Il Teorema del Sandwich: Osservazioni e Commenti

Paola Bonetto **Walter Cazzola**
Sabrina De Capitani di Vimercati **Isabella Merlo**
Andrea Savigni **Italo Zoppis**
E-mail: {bonetto|cazzola|merloisa}@disi.unige.it
{decapita|savigni|italo}@dsi.unimi.it

Indice

Introduzione

L'esercizio richiedeva lo svolgimento dei seguenti tre punti:

1. dimostrazione del sandwich theorem;
2. riscrittura della dimostrazione delle disuguaglianze che coinvolgono le varie definizioni di ϑ;
3. dimostrazione della polinomialità del calcolo di ϑ.

La nostra intenzione era quella di scrivere un trattato "self-contained", accessibile anche a lettori senza preparazione specifica sulla materia.

I punti 1 e 2 sono stati una riscrittura dell'articolo [2], ovviamente approfondita e arricchita da numerosi particolari e dimostrazioni. Inoltre, alcune dimostrazioni sono state completamente riorganizzate e in alcuni casi scomposte in lemmi, al fine di ottenere una maggiore modularità e leggibilità. Ad esempio, nella dimostrazione $\vartheta_2(G, w) \leq \vartheta_3(G, w)$ è stato utilizzato un approccio top-down perché è stato ritenuto più intuitivo e comprensibile da parte di un non-specialista. Come ulteriore esempio del nostro approccio, la dimostrazione $\vartheta_4(G, w) \leq \vartheta(G, w)$ è stata riorganizzata in più lemmi per facilitarne la comprensione.

Per quanto riguarda il punto 3, il discorso è radicalmente diverso, in quanto tale argomento non è affatto coperto dall'articolo citato. In questo caso, dunque, è stato necessario procedere ad una ricerca bibliografica per individuare il materiale opportuno. Volendo anche in questo caso scrivere un trattato "self-contained" come nei due punti precedenti, abbiamo riportato nel lavoro tutte le conoscenze preliminari necessarie alla piena comprensione del problema (v. ad esempio la sezione 3.3 in cui è illustrato l'algoritmo dell'ellissoide, necessario per la dimostrazione del teorema di Yudin-Nemirovskiĭ).

Il lavoro è diviso in due parti: nella prima parte, che comprende le sezioni da 1 a 3, vengono trattati alcuni argomenti preliminari indispensabili alla comprensione del lavoro. Il lettore esperto in materia può tralasciare questa parte e passare direttamente alla seconda, che contiene il lavoro vero e proprio.
Nella **sezione 1** si trovano alcuni richiami di algebra lineare e algebra delle matrici, compresi alcuni teoremi (con dimostrazione) che verranno utilizzati nel seguito. Stesso discorso vale per la **sezione 2**, in cui vengono introdotte le nozioni fondamentali di teoria dei grafi. La **sezione 3** contiene una presentazione informale dei concetti di teoria della calcolabilità necessari per la comprensione dell'argomento. Si noti che i concetti non direttamente utilizzati nel lavoro non sono stati trattati, ad esempio il concetto di Macchina di Turing. Questa sezione contiene inoltre una definizione di alcuni problemi classici di ottimizzazione su insiemi convessi, oltre alla esposizione dettagliata dell'algoritmo dell'ellissoide.
La seconda parte comincia con la **sezione 4** in cui viene enunciato e dimostrato il Sandwich Theorem. Nella **sezione 5** si dimostra l'equivalenza delle varie definizioni alternative di ϑ. Infine, la **sezione 6** dimostra che ϑ è calcolabile in tempo polinomiale.

Parte I
Preliminari

1 Richiami di algebra lineare

1.1 Spazi lineari

Nel seguito tutti i vettori saranno considerati come vettori colonna, indicizzati o dai vertici di un grafo o da interi.

Definizione 1.1.1 (Prodotto scalare) *Consideriamo due vettori $a, b \in \mathbb{R}^n$:*

- *si dice* ***prodotto scalare*** *di a e b la quantità $a \cdot b = a^T b$, ovvero $\sum_{k=1}^{n} a_k b_k$;*
- *a e b si dicono* ***ortogonali*** *sse $a \cdot b = 0$.*

Definizione 1.1.2 (Norma) *Dato uno spazio lineare $\mathbb{R}^n$, si dice* ***norma*** *su $\mathbb{R}^n$ una funzione N: $\mathbb{R}^n \to \mathbb{R}$ che soddisfa le seguenti condizioni:*

- *$N(x) \geq 0$ $\forall x \in \mathbb{R}^n$, $N(x) = 0$ sse $x = 0$;*
- *$N(\alpha x) = |\alpha| N(x)$ $\forall x \in \mathbb{R}^n, \alpha \in \mathbb{R}$;*
- *$N(x + y) \leq N(x) + N(y)$ $\forall x, y \in \mathbb{R}^n$ (disuguaglianza triangolare).*

Per i nostri scopi sarà sufficiente considerare la norma Euclidea definita come segue.

Definizione 1.1.3 (Norma Euclidea) *Consideriamo un vettore $a \in \mathbb{R}^n$. Si dice* ***norma Euclidea*** *di a la quantità $\| a \| = \sqrt{a \cdot a}$, ovvero $\sqrt{\sum_{k=1}^{n} a_k^2;}$.*

Definizione 1.1.4 (Norma massima) *Dato un vettore $x \in \mathbb{R}^n$, si dice* ***norma massima*** *di x la quantità*

$$\| x \|_\infty = \max_{1 \leq i \leq n} |x_i| \,.$$

Nel seguito ogni qualvolta si parlerà di norma su uno spazio lineare $\mathbb{R}^n$, senza specificare il tipo di norma, si intenderà la norma Euclidea.

Osservazione. La nozione di ortogonalità data sopra, che è valida in $\mathbb{R}^n$ $\forall n \geq 1$, coincide, nel caso $n = 2$, con la usuale nozione di perpendicolarità geometrica. Consideriamo infatti due vettori $a, b \in \mathbb{R}^2$ perpendicolari fra loro. Applicando il teorema di Pitagora, si ha

$$\| a + b \|^2 = \| a \|^2 + \| b \|^2 \tag{1.1.1}$$

Inoltre, dalla definizione di norma scende

$$\| a+b \|^2 = (a+b)\cdot(a+b) = \| a \|^2 + \| b \|^2 + a^T b + b^T a \tag{1.1.2}$$

da cui, uguagliando i primi membri di (1.1.1) e (1.1.2), si ottiene

$$a^T b + b^T a = 2(a \cdot b) = 0$$

La dimostrazione del caso opposto è del tutto analoga e non verrà riportata. □

Lemma 1.1.1 (Cauchy-Schwarz) *Dati due vettori $a, b \in \mathbb{R}^n$, vale la seguente disuguaglianza:*

$$a \cdot b \leq \| a \| \, \| b \| \tag{1.1.3}$$

dove l'uguaglianza vale se e solo se uno dei vettori è multiplo scalare dell'altro.

Dimostrazione. Il secondo membro della (1.1.3) è sicuramente ≥ 0, mentre il primo membro non è vincolato in segno. Qualora però il primo membro fosse < 0, la disuguaglianza sarebbe banalmente verificata. Possiamo dunque assumere $a \cdot b \geq 0$ ed elevare entrambi i membri al quadrato. Ciò che dobbiamo dimostrare è dunque:

$$(a \cdot b)^2 \leq \| a \|^2 \, \| b \|^2$$

o, alternativamente,

$$\left(\sum_{k=1}^{n} a_k b_k \right)^2 \leq \left(\sum_{k=1}^{n} a_k^2 \right) \left(\sum_{k=1}^{n} b_k^2 \right)$$

Consideriamo la quantità $\displaystyle\sum_{k=1}^{n} (t a_k + b_k)^2$, che risulta essere $\geq 0 \ \forall \ t \in \mathbb{R}$ perché è una somma di quadrati e sviluppiamo il quadrato che si trova al suo interno; otterremo:

$$\sum_{k=1}^{n} (t^2 a_k^2 + 2t a_k b_k + b_k^2) = t^2 \sum_{k=1}^{n} a_k^2 + 2t \sum_{k=1}^{n} a_k b_k + \sum_{k=1}^{n} b_k^2$$

ovvero:

$$t^2 \| a \|^2 + 2t(a \cdot b) + \| b \|^2 \geq 0 \ \forall t \in \mathbb{R}$$

Evidentemente, questa disuguaglianza può essere vera per ogni t se e solo se il discriminante dell'equazione associata

$$t^2 \| a \|^2 + 2t(a \cdot b) + \| b \|^2 = 0 \tag{1.1.4}$$

è sempre non positivo (visto che $\| a \|^2 \geq 0$) e dunque se e solo se $(a \cdot b)^2 \leq \| a \|^2 \| b \|^2$, il che prova la tesi. Rimane ora da dimostrare che l'uguaglianza nella (1.1.3) vale se e solo se uno dei vettori è multiplo scalare dell'altro. Supponiamo dapprima che uno dei due sia multiplo dell'altro e scriveremo quindi, ad esempio, $a = kb, \ k \in \mathbb{R}$. Allora avremo:

$$(kb) \cdot b = k(b \cdot b) = k \| b \|^2$$

Al contrario, supponiamo che nella (1.1.3) valga l'uguaglianza. Allora il discriminante della (1.1.4) è nullo e dunque esiste ed è unico $t \in \mathbb{R}$ tale che

$$t^2 \| a \|^2 + 2t(a \cdot b) + \| b \|^2 = 0$$

il che equivale a dire che esiste un unico t tale che $\sum_{k=1}^{n}(ta_k + b_k)^2 = 0$. Poiché questa è una somma di quadrati, essa è nulla se e solo se i suoi addendi sono tutti nulli, cioè se e solo se $ta_k + b_k = 0 \ \forall k = 1, \ldots, n$, il che significa, per definizione, che i vettori a e b sono linearmente dipendenti. □

Definizione 1.1.5 (Segmento) *Dato uno spazio lineare L su $\mathbb{R}$ e dati due punti a e b di L, si dice* ***segmento*** *in L che unisce a e b l'insieme di tutti e soli i punti di L della forma $\lambda a + (1-\lambda)b$ dove $0 \leq \lambda \leq 1$.*

Nel caso dello spazio lineare $\mathbb{R}^2$, questo concetto coincide con l'usuale concetto di segmento geometrico.

Definizione 1.1.6 (Insieme convesso) *Dato uno spazio lineare L su $\mathbb{R}$, un insieme $M \subseteq L$ è detto* ***convesso*** *se e solo se ogni qualvolta esso contiene due punti a e b, contiene anche il segmento che li unisce.*

Ad esempio, nello spazio $\mathbb{R}^3$ sono convessi la sfera, il parallelepipedo, il cono, ecc. mentre non è convesso il toro.

Lemma 1.1.2 *Dato uno spazio lineare L su $\mathbb{R}$ e una famiglia M_α di insiemi convessi in L, l'insieme $M = \bigcap_\alpha M_\alpha$ è anch'esso convesso.*

Dimostrazione. Siano a e b due punti di M, allora essi appartengono a tutti gli M_α. Ma, essendo questi convessi, anche il segmento che unisce a e b appartiene ad ognuno di essi e dunque anche a M. □

Definizione 1.1.7 (Involucro convesso) *Dato uno spazio lineare L su $\mathbb{R}$ e dato un qualunque sottoinsieme $M \subseteq L$, si dice* ***involucro convesso*** *di M il più piccolo insieme convesso di L che contiene M.*

Osservazione. Tale insieme minimo esiste perché almeno lo spazio lineare stesso L è convesso e contiene M.

Definizione 1.1.8 *Dato un insieme $K \subseteq \mathbb{R}^n, a \in \mathbb{R}^n$ ed un numero reale positivo ε, diamo le seguenti definizioni:*

1. *si dice* ***sfera di raggio ε attorno a K*** *l'insieme*

$$S(K, \varepsilon) = \{x \in \mathbb{R}^n \mid \| x - y \| \leq \varepsilon \text{ per qualche } y \in K\};$$

2. *si dice* ***sfera di raggio ε con centro a*** *l'insieme*

$$S(a, \varepsilon) = S(\{a\}, \varepsilon);$$

3. *si dice* ***sfera interna di raggio ε di K*** *l'insieme*

$$S(K, -\varepsilon) = \{x \in K \mid S(x, \varepsilon) \subseteq K\}.$$

Nel caso in cui $K \subseteq \mathbb{R}^{n\times n}$ le definizioni sono analoghe, ma si ricorre all'uso della norma di Frobenius $\|\cdot\|_2$ definita su matrici.

Definizione 1.1.9 (Poliedro e politopo) *Data una matrice $A \in \mathbb{R}^{m\times n}$ e $b \in \mathbb{R}^n$, l'espressione $Ax \leq b$ viene detta* ***sistema lineare di disequazioni****, mentre l'espressione $Ax = b$ è detta* ***sistema lineare di equazioni****. L'insieme delle soluzioni di un sistema lineare di disequazioni, ovvero l'insieme $\{x \in \mathbb{R}^n \mid Ax \leq b\}$ è detto* **poliedro**. *Un poliedro P limitato, ovvero tale che $\exists R > 0 \mid P \subseteq S(0, R)$ è detto* **politopo**. *Nel caso in cui $a \in \mathbb{R}^n \setminus \{0\}$ e $a_0 \in \mathbb{R}$ il poliedro $\{x \in \mathbb{R}^n \mid a^T x \leq a_0\}$ è detto* ***semispazio*** *e il poliedro $\{x \in \mathbb{R}^n \mid a^T x = a_0\}$ è detto* ***iperpiano****.*

Definizione 1.1.10 *Dati $n+1$ vettori $x, x_1, \ldots, x_n \in \mathbb{R}^n$ e dato $S \subseteq \mathbb{R}^n$, diamo le seguenti definizioni:*

1. *x è detto* ***combinazione affine*** *di $x_1, \ldots, x_n$ se e solo se:*
   (a) *x è combinazione lineare di $x_1, \ldots, x_n$, ovvero $\exists\ \lambda \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \lambda_i x_i$;*
   (b) $\sum_{i=1}^{n} \lambda_i = 1$.
2. *si dice* ***involucro affine*** *di S (e si denoterà con $\mathrm{aff}(S)$) l'insieme di tutte e sole le combinazioni affini finite di elementi di S. Si ha per convenzione $\mathrm{aff}(\emptyset) = \emptyset$;*
3. *S è detto* ***sottospazio affine*** *se e solo se $S = \mathrm{aff}(S)$, ovvero:*
   (a) *ogni elemento di S è esprimibile come combinazione affine di elementi di S;*
   (b) *ogni combinazione affine di elementi di S appartiene a S.*
4. *S è* ***affinemente indipendente*** *se e solo se S non contiene alcun elemento che è combinazione affine propria* di elementi di S;*
5. *si dice* ***dimensione*** *di S ($\dim(S)$) la cardinalità del più grande sottoinsieme affinemente indipendente di S meno 1. S è detto* ***di dimensione massima*** *se e solo se $\dim(S) = n$.*

Definizione 1.1.11 *Diamo ora alcune definizioni riguardanti gli insiemi convessi:*

1. *un* ***insieme convesso circoscritto*** *è una tripla (K;n,R) dove:*
   (a) *$K \subseteq \mathbb{R}^n$ è un insieme convesso;*
   (b) *$R \in \mathbb{Q}^+$ è un numero razionale positivo tale che $K \subseteq S(0, R)$.*
2. *un* ***insieme convesso ben delimitato*** *è una quadrupla (K;n,R,r) dove:*
   (a) *(K;n,R) è un insieme convesso circoscritto;*

*Si dice **propria** una combinazione affine in cui $\lambda_i \neq 0\ \forall i = 1, \ldots, n$

(b) *K contiene una sfera di raggio r e di centro imprecisato.*

3. *un **insieme convesso centrato** è una quintupla (K;n,R,r,a) dove:*

   (a) *(K;n,R,r) è un insieme convesso ben delimitato;*

   (b) *$a \in \mathbb{Q}^n$ è un vettore tale che $S(a, r) \subseteq K$.*

4. *un **corpo convesso** è un insieme convesso compatto e di dimensione massima. Per i corpi convessi possono essere date le stesse definzioni date sopra per gli insiemi convessi; avremo quindi corpi convessi circoscritti, ben delimitati e centrati.*

Definizione 1.1.12 (*n*-cubo) *Si dice **n-cubo** l'insieme*

$$\{x \in \mathbb{R}^n \mid 0 \leq x_i \leq 1 \ \forall i = 1, \ldots, n\}$$

L'n-cubo è un insieme convesso per ogni n. Infatti, comunque scelti x e y appartenenti all'n-cubo, verifichiamo che l'insieme:

$$P = \{z \in \mathbb{R}^n \mid z = \lambda x + (1 - \lambda)y\}$$

è incluso nell'n-cubo. Dato $z = [z_1, \ldots, z_n] \in P$, il generico componente z_i avrà la forma: $z_i = \lambda x_i + (1 - \lambda)y_i \ \forall i = 1, \ldots, n$. Tale quantità è evidentemente non negativa perché è una somma di quantità non negative. Resta quindi da dimostrare che essa è non maggiore di 1. Avremo:

$$\begin{aligned} z_i = \lambda x_i + (1 - \lambda)y_i &\leq 1 \\ \lambda(x_i - y_i) &\leq 1 - y_i \end{aligned}$$

Ora, se $(x_i - y_i) \leq 0$, la disuguaglianza è banalmente verificata. Possiamo dunque assumere $(x_i - y_i) > 0$. Allora ciò che bisogna verificare è:

$$\lambda \leq \frac{1 - y_i}{x_i - y_i}$$

Poiché λ per ipotesi è sempre ≤ 1, se dimostriamo che il secondo membro di questa disuguaglianza è sempre ≥ 1, abbiamo dimostrato la tesi.

$$\begin{aligned} \frac{1 - y_i}{x_i - y_i} &\geq 1 \\ (1 - y_i) &\geq (x_i - y_i) \\ x_i &\leq 1 \end{aligned}$$

che è sempre vera per ipotesi. □

Definizione 1.1.13 (*n*-simplesso) *Si dice **n-simplesso** l'insieme*

$$\{x \in \mathbb{R}^n, \ x \geq 0 \mid \sum_{i=1}^{n} x_i \leq 1\}$$

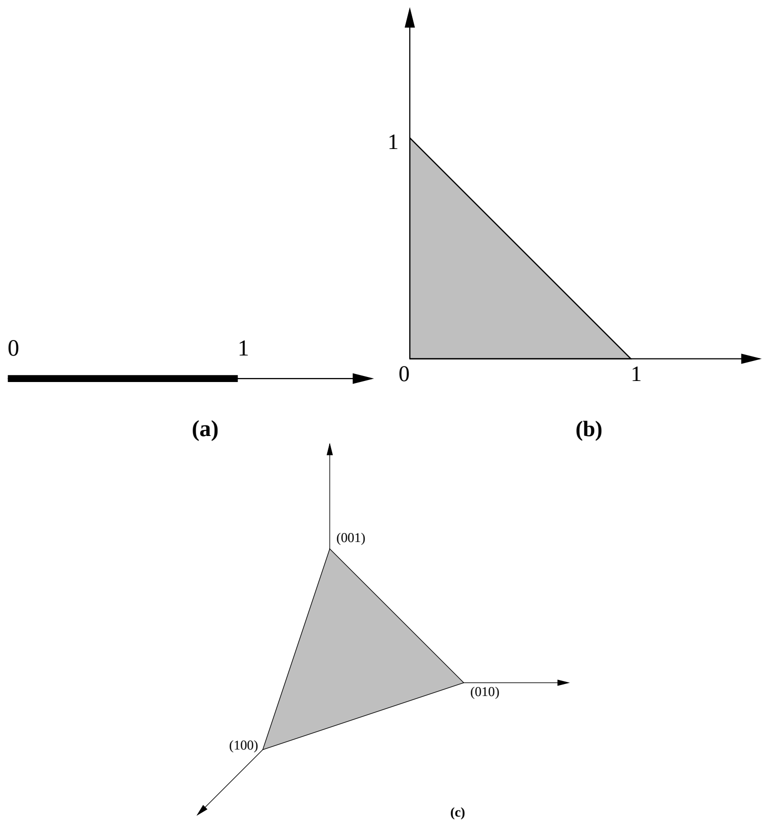

Figura 1.1.1: 1-simplesso(a), 2-simplesso(b), 3-simplesso(c)

In termini informali, si può dire che l'n-simplesso è la più semplice figura geometrica finita di dimensione n. Si può inoltre notare che l'n-simplesso è la parte di $\mathbb{R}^n$ delimitata dagli $n+1$ $(n-1)$-simplessi. Lo 0-simplesso è, per convenzione, un punto; l'1-simplesso è una linea (in particolare, è il segmento che unisce i punti 0 e 1); il 2-simplesso è un triangolo (il triangolo di vertici $(1,0)$, $(0,0)$, $(0,1)$, ovvero la parte di $\mathbb{R}^2$ delimitata dai 3 2-simplessi); il 3-simplesso è il tetraedro delimitato dai quattro 2-simplessi, cioè dai quattro triangoli di vertici $(0,0,0)$, $(0,0,1)$, $(0,1,0)$ e $(1,0,0)$ e così via. In figura 1.1.1 sono riportati gli n-simplessi per $n = 1, 2, 3$. Sottolineiamo altresì che l'n-simplesso è un insieme convesso per ogni n. Infatti, comunque presi x e y appartenenti all'n-simplesso, avremo:

$$\lambda x + (1-\lambda)y = \lambda \sum_{i=1}^{n} x_i + (1-\lambda) \sum_{i=1}^{n} y_i \leq \lambda + (1-\lambda) = 1$$

1.2 Algebra delle matrici

Definizione 1.2.1 (Prodotto scalare) *Consideriamo due matrici $A, B \in \mathbb{R}^{m\times n}$. Si dice* ***prodotto scalare*** *di A e B la quantità $A \cdot B = \mathrm{tr}(A^T B)$, ovvero $\sum_{i=1}^{n} (A^T B)_{ii}$.*

Definizione 1.2.2 (Norma di matrice) *Dato uno spazio lineare $\mathbb{R}^{m\times n}$, si dice* ***norma di matrice*** *su $\mathbb{R}^{m\times n}$ una funzione M: $\mathbb{R}^{m\times n} \to \mathbb{R}$ che soddisfa le seguenti condizioni:*

- $M(A) \geq 0 \; \forall A \in \mathbb{R}^{m\times n}$, $M(A) = 0$ *sse* $A = 0$;
- $M(\alpha A) = |\alpha| \, M(A) \; \forall A \in \mathbb{R}^{m\times n}, \alpha \in \mathbb{R}$;
- $M(A+B) \leq M(A) + M(B) \; \forall A, B \in \mathbb{R}^{m\times n}$ *(disuguaglianza triangolare).*

Si osservi che il concetto di norma di matrice qui introdotto è una estensione di quello presentato nella definizione 1.1.3. Infatti in questo caso si parla di norma su uno spazio lineare $\mathbb{R}^{m\times n}$.

Definizione 1.2.3 (Norme di Matrici) *Sia $A \in \mathbb{R}^{n\times n}$; si definiscono le seguenti norme:*

- *norma spettrale:* $||A|| = \sqrt{\Lambda(A^T A)}$ *(dove $\Lambda(A)$ è il più grande autovalore di A).*
- *norma di Frobenius:* $||A||_2 = \sqrt{\displaystyle\sum_{i,j=1}^{n} A_{ij}^2}$
- *norma massima:* $||A||_{\max} = n \max |A_{ij}| \; i, j = 1, \ldots n$

Definizione 1.2.4 (Compatibilità tra norme) *Diamo due definizioni di compatibilitá tra norme definite su differenti spazi lineari.*

1. *Sia N_1 una norma su $\mathbb{R}^n$ e N_2 una norma su $\mathbb{R}^m$. La norma di matrice M su $\mathbb{R}^{m\times n}$ si dice **compatibile** con N_1 e N_2 se $N_2(Ax) \leq M(A)N_1(x) \; \forall x \in \mathbb{R}^n$ e $\forall A \in \mathbb{R}^{m\times n}$.*
2. *Sia N una norma su $\mathbb{R}^n$. La norma di matrice M su $\mathbb{R}^{n\times n}$ si dice **compatibile** con N se $N(Ax) \leq M(A)N(x) \; \forall x \in \mathbb{R}^n$ e $\forall A \in \mathbb{R}^{n\times n}$.*

Definizione 1.2.5 (Determinante) *Data $A \in \mathbb{R}^{n\times n}$ si definisce determinante la quantità espressa dalla formula di Laplace:*

$$\det(A) = \sum_{i-1}^{n} (-1)^{i+1} a_{i1} \det\left(\left(A'\right)_{i1}\right)$$

dove $(A')_{i1}$ è una matrice in $\mathbb{R}^{(n-1)\times(n-1)}$ ottenuta togliendo da A la i-esima riga e la prima colonna.

