Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Magistrale in Matematica

MATROIDI E ALGORITMO GREEDY

Tesi di Laurea

Relatore:
Chiar.ma Prof.ssa MARILENA BARNABEI

Presentata da:
LUCIA DORE

Sessione Unica
Anno Accademico 2019/2020

Indice

Introduzione

Il matematico americano Hassler Whitney nell'articolo del 1935 *On the abstract properties of linear dependence* introdusse per primo il concetto di matroide con l'obiettivo di descrivere una struttura che potesse generalizzare tanto gli spazi vettoriali quanto i grafi. Le quattro definizioni assiomatiche originali proposte da Whitney, basate sulle nozioni di rango, circuito, indipendente e base, sono poi state affiancate nel tempo da numerose altre definizioni, che si dimostrano essere equivalenti, o meglio criptomorfe, tra loro.

Un'interessante proprietà delle matroidi è la relazione che intercorre con l'algoritmo greedy. Un algoritmo greedy ricerca la soluzione ottima di un dato problema di ottimizzazione attraverso la scelta di un ottimo locale ad ogni passo. Il matematico tedesco Richard Rado nel 1957 per primo rilevò come un algoritmo greedy soddisfi il problema analizzato se la struttura sottostante ha forma matroidale. Una generalizzazione di ciò fu fornita nel 1981 da Bernhard Korte e László Lovász attraverso l'introduzione di un nuovo oggetto: il greedoide. Come il nome suggerisce, il greedoide generalizza il concetto di matroide considerando tutte le strutture su cui un algoritmo greedy risulta ottimo, ovvero capace di risolvere il problema di ottimizzazione dato. Dunque tanto i greedoidi quanto le matroidi sono caratterizzati per mezzo dell'algoritmo greedy, ma i primi risolvono problemi di ottimizzazione su funzioni obiettivo più generali, mentre le seconde riguardano funzioni obiettivo specifiche, dette lineari.

Il primo capitolo di questa trattazione presenta nove differenti definizioni assiomatiche di matroide, tra cui le quattro originali di Whitney. Dimostreremo inoltre l'equivalenza delle definizioni attraverso il concetto di criptomorfismo.

Nel secondo capitolo andremo a studiare le matroidi grafiche come esempio di matroidi. Col termine 'matroide grafica' indichiamo la struttura assunta da un grafo che si verifica soddisfare i vari sistemi assiomatici introdotti nel capitolo precedente. Un'attenzione particolare è data al Polinomio di

Tutte, nato come oggetto definito per i grafi ed esteso successivamente alle matroidi.

L'ultimo capitolo vede invece lo studio degli algoritmi greedy per le matroidi, con esempi quali l'Algoritmo di Kruskal e l'Algoritmo di Prim per la ricerca di alberi generatori di peso minimo di un grafo dato. Viene inoltre introdotto il concetto di greedoide con l'obiettivo di dimostrare che un algoritmo greedy risolve un problema di ottimizzazione se e solo se la struttura in analisi è proprio quella di un greedoide.

Capitolo 1

Definizione assiomatica di matroide

In questo capitolo analizzeremo nove differenti sistemi assiomatici che nel corso del XX secolo sono stati proposti per definire il concetto di matroide, e ne dimostreremo l'equivalenza.

Scegliamo di considerare un così elevato numero di definizioni equivalenti per due motivi: innanzitutto interessanti risultati sulle matroidi sono dimostrabili più facilmente a partire da differenti definizioni; ed inoltre ciò permette di comprendere l'importanza e l'estensione della teoria che stiamo analizzando.

1.1 Assiomi delle basi

In questa sezione andremo ad analizzare gli assiomi che permettono di definire le matroidi attraverso il concetto di base.

Sia E un insieme finito e $\mathscr{P}(E)$ l'insieme delle parti di E, ossia l'insieme di tutti i sottinsiemi di E, possiamo allora dare la seguenti definizioni:

Definizione 1.1. $\mathscr{A} \subseteq \mathscr{P}(E)$ è un'**anticatena** di E se per ogni $X, Y \in \mathscr{A}$ tali che $X \subseteq Y$, allora $X = Y$.

Definizione 1.2. $\mathscr{B} \subseteq \mathscr{P}(E)$ è una **famiglia di basi** per E, e i suoi elementi sono detti **basi**, se soddisfa i seguenti assiomi:

(B1) $\mathscr{B} \neq \emptyset$,

(B2) $\mathscr{B}$ è un'anticatena di E,

(B3) Per ogni $X, Y \subseteq E$, $X \subseteq Y$, se esistono B_1, $B_2 \in \mathscr{B}$ tali che $X \subseteq B_1$ e $B_2 \subseteq Y$, allora esiste $B_3 \in \mathscr{B}$ tale che $X \subseteq B_3 \subseteq Y$.

Chiameremo $\mathbf{B}(E)$ l'insieme di tutte le famiglie di basi per E.

Definizione 1.3. Una **matroide** (finita) $M(E)$ è una coppia $(E, \mathscr{B})$, dove $\mathscr{B} \in \mathbf{B}(E)$.

Definizione 1.4. Dua matroidi $M_1 = (E_1, \mathscr{B}_1)$ e $M_2 = (E_2, \mathscr{B}_2)$ si dicono **isomorfe** se esiste una biezione $\phi : E_1 \to E_2$ che induce una biezione $\phi' : \mathscr{B}_1 \to \mathscr{B}_2$. Scriveremo allora $M_1 \simeq M_2$.

Notazione 1. Dato un insieme A e un generico elemento a, scriveremo $A \cup a$ in luogo di $A \cup \{a\}$, e $A \smallsetminus a$ in luogo di $A \smallsetminus \{a\}$.

L'assioma (B3) può essere sostituito con altre formulazioni; in particolare, in questa sede, andremo a dimostrare la seguente equivalenza:

Proposizione 1.1.1. *Sia $\mathscr{B} \in \mathscr{P}(E)$ un'anticatena non vuota, allora sono equivalenti*

(B3) *Per ogni $X, Y \subseteq E$, $X \subseteq Y$, se esistono B_1, $B_2 \in \mathscr{B}$ tali che $X \subseteq B_1$ e $B_2 \subseteq Y$, allora esiste $B_3 \in \mathscr{B}$ tale che $X \subseteq B_3 \subseteq Y$.*

(B3') *Per ogni $B_1, B_2 \in \mathscr{B}$ e per ogni $b_1 \in B_1$ esiste $b_2 \in B_2$ tale che $(B_1 \smallsetminus b_1) \cup b_2 \in \mathscr{B}$.*

Dimostrazione. Supponiamo valga (B3).

Dimostriamo preliminarmente che, dati $B_1, B_2 \in \mathscr{B}$, se $|B_1 \smallsetminus B_2| = 1$ allora $|B_2 \smallsetminus B_1| = 1$:
Sia $x = B_1 \smallsetminus B_2$ e $A = B_1 \cap B_2 = B_1 \smallsetminus x$. Se fosse $B_2 = A$ allora $B_2 \subseteq B_1$, ma allora, poiché $\mathscr{B}$ è un'anticatena, $B_2 = B_1$, e ciò è assurdo. Esiste quindi $y \in B_2 \smallsetminus A$. Abbiamo

$$\begin{aligned} A \cup y &\subseteq B_1 \cup y \\ A \cup y &\subseteq B_2 \\ B_1 &\subseteq B_1 \cup y, \end{aligned}$$

e quindi, per ipotesi, esiste $B_3 \in \mathscr{B}$ tale che

$$(B_1 \smallsetminus x) \cup y = A \cup y \subseteq B_3 \subseteq B_1 \cup y.$$

Se fosse $B_3 = B_1 \cup y$ allora $B_1 \subset B_3$, il che non è possibile poiché $\mathscr{B}$ è un'anticatena; quindi necessariamente

$$B_3 = (B_1 \smallsetminus x) \cup y,$$

poiché $(B_1 \setminus x) \cup y$ e $B_1 \cup y$ differiscono per un solo elemento. Quindi $B_3 = (B_1 \setminus x) \cup y \subseteq B_2$, e, per le proprietà di $\mathscr{B}$ come anticatena, $B_3 = B_2$. Allora $B_2 \setminus B_1 = y$ e $|B_2 \setminus B_1| = 1$.

Consideriamo ora $B_1, B_2 \in \mathscr{B}$, $B_1 \neq B_2$, $x \in B_1 \setminus B_2$ e definiamo

$$X := B_1 \setminus x$$
$$Y := B_2 \cup X.$$

Osserviamo che

$$X \subseteq Y$$
$$X \subseteq B_1$$
$$B_2 \subseteq Y,$$

allora, per (B3), esiste $B_3 \in \mathscr{B}$ tale che

$$X \subseteq B_3 \subseteq Y.$$

Poiché $X = B_1 \setminus x$ e $X \subseteq B_3$, $x \notin B_3$, e quindi $B_1 \setminus B_3 = x$ e $|B_1 \setminus B_3| = 1$. Per quanto dimostrato in precedenza, $|B_3 \setminus B_1| = 1$, cioè esiste $y \in B_3 \subseteq Y$ tale che $B_3 = X \cup y$; ma $Y = X \cup B_2$, allora $y \in B_2$.

Viceversa, supponiamo che valga (B3').

Siano $B_1, B_2 \in \mathscr{B}$ tali che

$$B_1 \neq B_2,\ X \subseteq B_1,\ B_2 \subseteq Y,\ X \subseteq Y.$$

Poichè $\mathscr{B}$ è finito, nella famiglia di tutti gli insiemi in $\mathscr{B}$ che contengono X possiamo scegliere B_3 tale che $B_2 \cap B_3$ sia massimale.

Procediamo ora per assurdo: se $B_3 \nsubseteq Y$, esiste $x \in B_3 \setminus Y$, allora per (B3') esiste $y \in B_2$ tale che $(B_3 \setminus x) \cup y \in \mathscr{B}$. L'insieme $(B_3 \setminus x) \cup y$ appartiene alla famiglia di tutti gli insiemi in $\mathscr{B}$ che contengono X, infatti

$$X \subseteq Y \text{ e } x \in B_3 \setminus Y \Rightarrow x \notin X \Rightarrow X \subseteq B_3 \setminus x \Rightarrow X \subseteq (B_3 \setminus x) \cup y.$$

Inoltre $x \in B_3 \setminus B_2$ poichè $x \in B_3 \setminus Y$ e $B_2 \subseteq Y$; quindi

$$B_2 = B_3 \subseteq B_2 \cap (B_3 \setminus x) \subset B_2 \cap (B_3 \setminus x \cup y).$$

Ciò contraddice la massimalità di $B_2 \cap B_3$, quindi $B_3 \subseteq Y$.

□

Corollario 1.1.2. *Tutte le basi di una matroide hanno la stessa cardinalità.*

Dimostrazione. Siano $B_1, B_2 \in \mathscr{B}$ e supponiamo per assurdo che $|B_1| > |B_2|$, cioè

$$B_1 = \{x_1, \ldots, x_n\},\ B_2 = \{y_1, \ldots, y_m\} \text{ con } n > m.$$

Esiste un ordinamento di B_1 tale che, per (B3'):

$$\begin{aligned}
&B_2^{(1)} := (B_2 \smallsetminus y_1) \cup x_1 = \{x_1, y_2, \ldots, y_m\} \in \mathscr{B} \\
&B_2^{(2)} := (B_2^{(1)} \smallsetminus y_2) \cup x_2 = \{x_1, x_2, y_3, \ldots, y_m\} \in \mathscr{B} \\
&\vdots \\
&B_2^{(m)} := (B_2^{(m \smallsetminus 1)} \smallsetminus y_m) \cup x_m = \{x_1, \ldots, x_m\} \in \mathscr{B};
\end{aligned}$$

quindi $B_2^{(m)} \subset B_1$ e ciò è assurdo poichè $\mathscr{B}$ è un'anticatena. □

Esempio 1. Sia E uno spazio vettoriale su un campo finito. Possiamo allora definire una matroide $M(E) = (E, \mathscr{B})$ dove $\mathscr{B}$ è l'insieme di tutte le basi di E come spazio vettoriale.

Notiamo che l'assioma (B3), anche detto assioma della base intermedia, risulta essere poco familiare per quanto riguarda $\mathscr{B}$ così definito; al contrario, l'assioma (B'3) è abbastanza standard. Sottolineiamo inoltre che il Corollario 1.1.2 conferma l'equicardinalità delle basi di uno spazio vettoriale finito.

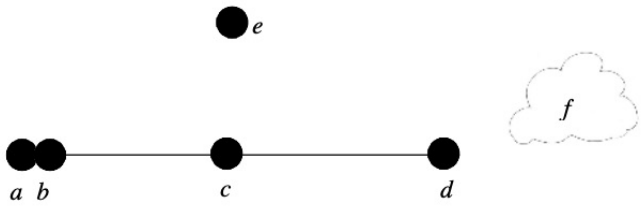


Figura 1.1: Matroide dell'Esempio 2

Esempio 2. Sia $M = (E, \mathscr{B})$ la matroide sull'insieme $E = \{a, b, c, d, e, f\}$ con basi $\{ace, ade, bce, bde, cde\}$. Nella figura 1.1, le basi corrispondono alle collezioni di tre punti non allineati. Notiamo che l'elemento e è in ogni base, mentre f non è in nessuna: questo ci permetterà di fare interessanti osservazioni negli esempi successivi.

1.2 Assiomi degli indipendenti e dei generatori

In questa sezione andremo a proporre due nuovi sistemi assiomatici che definiscono le matroidi e ne dimostreremo l'equivalenza con gli assiomi delle basi attraverso il concetto di criptomorfismo. Prima di introdurre gli assiomi, diamo l'enunciato del *Principio di Dualità*, poichè i sistemi che analizzeremo possono essere visti l'uno come il duale dell'altro.

Per ogni affermazione ρ di teoria delle matroidi, la sua affermazione duale ρ^* si ottiene invertendo la relazione d'ordine definita su $\mathscr{P}(E)$ e sostituendo ad ogni nozione la sua duale nel senso dell'ordine.

Proposizione 1.2.1 (Principio di dualità)**.** *Se ρ è una proposizione di teoria delle matroidi, allora ρ^* è ancora una proposizione.*

Risulta allora naturale definire la matroide duale:

Definizione 1.5. Data una matroide $M(E) := (E, \mathscr{B})$, la sua **matroide duale** (o **matroide ortogonale**) è la matroide

$$M^*(E) := (E, \mathscr{B}^*),$$

dove $\mathscr{B}^* := \{E \setminus B : B \in \mathscr{B}\}$.

Diamo ora alcune definizioni necessarie all'introduzione degli assiomi successivi.

Definizione 1.6. Una **famiglia discendente** in E è una famiglia $\mathscr{A} \subseteq \mathscr{P}(E)$ tale che per ogni $X, Y \subseteq E$

$$\text{se } X \subseteq Y \text{ e } Y \in \mathscr{A} \text{ allora } X \in \mathscr{A}.$$

Dualmente:

Definizione 1.7. Una **famiglia ascendente** in E è una famiglia $\mathscr{A} \subseteq \mathscr{P}(E)$ tale che per ogni $X, Y \subseteq E$

$$\text{se } X \supseteq Y \text{ e } Y \in \mathscr{A} \text{ allora } X \in \mathscr{A}.$$

Definizione 1.8. Sia $\mathscr{A} \subseteq \mathscr{P}(E)$, allora

$$\begin{aligned}
\mathbf{upp}(\mathscr{A}) &:= \{X \subseteq E \mid \exists A \in \mathscr{A}, X \supseteq A\},\\
\mathbf{low}(\mathscr{A}) &:= \{X \subseteq E \mid \exists A \in \mathscr{A}, X \subseteq A\},\\
\mathbf{max}(\mathscr{A}) &:= \{A \in \mathscr{A} \mid A \text{ è massimale in } \mathscr{A}\},\\
\mathbf{min}(\mathscr{A}) &:= \{A \in \mathscr{A} \mid A \text{ è minimale in } \mathscr{A}\},\\
\mathbf{opp}(\mathscr{A}) &:= \{X \subseteq E \mid X \notin \mathscr{A}\}.
\end{aligned}$$

Chiaramente upp($\mathscr{A}$) è una famiglia ascendente, e low($\mathscr{A}$) è una famiglia discendente.

Definizione 1.9. Sia $M(E)$ una matroide, allora $X \subseteq E$ è un **insieme indipendente** in $M(E)$ se $X \in \text{low}(\mathscr{B})$.

Dualmente, $X \subseteq E$ è un **insieme generatore** in $M(E)$ se $X \in \text{upp}(\mathscr{B})$. Chiameremo

$$\mathscr{I} := \text{low}(\mathscr{B}) \text{ e } \mathscr{S} := \text{upp}(\mathscr{B}),$$

e rispettivamente

$$\mathbf{I}(E) := \{\mathscr{I} | \mathscr{I} \text{ è una famiglia di indipendenti}\},$$
$$\mathbf{S}(E) := \{\mathscr{S} | \mathscr{S} \text{ è una famiglia di generatori}\}.$$

Osservazione 1. Gli insiemi indipendenti della matroide duale $M^*(E)$ sono i complementari degli insiemi generatori di $M(E)$, e dualmente.

Proposizione 1.2.2. *Una famiglia $\mathscr{I} \in \boldsymbol{I}(E)$ se e solo se soddisfa le seguenti condizioni:*

(I1) $\mathscr{I} \neq \varnothing$,

(I2) $\mathscr{I}$ *è una famiglia discendente,*

(I3) *Per ogni $I_1, I_2 \in \mathscr{I}$, se $|I_1| < |I_2|$, allora esiste $x \in I_2 \setminus I_1$ tale che $I_1 \cup x \in \mathscr{I}$.*

Dualmente, una famiglia $\mathscr{S} \in \boldsymbol{S}(E)$ se e solo se soddisfa le seguenti condizioni:

(S1) $\mathscr{S} \neq \varnothing$,

(S2) $\mathscr{S}$ *è una famiglia ascendente,*

(S3) *Per ogni $S_1, S_2 \in \mathscr{S}$, se $|S_1| > |S_2|$, allora esiste $x \in S_1 \setminus S_2$ tale che $S_1 \setminus x \in \mathscr{S}$.*

Dimostrazione. Supponiamo che $\mathscr{B} \in \mathbf{B}(E)$ e $\mathscr{I} := \text{low}(\mathscr{B})$, allora $\mathscr{I}$ soddisfa ovviamente (I1) e (I2).
Siano $I_1, I_2 \in \mathscr{I}$ con $|I_1| < |I_2|$, per come abbiamo definito $\mathscr{I}$ esistono $B_1, B_2 \in \mathscr{B}$ tali che $I_1 \subseteq B_1$ e $I_2 \subseteq B_2$. Definito $Y := B_2 \cup I_1$, abbiamo

$$I_1 \subseteq Y$$
$$I_1 \subseteq B_1$$
$$B_2 \subseteq Y;$$

allora per (B3) esiste $B_3 \in \mathscr{B}$ tale che

$$I_1 \subseteq B_3 \subseteq Y.$$

Ne consegue che $B_3 \setminus I_1 \subseteq Y \setminus I_1 \subseteq B_2$. Per il Corollario 1.1.2 tutti gli insiemi in $\mathscr{B}$ hanno la stessa cardinalità, quindi $|B_3| = |B_2|$ e $|B_3 \setminus I_1| > |B_2 \setminus I_2|$. Esiste allora $x \in I_2 \cap (B_3 \setminus I_1) \subseteq I_2 \setminus I_1$; poiché $I_1 \cup x \subseteq B_3$, allora $I_1 \cup x \in \mathscr{I}$.

Viceversa, supponiamo che $\mathscr{I}$ soddisfi (I1), (I2), (I3), e sia $\mathscr{B} := \max(E)$. Ovviamente $\mathscr{B}$ soddisfa (B1) e (B2).
Gli elementi di $\mathscr{B}$ hanno tutti la stessa cardinalità, infatti, se per assurdo esistono $B_1, B_2 \in \mathscr{B} \subseteq \mathscr{I}$ tali che $|B_1| < |B_2|$ allora per (I3) esiste $x \in B_2 \setminus B_1$ tale che $B_1 \cup x \in \mathscr{I}$, e questo contraddice la massimalità di B_1. Conseguentemente, se $I \in \mathscr{I}, B \in \mathscr{B}$ tali che $|I| = |B|$, allora $I \in \mathscr{B}$.
Consideriamo ora $X, Y \in E$, $B_1, B_2 \in \mathscr{B}$ tali che

$$X \subseteq Y$$
$$X \subseteq B_1$$
$$B_2 \subseteq Y;$$

poichè $B_1, B_2 \in \mathscr{B} \subseteq \mathscr{I}$, allora $X, Y \in \mathscr{I}$ per (I2). Se $|X| < |B_2|$, allora per (I3) esiste $Z \subseteq B_2$ tale che $X \cup Z \in \mathscr{I}$ e $|X \cup Z| = |B_2|$. Quindi $X \cup Z \in \mathscr{B}$ e vale

$$X \subseteq X \cup Z \subseteq Y \cup B_2 = Y.$$

(B3) risulta soddisfatto, e ciò dimostra che $\mathscr{B} \in \mathbf{B}(E)$.

Per il principio di dualità, le condizioni (S1), (S2), (S3) caratterizzano le famiglie in $\mathbf{S}(E)$. □

Vogliamo ora introdurre il concetto di criptomorfismo e dimostrare che i sistemi fino ad ora introdotti sono criptomorfi, ossia equivalenti: così facendo potremo definire le matroidi assumendo indifferentemente come assiomi (B1), (B2) e (B3), oppure (I1), (I2) e (I3), oppure (S1), (S2) e (S3).

Sottolineiamo che la nozione di criptomorfismo risulta abbastanza generica, e la definizione di tale termine rimane informale.

Definizione 1.10. Siano (U1), (U2), ..., (Un) e (V1), (V2), ..., (Vm) due sistemi assiomatici riguardanti rispettivamente le famiglie $\mathscr{U}$ e $\mathscr{V}$ di sottoinsiemi di E, e siano

$$\mathrm{U}(E) := \{\mathscr{U} | \mathscr{U} \text{ soddisfa (U1),...,(Un)}\},$$
$$\mathrm{V}(E) := \{\mathscr{V} | \mathscr{V} \text{ soddisfa (V1),...,(Vm)}\}.$$

Chiamiamo allora **interpretazione** una funzione

$$\alpha : \mathrm{U}(E) \to \mathrm{V}(E)$$

data specificatamente come regola per costruire $\mathscr{V} := \alpha(\mathscr{U})$.

Noi siamo interessati unicamente alle interpretazioni che corrispondono ad una connessione "naturale" tra U(E) e V(E). Questo ci permette di provare che gli assiomi (U1), ..., (Un) implicano gli assiomi (V1), ..., (Vm).

Definizione 1.11. I sistemi (U1), (U2), ..., (Un) e (V1), (V2), ..., (Vm) sono **criptomorfi** se esistono le interpretazioni

$$\alpha : \mathrm{U}(E) \to \mathrm{V}(E) \text{ e } \beta : \mathrm{V}(E) \to \mathrm{U}(E),$$

e queste sono l'una l'inversa dell'altra.

In questo caso α e β sono chiamati **criptomorfismi**.

