Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea Magistrale in Matematica

RAPPRESENTAZIONI LINEARI DI MATROIDI

Tesi di Laurea

Relatore:
Chiar.mo Prof.
FRANCESCO REGONATI

Presentata da:
CHIARA BUCCIARELLI

Anno Accademico 2017/2018

Itaca ti ha dato il bel viaggio,
senza di lei mai ti saresti messo
sulla strada: che cos'altro ti aspetti?
E se la trovi povera, non per questo Itaca ti avrà deluso.
Fatto ormai savio, con tutta la tua esperienza addosso
già tu avrai capito ciò che Itaca vuole significare.
ITACA, *C. Kavafis*

Indice

Elenco delle figure

Introduzione

Sono varie le strutture matematiche che derivano dall'astrazione di strutture già esistenti. Tale processo di astrazione si rivela tanto più fruttuoso quanto più risulta possibile sviluppare una nuova teoria a partire dai nuovi oggetti trovati. Rimane interessante la risoluzione del problema di caratterizzare nei termini più astratti gli oggetti che avevano suggerito l'astrazione. In questa tesi si è considerata un'istanza di questo problema nella teoria delle matroidi, studiando le risposte che sono state date dai matematici che se ne sono occupati.

Il primo a parlare di matroidi fu il matematico americano Hassler Whitney che nel 1935 scrisse un articolo, *On the abstract properties of linear dependence*, in cui fornì un unico trattamento astratto della dipendenza nell'algebra lineare e nella teoria dei grafi. Whitney volle astrarre la struttura dei grafi per cercare di risolvere il famoso problema dei quattro colori. Non ci riuscì, ma diede vita a una nuova teoria. Negli anni molti altri matematici approfondirono il discorso, ampliandolo e scoprendone nuovi aspetti e applicazioni. In particolare ben presto ci si pose il problema della rappresentabilità delle matroidi. Tra coloro che diedero un contributo alla risoluzione di questo problema è doveroso ricordare William T. Tutte, che nel 1958 e 1959 determinò una caratterizzazione per le matroidi binarie e grafiche e enunciò il primo grande teorema riguardo la caratterizzazione delle matroidi regolari in termini di minori esclusi. Si deve a lui anche la caratterizzazione delle matroidi regolari in termini di matrici totalmente unimodulari, il cui studio ha portato

a importanti sviluppi nell'ambito della programmazione lineare. In seguito si cercò anche una caratterizzazione delle matroidi rappresentabili su $GF(3)$, a cui lavorarono numerosi matematici tra cui Paul D. Seymour. Egli inoltre enunciò un importante teorema riguardo alla costruzione delle matroidi regolari che ha significanti implicazioni nell'ottimizzazione combinatoria. La caratterizzazione delle classi di matroidi tramite lo studio dei minori esclusi portò Gian Carlo Rota a formulare nel 1970 una congettura che solo in anni recenti ha trovato dimostrazione.

Questa tesi inizia presentando le matroidi come astrazione del concetto di indipendenza nelle matrici e nei grafi. Esistono numerose assiomatizzazioni equivalenti per definire le matroidi, in questa tesi ne vengono presentate tre: quella per gli indipendenti, quella per i circuiti e quella per le basi, a seguito delle quali viene menzionato il concetto di rango. Si osserva che a diverse matrici può corrispondere una stessa matroide, così come a diversi grafi. In particolare si mostra che le matroidi grafiche possono essere rappresentate come matrici su tutti i campi. Vengono poi descritte le operazioni di duale, sottrazione e contrazione effettuabili sulle matroidi, osservando come agiscono sulle matroidi vettoriali e grafiche. Una volta date queste nozioni generali e dopo aver osservato che le classi delle matroidi rappresentabili su un campo sono chiuse per minori, è stato esposto il seguente problema: quali condizioni matroidali caratterizzano le matroidi rappresentabili su un determinato campo? In particolare è stato presentato un esempio di matroide non rappresentabile su alcun campo, per poi dare una caratterizzazione delle matroidi rappresentabili su $GF(2)$ e $GF(3)$ in termini di minori esclusi. Infine è stato considerato il problema della caratterizzazione delle matroidi regolari, cioè le matroidi rappresentabili su tutti i campi. Si è arrivati quindi a enunciare il Teorema di Tutte che caratterizza le matroidi regolari in termini di minori esclusi e di matrici totalmente unimodulari. È stato approfondito il discorso riguardo a questo Teorema. Il lavoro è stato svolto su due fronti: da una parte sono stati osservati alcuni aspetti dell'enunciato più frequente,

dall'altra si è cercato di mettere in luce l'equivalenza dell'enunciato originale con quello maggiormente conosciuto. Infatti nel lavoro svolto da W. T. Tutte le matroidi emergono in maniera differente rispetto alla presentazione fatta da Whitney, e anche la definizione di matroide regolare pare non avere analogie con quanto definito precedentemente. Dunque sono stati presentati i gruppi di catene, una delle strutture grazie alle quali Tutte definisce il concetto di matroide. Un enunciato equivalente del Teorema di Tutte ha ricevuto una dimostrazione piuttosto semplice ad opera di A. M. H. Gerards, è stata riportata l'equivalenza tra i due enunciati messa in luce da Schrijver.

Per scrivere questa tesi è stato svolto innanzitutto un lavoro di comprensione dell'articolo introduttivo alla teoria delle matroidi di James G. Oxley [4], nel quale è stato individuato nel Teorema di Tutte il punto focale della nostra riflessione. Per un approfondimento riguardo a questo Teorema, è stato consultato il lavoro di Paul D. Seymour [2] a cui rimanda Oxley. Si è studiato l'articolo di A. M. H. Gerards [1] suggerito da Seymour per trovare una dimostrazione semplificata dell'enunciato originale. Infine, per mostrare l'equivalenza tra le diverse formulazioni del Teorema è stato fatto riferimento all'opera di Alexander Schrijver [6]. Parallelamente sono stati consultati alcuni dei lavori di William T. Tutte ([8], [9] e [10]) nei quali è descritto il suo approccio al problema ed i suoi risultati, evidenziando la relazione tra il suo enunciato e quello più frequente.

Capitolo 1

Introduzione alle matroidi

Per poter parlare di rappresentazione di matroidi è necessario innanzitutto introdurre alcuni concetti, primo tra tutti quello di matroide.

1.1 Che cos'è una matroide?

Consideriamo una generica matrice

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

a elementi in un campo. Indichiamo con E l'insieme $\{1, 2, \ldots n\}$ degli indici di colonna e con $\mathcal{I}$ la collezione dei sottoinsiemi I di E la cui sequenza di colonne corrispondenti è linearmente indipendente. Chiamiamo l'insieme E *insieme sostegno*, mentre $\mathcal{I}$ lo chiamiamo *insieme degli indipendenti*. Consideriamo alcune proprietà di $\mathcal{I}$:

(I1) $\mathcal{I}$ è non vuoto.

(I2) Ogni sottoinsieme di ogni insieme di $\mathcal{I}$ è a sua volta un insieme di $\mathcal{I}$.

(I3) Se X e Y sono insiemi di $\mathcal{I}$ e $|X| = |Y| + 1$, allora esiste un elemento x appartenente a $X - Y$ tale che $Y \cup \{x\}$ è un insieme di $\mathcal{I}$.

Teorema 1.1.1. *Sia A una matrice su un campo F. Sia E l'insieme degli indici di colonna di A e sia $\mathcal{I}$ la collezione dei sottoinsiemi I di E per cui le colonne indicate da I sono vettori linearmente indipendenti. Allora $(E, \mathcal{I})$ soddisfa (**I1**)-(**I3**).*

Dimostrazione. Ovviamente $\mathcal{I}$ soddisfa (**I1**) e (**I2**), verifchiamo che soddisfi anche (**I3**).
Siano $X = \{x_1, x_2, \dots x_n, x_{n+1}\}$ e $Y = \{y_1, y_2, \dots y_n\}$ due sottoinsiemi di E appartenenti a $\mathcal{I}$ che individuano due insiemi di colonne di A che chiamiamo ancora per semplicità $X = \{x_1, x_2, \dots x_n, x_{n+1}\}$ e $Y = \{y_1, y_2, \dots y_n\}$. Possiamo farlo perché, essendo colonne linearmente indipendenti, sono a due a due distinte.
Assumiamo per assurdo che non ci sia un $x \in X - Y$ tale che $Y \cup \{x\}$ sia un insieme di vettori linearmente indipendenti. Allora

$$\begin{aligned} x_1 = &\quad c_{1,1}y_1 + c_{1,2}y_2 + \cdots + c_{1,n}y_n \\ x_2 = &\quad c_{2,1}y_1 + c_{2,2}y_2 + \cdots + c_{2,n}y_n \\ &\quad \cdots \\ x_{n+1} = &\quad c_{n+1,1}y_1 + c_{n+1,2}y_2 + \cdots + c_{n+1,n}y_n. \end{aligned}$$

Supponendo che $c_{1,1} \neq 0$, posso sommare a x_2 il vettore $-\frac{c_{2,1}}{c_{1,1}}x_1$, ottenendo così una combinazione lineare di x_1 e x_2 uguale a una combinazione degli y_i dove il coefficiente di y_1 è uguale a zero. Consideriamo questo nuovo vettore al posto di x_2. Allo stesso modo è possibile sommare a x_3 i vettori x_1 e il nuovo vettore moltiplicati per un opportuno coefficiente, ottenendo una combinazione lineare di x_1,x_2 e x_3 uguale a una combinazione degli y_i con il coefficiente di y_1 e y_2 uguale a zero. Consideriamo quest'ultimo vettore al posto di x_3. Operiamo in questo per tutti i vettori x_i. L'ultimo vettore che si va a sostituire a x_{n+1} è uguale a una combinazione degli y_i dove i coefficienti sono tutti zero, cioè uguale al vettore nullo. Effettuando queste operazioni, la dipendenza lineare dei vettori $x_1, \dots x_{n+1}$ non viene alterata. Ma allora è impossibile che X sia un insieme di vettori linearmente indipendenti, dato che uno di questi vettori è il vettore nullo. □

In generale

Definizione 1.1.1. Una *matroide* è una coppia $(E, \mathcal{I})$ dove E è un insieme finito e $\mathcal{I}$ è una collezione di sottoinsiemi di E che soddisfano (**I1**)-(**I3**).

La matroide ottenuta da una matrice A è chiamata *matroide vettoriale di* A e si indica con $M[A]$.

Esempio 1.1.1. Riportiamo alcuni esempi di matroidi.

- Se $E = \emptyset$, esiste un unica matroide che abbia E come insieme sostegno, cioè quella con $\mathcal{I} = \{\emptyset\}$.
- Se $E = \{1\}$ allora esistono esattamente due matroidi su E, una con $\mathcal{I} = \{\emptyset\}$ e l'altra con $\mathcal{I} = \{\emptyset, \{1\}\}$.
- Sia E un insieme di n elementi e, per un intero r tale che $0 \leq r \leq n$, sia $\mathcal{I}$ la collezione di sottoinsiemi di E con al massimo r elementi. È semplice verificare che $(E, \mathcal{I})$ soddisfa (**I1**)-(**I3**) e che quindi è una matroide. Questa matroide è chiamata *matroide uniforme su* E e si indica con $U_{r,n}(E)$.
  Un caso banale è $U_{0,0}(\emptyset)$, cioè la matroide uniforme sull'insieme vuoto dove gli indipendenti sono gli insiemi con zero elementi; ciò significa che l'unico indipendente è l'insieme vuoto stesso. Un altro caso banale di matroide uniforme è $U_{n,n}(\{a_1, \dots a_n\})$, dove l'insieme degli indipendenti coincide con l'insieme delle parti di $\{a_1, \dots a_n\}$.

Osservazione 1.1.1. Se gli elementi di una matrice appartengono a un anello, non è detto che questa matrice dia luogo a una matroide.
Sia

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{bmatrix}$$

una matrice a elementi in $\mathbb{Z}_6$. Se consideriamo i due insiemi di colonne linearmente indipendenti $X = \{\binom{1}{0}, \binom{0}{1}\}$ e $Y = \{\binom{2}{3}\}$, si può osservare che (**I3**) non è soddisfatta dato che $2\binom{2}{3} - 4\binom{1}{0} = \binom{0}{0}$ e $3\binom{2}{3} - 3\binom{0}{1} = \binom{0}{0}$ e che quindi la matrice A non è la rappresentazione di una matroide.

Supponiamo di avere due matroidi $M_1 = (E_1, \mathcal{I}_1)$ e $M_2 = (E_2, \mathcal{I}_2)$ tali che esista una biezione tra E_1 e E_2 tale che un insieme è indipendente in M_1 se e solo se la sua immagine è indipendente in M_2. Allora si dice che M_1 e M_2 sono *isomorfe*, e si indica con $M_1 \cong M_2$.
Ad esempio, se $E_1 = E_2 = \{1, 2, 3\}$, $\mathcal{I}_1 = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ e $\mathcal{I}_2 = \{\emptyset, \{1\}, \{3\}, \{1, 3\}\}$, allora $M_1 \cong M_2$. Infatti esiste una biezione

$$\begin{array}{ccc} \phi : E_1 & \to & E_2 \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \end{array}$$

che preserva l'indipendenza.

