Appunti di Algebra e Matematica Discreta

Stevanato Giacomo

Maggio 2020

1 Algebra

1.1 Congruenze

Identità di Bezout

$$\forall a, b \in \mathbb{Z}\ d = \text{MCD}(a, b) \quad \exists m, n \in \mathbb{Z} : d = m \cdot a + n \cdot b$$

Sistemi di congruenze Sia data l'equazione $ax \equiv b \mod n$ e sia $d = \text{MCD}(a, n)$:

- Ho soluzioni solo se $d \mid b$
- Se ho soluzioni allora per Bezout $d = \alpha a + \beta n$ e $b = dq$, quindi $x_0 = \frac{b}{d}\alpha$ e $x = x_0 + k\frac{n}{d}$

Teorema cinese del resto

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

Condizione sufficiente perché il sistema abbia soluzioni è che $n_1, ...n_k$ siano a due a due coprimi. Tutte le soluzioni stanno nella classe di congruenza $n_1 \cdot ... \cdot n_k$.

Teorema di Newton

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

$$x_1 = b_1 \quad x_2 = x_1 + t_2 n_1$$

$$n_1 t_2 \equiv (b_2 - b_1) \mod n_2$$

Bisogna risolvere per t_2 e poi sostituire

Metodo di Lagrange

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

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.

Semplificare congruenza

$$ax \equiv b \mod n$$

$$d = \text{MCD}(a, n)$$

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

E se una soluzione è c, allora la seguente congruenza è equivalente a quella iniziale:

$$x \equiv c \mod \frac{n}{d}$$

1.2 Matrici

Matrice identità La matrice identità I_n è una matrice quadrata $n \times n$ con $a_{ii} = 1$ e $a_{ij} = 0$ se $i \neq j$. Con $\underline{e}_i$ si indica la i-esima colonna della matrice identità.

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

Proprietà delle matrici

- $\alpha A = A\alpha$
- $1A = A$
- $0A = \circledcirc$
- $(\alpha\beta)A = \alpha(\beta A)$
- $(-1)A = -A$

Proprietà della somma tra matrici

- $(\alpha + \beta)A = \alpha A + \beta A$
- $A + (B + C) = (A + B) + C$
- $A + B = B + A$
- $A + \circledcirc = A$
- $A + (-A) = \circledcirc$
- $\alpha(A + B) = \alpha A + \alpha B$

Proprietà del prodotto riga per colonna tra matrici

- $(AB)C = A(BC)$
- $\circledcirc A = \circledcirc$
- $\underset{n\times n}{A} \implies I_n A = A = AI_n$
- $A(B + C) = AB + AC$
- $(A + B)C = AC + BC$
- $\alpha(AB) = (\alpha A)B = A(\alpha B)$

Proprietà di matrici trasposte e H-trasposte

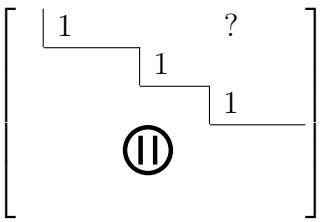
- $\alpha A^T = (\alpha A)^T$
- $(A + B)^T = A^T + B^T$
- $(A^T)^T = A$
- $(A\ B)^T = B^T\ A^T$
- $(\alpha A)^H = \overline{\alpha} A^H$
- $(A + B)^H = A^H + B^H$
- $(A^H)^H = A$
- $(A\ B)^H = B^H A^H$

Insieme delle matrici L'insieme delle matrici a coefficienti su $K \in \{\mathbb{R}, \mathbb{C}\}$ è $M_{m\times n}(K)$. Nel caso di matrici quadrate, quindi $m = n$, l'insieme si indica con $M_n(\mathbb{R})$.

Altre definizioni con le matrici

- A è simmetrica se $A^T = A$
- A è antisimmetrica se $A^T = -A$
- A è hermitiana se $A^H = A$
- A è antihermitiana se $A^H = -A$

Forma ridotta di Gauss Una matrice in forma ridotta di Gauss è una matrice "a gradini" in cui ogni sotto ci siano tutti 0, inoltre ogni gradino inizia con un 1.



Le colonne in cui si trova un inizio di gradino si chiamano colonne dominanti.

Eliminazione di Gauss Si può trovare una forma ridotta di Gauss di una matrice con una eliminazione di Gauss applicando ripetutamente le 3 operazioni base:

- Sommo alla i-esima riga della j-esima riga per uno scalare c ($E_{ij}(c)$)
- Moltiplico la i-esima riga per uno scalare $c \neq 0$ ($E_i(c)$)
- Scambio la i-esima e la j-esima riga (E_{ij})

Forma ridotta di Gauss-Jordan Una forma ridotta di Gauss-Jordan è una forma ridotta di Gauss particolare in cui le colonne dominanti sono le colonne della matrice identità.

Matrici invertibili

$$AB = I_n$$

Se esiste tale matrice B allora essa è l'inversa della matrice A, ovvero $A^{-1} = B$.
Condizione sufficiente e necessaria per la sua esistenza è che se U è una forma ridotta di Gauss di A, allora tutte le sue colonne devono essere dominanti.
Nel caso in cui A sia una matrice quadrata, allora è vero che $AA^{-1} = I_n = A^{-1}A$. Per trovare A^{-1} si devono effettuare le seguenti operazioni:

$$[A \mid I_n] \underset{\text{E.G.}}{\rightsquigarrow} [U \mid B] \underset{\text{E.G.J.}}{\rightsquigarrow} \left[I_n \mid A^{-1}\right]$$

1.3 Spazi vettoriali

Spazi vettoriali Uno spazio vettoriale V su $K \in \{\mathbb{R}, \mathbb{C}\}$ è un insieme non vuoto con definite due operazioni:

- Addizione $\quad (\underline{u}, \underline{v}) \longmapsto \underline{u} + \underline{v} \quad \underline{u}, \underline{v} \in V$
- Prodotto per scalare $\quad (\alpha, \underline{v}) \longmapsto \alpha\underline{v} \quad \alpha \in K, \underline{v} \in V$

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

- $\underline{o} \in U \quad$ oppure $\quad U \neq \emptyset$
- $\underline{u}_1 + \underline{u}_2 \in U \quad \forall \underline{u}_1, \underline{u}_2 \in U$
- $\alpha\underline{u} \in U \quad \forall \alpha \in K, \underline{u} \in U$

Insieme dei multipli di un vettore Sia V uno spazio vettoriale su $K \in \{\mathbb{R}, \mathbb{C}\}$ e $\underline{v} \in V$. Allora l'insieme dei multipli di $\underline{v}$ per gli elementi di K è un sottospazio di V e si indica con $\langle \underline{v} \rangle$:

$$\langle \underline{v} \rangle = \operatorname{span} \underline{v} = \{\alpha \underline{v} \mid \alpha \in K\}$$

Combinazione lineare di n vettori e n scalari Sia V uno spazio vettoriale su $K \in \{\mathbb{R}, \mathbb{C}\}$ e $\underline{v}_1, ..., \underline{v}_n \in V$.

$$\langle \underline{v}_1, ..., \underline{v}_n \rangle = \operatorname{span}(\underline{v}_1, ..., \underline{v}_n) = \{\alpha_1 \underline{v}_1 + ... + \alpha_n \underline{v}_n \mid \alpha_1, ..., \alpha_n \in K\}$$

$\langle \underline{v}_1, ..., \underline{v}_n \rangle$ è un sottospazio di V.

