Università degli Studi di Padova

Dipartimento di Matematica

Corso di Laurea in Matematica

Algoritmi per problemi su matroidi e polimatroidi

Laureando

Andrea Agnolin

Matricola

1074056

Relatore

Prof. Marco Di Summa

21 Aprile 2017 - A.A. 2016/2017

Indice

Introduzione

Il presente lavoro ha come oggetto principale i matroidi. Questo concetto fu introdotto con lo scopo di dare una descrizione generale dell'idea di indipendenza. Mostreremo come tramite i matroidi sia possibile dare una descrizione unica ad oggetti che provengono dalla combinatoria all'algebra lineare, alla teoria dei grafi.

Nel primo capitolo, dopo una introduzione delle prime proprietà e risultati presenteremo il problema di ottimizzare una funzione costo su elementi di un matroide e vedremo come questo problema sia strettamente legato al funzionamento corretto dell'algoritmo greedy.

Nel secondo capitolo affronteremo il problema di ottimizzazione su più matroidi contemporaneamente. Mostreremo come in generale questo sia un problema difficile, ma esporremo due differenti algoritmi per risolvere il problema di trovare la cardinalità massima di un insieme nell'intersezione di due matroidi.

Infine nel terzo capitolo presentiamo una descrizione poliedrale dei matroidi, trattando poi una loro generalizzazione, i polimatroidi. Vedremo come per i programmi lineari che otteniamo ci siano dei buoni algoritmi risolventi.

Capitolo 1

Matroidi

In questo capitolo presentiamo la definizione di matroide (come data in [1]), alcuni esempi e i primi risultati e proprietà. Gran parte degli enunciati e delle dimostrazioni proviene da [1], [2], [3] e [4]. Terminiamo il capitolo con la descrizione dell'algoritmo greedy e della sua relazione con i matroidi, dimostrando che questi sono l'unica classe di insieme chiusa per sottoinsiemi su cui greedy ottimizza correttamente [3],[1].

1.1 Motivazione

I matroidi sono stati introdotti per dare un'unica descrizione ad alcune strutture dell'algebra lineare e della teoria dei grafi.

Consideriamo i seguenti fatti:

1. Dato uno spazio vettoriale S e due insiemi $\mathcal{V}, \mathcal{W} \subset S$, entrambi insiemi di vettori linearmente indipendenti, tali che $|\mathcal{V}| > |\mathcal{W}|$ allora il *lemma di scambio* garantisce che esiste un vettore $v \in \mathcal{V} \setminus \mathcal{W}$ tale che $(\mathcal{W} \cup \{v\})$ è un insieme di vettori linearmente indipendenti.

2. Dato un grafo $G = (V, E)$ e due insiemi di vertici F_1, F_2 che non contengano cicli, ovvero tali che (V, F_1) e (V, F_2) siano due foreste, se vale che $|F_1| > |F_2|$ allora esiste un arco $e \in F_1 \setminus F_2$ tale che $(V, F_2 \cup \{e\})$ sia ancora una foresta.

Notiamo che esiste una analogia fra le due versioni (per indipendenza lineare e per le foreste) del *"lemma di scambio"*: in entrambi i casi posso aggiungere elementi di un insieme più grande a uno più piccolo preservando la proprietà richiesta. La definizione di matroide richiede questo fatto.

1.2 Definizioni

Definizione 1.2.1 (Matroide)**.** Sia E un insieme finito. Sia $\mathcal{I} \subseteq 2^E$ un insieme di parti di E. La coppia $(E, \mathcal{I})$ si dice *matroide* se valgono le seguenti proprietà:

1. $\emptyset \in \mathcal{I}$
2. Se $A \subset B$ e $B \in \mathcal{I}$ allora $A \in \mathcal{I}$
3. Se $A, B \in \mathcal{I}$ e $|A| > |B|$ allora esiste $x \in A \setminus B$ tale che $(B \cup \{x\}) \in \mathcal{I}$.

Allora ogni elemento di $\mathcal{I}$ è detto insieme *indipendente* del matroide, gli altri sottoinsiemi di E sono detti *dipendenti*.

Definizione 1.2.2. Ogni indipendente massimale rispetto alla relazione di inclusione di insiemi è detto *base*. Una base di un sottoinsieme $U \subseteq E$ è un indipendente massimale contenuto in U. Ogni sottoinsieme A dipendente di E tale che $\forall\, x \in A$ si abbia che $A \setminus \{x\} \in \mathcal{I}$ è detto *circuito*. Ovvero i circuiti sono gli insiemi dipendenti minimali.

Esempi: indipendenza lineare e foreste

Esempio 1.2.3. Sia $\mathbb{K}$ un campo e $A \in M_{m\times n}(\mathbb{K})$ una matrice. Sia $E = \{1, \dots, n\}$ l'insieme degli indici delle colonne, ovvero $A = [v_i]_{i\in E}$ per $v_i \in \mathbb{K}^m$. Se

$$\mathcal{I} = \{A \subseteq E : \{v_i\}_{i\in A} \text{ è un insieme di vettori linearmente indipendenti}\}$$

allora $(E, \mathcal{I})$ è un matroide. In questo caso gli indipendenti del matroide corrispondono ad insiemi di colonne linearmente indipendenti.

Esempio 1.2.4. Sia $G = (V, E)$ un grafo. Sia $\mathcal{I} \subset \mathcal{P}(E)$ tale che $A \in \mathcal{I}$ se e solo se (V, A) è una foresta. Allora $(E, \mathcal{I})$ è un matroide e gli insiemi di archi che non contengono cicli sono gli indipendenti del matroide.

Esempi: matroide partizione e uniforme

Esempio 1.2.5. Sia E un insieme finito, $\{P_i\}_{i\in I}$ una partizione di E e $\{a_i\}_{i\in I}$ una sequenza di naturali per cui valga $a_i \leq |P_i|\ \forall i \in I$. Sia

$$\mathcal{I} = \{A \subseteq E : |A \cap P_i| \leq a_i\, \forall i \in I\}$$

ovvero un insieme è indipendente se contiene al più a_i elementi di ogni elemento P_i della partizione. Allora $(E, \mathcal{I})$ è un matroide. I matroidi di questa forma sono detti matroide partizione.

Dimostrazione. (1) $\emptyset \in \mathcal{I}$ perché $|\emptyset \cap P_i| = 0 \leq a_i \in \mathbb{N}$ per ogni i.
(2) Se $A \subset B \in \mathcal{I}$ allora $A \cap P_i \subseteq B \cap P_i$, per cui $|A \cap P_i| \leq |B \cap P_i| \leq a_i \, \forall i$.
(3) Se $A, B \in \mathcal{I}$ e $|A| > |B|$, allora esiste un $\hat{i}$ per cui $|A \cap P_{\hat{i}}| > |B \cap P_{\hat{i}}|$ (se così non fosse avremmo che $|A| = \sum_{i \in I} |A \cap P_i| \leq \sum_{i \in \mathcal{I}} |B \cap P_i| = |B|$ che contraddice le ipotesi). Dato che $B \in \mathcal{I}$ allora $a_{\hat{i}} \geq |A \cap P_{\hat{i}}| > |B \cap P_{\hat{i}}|$. Per questo se scelgo un elemento $x \in (A \cap P_{\hat{i}}) \setminus B$ allora $|(B \cup \{x\}) \cap P_{\hat{i}}| \leq a_{\hat{i}}$. Infine $(B \cup \{x\}) \cap A_i = B \cap A_i$ per ogni $i \neq \hat{i}$ e quindi $|(B \cup \{x\}) \cap A_i| \leq a_i$ per cui $B \cup \{x\} \in \mathcal{I}$. □

Un caso particolare di matroide partizione sono i matroidi uniformi.

Esempio 1.2.6. Siano $n, r \in \mathbb{N}$, $r < n$, sia $E = \{1 \dots n\}$, sia $\mathcal{I}$ la famiglia dei sottoinsiemi di E che contengono al più r elementi: $\mathcal{I} = \{A \subseteq E : |A| \leq r\}$. Allora $U_{r,n} = (E, \mathcal{I})$ è un matroide detto matroide uniforme.

1.2.1 Matroidi isomorfi

Definizione 1.2.7. Due matroidi $M_1 = (E_1, \mathcal{I}_1)$ e $M_2 = (E_2, \mathcal{I}_2)$ si dicono isomorfi se esiste una funzione biunivoca $f : E_1 \to E_2$ tale che $A \in \mathcal{I}_1$ se e solo se $f(A) \in \mathcal{I}_2$ $\forall A \subseteq E_1$. In questo caso scriviamo $M_1 \cong M_2$.

1.2.2 Somma diretta

Proposizione 1.2.8. *Dati due matroidi $M_1 = (E_1, \mathcal{I}_1)$, $M_2 = (E_2, \mathcal{I}_2)$ con E_1 e E_2 due insiemi finiti disgiunti, sia $\mathcal{I}_1 \vee \mathcal{I}_2 = \{U \cup V : U \in \mathcal{I}_1, V \in \mathcal{I}_2\}$. Chiamiamo*

$$M_1 \oplus M_2 = (E_1 \cup E_2, \mathcal{I}_1 \vee \mathcal{I}_2),$$

allora $M_1 \oplus M_2$ è un matroide.

Dimostrazione. (1) Banale
(2) Siano $A_1 \subseteq A_2$ e $A_2 = U_2 \cup V_2$, con $U_2 \in \mathcal{I}_1$, $V_2 \in \mathcal{I}_2$, allora $U_1 = (A_1 \cap U_2) \subseteq U_2$, da cui segue $U_1 \in \mathcal{I}_1$. Analogamente $V_1 = (A_1 \cap V_2) \in \mathcal{I}_2$. Infine $U_1 \cup V_1 = A_1 \cap (U_2 \cup V_2) = A_1 \cap A_2 = A_1 \in \mathcal{I}_1 \vee \mathcal{I}_2$.
(3) Siano $A_1 = U_1 \cup V_1$ e $A_2 = U_2 \cup V_2$, con $U_1, U_2 \in \mathcal{I}_1$, $V_1, V_2 \in \mathcal{I}_2$, tali che $|A_1| > |A_2|$, allora o $|U_1| > |U_2|$ o $|V_1| > |V_2|$. Supponiamo, senza perdita di generalità, che $|U_1| > |U_2|$, dato che $U_1, U_2 \in \mathcal{I}_1$ esiste $x \in U_1 \setminus U_2 \subseteq A_1 \setminus A_2$ tale che $U_2 \cup \{x\} \in \mathcal{I}_1$. Infine $A_2 \cup \{x\} = (U_2 \cup \{x\}) \cup V_2 \in \mathcal{I}_1 \vee \mathcal{I}_2$. □

Definizione 1.2.9. $M_1 \oplus M_2$ è detta *somma diretta* di M_1 e M_2.

Un matroide partizione è la somma diretta di matroidi uniformi.

1.2.3 Minori di un matroide

Proposizione 1.2.10. *Dato un matroide $M = (E, \mathcal{I})$ e $x \in E$ allora*

$$M \setminus \{x\} = \big(E \setminus \{x\}, \{A \in \mathcal{I} : A \subseteq (E \setminus \{x\})\}\big)$$

è un matroide

Definizione 1.2.11 (Sottrazione)**.** La sottrazione di insieme U da un matroide $M = (E, \mathcal{I})$ è

$$M \setminus U = (E \setminus U, \{A \in \mathcal{I} : A \subseteq U^c\})$$

Dimostrazione della proposizione 1.2.10. Chiamo $\mathcal{I}' = \{A \in \mathcal{I} : A \subseteq (E \setminus \{x\})\}$.
(1) $\emptyset \in \mathcal{I}$ e $\emptyset \subseteq E \setminus \{x\}$ sempre, quindi $\emptyset$ è un indipendente.
(2) Se $A \subseteq B$ e $B \in \mathcal{I}'$, allora $B \in \mathcal{I}$ quindi $A \in \mathcal{I}$, e $B \subseteq (E \setminus \{x\})$ allora $A \subseteq (E \setminus \{x\})$.
(3) Siano $A, B \in \mathcal{I}'$, $|A| > |B|$, allora $A, B \subseteq (E \setminus \{x\})$. Dato che $A, B \in \mathcal{I}$ allora $\exists\, x \in A \setminus B$ per cui $B \cup \{x\} \in \mathcal{I}$, ma $B \cup \{x\} \subseteq A \cup B \subseteq (E \setminus \{x\})$, quindi $B \cup \{x\} \in \mathcal{I}'$. □

Se $U = \{x_1, x_2, \ldots, x_n\}$ allora $M \setminus U = M \setminus \{x_1\} \setminus \{x_2\} \cdots \setminus \{x_n\}$

Proposizione 1.2.12. *Dato un matroide $M = (E, \mathcal{I})$ e $U \subseteq E$ allora*

$$M/U = \big(E \setminus U, \{A \subseteq (E \setminus U) : \exists V \text{ base di } U : (A \cup V) \in \mathcal{I}\}\big)$$

è un matroide.

Definizione 1.2.13 (Contrazione)**.** La contrazione di un matroide $M = (E, \mathcal{I})$ rispetto ad un insieme $U \subseteq E$ è il matroide M/U.

Dimostrazione della proposizione 1.2.12. Chiamo $\mathcal{I}' = \{A \subseteq U^c : \exists V$ base di $U : (A \cup V) \in \mathcal{I})$.
(1) Sia V base di U, $\emptyset \cup V = V \in \mathcal{I}$, quindi $\emptyset \in \mathcal{I}'$.
(2) Se $A \subseteq B$ e $B \in \mathcal{I}'$, allora $B \cup V \in \mathcal{I}$ per V base di U quindi $A \cup V \in \mathcal{I}$ perché è contenuto in $B \cup V$.
(3) Siano $A, B \in \mathcal{I}'$ tali che $|A| > |B|$. Dato che $A, B \subseteq U^c$ allora $A \cap U = B \cap U = \emptyset$. Per ipotesi esistono V' e V'' sono basi di U, per cui $A \cup V'$ e $B \cup V''$ sono indipendenti di M e inoltre $|A \cup V'| > |B \cup V''|$. Segue quindi che esiste $x \in (A \cup V') \setminus (B \cup V'')$ per cui $B \cup \{x\} \cup V'' \in \mathcal{I}$. Se avessimo che $x \in (V' \setminus V'') \subseteq ((A \cup V') \setminus (B \cup V''))$ allora avremmo che $V'' \cup \{x\} \in \mathcal{I}$, ma questo viola la massimalità di V'', base di U. Quindi $x \in (A \setminus B)$. Dato che $x \in A \setminus B \subseteq U^c$ allora $B \cup \{x\} \subseteq U^c$. $B \cup \{x\} \in \mathcal{I}'$. □

I minori di un matroide $M = (E, \mathcal{I})$ sono le contrazioni e le sottrazioni rispetto a sottoinsiemi di E.

1.3 Rango

Proposizione 1.3.1. *Dato un matroide $M = (E, \mathcal{I})$ ogni base di M ha la stessa cardinalità.*

Dimostrazione. Supponiamo che esistano due basi B_1 e B_2 con differente cardinalità. Supponiamo che $|B_1| > |B_2|$, allora per la proprietà (3) esiste un elemento $x \in B_1 \setminus B_2$ tale che $B_2 \cup \{x\}$ è indipendente, ma questo viola la massimalità di B_2 che dunque non può essere una base. □

Definizione 1.3.2. La cardinalità delle basi di M è detta *rango* di M, indicato con $r(M)$.

Lemma 1.3.3. *Ogni insieme indipendente di un matroide M con cardinalità $r(M)$ è una base.*

Dimostrazione. Se così non fosse ed esistesse un insieme indipendente non massimale di cardinalità $r(M)$ allora dovrebbe esistere una base che lo contiene strettamente la quale avrebbe cardinalità strettamente maggiore del rango del matroide, e questo non è possibile per la proposizione 1.3.1. □

Proposizione 1.3.4. *Dato un matroide $M = (E, \mathcal{I})$ e un insieme $U \subseteq E$, allora tutti gli indipendenti contenuti in U massimali per l'inclusione hanno la stessa cardinalità.*

Dimostrazione. Gli indipendenti massimali contenuti in U sono le basi di $M \setminus U^c$. □

Definizione 1.3.5. Dato un matroide $M = (E, \mathcal{I})$, la funzione $r_M : 2^E \to \mathbb{N}$, rango in M di un sottoinsieme $U \subseteq E$, è la cardinalità degli insiemi indipendenti massimali contenuti in U (basi di U).

Ovviamente $r_M(E) = r(M)$ e $r_M(U) = r(M \setminus U^c)$. Se non c'è ambiguità indichiamo talvolta r_M semplicemente con r.

1.3.1 Proprietà del rango

Proposizione 1.3.6. *La funzione rango è crescente e maggiorata dalla cardinalità.*

Dimostrazione. $|U| \geq r(U)$ segue banalmente dalla definizione.
$r(U) \geq r(V)$ per $U \supseteq V$ perché ogni base di V è un indipendente contenuto in U, quindi è contenuta nelle basi di U. □

Proposizione 1.3.7. *La funzione rango è submodulare, cioè dati U, V due insiemi allora*

$$r(U \cup V) + r(U \cap V) \leq r(U) + r(V).$$

Dimostrazione. Siano $U, V \subseteq E$.
Sia B_1 una base di $U \cap V$, allora, dato che B_1 è un indipendente contenuto in U, esiste una base B_2 di U che contiene B_1, ovvero se $A_2 = B_2 \setminus B_1$, allora $B_2 = B_1 \sqcup A_2$. Per lo stesso motivo esiste B_3 base di $U \cup V$ con $B_3 = B_2 \sqcup A_3 = B_1 \sqcup A_2 \sqcup A_3$. Per via della massimalità delle basi $A_3 \cap U = \emptyset$ quindi $A_3 \subseteq V$ indipendente e perciò $B_1 \sqcup A_3$ è un indipendente contenuto in V, quindi $r(V) \geq |B_1| + |A_3|$. Infine, dato che $r(U \cap V) = |B_1|$, $r(U \cup V) = |B_3| = |B_1| + |A_2| + |A_3|$, $r(U) = |B_2| = |B_1| + |A_2|$, allora

$$r(U) + r(V) \geq |B_1| + |A_2| + |B_1| + |A_3| = |B_1| + (|B_1| + |A_2| + |A_3|) = r(U \cup V) + r(U \cap V). \quad \square$$

Corollario 1.3.8. Dato che $r(\emptyset) = 0$ allora r è sub-additiva, cioè $r(A \cup B) \leq r(A) + r(B)$.

