Algebra e Matematica Discreta Semplici (per davvero)

Gabriel Rovesti

20 aprile 2025

Indice

Prefazione

Questi appunti coprono gli argomenti trattati nel corso di Algebra e Matematica Discreta per il Corso di Laurea in Informatica. Il documento è diviso in due parti principali:

- La prima parte tratta l'Algebra, dove verranno affrontati argomenti come numeri complessi, congruenze, polinomi, matrici, spazi vettoriali, determinanti e autosistemi.
- La seconda parte tratta la Matematica Discreta, dove verranno affrontati argomenti come teoria dei grafi, combinatoria e relazioni di ricorrenza.

Questi appunti sono progettati per servire come guida allo studio, fornendo una presentazione formale e completa degli argomenti trattati nel corso.

Parte I

Algebra

Capitolo 1

Numeri complessi

1.1 Definizione e rappresentazione

Definizione 1.1. Un numero complesso è un numero che può essere espresso nella forma $a + bi$ dove a e b sono numeri reali e i è l'unità immaginaria che soddisfa $i^2 = -1$.

- a è detto parte reale del numero complesso e si indica con $\Re(z)$.
- b è detto parte immaginaria del numero complesso e si indica con $\Im(z)$.

Definizione 1.2. L'insieme dei numeri complessi, indicato con $\mathbb{C}$, è l'insieme di tutte le espressioni della forma $a + bi$ con $a, b \in \mathbb{R}$.

1.1.1 Rappresentazione geometrica

Un numero complesso $z = a + bi$ può essere rappresentato come un punto (a, b) nel piano cartesiano, chiamato piano complesso:

- L'asse x rappresenta la parte reale.
- L'asse y rappresenta la parte immaginaria.

1.1.2 Forma polare

Un numero complesso $z = a + bi$ può essere scritto in forma polare come:

$$z = r(\cos\theta + i\sin\theta) = re^{i\theta}$$

dove:

- $r = |z| = \sqrt{a^2 + b^2}$ è il modulo di z.
- $\theta = \arg(z)$ è l'argomento di z, cioè l'angolo che il vettore da origine a z forma con l'asse reale positivo.

1.2 Operazioni con i numeri complessi

1.2.1 Operazioni algebriche

Siano $z_1 = a + bi$ e $z_2 = c + di$ due numeri complessi. Le operazioni fondamentali sono:

- Somma: $z_1 + z_2 = (a + c) + (b + d)i$
- Sottrazione: $z_1 - z_2 = (a - c) + (b - d)i$
- Prodotto: $z_1 \cdot z_2 = (ac - bd) + (ad + bc)i$
- Divisione: $\frac{z_1}{z_2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$ per $z_2 \neq 0$

1.2.2 Coniugato di un numero complesso

Definizione 1.3. Il coniugato di un numero complesso $z = a + bi$ è $\overline{z} = a - bi$.

Teorema 1.1. *Per ogni numero complesso z:*

- $z \cdot \overline{z} = |z|^2$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

1.2.3 Modulo di un numero complesso

Definizione 1.4. Il modulo di un numero complesso $z = a + bi$ è $|z| = \sqrt{a^2 + b^2}$.

Teorema 1.2. *Per ogni numero complesso z_1, z_2:*

- $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$
- $|z_1 + z_2| \leq |z_1| + |z_2|$ *(disuguaglianza triangolare)*

1.3 Formula di Eulero e applicazioni

Teorema 1.3 (Formula di Eulero)**.** *Per ogni angolo θ in radianti:*

$$e^{i\theta} = \cos\theta + i\sin\theta$$

Corollario 1.1. *Per $\theta = \pi$, otteniamo l'identità di Eulero:*

$$e^{i\pi} + 1 = 0$$

Teorema 1.4. *Per ogni numero complesso in forma polare $z = re^{i\theta}$:*

- $z^n = r^n e^{in\theta}$
- *L'equazione $z^n = w$ ha esattamente n soluzioni distinte date da:*

$$z_k = \sqrt[n]{|w|} \cdot e^{i(\frac{\arg(w)+2\pi k}{n})}$$

per $k = 0, 1, 2, \ldots, n-1$.

Capitolo 2

Polinomi

2.1 Definizioni e proprietà di base

Definizione 2.1. Un polinomio in una variabile x a coefficienti in un campo K è un'espressione della forma:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

dove $a_0, a_1, \ldots, a_n \in K$ e $a_n \neq 0$.

- n è il grado del polinomio, indicato con $\deg(P)$.
- a_n è il coefficiente direttivo.
- a_0 è il termine noto.

Definizione 2.2. L'insieme di tutti i polinomi a coefficienti in K si indica con $K[x]$.

2.1.1 Operazioni sui polinomi

Siano $P(x) = \sum_{i=0}^{n} a_i x^i$ e $Q(x) = \sum_{j=0}^{m} b_j x^j$ due polinomi:

- Somma: $P(x) + Q(x) = \sum_{k=0}^{\max(n,m)} (a_k + b_k) x^k$, dove $a_k = 0$ per $k > n$ e $b_k = 0$ per $k > m$.
- Prodotto: $P(x) \cdot Q(x) = \sum_{k=0}^{n+m} c_k x^k$, dove $c_k = \sum_{i+j=k} a_i b_j$.

Teorema 2.1. *Siano $P(x)$ e $Q(x)$ due polinomi non nulli:*

- $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$
- $\deg(P \cdot Q) = \deg(P) + \deg(Q)$

2.2 Divisione tra polinomi

Teorema 2.2 (Algoritmo della divisione)**.** *Dati due polinomi $P(x)$ e $Q(x)$ con $Q(x) \neq 0$, esistono unici polinomi $S(x)$ e $R(x)$ tali che:*

$$P(x) = Q(x) \cdot S(x) + R(x)$$

dove $R(x) = 0$ oppure $\deg(R) < \deg(Q)$.

Definizione 2.3. Se $R(x) = 0$, si dice che $Q(x)$ divide $P(x)$, o che $P(x)$ è divisibile per $Q(x)$, e si scrive $Q(x) | P(x)$.

2.2.1 Regola di Ruffini

Teorema 2.3 (Teorema del resto)**.** *Il resto della divisione di un polinomio $P(x)$ per $(x-a)$ è $P(a)$.*

Corollario 2.1. *a è una radice di $P(x)$ se e solo se $(x-a)$ divide $P(x)$.*

Teorema 2.4 (Regola di Ruffini)**.** *Per dividere un polinomio $P(x) = a_n x^n + \cdots + a_1 x + a_0$ per $(x-a)$, si procede come segue:*

1. *Si scrivono in sequenza i coefficienti di $P(x)$: $a_n, a_{n-1}, \ldots, a_1, a_0$.*
2. *Si moltiplica il primo coefficiente per a e si somma al secondo: $a \cdot a_n + a_{n-1} = b_{n-1}$.*
3. *Si continua moltiplicando ogni risultato ottenuto per a e sommandolo al coefficiente successivo.*
4. *L'ultimo valore ottenuto è il resto R, e i valori precedenti sono i coefficienti del quoziente.*

2.3 Radici e fattorizzazione

Definizione 2.4. Un numero $a \in K$ è detto radice o zero di un polinomio $P(x)$ se $P(a) = 0$.

Teorema 2.5. *Un polinomio di grado n ha al più n radici distinte.*

Teorema 2.6 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio non costante a coefficienti complessi ha almeno una radice complessa.*

Corollario 2.2. *Ogni polinomio $P(x)$ di grado $n \geq 1$ a coefficienti complessi può essere fattorizzato come:*

$$P(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n)$$

dove $r_1, r_2, \ldots, r_n$ sono le radici di $P(x)$ (non necessariamente distinte).

2.3.1 Polinomi irriducibili

Definizione 2.5. Un polinomio $P(x)$ a coefficienti in un campo K si dice irriducibile su K se non può essere espresso come prodotto di polinomi di grado inferiore a coefficienti in K.

Teorema 2.7. *Ogni polinomio a coefficienti in un campo K può essere espresso in modo unico (a meno di fattori costanti) come prodotto di polinomi irriducibili su K.*

Teorema 2.8. *Sui numeri reali, i polinomi irriducibili sono solo di primo o secondo grado.*

2.3.2 Molteplicità di una radice

Definizione 2.6. Se un polinomio $P(x)$ può essere scritto come $P(x) = (x-a)^m \cdot Q(x)$ dove $Q(a) \neq 0$, allora a è una radice di $P(x)$ con molteplicità m.

2.4 Polinomi a coefficienti reali

Teorema 2.9. *Se $P(x)$ è un polinomio a coefficienti reali e $a+bi$ (con $b \neq 0$) è una sua radice, allora anche $a-bi$ è una radice.*

Corollario 2.3. *Ogni polinomio a coefficienti reali di grado dispari ha almeno una radice reale.*

Teorema 2.10. *Un polinomio di secondo grado $ax^2 + bx + c$ con $a \neq 0$ e a coefficienti reali ha:*

- *Due radici reali distinte se $\Delta = b^2 - 4ac > 0$*
- *Una radice reale doppia se $\Delta = 0$*
- *Due radici complesse coniugate se $\Delta < 0$*

dove Δ è detto discriminante.

Capitolo 3

Congruenze

3.1 Divisibilità e MCD

Definizione 3.1. Dati $a, b \in \mathbb{Z}$ con $b \neq 0$, si dice che b divide a (in simboli $b|a$) se esiste $c \in \mathbb{Z}$ tale che $a = bc$.