Osservazione 1.1.2. Presi due insiemi qualsiasi E ed E', entrambi con cardinalità n, si può facilmente verificare che $U_{r,n}(E) \cong U_{r,n}(E')$. Quindi, dato che le matroidi uniformi su un insieme di n elementi con cardinalità degli indipendenti $\leq r$ sono tutte isomorfe, si parla di matroide uniforme e si indica $U_{r,n}$.

Una matroide M isomorfa a $M[A]$ per una qualche matrice A su un campo F si dice che è *rappresentabile su* F, e A è chiamata *rappresentazione di* M *su* F. In particolare, se $F = GF(2)$ allora si dice che la matroide è *binaria* mentre se $F = GF(3)$ la matroide è chiamata *ternaria*. Se una matroide è rappresentabile su tutti i campi, allora si dice che la matroide è *regolare*.

Come mostra il prossimo Teorema, è possibile ottenere una matroide anche a partire da un grafo.

Teorema 1.1.2. *Sia $G = (V, E)$ un grafo. Sia E la collezione dei suoi archi e sia $\mathcal{I}$ la collezione degli insiemi di lati che individuano una foresta in G. Allora $(E, \mathcal{I})$ è una matroide.*

Dimostrazione. Dobbiamo mostrare che $\mathcal{I}$ soddisfa (**I1**)-(**I3**). Il fatto che soddisfi (**I1**) e (**I2**) è banale, verifichiamo che soddisfi anche (**I3**).

Siano X e Y due insiemi di lati che individuano ciascuno una foresta (per semplicità diremo che X e Y sono due foreste) tali che $|Y| = |X| + 1$. Supponiamo per assurdo che per ogni $y \in Y - X$, $X \cup \{y\}$ non sia una foresta. Allora questo significa che tutti gli y di Y collegano due vertici che sono estremi di archi di X apparteneti alla stessa componente connessa (cioè allo stesso albero). Dunque l'insieme dei vertici di ciascun albero di Y è contenuto nell'insieme dei vertici di un albero di X. Guardiamo ora X come l'unione di n alberi: $X = \bigcup_{i=1}^{n} T_i$. Il numero di lati di ogni albero T_i è $e_i = v_i - 1$, dove v_i è il numero di vertici di quell'albero. Voglio dimostrare che il numero di lati di Y che ha vertici in comune con T_i è minore o uguale a e_i. Consideriamo tutti gli archi di Y che hanno come estremi vertici di T_i (supponiamo che questi vertici ci siano, nel caso in cui non ci siano banalmente $0 < e_i$). Questi archi sono raggruppati in m alberi, con $m \geq 1$. Allora il loro numero è $e'_i = v'_i - m$, con $v'_i \leq v_i$ numero di vertici degli archi e dunque $e'_i \leq e_i \quad \forall i = 1, \dots n$. Ma questo significa che $|X| = \sum e_i \geq \sum e'_i = |Y|$, che è in contraddizione con l'ipotesi. □

Questa matroide è chiamata *matroide dei cicli* e si indica con $M(G)$. Una matroide isomorfa alla matroide dei cicli di un qualche grafo è chiamata *matroide grafica*.

Esempio 1.1.2. Consideriamo il grafo G mostrato in Figura 1.1. L'insieme E

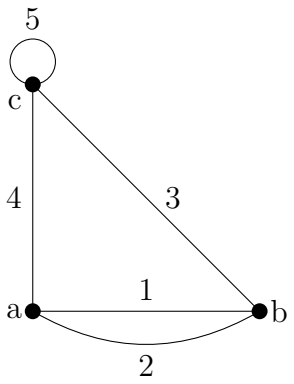

Figura 1.1: Grafo G

dei suoi archi è $\{1, 2, 3, 4, 5\}$, mentre $\mathcal{I}$ contiene tutti i sottoinsiemi di E che formano un albero in G, cioè $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$.

Se si vuole rappresentare una matroide nella quale vi siano al più tre elementi indipendenti è possibile farne una *rappresentazione geometrica*. Questa consiste nel rappresentare gli elementi della matroide come punti nel piano, e la relazione di indipendenza tra elementi si può rappresentare tramite il non allineamento dei punti. È possibile ricorrere all'ausilio di linee curve per indicare la dipendenza tra elementi quando non è possibile farlo tramite la geometria euclidea.

Esempio 1.1.3. Un altro esempio molto importante di matroide è il seguente. Consideriamo la matrice

$$A_7 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

e consideriamo la matroide che è rappresentata da A_7 su $GF(2)$. La chiamiamo *matroide di Fano* e la indichiamo con F_7. La matroide rappresentata da A_7 su $GF(3)$ si chiama *matroide non-Fano* e viene indicata con F_7^-. La

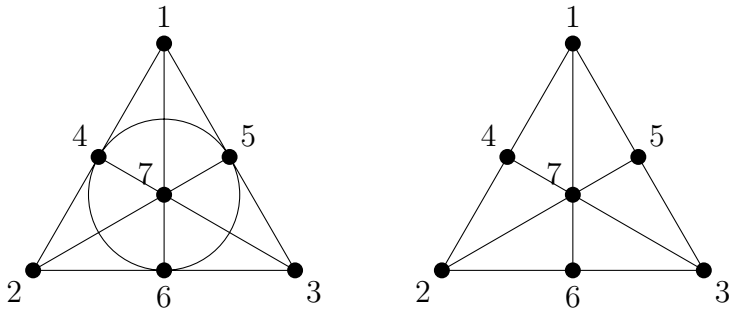

Figura 1.2: Matroide di Fano e matroide non-Fano

Figura 1.2 è la rappresentazione geometrica delle matroidi F_7 e F_7^-. Gli elementi dell'insieme sostegno sono $\{1, 2, 3, 4, 5, 6, 7\}$ mentre gli indipendenti sono i sottoinsiemi di E con cardinalità minore o uguale a 3 e tale che non contenga tre punti collineari. In F_7 risultano collineari anche i punti $4, 5$ e 6.

Proposizione 1.1.3. *Siano M_1 e M_2 le matroidi $(E_1, \mathcal{I}_1)$ e $(E_2, \mathcal{I}_2)$, con E_1 e E_2 disgiunti. Allora*

$$\{E_1 \cup E_2, \{I_1 \cup I_2 : I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}\}$$

è una matroide.

La dimostrazione di questa Proposizione si ha verificando che sono soddisfatte (**I1**)-(**I3**).
La matroide della Proposizione 1.1.3 si chiama *somma diretta di M_1 e M_2* e si indica con $M_1 \oplus M_2$. Si può notare che la somma diretta di due matroidi rappresentabili su F è anch'essa rappresentabile su F. Infatti se A_1 e A_2 sono le rappresentazioni di M_1 e M_2 su F, allora $\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$ è la rappresentazione di $M_1 \oplus M_2$ su F.

1.2 Altre assiomatizzazioni

Come mostra Whitney in [12], è possibile, considerando famiglie di insiemi diverse dalla famiglia degli indipendenti, dare proprietà equivalenti a (**I1**)-(**I3**) che consentano di individuare le matroidi. Dalla proprietà (**I2**) si può dedurre che una matroide è unicamente determinata dalla sua collezione di insiemi indipendenti massimali, che sono chiamati *basi*, oppure dalla collezione dei suoi insiemi dipendenti minimali, che sono chiamati *circuiti*.

Osservazione 1.2.1. Per una matroide dei cicli $M(G)$ le basi sono gli insiemi degli archi di G che formano le foreste massimali, mentre i circuiti sono gli insiemi degli archi di G che formano i cicli. Le matroidi dei cicli sono naturalmente definite in termini di circuiti.

Osservazione 1.2.2. Esiste anche una caratterizzazione dei circuiti di una matroide vettoriale. Sia A una matrice a elementi in un campo F, sia $M[A]$ la matroide vettoriale rappresentata da A e siano $c_1, \dots c_n$ le colonne di A. Allora $C = \{i_1, \dots i_m\}$ è un circuito di $M[A]$ se e solo se esiste una e una

sola (a meno di costanti moltiplicative) scrittura $\sum_{j=1}^{m} \alpha_j c_{i_j} = 0$ con qualche $\alpha_j \neq 0$. In tal caso tutti gli α_j sono diversi da 0.

Utilizzando le proprietà (**I1**)-(**I3**) si può dimostrare che la collezione $\mathcal{C}$ dei circuiti di una matroide M ha le seguenti proprietà:

(C1) L'insieme vuoto non è un elemento di $\mathcal{C}$.

(C2) Nessun elemento di $\mathcal{C}$ è un sottoinsieme proprio di un altro elemento di $\mathcal{C}$.

(C3) Se C_1 e C_2 sono elementi distinti di $\mathcal{C}$ e $e \in C_1 \cap C_2$, allora $(C_1 \cup C_2) - \{e\}$ contiene un elemento di $\mathcal{C}$.

Queste tre proprietà caratterizzano le collezioni di insiemi che possono essere circuiti di una matroide. Più formalmente:

Teorema 1.2.1. *Sia M una matroide e sia $\mathcal{C}$ la sua collezione di circuiti. Allora $\mathcal{C}$ soddisfa (**C1**)-(**C3**). Viceversa, supponiamo che $\mathcal{C}$ sia una collezione di sottoinsiemi di un insieme finito E che soddisfa (**C1**)-(**C3**) e sia $\mathcal{I}$ la collezione dei sottoinsiemi di E che non contengono nessun elemento di $\mathcal{C}$. Allora $(E, \mathcal{I})$ è una matroide che ha $\mathcal{C}$ come collezione dei suoi circuiti.*

Sempre utilizzando le proprietà (**I1**)-(**I3**) è possibile mostrare che la collezione $\mathcal{B}$ delle basi di una matroide M gode delle seguenti proprietà:

(B1) $\mathcal{B}$ è non vuota.

(B2) Se B_1 e B_2 sono elementi di $\mathcal{B}$ e $x \in B_1 - B_2$, allora esiste un elemento y di $B_2 - B_1$ tale che $(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}$.

Queste proprietà caratterizzano le matroidi in termini di collezione di basi. Infatti vale il seguente Teorema:

Teorema 1.2.2. *Sia $\mathcal{B}$ una collezione di sottoinsiemi di un insieme finito E. Allora $\mathcal{B}$ è la collezione di basi di una matroide su E se e solo se $\mathcal{B}$ soddisfa (**B1**) e (**B2**).*

Segue da (**I3**) che tutte le basi di una matroide M hanno la stessa cardinalità che è chiamata *rango* di M e si indica con $r(M)$. Di conseguenza il rango di una matroide vettoriale $M[A]$ è uguale al rango della matrice A (inteso come numero massimo di colonne di A linearmente indipendenti). Se G è un grafo connesso e ha m vertici, allora $r(M(G)) = m - 1$. Questo rappresenta il numero di archi di un qualsiasi albero massimale di G. In generale il rango di un grafo è uguale al numero dei suoi vertici a cui viene sottratto il numero delle sue componenti connesse.
Whitney fornisce anche una caratterizzazione delle matroidi in termini di rango, enunciando tre proprietà equivalenti a (**I1**)-(**I3**) che però non riportiamo.

1.3 Osservazioni sulle matroidi vettoriali e dei cicli

Sia per quanto riguarda sia le matroidi vettoriali che quelle dei cicli, le rappresentazioni tramite matrici e tramite grafi rispettivamente non sono uniche.

Proposizione 1.3.1. *Sia A una matrice a elementi in un campo F. Allora $M[A]$ rimane inalterata se vengono compiute le seguenti operazioni su A:*

1. *scambio di due righe;*
2. *moltiplicazione di una riga per un elemento di F diverso da zero;*
3. *sostituzione di una riga con la somma di quella riga e un'altra;*
4. *rimozione di una riga di zeri (a meno che non sia l'unica riga);*
5. *scambio di due colonne;*
6. *moltiplicazione di una colonna per un elemento di F diverso da zero.*

Consideriamo una matrice A non nulla di rango r. Allora effettuando le operazioni descritte dalla Proposizione 1.3.1 è possibile trasformare A in una matrice della forma $[I_r|D]$, dove I_r è la matrice identità $r \times r$. Questo significa che tutte le matroidi vettoriali ammettono una rappresentazione di questa forma. La matroide che è rappresentata dalla matrice nulla è isomorfa a $U_{0,n}$.

Notiamo anche che grafi non isomorfi tra loro possono avere matroidi dei cicli isomorfe. Ad esempio, le matroidi dei cicli di grafi che differiscono solo per una collezione di vertici isolati sono isomorfe. In generale, se un grafo ha k componenti connesse $G_1, G_2, \dots G_k$, e v_i è un vertice qualsiasi della componente G_i, allora il grafo ottenuto identificando tutti i vertici v_i ha la stessa matroide dei cicli di G. Infatti l'identificazione di vertici di componenti connesse distinte non varia l'insieme degli archi di nessun ciclo.

La *matrice di incidenza* di un grafo è la matrice $A_{m\times n}$ con m numero dei vertici del grafo e n numero dei suoi archi tale che

$$a_{i,j} = \begin{cases} 1 & \text{se } i \text{ è un vertice dell'arco } j, \\ 0 & \text{altrimenti.} \end{cases}$$

Nel caso il cui l'arco j sia un cappio, $a_{i,j} = 0 \ \forall i$.