Definizione 1.2.6 (Formula di Binet) *Date A, B e C appartenenti a $\mathbb{R}^{n\times n}$ se vale $A = B \cdot C$ allora si ha:*

$$\det(A) = \det(B)\det(C)$$

Definizione 1.2.7 (Matrice ortogonale) *Una **matrice ortogonale** Q è una matrice quadrata tale che $Q^T Q = I$ dove I è la matrice identità.*

In altre parole, una matrice è ortogonale se e solo se la sua inversa è uguale alla sua trasposta. Poiché data una qualsiasi matrice A abbiamo che:

$$(A^T A)_{uv} = \sum_{k=1}^{n} (A^T)_{uk} A_{kv} = \sum_{k=1}^{n} A_{ku} A_{kv} = A_u \cdot A_v \tag{1.2.1}$$

possiamo dire che Q è ortogonale se e solo se:

1. $\| Q_i \| = Q_i \cdot Q_i = (Q^T Q)_{ii} = 1 \ \forall i$ (le sue colonne sono vettori di norma uno);
2. $Q_i \cdot Q_j = (Q^T Q)_{ij} = 0 \ \forall i, j \mid i \neq j$ (le sue colonne sono vettori a due a due ortogonali).

Definizione 1.2.8 (Matrice simmetrica) *Una **matrice simmetrica** A è una matrice quadrata tale che $A = A^T$.*

Definizione 1.2.9 (Sottomatrice principale) *Sia $A \in \mathbb{R}^{n \times n}$ una matrice e $I = \{1, \ldots, n\}$ un insieme di indici. Si dice **sottomatrice principale** di A di ordine $|I|$ la matrice A_{II} che ha come righe e colonne quelle indicate dall'insieme I.*

Definizione 1.2.10 (Rango) *Una matrice $A \in \mathbb{R}^{n \times n}$ ha **rango** r se soddisfa le seguenti due proprietà:*

1. *esiste una sottomatrice principale A_{II} di ordine r con determinante diverso da zero;*
2. *tutte le sottomatrici principali A_{II} di ordine $(r+1)$ hanno determinante nullo.*

Definizione 1.2.11 (Matrice Semidefinita Positiva) *A si dice **semidefinita positiva** se è una matrice simmetrica e $x^T A x \geq 0$ per ogni $x \in \mathbb{R}^n \setminus \{0\}$. Inoltre sono equivalenti le seguenti condizioni:*

1. *A è semidefinita positiva*
2. *Tutti gli autovalori di A sono reali non-negativi*
3. *$A = B^T B$ per qualche B*
4. *$\det(A_{II}) \geq 0$ per ogni sottomatrice principale A_{II} di A*
5. *Esiste una sottomatrice principale semidefinita positiva A_{II} di A t.c. $|I| = rango(A)$*

Nel caso in cui $x^T A x > 0$, la matrice A si dice ***definita positiva***.

Lemma 1.2.1 *Dati k vettori a due a due ortogonali, esiste una matrice ortogonale avente questi vettori come prime k colonne.*

Dimostrazione. La dimostrazione procede per induzione.

- Sia $k = 1$, e sia $x \in \mathbb{R}^d$ avente norma unitaria. Se $x_1 = 1$ (e dunque $x_i = 0 \ \forall i = 2, \ldots, d$), la matrice cercata è la matrice identità. Altrimenti costruiamo una nuova matrice come segue. Definiamo il vettore y nel seguente modo:

$$y_1 = \sqrt{\tfrac{1-x_1}{2}} \quad y_j = -\tfrac{x_j}{2y_1} \quad \text{per } 1 < j \leq d$$

Si può facilmente verificare che il vettore y così ottenuto ha norma unitaria. Infatti

$$\| y \|^2 = y_1^2 + \frac{x_2^2 + \ldots + x_d^2}{4y_1^2} = \frac{1 - x_1}{2} + \frac{1 - x_1^2}{2(1 - x_1)} = 1$$

A partire dal vettore y, costruiamo ora la matrice

$$Q = I - 2yy^T$$

Dimostriamo ora che:

1. x è la prima colonna di Q;
2. Q è ortogonale.

La matrice Q ha la forma:

$$Q = \begin{bmatrix} 1 - 2y_1^2 & -2y_1y_2 & \ldots & -2y_1y_d \\ \ldots & \ldots & \ldots & \ldots \\ -2y_dy_1 & -2y_dy_2 & \ldots & 1 - 2y_d^2 \end{bmatrix}$$

Il punto 1 può essere verificato tramite una semplice sostituzione. Per quanto riguarda invece il punto 2, osserviamo che

$$Q^TQ = Q^2 = I - 4yy^T + 4yy^Tyy^T = I$$

- Supponiamo ora di aver dimostrato il lemma per un generico $k \geq 1$ e lo dimostreremo per $k+1$. Sia Q una matrice ortogonale e sia x un vettore ortogonale alle sue prime k colonne. Vogliamo costruire una nuova matrice Q' avente come prime k colonne le prime k colonne di Q e come $(k+1)$-esima colonna il vettore x. Poiché x è per ipotesi ortogonale alle prime k colonne, sarà

$$Q^Tx = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ z \end{bmatrix}$$

dove il vettore Q^Tx ha le prime k righe nulle, mentre il vettore z ha dimensione $(d - k)$. Questo vettore risulta avere norma unitaria, in quanto

$$\| z \|^2 = Q^Tx \cdot Q^Tx = x^TQQ^Tx = x^Tx = 1$$

Avendo z norma unitaria, deve essere $z \neq 0$ e dunque $k < d$. A questo punto abbiamo un vettore z di dimensione $(d-k)$ quindi possiamo utilizzare la base di induzione per costruire una matrice ortogonale R di ordine $(d-k)$ avente z come prima colonna. Allora, detta P la matrice

$$P = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & R \end{bmatrix}$$

la matrice $Q' = QP$ è la matrice cercata. Infatti:

- la $(k+1)$-esima colonna di Q' coincide con il vettore x, poiché la $(k+1)$-esima colonna di P è pari a $Q^T x$ e quindi la $(k+1)$-esima colonna di Q' è pari a $QQ^T x$ che è uguale a x essendo Q ortogonale;
- Q' è ortogonale perché è il prodotto di matrici ortogonali. Infatti, Q è ortogonale per ipotesi induttiva, P lo è per costruzione.

□

Lemma 1.2.2 *Una matrice quadrata A è simmetrica se e solo se può essere espressa nella forma $A = QDQ^T$ dove Q è una matrice ortogonale e D è una matrice diagonale.*

Dimostrazione. Supponiamo che una matrice quadrata A possa essere espressa nella forma $A = QDQ^T$ dove Q è una matrice ortogonale e D è una matrice diagonale. Allora $A^T = (QDQ^T)^T$. Poiché $\forall A, B\ (AB)^T = B^T A^T$, $A^T = QD^T Q^T$, ma, essendo D diagonale, $D^T = D$ e quindi $A = A^T$. Viceversa, sia A una matrice simmetrica. Quello che vogliamo dimostrare è che esiste una matrice ortogonale Q e una matrice diagonale D tale che $A = QDQ^T$ o, analogamente, $D = Q^T AQ$. La dimostrazione procede per induzione sull'ordine di A.

Passo base. Sia A una matrice simmetrica di ordine 2, λ_1 un autovalore di A e x_1 il corrispondente autovettore (senza perdita di generalità possiamo supporre che $\| x_1 \| = 1$). Scegliamo un vettore x_2 sempre di norma unitaria e tale per cui $x_1 \cdot x_2 = 0$. Per il lemma 1.2.1 possiamo costruire una matrice ortogonale Q avente questi vettori come sue colonne. Dunque si ha:

$$Q^T AQ = \begin{bmatrix} x_1^T \\ x_2^T \end{bmatrix} A\,[x_1 x_2] = \begin{bmatrix} x_1^T \\ x_2^T \end{bmatrix} [\lambda_1 x_1 A x_2]$$

essendo $Ax_1 = \lambda_1 x_1$. Svolgengo il prodotto abbiamo:

$$Q^T AQ = \begin{bmatrix} \lambda_1 x_1^T x_1 & x_1^T A x_2 \\ \lambda_1 x_2^T x_1 & x_2^T A x_2 \end{bmatrix} = \begin{bmatrix} \lambda_1 & b_1^T \\ 0 & n_1 \end{bmatrix}$$

dove $b_1^T = x_1^T A x_2$ e $n_1 = x_2^T A x_2$ è un numero. Essendo $Q^T AQ$ una matrice simmetrica ($(Q^T AQ)^T = Q^T A^T Q = Q^T AQ$) avremo che $b_1^T = 0$ e pertanto la matrice $\begin{bmatrix} \lambda_1 & b_1^T \\ 0 & n_1 \end{bmatrix}$ è una matrice diagonale.

Passo di induzione. Supponiamo ora di aver dimostrato il teorema per matrici di ordine $(n-1)$. Sia λ_1 un autovalore di A e sia x_1 il corrispondente autovettore di norma unitaria. Per il lemma 1.2.1 possiamo costruire una matrice ortogonale Q avente x_1 come prima colonna, cioè

$Q = [x_1 u_2 \dots u_n]$ e, ponendo $Q_1 = [u_2 \dots u_n]$, $Q_1^T x_1 = 0$. Con passaggi analoghi a quelli visti per il passo base ottengo:

$$Q^T A Q = \begin{bmatrix} \lambda_1 & b_1^T \\ 0 & A_1 \end{bmatrix}$$

dove $b_1^T = x_1^T A Q_1$ e $A_1 = Q_1^T A Q_1$ è una matrice quadrata di ordine (n-1). Per A_1 esiste una matrice ortogonale W di ordine $(n-1)$ tale che $D = W^T A_1 W$ dove D è una matrice diagonale (è vero perché si suppone di aver dimostrato il teorema per matrici di ordine $(n-1)$). La matrice $V = \begin{bmatrix} 1 & 0 \\ 0 & W \end{bmatrix}$ è una matrice ortogonale. Inoltre

$$V^T Q^T A Q V = \begin{bmatrix} 1 & 0 \\ 0 & W^T \end{bmatrix} \begin{bmatrix} \lambda_1 & b_1^T \\ 0 & A_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & W \end{bmatrix}$$

Svolgendo i calcoli e ponendo $U = QV$ si ha:

$$U^T A U = \begin{bmatrix} \lambda_1 & b_1^T W \\ 0 & W^T A_1 W \end{bmatrix} = \begin{bmatrix} \lambda_1 & b_1^T W \\ 0 & D \end{bmatrix}$$

La matrice U è una matrice ortogonale perché è data dal prodotto di matrici ortogonali, $b_1^T W = 0$ perché $U^T A U$ è una matrice simmetrica (vedi passo base) e per finire $\begin{bmatrix} \lambda_1 & b_1^T W \\ 0 & D \end{bmatrix}$ è una matrice diagonale perché D è diagonale. □

Lemma 1.2.3 *Se M è una norma di matrice su $\mathbb{R}^{n \times n}$ compatibile con qualche norma su $\mathbb{R}^n$, allora $|\lambda| \leq M(A)$ per ogni autovalore λ di $A \in \mathbb{R}^{n \times n}$.*

Dimostrazione. Sia N una norma su $\mathbb{R}^n$ compatibile con M; $N(Ax) \leq M(A)N(x)$ $\forall x \in \mathbb{R}^n$ e $\forall A \in \mathbb{R}^{n \times n}$. Sia inoltre λ un autovalore di A e $\bar{x}$ il corrispondente autovettore. Dalla definizione 1.1.3 scende che $N(\lambda \bar{x}) = |\lambda| N(\bar{x})$. Inoltre poiché $A\bar{x} = \lambda \bar{x}$ possiamo scrivere che $|\lambda| N(\bar{x}) = N(\lambda \bar{x}) = N(A\bar{x})$. La compatibilità di M con N è valida per ogni vettore $x \in \mathbb{R}^n$ e dunque sarà valida anche per $\bar{x}$. Per questo motivo si ha:

$$|\lambda| N(\bar{x}) = N(\lambda \bar{x}) = N(A\bar{x}) \leq M(A)N(\bar{x})$$

$$|\lambda| \leq M(A)$$

□

2 Richiami di teoria dei grafi

2.1 Grafi

Definizione 2.1.1 (Grafo) *Un **grafo** G è una coppia $\langle V, E \rangle$ dove:*

- *V è un insieme ordinato $\{v_1, \dots, v_n\}$ i cui elementi sono detti **vertici**;*
- *$E \subseteq V \times V$ è un insieme i cui elementi sono detti **archi**.*

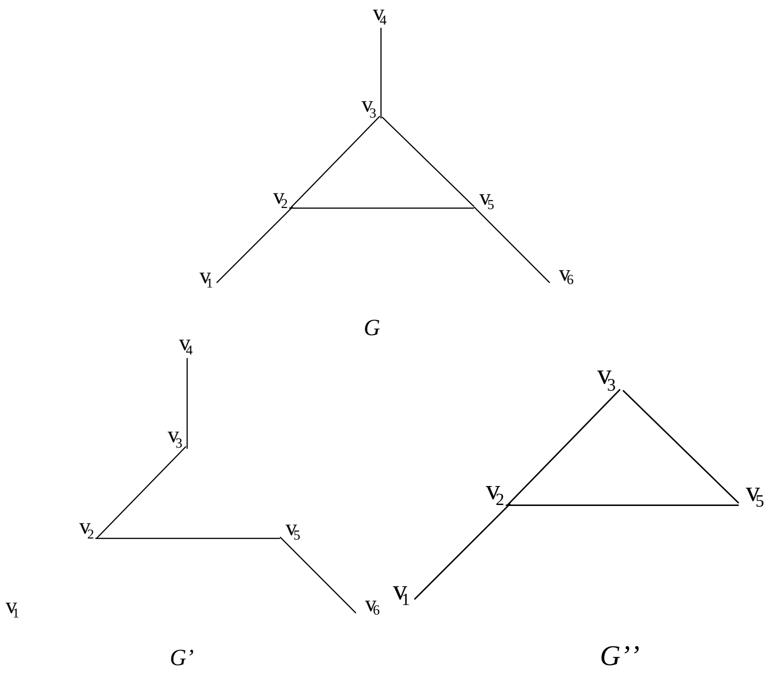

Figura 2.1.1: $G' \subseteq G$, mentre G'' è sottografo di G.

Per i nostri scopi, un grafo si intenderà sempre non orientato, il che significa che $\forall i, j = 1, \ldots, n$ $(v_i, v_j) \in E \rightarrow (v_j, v_i) \in E$. Due nodi v_i e v_j tali che $(v_i, v_j) \in E$ si dicono **connessi** (e verranno denotati con $v_i — v_j$), altrimenti si dicono **sconnessi** (nel qual caso, si userà la notazione $v_i \not\!\!— v_j$). Un grafo in cui tutti i nodi sono connessi si dice **completo**.

Definizione 2.1.2 (Grafo complementare) *Dato un grafo $G = \langle V, E \rangle$, si dice* ***grafo complementare*** *di G il grafo $\overline{G} = \langle V, \overline{E} \rangle$ avente lo stesso insieme di vertici di G e in cui $\overline{E} = \{(v_i, v_j) \in V \times V \mid (v_i, v_j) \notin E\}$.*

Definizione 2.1.3 (Sottografo) *Dato un grafo $G = \langle V, E \rangle$, si dice* ***sottografo*** *di G un grafo $G' = \langle V', E' \rangle$ dove:*

- *$V' \subseteq V$;*
- *$E' = \{(v_i, v_j) \in E \mid v_i \in V' \wedge v_j \in V'\}$.*

Un sottografo G' di G è dunque un grafo i cui vertici sono un sottoinsieme dei vertici di G e i cui archi sono tutti e soli gli archi di G che hanno come estremi elementi di V'.

Definizione 2.1.4 (Grafo parziale) *Dato un grafo $G = \langle V, E \rangle$, si dice* ***grafo parziale*** *di G un grafo $G' = \langle V, E' \rangle$ avente lo stesso insieme di vertici V e $E' \subseteq E$ cioè $\forall\ v_i, v_j \in V,\ v_i — v_j$ in G' implica $v_i — v_j$ in G.*

La relazione di grafo parziale verrà denotata con il simbolo $\subseteq$. Da notare che, come evidenziato in figura 2.1.1, le relazioni di sottografo e di grafo parziale sono relazioni diverse.

Definizione 2.1.5 (Insieme stabile) *Dato un grafo $G = \langle V, E \rangle$, un insieme $S \subseteq V$ si dice* ***stabile*** *sse $\forall v_i, v_j \in S \ (v_i, v_j) \notin E$.*

Dato un grafo $G = \langle V, E \rangle$, un insieme stabile di G può anche essere visto come un sottografo $G' = \langle V', E' \rangle$ dove $E' = \emptyset$, cioè in cui i nodi sono tutti sconnessi fra loro.

Definizione 2.1.6 (Clique) *Dato un grafo $G = \langle V, E \rangle$, un sottografo $Q = \langle V', E' \rangle$ si dice* ***clique*** *sse $\forall v_i, v_j \in V' \ (v_i, v_j) \in E'$.*

In altre parole, una clique è un sottografo completo. La clique di ordine n viene solitamente indicata con K_n. Di conseguenza, il grafo completamente sconnesso verrà indicato con $\overline{K}_n$, essendo esso il grafo complementare della clique di ordine n.
Diamo ora alcune definizioni che torneranno utili in seguito.

Definizione 2.1.7 *Dato un grafo G:*

- *$\omega(G)$ è la dimensione della massima clique di G;*
- *$\chi(G)$ è il numero cromatico di G, ovvero il minimo numero di colori necessari per colorare i vertici di G in modo tale che due vertici connessi abbiano sempre colori diversi;*
- *$\overline{\chi}(G)$ è il minimo numero di clique che copre i vertici di G.*

2.2 Labeling reali e vettoriali

Definizione 2.2.1 (Labeling reale) *Dato un grafo $G = \langle V, E \rangle$ avente n vertici, assegnare un* ***labeling reale*** *al grafo significa associare un numero reale x_v ad ognuno dei suoi vertici.*

Un labeling reale si può dunque pensare come un vettore di $\mathbb{R}^n$.

Definizione 2.2.2 (Labeling caratteristico) *Dato un grafo $G = \langle V, E \rangle$ e dato un sottoinsieme U di V, si dice* ***labeling caratteristico*** *di U un labeling reale di G tale che*

$$x_v = \begin{cases} 1 & \textit{se } v \in U; \\ 0 & \textit{se } v \notin U. \end{cases}$$

Un labeling caratteristico può dunque essere utilizzato per individuare un dato sottoinsieme dei vertici di un grafo. In particolare, risultano interessanti i seguenti labeling caratteristici:

- **labeling stabile** è il labeling caratteristico di un insieme stabile (un esempio è mostrato in figura 2.2.1(a));
- **clique labeling** è il labeling caratteristico di una clique (un esempio è mostrato in figura 2.2.1(b)).

Più in generale, un labeling può anche essere realizzato assegnando ad ogni vertice del grafo un vettore di $\mathbb{R}^d$, con d arbitrario, ottenendo così un **labeling vettoriale**†. Un caso particolarmente interessante di labeling vettoriale è il seguente.

†Nel seguito, si indicherà con d la dimensione dei vettori di un labeling vettoriale.

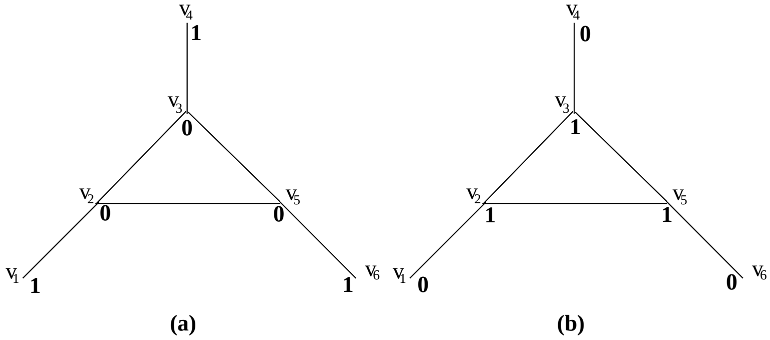

Figura 2.2.1: Un esempio di labeling stabile e di clique labeling

Definizione 2.2.3 (Labeling ortogonale) *Dato un grafo $G = \langle V, E \rangle$, un* ***labeling ortogonale*** *per G è un labeling vettoriale in cui $\forall v_i, v_j \in V$, $v_i \not\sim v_j \rightarrow (a_i \cdot a_j = 0)$, dove a_i e a_j indicano rispettivamente il vettore associato al nodo v_i e al nodo v_j.*

Un labeling ortogonale è dunque un labeling vettoriale in cui a due nodi non connessi sono associati vettori ortogonali. Si noti che nessuna condizione è data per nodi connessi. Inoltre, si può notare che moltiplicando un qualunque vettore di un labeling ortogonale per uno scalare non nullo, la proprietà di ortogonalità non viene violata.

Definizione 2.2.4 (Labeling ortogonale normalizzato) *Dato un grafo $G = \langle V, E \rangle$, un* ***labeling ortogonale normalizzato*** *per G è un labeling ortogonale a per cui vale*

$$\sum_v \| a_v \|^2 = 1$$

Definizione 2.2.5 (Costo) *Dato un grafo $G = \langle V, E \rangle$ e un labeling ortogonale ad esso associato, si dice* ***costo*** *del vettore a_i associato al vertice v_i la quantità*

$$c(a_i) = \begin{cases} 0 & se\ a_i = 0; \\ \frac{a_{1i}^2}{\| a_i \|^2} & altrimenti. \end{cases}$$

dove con a_{ji} si intende la componente j-esima di a_i.

Il costo, così come è stato definito, risulta godere delle seguenti proprietà:

1. $0 \leq c(a_i) \leq 1\ \forall i$;

2. $c(a_i) = c(ta_i)\ \forall i\ \forall t \in \mathbb{R}, t \neq 0$.

Definizione 2.2.6 (Matrice ammissibile) *Dato un grafo $G = \langle V, E \rangle$ e un labeling reale w, si dice* ***matrice ammissibile (o feasible)*** *una matrice A tale che:*

- *$a_{vv} = w_v$ per tutti i $v \in V$;*

- *$a_{uv} = \sqrt{w_u w_v}$ ogni qualvolta $u \not\sim v$ in G.*

Gli altri elementi di A non sono vincolati.

Lemma 2.2.1 *Dato un grafo $G = \langle V, E\rangle$, un labeling ortogonale su di esso e un insieme stabile $S \subseteq V$ allora*

$$\sum_{v_i \in S} c(a_i) \leq 1$$

Dimostrazione. Si può assumere, senza perdita di generalità, che $\| a_i \| = 1$ $\forall i$. Infatti, se fosse $\| a_i \| = h$, $h \neq 1$, si potrebbe semplicemente moltiplicare a_i per $\frac{1}{h}$ e si otterrebbe un nuovo vettore avente lo stesso costo e norma unitaria. Inoltre, per quanto visto sopra, la moltiplicazione di un vettore per uno scalare non compromette l'ortogonalità del labeling. Sia k la cardinalità di S. Essendo S un insieme stabile, per la definizione di labeling ortogonale risulta che i vettori associati ai vertici di S sono tutti a due a due ortogonali. Allora, dal lemma 1.2.1 scende che esiste una matrice ortogonale $d \times d$ avente i vettori del labeling associati agli elementi di S come prime k colonne. Otterremo quindi una matrice del tipo:

$$Q = \begin{bmatrix} q_{11} & \cdots & q_{1k} & \cdots & q_{1d} \\ q_{21} & \cdots & q_{2k} & \cdots & q_{2d} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ q_{d1} & \cdots & q_{dk} & \cdots & q_{dd} \end{bmatrix}$$

dove $q_{1i} = \sqrt{c(a_i)}$, $i = 1, \ldots, k$, perché i vettori a_i hanno, come detto, tutti norma unitaria e dunque il loro costo coincide con il quadrato del primo elemento. La somma dei costi coincide dunque con la somma dei q_{1i}^2, $i = 1, \ldots, k$. Essendo Q ortogonale, se si moltiplica la prima riga di Q per la prima colonna di Q^T, si ottiene di fatto la somma dei q_{1i}^2, $i = 1, \ldots, k$ più la somma dei quadrati degli altri $d - k$ elementi della prima riga di Q; tale somma è globalmente pari a 1, sempre grazie all'ortogonalità di Q. Evidentemente quindi la somma dei q_{1i}^2, $i = 1, \ldots, k$ (che coincide con la somma dei costi) sarà maggiorata da 1. $\square$

3 Altri preliminari utili

Poiché i concetti di macchina a oracolo e di algoritmo di oracolo con complessità polinomiale nel tempo ci torneranno utili nel seguito, discutiamo qui, brevemente e in maniera largamente informale, questi concetti.