Definizione 3.2. Dati $a, b \in \mathbb{Z}$ non entrambi nulli, si dice Massimo Comun Divisore di a e b, indicato con $\text{MCD}(a, b)$, il più grande intero positivo che divide sia a che b.

Teorema 3.1 (Identità di Bézout)**.** *Dati $a, b \in \mathbb{Z}$, sia $d = MCD(a, b)$. Allora esistono $m, n \in \mathbb{Z}$ tali che:*

$$d = m \cdot a + n \cdot b$$

3.2 Congruenza modulo n

Definizione 3.3. Dati $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$ con $n > 0$, si dice che a è congruente a b modulo n (in simboli $a \equiv b \mod n$) se $n|(a - b)$, cioè se a e b danno lo stesso resto quando divisi per n.

Esempio 3.1. $17 \equiv 2 \mod 5$ perché $17 = 3 \cdot 5 + 2$ e $2 = 0 \cdot 5 + 2$.

Proposizione 3.1. *La relazione di congruenza modulo n è una relazione di equivalenza, cioè gode delle proprietà:*

- *Riflessiva: $a \equiv a \mod n$*
- *Simmetrica: se $a \equiv b \mod n$ allora $b \equiv a \mod n$*
- *Transitiva: se $a \equiv b \mod n$ e $b \equiv c \mod n$ allora $a \equiv c \mod n$*

3.2.1 Sistemi di congruenze

Teorema 3.2. *Sia data l'equazione $ax \equiv b \mod n$ e sia $d = MCD(a, n)$:*

- *L'equazione ha soluzioni se e solo se $d|b$*
- *Se ha soluzioni, allora per l'identità di Bézout $d = \alpha a + \beta n$ e $b = dq$. Quindi $x_0 = \frac{b}{d}\alpha$ è una soluzione.*
- *L'insieme di tutte le soluzioni è $x = x_0 + k\frac{n}{d}$ al variare di $k \in \mathbb{Z}$.*

Teorema 3.3 (Teorema cinese del resto)**.** *Sia dato il sistema di congruenze:*

$$\begin{aligned} a_1 x &\equiv b_1 \mod n_1 \\ &\vdots \\ a_k x &\equiv b_k \mod n_k \end{aligned}$$

Una condizione sufficiente perché il sistema abbia soluzioni è che $n_1, n_2, \ldots, n_k$ siano a due a due coprimi. In tal caso, tutte le soluzioni appartengono alla stessa classe di congruenza modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

3.2.2 Metodi di risoluzione

Teorema di Newton

Per risolvere un sistema di congruenze del tipo:

$$\begin{aligned} x &\equiv b_1 \mod n_1 \\ x &\equiv b_2 \mod n_2 \end{aligned}$$

Si procede ponendo $x_1 = b_1$ e $x_2 = x_1 + t_2 n_1$, e si risolve l'equazione $n_1 t_2 \equiv (b_2 - b_1) \mod n_2$ per trovare t_2. Quindi x_2 è la soluzione cercata.

Metodo di Lagrange

Per risolvere un sistema di congruenze del tipo:

$$\begin{aligned} x &\equiv b_1 \mod n_1 \\ x &\equiv b_2 \mod n_2 \end{aligned}$$

Se $1 = \alpha_1 n_1 + \alpha_2 n_2$, allora $z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$ è una soluzione.

3.2.3 Semplificazione di congruenze

Data la congruenza $ax \equiv b \mod n$ con $d = \text{MCD}(a, n)$, possiamo semplificarla come:

$$\frac{a}{d} x \equiv \frac{b}{d} \mod \frac{n}{d}$$

Se una soluzione è c, allora la congruenza equivalente è $x \equiv c \mod \frac{n}{d}$.

Capitolo 4

Matrici

4.1 Definizione e notazioni

Definizione 4.1. Una matrice A di dimensione $m \times n$ è una tabella rettangolare di elementi disposti in m righe e n colonne. Se $m = n$, la matrice si dice quadrata di ordine n.

Definizione 4.2. La matrice identità di ordine n, indicata con I_n, è una matrice quadrata con elementi $a_{ii} = 1$ per $i = 1, 2, \ldots, n$ e $a_{ij} = 0$ per $i \neq j$.

Indicheremo con e_i l'i-esima colonna della matrice identità.

4.2 Operazioni con le matrici

4.2.1 Somma di matrici

Date due matrici A e B di dimensione $m \times n$, la loro somma $A + B$ è una matrice di dimensione $m \times n$ i cui elementi sono la somma degli elementi corrispondenti di A e B:

$$(A + B)_{ij} = A_{ij} + B_{ij}$$

4.2.2 Prodotto per uno scalare

Dato uno scalare α e una matrice A di dimensione $m \times n$, il prodotto αA è una matrice di dimensione $m \times n$ i cui elementi sono il prodotto di α per gli elementi corrispondenti di A:

$$(\alpha A)_{ij} = \alpha \cdot A_{ij}$$

4.2.3 Prodotto di matrici

Date due matrici A di dimensione $m \times n$ e B di dimensione $n \times p$, il loro prodotto AB è una matrice di dimensione $m \times p$ i cui elementi sono:

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} \cdot B_{kj}$$

4.3 Proprietà delle matrici

4.3.1 Proprietà algebriche di base

- $\alpha A = A\alpha$
- $1A = A$
- $0A = \mathbf{0}$

- $(\alpha\beta)A = \alpha(\beta A)$
- $(-1)A = -A$

4.3.2 Proprietà della somma

- $(A + B) + C = A + (B + C)$
- $A + B = B + A$
- $A + \mathbf{0} = A$
- $A + (-A) = \mathbf{0}$
- $\alpha(A + B) = \alpha A + \alpha B$
- $(\alpha + \beta)A = \alpha A + \beta A$

4.3.3 Proprietà del prodotto

- $(AB)C = A(BC)$
- $\mathbf{0}A = \mathbf{0}$
- Se A è quadrata di ordine n, allora $I_n A = A = AI_n$
- $A(B + C) = AB + AC$
- $(A + B)C = AC + BC$
- $\alpha(AB) = (\alpha A)B = A(\alpha B)$

4.4 Matrici trasposte e coniugate

Definizione 4.3. La trasposta di una matrice A di dimensione $m \times n$ è una matrice A^T di dimensione $n \times m$ i cui elementi sono $A^T_{ij} = A_{ji}$.

Definizione 4.4. La coniugata di una matrice A di dimensione $m \times n$ è una matrice $\overline{A}$ i cui elementi sono $\overline{A}_{ij} = \overline{A_{ij}}$, dove $\overline{A_{ij}}$ è il coniugato complesso di A_{ij}.

Definizione 4.5. La trasposta coniugata (o hermitiana) di una matrice A è indicata con $A^H = \overline{A}^T$.

4.4.1 Proprietà delle trasposte e coniugate

- $\alpha A^T = (\alpha A)^T$
- $(A + B)^T = A^T + B^T$
- $(A^T)^T = A$
- $(AB)^T = B^T A^T$
- $(\alpha A)^H = \overline{\alpha} A^H$
- $(A + B)^H = A^H + B^H$
- $(A^H)^H = A$
- $(AB)^H = B^H A^H$

4.5 Tipi particolari di matrici

Definizione 4.6. Una matrice A si dice simmetrica se $A^T = A$.

Definizione 4.7. Una matrice A si dice antisimmetrica se $A^T = -A$.

Definizione 4.8. Una matrice A si dice hermitiana se $A^H = A$.

Definizione 4.9. Una matrice A si dice antihermitiana se $A^H = -A$.

4.6 Forma ridotta di Gauss

Definizione 4.10. Una matrice si dice in forma ridotta di Gauss se:

- È "a gradini", cioè sotto ogni elemento non nullo di una riga ci sono tutti zeri.
- Ogni riga non nulla inizia con un 1 (detto elemento dominante).
- Ogni colonna che contiene un elemento dominante ha tutti gli altri elementi pari a zero.

Le colonne contenenti gli elementi dominanti si chiamano colonne dominanti o pivot.

4.6.1 Eliminazione di Gauss

Per ottenere la forma ridotta di Gauss di una matrice si applicano ripetutamente le operazioni elementari di riga:

- $E_{ij}(c)$: Somma alla i-esima riga la j-esima riga moltiplicata per uno scalare c.
- $E_i(c)$: Moltiplica la i-esima riga per uno scalare $c \neq 0$.
- E_{ij}: Scambia la i-esima e la j-esima riga.

4.6.2 Forma ridotta di Gauss-Jordan

Una forma ridotta di Gauss-Jordan è una forma ridotta di Gauss dove le colonne dominanti sono esattamente le colonne della matrice identità.

4.7 Matrici invertibili

Definizione 4.11. Una matrice quadrata A di ordine n si dice invertibile se esiste una matrice B tale che $AB = I_n$. In tal caso, B è l'inversa di A e si indica con A^{-1}.

Teorema 4.1. *Una matrice quadrata A è invertibile se e solo se la sua forma ridotta di Gauss è la matrice identità.*

Teorema 4.2. *Se A è invertibile, allora $AA^{-1} = I_n = A^{-1}A$.*

Per trovare l'inversa di una matrice A, si applica l'eliminazione di Gauss alla matrice aumentata $[A|I_n]$ fino a ottenere $[I_n|A^{-1}]$.