Proposizione 1.2.3. *Gli assiomi delle basi, degli indipendenti e dei generatori sono tra loro criptomorfi.*

Dimostrazione. Nella Proposizione 1.2.2 abbiamo dimostrato che

$$\mathrm{low} : \mathbf{B}(E) \to \mathbf{I}(E) \quad \text{e} \quad \max : \mathbf{I}(E) \to \mathbf{B}(E)$$

sono interpretazioni, e sono chiaramente l'una l'inversa dell'altra.

Dualmente, $\mathbf{B}(E)$ e $\mathbf{S}(E)$ sono criptomorfi.

□

Esempio 3. Riprendiamo l'Esempio 1, ricordando che E è uno spazio vettoriale su un campo finito. Possiamo definire una matroide $M(E) = (E, \mathscr{I})$ con $X = \{x_1, \ldots, x_k\} \in \mathscr{I}$ se e solo se i vettori $x_1, \ldots, x_k$ sono linearmente indipendenti in E.

Analogamente, definiamo una matroide $M(E) = (E, \mathscr{S})$ con $X = \{x_1, \ldots, x_k\} \in \mathscr{S}$ se e solo se i vettori $x_1, \ldots, x_k$ sono un sistema di generatori per E.

Notiamo che (I3) ed (S3) sono banalmente soddisfatti da $\mathscr{I}$ e da $\mathscr{S}$ grazie all'equicardinalità delle basi, intese come sistemi di generatori linearmente indipendenti.

Esempio 4. Riprendiamo la matroide descritta nell'Esempio 2. Come osservato in tale esempio, l'elemento e appartiene ad ogni base, equivalentemente esso può essere aggiunto ad ogni insieme indipendente a cui non appartiene per ottenere un altro insieme indipendente. Un elemento con tale comportamento è detto **ponte**.

Al contrario, f non appartiene a nessuna base, e quindi a nessun insieme indipendente. Un elemento con tale comportamento è detto **cappio**.

L'uso dei termini ponte e cappio è interessante in quanto proviene dalla Teoria dei Grafi: difatti il concetto di matroide nasce anche come generalizzazione dei grafi.

1.3 Assiomi dei dipendenti e degli insiemi non generatori

In questa sezione andremo a proporre gli assiomi dei dipendenti e degli insiemi non generatori. Questi ultimi sono poco usati, ma si è deciso di includerli nella trattazione poichè trovano la loro naturale collocazione nello schema del Teorema 1.4.3.

Definizione 1.12. Sia $M(E)$ una matroide, allora $X \subseteq E$ è un **insieme dipendente** in $M(E)$ se $X \in \text{opp}(\mathscr{I})$.

Dualmente, $X \subseteq E$ è un **insieme non generatore** in $M(E)$ se $X \in \text{opp}(\mathscr{S})$. Chiameremo

$$\mathscr{D} := \text{opp}(\mathscr{I}) \text{ e } \mathscr{N} := \text{opp}(\mathscr{S}),$$

e rispettivamente

$$\mathbf{D}(E) := \{\mathscr{D} | \mathscr{D} \text{ è una famiglia di insiemi dipendenti}\},$$
$$\mathbf{N}(E) := \{\mathscr{N} | \mathscr{N} \text{ è una famiglia di insiemi non generatori}\}.$$

Proposizione 1.3.1. *Una famiglia $\mathscr{D} \in \boldsymbol{D}(E)$ se e solo se soddisfa le seguenti condizioni:*

(D1) $\varnothing \notin \mathscr{D}$,

(D2) $\mathscr{D}$ *è una famiglia ascendente,*

(D3) *Per ogni $D_1, D_2 \in \mathscr{D}$, se $D_1 \cap D_2 \notin \mathscr{D}$, allora per ogni $x \in E$ vale $(D_1 \cup D_2) \setminus x \in \mathscr{D}$.*

Dualmente, una famiglia $\mathscr{N} \in \boldsymbol{N}(E)$ se e solo se soddisfa le seguenti condizioni:

(N1) $E \notin \mathscr{N}$,

(N2) $\mathscr{N}$ *è una famiglia discendente,*

(N3) *Per ogni $N_1, N_2 \in \mathscr{N}$, se $N_1 \cup N_2 \notin \mathscr{N}$, allora per ogni $x \in E$ vale $(N_1 \cap N_2) \cup x \in \mathscr{N}$.*

Dimostrazione. Supponiamo che $\mathscr{D} \in \mathbf{D}(E)$, allora $\mathscr{I}$ soddisfa (I1), (I2) e (I3): ciò implica banalmente che $\mathscr{D}$ soddisfa (D1) e (D2).
Siano $D_1, D_2 \in \mathscr{D}$ tali che $D_1 \cap D_2 \notin \mathscr{D}$, cioè $D_1 \cap D_2 \in \mathscr{I}$. Abbiamo che

$$D_1 \setminus D_2 \neq \varnothing \neq D_2 \setminus D_1; \tag{1.1}$$

infatti se per assurdo $D_1 \smallsetminus D_2 = \varnothing$, allora $D_1 \subseteq D_2$, e quindi $D_1 \cap D_2 = D_1 \in \mathscr{D}$. Analogamente per $D_2 \smallsetminus D_1$. Se $x \notin D_1 \cap D_2$, allora, utilizzando (D2), abbiamo che:

$$\begin{aligned}
&\text{se } x \in D_1 \smallsetminus D_2 \Rightarrow D_2 \subseteq (D_1 \smallsetminus x) \cup D_2 = (D_1 \cup D_2) \smallsetminus x \in \mathscr{D},\\
&\text{se } x \in D_2 \smallsetminus D_1 \Rightarrow D_1 \subseteq D_1 \cup (D_2 \smallsetminus x) = (D_1 \cup D_2) \smallsetminus x \in \mathscr{D},\\
&\text{se } x \notin D_1 \cup D_2 \Rightarrow D_1 \subseteq (D_1 \cup D_2) \smallsetminus x \in \mathscr{D}.
\end{aligned}$$

Consideriamo ora il caso in cui $x \in D_1 \cap D_2$ e supponiamo per assurdo che $(D_1 \cup D_2) \smallsetminus x \in \mathscr{I}$. Per (1.1) abbiamo che $|D_1 \cap D_2| < |(D_1 \cup D_2) \smallsetminus x|$, allora per (I3) esiste $y \in [(D_1 \cup D_2) \smallsetminus x] \smallsetminus (D_1 \cap D_2)$ tale che $I := (D_1 \cap D_2) \cup y \in \mathscr{I}$. Sappiamo che

$$\begin{aligned}
&D_1 \cap D_2 \subseteq I\\
&I \subseteq [(D_1 \cup D_2) \smallsetminus x] \cup (D_1 \cap D_2) = D_1 \cup D_2,
\end{aligned}$$

inoltre $|I| \leqslant |(D_1 \cup D_2) \smallsetminus x|$. Se $|I| < |(D_1 \cup D_2) \smallsetminus x|$ possiamo reiterare il procedimento precedente fino ad ottenere $|I'| = |(D_1 \cup D_2) \smallsetminus x|$. Abbiamo allora che $D_1 \subseteq I'$ oppure $D_2 \subseteq I'$, e quindi per (I2) D_1 o $D_2 \in \mathscr{I}$, in contraddizione con le ipotesi.

Viceversa, supponiamo che la famiglia $\mathscr{D}$ soddisfi (D1), (D2), (D3) e definiamo $\mathscr{I} := \mathrm{opp}(\mathscr{D})$. Banalmente $\mathscr{I}$ soddisfa (I1) e (I2).
Siano $I_1, I_2 \in \mathscr{I}$ con $|I_1| < |I_2|$ e procediamo per induzione su $|I_1 \smallsetminus I_2|$. Se $|I_1 \smallsetminus I_2| = 0$ allora $I_1 \subseteq I_2$ e (I3) è banalmente soddisfatto.
Procediamo quindi con il passo induttivo. Siano I_1, I_2 tali che $|I_1 \smallsetminus I_2| = n+1$. Consideriamo $y \in I_1 \smallsetminus I_2$ e sia $I_1' := I_1 \smallsetminus y$, allora $I_1' \in \mathscr{I}$, $|I_1'| < |I_1| < |I_2|$ e $|I_1' \smallsetminus I_2| = n$. Per induzione vale (I3), cioè esiste $I_2' \in \mathscr{I}$ tale che

$$I_1' \subseteq I_2' \subseteq I_1' \cup I_2 \text{ e } |I_2'| = |I_1'| + 1.$$

Iterando il procedimento possiamo costruire $|I_2''| = |I_2|$; quindi esistono $x_1, x_2 \in I_2'' \smallsetminus I_1$, $x_1 \neq x_2$. Se $I_1 \cup x_1, I_1 \cup x_2 \in \mathscr{D}$ allora, per (D3), $(I_1 \cup x_1 \cup x_2) \smallsetminus y \in \mathscr{D}$, e ciò è assurdo poiché $(I_1 \cup x_1 \cup x_2) \smallsetminus y \subseteq I_2'' \in \mathscr{I}$. Quindi $I_1 \cup x_1 \in \mathscr{I}$ o $I_1 \cup x_2 \in \mathscr{I}$, soddisfacendo (I3).

Per il principio di dualità, le condizioni (N1), (N2) e (N3) caratterizzano le famiglie in $\mathbf{N}(E)$.

□

Esempio 5. Riprendiamo l'Esempio 1, ricordando che E è uno spazio vettoriale su un campo finito.

Possiamo definire una matroide $M(E) = (E, \mathscr{D})$ con $X = \{x_1, \ldots, x_k\} \in \mathscr{D}$ se e solo se i vettori $x_1, \ldots, x_k$ sono linearmente dipendenti in E.

Analogamente, definiamo una matroide $M(E) = (E, \mathscr{N})$ con $X = \{x_1, \ldots, x_k\} \in \mathscr{N}$ se e solo se $\mathrm{Span}(x_1, \ldots, x_k) \subset E$.

1.4 Assiomi dei circuiti e degli iperpiani

In questa sezione andremo ad analizzare gli assiomi dei circuiti e degli iperpiani. Tali concetti ci risultano familiari in ambiti quali i grafi e gli spazi vettoriali, difatti questi possono essere visti come esempi di matroidi.

Definizione 1.13. Sia $M(E)$ una matroide, allora $X \subseteq E$ è un **circuito** in $M(E)$ se $X \in \min(\mathscr{D})$.

Dualmente, $X \subseteq E$ è un **iperpiano** in $M(E)$ se $X \in \max(\mathscr{N})$. Chiameremo

$$\mathscr{C} := \min(\mathscr{D}) \text{ e } \mathscr{H} := \max(\mathscr{N}),$$

e rispettivamente

$$\mathbf{C}(E) := \{\mathscr{C} | \mathscr{C} \text{ è una famiglia di circuiti}\},$$
$$\mathbf{H}(E) := \{\mathscr{H} | \mathscr{H} \text{ è una famiglia di iperpiani}\}.$$

Osservazione 2. I circuiti della matroide duale $M^*(E)$ sono i complementari degli iperpiani di $M(E)$, e dualmente.

Proposizione 1.4.1. *Una famiglia $\mathscr{C} \in \boldsymbol{C}(E)$ se e solo se soddisfa le seguenti condizioni:*

(C1) $\varnothing \notin \mathscr{C}$,

(C2) $\mathscr{C}$ *è un'anticatena,*

(C3) *Per ogni $C_1, C_2 \in \mathscr{C}$ tali che $C_1 \neq C_2$, e per ogni $x \in E$, esiste $C_3 \in \mathscr{C}$ tale che $C_3 \subseteq (C_1 \cup C_2) \setminus x$.*

Dualmente, una famiglia $\mathscr{H} \in \boldsymbol{H}(E)$ se e solo se soddisfa le seguenti condizioni:

(H1) $E \notin \mathscr{H}$,

(H2) $\mathscr{H}$ *è un'anticatena,*

(H3) *Per ogni $H_1, H_2 \in \mathscr{H}$, tali che $H_1 \neq H_2$, e per ogni $x \in E$, esiste $H_3 \in \mathscr{H}$ tale che $(H_1 \cap H_2) \cup x \subseteq H_3$.*

Dimostrazione. Supponiamo $\mathscr{C} \in \mathbf{C}(E)$, dato che $\mathscr{D}$ soddisfa (D1), (D2) e (D3): abbiamo banalmente che (C1) e (C2) sono soddisfatti da $\mathscr{C}$.
Siano $C_1, C_2 \in \mathscr{C}$ tali che $C_1 \neq C_2$, allora $C_1, C_2 \in \mathscr{D}$ e $C_1 \cap C_2 \notin \mathscr{D}$; infatti ricordiamo che $\mathscr{C} := \min(\mathscr{D}) \subseteq \mathscr{D}$ e se fosse $C_1 \cap C_2 \in \mathscr{D}$ allora $C_1 \cap C_2 \subset C_1 \in \mathscr{D}$ e $C_1 \cap C_2 \subset C_2 \in \mathscr{D}$, assurdo per la minimalità di C_1 e C_2.

Per (D3) abbiamo che per ogni $x \in E$, l'insieme $(C_1 \cup C_2) \smallsetminus x \in \mathscr{D}$, quindi, per definizione di $\mathscr{C}$, esiste $C_3 \in \mathscr{C}$ tale che $C_3 \subseteq (C_1 \cup C_2) \smallsetminus x$.

Viceversa, supponiamo che la famiglia $\mathscr{C}$ soddisfi (C1), (C2), (C3), e sia $\mathscr{D} = \mathrm{upp}(\mathscr{C})$. Banalmente $\mathscr{D}$ soddisfa (D1) e (D2).
Siano $D_1, D_2 \in \mathscr{D}$, $D_1 \cap D_2 \notin \mathscr{D}$, e siano $C_1, C_2 \in \mathscr{C}$ tali che $C_1 \subseteq D_1$, $C_2 \subseteq D_2$; allora $C_1 \neq C_2$. Per ogni $x \in E$, se $x \notin C_1 \cap C_2$ allora

$$C_i \subseteq (D_1 \cup D_2) \smallsetminus x \text{ con } i = 1 \text{ o } i = 2,$$

e quindi, per definizione di $\mathscr{D}$ abbiamo che $(D_1 \cup D_2) \smallsetminus x \in \mathscr{D}$.
Consideriamo ora $x \in C_1 \cap C_2$; per (C3) esiste $C_3 \in \mathscr{C}$ tale che

$$C_3 \subseteq (C_1 \cup C_2) \smallsetminus x \subseteq (D_1 \cup D_2) \smallsetminus x,$$

e ciò implica che $(D_1 \cup D_2) \smallsetminus x \in \mathscr{D}$. Quindi (D3) è soddisfatto e $\mathscr{D} \in \mathbf{D}(E)$.

Per il principio di dualità, le condizioni (H1), (H2) e (H3) caratterizzano le famiglie in $\mathbf{H}(E)$.

□

Gli assiomi (C3) e (H3) possono essere sostituiti dalle seguenti formulazioni, più forti:

Proposizione 1.4.2. *Sia $\mathscr{A}$ un'anticatena.*

Sono equivalenti:

(C3) *Per ogni $C_1, C_2 \in \mathscr{A}$ tali che $C_1 \neq C_2$, e per ogni $x \in E$, esiste $C_3 \in \mathscr{A}$ tale che $C_3 \subseteq (C_1 \cup C_2) \smallsetminus x$,*

(C3') *Per ogni $C_1, C_2 \in \mathscr{A}$ tali che $C_1 \neq C_2$, e per ogni $x \in C_1 \cap C_2$, $y \in C_1 \smallsetminus C_2$, esiste $C_3 \in \mathscr{A}$ tale che $y \in C_3 \subseteq (C_1 \cup C_2) \smallsetminus x$.*

Dualmente, sono equivalenti:

(H3) *Per ogni $H_1, H_2 \in \mathscr{A}$, tali che $H_1 \neq H_2$, e per ogni $x \in E$, esiste $H_3 \in \mathscr{A}$ tale che $(H_1 \cap H_2) \cup x \subseteq H_3$,*

(H3') *Per ogni $H_1, H_2 \in \mathscr{A}$ tali che $H_1 \neq H_2$, e per ogni $x \notin H_1 \cup H_2$, $y \in H_2 \smallsetminus H_1$, esiste $H_3 \in \mathscr{A}$ tale che $y \notin H_3 \supseteq (H_1 \cap H_2) \cup x$.*

Dimostrazione. Supponiamo valga (C3').
Se $x \in C_1 \cap C_2$ o $x \in E \smallsetminus (C_1 \cup C_2)$, allora (C3) è ovviamente soddisfatto.
Se $x \in C_1 \smallsetminus (C_1 \cap C_2)$ allora $C_2 \subseteq (C_1 \cup C_2) \smallsetminus x$, e analogamente per $x \in C_2 \smallsetminus (C_1 \cap C_2)$, quindi (C3) è soddisfatto.

Viceversa, supponiamo sia soddisfatto (C3) e procediamo per induzione su $|C_1 \cup C_2|$, notando che per $|C_1 \cup C_2| \leqslant 3$ la condizione (C3') è facilmente

verificata.
Supponiamo che (C3') valga per tutti i circuiti la cui unione abbia cardinalità minore di $|C_1 \cup C_2|$, e siano $x \in C_1 \cap C_2$ e $y \in C_1 \setminus C_2$. Per (C3) esiste $C_3 \in \mathscr{A}$ tale che

$$C_3 \subseteq C_1 \cup C_2 \setminus x.$$

Supponiamo che $y \notin C_3$, altrimenti è banale. Abbiamo allora che $|C_3 \cup C_2| < |C_1 \cup C_2|$, poichè $y \notin C_2 \cup C_3$. Poichè $\mathscr{A}$ è un'anticatena, se $C_3 \subseteq C_1$ allora $C_3 = C_1$, il che è assurdo poichè $y \in C_1 \setminus C_3$, quindi necessariamente $C_3 \nsubseteq C_1$; allora esiste

$$z \in C_3 \cap (C_2 \setminus C_1) = (C_2 \cap C_3) \setminus C_1 \subseteq C_2 \cap C_3.$$

Per ipotesi induttiva, notando che $x \in C_2 \setminus C_3$, esiste $C_4 \in \mathscr{A}$ tale che

$$x \in C_4 \subseteq C_3 \cup C_2 \setminus z.$$

Ora $x \in C_1 \cap C_4$, $y \in C_1 \setminus C_4$ e $|C_1 \cup C_4| < |C_1 \cup C_2|$ poiché $z \notin C_1 \cup C_4$. Per ipotesi induttiva esiste $C_5 \in \mathscr{A}$ tale che

$$y \in C_5 \subseteq C_1 \cup C_4 \setminus x \subseteq C_1 \cup C_2 \setminus x,$$

dimostrando così la tesi.

Per il principio di dualità, (H3) e (H3') sono equivalenti.

□

I risultati precedenti ci permettono di affermare che:

Teorema 1.4.3. *Gli assiomi dei circuiti, dei dipendenti, degli indipendenti, delle basi, dei generatori, degli insiemi non generatori e degli iperpiani sono criptomorfi attraverso il seguente schema:*

$$\boldsymbol{C}(E) \underset{min}{\overset{upp}{\rightleftarrows}} \boldsymbol{D}(E) \underset{opp}{\overset{opp}{\rightleftarrows}} \boldsymbol{I}(E) \underset{low}{\overset{max}{\rightleftarrows}} \boldsymbol{B}(E) \underset{min}{\overset{upp}{\rightleftarrows}} \boldsymbol{S}(E) \underset{opp}{\overset{opp}{\rightleftarrows}} \boldsymbol{N}(E) \underset{low}{\overset{max}{\rightleftarrows}} \boldsymbol{H}(E).$$

Esempio 6. Riprendiamo l'Esempio 1, ricordando che E è uno spazio vettoriale su un campo finito. Possiamo definire una matroide $M(E) = (E, \mathscr{C})$, dove $X \in \mathscr{C}$ se e solo se è un sottoinsieme dipendente minimale di E, ovvero se $X = \{x_1, \ldots, x_k\}$ e $\dim(\mathrm{Span}(x_1, \ldots, x_k)) = k - 1$.

Se E ha dimensione n, definiamo una matroide $M(E) = (E, \mathscr{H})$ con $H \in \mathscr{H}$ se e solo H è un sottospazio di E di dimensione $n - 1$.

Esempio 7. Consideriamo la matroide M descritta nell'Esempio 2, di cui riportiamo l'immagine. L'insieme dei circuiti di M è $\mathscr{C} = \{f, ab, acd, bcd\}$.

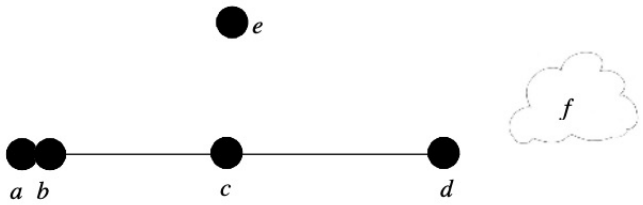


Figura 1.2: Matroide dell'Esempio 2

In termini geometrici, notiamo che questi sono tutti gli insiemi dipendenti minimali. In particolare, i circuiti acd e bcd corrispondono a tre punti allineati.

Gli iperpiani della matroide M, come si evince facilmente dalla sua rappresentazione geometrica, sono gli insiemi che identificano le linee rette con l'aggiunta del cappio f, ovvero $abcdf, abef, cef, def$.

1.5 Assiomi di chiusura e di rango

In questa sezione andremo ad analizzare gli ultimi due sistemi assiomatici proposti in questa trattazione. Notiamo che questi si differenziano dai precedenti poiché non riguardano una famiglia di insiemi, bensì di applicazioni.

Definizione 1.14. Una **funzione rango** su E è una funzione r: $\mathscr{P}(E) \to \mathbb{N}$ che soddisfa le seguenti condizioni:

(R1) Per ogni $X \subseteq E$, $0 \leqslant \mathrm{r}(X) \leqslant |X|$,

(R2) Per ogni $X, Y \subseteq E$, se $X \subseteq Y$ allora $\mathrm{r}(X) \leqslant \mathrm{r}(Y)$,

(R3) Per ogni $X, Y \subseteq E$, $\mathrm{r}(X \cup Y) + \mathrm{r}(X \cap Y) \leqslant \mathrm{r}(X) + \mathrm{r}(Y)$.

La collezione di tutte le funzioni rango sarà denotata con $\mathbf{r}(E)$.

Come alternativa degli assiomi di rango appena visti, è possibile dare una formulazione di carattere "locale" che risulta più adatta nelle dimostrazioni per induzione. L'equivalenza dei due sistemi sarà mostrata nella Proposizione 1.5.1.

Definizione 1.15. Una **funzione rango locale** su E è una funzione $\mathrm{r}' : \mathscr{P}(E) \to \mathbb{N}$ che soddisfa le seguenti condizioni:

(R'1) $\mathrm{r}'(\varnothing) = 0$,

(R'2) Per ogni $X \subseteq E$ e per ogni $y \in E$, $\mathrm{r}'(X) \leqslant \mathrm{r}'(X \cup y) \leqslant \mathrm{r}'(X) + 1$,

(R'3) Per ogni $X \subseteq E$ e per ogni $y, z \in E$, se $\mathrm{r}'(X) = \mathrm{r}'(X \cup y) = \mathrm{r}'(X \cup z)$ allora $\mathrm{r}'(X) = \mathrm{r}'(X \cup y \cup z)$.

La collezione di tutte le funzioni rango locale sarà denotata con $\mathbf{r}'(E)$.