Una **macchina a oracolo** è un modello "potenziato" di macchina di Turing. Essa consiste di una normale macchina di Turing a k nastri, di cui però gli ultimi n sono detti **nastri dell'oracolo**. Ognuno di questi nastri è associato a un oracolo, ovvero a un misterioso ente esterno in grado di risolvere un determinato problema. Il funzionamento di una macchina a oracolo coincide con quello di una normale macchina di Turing per quanto concerne i primi $k - n$ nastri; come prevedibile, il comportamento caratterizzante di questo modello computazionale entra in gioco quando si passa a considerare gli n nastri dell'oracolo. Quando la macchina vuole consultare un oracolo, scrive una codifica di un'istanza del problema da risolvere sul nastro su cui opera l'oracolo opportuno e, al passo successivo, torna sullo stesso nastro per leggere la risposta. Il punto fondamentale di questo modello sta nel fatto che la consultazione dell'oracolo viene effettuata in *esattamente un* passo computazionale, indipendentemente dalla natura del problema e dalla lunghezza dell'istanza.

A questo proposito però è necessario fare un'assunzione fondamentale: la stringa prodotta in output dall'oracolo, che contiene la codifica della soluzione del problema, deve essere limitata superiormente da un polinomio nella lunghezza della stringa in input. Questa assunzione è assolutamente inevitabile in quanto una stringa che cresca esponenzialmente richiederebbe ovviamente un tempo esponenziale per essere letta. Un oracolo può dunque essere descritto da una coppia (Π, P) dove Π rappresenta il problema risolto dall'oracolo e P è il polinomio di cui si è detto.

A questo punto, è necessario estendere il concetto di complessità temporale al nuovo modello. Sempre in termini informali, la **funzione complessità temporale** di una macchina a oracolo è definita come il massimo numero di passi eseguiti dalla macchina a fronte di un certo input e di tutte le possibili risposte date dagli oracoli durante l'esecuzione[‡]. Come si vede, nessuna assunzione è fatta circa il tempo impiegato dagli oracoli per risolvere i rispettivi problemi; parlando in termini molto colloquiali, è come se si avesse a disposizione un modello di potenza infinita cui delegare alcuni dei nostri problemi: tutto ciò di cui dobbiamo preoccuparci è di codificare l'input del problema e, al passo successivo, leggere la risposta.

Visto che le macchine di Turing e gli algoritmi hanno uguale potenza computazionale, il che fa sì che i due concetti risultino intercambiabili, si può pensare di estendere il modello a oracolo anche agli algoritmi. Avremo così gli **algoritmi a oracolo**, ovvero algoritmi arricchiti dalla possibilità di chiamare una subroutine, che è in grado di risolvere uno specifico problema in un passo. Analogamente a quanto accade nel normale modello di Turing, un algoritmo a oracolo si dice avere **complessità temporale polinomiale** quando la sua funzione di complessità temporale è limitata superiormente da un polinomio nella lunghezza dell'input.

Un concetto strettamente legato a quello di modello di calcolo è il concetto di **codifica**. Come è noto, per poter sottoporre un'istanza di un certo problema ad una macchina di Turing, questa deve essere opportunamente codificata in una stringa composta di soli zero o uno[§]. Quando si specifica un modello di calcolo, non si fanno in generale assunzioni sulla particolare funzione di codifica utilizzata, a patto che essa sia "ragionevole", ovvero che non aumenti artificialmente la lunghezza della codifica. Ovviamente, in generale si sceglie la codifica minimale, quella cioè che permette di esprimere l'input usando il minor numero possibile di celle. Per gli interi, tale numero è chiaramente dato da $\langle n \rangle = 1 + \lceil \log_2 (|n| + 1) \rceil$, $n \in \mathbb{Z}$. Infatti, un bit (e quindi una cella) è richiesto per il segno, mentre il valore assoluto occupa $\lceil \log_2 (|n| + 1) \rceil$ celle. Questa funzione di codifica si estende agevolmente al caso dei numeri razionali, in quanto, per definizione, il campo razionale è dato dall'insieme di tutti e soli quei numeri che sono esprimibili come rapporto di due interi primi fra loro. La codifica di un tale numero occuperà dunque un numero di celle pari alla somma delle celle occupate dai due fattori.

Per i numeri reali, invece, il problema è ben più arduo, in quanto notoriamente non esiste un metodo di codifica che permetta di esprimere in forma finita *tutti* i numeri irrazionali. In questo caso, dunque, è necessario ricorrere ad approssimazioni che permettano di passare da numeri reali a numeri razionali, i quali possono poi essere codificati secondo quanto visto sopra.

[‡]Ricordiamo che la lunghezza della codifica di ognuna di tali risposte è limitata superiormente da un polinomio nella lunghezza dell'input.

[§]Per la precisione, è sufficiente che la codifica venga effettuata in un alfabeto finito avente almeno due simboli, ma, poiché tutti gli alfabeti siffatti sono equivalenti a questo scopo, l'alfabeto binario è quello usato sistematicamente.

3.1 Alcuni problemi rilevanti

Introduciamo ora alcuni problemi computazionali definiti su insiemi convessi e, come vedremo, strettamente collegati fra loro. In tutte le definizioni seguenti, K denoterà un insieme convesso e compatto di $\mathbb{R}^n$.

Definizione 3.1.1 (Strong Optimization Problem (SOPT)) *Dato un vettore $c \in \mathbb{R}^n$, trovare un vettore $y \in K$ che massimizzi $c^T x$ su K, oppure affermare che K è vuoto.*

Definizione 3.1.2 (Strong Violation Problem (SVIOL)) *Dato un vettore $c \in \mathbb{R}^n$ e un numero $\gamma \in \mathbb{R}$, decidere se $c^T x \leq \gamma \ \forall x \in K$ o, in caso contrario, trovare un vettore $y \in K \mid c^T y > \gamma$.*

Definizione 3.1.3 (Strong Nonemptiness Problem (SNEMPT)) *Decidere se K è vuoto o, in caso contrario, trovare un punto che gli appartenga.*

Definizione 3.1.4 (Strong Validity Problem (SVAL)) *Dato un vettore $c \in \mathbb{R}^n$ e un numero $\gamma \in \mathbb{R}$, decidere se $c^T x \leq \gamma \ \forall x \in K$.*

Definizione 3.1.5 (Strong Separation Problem (SSEP)) *Dato un vettore $y \in \mathbb{R}^n$, decidere se $y \in K$ o, in caso contrario, trovare un vettore $c \in \mathbb{R}^n$ tale che $c^T y > \max\{c^T x \mid x \in K\}$, ovvero trovare un iperpiano che separi y da K.*

Definizione 3.1.6 (Strong Membership Problem (SMEM)) *Dato un vettore $y \in \mathbb{R}^n$, decidere se $y \in K$.*

Studiamo ora quali relazioni intercorrono fra i diversi problemi sopra esposti. In questo paragrafo, la notazione P1$\longrightarrow$P2 significa che se il problema P1 è risolvibile, lo è anche il problema P2; più precisamente, se esiste un oracolo che risolve P1 in tempo polinomiale, allora ne esiste uno che risolve P2 in tempo polinomiale.

- SSEP$\longrightarrow$SMEM. Ovvia, SMEM è in effetti una semplificazione di SSEP;
- SOPT$\longrightarrow$SVIOL. Infatti SVIOL è la versione di decisione di SOPT, che è un problema di ottimizzazione, e come tale è più debole;
- SVIOL$\longrightarrow$SVAL. Ovvia, SVAL è un caso semplificato di SVIOL;
- SVIOL$\longrightarrow$SNEMPT, poiché il secondo è un caso particolare del primo, ottenuto prendendo $c = 0$ e $\gamma = -1$.

La figura 3.1.1 riassume tutte queste relazioni. La relazione$\longrightarrow$risulta essere riflessiva e transitiva¶. Questa relazione però non è una relazione di equivalenza, non essendo necessariamente simmetrica. Ad esempio, dato un oracolo che risolve SVAL, non è detto che ne esista uno che risolve SVIOL; infatti, nella formulazione di SVAL nulla è detto riguardo al caso in cui $c^T x > \gamma$, mentre in questo caso SVIOL richiede esplicitamente un controesempio. D'altra parte,$\longrightarrow$non è una relazione d'ordine né in senso stretto (non essendo ovviamente asimmetrica), né in senso lato, non essendo necessariamente antisimmetrica (due problemi possono infatti avere difficoltà equivalente senza per questo coincidere).

¶Queste due proprietà scendono immediatamente dalla definizione.

$$\begin{array}{ccccc} & & \boxed{SNEMPT} & & \\ & & \uparrow & & \\ \boxed{SOPT} & \longrightarrow & \boxed{SVIOL} & \longrightarrow & \boxed{SVAL} \end{array}$$

$$\boxed{SSEP} \longrightarrow \boxed{SMEM}$$

Figura 3.1.1: Le relazioni intercorrenti fra i vari problemi.

3.2 I problemi espressi in forma debole

Avendo definito i problemi come sopra, resta aperto un punto fondamentale: cosa succede se uno di questi problemi risulta avere solo soluzioni irrazionali? Come è noto, non esiste uno schema di codifica che permetta di codificare ogni numero irrazionale in forma finita e dunque tali numeri non sono in generale trattati dagli usuali modelli di calcolo (nel nostro caso, in particolare, le macchine a oracolo). È dunque necessario riformulare i problemi in modo tale da essere sicuri di non avere soluzioni irrazionali. Inoltre, questa formulazione dei problemi può essere troppo stretta e in alcuni casi può essere utile rilassarla nel modo seguente:

- tutte le disuguaglianze strette diventano disuguaglianze in senso lato;
- la frontiera degli insiemi viene rilassata fino a diventare un'ipersfera, che viene quindi ad essere una sorta di zona di tolleranza.

Date queste premesse, i problemi fondamentali diventano:

Definizione 3.2.1 (Weak Optimization Problem) *Dato un vettore $c \in \mathbb{Q}^n$ e un numero razionale $\varepsilon > 0$,*

- *trovare un vettore $y \in \mathbb{Q}^n$ tale che $y \in S(K, \varepsilon)$ e $c^T x \leq c^T y + \varepsilon$ $\forall x \in S(K, -\varepsilon)$; oppure*
- *affermare che $S(K, -\varepsilon)$ è vuoto.*

Definizione 3.2.2 (Weak Violation Problem) *Dato un vettore $c \in \mathbb{Q}^n$, un numero razionale γ e un numero razionale $\varepsilon > 0$,*

- *affermare che $c^T x \leq \gamma + \varepsilon$ $\forall x \in S(K, -\varepsilon)$ oppure*
- *trovare un vettore $y \in S(K, \varepsilon)$ tale che $c^T y \geq \gamma - \varepsilon$.*

Definizione 3.2.3 (Weak Validity Problem) *Dato un vettore $c \in \mathbb{Q}^n$, un numero razionale γ e un numero razionale $\varepsilon > 0$,*

- *affermare che $c^T x \leq \gamma + \varepsilon$ $\forall x \in S(K, -\varepsilon)$ oppure*
- *affermare che $c^T x \geq \gamma - \varepsilon$ per qualche $x \in S(K, \varepsilon)$.*

Definizione 3.2.4 (Weak Separation Problem) *Dato un vettore $y \in \mathbb{Q}^n$ e un numero razionale $\delta > 0$,*

- *affermare che* $y \in S(K, \delta)$ *oppure*
- *trovare un vettore* $c \in \mathbb{Q}^n$ *con* $\| c \|_\infty = 1$ *tale che* $c^T x \leq c^T y + \delta \ \forall x \in S(K, -\delta)$.

Definizione 3.2.5 (Weak Membership Problem) *Dato un vettore* $y \in \mathbb{Q}^n$ *e un numero razionale* $\delta > 0$,

- *affermare che* $y \in S(K, \delta)$ *oppure*
- *affermare che* $y \notin S(K, \delta)$.

3.3 Il metodo dell'ellissoide

3.3.1 Introduzione

Il metodo dell'ellissoide è un algoritmo nato per risolvere problemi di ottimizzazione non lineare, ma che è stato anche utilizzato, in forma modificata, allo scopo di determinare in tempo polinomiale se un sistema di disequazioni lineari ammette soluzione.
Nel contesto della nostra trattazione, il metodo dell'ellissoide trova applicazione nella risoluzione in tempo polinomiale del problema di strong non-emptiness. In questa sezione verranno esposte alcune definzioni e proprietà degli ellissoidi, mentre l'algoritmo verrà trattato nelle sezioni successive.

Definizione 3.3.1 (Ellissoide) *Un insieme* $E \subseteq \mathbb{R}^n$ *si definisce* ***ellissoide*** *se esiste un vettore* $a \in \mathbb{R}^n$ *e una matrice quadrata definita positiva* A *tali che:*

$$E = E(A, a) = \{x \in \mathbb{R}^n \mid (x - a)^T A^{-1} (x - a) \leq 1\}$$

Il vettore a è chiamato **centro** di E mentre la quantità $E(A, a)$ è definita **ellissoide associato ad** A **e** a.
Riportiamo ora alcune importanti proprietà geometriche legate all'ellissoide.

Proprietà 3.3.1 *Il diametro di* E *(ovvero la lunghezza dell'asse più lungo) risulta essere uguale a* $2\sqrt{\Lambda}$, *dove* Λ *rappresenta il più grande autovalore di* A.

Proprietà 3.3.2 *L'altezza di* E *(lunghezza dell'asse più corto) è uguale a* $2\sqrt{\lambda}$, *dove* λ *è il più piccolo autovalore di* A.

In figura 3.3.1 è rappresentato un ellissoide che riassume le proprietà suesposte.

Proprietà 3.3.3 *Il volume di un ellissoide* $E(A, a)$ *dipende solo dal determinante di* A *e dalla dimensione dello spazio. Più precisamente*

$$vol(E(A, a)) = V_n \sqrt{det A} \tag{3.3.1}$$

dove V_n *è il volume della sfera unitaria* $S(0, 1)$ *in* $\mathbb{R}^n$. *Questo volume è dato da:*

$$V_n = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2} + 1\right)} \sim \frac{1}{\sqrt{\pi n}} \left(\frac{2e\pi}{n}\right)^{\frac{n}{2}}$$

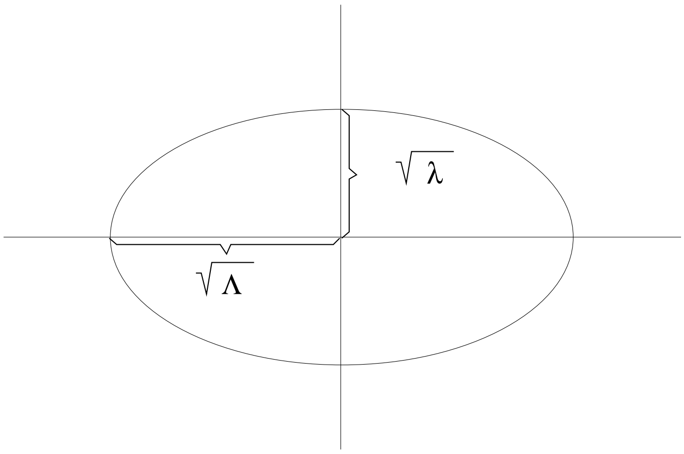

Figura 3.3.1: Relazione che lega autovalori, diametro e altezza di un ellissoide.

dove

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1}\, dt \qquad per \;\; x > 0$$

è la funzione Gamma.

Proprietà 3.3.4 *Per ogni matrice definita positiva A, la relazione che lega la sfera $S(0,1)$ all'ellissoide $E(0,1)$ è data da:*

$$E(A,a) = A^{\frac{1}{2}} S(0,1) + a \tag{3.3.2}$$

Quindi ogni ellissoide è l'immagine di una sfera unitaria sotto una trasformazione biiettiva affine.

Proprietà 3.3.5 *Se $x \to Dx + d$ è una trasformazione biiettiva affine T allora $vol(E(A,a)) = V_n\,(detD)\,\sqrt{detA}$ quindi in particolare si ha che*

$$\frac{vol(E(A,a))}{vol(E(B,b))} = \frac{vol(T(E(A,a)))}{vol(T(E(B,b)))}$$

Questo vuol dire che il quoziente del volume di 2 ellissoidi è invariante sotto trasformazioni biiettive affini.

La prossima proprietà ci dà un'idea su come ottimizzare funzioni obiettivo lineari su ellissoidi.

Proprietà 3.3.6 *Se $c \neq 0$ allora* $\max\{c^T x, x \in S(a,1)\}$ *è dato dal vettore $a + c/\|\, c\,\|$.*

Dimostrazione. Sia $E(A,a) \subseteq \mathbb{R}^n$ un ellissoide e sia $c \in \mathbb{R}^n \backslash \{0\}$. Sia inoltre $Q = A^{1/2}$, dalla (3.3.1) segue che $Q^{-1}E(A,a) = S(0,1) + Q^{-1}a = S(Q^{-1}a, 1)$ e quindi

$$\begin{aligned}
\max\{c^T x \mid x \in E(A,a)\} &= \max\{c^T Q Q^{-1} x \mid Q^{-1}x \in Q^{-1}E(A,a)\} \\
&= \max\{c^T Q y \mid y \in S(Q^{-1}a, 1))\} \\
&= c^T Q \frac{1}{\| Qc \|} Qc + c^T Q Q^{-1} a \\
&= c^T \frac{1}{\sqrt{c^T A c}} Ac + c^T a \\
&= c^T a + \sqrt{c^T A c}
\end{aligned}$$

Ponendo

$$\begin{aligned}
b &= \frac{1}{\sqrt{c^T A c}} Ac \qquad (3.3.3) \\
z_{max} &= a + b \\
z_{min} &= a - b
\end{aligned}$$

otteniamo

$$\begin{aligned}
c^T z_{max} &= \max\{c^T x \mid x \in E(A,a)\} = c^T a + \sqrt{c^T A c} = c^T a + \|c\|_{A^{-1}} \\
c^T z_{min} &= \min\{c^T x \mid x \in E(A,a)\} = c^T a - \sqrt{c^T A c} = c^T a - \|c\|_{A^{-1}}
\end{aligned}$$

Questo significa quindi che z_{max} e z_{min} massimizzano e minimizzano rispettivamente $c^T x$ su $E(A,a)$. □

Proprietà 3.3.7 *Per ogni corpo convesso $K \subseteq \mathbb{R}^n$, esiste un unico ellissoide E di volume minimo che contiene K. Inoltre K contiene l'ellissoide ottenuto da E restringendolo a partire dal suo centro di un fattore f.*

La prima parte di questa proprietà è importante per il funzionamento dell'algoritmo: l'ellissoide di volume minimo che contiene il corpo convesso K viene definito *ellissoide di Lőwner-John* di K. Nel seguito sarà utilizzata anche la seguente definizione:

$$E'(A,a,c) := E(A,a) \cap \{x \in \mathbb{R}^n \mid c^T x \leq c^T a\}$$

La quantità $E'(A,a,c)$ è quindi una sezione di ellissoide ottenuta tagliando $E(A,a)$ attraverso il suo centro a con l'iperpiano separatore $c^T x = c^T a$. L'ellissoide di Lőwner-John di $E(A,a,c)$ è l'ellissoide $E(A',a')$ dato dalle seguenti formule:

$$a' = a - \frac{1}{n+1} b \qquad (3.3.4)$$

$$A' = \frac{n^2}{n^2-1}\Big(A - \frac{2}{n+1} b b^T\Big) \qquad (3.3.5)$$

dove b è il vettore definito nella 3.3.2.

3.3.2 Descrizione dell'algoritmo base

Descriviamo questo metodo con il fine di risolvere un *strong nonemptiness problem* per un dato politopo P. In altri termini, dato il sistema di disequazioni $c_i^T \leq \gamma_i$ con n variabili a coefficienti interi, si vuole determinare se

$$P = \{x \in \mathbb{R}^n \mid c_i^T \leq \gamma_i \quad \text{per} i = 1 \dots n\} = \{x \in \mathbb{R}^n \mid Cx \leq d\}$$

è vuoto oppure no, e se non lo è si vuole trovare un punto in P.
Da notare che non si può garantire che P sia un politopo, poiché l'insieme delle soluzioni di un sistema lineare di disequazioni non è in generale limitato. Sarà dunque necessario imporre alcune condizioni aggiuntive, cioè:

1. P è limitato;
2. P è o vuoto o full-dimensional.

Nel corso della dimostrazione emergerà che queste due condizioni non sono strettamente necessarie, in quanto esiste una versione generalizzata dell'algoritmo per poliedri illimtati e non full-dimensional ma, poiché la descrizione che ne daremo fa uso di queste restrizioni, esse risultano in questa sede necessarie.
Informalmente il metodo è basato sulla costruzione di una successione di ellissoidi $E_0, \dots, E_n$, tali che $\forall i = 1, \dots, n$

- $Vol(E_i) < Vol(E_{i-1})$
- $P \subseteq E_i$

Più precisamente, iniziamo a considerare la sfera $S(0, r)$ centrata nell'origine e con raggio tale da contenere il politopo P. Se il sistema di disequazioni contiene degli espliciti limiti inferiori o superiori sulle incognite x_i, ad esempio:

$$l_i \leq x_i \leq u_i \qquad \forall i$$

allora la scelta del raggio r in modo tale che $P \subseteq S(0, r)$ è immediata; si prenda infatti

$$r = \sqrt{\sum_{i=1}^{n} \max\{u_i^2, l_i^2\}}$$

Se le variabili non sono invece limitate esplicitamente vale la seguente

Proprietà 3.3.8 *$P \subseteq S(0, r)$ quando $R = \sqrt{n} \cdot 2^{<C,d>-n^2}$ dove $\langle C, d \rangle$ è la lunghezza di codifica di C e d.*

Scegliamo quindi l'ellissoide $E_0(A_0, a_0)$ con $A_0 = R^2 I$ e $a_0 = 0$, come base iniziale per la costruzione della successione: siamo infatti sicuri che con tale scelta del raggio, essa contiene il politopo P (si noti che la scelta di A_0 deriva dalla proprietà 3.3.1). Il metodo prosegue con la costruzione dell'ellissoide $E_k(A_k, a_k)$ a partire da $E_{k-1}(A_{k-1}, a_{k-1})$. Fermo restando che il seguente procedimento è generalizzabile per qualsiasi $E_k(A_k, a_k)$ costruiamo $E_1(A_1, a_1)$ a partire da $E_0(A_0, a_0)$. Dato E_0, noi conosciamo un suo punto particolare, ovvero a_0; sostituendo perciò

a_0 nel sistema di disequazioni possiamo facilmente verificare se questo viene soddisfatto. In questo caso possiamo bloccare l'algoritmo in quanto abbiamo trovato una soluzione ammissibile. In caso contrario esiste almeno una disequazione del sistema che viene violata. Supponiamo che il punto a_0 non soddisfi completamente il sistema; non sia quindi vero che $c^T x \leq \gamma$ ma $c^T a_0 > \gamma$. L'iperpiano $\{x \in \mathbb{R}^n \mid c^T x = c^T a_0\}$ passa allora attraverso il centro di E_0 e lo taglia in due metà. Sappiamo che, per costruzione, il politopo P è contenuto nella parte

$$E(A_0, a_0, c) = \{x \in E_0(A_0, a_0) \mid c^T x \leq c^T a_0\}$$

quindi possiamo scegliere come prossimo ellissoide nella sequenza l'ellissoide di Lőwner-John di $E(A_0, a_0, c)$, iterando così di un passo l'algoritmo. A questo punto viene spontaneo chiedersi quale sia il criterio di stop: se il centro a_k (punto noto di E_k) sta in P (facile da verificarsi) possiamo tranquillamente bloccare il procedimento in quanto abbiamo trovato una soluzione ammissibile. In caso contrario, alla base del criterio di stop vi sono delle considerazioni sul volume di E_k che derivano dalle seguenti proprietà:

Proprietà 3.3.9 *Sia $E \subseteq \mathbb{R}^n$ un ellissoide e E' l'ellissoide ottenuto da E utilizzando le (3.3.3), (3.3.4) e (3.3.5) per qualche vettore $c \in \mathbb{R}^n$. Si ha allora che*

$$\frac{vol(E')}{vol(E)} = \left(\left(\frac{n}{n+1}\right)^{n+1}\left(\frac{n}{n-1}\right)^{n-1}\right)^{1/2} < e^{-1/(2n)} < 1$$