Capitolo 5

Spazi vettoriali

5.1 Definizione di spazio vettoriale

Definizione 5.1. Uno spazio vettoriale V su un campo $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ è un insieme non vuoto con due operazioni:

- Addizione: $(u, v) \mapsto u + v$ per $u, v \in V$
- Prodotto per scalare: $(\alpha, v) \mapsto \alpha v$ per $\alpha \in \mathbb{K}$, $v \in V$

che soddisfano le seguenti proprietà:

1. $(u + v) + w = u + (v + w)$ per ogni $u, v, w \in V$
2. $u + v = v + u$ per ogni $u, v \in V$
3. Esiste un elemento $0 \in V$ tale che $v + 0 = v$ per ogni $v \in V$
4. Per ogni $v \in V$ esiste $-v \in V$ tale che $v + (-v) = 0$
5. $\alpha(\beta v) = (\alpha\beta)v$ per ogni $\alpha, \beta \in \mathbb{K}$, $v \in V$
6. $1v = v$ per ogni $v \in V$
7. $(\alpha + \beta)v = \alpha v + \beta v$ per ogni $\alpha, \beta \in \mathbb{K}$, $v \in V$
8. $\alpha(u + v) = \alpha u + \alpha v$ per ogni $\alpha \in \mathbb{K}$, $u, v \in V$

5.2 Sottospazi

Definizione 5.2. Sia V uno spazio vettoriale su $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. Un sottoinsieme $U \subseteq V$ è un sottospazio di V se e solo se:

- $0 \in U$ (o equivalentemente $U \neq \emptyset$)
- $u_1 + u_2 \in U$ per ogni $u_1, u_2 \in U$ (chiusura rispetto all'addizione)
- $\alpha u \in U$ per ogni $\alpha \in \mathbb{K}$, $u \in U$ (chiusura rispetto al prodotto per scalare)

5.2.1 Insieme dei multipli di un vettore

Definizione 5.3. Sia V uno spazio vettoriale su $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ e $v \in V$. L'insieme dei multipli di v è:

$$\langle v \rangle = \text{span } v = \{\alpha v | \alpha \in \mathbb{K}\}$$

Questo è un sottospazio di V.

5.2.2 Combinazioni lineari

Definizione 5.4. Sia V uno spazio vettoriale su $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ e $v_1, \ldots, v_n \in V$. Una combinazione lineare di questi vettori è un vettore della forma:

$$\alpha_1 v_1 + \ldots + \alpha_n v_n$$

dove $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ sono scalari.

Definizione 5.5. Il sottospazio generato da $v_1, \ldots, v_n$ è:

$$\langle v_1, \ldots, v_n \rangle = \text{span}(v_1, \ldots, v_n) = \{\alpha_1 v_1 + \ldots + \alpha_n v_n | \alpha_1, \ldots, \alpha_n \in \mathbb{K}\}$$

5.3 Sistemi di generatori e basi

Definizione 5.6. Sia V uno spazio vettoriale su $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ e $v_1, \ldots, v_n \in V$. Se $\langle v_1, \ldots, v_n \rangle = V$, allora $\{v_1, \ldots, v_n\}$ è un sistema di generatori di V.

Definizione 5.7. Un insieme di vettori $A = \{v_1, \ldots, v_n\}$ in uno spazio vettoriale V è linearmente indipendente se l'unica combinazione lineare che dà come risultato il vettore nullo è quella con tutti i coefficienti nulli, ovvero:

$$\alpha_1 v_1 + \ldots + \alpha_n v_n = 0 \iff \alpha_1 = \ldots = \alpha_n = 0$$

Definizione 5.8. Un insieme di vettori $A = \{v_1, \ldots, v_n\}$ in uno spazio vettoriale V è linearmente dipendente se non è linearmente indipendente, cioè se esiste una combinazione lineare non banale che dà come risultato il vettore nullo.

Osservazione 5.1. Per convenzione, l'insieme vuoto $\emptyset$ è linearmente indipendente. Un insieme formato da un solo vettore $\{v\}$ è linearmente dipendente se e solo se $v = 0$.

Definizione 5.9. Una base di uno spazio vettoriale V è un insieme di generatori linearmente indipendente.

Teorema 5.1. *Ogni spazio vettoriale ha almeno una base. Inoltre, tutte le basi di uno spazio vettoriale hanno lo stesso numero di elementi, che definisce la dimensione dello spazio.*

Definizione 5.10. La dimensione di uno spazio vettoriale V, indicata con $\dim V$, è il numero di elementi di una sua base. Per convenzione, $\dim\{0\} = |\emptyset| = 0$.

5.4 Somma e somma diretta di sottospazi

Definizione 5.11. Sia V uno spazio vettoriale e $U_1, U_2, \ldots, U_n$ sottospazi di V. La somma dei sottospazi è:

$$U_1 + U_2 + \ldots + U_n = \{u_1 + u_2 + \ldots + u_n | u_i \in U_i\} = \sum_{i=1}^{n} U_i$$

Definizione 5.12. Se $U_i \cap \left(\sum_{j \neq i} U_j\right) = \{0\}$ per ogni $i = 1, \ldots, n$, allora la somma è detta diretta e si indica con:

$$U_1 \oplus U_2 \oplus \ldots \oplus U_n = \bigoplus_{i=1}^{n} U_i$$

Teorema 5.2 (Teorema di Grassmann)**.** *La dimensione della somma di due sottospazi è la somma delle loro dimensioni meno la dimensione della loro intersezione:*

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$$

In particolare, se $U_1 \cap U_2 = \{0\}$, allora:

$$\dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2$$

5.5 Spazio delle colonne e spazio nullo di una matrice

Definizione 5.13. Sia A una matrice $m \times n$ a coefficienti in $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, con $A = [a_1, \ldots, a_n]$ dove $a_i \in \mathbb{K}^m$ sono le colonne di A. Lo spazio delle colonne di A è:

$$C(A) = \langle a_1, \ldots, a_n \rangle$$

Definizione 5.14. Lo spazio nullo di una matrice A è l'insieme delle soluzioni dell'equazione $Ax = 0$:

$$N(A) = \{v \in \mathbb{K}^n | Av = 0\}$$

Teorema 5.3. *Sia A una matrice $m \times n$ e sia $rkA = k$ il suo rango. Allora:*

$$\dim N(A) = n - k$$

Teorema 5.4 (Teorema di Rouché-Capelli)**.** *Sia $Ax = b$ un sistema di equazioni lineari. Allora:*

- *Il sistema ha soluzioni se e solo se $rk[A|b] = rkA$*
- *Il sistema ha un'unica soluzione se e solo se $rkA = n$, dove n è il numero di incognite*

5.5.1 Basi dello spazio delle colonne e dello spazio nullo

Per trovare una base dello spazio delle colonne di una matrice A, si applica l'eliminazione di Gauss ad A per ottenere la forma ridotta di Gauss U. Se le colonne dominanti di U sono $u_{i_1}, \ldots, u_{i_k}$, allora $\{a_{i_1}, \ldots, a_{i_k}\}$ è una base di $C(A)$.

Per trovare una base dello spazio nullo di A, si risolve il sistema omogeneo $Ax = 0$. Se $\dim N(A) = n - k$, si ottengono $n - k$ vettori linearmente indipendenti che formano una base di $N(A)$.

5.6 Coordinate rispetto a una base

Definizione 5.15. Sia $B = \{v_1, \ldots, v_n\}$ una base ordinata di uno spazio vettoriale V su $\mathbb{K}$ e sia $v \in V$. Il vettore delle coordinate di v rispetto a B è:

$$C_B(v) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{K}^n$$

dove $v = \alpha_1 v_1 + \ldots + \alpha_n v_n = \sum_{i=1}^{n} \alpha_i v_i$.

Definizione 5.16. La mappa delle coordinate è la funzione:

$$C_B : V \to \mathbb{K}^n, \quad v \mapsto C_B(v)$$

Teorema 5.5. *La mappa delle coordinate C_B gode delle seguenti proprietà:*

- $C_B(v + w) = C_B(v) + C_B(w)$ *per ogni* $v, w \in V$
- $C_B(\alpha v) = \alpha C_B(v)$ *per ogni* $\alpha \in \mathbb{K}$, $v \in V$
- *È suriettiva*
- *È iniettiva*

Quindi C_B è un isomorfismo tra spazi vettoriali.

5.7 Applicazioni lineari

Definizione 5.17. Siano V e W due spazi vettoriali su $\mathbb{K}$. Una funzione $T : V \to W$ è un'applicazione lineare se:

- $T(v_1 + v_2) = T(v_1) + T(v_2)$ per ogni $v_1, v_2 \in V$
- $T(\alpha v) = \alpha T(v)$ per ogni $\alpha \in \mathbb{K}$, $v \in V$

Osservazione 5.2. Da queste proprietà segue che $T(0_V) = 0_W$.