Introduciamo ora alcune funzioni che dimostreremo essere interpretazioni, necessarie per mostrare i criptomorfismi tra gli assiomi di rango, rango locale e degli indipendenti.

Definizione 1.16. Sia $\mathscr{I} \in \mathbf{I}(E)$ una famiglia di insiemi indipendenti, definiamo una funzione $\gamma(\mathscr{I}) : \mathscr{P}(E) \to \mathbb{N}$ tale che per ogni $X \subseteq E$ vale:

$$[\gamma(\mathscr{I})](X) := \max\{|I| : I \subseteq X, I \in \mathscr{I}\}.$$

Definizione 1.17. Sia $\mathrm{r} \in \mathbf{r}'(E)$ una funzione rango locale, definiamo la famiglia $\epsilon(\mathrm{r})$ come:

$$\epsilon(\mathrm{r}) := \{X \subseteq E \mid \mathrm{r}(X) = |X|\}.$$

Proposizione 1.5.1. *Gli assiomi di rango, rango locale e degli indipendenti sono criptomorfi attraverso i seguenti criptomorfismi:*

$$\boldsymbol{I}(E) \xrightarrow{\gamma} \boldsymbol{r}(E) \xrightarrow{\delta} \boldsymbol{r}'(E) \xrightarrow{\epsilon} \boldsymbol{I}(E),$$

con γ ed ϵ definite come sopra, e δ funzione identità su $r(E)$.

Dimostrazione. Innanzitutto dimostriamo che γ è un'applicazione da $\mathbf{I}(E)$ a $\mathbf{r}(E)$. Siano $\mathscr{I} \in \mathbf{I}(E)$ e $\mathrm{r} := \gamma(\mathscr{I})$; le condizioni (R1), (R2) seguono banalmente da (I1) e (I2).
Siano $X, Y \subseteq E$ e chiamiamo $u := \mathrm{r}(X \cap Y)$, $v := \mathrm{r}(X \cup Y)$. Consideriamo $U \in \mathscr{I}$ tale che $U \subseteq X \cap Y$, $|U| = u$; e $V \in \mathscr{I}$ tale che $V \subseteq X \cup Y$, $|V| = v$. Per (R2) abbiamo che $u \leqslant v$, e se $u < v$ per (I3) possiamo aggiungere $v \smallsetminus u$ elementi distinti di $V \smallsetminus U$ ad U, ottendendo $V' \in \mathscr{I}$ tale che $|V'| = v$ e $U \subseteq V' \subseteq X \cup Y$. Notiamo che

$$V' = U \cup (V' \smallsetminus (X \cap Y)) = U \cup (V' \smallsetminus X) \cup (V' \smallsetminus Y), \tag{1.2}$$

poiché U è un sottoinsieme di $X \cap Y$ indipendente massimale per definizione di r. Per (I2) vale che $V' \cap X, V' \cap Y \in \mathscr{I}$, quindi

$$\begin{aligned} \mathrm{r}(X) + \mathrm{r}(Y) &\overset{def}{\geqslant} |V' \cap X| + |V' \cap Y| \\ &= |U| + |V' \smallsetminus Y| + |U| + |V' \smallsetminus X| \\ &\overset{(1.2)}{=} |U| + |V'| \\ &= r(X \cap Y) + r(X \cup Y). \end{aligned}$$

La condizione (R3) è soddisfatta, quindi $\gamma : \mathbf{I}(E) \to \mathbf{r}(E)$.

Per provare che δ è un'applicazione da $\mathbf{r}(E)$ a $\mathbf{r}'(E)$, consideriamo $\mathrm{r} \in \mathbf{r}(E)$ e sia $\mathrm{r}'(E) := \mathrm{r}(E)$. Da (R1) otteniamo banalmente (R'1).
Se $Z \subseteq E$ e $x \in E$, allora per (R2) vale $\mathrm{r}(Z) \leqslant \mathrm{r}(Z \cup x)$, e per (R1) abbiamo che $0 \leqslant \mathrm{r}(x) \leqslant 1$. Possiamo allora dimostrare (R'2) attraverso (R3):

$$\mathrm{r}(Z \cup x) \leqslant \mathrm{r}(Z \cup x) + (Z \cap x) \overset{(R3)}{\leqslant} \mathrm{r}(Z) + \mathrm{r}(x) \leqslant \mathrm{r}(Z) + 1.$$

Consideriamo ora $Z \subseteq E$ e $x, y \in E$ tali che $\mathrm{r}(Z \cup x) = \mathrm{r}(Z \cup y) = \mathrm{r}(Z)$, allora

$$\begin{aligned} &\mathrm{r}(Z \cup x \cup y) = \mathrm{r}\big[(Z \cup x) \cup (Z \cup y)\big] \\ &\overset{(R3)}{\leqslant} \mathrm{r}(Z \cup x) + \mathrm{r}(Z \cup y) \smallsetminus \mathrm{r}\big[(Z \cup x) \cap (Z \cup y)\big] = \mathrm{r}(Z); \end{aligned}$$

quindi (R'3) è soddisfatto.

Vogliamo ora mostrare che $\epsilon : \mathbf{r}'(E) \to \mathbf{I}(E)$. Sia $\mathrm{r} \in \mathbf{r}'(E)$ e definiamo $\mathscr{I} := \epsilon(\mathrm{r})$. Per (R'1) abbiamo che $\{\varnothing\} \in \mathscr{I}$, quindi $\mathscr{I}$ soddisfa (I1).
Per ogni $X \subseteq E$ vogliamo dimostrare che vale

$$0 \leqslant r(X) \leqslant |X|,$$

procedendo per induzione su $|X|$. Se $|X| = 1$ per (R'2) abbiamo che $0 = \mathrm{r}(\varnothing) \leqslant \mathrm{r}(X) \leqslant 1 = |X|$. Supponiamo $|X| = n + 1$, allora $X = X' \cup y$ con $|X'| = n$; per (R'2) e per ipotesi induttiva abbiamo che:

$$0 \leqslant \mathrm{r}(X') \leqslant \mathrm{r}(X) \leqslant \mathrm{r}(X') + 1 = |X'| + 1 = |X|.$$

Quindi, poiché $\mathrm{r}(X) \leqslant |X|$, per definizione di $\mathscr{I}$ vale che $X \notin \mathscr{I}$ se e solo se $\mathrm{r}(X) < |X|$. Per ogni $X, Y \subseteq E$ tali che $X \subseteq Y$, vogliamo dimostrare per induzione su $|Y \smallsetminus X|$ che vale

$$\mathrm{r}(Y) \leqslant \mathrm{r}(X) + |Y \smallsetminus X|.$$

Se $|Y \smallsetminus X| = 1$, allora $Y = X \cup y$ per un certo $y \in E \smallsetminus X$, e l'enunciato è ovvio per (R'2). Supponiamo $|Y \smallsetminus X| = n + 1$, allora $Y = Y' \cup y$ con $|Y' \smallsetminus X| = n$; per (R'2) e per ipotesi induttiva abbiamo che:

$$\mathrm{r}(Y) = \mathrm{r}(Y' \cup y) \leqslant \mathrm{r}(Y') + 1 \leqslant \mathrm{r}(X) + |Y' \smallsetminus X| + 1 = \mathrm{r}(X) + |Y \smallsetminus X|,$$

concludendo così l'induzione. Se $X \notin \mathscr{I}$, allora

$$\mathrm{r}(Y) \leqslant \mathrm{r}(X) + |Y \smallsetminus X| < |X| + |Y \smallsetminus X| = |Y|,$$

quindi $Y \notin \mathscr{I}$, provando (I2).
Infine, siano $U, V \in \mathscr{I}$ tali che $|U| < |V|$. Supponiamo per assurdo che per ogni $x \in V$ valga $\mathrm{r}(U \cup x) = \mathrm{r}(U)$, allora possiamo dedurre induttivamente da (R'3) che $\mathrm{r}(U \cup V) = \mathrm{r}(U) = \mathrm{r}(V)$, e questo contraddice $|U| < |V|$. Quindi esiste $x \in V$ tale che $\mathrm{r}(U \cup x) = \mathrm{r}(U) + 1 = |U| + 1 = |U \cup x|$, ed allora $U \cup x \in \mathscr{I}$, dimostrando così (I3).

Rimane da dimostrare che γ, δ e ϵ hanno un'inversa.
Si vede facilmente che

$$\{X \subseteq E : \max\{|I| : I \subseteq X, I \in \mathscr{I}\} = |X|\} = \mathscr{I},$$

cioè che $\epsilon\delta\gamma$ è l'identità su $\mathbf{I}(E)$.
Per $\mathrm{r} \in \mathbf{r}(E)$, consideriamo $\gamma\epsilon\delta(\mathrm{r}) \in \mathbf{r}(E)$: per ogni $X \subseteq E$,

$$[\gamma\epsilon\delta(\mathrm{r})](X) = \max\{|I| : I \subseteq X, |I| = \mathrm{r}(I)\}.$$

Vogliamo dimostrare che $\gamma\epsilon\delta$ è l'identità su $\mathbf{r}(E)$, cioè che per ogni $X \subseteq E$ esiste $I \subseteq X$ massimale tale che $|I| = \mathrm{r}(I) = \mathrm{r}(X)$, dove $\mathrm{r} \in \mathbf{r}(E)$ e quindi $\mathrm{r} \in \mathbf{r}'(E)$. Ma se I è un sottoinsieme massimale di X che soddisfa $|I| = \mathrm{r}(I)$, allora per ogni $x \in X$ vale $\mathrm{r}(I \cup x) = \mathrm{r}(I)$, e quindi, procedendo induttivamente attraverso (R'3), abbiamo che $\mathrm{r}(X) = \mathrm{r}(I) = |I|$, provando che $\gamma\epsilon\delta$ è l'identità su $\mathbf{r}(E)$.
Analogamente si dimostra che $\delta\gamma\epsilon$ è l'identità su $\mathbf{r}'(E)$.
Quindi

$$\begin{aligned}\gamma^{-1} &= \epsilon\delta,\\ \delta^{-1} &= \gamma\epsilon,\\ \epsilon^{-1} &= \delta\gamma.\end{aligned}$$

□

Diamo ora la definizione di operatore di chiusura, strettamente legato al concetto di rango.

Definizione 1.18. Sia $M = (E, \mathrm{r})$ una matroide con $\mathrm{r} \in \mathbf{r}(E)$, allora un **operatore di chiusura** su E è un operatore cl: $\mathscr{P}(E) \to \mathscr{P}(E)$ tale che, per ogni $X \subseteq E$, vale

$$\mathrm{cl}(X) = \{x \in E : \mathrm{r}(X \cup x) = \mathrm{r}(X)\}.$$

La collezione di tutte gli operatori di chiusura sarà denotata con $\mathbf{cl}(E)$.

Osservazione 3. Notiamo che $\mathbf{cl}(E)$ e $\mathbf{r}(E)$ sono collezioni non vuote, infatti l'identità è un elemento di $\mathbf{cl}(E)$ e la cardinalità è un elemento di $\mathbf{r}(E)$.

Proposizione 1.5.2. *Se $cl \in \boldsymbol{cl}(E)$ allora soddisfa le seguenti condizioni:*

(Cl1) *Per ogni $X \subseteq E$, $X \subseteq cl(X)$,*

(Cl2) *Per ogni $X, Y \subseteq E$, se $X \subseteq Y$ allora $cl(X) \subseteq cl(Y)$,*

(Cl3) *Per ogni $X \subseteq E$, $cl[cl(X)] = cl(X)$,*

(Cl4) *Per ogni $X \subseteq E$ e per ogni $y, z \in E$, se $y \in cl(X \cup z) \setminus cl(X)$, allora $z \in cl(X \cup y) \setminus cl(X)$.*

Dimostrazione. In tale dimostrazione andremo ad utilizzare $\mathrm{r} \in \mathbf{r}'(E)$, poiché $\mathbf{r}(E)$ ed $\mathbf{r}'(E)$ sono equivalenti. Supponiamo $\mathrm{cl} \in \mathbf{cl}(E)$, allora r soddisfa (R'1), (R'2) ed (R'3): abbiamo banalmente che (Cl1) è soddisfatto da cl. Per dimostrare (Cl2) consideriamo $X, Y \in E$ tali che $X \subseteq Y$ e procediamo per induzione su $|Y \setminus X|$. Se $|Y \setminus X| = 0$, allora $X = Y$ e (Cl2) è banale. Se $|Y \setminus X| = n+1$ allora esistono $Y' \subseteq E$, $y \in E$ tali che $Y = Y' \cup y$, $X \subseteq Y$ e $|Y' \setminus X| = n$. Consideriamo $x \in \mathrm{cl}(X)$, per passo induttivo $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y')$, quindi $x \in \mathrm{cl}(Y')$, ovvero

$$\mathrm{r}(Y' \cup x) = \mathrm{r}(Y'). \tag{1.3}$$

Per (R'2) abbiamo che:

$\mathrm{r}(Y) \leqslant \mathrm{r}(Y \cup x)$,
$\mathrm{r}(Y') \leqslant \mathrm{r}(Y' \cup y) = \mathrm{r}(Y) \leqslant \mathrm{r}(Y') + 1$,
$\mathrm{r}(Y') \overset{(1.3)}{=} \mathrm{r}(Y' \cup x) \leqslant \mathrm{r}(Y' \cup y \cup x) = \mathrm{r}(Y \cup x) \leqslant \mathrm{r}(Y' \cup x) + 1 \overset{(1.3)}{=} \mathrm{r}(Y') + 1$;

dunque l'unico caso che ci rimane da verificare è se, per assurdo,

$$\mathrm{r}(Y) = \mathrm{r}(Y' \cup x) \text{ e } \mathrm{r}(Y \cup x) = \mathrm{r}(Y' \cup x) + 1. \tag{1.4}$$

Sappiamo che

$$\mathrm{r}(Y' \cup y) = \mathrm{r}'(Y) \overset{(1.4)}{=} \mathrm{r}(Y' \cup x) \overset{(1.3)}{=} \mathrm{r}(Y'),$$

allora per (R'3) vale

$$\mathrm{r}(Y' \cup x) \overset{(1.3)}{=} \mathrm{r}(Y') \overset{(\mathrm{R'3})}{=} \mathrm{r}(Y' \cup y \cup x) = \mathrm{r}(Y \cup x);$$

il che è assurdo per (1.4). Quindi (Cl2) è soddisfatto.
Per dimostrare (Cl3), osserviamo in primo luogo che per (Cl1) vale $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(X))$. Consideriamo ora $x \in \mathrm{cl}(\mathrm{cl}(X))$, allora

$$\mathrm{r}(\mathrm{cl}(X) \cup x) = \mathrm{r}(\mathrm{cl}(X)). \tag{1.5}$$

Per definizione di $\mathrm{cl}(X)$, per ogni $y \in \mathrm{cl}(X) \setminus X$ vale $\mathrm{r}(X \cup y) = \mathrm{r}(X)$; quindi per (R'3), procedendo con una facile induzione, possiamo affermare che

$$\mathrm{r}(X) = \mathrm{r}(X \cup (\mathrm{cl}(X) \setminus X)) = \mathrm{r}(\mathrm{cl}(X)). \tag{1.6}$$

Quindi, per (1.5) e (1.6), abbiamo che $\mathrm{r}(\mathrm{cl}(X) \cup x) = \mathrm{r}(X)$. Da (R'2) possiamo inoltre dedurre che

$$\mathrm{r}(X) \leqslant \mathrm{r}(X \cup x) \leqslant \mathrm{r}(\mathrm{cl}(X) \cup x) = \mathrm{r}(X);$$

allora $\mathrm{r}(X) = \mathrm{r}(X \cup x)$, quindi $x \in \mathrm{cl}(X)$ e $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(X))$. Allora $\mathrm{cl}(X) = \mathrm{cl}(\mathrm{cl}(X))$ e (Cl3) è soddisfatto.
Consideriamo ora $X \subseteq E$, $y, z \in E$ tali che $y \in \mathrm{cl}(X \cup z) \setminus \mathrm{cl}(X)$; abbiamo allora che $\mathrm{r}(X \cup z \cup y) = \mathrm{r}(X \cup z)$ e $\mathrm{r}(X \cup y) \neq \mathrm{r}(X)$. Per (R'2) vale $\mathrm{r}(X \cup y) = \mathrm{r}(X) + 1$ e

$$\mathrm{r}(X) + 1 = \mathrm{r}(X \cup y) \leqslant \mathrm{r}(X \cup y \cup z) = \mathrm{r}(X \cup z) \leqslant \mathrm{r}(X) + 1.$$

Allora $\mathrm{r}(X \cup y \cup z) = \mathrm{r}(X \cup y)$, e quindi $z \in \mathrm{cl}(X \cup y) \setminus \mathrm{cl}(X)$, soddisfacendo così (Cl4). □

Vogliamo ora mostrare che gli assiomi di chiusura, rango e rango locale sono criptomorfi ai sistemi assiomatici visti in precedenza.

Proposizione 1.5.3. *Sia cl un operatore che soddisfa (Cl1)-(Cl4), e definiamo*

$$\mathscr{I} := \{X \subseteq E : x \notin cl(X \setminus x)\ \forall x \in X\};$$

allora $\mathscr{I} \in \boldsymbol{I}(E)$.

Dimostrazione. (I1) è banalmente soddisfatto.
Consideriamo $I \in \mathscr{I}$ e $I' \subseteq I$; se $x \in I'$, allora $x \in I$ e quindi $x \notin \mathrm{cl}(I \setminus x)$. Per (Cl2), $\mathrm{cl}(I' \setminus x) \subseteq \mathrm{cl}(I \setminus x)$, e quindi $x \notin \mathrm{cl}(I' \setminus x)$. Abbiamo allora che $I' \in \mathscr{I}$ e (I2) è soddisfatto.
Nella dimostrazione restante andremo ad utilizzare il seguente risultato:

Lemma 1.5.4. *Sia $X \subseteq E$ e $x \in E$, se $X \in \mathscr{I}$ e $(X \cup x) \notin \mathscr{I}$, allora $x \in cl(X)$.*

Dimostrazione. Poiché $X \cup x \notin \mathscr{I}$, esiste $y \in (X \cup x)$ tale che $y \in \mathrm{cl}((X \cup x) \setminus y)$. Se $x = y$, la tesi è banale. Supponiamo $x \neq y$, allora $(X \cup x) \setminus y = (X \setminus y) \cup x$ e $y \in \mathrm{cl}((X \setminus y) \cup x) \setminus \mathrm{cl}(X \setminus y)$. Per (Cl4), $x \in \mathrm{cl}((X \setminus y) \cup y) = \mathrm{cl}(X)$.
□

Vogliamo ora dimostrare che (I3) è soddisfatto. Consideriamo $I_1, I_2 \in \mathscr{I}$ tali che $|I_1| < |I_2|$ e supponiamo per assurdo che (I3) non valga per la coppia (I_1, I_2). Tra tutte le coppie tali che (I3) non è soddisfatto, scegliamo (I_1, I_2) tale che $|I_1 \cap I_2|$ sia massimale. Scegliamo $y \in I_2 \setminus I_1$ e consideriamo $I_2 \setminus y$. Assumiamo che $I_1 \subseteq \mathrm{cl}(I_2 \setminus y)$, allora per (Cl2) e (Cl3) abbiamo che

$$\mathrm{cl}(I_1) \subseteq \mathrm{cl}(I_2 \setminus y);$$

e poiché $y \notin \mathrm{cl}(I_2 \setminus y)$, vale $y \notin \mathrm{cl}(I_1)$. Per il Lemma 1.5.4, $I_1 \cup y \in \mathscr{I}$, e quindi (I3) vale per la coppia (I_1, I_2) così scelta: il che è una contraddizione. Possiamo allora concludere che $I_1 \nsubseteq \mathrm{cl}(I_2 \setminus y)$ e quindi esiste $t \in I_1$ tale che $t \notin \mathrm{cl}(I_2 \setminus y)$: chiaramente $t \in I_1 \setminus I_2$. Inoltre, per il Lemma 1.5.4, $((I_2 \setminus y) \cup t) \in \mathscr{I}$. Poiché

$$|I_1 \cap ((I_2 \setminus y) \cup t)| > |I_1 \cap I_2|,$$

allora (I3) vale per la coppia $(I_1, (I_2 \setminus y) \cup t)$. Allora esiste $x \in ((I_2 \setminus y) \cup t) \setminus I_1$ tale che $I_1 \cup x \in \mathscr{I}$. Ma $x \in I_2 \setminus I_1$, quindi (I3) è soddisfatto da (I_1, I_2), contraddicendo l'ipotesi per assurdo. Quindi (I3) è soddisfatto.

□

Grazie a quanto visto in precedenza, possiamo affermare che:

Proposizione 1.5.5. *Gli assiomi di rango, di chiusura e degli indipendenti sono criptomorfi attraverso i seguenti criptomorfismi:*

$$\boldsymbol{r}(E) \xrightarrow{1.5.2} \boldsymbol{cl}(E) \xrightarrow{1.5.3} \boldsymbol{I}(E) \xrightarrow{\epsilon\delta} \boldsymbol{r}(E).$$

E quindi vale:

Corollario 1.5.6. *Un operatore $cl \in \boldsymbol{cl}(E)$ se e solo se soddisfa le seguenti condizioni:*

(Cl1) *Per ogni $X \subseteq E$, $X \subseteq cl(X)$,*

(Cl2) *Per ogni $X, Y \subseteq E$, se $X \subseteq Y$ allora $cl(X) \subseteq cl(Y)$,*

(Cl3) *Per ogni $X \subseteq E$, $cl(cl(X)) = cl(X)$,*

(Cl4) *Per ogni $X \subseteq E$ e per ogni $y, z \in E$, se $y \in cl(X \cup z) \setminus cl(X)$, allora $z \in cl(X \cup y) \setminus cl(X)$.*

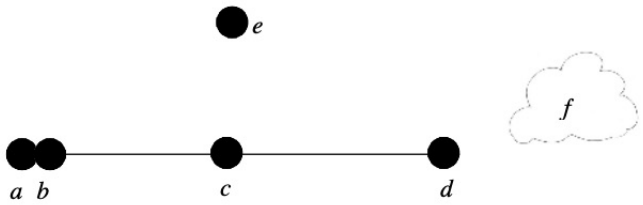


Figura 1.3: Matroide dell'Esempio 2

Esempio 8. Riprendiamo l'Esempio 1, ricordando che E è uno spazio vettoriale su un campo finito. Definiamo una matroide $M(E) = (E, \mathrm{r})$ dove la funzione rango r è semplicemente la funzione dimensione su E. Notiamo che la formula di Grassman è un caso particolare di (R3).

Possiamo definire una matroide $M(E) = (E, \mathrm{cl})$, dove l'operatore di chiusura cl è la funzione Span.

Esempio 9. Continuiamo ad analizzare la matroide definita nell'Esempio 2; in particolare vogliamo trovare il rango dei vari sottoinsiemi. Una lista completa prevederebbe l'elencazione di $2^6 = 64$ sottoinsiemi, ma possiamo organizzare i dati per rendere l'analisi più scorrevole.
Sia $A \subseteq E$, allora:

- $\mathrm{r}(A) = 0$: $\mathrm{r}(\varnothing) = 0$ è sempre vero; inoltre anche ogni cappio ha rango 0, quindi nel nostro caso $\mathrm{r}(f) = 0$.

