Matroide

Nota istorica

Introdotti da Whitney '1935

Sono oggi uno strumento centrale in diverse aree della matematica, in particolare ottimizzazione combitanoria, Geometria e topologia, geometria conversa (lineare), network theory & coding theory.

Gian Carlo Rota: " Anyone who has worked with matroids has come away with the conviction that matroids are one of the most richest and most useful ideas of our days".

Idea: "astrarre" l'idea di indipendenza

- algebra lineare
- lati di un grafo

Bibliografia | Wilson, "Int. to graph theory", ch. 9
Oxley, "Matroid theory"
(Welsh)

ground set

Def Una <u>matroide</u> M è una coppia $M = (E, \mathcal{I})$, dove $E \neq \emptyset$ è un insieme finito, e $\mathcal{I} \subset \mathcal{P}(E)$ è una collezione di sottoinsiemi di E, detti <u>insiemi indipendenti</u>, t.c.

(I1) $\emptyset \in \mathcal{I}$;

(I2) se $I \in \mathcal{I}$ e $I' \subset I \Rightarrow I' \in \mathcal{I}$; (un sottoinsieme di un insieme indipendente è indipendente)

(I3) se I e J sono indipendenti e $|J| > |I|$, allora $\exists\, e \in E$: $e \in J \setminus I$ e $I \cup \{e\} \in \mathcal{I}$.

- Dato $A \subset E$, se $A \notin \mathcal{I}$ diciamo che A è dipendente.

Esempi

1) Matroide ciclica associata a un grafo G, $M(G)$:

- $E = \{e_1, \dots, e_m\}$ lati di G
- $\mathcal{I} \subset \mathcal{P}(E)$ sono gli insiemi di lati di G che non contengono cicli di G.

$M(G)$ è una matroide per l'esercizio 6 del foglio 1.

2) Matroide vettoriale associata a una matrice $A \in M_{m \times n}(\mathbb{K})$ è t.c. $E = \{v_1, \dots, v_n\}$ è l'insieme delle colonne di A e $\mathcal{I}$ è la collezione di insiemi di vettori linearmente indipendenti in $\langle v_1, \dots, v_n \rangle$.

Infatti, (I1) ok

(I2) ok

(I3) Siano $I_1, I_2 \in \mathcal{I}$, con $|I_1| < |I_2|$.

Sia $W = \langle I_1, I_2 \rangle$. Allora $\dim W \geq |I_2|$. (I_2 lin. indep.)

Supp. p.a., che $\forall e \in I_2$, $I_1 \cup \{e\}$ sia dipendente.

Allora $I_2 \subset \langle I_1 \rangle \Rightarrow W = \langle I_1 \rangle$.

$\Rightarrow |I_2| \leq \dim W = |I_1| < |I_2|$ ↯

$\Rightarrow \exists\, e \in I_2 : I_1 \cup \{e\}$ è indipendente, ossia

t.c. $I_1 \cup \{e\} \in \mathcal{I}$.

La matroide (vettoriale) associata a tale matrice A

si denota con $M[A]$.

→ Terminologia "matroid" da Whitney viene da questa situazione.

Esempio se $A = \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array} \in M_{2,5}(\mathbb{R})$

Allora $M[A] = (E, \mathcal{I})$, dove

- $E = \{v_1, v_2, v_3, v_4, v_5\}$

$\mathcal{I} = \{ \emptyset, \{v_1\}, \{v_2\}, \{v_4\}, \{v_5\}, \{v_1, v_2\}, \{v_1, v_5\},$
$\{v_2, v_4\}, \{v_2, v_5\}, \{v_4, v_5\} \}$

Insiemi dipendenti sono

$\{\{v_3\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_3, v_5\}\}$

$\cup \{X \subseteq E : |X| \geq 3\}$.

Sia $M = (E, \mathcal{I})$ una matroide.