Dimostrazione. Per stimare il rapporto fra i due volumi supponiamo innanzitutto che l'ellissoide iniziale sia $F = E(I, 0)$ ovvero la sfera unitaria intorno all'origine, e che il vettore c utilizzato per calcolare b nella (3.3.3) sia $(-1, 0, \ldots, 0)^T$. Utilizzando le (3.3.3), (3.3.4) e (3.3.5), si ottiene

$$\begin{aligned}
b &= (-1, 0, \ldots, 0)^T \\
a' &= a - \frac{1}{n+1} b \\
&= \left(\frac{1}{n+1}, 0, \ldots, 0\right)^T \\
A' &= \frac{n^2}{n^2-1}\left(1 - \frac{2}{n+1}(-1, 0, \ldots, 0)^T(-1, 0, \ldots, 0)\right) \\
&= diag\left(\left(\frac{n^2}{(n^2+1)^2}, \frac{n^2}{n^2-1}, \ldots, \frac{n^2}{n^2-1}\right)^T\right)
\end{aligned}$$

da questo risultato e dalla (3.3.1) posiamo concludere che il rapporto fra il volume di $F = E(A, a)$ e $F' = E(A', a')$ è dato da:

$$\begin{aligned}
\frac{vol(F')}{vol(F)} &= \frac{\sqrt{detA'}\ V_n}{\sqrt{detA}\ V_n} = \sqrt{detA'} = \left(\frac{n^{2n}}{(n+1)^n}(n-1)^n \frac{n-1}{n+1}\right)^{\frac{1}{2}} \\
&= \left(\left(\frac{n}{n+1}\right)^{n+1}\left(\frac{n}{n-1}\right)^{n-1}\right)^{\frac{1}{2}}
\end{aligned}$$

Prendendo quindi il logaritmo naturale ln si ottiene:

$$\begin{aligned}
\frac{vol(F')}{vol(F)} < e^{-\frac{1}{2n}} \quad &\iff \quad e^{\frac{1}{n}} < \left(\frac{n+1}{n}\right)^{n+1}\left(\frac{n-1}{n}\right)^{n-1} \\
&\iff \quad \frac{1}{n} < (n+1)\ln\left(1 + \frac{1}{n}\right) + (n-1)\ln\left(1 - \frac{1}{n}\right)
\end{aligned}$$

Utilizzando lo sviluppo in serie di potenze di $\ln x = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(x-1)^k}{k}$ per $0 < x \leq 2$ si ottiene

$$\begin{aligned}
(n+1)\ln\left(1+\frac{1}{n}\right) + (n-1)\ln\left(1-\frac{1}{n}\right) &= \sum_{k=1}^{\infty} (-1)^{k+1} \frac{n+1}{kn^k} - \sum_{k=1}^{\infty} \frac{n-1}{kn^k} \\
&= \sum_{k=1}^{\infty} (-1)^{k+1} \frac{2}{kn^k} - \sum_{k=1}^{\infty} \frac{2(n-1)}{2kn^{2k}} \\
&= \sum_{k=1}^{\infty} \frac{2}{(2k-1)n^{2k-1}} - \sum_{k=1}^{\infty} \frac{2}{2kn^{2k}} - \sum_{k=1}^{\infty} \frac{1}{kn^{2k-1}} + \sum_{k=1}^{\infty} \frac{1}{kn^{2k}} \\
&= \sum_{k=1}^{\infty} \frac{1}{(2k-1)k} \frac{1}{n^{2k-1}} \\
&> \frac{1}{n}
\end{aligned}$$

Ciò conclude la dimostrazione della proprietà avendo però assunto la scelta particolare per l'ellissoide iniziale e per il vettore c. Consideriamo ora un qualsiasi ellissoide $E = E(A, a)$, e supponiamo che $E' = E(A', a')$ sia l'ellissoide costruito da E utilizzando la (3.3.3), (3.3.4) e (3.3.5) per qualche vettore $c \in \mathbb{R}^n \backslash \{0\}$. Per la 3.3.2 $E = A^{\frac{1}{2}} E(I, 0) + a = A^{\frac{1}{2}} F + a$. Esiste quindi una matrice ortogonale, diciamo Q, che trasforma $A^{1/2}c$ in un multiplo positivo di $(-1, 0, \ldots, 0)$. In altri termini esiste una matrice ortogonale Q tale che

$$(-1, 0, \ldots, 0) = \frac{1}{\| QA^{1/2}c \|} QA^{1/2}c$$

La quantità

$$T(x) = A^{1/2} Q^T x + a$$

è una trasformazione biiettiva affine con $T^{-1}(x) = QA^{-1/2}(x - a)$. Si ha che

$$\begin{aligned}
T(F) &= \{T(y) \mid y^T y \leq 1\} \\
&= \{x \mid (T^{-1}x)^T (T^{-1}x) \leq 1\} \\
&= \{x \mid (x-a)^T A^{-1/2} Q^T Q A^{-1/2} (x-a) \leq 1\} \\
&= \{x \mid (x-a)^T A^{-1} (x-a) \leq 1\} \\
&= E
\end{aligned}$$

In modo simile si ottiene, per l'ellissoide F' definito sopra, $T(F') = E'$. Nella proprietà 3.3.5 definita precedentemente, abbiamo visto che il rapporto fra il volume di due ellissoidi è invariante rispetto a trasformazioni biiettive. Quindi si ha

$$\frac{vol(E')}{vol(E)} = \frac{vol(T(F'))}{vol(T(F))} = \frac{vol(F')}{vol(F)} = \left(\left(\frac{n}{n+1}\right)^{n+1}\left(\frac{n}{n-1}\right)^{n-1}\right)^{1/2} < e^{-1/(2n)}$$

che completa la dimostrazione. □

Proprietà 3.3.10 *Se $P = \{x \in \mathbb{R}^n \mid Cx \leq d\}$ è un politopo full dimensional allora*

$$vol(P) \geq 2^{-(n+1)<C>+n^3}$$

Dimostrazione. Dalla teoria dei poliedri si dimostra che ogni politopo *full dimensional* in $\mathbb{R}^n$ contiene $n+1$ vertici $v_0, v_1, \ldots, v_n$ che sono affinemente indipendenti. L'involucro convesso di questi vertici forma un simplesso S il quale è contenuto in P. Quindi il volume di P è limitato inferiormente dal volume di S. Il volume di un simplesso può essere determinato con la seguente formula:

$$vol(S) = \frac{1}{n!}\left| det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ v_0 & v_1 & \ldots & v_n \end{pmatrix} \right|$$

Dalla regola di Cramer, per ogni vertice v_j si ha che la sua i-esima componente ha la forma $\frac{detB_{ji}}{detB_j}$, dove B_j è una sottomatrice di C e B_{ji} una sottomatrice di (C, d). Si ottiene quindi

$$\left| det \begin{pmatrix} 1 & \ldots & 1 \\ v_0 & \ldots & 1 \end{pmatrix} \right| = \left| \frac{1}{detB_0 * \cdots * detB_n} \right| \left| det \begin{pmatrix} detB_0 & \ldots & detB_n \\ u_0 & \ldots & u_n \end{pmatrix} \right|$$

dove $u_0, \ldots, u_n$ sono vettori in $\mathbb{R}^n$. Dal momento che l'ultimo determinante è un intero diverso da zero, e dal fatto che si può dimostrare la diseguaglianza $|detB_j| \leq 2^{\langle C \rangle - n^2}$ allora si ha

$$\left| det \begin{pmatrix} 1 & \ldots & 1 \\ v_0 & \ldots & v_n \end{pmatrix} \right| \geq \frac{1}{|detB_0| * \cdots * |detB_n|} \geq \left(2^{\langle C \rangle - n^2}\right)^{-(n+1)}$$

Inoltre utilizzando la diseguaglianza $n! \leq 2^{n^2}$, si ottiene

$$vol(P) \geq vol(S) \geq \frac{1}{n!}\left(2^{\langle C \rangle - n^2}\right)^{-(n+1)} \geq 2^{-(n+1)<C>+n^3}$$

La proprietà 3.3.6 assicura che il metodo consente di costruire ellissoidi con volume sempre più piccolo, mentre la 3.3.7 fornisce un limite inferiore al volume di P. Possiamo quindi iterare la procedura fintanto che l'attuale ellissoide E_k ha un volume che è più piccolo di tale limite. Infatti raggiungendo questa situazione, supponiamo in n passi, si dovrebbe avere che $P \subseteq E_n$ e $vol(E_n) < vol(P)$, il che è chiaramente impossibile. □

Si tenga presente comunque che l'implementazione algoritmica del metodo richiede alcuni pratici accorgimenti numerici.

3.3.3 Alcune considerazioni sulla complessità dell'algoritmo

Poiché per i nostri scopi la polinomialità dell'algoritmo descritto è un requisito irrinunciabile, vediamo nel seguito una sommaria analisi di complessità. Per far ciò è però indispensabile riassumere i passi dell'algoritmo in maniera più formale.

Dato un sistema lineare $m \times n$ di disequazioni a coefficienti interi $Cx \leq d$, il seguente algoritmo determina in tempo polinomiale se questo sistema ammette soluzioni.

Inizializzazione.

1. $k := 0$. k è un contatore;

2. $N := 2n\left((2n+1)\langle C \rangle + n\langle d \rangle - n^3\right)$. N è una stima del numero massimo di passi dell'algoritmo, al di sopra del quale cadiamo nella condizione impossibile (3.3.2);

3. $A_0 := R^2 I$ con $R = \sqrt{n} 2^{\langle C,d \rangle - n^2}$;. A_0 è la matrice associata al primo ellissoide della successione;

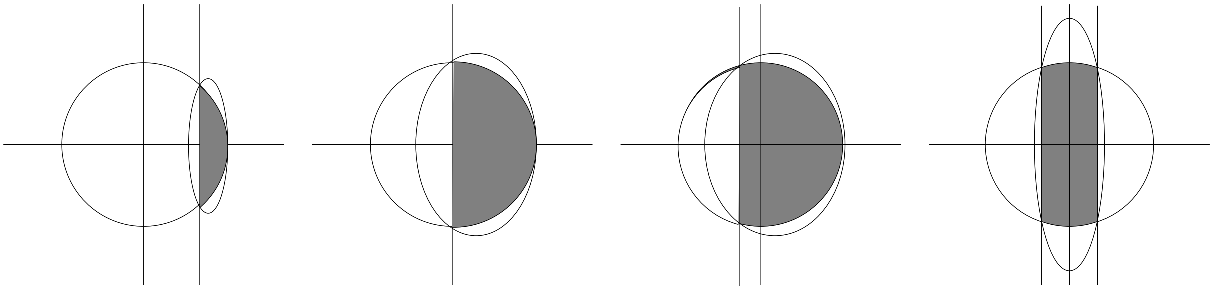

Figura 3.3.2: Esempi di deep cut(a), central cut(b), shallow cut(c) e centrally simmetric parallel cut(d)

4. $a_0 := 0$; a_0 è il centro del primo ellissoide della successione;

Passo generale

1. Se $k = N$, STOP. Condizione di stop che dichiara $P = \emptyset$; v. 2;
2. se $a_k \in P$, STOP. Il centro del k-esimo ellissoide sta in P, quindi è stata trovata una soluzione ammissibile;
3. se $a_k \notin P$, questo significa che almeno una disequazione del sistema $Cx \leq d$ è stata violata da a_k. Quindi:
   (a) $b := \frac{1}{\sqrt{c^T A_k c}} A_k c$, v. (3.3.3);
   (b) $a_{k+1} := a_k - \frac{1}{n+1} b$, per v. (3.3.4);
   (c) $A_{k+1} := \frac{n^2}{n^2-1} \left(A_k - \frac{2}{n+1} bb^T \right)$, v. (3.3.5).
   (d) vai a 3.

Secondo la prassi usuale, ogni passo computazionale verrà considerato di costo unitario. L'inizializzazione comporterà $O(mn)$ passi. Per ogni esecuzione dei passi generali 3a, ... ,3d dobbiamo sostituire a_k nel sistema, il che richiede $O(mn)$ operazioni. Il passo 3b richiede $O(n)$ operazioni, mentre 3c ne richiede $O(n^2)$. Il passo generale viene eseguito un numero di volte limitato superiormente da $O(n^2 \langle C, d \rangle)$. Poichè P è un politopo, $m \geq n$ e dunque il numero totale di passi elementari è $O(mn^3 \langle C, d \rangle)$. La complessità dell'algoritmo è dunque maggiorata da un polinomio in m e n.

3.3.4 Central Cut, Deep Cut, Shallow Cut

Si è precedentemente accennato al fatto che l'iperpiano separatore taglia l'ellissoide E_k nel suo centro: una differente scelta del taglio dell'iperpiano genera una leggera variante al metodo stesso. Per fare solo qualche esempio si può fare in modo che l'iperpiano tagli l'ellissoide in altri punti del suo asse come mostra la figura 3.3.2.
I relativi algoritmi prendono il nome di *central cut method, deep cut method* e *shallow cut method*.

Parte II
Svolgimento

4 The Sandwich Theorem

4.1 STAB, QSTAB, TH

Definizione 4.1.1 *Dato un grafo $G = \langle V, E \rangle$ con $|V| = n$, ad esso possono essere associati i seguenti insiemi:*

- STAB(G) *è l'involucro convesso dell'insieme dei labeling stabili di G;*
- QSTAB(G) $= \left\{ x \in \mathbb{R}^n, x \geq 0 \mid \sum_{v \in Q} x_v \leq 1 \text{per tutte le clique } Q \text{ di } G \right\}$;
- *TH(G)* $= \left\{ x \in \mathbb{R}^n, x \geq 0 \mid \sum_{v \in V} c(a_v) x_v \leq 1 \text{per tutti i labeling ortogonali } a \text{ di } G \right\}$.

Osservazione. Gli insiemi stabili di G sono in numero finito perché sono al più 2^n, nel caso di un grafo completamente sconnesso, mentre sono n nel caso di un grafo completamente connesso. Le clique di G sono anch'esse in numero finito perché sono al più 2^n, nel caso di un grafo completamente connesso e sono almeno n, nel caso di un grafo completamente sconnesso.

Lemma 4.1.1 *Dato un qualunque grafo $G = \langle V, E \rangle$, vale la seguente relazione:*

$$\text{STAB}(G) \subseteq \mathit{TH}(G) \subseteq \text{QSTAB}(G) \tag{4.1.1}$$

Dimostrazione. Cominciamo con l'osservare che ogni labeling stabile di G appartiene a TH(G). Infatti, sia $S \subseteq V$ un insieme stabile di G e sia x il suo labeling caratteristico; allora $\sum_{v \in V} c(a_v) x_v = \sum_{v \in S} c(a_v)$ e, grazie al lemma 2.2.1, $\sum_{v \in S} c(a_v) \leq 1$ e quindi $x \in \text{TH}(G)$. Inoltre, TH(G) è un insieme convesso; infatti, presi comunque due punti in esso, il segmento che li unisce risulta anch'esso appartenere a TH(G). In simboli: $\forall\ x, y \in \text{TH}(G)$

$$\lambda \sum_{v \in V} c(a_v) x_v + (1 - \lambda) \sum_{v \in V} c(a_v) y_v \leq \lambda + (1 - \lambda) = 1$$

Le due osservazioni precedenti dimostrano quindi che $\text{STAB}(G) \subseteq \text{TH}(G)$. Per dimostrare la seconda parte della (4.1.1), osserviamo che ogni clique labeling è, per definizione, un labeling ortogonale di dimensione 1. Poiché la formula

$$\forall x \in \text{TH}(G) \ \sum_{v \in V} c(a_v) x_v \leq 1$$

vale per tutti i labeling ortogonali a di G, essa vale in particolare anche per tutti i clique labeling, quindi $x \in \text{QSTAB}(G)$. □

Monotonicità di STAB, QSTAB, TH

Dato un grafo $G = \langle V, E \rangle$ e un grafo parziale $G' \subseteq G$, valgono le seguenti relazioni:

1. ogni insieme stabile di G è un insieme stabile di G';
2. ogni clique di G' è una clique di G;
3. ogni labeling ortogonale di G' è un labeling ortogonale di G.

Da queste si possono ricavare le seguenti proprietà di STAB, QSTAB e TH:

1. $\mathrm{STAB}(G) \subseteq \mathrm{STAB}(G')$; infatti, preso un qualunque labeling stabile x di G, per il punto 1 esso risulta stabile anche per G';
2. $\mathrm{QSTAB}(G) \subseteq \mathrm{QSTAB}(G')$; infatti, preso un qualunque $x \in \mathrm{QSTAB}(G)$, esso appartiene sicuramente anche a $\mathrm{QSTAB}(G')$ poiché per il punto 2 le clique di G' sono un sottoinsieme delle clique di G;
3. $\mathrm{TH}(G) \subseteq \mathrm{TH}(G')$; infatti, preso un labeling reale $x \in \mathrm{TH}(G)$, esso appartiene anche a $\mathrm{TH}(G')$ perché per il punto 3 i labeling ortogonali di G' sono un sottoinsieme dei labeling ortogonali di G.

Le proprietà esposte possono essere sintetizzate dicendo che STAB, QSTAB e TH sono **monotone non crescenti** nel loro argomento G.

Casi particolari

Osserviamo che la relazione (4.1.1) vale con il segno di uguaglianza nei due casi estremi, ovvero nei casi della clique e del grafo vuoto. Infatti avremo:

$$\mathrm{STAB}(K_n) = \mathrm{TH}(K_n) = \mathrm{QSTAB}(K_n) = \left\{ x \in \mathbb{R}^n, x \geq 0 \mid \sum_{v \in V} x_v \leq 1 \right\}$$

In altre parole, nel caso della clique le tre quantità coincidono fra loro e sono uguali all'n-simplesso. Infatti, i labeling stabili sono tutti e soli i vettori di $\mathbb{R}^n$ della forma $\{\exists!\ i = 1, \ldots, n \mid x_i = 1 \wedge x_j = 0\ \forall j \neq i\}\ \forall i = 1, \ldots, n$, più il vettore nullo; in altre parole, i possibili labeling stabili coincidono con i vertici dell'n-simplesso e dunque STAB coincide con l'n-simplesso stesso. Per quanto riguarda QSTAB, il fatto che esso coincida con l'n-simplesso è una conseguenza immediata della definizione. Essendo TH sempre compreso fra i due, anch'esso deve coincidere con l'n-simplesso.
Nel caso invece del grafo vuoto, la relazione sarà:

$$\mathrm{STAB}(\overline{K}_n) = \mathrm{TH}(\overline{K}_n) = \mathrm{QSTAB}(\overline{K}_n) = \{x \in \mathbb{R}^n \mid 0 \leq x_v \leq 1\ \forall v \in V\} \tag{4.1.2}$$

Ovvero in questo caso i tre insiemi coincidono con l'n-cubo. Infatti i labeling stabili sono tutti e soli i labeling caratteristici (cioè i vettori di $\mathbb{R}^n$ i cui elementi sono solo zero o uno), ovvero i vertici dell'n-cubo. Dunque, STAB coincide con l'n-cubo. Per quanto riguarda QSTAB, poiché nel caso del grafo vuoto le clique hanno tutte dimensione 0 o 1, dalla definizione scende immediatamente che deve essere $0 \leq x_v \leq 1\ \forall v = 1, \ldots, n$, il che coincide con la nozione di n-cubo. Dunque tutti e tre gli insiemi coincidono con l'n-cubo.
Si può quindi concludere che per ogni grafo G i tre insiemi saranno sempre compresi fra l'n-simplesso e l'n-cubo. In figura 4.1.1 è evidenziata la regione in cui i tre insiemi possono variare.

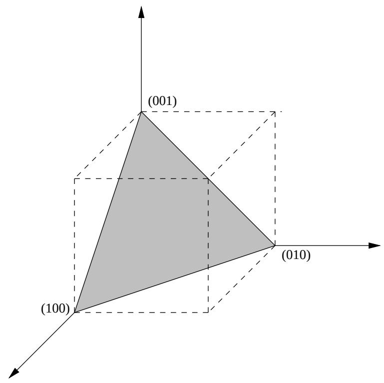

Figura 4.1.1: La "regione ammissibile" per STAB, QSTAB e TH nel caso di $\mathbb{R}^3$

4.2 La funzione ϑ

Definizione 4.2.1 (La funzione ϑ) *Dato un grafo $G = \langle V, E\rangle$ e dato un labeling reale non negativo w su G, si definisce la funzione ϑ nel seguente modo:*

$$\vartheta(G, w) = \max\{w \cdot x \mid x \in TH(G)\}$$

Per brevità di scrittura, quando $w = \mathbb{1}$ (dove $\mathbb{1}$ è il labeling $w_v = 1\ \forall v$) si userà la notazione $\vartheta(G)$ con cui si intenderà $\vartheta(G, \mathbb{1})$. Dato un grafo G, $\vartheta(G)$ si dice **numero di Lovász** di G.

Proprietà di ϑ

Grazie alla monotonicità di TH, si può immediatamente dimostrare la monotonicità di ϑ, ovvero:

$$G' \subseteq G \Longrightarrow \vartheta(G', w) \geq \vartheta(G, w)\ \forall w \geq 0$$
$$w \leq w' \Longrightarrow \vartheta(G, w) \leq \vartheta(G, w')\ \forall G$$

Ciò significa che ϑ è monotona non crescente nel suo parametro G, monotona non decrescente in w.

Casi particolari

La ϑ assume il suo valore minimo in corrispondenza della clique. Si ha infatti:

$$\vartheta(K_n, w) = \max\{w_1, \ldots, w_n\}; \qquad \vartheta(K_n) = 1$$

Diamo ora una dimostrazione di questa uguaglianza. Poiché

$$\vartheta(K_n, w) = \max\left\{\sum_{i=1}^{n} w_i x_i \mid x \in \mathrm{TH}(K_n)\right\}$$

bisogna dimostrare che

$$\max\left\{\sum_{i=1}^{n} w_i x_i \mid x \in \mathrm{TH}(K_n)\right\} = \max\{w_1, \ldots, w_n\}$$

La dimostrazione procede per assurdo. Sia $w_M = \max\{w_1, \dots, w_n\}$. Supponiamo che esista $\bar{x} \in \mathrm{TH}(K_n)$ tale che $\sum_{i=1}^{n} w_i \bar{x}_i > w_M$. Allora:

$$\sum_{\substack{i=1 \\ i \neq M}}^{n} w_i \bar{x}_i > w_M (1 - \bar{x}_M) \tag{4.2.1}$$

Essendo K_n un grafo completo, avremo $\mathrm{TH}(K_n) = \{x \geq 0 \mid \sum_{i=1}^{n} x_i \leq 1\}$ e quindi in particolare:

$$\sum_{i=1}^{n} \bar{x}_i \leq 1 \tag{4.2.2}$$

Naturalmente, per come w_M è stato definito, sarà:

$$w_M \geq w_i \; \forall i = 1, \dots, n \tag{4.2.3}$$

Da (4.2.3) e (4.2.2) possiamo ricavare:

$$\sum_{\substack{i=1 \\ i \neq M}}^{n} w_i \bar{x}_i \overset{(4.2.3)}{\leq} w_M \sum_{\substack{i=1 \\ i \neq M}}^{n} \bar{x}_i \overset{(4.2.2)}{\leq} w_M (1 - \bar{x}_M) \tag{4.2.4}$$

Dunque, da (4.2.1) e (4.2.4) avremo:

$$w_M (1 - \bar{x}_M) \overset{(4.2.1)}{<} \sum_{\substack{i=1 \\ i \neq M}}^{n} w_i \bar{x}_i \overset{(4.2.4)}{\leq} w_M (1 - \bar{x}_M)$$

il che porta evidentemente all'assurdo. $\square$

L'altro caso estremo riguarda il grafo vuoto, in corrispondenza del quale ϑ assume il suo valore massimo. Avremo:

$$\vartheta(\overline{K}_n, w) = w_1 + \ldots + w_n; \qquad \vartheta(\overline{K}_n) = n$$

La dimostrazione in questo caso è immediata. Infatti, per la (4.1.2) ϑ assume il valore massimo in corrispondenza del vettore $x = \mathbb{1}$, dove vale $w_1 + \ldots + w_n$. Definizioni analoghe alla ϑ possono essere date anche per STAB e QSTAB.

Definizione 4.2.2 (La funzione α) *Dato un grafo $G = \langle V, E \rangle$ e dato un labeling reale non negativo w su G, si definisce la funzione α nel seguente modo:*

$$\alpha(G, w) = \max\{w \cdot x \mid x \in \mathrm{STAB}(G)\}$$

Anche in questo caso, $\alpha(G)$ denoterà $\alpha(G, \mathbb{1})$. Osserviamo che $\alpha(G)$ corrisponde alla dimensione del più grande insieme stabile di G. Infatti $\alpha(G) = \max\{x_1 + \ldots + x_n \mid x \in \mathrm{STAB}(G)\}$ e dunque assumerà il suo valore massimo in corrispondenza del labeling stabile più grande possibile.