Sistema di generatori Sia V uno spazio vettoriale su $K \in \{\mathbb{R}, \mathbb{C}\}$ e $\underline{v}_1, ..., \underline{v}_n \in V$. Se $\langle \underline{v}_1, ..., \underline{v}_n \rangle = V$ allora $\{\underline{v}_1, ..., \underline{v}_n\}$ è un sistema di generatori di V

Insieme di vettori linearmente dipendenti e indipendenti Sia V uno spazio vettoriale su $K \in \{\mathbb{R}, \mathbb{C}\}$ e $A = \{\underline{v}_1, ..., \underline{v}_n\}$. A è linearmente indipendente se l'unica combinazione lineare nulla ($= \underline{o}$) è quella con coefficienti tutti nulli. Per convenzione $\emptyset$ è linearmente indipendente. $\{\underline{v}\}$ è linearmente dipendente se e solo se $\underline{v} = \underline{o}$.

Proprietà di un insieme di generatori di V

- Se A è un insieme di generatori di V e $A \subseteq B \subseteq V$ allora anche B è un insieme di generatori di V
- Se da un insieme di generatori di V tolgo un elemento che è combinazione lineare degli altri elementi dell'insieme, ottengo ancora un insieme di generatori di V.
- Un insieme che contiene un insieme linearmente dipendente è anch'esso linearmente dipendente
- Un insieme contenuto in un insieme linearmente indipendente è anche'esso linearmente indipendente

Basi Una base di uno spazio vettoriale V è un insieme di generatori di V che è anche linearmente indipendente. Ogni spazio vettoriale ha almeno una base. Inoltre basi di uno spazio vettoriale V sono equipotenti, cioé hanno la stessa dimensione di V. NB: $\dim\{\underline{o}\} = |\emptyset| = 0$

Somma e somma diretta di sottospazi Sia V uno spazio vettoriale e U_1, U_2, ... e U_n n sottospazi di V. È definita la somma tra U_1, U_2, ... e U_n come segue:

$$U_1 + U_2 + ... + U_n = \{\underline{u}_1 + \underline{u}_2 + ... + \underline{u}_n \mid \underline{u}_i \in U_i\} = \sum_{i=1}^{n} U_i \leq V$$

Inoltre se $U_i \cap (\sum_{i \neq j} U_j) = \{\underline{o}\}\ \forall i = 1, ..., n$ allora si definisce la somma diretta:

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

Teorema di Grassmann La dimensione della somma di due sottospazi è la somma delle loro dimensioni meno la dimensione della loro intersezione:

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

Nel caso particolare in cui $U_1 \cap U_2 = \{\underline{o}\}$ allora la dimensione della loro intersezione è 0 e può essere esclusa:

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

NB: Se S è un insieme di generatori di V, B una base di V e $|S| = \dim V = n$, allora $|B| = n$ e S è una base di V.

Spazio delle colonne di una matrice Sia A una matrice $m \times n$ a coefficienti in $K \in \{\mathbb{R}, \mathbb{C}\}$

$$A = [\underline{a}_1, ..., \underline{a}_n] \qquad \text{con } \underline{a}_i \in K^m$$

Lo spazio delle colonne di A è:

$$C(A) = \langle \underline{a}_1, ..., \underline{a}_n \rangle$$

Per trovare una base di $C(A)$ applico una riduzione di Gauss ad A:

$$A \underset{\text{E.G.}}{\rightsquigarrow} U$$

Se k è il numero di colonne dominanti di U e $\underline{u}_{i_1}, ..., \underline{u}_{i_k}$ sono le colonne dominanti di U, allora $B = \{\underline{a}_{i_1}, ..., \underline{a}_{i_k}\}$ è una base di $C(A)$.
$\dim C(A) = |B| = k = \operatorname{rk} A$

Spazio nullo È l'insieme delle soluzioni dell'equazione $A\underline{x} = \underline{o}$, dove A è una matrice $m \times n$, quindi $\underline{x}$ è un vettore alto n. Lo spazio nullo di una matrice è un sottospazio di $\mathbb{C}^n$

$$N(A) = \{\underline{v} \in \mathbb{C}^n \mid A\ \underline{v} = \underline{o}\}$$

Teorema nullità + rango Sia A una matrice $m \times n$ e $\operatorname{rk} A = k$, allora $\dim N(A) = n - k$

Teorema di Rouché-Capelli Si consideri l'equazione $A\underline{x} = \underline{b}$.

$$[A \mid \underline{b}] \underset{\text{E.G.}}{\rightsquigarrow} [U \mid \underline{d}]$$

- Ho soluzioni se e solo se $\underline{d}$ è libera (ovvero $\operatorname{rk}[A \mid \underline{b}] = \operatorname{rk} A$)
- Ho una sola soluzione se tutte le colonne di U sono dominanti (ovvero $\operatorname{rk} A = n$)

Trovare una base di $N(A)$
Sia A una matrice $m \times n$ e si applichi una riduzione di Gauss su di essa.

$$A \underset{\text{E.G.}}{\rightsquigarrow} U \quad \iff \quad [A \mid \underline{o}] \underset{\text{E.G.}}{\rightsquigarrow} [U \mid \underline{o}]$$

$$N(A) = \{\underline{x} \mid A\underline{x} = \underline{o}\} = \{\underline{x} \mid U\underline{x} = \underline{o}\} = N(U)$$

Per il teorema nullità + rango ho $\dim N(A) = n - k$ soluzioni descritte da $n - k$ parametri $h_1, ..., h_{n-k}$. Sia $\underline{v}_i$ il vettore di $N(A)$ che si ottiene ponendo $h_i = 1$ e $h_j = 0\ \forall j \neq i$. Allora $B = \{\underline{v}_1, ..., \underline{v}_{n-k}\}$ è una base di $N(A)$

Basi dello spazio delle colonne Sia A una matrice $m \times n$ a coefficienti in $K \in \{\mathbb{R}, \mathbb{C}\}$

$$A = [\underline{a}_1 ... \underline{a}_n]$$

$$C(A) = \langle \underline{a}_1, ..., \underline{a}_n \rangle$$

Si applichi una riduzione di Gauss su A, $A \underset{\text{E.G.}}{\rightsquigarrow} U$. Se $\underline{u}_{i_1}, ..., \underline{u}_{i_k}$ sono le colonne dominanti di U, allora $\{\underline{a}_{i_1}, ..., \underline{a}_{i_k}\}$ è una base di $C(A)$
Applicazione:
Verificare che $B = \{\underline{v}_1, ..., \underline{v}_n\}$ sia o meno una base di K^n. NB: Ho n vettori e K^n.
Costruisco la matrice $A = [\underline{v}_1 ... \underline{v}_n]$. Allora $\langle B \rangle = C(A)$. B è insieme di generatori di $K^n \iff \langle B \rangle = C(A) = K^n \iff \dim C(A) = \operatorname{rk} A = n$

Basi ordinate Una base ordinata è una base con l'ordine degli elementi fissato.