<u>Def.</u> Una <u>base</u> di M è un sottoinsieme indipendente massimale.

<u>Lemma</u> Siano B_1 e B_2 basi di una matroide M.
Allora $|B_1| = |B_2|$.

<u>dim</u> E' una conseguenza facile dell'assioma $(\mathcal{I}3)$.
Infatti, supponiamo per assurdo che $|B_2| > |B_1|$.
Allora $(\mathcal{I}3) \Rightarrow \exists\, e \in B_2 : B_1 \cup \{e\} \in \mathcal{I}$, e quindi
B_1 non sarebbe un insieme indipendente massimale. ∎

Sia $\mathcal{B}$ l'insieme delle basi di una matroide M.
Allora $\mathcal{B} \neq \emptyset$ (come conseguenza di $I1$). (B1)

<u>Def</u> Data una matroide M, il <u>rango di M</u> si definisce come $|B|$, dove $B \in \mathcal{B}$ è una qualsiasi base di M.

<u>Lemma</u> $\mathcal{B}$ soddisfa la proprietà seguente:

(B2) Dati $B_1, B_2 \in \mathcal{B}$ e $x \in B_1 - B_2$, $\exists\, y \in B_2 - B_1$ t.c. $(B_1 - x) \cup y \in \mathcal{B}$.

<u>dim</u> $B_1 - x$ e $B_2 \in \mathcal{I}$ e $|B_1 - x| < |B_2|$ (perché $\overset{\text{Lemma}}{|B_1| = |B_2|}$)

$\underset{(I3)}{\Rightarrow}$ $\exists\, y \in B_2 - (B_1 - x) \underset{x \in B_1 - B_2}{=} B_2 - B_1$: $(B_1 - x) \cup y \in \mathcal{I}$

Ma siccome $|(B_1 - x) \cup y| = |B_1| \overset{\text{Lemma}}{\Longrightarrow} (B_1 - x) \cup y$ non può essere prop. contenuto in nessun insieme indipendente $\Rightarrow (B_1 - x) \cup y \in \mathcal{B}$. ∎

Teorema Sia E un insieme e $\mathcal{B} \subset \mathcal{P}(E)$
una colezione di sottoinsiemi di E che soddisfa (B1) e (B2).
Sia $\mathcal{I}$ la colezione dei sottoinsiemi di E che sono contenuti
in un elemento di $\mathcal{B}$. Allora $M = (E, \mathcal{I})$ è una
matroide per la quale $\mathcal{B}$ è la colezione delle basi di M.

oss. Il teorema ci garantisce che la nozione di matroide
si può dare equivalentemente a partire dagli assiomi delle
basi, i.e.:

Def Una matroide è una coppia $M = (E, \mathcal{B})$ dove $\mathcal{B} \subset \mathcal{P}(E)$
è tale che:

(B1) $\mathcal{B} \neq \emptyset$

(B2) se $B_1, B_2 \in \mathcal{B}$ e $x \in B_1 - B_2 \Rightarrow \exists\, y \in B_2 - B_1$:
$(B_1 - x) \cup y \in \mathcal{B}$.

Infatti, in queste condizioni, possiamo definire gli elementi indipendenti $\mathcal{I}$ come i sottoinsiemi di E che sono contenuti in una base $B \in \mathcal{B}$. Dal teorema $\mathcal{I}$ soddisfa (I_1), (I_2) e (I_3), e quindi $\Pi = (E, \mathcal{I})$ è una matroide d'accordo con la def. iniziale.

D'altra parte, se $\Pi = (E, \mathcal{I})$, con $\mathcal{I}$ col. dei sottoinsiemi indipendenti di Π, i.e., con $\mathcal{I}$ che soddisfa $(I1)$, $(I2)$ e $(I3)$, allora l'insieme delle basi di Π soddisfa $(B1)$ e (B_2).