1.3.2 Caratterizzazione del rango

Proposizione 1.3.9. *Sia M un matroide su E con funzione rango $r : 2^E \to \mathbb{N}$ allora $M = (E, \mathcal{I}(r))$ con*

$$\mathcal{I}(r) = \{U \subseteq E : r(U) = |U|\}$$

Ovvero gli indipendenti sono tutti e soli gli insiemi che hanno rango uguale alla cardinalità.

Dimostrazione. Sia U un indipendente di M, allora U è l'indipendente massimale contenuto in se stesso, quindi $r(U) = |U|$. Allo stesso modo se $r(U) = U$, allora $\exists V \subseteq U : V \in \mathcal{I}(M), |U| = |V|$, quindi U è indipendente. $\square$

Teorema 1.3.10. *Data una funzione $r : 2^E \to \mathbb{N}$ che soddisfa le proprietà:*

1. *$r(X) \leq |X|$*
2. *r è crescente: se $Y \subseteq X$ allora $r(Y) \leq r(X)$*
3. *r è submodulare: $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$*

Allora $(M, \mathcal{I}(r))$ è un matroide ed r la sua funzione rango.

Dimostrazione. Verifichiamo le proprietà della definizione 1.2.1 di matroide.
Per l'ipotesi (1) allora $0 \leq r(\emptyset) \leq 0$ da cui $r(\emptyset) = |\emptyset|$, da cui $\emptyset \in \mathcal{I}(r)$, verificando (1.2.1:1).
Siano $X \in \mathcal{I}(r)$ e $Y \subseteq X$ e sia $Z = X \setminus Y$. Usiamo la submodularità (3), allora

$$\begin{aligned} r(Y \cup Z) + r(Y \cap Z) &\leq r(Y) + r(Z) \\ r(X) + r(\emptyset) &\leq r(Y) + r(Z) \leq r(Y) + |Z| \\ |X| &\leq r(Y) + |X| - |Y|\,. \end{aligned}$$

Dato che $|Y| \geq r(Y)$ per (1), allora $r(Y) = Y$. Questo dimostra $Y \in \mathcal{I}(r)$ e quindi verifica la condizione (1.2.1:2).
Siamo $X, Y \in \mathcal{I}(r)$ e supponiamo $|X| > |Y|$, dimostriamo (1.2.1:3) per assurdo, supponendo quindi che non esiste nessun $x \in X \setminus Y$ per cui $r(Y \cup \{x\}) = |Y \cup \{x\}| = |Y| + 1$. Se $(X \setminus Y) = \{x\}$ allora $Y \cup \{x\} = X$ è indipendente, supponiamo perciò $|X \setminus Y| \geq 2$.
Sia $x \in X \setminus Y$, $|Y| \leq r(Y \cup \{x\}) < |Y| + 1$, per cui $r(Y \cup \{x\}) = |Y| \, \forall x \in (X \setminus Y)$.
Siano $x_1, x_2 \in X \setminus Y$, allora per l'ipotesi (2) $r(Y \cup \{x_1, x_2\}) \geq r(Y)$, quindi per la submodularità (3)

$$2r(Y) \leq r\left(Y \cup \{x_1, x_2\}\right) + r(Y) \leq r\left(Y \cup \{x_1\}\right) + r\left(Y \cup \{x_2\}\right) = 2r(Y)$$

quindi $r(Y \cup \{x_1, x_2\}) = |Y| \ \forall x_1, x_2 \in (X \setminus Y)$. Da cui segue $r\Big((Y \cup \{x_1\}) \cup \{x_2\}\Big) = r(Y) \, \forall x_2 \in (X \setminus (Y \cup \{x_1\})) \, \forall x_1 \in (X \setminus Y)$
Verifico quindi per induzione che per $x_1, x_2, \ldots x_n \in X \setminus Y$ e $Y_n = (Y \cup \{x_1, x_2, \ldots x_n\})$

$$r\Big((Y \cup \{x_1, x_2, \ldots x_n\}) \cup \{x_{n+1}\}\Big) = r(Y) \, \forall x_{n+1} \in (X \setminus Y_n)$$

Come sopra $2r(Y_{n-1}) \leq r(Y_{n-1} \cup \{x_n, x_{n+1}\}) + r(Y_{n-1}) \leq r(Y' \cup \{x_n\}) + r(Y' \cup \{x_{n+1}\}) = 2r(Y_{n-1})$ allora $r\big((Y_{n-1} \cup \{x_n\}) \cup \{x_{n+1}\}\big) = r(Y_{n-1}) = r(Y) \, \forall x_{n+1} \in (X \setminus (Y_{n-1} \cup \{x_n\}))$. Quindi so che comunque aggiungo elementi di $X \setminus Y$ a Y il rango deve sempre rimanere $r(Y)$, se li aggiunto tutti trovo $|Y| = r(Y) = r(Y \cup (X \setminus Y)) = r(X \cup Y) \geq r(X) = |X| > |Y|$, ma questo è assurdo. □

1.4 Basi e duale

1.4.1 Caratterizzazione dell'insieme delle basi

Teorema 1.4.1. *Sia E un insieme finito e $\mathcal{B} \subseteq 2^E$ una famiglia di sottoinsiemi di E. Se $\mathcal{B}$ è l'insieme della basi di un matroide, allora gode delle seguenti proprietà:*

1. $\mathcal{B} \neq \emptyset$
2. *Se $B_1, B_2 \in \mathcal{B}$ e $x \in B_1 \setminus B_2$ allora $\exists y \in B_2 \setminus B_1$ tale che $B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$*

Inoltre se un insieme $\mathcal{B}$ soddisfa queste due proprietà esiste un matroide $M = (E, \mathcal{I})$, con $\mathcal{I} = \{A \subseteq E : A \subseteq B \ \exists B \in \mathcal{B}\}$, di cui $\mathcal{B}$ è l'insieme delle basi.

Dimostriamo ora che che l'insieme delle basi di un matroide soddisfa le proprietà 1 e 2. Successivamente enunciamo e dimostriamo un lemma che useremo per dimostrare il viceversa.

Dimostrazione prima parte. (1) Sia $M = (E, \mathcal{I})$ un matroide, dato che $\emptyset \in \mathcal{I}$ allora $\mathcal{I}$ non è vuoto ed esiste un elemento massimale, ovvero una base.
(2) Siano ora B_1, B_2 due basi e $x \in B_1 \setminus B_2$. $|B_1 \setminus \{x\}| < |B_2|$, quindi $\exists y \in B_2 \setminus (B_1 \setminus \{x\})$ tale che $B_1 \setminus \{x\} \cup \{y\} \in \mathcal{I}$, voglio mostrare che $y \in B_2 \setminus B_1$ e che $B_1 \setminus \{x\} \cup \{y\}$ è una base. Dato che $x \in B_1 \setminus B_2$ allora $x \notin B_2$ e dunque $B_2 \setminus (B_1 \setminus \{x\}) = B_2 \setminus B_1$ e dunque $y \in B_2 \setminus B_1$. E dato che $|B_1 \setminus \{x\} \cup \{y\}| = |B_1| = r(M)$ allora per 1.3.3 $B_1 \setminus \{x\} \cup \{y\}$ è una base di M. □

Lemma 1.4.2. *Una famiglia $\mathcal{B}$ con le proprietà (1) e (2) ha tutti gli insiemi della medesima cardinalità.*

Dimostrazione. Supponiamo che non sia così e tra le coppie di elementi di $\mathcal{B}$ che hanno diversa cardinalità scegliamo la coppia B_1, B_2 tale che $|B_1| > |B_2|$ e tale che $|B_1 \setminus B_2|$ sia minimo. Sia $x \in (B_1 \setminus B_2)$, per (2) esiste $y \in B_2 \setminus B_1$ tale che $B_3 = B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$. Banalmente $|B_3| = |B_1| > |B_2|$, quindi per l'ipotesi di minimalità nella scelta di B_1 e B_2 sappiamo che $|B_3 \setminus B_2| \geq |B_1 \setminus B_2|$. Però è pur vero che, dato che $y \in B_2$ e $x \notin B_2$, $(B_3 \setminus B_2) = ((B_1 \setminus \{x\}) \cup \{y\}) \setminus B_2 = (B_1 \setminus \{x\}) \setminus B_2 = B_1 \setminus B_2 \setminus \{x\}$ e dunque $|B_3 \setminus B_2| = |B_1 \setminus B_2 \setminus \{x\}| < |B_1 \setminus B_2|$. Questo è un assurdo. □

Dimostrazione della seconda parte di 1.4.1.
(1) $\emptyset \subseteq B$ per un qualunque $B \in \mathcal{B}$ quindi $\emptyset \in \mathcal{I}$
(2) Se $U \subset V \in \mathcal{I}$ allora $\exists B \in \mathcal{B}$ per cui $U \subset V \subseteq B$ quindi $U \in \mathcal{I}$.
(3) [2] Supponiamo per assurdo che esistano $U, V \in \mathcal{I}$, tali che $|U| > |V|$, che violino la proprietà richiesta, ovvero per cui $\forall x \in U \setminus V$ si abbia che $V \cup \{x\}$ non sia contenuto in nessun elemento di $\mathcal{B}$.
Siano $B_1, B_2 \in \mathcal{B}$ tali che $U \subseteq B_1$, $V \subseteq B_2$.
Dato che $V \cup \{x\} \nsubseteq B_2 \, \forall x \in U \setminus V$ allora $(U \setminus V)$ e B_2 sono due insiemi disgiunti, da questo segue che $U \setminus V = U \setminus V \setminus B_2$ e dunque $U \setminus V = U \setminus B_2$.
Ora scegliamo B_1 fra le basi che contengono U in modo che $|B_1 \setminus (U \cup B_2)|$ sia minimo e dimostriamo che $B_1 \subseteq (U \cup B_2)$ mostrando che se così non fosse trovo un elemento di $\mathcal{B}$ che contiene U e che violerebbe la minimalità richiesta. Sia $x \in B_1 \setminus (U \cup B_2)$, allora esiste un elemento $y \in B_2 \setminus B_1$ per cui $B_3 = B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$. Notiamo che $U \subseteq B_3$ perché $U \subseteq B_1$ e $x \notin U$. Dato che $y \in B_2$ allora $(B_1 \cup \{y\} \setminus (U \cup B_2)) = (B_1 \setminus (U \cup B_2))$, e dato che $x \in B_1$ ma $x \notin U, x \notin B_2$ allora $B_3 \setminus (U \cup B_2) = (B_1 \setminus \{x\} \cup \{y\} \setminus (U \cup B_2)) = B_1 \setminus (U \cup B_2) \setminus \{x\} \subset (B_1 \setminus (U \cup B_2))$ e perciò $|B_3 \setminus (U \cup B_2)| < |B_1 \setminus (U \cup B_2)|$.
Dato che $B_1 \subseteq (U \cup B_2)$ e che $U \subseteq B_1$ allora, sottraendo U_2, troviamo, $U \setminus B_2 \subseteq B_1 \setminus B_1 \subseteq (B_2 \cup U) \setminus B_2 = U \setminus B_2$, ovvero $U \setminus B_2 = B_1 \setminus B_2$ e dato che $U \setminus B_2 = U \setminus V$ allora

$$U \setminus V = B_1 \setminus B_2.$$

Dimostriamo ora che $B_2 \subseteq (V \cup B_1)$, se così non fosse $\exists x \in B_2 \setminus (V \cup B_1)$ e $y \in B_1 \setminus B_2$ tali che $B_4 = B_2 \setminus \{x\} \cup \{y\} \in \mathcal{B}$, ma dato che $x \notin V$ allora $V \subseteq B_4$ e inoltre $V \cup \{y\} \subseteq B_4$, ma dato che $y \in B_1 \setminus B_2 = U \setminus V$ questo non può accadere dato che avevo supposto che per ogni $y \in U \setminus V$ non ci fosse un elemento di $\mathcal{B}$ che contiene $V \cup \{y\}$.
Analogamente a quanto fatto sopra da $B_2 \subseteq (V \cup B_1)$ otteniamo che $V \setminus B_1 = B_2 \setminus B_1$. Dato che $B_1 \supseteq U$, e che quindi $V \setminus B_1 \subseteq V \setminus U$, si ha che

$$B_2 \setminus B_1 \subseteq V \setminus U.$$

Ora per il lemma 1.4.2 sappiamo che $|B_1| = |B_2|$, da questo segue che $|B_1 \setminus B_2| = |B_2 \setminus B_1|$, per quanto dimostrato segue che $|U \setminus V| = |B_1 \setminus B_2| = |B_2 \setminus B_1| \leq |V \setminus U|$, da cui $|U| \leq |V|$. Ma questo viola le ipotesi che imponevano $|U| > |V|$.
Concludiamo così che $M = (E, \mathcal{I})$ è un matroide. □

1.4.2 Circuiti

Proposizione 1.4.3. *Siano C_1 e C_2 due circuiti distinti di un matroide e $e \in C_1 \cap C_2$ allora $(C_1 \cup C_2 \setminus \{e\}) \notin \mathcal{I}$, ovvero, equivalentemente, esiste un circuito C_3 dello stesso matroide contenuto in $(C_1 \cup C_2 \setminus \{e\})$.*

Dimostrazione. Sia $f \in C_2 \setminus C_1$ e sia r il rango del matroide.
Per la definizione di circuito vale che, dato C circuito, $r(C) = r(C \setminus \{e\})\ \forall e \in C$.
Allora, usando la submodularità:

$$\begin{aligned} r(C_1) + r(C_1 \cup C_2 \setminus \{e, f\}) + r(C_2) &\geq r(C_1 \setminus \{e\}) + r(C_1 \cup C_2 \setminus \{f\}) + r(C_2) \\ &\geq r(C_1 \setminus \{e\}) + r(C_1 \cup C_2) + r(C_2 \setminus \{f\}) \\ &= r(C_1) + r(C_1 \cup C_2) + r(C_2). \end{aligned}$$

Infatti $(C_1) \cap (C_1 \cup C_2 \setminus \{e, f\}) = (C_1 \setminus \{e\} \setminus \{f\}) = (C_1 \setminus \{e\})$ perché $f \notin C_1$ e $(C_1) \cup (C_1 \cup C_2 \setminus \{e, f\}) = (C_1 \cup C_2 \setminus \{f\})$ perché $e \in C_1$. In modo simile si ottiene la disuguaglianza successiva.
Quindi da $(C_1 \cup C_2 \setminus \{e, f\}) \subseteq (C_1 \cup C_2)$ e dalla monotonia di r si ottiene $r(C_1 \cup C_2 \setminus \{e, f\}) = r(C_1 \cup C_2) = r(C_1 \cup C_2 \setminus \{e\})$. Per cui $r(C_1 \cup C_2 \setminus \{e\}) \leq |C_1 \cup C_2 \setminus \{e, f\}| < |C_1 \cup C_2 \setminus \{e\}|$ dunque $(C_1 \cup C_2 \setminus \{e\}) \notin \mathcal{I}$. □

Teorema 1.4.4. *Sia $A \in \mathcal{I}$ un indipendente di $M = (E, \mathcal{I})$ matroide e $e \in E$ tale che $(A \cup \{e\}) \notin \mathcal{I}$. Allora esiste un unico circuito contenuto in $A \cup \{e\}$.*

Dimostrazione. Supponiamo ci siano C_1, C_2 circuiti distinti di M entrambi contenuti in $A \cup \{e\}$. Entrambi contengono e perché altrimenti sarebbero contenuti in A e quindi indipendenti, allora per la proposizione 1.4.3 si ha che $C_1 \cup C_2 \setminus \{e\} \notin \mathcal{I}$, ma $C_1 \cup C_2 \setminus \{e\} \subseteq (A \cup \{e\}) \setminus \{e\} = A$ quindi $(C_1 \cup C_2 \setminus \{e\}) \in \mathcal{I}$, producendo una contraddizione. □

Definizione 1.4.5. Sia $M = (E, \mathcal{I})$, $A \in \mathcal{I}$ e $e \in E$. Indichiamo con $C_M(A, e) = C(A, e)$ l'insieme vuoto se $A \cup \{e\}$ è indipendente, altrimenti l'unico circuito contenuto in $A \cup \{e\}$.

1.4.3 Matroide duale

Proposizione 1.4.6. *Sia $M = (E, \mathcal{I})$ un matroide e sia $\mathcal{B}$ l'insieme delle basi di M, sia $\mathcal{I}^* = \{A : A \subseteq B^c \; \exists B \in \mathcal{B}\}$, allora $(E, \mathcal{I}^*)$ è un matroide.*

Definizione 1.4.7. Il matroide $M^* = (E, \mathcal{I}^*)$ è detto *matroide duale* di M, l'insieme delle basi di M^* è $\mathcal{B}^* = \{E \setminus B : B \in \mathcal{B}\}$.