5.7.1 Nucleo e immagine

Definizione 5.18. Sia $T : V \to W$ un'applicazione lineare. Il nucleo di T è:

$$\mathrm{Ker}T = \{v \in V | T(v) = 0_W\}$$

Definizione 5.19. Sia $T : V \to W$ un'applicazione lineare. L'immagine di T è:

$$\mathrm{Im}T = \{T(v) | v \in V\}$$

Teorema 5.6. *Sia $T : V \to W$ un'applicazione lineare. Allora:*

- *$KerT$ è un sottospazio di V*
- *ImT è un sottospazio di W*
- *T è iniettiva se e solo se $KerT = \{0\}$*

5.7.2 Applicazione lineare indotta da una matrice

Definizione 5.20. Sia A una matrice $m \times n$ su $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. L'applicazione lineare indotta da A è:

$$L_A : \mathbb{K}^n \to \mathbb{K}^m, \quad v \mapsto L_A(v) = Av$$

Teorema 5.7. *Sia L_A l'applicazione lineare indotta da una matrice A. Allora:*

- *$KerL_A = N(A)$*
- *$ImL_A = C(A)$*

5.7.3 Matrice associata a un'applicazione lineare

Teorema 5.8. *Siano V e W due spazi vettoriali su $\mathbb{K}$, $T : V \to W$ un'applicazione lineare, $B = \{b_1, \ldots, b_n\}$ una base di V e $D = \{d_1, \ldots, d_m\}$ una base di W. Allora esiste un'unica matrice $A_{m\times n}$ associata all'applicazione lineare T rispetto alle basi B e D tale che il seguente diagramma commuta:*

$$V@>T>>W@VC_BVV@VVC_DV\mathbb{K}^n@>L_A>>\mathbb{K}^m$$

Cioè $C_D \circ T = L_A \circ C_B$, quindi $C_D(T(v)) = L_A(C_B(v)) = AC_B(v)$.

La matrice A si ottiene come:

$$A = [C_D(T(b_1)), \ldots, C_D(T(b_n))]$$

5.7.4 Matrice di passaggio tra basi

Definizione 5.21. Sia V uno spazio vettoriale su $\mathbb{K}$ con basi ordinate B e B'. La matrice di passaggio da B' a B è:

$$M_{B\leftarrow B'} = [C_B(b'_1), \ldots, C_B(b'_n)]$$

Teorema 5.9. *Sia $M_{B\leftarrow B'}$ la matrice di passaggio da B' a B. Allora:*

$$M_{B\leftarrow B'} = M^{-1}_{B'\leftarrow B}$$

Capitolo 6

Spazi metrici

6.1 Norme

Definizione 6.1. Una norma su uno spazio vettoriale V è una funzione $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ che soddisfa:

- $\|v\| \geq 0$ per ogni $v \in V$ e $\|v\| = 0$ se e solo se $v = 0$
- $\|\alpha v\| = |\alpha| \cdot \|v\|$ per ogni $v \in V$, $\alpha \in \mathbb{K}$
- $\|v + w\| \leq \|v\| + \|w\|$ per ogni $v, w \in V$ (disuguaglianza triangolare)

6.1.1 Esempi di norme

Esempio 6.1 (Norma euclidea)**.** La norma euclidea su $\mathbb{K}^n$ è:

$$\|v\|_2 = \sqrt{v^H v} = \sqrt{|v_1|^2 + \ldots + |v_n|^2}$$

Esempio 6.2 (Norma di Manhattan)**.** La norma di Manhattan (o taxi-driver) su $\mathbb{C}^n$ è:

$$\|v\|_1 = |v_1| + \ldots + |v_n|$$

Esempio 6.3 (Norma infinito)**.** La norma infinito su $\mathbb{C}^n$ è:

$$\|v\|_\infty = \max(|v_1|, \ldots, |v_n|)$$

6.2 Prodotto scalare

Definizione 6.2. Un prodotto scalare su uno spazio vettoriale V su $\mathbb{K}$ è una funzione:

$$(\cdot|\cdot) : V \times V \to \mathbb{K}$$

che soddisfa:

- $(v|w) = \overline{(w|v)}$ per ogni $v, w \in V$
- $(v|\alpha w + \beta z) = \alpha(v|w) + \beta(v|z)$ per ogni $v, w, z \in V$, $\alpha, \beta \in \mathbb{K}$
- $(v|v) \in \mathbb{R}$ e $(v|v) > 0$ per ogni $v \neq 0$, $(0|0) = 0$

Esempio 6.4 (Prodotto scalare canonico)**.** Il prodotto scalare canonico su $\mathbb{K}^n$ è:

$$(v|w) = v^H w = \sum_{i=1}^{n} \overline{v_i} w_i$$

Definizione 6.3. Uno spazio vettoriale dotato di un prodotto scalare si chiama spazio metrico (o spazio con prodotto interno).

6.2.1 Norma indotta

Definizione 6.4. Dato uno spazio vettoriale V su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$, la norma indotta è:

$$\|v\| = \sqrt{(v|v)}$$

6.2.2 Angolo tra vettori

Definizione 6.5. Dato uno spazio vettoriale V su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$ e norma indotta $\|\cdot\|$, il coseno dell'angolo $\widehat{vw}$ tra due vettori non nulli v e w è:

$$\cos \widehat{vw} = \frac{|(v|w)|}{\|v\| \cdot \|w\|}$$

6.3 Ortogonalità

Definizione 6.6. Dato uno spazio vettoriale V su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$, due vettori v e w sono ortogonali se $(v|w) = 0$, e si scrive $v \perp w$.

Definizione 6.7. Un insieme di vettori si dice ortogonale se i vettori sono a due a due ortogonali.

Definizione 6.8. Un vettore v si dice normalizzato se $\|v\| = 1$. Normalizzare un vettore significa considerare il vettore $\frac{v}{\|v\|}$.

Definizione 6.9. Un insieme di vettori si dice ortonormale se è ortogonale e tutti i vettori hanno norma 1.

6.3.1 Algoritmo di Gram-Schmidt

Algoritmo 6.1 (Algoritmo di Gram-Schmidt). Dato uno spazio vettoriale V su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$ e norma indotta $\|\cdot\|$, sia $S = \{v_1, \ldots, v_n\}$ un insieme di generatori di V. L'algoritmo permette di costruire un insieme di generatori ortogonali $S' = \{u_1, \ldots, u_n\}$ come segue:

1. $u_1 = v_1$
2. Per $j = 2, \ldots, n$:

$$u_j = v_j - \sum_{i=1}^{j-1} \alpha_{ij} u_i$$

dove $\alpha_{ij} = \begin{cases} 0 & \text{se } u_i = 0 \\ \frac{(u_i|v_j)}{(u_i|u_i)} & \text{se } u_i \neq 0 \end{cases}$

Per ottenere un insieme ortonormale, si normalizzano i vettori u_i ottenuti.

6.4 Complemento ortogonale

Definizione 6.10. Sia V uno spazio metrico su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$ e $U \leq V$ un sottospazio. Il complemento ortogonale $U^\perp$ di U è:

$$U^\perp = \{v \in V | (u|v) = 0 \text{ per ogni } u \in U\}$$

Teorema 6.1. *Sia U un sottospazio di uno spazio metrico V. Allora:*

- $U \cap U^\perp = \{0\}$
- $U \oplus U^\perp = V$
- $\dim U^\perp = \dim V - \dim U$

Teorema 6.2. *Sia $V \in \{\mathbb{R}^n, \mathbb{C}^n\}$ e $U \leq V$. Se $U = \langle u_1, \ldots, u_k \rangle$, allora:*

$$U^\perp = C(A)^\perp = N(A^H)$$

dove $A = [u_1, \ldots, u_k]$.

6.5 Proiezione ortogonale

Teorema 6.3. *Sia V uno spazio metrico su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$ e $U \leq V$ un sottospazio. Allora, per ogni $v \in V$, esistono unici $u \in U$ e $w \in U^\perp$ tali che $v = u + w$.*

Definizione 6.11. Nelle ipotesi del teorema precedente, $u = P_U(v)$ si chiama proiezione ortogonale di v su U.

Teorema 6.4. *Se $\{u_1^*, \ldots, u_k^*\}$ è una base ortonormale di U, allora:*

$$P_U(v) = \sum_{i=1}^{k} (u_i^*|v) u_i^*$$

6.5.1 Matrici di proiezione

Definizione 6.12. Sia V uno spazio metrico su $\mathbb{K}$ con un prodotto scalare $(\cdot|\cdot)$, $U \leq V$ e $\{u_1^*, \ldots, u_k^*\}$ una base ortonormale di U. Allora si definiscono le matrici $Q_{n\times k} = [u_1^*, \ldots, u_k^*]$ e $P_{n\times n} = QQ^H$. La matrice P si chiama matrice di proiezione di V su U ed è tale che $P_U(v) = Pv$.

Teorema 6.5. *La matrice di proiezione su $U^\perp$ è $I_n - P$.*

Capitolo 7

Determinanti

7.1 Definizione e calcolo

Definizione 7.1. Sia $A = (a_{ij})$ una matrice quadrata $n \times n$. Il determinante di A, indicato con $\det A$, è definito come segue:

- Se $n = 1$, allora $\det A = a_{11}$.
- Se $n > 1$, sia C_{ij} la matrice che si ottiene da A eliminando la i-esima riga e la j-esima colonna, e sia $A_{ij} = (-1)^{i+j} \det C_{ij}$. Allora:

$$\det A = \sum_{j=1}^{n} a_{ij} A_{ij}$$

per qualsiasi riga i, oppure:

$$\det A = \sum_{i=1}^{n} a_{ij} A_{ij}$$

per qualsiasi colonna j.