Definizione 4.2.3 (La funzione κ) *Dato un grafo $G = \langle V, E\rangle$ e dato un labeling reale non negativo w su G, si definisce la funzione κ nel seguente modo:*

$$\kappa(G, w) = \max\{w \cdot x \mid x \in \mathrm{QSTAB}(G)\}$$

$\kappa(G)$ vale al più $\overline{\chi}(G)$[‖]. Infatti supponiamo che i vertici di G possano essere partizionati in n clique $Q_1, \ldots, Q_n$, allora:

$$\kappa(G) = \max\left\{\sum_{v\in Q_1} x_v + \ldots + \sum_{v\in Q_n} x_v\right\}$$

al variare di x in $\mathrm{QSTAB}(G)$. Ora, poiché ognuna delle sommatorie che appaiono in questa equazione è ≤ 1, sarà $\kappa(G) \leq n$.

Lemma 4.2.1 *Dato un grafo G, $\omega(G) = \alpha(\overline{G})$.*

Dimostrazione. $\omega(G)$ è la dimensione della massima clique di G. Complementando il grafo, la massima clique di G diventa evidentemente il massimo insieme stabile di $\overline{G}$. Dunque, essendo $\alpha(\overline{G})$ la dimensione del massimo insieme stabile di $\overline{G}$, le due quantità coincidono. □

Lemma 4.2.2 *Dato un grafo $G = \langle V, E\rangle$, $\overline{\chi}(G) = \chi(\overline{G})$.*

Dimostrazione. Ricordiamo che $\chi(\overline{G})$ è il numero cromatico di $\overline{G}$, mentre $\overline{\chi}(G)$ è il minimo numero di clique che coprono i vertici di G. Consideriamo l'insieme di tutte e sole le possibili partizioni di G in sottografi completi e fra tutte queste partizioni consideriamo quella di cardinalità minima. Otterremo così una famiglia $Q = \{Q_1, \ldots, Q_n\}$ di sottografi di G ognuno dei quali è una clique e tale che $n = \overline{\chi}(G)$. Allora:

$$\forall Q_i, Q_j \in Q \ \exists\ a \in Q_i, b \in Q_j \mid a \not- b \tag{4.2.5}$$

altrimenti anche $Q_i \cup Q_j$ sarebbe una clique e dunque esisterebbe una nuova partizione di cardinalità $< n$ contro l'ipotesi. Quando complementiamo il grafo, otteniamo una famiglia $\overline{Q} = \{\overline{Q}_1, \ldots, \overline{Q}_n\}$ in cui ogni $\overline{Q}_i$ è il grafo complementare di Q_i ed è dunque un insieme stabile. In figura 4.2.1 è mostrato un esempio di grafo partizionato in clique (a) e del suo complementare (b). Allora la (4.2.5) diventa:

$$\forall \overline{Q}_i, \overline{Q}_j \in \overline{Q} \ \exists\ a \in \overline{Q}_i, b \in \overline{Q}_j \mid a — b$$

Dunque, dato un qualunque $\overline{Q}_i$, tutti i suoi nodi potranno essere colorati con lo stesso colore, mentre, comunque scelti $\overline{Q}_i$ e $\overline{Q}_j$, essi dovranno essere colorati con colori diversi. Ne consegue che il numero cromatico di $\overline{G}$ è pari a n, il che prova la tesi. □

A questo punto possiamo finalmente enunciare il teorema fondamentale dell'articolo.

Teorema 4.2.1 (The Sandwich Theorem) *Dato un grafo G, vale la seguente relazione:*

$$\omega(G) \leq \vartheta(\overline{G}) \leq \chi(G) \tag{4.2.6}$$

[‖]Ricordiamo che $\overline{\chi}(G)$ è il più piccolo numero di clique che copre i vertici di G.

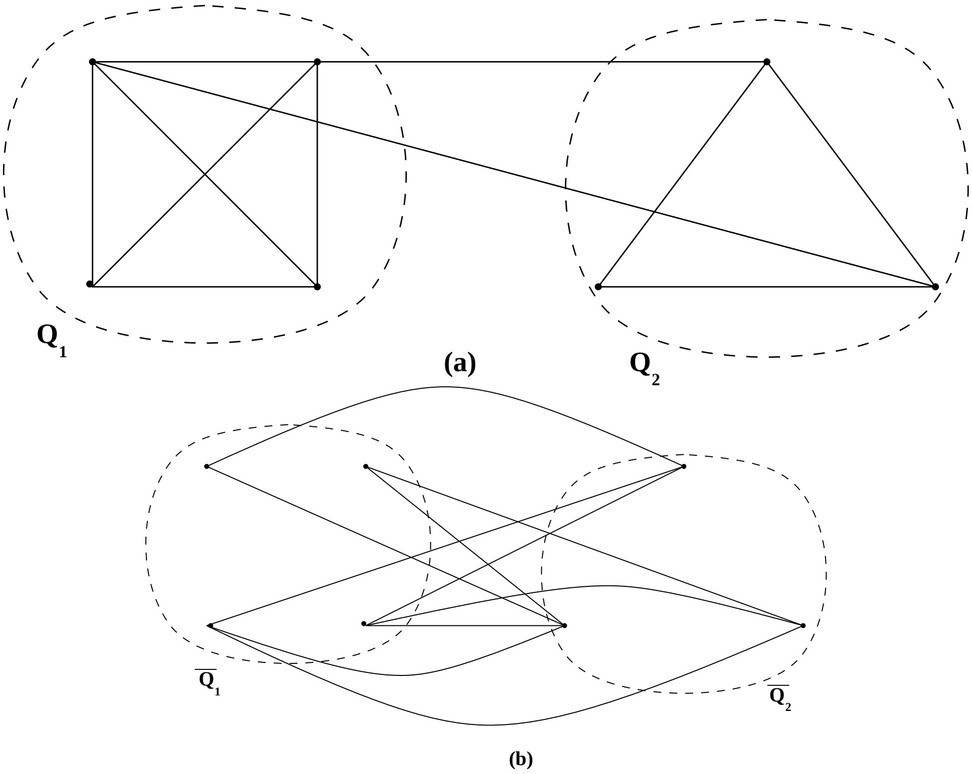

Figura 4.2.1: Un grafo partizionato in clique (a) e il suo complementare (b)

Dimostrazione. Ricordiamo che, come visto sopra, $\kappa(G) \leq \overline{\chi}(G)$. Da questa osservazione, dalle definizioni di α, ϑ e κ e da (4.1.1), scende immediatamente:

$$\alpha(G) \leq \vartheta(G) \leq \kappa(G) \leq \overline{\chi}(G)$$

A questo punto, per i lemmi 4.2.2 e 4.2.1, scende:

$$\omega(\overline{G}) \leq \vartheta(G) \leq \chi(\overline{G})$$

da cui deriva immediatamente la tesi. $\square$

5 Dimostrazione di Equivalenza dei ϑ

5.1 $\vartheta \leq \vartheta_1$

In questa sezione viene riscritta e commentata la prova di $\vartheta(G, w) \leq \vartheta_1(G, w)$.

Teorema 5.1.1 *Dato un grafo G ed un labeling reale non negativo w, su cui sono definite le funzioni*

$$\vartheta(G, w) = \max\{w \cdot x \mid x \in TH(G)\}$$

$$\vartheta_1(G, w) = \min_a \max_v \left(\frac{w_v}{c(a_v)}\right) \; \forall a \text{ labeling ortogonale di } G$$

si ha che $\vartheta(G, w) \leq \vartheta_1(G, w)$.

Dimostrazione. Siano $\overline{x} \in \mathrm{TH}(G)$ quel valore che massimizza $w \cdot x$ e $\overline{a}$ il labeling ortogonale che minimizza $\max_v (w_v/c(a_v))$.
La tesi è dimostrata dalla seguente catena di disuguaglianze:

$$\begin{aligned}\vartheta(G,w) &\overset{\text{def.}\vartheta}{=} w \cdot \overline{x} = \sum_v w_v \overline{x}_v = \sum_v \frac{c(\overline{a}_v)}{c(\overline{a}_v)} w_v \overline{x}_v \le \max_i \frac{w_i}{c(\overline{a}_i)} \sum_v c(\overline{a}_v)\overline{x}_v \\ &\overset{\overline{x}\in\mathrm{TH}(G)}{\le} \max_i \frac{w_i}{c(\overline{a}_i)} \overset{\text{def.}\overline{a}}{=} \min_a \max_i \frac{w_i}{c(a_i)} \overset{\text{def.}\vartheta_1}{=} \vartheta_1(G,w)\end{aligned}$$

dove si considera $w_i/c(a_i) = 0$ se $w_i = c(a_i) = 0$ e $w_i/c(a_i) = +\infty$ se per qualche i si ha $w_i > 0$ e $c(a_i) = 0$.

□

5.2 $\vartheta_1 \le \vartheta_2$

In questa sezione viene riscritta e commentata la prova di $\vartheta_1(G,w) \le \vartheta_2(G,w)$.

Teorema 5.2.1 *Data la funzione*

$$\Lambda(A) = \max\{x^T A x \mid x \in \mathbb{R}^V,\ \| x \| = 1\}$$

definita per qualsiasi matrice A reale e simmetrica e dati un grafo G ed un labeling reale non negativo w, su cui sono definite le funzioni

$$\vartheta_1(G,w) = \min_a \max_v \left(\frac{w_v}{c(a_v)}\right) \ \forall a \textit{ labeling ortogonale di } G$$

$$\vartheta_2(G,w) = \min\{\Lambda(A) \mid A \textit{ è una matrice feasible per } G \textit{ e } w\}$$

si ha che $\vartheta_1(G,w) \le \vartheta_2(G,w)$

Dimostrazione. Nel seguito della dimostrazione si supporrà $w \ne 0$; è possibile fare tale assunzione senza perdere di generalità in quanto se $w = 0$ si ha $\vartheta_1(G,w) = \vartheta_2(G,w) = 0$. Infatti $\vartheta_1(G,0) = 0$ per definizione di ϑ_1; inoltre, se $w = 0$ la matrice nulla è feasible ed il suo massimo autovalore è il minimo possibile, ovvero è nullo. Dunque anche $\vartheta_2(G,0) = 0$.

Sia $\overline{A}$ la matrice feasible in corrsispondenza della quale $\Lambda(A)$ ha il suo minimo e sia $\lambda > 0$ tale minimo. Allora una condizione sufficiente affinché la tesi sia soddisfatta, è che esista un labeling ortogonale $\widetilde{a}$ t.c.

$$\max_v \left(\frac{w_v}{c(\widetilde{a}_v)}\right) = \lambda$$

Infatti, in questo caso si ha**:

$$\vartheta_1(G,w) = \min_a \max_v \left(\frac{w_v}{c(a_v)}\right) \le \max_v \left(\frac{w_v}{c(\widetilde{a}_v)}\right) = \lambda = \min_A (\Lambda(A)) = vartheta_2(G,w)$$

**Per semplicità, si supponga da ora in poi A matrice feasible e a labeling ortogonale.

Vediamo dunque come costruire un siffatto labeling ortogonale $\widetilde{a}$.
Ricordando che

$$A = Q \begin{pmatrix} \lambda_1^A & & \\ & \ddots & \\ & & \lambda_n^A \end{pmatrix} Q^T$$

si definisce una matrice

$$B = \lambda I - A = \lambda Q I Q^T - A =$$

$$= Q(\lambda I)Q^T - Q \begin{pmatrix} \lambda_1^A & & \\ & \ddots & \\ & & \lambda_n^A \end{pmatrix} Q^T = Q \begin{pmatrix} \lambda - \lambda_1^A & & \\ & \ddots & \\ & & \lambda - \lambda_n^A \end{pmatrix} Q^T$$

Riassumendo l´ultimo termine come $X^T X$, dove $X = \begin{pmatrix} \sqrt{\lambda - \lambda_1^A} & & \\ & \ddots & \\ & & \sqrt{\lambda - \lambda_n^A} \end{pmatrix} Q^T$, si può definire con maggiore agilità il labeling ortogonale cercato:

$$\widetilde{a_v} = \begin{pmatrix} \sqrt{w_v} \\ X_{1v} \\ \vdots \\ X_{nv} \end{pmatrix}$$

$\widetilde{a}$ è un labeling ortogonale, infatti, se $u \not\to v$ si ha

$$\widetilde{a_v} \cdot \widetilde{a_u} = \sqrt{w_v w_u} + X_v \cdot X_u = \sqrt{w_v w_u} + B_{vu} = \sqrt{w_v w_u} - A_{vu} = 0$$

L´ultima uguaglianza segue dalla definizione di A, mentre la penultima dalla definizione di $B = \lambda I - A$. Inoltre

$$c(\widetilde{a_v}) = \frac{w_v}{||\widetilde{a_v}||^2} = \frac{w_v}{w_v + X_{1v}^2 + \cdots + X_{nv}^2} = \frac{w_v}{w_v + B_{vv}} = \frac{w_v}{w_v + \lambda - w_v} = \frac{w_v}{\lambda}$$

quindi

$$\frac{w_v}{c(\widetilde{a_v})} = \lambda$$

e in particolare

$$\max_v \left(\frac{w_v}{c(\widetilde{a_v})} \right) = \lambda$$

$\square$

5.3 $\vartheta_2 \leq \vartheta_3$

In questa sezione viene riscritta e commentata la prova di $\vartheta_2(G, w) \leq \vartheta_3(G, w)$. Questa dimostrazione è il "cuore" della catena, perché è la prova della buona caratterizzazione di ϑ: infatti permette di passare da una definizione contenente un "min" a una con un "max".
L'approccio usato per la dimostrazione, a differenza di quello adottato da Knuth, è di tipo top-down; ovvero la tesi viene dimostrata in un primo tempo in linee generali, cioè ad "alto livello" e successivamente si scende nei particolari, dimostrando approfonditamente i "passaggi chiave".

Teorema 5.3.1 *Data la funzione*

$$\Lambda(A) = \max\{x^T A x \mid x \in \mathbb{R}^V,\ \| x \| = 1\}$$

definita per qualsiasi matrice A reale e simmetrica e dati un grafo G ed un labeling reale non negativo w, su cui sono definite le funzioni

$$\vartheta_2(G, w) = \min\{\Lambda(A) \mid A \textit{ è una feasible matrix per } G \textit{ e } w\}$$

$$\vartheta_3(G, w) = \max\left\{\sum_{u,v}(\sqrt{w_u} b_u) \cdot (\sqrt{w_v} b_v) \mid b \textit{ è un labeling ortogonale normalizzato per } \overline{G}\right\}$$

si ha che $\vartheta_2(G, w) \leq \vartheta_3(G, w)$

Dimostrazione. A puro scopo di maggiore leggibilità introduciamo le seguenti notazioni:

$$\begin{array}{rcll}
\mathcal{M} & = & \{A = (a_{ij}) \in \mathbb{R}^{V \times V} \text{ simmetrica} \mid a_{ij} = 0 \, se \; i \text{ — } j \text{ in } G\} & \\
\mathcal{M}^{\perp} & = & \{A = (a_{ij}) \in \mathbb{R}^{V \times V} \text{ simmetrica} \mid a_{ij} = 0 \, se \; i \not\text{—}\; j \text{ in } G \, e \, a_{ii} = 0 \, \forall i \in V\} & \\
\mathcal{D} & = & \{A = (a_{ij}) \in \mathbb{R}^{V \times V} \mid A \text{ reale, simmetrica, semidefinita positiva}\} & \\
\mathcal{M}_1 & = & \{B \in \mathcal{M} \mid \text{tr}(B) = 1\} & (5.3.1) \\
\mathcal{K} & = & \mathcal{M}_1 \cap \mathcal{D} & (5.3.2) \\
\mathcal{P}^{\circ} & = & \{A = (a_{ij}) \in \mathbb{R}^{V \times V} \mid \text{tr}(A^T B) \leq 0 \, \forall \, B \in \mathcal{P} \subseteq \mathbb{R}^{V \times V}\} &
\end{array}$$

Si noti, innanzi tutto, che definendo

$$\begin{array}{rcl}
\overline{w} & = & (\sqrt{w_i} \mid i \in V) \in \mathbb{R}^V \\
B & = & (b_i \cdot b_j \mid i, j \in V) \in \mathbb{R}^{V \times V}
\end{array}$$

si può riscrivere ϑ_3 nel seguente modo:

$$\vartheta_3(G, w) = \max\left\{\overline{w}^T B \overline{w} \mid B \in \mathcal{D} \cap \mathcal{M} \; t.c.,\ \text{tr}(B) = 1\right\}$$

Da questa definizione è immediato vedere che per ogni matrice $B \in \mathcal{D} \cap \mathcal{M}$ vale

$$\overline{w}^T B \overline{w} \leq \vartheta_3 \cdot \text{tr}(B)$$

ovvero[††]

$$0 \geq \overline{w}^T B \overline{w} - \vartheta_3 \cdot \text{tr}(B) = \text{tr}(\overline{W}^T B) - \text{tr}((\vartheta_3 I) B) = \text{tr}(\overline{W}^T B - (\vartheta_3 I)^T B) = \text{tr}((\overline{W} - \vartheta_3 I)^T B) \quad (5.3.3)$$

dove $\overline{W}$ è una matrice reale e simmetrica definita in termini del vettore $\overline{w}$:

$$\overline{W} = \overline{w}\,\overline{w}^T = \left(\sqrt{w_i w_j} | i, j \in V\right).$$

Come si dimostrerà poco più avanti, dall'ultima disuguaglianza, segue che

[††] $x^T B x = \text{tr}(X^T B)$ per $x \in \mathbb{R}^V$, $X = x x^T = (x_i x_j) \in \mathbb{R}^{V \times V}$ e $B \in \mathbb{R}^{V \times V}$; infatti $x^T B x = \sum_j x^T B_j x_j = \sum_j (\sum_i x_i b_{ij})_j = \sum_j \sum_i x_i x_j b_{ij} = \sum_j \sum_i X_{ij} b_{ij} = \sum_j X_j^T B_j = X^T B$

$$\overline{W} - \vartheta_3 I = -D - A' \tag{5.3.4}$$

dove $D \in \mathcal{D}$ e $-A' \in \mathcal{M}^\perp$. Dalla (5.3.4) si ricava

$$\vartheta_3 I - (A' + \overline{W}) = D$$

Pertanto il termine $\vartheta_3 I - (A' + \overline{W}) \in \mathcal{D}$ e in particolare è semidefinito positivo; dunque ϑ_3 non è più piccolo del più grande autovalore di $A' + \overline{W}$, la matrice $A' + \overline{W}$ ha la stessa forma e le stesse proprietá di A. In termini matematici:

$$\vartheta_3 \geq \Lambda(A' + \overline{W}) = \Lambda(A) \geq \vartheta_2$$

Vediamo ora, come si arriva alla (5.3.4). Dalla (5.3.3) si ha che $\overline{W} - \vartheta_3 I \subseteq (\mathcal{D} \cap \mathcal{M})^\circ$, pertanto affinché la (5.3.4) sia soddisfatta è sufficiente che:

$$(\mathcal{D} \cap \mathcal{M})^\circ \in \mathcal{D}^\circ + \mathcal{M}^\circ = -\mathcal{D} + \mathcal{M}^\perp$$

L'uguaglianza $\mathcal{D}^\circ = -\mathcal{D}$ è di immediata verifica; infatti

$$\begin{gathered} X \in \mathcal{D}^\circ \Leftrightarrow \\ \mathrm{tr}\,(X^T A) \leq 0\, \forall A \in \mathcal{D} \Leftrightarrow \\ (A_j)^T X A_j \leq 0\, \forall\, A_j \; \textit{vettore colonna di } A \Leftrightarrow \\ X \in -\mathcal{D} \end{gathered}$$

Anche l'uguaglianza $\mathcal{M}^\circ = \mathcal{M}^\perp$ è di verifica immediata; infatti

$$X \in M^\circ \Leftrightarrow \mathrm{tr}\,(X^T A) = \sum_i X_i \cdot A_i = \sum_j \sum_i X_{ij} A_{ij} \leq 0\, \forall A \in M \Leftrightarrow$$

$$\sum_{ij\, i \neq j} X_{ij} A_{ij} \leq 0\, \forall A \in M \Leftrightarrow \begin{cases} X_{ij} = 0\, \forall i, j\; i \neq j \\ X_{ii} = 0\, \forall\, i \in V \end{cases} \Leftrightarrow X \in M^\perp$$

Per verificare l'inclusione $(\mathcal{D} \cap \mathcal{M})^\circ \subseteq \mathcal{D}^\circ + \mathcal{M}^\circ$ si considerino i seguenti tre fatti, dove C e F sono due generici insiemi:

F1: $C \subseteq F \Rightarrow C^\circ \supseteq F^\circ$ che è di verifica immediata.

F2: $C^\circ \cap F^\circ \supseteq (C + F)^\circ$ si ottiene applicando F1 a $C \subseteq C + F$ e $F \subseteq C + F$.

Premessa a F3: Se C è un insieme chiuso e convesso e $x \notin C$ allora esiste un iperpiano che separa x da C, ovvero esistono un vettore y e un reale b t.c. $x \cdot y > b$ e $c \cdot y \leq b$ per ogni $c \in C$.

Basta prendere $y = x - c_\infty$ e $b = c_\infty \cdot y$ dove c_∞ è tale per cui $||x - c_\infty||^2 = inf_{c \in C}||x - c||^2$. Sia d tale limite inferiore. Allora si ha che $x \cdot y = (y + c_\infty) \cdot y = y \cdot y + c_\infty \cdot y = y \cdot y + b > b$. Per vedere invece che $c \cdot y \leq b$ si osservi innanzi tutto che $c_\infty \in C$ perché C è chiuso e c_∞ può essere visto come il punto limite della sequenza di vettori c_k t.c. $||x - c_k||^2 < d + 1/k$ – vettori che stanno in C. Pertanto, essendo C un insieme convesso, anche il vettore $\varepsilon c + (1-\varepsilon)c_\infty$è contenuto in C per qualunque $c \in C$ e $\varepsilon > 0$. Ma allora $||x - (\varepsilon c + (1-\varepsilon)c_\infty)||^2 \geq d$ ovvero $||x - (\varepsilon c + (1-\varepsilon)c_\infty)||^2 - d = ||x - c_\infty - \varepsilon(c - c_\infty)||^2 - d = -2\varepsilon y \cdot (c - c_\infty) + \varepsilon^2 ||c - c_\infty||^2 > 0$. Questo è soddisfatto per un generico $\varepsilon > 0$ solo se $y \cdot (c - c_\infty) \leq 0$ ovvero se $c \cdot y \leq c_\infty \cdot y = b$.

F3: $C = C^{\circ\circ}$ per ogni C insieme limitato e chiuso rispetto addizione e moltiplicazione per scalari non negativi (e dunque convesso).
L´inclusione "$\subseteq$" è ovvia.
L´inclusione "$\supseteq$" si dimostra per assurdo: supponiamo che $x \in C^{\circ\circ}$ ma $x \notin C$ e sia $(y,\, b)$ un iperpiano come visto nella premessa; allora anche $(y,\, 0)$ è un tale iperpiano[‡‡] e si ottiene la seguente contraddizione:

$$(y,\, 0)\, \text{è } iperpiano \Leftrightarrow \begin{cases} x \cdot y > 0 \\ c \cdot y \leq 0\, \forall c \in C \end{cases} \Rightarrow\; y \in C^{\circ} \;\Rightarrow\; x \cdot y \leq 0\, essendo\, x\, \in C^{\circ\circ}$$

Considerando gli insiemi $\mathcal{D}^{\circ}$ e $\mathcal{M}^{\circ}$(che soddisfano banalmente le condizioni di F3) si ottiene quindi

$$\begin{array}{lrcl} F2: & \mathcal{D}^{\circ\circ} \cap \mathcal{M}^{\circ\circ} & \supseteq & (\mathcal{D}^{\circ} + \mathcal{M}^{\circ})^{\circ} \quad \Rightarrow \\ F1: & (\mathcal{D}^{\circ\circ} \cap \mathcal{M}^{\circ\circ})^{\circ} & \subseteq & (\mathcal{D}^{\circ} + \mathcal{M}^{\circ})^{\circ\circ} \quad \Leftrightarrow \\ F3: & (\mathcal{D} \cap \mathcal{M})^{\circ} & \subseteq & \mathcal{D}^{\circ} + \mathcal{M}^{\circ} \end{array}$$

□

5.4 $\vartheta_3 \leq \vartheta_4$

In questa sezione viene riscritta e commentata la prova di $\vartheta_3(G, w) \leq \vartheta_4(G, w)$.

