A. Machì

Dispensa V

Combinatoria estremale

I problemi *estremali* sono quei problemi di combinatoria che richiedono di determinare la cardinalità massima che può avere una famiglia $\mathcal{F}$ di insiemi che soddisfa certe condizioni.

1 Metodi di Algebra lineare

Un metodo spesso efficace per risolvere un problema estremale consiste nell'associare a ogni elemento di una famiglia $\mathcal{F}$ di insiemi un vettore di un opportuno spazio vettoriale V, in modo univoco. Se si riesce a dimostrare che i vettori così ottenuti sono linearmente indipendenti, si otterrà la maggiorazione richiesta: la cardinalità della famiglia $\mathcal{F}$ non potrà infatti superare la dimensione dello spazio V.

Sia ora dato un insieme di cardinalità n. Denoteremo gli elementi dell'insieme con i primi n interi $\{1, 2, \ldots, n\}$, e l'insieme con $[n]$. Un sottoinsieme I di $[n]$ si può rappresentare con un vettore le cui componenti costituiscono una $n-$pla di 0 e 1, nella quale c'è 1 nel posto k se $k \in I$ e 0 se $k \notin I$ (*vettore di incidenza* dell'insieme I). In particolare la $n-$pla con tutti 0 rappresenta l'insieme vuoto, e quella con tutti 1 l'intero insieme. L'insieme di questi vettori costituisce uno spazio vettoriale V sopra il campo con due elementi $\{0,1\}$, con la somma modulo 2. La cardinalità di V è pertanto uguale a quella della famiglia di tutti i sottoinsiemi, cioè 2^n.

L'operazione di somma modulo 2 di due vettori di incidenza corrisponde alla differenza simmetrica dei sottoinsiemi che essi rappresentano. (Poiché la differenza simmetrica di due insiemi I e J è l'insieme $(I \cup J) \setminus (I \cap J)$, e dunque nel vettore che la rappresenta c'è uno zero nei posti relativi agli elementi di $I \cap J$, ciò spiega perché se due vettori hanno un 1 nel posto i, la loro somma ha 0 nel posto i). La differenza simmetrica è associativa, come lo è la somma dei vettori.

Un sottoinsieme di $[n]$ si ottiene in modo unico come unione di alcuni tra i singleton $\{1\}, \{2\}, \ldots, \{n\}$ (è un altro modo di dire che un insieme è unione dei propri elementi; unione e differenza simmetrica sono la stessa cosa per singleton distinti). In termini di vettori di incidenza i singleton corrispondono ai vettori $e_1 = (1, 0, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1)$; un vettore di incidenza si ottiene in modo unico come somma di questi. Gli e_i sono quindi una base dello spazio V che pertanto ha dimensione n. Se I è un sottoinsieme di vettore di incidenza v scriveremo $v = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n$ con $\lambda_i = 1, 0$ a seconda che l'elemento i dell'insieme appartenga o no a I.

In uno spazio vettoriale di base $\{e_i\}$, il prodotto scalare di due vettori u e v è definito come la somma dei prodotti componente per componente dei due vettori; si denota con $< u, v >$:

$$< u, v > = < \sum \lambda_i e_i, \sum \mu_i e_i > = \sum \lambda_i \mu_i .$$

Il prodotto scalare è lineare nella prima e nella seconda variabile (bilineare):

$$< u + v, w > = < u, w > + < v, w >, \ < u, v + w > = < u, v > + < u, w >$$

$$< \lambda u, v > = \lambda < u, v >, \ \ < u, \mu v > = \mu < u, v > .$$

Nel caso dello spazio dei vettori associati ai sottoinsiemi di un insieme, il numero di 1 nel prodotto scalare di due vettori di incidenza conta allora gli elementi che i sottoinsiemi corrispondenti hanno in comune:

$$< u, v > = |I \cap J|, \tag{1}$$

dove I e J corrispondono rispettivamente a u e a v. In particolare $< u, u >$ dà il numero di elementi dell'insieme associato a u.