7.2 Proprietà dei determinanti

Teorema 7.1. *Sia A una matrice quadrata. Allora:*

- $\det A = \det A^T$
- $\det A^H = \overline{\det A}$
- $\det(AB) = \det A \cdot \det B$
- *A è non singolare (invertibile) se e solo se* $\det A \neq 0$
- *Se A è invertibile, allora* $\det(A^{-1}) = \frac{1}{\det A}$

7.3 Determinanti di matrici particolari

Teorema 7.2. *Il determinante di una matrice triangolare è il prodotto degli elementi sulla diagonale principale.*

Corollario 7.1. *Il determinante di una matrice diagonale è il prodotto degli elementi sulla diagonale. In particolare,* $\det(\alpha I_n) = \alpha^n$.

Capitolo 8

Autosistemi

8.1 Autovalori, autospazi e autovettori

Definizione 8.1. Sia A una matrice quadrata $n \times n$ su $\mathbb{K}$ e $\lambda \in \mathbb{K}$. Si definisce:

$$E_A(\lambda) = \{v \in \mathbb{K}^n | Av = \lambda v\} = N(A - \lambda I_n)$$

Se $E_A(\lambda) \neq \{0\}$, allora λ è un autovalore di A, $E_A(\lambda)$ è l'autospazio di A relativo all'autovalore λ, e ogni vettore non nullo in $E_A(\lambda)$ è un autovettore di A relativo all'autovalore λ.

8.2 Spettro e molteplicità

Definizione 8.2. L'insieme di tutti gli autovalori di una matrice A si chiama spettro e si indica con Spec$A$.

Definizione 8.3. La molteplicità geometrica di un autovalore λ di una matrice A è la dimensione dell'autospazio relativo a λ:

$$d(\lambda) = \dim E_A(\lambda) = n - \mathrm{rk}(A - \lambda I_n)$$

8.2.1 Polinomio caratteristico

Definizione 8.4. Sia A una matrice quadrata $n \times n$. Il polinomio caratteristico di A è:

$$P_A(x) = \det(A - xI_n)$$

L'equazione caratteristica di A è $P_A(x) = 0$.

Teorema 8.1. *Un numero $\lambda \in \mathbb{K}$ è un autovalore di una matrice A se e solo se $P_A(\lambda) = 0$.*

Teorema 8.2. *Gli autovalori di una matrice triangolare sono gli elementi della sua diagonale principale.*

8.2.2 Molteplicità algebrica

Definizione 8.5. Sia A una matrice $n \times n$ e Spec$A = \{\lambda_1, \ldots, \lambda_k\}$. Allora:

$$P_A(x) = (-1)^n (x - \lambda_1)^{m_1} \cdot \ldots \cdot (x - \lambda_k)^{m_k}$$

dove $n = m_1 + \ldots + m_k = \sum_{i=1}^{k} m_i$.

m_i è la molteplicità algebrica dell'autovalore λ_i di A e si indica con $m(\lambda_i)$.

Teorema 8.3. *Sia A una matrice $n \times n$ e λ un autovalore di A. Allora:*

$$1 \leq d(\lambda) \leq m(\lambda)$$

In particolare, se $m(\lambda) = 1$, allora $d(\lambda) = 1$.

8.3 Proprietà degli autospazi

Teorema 8.4. *Sia A una matrice $n \times n$ e $SpecA = \{\lambda_1, \ldots, \lambda_k\}$. Allora:*

$$E_A(\lambda_1) + \ldots + E_A(\lambda_k) = E_A(\lambda_1) \oplus \ldots \oplus E_A(\lambda_k)$$

Inoltre, se B_i è una base di $E_A(\lambda_i)$, allora $B = B_1 \cup \ldots \cup B_k$ è una base di $E_A(\lambda_1) \oplus \ldots \oplus E_A(\lambda_k)$.

8.4 Matrici simili

Definizione 8.6. Due matrici A e B di dimensione $n \times n$ si dicono simili se esiste una matrice invertibile S tale che $A = SBS^{-1}$.

Teorema 8.5. *Se A e B sono matrici simili, allora:*

- $P_A(x) = P_B(x)$
- $SpecA = SpecB$
- *Un autovalore $\lambda \in SpecA$ ha la stessa molteplicità algebrica e geometrica di $\lambda \in SpecB$*
- *Se $v \in E_B(\lambda)$, allora $Sv \in E_A(\lambda)$*

8.5 Matrici diagonalizzabili

Definizione 8.7. Una matrice A si dice diagonalizzabile se esiste una matrice diagonale D simile ad A, cioè se esistono una matrice invertibile S e una matrice diagonale D tali che $A = SDS^{-1}$.

Teorema 8.6. *Sia A una matrice $n \times n$ e $\lambda_1, \ldots, \lambda_k$ i suoi autovalori. Sia m_i la molteplicità algebrica e d_i la molteplicità geometrica di λ_i. Allora A è diagonalizzabile se e solo se $m_i = d_i$ per ogni $i = 1, \ldots, k$.*

8.5.1 Diagonalizzazione di una matrice

Se una matrice A è diagonalizzabile, allora:

- D è una matrice diagonale che ha come elementi della diagonale gli autovalori di A ripetuti con la loro molteplicità algebrica
- S è una matrice le cui colonne sono autovettori di A, in modo che la j-esima colonna di S sia un autovettore relativo all'autovalore che compare nella j-esima posizione della diagonale di D

8.6 Matrici unitariamente diagonalizzabili

Definizione 8.8. Una matrice A si dice unitariamente diagonalizzabile se esistono una matrice unitaria U e una matrice diagonale D tali che $A = UDU^H = UDU^{-1}$.

Definizione 8.9. Una matrice U si dice unitaria se $U^{-1} = U^H$.

Definizione 8.10. Una matrice U si dice ortogonale se $U^{-1} = U^T$.

Definizione 8.11. Una matrice A si dice normale se $AA^H = A^H A$.

Teorema 8.7 (Teorema spettrale (versione moltiplicativa))**.** *Una matrice A è unitariamente diagonalizzabile se e solo se A è normale.*

8.6.1 Diagonalizzazione unitaria

Per calcolare una diagonalizzazione unitaria di una matrice A normale:

- D si ottiene con lo stesso procedimento usato per una matrice diagonalizzabile
- U si ottiene prendendo basi ortonormali Q_i degli autospazi di A

Teorema 8.8 (Teorema spettrale (versione additiva))**.** *Sia A una matrice unitariamente diagonalizzabile e sia P_i la matrice di proiezione di $\mathbb{C}^n$ su $E_A(\lambda_i)$. Allora:*

$$A = \lambda_1 P_1 + \ldots + \lambda_k P_k = \sum_{i=1}^{k} \lambda_i P_i$$

8.7 Matrici hermitiane e simmetriche

Teorema 8.9. *Data una matrice A hermitiana, cioè con $A = A^H$, allora tutti i suoi autovalori sono reali ed essa è unitariamente diagonalizzabile.*

Teorema 8.10. *Data una matrice A reale simmetrica, cioè con $A = A^T$, allora esiste una matrice ortogonale reale U e una matrice diagonale reale D tali che $A = UDU^T$.*

Parte II

Matematica Discreta

Capitolo 9

Teoria dei grafi

9.1 Definizioni di base

Definizione 9.1. Un grafo non orientato $G(V, E)$ è una coppia di insiemi dove:

- $V = \{v_1, \ldots, v_n\}$ è un insieme finito di vertici (o nodi)
- E è un insieme di archi che sono coppie non ordinate di vertici

Definizione 9.2. Un grafo orientato $D(V, A)$ è una coppia di insiemi dove:

- $V = \{v_1, \ldots, v_n\}$ è un insieme finito di vertici (o nodi)
- A è un insieme di archi che sono coppie ordinate di vertici

9.1.1 Terminologia di base

Definizione 9.3. Gli estremi di un arco sono i due vertici della coppia che lo definisce.

Definizione 9.4. Un arco è incidente a un vertice se il vertice è un estremo dell'arco.

Definizione 9.5. Due vertici sono adiacenti se esiste un arco che li ha come estremi.

Definizione 9.6. Il grado di un vertice v in un grafo non orientato, indicato con $d(v)$, è il numero di archi incidenti in v.

Definizione 9.7. In un grafo orientato, il grado entrante di un vertice v, indicato con $d_{in}(v)$, è il numero di archi che terminano in v. Il grado uscente, indicato con $d_{out}(v)$, è il numero di archi che partono da v.

9.1.2 Proprietà fondamentali

Teorema 9.1. *In un grafo non orientato $G(V, E)$, la somma dei gradi dei vertici è uguale al doppio del numero degli archi:*

$$\sum_{v \in V} d(v) = 2|E|$$

Corollario 9.1. *In un grafo non orientato, il numero di vertici con grado dispari è sempre pari.*

Teorema 9.2. *In un grafo orientato $D(V, A)$, la somma dei gradi entranti è uguale alla somma dei gradi uscenti, che è uguale al numero degli archi:*

$$\sum_{v \in V} d_{in}(v) = \sum_{v \in V} d_{out}(v) = |A|$$

Teorema 9.3. *Un grafo non orientato semplice con n vertici ha al massimo $\binom{n}{2} = \frac{n(n-1)}{2}$ archi.*

9.2 Cammini e cicli

Definizione 9.8. Un cammino in un grafo non orientato è una sequenza di vertici distinti dove ogni coppia consecutiva di vertici è adiacente.

Definizione 9.9. Un ciclo è un cammino dove il primo e l'ultimo vertice sono coincidenti.

Definizione 9.10. Un percorso è una sequenza di vertici non necessariamente distinti dove ogni coppia consecutiva di vertici è adiacente. Un percorso si dice chiuso se le estremità coincidono.