- $\mathrm{r}(A) = 1$: Tutti i singoletti, eccettuati i cappi, hanno rango 1; inoltre se si aggiunge il cappio f ad un sottoinsieme, il rango di questi non aumenta. Dunque hanno rango 1 i sottoinsiemi $a, b, c, d, e, af, bf, cf, df, ef$. Infine anche ab e abf hanno rango 1.

- $\mathrm{r}(A) = 2$: Un insieme ha rango 2 se geometricamente genera una linea retta. Quindi tra i punti a, b, c e d possiamo sceglierne due o più (eccetto ab) per generare la retta che contiene questi quattro punti. Ci sono dieci differenti sottoinsiemi così costruibili. Anche alcuni insiemi che contengono e possono avere rango 2, in particolare $\mathrm{r}(abe) = \mathrm{r}(ae) = \mathrm{r}(be) = \mathrm{r}(ce) = \mathrm{r}(de) = 2$. Questi corrispondono alla linea passante per quei due punti, non rappresentata in figura. Infine, come nel punto precedente, a questi insiemi possiamo aggiungere il cappio f senza aumentarne il rango.

- r$(A) = 3$: r$(A) = 3$ se A contiene una base. Nel nostro caso ricordiamo che le basi sono ace, ade, bce, bde e cde; quindi ogni sovrainsieme di uno di questi avrà rango 3.

Vediamo alcuni esempi di chiusura di elementi di M. Dato ad, abbiamo che cl(ad)=$abcdf$: questo si evince facilmente dalla definizione 1.18, difatti aggiungere ad ad elementi che giaciono sulla retta ad non va ad aumentarne il rango, così come aggiungere il cappio f.

Considerando l'elemento a abbiamo invece cl$(a) = abf$, poiché aggiungere tanto l'elemento b quanto l'elemento f non ne aumenta il rango.

1.6 Matroidi rappresentabili

In questa sezione daremo un'idea del concetto di matroide rappresentabile attraverso alcuni esempi. L'esposizione sarà superficiale in quanto si è scelto di presentare tale argomento per completezza e non per rilevanza nella trattazione.

Definizione 1.19. Una matroide $M(E)$ è **rappresentabile su un campo** F se esiste uno spazio vettoriale V su F ed un'applicazione $f : E \to V$ tale che $A \subseteq E$ è un insieme indipendente di E se e solo se $f(A)$ è linearmente indipendente in V. Diciamo allora che f è una **rappresentazione** di $M(E)$.

Definizione 1.20. Una matroide $M(E)$ è **rappresentabile** o **lineare** se esiste un campo F tale che $M(E)$ è rappresentabile su F.

Osservazione 4. La rappresentazione di una matroide su E può essere descritta attraverso una matrice a coefficienti in F tale che, se $C = \{c_1, \ldots, c_n\}$ è l'insieme delle colonne di A e $E = \{x_1, \ldots, x_n\}$, allora $f(x_i) = c_i$ per ogni $i = 1, .., n$.

Esempio 10. La matroide uniforme U_n^r è definita come la matroide su un insieme E di n elementi i cui insiemi indipendenti sono tutti e soli gli insiemi che contengono al più r elementi.

Vediamo che U_4^2 non è rappresentabile su $\mathbb{Z}_2$.

Per definizione di U_4^2 sappiamo che per $U \subseteq E$, r$(U) = |U|$ se $|U| \leqslant 2$, e r$(U) = 2$ se $|U| > 2$. In particolare, r$(E) = 2$. Se esistesse una rappresentazione di U_4^2 su $\mathbb{Z}_2$, la matrice corrispondente sarebbe della forma

$$A = \begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{bmatrix}$$

con $* \in \mathbb{Z}_2$, nessuna colonna nulla e due colonne quasiasi linearmente indipendenti. Questo è impossibile poiché in $\mathbb{Z}_2$ esistono solo tre possibili colonne distinte non nulle.

Notiamo però che U_4^2 è rappresentabile su altri campi. Per esempio, su $\mathbb{R}$, abbiamo una possibile rappresentazione data da

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}.$$

Definizione 1.21. Una matroide è **binaria** se è rappresentabile su $\mathbb{Z}_2$.

Nell'esempio precedente abbiamo visto che la matroide uniforme U_4^2 è rappresentabile solo in alcuni campi; ci chiediamo quindi se esistano matroidi non rappresentabili su nessun campo. La risposta è affermativa: varie matroidi non rappresentabili sono state trovate nel tempo, qui ne proponiamo una a titolo di esempio.

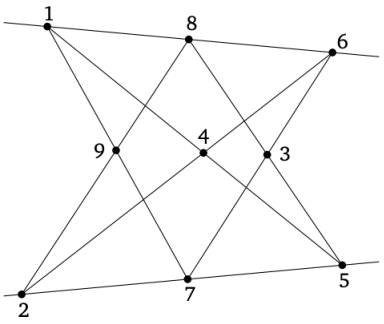


Figura 1.4: Matroide Non-Pappo

Esempio 11 (Matroide 'Non-Pappo')**.** Sia M la matroide di rango 3 su 9 elementi la cui rappresentazione geometrica è data nella Figura 1.4. La configurazione riprende la configurazione di Pappo senza la linea $(3, 4, 9)$. Se M fosse rappresentabile su un campo, un risultato base della geometria proiettiva ci permetterebbe di affermare che l'insieme dei punti $\{3, 4, 9\}$ è linearmente dipendente, ma ciò non è vero in M. Quindi M non è rappresentabile su nessun campo.

Capitolo 2

Un esempio di matroide: le matroidi grafiche

I due esempi fondamentali presentati da Whitney nell'articolo *On the Abstract Properties of Linear Dependence* sono le matroidi vettoriali e le matroidi grafiche. Non ci deve quindi sorprendere che molti degli aspetti della Teoria delle Matroidi sono estensioni o sviluppi di concetti originariamente introdotti negli spazi vettoriali o nei grafi.

In questo capitolo andremo ad analizzare in particolare la struttura dei grafi e osserveremo come questa soddisfi i diversi sistemi assiomatici che caratterizzano il concetto di matroide. Sarà quindi possibile definire una matroide grafica sull'insieme dei lati di un grafo.

Scegliamo di non seguire strettamente l'ordine di presentazione dato nel capitolo precedente, in quanto alcuni elementi sono più facilmente introducibili in un secondo momento: ad esempio il concetto di base si può facilmente introdurre come indipendente massimale.

L'ultima sezione tratterà del polinomio di Tutte. Nel 1947 W.T. Tutte introdusse un polinomio a variabili indipendenti x, y, associato ad un grafo dato, che contiene numerose informazioni sul grafo in questione. L'approccio di Tutte fu esteso da H.H. Crapo e T.H. Brylawski attraverso l'introduzione di un analogo polinomio per le matroidi.

2.1 Nozioni preliminari

In questa sezione presenteremo alcune nozioni di Teoria dei Grafi, necessarie alla comprensione delle sezioni successive.

Sia $G = (V, E)$ un grafo finito non orientato dove V rappresenta l'insieme dei vertici ed E l'insieme dei lati, possiamo allora dare le seguenti definizioni:

Definizione 2.1. Un lato $e \in E$ è un **cappio** se $e = (v, v)$ con $v \in V$.

Definizione 2.2. Una successione finita di vertici $(v_1, \ldots, v_n)$ è un **cammino** se $(v_i, v_{i+1}) \in E$ per ogni $i = 1, .., n-1$.

Definizione 2.3. Un **circuito** è un cammino $(v_1, \ldots, v_n)$ tale che $v_i \neq v_j$ per ogni $i \neq j$ tranne $v_1 = v_n$.

Definizione 2.4. Un grafo $G' = (V', E')$ è un **sottografo** di $G = (E, V)$ se $V' \subseteq V$ e $E' \subseteq E$.

Definizione 2.5. Un **sottografo indotto** $G' = (V', E')$ è un grafo tale che $V' \subseteq V$ ed $(u, v) \in E' \subseteq E$ se e solo se $u, v \in V'$.

Definizione 2.6. Dato $e \in E$ possiamo definire la **restrizione rispetto ad un lato** di G come il grafo ottenuto dall'eliminazione di e da G. Lo indicheremo con $G \setminus e$.

Definizione 2.7. Dato $e \in E$ che non sia un cappio, possiamo definire la **contrazione rispetto ad un lato** di G come il grafo ottenuto dall'identificazione degli estremi di e e dall'eliminazione di e da G. Lo indicheremo con $G \cdot e$.

Definizione 2.8. Un grafo G è **connesso** se per ogni $u, v \in V$ esiste un cammino che li collega.

Una **componente connessa** $G' = (V', E')$ di $G = (V, E)$ è un sottografo di G connesso tale che per ogni $w \in V'$ non esistono cammini che lo congiungono a un vertice $v \in V \setminus V'$.

Definizione 2.9. Un lato $e \in E$ è un **ponte** se la sua rimozione aumenta il numero di componenti connesse di G.

Definizione 2.10. Un **albero** è un grafo connesso privo di circuiti.

Una **foresta** è un grafo privo di circuiti, ovvero tale che le sue componenti connesse sono alberi.

Osservazione 5. Un vertice isolato è un albero. Analogamente, un insieme di punti isolati è una foresta.

Definizione 2.11. Un **sottoalbero** di G è un albero sottografo di G .

Una **sottoforesta** di G è una foresta sottografo di G .

Definizione 2.12. Il vertice $v \in V$ è una **foglia** se esiste uno e un solo lato $e \in E$ tale che $v \in e$.

Proposizione 2.1.1. *Un albero contiene sempre due foglie.*

Dimostrazione. Consideriamo un cammino massimale $(v_1, \ldots, v_n)$ e supponiamo per assurdo che v_1 non sia una foglia: esiste quindi un lato $(v_1, w) \in E$ tale che $(v_1, w) \neq (v_1, v_2)$. Se $w = v_i$ per un certo $i = 1, \ldots, n$, allora esiste un circuito, e ciò contraddice il fatto che il grafo considerato è un albero. Se $w \neq v_i$ per ogni $i = 3, \ldots, n$, allora posso prolungare il cammino scelto, in contraddizione con l'ipotesi di massimalità. Un ragionamento analogo dimostra che anche v_n è una foglia.

□

Proposizione 2.1.2. *Se G è un albero allora $|E| = |V| - 1$.*

Dimostrazione. Procediamo per induzione su $|V|$.
Se $|V| = 1$, ovviamente $|E| = 0$ poichè non possono esserci cappi, quindi $|E| = |V| - 1$.
Supponiamo ora che $|V| = n + 1$. Per la Proposizione 2.1.1 l'albero G ha una foglia v, quindi il sottografo indotto $G' = (V' = V \setminus v, E')$ è ancora un albero con $|V'| = n$. Per ipotesi induttiva abbiamo che

$$|E| - 1 = |E'| = |V'| - 1 = |V| - 1 - 1,$$

e quindi $|E| = |V| - 1$.

□

Corollario 2.1.3. *Se G è una foresta allora $|E| = |V| - c(G)$, dove $c(G)$ è il numero delle componenti connesse di G.*

Definizione 2.13. Se G è connesso, possiamo definire un **albero generatore** di G come un sottoalbero $G' = (V', E')$ di G tale che $V' = V$.

Una **foresta generatrice** di G è una sottoforesta di G tale che le sue componenti connesse sono alberi generatori delle componenti connesse di G.

Proposizione 2.1.4. *Se G è connesso allora possiede un albero generatore.*

Dimostrazione. Per dimostrare l'esistenza di un albero generatore, procediamo con la costruzione dello stesso attraverso l'algoritmo di visita in profondità.

Consideriamo $v \in V$, $T = \{v\}$ e procediamo come segue:

1. Consideriamo un qualsiasi vertice $w \notin T$ che sia adiacente a v, aggiungiamo a T il vertice w e il lato (v, w);

2. Ripartiamo dal punto 1. sostituendo v con w. Se non esiste $w \notin T$ e adiacente a v, ripartiamo dal vertice inserito nel passo precedente;

3. L'algoritmo termina quando tutti i vertici di G sono stati inseriti in T.

□

Corollario 2.1.5. *Ogni grafo possiede una foresta generatrice.*

Definizione 2.14. Sia $G = (V, E)$, consideriamo $P_1, \ldots, P_n \in \mathbb{R}^3$ punti distinti con $n = |V|$ e sia $f : V \to \{P_1, \ldots, P_n\}$ un'applicazione tale che $f(v_i) = P_i$ per ogni $i = 1, \ldots, n$. Indichiamo con $[P_i, P_j]$ i segmenti di estremi P_i e P_j, definiamo allora una **realizzazione piana** di G come

$$R(G) := \cup\{[P_i, P_j] : v_i \text{ è adiacente a } v_j \text{ in } G\} \cup \{P_1, \ldots, P_n\}.$$

Definizione 2.15. Un grafo $G = (V, E)$ si dice **planare** se è rappresentabile sul piano senza intersezioni di lati al di fuori dei vertici, ovvero se esiste una realizzazione piana $R(G)$ omoemorfa a un sottoinsieme di $\mathbb{R}^2$.

Definizione 2.16. Un **grafo piano** è un insieme di punti $V = \{P_1, \ldots, P_n\}$ in $\mathbb{R}^2$ e di m segmenti di curve semplici di $\mathbb{R}^2$ tali che:

1. ogni segmento sia incidente con al più due punti di V;

2. dati due segmenti e_1, e_2 vale $e_1 \cap e_2 \subseteq V$.

Definizione 2.17. Se G è un grafo piano, una **faccia** di G è una componente connessa di $\mathbb{R}^2 \setminus E$, dove E è l'insieme dei lati di G.

Definizione 2.18. Sia $G = (V, E)$ un grafo piano, definiamo il **grafo duale** $G^* = (F, E^*)$ in cui ogni vertice di F è una faccia di G, ed $e^* = (f_1, f_2) \in E^*$ se e solo se esiste $e \in E$ che sia adiacente a f_1 ed f_2.

Osservazione 6. Due realizzazioni piane possono avere grafi duali differenti, per questo definiamo il duale di grafi piani e non planari.

Osservazione 7. Notiamo che vi è una naturale corrispondenza tra i lati di G e quelli di G^*.

Proposizione 2.1.6. *Se G è un grafo piano connesso e G^* è il suo grafo duale, allora $(G^*)^* = G$.*

Definizione 2.19. Un **taglio** di G è un insieme di lati $T \subseteq E$ che collegano un dato sottoinsieme $S \subseteq V$ con il suo complementare..

Per un grafo connesso, questo equivale a dire che:

- $(V, E \setminus T)$ è sconnesso,

- $(V, E \setminus (T \setminus t))$ è connesso per ogni $t \in T$.

In un grafo qualsiasi, la rimozione di un taglio sconnette una componente connessa, comportando così l'aumento di 1 del numero di componenti connesse.

Osservazione 8. Sia G un grafo e G^* il suo duale, allora C è un circuito di G se e solo se è un taglio di G^*.

Analogamente, poiché $(G^*)^* = G$, l'insieme T è un taglio di G se e solo se è un circuito di G^*.

2.2 Indipendenti e basi in un grafo

In questa sezione andremo ad analizzare la famiglia degli insiemi indipendenti in un grafo, osservando come questa coincida con l'insieme delle sottoforeste. Utilizzeremo inoltre i criptomorfismi introdotti nel capitolo precedente per analizzare la famiglia delle basi in un grafo. Sarà quindi possibile definire il concetto di matroide grafica e di matroide grafica duale sull'insieme dei lati del grafo.

Notazione 2. Per semplicità, diremo che I è una sottoforesta di G per indicare che I è l'insieme dei lati di una sottoforesta di G. Analogamente per B sottoforesta generatrice di G.

Proposizione 2.2.1. *La famiglia $\mathscr{I}$ delle sottoforeste di G soddisfa gli assiomi:*

(I1) $\mathscr{I} \neq \varnothing$,

(I2) $\mathscr{I}$ *è una famiglia discendente,*

(I3) *Per ogni $I_1, I_2 \in \mathscr{I}$, se $|I_1| < |I_2|$, allora esiste $x \in I_2 \setminus I_1$ tale che $I_1 \cup x \in \mathscr{I}$.*

Dimostrazione. L'insieme vuoto non è un circuito, quindi $\varnothing \in \mathscr{I}$ e (I1) è soddisfatto.

Consideriamo $I_1, I_2 \subseteq E$ tali che $I_1 \subseteq I_2$ e $I_2 \in \mathscr{I}$; allora I_2 non contiene circuiti, e quindi neanche I_1. Dunque $I_1 \in \mathscr{I}$ e (I2) è soddisfatto.

Siano $I_1, I_2 \in \mathscr{I}$ tali che $|I_1| < |I_2|$. Per il Corollario 2.1.3 sappiamo che $|I_1| = |V| - k_1$ dove k_1 è il numero delle componenti connesse di I_1; analogamente $|I_2| = |V| - k_2$. Poiché $|I_1| < |I_2|$, abbiamo che $k_1 > k_2$, cioè I_2 ha meno componenti connesse di I_1; allora esiste $x = (u, v) \in I_2$ tale che u e v appartengono a due componenti connesse diverse di I_1, ovvero non esiste

un cammino in I_1 che congiunge tali vertici. Poiché l'aggiunta del lato x a I_1 non genera un circuito, abbiamo che $I_1 \cup x \in \mathscr{I}$, soddisfacendo così (I3).
□

Osservazione 9. Possiamo definire la matroide $M(G) = (E, \mathscr{I})$, dove ricordiamo che E è l'insieme dei lati del grafo G. Questa matroide è chiamata **matroide dei cicli**. Una matroide isomorfa alla matroide dei cicli di un qualche grafo è chiamata **matroide grafica**.

Introduciamo la famiglia delle basi di G attraverso il concetto di foresta generatrice.

Proposizione 2.2.2. *La famiglia $\mathscr{B}$ delle foreste generatrici di G soddisfa gli assiomi:*

(B1) *$\mathscr{B} \neq \varnothing$,*

(B2) *$\mathscr{B}$ è un'anticatena di E,*

(B3) *Per ogni $X, Y \subseteq E$, $X \subseteq Y$, se esistono B_1, $B_2 \in \mathscr{B}$ tali che $X \subseteq B_1$ e $B_2 \subseteq Y$, allora esiste $B_3 \in \mathscr{B}$ tale che $X \subseteq B_3 \subseteq Y$.*

Dimostrazione. Per semplicità supponiamo che G sia connesso, ma il ragionamento seguito è facilmente estendibile alle componenti connesse di G nel caso in cui questo non sia connesso.

Vogliamo dimostrare che $\mathscr{B} = \max(\mathscr{I})$, dove $\mathscr{I}$ ricordiamo essere la famiglia delle sottoforeste di G. Ovviamente $\mathscr{B} \subseteq \mathscr{I}$. Sia $B \in \mathscr{B}$ e consideriamo $I \in \mathscr{I}$ tale che $B \subseteq I$. Se per assurdo vale $B \subset I$, allora esiste $e \in I \setminus B$. Poiché abbiamo supposto G connesso, B è un albero generatore e quindi connette tutti i vertici di G; allora il lato e ha come estremi due vertici che sono già connessi da un altro cammino, generando un circuito. Il che è assurdo poiché I è un albero. Abbiamo dimostrato che $\mathscr{B} \subseteq \max(\mathscr{I})$.

Viceversa, sia $I \in \max(\mathscr{I})$, allora ricopre tutti i vertici di G. Infatti, se esiste $u \in V$ ma non estremo di qualche lato in I, allora, poiché G è connesso, si può aggiungere ad I il lato (u, v) per un certo $v \in V$, e quindi la massimalità non è soddisfatta. Allora $\max(\mathscr{I}) \subseteq \mathscr{B}$, e quindi $\mathscr{B} = \max(\mathscr{I})$.

Per la Proposizione 2.2.1 sappiamo che $\mathscr{I}$ soddisfa (I1)-(I3); quindi, per l'interpretazione presentata nella Proposizione 1.2.3, abbiamo che $\mathscr{B}$ soddisfa le condizioni (B1)-(B3).

□

Osservazione 10. L'esistenza delle foreste generatrici, e quindi l'assioma (B1), ci è garantita dal Corollario 2.1.5.

Osservazione 11. Possiamo definire la matroide $(E, \mathscr{B})$: queste è criptomorfa alla matroide dei cicli.

Ora che abbiamo definito le basi in un grafo G, risulta naturale verificare la relazione tra la matroide grafica duale e il grafo duale G^*.

Definizione 2.20. Sia $G = (V; E)$ un grafo piano e $G^* = (F; E^*)$ il suo duale, definiamo allora $\mathscr{B}_*$ l'insieme delle foreste generatrici di G^*.

Proposizione 2.2.3. *Siano* $M_G(E) := (E, \mathscr{B})$ *e* $M_{G^*}(E^*) := (E^*, \mathscr{B}_*)$, *allora* $M_G^*(E) \cong M_{G^*}(E^*)$.

Dimostrazione. Ricordiamo che $M_G^*(E) = (E, \mathscr{B}^*)$ dove $\mathscr{B}^* = \{E \setminus B : B \in \mathscr{B}\}$. Innanzitutto notiamo che vi è una naturale corrispondenza tra E ed E^* per definizione di E^*.

Supponiamo per semplicità che G sia connesso, ma il ragionamento seguito è facilmente estendibile alle componenti connesse di G, nel caso in cui non sia connesso.

Se G è un albero, la sua unica base è E stesso, e quindi $\mathscr{B}^* = \{\varnothing\}$; inoltre G^* avrà un unico vertice corrispondente all'unica faccia di G, e dunque $\mathscr{B}_* = \{\varnothing\} = \mathscr{B}^*$.

Supponiamo allora che G non sia un albero. Consideriamo un albero generatore $B \in \mathscr{B}^*$, sia B' il corrispondente insieme di lati in E^* e definiamo $B^* = E^* \setminus B'$. Se per assurdo B^* non è incidente a tutti i vertici di F, allora, grazie alla Proposizione 2.1.6, si osserva facilmente che B contiene un ciclo e questo è assurdo poiché B è un albero. Se per assurdo B^* contiene un circuito, allora esso circonda una faccia f^* che non è adiacente a nessun lato di B', ed il vertice di $G = (G^*)^*$ corrispondente a tale faccia non è toccato da B. Ciò è assurdo poiché B è un albero generatore, quindi B^* è un albero che tocca tutti i vertici, e dunque è un albero generatore per G^*.

Abbiamo dimostrato che $\mathscr{B}^* \subseteq \mathscr{B}_*$; un ragionamento analogo dimostra l'inclusione inversa, e quindi $\mathscr{B}^* = \mathscr{B}_*$.

□

Esempio 12. Riprendiamo l'Esempio 4, ricordando che M è la matroide sull'insieme $E = \{a, b, c, d, e, f\}$ con basi $\{ace, ade, bce, bde, cde\}$. Una sua rappresentazione è riportata nella Figura 2.1, (i).

Il grafo G (Figura 2.1, (ii)) corrisponde ad una differente rappresentazione di M, definita matroide grafica.

Poichè G è connesso, gli indipendenti di G sono tutti i sottoalberi; invece le basi sono gli alberi generatori.

Come osservato in precedenza, l'elemento e è un ponte, quindi esso può essere aggiunto ad ogni insieme indipendente a cui non appartiene per ottenere un altro insieme indipendente. In particolare, e è in tutte le basi.