Lemma 5.4.1 *Dato $b'_v = Qb_v$, dove Q è una matrice ortogonale e b è un labeling ortogonale normalizzato per il grafo $\overline{G}$, b' è un labeling ortogonale normalizzato per il grafo $\overline{G}$.*

Dimostrazione. La dimostrazione consiste nel provare che: b' è un labeling ortogonale di $\overline{G}$ e che vale $\sum_v \| b'_v \|^2 = 1$.

Per vedere che b' è un labeling ortogonale per $\overline{G}$ occorre dimostrare che:

$$\forall u, v \in V b'_u \cdot b'_v = 0 \text{ quando } u \not\sim_{\overline{G}} v.$$

Si consideri il prodotto scalare $b'_u \cdot b'_v$ di due vettori di b'; questo utilizzando la definizione di b'_v può essere riscritto in:

$$(Qb_u) \cdot (Qb_v)$$

applicando la definizione di prodotto scalare (definizione 1.1.1) si ottiene:

$$(Qb_u)^T (Qb_v)$$

quindi per la nota proprietà del prodotto di matrici $(AB)^T = (B^T A^T)$ si ha:

$$b_u^T Q^T Q b_v$$

‡‡infatti, essendo C chiuso e convesso, $0 \in C$ e dunque $x \cdot y > b \geq 0 \cdot y = 0$;
inoltre $c \cdot y \leq 0$ perché se cosi non fosse, $(\lambda c) \cdot y$ sarebbe illimitato, contrariamente alla definizione dell´iperpiano $(y,\, b)$.

siccome Q è una matrice ortogonale il prodotto Q^TQ è pari a I (l'identità), si ha quindi:

$$b_u^T b_v$$

riapplicando a ritroso la definizione di prodotto scalare la quantità $b_u^T b_v$ è riscrivibile in:

$$b_u \cdot b_v$$

per ipotesi b è un labeling ortogonale normalizzato per $\overline{G}$ quindi vale che $b_u \cdot b_v = 0$ quando $u \not\sim_{\overline{G}} v$ quindi per quanto dimostrato sopra: $b'_u \cdot b'_v = b_u \cdot b_v$, allora anche b' è un labeling ortogonale.

Effettuando i seguenti passaggi (spiegati analogamente a prima)

$$\sum_v \| b'_v \|^2 = \sum_v \| Qb_v \|^2 = \sum_v \left(\sqrt{(Qb_v) \cdot (Qb_v)} \right)^2 = \sum_v (Qb_v)^T (Qb_v) = \sum_v b_v^T Q^T Q b_v =$$

$$= \sum_v b_v^T b_v = \sum_v b_v \cdot b_v = \sum_v \sqrt{b_v \cdot b_v}^2 = \sum_v \| b_v \|^2 = 1$$

l'ultimo passaggio è giustificato dal fatto che, per ipotesi, b è un labeling ortogonale normalizzato.

Quindi b' è un labeling ortogonale normalizzato per il grafo $\overline{G}$. $\square$

Teorema 5.4.1 *Dato un grafo G ed il suo complementare $\overline{G}$ ed un labeling reale w non negativo su cui sono definite le funzioni*

$$\vartheta_3(G, w) = \max \left\{ \sum_{u,v} (\sqrt{w_u} b_u) \cdot (\sqrt{w_v} b_v) \,\middle|\, b \text{ è un labeling ortogonale normalizzato di } \overline{G} \right\}$$

$$\vartheta_4(G, w) = \max \left\{ \sum_v c(b_v) w_v \,\middle|\, b \text{ è un labeling ortogonale di } \overline{G} \right\}$$

si ha che $\vartheta_3 \leq \vartheta_4$.

Dimostrazione. Supposto che b sia il labeling ortogonale normalizzato di $\overline{G}$ per cui si ottiene il massimo richiesto in ϑ_3; e si supponga che i vettori elementi di b abbiano dimensione d.

Sia

$$x_k = \sum_v b_{kv} \sqrt{w_v}, \qquad 1 \leq k \leq d$$

allora

$$\vartheta_3(G, w) \stackrel{\star}{=} \sum_{u,v} (\sqrt{w_u} b_u) \cdot (\sqrt{w_v} b_v) \stackrel{*}{=} \sum_k x_k^2$$

- $\star$ per come è stato scelto b, cioè quel labeling ortogonale normalizzato che rende massima la quantità $\sum_{uv} (\sqrt{w_u} b_u) \cdot (\sqrt{w_v} b_v)$; $\square\star$

* il termine

$$\sum_{u,v} (\sqrt{w_u} b_u) \cdot (\sqrt{w_v} b_v)$$

applicando la definizione di prodotto scalare e la proprietà commutativa della moltiplicazione può essere riscritto in

$$\sum_{u,v} \left(\sum_k b_{ku} \sqrt{w_u} b_{kv} \sqrt{w_v} \right)$$

applicando la commutatività del prodotto e l'associatività della somma può essere riscritto in:

$$\sum_{k,u} \left(b_{ku} \sqrt{w_u} \sum_v b_{kv} \sqrt{w_v} \right)$$

per la definizione di x_k si ha:

$$\sum_{k,u} b_{ku} \sqrt{w_u} x_k$$

con motivazione analoghe si possono scrivere i seguenti passaggi:

$$\sum_k \left(\sum_u b_{ku} \sqrt{w_u} x_k \right) = \sum_k \left(x_k \sum_u b_{ku} \sqrt{w_u} \right) = \sum_k x_k x_k = \sum_k x_k^2$$

$\square *$

Data Q matrice ortogonale quadrata di dimensione d la cui prima riga è $(\frac{x_1}{\sqrt{\vartheta_3}}, \ldots, \frac{x_d}{\sqrt{\vartheta_3}})^T$, e $b'_v = Qb_v$, che per il lemma 5.4.1 è un labeling ortogonale normalizzato del grafo $\overline{G}$ abbiamo:

$$x'_k \stackrel{\star}{=} \sum_v b'_{kv} \sqrt{w_v} \stackrel{*}{=} \sum_{v,j} Q_{kj} b_{jv} \sqrt{w_v} \stackrel{\dagger}{=} \sum_j Q_{kj} x_j \stackrel{\ddagger}{=} \begin{cases} \sqrt{\vartheta_3} & k = 1; \\ 0 & k > 1. \end{cases}$$

⋆ x' è definito in modo analogo a x_k usando b' al posto di b; $\square\star$

* si applica la definizione di $b'_{kv} = (Qb_v)_k = \sum_j Q_{kj} b_{jv}$; $\square *$

† siccome Q_{kj} rimane costante al variare di v, allora può essere estratto dalla sommatoria per v ottenendo

$$\sum_j \left(Q_{kj} \sum_v b_{jv} \sqrt{w_v} \right)$$

quindi essendo $x_j = \sum_v b_{jv} \sqrt{w_v}$ si ottiene:

$$\sum_j Q_{kj} x_j$$

$\square\dagger$

‡ si hanno due casi:

$k = 1$: sappiamo che $Q_{1j} = \dfrac{x_j}{\sqrt{\vartheta_3}}$; utilizzando questa conoscenza si ha:

$$\sum_j Q_{kj} x_j = \sum_j \frac{x_j}{\sqrt{\vartheta_3}} x_j = \sum_j \frac{x_j^2}{\sqrt{\vartheta_3}}$$

banalmente per il fatto che $\frac{1}{\sqrt{\vartheta_3}}$ è costante al variare di j si può scrivere:

$$\frac{1}{\sqrt{\vartheta_3}} \sum_j x_j^2$$

precedentemente si è dimostrato che $\vartheta_3(G, w) = \sum_k x_k^2$ per cui si ha:

$$\frac{1}{\sqrt{\vartheta_3}} \sum_j x_j^2 = \frac{\vartheta_3}{\sqrt{\vartheta_3}} = \sqrt{\vartheta_3}$$

$k > 1$ per ipotesi Q è una matrice ortogonale quindi si ha che le sue colonne sono linearmente indipendenti, cioè $\forall i, j \; i \neq j \; Q_i \cdot Q_j = 0$.
Moltiplicando e dividendo $\sum_j Q_{kj} x_j$ per $\sqrt{\vartheta_3}$ si ottiene:

$$\frac{\sqrt{\vartheta_3}}{\sqrt{\vartheta_3}} \sum_j Q_{kj} x_j$$

$\dfrac{1}{\sqrt{\vartheta_3}}$ essendo una quantità costante al variare di j, può essere portato all'interno della sommatoria, ottenendo

$$\sqrt{\vartheta_3} \sum_j Q_{kj} \frac{x_j}{\sqrt{\vartheta_3}}$$

ricordiamo che $Q_{1j} = \frac{x_j}{\sqrt{\vartheta_3}}$ e quindi:

$$\sqrt{\vartheta_3} \sum_j Q_{kj} Q_{1j} \overset{\text{def.}\cdot}{=} \sqrt{\vartheta_3} Q_k \cdot Q_1$$

che per la proprietà delle matrici ortogonali (riportata sopra) è pari a zero quando $k > 1$.

□‡

per quanto visto prima si sa che $x'_1 = \sqrt{\vartheta_3}$ quindi si ha che:

$$\vartheta_3(G, w) = \left(\sqrt{\vartheta_3(G, w)}\right)^2 = \left(x'_1\right)^2 \overset{\text{def} x'_1}{=} \left(\sum_v b'_{1v} \sqrt{w_v}\right)^2$$

moltiplicando e dividendo il v-esimo addendo della sommatoria per $\| b'_v \|$ si ottiene*:

$$\vartheta_3 = \left(\sum_v \frac{\| b'_v \|}{\| b'_v \|} b'_{1v} \sqrt{w_v} \right)^2 = v_1 \cdot v_2$$

dove v_1 e v_2 sono due vettori le cui componenti, indiciate su $v \in V$, sono rispettivamente $\| b'_v \|$ e $\frac{b'_{1v}}{\| b'_v \|} \sqrt{w_v}$, quindi applicando la disuguaglianza di Cauchy (lemma 1.1.1) a $(v_1 \cdot v_2)$ si ottiene:

$$(v_1 \cdot v_2)^2 \leq (\| v_1 \| \| v_2 \|)^2$$

applicando la definizione di norma si ha:

$$(\sqrt{v_1 \cdot v_1} \sqrt{v_2 \cdot v_2})^2 \overset{\text{def.}}{=} \left(\sum_v (v_1)_v^2 \sum_v (v_2)_v^2 \right)$$

applicando le definizioni di v_1 e v_2 si ha:

$$\vartheta_3 \leq \left(\sum_v \| b'_v \|^2 \right) \left(\sum_v \frac{b'^2_{1v}}{\| b'_v \|^2} w_v \right)$$

siccome b' è un labeling ortogonale normalizzato si ha che vale $\sum_v \| b'_v \|^2 = 1$ e quindi si ha:

$$\vartheta_3 \leq \sum_v \frac{b'^2_{1v}}{\| b'_v \|^2} w_v \overset{\text{defc}}{=} \sum_v c(b'_v) w_v \leq \vartheta_4(G, w)$$

l'ultima disuguaglianza dipende dal fatto che $\vartheta_4(G, w)$ è definita come il massimo al variare di v delle quantità $\sum_v c(b'_v) w_v$. □

5.5 $\vartheta_4 \leq \vartheta$

In questa sezione viene riscritta e commentata la prova di $\vartheta_4(G, w) \leq \vartheta(G, w)$.

Lemma 5.5.1 *Dato un grafo generico $G = \langle V, E \rangle$, il suo complementare $\overline{G}$, il grafo $\overline{K}_{|V|}$ ed un labeling per gli elementi $v \in V$ di matrici A_v di dimensione $d \times d'$ definite da:*

$$A_v = a_v b_v^T$$

dove a_v e b_v sono labeling ortogonale rispettivamente di G e $\overline{G}$, rispettivamente di dimensione d e d' si ha che tale assegnamento è un labeling ortogonale per $\overline{K}_{|V|}$.

Dimostrazione. Per vedere che l'assegnamento A è un labeling ortogonale di $\overline{K}_{|V|}$ occorre vedere che

$$\forall u, v \in V \text{ tc } u \not\to v \Longrightarrow A_u \cdot A_v = 0$$

*D'ora in poi ci si restringe ai v per cui $\| b'_v \| \neq 0$; ciò non è restrittivo, infatti se per qualche v $\| b'_v \| = 0$ allora $b'_{1v} = 0$ e tutto il termine nella sommatoria è nullo.

dove dalla definizione di prodotto scalare tra matrici scende che:

$$A_u \cdot A_v \overset{\text{def.}\cdot}{\equiv} \operatorname{tr}\left(A_u^T A_v\right) \overset{\text{def.}A_v}{\equiv} \operatorname{tr}\left(\left(a_u b_u^T\right)^T a_v b_v^T\right) \overset{(AB)^T = B^T A^T}{\equiv} \operatorname{tr}\left(b_u a_u^T a_v b_v^T\right)$$

Siccome il prodotto matriciale è associativo, la quantità $a_u^T a_v$ è uno scalare. Si noti inoltre che dato c scalare $\operatorname{tr}(cA) = c \operatorname{tr}(A)$. Quindi utilizzando la commutatività del prodotto per uno scalare si può riscrivere il tutto come

$$a_u^T a_v \operatorname{tr}\left(b_u b_v^T\right)$$

Siccome la matrice di dimensione $d' \times d'$, ottenuta moltiplicando due vettori (uno colonna e l'altro riga) di dimensione d', ha la caratteristica di avere l'elemento i-esimo della diagonale pari al prodotto degli elementi i-esimi dei due vettori, si ha che

$$\operatorname{tr}\left(b_u b_v^T\right) = \sum_{i=1}^{d'} (b_u)_i (b_v)_i \overset{\text{def.}\cdot}{\equiv} b_u \cdot b_v$$

Quindi si ottiene

$$A_u \cdot A_v = (a_u \cdot a_v)(b_u \cdot b_v)$$

Quantità, banalmente uguale a zero in quanto $a_u^T a_v$ è zero quando non lo è $b_v^T b_u$ e viceversa (sono labeling ortogonale uno di G e l'altro di $\overline{G}$). $\square$

Lemma 5.5.2 *Dato un grafo $G \equiv (V, E)$ ed il suo complementare $\overline{G}$, per $\forall a$ labeling ortogonale di G di dimensione d e $\forall b$ labeling ortogonale di $\overline{G}$ di dimensione d' si ha che:*

$$\sum_{v \in V} c(a_v) c(b_v) \leq 1$$

Dimostrazione. Si consideri la matrice A_v di dimensione $d \times d'$ definita come:

$$A_v = a_v b_v^T$$

per il lemma 5.5.1 la matrice è un labeling ortogonale per il grafo $\overline{K}_{|V|}$ e quindi per il lemma 2.2.1

$$\sum_{v \in S} c\left(A_v\right) \leq 1$$

dove $S \subseteq V$ è un *stable set* cioè vale che

$$\forall u, v \in S \; u \not\sim v.$$

Siccome A_v è un labeling ortogonale per il grafo $\overline{K}_{|V|}$ si ha che la precedente disuguaglianza vale per $S = V$ (in quanto, per definizione di $\overline{K}_{|V|}$ nessun elemento di V è adiacente ad un altro elemento di V in $\overline{K}_{|V|}$).

il costo di A_v è definito da:

$$c(A_v) \overset{\text{def.}c}{\equiv} \frac{A_{1v}^2}{\| A_v \|^2} \overset{\text{def.}A_v}{\equiv} \frac{(a_{1v} b_{1v})^2}{\| A_v \|^2} \overset{\| A_v \| = \sqrt{A_v \cdot A_v}}{\equiv} \frac{(a_{1v} b_{1v})^2}{A_v \cdot A_v} \overset{\dagger}{=} \frac{(a_{1v} b_{1v})^2}{\| a_v \|^2 \| b_v \|^2} =$$

$$= \frac{a_{1v}^2 b_{1_v}^2}{\| a_v \|^2 \| b_v \|^2} = \frac{a_{1v}^2}{\| a_v \|^2} \frac{b_{1v}^2}{\| b_v \|^2} \stackrel{\mathsf{def.}c}{=} c(a_v)c(b_v)$$

dove † è dovuto a:

$$A_v \cdot A_v \stackrel{\mathsf{def.}\cdot e A_v}{=} \operatorname{tr}\left(\left(a_v^T a_v\right)\left(b_v^T b_v\right)\right) \stackrel{\mathsf{def.}norma}{=} \operatorname{tr}\left(\| a_v \|^2 \| b_v \|^2\right) \stackrel{\operatorname{tr}(c)=c}{=} \| a_v \|^2 \| b_v \|^2$$

Quindi $\sum_v c(a_v)c(b_v) = \sum_v c(A_v) \leq 1$ □

Teorema 5.5.1 *Dato un grafo G ed il suo complementare $\overline{G}$ ed un labeling reale w non negativo su cui sono definite le funzioni*

$$\vartheta_4(G, w) = \max \left\{ \sum_v c(b_v) w_v \;\middle|\; b \text{ è un labeling ortogonale di } \overline{G} \right\}$$

$$\vartheta(G, w) = \max \{ w \cdot x \mid x \in TH(G) \}$$

si ha che $\vartheta_4 \leq \vartheta$.

Dimostrazione. Per dimostrare la disuguaglianza $\vartheta_4 \leq \vartheta$ preso b labeling ortogonale di $\overline{G}$ per il quale si ottiene il massimo delle quantità $\sum_v c(b_v) w_v$ e quindi ϑ_4 occorre far vedere che il labeling reale x definito da

$$x_v = c(b_v) \stackrel{\mathsf{def.}c}{=} \frac{b_{1v}^2}{\| b_v \|^2}$$

appartiene a TH(G). Quindi, per definizione di $\vartheta(G, w)$, $\vartheta_4(G, w) = w \cdot x$ è minore o al più uguale a $\vartheta(G, w)$.

Per dimostrare che x appartiene a TH(G) si deve dimostrare (dalla definizione di TH(G)) che:

$$\forall a \text{ labeling ortogonale di } G \qquad \sum_{v \in V} c(a_v) x_v = \sum_{v \in V} c(a_v) c(b_v) \leq 1$$

questo segue dal lemma 5.5.2 che afferma che

$$\forall a \text{ labeling ortogonale di } G \text{ e } \forall b \text{ labeling ortogonale di } \overline{G} \qquad \sum_{v \in V} c(a_v) c(b_v) \leq 1$$

e che quindi vale anche nel caso particolare di b. □

6 Complessità del Calcolo di ϑ

6.1 Il Calcolo di ϑ è Polinomiale

Lemma 6.1.1 *Sia $\mathcal{K}$ l'insieme definito in 5.3.2 allora $\mathcal{K}$ è convesso.*

Dimostrazione. La convessità di $\mathcal{K}$ segue ricorsivamente dalla sua definizione: infatti sia $\mathcal{M}_1$ che $\mathcal{D}$ risultano essere convessi.
Per verificare la convessità di $\mathcal{M}_1$ è sufficiente vedere che, date due matrici B_1 e $B_2 \in \mathcal{M}_1$, anche la matrice $B = \lambda B_1 + (1-\lambda)B_2$ appartiene all'insieme $\mathcal{M}_1$, ovvero:

- B è simmetrica; infatti la simmetria si conserva rispetto a combinazioni lineari.
- $B_{ij} = 0$ se i — j in G; infatti $B_{ij} = \lambda(B_1)_{ij} + (1-\lambda)(B_2)_{ij} = \lambda 0 + (1-\lambda)0 = 0$.
- $\operatorname{tr}(B) = 1$; infatti $\operatorname{tr}(B) = \lambda \operatorname{tr}(B_1) + (1-\lambda)\operatorname{tr}(B_2) = \lambda + (1-\lambda) = 1$.

In modo del tutto analogo si dimostra che anche l'insieme $\mathcal{D}$ è convesso. □

Lemma 6.1.2 *Siano $\mathcal{K}$ l'insieme definito in 5.3.2 e S una sfera centrata in 0 e di raggio n, come definita in 1.1.8 allora vale che $\mathcal{K} \subseteq S(0,n)$*

Dimostrazione. Sia $B = (B_{ij}) \in \mathcal{K}$; la tesi può essere formulata come

$$B \in S(0,n) \Leftrightarrow ||B - 0||_2 \leq n \Leftrightarrow ||B||_2 \leq n$$

e viene dimostrata dalla seguente catena di disuguaglianze:

$$\| B \|_2 \overset{\text{def.}\|\,\|_2}{=} \sqrt{\sum_{k,l=1}^{n} B_{kl}^2} \leq \sqrt{\sum_{k,l=1}^{n} \max_{ij}(B_{ij}^2)} = \sqrt{n^2 \max_{ij}(B_{ij}^2)} =$$

$$= n \max_{ij} \sqrt{B_{ij}^2} = n \max_{ij} |B_{ij}| \overset{\dagger}{\leq} n \max_{ij} \sqrt{B_{ii}B_{jj}} \overset{\ddagger}{\leq} n \max_{ij} \sqrt{1 * 1} = n$$

† Dalla caratterizzazione di matrice semidefinita positiva (definizione 1.2.11) si ha che tutte le sottomatrici principali $B_{\{ij\}\{ij\}} \in \mathbb{R}^{2\times 2}$, con $1 \leq i < j \leq n$ hanno determinante non negativo; pertanto, tenendo presente che B è una matrice simmetrica (definizione 1.2.8), cioè $B_{ij} = B_{ji}$) si ha che:

$$\det \begin{pmatrix} B_{ii} & B_{ij} \\ B_{ji} & B_{jj} \end{pmatrix} = B_{ii}B_{jj} - B_{ji}B_{ij} = B_{ii}B_{jj} - B_{ij}^2 \geq 0 \quad \Leftrightarrow$$

$$B_{ij}^2 \leq B_{ii}B_{jj} \quad \Leftrightarrow$$

$$|B_{ij}| \leq \sqrt{B_{ii}B_{jj}}$$

L'ultima equivalenza richiede che $B_{ii} \geq 0 \, \forall i \in [1,n]$. Questo segue di nuovo dalla definizione di B come matrice semidefinita positiva (ovvero B soddisfa $x^T B x \geq 0 \, \forall x \in \mathbb{R}^n$). Infatti, considerando il vettore $x^T = (0, \ldots, 0, 1, 0, \ldots, 0)$ con $x_i = 1$, $i \in [1,n]$ si trova:

$$0 \leq x^T B x = \sum_j (x^T B)_j x_j = (x^T B)_i * 1 = \sum_j x_j B_{ji} = 1 * B_{ii}$$

‡ $B_{jj} \leq 1$, $j = 1, \ldots, n$ segue banalmente dal fatto che $\operatorname{tr}(B) = \sum_{i=1}^{n} B_{ii} = 1$.