Esempio 1.3.1. Riprendendo l'Esercizio 1.1.2, la matrice di incidenza associata al grafo G è

$$A_G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

dove le righe indicano nell'ordine i vertici a, b e c di G e le colonne indicano gli archi $1, 2, 3, 4$ e 5 rispettivamente. Si può osservare che gli insiemi di colonne linearmente indipendenti sono tutti e soli gli insiemi contenuti nell'insieme degli indipendenti di $M(G)$.

Teorema 1.3.2. *Sia G un grafo, e sia A_G la sua matrice di incidenza di dimensione $m \times n$. Sia A'_G la matrice ottenuta da A_G sostituendo in ogni*

colonna non nulla il secondo 1 *con un* -1*. Allora* A'_G *rappresenta* $M(G)$ *su tutti i campi.*

Dimostrazione. Sia C un ciclo di G, voglio dimostrare che il corrispondente insieme di colonne $X = \{x_1, \dots x_l\}$ di A'_G è linearmente dipendente minimale. Se C è un cappio, allora la colonna corrispondente è una colonna con elementi uguali a zero, che costituisce un insieme linearmente dipendente minimale. Supponiamo che C non sia un cappio. Allora è possibile ordinare i lati del ciclo e i vertici su cui incidono i lati in una sequenza ciclica $v_1\, x_{j_1}\, v_2 \dots v_l\, x_{j_l}$, dove $j_1, \dots j_l$ sono gli indici delle colonne di X riordinati, in modo da ottenere come matrice di incidenza del sottografo individuato da C (a cui ho sostituito il secondo 1 con un -1)

$$A'_C = \begin{array}{c} \begin{matrix} x_{j_1} & x_{j_2} & x_{j_3} & \cdots & x_{j_{l-1}} & x_{j_l} \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & -1 & -1 \end{bmatrix} \end{array}.$$

Allora si ha che $\sum_{i=1}^{l} \alpha_i x_{j_i} = 0$ se $\alpha_i = 1 \ \ \forall i \neq l$ e $\alpha_l = -1$ e quindi le colonne corrispondenti a C sono linearmente dipendenti. Togliendo una qualsiasi di queste colonne, rimangono due righe con un solo elemento diverso da zero, e quindi è impossibile poter scrivere ciascuna colonna come combinazione lineare delle altre. Ciò significa che X è un insieme di vettori linearmente dipendenti minimale.
Viceversa, supponiamo di avere un insieme $X = \{x_1, \dots x_l\}$ di colonne di A'_G che formano un circuito. Queste colonne formano una matrice di dimensione $m \times l$. Consideriamo questa matrice a cui tolgliamo le righe con tutti gli elementi nulli, ottenendo una matrice B di dimensione $m' \times l$. Dato che ciascun vettore di X ha una componente uguale a 1 e una uguale a -1, la somma delle righe di B sarà il vettore nullo, e questo significa che $r(B) \leq$

$m' - 1$. Inoltre, dato che le colonne di B formano un circuito, avremo anche che $r(B) = l - 1$. Quindi $l \leq m'$.
Indichiamo ora con $r_1, r_2, \ldots r_{m'}$ il numero di elementi diversi da 0 nelle righe $1, 2, \ldots m'$ rispettivamente. Dato che ogni colonna si deve poter scrivere come combinazione lineare delle altre, è necessario che $r_i \geq 2 \ \forall i$. Analogamente siano $c_1, c_2, \ldots c_l$ il numero di elementi non nulli per ogni colonna. Allora, per come è costruita A'_G, $c_i = 2 \ \forall i$. Dunque, dato che $\sum_{i=1}^{m'} r_i = \sum_{i=1}^{l} c_i (= 2l)$ si ottiene che $m' \leq l$. Quindi $m' = l$ e in particolare $r_i = 2 \ \forall i$. Questo significa che nel sottografo di G individuato da B ogni vertice ha esattamente due archi collegati. Inoltre, essendo X un dipendente minimale, non è possibile che il sottografo individuato abbia più di una componente connessa. Quindi il sottografo rappresenta un ciclo di G. □

In particolare, se siamo in $GF(2)$, la matrice di incidenza A_G coincide con A'_G e quindi $M[A_G] = M(G)$. Ciò significa che ogni matroide grafica è binaria, dato che è possibile averne una rappresentazione su $GF(2)$.

Capitolo 2

Operazioni sulle matroidi

Esistono tre operazioni fondamentali per le matroidi: il passaggio al duale, la sottrazione e la contrazione.

2.1 Duale di una matroide

Sia M una matroide con insieme sostegno E, e sia $\mathcal{B}$ la collezione delle basi di M. Sia $\mathcal{B}^* = \{E - B : B \in \mathcal{B}\}$. Allora si può mostrare che $\mathcal{B}^*$ è la collezione delle basi di una matroide con insieme sostegno E. Questa matroide è chiamata *duale* di M e viene indicata con M^*. Le basi di M^* sono chiamate *cobasi* di M e, allo stesso modo, i circuiti di M^* sono chiamati *cocircuiti* di M.

Proposizione 2.1.1. *Valgono le seguenti proprietà:*

1. $M = (M^*)^*$;
2. $(M_1 \oplus M_2)^* = M_1^* \oplus M_2^*$;
3. $U_{r,n}^* \cong U_{n-r,n}$;
4. *per una matroide M con insieme sostegno di cardinalità n vale* $r(M) + r(M^*) = n$.

Osservazione 2.1.1. Dato un grafo planare[1] G, è possibile costruire il grafo duale G^* i cui cicli sono i *tagli* di G, cioè gli insiemi minimali di archi di G con la proprietà che la loro rimozione aumenta il numero delle componenti connesse di G. La sua costruzione è piuttosto complicata da riportare e esula dagli scopi della tesi. Si può però dimostrare che la matroide associata al grafo G^*, $M(G^*)$, coincide con la duale della matroide associata a G, $M^*(G)$. È interessante osservare che a partire da un grafo, si può costruire una matroide considerando i suoi cicli (matroide grafica) o considerando i suoi tagli (*matroide cografica*).

Teorema 2.1.2. *Sia M una matroide con insieme sostegno di cardinalità n rappresentabile su un campo F tramite la matrice $[I_r|D]$. Allora anche M^* è rappresentabile su F, e la sua rappresentazione è data dalla matrice $[-D^T|I_{n-r}]$.*

Teorema 2.1.3. *Sia M una matroide.*

- *Un insieme C^* è un cocircuito di M se e solo se C^* è un insieme minimale che ha intersezione non vuota con tutte le basi di M.*
- *Un insieme B è una base di M se e solo se B è un insieme minimale che ha intersezione non vuota con ogni cocircuito di M.*

2.2 Sottrazione e contrazione

Sia M una matroide $(E, \mathcal{I})$ e sia e un elemento di E. Sia $\mathcal{I}' = \{I \subseteq E - \{e\} : I \in \mathcal{I}\}$. Allora si può facilmente mostrare che $(E - \{e\}, \mathcal{I}')$ è una matroide. Indichiamo questa matroide con $M \setminus e$ e la chiamiamo *sottrazione* di e da M.

[1] Un grafo (V, E) è un *grafo planare* se esiste una funzione che associa a ogni elemento di V un punto del piano e a ogni elemento di E una curva topologica tale che e incide su v se e solo se la curva $f(e)$ ha come estremo il punto $f(v)$ e tale che le curve associate agli archi non si intersechino tra loro.

Osservazione 2.2.1. La rappresentazione della sottrazione di un elemento e da una matroide vettoriale $M[A]$ è data dalla matrice A a cui viene rimossa la colonna e.
Se invece abbiamo una matroide dei cicli $M(G)$, la rappresentazione della sottrazione di un elemento e è data dal grafo G da cui viene eliminato l'arco e (Figura 2.1a).
Infine la sottrazione di una elemento dalla matroide uniforme $U_{r,n}$ dà come risultato la matroide uniforme $U_{r,n-1}$.

Prendiamo una matroide $M = (E, \mathcal{I})$ e sia e un elemento di E indipendente. Sia $\mathcal{I}'' = \{I \subseteq E - \{e\} : I \cup \{e\} \in \mathcal{I}\}$. Allora anche $(E - \{e\}, \mathcal{I}'')$ è una matroide. Questa matroide è chiamata *contrazione* di e su M e si indica con M/e. Nel caso in cui e sia un dipendente, $M/e = M \setminus e$.

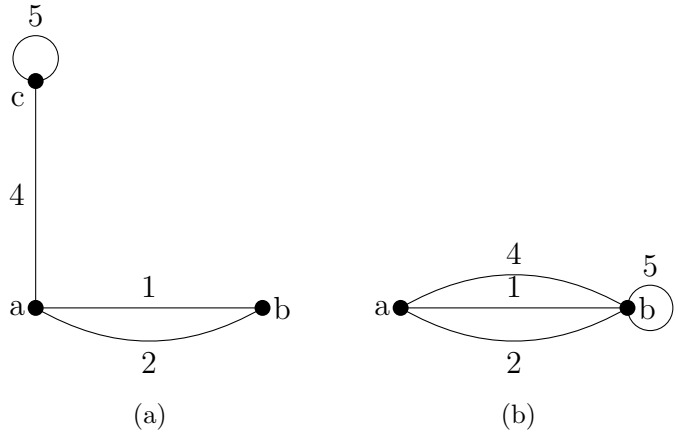

Figura 2.1: Sottrazione (a) e contrazione (b) dell'arco 3 dal grafo G

Osservazione 2.2.2. La rappresentazione della contrazione di un elemento e su una matroide vettoriale $M[A]$ è rappresentata nel seguente modo:

- se e è una colonna di zeri, la matrice che rappresenta M/e è la matrice A a cui viene rimossa la colonna e;
- se e è un vettore della base canonica, la matrice che rappresenta M/e è la matrice a cui vengono rimosse la colonna e e la riga che essa determina;

- nel caso e non sia né il vettore nullo né un vettore della base canonica, si effettuano alcune tra le operazioni descritte nella Proposizione 1.3.1 su A in modo da ottenere una matrice A' in cui e è un vettore della base canonica e si opera come nel punto precedente sulla matrice A'.

Nel caso di una matroide dei cicli $M(G)$, la contrazione di un elemento e è data dalla matroide dei cicli associata al grafo G a cui viene tolto l'arco e e i cui due vertici vengono identificati (Figura 2.1b).
Infine la contrazione di un elemento della matroide $U_{r,n}$ dà luogo alla matroide $U_{r-1,n-1}$.

2.3 Minori

Proposizione 2.3.1. *Sia M una matroide e siano e ed f due elementi distinti di M. Allora valgono le seguenti proprietà:*

- $M \setminus e \setminus f = M \setminus f \setminus e$;
- $M/e/f = M/f/e$;
- $M \setminus e/f = M/f \setminus e$.

Questo significa che se $M = (E, \mathcal{I})$ è una matroide e X e Y sono sottoinsiemi disgiunti di E, allora le matroidi $M \setminus X$, M/Y e $M \setminus X/Y$ sono ben definite.

Definizione 2.3.1. Sia M una matroide. Un *minore* di M è una matroide che può essere ottenuta da M tramite una sequenza di sottrazioni e contrazioni, cioè una matroide della forma $M \setminus X/Y$ o, equivalentemente, $M/Y \setminus X$. Se $X \cup Y \neq \emptyset$ allora $M \setminus X/Y$ è un *minore proprio* di M.

La seguente Proposizione mostra la caratterizzazione degli indipendenti, delle basi e dei circuiti di M/T e $M \setminus T$, con T sottoinsieme dell'insieme sostegno.

Proposizione 2.3.2. *Sia M una matroide su un insieme E, e sia T un sottoinsieme di E. Allora $M \setminus T$ e M/T sono matroidi su $E - T$. Inoltre, per un sottoinsieme X di $E - T$*

1. *X è un indipendente di $M \setminus T$ se e solo se X è un indipendente di M;*
2. *X è un circuito di $M \setminus T$ se e solo se X è un circuito di M;*
3. *X è una base di $M \setminus T$ se e solo se X è un sottoinsieme massimale di $E - T$ che è indipendente in M;*
4. *X è un indipendente di M/T se e solo se $X \cup B_T$ è un indipendente di M per un qualche sottoinsieme massimale B_T di T che è indipendente in M;*
5. *X è un circuito di M/T se e solo se X è un elemento non vuoto minimale di $\{C - T : C$ è un circuito di $M\}$;*
6. *X è una base di M/T se e solo se $X \cup B_T$ è una base di M per un qualche sottoinsieme massimale B_T di T che è indipendente in M.*

Osservazione 2.3.1. Dagli ultimi due punti di questa Proposizione segue che $M^*/T = (M \setminus T)^*$ e $M^* \setminus T = (M/T)^*$.

Alcune classi di matroidi sono *chiuse per minori*, cioè tutti i minori di ogni membro di quella classe appartengono a loro volta a quella classe.

Osservazione 2.3.2. La classe delle matroidi uniformi è chiusa per minori e per dualità.

Teorema 2.3.3. *Le classi delle matroidi grafiche e cografiche sono chiuse per minori. Inoltre, per qualsiasi campo F, la classe delle matroidi rappresentabili su F è chiusa per minori e per dualità.*

La validità del Teorema 2.3.3 si può verificare osservando quanto detto per le operazioni di duale, sottrazione e contrazione riguardo a queste classi.