Vettore delle coordinate Sia $B = \{\underline{v}_1, ..., \underline{v}_n\}$ una base ordinata di V su K e $\underline{v} \in V$. Il vettore delle coordinate di $\underline{v}$ rispetto a B è il vettore:

$$C_B(\underline{v}) = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \in K^n \mid \underline{v} = \alpha_1\underline{v}_1 + ... + \alpha_n\underline{v}_n = \sum_{i=1}^{n} \alpha_i\underline{v}_i$$

Mappa delle coordinate Sia V uno spazio vettoriale su K. Fissata una base ordinata $B = \{\underline{v}_1, ..., \underline{v}_n\}$, la mappa delle coordinate è la funzione:

$$\begin{array}{rccc} C_B: & V & \longrightarrow & K^n \\ & \underline{v} & \longmapsto & C_B(\underline{v}) \end{array}$$

Essa ha le seguenti proprietà:

- Conserva la somma $C_B(\underline{v} + \underline{w}) = C_B(\underline{v}) + C_B(\underline{w})$
- Conserva il prodotto per scalari $C_B(\alpha\underline{v}) = \alpha C_B(\underline{v})$
- È suriettiva $\forall y \exists x : y = f(x)$
- È iniettiva $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$

C_B è un isomorfismo tra spazi vettoriali.

Applicazioni lineari Siano V e W due spazi vettoriali su K. Una funzione del tipo $T : V \longrightarrow W$ è un'applicazione lineare se e solo se:

- $T(\underline{v}_1 + \underline{v}_2) = T(\underline{v}_1) + T(\underline{v}_2) \qquad \forall \underline{v}_1, \underline{v}_2 \in V$
- $T(\alpha\underline{v}) = \alpha T(\underline{v}) \qquad \forall \underline{v} \in V, \alpha \in K$

NB: $T(\underline{o}_V) = \underline{o}_W$

Nucleo di un'applicazione lineare Sia $T : V \longrightarrow W$ un'applicazione lineare. Il suo nucleo è l'insieme dei vettori $\underline{v} \in V$ la cui immagine è lo zero di W e si indica con $\mathrm{Ke}\, T$:

$$\mathrm{Ke}\, T = \{\underline{v} \in V \mid T(\underline{v}) = \underline{o}_W\}$$

Immagine di un'applicazione lineare Sia $T : V \longrightarrow W$ un'applicazione lineare. La sua immagine è l'insieme dei valori che può assumere $T(\underline{v})$ e si indica con $\operatorname{Im} T$:

$$\operatorname{Im} T = \{T(\underline{v}) \mid \underline{v} \in V\}$$

Applicazioni lineari iniettive e suriettive Sia $T : V \longrightarrow W$ un'applicazione lineare. T è iniettiva e/o suriettiva se lo è in quanto funzione.
NB: T è iniettiva $\iff \operatorname{Ke} T = \{\underline{o}\}$

Applicazine lineare indotta dalla matrice A Sia A una matrice $m \times n$ su $K \in \{\mathbb{R}, \mathbb{C}\}$. La sua applicazione indotta è la funzione:

$$\begin{array}{rccc} L_A : & K^n & \longrightarrow & K^m \\ & \underline{v} & \longmapsto & L_A(\underline{v}) = A\underline{v} \end{array}$$

- $\operatorname{Ke} L_A = N(A)$
- $\operatorname{Im} L_A = C(A)$

Matrice associata ad una applicazione lineare rispetto a fissate basi su dominio e codominio Siano V e W due spazi vettoriali su K. Sia $T : V \longrightarrow W$ un'applicazione lineare, $B = \{\underline{b}_1, ..., \underline{b}_n\}$ una base di V e $D = \{\underline{d}_1, ..., \underline{d}_m\}$ una base di W. Allora $\exists! \underset{m \times n}{A}$ la matrice associata all'applicazione lineare T rispetto alle basi V e W di dominio e codominio e tale che sia commutativo il diagramma:

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle C_B}\downarrow & & \downarrow{\scriptstyle C_D} \\ K^n & \xrightarrow[L_A]{} & K^m \end{array}$$

Cioé che $C_D \circ T = L_A \circ C_B$, quindi $C_D(T(\underline{v})) = L_A(C_B(\underline{v})) = AC_B(\underline{v})$.

$$\underline{a}_i = A\underline{e}_i = AC_B(\underline{b}_i) = C_D(T(\underline{b}_i))$$

$$A = [C_D(T(\underline{b}_1))...C_D(T(\underline{b}_n))]$$

Matrice di passaggio da una base ordinata ad un'altra È la matrice associata alla funzione identità id_V, ovvero quella funzione tale che $id_V(\underline{v}) =$

$\underline{v}$ $\forall \underline{v} \in V$, e si indica con $M_{B \leftarrow B'}$

$$\begin{array}{ccc} V & \xrightarrow{id_V} & V \\ {\scriptstyle C_{B'}}\downarrow & & \downarrow{\scriptstyle C_B} \\ K^n & \xrightarrow[L_{M_{B \leftarrow B'}}]{} & K^n \end{array}$$

$$M_{B \leftarrow B'} = [C_B(\underline{b'}_1)...C_B(\underline{b'}_n)]$$
$$M_{B \leftarrow B'} = M^{-1}_{B' \leftarrow B}$$

1.4 Spazi metrici

Norme Una norma è una funzione $\|\cdot\|$ che gode delle seguenti proprietà:

- $\|\underline{v}\| \geq 0 \ \forall \underline{v} \in V$ e $\|\underline{v}\| = 0 \iff \underline{v} = \underline{o}$
- $\|\alpha \underline{v}\| = |\alpha| \|\underline{v}\| \ \forall \underline{v} \in V, \forall \alpha \in K$
- $\|\underline{v} + \underline{w}\| \leq \|\underline{v}\| + \|\underline{w}\| \ \forall \underline{v}, \underline{w} \in V$ (disuguaglianza triangolare)

Alcune norme diffuse:

- Norma euclidea:
$$\begin{array}{rccc} \|\cdot\|_2 : & V & \longrightarrow & \mathbb{R} \geq 0 \\ & \underline{v} & \longmapsto & \sqrt{\underline{v}^H \underline{v}} \end{array}$$
- Norma taxi-driver o di Manhattan:
$$\begin{array}{rccc} \|\cdot\|_1 : & \mathbb{C}^n & \longrightarrow & \mathbb{R} \geq 0 \\ & \underline{v} & \longmapsto & |v_1| + ... + |v_n| \end{array}$$
- Norma infinito (?):
$$\begin{array}{rccc} \|\cdot\|_\infty : & \mathbb{C}^n & \longrightarrow & \mathbb{R} \geq 0 \\ & \underline{v} & \longmapsto & \max(|v_1|, ..., |v_n|) \end{array}$$

Prodotto scalare Un prodotto scalare o interno di uno spazio vettoriale V su K è una funzione del tipo:

$$(\cdot \mid \cdot) : V \times V \longrightarrow K$$

che soddisfa le seguenti proprietà:

- $(\underline{v} \mid \underline{w}) = \overline{(\underline{w} \mid \underline{v})}$
- $(\underline{v} \mid \alpha \underline{w} + \beta \underline{z}) = \alpha(\underline{v} \mid \underline{w}) + \beta(\underline{v} \mid \underline{z})$
- $(\underline{v} \mid \underline{v}) \in \mathbb{R} > 0$ se $\underline{v} \neq 0$ e $(\underline{o} \mid \underline{o}) = 0$

Prodotto scalare canonico Il prodotto scalare canonico è definito come $(\underline{v} \mid \underline{w}) = \underline{v}^H \underline{w}$

Spazio metrico Uno spazio vettoriale su cui è definito un prodotto scalare si chiama spazio metrico rispetto a questo prodotto.