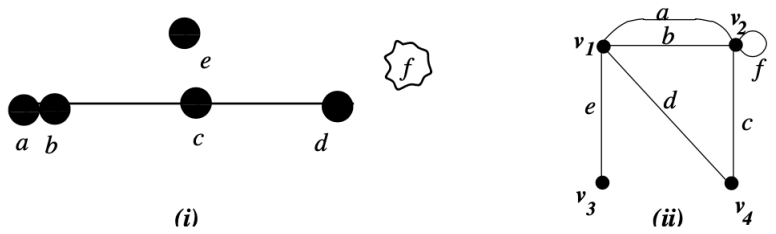


Figura 2.1: (i) Matroide dell'Esempio 2 (ii) Grafo G

2.3 Dipendenti, generatori e insiemi non generatori in un grafo

In questa sezione andremo ad analizzare il concetto di insieme dipendente, insieme generatore e insieme non generatore in un grafo.

Notazione 3. Per semplicità, diremo che D è una sottografo di G per indicare che è l'insieme dei lati di un sottografo di G.

Definizione 2.21. Definiamo la famiglia $\mathscr{D}$ degli insiemi dipendenti di un grafo come $\mathscr{D} := \text{opp}(\mathscr{I})$, dove $\mathscr{I}$ è la famiglia delle sottoforeste. Quindi $D \in \mathscr{D}$ se e solo se D è un sottografo di G che contiene circuiti.

Proposizione 2.3.1. *La famiglia $\mathscr{D}$ soddisfa gli assiomi:*

(D1) $\varnothing \notin \mathscr{D}$,

(D2) $\mathscr{D}$ *è una famiglia ascendente,*

(D3) *Per ogni $D_1, D_2 \in \mathscr{D}$, se $D_1 \cap D_2 \notin \mathscr{D}$, allora per ogni $x \in E$ vale $(D_1 \cup D_2) \setminus x \in \mathscr{D}$.*

Dimostrazione. La tesi è ovvia per la Definizione 1.12 e la Proposizione 1.3.1. □

Definizione 2.22. Se $G = \bigcup_{i \in I} T_i$ dove $T_i = (V_i, E_i)$ sono le componenti connesse di G, allora $S \in \mathscr{S}$ se e solo se $S = \bigcup_{i \in I} T_i'$ con $T_i' = (V_i', E_i)$ sottografo connesso di T_i tale che $V_i' = V_i$ per ogni $i \in I$.

Notiamo che i vertici di S coincidono con i vertici di G.

Proposizione 2.3.2. *La famiglia $\mathscr{S}$ soddisfa gli assiomi:*

(S1) $\mathscr{S} \neq \varnothing$,

(S2) *$\mathscr{S}$ è una famiglia ascendente,*

(S3) *Per ogni $S_1, S_2 \in \mathscr{S}$, se $|S_1| > |S_2|$, allora esiste $x \in S_1 \setminus S_2$ tale che $S_1 \setminus x \in \mathscr{S}$.*

Dimostrazione. Vogliamo dimostrare che $\mathscr{S} = \text{upp}(\mathscr{B})$, dove $\mathscr{B}$ ricordiamo essere la famiglia delle foreste generatrici di G. Ovviamente $\mathscr{B} \subseteq \mathscr{S}$.

Per semplicità supponiamo che G sia connesso, ma il ragionamento seguito è facilmente estendibile alle componenti connesse di G nel caso in cui questo non sia connesso.

Sia $S \in \mathscr{S}$, allora i vertici di S coincidono con V. Per la Proposizione 2.1.4 il grafo S ha un albero generatore B il cui insieme dei vertici coincide con V; quindi B è albero generatore di G, ovvero $B \in \mathscr{B}$, e $B \subseteq S$. Allora $S \in \text{upp}(\mathscr{B})$, e quindi $\mathscr{S} \subseteq \text{upp}(\mathscr{B})$.

Viceversa, sia $S \in \text{upp}(\mathscr{B})$, allora esiste $B \in \mathscr{B}$ tale che $B \in \mathscr{B}$ e $B \subseteq S$. Abbiamo che S ricopre tutti i vertici di G; inoltre S è connesso poiché ottenuto aggiungendo lati a B, che sappiamo essere connesso. Quindi $S \in \mathscr{S}$ e $\text{upp}(\mathscr{B}) \subseteq \mathscr{S}$. Allora $\mathscr{S} = \text{upp}(\mathscr{B})$.

Per la Proposizione 2.2.2 sappiamo che $\mathscr{B}$ soddisfa (B1)-(B3); quindi, per il Teorema 1.4.3, abbiamo che $\mathscr{S}$ soddisfa le condizioni (S1)-(S3).

□

Analogamente all'introduzione degli insiemi dipendenti in un grafo, possiamo descrivere il concetto di insieme non generatore in un grafo.

Definizione 2.23. Definiamo la famiglia $\mathscr{N}$ degli insiemi non generatori di un grafo come $\mathscr{N} := \text{opp}(\mathscr{S})$, dove $\mathscr{S}$ è la famiglia degli insiemi generatori di G.

Proposizione 2.3.3. *La famiglia $\mathscr{N}$ soddisfa gli assiomi:*

(N1) *$E \notin \mathscr{N}$,*

(N2) *$\mathscr{N}$ è una famiglia discendente,*

(N3) *Per ogni $N_1, N_2 \in \mathscr{N}$, se $N_1 \cup N_2 \notin \mathscr{N}$, allora per ogni $x \in E$ vale $(N_1 \cap N_2) \cup x \in \mathscr{N}$.*

Dimostrazione. La tesi è ovvia per la Definizione 2.23 e la Proposizione 1.3.1.

□

Esempio 13. Riprendiamo l'Esempio 12. L'elemento f è un cappio, termine usato anche nella Teoria delle Matroidi per indicare un elemento che non appartiene a nessun indipendente. Notiamo infatti che f è un circuito,

quindi è un insieme dipendente e qualsiasi insieme lo contenga è a sua volta dipendente.

Vari sono gli insiemi generatori di G: in particolare lo sono tutte le basi, che ricordiamo essere ace, ade, bce, bde, cde, e qualsiasi insieme ottenuto da esse attraverso l'aggiunta di uno o più lati.

2.4 Rango e chiusura di un grafo

In questa sezione andremo a definire il rango di un grafo e verificheremo come questo soddisfi gli assiomi di rango per una matroide. Procederemo analogamente per il concetto di chiusura transitiva.

Definizione 2.24. Dato un grafo $G = (V, E)$, possiamo definire la funzione **rango** r tale che $\mathrm{r}(E) = |V| - c(G)$ dove $c(G)$ è il numero di componenenti connesse di G.

Proposizione 2.4.1. *Il rango di un grafo soddisfa gli assiomi:*

(R1) *Per ogni* $X \subseteq E$, $0 \leqslant r(X) \leqslant |X|$,

(R2) *Per ogni* $X, Y \subseteq E$, *se* $X \subseteq Y$ *allora* $r(X) \leqslant r(Y)$,

(R3) *Per ogni* $X, Y \subseteq E$, $r(X \cup Y) + r(X \cap Y) \leqslant r(X) + r(Y)$.

Dimostrazione. Per il Corollario 2.1.3, $\mathrm{r}(E) = |B|$ dove B è una qualsiasi foresta generatrice di G, ovvero $B \in \mathscr{B}$. Ma per la Proposizione 1.5.1, considerando che $\mathscr{B} = \max(\mathscr{I})$, il rango di E nel senso delle matroidi coincide con la cardinalità delle basi della matroide stessa. Quindi, poiché $\mathscr{B}$ è l'insieme delle basi della matroide grafica di G, le condizioni (R1)-(R3) sono soddisfatte.

□

Definizione 2.25. Un grafo $G' = (V, E')$ è la **chiusura transitiva** di $G = (V, E)$ se per ogni $u, v \in V$ abbiamo che $(u, v) \in E'$ se e solo se esiste un cammino in G da u a v.

Possiamo allora definire l'operatore di chiusura cl: $\mathscr{P}(E) \to \mathscr{P}(E)$ tale che se $S = (W, X)$ è un sottografo di $G = (V, E)$ e $S' = (W, X')$ è la sua chiusura transitiva, allora $\mathrm{cl}(X) = X' \cap E$.

Proposizione 2.4.2. *L'operatore di chiusura cl sopra definito soddisfa gli assiomi:*

(Cl1) *Per ogni* $X \subseteq E$, $X \subseteq cl(X)$,

(Cl2) *Per ogni* $X, Y \subseteq E$*, se* $X \subseteq Y$ *allora* $cl(X) \subseteq cl(Y)$*,*

(Cl3) *Per ogni* $X \subseteq E$*,* $cl(cl(X)) = cl(X)$*,*

(Cl4) *Per ogni* $X \subseteq E$ *e per ogni* $y, z \in E$*, se* $y \in cl(X \cup z) \setminus cl(X)$*, allora* $z \in cl(X \cup y) \setminus cl(X)$*.*

Dimostrazione. La condizione (Cl1) è banalmente soddisfatta.

Consideriamo ora $X, Y \subseteq E$ tali che $X \subseteq Y$. Se due vertici u e v sono connessi in X, sicuramente lo sono anche in Y; quindi se $(u, v) \in \mathrm{cl}(X)$ allora $(u, v) \in \mathrm{cl}(Y)$, ovvero $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$ e (Cl2) è soddisfatto.

Sia $X \subseteq E$, per (Cl2) abbiamo che $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(X))$. Viceversa, se $(u, v) \in \mathrm{cl}(\mathrm{cl}(X))$ allora esiste un cammino in $\mathrm{cl}(X)$ che collega i vertici u e v; poiché la chiusura non altera la connessione, i vertici u e v sono connessi anche in X, e quindi $(u, v) \in \mathrm{cl}(X)$. Allora $\mathrm{cl}(\mathrm{cl}(X)) \subseteq \mathrm{cl}(X)$, $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ e (Cl3) è soddisfatto.

Siano $X \subseteq E$ e $y, z \in E$ tali che $y \in \mathrm{cl}(X \cup z) \setminus \mathrm{cl}(X)$. Osserviamo innanzitutto che $z = (u, v) \notin X$, quindi almeno uno dei vertici u e v non è vertice dei lati in X; in particolare, senza perdere di generalità, possiamo supporre che v non sia in X. Se u non è vertice di qualche lato in X, allora $y = z$ e (Cl4) è ovvio. Consideriamo quindi u vertice in X. Poiché $y \in \mathrm{cl}(X \cup z) \setminus \mathrm{cl}(X)$, allora $y = (w, v)$ con w vertice di qualche lato in X e appartenente alla stessa componente connessa di u. Quindi esiste in X un cammino che collega u a w, e in $X \cup y$ un cammino che collega u a v. Allora $z = (u, v) \in \mathrm{cl}(X \cup y) \setminus \mathrm{cl}(X)$, e (Cl4) è soddisfatto.

□

Osservazione 12. Abbiamo che $\mathrm{r}(X) = \mathrm{r}(\mathrm{cl}(X))$, infatti nella chiusura di X abbiamo aggiunto lati i cui vertici erano già connessi in X, e quindi il rango rimane invariato.

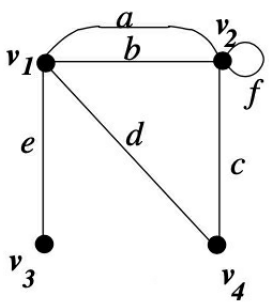


Figura 2.2: Grafo G

Esempio 14. Riprendiamo l'Esempio 12.

Vediamo alcuni esempi del rango di elementi di M. Si comprende facilmente che ogni lato ha rango 1, tranne f: infatti esso ha un unico vertice ed un'unica componente connessa, quindi $\mathrm{r}(f) = 0$. Notiamo che l'aggiunta dell'elemento f ad un qualsiasi insieme di lati X non ne aumenta il rango: infatti se il vertice v_2 è già vertice di uno dei lati in X, allora il lato f non va a cambiarne la connessione; se invece v_2 non è in X, allora vi è l'aggiunta tanto di un vertice quanto di una componente connessa.

Dato bc, abbiamo che $\mathrm{cl}(bc) = abcdf$: questo perché andiamo a considerare tutti i lati di G i cui estremi sono nell'insieme $\{v_1, v_2, v_3\}$. Può succedere inoltre che $X = \mathrm{cl}(X)$; per esempio se $X = \{e\}$ vediamo facilmente che l'unico lato ad avere estremi in $\{v_1, v_3\}$ è e stesso.

2.5 Circuiti ed iperpiani in un grafo

In questa sezione andremo ad analizzare il concetto di circuito in un grafo e verificheremo come questo soddisfi gli assiomi dei circuiti per una matroide. Inoltre introdurremo la struttura di iperpiano attraverso il taglio di un grafo.

Ricordiamo che:

Definizione 2.26. Un **circuito** è un cammino $(e_{1,2}, e_{2,3}, \ldots, e_{n-1,n})$ tale che $v_i \neq v_j$ per ogni $i \neq j$ tranne $v_1 = v_n$.

Proposizione 2.5.1. *Sia $\mathscr{C}$ l'insieme dei circuiti di G, allora $\mathscr{C}$ soddisfa gli assiomi:*

(C1) $\varnothing \notin \mathscr{C}$,

(C2) *$\mathscr{C}$ è un'anticatena,*

(C3) *Per ogni $C_1, C_2 \in \mathscr{C}$ tali che $C_1 \neq C_2$, e per ogni $x \in E$, esiste $C_3 \in \mathscr{C}$ tale che $C_3 \subseteq (C_1 \cup C_2) \setminus x$.*

Dimostrazione. In Teoria delle Matroidi un circuito è un insieme dipendente minimale: se dimostriamo che $\mathscr{C} = \min(\mathscr{D})$, ovvero che i circuiti di G coincidono con gli insiemi dipendenti minimali di G, ovviamente $\mathscr{C}$ soddisfa (C1)-(C3).

Banalmente $\mathscr{C} \subseteq \mathscr{D}$.

Sia $C \in \mathscr{C}$ un circuito: attraverso l'eliminazione di un qualsiasi suo lato si ottiene un albero, quindi un circuito è un insieme dipendente minimale, ovvero $\mathscr{C} \subseteq \min(\mathscr{D})$.

Viceversa, sia $D \in \min(\mathscr{D})$; per definizione di $\mathscr{D}$ esiste un circuito $C \in \mathscr{C} \subseteq \mathscr{D}$ tale che $C \subseteq D$, allora per minimalità di D abbiamo che $C = D$. Quindi $\min(\mathscr{D}) \subseteq \mathscr{C}$ e vale $\min(\mathscr{D}) = \mathscr{C}$.

□

Una differente dimostrazione della Proposizione 2.5.1 può essere data attraverso la verifica diretta degli assiomi (C1)-(C3) per la famiglia $\mathscr{C}$ dei circuiti di G. Seppure non sia necessaria, la riportiamo in tale sede poiché interessante di per sé.

Dimostrazione. Chiaramente $\varnothing \notin \mathscr{C}$, quindi (C1) è soddisfatto.

Consideriamo $C_1, C_2 \in \mathscr{C}$ tali che $C_1 \subseteq C_2$. Se $C_1 = (e_{1,2}, \ldots, e_{m-1,m})$ e $C_2 = (e_{1,2}, \ldots, e_{m-1,m}, \ldots, e_{n-1,n})$, ovvero $C_1 \subset C_2$, allora $v_m = v_1$, ma questo è assurdo poiché, siccome C_2 è un circuito, abbiamo che $v_m \neq v_1$. Quindi $\mathscr{C}$ è un'anticatena e (C2) è soddisfatto.

Consideriamo $C_1, C_2 \in \mathscr{C}$ tali che $C_1 \neq C_2$, e sia $x \in E$. Se $x \notin C_1 \cap C_2$, (C3) è banale; supponiamo quindi che $x = (u, v) \in C_1 \cap C_2$, ovvero x è un lato di entrambi i circuiti. Per costruire il circuito C_3 che contiene solo lati di $(C_1 \cup C_2) \setminus x$ procediamo come segue: partendo dal vertice u, seguiamo il cammino di $C_2 \setminus x$ fino al primo vertice w tale che il lato successivo di $C_2 \setminus x$ non è in C_1. Tale vertice, che può anche essere uguale ad u, esiste poiché $C_1 \neq C_2$. Proseguiamo ora lungo $C_2 \setminus x$ fino ad incontrare un vertice $z \in C_1$; poiché in particolare $v \in C_1$, esiste un vertice z così definito. Sia $C_1 \setminus x$ che $C_2 \setminus x$ contengono un cammino che congiunge w e z: unendo questi due cammini otteniamo il circuito C_3 cercato. Quindi (C3) è soddisfatto.

□

Osservazione 13. Possiamo definire la matroide $M(G) = (E, \mathscr{C})$, dove E è l'insieme dei lati del grafo G. Tale matroide è criptomorfa alla matroide $(E, \mathscr{I})$, possiamo quindi definirla matroide grafica.

Notiamo inoltre che i circuiti dei grafi corrispondono ai circuiti delle matroidi: questo perché il termine è stato ripreso da Teoria dei Grafi in Teoria delle Matroidi.

Proponiamo ora un esempio che ci permette di osservare che esistono matroidi non grafiche:

Esempio 15. Diamo come noto che se $C_1, C_2 \in \mathscr{C}$ sono circuiti distinti di un grafo G, allora la differenza simmetrica $C_1 \triangle C_2 = (C_1 \cup C_2) \setminus (C_1 \cap C_2)$ è unione disgiunta di circuiti di G. Questo si nota facilmente nella Figura 2.3 dove $C_1 = \{a, b, c, d, e, f\}$, $C_2 = \{c, h, f, g\}$ e $C_1 \triangle C_2 = \{a, b, g\} \cup \{d, e, h\}$.

Quindi condizione necessaria affinché una matroide M sia grafica, è che la differenza simmetrica di due circuiti sia unione disgiunta di circuiti.

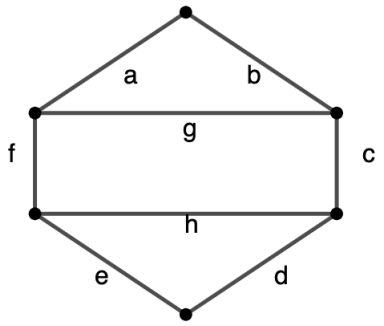


Figura 2.3: Grafo G

Consideriamo allora $E = \{1, 2, 3, 4\}$, e sia $M(E)$ la matroide su E i cui circuiti sono tutti i sottoinsiemi di E di cardinalità 3. Allora

$$\{1, 2, 3\} \triangle \{1, 2, 4\} = \{3, 4\};$$

ma $\{3, 4\}$ è un indipendente di $M(S)$, poiché ha cardinalità 2. Quindi $M(E)$ non è una matroide grafica.

Definizione 2.27. Definiamo la famiglia $\mathscr{H}$ come $H \in \mathscr{H}$ se e solo se esiste un taglio T di G tale che $H = E \setminus T$.

Proposizione 2.5.2. *La famiglia $\mathscr{H}$ soddisfa gli assiomi:*

(H1) *$E \notin \mathscr{H}$,*

(H2) *$\mathscr{H}$ è un'anticatena,*

(H3) *Per ogni $H_1, H_2 \in \mathscr{H}$, tali che $H_1 \neq H_2$, e per ogni $x \in E$, esiste $H_3 \in \mathscr{H}$ tale che $(H_1 \cap H_2) \cup x \subseteq H_3$.*

Dimostrazione. Per l'Osservazione 8 l'insieme T è un taglio di G se e solo se è un circuito di G^*; ovvero, se $T \in \mathscr{C}^*$ è un circuito di G^*, allora T è un taglio di G. Per l'Osservazione 2, i circuiti della matroide duale $M_G^*(E)$ sono i complementari degli iperpiani di $M_G(E)$; cioè, chiamata $\mathscr{H}'$ la famiglia degli iperpiani di $M_G(E)$, abbiamo che

$$\mathscr{H}' = \{E \setminus C : C \in \mathscr{C}^*\} = \{E \setminus T : T \text{ è un taglio di } G\} = \mathscr{H}.$$

Quindi $\mathscr{H}$ è una famiglia di iperpiani e soddisfa (H1)-(H3).

□

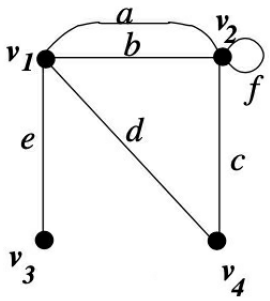


Figura 2.4: Grafo G

Osservazione 14. Poiché un taglio è un insieme minimale la cui rimozione aumenta di 1 il numero di componenti connesse, abbiamo che se $H \in \mathscr{H}$ allora $\mathrm{r}(H) = \mathrm{r}(E) - 1$.

Esempio 16. Riprendiamo l'Esempio 12. Dalla figura si nota facilmente che l'insieme dei circuiti di G è $\mathscr{C} = \{f, ab, acd, bcd\}$.

Osservando la rappresentazione di G, possiamo trovare rapidamente C_3 che soddisfi l'assioma (C3). In particolare, consideriamo $C_1 = acd$, $C_2 = bcd$ e $x = c$, allora $C_3 = ab$. Lo stesso risultato si ottiene seguendo la dimostrazione costruttiva della Proposizione 2.5.1.

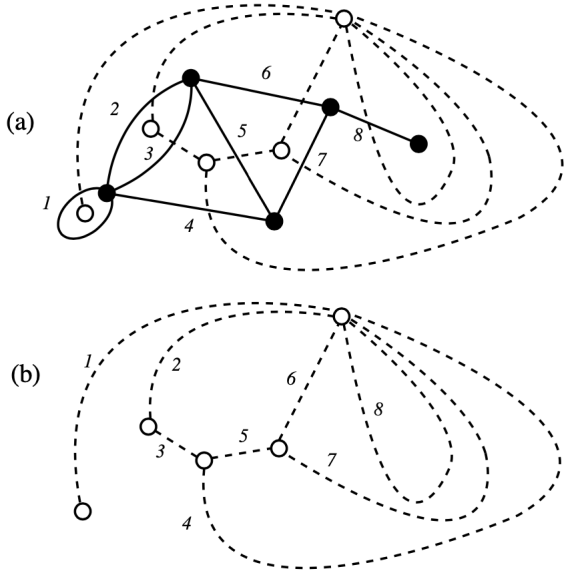


Figura 2.5: (a) Grafo G e costruzione del suo duale G^* (b) Grafo duale G^*

Esempio 17. Nella Figura 2.5 possiamo osservare il grafo G e la costruzione del suo duale G^*. Si nota facilmente che i circuiti di G^* corrispondono ai tagli in G, e viceversa. Per esempio, il circuito $\{2,3,5,6\}$ in G^*, è un taglio in G che sconnette un vertice dal grafo: allora $H = E \setminus \{2,3,5,6\} = \{1,4,7,8\}$ è un iperpiano. Osserviamo che

$$\mathrm{r}(E) = 5 - 1 = 4 \quad \text{e} \quad \mathrm{r}(H) = |V| - c(H) = 5 - 2 = 4 = \mathrm{r}(E) - 1.$$

2.6 Polinomio di Tutte

In questa sezione andremo a definire il polinomio di Tutte per i grafi, e analizzeremo la sua generalizzazione per le matroidi.