□

Lemma 6.1.3 $S\left(\frac{1}{n}I, \frac{1}{n}\right) \cap \mathcal{M}_1 \subseteq \mathcal{K}$

Dimostrazione. Si consideri una matrice simmetrica $B \in \mathcal{M}_1$ in $\mathbb{R}^{V \times V}$ tale che $\left\| \frac{1}{n}I - B \right\|_2 \leq \frac{1}{n}$ (B è una matrice che appartiene a $S\left(\frac{1}{n}I, \frac{1}{n}\right) \cap \mathcal{M}_1$). Dal lemma 1.2.3 scende che il valore assoluto di tutti gli autovalori della matrice $\frac{1}{n}I - B$ sono minori o uguali della sua norma (in questo caso si considera la norma di Frobenius). Quindi si avrà:

$$|\lambda| \leq \left\| \frac{1}{n}I - B \right\|_2 \leq \frac{1}{n} \tag{6.1.1}$$

dove λ è un autovalore di $\frac{1}{n}I - B$. Gli autovalori della matrice $\frac{1}{n}I - B$ sono pari a $\frac{1}{n}$ meno gli autovalori di B. Infatti, essendo B una matrice simmetrica dal lemma 1.2.2 segue che $B = QDQ^T$ dove Q è la matrice ortogonale che ha come colonne gli autovettori di B, mentre D è la matrice diagonale avente come elementi sulla diagonale principale gli autovalori di B. Dunque possiamo scrivere che:

$$\frac{1}{n}I - B = \frac{1}{n}QIQ^T - QDQ^T = Q\left(\frac{1}{n}I - D\right)Q^T$$

Sia λ_M l'autovalore massimo di $\frac{1}{n}I - B$. Dalla uguaglianza sopra riportata ne consegue che $\lambda_M = \frac{1}{n} - \lambda_{min}$ dove λ_{min} è l'autovalore minimo di B. La (6.1.1) è valida per tutti gli autovalori della matrice $\frac{1}{n}I - B$ e quindi in particolare anche per λ_M. Per questo motivo possiamo scrivere che $\lambda_M = \frac{1}{n} - \lambda_{min} \leq \frac{1}{n}$ e dunque $\lambda_{min} \geq 0$. Si è cosìdimostrato che tutti gli autovalori di B sono non negativi e possiamo quindi concludere che $B \in \mathcal{D}$ e che $B \in \mathcal{D} \cap \mathcal{M}_1 = \mathcal{K}$. □

Lemma 6.1.4 *Sia $B \in \mathbb{R}^{n \times n}$ matrice semidefinita positiva; allora la matrice $B' \in \mathbb{R}^{(n-1)\times(n-1)} = (B'_{ij})_{i,j=2}^{n}$ ottenuta da B ponendo $B'_{ij} = B_{ij} - \frac{B_{i1}}{B_{11}}B_{1j}$ è semidefinita positiva.*

Dimostrazione. Per la caratterizzazione (presente nella definizione 1.2.11 come punto 4) di matrice semidefinita positiva, per dimostrare che B' è semidefinita positiva basta verificare che essa ha tutte sottomatrici principali con determinante positivo. Tali sottomatrici sono anche le sottomatrici principali della matrice ottenuta estendendo B' al caso $n \times n$, ovvero $B''_{ij} = B_{ij} - \frac{B_{i1}}{B_{11}}B_{1j}$ con $i = 2, \ldots, n$; $j = 1, \ldots, n$ e $B''_{1j} = B_{1j}$. B'' può essere ottenuta direttamente da B, modificando una per una tutte le righe eccetto la prima. Pertanto, senza perdita di generalità, è sufficiente dimostrare che la matrice $B^{\heartsuit} \in \mathbb{R}^{n \times n}$ con una sola riga k modificata, ha tutte sottomatrici principali con determinante positivo.
Sia dunque

$$B^{\heartsuit} = \begin{cases} B_{ij} & se\ i \neq k \\ B_{kj} - \frac{B_{k1}}{B_{11}}B_{1j} & se\ i = k \end{cases}$$

È facile vedere che $B^{\heartsuit}$ può essere scritta come come prodotto tra una matrice P e la matrice B: $B^{\heartsuit} = P \cdot B$ dove

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & & & & & 0 \\ \vdots & 0 & 1 & 0 & & & & 0 \\ 0 & & 0 & 1 & \ddots & & & \vdots \\ -\frac{B_{k1}}{B_{11}} & & & \ddots & \ddots & & & \\ 0 & & & & 0 & 1 & 0 & 0 \\ \vdots & & & & & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix}$$

e che le sue sottomatrici principali (vedere definizione 1.2.9) $B^{\heartsuit}_{JJ}$ sono date da $P_{JJ} \cdot B_{JJ}$. Per dimostrare che tali sottomatrici hanno determinante positivo, si sfrutta la *formula di Binet* (definizione 1.2.6)[†] per il calcolo del determinante:

$$\det(B^{\heartsuit}_{JJ}) = \det(P_{JJ}) \cdot \det(B_{JJ})$$

e si distinguono due casi:

1. $k \notin J$: in questo caso $P_{JJ} = I \in \mathbb{R}^{|J|\times|J|}$ e dunque

   $$\det(B^{\heartsuit}_{JJ}) = \det(I) \cdot \det(B_{JJ}) = 1 \cdot \det(B_{JJ}) > 0$$

   per l'ipotesi di B semidefinita positiva e per la caratterizzazione (definizione 1.2.11 punto 4) di matrici semidefinite positive.

2. $k \in J$: in questo caso P_{JJ} ha una forma simile a P e conviene calcolarne il determinate con la *formula di Laplace* (definizione 1.2.5); a tal proposito sia $(P'_{JJ})_{lm}$ la matrice in $\mathbb{R}^{(|J|-1)\times(|J|-1)}$ ottenuta togliendo a P_{JJ} la l-esima riga e la m-esima colonna. Allora si ha:

   $$\det(P_{JJ}) = \sum_{j\in J}(-1)^{j+1}(P_{JJ})_{j1}\det((P'_{JJ})_{j1}) = (-1)^{1+1}\cdot 1\cdot\det(I)+(-1)^{1+k}\cdot\left(-\frac{B_{k1}}{B_{11}}\right)\cdot\det(P'_{JJ})_{k1}$$

   Essendo

[†] La dimostrazione di tale formula viene effettuata per esempio scrivendo per esteso il determinante, e gli elementi di $B^{\heartsuit}$ come prodotto tra righe di P e colonne di B. Essa consiste dunque in lunghi "calcoli" che evitiamo in questa sede di riportare. Si consulti al proposito un appropriato testo di algebra lineare.

$$(P'_{JJ})_{kl} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & & & & & \\ 0 & \ddots & \ddots & & & & \vdots \\ & \ddots & 1 & 0 & 0 & & \\ \vdots & & 0 & 0 & 1 & \ddots & \\ & & & & \ddots & \ddots & 0 \\ 0 & & \cdots & & & 0 & 1 \end{pmatrix}$$

$\det((P'_{JJ})_{kl})$ è nullo e così pure l'ultimo termine della sommatoria e dunque $\det(P_{JJ}) = 1 > 0$.

Riassumendo: ogni sottomatrice principale $B^{\heartsuit}_{JJ}$ di $B^{\heartsuit}$ ha determinate positivo, pertanto se ne può dedurre che $B' \in \mathbb{R}^{(n-1)\times(n-1)}$ è semidefinita positiva.

□

Lemma 6.1.5 (Weak Membership Problem) *Il* weak membership problem *per $\mathcal{K}$ è risolvibile in tempo polinomiale.*

Dimostrazione. Data una matrice razionale simmetrica B di ordine n si deve verificare se B è semidefinita positiva. Un controllo efficiente di questa proprietà può usare una qualunque delle caratterizzazione presentate in (1.2.11). Nel seguito descriviamo un algoritmo che lavora in tempo polinomiale e che si basa sulla eliminazione Gaussiana.
Sappiamo che B è semidefinita positiva se $\det(B_{II}) \geq 0$ per ogni sottomatrice principale B_{II} di B. Si possono presentare quattro casi.

1. $b_{11} < 0$. Possiamo subito concludere che B non è semidefinita positiva. Infatti $\det(B_{II})$, con $I = \{1\}$, è negativo. Infatti $B_{\{1\}\{1\}} = [b_{11}]$ e il suo determinante è pari a b_{11} che per ipotesi è minore di zero.

2. $b_{11} = 0$ e $b_{1i} \neq 0 \; \forall i = 2, \ldots, n$. Anche in questo caso B non è semidefinita positiva. Infatti $\det(B_{II})$, con $I = \{1, i\}$, è negativo. Infatti
$$B_{\{1i\}\{1i\}} = \begin{bmatrix} b_{11} & b_{1i} \\ b_{i1} & b_{ii} \end{bmatrix}$$
e il suo determinante è pari a $-b_{1i}^2$ essendo B una matrice simmetrica.

3. $b_{1i} = 0 \; \forall i = 1, \ldots, n$. In questo caso è possibile eliminare la prima riga e la prima colonna della matrice B in modo da applicare l'algoritmo alla restante matrice di ordine $(n-1)$.

4. $b_{11} > 0$. In questo caso si scegli come elemento di pivot b_{11}. La matrice B viene cosìtrasformata in una nuova matrice B' tale che $b'_{ij} = b_{ij} - \frac{b_{i1}}{b_{11}} b_{1j}$. La nuova matrice B' è semidefinita positiva se e solo se B è semidefinita positiva (per il lemma 6.1.4). Poiché per costruzione $b'_{1i} = 0 \; \forall i = 1, \ldots, n$, la verifica si riduce ad un problema di ordine $(n-1)$. Infatti per il punto precedente è possibile eliminare la prima riga e la prima colonna di B' e considerare cosìla restante matrice di ordine $(n-1)$.

Dunque per controllare se una data matrice simmetrica B è semidefinita positiva si applica iterativamente l'algoritmo sopra descritto.
Osservazione. È anche necessario verificare che gli elementi delle matrici di ordine inferiore ottenute con questo procedimento richiedano spazio polinomiale. Questo fatto scende però dall'utilizzo della eliminazione Gaussiana. $\square$

Lemma 6.1.6 *Dato un corpo convesso centrato $(K; n, R, r, a)$ ed un oracolo che risolve il weak membership problem per tale corpo e per $\forall y \in \mathbb{Q}^n$ e $\forall \delta \in \mathbb{Q}, \delta > 0$ allora esiste una macchina con oracolo che in tempo polinomiale stabilisce se:*

- $y \in S(K, \delta)$, *o*
- $y \notin K$

Dimostrazione. La dimostrazione è fatta costruendo la macchina in questione come oracolo si considera la macchina che risolve il weak membership problem data in ipotesi.
Fissati y e δ si distinguono due casi:

- $\| y - a \| \geq 2R$ allora per la definizione di corpo convesso centrato (y cade al di fuori della sfera esterna a K) $y \notin K$ che è anche la risposta che l'oracolo fornisce in questo caso.

- $\| y - a \| < 2R$. In questo caso viene richiamato l'oracolo che risolve il problema della membership per K con i seguenti valori:

$$y' = \left(1 - \frac{\delta}{4R}\right) y + \frac{\delta}{4R} a \text{ e } \delta' = \frac{r\delta}{4R}$$

si hanno ulteriori due casi; l'oracolo risponde:

  - $y' \in S(K, \delta')$ allora si ha

$$\| y - y' \| \stackrel{\text{def.}y'}{=} \left\| y - \left(1 - \frac{\delta}{4R}\right) y - \frac{\delta}{4R} a \right\| = \left\| \frac{\delta}{4R} y - \frac{\delta}{4R} a \right\| \stackrel{\text{def. 1.1.3}}{=} \frac{\delta}{4R} \| y - a \| \stackrel{\dagger}{<} \frac{\delta}{2}$$

dove $\dagger$ è dovuto al fatto che

$$\| y - a \| < 2R \equiv \frac{\delta}{4R} \| y - a \| < \frac{\delta}{4R} 2R = \frac{\delta}{2}$$

siccome il responso dell'oracolo afferma che $y' \in S(K, \delta')$ e che vale $\| y - y' \| < \dfrac{\delta}{2}$ allora si ha che

$$y \in S\left(K, \delta' + \frac{\delta}{2}\right) \stackrel{\text{def.}\delta'}{=} S\left(K, \left(\frac{r}{4R} + \frac{1}{2}\right)\delta\right) \stackrel{\text{def.1.1.11}\, r \leq R}{\subseteq} S(K, \delta)$$

Quindi l'oracolo che si sta costruendo risponderà che $y \in S(K, \delta)$

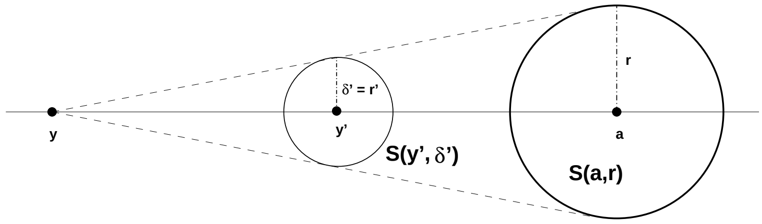

Figura 6.1.1:

- $y' \notin S(K, -\delta')$. In questo caso l'oracolo in costruzione risponderà che $y \notin K$.
  Si supponga per assurdo che $y \in K$. Dalla definizione di corpo convesso centrato in a si ha che $a \in K$ e $S(a,r) \subseteq K$ inoltre anche $y' \in K$, perchè è definito come una particolare combinazione lineare dei punti a e y tale che giaccia sul segmento $\overline{ay}$. Come si può vedere in figura 6.1.1 (che per semplicità rappresenta il caso bidimensionale), sempre per la convessità di K, sono in K anche tutti i punti "intorno" a y', appartenenti ad una sfera di raggio r'. r' è calcolabile grazie alla relazione tra triangoli simili:
  $$\| y - a \| : \| y - y' \| = r : r'$$
  da cui
  $$r' = \frac{\| y - y' \| r}{\| y - a \|} = \frac{\delta r}{4R} \frac{\| y - a \|}{\| y - a \|} = \delta'$$
  Quindi, come si può osservare in figura 6.1.1, la sfera $S(y', \delta') \subseteq K$ ma questo contraddice il responso dell'oracolo
  $$y' \notin S(K, -\delta') \stackrel{\text{def. 1.1.8}}{\Longrightarrow} S(y', \delta') \nsubseteq K$$
  da cui l'assurdo.

□

Lemma 6.1.7 *Esiste un algoritmo con oracolo che, dato un punto $y \in \mathbb{Q}^n$, per ogni coppia di numeri razionali $0 < \delta, \beta < 1$ e per qualsiasi corpo convesso centrato $(K; n, R, r, a)$ per cui è dato un algoritmo che risolve il weak membership problem, allora l'algoritmo:*

1. *determina che $y \in S(K, \delta)$, oppure*
2. *trova un vettore $c \in \mathbb{Q}^n$ tale che $c \neq 0$ e $\forall x \in K, c^T x \leq c^T y + (\delta + \beta \| x - y \|) \| c \|$.*

Il tempo di esecuzione dell'algoritmo è oracle-polynomial in $\left\lceil \frac{1}{\beta} \right\rceil, \langle K \rangle, \langle y \rangle e \langle \delta \rangle$.

Dimostrazione. La dimostrazione è costruttiva e determina un algoritmo, non fondato sul metodo dell'ellissoide, per risolvere il problema della separazione. Fissati K, y, δ e β, si distinguono due casi: se $\| y - a \| \geq 2R$; allora, per definizione di corpo convesso centrato, y cade al di fuori della sfera esterna a K (ovvero $y \notin K$) e quindi, imponendo $c = \frac{y - a}{\| y - a \|}$, si ha $c^T x \leq c^T y$ e dunque il punto 2 risulta banalmente verificato.
Sia dunque $\| y - a \| < 2R$. Poiché l'algoritmo che si sta costruendo deve essere oracle-polynomial time, si considera come oracolo la macchina ottenuta nel lemma 6.1.6. Si interpella tale oracolo con input K, y e δ. Sono possibili due responsi:

- $y \in S(K, \delta)$; nel qual caso il punto 1 è soddisfatto;
- $y \notin K$. Allora si pone:

$$\alpha = \arctan\left(\frac{\beta}{4n^2}\right) \qquad \delta_1 = \frac{r\delta}{R+r}$$
$$r_1 = \frac{r\delta_1}{4nR} = \frac{r^2\delta}{4nR(R+r)} \qquad \varepsilon_1 = \frac{\beta^2 r_1}{16n^4} = \frac{\beta^2 r^2 \delta}{64n^5 R(R+r)}$$

Trattandosi di problemi in forma debole, le grandezze numeriche in gioco dovrebbero limitarsi a vettori con componenti razionali, mentre le grandezze definite qui sopra non sono necessariamente razionali. Nel seguito, tuttavia, si ignoreranno i problemi dovuti all'arrotondamento visto che è ben noto che la conversione dei numeri da reali in razionali può essere resa arbitrariamente precisa.
Consideriamo sul segmento $\overline{ay}$ due punti v e v' tali che

- $v \notin K$;
- v' è quasi appartenente a K, cioè $v' \in S(K, \varepsilon_1)$;
- v e v' sono arbitrariamente vicini, in particolare $\| v - v' \| \leq \dfrac{\delta_1}{2n}$

L'esistenza di v e v' con le suddette proprietà è garantita dal fatto che essi sono punti a coordinate reali e dunque, procedendo dicotomicamente, è possibile trovarne due che rispettino la distanza fissata. Per definizione di corpo convesso centrato in a, il punto a è sicuramente interno a K e inoltre l'intorno di a di raggio r è parimenti contenuto in K. Poiché siamo sotto l'ipotesi che $y \notin K$, il segmento $\overline{ay}$ in parte appartiene a K in parte a K^C e dunque è possibile trovare v non appartenente a K e v' quasi appartenente a K. Preso il punto

$$v'' = \frac{(r - r_1)v' + (r_1 + \varepsilon_1)a}{r + \varepsilon_1} \qquad v' = \frac{r + \varepsilon_1}{r - r_1} v'' - (r_1 + \varepsilon_1)a \tag{6.1.2}$$

si ha $S(v'', r_1) \subseteq K$. Altrimenti esisterebbe $d \in \mathbb{R}^n$ e $\gamma \in \mathbb{R}$ tali che $\| d \| = 1, d^T x \leq \gamma$ per ogni $x \in K$, e $d^T v'' > \gamma - r_1$; ma allora $d^T v \leq \gamma + \varepsilon_1$ e $d^T a \leq \gamma - r$ che implica $d^T v'' = (r + \varepsilon_1)^{-1}((r - r_1)d^T v' + (r_1 + \varepsilon_1)d^T a) \leq \gamma - r_1$.
Si noti che usando dei passaggi geometrici si ha:

$$\| v - v'' \| \overset{\text{def. } 1.1.2.3}{\leq} \frac{\delta_1}{2n} + \| v' - v'' \| \overset{eq.\ 6.1.2}{=} \frac{\delta_1}{2n} + \frac{r_1 + \varepsilon_1}{r - r_1} \| v'' - a \| < \frac{\delta_1}{n} \tag{6.1.3}$$

senza perdere di generalità si può assumere $v'' = 0$. Pertanto $\| v \| < \dfrac{\delta_1}{n}$.

Sia H un iperpiano perpendicolare a v e passante per il punto $(\cos^2 \alpha)v$. Siano $v_1, \ldots, v_n$ i vertici di un simplesso regolare di H con centro in $(\cos^2 \alpha)v$ tale che l'angolo tra v e v_i con $i \in [1, n]$ è α. Quindi

$$\| v_i \| = (\cos \alpha) \| v \| \tag{6.1.4}$$

Si noti che per la definizione di α $\cos\alpha$ è sempre maggiore di zero.
Per ogni v_i si esegue l'algoritmo costruito nel lemma 6.1.6 con parametro d'errore ε_1. Inizialmente si supponga che l'algoritmo concluda che uno dei vettori v_i non appartenga a K per esempio $v_1 \notin K$. Quindi si ricostruisce il simplesso considerando come v il vettore v_1 e quindi si richiama l'algoritmo del lemma 6.1.6. Si supponga di iterare il procedimento per p volte.
Considerando la successione $v_1, \ldots, v_p = \overline{v}$ formata dai vertici del simplesso che ad ogni passo risultano non appartenere a K. Siccome per come vengono determinati i vari v_i si ha che

$$\| v_i \| = \cos\alpha \, \| v_{i-1} \|$$

per cui

$$\| \overline{v} \| = \cos\alpha \, \| v_{p-1} \| = \underbrace{\cos\alpha \cdot \ldots \cdot \cos\alpha}_{p \text{ volte}} \| v \| = \cos^p \alpha \, \| v \| < \cos^p \alpha R \tag{6.1.5}$$

Siccome si ha $S(0, r_1) \subseteq K$, questo può accadere solo se $(\cos\alpha)^p R > r_1$ cioè se:

$$p < \frac{\left|\ln\left(\frac{R}{r_1}\right)\right|}{|\ln\cos\alpha|}$$

Siccome si ha che:

$$\ln\cos\alpha \overset{\ln x^n = n\ln x}{=} \frac{1}{2}\ln\cos^2\alpha \overset{\cos^2\alpha = 1-\sin^2\alpha}{=} \frac{1}{2}\ln(1-\sin^2\alpha) \overset{\ln(1+x)\leq x}{\leq} -\frac{1}{2}\sin^2\alpha =$$

$$\overset{\sin\alpha = \frac{\operatorname{tg}\alpha}{\sqrt{1+\operatorname{tg}^2\alpha}}}{=} -\frac{1}{2}\frac{\operatorname{tg}^2\alpha}{1+\operatorname{tg}^2\alpha} \overset{\text{def.}\alpha}{=} -\frac{\left(\frac{\beta}{4n^2}\right)^2}{2\left(1+\left(\frac{\beta}{4n^2}\right)^2\right)} = -\frac{\beta^2}{32n^4+2\beta^2} \leq -\frac{\beta^2}{34n^4}$$

Si noti che per come è definita α $\operatorname{tg}\alpha$ è sempre definita.

per cui $p < \dfrac{34n^4\left|\ln\left(\frac{R}{r_1}\right)\right|}{\beta^2}$

Da questo segue che dopo un numero di iterazioni polinomiale in $n, \langle r\rangle, \langle R\rangle$ e $\left\lceil \frac{1}{\beta} \right\rceil$ si ha che l'algoritmo del lemma 6.1.6 conclude con $\overline{v_1}, \ldots, \overline{v_n} \in S(K, \varepsilon_1)$; i vettori $\overline{v_1}, \ldots, \overline{v_n}$ sono stati costruiti a partire dal vettore $\overline{v} \notin K$, proprio come i vettori $v_1, \ldots, v_n$ sono stati ottenuti da v.