Norma indotta Dato uno spazio vettoriale V su K, con un prodotto scalare $(\ \cdot \mid \cdot\ )$, si può definire una norma indotta $\|\cdot\|$ come:

$$\begin{array}{rccc} \|\cdot\|_\infty : & V & \longrightarrow & \mathbb{R} \geq 0 \\ & \underline{v} & \longmapsto & \sqrt{(\underline{v} \mid \underline{v})} \end{array}$$

Nel caso si consideri il prodotto scalare canonico, allora la media indotta corrisponde alla norma euclidea

Angolo tra due vettori in uno spazio metrico Dato uno spazio vettoriale V su K, con un prodotto scalare $(\ \cdot \mid \cdot\ )$ e media indotta $\|\cdot\|$, il coseno dell'angolo $\underline{v\hat{w}}$ tra due vettori $\underline{v}$ e $\underline{w}$ non nulli è definito come:

$$\cos \underline{v\hat{w}} = \frac{(\underline{v} \mid \underline{w})}{\|\underline{v}\|\|\underline{w}\|} \quad \forall \underline{v} \neq \underline{o} \neq \underline{w}, \underline{v}, \underline{w} \in V$$

Vettori ortogonali Dato uno spazio vettoriale V su K, con un prodotto scalare $(\ \cdot \mid \cdot\ )$ e media indotta $\|\cdot\|$, due vettori $\underline{v}$ e $\underline{w}$ sono ortogonali se e solo se $\cos \underline{v\hat{w}} = 0 \iff (\underline{v} \mid \underline{w}) = 0$, e si scrive $\underline{v} \perp \underline{w}$.
NB: $(\underline{o} \mid \underline{v}) = (\underline{v} \mid \underline{o}) = 0 \quad \forall \underline{v} \in V$

Insieme di vettori ortogonale Un insieme di vettori si dice ortogonale se sono a due a due ortogonali

Normalizzare un vettore Dato un vettore $\underline{v}$, normalizzarlo significa considerare il vettore $\underline{z} = \frac{\underline{v}}{\|\underline{v}\|}$, tale che $\|\underline{z}\| = 1$

Insieme di vettori ortonormale Un insieme di vettori si dice ortonormale se è ortogonale e tutti i suoi vettori hanno norma uguale a 1.

Insieme di generatori ortogonale È un insieme di generatori che è anche un insieme ortogonale

Insieme di generatori ortonormale È un insieme di generatori che è anche un insieme ortonormale

Algoritmo di Gram Schmidt (G.S.) Dato uno spazio vettoriale V su K, con un prodotto scalare $(\cdot \mid \cdot)$ e media indotta $\|\cdot\|$, sia $S = \{\underline{v}_1, ..., \underline{v}_n\}$ un insieme di generatori di V. L'algoritmo permette di costruire un insieme di generatori ortogonali di V a partire da S.
$S_0 = \{\underline{u}_1, ..., \underline{u}_n\}$ è l'insieme di generatori ortogonali di V, ed i suoi elementi sono calcolati nel seguente modo:

$$\underline{u}_j = \underline{v}_j - \sum_{i=1}^{j-1} \alpha_{ij} \underline{u}_i$$

Dove α_{ij} è definito come:

$$\alpha_{ij} = \begin{cases} \underline{o} & \text{se } \underline{u}_i = \underline{o} \\ \frac{(\underline{u}_i \mid \underline{v}_j)}{(\underline{u}_i \mid \underline{u}_i)} & \text{se } \underline{u}_i \neq \underline{o} \end{cases}$$

Complemento ortogonale di un sottospazio U di uno spazio metrico V Sia V uno spazio metrico su K con un prodotto scalare $(\cdot \mid \cdot)$ e $U \leq V$, il complemento ortogonale $U^\perp$ di U è l'insieme di tutti i vettori di V che sono ortogonali a tutti i vettori di U.

$$U^\perp = \{\underline{v} \in V \mid (\underline{u} \mid \underline{v}) = 0 \ \forall \underline{u} \in U\}$$

NB1: Sia $\{\underline{u}_1, ..., \underline{u}_k\}$ un insieme di generatori di U. Allora:

$$U^\perp = \{\underline{v} \in V \mid (\underline{u}_i \mid \underline{v}) = 0 \ \forall i = 1, ..., k\}$$

NB2: $U \cap U^\perp = \{\underline{o}\}$ e $U \oplus U^\perp = V$, quindi $\dim U^\perp = \dim V - \dim U$

Calcolo del complemento ortogonale Sia $V \in \{\mathbb{R}^n, \mathbb{C}^n\}$ e $U \leq V$. Se $U = \langle \underline{u}_1, ..., \underline{u}_k \rangle$ allora posso costruire $A = [\underline{u}_1 ... \underline{u}_k]$ e si può provare che $U^\perp = C(A)^\perp = N(A^H)$

Proiezione ortogonale Sia V uno spazio metrico su K con un prodotto scalare $(\cdot \mid \cdot)$ e $U \leq V$. Allora:

$$\forall \underline{v} \in V \ \exists! \ \underline{u} \in U \ \exists! \ \underline{w} \in U^\perp \mid \underline{v} = \underline{u} + \underline{w}$$

Tale $\underline{u} = P_U(\underline{v})$ si chiama proiezione ortogonale di $\underline{v}$ su U. Se $\{\underline{u}_1^*, ..., \underline{u}_k^*\}$ è una base ortonormale di U, allora si può esprimere $P_U(\underline{v})$ come:

$$P_U(\underline{v}) = \sum_{i=1}^{k} (\underline{u}_i^* \mid \underline{v}) \underline{u}_1^*$$

Matrici di proiezione Sia V uno spazio metrico su K con un prodotto scalare $(\ \cdot\ |\ \cdot\ )$, $U \leq V$ e $\{\underline{u}_1^*, ..., \underline{u}_k^*\}$ una base ortonormale di U. Allora si possono definire le matrici $\underset{n\times k}{Q} = [\underline{u}_1^* ... \underline{u}_k^*]$ e $\underset{n\times n}{P} = QQ^H$. La matrice P si chiama matrice di proiezione di V su U ed è tale che $P_U(\underline{v}) = P\underline{v}$. Inoltre si può provare che la matrice di proiezione di $U^\perp$ è $I_n - P$.

1.5 Determinanti

Calcolo di determinanti Sia $A = (a_{ij})$ una matrice quadrata $n \times n$. Nel caso in cui $n = 1$ allora il determinante è $\det A = a_{11}$. In caso $n \neq 1$ viene definita C_{ij} come la matrice che si ottiene da A togliendo la i-esima riga e la j-esima colonna e $A_{ij} = (-1)^{i+j} \det C_{ij}$. Allora lo sviluppo del determinante di A rispetto alla i-esima riga è:

$$\det A = \sum_{j=1}^{n} a_{ij} A_{ij} = [a_{i1} ... a_{in}] \begin{bmatrix} A_{i1} \\ \vdots \\ A_{in} \end{bmatrix}$$

Lo sviluppo del determinante di A rispetto alla j-esima colonna invece è:

$$\det A = \sum_{i=1}^{n} a_{ij} A_{ij} = [a_{1j} ... a_{nj}] \begin{bmatrix} A_{1j} \\ \vdots \\ A_{nj} \end{bmatrix}$$

Si può dimostrare che lo sviluppo del determinante di A rispetto la i-esima riga e rispetto alla j-esima colonna sono sempre uguali tra di loro.