<u>Lemma</u> Se $\mathcal{B} \subset \mathcal{P}(E)$ soddisfa $(B1)$ e $(B2)$, allora $\forall B_1, B_2 \in \mathcal{B}$, $|B_1| = |B_2|$.

<u>dim</u> Supp. p.a. che $B_1 \neq B_2 \in \mathcal{B}$ sono tali che $|B_1| > |B_2|$ con $|B_1 - B_2|$ minimali tra le possibili scelte di tali B_1, B_2.

Sia $x \in B_1 - B_2 (\neq \emptyset)$. Quindi per (B2), $\exists\, y \in B_2 - B_1$:

$(B_1 - x) \cup y \in \mathcal{B}$.

Ha allora $|(B_1 - x) \cup y| = |B_1| > |B_2|$

e $|((B_1 - x) \cup y) - B_2| < |B_1 - B_2|$.

Questo contradisce la scelta di B_1 e B_2, e dimostra il Lemma. $\blacksquare$

<u>dim</u> (del teorema)

È chiaro che $\mathcal{I}$ soddisfa (I1) e (I2).

Vediamo che $\mathcal{I}$ soddisfa anche (I3).

Siano quindi I_1, I_2 : $\begin{cases} I_1 \subset B_1 \in \mathcal{B} \\ I_2 \subset B_2 \in \mathcal{B} \end{cases}$, con $|I_1| < |I_2|$.

Supp. p.a. che $\forall\, e \in I_2 \setminus I_1$, $I_1 \cup e \notin \mathcal{I}$, ossia,

$I_1 \cup e$ non è contenuto in alcun insieme di $\mathcal{B}$.

Supp. che tra tutte le possibili scelte per B_2, scegliamo B_2 in modo che $|B_2 - (I_2 \cup B_1)|$ sia minimale.

Siccome per ogni $e \in I_2 - I_1$, $I_1 \cup e \notin \mathcal{I}$, $e \notin B_1$

$\Rightarrow I_2 - B_1 = I_2 - I_1$. $(\otimes)$

. Vediamo che $B_2 - (I_2 \cup B_1)$ è vuoto. Infatti, se non lo fosse,

$\exists\ x \in B_2 - (I_2 \cup B_1)$.

Per (B2), $\exists\ y \in B_1 - B_2$ t.c. $(B_2 - x) \cup y \in \mathcal{B}$.

Ha allora $|((B_2 - x) \cup y) - (I_2 \cup B_1)| < |B_2 - (I_2 \cup B_1)|$,

il che contraddice la scelta di B_2.

Quindi $B_2 - (I_2 \cup B_1) = \emptyset$

$$\Rightarrow B_2 - B_1 = I_2 - B_1 \overset{(\otimes)}{=} I_2 - I_1.$$

Mostriamo adesso che $B_1 - (I_1 \cup B_2) = \emptyset$.

Infatti, se non fosse così, $\exists\, x \in B_1 - (I_1 \cup B_2)$ e, come prima, anche $y \in B_2 - B_1 : (B_1 - x) \cup y \in \mathcal{B}$.

Ma $I_1 \cup y \subseteq (B_1 - x) \cup y \in \mathcal{B}$, il che contradisce la nostra ipotesi che I_1, I_2 non soddisfano (I3).

$$\Rightarrow B_1 - (I_1 \cup B_2) = \emptyset.$$

$$\Rightarrow B_1 - B_2 = I_1 - B_2 \subset I_1 - I_2$$

Per il Lemma precedente $|B_1| = |B_2| \Rightarrow |B_1 - B_2| = |B_2 - B_1|$

$$\Rightarrow |I_1 - I_2| \geq |B_1 - B_2| = |B_2 - B_1| = |I_2 - I_1|$$

$$\Rightarrow |I_1| \geq |I_2| \quad ⨍$$

Quindi M è una matroide per la quale $\mathcal{B}$ è l'insieme delle basi. ∎

<u>Esempi</u> 1) Se $M = M[A]$ è una matroide vettoriale, una base è un sottoinsieme B di vettori indipendenti di $\{v_1, v_2, \ldots, v_n\} = E$ t.c. $\langle B \rangle = \langle v_1, \ldots, v_n \rangle$.