Definizione 2.28. Sia $G = (V, E)$, allora possiamo definire il **polinomio di Tutte** come

$$T(G; x, y) = \sum\nolimits_{A \subseteq E} (x-1)^{c(G')-c(G)} (y-1)^{c(A)+|A|-|V|},$$

dove $c(G'), c(G)$ sono rispettivamente le componenti connesse di $G' = (V, A)$ e di G.

Equivalentemente, il polinomio di Tutte può essere definito ricorsivamente come

- $T(G; x, y) = 1$ se $E = \varnothing$,
- $T(G; x, y) = T(G \setminus e; x, y) + T(G \cdot e; x, y)$ se $e \in E$ non è né un cappio né un ponte,
- $T(G; x, y) = xT(G \cdot e; x, y)$ se $e \in E$ è un ponte,
- $T(G; x, y) = yT(G \setminus e; x, y)$ se $e \in E$ è un cappio.

Osservazione 15. Il polinomio di Tutte gode delle seguenti proprietà:

1. Se $G = \bigcup\limits_{i \in I} G_i$ dove G_i sono le componenti connesse di G, allora

$$T(G; x, y) = \prod_{i \in I} T(G_i; x, y);$$

2. Se G è un grafo piano e G^* è il suo duale, allora

$$T(G; x, y) = T(G^*; y, x).$$

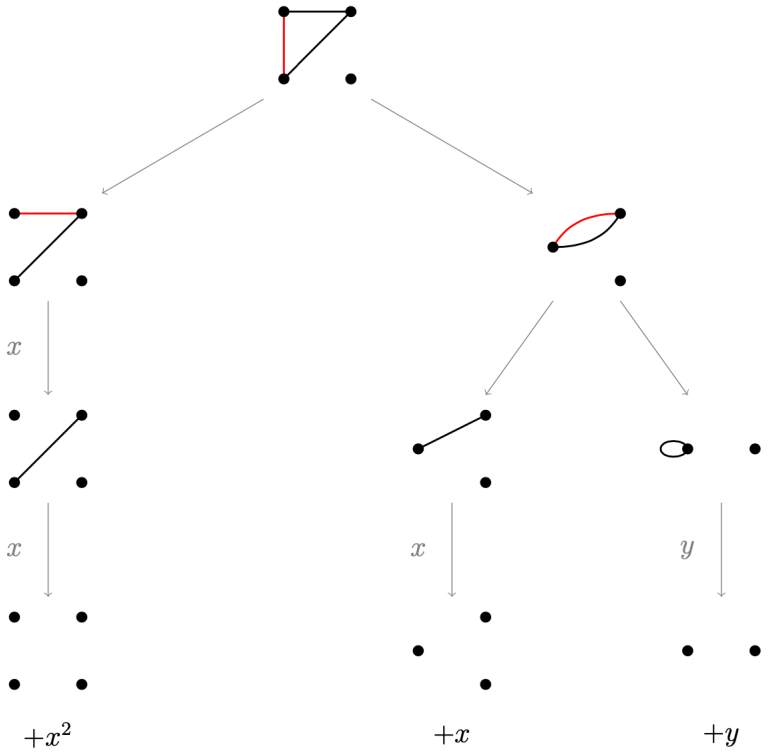


Figura 2.6: Costruzione del polinomio di Tutte

Esempio 18. Nella figura 2.6 possiamo osservare la costruzione del polinomio di Tutte del grafo G attraverso la definizione ricorsiva.

Estendiamo ora il polinomio di Tutte alle matroidi:

Definizione 2.29. Possiamo definire il **polinomio di Tutte** di una matroide $M(E)$ come

$$T(M; x, y) = \sum_{A \subseteq E} (x-1)^{\mathrm{r}(E)-\mathrm{r}(A)} (y-1)^{|A|-\mathrm{r}(A)},$$

dove $\mathrm{r}(A), \mathrm{r}(E)$ sono rispettivamente il rango di A e di E.

Osservazione 16. Se $M(G)$ è una matroide grafica, allora $T(M; x, y) = T(G; x, y)$; poiché ricordiamo che in un grafo vale $\mathrm{r}(E) = |V| - c(G)$.

Come il polinomio di Tutte di un grafo, analogamente il polinomio di Tutte di una matroide può essere definito ricorsivamente attraverso le operazioni di restrizione e di contrazione.

Definizione 2.30. Se $M(E)$ è una matroide su E, ed $S \subseteq E$, la **restrizione** di $M(E)$ su S è la matroide $M(S)$ su S la cui funzione rango è quella di $M(E)$ ristretta ai sottoinsiemi di S. Se $T = E \setminus S$, allora possiamo indicare la restrizione come $M(E) \setminus T$.

Definizione 2.31. Se $M(E)$ è una matroide su E, e $T \subseteq E$, la **contrazione** di $M(E)$ rispetto a T è la matroide su $E \setminus T$ con funzione rango $\mathrm{r}'(A) = \mathrm{r}(A \cup T) - \mathrm{r}(T)$ per ogni $A \subseteq E \setminus T$. La indichiamo con $M(E) \cdot T$.

Definizione 2.32. Il polinomio di Tutte $T(M; x, y)$ può essere definito come

- $T(M; x, y) = 1$ se $E = \varnothing$,
- $T(M; x, y) = T(M \setminus e; x, y) + T(M \cdot e; x, y)$ se $e \in E$ non è né un cappio né un ponte,
- $T(M; x, y) = xT(M \cdot e; x, y)$ se $e \in E$ è un ponte,
- $T(M; x, y) = yT(M \setminus e; x, y)$ se $e \in E$ è un cappio.

Osservazione 17. Il polinomio di Tutte di una matroide $M(E)$ contiene interessanti informazioni sulla matroide stessa:

1. Se $M^*(E)$ è la matroide duale di $M(E)$, allora
$$T(M; x, y) = T(M^*; y, x).$$
Infatti i ponti e i cappi di $M(E)$ sono rispettivamente i cappi e i ponti di $M^*(E)$.

2. $T(M; 1, 1)$ = numero di basi di $M(E)$.
Infatti gli addendi di $T(M; 1, 1)$, per la Definizione 2.29, sono nella forma
$$(x-1)^{\mathrm{r}(E)-\mathrm{r}(A)}(y-1)^{|A|-\mathrm{r}(A)} = \begin{cases} 1 & \text{se } |A| = \mathrm{r}(A) = \mathrm{r}(E), \\ 0 & \text{altrimenti;} \end{cases}$$
ma gli insiemi $A \subseteq E$ tali che $|A| = \mathrm{r}(A) = \mathrm{r}(E)$ sono proprio le basi di $M(E)$.

3. $T(M; 2, 1)$ = numero di insiemi indipendenti di $M(E)$.
Infatti gli addendi di $T(M; 2, 1)$ sono nella forma
$$(x-1)^{\mathrm{r}(E)-\mathrm{r}(A)}(y-1)^{|A|-\mathrm{r}(A)} = \begin{cases} 1 & \text{se } |A| = \mathrm{r}(A), \\ 0 & \text{altrimenti;} \end{cases}$$
ma gli insiemi $A \subseteq E$ tali che $|A| = \mathrm{r}(A)$ sono gli indipendenti di $M(E)$.

4. $T(M;1,2)$ = numero di insiemi generatori di $M(E)$.

   Questa osservazione è banale per i punti 1 e 3.

5. $T(M;2,2) = 2^{|E|}$.

   Infatti tutti gli addendi di $T(M;2,2)$ valgono 1, quindi $T(M;2,2)$ conta tutti i sottoinsiemi di E, ovvero $T(M;2,2) = |\mathscr{P}(E)| = 2^{|E|}$.

Vogliamo ora introdurre l'equivalente delle componenti connesse dei grafi per le matroidi, così da potere estendere la proprietà 2 dell'Osservazione 15 del polinomio di Tutte.

Definizione 2.33. Siano $M(E_1) = (E_1, \mathscr{I}_1)$ e $M(E_2) = (E_2, \mathscr{I}_2)$ due matroidi con $E_1 \cap E_2 = \varnothing$, allora la loro **somma diretta** è la matroide $M(E) = (E, \mathscr{I})$ dove $E = E_1 \cup E_2$ e la famiglia degli indipendenti $\mathscr{I} := \{I_1 \cup I_2 : I_1 \in \mathscr{I}_1, B \in \mathscr{I}_2\}$. La indichiamo con $M(E) = M(E_1) \oplus M(E_2)$.

Osservazione 18. Se $M = \bigoplus_{i \in I} M_i$, allora

$$T(M;x,y) = \prod_{i \in I} T(M_i;x,y).$$

Capitolo 3

Algoritmo greedy e greedoidi

La più nota proprietà algoritmica delle matroidi è la loro intima relazione con ciò che è stato definito "algoritmo greedy": ovvero algoritmo goloso, avido. L'obiettivo di un algoritmo greedy è la ricerca di una soluzione ottima da un punto di vista globale per una data funzione obiettivo attraverso la scelta della soluzione più golosa ad ogni passo locale. Ciò generalmente conduce ad un ottimo locale, ma non necessariamente ad un ottimo globale.

L'idea di base di un algoritmo greedy per i grafi è nota come "algoritmo di Kruskal", dal matematico W. Kruskal che per primo l'ha introdotto. L'estensione alle matroidi fu proposta dal matematico tedesco R. Rado.

Nel 1981 i matematici B. Korte e L. Lovász proposero una generalizzazione del concetto di matroide derivata dalla combinatoria. Korte e Lovász osservarono come l'ottimalità di un algoritmo greedy dipendesse dalla struttura sottostante, che non aveva carattere matroidale, bensì, come fu definita, di greedoide (nome che deriva dalla crasi dei termini 'greedy' e 'matroide').

La principale distinzione tra matroide e greedoide è che quest'ultimo è modellato sulla costruzione algoritmica di certi insiemi, e ciò implica che l'ordine degli elementi in un insieme gioca un ruolo importante. Rimane comunque possibile, come vedremo, caratterizzare i greedoidi in termini di insiemi (versione non ordinata), ma la formulazione che si basa sul linguaggio (versione ordinata) resta fondamentale.

3.1 Algoritmo greedy in una matroide

In questa sezione presenteremo una prima descrizione di un algoritmo greedy attraverso la nozione di indipendente in una matroide. Introdurremo inoltre il concetto di matroide pesata e di algoritmo greedy per questa.

Consideriamo $M(E) = (E, \mathscr{I})$ una matroide degli indipendenti, ovvero tale che E è un insieme finito e $\mathscr{I}$ è l'insieme degli indipendenti di $M(E)$.

Definizione 3.1. L'**algoritmo greedy su una matroide** $M(E)$ procede come segue:

1. $X := \varnothing$ e $Y := E$.
2. Consideriamo $x \in Y$: se $X \cup x \in \mathscr{I}$, allora $X := X \cup x$.
3. Ritorniamo al punto 2 con $Y = Y \setminus x$.

   Se $Y = \varnothing$, l'algoritmo termina restituendo X.

Notiamo che l'algoritmo termina poiché E è un insieme finito.

Proposizione 3.1.1. *L'insieme X ottenuto dall'algoritmo greedy su $M(E)$ è una base di $M(E)$.*

Dimostrazione. Notiamo innanzitutto che $X \in \mathscr{I}$. Se per assurdo X non è un elemento massimale di $\mathscr{I}$, allora esiste $x \in E \setminus X$ tale che $X \cup x \in \mathscr{I}$. Allora, per il punto 2 dell'algoritmo, $x \in X$, e ciò è assurdo. Quindi $X \in \max(\mathscr{I}) \stackrel{\text{def}}{=} \mathscr{B}$.

□

Esempio 19. Consideriamo

$$E = \{e_1, e_2, e_3\} \text{ e } \mathscr{I} = \{\varnothing, \{e_1\}, \{e_2\}, \{e_3\}, \{e_1, e_2\}, \{e_2, e_3\}\},$$

ovvero gli indipendenti sono tutti gli insiemi che non contengono sia e_1 che e_3. Si nota banalmente che le basi sono $\{e_1, e_2\}$ e $\{e_2, e_3\}$.

Dopo il primo passo dell'algoritmo greedy, avremo $X = \{e_1\}$; al termine del secondo passo $X = \{e_1, e_2\}$. Il terzo passo valuterà l'elemento e_3, ma $X \cup e_3$ non è un indipendente, quindi X sarà lo stesso del secondo passo. L'algoritmo quindi termina restituendo $X = \{e_1, e_2\}$, che sappiamo essere una base.

L'algoritmo restituisce la base $\{e_2, e_3\}$ nel caso in cui la valutazione di e_3 sia compiuta prima di e_1, quindi l'algoritmo greedy dipende dall'ordine di valutazione.

Generalizziamo ora l'algoritmo nel caso in cui $M(E)$ sia una matroide pesata.

Definizione 3.2. Una **funzione peso** è una funzione $w : E \to \mathbb{R}^+ \cup \{0\}$ che assegna un peso non negativo a ciascun elemento di E. Questa può essere estesa banalmente ai sottoinsiemi di E come $w : \mathscr{P}(E) \to \mathbb{R}^+ \cup \{0\}$ tale che

$$w(A) = \sum_{e \in A} w(e) \text{ per ogni } A \in \mathscr{P}(E).$$

Se esiste una funzione peso sulla matroide $M(E)$, allora questa è detta **matroide pesata**.

Definizione 3.3. Siano E un insieme finito, $\mathscr{I} \subseteq \mathscr{P}(E)$ una famiglia discendente e $w : E \to \mathbb{R}^+ \cup \{0\}$ una funzione peso. Il **problema di ottimizzazione** $(\mathscr{I}, w)$ consiste nel trovare $X \subseteq E$ tale che

(i) $X \in \mathscr{I}$,

(ii) $w(X) \geqslant w(A)$ per ogni $A \in \mathscr{I}$.

Definizione 3.4. L'**algoritmo greedy su una matroide pesata** $M(E)$ procede come segue:

1. $X := \varnothing$ e Y è l'insieme degli elementi di E ordinato rispetto al peso decrescente.
2. Consideriamo il primo elemento $x \in Y$: se $X \cup x \in \mathscr{I}$, allora $X := X \cup x$.
3. Ritorniamo al punto 2 con $Y = Y \setminus x$.

   Se $Y = \varnothing$, l'algoritmo termina restituendo X.

Osservazione 19. L'insieme X ottenuto dall'algoritmo greedy sulla matroide pesata $M(E)$ è una base di $M(E)$, poiché questo algoritmo è un caso particolare dell'algoritmo greedy su una matroide generica.

Proposizione 3.1.2. *L'algoritmo greedy su una matroide pesata* $M(E) = (E, \mathscr{I})$ *risolve il problema di ottimizzazione* $(\mathscr{I}, w)$.

Dimostrazione. Innanzitutto notiamo che per (I2), $\mathscr{I}$ è una famiglia discendente.

Sia B una base di $M(E)$ selezionata dall'algoritmo greedy e supponiamo per assurdo che esista una base $T \neq B$ di $M(E)$ tale che $w(T) > w(B)$ e $|T \cup B|$ sia massimo. Poiché B e T sono basi, queste sono equicardinali; inoltre $T \neq B$, quindi esiste un elemento x tale che $x \in B \setminus T$. Allora $T \cup x$ è un insieme dipendente, e quindi esiste un circuito C tale che

$$x \in C \subseteq T \cup x.$$

La base B in particolare è un indipendente, quindi non contiene cicuiti: esiste allora $y \in C \setminus B$ tale che $T' := (T \setminus y) \cup x$ è una base di $M(E)$. Poiché T ha peso massimo, allora $w(x) \leqslant w(y)$; ma non può verificarsi che $w(x) < w(y)$, se no l'algoritmo greedy avrebbe selezionato y e non x. Quindi $w(x) = w(y)$, e dunque anche T' ha peso massimo. Ma $x \in T'$ e $x \notin T$, quindi

$$|T' \cap B| > |T \cap B|$$

e ciò contraddice la scelta di T. Allora B è soluzione del problema $(\mathscr{I}, w)$.
□

3.2 Generalizzazione dell'algoritmo greedy

In questa sezione presenteremo la generalizzazione dell'algoritmo greedy per un generico problema di ottimizzazione su un dato insieme, e dimostreremo come l'algoritmo soddisfi tale problema se l'insieme considerato è una famiglia di indipendenti di una certa matroide.

Definizione 3.5. Siano E un insieme finito, $\mathscr{F} \subseteq \mathscr{P}(E)$ una famiglia discendente non vuota e $w : E \to \mathbb{R}^+ \cup \{0\}$ una funzione peso. L'**algoritmo greedy per il problema** $(\mathscr{F}, w)$ procede come segue:

1. $X := \varnothing$ e Y è l'insieme degli elementi di E ordinato rispetto al peso decrescente.

2. Consideriamo il primo elemento $x \in Y$: se $X \cup x \in \mathscr{F}$, allora $X := X \cup x$.

3. Ritorniamo al punto 2 con $Y = Y \setminus x$.

   Se $Y = \varnothing$, l'algoritmo termina restituendo X.

Proposizione 3.2.1. *Siano E un insieme finito e $\mathscr{F} \subseteq \mathscr{P}(E)$ una famiglia discendente. Se l'algoritmo greedy risolve il problema di ottimizzazione $(\mathscr{F}, w)$ per ogni funzione peso w allora $\mathscr{F}$ è la famiglia di insiemi indipendenti di una matroide su E.*

Dimostrazione. Le condizioni (I1) e (I2) sono banalmente soddisfatte.

Dobbiamo solo mostrare che vale (I3), ovvero che se $I_1, I_2 \in \mathscr{F}$ tali che $|I_1| < |I_2|$, allora esiste $x \in I_2 \setminus I_1$ tale che $I_1 \cup x \in \mathscr{F}$. In particolare supponiamo senza perdere di generalità che $I_1 = \{a_1, \ldots, a_k\}$ e $I_2 = \{b_1, \ldots, b_{k+1}\}$; e sia w una funzione peso su E definita come segue:

$$\begin{aligned} w(a_i) &= u & 1 \leqslant i \leqslant k, \\ w(b_i) &= v & b_i \in B \setminus A, \\ w(e) &= 0 & e \in S \setminus (A \cup B), \end{aligned}$$

con $u > v > 0$. L'algoritmo greedy seleziona così gli elementi $a_1, \ldots, a_k$ in ordine.

Se per assurdo non esiste $i \in \{1, \ldots, k\}$ tale che $\{b_i, a_1, \ldots, a_k\} \in \mathscr{F}$, allora l'algoritmo aggiungerà ad X elementi di $S \setminus (A \cup B)$, ottenendo un insieme di peso $w(A)$. Se $|B \setminus A| = t$, allora

$$w(A) = ku \quad \text{e} \quad w(B) = tu + (k + 1 - t)v.$$

Scegliamo $u, v \in \mathbb{R}^+$ tali che $u > v$ e $w(A) < w(B)$; questa scelta è chiaramente possibile, e dunque l'algoritmo greedy avrebbe non avrebbe selezionato un insieme di peso massimo. Questa è una contraddizione, e quindi la tesi è soddisfatta. □

Il risultato ottenuto ci permette di dare la seguente caratterizzazione delle matroidi:

Teorema 3.2.2. *Sia E un insieme finito, allora una famiglia non vuota $\mathscr{F} \subseteq \mathscr{P}(E)$ è la famiglia degli indipendenti di una matroide su E se e solo se*

(i) *$\mathscr{F}$ è una famiglia discendente,*

(ii) *per ogn funzione peso $w : E \to \mathbb{R}^+ \cup \{0\}$ l'algoritmo greedy seleziona un elemento $X \in \mathscr{F}$ con*

$$w(X) \geqslant w(A)$$

per ogni $A \in \mathscr{F}$.

Osservazione 20. Un algoritmo greedy può essere utilizzato anche per problemi di minimizzazione: supponiamo di volere trovare $X \subseteq E$ tale che

(i) $X \in \mathscr{F}$,

(ii) $w(X) \leqslant w(A)$ per ogni $A \in \mathscr{F}$.

Sarà sufficiente invertire la funzione peso come

$$w_{\min}(x) = W - w(x) \text{ con } W = \max_{e \in E}(w(e))$$

e risolvere il problema $(\mathscr{F}, w_{\min})$.

Vediamo ora un esempio nel quale l'algoritmo greedy non risolve il problema di ottimizzazione dato. Questo avviene, in pieno rispetto del Teorema 3.2.2, poiché l'insieme d'azione non è l'insieme degli indipendenti di una matroide.

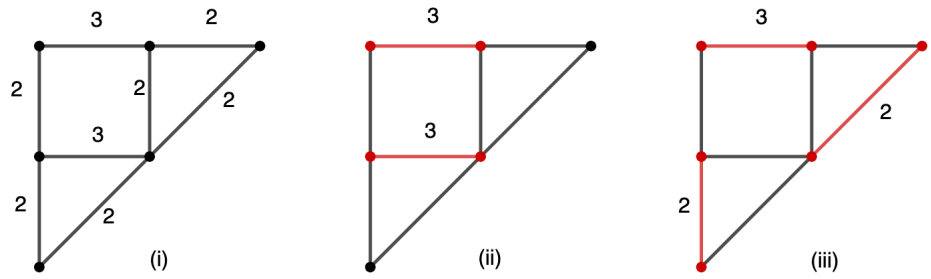


Figura 3.1: (i) Grafo G con pesi (ii) Matching M (iii) Matching massimo

Esempio 20. Sia G un grafo, un **matching** di G è un insieme di lati a due a due non adiacenti. Indichiamo con $\mathscr{M}$ l'insieme dei matching di G.

Ricordiamo che in un grafo la famiglia degli indipendenti $\mathscr{I}$ è l'insieme di tutte le sottoforeste, mentre l'insieme dei matching $\mathscr{M} \subset \mathscr{I}$.

Consideriamo il grafo G in Figura 3.1 e cerchiamo di risolvere il problema di ottimizzazione $(\mathscr{M}, c)$ dove il peso c di ogni lato è indicato in figura (i). La ricerca di un matching M di peso massimo attraverso un algoritmo greedy, proposto in figura (ii), seleziona i due lati di peso 3, con $c(M) = 6$. Si nota facilmente che M non è un matching massimo, infatti il matching proposto nella figura (iii) ha peso 7. L'algoritmo quindi non risolve il problema proposto.

Sorge naturale un dubbio: può $\mathscr{M}$ essere un insieme di indipendenti, anche se non della matroide grafica associata a G? La risposta è negativa; infatti l'assioma (I3) non è soddisfatto. Consideriamo per esempio i due matching in Figura 3.1 (ii) e (iii): la cardinalità del secondo è strettamente maggiore della cardinalità del primo, ma nessuno dei due lati di peso 2 può essere aggiunto al matching in (ii) ottenendo ancora un matching.

3.3 Algoritmi greedy nei grafi

In questa sezione presentiamo alcuni algoritmi greedy applicati ai grafi. Di particolare rilevanza storica è l'algoritmo di Kruskal per la ricerca degli alberi generatori con costo minimo.

Definizione 3.6. Siano $G = (V, E)$ un grafo connesso e $c : E \to \mathbb{R}^+ \cup \{0\}$ una funzione peso, l'**algoritmo di Kruskal** procede come segue:

1. $T := \varnothing$ e Y è l'insieme degli archi di G ordinato rispetto al peso crescente.