Non tutte le classi di matroidi sono chiuse per minori. Un esempio di classe di matroidi non chiusa per minori è la classe delle *matroidi trasversali*.
Sia $\mathcal{A}$ una collezione $(A_1, A_2, \dots A_m)$ di sottoinsiemi di un insieme finito E. Un sottoinsieme $X = \{x_1, x_2, \dots x_k\}$ di E è un *trasversale parziale* di $\mathcal{A}$ se esiste una mappa iniettiva $\phi : \{1, 2, \dots k\} \to \{1, 2, \dots m\}$ tale che $x_i \in A_{\phi(i)}$ per ogni i.

Teorema 2.3.4. *Sia $\mathcal{A}$ una collezione di sottoinsiemi di un insieme finito E. Sia $\mathcal{I}$ la collezione di tutti i trasversali parziali di $\mathcal{A}$. Allora $(E, \mathcal{I})$ è una matroide.*

La matroide descritta in questo Teorema viene indicata con $M[\mathcal{A}]$, e tutte le matroidi isomorfe a una matroide di questo tipo si chiamano *matroidi trasversali*.

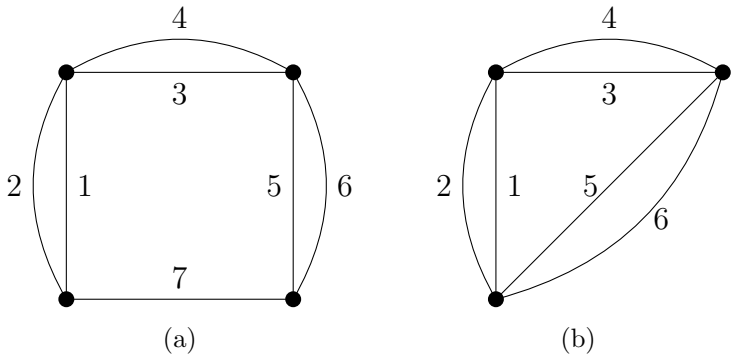

Figura 2.2: (a) $M(G)$ è trasversale, (b) $M(G/7)$ non è trasversale

Esempio 2.3.1. Consideriamo i grafi G e $G/7$ mostrati nella Figura 2.2a e 2.2b rispettivamente. La matroide dei cicli $M(G)$ è trasversale, infatti si può facilmente osservare che è isomorfa a $M[\mathcal{A}]$, dove $\mathcal{A} = (\{1, 2, 7\}, \{3, 4, 7\}, \{5, 6, 7\})$ (si può ad esempio osservare che la collezione degli archi degli alberi massimali di G e la lista dei trasversali parziali con $k = 3$ coincidono). La matroide $M(G/7)$, invece, non è trasversale.
Supponiamo che $M(G/7)$ sia trasversale, allora esiste una famiglia $\mathcal{A}'$ di insiemi tale che $M(G/7) = M[\mathcal{A}']$. Ogni sottoinsieme di $E = \{1, 2, 3, 4, 5, 6\}$

formato da un singoletto è un indipendente, ma $\{1,2\},\{3,4\}$ e $\{5,6\}$ sono dipendenti. Questo significa che ognuno di $\{1,2\},\{3,4\}$ e $\{5,6\}$ è sottoinsieme di esattamente un insieme di $\mathcal{A}'$. Siano questi insiemi A'_1, A'_2 e A'_3 rispettivamente. Inoltre, dato che $\{1,3\},\{1,5\}$ e $\{3,5\}$ sono indipendenti, A'_1, A'_2 e A'_3 sono necessariamente distinti. Quindi $\{1,3,5\}$ è un parziale trasversale di $\mathcal{A}'$ e dunque è indipendente in $M(G/7)$, e questa è una contraddizione.

In seguito a questo Esempio, possiamo concludere che la classe delle matroidi trasversali non è chiusa per minori.

Consideriamo ora le classi di matroidi chiuse per minori. È possibile descriverle osservando le matroidi minimali che non rientrano in tale classe, cioè se $\mathcal{M}$ è una classe di matroidi chiusa per minori, studiamo la collezione di matroidi minimali non contenute in $\mathcal{M}$ che indichiamo con $\mathcal{EX}(\mathcal{M})$. Più formalmente, $N \in \mathcal{EX}(\mathcal{M})$ se e solo se $N \notin \mathcal{M}$ e ogni minore proprio di N è contenuto in $\mathcal{M}$. Gli elementi di $\mathcal{EX}(\mathcal{M})$ sono chiamati *minori esclusi* di $\mathcal{M}$.

Proposizione 2.3.5. *L'unico minore escluso per la classe delle matroidi uniformi* $\mathcal{U}$ *è* $U_{0,1} \oplus U_{1,1}$.

Dimostrazione. La matroide $U_{0,1} \oplus U_{1,1}$ non è uniforme poiché ha un indipendente con un elemento, ma non tutti gli insiemi da un elemento sono indipendenti. Inoltre si può facilmente vedere che ogni minore proprio di $U_{0,1} \oplus U_{1,1}$ è uniforme. Quindi $U_{0,1} \oplus U_{1,1}$ è un minore escluso di $\mathcal{U}$.
Supponiamo ora che N sia un minore escluso per $\mathcal{U}$. Dobbiamo mostrare che $N \cong U_{0,1} \oplus U_{1,1}$. Dato che N non è uniforme, esiste un intero k tale che N abbia sia insiemi indipendenti con k elementi sia insiemi dipendenti con altrettanti elementi. Prendiamo il minore di questi k e sia C un insieme dipendente con k elementi. Allora C è un circuito di N. Prendiamo un $e \in C$, allora $C - \{e\}$ è un indipendente con $k-1$ elementi. Dato che N possiede anche degli indipendenti con k elementi, allora per la proprietà (**I3**) uno di loro ha un elemento f tale che $(C - \{e\}) \cup \{f\}$ è un indipendente. Quindi $N/(C - \{e\})$ ha $\{e\}$ come circuito e $\{f\}$ come indipendente.

Dato che N è un minore escluso per $\mathcal{U}$, deduciamo che $N/(C - \{e\}) = N$ (dato che altrimenti $N/(C - \{e\})$ dovrebbe essere una matroide uniforme e invece non lo è) e quindi $C - \{e\}$ è vuoto. Se ora rimuoviamo da N tutti gli elementi eccetto e e f, abbiamo ancora una matroide per la quale $\{e\}$ è un circuito e $\{f\}$ è un indipendente. Il fatto che N sia un minore escluso implica che l'insieme sostegno di N sia $\{e, f\}$ e quindi possiamo concludere che $N = U_{0,1} \oplus U_{1,1}$. □

Non per tutte le classi di matroidi è semplice descrivere la categoria dei minori esclusi come per la classe delle matroidi uniformi: è difficile descriverne gli elementi e stabilire se sono in numero finito oppure no.
Un'osservazione generale che si può fare è che se $\mathcal{M}$ è una classe di matroidi chiusa per minori e per dualità, allora i duali dei minori esclusi per $\mathcal{M}$ sono a loro volta dei minori esclusi per $\mathcal{M}$.

Capitolo 3

Rappresentazioni lineari delle matroidi

Abbiamo visto come, a partire da una matrice a elementi in un campo F, è possibile trovare la matroide associata alla matrice. È lecito chiedersi ora se, data una matroide, è possibile trovarne una rappresentazione lineare. Studieremo anche la categoria dei minori esclusi per la classe delle matroidi binarie, ternarie e regolari.

3.1 Matroidi non rappresentabili

Osservazione 3.1.1. È innanzitutto interessante ricordare che esiste un'immersione di campi $GF(p) \hookrightarrow F$, dove F è un qualsiasi campo di caratteristica p. Questo significa che se una matroide è rappresentabile su $GF(p)$ allora è rappresentabile anche su un qualsiasi altro campo di caratteristica p. Non vale però il viceversa: se una matroide è rappresentabile su un campo qualsiasi di caratteristica p, non è detto che lo sia anche in $GF(p)$.

Consideriamo una matroide M con insieme sostegno E ed una sua base B. Se $e \in E - B$, allora $B \cup \{e\}$ contiene un circuito. Questo circuito è unico, lo chiamiamo *circuito fondamentale di e rispetto a B* e lo indichiamo con $C(e, B)$. Infatti se $C(e, B)$ non fosse unico, ci sarebbero due circuiti C_1

e C_2 che soddisfano queste caratteristiche. Per il terzo assioma della caratterizzazione delle matroidi tramite circuiti, poiché $e \in C_1 \cap C_2$, $(C_1 \cup C_2) - \{e\}$ deve contenere un circuito. Ma $(C_1 \cup C_2) - \{e\} \subseteq B$ e ciò è impossibile.
Ora supponiamo che M sia rappresentata su un campo F dalla matrice $[I_r|D]$ dove le prime r colonne $b_1, b_2, \ldots b_r$ di questa matrice corrispondono alla base B. Supponiamo che e sia una colonna di D e sia $C(e, B) = \{b_{i_1}, b_{i_2}, \ldots b_{i_k}, e\}$. Allora esiste una combinazione lineare delle colonne $b_{i_1}, b_{i_2}, \ldots b_{i_k}, e$ che dà il vettore nullo. Inoltre $C(e, B)$ è un insieme dipendente minimale, quindi tutti i coefficienti della combinazione lineare devono essere diversi da zero. Segue quindi che la colonna e ha componente j-esima diversa da zero se e solo se $j \in \{i_1, i_2, \ldots i_k\}$. Dunque i circuiti fondamentali di B determinano completamente gli elementi di D che sono uguali o diversi da zero. In particolare, se $F = GF(2)$ allora, dato che $GF(2)$ ha un solo elemento diverso da zero, i circuiti fondamentali di B determinano univocamente la matrice D. Quindi formalmente abbiamo la seguente Proposizione:

Proposizione 3.1.1. *Se M è una matroide binaria con insieme sostegno E e una base B, allora M è univocamente determinata da B e dall'insieme di circuiti $C(e, B)$ tali che $e \in E - B$.*

Con queste premesse è possibile ora studiare la rappresentabilità delle matroidi F_7 e F_7^-.

Proposizione 3.1.2. *Sia F un campo.*

- *F_7 è F-rappresentabile se e solo se la caratteristica di F è due.*
- *F_7^- è F-rappresentabile se e solo se la caratteristica di F è diversa da due.*

Dimostrazione. Sia $M \in \{F_7, F_7^-\}$ e sia M rappresentabile su un qualche campo F. Dato che sappiamo che M è rappresentata da A_7 su un qualche campo e considerando i circuiti fondamentali, sappiamo che una rappresentazione di M su F deve avere gli elementi uguali a zero e diversi da zero

nelle stesse posizioni degli elementi uguali e diversi da zero di A_7. Dunque possiamo assumere che M sia rappresentata su F dalla matrice

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

dove $*$ rappresenta un elemento di F diverso da zero e due distinti $*$ non sono necessariamente uguali. Moltiplicando ora le colonne di A' per elementi di F non nulli possiamo rendere il primo elemento di ogni colonna uguale a 1. Moltiplicando poi la seconda e la terza riga e la seconda, la terza e la sesta colonna per elementi non nulli di F, possiamo rendere tutti gli elementi della settima colonna uguali a 1 mantenendo il primo elemento diverso da zero di ciascuna colonna uguale a 1. Possiamo così assumere che

$$A' = \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & a & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & b & c & 1 \end{bmatrix} \end{array}$$

dove a, b e c sono elementi non nulli di F. Dato che M ha come circuiti $\{3,4,7\}, \{2,5,7\}$ e $\{1,6,7\}$ (sia che si tratti di F_7, sia che si tratti di F_7^-) allora segue che $a = b = c = 1$. Quindi $A' = A_7$. Possiamo concludere che se M è rappresentabile su F, allora è rappresentata dalla matrice A_7.

Consideriamo la matrice 3×3 che ha come colonne $4, 5$ e 6 e osserviamo che ha determinante -2. In F_7 l'insieme $\{4,5,6\}$ è un circuito mentre in F_7^- è una base. Ciò significa che se F_7 è F-rappresentabile, allora $-2 = 0$ in F e quindi F ha caratteristica 2. Allo stesso modo, se F_7^- è F-rappresentabile, allora $-2 \neq 0$ in F e quindi F dovrà avere caratteristica diversa da 2.

Per la sua definizione, F_7 è $GF(2)$-rappresentabile e quindi è rappresentabile su tutti i campi di caratteristica 2. Abbiamo quindi dimostrato il primo punto della Proposizione.

Per completare la dimostrazione, è necessario mostrare che $M[A_7]$ e F_7^- hanno lo stesso insieme di circuiti quando si osserva A_7 in un campo di caratteristica

diversa da 2. Sappiamo già che $M[A_7]$ e F_7^- condividono come circuiti tutti gli insiemi costituiti da tre punti collineari nella Figura 1.2 se guardiamo A_7 su $GF(3)$. Inoltre è facilmente verificabile che i minori di A_7 sono diversi da 0 in $GF(3)$ se e solo se sono diversi da 0 in $GF(p)$ ($p \neq 2$) dato che le sottomatrici quadrate di A_7 hanno tutte determinante uguale a $0, \pm 1, \pm 2$. Dunque anche il secondo punto della Proposizione è dimostrato. □

Una conseguenza immediata di questa Proposizione è che la matroide $F_7 \oplus F_7^-$ non è rappresentabile. Questa non è l'unica matroide non rappresentabile, e nemmeno la più piccola. È comunque interessante osservare che non tutte le matroidi sono rappresentabili.