Se si considerano 0 e 1 come gli elementi del campo con due elementi $\mathbf{Z}_2$ si ha:

$$< v_i, v_j > = |I \cap J| = \begin{cases} 1, & \text{se } |I \cap J| \text{ è dispari;} \\ 0, & \text{se } |I \cap J| \text{ è pari.} \end{cases} \tag{2}$$

Nel caso di un'intersezione pari, il prodotto scalare su $\mathbf{Z}_2$ di due vettori è zero: come nel caso classico essi si dicono allora *ortogonali*.

Vediamo ora alcuni esempi di applicazione della tecnica detta. Non sembra che vi siano dimostrazioni più semplici di questi risultati con altre tecniche.

Teorema 1. *Sia $\mathcal{F}$ una famiglia di sottoinsiemi di $[n]$ tale che:*

i) ogni sottoinsieme di $\mathcal{F}$ ha un numero dispari di elementi;

ii) due sottoinsiemi di $\mathcal{F}$ si intersecano in un numero pari di elementi. Allora la famiglia $\mathcal{F}$ consta di al più n sottoinsiemi.

Dim. In termini di vettori di incidenza considerati sul campo $\mathbf{Z}_2$ le ipotesi i) e ii) si traducono come segue:

$$< v_i, v_j >= \begin{cases} 1, \text{ se } i = j; \\ 0, \text{ se } i \neq j. \end{cases} \tag{3}$$

Facciamo vedere allora che sotto le ipotesi dette i vettori della famiglia $\mathcal{F}$ sono linearmente indipendenti, cioè che l'unica combinazione lineare di questi vettori che è uguale a zero è quella banale, cioè quella con i λ_i tutti nulli: se $|\mathcal{F}| = m$ occorre cioè dimostrare che:

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0 \text{ implica } \lambda_1 = \lambda_2 = \ldots = \lambda_m = 0. \tag{4}$$

Per vedere, ad esempio, che $\lambda_1 = 0$ calcoliamo il prodotto scalare dei due membri della (4) per v_1:

$$\lambda_1 < v_1, v_1 > + \lambda_2 < v_2, v_1 > + \cdots + \lambda_m < v_m, v_1 >=< 0, v_1 >= 0. \tag{5}$$

Per la (2), tutti i prodotti scalari che compaiono sono nulli eccetto $< v_1, v_1 >$ che vale 1. L'uguaglianza si riduce allora a $\lambda_1 = 0$, che è quanto si voleva. Analogamente, moltiplicando per $v_2, \ldots, v_n$ si ha $\lambda_2 = \lambda_3 = \ldots = \lambda_m = 0.\diamondsuit$

Esempio. Sia $\mathcal{F}$ una famiglia di singleton (distinti) dell'insieme $[n]$. Due singleton si intersecano in un numero pari di elementi (zero), e per il teorema non vi possono essere più di n sottoinsiemi nella famiglia. In altre parole, con questa famiglia $\mathcal{F}$ si ottiene il fatto ovvio che un insieme con n elementi contiene al più n elementi.

Consideriamo ora una famiglia $\mathcal{F}$ di sottoinsiemi di $[n]$ che a due a due hanno un fissato numero di elementi in comune. Anche qui ci chiediamo: qual è la massima cardinalità che può avere $\mathcal{F}$? La risposta è data dal seguente teorema. Lo spazio vettoriale che ora utilizziamo non sarà più sul campo con due elementi (che in questo caso sembra non funzionare) ma sui reali o sui razionali.

Teorema 2. (FISHER) *Siano $A_1, A_2, \ldots, A_m$ sottoinsiemi distinti di $[n]$ tali che a due a due abbiano intersezione della stessa cardinalità:*

$$|A_i \cap A_j| = k, \; i \neq j, \; 1 \leq k \leq n, \; |A_i| > k.$$

Allora la famiglia consta di al più n sottoinsiemi.