Dimostrazione. Dimostro che M^* è un matroide esibendo una funzione rango r^* che soddisfa le ipotesi del teorema 1.3.10 e per cui $\mathcal{I}(r^*) = \mathcal{I}^*$.
Sia r il rango per M. La funzione rango r^* deve soddisfare la proprietà che $r^*(A) = |A|$ se e solo se esiste $B \in \mathcal{B}$ per cui ogni $A \subseteq B^c$, quindi se $\exists B \in \mathcal{B} : A^c \supseteq B$ che equivale a dire che $r(A^c) = r(E)$, infatti se A^c contiene una base allora il suo rango è $r(M)$, e viceversa. Quindi è necessario trovare r^* tale che $r^*(A) = |A|$ se e solo se $r(A^c) = r(E)$, allora

$$r^*(A) = |A| + r(A^c) - r(E).$$

Verifico le ipotesi di 1.3.10:
(1) Dato che $r(E) - r(A^c) \geq 0$, allora $r^*(A) \leq |A|$.
(2) Sia $A \subseteq B$. Guardiamo come si comporta il rango dei loro complementari in M, per la subaddività $r(A^c) \leq r(B^c) + r(A^c \setminus B^c) = r(B^c) + r(B \setminus A)$. Inoltre $|B| = |A| + |B \setminus A| \geq |A| + r(B \setminus A)$. Allora

$$r^*(A) = |A| + r(A^c) - r(E) \leq (|B| - r(B \setminus A)) + (r(B^c) + r(B \setminus A)) - r(E) = r^*(B).$$

(3) Siano $A, B \subseteq E$, allora $|A \cup B| + |A \cap B| = |A| + |B|$ e per r submodulare:

$$\begin{aligned} & r^*(A \cup B) + r^*(A \cap B) \\ = \; & |A \cup B| + |A \cap B| + r((A \cup B)^c) + r((A \cap B)^c) - 2r(E) \\ = \; & |A| + |B| + r(A^c \cap B^c) + r(A^c \cup B^c) - 2r(E) \\ \leq \; & |A| + |B| + r(A^c) + r(B^c) - 2r(E) \\ = \; & r^*(A) + r^*(B). \qquad \square \end{aligned}$$

Proposizione 1.4.8. *Sia M matroide, $(M^*)^* = M$.*

Dimostrazione. Basta mostrare che le basi $\mathcal{B}^{**}$ di M^{**} e $\mathcal{B}$ di M sono le stesse. E questo perché il passaggio al complementare è una funzione biunivoca fra $\mathcal{B}$ e $\mathcal{B}^*$ e la sua inversa è se stessa. $\square$

Proposizione 1.4.9. *Sia $M = (E, \mathcal{I})$ matroide allora $r(M) + r(M^*) = |E|$.*

Dimostrazione. Se B è una base di M, B^c lo è di M^*, allora $r(M) + r(M^*) = |B| + |E \setminus B| = |E|$. □

Proposizione 1.4.10. *Dato $M = (E, \mathcal{I})$ matroide e $U \subseteq E$ allora la contrazione M/E è uguale a $(M^* \setminus U)^*$*

Dimostrazione. Sia $M/U = (E \setminus U, \mathcal{I}')$. Mostriamo che per il rango di $(M^* \setminus U)^*$ vale $r_{(M^* \setminus U)^*}(X) = r(X \cup U) - r(U)$ per ogni $X \subseteq E \setminus U$.

$$\begin{aligned} r_{(M^* \setminus U)^*}(X) &= |X| + r_{M^*}(U^c \setminus X) - r_{M^*}(U^c) \\ &= |X| + \big(|U^c \setminus X| + r((U^c \setminus X)^c) - r(M)\big) + \big(|U^c| + r((U^c)^c) - r(M)\big) \\ &= |X| + |U^c| - |X| + |U^c| + r(U \cup X) + r(U) = r(X \cup U) - r(U). \end{aligned}$$

Mostreremo ora che $r_{(M^* \setminus U)^*} = r_{M/U}$ mostrando che $r_{(M^* \setminus U)^*}(A) = |A|$ se e solo se $A \in \mathcal{I}'$.
Sia $A \in \mathcal{I}'$, allora esiste B_A base di U tale che $A \cup B_A \in \mathcal{I}$. A e B_A sono disgiunti perché contenuti in rispettivamente in U^c e U, inoltre $A \cup B_A$ è una base di $A \cup U$ perché se diversamente avessi un indipendente $B' \subseteq A \cup U$ con $|B'| > |A \cup B_A|$ dovrei avere $|B' \cap U| > |B_A|$ violando il fatto che B_A sia una base. Quindi $r(A \cup U) = |A \cup B_A| = |A| + |B_A| = |A| + r(U)$. Riassumendo abbiamo che $|A| = r(A \cup U) - r(U)$ per ogni $A \in \mathcal{I}'$.
Sia $A \subseteq U^c$ tale che $|A| = r(A \cup U) - r(U)$. Per la submodularità del rango $r(A \cup U) \leq r(A) + r(U) \leq |A| + r(U)$, ma dalla ipotesi su A segue che $|A| + r(U) = r(A \cup U)$, per cui le disuguaglianze sono uguaglianze, ed in particolare $r(A \cup U) = r(A) + r(U)$ e $r(A) = |A|$, da cui segue $A \in \mathcal{I}$.
Sia $B \subseteq U$ una base di U. Per la monotonia del rango $r(A \cup B) \leq r(A \cup U)$, inoltre se valesse $r(A \cup B) < r(A \cup U)$ analogamente a quando detto sopra troverei un indipendente di U con cardinalità maggiore di B contraddicendo l'ipotesi per cui è una base, da questo segue $r(A \cup B) = r(A \cup U)$. Allora $|A \cup B| = |A| + |B| = r(A) + r(U) = r(A \cup U) = r(A \cup B)$. Riassumendo $A \cup B \in \mathcal{I}$ per ogni B base di U e ogni $A \subseteq U^c$ per cui $|A| = r(A \cup U) - r(U)$. □

Corollario 1.4.11. Se $M = (E, \mathcal{I})$ e $M/U = (E, \mathcal{I}')$ sono un matroide e la sua contrazione rispetto ad insieme $U \subseteq E$ e $A \in \mathcal{I}'$ è un indipendente di M/U allora $A \cup B \in \mathcal{I}$ per ogni B base di U.

1.5 Algoritmo greedy

Definizione 1.5.1 (Sistema di indipendenza)**.** Sia E un insieme finito e sia $\mathcal{I} \subseteq 2^E$, $(E, \mathcal{F})$ si dice *sistema di indipendenza* se $\mathcal{I}$ soddisfa la proprietà (1) e (2) nella definizione 1.2.1. Ovvero se $\mathcal{I}$ è un insieme non vuoto e chiuso per sottoinsiemi.

Possiamo definire per un sistema di indipendenza le sue basi, i suoi circuiti e il suo duale come li abbiamo definiti per un matroide.

Descriviamo ora una importante classe di problemi dei quali faremo successivamente alcuni esempi.

Problema 1.5.2 (Indipendente di costo massimo)**.**
Sia $(E, \mathcal{I})$ un sistema di indipendenza, sia $c : E \to \mathbb{R}$ una funzione *costo* sugli elementi di E. Il costo di un insieme $U \subseteq E$ è

$$C(U) = \sum_{x \in U} c(x).$$

OBIETTIVO: Trovare $X \in \mathcal{I}$ tale che il costo $C(X)$ sia massimo/minimo.

Problema 1.5.3 (Base di costo massimo)**.**
Siano dati $(E, \mathcal{I})$ e c come nel problema 1.5.2.
OBIETTIVO: Trovare una base X di $(E, \mathcal{I})$ per cui $C(X)$ sia massimo/minimo.

Nella esecuzione di un algoritmo per un problema su matroidi o su sistemi di indipendenza il dato di questi può essere fornito in diversi modi. Possiamo, ad esempio, supporre di avere ricevuto la lista dei sistemi indipendenti o la lista delle basi. Tuttavia in generale avere una lista è molto scomodo e computazionalmente problematico. Supporremo quindi che questi dati ci vengano forniti come delle funzioni, che saranno delle sub-routine del nostro algoritmo che verificano o calcolano delle proprietà in modo veloce.

Definizione 1.5.4 (Oracoli)**.** Diciamo che un sistema di indipendenza/matroide su E ci viene dato tramite un *oracolo di indipendenza* se supponiamo di avere una funzione (oracolo) che dato un insieme $U \subseteq E$ ci dica in tempo polinomiale se U sia un insieme indipendente o dipendente.
Diciamo che un sistema di indipendenza/matroide su E ci viene dato tramite un *oracolo di basis-superset* se supponiamo di avere una funzione (oracolo) che dato un insieme $U \subseteq E$ ci dica in tempo polinomiale se U contiene o non contiene una base.

Esempio 1.5.5 (Problema dello zaino)*.*
Siano dati n oggetti numerati, ciascuno con un peso w_i ed un valore c_i, e sia dato un peso massimo W trasportabile:
OBIETTIVO: Scegliere un insieme S di oggetti (da mettere nello zaino) di peso complessivo inferiore a W e valore complessivo massimo, ovvero:

$$S \subseteq \{1, 2, \dots n\} \qquad \sum_{i \in S} c_i \text{ massimo} \quad \text{s.a} \quad \sum_{i \in S} w_i \leq W$$

Notiamo che $(E, \mathcal{I})$, con $E = \{1, 2, \dots n\}$ e $\mathcal{I} = \{A \subseteq E : \sum_{i \in A} w_i \leq W\}$ è un sistema di indipendenza e dunque il problema dello zaino è una istanza del problema 1.5.2.

Esempio 1.5.6 (Albero ricoprente di peso minimo).
Sia dato un grafo connesso $G = (V, E)$ e dei costi c_e $\forall e \in E$
OBIETTIVO: Trovare $S \subseteq E$, tale che (V, S) sia albero ricoprente (ovvero un albero che tocchi tutti i nodi in V), e che il costo $C(S)$ sia minimo.
Abbiamo notato che $(E, \mathcal{I})$ con $\mathcal{I}$ contenente le foreste è un matroide e quindi un sistema di indipendenza, notiamo che gli alberi ricoprenti di un grafo connesso sono le foreste massimali. Quindi questo è un problema del tipo 1.5.3.

In generale istanze dei problemi 1.5.3 e 1.5.2 sono computazionalmente problematiche, basti notare che il problema dell'esempio 1.5.5 è un problema NP-Completo. Tuttavia vediamo ora come le istanze di questi problemi siano molto semplici quando trattiamo con matroidi. Ad esempio vedremo che il problema dell'esempio 1.5.6 si risolve in tempo quadratico.

Algoritmo 1.1 (Algoritmo greedy best-in)**.** *Siano dati un sistema di indipendenza $(E, \mathcal{I})$ tramite oracolo di indipendenza e una funzione costo c.*
Algortimo:

1. *Ordina $E = \{e_1, e_2, e_3 \dots e_n\}$ di modo che $c(e_1) \geq c(e_2) \geq \cdots \geq c(e_n)$.*
2. *Poni $A \leftarrow \emptyset$, $i \leftarrow 1$*
3. *Finchè $i \leq n$ fai:*
   (a) *Se $A \cup \{e_i\} \in \mathcal{I}$ allora $A \leftarrow A \cup \{e_i\}$*
   (b) *$i \leftarrow i + 1$*
4. *Restituisci l'insieme $A \in \mathcal{I}$ base di $(E, \mathcal{I})$*

Algoritmo 1.2 (Algoritmo greedy worst-out)**.** *Siano dati un sistema di indipendenza $(E, \mathcal{I})$ tramite oracolo di basi-superset e una funzione costo c.*
Algortimo:

1. *Ordina $E = \{e_1, e_2, e_3 \dots e_n\}$ di modo che $c(e_1) \leq c(e_2) \leq \cdots \leq c(e_n)$.*
2. *Poni $U \leftarrow E$, $i \leftarrow 1$*
3. *Finchè $i \leq n$ fai:*
   (a) *Se $U \setminus \{e_i\}$ contiene una base allora $U \leftarrow U \setminus \{e_i\}$*
   (b) *$i \leftarrow i + 1$*

4. Restituisci l'insieme U base di $(E, \mathcal{I})$

Proposizione 1.5.7. *Gli insiemi restituiti dagli algoritmi 1.1 e 1.2 sono veramente della basi di $(E, \mathcal{I})$*

Dimostrazione.
(1.1) la verifica 3a assicura che $A \in \mathcal{I}$, ora A è massimale perché se non lo fosse esisterebbe $e_i \in E$ per cui $A \cup \{e_i\} \in \mathcal{I}$, ma allora avrei aggiunto e_i ad A.
(1.2) la verifica 3a assicura che A contiene una base, ora A è anche indipendente perché se non lo fosse esisterebbe $e_i \in E$ per cui $A \setminus \{e_i\}$ conterebbe ancora una base, ma allora avrei tolto e_i ad A. □

Teorema 1.5.8. *Sia $(E, \mathcal{I})$ un matroide, e sia $c : E \to \mathbb{R}$ allora l'argoritmo greedy 1.1 restituisce una base di costo massimo e quindi risolve il problema 1.5.3.*

Corollario 1.5.9. Se $(E, \mathcal{I})$ è un matroide e $c : E \to \mathbb{R}_{\geq 0}$ allora 1.1 risolve il problema 1.5.2.

Dimostrazione.
Sia $E = \{e_1, e_2, \ldots, e_n\}$ ordinati in senso decrescente, sia $r = r(E)$ e chiamiamo $A = \{e_{n_1}, e_{n_2} \ldots e_{n_r}\}$ la base restituita da 1.1, supponiamo per assurdo che esista un'altra base $B = \{e_{m_1}, e_{m_2} \ldots e_{m_r}\}$ con $C(B) > C(A)$. Supponiamo di avere gli elementi di A e B ordinati in ordine decrescente per costo, ovvero $c(e_{n_i}) \geq c(e_{n_j})$ e $n_i < n_j$ per $i < j$, e similmente, $c(e_{m_i}) \geq c(e_{m_j})$ e $m_i < m_j$. Dato che $\sum_{i=1}^{r} c(e_{n_i}) < \sum_{i=1}^{r} c(e_{m_i})$ allora esiste i per cui $c(e_{m_i}) > c(e_{n_i})$, supponiamo che j sia il minimo indice con questa proprietà.
Per la minimalità di j sappiamo che $c(e_{n_i}) \geq c(e_{m_i})$ e quindi $n_i \geq m_i \ \forall i < j$, inoltre dato che $c(e_{m_i}) \geq c(e_{m_j}) \ \forall i < j$ allora $c(e_{m_i}) > c(e_{n_j}) \ \forall i < j$. Siano $A_k = \{e_{n_i} : i \leq k\} \subset A$, $B_k = \{e_{m_i} : i \leq k\} \subset B$ gli insiemi contenenti i primi k elementi di A e B.
Notiamo che $|B_j| = |A_{j-1}|+1$ dunque $\exists \bar{k} : 1 \leq \bar{k} \leq j$ per cui $A_{j-1} \neq A_{j-1} \cup \{e_{m_{\bar{k}}}\} \in \mathcal{I}$. Per quando detto sopra $c(e_{m_{\bar{k}}}) > c(e_{n_j})$ da cui $m_{\bar{k}} > n_j$, ma allora l'algoritmo greedy al passo $m_{\bar{k}}$ avrebbe dovuto aggiungere $e_{m_{\bar{k}}}$ alla base che stava costruendo, infatti se $A_{j-1} \cup \{e_{m_{\bar{k}}}\} \in \mathcal{I}$ lo stesso quale per $A_{m_{\bar{k}}} \cup \{e_{\bar{k}}\}$ che è un suo sottoinsieme, con $A_{m_{\bar{k}}}$ la versione di A al passo $m_{\bar{k}}$-esimo. Questa è una contraddizione. □

Teorema 1.5.10. *Sia $(E, \mathcal{I})$ un sistema di indipendenza, se per ogni funzione costo $c : E \to \mathbb{R}$ l'argoritmo greedy 1.1 risolve il problema 1.5.3, allora $(E, \mathcal{I})$ è un matroide.*

Dimostrazione.
Dobbiamo verificare che valga la proprietà (1.2.1:3), supponiamo dunque per assurdo che esistano due insiemi $A, B \in \mathcal{I}$ per cui $|A| = |B| + 1$ ma tali che $B \cup \{x\} \notin \mathcal{I}$

per ogni $x \in A \setminus B$, in questo caso $B \not\subseteq A$.
Notiamo che $A = (A \cap B) \sqcup (A \setminus B)$, da cui $|A| = |A \cap B| + |A \setminus B|$, dunque $|A \setminus B| = |B| + 1 - |A \cap B|$ e analogamente $|B \setminus A| = |B| - |A \cap B|$. Da questo $|A \setminus B| = |B \setminus A| + 1$ e $\frac{1}{|B\setminus A|} > \frac{1}{|A\setminus B|}$.
Per mostrare l'assurdo esibiamo una funzione costo per cui l'algoritmo greedy non trova la base di costo massimo. Sia $\epsilon > 0$ tale che $\frac{1+2\epsilon}{|A\setminus B|} < \frac{1}{|B\setminus A|}$. Tale ϵ esiste perché basta scegliere $\epsilon < \frac{1}{2}(\frac{|A\setminus B|}{|B\setminus A|} - 1) = \frac{1}{2|B\setminus A|} > 0$. Sia poi

$$c : E \to \mathbb{R}_+ \qquad c(e) = \begin{cases} 2 & \text{se } e \in (A \cap B) \\ \frac{1}{|B\setminus A|} & \text{se } e \in (B \setminus A) \\ \frac{1+2\epsilon}{|A\setminus B|} & \text{se } e \in (A \setminus B) \\ \frac{\epsilon}{|A\setminus B|\cdot|(A\cup B)^c|} & \text{se } E \neq (A \cup B) \text{ e } e \notin (A \cup B) \end{cases}$$