Proprietà dei determinanti

- $\det \overline{A} = \overline{\det A}$
- $\det A^T = \det A$
- $\det A^H = \overline{\det A}$
- $\det(AB) = \det(A) \det(B)$
- A è non singolare $\iff \det A \neq 0$
- Se $\exists A^{-1}$ allora $\det(A^{-1}) = \frac{1}{\det A}$

Determinanti di matrici triangolari Il determinante di una matrice triangolare è il prodotto dei valori della diagonale. Nel caso particolare di αI_n, il determinante è $\det \alpha I_n = \alpha^n$

1.6 Autosistemi

Autovalori, autospazi e autovettori Sia A una matrice quadrata $n \times n$ su K e $\lambda \in K$. Viene definita la funzione:

$$E_A(\lambda) = \{\underline{v} \in K^n \mid A\underline{v} = \lambda\underline{v}\} = N(A - \lambda I_n)$$

Se $E_A(\lambda) \neq \{\underline{o}\}$ allora λ è un autovalore di A, $E_A(\lambda)$ si chiama autospazio di A relativo all'autovalore λ e ogni elemento di $E_A(\lambda) \setminus \{\underline{o}\}$ si chiama autovettore di A relativo all'autovalore λ.

Spettro di una matrice L'insieme di tutti gli autovalori di una matrice A si chiama spettro e si indica con $\operatorname{Spec} A$

Molteplicità geometrica di un autovalore La molteplicità geometrica di un autovalore λ di una matrice A si indica con $\mathrm{d}(\lambda)$ ed è uguale alla dimensione dell'autospazio relativo a λ.

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

Equazione e polinomio caratteristici di una matrice 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 invece:

$$P_A(x) = \det(A - xI_n) = 0$$

Calcolo di autovalori Sia A una matrice quadrata $n \times n$ su K e $\lambda \in K$. λ è un autovalore di A se e solo se:

$$\begin{aligned}
& E_A(\lambda) \neq \{\underline{o}\} \\
\iff\ & N(A - \lambda I_n) \neq \{\underline{o}\} \\
\iff\ & \dim(N(A - \lambda I_n)) \neq 0 \\
\iff\ & n - \operatorname{rk}(A - \lambda I_n) \neq 0 \\
\iff\ & \operatorname{rk}(A - \lambda I_n) < n \\
\iff\ & A - \lambda I_n \text{ non ha inversa} \\
\iff\ & \det(A - \lambda I_n) = 0 \\
\iff\ & P_A(\lambda) = 0
\end{aligned}$$

Si possono quindi trovare tutti gli autovalori di A risolvendo l'equazione caratteristica di A.

Autovalori di una matrice triangolare Gli autovalori di una matrice triangolare (superiore e/o inferiore) sono i valori della sua diagonale.

Molteplicità algebrica di un autovalore Sia A una matrice $n \times n$ e $\operatorname{Spec} A = \{\lambda_1, ..., \lambda_k\}$. Allora:

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

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

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

Relazione molteplicità algebrica e geometrica Sia A una matrice $n \times n$ e λ un autovalore di A. Sia $d(\lambda)$ la molteplicità geometrica di λ e $m(\lambda)$ la molteplicità algebrica. Allora:

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

Ricordarsi che $m(\lambda) = 1 \implies d(\lambda) = 1$

Indipendenza di autospazi distinti Sia A una matrice $n \times n$ e $\operatorname{Spec} A = \{\lambda_1, ..., \lambda_k\}$. Allora:

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

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

Matrici simili Siano A e B due matrici $n \times n$. Esse si dicono simili se $\exists S$ tale che $A = SBS^{-1}$. Se A e B sono simili allora godono di queste proprietà:

- $P_A(x) = P_B(x)$
- $\operatorname{Spec} A = \operatorname{Spec} B$
- $\lambda \in \operatorname{Spec} A$ ha la stessa molteplicità algebrica e geometrica di $\lambda \in \operatorname{Spec} B$.
- Se $\underline{v} \in E_B(\lambda)$ allora $S\underline{v} \in E_A(\lambda)$

Matrici diagonalizzabili Una matrice A si dice diagonalizzabile se $\exists D$ una matrice diagonale simile ad A. Cioé se $\exists S$ invertibile e $\exists D$ diagonale tali che $A = SDS^{-1}$

Diagonalizzare una matrice Sia A una matrice $n \times n$ e $\lambda_1, ..., \lambda_k$ i suoi autovalori. Sia m_i la molteplicità algebrica e d_i la molteplicità geometrica di λ_i. A è diagonalizzabile $\iff m_i = d_i \ \forall i = 1, ..., k$.

Se A è diagonalizzabile allora bisogna trovare due matrici D diagonale e S invertibile tali che $A = SDS^{-1}$.

D è una matrice diagonale che ha come valori della sua diagonale gli autovalori di A ripetuti con la loro molteplicità. Questo perché A e D hanno gli stessi autovalori con la loro molteplicità, e gli autovalori di una matrice diagonale sono i valori della sua diagonale.

Per trovare S invec chiamo B_i una base di $E_A(\lambda_i)$. Posso costruire S in modo tale che se la j-esima colonna di D contiene λ_i allora la colonna j di S è uguale ad un elemento della base B_i, e senza ripetere elementi di B_i.

Matrici unitarie Una matrice U si dice unitaria se $U^{-1} = U^H$

Matrici ortogonali Una matrice U si dice ortogonale se $U^{-1} = U^T$

Matrici unitariamente diagonalizzabili Una matrice A si dice unitariamente diagonalizzabile se $\exists U$ unitaria e $\exists D$ diagonale tali che $A = UDU^H = UDU^{-1}$

Matrici normali Una matrice A si dice normale se $AA^H = A^HA$

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

Calcolo di una diagonalizzazione unitaria Sia A una matrice unitariamente diagonalizzabile, quindi $\exists U$ unitaria e $\exists D$ diagonale tali che $A = UDU^H$. D si ottiene con lo stesso procedimento che si applica ad una matrice diagonalizzabile. U invece si trova allo stesso modo ma prendendo basi ortonormali Q_i degli autospazi di A. Inoltre valgono le seguenti proprietà:

- $Q_i^HQ_i = I_{m_i} \ \forall i = 1, ..., k$
- $U^HU = I_n \implies U^H = U^{-1}$
- $P_i = Q_iQ_i^H$ è la matrice di proiezione di $\mathbb{C}^n$ su $E_A(\lambda_i)$

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:

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

Calcolo delle matrici di proiezione nel caso $k = 2$ Sia A una matrice unitariamente diagonalizzabile e siano λ_1 e λ_2 i suoi autovalori. Allora $E_A(\lambda_1) = E_A(\lambda_2)^{\perp}$ e $E_A(\lambda_2) = E_A(\lambda_1)^{\perp}$. Ne segue quindi che $P_1 = I_n - P_2$ e $P_2 = I_n - P_1$. Si può quindi evitare di trovare entrambe le basi ortonormali ma soltando una delle due, possibilmente quella con meno elementi perché richiede meno calcoli.

Teorema 1 *Data una matrice A hermitiana, cioé con $A = A^H$, allora tutti i suoi autovalori sono reali ed essa è unitariamente diagonalizzabile.*

Teorema 2 *Data una matrice A reale. $A = A^T$ se e solo se $\exists U$ ortogonale reale e $\exists D$ diagonale reale tali che $A = UDU^T$. In particolare per la parte $\Longleftarrow$ è richiesto solo che $A = UDU^T$ e D diagonale.*

2 Matematica Discreta

2.1 Grafi

Definizione Un grafo non orientato $G(V, E)$ è composto da un insieme di vertici o nodi V e un insieme di archi, ovvero coppie non ordinate di vertici, E.

Estremi di un arco Gli estremi di un arco sono i 2 vertici della coppia.

Archi incidenti Un arco è incidente ad un vertice se esso è un estremo dell'arco.

Vertici adiacenti Due vertici sono adiacenti se c'è un arco che li ha come estremi.