Dim. Per ipotesi, $|A_i| = k + m_i$ per certi $m_i > 0$. Dimostriamo che i vettori di incidenza v_i degli A_i sono indipendenti facendo vedere che se si ha una relazione come la (4) tra i v_i, questa volta con i λ_i numeri razionali, allora i λ_i sono tutti nulli. Per la (1), $< v_i, v_j >= k$, se $i \neq j$, e $< v_i, v_i >= |A_i|$. Consideriamo il prodotto scalare (5) di entrambi i membri della (4) per v_1. Si ha

$$\lambda_1|A_1| + \lambda_2 k + \cdots + \lambda_m k =< 0, v_1 >= 0.$$

Ma $|A_1| = k + m_1$, e dunque la precedente uguaglianza diventa:

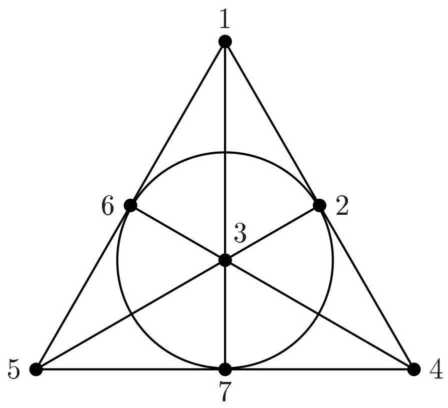
$$\lambda_1 k + \lambda_1 m_1 + \lambda_2 k + \cdots + \lambda_m k = (\lambda_1 + \lambda_2 + \cdots + \lambda_m)k + \lambda_1 m_1 = 0$$

Posto $a = \sum \lambda_i$, abbiamo $ak + \lambda_1 m_1 = 0$. Analogamente, ripetendo l'operazione per $i = 2, 3, \ldots, m$, si ha $ak + \lambda_i m_i = 0$. Dimostriamo che $a = 0$. Se $a \neq 0$, poiché k e m_i sono positivi, dalla $ak + \lambda_i m_i = 0$ segue che, per ogni i, λ_i è diverso da zero e di segno opposto a quello di a. Ma ciò è impossibile in quanto a è la somma dei λ_i. Allora $a = 0$, e dunque $\lambda_i m_i = 0$ per ogni i, e poiché $m_i > 0$ è anche $\lambda_i = 0$. $\diamondsuit$

Esempio Consideriamo, per $n = 7$ la famiglia di sottoinsiemi di [7] che consta delle 7 terne:

$$\{1,2,4\}, \{1,3,7\}, \{1,5,6\}, \{2,3,5\}, \{2,6,7\}, \{3,4,6\}, \{4,5,7\}$$

che costituiscono le 7 "rette" del seguente *piano di Fano*:



Le rette contengono ciascuna tre punti, e sono indicate dai lati e dalle altezze del triangolo e dal cerchio inscritto. Due rette qualunque si incontrano in un punto, e per il teorema non possono esistere più di 7 rette. In questo caso ne abbiamo esattamente 7.

2 Teorema di Sperner

Abbiamo visto nell'*es.* III–12 *i*) che prendendo più della metà dei sottoinsiemi di un insieme ve ne sono due tali che uno dei due è contenuto nell'altro. In realtà la metà dei sottoinsiemi è un numero troppo grande: ne bastano molti di meno per trovarne due che siano uno contenuto nell'altro.

Una famiglia di sottoinsiemi di un insieme si dice *famiglia di Sperner* se presi comunque due sottoinsiemi della famiglia nessuno dei due è contenuto nell'altro.

È chiaro che una qualunque famiglia che consti di insiemi della stessa cardinalità è di Sperner. Ad esempio, la famiglia di tutti i sottoinsiemi di $[n]$ con k elementi è una famiglia di Sperner di cardinalità $\binom{n}{k}$. La più grande fra queste si ottiene per $k = \frac{n}{2}$ se n è pari, e per $k = \frac{n-1}{2}$ se n è dispari (v. oltre). Il teorema di Sperner afferma che nessun'altra famiglia di Sperner può contenere un numero maggiore di sottoinsiemi. Prima di dimostrare il teorema introduciamo la seguente definizione.