2. Consideriamo il primo elemento $e \in Y$: se l'aggiunta di e a T non genera un ciclo, allora $T = T \cup e$.

3. Ritorniamo al punto 2 con $Y = Y \setminus e$.

   Se $Y = \varnothing$, l'algoritmo termina restituendo T.

Notazione 4. Se G è un grafo connesso pesato, indichiamo con MST (minimum spanning tree) un albero generatore di G con peso minimo.

Proposizione 3.3.1. *L'algoritmo di Kruskal produce un MST.*

Dimostrazione. Ricordiamo che un indipedente in un grafo G è una sottoforesta di G, ovvero un insieme di lati privo di circuiti; quindi l'algoritmo di Kruskal è un algoritmo greedy applicato alla matroide grafica $M(G) = (E, \mathscr{I})$. Per la Proposizione 3.1.2 abbiamo allora che l'algoritmo risolve il problema di minimo $(\mathscr{I}, c)$, e la soluzione è una base di $M(G)$. La tesi è quindi ovvia osservando che le basi di un grafo G connesso sono gli alberi generatori.

□

Proponiamo una seconda dimostrazione della Proposizione 3.3.1, non necessaria, interessante in quanto utilizza solo nozioni di Teoria dei Grafi.

Dimostrazione. L'insieme T ottenuto attraverso l'algoritmo di Kruskal non contiene cicli per costruzione. Poiché G è connesso, per ogni $v \in V$ esiste $e = (v, w) \in E$ per un qualche $w \in V$; quindi se esistesse un vertice v di G non connesso in T, allora $T \cup e$ non conterrebbe cicli, e dunque l'algoritmo avrebbe aggiunto e a T. Allora T copre tutti i vertici di G. Un ragionamento analogo ci permette di concludere che T è connesso, e quindi è un albero.

Dobbiamo ora verificare che T ha peso minimo. In particolare dimostriamo per induzione che se T_n è l'insieme dei lati scelti al passo n dell'algoritmo, allora esiste un MST che contiene T_n per ogni $n = 1, \dots, k$ con k numero totale di passi dell'algoritmo.
Poiché $T_0 = \varnothing$, allora ovviamente qualsiasi MST contiene T_0, e per la Proposizione 2.1.4 ne esiste almeno uno.
Supponiamo allora che T' sia un MST contenente T_n, e sia e l'arco che si considera al passo $n + 1$. Se $T_n \cup e$ genera un circuito, allora $T_{n+1} = T_n$ e $T_{n+1} \subseteq T'$. Se $T_{n+1} = T_n \cup e$, allora $T_{n+1} \subseteq T'$, e l'induzione termina, oppure

$T' \cup e$ contiene un circuito C. Esiste quindi $f \in C$ tale che $f \in T'$. Poiché f non è stato aggiunto a T_{n+1} dall'algoritmo, sicuramente $c(f) \geqslant c(e)$. Allora $T'' := T' \setminus f \cup e$ è un albero tale che $c(T'') \leqslant c(T')$, cioè T" è un MST. Poiché $T_{n+1} = T_n \cup e \subseteq T''$, l'induzione termina.

In particolare esiste un MST T' tale che $T = T_k \subseteq T'$, ma poiché T è un albero generatore, allora $T = T'$ è un MST.

□

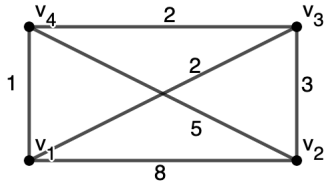


Figura 3.2: Grafo G

Esempio 21. Vediamo la costruzione di un MST del grafo G (Figura 3.2) attraverso l'algoritmo di Kruskal.

Innanzitutto $T = \varnothing$ e $Y = \{(v_1, v_4), (v_1, v_3), (v_3, v_4), (v_2, v_3), (v_2, v_5), (v_1, v_2)\}$ ordinato rispetto al peso degli archi. Notiamo che se dua archi hanno lo stesso peso, l'ordine è scelto a piacere.

1. L'algoritmo considera il lato (v_1, v_4) e lo aggiunge all'insieme T, quindi $c(T) = 1$;

2. L'algoritmo considera il lato (v_1, v_3) e lo aggiunge all'insieme T, quindi $c(T) = 3$;

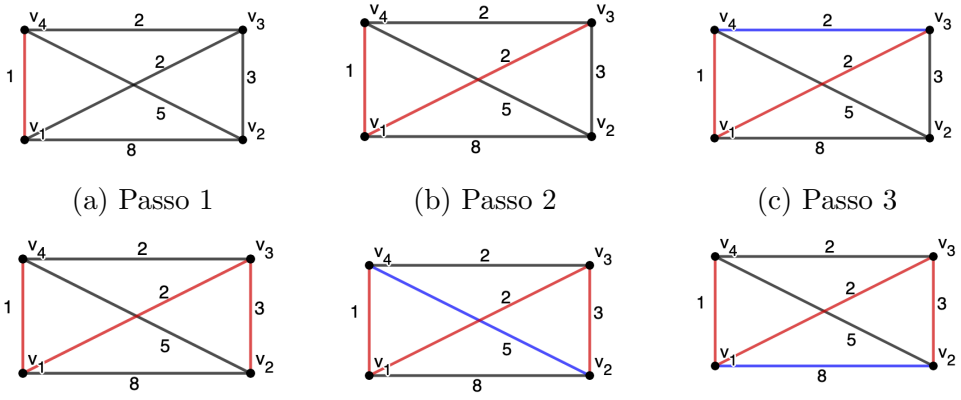
3. L'algoritmo considera il lato (v_3, v_4): il suo inserimento in T genererebbe un circuito, quindi non viene aggiunto a T;

4. L'algoritmo considera il lato (v_2, v_3) e lo aggiunge all'insieme T, quindi $c(T) = 6$;

5. L'algoritmo considera il lato (v_2, v_5): il suo inserimento in T genererebbe un circuito, quindi non viene aggiunto a T;

6. L'algoritmo considera il lato (v_1, v_2): il suo inserimento in T genererebbe un circuito, quindi non viene aggiunto a T.

Avendo analizzato tutti i lati di G, l'algoritmo termina. L'MST trovato, con $c(T) = 6$, è segnato in rosso nella Figura 3.3f.



(a) Passo 1 (b) Passo 2 (c) Passo 3

(d) Passo 4 (e) Passo 5 (f) Passo 6

Figura 3.3: Algortimo di Kruskal su G

Definizione 3.7. Siano $G = (V, E)$ un grafo connesso e $c : E \to \mathbb{R}^+ \cup \{0\}$ una funzione peso, l'**algoritmo di Prim** procede come segue:

1. $T = \varnothing$, $W = \{v\}$ per un certo $v \in V$ e $L = V \setminus W$.
2. Consideriamo tutti i lati in E del tipo (w, u) con $w \in W$ e $u \in L$; scegliamo tra questi il lato $e = (w', u')$ di peso minore. Allora $T = T \cup e$.
3. Ritorniamo al punto 2 con $W = W \cup u'$ e $L = L \setminus u'$.

   Se $L = \varnothing$, l'algoritmo termina restituendo T.

Proposizione 3.3.2. *L'algoritmo di Prim produce un MST.*

Dimostrazione. L'insieme T ottenuto attraverso l'algoritmo di Prim è ovviamente connesso per costruzione. Inoltre non contiene cicli: infatti ad ogni passo si aggiunge un elemento che unisce due insiemi sconnessi. Infine, l'algoritmo termina quando tutti i vertici di V sono in T, quindi T è un albero generatore.

Dobbiamo ora verificare che T abbia peso minimo. Chiamiamo T_n e W_n rispettivamente l'insieme T e l'insieme W ottenuto alla n-esima iterazione dell'algoritmo. Procediamo per induzione sui passi dell'algoritmo, dimostrando che T_n è un MST per il sottografo di G indotto da W_n.
Al primo passo $T_1 = \{(u, v)\}$ e $W_1 = \{u, v\}$: ovviamente T_1 è albero generatore, ed ha peso minimo poiché se esistesse un lato parallelo a quello scelto e di peso minore, l'algoritmo lo avrebbe selezionato.
Supponiamo che T_n sia un albero generatore e consideriamo il passo $n + 1$.

Chiamiamo $e = (u, v)$ il lato aggiunto all'$(n + 1)$-esimo passo. Poiché $v \in W_{n+1} \setminus W_n$, allora $T_{n+1} := T_n \cup e$ è un albero generatore. Inoltre

$$c(T_{n+1}) = c(T_n) + c(e),$$

ma sappiamo che per induzione T_n ha peso minimo, e, per scelta dell'algoritmo, e ha peso minimo, quindi T_{n+1} è un MST per il grafo indotto da W_{n+1}. All'ultimo passo dell'algoritmo abbiamo quindi che T è un MST per il sottografo indotto da $W = V$, cioè G stesso. □

Osservazione 21. L'algoritmo di Prim è un algoritmo greedy. Ciò non è direttamente osservabile attraverso la struttura matroidale, bensì attraverso quella di greedoide (Esempio 27).

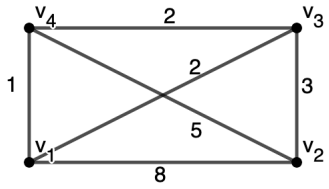


Figura 3.4: Grafo G

Esempio 22. Riprendiamo l'Esempio 21, e vediamo la costruzione di un MST del grafo G in Figura 3.4 con l'algoritmo di Prim.

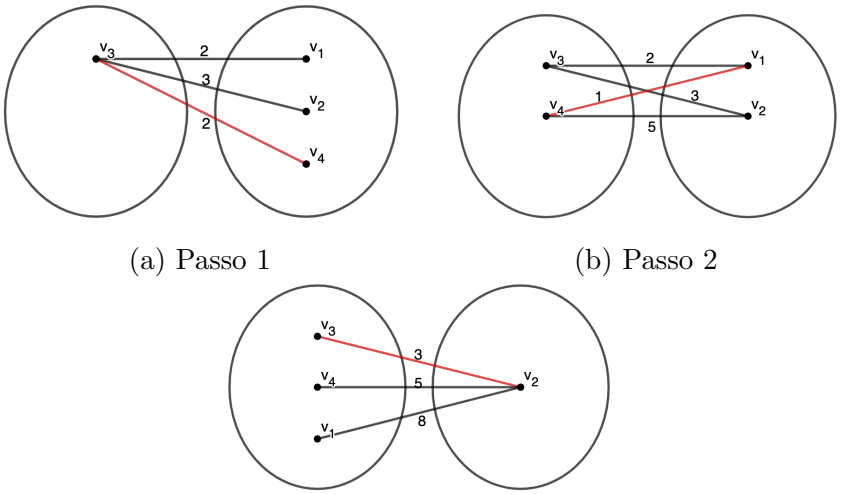
Scegliamo $W = \{v_3\}$.

1. L'algoritmo considera i lati $(v_3, v_1), (v_3, v_2)$ e (v_3, v_4). Sceglie il lato (v_3, v_4) (equivalentemente tra (v_3, v_1) e (v_3, v_4)) e lo aggiunge all'insieme T, quindi $c(T) = 2$;

2. L'algoritmo considera i lati $(v_3, v_1), (v_3, v_2), (v_4, v_1)$ e (v_4, v_2). Sceglie il lato (v_4, v_1) e lo aggiunge all'insieme T, quindi $c(T) = 3$;

3. L'algoritmo considera i lati $(v_3, v_2), (v_4, v_2)$ e (v_1, v_2). Sceglie il lato (v_3, v_2) e lo aggiunge all'insieme T, quindi $c(T) = 6$.

Notiamo che l'MST trovato nei due esempi non è lo stesso; ma, come ci si aspetta, in entrambi i casi vale $|T| = 3$ e $c(T) = 6$.



(a) Passo 1

(b) Passo 2

(c) Passo 3

Figura 3.5: Algoritmo di Prim su G

3.4 Greedoidi

In questa sezione presenteremo il concetto di greedoide, proponendo due definizioni equivalenti: l'una basata sui sottoinsiemi di un insieme finito, l'altra sulla nozione di linguaggio.

Ricordiamo che con E indichiamo un insieme finito.

Definizione 3.8. Un **greedoide** è una coppia $(E, \mathscr{F})$, dove $\mathscr{F} \subseteq \mathscr{P}(E)$ soddisfa le seguenti condizioni:

(G1) $\mathscr{F} \neq \varnothing$,

(G2) Per ogni $F \in \mathscr{F}$ tale che $F \neq \varnothing$, esiste $x \in F$ tale che $F \setminus x \in \mathscr{F}$,

(G3) Per ogni $F_1, F_2 \in \mathscr{F}$, se $|F_1| < |F_2|$, allora esiste $x \in F_2 \setminus F_1$ tale che $F_1 \cup x \in \mathscr{F}$. [**Proprietà di scambio**]

Se $F \in \mathscr{F}$ allora è detto **insieme possibile**.

Osservazione 22. Una matroide degli indipendenti $(E, \mathscr{I})$ è un greedoide. Infatti gli assiomi (I1) e (I3) coincidono rispettivamente con (G1) e (G3), mentre l'assioma (I2), che ricordiamo descrivere $\mathscr{I}$ come una famiglia discendente, implica banalmente (G2).

Un greedoide è una matroide se soddisfa (I2); in tal caso di dice **ereditario**.

Vediamo ora un esempio di un greedoide non ereditario.

Esempio 23. Consideriamo un grafo con radice $T = (V, E, r)$ con $r \in V$, e sia $\mathscr{F}$ la famiglia dei sottoalberi di T contenenti la radice.

Sia $F \in \mathscr{F}$ tale che $F \neq \varnothing$. Poiché sappiamo che ogni albero contiene almeno due foglie, sicuramente esiste una foglia $x \neq r$; allora $F \setminus x$ è ancora un albero contenente la radice, ovvero $F \setminus x \in \mathscr{F}$.

Siano $F_1, F_2 \in \mathscr{F}$ tali che $|F_1| < |F_2|$. Sappiamo che in un albero vale $|E| = |V| - 1$, quindi F_2 avrà più vertici di F_1, ed in particolare esiste $v \in V \setminus r$ che è contenuto in F_2 ma non in F_1. Percorriamo l'unico cammino in F_2 da r a v e sia x il primo lato di tale cammino che non appartiene ad F_1: chiaramente $F_1 \cup x$ è un albero contenente r.

Quindi (G1), (G2) e (G3) sono soddisfatti e $(E, \mathscr{F})$ è un greedoide. Si nota facilmente che $\mathscr{F}$ non è una famiglia discendente: infatti dato $F \in \mathscr{F}$, qualsiasi sottoalbero di F non contenente r non appartiene a $\mathscr{F}$. Quindi $(E, \mathscr{F})$ non è ereditario.

Definizione 3.9. Sia $(E, \mathscr{F})$ un greedoide.

Una **base** è un insieme possibile massimale.

Per ogni $A \subseteq E$ definiamo il **rango** di A come

$$r(A) := \max\{|X| : X \subseteq A, X \in \mathscr{A}\}.$$

Osservazione 23. Segue banalmente da (G3) che le basi di un greedoide sono equicardinali.

Introduciamo ora alcuni elementi necessari per dare l'equivalente definizione "ordinata" dei greedoidi in termini di linguaggio.

Definizione 3.10. Sia E un insieme finito che chiameremo **alfabeto**; i suoi elementi sono detti **lettere**.

Una **parola** su E è una stringa ordinata di lettere, non necessariamente distinte. Denoteremo con E^* l'insieme delle parole su E.

Sia $\alpha \in E^*$, la **lunghezza** di α è il numero di lettere in α e si indica con $|\alpha|$.

Il **supporto** di $\alpha \in E^*$ è l'insieme delle lettere in α e si indica con $\tilde{\alpha}$.

Una parola α è **semplice** se contiene solo lettere distinte; ovvero se $|\alpha| = |\tilde{\alpha}|$. Denoteremo con E^*_S l'insieme delle parole semplici su E.

Siano $\alpha, \beta \in E^*$, la **concatenazione** delle due parole è la stringa ottenuta dalla giustapposizione di α e β. La indichiamo con il simbolo $\alpha\beta$.

Definizione 3.11. Sia E un alfabeto, un **linguaggio** $\mathscr{L}$ su E è un insieme non vuoto $\mathscr{L} \subseteq E^*$ di parole.

Un linguaggio $\mathscr{L}$ si dice **semplice** se ogni sua parola è semplice.

Il **supporto** di $\mathscr{L}$ è l'insieme $\tilde{\mathscr{L}} := \{\tilde{\alpha} : \alpha \in \mathscr{L}\}$.

Definizione 3.12. Un **greedoide di linguaggio** su E è una coppia $(E, \mathscr{L})$ dove $\mathscr{L}$ è un linguaggio semplice che soddisfa le seguenti condizioni:

(L1) $\mathscr{L} \neq \emptyset$,

(L2) Se $\alpha = \beta\gamma$ e $\alpha \in \mathscr{L}$, allora $\beta \in \mathscr{L}$,

(L3) Per ogni $\alpha, \beta \in \mathscr{L}$, se $|\alpha| < |\beta|$ allora β contiene una lettera $x \notin \tilde{\alpha}$ tale che $\alpha x \in \mathscr{L}$.

Le parole in $\mathscr{L}$ sono dette **possibili**.

Esempio 24. Consideriamo, come nell'Esempio 23, un grafo con radice $T = (V, E, r)$ con $r \in V$. Una parola $x_1 \dots x_k$ di lati distinti $x_i \in E$ è possibile se il sottografo $\{x_1, \dots, x_{i-1}\}$ connette la radice r ad uno e uno solo dei due vertici di x_i per ogni $i = 1, \dots, k$.

Il grafo T con il linguaggio $\mathscr{L}$ delle parole possibili sopra descritte si dimostra essere un greedoide di linguaggio.

Le condizioni (L1) e (L2) sono banalmente soddisfatte.

Consideriamo $\alpha, \beta \in \mathscr{L}$ tali che $|\alpha| < |\beta|$. Notiamo che una parola è possibile se il suo supporto è un albero contenente la radice. Sappiamo che in un albero vale $|E| = |V| - 1$, quindi $\tilde{\beta}$ avrà più vertici di $\tilde{\alpha}$, ed in particolare esiste $v \in V \setminus r$ che è contenuto in $\tilde{\beta}$ ma non in $\tilde{\alpha}$. Percorriamo l'unico cammino in $\tilde{\beta}$ da r a v e sia x il primo lato di tale cammino che non appartiene ad $\tilde{\alpha}$: chiaramente $\alpha x \in \mathscr{L}$.

Definizione 3.13. Se un linguaggio $\mathscr{L}$ soddisfa (L2), allora si dice **ereditario**.

Definizione 3.14. Sia $(E, \mathscr{L})$ un greedoide di linguaggio, le parole massimali in $\mathscr{L}$ sono dette **parole base**.

Proposizione 3.4.1. *I greedoidi e i greedoidi di linguaggio sono equivalenti nel senso seguente:*

(i) *Se $(E, \mathscr{L})$ è un greedoide di linguaggio, allora $(E, \tilde{\mathscr{L}})$ è un greedoide;*

(ii) *Se $(E, \mathscr{F})$ è un greedoide, allora $(E, \mathscr{L}(F))$ è un greedoide di linguaggio, dove*

$$\mathscr{L}(F) := \{x_1 \dots x_n \in E_S^* : \{x_1, \dots, x_i\} \in \mathscr{F} \text{ per ogni } 1 \leqslant i \leqslant n\};$$

(iii) *Vi è una corrispondenza biunivoca tra greedoidi e greedoidi di linguaggio, ovvero $\mathscr{L}(\tilde{\mathscr{F}}) = \mathscr{F}$ e $\mathscr{L}(\tilde{\mathscr{L}}) = \mathscr{L}$.*

Dimostrazione. **(i)** Il linguaggio $\mathscr{L}$ soddisfa le condizioni (L1)-(L3). Il supporto $\tilde{\mathscr{L}}$ soddisfa banalmente (G1).

Sia $\alpha \in \mathscr{L}$, allora può essere scritto come $\alpha = \beta x$ per un certo $\beta \in E^*$ ed $x \in E$. Per (L2) sappiamo che $\beta \in \mathscr{L}$, cioè $\tilde{\beta} \in \tilde{\mathscr{L}}$. Ma $\tilde{\beta} = \tilde{\alpha} \setminus x$, e quindi (G2) è soddisfatto.

La condizione (G3) è banalmente soddisfatta per (L3).

Quindi $\tilde{\mathscr{L}}$ soddisfa le condizioni (G1)-(G3) e $(E, \tilde{\mathscr{L}})$ è un greedoide.

(ii) L'insieme $\mathscr{F}$ soddisfa (G1)-(G3). L'insieme $\mathscr{L}(F)$ soddisfa banalmente (L1).

Sia $\alpha = \beta\gamma$ con $\alpha = x_1 \dots x_n \in \mathscr{L}(F)$ e $\beta = x_1 \dots x_k$ dove $k < n$. Poiché $\alpha \in \mathscr{L}(F)$, abbiamo che $\{x_1, \dots, x_i\} \in \mathscr{F}$ per ogni $1 \leqslant i \leqslant k$, e quindi $\beta \in \mathscr{L}(F)$.

La condizione (L3) è banalmente soddisfatta per (G3).

Quindi $\mathscr{L}(F)$ soddisfa le condizioni (L1)-(L3) e $(E, \mathscr{L}(F))$ è un greedoide di linguaggio.

(iii) Sia $F = \{x_1, \dots, x_n\} \in \mathscr{F}$; è possibile ordinare gli elementi di F in modo che l'elemento $x \in F$ tale che $F \setminus x \in \mathscr{F}$ (condizione (G2)) sia proprio x_n, ed analogamente per i sottoinsiemi $\{x_1, \dots, x_i\}$ per ogni $1 \leqslant i \leqslant n$. Quindi $\{x_1, \dots, x_i\} \in \mathscr{F}$ per ogni $1 \leqslant i \leqslant n$. Allora $x_1 \dots x_n \in \mathscr{L}(F)$ e $F \in \tilde{\mathscr{L}(\mathscr{F})}$. Quindi $\mathscr{F} \subseteq \tilde{\mathscr{L}(\mathscr{F})}$.

Ovviamente $\tilde{\mathscr{L}(\mathscr{F})} \subseteq \mathscr{F}$, quindi $\tilde{\mathscr{L}(\mathscr{F})} = \mathscr{F}$.

Sia $\alpha = x_1 \dots x_n \in \mathscr{L}$, per (L2) abbiamo che $x_1 \dots x_i \in \mathscr{L}$ per ogni $1 \leqslant i \leqslant n$. Allora $\alpha \in \mathscr{L}(\tilde{\mathscr{L}})$ e quindi $\mathscr{L} \subseteq \mathscr{L}(\tilde{\mathscr{L}})$.

Viceversa, sia $\alpha_n = x_1 \dots x_n \in \mathscr{L}(\tilde{\mathscr{L}})$. Procediamo per induzione sulla lunghezza n.
Se $\alpha_1 = x_1$ allora $\{x_1\} \in \tilde{\mathscr{L}}$ e $x_1 \in \mathscr{L}$.
Supponiamo $\alpha_{n-1} \in \mathscr{L}$ e consideriamo α_n. Abbiamo che $\{x_1, \dots, x_n\} \in \tilde{\mathscr{L}}$, e quindi esiste una parola $\beta \in \mathscr{L}$ tale che $\tilde{\beta} = \{x_1, \dots, x_n\}$. Ma per (L3) esiste $x \in \beta$ tale che $x \notin \alpha_{n-1}$ e $\alpha_{n-1}x \in \mathscr{L}$, e tale x può essere solo x_n. Quindi $\alpha_n = \alpha_{n-1}x_n \in \mathscr{L}$.
Allora $\mathscr{L}(\tilde{\mathscr{L}}) \subseteq \mathscr{L}$ e quindi $\mathscr{L}(\tilde{\mathscr{L}}) = \mathscr{L}$.