Teorema 9.4. *Dato un percorso con estremità v_1 e v_n, esiste un cammino da v_1 a v_n.*

Teorema 9.5. *Ogni percorso chiuso di lunghezza dispari contiene un ciclo di lunghezza dispari.*

Definizione 9.11. Un cammino orientato in un grafo orientato è una sequenza di vertici distinti dove ogni coppia consecutiva di vertici è collegata da un arco nella direzione del cammino.

Definizione 9.12. Un circuito o ciclo orientato è un cammino orientato dove il primo e l'ultimo vertice sono coincidenti.

9.3 Tipi particolari di grafi

Definizione 9.13. Un grafo completo con n vertici, indicato con K_n, è un grafo in cui ogni coppia di vertici è adiacente.

Definizione 9.14. Un grafo bipartito è un grafo i cui vertici possono essere partizionati in due sottoinsiemi U e W tali che ogni arco collega un vertice di U con un vertice di W.

Definizione 9.15. Un grafo bipartito completo, indicato con K_{n_1,n_2}, è un grafo bipartito dove ogni vertice del primo insieme è adiacente a ogni vertice del secondo insieme.

Definizione 9.16. Una foresta è un grafo senza cicli (aciclico).

Definizione 9.17. Un albero è una foresta connessa.

Definizione 9.18. Un grafo k-regolare è un grafo in cui ogni vertice ha grado k. I grafi 3-regolari si chiamano grafi cubici.

Definizione 9.19. Un grafo si dice semplice se non ha archi multipli (più di un arco tra la stessa coppia di vertici) e non ha cappi (archi che collegano un vertice a se stesso).

Definizione 9.20. Un multigrafo è un grafo che può avere archi multipli e cappi.

Definizione 9.21. Un torneo è un grafo orientato in cui per ogni coppia di vertici esiste esattamente uno dei due possibili archi orientati.

9.4 Rappresentazione dei grafi

9.4.1 Matrici di incidenza e adiacenza

Definizione 9.22. La matrice di incidenza vertici-archi di un grafo non orientato è una matrice con tante righe quanti sono i vertici e tante colonne quanti sono gli archi, dove l'elemento (i, j) è 1 se il vertice i è un estremo dell'arco j, 0 altrimenti.

Definizione 9.23. La matrice di incidenza vertici-archi di un grafo orientato è una matrice con tante righe quanti sono i vertici e tante colonne quanti sono gli archi, dove l'elemento (i, j) è 1 se il vertice i è l'origine dell'arco j, -1 se è la destinazione, 0 altrimenti.

Definizione 9.24. La matrice di adiacenza di un grafo è una matrice quadrata con tante righe e colonne quanti sono i vertici, dove l'elemento (i, j) è 1 se esiste un arco dal vertice i al vertice j, 0 altrimenti.

9.4.2 Grafo complementare

Definizione 9.25. Dato un grafo non orientato semplice $G(V, E)$, il suo complementare è il grafo $G^C(V, E^C)$ dove $E^C = \{(v_i, v_j) | (v_i, v_j) \notin E, i \neq j\}$.

9.5 Connettività

Definizione 9.26. Un grafo non orientato si dice connesso se per ogni coppia di vertici esiste un cammino che li collega.

Definizione 9.27. Un grafo orientato si dice fortemente connesso se per ogni coppia di vertici u e v esiste un cammino orientato da u a v e un cammino orientato da v a u.

Definizione 9.28. Una componente connessa di un grafo non orientato è un sottografo connesso massimale.

Teorema 9.6. *Due vertici u e v di un grafo non orientato sono connessi se e solo se esiste un cammino che li collega.*

9.5.1 Tagli

Definizione 9.29. Dato un grafo $G(V, E)$ e un sottoinsieme $S \subseteq V$, il taglio associato a S è:

$$\delta(S) = \{uv \in E || S \cap \{u, v\}| = 1\}$$

Ovvero è l'insieme degli archi con una sola estremità in S.

Definizione 9.30. Si dice che un taglio $\delta(S)$ separa due vertici u e v se uno dei due appartiene a S e l'altro no.

Teorema 9.7. *Dato un taglio $\delta(S)$ che separa due vertici u e v, e dato un cammino P tra u e v, allora $\delta(S)$ e P hanno almeno un arco in comune, cioè $|P \cap \delta(S)| \geq 1$.*

Teorema 9.8. *Due vertici u e v stanno nella stessa componente connessa di un grafo G se e solo se non esiste un taglio $\delta(S) = \emptyset$ che li separa.*

9.5.2 Algoritmo per trovare una componente connessa

Algoritmo 9.1. Per trovare la componente connessa di un grafo $G(V, E)$ contenente un vertice v:

1. Inizializza $C = \{v\}$ e marca v come non esaminato.
2. Finché ci sono vertici non esaminati in C:
   (a) Scegli un vertice non esaminato $x \in C$.
   (b) Aggiungi a C tutti i vertici adiacenti a x che non sono già in C.
   (c) Marca x come esaminato.
3. Al termine, C è la componente connessa contenente v.

9.5.3 Connettività sugli archi e sui vertici

Definizione 9.31. L'arcoconnettività tra due vertici u e v di un grafo G, indicata con $k^E_{uv}(G)$, è la cardinalità minima di un taglio che separa u e v.

Definizione 9.32. L'arcoconnettività di un grafo G, indicata con $k^E(G)$, è il minimo di $k^E_{uv}(G)$ su tutte le coppie di vertici.

Teorema 9.9. *L'arcoconnettività tra due vertici u e v è il numero minimo di archi da rimuovere affinché u e v si trovino in componenti connesse distinte.*

Teorema 9.10. *L'arcoconnettività tra due vertici u e v è il numero massimo di cammini con estremità u e v che non hanno archi in comune.*

Definizione 9.33. La connettività sui vertici di un grafo connesso, semplice e non completo G, indicata con $k(G)$, è il numero minimo di vertici la cui rimozione rende G non connesso. Per convenzione, la connettività sui vertici di un grafo completo K_n è $n-1$.

Definizione 9.34. Un separatore di un grafo G è un insieme $S \subseteq V$ tale che $G \setminus S$ è un grafo non connesso.

Definizione 9.35. Dati due vertici non adiacenti u e v, $k_{uv}(G)$ è la cardinalità minima di un separatore S tale che u e v sono in componenti connesse distinte di $G \setminus S$.

Teorema 9.11. *La connettività sui vertici di un grafo è il minimo di $k_{uv}(G)$ su tutte le coppie di vertici non adiacenti:*

$$k(G) = \min_{u,v \text{ non adiacenti}} k_{uv}(G)$$

Teorema 9.12. *Dati due vertici non adiacenti u e v, un cammino P tra u e v e un separatore S che separa u e v, allora S contiene almeno un vertice intermedio di P.*

Teorema 9.13. *La connettività $k_{uv}(G)$ tra due vertici non adiacenti è il numero massimo di cammini internamente disgiunti (cioè che non hanno vertici interni in comune) con estremità u e v.*

Teorema 9.14. *In un grafo G, vale la relazione:*

$$k(G) \leq k^E(G) \leq \delta(G)$$

dove $\delta(G)$ è il grado minimo dei vertici di G.

9.6 Alberi e foreste

Teorema 9.15. *Se $F(V,E)$ è una foresta con n componenti connesse, allora $|E| = |V| - n$.*

Corollario 9.2. *Se $T(V,E)$ è un albero, allora $|E| = |V| - 1$.*

Teorema 9.16. *Un albero con almeno due vertici ha almeno due vertici di grado 1.*

Teorema 9.17. *Le seguenti affermazioni sono equivalenti per un grafo connesso T:*

1. *T è un albero (cioè è connesso e senza cicli)*
2. *Per ogni coppia di vertici distinti, esiste un unico cammino che li collega*
3. *T è minimamente connesso, cioè la rimozione di un qualsiasi arco lo rende non connesso*

9.6.1 Algoritmo di Kruskal

Algoritmo 9.2 (Algoritmo di Kruskal). Per trovare un albero di peso minimo in un grafo connesso $G(V,E)$ con pesi sugli archi:

1. Ordina gli archi in ordine non decrescente di peso: $w(e_1) \leq w(e_2) \leq \ldots \leq w(e_m)$.
2. Inizializza $T = \emptyset$.
3. Per $i = 1, 2, \ldots, m$:
   (a) Se l'aggiunta dell'arco e_i a T non crea cicli, allora $T \leftarrow T \cup \{e_i\}$.
4. Al termine, il grafo (V,T) è un albero di peso minimo.

9.6.2 Algoritmo di Dijkstra

Algoritmo 9.3 (Algoritmo di Dijkstra). Per trovare i cammini minimi da un vertice r a tutti gli altri vertici in un grafo con pesi non negativi $l(e)$ sugli archi:

1. Inizializza $d(r) = 0$, $d(v) = \infty$ per ogni $v \in V \setminus \{r\}$, $i = 0$ e $S_0 = \{r\}$.
2. Mentre $i < |V| - 1$:
   (a) Per ogni $v \in V \setminus S_i$, aggiorna $d(v) = \min\{d(v), d(u) + l(uv) | u \in S_i, uv \in E\}$.
   (b) Sia v il vertice di $V \setminus S_i$ con $d(v)$ minimo.
   (c) $i \leftarrow i + 1$, $S_i \leftarrow S_{i-1} \cup \{v\}$.
3. Al termine, $d(v)$ è la distanza minima da r a v per ogni $v \in V$.