Grado di un vertice Il grado di un vertice v è il numero di archi incidenti in quel vertice e si indica con $d(v)$

Proprietà base di un grafo

- La somma dei gradi dei vertici è uguale a 2 volte il numero degli archi

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

- Ogni grafo ha un numero pari di vertici con grado dispari.
- Ogni grafo ha massimo $\binom{n}{2} = \frac{n(n-1)}{2}$ archi, dove $n = |V|$

Cammini Un cammino è una sequenza di vertici **distinti** dove ogni coppia consecutiva di vertici è adiacente.

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

Grafi connessi Un grafo si dice connesso se per ogni coppia di vertici esiste un cammino che li collega.

Percorsi 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 3 *Dato un percorso con le estremità distinte v_1 e v_n, esiste un cammino da v_1 a v_n.*

Teorema 4 *Ogni percorso chiuso di lunghezza dispari contiene un ciclo di lunghezza dispari.*

Grafi completi Un grafo si dice completo se ogni coppia di vertici è adiacente. Il grafo completo di n vertici si indica con K_n.

Un grafo completo di n vertici ha $\frac{n(n-1)}{2}$ archi.

Grafi n-regolare Un grafo si dice n-regolare se ogni vertice ha grafo n, in particolare i grafi 3-regolari si chiamano cubici.

Grafi semplici Un grafo si dice semplice se c'è al massimo un arco tra due vertici e non ci sono archi con estremità coincidenti.

Multigrafi Un grafo si chiama multigrafo se può avere archi paralleli e cappi.

Grafi orientati Un grafo si dice orientato se gli archi sono espressi come coppie **ordinate** di vertici.

Grafi orientati semplici Un grafo si dice orientato semplice se è orientato e non sono presenti archi paralleli o cappi. Il numero massimo di archi è $n(n-1)$ dove $n = |V|$.

Cammini orientati Un cammino orientato è una sequenza ordinata di vertici distinti dove ogni coppia consecutiva di vertici è adiacente.

Grafi fortemente connessi Un grafo fortemente connesso è un grafo in cui per ogni coppia di vertici esiste un cammino orientato che li collega.

Circuiti o cicli orientati Un circuito è un cammino orientato dove il primo e l'ultimo vertice sono coincidenti.

Grado entrante Il grado entrante di un vertice v è il numero di archi che terminano in questo vertice e si indica con $d^{in}(v)$.

Grado uscente Il grado uscente di un vertice v è il numero di archi che partono da questo vertice e si indica con $d^{out}(v)$.

Teorema 5 *Per ogni grafo orientato $D(V, A)$ vale la seguente relazione:*

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

Tornei Un torneo è un grafo orientato semplice dove per $\forall v, u$ vertici esiste esattamente uno tra gli archi uv e vu.

Matrice in incidenza vertici-archi La matrice di incidenza vertici-archi di un grafo è una matrice con tante righe quanti i vertici e tante colonne quanti gli archi.

Nel caso di un grafo non orientato, ogni colonna presenta un 1 sulle righe dei suoi estremi.

Nel caso di un grado orientato ogni colonna presenta un 1, che rappresenta il vertice di partenza, e un -1, che rappresenta quello di arrivo.

Matrice di incidenza vertici-vertici La matrice di incidenza vertici-vertici esiste solo per grafi non orientati semplici e presenta un 1 in un cella se e solo se c'è un arco che collega i 2 vertici rappresentati dalla riga e dalla colonna.

Grafo complementare Dato un grafo $G(V, E)$, il suo complementare è il grafo $GC(V, EC)$ tale che $EC = \{v_i v_j \mid v_i v_j \notin E\}$

Grafi bipartiti Un grafo $G(V, E)$ si dice bipartito se i suoi vertici sono partizionabili in due insiemi U e W tali per cui ogni arco ha un estremo in U e uno in W e si può scrivere $G(U, W; E)$. Il massimo numero di archi è $|U||W|$.

Grafi bipartiti completi Un grafo bipartito si dice completo se ogni vertice dell'insieme U è adiacente ad ogni vertice dell'insieme W e si indica con K_{n_1,n_2} dove $n_1 = |U|$ e $n_2 = |W|$.

Condizione necessaria e sufficiente affinché un grafo sia bipartito Un grafo $G(V, E)$ è bipartito se e solo se non contiene un ciclo di lunghezza dispari.

Grafi isomorfi Due grafi si chiamano isomorfi se sono differenti solo nel modo in cui vengono disegnati. Più formalmente $G(V, E)$ e $G'(V', E')$ sono isomorfi se e solo se c'è una biezione f che va da V in V' e preserva le adiacenze, ovvero che se uv è un arco di G allora $f(u)f(v)$ è un arco di G'.

Stabilire isomorfismo tra grafi Stabilire isomorfismo tra due grafi ($G \simeq G'$) è un problema difficile. Esso richiede le seguenti condizioni necessarie, ma non sufficienti:

- G e G' hanno lo stesso numero di vertici
- G e G' hanno lo stesso numero di archi
- G e G' hanno lo stesso numero di vertici con lo stesso grado
- I complementari di G e G' devono essere a loro volta isomorfi
- G e G' hanno gli stessi sottografi indotti da vertici corrispondenti.

Vertici connessi Dato un grafo $G(V, E)$, due vertici u e v sono connessi se esiste un cammino con estremità u e v. Questa relazione gode delle seguenti proprietà:

- Riflessività: u è connesso a sé stesso
- Simmetria: u è connesso a v se e solo se v è connesso a u
- Transitività: se u è connesso a t e t è connesso a v allora u è connesso a v

Componenti connesse Dato un grafo $G(V, E)$ esiste una partizione di V in $V_1, ..., V_k$ tale che u e v sono connessi se e solo se sono nello stesso insieme V_i. Gli insiemi $V_1, ..., V_k$ si chiamano componenti connesse di G. G è un grafo connesso se e solo se ha una sola componente connessa. Con $\gamma(G)$ si indica il numero di componenti connesse di G.

Tagli Sia $G(V, E)$ un grafo e $S \subseteq V$, allora il taglio associato a S è:

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

Ovvero è l'insieme degli archi con una sola estremità in S. Si dice che $\delta(S)$ separa due nodi se uno sta in S e l'altro no. Notare come dato $\overline{S} = V \setminus S$ allora $\delta(S) = \delta(\overline{S})$.

Teorema 6 *Dato $\delta(S)$ un taglio che separa u e v e P un cammino tra u e v allora $\delta(S)$ e P hanno almeno un arco in comune, ovvero $|P \cap \delta(S)| \geq 1$*

Teorema 7 *Dato un grafo $G(V, E)$ e due nodi u e v, u e v stanno nella stessa componente connessa di G se e solo se non esistono tagli $\delta(S) = \emptyset$ che separano u e v*

Algoritmo per trovare una componente connessa Dato un grafo $G(V, E)$ e un nodo x per trovare una componente connessa si inizia con un insieme C contenente x. Per ogni elemento non esaminato u di C si aggiungono a C i nodi adiacenti ad u e lo si marca esaminato. Si continua finché ogni nodo di C è esaminato, a quel punto C è la componente connessa di G contenente x. Notare come $\delta(C) = \emptyset$

Connettività sugli archi Dato un grafo $G(V, E)$, l'arcoconnettività fra due nodi u e v è la cardinalità minima (ovvero il numero minimo di elementi) di un taglio che separa u e v e si indica con $k^E_{uv}(G)$.