Dato che $\frac{1}{|B\setminus A|} \leq 1 < 2$ allora $c(x) > c(y)\ \forall x \in (A \cap B), y \in (B \setminus A)$. Dato che $\frac{1}{|B\setminus A|} > \frac{1+2\epsilon}{|A\setminus B|}$ allora $c(y) > c(z)\ \forall y \in (B \setminus A), z \in (A \setminus B)$. Dato che $\frac{1+2\epsilon}{|A\setminus B|} > \frac{\epsilon}{|A\setminus B|} \geq \frac{\epsilon}{|A\setminus B|\cdot|(A\cup B)^c|}$ allora $c(z) > c(t)\ \forall z \in (A \setminus B), t \notin (A \cup B)$.
Se applichiamo l'algoritmo greedy 1.1 allora nell'ordinamento iniziale di E troviamo, in successione, gli elementi di $(A \cap B)$, $(B \setminus A)$, $(A \setminus B)$, $(A \cup B)^c$. Dato che $B = (A \cap B) \cup (B \setminus A)$ è indipendente, nei primi passi dell'algoritmo aggiungiamo alla base che stiamo costruendo tutti gli elementi di $(A \cap B)$ e $(B \setminus A)$ fino ad ottenere B, poi non aggiungiamo nessun elemento di $(A \setminus B)$, infatti abbiamo ipotizzato che $B \cup \{x\} \notin \mathcal{I} \forall x \in A \setminus B$, successivamente aggiungiamo qualche elemento di $(A \cup B)^c$ fino ad ottenere una base che sarà restituita dall'algoritmo, la chiamiamo B_g.
Per mostrare l'assurdo dobbiamo esibire una base con un costo maggiore di B_g, calcoliamo il costo

$$\begin{aligned} C(B_g) &= \sum_{e\in B_g} c(e) = \sum_{e\in(B\cap A)} c(e) + \sum_{e\in(B\setminus A)} c(e) + \sum_{e\in(B\cup A)^c\cap B_g} c(e) \\ &= 2\,|A \cap B| + \frac{1}{|B \setminus A|} \cdot |B \setminus A| + \frac{\epsilon}{|A \setminus B|\,|(A \cup B)^c|} \cdot |(B \cup A)^c \cap B_g| \\ &\leq 2\,|A \cap B| + 1 + \frac{\epsilon}{|A \setminus B|} < 2\,|A \cap B| + 1 + \epsilon. \end{aligned}$$

Sia ora B_m una base che contiene A, voglio mostrare che $C(B_m) > C(B_g)$

$$\begin{aligned} C(B_m) &= \sum_{e\in B_m} c(e) > \sum_{e\in A} c(e) = \sum_{e\in(B\cap A)} c(e) + \sum_{e\in(A\setminus B)} c(e) \\ &= 2\,|A \cap B| + |A \setminus B| \cdot \frac{1+2\epsilon}{|A \setminus B|} \\ &= 2\,|A \cap B| + 1 + 2\epsilon > 2\,|A \cap B| + 1 + \epsilon > C(B_g). \end{aligned}$$

Quindi l'algoritmo greedy fallisce contraddicendo le ipotesi. □

Osserviamo che è possibile usare l'algoritmo greedy 1.1 per risolvere il problema 1.5.3 nella versione di minimo semplicemente invertendo l'ordinamento iniziale degli elementi. Infatti minimizzare la funzione costo c è equivalente a massimizzazione $-c$ che da un ordinamento iniziale opposto a quello di c.

Notiamo inoltre che aggiungendo all'istruzione 3 una verifica sulla non negatività di $c(e_i)$ è possibile trovare l'indipendenze di costo massimo anche quando c è non sempre positiva.

Mostriamo ora, tramite la dualità, come gli algoritmi 1.1 e 1.2 per matroidi siamo equivalenti.

Lemma 1.5.11. *Dare un sistema di indipendenza $(E, \mathcal{I})$ tramite oracolo di indipendenza è equivalente a dare un oracolo di basis-superset per il suo duale.*

Dimostrazione. Supponiamo di voler sapere, dato $A \subseteq E$ se $\exists B \in \mathcal{B}^*$ tale che $B \subseteq A$, mostriamo che basta verificare che $A^c \in \mathcal{I}$. Infatti $A^c \in \mathcal{I}$ se e solo se $\exists B' \in \mathcal{B}$ tale che $A^c \subseteq B'$, da cui $\exists B = B'^c \in \mathcal{B}^*$ per cui $B'^c \subseteq (A^c)^c = A$.
Similmente se volessimo sapere se $A \in \mathcal{I}$ possiamo invertire i passaggi e ricondurci a verificare che $\exists B \in \mathcal{B}^*$ per cui $B \subseteq A^c$. □

Lemma 1.5.12. *Applicare l'algoritmo 1.2 dato un sistema di indipendenza $(E, \mathcal{I})$ e una funzione c è equivalente ad applicare l'algoritmo 1.1 a $(E, \mathcal{I}^*)$ con funzione costo $-c$. Ovvero se 1.2 restituisce $B \in \mathcal{B}$ allora 1.1 restituisce B^c.*

Dimostrazione. Mostriamo che gli ordinamenti iniziali sono i medesimi e che ad ogni passo dei successivi $U^c = A$ con U e A negli algoritmi 1.2 e 1.1 rispettivamente.
Se $c(e_i) \leq c(e_j)$ allora $(-c)(e_i) \geq (-c)(e_j)$.
Inizialmente $A = \emptyset$ e $U = E$, quindi $U^c = A$. Ad ogni passo successivo e_i viene tolto da U se $U \setminus \{e_i\}$ contiene una base e viene aggiunto solo se $A \cup \{e_i\}$ è un indipendente del duale, ma abbiamo mostrato che queste condizioni sono equivalenti. Inoltre $(U \setminus \{e_i\})^c = U^c \cup \{e_i\} = A \cup \{e_i\}$. Quindi la proprietà $U^c = A$ rimane valida anche per le nuove versioni di U e A. □

Corollario 1.5.13. I teoremi 1.5.8 e 1.5.10 sono validi anche usando l'algoritmo 1.2. Ovvero $(E, \mathcal{I})$ è un matroide se e solo se per ogni funzione costo l'algoritmo 1.2 trova la base di costo massimo/minimo.

Esempio 1.5.14 (Algoritmo di Kruskal). Riprendiamo l'esempio 1.5.6 per mostrare come l'algoritmo greedy consenta di risolverlo in tempo quadratico.
Se $G = (V, E)$ è connesso allora il problema dell'albero ricoprente di costo minimo è equivalente e trovare la base di costo minimo di $M = (E, \mathcal{I} = \{A \subseteq E : A \text{ è albero}\})$ che abbiamo detto essere un matroide. Possiamo quindi applicare l'algoritmo greedy.

Notiamo che, dato $S \subseteq E$, verificare che S sia un albero o meno richiede un tempo che è lineare nella cardinalità di S, ovvero in numero di operazioni necessarie sta in $O(|S|)$. Basta fare una ricerca in profondità o in ampiezza per ogni componente connessa (sono presenti cicli se e solo se la ricerca torna nuovamente su un nodo già visitato).
Scriviamo quindi l'algoritmo:

1. Ordiniamo $e_1, e_2, e_3 \dots e_n$ di modo che $c(e_1) \geq c(e_2) \geq \cdots \geq c(e_n)$.
2. Poniamo $S \leftarrow \emptyset$, $i \leftarrow 1$
3. Per $1 \leq i \leq n$ facciamo:
   (a) Controlliamo se $S \cup \{e_i\}$ contiene un ciclo, se non ne contiene poniamo $S \to S \cup \{e_i\}$
4. Restituiamo S

Il teorema 1.5.8 ci assicura che S sarà l'albero ricoprente di costo minimo (*minimum spanning tree*)

Capitolo 2

Intersezione di matroidi

Il tema principale di questo capitolo è cercare di ottimizzare contemporaneamente su più matroidi. Presentiamo principalmente risultati riguardanti l'intersezione di due matroidi, nella sezione 2.1.1 un importante risultato teorico [4] e successivamente due algoritmi [3] [5] per risolvere il problema in tempo polinomiale.

Esempio 2.0.1. Sia $D = (V, E)$ un grafo orientato, possiamo partizionare gli archi E di G in base al nodo di G in cui entrano ed ottenere la partizione $\mathcal{V}^+ = \{\delta_D^+(v) : v \in V\}$ di E. $M = (E, \{U \subseteq E : d^+_{(V,U)}(v) \leq 1 \, \forall v \in V\})$ è un matroide partizione per la partizione $\mathcal{V}^+$, in particolare U è indipendente se da ogni nodo esce al più un arco di U.
Similmente dato un grafo G bipartito in $V = A \sqcup B$ anche $M_A = (E, \{U \subseteq E : d_G(v) \leq 1 \, \forall v \in A\})$ e $M_B = (E, \{U \subseteq E : d_G(v) \leq 1 \, \forall v \in B\})$ sono due matroidi, rispettivamente matroidi partizione per $\{\delta_G(v) : v \in A\}$ e $\{\delta_G(v) : v \in B\}$.
Ogni insieme di archi indipendente sia per M_A che per M_B è un matching, infatti $|U \cap \delta_G(v)| \leq 1$ per ogni vertice, quindi in ogni vertice arriva al più un arco di U, questo ci suggerisce che un problema sui matching del grafo G possa essere affrontato come problema sugli indipendenti comuni di M_A e M_B.
In particolare trovare un matching massimale si riconduce a trovare un insieme indipendente sia per M_A che per M_B di cardinalità massima.

Ora definiremo l'intersezione di due o più matroidi. Mostreremo che in generale non è un matroide. Affronteremo poi il problema di trovare un elemento di cardinalità massima nell'intersezione di due o più matroidi.

2.1 Definizione

Definizione 2.1.1 (Intersezione di matroidi)**.**
Siano $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2), \ldots, M_n = (E, \mathcal{I}_n)$ dei matroidi su E. L'interse-

zione di questi matroidi è la coppia

$$M_1 \cap M_2 \cap \dots M_n = \left(E, \bigcap_{i=1}^{n} \mathcal{I}_i \right).$$

Proposizione 2.1.2. *Siano $M_1, M_2, \dots M_n$ matroidi con $M_i = (E, \mathcal{I}_i)$, allora $\bigcap_{1 \leq i \leq n} M_i$ è un sistema di indipendenza.*

Dimostrazione. Devo verificare che $\mathcal{I} = \bigcap_{i \leq i \leq n} \mathcal{I}_i$ contenga $\emptyset$ e sia chiuso per sottoinsiemi.
(1) $\emptyset \in \mathcal{I}_i$ per ogni i, quindi $\emptyset \in \mathcal{I}$
(2) Se $A \in \mathcal{I}$ e $B \subseteq A$, allora $A \in \mathcal{I}_i$ per ogni i, quindi $B \in \mathcal{I}_i$ per ogni i, dunque $B \in \mathcal{I}$. □

Esempio 2.1.3. L'intersezione di matroidi è quindi un sistema di indipendenza, ma, in generale, non un matroide.
Mostriamo ora un grafo $G = (A \cup B, E)$ per cui l'intersezione $M_A \cap M_B$ come nell'esempio 2.0.1 non rispetta la proprietà (1.2.1:3).
Sia $G = (\{1,2,3,4\}, \{12, 23, 34\})$ con $A = \{1,3\}, B = \{2,4\}$, sia $M_A = (E, \mathcal{I}_A), M_B = (E, \mathcal{I}_B)$, allora

$$\mathcal{I}_A = \{\emptyset, \{12\}, \{12,23\}, \{23\}, \{12,34\}, \{34\}\} \quad \mathcal{I}_B = \{\emptyset, \{12\}, \{23\}, \{34\}, \{12,34\}\}.$$

Perciò $\mathcal{I}_A \cap \mathcal{I}_B = \{\emptyset, \{12\}, \{23\}, \{34\}, \{12,34\}\}$. Notiamo che $A = \{12,34\}$ e $B = \{23\}$ verificano l'ipotesi $|A| > |B|$ ma né $\{23,34\}$ né $\{23,12\}$ stanno in $\mathcal{I}_A \cap \mathcal{I}_B$. Quindi $M_A \cap M_B$ non può essere un matroide.

Tuttavia intersecando con un matroide uniforme si ottiene sempre un matroide.

Proposizione 2.1.4. *Se $M = (E, \mathcal{I})$ è un matroide e $U_{n,r} = (E, \mathcal{U})$ un matroide uniforme con $0 \leq r \leq n = |E|$. Allora l'intersezione $M \cap U_{n,r}$ è un matroide.*

Dimostrazione. Per la proposizione 2.1.2 so che $M \cap U_{n,r}$ è un sistema di indipendenza quindi verifica le proprietà (1) e (2) della definizione di matroide 1.2.1. Dimostro che verifica anche la proprietà (3).
(3) Siano $A, B \in (\mathcal{I} \cap \mathcal{U})$ e $|A| > |B|$. Dato che $A \in \mathcal{U}$, allora $|A| \leq r$, inoltre, visto che $A, B \in \mathcal{I}$ esiste $x \in A \backslash B$ per cui $B \cup \{x\} \in \mathcal{I}$, ma $|B \cup \{x\}| = |B| + 1 \leq |A| \leq r$ per cui $B \cup \{x\} \in \mathcal{U}$ e quindi $B \cup \{x\}$ è un indipendente di $M \cap U_{n,r}$. □

Problema 2.1.5 (Problema dell'intersezione di matroidi)**.**
Siano $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$ matroidi.
Obiettivo: Trovare un insieme $X \in \mathcal{I}_1 \cap \mathcal{I}_2$ tale che $|X|$ sia massimo.

2.1.1 Teorema dell'intersezione di matroidi

Teorema 2.1.6 (Teorema dell'intersezione di matroidi)**.**
Siano $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$ due matroidi con funzioni rango r_1 e r_2. Allora la massima cardinalità di un elemento di $M_1 \cap M_2$ è il minimo di $(r_1(U) + r_2(U^c))$ per $U \subseteq E$

$$\max_{A \in \mathcal{I}_1 \cap \mathcal{I}_2} |A| = \min_{U \subseteq E} \big(r_1(U) + r_2(U^c)\big). \tag{2.1}$$

Dimostrazione. Sia $m = \min_{U \subseteq E} \big(r_1(U) + r_2(U^c)\big)$.
Se $|E| = 1$, allora ho poche possibilità. Queste sono $M_1 = M_2 \cong \mathcal{U}_{0,0}$, $M_1 = M_2 \cong \mathcal{U}_{1,0}$, $M_1 \cong \mathcal{U}_{1,1}, M_2 \cong \mathcal{U}_{1,0}$, $M_1 \cong M_2 \cong \mathcal{U}_{1,1}$. In tutti casi eccetto l'ultimo l'indipendente comune massimale è $\emptyset$ e scegliendo $U = \emptyset$ si ottiene $r_1(U)+r_2(U^c) = 0$, nell'ultimo caso l'indipendente comune massimale è E e per $U \in \{\emptyset, E\}$ trovo $r_1(U) + r_2(U^c) = 1 = |E|$. Continuiamo ora la dimostrazione per $|E| \geq 2$.
Sia A un insieme indipendente comune e sia $U \subseteq E$. Dato che sono contenuti in A, allora $A \cap U$ e $A \setminus U$ sono pure indipendenti comuni, e sono disgiunti. Essendo indipendenti il loro rango è pari alla loro cardinalità. Quindi

$$|A| = |A \cap U| + |A \setminus U| = r_1(A \cap U) + r_2(A \setminus U) \leq r_1(U) + r_2(E \setminus U).$$

Dunque $|A| \leq m$ per ogni indipendente comune.
Ora mostriamo per induzione su $|E|$ che esiste un indipendente comune di cardinalità proprio m. Il passo base è dato dai casi $|E| \leq 1$. Trattiamo separatamente due casi.
Caso 1: m è ottenuto solo per E o $\emptyset$, ovvero $m < \big(r_1(U) + r_2(U^c)\big)\, \forall U \notin \{E, \emptyset\}$.
Sia $e \in E$ e sia $U \subseteq (E \setminus \{e\})$. $E \setminus \{e\} \neq \emptyset$ perché $|E| \geq 2$. Se $U \neq \emptyset$, allora $m < r_1(U) + r_2(U^c) \leq r_1(U) + r_2(U^c \setminus \{e\}) + 1$, da cui segue $m \leq r_1(U) + r_2((E \setminus \{e\}) \setminus U)$. Se $U = \emptyset$ vale comunque che $m \leq r_1(\emptyset) + r_2(E \setminus \{e\})$ perché $m < r_1(e) + r_2(E \setminus \{e\}) \leq 1 + r_2(E \setminus \{e\}) = r_1(\emptyset) + r_2(E \setminus \{e\}) + 1$. Riassumendo $m \leq r_1(U) + r_2((E \setminus \{e\}) \setminus U)$ per ogni $U \subseteq (E \setminus \{e\})$.
Notiamo che o $\emptyset$ o $E \setminus \{e\}$ realizzano l'uguaglianza perché, se $m = r_1(\emptyset) + r_2(E)$ allora $m \geq r_1(\emptyset)+r_2(E\setminus\{e\})$, e se $m = r_1(E)+r_2(\emptyset)$ allora $m \geq r_1(E\setminus\{e\})+r_2(\emptyset)$. Quindi $m = \min_{U \subseteq (E\setminus\{e\})} r_1(U) + r_2((E \setminus \{e\}) \setminus U)$. Per induzione deduciamo che esiste un indipendente di cardinalità m comune ai matroidi $M_1 \setminus \{e\}$ e $M_2 \setminus \{e\}$. Lo stesso insieme è anche un indipendente di $M_1 \cap M_2$.
Caso 2: Esiste $U \notin \{E, \emptyset\}$ per cui $m = \big(r_1(U) + r_2(U^c)\big)$.
Consideriamo i matroidi $M_1' = (M_1 \setminus U^c)$ e $M_2' = (M_2/U^c)$ e le rispettive funzioni rango r_1' e r_2'. Vale che per $T \subseteq U$ $r_1'(T) = r_1(T)$ e $r_2'(T) = r_2(T \cup U^c) - r_2(U^c)$.
Sia $T \subseteq U \subseteq E$, U realizza il minimo m quindi $m = r_1(U) + r_2(U^c) \leq r_2(T) + r_2(T^c)$. Quindi $r_1(U) \leq r_1(T) + r_2(T^c) - r_2(U^c) = r_1'(T) + r_2'(U \setminus T)$. Inoltre $r_1(U) = \min_{T \subseteq U} \big(r_1'(T) + r_2'(U \setminus T)\big)$ perché l'espressione valutata con $T = U$ realizza il minimo.