3.2 Caratterizzazione delle matroidi binarie e ternarie

Lemma 3.2.1. *La matroide $U_{2,n}$ è rappresentabile su un campo F se e solo se F ha almeno $n-1$ elementi.*

Dimostrazione. Per definizione la matroide $U_{2,n}$ è rappresentabile su un campo F se e solo se è la matroide associata a una matrice $2 \times n$ a elementi in F tale che le colonne siano a due a due linearmente indipendenti. Possiamo quindi supporre che la prima colonna della matrice sia il vettore $(0,1)^T$ mentre le altre $n-1$ colonne siano vettori della forma $(1,*)^T$, dove $*$ rappresenta un elemento qualsiasi di F. Affinchè tutte le colonne siano a due a due linearmente indipendenti, è necessario che le $n-1$ colonne siano tra di loro diverse e che quindi ci siano in F almeno $n-1$ elementi. □

Questo significa che $U_{2,4}$ non è binaria, che $U_{2,5}$ non è né binaria né ternaria e così via.

Teorema 3.2.2. *Una matroide è binaria se e solo se non ha minori isomorfi a $U_{2,4}$.*

Riportiamo una dimostrazione che mostra le linee principali delle dimostrazioni della caratterizzazione di altre classi di matroidi.

Dimostrazione. Abbiamo visto, grazie al Lemma 3.2.1, che $U_{2,4}$ è un minore escluso per la classe delle matroidi binarie.
Sia M un arbitrario minore escluso per la classe delle matroidi binarie. Allora in M ogni insieme formato da uno o due elementi è un indipendente. Questo perché se fosse un circuito, togliendo l'elemento o gli elementi dal minore si dovrebbe trovare qualcosa di rappresentabile in $GF(2)$. Ma anche i circuiti di uno e due elementi sono rappresentabili in $GF(2)$, e quindi M non sarebbe un minore escluso. Inoltre, se M è un minore escluso, anche M^* lo è. Questo significa che M non ha nemmeno cocircuiti di uno e due elementi.
Se prendiamo X indipendente in M^*, allora esiste una base B di M^* tale che $X \subseteq B$. Ma se B è una base di M^*, allora $E - B$ è una base di M (E insieme sostegno di M). Questo significa che esiste una base di M disgiunta da X.
Consideriamo x e $y \in E$ indipendenti in M^*. Allora esiste una base di M disgiunta da $\{x, y\}$. Questo significa che il rango di M è uguale al rango di $M \setminus \{x, y\}$ ($r(M) = r(M \setminus \{x, y\})$). Inoltre $M \setminus \{x, y\}$ è binaria in quanto minore di M, sia $[I_r|D]$ la matrice che la rappresenta su $GF(2)$. Siccome $M \setminus x$ e $M \setminus y$ sono binarie, allora esistono due vettori v_y e v_x tali che $[I_r|D|v_y]$ e $[I_r|D|v_x]$ rappresentano rispettivamente $M \setminus x$ e $M \setminus y$ su $GF(2)$.
Sia ora M' la matroide rappresentata su $GF(2)$ da $[I_r|D|v_x|v_y]$. Allora $M \setminus x = M' \setminus x$ e $M \setminus y = M' \setminus y$. Dato che $M \neq M'$ allora esiste un insieme che è indipendente in una delle due matroidi e che è dipendente nell'altra. Sia Z un insieme minimale che gode di questa proprietà. Allora Z è indipendente in una tra M e M', chiamiamola M_I, e dipendente nell'altra, chiamiamola M_C. Siccome $M_I \setminus x = M_C \setminus x$ e $M_I \setminus y = M_C \setminus y$, abbiamo che $\{x, y\} \subseteq Z$. Mostriamo che se J è un insieme indipendente di M_I che contiene Z allora $J = \{x, y\}$.
Supponiamo per assurdo che $J \setminus \{x, y\}$ sia non vuoto. Questo insieme è indipendente in $M_I \setminus \{x, y\}$ e quindi anche in $M_C \setminus \{x, y\}$ (poiché sono uguali).

Contraendo $J\backslash\{x,y\}$ da M_I e M_C otteniamo le matroidi $N_I = M_I/(J\backslash\{x,y\})$ e $N_C = M_C/(J\backslash\{x,y\})$ con lo stesso rango. Poiché una tra M_I e M_C è binaria mentre l'altra è un minore escluso per le classe delle matroidi binarie, allora sia N_I che N_C sono binarie. Ovviamente $N_I \neq N_C$. Infatti $J\backslash\{x,y\}\cup\{x,y\} = J$ è indipendente in N_I dato che lo è in M_I per ipotesi, ed è dipendente in N_C poiché contiene Z che è dipendente in M_C .
Ma $N_I \setminus x = N_C \setminus x$ e $N_I \setminus y = N_C \setminus y$. Si ha che $N_I \setminus \{x,y\}$ è uguale a $N_C \setminus \{x,y\}$. Infatti

$$\begin{aligned} N_I \setminus \{x,y\} &= (M_I/(J \setminus \{x,y\})) \setminus \{x,y\} = \\ &= (M_I \setminus \{x,y\})/(J \setminus \{x,y\}) = \\ &= (M_C \setminus \{x,y\})/(J \setminus \{x,y\}) =. \\ &= (M_C/(J \setminus \{x,y\})) \setminus \{x,y\} = \\ &= N_C \setminus \{x,y\} \end{aligned}$$

In particolare $N_I \setminus \{x,y\}$ e $N_C \setminus \{x,y\}$ hanno lo stesso rango di N_I e N_C. Infatti

$$\begin{aligned} r(N_I \setminus \{x,y\}) &= r((M_I/(J \setminus \{x,y\})) \setminus \{x,y\}) = \\ &= r((M_I \setminus \{x,y\})/(J \setminus \{x,y\})) = \\ &= r(M_I \setminus \{x,y\}) - r(J \setminus \{x,y\}) = \\ &= r(M_I) - r(J \setminus \{x,y\}) = r(N_I) \end{aligned}$$

Analogamente $r(N_C \setminus \{x,y\}) = r(N_C)$.
N_I e N_C sono entrambe binarie, hanno lo stesso rango e $N_I \setminus \{x\} = N_C \setminus \{x\}$. È possibile quindi rappresentare $N_I \setminus \{x\} = N_C \setminus \{x\}$ in $GF(2)$ con una matrice $[I|A]$. Aggiungendo una colonna che rappresenti x alla matrice si trova la rappresentazione matriciale di N_I. Il vettore da aggiungere è determinato univocamente in $GF(2)$ e dunque la nuova matrice rappresenta anche N_C. Ciò significa che $N_I = N_C$. Poiché N_I e N_C non possono essere sia uguali che diversi, siamo giunti a una contraddizione e quindi $J = \{x,y\}$. Ciò significa che $Z = \{x,y\}$. Poiché Z è un indipendente di M_I, allora è contenuto in una sua base J. Ma abbiamo appena visto che $J = \{x,y\}$

quindi il rango di M_I è 2, così come il rango di M_C e quindi il rango di M. Inoltre sappiamo che M non ha circuiti formati da uno o due elementi, quindi significa che M è una matroide uniforme di rango due con almeno quattro elementi. Tutte le matroidi uniformi $U_{2,n}$ non sono binarie eccetto $U_{2,3}$ e M deve essere tale che tutti i suoi minori sono binari, quindi $M \cong U_{2,4}$. □

Proposizione 3.2.3. *F_7 è un minore escluso per la classe delle matroidi ternarie.*

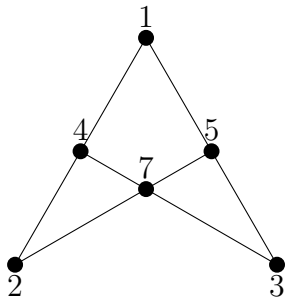

Figura 3.1: Sottrazione di un elemento a F_7

Dimostrazione. Sappiamo che F_7 non è rappresentabile su $GF(3)$, dobbiamo soltanto mostrare che i minori di F_7 sono ternari.
Consideriamo la sottrazione di un elemento a F_7: grazie alla simmetria della matroide di Fano si può facilmente vedere che la sottrazione di un elemento piuttosto che un altro dà luogo a minori di F_7 isomorfi. Il minore risultante può essere rappresentato dalla rappresentazione geometrica mostrata in Figura 3.1. Si osserva che questo minore è isomorfo al minore ottenuto da F_7^- sottraendo un elemento che non sia 7. Poiché F_7^- è ternario, anche i suoi minori lo sono, e quindi lo è anche la sottrazione di un qualsiasi elemento a F_7.
Prendiamo in esame invece il minore ottenuto da F_7 contraendo un suo elemento. Se prendiamo la rappresentazione lineare di F_7

$$A_7 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

contraendo un suo elemento qualsiasi si ottiene la matrice

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

I minori di questa matrice sono tutti $0, 1$ o -1 e quindi il minore che si ottiene contraendo un elemento qualsiasi di F_7 è rappresentabile su $GF(3)$. □

Teorema 3.2.4. *Una matroide è ternaria se e solo se non ha minori isomorfi a* $U_{2,5}, U_{3,5}, F_7$ *e* F_7^*.

È possibile mostrare in maniera analoga alla dimostrazione del Teorema 3.2.2 che i minori esclusi della categoria delle matroidi rappresentabili su $GF(3)$ o i loro duali hanno rango al massimo pari a 3 (si vedano i dettagli in [2]). Questo ci permette di cercare i minori esclusi di $GF(3)$ soltanto tra le matroidi di rango 3, trovando che questi sono $U_{2,5}, F_7$ e i loro duali.

3.3 Caratterizzazione delle matroidi regolari

Definizione 3.3.1. Sia A una matrice con ogni elemento uguale a $0, 1$ o -1. Diciamo che A è una *matrice totalmente unimodulare* se il determinante di ogni sottomatrice quadrata vale $0, 1$ o -1.

Le matrici totalmente unimodulari si possono osservare sia come matrici a elementi in $\mathbb{Z} \subseteq \mathbb{Q}$ sia come matrici a elementi in $\mathbb{Z}_p$ (nel caso in cui $p = 2$ i -1 vanno sostituiti con degli 1).
Consideriamo la mappa

$$\begin{array}{ccc} \mathbb{Z} & \leftarrow & M_n(\mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p & \leftarrow & M_n(\mathbb{Z}_p) \end{array}$$

dove $\mathbb{Z} \to \mathbb{Z}_p$ e $M(\mathbb{Z}) \to M(\mathbb{Z}_p)$ sono epimorfismi di anelli dove a ogni elemento di $\mathbb{Z}$ viene associata la classe di resto $\pmod p$ a cui appartiene e $M(\mathbb{Z}) \to \mathbb{Z}$ e $M(\mathbb{Z}_p) \to \mathbb{Z}_p$ sono funzioni che associano a ogni matrice il

suo determinante. Questo significa che prendere una matrice a elementi in $\mathbb{Z}$, calcolarne il determinante e poi passarlo al quoziente equivale a prendere la stessa matrice, passare al quoziente tutti i suoi elementi e calcolarne il determinante. In generale il discorso vale anche se al posto delle matrici quadrate consideriamo matrici $r \times n$ di rango massimo (supponiamo $r \leq n$):

$$\begin{array}{ccc} \mathbb{Z}^{\binom{n}{r}} & \leftarrow & M_{r,n}(\mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p^{\binom{n}{r}} & \leftarrow & M_{r,n}(\mathbb{Z}_p) \end{array},$$

in questo caso $M(\mathbb{Z}) \to \mathbb{Z}^{\binom{n}{r}}$ e $M(\mathbb{Z}_p) \to \mathbb{Z}_p^{\binom{n}{r}}$ associano a ogni matrice un vettore che ha come elementi i determinanti delle sottomatrici di dimensione massima.

Le matroidi associate alle matrici con minori massimi uguali a $0, 1$ o -1 in $\mathbb{Z}$ sono isomorfe alle matroidi rappresentate dalle stesse matrici viste su $\mathbb{Z}_p$, dato che i valori dei minori massimi non cambiano con il passaggio al quoziente. Le matrici che godono di questa proprietà sono le matrici totalmente unimodulari e dunque, per quanto appena osservato, le matroidi associate a tali matrici sono regolari.

Le matroidi rappresentate da matrici totalmente unimodulari sono un esempio interessante di matroidi regolari e, come vedremo, anche l'unico.

Proposizione 3.3.1. *Le sottomatrici quadrate di una matrice B sono in corrispondenza biunivoca con le sottomatrici quadrate di dimensione massima della matrice $[B|I]$ e conservano il determinante a meno del segno.*

Dimostrazione. Consideriamo la sottomatrice quadrata C che si ottiene da B prendendo le righe $i_1 < i_2 < \cdots < i_k$ e le colonne $j_1 < j_2 < \cdots < j_k$. A C associamo la sottomatrice di $[B|I]$ formata dalle colonne di I eccetto la i_1-esima, la i_2-esima, ..., la i_k-esima, a cui sostituiamo le colonne $j_1, j_2, \ldots j_k$ di B. Otteniamo così una sottomatrice di $[B|I]$ di dimensione massima con lo stesso determinante di C a meno del segno.

Viceversa sia C' una sottomatrice quadrata di dimensione massima di $[B|I]$.