9.7 Grafi bipartiti

Teorema 9.18. *Un grafo $G(V, E)$ è bipartito se e solo se non contiene cicli di lunghezza dispari.*

Algoritmo 9.4. Per verificare se un grafo $G(V, E)$ è bipartito e trovare una bipartizione:

1. Scegli un vertice $v \in V$ e assegnalo all'insieme R.
2. Per ogni vertice u adiacente a v, assegnalo all'insieme B.
3. Continua questo processo: per ogni vertice già assegnato, assegna i suoi vicini non ancora assegnati all'insieme opposto.
4. Se a un certo punto un vertice dovrebbe essere assegnato a entrambi gli insiemi, allora il grafo non è bipartito.
5. Altrimenti, al termine R e B formano una bipartizione del grafo.

9.8 Isomorfismo di grafi

Definizione 9.36. Due grafi $G(V, E)$ e $G'(V', E')$ sono isomorfi se esiste una biezione $f : V \to V'$ tale che $(u, v) \in E$ se e solo se $(f(u), f(v)) \in E'$.

Teorema 9.19. *Se due grafi sono isomorfi, allora:*

- *Hanno lo stesso numero di vertici*
- *Hanno lo stesso numero di archi*
- *Hanno lo stesso numero di vertici con lo stesso grado*
- *I loro complementari sono isomorfi*
- *Hanno gli stessi sottografi indotti da vertici corrispondenti*

9.9 Grafi planari

Definizione 9.37. Un grafo si dice planare se può essere disegnato sul piano senza intersezioni tra gli archi. Tale disegno si dice rappresentazione piana del grafo.

Definizione 9.38. Un minore di un grafo G è un grafo ottenuto da G mediante una sequenza di operazioni di rimozione di archi, rimozione di vertici isolati e contrazione di archi.

Teorema 9.20. *Se un grafo G è planare e G' è un suo minore, allora anche G' è planare.*

Teorema 9.21 (Teorema di Kuratowski)**.** *Un grafo è planare se e solo se non contiene K_5 o $K_{3,3}$ come minore.*

Definizione 9.39. Ogni rappresentazione piana di un grafo divide il piano in regioni o facce. La frontiera di una faccia è l'insieme degli archi che la delimitano, mentre il perimetro è il percorso chiuso che percorre la frontiera.

Teorema 9.22 (Formula di Eulero)**.** *Sia $G(V, E)$ un grafo connesso e planare con r facce. Allora:*

$$r = |E| - |V| + 2$$

Corollario 9.3. *Se $G(V, E)$ è un grafo semplice, planare con $|V| \geq 3$, allora:*

$$|E| \leq 3|V| - 6$$

Corollario 9.4. *Se $G(V, E)$ è un grafo semplice, planare e bipartito, allora:*

$$|E| \leq 2|V| - 4$$

Corollario 9.5. *Ogni grafo planare contiene almeno un vertice con grado ≤ 5.*

9.9.1 Metodo del cerchio e delle corde

Algoritmo 9.5 (Metodo del cerchio e delle corde). Per stabilire se un grafo G che contiene un ciclo hamiltoniano è planare:

1. Disegna il ciclo hamiltoniano come un cerchio.
2. Disegna gli archi che non fanno parte del ciclo (detti corde) all'interno o all'esterno del cerchio.
3. Se una corda ne incrocia un'altra, prova a disegnare una delle due all'esterno e l'altra all'interno.
4. Se è possibile disegnare tutte le corde senza incroci, il grafo è planare. Altrimenti non lo è.

9.10 Cicli hamiltoniani e percorsi euleriani

Definizione 9.40. Un ciclo hamiltoniano in un grafo $G(V, E)$ è un ciclo che visita ogni vertice esattamente una volta. Un grafo che contiene un ciclo hamiltoniano si dice hamiltoniano.

Teorema 9.23. *Condizioni necessarie affinché un grafo $G(V, E)$ sia hamiltoniano:*

- *Il grado di ogni vertice è almeno 2: $d(v) \geq 2$ per ogni $v \in V$*
- *La connettività del grafo è almeno 2: $k(G) \geq 2$*
- *Per ogni sottoinsieme S di V, il numero di componenti connesse di $G \setminus S$ è minore o uguale a $|S|$*

Teorema 9.24 (Teorema di Dirac)**.** *Sia $G(V, E)$ un grafo semplice con $n > 2$ vertici. Se $d(v) \geq \frac{n}{2}$ per ogni vertice $v \in V$, allora G è hamiltoniano.*

Definizione 9.41. Un percorso euleriano in un grafo $G(V, E)$ è un percorso chiuso che contiene ogni arco esattamente una volta. Un grafo che contiene un percorso euleriano si dice euleriano.

Teorema 9.25 (Teorema di Eulero)**.** *Un grafo $G(V, E)$ è euleriano se e solo se è connesso e ogni vertice ha grado pari.*

9.11 Colorazione dei grafi

Definizione 9.42. Il numero arcromatico $\chi'(G)$ di un grafo $G(V, E)$ è il minimo numero di colori necessari a colorare gli archi di G in modo che archi incidenti in uno stesso vertice abbiano colori diversi.

Teorema 9.26. *Se $G(V, E)$ è un grafo bipartito, allora $\chi'(G) = d_{max}(G)$, dove $d_{max}(G)$ è il grado massimo dei vertici di G.*

Teorema 9.27 (Teorema di Vizing)**.** *Se $G(V, E)$ è un grafo semplice, allora:*

$$d_{max}(G) \leq \chi'(G) \leq d_{max}(G) + 1$$

Definizione 9.43. Il numero cromatico $\chi(G)$ di un grafo $G(V, E)$ è il minimo numero di colori necessari a colorare i vertici di G in modo che vertici adiacenti abbiano colori diversi.

Teorema 9.28. *Se $G(V, E)$ è un grafo, allora $\chi(G) \leq d_{max}(G) + 1$.*

Teorema 9.29 (Teorema dei quattro colori)**.** *Se $G(V, E)$ è un grafo planare, allora $\chi(G) \leq 4$.*

Algoritmo 9.6 (Colorazione sequenziale). Per colorare i vertici di un grafo:

1. Ordina i vertici del grafo $v_1, v_2, \ldots, v_n$.
2. Per $i = 1, 2, \ldots, n$, assegna a v_i il colore con indice minimo che non è già stato assegnato ai suoi vicini già colorati.

Questo metodo non garantisce l'uso del numero minimo di colori.

Capitolo 10

Calcolo combinatorio

10.1 Principi fondamentali

Teorema 10.1 (Principio di addizione)**.** *Se si hanno n insiemi disgiunti, dove l'insieme i ha r_i elementi, allora il numero totale di modi per scegliere un elemento da uno di questi insiemi è $r_1 + r_2 + \ldots + r_n$.*

Teorema 10.2 (Principio di moltiplicazione)**.** *Se una procedura consiste di n fasi, dove la fase i può essere eseguita in r_i modi, indipendentemente dalle scelte fatte nelle altre fasi, allora il numero totale di modi per eseguire l'intera procedura è $r_1 \cdot r_2 \cdot \ldots \cdot r_n$.*

10.2 Permutazioni e combinazioni

Definizione 10.1. Una permutazione di n oggetti distinti è un ordinamento di questi oggetti. Il numero di permutazioni di n oggetti è $P(n, n) = n!$.

Definizione 10.2. Una r-permutazione di n oggetti distinti è un ordinamento di r degli n oggetti. Il numero di r-permutazioni di n oggetti è $P(n, r) = \frac{n!}{(n-r)!}$.

Definizione 10.3. Una r-combinazione di n oggetti distinti è un sottoinsieme non ordinato di r degli n oggetti. Il numero di r-combinazioni di n oggetti è $C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$.

10.3 Coefficienti binomiali

Definizione 10.4. Il coefficiente binomiale $\binom{n}{k}$, dove n e k sono numeri naturali con $k \leq n$, è definito come:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Se $k > n$, allora $\binom{n}{k} = 0$.

Teorema 10.3 (Teorema binomiale)**.** *Per ogni $n \in \mathbb{N}$:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Corollario 10.1.

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

10.3.1 Identità binomiali

Teorema 10.4. *Per i coefficienti binomiali valgono le seguenti identità:*

- $\binom{n}{k} = \binom{n}{n-k}$ *per* $k \leq n$
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ *per* $k \leq n$
- $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{n-k}$ *per* $m \leq k \leq n$
- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
- $\binom{n+1}{r+1} = \sum_{k=r}^{n} \binom{k}{r} = \binom{r}{r} + \binom{r+1}{r} + \ldots + \binom{n}{r}$
- $\binom{n}{k} = \binom{n-2}{k} + \binom{n-2}{k-2} + 2\binom{n-2}{k-1}$

10.3.2 Triangolo di Pascal

Il triangolo di Pascal è una rappresentazione grafica dei coefficienti binomiali dove il $(k+1)$-esimo elemento della $(n+1)$-esima riga è $\binom{n}{k}$.