Teorema 8 *$k^E_{uv}(G)$ è il numero minimo di archi da togliere affinché u e v si trovino in componenti connesse distinte.*

Teorema 9 *$k^E_{uv}(G)$ è il numero massimo di cammini con estremità u e v che non hanno archi in comune.*

Arcoconnettività di un grafo L'arcoconnettività di un grafo è il numero minimo di archi da togliere affinché G sia disconnesso e si indica con $k^E(G) = \min k^E_{uv}(G)$

Connettività sui vertici Dato un grafo $G(V, E)$ connesso, semplice e non completo la connettività sui vertici è il numero minimo di vertici la cui rimozione trasforma G in un grafo non connesso e si indica con $k(G)$. Per convenzione se K_n è un grafo completo allora $k(K_n) = n - 1$.

Teorema 10

$$k(G) \leq k^E(G) \leq d^{min}(G)$$

Dove $d^{min}(G)$ è il grado minimo di un vertice di G. Nel caso particolare in cui G sia un grafo completo con n vertici allora $k(G) = k^E(G) = d^{min}(G) = n-1$

Separatori Dato un grafo $G(V, E)$ un separatore di G è un insieme $S \subseteq V$ tale che $G \setminus S$ sia un grafo non connesso.

Cardinalità minima di separatori Dato un grafo $G(V, E)$ e due vertici u e v non adiacenti, $k_{uv}(G)$ è la cardinalità minima (ovvero il numero minimo di elementi) di un separatore S tale che u e v sono in componenti connesse distinte di $G \setminus S$.

Teorema 11

$$k(G) = \min k_{uv}(G)$$

Teorema 12 *Dato un grafo $G(V, E)$, u e v due nodi non adiacenti, P un cammino con estremità u e v e S un separatore con u e v in componenti connesse distinte di $G \setminus S$ allora S contiene almeno un vertice intermedio di P.*

Teorema 13 *$k_{uv}(G)$ è il numero massimo di cammini internamente disgiunti con estremità u e v.*

Foreste Una foresta è un grafo senza cicli. Se n è il numero di componenti connesse di una foresta $F(V, E)$ allora vale la relazione $|E| = |V| - n$

Alberi Un albero è una foresta connessa. Dato un albero $T(V, E)$ vale la relazione $|E| = |V| - 1$

Teorema 14 *Dato un albero $T(V, E)$, se esso ha almeno 2 nodi, allora ha almeno 2 nodi di grado 1.*

Teorema 15 *Le seguenti affermazioni sono equivalenti:*

- *T è un albero, ovvero è un grafo senza cicli e connesso*
- *$\forall x, y \in V$ nodi distinti $\exists!$ il cammino che li collega*
- *T è minimamente connesso, ovvero la rimozione di un qualunque arco lo disconnette, ovvero ogni arco è un taglio.*

Algoritmo di Kruskal Dato un grafo $G(V, E)$ connesso in cui ad ogni arco è associato un peso, l'algoritmo di Kruskal permette di ottenere l'albero di peso minimo che è anche un sottografo di G. Si inizia ponendo $S = \{\}$. Poi per ogni arco, presi in ordine di peso, lo si aggiunge ad S se e solo se non si creano cicli nel grafo $T(V, S)$. Quando si hanno considerati tutti gli archi, $T(V, S)$ è l'albero cercato.

Teorema 16 *Dato un grafo $G(V, E)$ non orientato semplice e connesso, se $|E| = |V| - 1$ allora esso è un albero.*

Algoritmo di Dijkstra Dato un grafo $G(V, E)$ in cui ad ogni arco uv è associato un peso $l(uv)$, l'algoritmo di Dijkstra permette di trovare la distanza tra un nodo r e tutti gli altri. Si inizia ponendo $d(r) = 0$, $d(v) = \infty \ \forall v \in V \backslash \{r\}$, $i = 0$ e $S_0 = \{r\}$. Per ogni $v \in V \backslash S_i$ si pone $d(v) = \min\{d(u) + l(uv)\}$. Sia poi u il vertice di $V \setminus S_i$ per cui sia minimo $d(u)$. Si ponga $i = i + 1$ e $S_i = S_{i-1} \cup \{u\}$. Ci si ferma quando $i = |V| - 1$

Grafi planari Un grafo si definisce planare se è possibile disegnarlo su un piano senza intersezioni tra gli archi. Tale disegno si dice rappresentazione piana del grafo.

Minori di un grafo Un minore di un grafo $G(V, E)$ è un grafo $G'(V', E')$ che si ottiene da G per:

- Contrazione di archi (dato arco uv fa coincidere i vertici u e v)
- Rimozione di archi
- Rimozione di vertici isolati

Teorema 17 *Dato un grafo G planare e G' minore di G, allora anche G' è planare.*

Teorema 18 *Un grafo G è planare se e solo se non contiene $K_{3,3}$ o K_5 come minori.*

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

Metodo del cerchio e delle corde Il metodo del cerchio e delle corde permette di stabilire se un un grafo è planare o meno con il prerequisito di poter individuare un ciclo hamiltoniano. Si disegna quindi il ciclo hamiltoniano e si disegna un arco qualsiasi del grafo dentro o fuori al cerchio. Tutti gli archi che lo incrocierebbero vanno disegnati nella parte opposta. Se si riesco a disporre tutti gli archi allora il grafo è planare, in caso contrario non lo è.

Formula di Eulero Dato $G(V, E)$ un grafo connesso e planare con r regioni allora vale la relazione $r = |E| - |V| + 2$. Se G è semplice e planare allora valgono i seguenti corollari:

- Se $|V| \geq 3$ allora vale anche $|E| \leq 3|V| - 6$
- Se G è bipartito allora vale anche $|E| \leq 2|V| - 4$
- G contiene almeno un vertice con grado ≤ 5

Cicli hamiltoniani Un ciclo si dice hamiltoniano se visita ogni vertice esattamente una volta. Se un grafo ha un ciclo hamiltoniano allora si dice hamiltoniano.
Condizioni necessarie affinché un grafo $G(V, E)$ sia hamiltoniano:

- $d(v) \geq 2 \ \forall v \in V$
- $K(G) \geq 2$
- $|S| \geq \gamma(G \setminus S) \ \forall S \subseteq V$

Teorema 19 *Teorema di Dirac: Dato un grafo $G(V, E)$ semplice con $n > 2$ vertici. Se $d(v) \geq \frac{n}{2} \ \forall v \in V$ allora G è un grafo hamiltoniano.*

Ricerca di un grafo hamiltoniano

- Se $K(G) \leq 1$ non c'è
- Se $d(v) = 2$ allora entrambi gli archi incidenti in v fanno parte del ciclo
- Un ciclo hamiltoniano non può contenere sottocicli propri
- Se sono già stati individuati 2 archi incidenti in v allora tutti gli altri archi incidenti in v vanno scartati

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

Teorema 20 *Teorema di Eulero: un grafo $G(V, E)$ è euleriano se e solo se è connesso e ogni vertice ha un grado pari.*

Numero arcromatico Il numero arcromatico $X'(G)$ di un grafo $G(V, E)$ è il minimo numero di colori necessari a colorare gli archi di G affinché archi con estremi in comune abbiano colori diversi.

Teorema 21 *Se $G(V, E)$ è un grafo bipartito allora $X'(G) = d^{max}(G)$*

Teorema 22 *Teorema di Vizing: se $G(V, E)$ è un grafo semplice allora vale:*

$$d^{max}(G) \leq X'(G) \leq d^{max}(G) + 1$$

Numero cromatico Il numero cromatico $X(G)$ di un grafo $G(V, E)$ è il numero minimo di colori necessari a colorare i vertici di G affinché vertici adiacenti abbiano colori diversi.