Allora avrà come colonne alcuni vettori della base canonica, supponiamo siano tutti eccetto $e_{i_1}, e_{i_2}, \dots e_{i_k}$, e k colonne di B. Allora associamo a C' la sottomatrice quadrata di B formata dalle k colonne presenti in C' e dalle righe $i_1, i_2, \dots i_k$. Le due matrici avranno lo stesso determinante a meno del segno. □

Lemma 3.3.2. *Ogni matrice quadrata B con elementi in $\{0, 1, -1\} \subseteq \mathbb{Z}$ e tale che $|det(B)| > 2$ ha almeno una sottomatrice con determinante ± 2.*

Dimostrazione. Sia B una matrice $n \times n$ con elementi in $\{0, 1, -1\}$ e tale che $|\det(B)| > 2$, e consideriamo la matrice $C = [B|I]$. Sommando o sottraendo righe ad altre righe ed eventualmente moltiplicando colonne per -1, è possibile ottenere da C una matrice C' tale che

1. C' sia una matrice con elementi in $\{0, 1, -1\}$;
2. C' contenga tra le sue colonne gli n vettori della base canonica;
3. C' contenga tra le prime n colonne quanti più vettori della base canonica possibili.

Indichiamo con k il numero di vettori della base canonica presenti tra le prime n colonne. Si può supporre, per semplificare l'esposizione, che

$$C' = \left[\begin{array}{c|c|c} I_k & & 0 \\ & B' & \\ 0 & & I_{n-k} \end{array}\right]$$

per una determinata matrice B' $n \times n$ (il caso generale segue su linee analoghe). Sappiamo che le prime n colonne di C, e quindi anche di C', formano una matrice con determinante diverso da 0. Quindi esiste un elemento diverso da 0 in posizione $(i, k+1)$ in C' con $k+1 \leq i \leq n$. Senza ledere di generalità possiamo supporre che questo elemento sia 1. Per la condizione 3 non è possibile trasformare la colonna j-esima in un vettore della base canonica tramite operazioni elementari tra le righe senza violare la condizione 1. Quindi esiste una coppia (i', j') tale che la sottomatrice 2×2 che ha come

indici di riga i e i' e come indici di colonna j e j' ha la forma $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ oppure $\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$ a meno dei segni della seconda colonna. Quindi la sottomatrice di C' formata dalle colonne j, j' e i vettori colonna della base canonica eccetto l'i-esimo e l'i'-esimo ha determinante ± 2. Operando come nella Proposizione 3.3.1 troviamo un minore di ordine n di C' che vale ± 2. Dato che le operazioni effettuate per passare da C a C' preservano i minori di dimensione massima, esiste un minore di dimensione massima di C che vale ± 2. Dunque, per la Proposizione 3.3.1, B ha una sottomatrice quadrata con determinante ± 2. □

Questo significa che una matrice non totalmente unimodulare minimale ha determinante uguale a ± 2.

Vale il seguente Teorema, enunciato da Tutte nel 1958 e così riformulato comunemente.

Teorema 3.3.3 (**Tutte**). *Le seguenti affermazioni sono equivalenti per la matroide M.*

1. *M è regolare.*
2. *M è sia binaria che ternaria.*
3. *M è rappresentabile su $\mathbb{R}$ da una matrice totalmente unimodulare.*
4. *M non ha minori isomorfi a $U_{2,4}, F_7$ o F_7^*.*

Dimostrazione. $1 \Rightarrow 2$ Ovvio.

$2 \Leftrightarrow 4$ Segue dai Teoremi 3.2.2 e 3.2.4. Infatti $U_{2,4}$ è un minore di $U_{2,5}$ (si ottiene tramite la sottrazione di un elemento) e di $U_{3,5}$ (si ottiene contraendo un elemento).

$3 \Rightarrow 1$ Ovvio.

$2 \Rightarrow 3$ Scegliamo una rappresentazione $[I|A]$ di M su $GF(3)$, e guardiamo A come una matrice reale con elementi $0, 1$ e -1. Poiché M è binaria segue che $[I|A]$ rappresenta M anche su $GF(2)$ (sostituendo gli 1 con dei -1); e poiché c'è una biezione tra le basi di M e le sottomatrici non singolari di A, segue che per ogni sottomatrice quadrata B di A

$$\det(B) \equiv 0 (\text{mod } 2) \Leftrightarrow \det(B) \equiv 0 (\text{mod } 3).$$

Dato che per il Lemma 3.3.2 sappiamo che una matrice non totalmente unimodulare minimale ha determinante ± 2, segue che A è totalmente unimodulare (altrimenti una matrice non totalmente unimodulare avrebbe determinante uguale a 0 in $GF(2)$ e diverso da 0 in $GF(3)$).

□

In seguito a questo importante Teorema e alla caratterizzazione delle matroidi binarie e ternarie, nel 1970 Gian Carlo Rota ipotizzò la seguente congettura:

Congettura 3.3.4 (Rota)**.** *Per ogni campo finito $GF(q)$, la collezione dei minori esclusi per la classe di matroidi rappresentabili su $GF(q)$ è finita.*

Questa congettura è stata il punto focale della ricerca sulla teoria delle matroidi e, dopo anni di lavoro, è stata dimostrata da Geelen, Gerards e Whittle nel 2013.

La Congettura di Rota non vale per i campi di caratteristica 0. Infatti vale la seguente Proposizione:

Proposizione 3.3.5. *Sia L_p la matroide vettoriale rappresentata dalla matrice $[I_{p+1}|J_{p+1}]$ su $GF(p)$ con J_k matrice $k \times k$ uguale a* $\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}$. *Sia F un campo di caratteristica 0. Allora per ogni p primo, L_p è un minore escluso per la rappresentabilità su F.*

Questo significa che F ha infiniti minori esclusi.

Dimostrazione. Verifichiamo l'enunciato per $p = 2$. La matrice che rappresenta L_2 è

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

Si può osservare che su $GF(2)$ $C = \{(0,1,1)^T, (1,0,1)^T, (1,1,0)^T\}$ è un circuito dato che $\det J_3 = 0$ in tutti e soli i campi di caratteristica 2. Questo significa però che C non può essere un circuito in F e che dunque L_2 non è rappresentabile su F. Inoltre tutti i minori di questa matrice valgono $0, \pm 1$ e dunque sono rappresentabili su F.
In generale considerando $J_{p+1} - \lambda I$ si ottiene la matrice

$$\begin{bmatrix} -\lambda & 1 & \cdots & 1 \\ 1 & -\lambda & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & -\lambda \end{bmatrix}.$$

In questa matrice l'autovalore -1 ha molteplicità p, mentre l'autovalore p ha molteplicità 1. Dunque il polinomio caratteristico è $(\lambda + 1)^p(\lambda - p)$. Da qui segue che $\det J_{p+1} = \det(J_{p+1} - 0I) = (0 + 1)^p(0 - p)$ che è uguale a 0 se e solo se il campo ha caratteristica p.
Non riportiamo qui la dimostrazione del fatto che i minori di L_p siano rappresentabili in F né quella del fatto che tutte le matrici che rappresentano L_p non siano rappresentabili su F. □

Capitolo 4

Commento al Teorema di Tutte

La caratterizzazione delle matroidi regolari presentata dal Teorema 3.3.3 non è esattamente quella enunciata da Tutte. In realtà egli diede anche una definizione diversa di matroidi regolari, ma che, grazie al suo Teorema, sappiamo essere equivalente a quella fornita in questa tesi, la stessa usata da Oxley. Vediamo ora la definizione di Tutte di matroide regolare e l'enunciato originale del Teorema, utilizzando la sua notazione e la sua terminologia. Vediamo inoltre come il Teorema ha trovato una dimostrazione semplificata grazie al lavoro di Schrijver e Gerards.

4.1 Catene e gruppi di catene

Tutte definì il concetto di matroide regolare nella seguente maniera.

Sia $R = \mathbb{Z}$ oppure $R = GF(p)$, con p primo. Se E è un insieme finito, definiamo *catena* di E su R una funzione $f : E \to R$. Sia $a \in E$, chiamiamo $f(a)$ *coefficiente* di a in f. L'insieme di tutti gli $a \in E$ tali che $f(a) \neq 0$ è il supporto $|f|$ di f.
La somma $f + g$ di due catene f e g di E su R è una catena di E su R definita nel seguente modo:

$$(f + g)(a) = f(a) + g(a) \qquad \forall a \in E.$$

Con questa operazione, le catene di E su R formano un gruppo abeliano additivo, che indichiamo con $A(E, R)$. Il suo elemento neutro è la catena nulla $f(a) = 0\ \forall a \in E$, e l'opposto di una catena f si ottiene moltiplicando ogni coefficiente di f per -1. Chiamiamo *gruppo di catene* di E su R ogni sottogruppo di $A(E, R)$.

Una catena f di N è *elementare* se non è la catena nulla e se non esiste una catena $g \in N$ tale che $|g|$ sia un sottoinsieme proprio di $|f|$. Se $R = \mathbb{Z}$, diciamo che f è una catena *primitiva* di N se è una catena elementare i cui coefficienti assumono solo i valori $0, 1$ e -1.
Chiamiamo N *binario* se $R = GF(2)$, lo chiamiamo *regolare* se $R = \mathbb{Z}$ e per ogni catena elementare $f \in N$ esiste una catena primitiva $g \in N$ tale che $|f| = |g|$.

Sia N un gruppo di catene di E su R, e siano $f_1, f_2, \dots f_k$ catene di N. Diciamo che sono *linearmente dipendenti* (su R) se esistono degli elementi $\lambda_1, \lambda_2, \dots \lambda_k$ di R non tutti nulli tali che

$$\sum_{i=1}^{k} \lambda_i f_i = 0.$$

Il *rango* di N è il numero massimo di catene f di N che non sono linearmente dipendenti, e si indica con $r(N)$.

Consideriamo un insieme $B = \{f_1, f_2, \dots f_r\}$ di catene di N linearmente indipendenti, con $r = r(N)$. Allora ogni altra catena di N è dipendente in B, cioè per ogni $f \in N$ esiste $\lambda \in R$ tale che $\lambda \neq 0$ e λf è una somma di multipli degli elementi di B per elementi di R. Se è possibile prendere $\lambda = 1$ per ogni f diciamo che B è una *base* di N. Ciò è sempre possibile quando R è un campo. Se $E = \{e_1, e_2, \dots e_n\}$, è possibile rappresentare B tramite una matrice $K = (k_{i,j})$ con r righe e n colonne, dove $k_{i,j}$ è il coefficiente di e_j in f_i. Se B è una base di N, chiamiamo K una *matrice rappresentativa* di N. Se invece sappiamo solo che gli r elementi di B sono linearmente indipendenti

diciamo che K è una *matrice rappresentativa debole* di N.
Per ogni catena di $f \in N$ si ha il vettore riga

$$(f(e_1), f(e_2), \ldots, f(e_n)),$$

e lo chiamiamo *vettore rappresentativo* di f. Dunque le righe di K sono i vettori rappresentativi delle catene f_i. Ovviamente ogni combinazione lineare di vettori rappresentativi è il vettore rappresentativo della corrispondente combinazione lineare di catene. Per i risultati standard dell'algebra lineare, la proprietà di essere matrice rappresentativa di N è invariante per le "operazioni elementari", cioè

1. permutazione di righe,
2. aggiunta a una riga di un'altra riga moltiplicata per un elemento di R,
3. moltiplicazione di una riga per -1.

La proprietà di essere una matrice rappresentativa debole è invariante sotto l'operazione di moltiplicare le righe per un elemento di R diverso da 0.
Sia K una matrice rappresentativa debole di N, e sia S un qualunque sottoinsieme di E. Definiamo $K(S)$ come la sottomatrice di K formata dalle colonne che corrispondono agli elementi di S. Se la cardinalità di S è uguale a r, allora può succedere che $K(S)$ sia una *matrice diagonale* che ha gli elementi lungo la diagonale non nulli e tutti gli altri uguali a 0. Possiamo allora dire che K è in *forma diagonale* rispetto a S.

Proposizione 4.1.1. *Sia K una matrice rappresentativa debole di un gruppo di catene N, e sia $S \subseteq E$ con cardinalità uguale a $r = r(N)$. Allora esiste una matrice rappresentativa debole di N, chiamiamola J, che è in forma diagonale rispetto a S se e solo se $K(S)$ è non singolare.*

Proposizione 4.1.2. *Sia K una matrice rappresentativa debole di N, diagonale rispetto a qualche $S \subseteq E$. Sia s_i l'i-esimo elemento di S e sia f_i la catena di N rappresentata dalla i-esima riga di K. Allora f_i è elementare. Inoltre, se f è una qualche catena di N tale che $|f| \cap S = \{s_i\}$, allora $|f| = |f_i|$.*

Proposizione 4.1.3. *Sia f una catena elementare di N. Allora esiste una matrice rappresentativa debole K di N, diagonale rispetto a un qualche $S \subseteq E$ tale che una qualche riga di K sia il vettore rappresentativo di f.*

Sia K una matrice rappresentativa debole di N diagonale rispetto a un qualche $S \subseteq E$. Può succedere che $K(S)$ sia la matrice identità. In questo caso K è una vera matrice rappresentativa di N dato che un'arbitraria catena di N può essere scritta come

$$f = \sum_{i=1}^{r} f(s_i) f_i$$

dove s_i è l'i-esimo elemento di S, e f_i è la catena rappresentata dalla i-esima riga di K. In questo caso chiamiamo K una *matrice rappresentativa standard* di N associata a S.
Se R è un campo, K può sempre essere ridotta in forma standard rispetto a S moltiplicando le righe per elementi appropriati di R.