Per induzione quindi $M_1' \cap M_2'$ contiene un indipendente A con $|A| = r_1(U)$.
Analogamente consideriamo $M_1'' = (M_1/U)$ e $M_2'' = (M_2 \setminus U)$ e troviamo un indipendente comune B in $M_1'' \cap M_2''$ con $|B| = r_2(U^c)$.
Ora dimostriamo che $A \cup B$ è un indipendente di $M_1 \cap M_2$. A è un indipendente di $(M_1 \setminus U^c)$ quindi è contenuto in una base X di U, B è un indipendente di (M_1/U) quindi per il corollario 1.4.11 $B \cup X \in \mathcal{I}_1$ e quindi $A \cup B \in \mathcal{I}_1$. Similmente A è indipendente in (M_2/U^c) e B di $(M_2 \setminus U)$ dunque $A \cup B \in \mathcal{I}_2$.
Dato che sono insiemi disgiunti, $|A| = r_1(U)$ e $|B| = r_2(U^c)$, allora $|A \cup B| = r_1(U) + r_2(U^c) = m$. □

2.2 Algoritmo classico

Introduciamo alcune notazioni. Dati $M_1 = (E, \mathcal{I}_1)$, $M_2 = (E, \mathcal{I}_2)$ due matroidi, e $A \in \mathcal{I}_1 \cap \mathcal{I}_2$, sia $D_{M_1,M_2}(A) = (E, E(D))$ un grafo orientato su E, con

$$E(D) = \{(x,y) \in A \times A^c : (A \setminus \{x\} \cup \{y\}) \in \mathcal{I}_1\} \cup \{(y,x) \in A^c \times A : (A \setminus \{x\} \cup \{y\}) \in \mathcal{I}_2\}.$$

Dato un grafo ed un cammino $P = \{v_0, e_1, v_1, e_2 \dots e_k, v_k\}$ del grafo indichiamo con $V(P)$ i vertici del cammino ovvero $V(P) = \{v_0, v_1, \dots v_k\}$ con $e_i = (v_{i-1}, v_i)$.

Presentiamo ora un algoritmo che risolve il problema 2.1.5 restituendo un insieme A indipendente di cardinalità massima comune a due matroidi dati.

Algoritmo 2.1 (Algoritmo classico (Edmonds) per intersezione di due matrodi)**.**

Siano dati due matroidi $M_1 = (E, \mathcal{I}_1)$ e $M_2 = (E, \mathcal{I}_2)$ tramite oracolo di indipendenza.
Algortimo:

- *Inizializza ponendo $A \leftarrow \emptyset$*
- *Continua a ripetere:*
  1. *$V_1 \leftarrow \{e \in A^c : A \cup \{e\} \in \mathcal{I}_1\}$*
  2. *$V_2 \leftarrow \{e \in A^c : A \cup \{e\} \in \mathcal{I}_2\}$*
  3. *$G \leftarrow D_{M_1,M_2}(A)$*
  4. *Trova un cammino P in D di lunghezza minima che inizi in V_1 e che termini in V_2*
     (a) *Se un cammino di questo tipo esiste poni $A \leftarrow A \triangle V(P)$*
     (b) *Se non esiste termina il ciclo*
- *Restituisci l'insieme A*

Per dimostrare la correttezza dell'algoritmo occorre dimostrare che $A \in \mathcal{I}_1 \cap \mathcal{I}_2$ e che A ha cardinalità massima, ovvero, per il teorema 2.1.6, che $|A| = \min_{U \subseteq E} \big(r_1(U) + r_2(U^c)\big)$.

Lemma 2.2.1. *Sia $M = (E, \mathcal{I})$ un matroide, $A \in \mathcal{I}$, $x_1, x_2 \dots x_s \in A$ elementi di A e $y_1, \dots y_s \notin A$ elementi del complementare di A. Se valgono queste proprietà:*

1. *$(A \cup \{y_i\} \setminus \{x_i\}) \in \mathcal{I}$ per ogni $1 \leq i \leq s$*
2. *$(A \cup \{y_i\} \setminus \{x_j\}) \notin \mathcal{I}$ per ogni $1 \leq j < i \leq s$*

allora $(A \cup \{y_1, \dots y_s\} \setminus \{x_1, \dots x_s\}) \in \mathcal{I}$.

Dimostrazione. Per $1 \leq r \leq s$ sia $A_r = (A \cup \{y_1, \dots y_r\} \setminus \{x_1, \dots x_r\})$, dimostriamo la tesi dimostrando per induzione che $A_r \in \mathcal{I}$.
Il passo $r = 1$ è ovvio per l'ipotesi (1) con $i = 1$.
Sia ora $1 < r \leq s$, assumiamo $A_{r-1} \in \mathcal{I}$. Notiamo che $A_r = A_{r-1} \cup \{y_r\} \setminus \{x_r\}$.
Se $A_{r-1} \cup \{y_r\} \in \mathcal{I}$, allora da $A_r \subseteq A_{r-1} \cup \{y_1\}$ segue l'indipendenza di A_r.
Supponiamo quindi che $A_{r-1} \cup \{y_r\}$ sia dipendente. Notiamo che $A \cup \{y_r\}$ non è indipendente perché contiene $(A \cup \{y_r\} \setminus \{x_j\})$ per ogni $j < r$ se $r > 1$.
Per il teorema 1.4.4 $A \cup \{y_r\}$ contiene un unico circuito C, questo circuito non contiene nessun x_j, $j < r$, se fosse diversamente infatti avremmo $(A \cup \{y_i\} \setminus \{x_j\}) \in \mathcal{I}$, che contraddice (2). Inoltre per (1) $x_r \in C$. Quindi C è contenuto in $(A \cup \{y_r\} \setminus \{x_j : j < r\}) \subseteq (A_{r-1} \cup \{y_r\})$. Dato che $C \subseteq A_{r-1} \cup \{y_r\}$ per il teorema 1.4.4 C è l'unico circuito contenuto in $A_{r-1} \cup \{y_r\}$ e dato che $x_r \in C$, allora $A_{r-1} \cup \{y_r\} \setminus \{x_r\}$ è indipendente. □

Proposizione 2.2.2. *Nell'algoritmo 2.1, ad ogni iterazione del ciclo l'insieme A è un indipendente comune di M_1, sia di M_2.*

Dimostrazione che $A \in \mathcal{I}_1$.
$\emptyset \in \mathcal{I}_1$, quindi possiamo supporre per induzione che $A \in \mathcal{I}_1$ e cercare di dimostrare che A rimane indipendente anche dopo il passo 4a, ovvero che $A \triangle V(P) \in \mathcal{I}_1$.
Se $P = \{e\}$, $e \in E = V(D)$, allora $e \in (V_1 \cap V_2)$ e perciò $A \triangle \{e\} = A \cup \{e\} \in \mathcal{I}_1 \cap \mathcal{I}_2$.
Supponiamo quindi che P abbia lunghezza positiva.
Notiamo innanzitutto che $D_{M_1,M_2}(A)$ è un grafo bipartito, infatti $E(D) \subseteq (A \times A^c) \cup (A^c \times A)$, ovvero non esistono archi fra nodi di A^c e fra nodi di A, per definizione. Quindi ogni percorso alterna nodi in A e nodi in A^c, supponiamo che inizi con $y_0 \in V_1 \subseteq A^c$ termini con $y_s \in V_2 \subseteq A^c$ e sia $V(P) = \{y_0, x_1, y_1, \dots x_s, y_s\}$ con $x_i \in A, y_i \in A^c$.
Cerchiamo di mostrare che $A \triangle V(P) = A \setminus \{x_i : 1 \leq i \leq s\} \cup \{y_i : 0 \leq i \leq s\} = (A \cup \{y_0\}) \setminus \{x_i : 1 \leq i \leq s\} \cup \{y_i : 1 \leq i \leq s\} \in \mathcal{I}_1$ verificando le condizioni del lemma 2.2.1.

$(A \cup \{y_0\}) \in \mathcal{I}_1$ perché $y_0 \in V_1$.
(2.2.1:1) Dimostriamo $((A \cup \{y_0\}) \cup \{y_i\} \setminus \{x_i\}) \in \mathcal{I}$ per ogni i. Dato che $(x_i, y_i) \in D(A)$, allora per definizione $A \cup \{y_i\} \setminus \{x_i\} \in \mathcal{I}$, ma $|A \cup \{y_0\}| > |A \cup \{y_i\} \setminus \{x_i\}| = |A|$ quindi esiste e nella differenza dei due insiemi tale che se aggiunto e ad $A \cup \{y_i\} \setminus \{x_i\}$ l'unione è ancora un indipendente. $(A \cup \{y_0\}) \setminus (A \cup \{y_i\} \setminus \{x_i\}) = \{y_0, x_i\}$. Se avessi che $(A \cup \{y_i\} \setminus \{x_i\}) \cup \{x_i\} = A \cup \{y_i\} \in \mathcal{I}_1$, allora $y_i \in V_1$, ma avrei quindi potuto scegliere di far partire il cammino P da y_i, e questo viola la minimalità di P. Quindi $A \cup \{y_i\} \notin \mathcal{I}_1$ e allora $(A \cup \{y_i\} \setminus \{x_i\} \cup \{y_0\}) \in \mathcal{I}_1$.
(2.2.1:2) Dimostriamo $((A \cup \{y_0\}) \cup \{y_i\} \setminus \{x_j\}) \notin \mathcal{I}_1$ per ogni $j < i$. Se esistessero, $j, i : j < i$ per cui $((A \cup \{y_0\}) \cup \{y_i\} \setminus \{x_j\}) \in \mathcal{I}_1$, allora $(A \cup \{y_i\} \setminus \{x_j\}) \in \mathcal{I}_1$ e $(x_j, y_i) \in D(A)$, potrei quindi scegliere un cammino più contro scegliendo (x_j, y_i) anziché $(x_j, y_j), (y_i, x_{j+1}) \ldots, (x_i, y_i)$, violando la minimalità di P.
Per il lemma 2.2.1 quindi $A \triangle V(P) \in \mathcal{I}_1$. □

Dimostrazione che $A \in \mathcal{I}_2$. Ripeto la dimostrazione come sopra per induzione, solamente che uso il lemma 2.2.1 al contrario. Ovvero, dato che $y_s \in V_2$ allora $(A \cup \{y_s\}) \in \mathcal{I}_2$, dimostro quindi come sopra che gli insiemi $\{x_s, x_{s-1}, \ldots x_1\}$ e $\{y_{s-1}, \ldots y_1, y_0\}$ verificano le ipotesi del lemma. □

Proposizione 2.2.3. *Arrivati al passo 4 dell'algoritmo 2.1 se in $D_{M_1,M_2}(A)$ non esiste alcun cammino da V_1 a V_2, allora $|A| = \min_{U \subseteq E} \big(r_1(U) + r_2(U^c)\big)$.*

Dimostrazione.
Sia U l'insieme dei vertici raggiungibili da V_1, ovviamente $V_1 \subseteq U$ e dato che per ipotesi non esiste nessun cammino da V_1 e V_2, allora U e V_2 sono disgiunti.
Supponiamo che $r_2(U) > |A \cap U|$, allora U contiene un indipendente più grande di $(A \cap U) \in \mathcal{I}_2$, quindi esiste $y \in (U \setminus A)$ per cui $A \cap U \cup \{y\} \in \mathcal{I}_2$. Dato che U e V_2 sono disgiunti segue che $y \notin V_2$ e quindi $A \cup \{y\} \notin \mathcal{I}_2$, allora $A \cup \{y\}$ contiene un solo circuito che deve contenere almeno un elemento di $x \in A \setminus U$ (infatti se fosse contenuto interamente in $A \cap U \cup \{y\}$, allora questo non sarebbe indipendente). Quindi $A \cup \{y\} \setminus \{x\} \in \mathcal{I}_2$ dato che contiene nessun circuito e allora $(y, x) \in D_{M_1,M_2}(A)$, ma $y \in U$ e $x \notin V$, questo viola la definizione di U. Concludiamo che $r_2(U) \leq |A \cap U|$.
Allo stesso modo dimostriamo che $r_1(U^c) \leq |A \setminus U|$.
Otteniamo infine che $|A| \geq r_1(U^c) + r_2(U)$, e dato che $A \in \mathcal{I}_1 \cap \mathcal{I}_2$, allora per il teorema 2.1.6 possiamo concludere. □

Teorema 2.2.4. *Il problema 2.1.5 può essere risolto in tempo polimoniale.*

Dimostrazione. Per le proposizioni 2.2.2 e 2.2.3 l'algoritmo 2.1 trova un indipendente comune di cardinalità massima, mostriamo che impiega un tempo polinomiale.
Dato che $V(P) \setminus A \neq \emptyset$ allora $|V(P) \triangle A| > |A|$ e dato che $A \subseteq E$ allora il ciclo

$1 \to 4$ è ripetuto al più $|E|$ volte.
Se chiamiamo θ la complessità computazione del più "lento" degli oracoli, allora possiamo costruire gli insiemi V_1 e V_2 in tempo $O(|E \setminus A|\,\theta)$, basta controllare l'indipendenza di $A \cup \{e\}$ per ogni $e \in A^c$ usando l'oracolo.
Costruiamo il grafo nel passo 3 in tempo $O(|E \setminus A|\,|A|\,\theta)$ controllando per ogni $x \in A$ e ogni $y \in E \setminus A$ se gli archi $(x, y), (y, x)$ sono archi del grafo usando l'oracolo.
Il passo 4 può essere completato in tempo $O(|E|)$ usando una ricerca in ampiezza. □

2.3 Algoritmo con PSR

Mostriamo ora un algoritmo alternativo [5] a quello di Edmonds .

Definizione 2.3.1 (PSR)**.** Sia E un insieme e $\mathcal{S} = \{S_i\}_{1 \le i \le n}$ una partizione di E, consideriamo il matroide partizione di E i cui indipendenti contengono al più un solo elemento di ogni S_i, chiamiamo *insieme parziale di rappresentanti rispetto a* $\mathcal{S}$ (che abbrevieremo con la abbreviazione inglese *psr*) ogni indipendente di questo matroide.

Proposizione 2.3.2. *La massima cardinalità di un psr contenuto in $U \subseteq E$, ovvero il rango di U per il matroide dei psr , è il numero di elementi della partizione $\mathcal{S}$ non disgiunti da U, $|\{S \in \mathcal{S} : S \cap U \neq \emptyset\}|$*

Dimostrazione. Chiamo $\mathcal{S}_U = \{S \in \mathcal{S} : S \cap U \neq \emptyset\}$, l'insieme degli elementi della partizione *toccati* da U. Possiamo costruire un insieme $B \subseteq U$ tale che $|B \cap S| = 1\ \forall S \in \mathcal{S}_U$ scegliendo un elemento da ogni insieme di $\mathcal{S}_U$. Otteniamo quindi che B è un psr perché $|B \cap S| \le 1\, \forall S \in \mathcal{S}$, inoltre B è una base di U perché comunque aggiungiamo un elemento di $x \in U \setminus B$ a B abbiamo che esiste $S \in S_U$ per cui $x \in (S \cap U)$, quindi avrei $|S \cap U| = 2$. □

Teorema 2.3.3 (di Rado)**.** *Sia $M = (E, \mathcal{I})$ un matroide con funzione rango r, sia $\mathcal{S}$ una partizione di E. La massima cardinalità di un psr indipendente è*

$$\max_{A \in \mathcal{I}, A \text{ psr}} |A| = \min_{\mathcal{Z} \subseteq \mathcal{S}} \left(r\Big(\bigcup_{S \in \mathcal{Z}} S \Big) + |\mathcal{S}| - |\mathcal{Z}| \right). \tag{2.2}$$

Dimostrazione. Sia $M_p = (E, \mathcal{I}_{\mathcal{S}} = \{A \subseteq E : A \text{ psr per } \mathcal{S}\})$ il matroide dei psr di E. Un psr indipendente di M è un elemento indipendente di $M \cap M_p$, cerco quindi di usare il teorema dell'intersezione di matroidi 2.1.6 per dimostrare la tesi.
Per la proposizione 2.3.2 $r_{M_p}(U) = |\mathcal{S}_U| = |\{S \in \mathcal{S} : S \cap U \neq \emptyset\}| = |\{S \in \mathcal{S} : S \not\subseteq U^c\}|$.
Sia $U \subseteq E$, calcolo $r(U) + r_{M_p}(U^c) = r(U) + |\mathcal{S}_{U^c}| = r(U) + |\mathcal{S}| - |\mathcal{S}_U| + |\mathcal{S}_{U,U^c}|$

con $\mathcal{S}_{U,U^c} = \mathcal{S}_U \cap \mathcal{S}_{U^c} = \{S \in \mathcal{S} : S \nsubseteq U, S \nsubseteq (E \setminus U)\}$.
Sia ora $\bar{U} = \bigcup_{S\in\mathcal{S},S\subseteq U} S$, unione di tutti gli elementi di $\mathcal{S}$ contenuti in U. Chiaramente $\bar{U} \subseteq U$. Notiamo inoltre che $\mathcal{S}_{\bar{U}} = \mathcal{S}_U \setminus \mathcal{S}_{U,U^c}$, infatti gli elementi di $\mathcal{S}$ toccati da $\bar{U}$ sono tutti e soli quelli contenuti in U. E anche $\mathcal{S}_{\bar{U},\bar{U}^c} = \emptyset$ infatti se $S \cap \bar{U} \neq \emptyset$ allora $S \subseteq \bar{U}$ e quindi $S \cap \bar{U}^c = \emptyset$
Quindi $r(\bar{U}) + |\mathcal{S}| - |\mathcal{S}_{\bar{U}}| \leq r(U) + |\mathcal{S}| - (|\mathcal{S}_U| - |\mathcal{S}_{U,U^c}|)$. Per questo se cerchiamo il minimo di $(r(U) + r_{M_p}(U^c))$ possiamo limitarci a cercarlo tra quegli insiemi per cui $U = \bar{U}$ ovvero tra le unioni di elementi della partizione $\mathcal{S}$.
Allora per il teorema 2.1.6

$$\begin{aligned}
\max_{A\in\mathcal{I}\cap\mathcal{I}_\mathcal{S}} |A| &= \min_{S\subseteq E} \big(r(U) + r_{M_p}(U^c)\big) \\
&= \min_{\mathcal{Z}\in\mathcal{S}} \left(r\Big(\bigcup_{S\in\mathcal{Z}} S\Big) + r_{M_p}\Big(\bigcup_{S\notin\mathcal{Z}} S\Big)\right) \\
&= \min_{\mathcal{Z}\in\mathcal{S}} \left(r\Big(\bigcup_{S\in\mathcal{Z}} S\Big) + |\mathcal{S}| - |\mathcal{Z}|\right) \qquad \square
\end{aligned}$$

Descriviamo ora un algoritmo che, dato un psr indipendente A, rispetto ad un matroide M ed ad una partizione $\mathcal{S}$, permette di trovare o un psr indipendente A' con $|A'| > |A|$ oppure un insieme $\mathcal{Z}$ che verifica $|A| = \big(r\big(\bigcup_{S\in\mathcal{Z}} S\big) + |\mathcal{S}| - |\mathcal{Z}|\big)$.