2) Se $M = M(G)$ è una matroide ciclica associata a un grafo G, una base è un sottoinsieme di lati che forma un sottografo generante, senza cicli e massimale per questa proprietà.

Quindi una base di $M(G)$ è una foresta generante di G.

<u>OSS.</u> Esercizio 4, foglio di esercizi 2, ci garantisce che se prendiamo $M = (E(G), \mathcal{B})$, con $\mathcal{B}$ foreste generanti di G, allora $\mathcal{B}$ soddisfa (B2) (e anche (B1)) ed è quindi una matroide.

Def Sia $M = (E, \mathcal{I})$ una matroide.

Un sottoinsieme di E che è dipendente minimale è detto un circuito o un ciclo di M.

Useremo, data una matroide M, le notazioni:

- $\mathcal{I}(M)$: sottoinsiemi indipendenti
- $\mathcal{B}(M)$: basi di M
- $\mathcal{C}(M)$: circuiti di M.

e $E(M)$: ground set di M.

Oss Se conosciamo i circuiti di una matroide M, allora conosciamo anche gli indipendenti (e le basi): diciamo che $I \subset E$ è un elemento di $\mathcal{I}$ se I non contiene alcun elemento di $\mathcal{C}(M)$.

Esempio Se $M = M(G)$, $\mathcal{C}(M)$ è la collezione dei cicli di G.

Sarà una conseguenza dell'esercizio 10 (foglio 3) che $\mathcal{C}(M)$ soddisfa:

(C1) $\emptyset \notin \mathcal{C}(M)$

(C2) Se C_1 e $C_2 \in \mathcal{C}(M)$ e $C_1 \subseteq C_2 \Rightarrow C_1 = C_2$

(C3) Se C_1 e $C_2 \in \mathcal{C}(M)$, $C_1 \neq C_2$, e $e \in C_1 \cap C_2$, allora $\exists\, C_3 \in \mathcal{C}(M) : C_3 \subseteq (C_1 \cup C_2) - e$.

(circuit elimination axiom).

Inoltre, se $M = (E, \mathcal{C}(M))$ è tale che $\mathcal{C}(M) \subset \mathcal{P}(E)$ soddisfa (C1), (C2) e (C3), allora considerando

$\mathcal{I}(M) = \{ I \subset E : I \not\supset C,\ \forall C \in \mathcal{C}(M) \}$,

allora $(E, \mathcal{I}(M))$ è una matroide (con $\mathcal{I}(M)$ collezione degli indipendenti) e $\mathcal{C}(M)$ è la collezione dei suoi circuiti.

Prop Sia $I \in \mathcal{I}(M)$, la collezione degli indipendenti di una matroide M, e sia $e \in E$ t.c. $I \cup e$ sia dipendente. Allora esiste un <u>unico</u> circuito di M, $C \in \mathcal{C}(M)$, tale che $C \subset I \cup e$ e $e \in C$.

dim

Essendo $I \cup e$ dipendente, chiaramente contiene un circuito C. Inoltre, siccome I è indipendente, C necessariamente contiene e.

Se C' fosse un'altro tale circuito: contenuto in $I \cup e$ e con $e \in C'$, allora per (C3) $(C \cup C') - e$ contiene un circuito. Ma essendo $(C \cup C') - e \subset I$, questo e' un'assurdo poichè I e' indipendente. ∎

<u>Corollario</u> Sia $B \in \mathcal{B}(M)$ una base di una matroide M. Se $e \in E(M) - B$, allora $B \cup e$ contiene un'unico circuito, $C(e,B)$. Inoltre, $e \in C(e,B)$.