□

Definizione 3.15. Un **greedoide intervallo** $(E, \mathscr{F})$ è un greedoide che soddisfa la seguente proprietà:

se $A, B, C \in \mathscr{F}$ tali che $A \subseteq B \subseteq C$, $x \in E \setminus C$ tale che $A \cup x \in \mathscr{F}$ e $C \cup x \in \mathscr{F}$, allora $B \cup x \in \mathscr{F}$. [**Proprietà intervallo**]

Equivalentemente, in termini di greedoide linguaggio $(E, \mathscr{L})$, questo significa che se $\alpha x, \alpha\beta\gamma x \in \mathscr{L}$ allora $\alpha\beta x \in \mathscr{L}$.

Osservazione 24. Una matroide $(E, \mathscr{I})$ è un greedoide intervallo. Infatti $B \cup x \subseteq C \cup x$, ma $C \cup x \in \mathscr{I}$, allora per (I2) abbiamo che $B \cup x \in \mathscr{I}$.

3.5 Algoritmo greedy in un greedoide

In questa sezione dimostreremo che un algoritmo greedy risolve un problema di ottimizzazione se e solo se la struttura considerata è un greedoide.

Definizione 3.16. Siano E un insieme finito, $\mathscr{L}$ un linguaggio ereditario e $\omega : \mathscr{L} \to \mathbb{R}$ una funzione obiettivo. Il **problema di ottimizzazione** $(\mathscr{L}, \omega)$ consiste nel trovare $\alpha \in E^*$ tale che

(i) $\alpha \in \mathscr{L}$,

(ii) $\omega(\alpha) \geqslant \omega(\beta)$ per ogni $\beta \in \mathscr{L}$.

Definizione 3.17. Una funzione obiettivo $\omega : \mathscr{L} \to \mathbb{R}$ è **lineare** se è nella forma

$$\omega(x_1 \dots x_n) = \sum_{i=1}^{n} w(x_i)$$

per una data funzione $w : E \to \mathbb{R}$.

Osservazione 25. La funzione peso (Definizione 3.2) utilizzata negli algoritmi greedy per le matroidi è lineare.

Definizione 3.18. Siano E un insieme finito, $\mathscr{L}$ un linguaggio ereditario e $\omega : \mathscr{L} \to \mathbb{R}$ una funzione obiettivo. L'**algoritmo greedy per il problema** $(\mathscr{L}, \omega)$ procede come segue:

1. $\alpha := \varnothing$ e $Y = E$.
2. Consideriamo il primo elemento $x \in Y$: se $\alpha x \in \mathscr{L}$ e $\omega(\alpha x) \geqslant \omega(\alpha y)$ per ogni $y \in Y$ tale che $\alpha y \in \mathscr{L}$, allora $\alpha := \alpha x$.
3. Ritorniamo al punto 2 con $Y = Y \setminus x$.

   Se $Y = \varnothing$, l'algoritmo termina restituendo X.

Proposizione 3.5.1. *La parola α ottenuta dall'algoritmo greedy per $(\mathscr{L}, \omega)$ è una parola base di $\mathscr{L}$.*

Dimostrazione. Notiamo innanzitutto che $\alpha \in \mathscr{L}$. Se per assurdo α non è una parola base di $\mathscr{L}$, allora esiste $x \in E \setminus \tilde{\mathscr{L}}$ tale che $\alpha x \in \mathscr{L}$. Allora, per il punto 2 dell'algoritmo, $\alpha x \in \mathscr{L}$, e ciò è assurdo.

□

Diamo ora alcune definizioni e lemmi necessari alla dimostrazione del Teorema 3.5.5, cardine del capitolo.

Definizione 3.19. Una funzione obiettivo $\omega : \mathscr{L} \to \mathbb{R}$ è **compatibile** con $\mathscr{L}$ se soddisfa le seguenti condizioni:
se $\alpha x \in \mathscr{L}$ tale che $\omega(\alpha x) \geqslant \omega(\alpha y)$ per ogni $\alpha y \in \mathscr{L}$, allora

(i) $\alpha\beta x\gamma$, $\alpha\beta z\gamma \in \mathscr{L}$ implica che $\omega(\alpha\beta x\gamma) \geqslant \omega(\alpha\beta z\gamma)$,

(ii) $\alpha x\beta z\gamma$, $\alpha z\beta x\gamma \in \mathscr{L}$ implica che $\omega(\alpha x\beta z\gamma) \geqslant \omega(\alpha z\beta x\gamma)$,

per ogni β, $\gamma \in E^*$.

Intuitivamente, il significato della prima condizione è che se x è la scelta migliore possibile ad un certo punto, allora è il candidato migliore in qualsiasi scelta successiva. La seconda condizione traduce invece il fatto che è sempre meglio scegliere prima x e poi una qualsiasi altra lettera z.

Se ω è **stabile**, ovvero $\omega(\alpha)$ dipende solo da $\tilde{\alpha}$, allora la condizione (ii) è banalmente soddisfatta.

Definizione 3.20. Una **funzione a collo di bottiglia generalizzata** su $\mathscr{L}$ è una funzione obiettivo nella forma

$$\omega(x_1 \dots x_n) = \min\{f_1(x_1), \dots, f_n(x_n)\},$$

dove le $f_i : E \to \mathbb{R}$ sono funzioni che soddisfano $f_i(x) \leqslant f_{i+1}(x)$ per ogni $x \in E$, per ogni $1 \leqslant i < r$ con r la massima lunghezza di una parola in $\mathscr{L}$.

Proposizione 3.5.2. *Una funzione a collo di bottiglia generalizzata è compatibile con ogni linguaggio ereditario.*

Dimostrazione. Consideriamo l'ipotesi "se $\alpha x \in \mathscr{L}$ tale che $\omega(\alpha x) \geqslant \omega(\alpha y)$ per ogni $\alpha y \in \mathscr{L}$". Nel caso di una funzione a collo di bottiglia generalizzata due sono i casi che si possono verificare, supponendo $\alpha = x_1 \dots x_n$:

1. $f_{n+1}(x) \geqslant f_{n+1}(y)$,
2. $\omega(\alpha x) = \omega(\alpha y) = f_i(x_i)$ per un qualche $1 \leqslant i \leqslant n$,

per ogni $\alpha y \in \mathscr{L}$.

Verifichiamo allora le due condizioni:

(i) Consideriamo $\alpha\beta x\gamma$, $\alpha\beta z\gamma \in \mathscr{L}$; per (L2) abbiamo che $\alpha\beta x$, $\alpha\beta z \in \mathscr{L}$. Consideriamo i due casi distinti a seconda dell'ipotesi:

1. Procediamo per induzione su $|\beta|$.
   Se $|\beta| = 1$ allora $\beta = b$ e per (L2) sappiamo che $\alpha b \in \mathscr{L}$. Allora per ipotesi
   $$f_{n+1}(b) \leqslant f_{n+1}(x) \leqslant f_{n+2}(x)$$
   e quindi $\omega(\alpha bx) = f_{n+1}(b)$. Per definizione di ω vale
   $$\omega(\alpha bz) \leqslant f_{n+1}(b) = \omega(\alpha bx).$$
   Supponiamo allora $\beta = b_1 \dots b_{k-1}b_k$. Per ipotesi induttiva sappiamo che
   $$\omega(\alpha b_1 \dots b_{k-1}z) \leqslant \omega(\alpha b_1 \dots b_{k-1}x)$$
   per ogni $\alpha b_1 \dots b_{k-1}z \in \mathscr{L}$; e, poiché per (L2) vale $\alpha b_1 \dots b_k \in \mathscr{L}$, abbiamo che
   $$\omega(\alpha b_1 \dots b_{k-1}b_k) \leqslant \omega(\alpha b_1 \dots b_{k-1}x).$$
   Allora $\omega(\alpha\beta x) = f_{n+k}(b_k)$. Per definizione di ω vale
   $$\omega(\alpha\beta z) \leqslant f_{n+k}(b_k) = \omega(\alpha\beta x).$$

2. Supponiamo $\omega(\alpha x) = \omega(\alpha y) = f_i(x_i)$ per un qualche $1 \leqslant i \leqslant n$. Per (L2) abbiamo che $\alpha z \in \mathscr{L}$ e quindi
   $$\omega(\alpha x) = \omega(\alpha z) = f_i(x_i).$$
   Se $|\beta| = k$, per definizione delle f_i e di ω vale
   $$f_i(x_i) \leqslant f_{n+1}(x) \leqslant f_{n+k+1}(x) \text{ e } f_i(x_i) \leqslant f_{n+1}(z) \leqslant f_{n+k+1}(z);$$
   quindi
   $$\omega(\alpha\beta x) = \omega(\alpha\beta z) = f_i(x_i).$$

(ii) Supponiamo per assurdo che esistano $\alpha x\beta z\gamma$, $\alpha z\beta x\gamma \in \mathscr{L}$ tali che $\omega(\alpha x\beta z\gamma) < \omega(\alpha z\beta x\gamma)$ con $|\beta| = k$. Per (L2) vale $\alpha z \in \mathscr{L}$, allora si possono verificare due casi a seconda dell'ipotesi:

1.
   $$f_{n+1}(x) \geqslant f_{n+1}(z). \tag{3.1}$$
   Allora abbiamo che
   $$f_{n+1}(x) < \min\{f_{n+1}(z), f_{n+k+1}(x)\} \text{ o } f_{n+k+1}(z) < \min\{f_{n+1}(z), f_{n+k+1}(x)\}.$$

Nel primo caso

$$f_{n+1}(x) < \min\{f_{n+1}(z), f_{n+k+1}(x)\} \leqslant f_{n+1}(z)$$

e ciò è assurdo per (3.1); nel secondo caso

$$f_{n+k+1}(z) < \min\{f_{n+1}(z), f_{n+k+1}(x)\} \leqslant f_{n+1}(z)$$

e ciò è assurdo per definizione delle f_i.

2.
$$\omega(\alpha x) = \omega(\alpha z) = f_i(x_i) \text{ per un certo } 1 \leqslant i \leqslant n,$$

con $f_i(x_i) \leqslant f_{n+1}(z)$. Allora abbiamo che

$$f_{n+k+1}(z) < \min\{f_i(x_i), f_{n+k+1}(x)\} \leqslant f_{n+1}(z)$$

e ciò è assurdo per definizione delle f_i.

□

Lemma 3.5.3. *Sia $(E, \mathscr{L})$ un greedoide e $\alpha\beta \in \mathscr{L}$, $\alpha x \in \mathscr{L}$ per un certo $x \in E$. Allora β può essere partizionata in una sequenza di lettere y_i e sottostringhe β_i (eventualmente vuote) nella forma*

$$\beta = y_1\beta_1 y_2\beta_2 \dots y_r\beta_r$$

tale che $\alpha\beta' \in \mathscr{L}$, dove

$$\beta' := x\beta_1 y_1\beta_2 y_2 \dots y_{r-1}\beta_r.$$

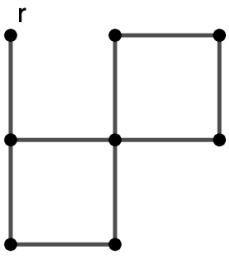
Dimostrazione. Procediamo per induzione su $|\beta|$.
Se $|\beta| = 1$ allora $\beta' = x$ e la tesi è ovvia.
Consideriamo allora $\alpha\gamma \in \mathscr{L}$ tale che $\gamma = \beta z$ per un certo $z \in E$. Per induzione, β può essere partizionato come

$$\beta = y_1\beta_1 y_2\beta_2 \dots y_s\beta_s$$

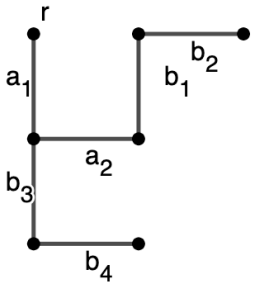
tale che per

$$\beta' = x\beta_1 y_1\beta_2 \dots y_{s-1}\beta_s$$

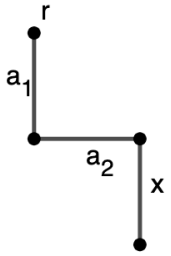
abbiamo $\alpha\beta' \in \mathscr{L}$. Poiché $\alpha\gamma$, $\alpha\beta' \in \mathscr{L}$ e $|\alpha\gamma| > |\alpha\beta'|$, per (L3) esiste $v \notin \alpha\beta'$ tale che $\alpha\beta' v \in \mathscr{L}$. La lettera v può assumere solo due valori: y_s o z. Se $v = y_s$ allora sceglieremo $r = s + 1$ e $\beta_r = \varnothing$; se $v = z$ allora $r = s$ e $\beta_r = \beta_s z$. □



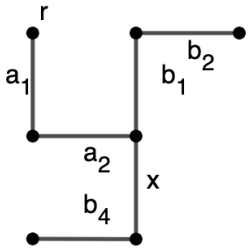
(a) Grafo T con radice r



(b) Parola $\alpha\beta$



(c) Parola αx



(d) Parola $\alpha\beta'$

Figura 3.6

Esempio 25. Consideriamo il grafo T con radice r in Figura 3.6a con la struttura di greedoide di linguaggio descritta nell'Esempio 24. Siano $\alpha = a_1a_2$, $\beta = b_1b_2b_3b_4$ e x tali che $\alpha\beta, \alpha x \in \mathscr{L}$ (Figura 3.6b e 3.6c). Per il Lemma 3.5.3 β può essere partizionata come

$$\beta = b_1\beta_1 b_2\beta_2 b_3\beta_3$$

con $\beta_1 = \beta_2 = \varnothing$ e $\beta_3 = y_4$, tale che per

$$\beta' = x\beta_1 b_1\beta_2 b_2\beta_3 = xb_1b_2b_4$$

abbiamo che $\alpha\beta' \in \mathscr{L}$ (Figura 3.6d).

Lemma 3.5.4. *Sia $(E, \mathscr{L})$ un greedoide e $\alpha\beta \in \mathscr{L}$, $\alpha x \in \mathscr{L}$ per un certo $x \in E$. Supponiamo β sia partizionata come nel lemma precedente, allora per $t = 1, \ldots, r$ abbiamo che $\alpha\beta^t \in \mathscr{L}$ dove*

$$\beta^t = y_1\beta_1 y_2\beta_2 \ldots \beta_{t-1} x\beta_t y_t\beta_{t+1} \ldots y_{r-1}\beta_r$$

.

Dimostrazione. Fissiamo t. Per ipotesi e per (L2) abbiamo che

$$\gamma := \alpha y_1 \beta_1 y_2 \dots y_{t-1} \beta_{t-1} \in \mathscr{L};$$

e per il Lemma 3.5.3 vale

$$\delta := \alpha x \beta_1 y_1 \dots \beta_{t-1} y_{t-1} \in \mathscr{L}.$$

Per (L3) con $|\delta| > |\gamma|$ abbiamo che $\gamma x \in \mathscr{L}$; e per (L2) ed (L3) con $|\alpha\beta'| > |\gamma x|$, dove β' è definito come nel lemma precedente, abbiamo che

$$\beta^t := \gamma x \beta_t y_t \dots y_{r-1} \beta_r \in \mathscr{L}.$$

□

Esempio 26. Riprendiamo l'Esempio 25. Gli elementi descritti nel Lemma 3.5.4 sono

$$\begin{aligned} \beta^1 &= \beta' = x b_1 b_2 b_4, \\ \beta^2 &= b_1 x b_2 b_4, \\ \beta^3 &= b_1 b_2 x b_4. \end{aligned}$$

Teorema 3.5.5. *Sia $\mathscr{L}$ un linguaggio semplice ed ereditario, la coppia $(E, \mathscr{L})$ è un greedoide se e solo se l'algoritmo greedy risolve il problema $(\mathscr{L}, \omega)$ per ogni funzione obiettivo ω compatibile con $\mathscr{L}$.*

Dimostrazione. Sia $\alpha \in \mathscr{L}$ una soluzione ottenuta dall'algoritmo greedy. Tra tutte le soluzioni ottimali consideriamo β tale che abbia stringa iniziale γ in comune con α massimale: se $\alpha = \beta$ allora α è ottimale e la tesi è ovvia, supponiamo quindi per assurdo che $\alpha \neq \beta$. Possiamo scrivere $\alpha = \gamma x \alpha'$ e $\beta = \gamma \beta'$, con $\gamma x \in \mathscr{L}$ per costruzione dell'algoritmo. Per i Lemmi 3.5.3 e 3.5.4 la stringa β' può essere partizionata come

$$\beta' = y_1 \beta_1 y_2 \beta_2 \dots y_r \beta_r$$

tale che per ogni $t = 1, \dots, r$

$$\gamma \beta^t = \gamma y_1 \beta_1 \dots y_{t-1} \beta_{t-1} x \beta_t y_t \dots y_{r-1} \beta_r \in \mathscr{L}.$$

Per la costruzione dell'algoritmo greedy, x è stata scelta tale che per ogni $y \in E$ con $\gamma y \in \mathscr{L}$ abbiamo che

$$\omega(\gamma x) \geqslant \omega(\gamma y).$$

Poiché ω è compatibile con $\mathscr{L}$, per la condizione (ii) abbiamo che

$$\begin{aligned}\omega(\gamma\beta^1) &= \omega(\gamma x\beta_1 y_1 \dots \beta_{r-1}y_{r-1}\beta_r) \geqslant \omega(\gamma\beta^2) \geqslant \dots \geqslant \omega(\gamma\beta^r)\\ &= \omega(\gamma y_1\beta_1 \dots y_{r-1}\beta_{r-1}x\beta_r) \geqslant \omega(\gamma y_1\beta_1 \dots y_{r-1}\beta_{r-1}y_r\beta_r)\\ &= \omega(\beta),\end{aligned}$$

dove l'ultima disuguaglianza segue dalla condizione (i) di compatibilità. Poiché β è una soluzione ottimale, anche $\gamma\beta^1$ deve essere ottimale. Ma $\gamma\beta^1$ ha come stringa iniziale in comune con α la stringa γx, più lunga di γ e ciò contraddice la scelta di β. Quindi α è una soluzione ottimale.

Viceversa, consideriamo $\alpha, \beta \in \mathscr{L}$ tali che $|\alpha| = m < k = |\beta|$. Vogliamo dimostrare che vale (L3), ovvero che esiste $x \in \tilde{\beta}$ tale che $\alpha x \in \mathscr{L}$. Consideriamo allora $\mathscr{A} = \tilde{\alpha} \cup \tilde{\beta}$ e definiamo una funzione a collo di bottiglia generalizzata ω come

$$f_1(x) = \dots = f_k(x) = \begin{cases} 0 & \text{se } x \notin \mathscr{A},\\ 1 & \text{se } x \in \mathscr{A},\end{cases}$$

$$f_{k+1}(x) = \dots = f_r(x) = \begin{cases} 1 & \text{se } x \notin \mathscr{A},\\ 2 & \text{se } x \in \mathscr{A}.\end{cases}$$

Sia $\delta := \beta\delta'$ una parola base ottenuta estendendo β. Allora $\omega(\delta) = 1$. Consideriamo $\gamma := \alpha x_1 \dots x_p$ una soluzione dell'algoritmo greedy ottenuta per estensione di α. Una soluzione così chiaramente esiste. Per ipotesi l'algoritmo greedy dà una soluzione ottimale, quindi abbiamo

$$1 = \omega(\delta) \leqslant \omega(\gamma) \leqslant f_{m+1}(x_1),$$

e poiché $m + 1 \leqslant k$ allora $x_1 \in \mathscr{A}$. Ora, $\beta x_1 \in \mathscr{L}$ poiché $\mathscr{L}$ è ereditario; ed inoltre $x_1 \in \mathscr{A} \setminus \tilde{\alpha} \subseteq \tilde{\beta}$, poiché $\mathscr{L}$ è semplice. Allora x_1 è la lettera cercata per soddisfare (L3).

□

Osservazione 26. Il Teorema 3.2.2 per l'algoritmo greedy sulle matroidi è un caso particolare del Teorema 3.5.5 per l'algoritmo greedy sui greedoidi, dove le funzioni obiettivo osservate sono lineari.

Esempio 27. Dato un grafo con radice, possiamo considerare la struttura di greedoide descritta nell'Esempio 24. Quindi l'algoritmo di Prim per un grafo $G = (V, E)$ descritto nella Definizione 3.7 può essere visto come l'algoritmo greedy per un greedoide applicato al grafo con radice (V, E, v) dove v è il vertice selezionato dall'algoritmo al primo passo.

Bibliografia

[1] D. A. M. Barrington: Greedy Algorithms and Matroids, Note del Corso CMPSCI611: Advanced Algorithms, University of Massachusetts Amhers, 2005, https://people.cs.umass.edu/~barring/cs611/lecture/4.pdf.

[2] A. Björner, G.M. Ziegler: Introduction to greedoids, in N. White (Ed), *Matroid Applications*, Encyclopedia of Mathematics and Its Applications, Vol. 40, Cambridge University Press, Cambridge, 1989, pp. 284–357.

[3] M. X. Goemans: Matroids, Note del Corso 18.438: Advanced Combinatorial Optimization, Massachusetts Institute of Technology, 2009, https://math.mit.edu/ goemans/18438F09/lec8.pdf.

[4] W. Johnson: Matroids, 2009, https://sites.math.washington.edu/~morrow/336_09/papers/Will.pdf.

[5] J. Kleinberg, É. Tardos: *Algorithm Design*, Pearson/Addison Wesley, Boston, 2006, pp 115-208.

[6] B. Korte, L. Lovász, R. Schrader: *Greedoids*, Algorithms and Combinatorics, Vol. 4, Springer-Verlag, Berlin, 1991.

[7] J. McNulty: Cryptomorphisms, MAA Short Course Lecture Notes, 2011, https://www.maa.org/sites/default/files/pdf/shortcourse/2011/crypto.pdf.

[8] J.G. Oxley: *Matroid Theory*, Oxford University Press, Oxford, 1992.

[9] J.G. Oxley: On the interplay between graphs and matroids, in J.W.P. Hirschfeld, *Surveys in Combinatorics 2001*, London Mathematical Society Lecture Note Series, Vool. 288, Cambridge University Press, Cambridge, 2001, pp 199–239.

[10] A.M. Porter: *The Tutte Polynomial and Applications*, Gr. thesis, Whitman College, 2015.

[11] S. Vempala: Greedy Algorithms, Note del Corso CS 6505: Computability and Algorithms, Georgia Tech, 2010, https://www.cc.gatech.edu/classes/AY2010/cs6505_spring/lectures/lecture3.pdf.

[12] D.J.A. Welsh: *Matroid Theory*, L.M.S. Monographs, Academic Press, London, 1976.

[13] N. White: *Theory of Matroids*, Encyclopedia of Mathematics and Its Applications, Vol. 26, Cambridge University Press, Cambridge, 1986.

[14] H. Whitney, On the abstract properties of linear dependence, Amer. J. Math. (1935), 509–533.