Una simile riduzione può essere fatta se N è regolare: ogni riga di K rappresenta un multiplo intero di una catena primitiva, per la Proposizione 4.1.2, e dobbiamo solo sostituire ogni riga con il vettore rappresentativo della catena primitiva corrispondente. Questo si può fare dividendo la riga per il suo elemento massimo. Mettendo insieme questa osservazione con la Proposizione 4.1.1, otteniamo la seguente Proposizione.

Proposizione 4.1.4. *Sia K una qualche matrice rappresentativa debole di un gruppo di catene regolare N di E. Sia S un sottoinsieme di E con r elementi, dove $r = r(N)$. Allora esiste una matrice rappresentativa standard di N associata a S se e solo se $K(S)$ è non singolare.*

Da qui in avanti N indicherà un gruppo di catene a elementi interi.

Teorema 4.1.5. *Sia N un gruppo di catene regolare di un insieme E. Sia K una matrice rappresentativa standard di N associata a un sottoinsieme S di E con r elementi. Sia T un qualsiasi sottoinsieme di E con la stessa cardinalità di S. Allora il determinante di $K(T)$ vale 1, 0 o -1.*

Dimostrazione. Supponiamo che $\det K(T) \neq 0$. Esiste allora una matrice rappresentativa standard K_1 associata a T per la Proposizione 4.1.4. Poiché le righe di K_1 sono combinazioni lineari di quelle di K esiste una matrice quadrata A a elementi interi tale che $AK = K_1$. Ma quindi $AK(T) = K_1(T)$. Passando ai determinanti abbiamo

$$\det A \cdot \det K(T) = 1$$

dato che $K_1(T)$ è la matrice identità. Dato che A e $K(T)$ sono matrici a elementi interi, segue che $\det K(T) = \pm 1$. □

Corollario 4.1.6. *I determinanti delle sottomatrici di $K(E - S)$ valgono* 1, 0 *o* -1.

Unendo i risultati del Teorema e del Corollario, possiamo dire che K è totalmente unimodulare.

Teorema 4.1.7. *Sia K una matrice rappresentativa debole di un gruppo di catene N, di rango r. Supponiamo che ogni sottomatrice $r \times r$ di K abbia determinante uguale a* $1, 0$ *o* -1. *Allora N è regolare e K è una vera matrice rappresentativa di N.*

Dimostrazione. Sia f una catena elementare di N. Per la Proposizione 4.1.3 esiste una matrice rappresentativa debole J di N diagonale rispetto a qualche $S \subseteq E$ tale che una qualche riga di J rappresenti f. Si ha che $\det K(S) = \pm 1$ per la Proposizione 4.1.1 e per le nostre ipotesi. Quindi $[K(S)]^{-1}$ è una matrice a elementi interi. Moltiplicando K per $[K(S)]^{-1}$ otteniamo una matrice rappresentativa standard K_1 di N associata a S, con la proprietà che $\det K_1(T) = 1, -1$ o 0 se la cardinalità di T è uguale a r. Una riga di K_1, diciamo la i-esima, rappresenta una catena g di N tale che $|g| = |f|$ per la Proposizione 4.1.2. Consideriamo un qualche $b \in |g| - S$. Sia S' l'insieme che deriva da S rimuovendo l'elemento di $|g| \cap S$ e aggiungendo b. Allora la cardinalità di S' è uguale a r, e quindi $\det K(S') = \pm 1$ o 0. Ma $\det K(S') = \pm g(b)$, per un'espansione per colonne di $\det K(S)$. Deduciamo

che i coefficienti di g sono ristretti ai valori $1, -1$ e 0. Quindi g è una catena primitiva e f deve essere un multiplo intero (per $f(b)g(b)$) di g. Segue che N è regolare e che K_1 è una matrice rappresentativa standard di N. Quindi ogni vettore rappresentativo delle catene di N è una combinazione lineare con multipli interi delle righe di K_1, e quindi delle righe di K. Di conseguenza K è una matrice rappresentativa di N. □

Teorema 4.1.8. *Sia K una matrice rappresentativa standard, associata a qualche $S \subseteq E$, di un gruppo di catene N di E. Supponiamo che $K(E-S)$ sia totalmente unimodulare. Allora N è regolare.*

Dimostrazione. Sia T un qualche sottoinsieme di E con cardinalità $r = r(N)$. Se $T = S$ abbiamo $\det K(T) = 1$. Se $T \neq S$ sia A la sottomatrice quadrata di $K(E-S)$ definita dall'intersezione delle colonne di $K(T)$ con le righe di K che non hanno degli 1 in $K(T \cap S)$. Allora $\det K(T) = \pm \det A$, per un'espansione per colonne di $\det K(T)$. In ogni caso abbiamo che $\det K(T) = 1, -1$ o 0 per le nostre ipotesi. Dunque N è regolare per il Teorema precedente. □

Considerando ora questi ultimi enunciati è possibile affermare che

Teorema 4.1.9. *Sia N un gruppo di catene di un insieme E su $\mathbb{Z}$. Allora N è regolare se e solo se esiste una matrice rappresentativa di N totalmente unimodulare.*

Sia N un qualsiasi gruppo di catene di E su R, e sia N^* la classe di tutte le catene g tali che

$$\sum_{a \in E} f(a)g(a) = 0$$

per ogni $f \in N$. Allora N^* è un sottogruppo di E su R e lo chiamiamo gruppo di catene *duale* di N.
Consideriamo ora una matrice rappresentativa standard K, rispetto a qualche $S \subseteq E$, di un guppo di catene regolare N di E. Supponiamo che $r(N) = r$ e che la cardinalità di E sia n. Costruiamo una matrice K^* $(n-r) \times n$ nel seguente modo: le colonne corrispondenti a $E - S$ formano una matrice

identità, e la sottomatrice complementare, formata dalle colonne rimanenti di K^*, è l'opposto della trasposta di $K(E-S)$. È facile verificare che ogni riga di K^* è ortogonale a ogni riga di K, e quindi rappresenta una catena di N^*. D'altra parte, sia f una catena di N^*. Aggiungendo ad f multipli interi delle catene di N^* rappresentate dalle righe di K^* possiamo ottenere una catena g di N^* tale che $|g| \subseteq S$. Ma allora $g = 0$, poiché è ortogonale alle catene rappresentate dalle righe di N. Deduciamo quindi che K^* è una matrice rappresentativa standard di N^* associata a $E-S$. Grazie all'ultimo Teorema possiamo affermare che

Teorema 4.1.10. *Se N è un gruppo di catene regolare di E, allora N^* è un gruppo di catene regolare e $r(N) + r(N^*) = n$, dove n è la cardinalità di E.*

Teorema 4.1.11. *Se N è un gruppo di catene regolari, allora $(N^*)^* = N$.*

Indichiamo con $M(N)$ la classe dei supporti delle catene elementari di N. È facile mostrare che questa è la collezione di circuiti di una matroide su E, la si chiama *matroide di N*. Diciamo che una matroide è *regolare* se è la matroide di un gruppo di catene regolare.

4.2 Il Teorema di Tutte

L'enunciato del Teorema originale è il seguente:

Teorema 4.2.1. *Una matroide è regolare se e solo se è binaria e non ha F_7 e F_7^* come minori.*

Confrontiamo ora l'enunciato comune del Teorema di Tutte (Teorema 3.3.3) e l'enunciato originale, vogliamo verificare che l'implicazione dell'enunciato originale di Tutte *se una matroide binaria non ha F_7 e F_7^* come minori, allora è regolare* è equivalente all'implicazione *se una matroide M non ha minori isomorfi a F_7, F_7^* e $U_{2,4}$ allora M è rappresentabile tramite una matrice totalmente unimodulare*. Questo, per il Teorema 3.2.2, è equivalente a dimostrare che *una matroide è regolare (nel senso di Tutte) se e solo se è rappresentabile tramite una matrice totalmente unimodulare.*

Dimostrazione. Sia $M = M[A]$ una matroide vettoriale con A matrice totalmente unimodulare. Allora le righe di A sono una base di un gruppo di catene regolare P, di cui consideriamo il duale P^* anch'esso regolare per il Teorema 4.1.10. Siano $a_1, \dots a_n$ le colonne di A e sia $x \in P^*, x = (x_1, \dots, x_n)$, allora la combinazione lineare $x_1a_1 + \cdots + x_na_n$ è uguale al vettore nullo per la definizione di duale. Ciò significa che le catene di P^* descrivono le relazioni di dipendenza tra le colonne di A. In particolare, il supporto delle catene elementari di P^* individua i circuiti formati dalle colonne di A. Quindi $M(P^*)$ è la matroide dei circuiti di A, mentre $M[A]$ è la matroide degli indipendenti della stessa matrice. Dunque le due matroidi coincidono.
Viceversa sia $M = M(N)$ una matroide regolare con N gruppo di catene regolare, vogliamo dimostrare che $M = M[A]$ con A matrice totalmente unimodulare. Per il Teorema 4.1.10 sappiamo che se N è regolare, allora anche N^* lo è. Dunque per il Teorema 4.1.9 N^* ha una matrice rappresentativa totalmente unimodulare, sia questa A. Chiamiamo $a_1, \dots a_n$ le colonne di A. Se $x \in N, x = (x_1, \dots, x_n)$, allora la combinazione lineare $x_1a_1 + \dots x_na_n$ è uguale al vettore nullo. Ciò significa che ogni catena di N descrive una relazione di dipendenza tra le colonne di A. Dato che per il Teorema 4.1.11 sappiamo che $(N^*)^* = N$, allora le catene di N descrivono la totalità di queste relazioni di dipendenza. Ciò significa che il supporto delle catene elementari di N individua tutti e soli i circuiti della matroide vettoriale $M[A]$. Dunque $M(N) = M[A]$. □

4.3 Un enunciato equivalente

La dimostrazione che diede Tutte del suo Teorema è alquanto articolata. Gerards diede una dimostrazione piuttosto semplice del seguente enunciato (si veda [1]), che Schrijver aveva dimostrato essere equivalente al Teorema.

Teorema 4.3.1. *Sia A una matrice con elementi in $\{0, 1\}$. Allora le seguenti condizioni sono equivalenti:*

1. *A ha una segnatura totalmente unimodulare;*

2. A non può essere trasformata in

$$M(F_7) = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

applicando le seguenti operazioni:

- *rimozione di righe o colonne;*
- *permutazione di righe o colonne;*
- *trasposizione della matrice;*
- *pivoting su* $GF(2)$.

L'operazione di *segnatura* di una matrice A a elementi in $\{0, 1\}$ si effettua sostituendo alcuni 1 con dei -1.
L'operazione di *pivoting* di una matrice A su un elemento ε si effettua sostituendo la matrice

$$A = \begin{bmatrix} \varepsilon & y^T \\ x & D \end{bmatrix} \text{ con la matrice } B = \begin{bmatrix} -\varepsilon^{-1} & \varepsilon^{-1} y^T \\ \varepsilon^{-1} x & D - \varepsilon^{-1} x y^T \end{bmatrix}.$$

Si può mostrare che se la matrice $[I|A]$ è rappresentazione di una matroide, allora anche la matrice $[I|B]$ lo è. Infatti è possibile passare da una matrice a un'altra tramite operazioni descritte nella Proposizione 1.3.1.

Dimostrazione dell'equivalenza tra il Teorema 4.2.1 e il Teorema 4.3.1 . Sapendo che la rappresentazione della matroide di Fano è

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \text{ mentre quella della sua duale è } \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

è sufficiente dimostrare che *per qualsiasi matrice A a elementi in $\{0, 1\}$ la matroide binaria M rappresentata da $[I|A]$ non ha minori isomorfi alla matroide di Fano o alla sua duale se e solo se A non può essere trasformata in*

$M(F_7)$ o nella sua trasposta tramite una successione delle operazioni descritte nel Teorema 4.3.1.

Innanzitutto supponiamo che A possa essere trasformata in $M(F_7)$ o in $M(F_7)^T$. Rimuovere la i-esima riga di A corrisponde a contrarre la i-esima colonna di M rappresentata dalla matrice $[I|A]$. Poiché la matroide non cambia facendo un'operazione di pivoting su A (eccetto che per l'ordine dei suoi elementi nella matrice che la rappresenta), segue che M ha minori isomorfi alla matroide di Fano o alla sua duale.

