamente determinato dalle coordinate dei punti in cui un passo verticale è seguito immediatamente da un passo orizzontale. Dato un cammino γ, chiamando (a_i, b_i) le coordinate dell'$i-$esima valle, abbiamo quindi che γ è univocamente determinato dal vettore

$$s = a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k.$$

Per il momento non consideriamo il fatto che il cammino γ deve stare al di sotto della diagonale principale e contiamo i generici cammini da $(0,0)$ in (n,n). Le condizioni da imporre sul vettore s perché quanto detto abbia senso sono quindi

$$\begin{cases} 0 \leq a_1 < a_2 < \cdots < a_k \leq n-1 \\ 1 \leq b_1 < b_2 < \cdots < b_k \leq n \end{cases}.$$

Questo mostra che, senza imporre la condizione sulla diagonale, il numero di cammini di semilunghezza n con k valli è $\binom{n}{k}\binom{n}{k}$, corrispondente alla scelta degli a_i e dei b_i. Analogamente a quanto fatto nel teorema 3.1.1, contiamo ora il numero di cammini con k valli che vanno al di sopra della diagonale principale, ovvero il numero di cammini per cui esiste un indice i tale che $a_i < b_i$; la tesi seguirà per differenza. Sia s il vettore che identifica un tale cammino e sia i il massimo indice tale che $a_i < b_i$. Definiamo

$$f(s) = (b_1, b_2, \ldots, b_{i-1}, a_{i+1}, \ldots, a_k, a_1, \ldots, a_i, b_i, \ldots, b_k).$$

Allora per $f(s)$ valgono le seguenti disuguaglianze:

$$\begin{cases} 1 \leq b_1 < b_2 < \cdots < b_{i-1} < a_{i+1} < \cdots < a_k \leq n-1 \\ 0 \leq a_1 < a_2 < \cdots < a_i < b_i < b_{i+1} < \cdots < b_k \leq n \end{cases} .$$

Vi sono quindi $\binom{n+1}{k+1}\binom{n-1}{k-1}$ scelte possibili per $f(s)$. Poiché $f(s)$ è una biezione, questo equivale al numero di cammini che non soddisfano la condizione di essere al di sotto della diagonale principale. Il numero di cammini di Dyck si semilunghezza n con k valli è quindi

$$\begin{aligned} \binom{n}{k}\binom{n}{k} - \binom{n+1}{k+1}\binom{n-1}{k-1} &= \binom{n}{k}\Big[\binom{n}{k} - \frac{n+1}{k+1}\binom{n-1}{k-1}\Big] \\ &= \binom{n}{k}\Big[\binom{n}{k} - \frac{n+1}{k+1}\frac{k}{n}\binom{n}{k}\Big] \\ &= \binom{n}{k}\binom{n}{k}\Big(\frac{n-k}{(n(k+1))}\Big) \\ &= \frac{1}{n}\binom{n}{k}\binom{n}{k+1} = N(n, k+1). \end{aligned}$$

Il numero di cammini di Dyck con k picchi corrisponde al numero di cammini con $k-1$ valli ed è quindi $N(n, k)$.

□

Conclusioni

La teoria dei q-analoghi è un argomento di studio molto vasto e quanto visto in questo lavoro è da intendersi come una prima introduzione all'argomento in ambito combinatorio.

Delle funzioni generatrici abbiamo esposto il concetto generale, focalizzandoci sul *modus operandi* e su come queste permettano di affrontare alcuni problemi combinatori. Uno studio dettagliato delle funzioni generatrici è presente in [5] e fa uso di strumenti più sofisticati per mostrare a fondo come questi oggetti forniscano un potente legame fra la matematica discreta e l'analisi continua.

Le partizioni di interi sono ancora ad oggi un campo di studio molto vivo a causa delle loro numerose applicazioni nel mondo della matematica. In particolare è possibile, a partire dalla funzione generatrice che abbiamo analizzato nel capitolo 2, ricavare formule di ricorrenza legate ai numeri pentagonali [9, 10], proprietà di congruenza e approssimazioni asintotiche per $p(n)$ [11].

I numeri di Catalan introdotti nel capitolo 3 sono un argomento vastissimo del quale abbiamo toccato appena la superficie; solo in [2] sono presentate più di 200 interpretazioni diverse di questi numeri in ambito combinatorio. Dato il così alto numero di possibili interpretazioni, è facile immaginare quante diverse generalizzazioni di questi numeri vi siano in letteratura. Rimanendo nell'ambito dei cammini di Dyck, alcune costruzioni di successioni polinomiali che generalizzino i numeri di Catalan sono approfondite in [7, 8].

Bibliografia

[1] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences* https://oeis.org/.

[2] Richard P. Stanley, *Catalan Numbers*. Cambridge University Press, 2015.

[3] Emeric Deutsch, *Dyck Path Enumeration*, Discrete Mathematics, Volume 204, Issues 1-3, 1999.

[4] Sarbajit Mazumdar, Jyotishka Ray Choudhury, *Partition Function*, HAL: Open Science, hal-01815249, 2018.

[5] Herbert S. Wilf, *generatingfunctionology*, Terza Edizione, A. K. Peters Ltd., 1990.

[6] Titu Andreescu, Zuming Feng. *102 Combinatorical Problems: From the Training of the USA IMO Team*, Springer Science & Business Media, 2002.

[7] Toufik Mansour, Yidong Sun, *Identities involving Narayana Polynomials and Catalan Numbers*, Discrete Mathematics, Volume 346, Issue 1, 2009.

[8] Marilena Barnabei, Flavio Bonetti, Matteo Silimbani, *Motzkin and Catalan Tunnel Polynomials*, Journal of Integer Sequences, Volume 21, Article 18.8.8, 2018.

[9] T. Kyle Petersen, *Eulerian Numbers*, Birkhäuser, 2015.

[10] Miklós Bóna, *Combinatorics of Permutations*, Seconda Edizione, CRC Press, 2012.

[11] https://en.wikipedia.org, *The Free Encyclopedia*: Gaussian Coefficients, Partition Function, Catalan Numbers, Narayana Numbers.

[12] Junkyu An, *Combinatorial Enumeration of Weighted Catalan Numbers*. Massachusetts Institute of Technology, Doctoral Theses, 2005.

[13] Brett Porter, *Cyclotomic Polynomials*, 2015.

[14] Müge Taşkin, *Properties of four partial orders on standard Young tableaux*, Journal of Combinatorial Theory, Series A, Volume 113, Issue 6, 2006.

[15] Richard P. Stanley, *Enumerative Combinatorics Volume* 1, Seconda Edizione, Cambridge University Press, 1997.