Algoritmo 2.2.
Siano dati un matroide $M = (E, \mathcal{I})$ tramite oracolo di indipendenza, una partizione $\mathcal{S}$ di E, un insieme $A \subseteq E$ che sia un psr per $\mathcal{S}$ ed un indipendente per M.
Algortimo:

1. *Se $|A| = |\{S \in \mathcal{S} : S \neq \emptyset\}|$ allora restituisci $\mathcal{Z} \leftarrow \{S \in \mathcal{S} : S = \emptyset\}$*
2. *Altrimenti scegli un elemento $e \in \{e \in S : S \in \mathcal{S}, S \cap A = \emptyset\}$*
3. *Se $A \cup \{e\} \in \mathcal{I}$ restituisci $A' \leftarrow A \cup \{e\}$*
4. *Altrimenti:*
   (a) *Poni $C \leftarrow C_M(A, e)$ l'unico circuito contenuto in $A \cup \{e\}$*
   (b) *$S_C \leftarrow \big(\bigcup_{S\in\mathcal{S},S\cap C\neq\emptyset} S\big) \setminus C$*
   (c) *$\mathcal{S}' \leftarrow \big(\{S \in \mathcal{S} : S \cap C = \emptyset\} \cup \{S_c\}\big)$*
   (d) *$M' \leftarrow M/C$, $A_C \leftarrow A \setminus C$*
   (e) *Applica ricorsivamente questo algoritmo a A_C per i matroide M' e la partizione $\mathcal{S}'$*
   (f) *Se l'algoritmo ritorna un insieme $\mathcal{Z}' \subseteq \mathcal{S}$ allora*

i. Restituisci $\mathcal{Z} \leftarrow \mathcal{Z}' \setminus \{S_C\} \cup \{S \in \mathcal{S} : S \cap C \neq \emptyset\}$

(g) Se l'algoritmo restituisce un psr indipendente A'_C *allora*

i. Trova $y \in C$ *tale che* $A'_C \cup C \setminus \{y\}$ *sia un psr*

ii. Restituisci $A' \leftarrow A'_C \cup C \setminus \{y\}$

Proposizione 2.3.4. *L'algoritmo 2.2 è corretto, ovvero ricevuto un insieme* A*, indipendente di* M *e psr per* $\mathcal{S}$*, restituisce sempre o un psr indipendente* A *di cardinalità* $|A|+1$ *oppure* $\mathcal{Z} \subseteq \mathcal{S}$ *che verifica il minimo nella uguaglianza 2.2 del teorema 2.3.3.*

Dimostrazione. Dimostriamo innanzitutto se che se l'algortimo termina al passo 1 o al passo 3 allora l'output è corretto.
Supponiamo $|A| = |\{S \in \mathcal{S} : S \neq \emptyset\}|$ e quindi $\mathcal{Z} = \{S \in \mathcal{S} : S = \emptyset\}$, ovviamente $\mathcal{S} = \{S \in \mathcal{S} : S \neq \emptyset\} \sqcup \mathcal{Z}$ allora $r(\bigcup_{S\in\mathcal{Z}} S) + |\mathcal{S}| - |\mathcal{Z}| = r(\emptyset) + |\{S \in \mathcal{S} : S \neq \emptyset\}| = |A|$. Se finisco al passo 1 A è un psr indipendente di cardinalità massima.
Essendo A psr, allora $|A| = |\{S \in \mathcal{S} : S \cap A \neq \emptyset\}| \leq |\{S \in \mathcal{S} : S \neq \emptyset\}|$ per la proposizione 2.3.2 . Se quindi $|A| \neq |\{S \in \mathcal{S} : S \neq \emptyset\}|$ allora $|\{S \in \mathcal{S} : S \cap A \neq \emptyset\}| < |\{S \in \mathcal{S} : S \neq \emptyset\}|$, perciò $\{S \in \mathcal{S} : S \cap A = \emptyset, S \neq \emptyset\}$ è non vuoto e posso scegliere un elemento e come al passo 2. Inoltre $e \in \bar{S}$ per qualche $\bar{S} \in \{S \in \mathcal{S} : S \cap A = \emptyset, S \neq \emptyset\}$, ma non è contenuto in altri insiemi di $\mathcal{S}$, dato che $\mathcal{S}$ è una partizione.
$A \cup \{e\}$ è un psr infatti $|S \cap A| = 1$ se $S \in \mathcal{S}_A \cup \{\bar{S}\}$, $|S \cap A| = 0$ altrimenti. Se quindi $A \cup \{e\} \in \mathcal{I}$ allora $A \cup \{e\}$ è psr indipendente di cardinalità $|A \cup \{e\}| = |A| + 1$ e perciò l'algoritmo è corretto se termina al passo 3.
Ora dimostreremo per induzione su $|E|$ che l'algoritmo è corretto in generale.
Se $|E| = 0$ allora $A = \emptyset$, quindi l'algoritmo è corretto perché termina in 1.
Se $|E| \geq 1$ e l'algoritmo non termina in 1 o 3 allora $A \cup \{e\}$ è un psr ma $A \cup \{e\} \notin \mathcal{I}$, quindi per il teorema 1.4.4 esiste un C circuito contenuto in $A \cup \{e\}$. Notiamo che questo circuito può essere costruito partendo da $A \cup \{e\}$ e togliendo gli elementi che non rendono indipendente l'insieme.
Per poter applicare l'algoritmo ricorsivamente nel passo 4e dimostriamo che A_C è un psr indipendente per $\mathcal{S}'$ e M'. $A_C = A \setminus C$ è un indipendente di M/C perché $C \setminus \{e\}$ è una base di C e $(A \setminus C) \cup (C \setminus \{e\}) = A \in \mathcal{I}$. A è un psr, quindi per $S \in \mathcal{S}$ vale $|A \cap S| \leq 1$, in particolare vale per gli S tali che $S \cap C = \emptyset$, per questi vale quindi che $|(A \setminus C) \cap S| \leq 1$. Allo stesso modo abbiamo anche che $|A \cap S| \leq 1$ se $S \cap C \neq \emptyset$, inoltre dato che $C \setminus \{e\} \subseteq A$ allora per ogni S tale che $S \cap C \neq \emptyset$ vale che o $A \cap S = C \cap S$ e $|A \cap S| = 1$ o $C \cap S = \{e\}$ e $|A \cap S| = 0$. Per questo $(A \setminus C) \cap S$ è o $\emptyset$ o $\{e\}$, quindi $S_C \cap A = \left(\bigcup_{S\in\mathcal{S}, S\cap C\neq\emptyset} S\right) \cap C^c \cap A = \left(\bigcup_{S\in\mathcal{S}, S\cap C\neq\emptyset} S \cap A \setminus C\right)$ è o $\{e\}$ o $\emptyset$, quindi $|S_C \cap A| \leq 1$. Quindi A_C è un psr per $\mathcal{S}'$.
Essendo quindi lecita la ricorsione del passo 4e e dato che $|E \setminus C| < |E|$ allora per ipotesi induttiva l'algoritmo produce un risultato corretto.
Notiamo che $|\{S \in \mathcal{S} : S \cap C \neq \emptyset\}| = |C|$ per la proposizione 2.3.2 dato che $A \cup \{e\}$ è un psr e quindi anche C lo è.
Se sono nel caso 4f allora il passo 4e ha prodotto $\mathcal{Z}'$, tale che, chiamato r' il rango

di M', valga $|A_C| = r'\big(\bigcup_{S\in\mathcal{Z}'} S\big) + |\mathcal{S}'| - |\mathcal{Z}'|$.
Dimostriamo che se l'algoritmo restituisce una sottopartizione $\mathcal{Z}$ e se $S\cap A = \emptyset$ per A insieme dato in input all'algoritmo e $S \in \mathcal{S}$ allora $S \in \mathcal{S}$. Se algoritmo restituisce $\mathcal{Z}$ allora è terminato al passo 1 o al passo 4(f)i, ma se è terminato al passo 4(f)i allora ho eseguito ricorsivamente l'algoritmo, dunque devo prima o poi avere terminato una ricorsione al passo 1. Se termino in 1 allora da $S \cap A = \emptyset$ segue $S = \emptyset$ perché A è psr e $|A| = |\{S \in \mathcal{S} : S \neq \emptyset\}|$, quindi $S \in \mathcal{Z} = \{S \in \mathcal{S} : S = \emptyset\}$. Possiamo dunque supporre che se termino al passo 4(f)i per induzione che se $S \cap A_C = \emptyset$ per $S \in \mathcal{S}'$ allora $S \in \mathcal{Z}'$. Ora, sia $S \in \mathcal{S}$, se $S \cap C \neq \emptyset$ allora $S \in \mathcal{S}$, se $S \cap A = \emptyset$ e $S \cap C = \emptyset$ segue $S \setminus C = S$, perciò $S \cap (A \setminus C) = \emptyset$, da cui $S \in \mathcal{Z}'$, ma $S \in \mathcal{S}$ quindi $S \neq S_C$ e perciò $S \in \mathcal{Z}$.
Da questo fatto segue che $S_C \in \mathcal{Z}'$, infatti A_C e S_C sono disgiunti.
Allora, se definiamo $\mathcal{Z} = \mathcal{Z}' \setminus \{S_C\} \cup \{S \in \mathcal{S} : S \cap C \neq \emptyset\}$ come in 4(f)i,

$$\textstyle\bigcup_{S\in\mathcal{Z}} S = (\bigcup_{S\in\mathcal{Z},S\cap C=\emptyset} S) \cup (\bigcup_{S\in\mathcal{Z},S\cap C\neq\emptyset} S) = (\bigcup_{S\in\mathcal{Z},S\cap C=\emptyset} S) \cup (S_C \cup C) = \big(\bigcup_{S\in\mathcal{Z}'} S\big) \cup C.$$

Per la proposizione 1.4.10 se $X \subseteq (E \setminus C)$ allora $r'(X) = r(X \cup C) - r(C)$, e dato che $C \setminus \{e\}$ è una base di C abbiamo $r(X \cup C) = r'(X) + |C| - 1$.
Inoltre, dato che $S_C \in \mathcal{Z}'$ e $|\{S \in \mathcal{S} : S \cap C \neq \emptyset\}| = |C|$ allora $|\mathcal{Z}| = |\mathcal{Z}'| + |C| - 1$ e $|\mathcal{S}| = (|\mathcal{S}| + |C| - 1)$.

Infine

$$\begin{aligned}
|A| &= |A_C| + |C| - 1 = r'\big(\bigcup_{S\in\mathcal{Z}'} S\big) + |\mathcal{S}'| - |\mathcal{Z}'| + |C| - 1 \\
&= \left(r\Big(\big(\bigcup_{S\in\mathcal{Z}'} S\big) \cup C\Big) - |C| + 1\right) + |\mathcal{S}'| - |\mathcal{Z}'| + |C| - 1 \\
&= r\big(\bigcup_{S\in\mathcal{Z}} S\big) + \big(|\mathcal{S}'| - |C| + 1\big) - \big(|\mathcal{Z}'| - |C| + 1\big) \\
&= r\big(\bigcup_{S\in\mathcal{Z}} S\big) + |\mathcal{S}| - |\mathcal{Z}|\,.
\end{aligned}$$

Questo garantisce che A sia un psr indipendente massimale di M.
Supponiamo ora di essere nel caso 4g, ovvero che al passo 4e la ricorsione abbia prodotto A'_C psr indipendente per M' e $\mathcal{S}'$ con cardinalità pari a $|A_C| + 1$.
Come sopra C è un psr dunque $|\{S \in \mathcal{S} : S \cap C \neq \emptyset\}| = |C|$ ed, essendo A'_C psr rispetto a $\mathcal{S}'$ $|A'_C \cap S_C| \leq 1$, quindi $|A'_C \cap S| = 1$ al più per un solo $\bar{S}$ tale che $\bar{S} \cap C \neq \emptyset$. Se questo $\bar{S}$ non esiste allora $A'_C \cup C$ è un psr, se esiste $A'_C \cup (C \setminus \{y\})$ con $y \in C \cap \bar{S}$ è pure un psr. In ogni caso posso scegliere un y come richiesto da 4(g)i.
Osserviamo ora che $A' = A'_C \cup (C \setminus \{y\})$ è un indipendente di M, infatti A'_C un indipendente di M/C e $C \setminus \{y\}$ è una base di C.
Quindi $A' = A'_C \cup C \setminus \{y\}$ è un psr indipendente di cardinalità $|A'| = |A'_C| + |C| - 1 = |A \setminus C| + |C| = |A| + 1$. Quindi anche in questo caso l'algoritmo è corretto. □

Notiamo che l'algoritmo 2.2 termina in un tempo che è $O(\theta\,|A|\,(|A|+|\mathcal{S}|))$ con θ complessità dell'oracolo. Infatti al passo 2 richiede al più un tempo $O(\mathcal{S})$, il passo 4a richiede al più $O(|A|\,\theta)$, i passi successivi un tempo $O(\mathcal{S})$, il passo 4g un tempo $O(A)$, gli altri passaggi richiedo o l'uso dell'oracolo o un tempo costante. La presenza della ricorsione aggiunge un altro fattore $|A|$.

Definizione 2.3.5. Nel seguente algoritmo indichiamo con *copia* di un insieme E un insieme E' disgiunto da E per cui esiste una corrispondenza biunivoca $\varphi : E \to E'$ $\varphi(e) = e'$. Chiamiamo inoltre *copia* di un matroide M un matroide M' disgiunto da M con $M' \cong M$.

Algoritmo 2.3.
Siano dati due matroidi $M_1 = (E, \mathcal{I}_1)$ e $M_2 = (E, \mathcal{I}_2)$, supponiamo di avere un oracolo di basis-superset per M_1 e un oracolo di indipendenza per M_2.
Algoritmo:

1. *Crea una copia $E' = \{e' : e \in E\}$ di E e una copia $M_2' = (E', \mathcal{I}_2')$ di M_2.*
2. *Poni $M \leftarrow M_1^* \oplus M_2' = (E \cup E', \mathcal{I}_1^* \vee \mathcal{I}_2')$ e $\mathcal{S} \leftarrow \big\{\{e, e'\} : e \in E, e' \in E'\big\}$*
3. *Poni $A \leftarrow \emptyset$*
4. *Continua a ripetere:*
   (a) *Applica l'algoritmo 2.2 con insieme dato A, matroide M e partizione $\mathcal{S}$ per trovare A' psr indipendente di cardinalità maggiore di A o $\mathcal{Z}$ che verifica il minimo in 2.3.3*
   (b) *Se l'algoritmo restituisce A' poni $A \leftarrow A'$*
   (c) *Se l'algoritmo restituisce $\mathcal{Z}$ esci dal ciclo*
5. *Poni $A_1 \leftarrow A \cap E$, $A_2 \leftarrow A \cap E'$*
6. *Trova una base B di M_1 disgiunta da A_1*
7. *Restituisci l'insieme $\{e \in E : e \in B, e' \in A_2\}$*

Proposizione 2.3.6. *L'algoritmo 2.3 restituisce un indipendente di $M_1 \cap M_2$ di cardinalità massima*

Dimostrazione.
$\emptyset$ è un psr indipendente, quindi per la proposizione 2.3.4 A è un psr indipendente dopo ogni iterazione del ciclo 4, inoltre, al termine del ciclo, l'insieme A ottenuto è un psr indipendente di cardinalità massima rispetto a $\mathcal{S}$ e M, e $|A| = r_M\Big(\bigcup_{S\in\mathcal{Z}} S\Big) + |\mathcal{S}| - |\mathcal{Z}|$.