10.4 Disposizioni con ripetizione e altre configurazioni

Definizione 10.5. Supponiamo di avere n oggetti di k tipi, con r_i oggetti di tipo i (con $r_1 + r_2 + \ldots + r_k = n$). Il numero di possibili disposizioni è:

$$\binom{n}{r_1, r_2, \ldots, r_k} = \frac{n!}{r_1! r_2! \ldots r_k!}$$

Definizione 10.6. Supponiamo di voler selezionare r oggetti identici da distribuire in n gruppi distinti. Il numero di possibili selezioni è:

$$\binom{r+n-1}{r} = \binom{r+n-1}{n-1}$$

10.4.1 Distribuzione di oggetti

Teorema 10.5. *Il numero di modi per distribuire r oggetti distinti in n scatole distinte è n^r.*

Teorema 10.6. *Il numero di modi per distribuire r oggetti distinti in n scatole distinte, con r_i oggetti nella scatola i (con $r_1 + r_2 + \ldots + r_n = r$) è:*

$$\binom{r}{r_1, r_2, \ldots, r_n} = \frac{r!}{r_1! r_2! \ldots r_n!}$$

Teorema 10.7. *Il numero di modi per distribuire r oggetti identici in n scatole distinte è $\binom{r+n-1}{r} = \binom{r+n-1}{n-1}$.*

Capitolo 11

Relazioni di ricorrenza

11.1 Definizione e tipi

Definizione 11.1. Una relazione di ricorrenza per una successione $\{a_n\}$ è una formula che esprime a_n in funzione di uno o più termini precedenti della successione, per $n \geq n_0$.

Definizione 11.2. La soluzione di una relazione di ricorrenza è la formula esplicita di a_n che dipende solo da n.

11.2 Relazioni lineari omogenee

Definizione 11.3. Una relazione di ricorrenza lineare omogenea di ordine r è una relazione della forma:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_r a_{n-r}$$

con r condizioni iniziali.

Teorema 11.1. *Per risolvere una relazione di ricorrenza lineare omogenea di ordine r, si pone $a_n = \alpha^n$ e si risolve l'equazione caratteristica:*

$$\alpha^r - c_1 \alpha^{r-1} - c_2 \alpha^{r-2} - \ldots - c_r = 0$$

Se $\alpha_1, \alpha_2, \ldots, \alpha_r$ sono le r radici (possibilmente ripetute) dell'equazione caratteristica, allora la soluzione generale è:

$$a_n = d_1 \alpha_1^n + d_2 \alpha_2^n + \ldots + d_r \alpha_r^n$$

dove i coefficienti $d_1, d_2, \ldots, d_r$ si determinano usando le condizioni iniziali.

Teorema 11.2. *Se una radice α dell'equazione caratteristica ha molteplicità m, allora la parte della soluzione generale corrispondente a questa radice è:*

$$(d_1 + d_2 n + d_3 n^2 + \ldots + d_m n^{m-1})\alpha^n$$

11.3 Relazioni lineari non omogenee

Definizione 11.4. Una relazione lineare non omogenea di ordine r è una relazione della forma:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_r a_{n-r} + f(n)$$

con r condizioni iniziali.

Teorema 11.3. *La soluzione generale di una relazione lineare non omogenea è la somma della soluzione generale dell'equazione omogenea associata e di una soluzione particolare dell'equazione non omogenea.*

11.3.1 Relazioni lineari non omogenee del primo ordine

Teorema 11.4. *Per risolvere una relazione del tipo $a_n = c \cdot a_{n-1} + f(n)$ con condizione iniziale a_0:*

- *Se $c = 1$, allora $a_n = a_0 + \sum_{k=1}^{n} f(k)$.*
- *Se $c \neq 1$, allora:*

$$a_n = c^n a_0 + \sum_{k=1}^{n} c^{n-k} f(k)$$

11.4 Casi particolari di relazioni di ricorrenza

11.4.1 Successione di Fibonacci

Definizione 11.5. La successione di Fibonacci è definita dalla relazione di ricorrenza:

$$F_n = F_{n-1} + F_{n-2}, \quad \text{per } n \geq 2$$

con condizioni iniziali $F_0 = 0$ e $F_1 = 1$.

Teorema 11.5. *La soluzione esplicita della successione di Fibonacci è:*

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

11.4.2 Relazioni di tipo "divide et impera"

Definizione 11.6. Una relazione di ricorrenza di tipo "divide et impera" ha la forma:

$$T(n) = a \cdot T\left(\frac{n}{b}\right) + f(n)$$

dove $a \geq 1$, $b > 1$ e $f(n)$ è una funzione data.

Teorema 11.6 (Teorema Master)**.** *Sia $T(n) = a \cdot T\left(\frac{n}{b}\right) + f(n)$ con $a \geq 1$, $b > 1$, e $f(n) = \Theta(n^d)$:*

- *Se $a > b^d$, allora $T(n) = \Theta(n^{\log_b a})$.*
- *Se $a = b^d$, allora $T(n) = \Theta(n^{\log_b a} \log n)$.*
- *Se $a < b^d$, allora $T(n) = \Theta(n^d)$.*

11.5 Esempi e applicazioni

Esempio 11.1 (Torre di Hanoi)**.** Il numero minimo di mosse T_n per spostare n dischi dalla prima piolo alla terza secondo le regole della Torre di Hanoi soddisfa la relazione:

$$T_n = 2T_{n-1} + 1, \quad T_1 = 1$$

La soluzione è $T_n = 2^n - 1$.

Esempio 11.2 (Problema dei conigli di Fibonacci)**.** Il numero di coppie di conigli F_n dopo n mesi, supponendo che inizialmente ci sia una coppia di conigli appena nati, che i conigli diventino fertili a due mesi e che ogni mese ogni coppia fertile generi una nuova coppia, soddisfa la relazione:

$$F_n = F_{n-1} + F_{n-2}, \quad F_1 = 1, \quad F_2 = 1$$

Questa è proprio la successione di Fibonacci.

Esempio 11.3 (Coefficienti binomiali)**.** I coefficienti binomiali soddisfano la relazione di ricorrenza:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \quad \binom{n}{0} = \binom{n}{n} = 1$$

11.6 Metodi di soluzione per casi particolari

11.6.1 Metodo delle iterazioni successive

Per risolvere relazioni di ricorrenza lineari non omogenee del primo ordine, possiamo applicare il metodo delle iterazioni successive:

Dato $a_n = c \cdot a_{n-1} + f(n)$ con a_0 dato, calcoliamo $a_1, a_2, \ldots$ iterativamente fino a identificare un pattern:

$$a_1 = c \cdot a_0 + f(1) \tag{11.1}$$
$$a_2 = c \cdot a_1 + f(2) = c^2 \cdot a_0 + c \cdot f(1) + f(2) \tag{11.2}$$
$$a_3 = c \cdot a_2 + f(3) = c^3 \cdot a_0 + c^2 \cdot f(1) + c \cdot f(2) + f(3) \tag{11.3}$$

Da cui si deduce il pattern generale:

$$a_n = c^n \cdot a_0 + \sum_{k=1}^{n} c^{n-k} \cdot f(k)$$

11.6.2 Metodo della funzione generatrice

Un altro potente strumento per risolvere relazioni di ricorrenza è l'uso delle funzioni generatrici:

Definizione 11.7. La funzione generatrice ordinaria di una successione $\{a_n\}_{n\geq 0}$ è la serie di potenze:

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

Esempio 11.4. Per la successione di Fibonacci, si ottiene:

$$G(x) = \frac{x}{1 - x - x^2}$$

Osservazione 11.1. Le funzioni generatrici permettono di trasformare una relazione di ricorrenza in un'equazione algebrica, semplificando la ricerca della soluzione.

Esempio 11.5. Per risolvere la ricorrenza $a_n = 2a_{n-1} + 3^n$ con $a_0 = 1$, si può usare la funzione generatrice:

$$G(x) = \frac{1 - 3x}{(1 - 2x)(1 - 3x)} = \frac{A}{1 - 2x} + \frac{B}{1 - 3x}$$

dove $A = 2$ e $B = -1$, quindi $a_n = 2 \cdot 2^n - 3^n$.

11.7 Applicazioni in informatica

Le relazioni di ricorrenza trovano numerose applicazioni in informatica, specialmente nell'analisi degli algoritmi:

- Analisi della complessità degli algoritmi ricorsivi (es. mergesort, quicksort)
- Calcolo dei coefficienti binomiali per il triangolo di Pascal
- Risoluzione di problemi di programmazione dinamica
- Modellazione di processi stocastici e sistemi dinamici

Esempio 11.6 (Complessità del Mergesort)**.** L'algoritmo Mergesort ha una complessità temporale che soddisfa la relazione:

$$T(n) = 2T\left(\frac{n}{2}\right) + \Theta(n)$$

Applicando il Teorema Master con $a = 2$, $b = 2$ e $d = 1$, si ha $a = b^d$, quindi $T(n) = \Theta(n \log n)$.

Esempio 11.7 (Complessità della ricerca binaria)**.** L'algoritmo di ricerca binaria ha una complessità temporale che soddisfa la relazione:

$$T(n) = T\left(\frac{n}{2}\right) + \Theta(1)$$

Applicando il Teorema Master con $a = 1$, $b = 2$ e $d = 0$, si ha $a = b^d$, quindi $T(n) = \Theta(\log n)$.

Bibliografia

[1] Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C. (2009). *Introduction to Algorithms*. MIT Press.

[2] Kleinberg, J., Tardos, É. (2005). *Algorithm Design*. Pearson Education.

[3] Rosen, K.H. (2011). *Discrete Mathematics and Its Applications*. McGraw-Hill.

[4] Graham, R.L., Knuth, D.E., Patashnik, O. (1994). *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley.

[5] Sedgewick, R., Flajolet, P. (2013). *An Introduction to the Analysis of Algorithms*. Addison-Wesley.