Viceversa, supponiamo che $M = (E, \mathcal{I})$ abbia un minore isomorfo alla matroide di Fano o alla sua duale. Questo minore si ottiene contraendo un certo $E_1 \subseteq E$ e rimuovendo un certo $E_2 \subseteq E$, e la collezione dei suoi indipendenti è $\mathcal{I}' = \{E' \subseteq E \setminus (E_1 \cup E_2) :$ le colonne di E' sono linearmente indipendenti modulo $\langle E_1 \rangle\}$, dove $\langle E_1 \rangle$ è il sottospazio vettoriale generato da E_1. Possiamo ora assumere che le colonne in E_1 sono linearmente indipendenti e che $\langle E \rangle = \langle E \setminus E_2 \rangle$. Tramite pivoting, possiamo assumere che E_1 corrisponda a alcune colonne di I nella rappresentazione $[I|A]$. Allora contraendo E_1 e sottraendo E_2 si ottiene una matroide binaria la cui rappresentazione è $[I|A']$, dove A' deriva da A rimuovendo le colonne corrispondenti a E_2 e rimuovendo le righe di A determinate dai vettori di E_1. Allora la matroide binaria rappresentata da $[I|A']$ è isomorfa alla matroide di Fano o alla sua duale. Quindi I deve avere ordine 3 o 4, e A' deve essere una matrice 3×4 o 4×3. Dunque A' deve essere o $M(F_7)$ o la sua trasposta, e l'abbiamo ottenuta da A effettuando operazioni di permutazione e rimozione di righe e colonne. □

Conclusioni

Con questa tesi si è voluto introdurre il lettore alla teoria delle matroidi, dando alcune nozioni generali e sviluppando il discorso riguardo alla rappresentabilità delle matroidi, con particolare attenzione alla caratterizzazione delle matroidi regolari.
Questi sono soltanto alcuni dei numerosi aspetti che riguardano questo affascinante ramo della matematica. Un aspetto particolarmente interessante, e che in questa tesi non è stato debitamente sviluppato, riguarda i numerosi collegamenti tra matroidi e grafi. Un'idea dell'importanza di questo legame è suggerita da un'affermazione di W. T. Tutte: "Se un teorema riguardo ai grafi può essere espresso soltanto in termini di archi e circuiti, allora probabilmente semplifica un teorema più generale riguardo le matroidi".
Inoltre la teoria delle matroidi, ed in particolare lo studio delle matroidi regolari, ha contribuito in maniera significativa allo sviluppo dell'ottimizzazione combinatoria e alla risoluzione di problemi di programmazione lineare.
Si conclude evidendenziando che le matroidi non presentano collegamenti soltanto con rami teorici della matematica, ma anche con discipline applicative come l'ingegneria strutturale.

Appendice A

Nozioni preliminari

Vogliamo ricordare le prime nozioni di algebra lineare, teoria dei grafi e teoria dei campi necessarie per comprendere gli argomenti trattati in questa tesi.

A.1 Algebra lineare

Sia $v_1, \dots v_n$ una sequenza di vettori in uno spazio vettoriale V su un campo K. Allora le seguenti affermazioni sono equivalenti:

- l'unica combinazione lineare dei vettori che dà come risultato il vettore nullo è quella a coefficienti tutti nulli;
- nessuno dei vettori può essere scritto come combinazione lineare degli altri (se $n = 1$, v_1 deve essere diverso dal vettore nullo).

Se una sequenza di vettori soddisfa una (e quindi entrambe) di queste condizioni, si dice che è *linearmente indipendente*. Se non è linearmente indipendente, si dice che è *linearmente dipendente*.

Si può mostrare che tutte le sottosequenze linearmente indipendenti massimali di una sequenza di vettori sono formate dallo stesso numero di vettori. Tale numero si dice *rango* della sequenza di vettori.

Sia K un campo e sia n un intero positivo fissato. Si identifichi $M_n(K)$ con $K^n \times \cdots \times K^n$, associando a ciascuna matrice A $n \times n$ su K la sequenza delle sue n colonne. Si può dimostrare che esiste una e una sola funzione multilineare

$$\det_n : M_n(K) \cong K^n \times \cdots \times K^n \to K$$

tale che: (**1**) se A è una matrice con due colonne uguali, $\det_n A = 0$; (**2**) $\det_n I = 1$, dove I è la matrice identità. Tale funzione è chiamata *determinante*. Inoltre si può provare che $\det_n A = \det_n A^T$.

Il determinante di una matrice $A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$ a elementi in un campo K si può definire equivalentemente nel seguente modo:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot \cdots \cdot a_{n,\sigma(n)}$$

dove S_n è il gruppo simmetrico su n e $\operatorname{sgn}(\sigma)$ è il segno della permutazione σ.
Dalla definizione del determinante segue una descrizione precisa di come le operazioni elementari effettuabili sulle righe e sulle colonne modificano il suo valore.

Si prova che se A è una matrice quadrata, allora le righe di A sono linearmente dipendenti se e solo se le colonne di A sono linearmente dipendenti se e solo se $\det A = 0$.

Sia A una matrice $m \times n$. Un *minore* di ordine k di A è il determinante di una sottomatrice $k \times k$ di A.
Si può dimostrare che il rango della sequenza delle righe di una matrice A è uguale al rango della sequenza delle colonne di A che è a sua volta uguale all'ordine dei minori massimali non nulli di A. Tale valore si chiama *rango* della matrice A, e si indica con $r(A)$.

A.2 Teoria dei grafi

Definizione A.2.1. Un *grafo* G è una coppia (V, E) di insiemi legati da una relazione di incidenza tale che ogni elemento di E è incidente ad almeno un elemento e a non più di due elementi di V. Gli elementi di V si chiamano *vertici* o *nodi*, mentre quelli di E si chiamano *archi* o *lati*.

Un *sottografo* G' di G è un grafo (V', E') tale che $V' \subseteq V$ e $E' \subseteq E$.

Un *cammino* C di G è una sequenza $v_0 e_1 v_1 e_2 \dots v_{k-1} e_k v_k$ tale che $v_0, v_1, \dots v_k$ siano vertici e $e_1, e_2, \dots e_k$ siano lati, e ogni vertice o lato della sequenza, eccetto v_k sia incidente con il suo successore nella sequenza.
Un cammino C in cui i vertici $v_0, v_1, \dots v_k$ sono distinti, e quindi anche i lati $e_1, e_2, \dots e_k$, si chiama *cammino semplice*. Gli *estremi* del cammino sono v_0 e v_k, e si dice che C va da v_0 a v_k.
Un *ciclo* di G è un cammino semplice in cui il primo e l'ultimo vertice coincidono. Un ciclo con un solo lato e un solo vertice si chiama *cappio*. Un ciclo con un numero di lati ≥ 2 può anche essere visto come un grafo connesso dove su ogni vertice insistono esattamente due lati.

Un grafo si dice che è *connesso* se per ogni coppia di vertici $v, v' \in V$ esiste un cammino da v a v'. Una *componente connessa* di un grafo è un sottografo connesso massimale. Dunque un grafo è connesso se e solo se ha una sola componente connessa.

Proposizione A.2.1. *Sia T un grafo. Allora le seguenti proprietà per T sono equivalenti:*

1. *è connesso e senza cicli;*
2. *esiste un solo cammino per ogni coppia di vertici;*
3. *è aciclico, ma se si aggiunge un lato per unire due vertici si forma un ciclo;*

4. è connesso, ma se si toglie un qualsiasi lato si perde la connessione.

Se un grafo soddisfa le proprietà elencate nella Proposizione A.2.1 si chiama *albero*. Un'unione disgiunta di alberi si chiama *foresta*.
Si può facilmente verificare che se un albero ha n lati, allora il numero dei suoi vertici è $n+1$. Analogamente, se una foresta ha m lati, allora il numero dei suoi vertici è $m+k$, dove k è il numero di alberi disgiunti da cui è formata.

Siano $G = (V, E)$ e $G' = (V', E')$ due grafi. Sia f un'applicazione iniettiva da V a V', sia g un'applicazione iniettiva da E a E' e sia θ la coppia ordinata (f, g). Diciamo che θ è un *isomorfismo* da G in G' se vale la seguente condizione: il vertice v è incidente con il lato e in G se e solo se il vertice $f(v)$ è incidente con il lato $g(e)$ in G'. Se esiste un isomorfismo tra G e G' si diche che G e G' sono *isomorfi* e si indica con $G \cong G'$. Ovviamente se $G \cong G'$, allora $|V| = |V'|$ e $|E| = |E'|$.
Si può osservare che gli isomorfismi di grafi preservano i cicli e la connessione.

A.3 Teoria dei campi

L'insieme C non vuoto dotato di due operazioni binarie $+$ e $*$ è un campo se valgono le seguenti proprietà:

- C con l'operazione $+$ è un gruppo abeliano il cui elemento neutro è 0;
- $C - \{0\}$ con l'operazione $*$ è un gruppo abeliano con elemento neutro 1;
- l'operazione $*$ è distributiva rispetto all'operazione $+$.

Teorema A.3.1. *Sia F un campo di cardinalità finita. Allora F ha p^k elementi, con p numero primo e k intero positivo. Inoltre dati un p primo e un k intero positivo, esiste un unico campo con p^k elementi.*

Il campo con p^k elementi si chiama *campo di Galois di ordine p^k* e si indica con $GF(p^k)$. Se $k = 1$, allora $GF(p) = \mathbb{Z}_p$. In questo caso $GF(p)$ ha come

elementi $0, 1, \ldots p-1$ e le operazioni sono l'addizione e la moltiplicazione mod p.
In seguito diamo una costruzione di $GF(P^k)$ con $k > 1$ cercando di utilizzare il minor numero di nozioni teoriche possibile. Sia $h(\omega)$ un polinomio di grado k a coefficienti in $GF(p)$ irriducibile, cioè tale che non sia prodotto di polinomi di grado minore su $GF(p)$. Consideriamo l'insieme S che contiene tutti i polinomi nella variabile ω di grado minore o uguale a $k-1$ a coefficienti in $GF(p)$. Allora, dato che è possibile scegliere esattamente in p modi diversi i k coefficienti degli elementi di S, si avrà che $|S| = p^k$. Inoltre con l'operazione di addizione mod p e l'operazione di moltiplicazione ottenuta considerando il resto della divisione tra il prodotto ottenuto con il polinomio $h(\omega)$, S è un campo.

Esempio A.3.1. Mostriamo la costruzione di $GF(4)$. Prendiamo come polinomio irriducibile $h(\omega) = \omega^2 + \omega + 1$. Allora gli elementi di $GF(4)$ sono $0, 1, \omega, \omega+1$ e l'addizione e la moltiplicazione sono tali che $2 = 0$ e $\omega^2 = \omega+1$.

La *caratteristica* di un campo è il minimo valore n tale che

$$\overbrace{1 + 1 + \cdots + 1}^{n \text{ volte}} = 0.$$

Se tale valore non esiste, si dice che il campo ha caratteristica 0.

Proposizione A.3.2. *Sia F campo. Allora $car(F) = 0$ oppure $car(F) = p$, con p numero primo. In particolare, $GF(p^k)$ ha caratteristica p.*

Bibliografia

[1] A. M. H. Gerards, A short proof of Tutte's characterization of totally unimodular matrices, *Linear Algebra and its Applications* **114** (1989), 207-212.

[2] J. Kahn, P. D. Seymour, On forbidden minors for $GF(3)$, *Proceedings of the American Mathematical Society* **102** (1988), 437-440.

[3] J. P. S. Kung, *A source book in matroid theory*, Birkhäuser, Boston, 1986.

[4] J. G. Oxley, What is a matroid?, *Cubo Mat. Educ. 5* **3** (2003), 179-218.

[5] J. G. Oxley, *Matroid theory*, Oxford University Press, Oxford, 1992.

[6] A. Schrijver, *Theory of linear and integer programming*, Wiley, Chichester, 1986.

[7] P. D. Seymour, Matroid minors in *Handbook of Combinatorics 1* (eds. R. Graham, M. Grötschel, L. Lovász), Elsevier, Amsterdam; MIT Press, Cambridge, 1995.

[8] W. T. Tutte, A class of abelian groups, *Canadian Journal of Mathematics* **8** (1956), 13-28.

[9] W. T. Tutte, A homotopy theorem for matroids, I, II, *Transactions of the American Mathematical Society* **88** (1958), 144-174.

[10] W. T. Tutte, *Introduction to the theory of matroids*, in *Modern analytic and computational mathods in science and mathematics* **37** (eds. R. Bellman), Elsevier, New York, 1971.

[11] W. T. Tutte, *Graph theory*, in *Encyclopedia of Mathematics and its Applications* **21** (eds. G. C. Rota), Addison-Wesley, Waterloo, 1984.

[12] H. Whitney, On the abstract properties of linear dependence, *American Journal of Mathematics* **57** (1935), 509-533.

Ringraziamenti

Molte persone, in un modo o nell'altro, mi hanno aiutata a raggiungere questo importante traguardo.
Ringrazio Francesco Regonati, che con infinita pazienza e disponibilità mi ha accompagnata in questi ultimi mesi, facendomi scoprire il vasto mondo delle matroidi e aiutandomi a trasformare nozioni, idee e intuizioni in un lavoro di cui vado fiera.
Ringrazio i miei genitori, per aver sempre creduto nelle mie capacità e senza i quali non sarei potuta arrivare fin qui.
Ringrazio i miei fratelli, che mi sopportano e che riescono sempre a strapparmi un sorriso.
Ringrazio i miei compagni di corso, senza i quali questi cinque anni non sarebbero volati via così in fretta.
Ringrazio i miei amici, che con due chiacchiere, una tisana o un bicchiere di birra mi hanno aiutata a distrarmi quando più ne avevo bisogno.
E, dulcis in fundo, ringrazio Mirko, che mi è rimasto accanto dall'inizio alla fine. Non avrà contribuito a migliorare questa tesi, ma di sicuro ha migliorato la sua autrice.