Essendo M somma diretta di M_1^* e M_2, essendo $A_1 \subseteq E$, $A_2 \subseteq E'$ ed essendo entrambi contenuti in un indipendente di M allora per gli insiemi prodotti al passo 5 vale $A_1 \in \mathcal{I}_1^*$ e $A_2 \in \mathcal{I}_2'$
Dato che $A_1 \in \mathcal{I}_1^*$ allora è contenuto nel complementare di una base di M_1, ovvero A_1^c contiene una base di M_1, possiamo allora togliere elementi a A_1^c fino a trovare una base B come cercata al passo 6.
Sia $\varphi' : e' \mapsto e$. Dato che $A_2 \in \mathcal{I}_2'$ e $M_2' \cong M_2$ allora $\varphi'(A_2) \in \mathcal{I}_2$, quindi l'insieme $X = \{e \in E : e \in B, e' \in A_2\} = B \cap \varphi'(A_2)$ del passo 7 è l'intersezione di un indipendente di M_1 e di uno di M_2, quindi è un indipendente di $M_1 \cap M_2$. Dimostriamo che è di cardinalità massima verificando l'uguaglianza (2.1) del teorema 2.1.6.
Osserviamo che A_1 e $\varphi'(A_2)$ sono disgiunti, infatti in $|A \cap \{e, e'\}| \leq 1$ per ogni $e \in E$ perché psr rispetto a $\mathcal{S}$. Quindi $A_1 \cap (\varphi'(A_2) \cup B) = \emptyset$.
Chiamo $r_1 = r_{M_1}$, $r_2 = r_{M_2}$ allora

$$\begin{aligned} |X| = \big|B \cap \varphi'(A_2)\big| &= |B| + \big|\varphi'(A_2)\big| - \big|\varphi'(A_2) \cup B\big| - |A_1| + |A_1| \\ &\geq r(M_1) + |A_2| - |E| + |A_1| \\ &= r_1(E) + |A| - |E| \\ &= r_1(E) + r_M\Big(\bigcup_{S \in \mathcal{Z}} S\Big) + |\mathcal{S}| - |\mathcal{Z}| - |E| \end{aligned}$$

Notiamo ora che $|E| = \big|\big\{\{e, e'\} : e \in E\big\}\big| = |\mathcal{S}|$ e che $r_M = r_1 + r_2$. Inoltre, se $U = \bigcup_{S \in \mathcal{Z}} S \cap E = \{e \in E : \{e, e'\} \in \mathcal{Z}\}$ è l'insieme degli elementi dell'unione di $\mathcal{Z}$ in E e $U' = \varphi(U)$ è quello dei loro corrispondenti in E' allora $|\mathcal{Z}| = |U| = |U'|$.

$$\begin{aligned} |X| &\geq r_1(E) + r_M(U \cup U') + |E| - |U| - |E| \\ &= r_1(E) + r_1^*(U) + r_2(U) - |U| \\ &= r_1(E) + (|U| - r_1(E) + r_1(U^c)) + r_2(U) - |U| \\ &= r_1(U^c) + r_2(U) = r_1(E \setminus U) + r_2(U) \end{aligned}$$

Quindi per il teorema 2.1.6 $|X|$ è pari al minimo di $r_1(U^c) + r_2(U)$ ed è un indipendente comune a M_1 e M_2 di cardinalità massima. □

Abbiamo quindi trovato un ulteriore algoritmo che impiega un tempo polinomiale per risolvere il problema 2.1.5. Avere più algoritmi per approcciare lo stesso problema ci consente di scegliere il metodo migliore. A titolo di esempio, se l'oracolo di indipendenza e quello di basis-superset di uno dei matroidi avessero complessità computazionale diversa potrei avere che l'algoritmi 2.1 e l'algoritmo 2.3 abbiano tempi differenti.

2.4 Intersezione di 3 o più matroidi

Consideriamo ora il problema di intersezione per un numero di matroidi qualsiasi

Problema 2.4.1. Siano $M_1, M_2 \dots M_n$ dei matroidi con $M_i = (E, \mathcal{I}_i)$
OBIETTIVO: Trovare un insieme $X \in \bigcap_{1 \leq i \leq n} \mathcal{I}_i$ tale che $|X|$ sia massimo.

Innanzitutto notiamo che, come mostrato nell'esempio 2.1.3 l'intersezione di matroidi non è un matroide, quindi non è possibile risolvere il problema 2.4.1 risolvendo ripetutamente delle istanze successive del problema 2.1.5 (intersezione di 2 matroidi).

Mostriamo ora come in realtà la risoluzione del problema 2.4.1 per $n \geq 3$ sia computazionalmente difficile.

Proposizione 2.4.2. *Sia $D = (V, E)$ un grafo orientato connesso tale che $|V| = n + 1$, allora i seguenti insiemi sono gli insiemi degli indipendente per 3 matroidi:*

1. *$\mathcal{I}_1 = \{A \in E : |A \cap \delta^+(v)| \leq 1 \forall v \in V, |A| \leq n\}$, in cui gli indipendenti sono insiemi di al più n archi tali che in ogni vertice di V entri al più un arco*

2. *$\mathcal{I}_2 = \{A \in E : |A \cap \delta^-(v)| \leq 1 \forall v \in V, |A| \leq n\}$, in cui gli indipendenti sono insiemi di al più n archi tali che da ogni vertice di V esca al più un arco*

3. *$\mathcal{I}_3 = \{A \in E : A$ è un albero nel grafo $(V, \{\{x, y\} : (x, y) \in E\})\}$, in cui gli indipendenti sono gli alberi del grafo non orientato.*

Dimostrazione. Siano $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2), M_3 = (E, \mathcal{I}_3)$.
M_1 e M_2 sono indipendenti perché ottenuti come intersezioni fra il matroide uniforme di rango n e i matroidi partizioni rispettivamente per le partizioni $\{\delta^+(v) \subseteq E : v \in V\}$ e $\{\delta^-(v) \subseteq E : v \in V\}$.
Il matroide M_3 è il matroide delle foreste del grafo non orientato associato a D, ovvero $(V, \{\{x, y\} : (x, y) \in E\})$. □

Teorema 2.4.3. *Un cammino P in D è un cammino hamiltoniano se e solo se gli archi che percorre sono un indipendente di cardinalità n in $M_1 \cap M_2 \cap M_3$.*

Dimostrazione. Se P è un cammino hamiltoniano e A sono gli archi che attraversa, allora, dato che $|V| = n + 1$, $|A| = n$. Inoltre A non contiene cicli: se li contenesse tornerebbe sullo stesso vertice e quindi P non sarebbe hamiltoniano. Infine dato che P passa una sola volta per ogni vertice allora A non può contenere più di un elemento di $\delta^+(v)$ e $\delta^-(v)$ per ogni $v \in V$.
Sia ora A è un indipendente comune ai tre matroidi e G la versione non orientata di D. Il grado di ogni nodo nel grafo G ristretto ad A è al massimo due, infatti se $\delta_G(v) \cap A = (\delta^+(v) \cap A) \cup (\delta^-(v) \cap A)$ per cui $|\delta_G(v) \cap A| \leq 2$, allora le componenti connesse di A del grafo non orientato possono essere solamente cicli o cammini. Dato che G ristretto ad A non contiene cicli perché A è un indipendente di M_3, allora contiene solo cammini ed, essendo $|A| = n = |V| + 1$, che A è un formato

da una solo cammino P nel grafo G.
Ora P è anche un cammino nel grafo orientato D, se non lo fosse esisterebbe una coppia di archi e_i, e_{i+1} consecutivi in P per cui o $e_i = (v, w), e_{i+1} = (t, w)$ o $e_i = (v, w), e_{i+1} = (v, t)$, ma questo contrasta con in fatto che A è un indipendente di M_1 e M_2, infatti o $|\delta^-(w) \cap A| = 2$ o $|\delta^+(v) \cap A| = 2$. □

Sappiamo che stabilire se un grafo contenga o meno un ciclo hamiltoniano è un problema NP-completo. Ma il teorema 2.4.3 ci mostra che se sapessimo dire quale sia la cardinalità massima di un indipendente comune a tre matroidi allora sapremmo dire se esiste un ciclo hamiltoniano. Ne concludiamo che risolvere il problema 2.4.1 nel caso di 3 o più matroidi sia NP-difficile.

Capitolo 3

Poliedri e matroidi

In questo capitolo cerchiamo di legare i matroidi alla programmazione lineare. Innanzitutto nella sezione 3.1 diamo una descrizione di come ricavare un poliedro, e quindi un programma lineare, da un matroide [6]. Nelle sezioni successive invece generalizziamo il concetto di matroide introducendo i polimatroidi tramite le funzioni submodulari [7] e mostriamo come anche in questo caso un algoritmo greedy ci permette di ottimizzare in modo efficiente.

3.1 Poliedro degli indipendenti

Sia E un insieme finito e $A \subseteq E$ un suo sottoinsieme, indichiamo con χ^A il vettore di incidenza di A, ovvero $\chi^A \in \mathbb{R}^E$ per cui ${\chi^A}_e = 1$ se $e \in A$ e ${\chi^A}_e = 0$ se $e \notin A$.

Definizione 3.1.1 (Poliedro degli indipendenti)**.** Sia $M = (E, \mathcal{I})$ un matroide, il *poliedro degli indipendenti* di M o il *poliedro del matroide* M è l'inviluppo convesso dell'insieme dei vettori di incidenza degli indipendenti di M

$$P(M) = conv\left(\{\chi^A : A \in \mathcal{I}\}\right) \subseteq \mathbb{R}^E.$$

Teorema 3.1.2 ([6])**.** *Sia $M = (E, \mathcal{I})$ un matroide con funzione rango r e sia*

$$P(E, r) = \left\{ x \in \mathbb{R}^E : \left\{ \begin{array}{l} x \geq 0 \\ \chi^S \cdot x \leq r(S) \text{ per ogni } S \subseteq E \end{array} \right. \right\},$$

allora i vertici di $P(E, r)$ sono tutti e soli i vettori di incidenza degli indipendenti di M.

Se indichiamo con V l'insieme dei vertici di $P(E, r)$ e con H l'insieme $\{\chi^A : A \in \mathcal{I}\}$, allora la tesi del teorema è $V = H$.

Presentiamo ora alcuni lemmi che utilizzeremo nella dimostrazione del teorema.

Lemma 3.1.3. *Siano $A, B \subseteq E$ insiemi, allora $\chi^A \cdot \chi^B = |A \cap B|$.*

Dimostrazione. $\chi^A \cdot \chi^B = \sum_{e \in E} {\chi^A}_e {\chi^B}_e = \sum_{e \in (A \cap B)} 1 = |A \cap B|$. □

Lemma 3.1.4. $P(E, r) \subseteq [0, 1]^E$.

Dimostrazione. Sia $x \in P(E, r)$, sia $e \in E$. Ponendo $S = \{e\}$ in $\chi^S \cdot x \leq r(S)$, troviamo $0 \leq x_e \leq r(\{e\}) \leq 1$. Dato che questo vale per ogni $e \in E$ allora $x \in [0, 1]^E$. □

Lemma 3.1.5. *Un vettore è contenuto in H se è solo se è un vettore a coordinate intere contenuto in $P(E, r)$.*

Dimostrazione. Dimostriamo che se $x \in H$ allora $x \in (\mathbb{Z}^E \cap P(E, r))$.
Sia $A \in \mathcal{I}$ e $x = \chi^A \in \mathbb{R}^E$, dalla definizione di vettore di incidenza segue che $x \geq 0$. Inoltre, dato un insieme $S \subseteq E$, per il lemma 3.1.3 otteniamo $x \cdot \chi^S = |A \cap S|$. Quindi $|A \cap S| = r(A \cap S)$ perché $A \cap S \subseteq A$ è un indipendente. Dunque $x \cdot \chi^S = r(A \cap S) \leq r(S)$ per la monotonia del rango. Da questo $x \in P(E, r)$.
Dimostramo ora che se $x \in \mathbb{Z}^E \cap P(E, r)$ allora esiste $A \in \mathcal{I}$ tale che $x = \chi^A$.
Per il lemma 3.1.4, se $x \in P(E, r) \cap \mathbb{Z}^E$, allora $x \in \{0, 1\}^E$, da questo segue che esiste un insieme $A \subset E$ di cui x è vettore di incidenza.
Pongo $S = A$ in $\chi^S \cdot x \leq r(S)$ e trovo $|A| = \chi^A \cdot \chi^A \leq r(A) \leq |A|$, da questo segue $r(A) = |A|$ e quindi $A \in \mathcal{I}$. □

Lemma 3.1.6. *Siano $c \in \mathbb{R}^E$ un vettore, k il numero di componenti non negative di c, r la funzione rango di un matroide e $n = |E|$, allora il seguente procedimento produce il vettore di incidenza di un insieme indipendente:*

- *Ordina gli elementi di E come le componenti di c, ovvero trova una permutazione $\sigma : \{1, \ldots, n\} \to E$ per cui $c_{\sigma(1)} \geq \cdots \geq c_{\sigma(k)} \geq 0 \geq c_{\sigma(k+1)} \geq \cdots \geq c_{\sigma(n)}$. Poni $A_0 = \emptyset$ e $A_i = \{\sigma(1), \ldots, \sigma(i)\}$ per ogni $1 \leq i \leq k$;*
- *Sia $\bar{x} \in \mathbb{R}^E$ tale che $\bar{x}_{\sigma(i)} = r(A_i) - r(A_{i-1})$ per ogni $1 \leq i \leq k$ e $\bar{x}_{\sigma(i)} = 0$ per ogni $k + 1 \leq i \leq n$.*

Dimostrazione. Notiamo che $r(A_i) - r(A_{i-1}) \leq r(\{\sigma(i)\}) \in \{0, 1\}$, quindi $\bar{x}_{\sigma(i)} \in \{0, 1\}$ per ogni $1 \leq i \leq n$, da cui $x \in \{0, 1\}^E$ è il vettore di incidenza di un insieme $\bar{A} \in \mathcal{I}$.
Chiamiamo $\bar{A}_i = \bar{A} \cap A_i$. Dato che per $i > k$ $\bar{x}_{\sigma(i)} = 0$, $\bar{A}_k = \bar{A}$. Mostriamo per induzione su i che $\bar{A}_i \in \mathcal{I}$.
Banalmente $\bar{A}_0 = \emptyset \in \mathcal{I}$. Supponiamo ora $\bar{A}_{i-1} \in \mathcal{I}$, allora se $\sigma(i) \notin \bar{A}_i$ abbiamo $\bar{A}_i = \bar{A}_{i-1} \in \mathcal{I}$, se invece $\sigma(i) \in \bar{A}_i$ allora $\sigma(i) \in \bar{A}$, quindi e dunque $\bar{x}_{\sigma(i)} = 1$, ovvero $r(A_i) - r(A_{i-1}) = 1$.
Per la submodularità del rango otteniamo $r(A_i) + r(\bar{A}_{i-1}) \leq r(A_{i-1}) + r(\bar{A}_i)$, inoltre $r(\bar{A}_{i-1}) = \left|\bar{A}_{i-1}\right|$ dato che $\bar{A}_{i-1} \in \mathcal{I}$. Quindi, se $\sigma(i) \in \bar{A}_i$, sostituendo otteniamo $r(\bar{A}_i) \geq \left|\bar{A}_{i-1}\right| + 1$, da cui segue $r(\bar{A}_i) = \left|\bar{A}_i\right|$, quindi $\bar{A}_i \in \mathcal{I}$. □

Notiamo inoltre che l'insieme $\bar{A}$ coincide con l'insieme indipendente prodotto dall'algoritmo greedy 1.1 per il matroide $M\backslash\{e : c_e < 0\}$ e la funzione costo $e \mapsto c_e$, infatti un elemento $\sigma(i)$ viene aggiunto a $\bar{A}_i$ solo se $\bar{A}_i \cup \{\sigma(i)\}$ è un indipendente.

Dimostrazione del teorema 3.1.2.
Sia $x \in H$, sia $A \in \mathcal{I}$ tale che $x = \chi^A$, mostriamo che $x \in V$.
Per il lemma 3.1.5 sappiamo $x \in P(E, r)$, dobbiamo mostrare che è un vertice. Notiamo che x è l'unica soluzione in $P(E, r)$ del sistema lineare:

$$\begin{cases} x_e = 0 \text{ per ogni } e \notin A \\ x \cdot \chi^A = r(A) = |A| \end{cases}$$

Infatti se $x \in P(E, r)$, allora $x_e \leq 1$ perché $x \in [0, 1]^E$ per il lemma 3.1.4, e dato che $x_e = 0$ per $e \notin A$, segue $x \cdot \chi^A = \sum_{e \in A} x_e \leq |A|$ e l'uguaglianza vale solo se $x_e = 1$ per ogni $e \in A$.
Questo sistema lineare è un sottosistema di quello che definisce $P(E, r)$ in cui però abbiamo delle uguaglianze al posto di disuguaglianze. Le soluzioni del sistema sono quindi un'intersezione di facce del poliedro, e dato che x è l'unica soluzione in $P(E, r)$, allora è un vertice del poliedro. Quindi $x \in V$.
Mostriamo ora che se $\bar{x} \in V$ allora $x \in \mathbb{Z}^E$.
Se $\tilde{x}$ è il vertice di un poliedro $P = P(E, r)$, allora $\tilde{x}$ è sia un punto estremo che un punto esposto per P. Essendo un punto esposto, allora esiste un vettore $c \in \mathbb{R}^E$ per cui $\hat{x}$ è l'unica soluzione ottima del programma lineare:

$$\begin{array}{l} \max c \cdot x \\ \text{s.a} \quad x \in P \end{array} \quad \Leftrightarrow \quad \begin{array}{l} \max c \cdot x \\ \text{s.a} \end{array} \begin{cases} x \geq 0 \\ x \cdot \chi_S \leq r(S) \ \ \forall S \subseteq E \end{cases}$$

Consideriamo ora il programma lineare duale

$$\begin{array}{l} \min r \cdot y \\ \text{s.a} \end{array} \begin{cases} y \in \mathbb{R}^{2^E} & \\ y_S \geq 0 & \forall S \subset E \\ \sum_{S \subseteq E} (\chi^S{}_e \, y_S) \geq c_e & \forall e \in E \end{cases}$$

Per il teorema di dualità debole sappiamo che per x e y soluzione ammissibili del primo e del secondo p.l. rispettivamente vale $c \cdot x \leq r \cdot y$.
Sia k il numero di componenti positive di c e siano $\bar{x} \in H$, σ e A_i come prodotti dal procedimento del lemma 3.1.6. Costruiamo $\bar{y} \in \mathbb{R}^{2^E}$ in questo modo: $\bar{y}_{A_i} = c_{\sigma(i)} - c_{\sigma(i+1)}$ per ogni A_i con $1 \leq i < k$ e $\bar{y}_{A_k} = c_{\sigma(k)}$, e inoltre $\bar{y}_A = 0$ per

ogni altro $A \subseteq E$. Notiamo che $\bar{y}$ è una soluzione ammissibile del secondo p.l. infatti dall'ordinamento dei E segue $c_k \geq c_{k+1}$ quindi $\bar{y}_A \geq 0$ per ogni $A \subseteq E$; inoltre $\sum_{S \subseteq E} (\chi^S{}_{e_i}\, \bar{y}_S) = \sum_{j=i}^{n} \bar{y}_{A_j} = \sum_{j=i}^{k-1} (c_{\sigma(j)} - c_{\sigma(j+1)}) + c_{\sigma(k)} = c_{\sigma(i)}$ per ogni $1 \leq i \leq k$, quindi per ogni $e \in E$ tale che $c_e \geq 0$, infine $\sum_{S \subseteq E} (\chi^S{}_e\, \bar{y}_S) = 0 > c_e$ per ogni e tale che $c_e < 0$.
Notiamo ora che

$$\begin{aligned} r \cdot \bar{y} - c \cdot \bar{x} &= \sum_{i=1}^{k-1} (r(A_i)(c_{\sigma(i)} - c_{\sigma(i+i)})) + r(A_k)c_{\sigma(k)} - c_1 r(A_1) - \sum_{i=2}^{k} (r(A_{\sigma(i)}) - r(A_{\sigma(i-1)}))c_{\sigma(i)} \\ &= \sum_{i=1}^{k} c_{\sigma(i)} r(A_i) - \sum_{i=1}^{k-1} c_{\sigma(i-i)} r(A_i) - \sum_{i=1}^{k} r(A_i)c_{\sigma(i)} + \sum_{i=2}^{k} r(A_{i-1})c_{\sigma(i)} = 0. \end{aligned}$$

Quindi $r \cdot \bar{y} = c \cdot \bar{x}$ e perciò $\bar{x}$ deve essere una soluzione ottima del primo programma lineare, ma quindi dev'essere che $\bar{x} = \tilde{x}$.
Per il lemma 3.1.6 esiste $\bar{A}$ tale che $\chi_{\bar{A}} = \bar{x} = \tilde{x}$, quindi $\tilde{x} \in H$. □

Corollario 3.1.7. Sia $M = (E, \mathcal{I})$ matroide e r il suo rango, allora $P(M) = P(E, r)$.