Ora si vede che

$$c = \frac{\overline{v}}{\| \overline{v} \|_\infty}$$

soddisfa il punto 2.
Dapprima si dimostra che $\forall x \in K$ vale

$$c^T x \leq \beta \| x \| + \delta_1 \tag{6.1.6}$$

Preso un $x \in K$ si pone

$$v_i' = \frac{r_1}{\varepsilon_1 + r_1}\overline{v_i},\ i = 1, \ldots, n \text{ e}$$

$$w = \frac{1}{n}\sum_{i=1}^{n} v_i' = \gamma \overline{v}$$

dove

$$\gamma = \frac{(\cos^2\alpha)\, r_1}{\varepsilon_1 + r_1} \overset{\text{def.}\varepsilon_1 \text{ e } r_1}{=} \frac{\frac{r^2\delta}{4nR(R+r)}}{\frac{r^2\delta}{4nR(R+r)} + \frac{\beta^2 r^2 \delta}{64n^5 R(R+r)}} \cos^2\alpha =$$

$$\frac{16n^4}{16n^4+\beta^2}\cos^2\alpha \overset{\text{def.}\alpha}{=} \frac{1}{1+\operatorname{tg}^2\alpha}\cos^2\alpha \overset{cos^2\alpha = \frac{1}{1+\operatorname{tg}^2\alpha}}{=} \cos^2\alpha\cos^2\alpha = \cos^4\alpha.$$

Analogamente a prima, siccome $S(0, r_1) \subseteq K$ segue che $v_i' \in K$ per $i = 1, \dots, n$. Si rappresenta x nella forma

$$x = \lambda \overline{v} + u \tag{6.1.7}$$

dove $u^T \overline{v} = 0$. Si distinguono due casi:

- $\lambda \leq 1$ allora dall'equazione 6.1.3 si ha

$$c^T x = \lambda c^T \overline{v} = \frac{\|\,\overline{v}\,\|^2}{\|\,\overline{v}\,\|_\infty} \overset{\|\,v\,\| \leq n \|\,v\,\|_\infty}{\leq} n\,\|\,\overline{v}\,\| \overset{eq.\ 6.1.5}{\leq} n\,\|\,v\,\| \overset{eq.\ 6.1.3}{\leq} \delta_1 \leq \beta\,\|\,x\,\| + \delta_1$$

  che verifica l'equazione 6.1.6

- $\lambda > 1$ Allora è possibile riscrivere l'equazione 6.1.7 in

$$\gamma\overline{v} + \frac{\gamma - 1}{\lambda - 1} u = z = \frac{\gamma-1}{\lambda-1}x + \frac{\lambda-\gamma}{\lambda-1}\overline{v} \tag{6.1.8}$$

  Osservando il lato destro dell'equazione 6.1.8 si nota che $\overline{v}$ è una combinazione lineare (convessa) di z e x cioè $\overline{v}$ è un punto del segmento $\overline{zx}$ e siccome $x \in K$ e $\overline{v} \notin K$ allora per la convessità di K, $z \notin K$. Invece osservando il lato sinistro dell'equazione 6.1.8 si nota che z è sull'iperpiano passante per $v_1', \dots, v_n'$. Siccome $z \notin K$ e $z \notin \operatorname{conv}\{v_1', \dots, v_n'\}$ si ha che

$$\|\,z - w\,\| \geq \frac{1}{n}\,\|\,v_1' - w\,\| \overset{w \angle v_1' = \alpha}{=} \frac{1}{n}\operatorname{tg}\alpha\,\|\,w\,\| \tag{6.1.9}$$

  dunque dall'espressione a sinistra dell'equazione 6.1.8 si può esprimere $u = \dfrac{\lambda-1}{\gamma-1}(z-w)$, quindi

$$\begin{aligned} \|\,u\,\| &= \left|\frac{\lambda-1}{\gamma-1}\right| \|\,z-w\,\| \overset{eq.\ 6.1.9}{\geq} \left|\frac{\lambda-1}{\gamma-1}\right| \frac{1}{n}\operatorname{tg}\alpha\,\|\,w\,\| \overset{\text{def.}w}{=} \\ &= \left|\frac{\lambda-1}{\gamma-1}\right| \frac{\gamma}{n}\operatorname{tg}\alpha\,\|\,\overline{v}\,\| \overset{\gamma\leq 1}{=} \frac{\lambda-1}{1-\gamma}\frac{\gamma}{n}\operatorname{tg}\alpha\,\|\,\overline{v}\,\| \end{aligned} \tag{6.1.10}$$

Usando l'equazione 6.1.7 si ha

$$\begin{aligned}
\| x \| &\overset{eq.\ 6.1.7}{=} \| \lambda\overline{v} + u \| \overset{\text{def. } 1.1.3}{=} \sqrt{\lambda^2\overline{v}^T\overline{v} + u^T u} \geq \| u \| \overset{eq.\ 6.1.10}{\geq} \frac{\lambda-1}{1-\gamma}\frac{\gamma}{n}\mathrm{tg}\,\alpha \| \overline{v} \| = \\
&= \frac{(\lambda-1)\| \overline{v} \|}{n}\frac{\gamma\mathrm{tg}\,\alpha}{1-\gamma} \overset{\text{def.}\gamma}{=} \frac{(\lambda-1)\| \overline{v} \|}{n}\frac{\cos^4\alpha\mathrm{tg}\,\alpha}{1-\cos^4\alpha} = \\
&\overset{\cos^2\alpha=1-\sin^2\alpha}{=} \frac{(\lambda-1)\| \overline{v} \|}{n}\frac{\cos^4\alpha\mathrm{tg}\,\alpha}{1-\cos^2\alpha+\sin^2\alpha\cos^2\alpha} \\
&\overset{\cos^2\alpha=1-\sin^2\alpha}{=} \frac{(\lambda-1)\| \overline{v} \|}{n}\frac{\cos^4\alpha\mathrm{tg}\,\alpha}{\sin^2\alpha(1+\cos^2\alpha)} = \\
&= \frac{(\lambda-1)\| \overline{v} \|}{n}\cos^2\alpha\frac{\cos^2\alpha\mathrm{tg}\,\alpha}{\sin^2\alpha(1+\cos^2\alpha)} \\
&\overset{\frac{\sin\alpha}{\cos\alpha}=\mathrm{tg}\,\alpha}{=} \frac{(\lambda-1)\| \overline{v} \|}{n}\cos^2\alpha\frac{\mathrm{tg}\,\alpha}{\mathrm{tg}^2\alpha(1+\cos^2\alpha)} = \\
&= \frac{(\lambda-1)\| \overline{v} \|}{n}\cos^2\alpha\frac{1}{\mathrm{tg}\,\alpha(1+\cos^2\alpha)} \overset{1+\cos^2\alpha\leq 2}{\geq} \frac{(\lambda-1)\| \overline{v} \|}{2n}\frac{\cos^2\alpha}{\mathrm{tg}\,\alpha} = \\
&= \frac{(\lambda-1)\| \overline{v} \|}{2n}\frac{16n^4+\beta^2}{8n^2\beta} = (\lambda-1)\| \overline{v} \|\frac{16n^4+\beta^2}{16n^3\beta} \geq \\
&\geq (\lambda-1)\| \overline{v} \|\frac{16n^4}{16n^3\beta} = (\lambda-1)\| \overline{v} \|\frac{n}{\beta}
\end{aligned}$$

Pertanto

$$\| x \| \geq (\lambda-1)\| \overline{v} \|\frac{n}{\beta} = \lambda\| \overline{v} \|\frac{n}{\beta} - \| \overline{v} \|\frac{n}{\beta} \iff \lambda\| \overline{v} \|\frac{n}{\beta} \leq \| x \| + \| \overline{v} \|\frac{n}{\beta} \iff \lambda \leq \frac{\| x \|}{\| \overline{v} \|}\frac{\beta}{n}+1.$$

Applicando quanto ottenuto nell'equazione 6.1.7 si ha

$$x = \lambda\overline{v} + u \iff \overline{v}^T x = \lambda\overline{v}^T\overline{v} + \overline{v}^T u \overset{\text{def. } 1.1.3}{=} \lambda\| \overline{v} \|^2 + \overline{v}^T u \overset{\overline{v}^T u=0}{=} \lambda\| \overline{v} \|^2 \iff$$

$$\overline{v}^T x \leq \frac{\| x \|}{\| \overline{v} \|}\frac{\beta}{n}\| \overline{v} \|^2 + \| \overline{v} \|^2 = \frac{\beta}{n}\| \overline{v} \|\| x \| + \| \overline{v} \|^2 \tag{6.1.11}$$

Quindi dall'equazione 6.1.3 si ha

$$c^T x \overset{\text{def.}c}{=} \frac{\overline{v}^T}{\| \overline{v} \|_\infty}x \overset{eq.\ 6.1.11}{\leq} \frac{\beta}{n}\frac{\| \overline{v} \|}{\| \overline{v} \|_\infty}\| x \| + \frac{\| \overline{v} \|^2}{\| \overline{v} \|_\infty} \overset{\| \overline{v} \|\leq n\| \overline{v} \|_\infty}{\leq}$$

$$\leq \beta\| x \| + n\| \overline{v} \| \overset{eq.\ 6.1.5}{\leq} \beta\| x \| + n\| v \| \overset{eq.\ 6.1.3}{\leq} \beta\| x \| + \delta_1$$

che prova la disuguaglianza 6.1.6 per qualsiasi $x \in K$

Per dimostrare che vale il punto 2 per $\forall x \in K$, si considera

$$x' = \frac{r}{R+r}(x-y) = \frac{r}{R+r}x - \frac{r}{R+r}y = \frac{r}{R+r}x - \frac{r}{R+r}\left(\frac{R}{R}y\right) = \frac{r}{R+r}x + \frac{R}{R+r}\left(\frac{-r}{R}y\right)$$

dove $x \in K$ e $\frac{-r}{R} y \in K$ in quanto è un punto che giace sul segmento che unisce i due punti di K, 0 e $-\frac{r}{\| y \|} y$, quindi si può osservare che x' è una combinazione lineare convessa di tali punti e quindi $x' \in K$.
Sostituendo x' nella disuguaglianza 6.1.6 si ottiene

$$\frac{r}{R+r} c^T (x-y) = c^T x' \leq \beta \frac{r}{R+r} \| x-y \| + \delta_1$$

e dunque

$$c^T (x-y) \leq \beta \| x-y \| + \delta_1 \frac{R+r}{r} = \delta + \beta \| x-y \|$$

Siccome $\| c \| \geq 1$ la dimostrazione è conclusa. □

Lemma 6.1.8 (Teorema di Yudin e Nemirovskiĭ) *Sia $(K; n, R, r, a_0)$ un corpo convesso centrato dato da un* ***weak membership oracle*** *allora esiste un* ***oracle-polynomial time algorithm*** *che risolve il* ***weak-violation problem*** *per K.*

Dimostrazione. In base alla definizione di **weak-violation problem**, quello che dobbiamo dimostrare è che esiste un algoritmo polinomiale tale che dati in input $c \in \mathbb{Q}^n$ e $\gamma, \varepsilon \in \mathbb{Q}$ con $\varepsilon > 0$:

1. afferma che $c^T x \leq \gamma + \varepsilon \; \forall x \in S(K, -\varepsilon)$, oppure
2. trova un vettore $y \in S(K, \varepsilon)$ tale che $c^T y \geq \gamma - \varepsilon$.

Sia $K' = K \cap \{x \in \mathbb{R}^n \mid c^T x \geq \gamma\}$

Il ***primo passo*** della dimostrazione consiste nel definire un **shallow separation oracle (SSO)** per K', cioè un oracolo che dati in input un ellissoide $E(A, a)$ descritto da una matrice definita positiva $A \in \mathbb{Q}^{n \times n}$ e un vettore $a \in \mathbb{Q}^n$:

1. trova un vettore $d' \in \mathbb{Q}^n$, $d' \neq 0$ tale che $K' \cap E(A, a) \subseteq H$ dove H è il semispazio definito come $H = \{x \in \mathbb{R}^n \mid d'^T x \leq d'^T a + (n+1)^{-1} \sqrt{d'^T A d'}\}$, oppure
2. afferma che $E(A, a)$ è tough, in altre parole afferma che $E(A, a)$ è un ellissoide tale che $E((n+1)^{-2} A, a) \subseteq K'$.

A questo punto si possono presentare due casi.

Caso 1: $c^T a \leq \gamma$
Il vettore $-c$ e il razionale $-\gamma$ sono output validi per il **SSO** per K'. Questo equivale a dire che $K' \cap E(A, a) \subseteq H$ con $H = \{x \in \mathbb{R}^n \mid -c^T x \leq -c^T a + (n+1)^{-1} \sqrt{(-c)^T A (-c)}\}$. Nel seguito dimostriamo che dato $x \in (K' \cap E(A, a))$ allora $x \in H$.
Dato un $x \in K' \cap E(A, a)$, esso soddisfa la seguente disuguaglianza:

$$c^T x \geq \gamma \text{ (per definizione di K}') \tag{6.1.12}$$

Dalla (6.1.12) e dall'ipotesi $c^T a \leq \gamma$ si ottiene:

$$-c^T x \leq -\gamma \leq -c^T a \leq -c^T a + (n+1)^{-1}\sqrt{(-c)^T A(-c)}$$

il che equivale a dire che $x \in H$. □

Caso 2: $c^T a > \gamma$

Si consideri la matrice Q definita positiva tale che $(n+1)^2 A^{-1} = QQ$ e il corpo convesso ben delimitato $(QK; n, \left\| Q^{-1} \right\|^{-1} r, \| Q \| R, Qa_0)$. Per ipotesi esiste un **weak membership oracle** per K e dunque a partire da esso si può ricavare un **weak membership oracle** per QK[‡]. Per tale motivo è possibile applicare l'algoritmo del Lemma 6.1.7 a $(QK; n, \left\| Q^{-1} \right\|^{-1} r, \| Q \| R, Qa_0)$. L'algoritmo, preso un $y \in \mathbb{Q}^n$ e una coppia di numeri razionali $0 < \delta, \beta < 1$:

(i) afferma che $y \in S(QK, \delta)$, oppure

(ii) trova un vettore $d \in \mathbb{Q}^n$ tale che $d \neq 0$ e $\forall x \in QK$, $d^T x \leq d^T y + (\delta + \beta \| x - y \|) \| d \|$.

Nel nostro caso il vettore y e i numeri razionali δ, β sono tali da soddisfare le seguenti uguaglianze:

$$y = Qa$$

$$\delta = min \left\{ \frac{1}{(n+2)^2}, \frac{\varepsilon}{\| Q^{-1} \|} \right\}$$

$$\beta = \frac{1}{(n+2)}$$

Vediamo ora cosa accade a seconda del tipo di risposta fornita dall'algoritmo.

Risposta (i)

L'algoritmo conclude che $y \in S(QK, \delta)$ e dunque il **SSO** per K' dovrebbe affermare che $E(A, a)$ è tough, cioè $E((n+1)^{-2}A, a) \subseteq K'$. Osserviamo che in questo caso $a \in S(K, \delta \left\| Q^{-1} \right\|) \subseteq S(K, \varepsilon)$. Infatti per ipotesi $y = Qa \in S(QK, \delta)$, cioè $\exists\ z \in K$ tale che $\| Q(a - z) \| \leq \delta$. Per le proprietà delle norme scende che:

$$\| a - z \| = \left\| Q^{-1} Q(a - z) \right\| \leq \left\| Q^{-1} \right\| \| Q(a - z) \| \leq \left\| Q^{-1} \right\| \delta$$

il che equivale a dire che $a \in S(K, \delta \left\| Q^{-1} \right\|)$.

Rimane da dimostrare che $S(K, \delta \left\| Q^{-1} \right\|) \subseteq S(K, \varepsilon)$. Tale fatto segue però dalla definizione di δ. Infatti poiché δ è il minimo tra due quantità possiamo affermare che $\delta \leq \frac{\varepsilon}{\| Q^{-1} \|}$, cioè $\delta \left\| Q^{-1} \right\| \leq \varepsilon$.

Risposta (ii)

L'algoritmo trova un vettore $d \in \mathbb{Q}^n$ tale che $d \neq 0$ e $\forall x \in QK$,

$$d^T x \leq d^T y + (\delta + \beta \| x - y \|) \| d \|$$

$$d^T x \leq d^T Qa + (\delta + \beta \| x - Qa \|) \| d \|$$

[‡]Si omette tale dimostrazione in quanto non rilevante in questo contesto.

che equivale ad affermare che

$$d^T Qz \leq d^T Qa + (\delta + \beta \parallel Q(z-a) \parallel) \parallel d \parallel \forall z \in K. \tag{6.1.13}$$

Se $z \in E(A, a)$ allora applicando la definizione di norma di un vettore, dal fatto che $(n+1)^2 A^{-1} = QQ$ e dalla definizione di ellissoide si ha:

$$\parallel Q(z-a) \parallel = \sqrt{(z-a)^T QQ(z-a)} = (n+1)\sqrt{(z-a)^T A^{-1}(z-a)} \leq n+1 \tag{6.1.14}$$

Quindi se $z \in K \cap E(A, a)$, applicando la definizione di δ, β e dalla (6.1.14), la (6.1.13) può essere riscritta come segue:

$$d^T Qz \leq d^T Qa + \left(\frac{1}{(n+2)^2} + \frac{n+1}{(n+2)}\right) \parallel d \parallel$$

$$< {}^{\S} d^T Qa + \left(1 - \frac{1}{(n+2)^2}\right) \parallel d \parallel.$$

Abbiamo così dimostrato che $K \cap E(A, a) \subseteq H'$ dove H' è il semispazio così definito: $H' = \{z \in \mathbb{R}^n \mid d^T Qz \leq d^T Qa + \left(1 - \frac{1}{(n+2)^2}\right) \parallel d \parallel\}$. Si può dimostrare che $H' \subseteq H = \{x \in \mathbb{R}^n \mid d^T Qx \leq d^T Qa + \left(\frac{1}{(n+1)}\sqrt{(Qd)^T AQd}\right)\}$. Tale dimostrazione consiste nel far vedere che:

$$d^T Qa + \left(1 - \frac{1}{(n+2)^2}\right) \parallel d \parallel \leq d^T Qa + \left(\frac{1}{(n+1)}\sqrt{(Qd)^T AQd}\right)$$

Il che è facilmente provabile tramite semplici passaggi algebrici. Si può inoltre osservare che essendo $K' \cap E(A, a) \subseteq K \cap E(A, a)$ si ha anche $K' \cap E(A, a) \subseteq H$. D'altra parte, H non include $E((n+1)^{-2}A, a)$. Infatti:

1. il vettore $a + \frac{Q^{-1}d}{\parallel d \parallel} \in E((n+1)^{-2}A, a)$. Infatti

$$\left(a + \frac{Q^{-1}d}{\parallel d \parallel} - a\right)^T ((n+1)^2 A^{-1}) \left(a + \frac{Q^{-1}d}{\parallel d \parallel} - a\right) = \left(\frac{d^T Q^{-1}}{\parallel d \parallel}\right) QQ \left(\frac{Q^{-1}d}{\parallel d \parallel}\right) = 1;$$

2. il vettore $a + \frac{Q^{-1}d}{\parallel d \parallel}$ viola la condizione $d^T Qz \leq d^T Qa + \left(1 - \frac{1}{(n+2)^2}\right) \parallel d \parallel$. Infatti

$$d^T Qz = d^T Qa + \frac{d^T QQ^{-1}d}{\parallel d \parallel} = d^T Qa + \parallel d \parallel > d^T Qa + \left(1 - \frac{1}{(n+2)^2}\right) \parallel d \parallel$$

ovvero $\parallel d \parallel > \left(1 - \frac{1}{(n+2)^2}\right) \parallel d \parallel$.

§perché $\left(\frac{1}{(n+2)^2} + \frac{n+1}{(n+2)}\right) < \left(1 - \frac{1}{(n+2)^2}\right)$

Possiamo così concludere che $d' = Qd$ e il numero $\gamma = d^T Qa + \left(1 - \frac{1}{(n+2)^2}\right) \| d \|$ sono degli output validi per il **SSO** per K'.

Il ***secondo passo*** della dimostrazione consiste nell'applicare il **shallow-cut ellipsoid method** (v. 3.3.4) all'insieme convesso K' dato dallo **SSO** definito nel primo passo della dimostrazione e ai numeri razionali $\varepsilon_1 = \left(\frac{r\varepsilon}{2Rn}\right)^n$ e R. Ciò significa che esiste un **oracle-polynomial time algorithm** che trova una matrice definita positiva $A \in \mathbb{Q}^{n\times n}$ e un vettore $a \in \mathbb{Q}^n$ tale che è soddisfatta una delle due seguenti condizioni:

(a) $E(A, a)$ viene dichiarato tough dall'oracolo;

(b) $K' \subseteq E(A, a)$ e $\mathrm{vol}(E(A, a)) \leq \varepsilon_1$.

Se $E(A, a)$ viene dichiarato tough allora si può concludere che il vettore a è una soluzione del **weak-violation problem** per K (punto 2 **weak-violation problem**). Tale fatto deriva dalla osservazione riportata nella precedente **Risposta (i)** dove si è visto che $a \in S(K, \delta \left\| Q^{-1} \right\|) \subseteq S(K, \varepsilon)$ e dunque $a \in S(K, \varepsilon)$. Inoltre poiché per ipotesi $c^T a > \gamma$ si ha $c^T a \geq \gamma - \varepsilon$.

Nel caso in cui il **shallow-cut ellipsoid method** conclude che $K' \subseteq E(A, a)$ e $\mathrm{vol}(E(A, a)) \leq \varepsilon_1$, allora possiamo affermare che $c^T x \leq \gamma + \varepsilon \ \forall x \in S(K, -\varepsilon)$ (punto 1 **weak-violation problem**). La dimostrazione di tale fatto procede per assurdo. Supponiamo che $x \in S(K, -\varepsilon)$ e che $c^T x > \gamma + \varepsilon$, quindi $S\left(K, \frac{\varepsilon}{n}\right) \subseteq K'$. Da ciò si deduce che $S\left(x, \frac{\varepsilon}{2n}\right) \subseteq S\left(K', -\frac{\varepsilon}{2n}\right) \subseteq E(A, a)$. Inoltre sappiamo che:

$$vol(E(A, a)) \leq \varepsilon_1 < vol\left(S\left(x, \tfrac{\varepsilon}{2n}\right)\right)$$

che è una contraddizione. $\square$

Teorema 6.1.1 *Dato un grafo G ed un labeling reale w su cui sono definite le funzioni*

$$\vartheta(G, w) = \vartheta_3(G, w) = \max\{w^T Bw \mid B \in \mathcal{D} \cap \mathcal{M},\ tr\,(B) = 1\}^{\P}$$

si ha che la quantità $\vartheta(G, w)$ è calcolabile in tempo polinomiale.

Dimostrazione. La dimostrazione avviene in tre passi:

1) Risolvere il weak membership problem per $\mathcal{K}$ in tempo polinomiale, utilizzando il lemma 6.1.5.

2) Partendo dal weak membership problem del punto 1), risolvere il weak violation problem per $\mathcal{K}$ in tempo polinomiale, utilizzando il lemma 6.1.8.

3) Partendo dal weak violation problem del punto 2) risolvere il weak optimization problem per $\mathcal{K}$ in tempo polinomiale; questo corrisponde a trovare il massimo richiesto in $\vartheta_3(G, w)$, ovvero calcolare $\vartheta(G, w)$ in tempo polinomiale.

[¶]la prova di uguaglianza tra la definizione data nell'articolo di Knuth e quella data in questa sede può essere trovata nella dimostrazione di $\vartheta_2 \leq \vartheta_3$ a pagina 38.

Questi tre passi vengono schematizzati nel seguente modo:

$$\mathbf{WMEM} \longrightarrow \mathbf{WVIOL} \longrightarrow \mathbf{WOPT}$$

Si noti, che considerare la versione "debole" dei problemi di cui sopra non è in alcun modo restrittivo, grazie all'arbitrarietà di ε. In altre parole, si può facilmente passare da una formulazione "debole" alla sua equivalente "forte" facendo tendere ε a zero; inoltre non è nemmeno restrittivo considerare matrici con componenti razionali anziché reali in quanto ogni reale è approssimabile con un razionale ottenendo la precisione desiderata.

Vediamo dunque nel dettaglio i tre punti della dimostrazione.

1) **WMEM** è risolto per $\mathcal{K}$ in tempo polinomiale, applicando il lemma 6.1.5.

2) **WVIOL** è risolto per $\mathcal{K}$ in tempo polinomiale per il lemma 6.1.8 ($\mathcal{K}$ è dato da un *weak membership oracle* al punto precedente). Infatti, dai primi tre lemmi si ricava che $\mathcal{K}$ è un corpo convesso centrato e well-bounded in $\mathcal{M}_1$:

   - Per il lemma 6.1.1 $\mathcal{K}$ è convesso;
   - Dai lemmi 6.1.2 e 6.1.3 si ha che

   $$S\left(\frac{1}{n}I, \frac{1}{n}\right) \cap \mathcal{M}_1 \overset{lemma\ 6.1.3}{\subseteq} \mathcal{K} \overset{lemma\ 6.1.2}{\subseteq} S(0, n)$$

   In particolare, per come è definito $\mathcal{K}$ si ha $\mathcal{K} \subseteq \mathcal{M}_1$; pertanto si può riscrivere la formula precedente come

   $$S\left(\frac{1}{n}I, \frac{1}{n}\right) \cap \mathcal{M}_1 \overset{lemma\ 6.1.3}{\subseteq} \mathcal{K} \overset{lemma\ 6.1.2}{\subseteq} S(0, n) \cap \mathcal{M}_1$$

   e lavorare nello spazio $\mathcal{M}_1$. Le grandezze a_0, r e R richieste tra le ipotesi del lemma 6.1.8 sono quindi rispettivamente $\frac{1}{n}I, \frac{1}{n}$ e n.

3) **WOPT** è risolto per $\mathcal{K}$ in tempo polinomiale: il massimo cercato si trova infatti facilmente risolvendo WVIOL (con costo polinomiale) per $\mathcal{K}$ e usando un algoritmo di ricerca binaria, il cui costo è in $\mathcal{O}(\log(cardinalit\grave{a}(\mathcal{K}))$.

□

Nota In questa dimostrazione si sono considerati i problemi *WOPT*, *WVIOL* e *WMEM* in riferimento a matrici - problemi la cui formulazione era invece data su vettori. Tuttavia, l'estensione al caso bidimensionale non è compito difficile e si evita dunque in questa sede di riportarla. Accenniamo solo brevemente, atitolo di esempio, alla corrispondenza esistente fra il termine $c^T x$ (con c e x vettori) che viene massimizzato in WOPT e il termine $w^T Bw$ (con w vettore e B matrice) che viene massimizzato in ϑ_3:

$$w^T Bw = \sum_{i=1}^{n}(w^T B)_i w_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} w_j B_{ji}\right) w_i = \sum_{i=1}^{n}\sum_{j=1}^{n} w_j B_{ji} w_i =$$
$$= \sum_{i,j=1}^{n} w_j w_i B_{ji} = \sum_{k=(1,1)}^{(n,n)} W_k B_k = W^T B \qquad \textit{dove}$$
$$W_k = W_{(i,j)} = w_i \cdot w_j$$

Dunque il termine $w^T Bw$ può essere facilmente riportato a una forma vettoriale del tipo $c^T x$.

Riferimenti bibliografici

[1] E.A.Maxwell. *Algebraic structure and matrices.* Cambridge university press edition, 1965. Ristampato nel 1969.

[2] Donald E.Knuth. The sandwich theorem. *The Electronic Journal of Combinatorics*, 1:1–48, 1994.

[3] Lipschutz and Seymour. *Linear algebra.* Collana Schaum, 1975.

[4] M.Grötschel, L.Lovász, and A.Schrijver. The ellipsoid method and its consequences in combinatorial optimization. *Combinatorica*, 1:169–197, 1981.

[5] M.Grötschel, L.Lovász, and A.Schrijver. *Geometric Algorithms and Combinatorial Optimization.* Springer-Verlag, 1988.

[6] N.Christofides. *Graph theory.* London : Academic press edition, 1975.

[7] R.J.Wilson. *Introduction to graph theory.* Edinburgh : Oliver and boyd edition, 1972.