Teorema 23 *Se $G(V, E)$ è un grafo allora $X(G) \leq d^{max}(G) + 1$*

Teorema 24 *Se $G(V, E)$ è un grafo planare allora $X(G) \leq 4$. La dimostrazione necessità di un calcolatore, è però possibile dimostrare a mano che $X(G) \leq 6$.*

Colorazione sequenziale Si ordinano i colori e i vertici. Per ogni vertici gli si assegna il primo colore che non è già stato assegnato ai precedenti vertici a cui è adiacente. Questo metodo permette di colorare un grafo ma non garantisce che il numero di colori usato sia minimo.

2.2 Combinatoria

Principio di addizione Se si hanno n insiemi tali che:

- L'insieme i ha r_i oggetti differenti
- Gli insiemi sono disgiunti a due a due

Allora il numero il possibilità per scegliere un oggetto da essi è $r_1 + r_2 + ... + r_n$

Principio di moltiplicazione Se si ha una procedura con n fasi tali che:

- La fase i ha r_i possibili esiti
- Il numero di esiti di una fase non è influenzato dagli esiti precedenti
- Tutti i possibili esiti della procedura sono differenti

Allora il numero di possibili esiti è $r_1 \cdot r_2 \cdot ... \cdot r_n$

Permutazioni Una permutazione è una disposizione ordinata degli n oggetti di un insieme. Dati n oggetti distinti il numero delle possibili permutazioni è $P(n, n) = n!$

r-Permutazioni Una r-permutazione è una disposizione ordinata di r degli n oggetti di un insieme. Dati n oggetti distinti il numero delle possibili r-permutazioni è $P(n, r) = \frac{n!}{(n-r)!}$

r-Combinazioni Una r-combinazione è un sottoinsieme o selezione non ordinata di r degli n oggetti di un insieme. Dati n oggetti distinti il numero delle possibili r-permutazioni è $C(n,r) = \frac{n!}{r!(n-r)!} = \binom{n}{r}$

Coefficienti binomiali Un coefficiente binomiale $\binom{n}{k}$ si legge come n su k ed è uguale a $\frac{n!}{k!(n-k)!}$ se $k \leq n$ o 0 se $n < k$, con entrambi n e k numeri naturali.

Teorema 25 *Teorema binomiale:*

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

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

Triangolo di Tartaglia o Pascal Il $(k+1)$-esimo elemento della $(n+1)$-esima riga del triangolo di Pascal o Tartaglia è il numero $\binom{n}{k}$.

Identità binomiali

- $\binom{n}{k} = \binom{n}{n-k}$ con $k \leq n$
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ con $k \leq n$
- $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{n-k}$ con $m \leq k \leq n$

Altre relazioni sono:

- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
- $\binom{n+1}{r+1} = \sum_{k=r}^{n} \binom{k}{r} = \binom{r}{r} + \binom{r+1}{r} + ... + \binom{n}{r}$
- $\binom{n}{k} = \binom{n-2}{k} + \binom{n-2}{k-2} + 2\binom{n-2}{k-1}$

Disposizioni con ripetizione Supponiamo di avere n oggetti di k tipi diversi e r_i di tipo i, con $r_1 + ...r_k = n$. Il numero di possibilità è $\binom{n}{r_1}\binom{n-r_1}{r_2}...\binom{r_k}{r_k} = \frac{n!}{r_1!r_2!...r_k!}$

Selezioni con ripetizione Supponiamo di avere r oggetti uguali e vogliamo dividerli in n gruppi. Il numero di possibilità è $\binom{r+n-1}{r}$

Distribuzione di oggetti distinti Supponiamo di avere r oggetti distinti e vogliamo dividerli in n gruppi. Il numero di possibilità è n^r
Supponiamo invece che nell'i-esimo gruppo ci vadano r_i oggetti, con $r_1 + r_2 + ...r_n = r$. Il numero di possibilità è $\binom{n}{r_1}\binom{n-r_1}{r_2}...\binom{r_k}{r_k} = \frac{n!}{r_1!r_2!...r_k!}$

2.3 Relazioni di ricorrenza

Relazioni di ricorrenza Le relazioni di ricorrenza sono formule che esprimono il termine di una successione a_n in funzione dei precedenti termini della successione. La soluzione della relazione è la formula esplicita di a_n che dipende solo da n.

Relazioni lineari omogenee Una relazione di ricorrenza lineare omogenea di ordine r è una relazione di ricorrenza in cui a_n dipende dai precedenti r termini della successione, ovvero $a_{n-1}, a_{n-2}, ..., a_{n-r}$.

$$\begin{cases} a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_r a_{n-r} \\ r \text{ condizioni iniziali} \end{cases}$$

Per risolvere una relazione di questo tipo si pone $a_n = \alpha^n$ e si risolve per α. In particolare si risolve l'equazione $\alpha^r - c_1\alpha^{r-1} - ... - c_r = 0$ che è chiamata equazione caratteristica della relazione. Questa equazione avrà r soluzioni, possibilmente ripetute. $a_n = \alpha^n$ è una soluzione particolare della relazione. Inoltre se α ha molteplicità m allora anche $n^1\alpha^n$, $n^2\alpha^n$, ... e $n^{m-1}\alpha^n$ sono soluzioni particolari della relazione. La soluzione generale della relazione è invece la combinazione lineare di queste soluzioni particolari. Infine con le r condizioni iniziali è possibile determinare gli r coefficienti della combinazione lineare e trovare la soluzione particolare della nostra relazione.

Relazioni lineari non omogenee Una relazione lineare non omogenea di ordine r è una relazione di ricorrenza in cui a_n dipende dai precedenti r termini della successione e da una funzione $f(n)$.

Relazioni lineare non omogenee del primo ordine Una relazione lineare non omogenea del primo ordine è una relazione del tipo:

$$\begin{cases} a_n = ca_{n-1} + f(n) \\ \text{una condizione iniziale } (a_0) \end{cases}$$

Per risolvere una relazione di questo tipo bisogna discutere il parametro c:

- Se $c = 1$ allora la soluzione è $a_n = a_0 + \sum_{k=1}^{n} f(k)$

- Se $c \neq 1$ allora bisogna cercare la soluzione generale dell'equazione lineare omogenea associata (quella senza $f(n)$) e gli si somma una soluzione particolare di quella non omogenea da cercare nella seguente tabella:

$f(n)$	soluzione particolare
d	B
$d \cdot n$	$B_1 \cdot n + B_2$
polinomio di grado m	polinomio di grado m
$e \cdot d^n$ $(d \neq c)$	Bd^n
$e \cdot c^n$	Bnc^n

Relazioni dividi e conquista Una relazione dividi e conquista è una relazione in cui a_n dipende da $a_{\frac{n}{2}}$

$$\begin{cases} a_n = ca_{\frac{n}{2}} + f(n) \\ \text{una condizione iniziale} \end{cases}$$

Anche qui bisogna distinguere diversi casi:

- $c = 1$ e $f(n) = d$: La soluzione generale è $a_n = d\lceil \log_2 n \rceil + A$
- $c = 2$ e $f(n) = d$: La soluzione generale è $a_n = An - d$
- $c = 2$ e $f(n) = dn$: La soluzione generale è $a_n = dn\,(\lceil \log_2 n \rceil + A)$
- $c > 2$ e $f(n) = dn$: La soluzione generale è $a_n = An^{\log_2 c} + \left(\frac{2d}{2-c}\right) n$