Dimostrazione. Dato che $P(M)$ è l'inviluppo convesso dei vertici di $P(E, r)$ che è un poliedro, quindi convesso, allora $P(M) = P(E, r)$. □

3.2 Funzioni submodulari

Definizione 3.2.1. Sia L un insieme su cui è definita una relazione d'ordine $\leq$. Supponiamo che per ogni $a, b \in L$ esistono due elementi $x, y \in L$: x tale che $x \leq a$, $x \leq b$, massimo fra gli elementi che hanno questa proprietà, e y tale che $a \leq y$, $b \leq y$, minimo fra gli elementi che hanno questa proprietà. Ovvero se $c \leq a$ e $c \leq b$, allora $c \leq x$; e se $c \geq a$ e $c \geq b$, allora $c \geq y$. Allora L è detto *reticolo* ed indichiamo $x = a \wedge b$ l'*estremo inferiore* di a e b, e con $y = a \vee b$ l'*estremo superiore* di a e b.

In ogni reticolo in cui esistono degli elementi minimali esiste un elemento minimo, che indichiamo con 0 o con $\emptyset$, in ogni reticolo in cui esistono elementi massimali esiste un massimo che indichiamo con 1. In un reticolo finito esistono sia 0 che 1.

Diamo ora una definizione di submodularità per funzioni su reticoli più generale di quella usata nel teorema 1.3.10.

Definizione 3.2.2. Sia L un reticolo e $A, B \in L$, allora una funzione $f : L \to \mathbb{R}$ si dice *submodulare* per L se $f(A \wedge B) + f(A \vee B) \leq f(A) + f(B)$.

Notiamo che se E è un insieme finito, allora l'insieme $L = 2^E$ con la relazione di inclusione è un reticolo in cui $A \wedge B = A \cap B$ e $A \vee B = A \cup B$, quindi la definizione

di submodularità 3.2.2 generalizza la definizione per cui $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$.

Se $L = \mathbb{R}^n$ e $\leq$ è la relazione per cui dati $a, b \in \mathbb{R}^n$ vale $a \leq b$ se $a_i \leq b_i$ per ogni i, allora L è un reticolo. In questo caso $(a \wedge b)_i = (\min\{a_i, b_i\})_i$ e $(a \vee b)_i = (\max\{a_i, b_i\})_i$ per ogni $i \in \{1, \ldots, n\}$.

Definizione 3.2.3 (Funzioni β_0 e funzioni β [7])**.** Sia L un reticolo in cui esiste un minimo 0, una funzione β_0 è una funzione $f : L \to \mathbb{R}$ tale che valgano:

1. $f(a) \geq 0$ per ogni $a \in (L \setminus \{0\})$
2. f è crescente, ovvero $f(a) \leq f(b)$ per $a \leq b$
3. f è submodulare

Una funzione β è una funzione β_0 per cui $f(0) = 0$.

Proposizione 3.2.4. *Sia E un insieme finito e sia $f : 2^E \to \mathbb{R}$. f è il rango di un matroide se e solo se f è una funzione β tale che $f(A) - f(B) \in \{0, 1\}$ per ogni $A, B \subseteq E$ per cui $|A \setminus B| = 1$.*

Dimostrazione. Per il teorema 1.3.10 basta dimostrare che, data f non negativa, submodulare e crescente, allora $f(A) \in \mathbb{Z}^+$ e $f(A) \leq |A|$ per $A \subseteq E$ se e solo se $f(\emptyset) = 0$ e $f(A) - f(B) \in \{0, 1\}$ per $A, B \subseteq E$ tali che $|A \setminus B| = 1$.
Mostriamo la prima implicazione. Banalmente $f(\emptyset) = 0$, inoltre se $A, B \subseteq E$ tali che $A \setminus B = \{e\}$ allora $f(A) \leq f(B) + f(\{e\})$, da cui $f(A) - f(B) \leq f(\{e\}) \leq |\{e\}| = 1$, e dato che $f(A) \geq f(B)$, segue $f(A) - f(B) \in [0, 1] \cap \mathbb{Z}^+ = \{0, 1\}$.
Mostriamo l'implicazione inversa per induzione su $|A|$. Se $A = \emptyset$, allora $f(\emptyset) = 0$ verifica $f(A) \leq |A|$ e $f(A) \in \mathbb{Z}$. Supponiamo $f(A) \leq |A|$ e $f(A) \in \mathbb{Z}$. Sia $e \notin A$, allora $f(A \cup \{e\}) - f(A) \in \{0, 1\}$, e quindi $f(A \cup \{e\}) \in \mathbb{Z}$. Infine, per la submodularità di f segue $f(A \cup \{e\}) \leq f(A) + f(\{e\}) \leq |A| + 1 = |A \cup \{e\}|$. □

Proposizione 3.2.5. *La somma di funzioni submodulari è una funzione submodulare.*

Dimostrazione. Siano f, g submodulari, allora $f(A \vee B) + f(A \wedge B) \leq f(A) + f(B)$ e $g(A \vee B) + g(A \wedge B) \leq g(A) + g(B)$, da cui $(f + g)(A \vee B) + (f + g)(A \wedge B) \leq (f + g)(A) + (f + g)(B)$. □

3.2.1 Alcuni esempi

Abbiamo visto che la funzione rango di un matroide è una funzione submodulare. Queste funzioni tuttavia compaiono naturalmente in altri ambiti.

Esempio 3.2.6 (Tagli di un grafo).
Sia $G = (V, E)$ un grado, $U \subset V$ un insieme di vertici, e $\delta(U)$ l'insieme dei vertici uscenti da U, allora la funzione $d : 2^V \to \mathbb{Z}$ per cui $d(U) = |\delta(U)|$) è submodulare. Se $c : E \to \mathbb{R}$ è una funzione *capacità* che associa un valore reale ad ogni arco, allora la funzione $C : 2^V \to \mathbb{R}$ per cui $C(U) = \sum_{e \in \delta(U)} c(e)$ è submodulare.

Esempio 3.2.7 (Massimo su insieme finito). Sia E un insieme finito e $h : E \to \mathbb{R}$ una funzione reale. Allora la funzione m che associa ad ogni sottoinsieme di E il massimo di h su E

$$m(U) = \max \{h(x) : x \in U\}$$

è submodulare.
Allo stesso modo anche la funzione che dato un vettore in $\mathbb{R}^n$ ritorna la componente più grande è una funzione submodulare per il reticolo $(\mathbb{R}^n, \leq)$.

Dimostrazione che m è submodulare. Siano $A, B \subseteq E$. Dato che se $x \in A \cap B$, allora o $x \in A$ o $x \in B$, segue che $m(A \cup B) = \max \{m(A), m(B)\}$. E dato che $m(A \cap B) \leq m(A)$ e $m(A \cap B) \leq m(B)$, allora $m(A \cap B) \leq \min \{m(A), m(B)\}$. Quindi otteniamo che $m(A \cup B) + m(A \cap B) \leq \min \{m(A), m(B)\} + \max \{m(A), m(B)\} = m(A) + m(B)$. □

Esempio 3.2.8. Sia la funzione modulo $f : A \mapsto |A|$ che il suo opposto $(-f) : A \mapsto (-|A|)$ sono funzioni submodulari. Infatti $|A \cap B| + |A \cup B| = |A| + |B|$.

3.3 Polimatroidi

Definizione 3.3.1 (Polimatroide)**.** Sia E un insieme finito e sia $L \subseteq 2^E$ un sottoinsieme delle parti di E chiuso per intersezioni e che contenga E e $\emptyset$. Sia $f : L \to \mathbb{R}$ una funzione β_0 su L con la relazione d'ordine data dall'inclusione di insiemi.
Il *polimatroide* rispetto a E e f è

$$P(E, f) = \left\{x \in \mathbb{R}^E : x \geq 0, x \cdot \chi^A \leq f(A) \text{ per ogni } A \in L \setminus \{\emptyset\}\right\}$$

Un polimatroide è un poliedro che sia $P(E, f)$ per qualche coppia (E, f).

Proposizione 3.3.2. *Sia M un matroide, allora il poliedro degli indipendenti $P(M)$ è un polimatroide.*

Dimostrazione. Dal proposizione 3.2.4 segue che il rango è una funzione β e inoltre per il teorema 3.1.2 il poliedro è $P(E, r)$. □

3.4 Algortimo greedy per polimatroidi

Consideriamo ora il problema di massimizzare una funzione lineare su un polimatroide, ovvero il programma lineare seguente.

Problema 3.4.1. Dato $c \in \mathbb{R}^E$ e f una funzione β risolvere:

$$\begin{array}{l} \max c \cdot x \\ \text{s.a} \quad \begin{cases} x & \geq & 0 \\ \chi^S \cdot x = \sum_{e \in S} x_e & \leq & f(S) \quad \forall S \subseteq E, S \neq \emptyset \end{cases} \end{array}$$

Mostriamo che questo problema, come nel caso dei matroidi, può essere risolto in modo molto veloce da un algoritmo greedy.

Algoritmo 3.1 (Greedy per polimatroidi)**.**
Siano dati un insieme E, una funzione/vettore costo $c \in \mathbb{R}^E$ e una f funzione β.

1. *Ordina gli elementi di E per costi decrescenti, ovvero trova una permutazione σ per cui $c_{\sigma(i)} \geq c_{\sigma(i+1)}$ per ogni i*
2. *Poni $k \leftarrow \max_{c_{\sigma(i)} \geq 0} i$ il massimo indice che abbia costo positivo*
3. *Poni $A_j \leftarrow \{\sigma(i) : 1 \leq i \leq j\}$*
4. *Crea un vettore $\bar{x} \in \mathbb{R}^E$ ponendo:*
   - $\bar{x}_{\sigma(1)} \leftarrow f(A_1)$
   - $\bar{x}_{\sigma(i)} \leftarrow f(A_i) - f(A_{i-1})$ *per* $2 \leq i \leq k$
   - $\bar{x}_{\sigma(i)} \leftarrow 0$ *per* $k < i \leq |E|$
5. *Restituisci $\bar{x}$.*

Teorema 3.4.2. *L'algoritmo 3.1 produce una soluzione ottima del programma lineare 3.4.1.*

Dimostrazione. Sia $\bar{x}$ l'output dell'algoritmo 3.1. Dimostriamo che è una soluzione ottima del programma lineare del polimatroide analizzando il programma lineare duale.

$$\begin{array}{l} \min \sum_{S \subseteq E, S \neq \emptyset} f(S) y_S \\ \text{s.a} \quad \begin{cases} y & \geq & 0 \\ \sum_{S \subseteq E, S \neq \emptyset} \chi^S{}_j \cdot y_S = \sum_{S : j \in S} y_S & \geq & c_j \quad \forall j \in E \end{cases} \end{array}$$

Sia $\bar{y} \in \mathbb{R}^{2^E - 1}$ tale che, per σ e A_i prodotti dall'algoritmo 3.1 vale:

- $\bar{y}_{A_i} = c_{\sigma(i)} - c_{\sigma(i+1)}$ per ogni $1 \leq i < k$
- $\bar{y}_{A_k} = c_{\sigma(k)}$
- $\bar{y}_A = 0$ per $A \in 2^E \setminus \{\emptyset\} \setminus \{A_i :\leq i \leq k\}$

Dimostriamo ora che $\bar{x}$ è una soluzione ammissibile di 3.4.1 e che $\bar{y}$ è una soluzione ammissibile del duale.
Verifichiamo che $\bar{x} \in P(E, f)$. Innanzitutto $\bar{x} \geq 0$ perché $A_i \subseteq A_{i+1}$ e f è monotona, quindi $f(A_i) - f(A_{i-1}) > 0$. Mostriamo poi che $\chi^{A_i} \cdot \bar{x} \leq f(A_i)$. $\chi^{A_i} \cdot \bar{x} = \sum_{1 \leq j \leq i} x_{e_{\sigma(j)}} = f(A_1) + \sum_{2 \leq j \leq jS} (f(A_j) - f(A_{j-2})) = f(A_i)$. Mostriamo che $\chi^S \cdot \bar{x} \leq f(S)$ per se esiste i per cui $S \subseteq A_i$. Procediamo per induzione su i supponendo che $\chi^S \cdot \bar{x} \leq f(S)$ per ogni $S \subseteq A_{i-1}$, dunque $\chi^S \cdot \bar{x} = \sum_{e \in A_{i-1} \cap S} + x_{e_{\sigma(i)}} \leq f(S \cap A_{i-1}) + f(A_i) - f(A_{i-i}) \leq f(S) - f(A_{i-1} \cup S) + f(A_i)) = f(S)$. Infine, per ogni $S \subset E$, abbiamo $\chi^S \cdot \bar{x} = \sum_{e \in A_k \cap S} x_e \leq f(A_k \cap S) \leq f(S)$.
Mostriamo che $\bar{y}$ è ammissibile per il duale. Innanzitutto dato che $c_{\sigma(i)} \geq c_{\sigma(i+1)}$ allora $\bar{y} \geq 0$. Questo garantisce anche che $\sum_{S:\sigma(j) \in S} \bar{y}_S \geq c_{\sigma(j)}$ per $j > k$. Se $j \leq k$ allora $\sum_{S:\sigma(j) \in S} \bar{y}_S = \sum_{j \leq i \leq n} \bar{y}_{A_i} = \sum_{j \leq i < k} (c_{\sigma(i)} - c_{\sigma(i+1)}) - c_{\sigma(k)} = c_{\sigma(j)} \geq c_{\sigma(j)}$.
Analogamente a quanto fatto nella dimostrazione di 3.1.2 dimostriamo che $c \cdot \bar{x} = \sum_{S \subseteq E, S \neq \emptyset} f(S) \bar{y}_S$ e che quindi, per il teorema di dualità forte, abbiamo che $\bar{x}$ è una soluzione ottima del problema 3.4.1. □

Corollario 3.4.3. Da questo risultato segue che è possibile risolvere il programma lineare del problema 3.4.1 in tempo $O(n \log n + n\theta)$, dove $n = |E|$ e θ è la complessità computazione del calcolo della funzione f.

Dimostrazione. L'ordinamento iniziale richiede un tempo $O(n \log n)$, poi la costruzione dell'insieme avviene calcolando f negli insieme $A_1, A_2, \ldots, A_k$. □

Da questo fatto segue il seguente teorema che non dimostriamo.

Teorema 3.4.4. *Sia f una funzione submodulare, E un insieme finito su un reticolo L sulle parti di E con la relazione di inclusione. Allora è possibile trovare un insieme $\bar{A} \in L$ tale che*

$$f(\bar{A}) = \min_{A \in L} f(A)$$

in tempo polinomiale rispetto a $|E|$.

Bibliografia

[1] J. Oxley, "What is a matroid?." `https://www.math.lsu.edu/~oxley/survey4.pdf`, oct 2014.

[2] J. G. Oxley, *Matroid Theory*. Oxford Graduate Texts in Mathematics, Oxford University Press, 1993.

[3] B. Korte and J. Vygen, *Ottimizzazione Combinatoria: Teoria e Algoritmi*. Unitext, Springer, 4 ed., 2011.

[4] A. Schrijver, *Combinatorial Optimization*, vol. B. Springer, 2003.

[5] G. Pap, "A matroid intersection algorthm," *EGRES Technical Report n. 2008-10*, 2008.

[6] J. Edmonds, "Matroids and the greedy algorithm," *Mathematical Programming 1*, pp. 127–136, 1971.

[7] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," in *Combinatorial Structure and Their Applications*, pp. 69–87, 1970.