Una famiglia di sottoinsiemi $\mathcal{F}$ di $[n]$ si dice *catena* se dati comunque $A, B \in \mathcal{F}$ si ha $A \subset B$ o $B \subset A$. Si dice *anticatena* se per nessun $A, B \in \mathcal{F}$ si ha $A \subset B$ o $B \subset A$. Anticatena è quindi sinonimo di famiglia di Sperner.

Una catena di lunghezza massima (catena *massimale*) nella famiglia di tutti i sottoinsiemi di $[n]$ consta di sottoinsiemi di ciascuna delle cardinalità $0, 1, 2, \ldots, n$, e si ottiene partendo dall'insieme vuoto, poi prendendo un qualunque singleton (e vi sono n scelte per questo), quindi un insieme con due elementi contenente il singleton scelto (e vi sono $n-1$ scelte), ecc. Queste catene massimali sono dunque in numero di $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$. Si ha allora una corrispondenza biunivoca tra le catene massimali su $[n]$ e le permutazioni di $1, 2, \ldots, n$. A ogni permutazione $(i_1, i_2, \ldots, i_n)$ corrisponde la catena massimale:

$$\emptyset \subset \{i_1\} \subset \{i_1, i_2\} \subset \ldots \subset \{i_1, i_2, \ldots, i_n\},$$

e viceversa a questa catena corrisponde la permutazione detta.

Dato un insieme $I \subseteq [n]$ vi sono $|I|!$ catene massimali da $\emptyset$ a I (tutte le permutazioni su $|I|$ elementi), ed $(n - |I|)!$ modi di estendere una di queste catene a una catena massimale. Per un dato I vi sono dunque:

$$|\mathcal{C}_I| = |I|!(n - |I|)!, \tag{6}$$

catene massimali che passano per I.

Sia ora $\mathcal{F}$ un'anticatena in $[n]$, I un elemento di $\mathcal{F}$. È chiaro che una catena massimale non può passare per più di un elemento di $\mathcal{F}$ (se passa per

I e per J, con $I, J \in \mathcal{F}$, allora per definizione di catena si avrebbe $I \subset J$ oppure $J \subset I$, contro l'ipotesi che $\mathcal{F}$ è un'anticatena). Per ogni coppia $I, J \in \mathcal{F}$ una catena massimale passante per I è allora disgiunta da una passante per J. Poiché il numero delle catene massimali è $n!$ abbiamo:

$$\sum_{I \in \mathcal{F}} |\mathcal{C}_I| \leq n!,$$

in quanto nessuna catena viene contata più di una volta nella somma. Per la (6) allora:

$$\sum_{I \in \mathcal{F}} |I|!(n - |I|)! \leq n!$$

o anche:

$$\sum_{I \in \mathcal{F}} \frac{|I|!(n - |I|)!}{n!} \leq 1.$$

Ricordando che:

$$\frac{n!}{|I|!(n - |I|)!} = \binom{n}{|I|},$$

possiamo concludere con il seguente:

Teorema 3. (DISUGUAGLIANZA LYM[1]) *Se $\mathcal{F}$ è una famiglia di Sperner di sottoinsiemi di un insieme con n elementi, allora:*

$$\sum_{I \in \mathcal{F}} \frac{1}{\binom{n}{|I|}} \leq 1. \tag{7}$$

Se x è un numero reale, denotiamo con $\lfloor x \rfloor$ il più grande numero intero minore o uguale a x, e con $\lceil x \rceil$ il più piccolo intero maggiore o uguale a x. Ad esempio $\lfloor 3, 14 \rfloor = 3$, mentre $\lceil 3, 14 \rceil = 4$. Sia n un intero; allora se n è pari $\lfloor \frac{n}{2} \rfloor = \lceil \frac{n}{2} \rceil = \frac{n}{2}$, mentre se n è dispari $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$ e $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$. Ricordiamo che il massimo valore del simbolo binomiale $\binom{n}{k}$ si ha per $k = \lfloor \frac{n}{2} \rfloor$. Si ha infatti:

$$\frac{\binom{n}{r+1}}{\binom{n}{r}} = \frac{\frac{n!}{(r+1)!(n-(r+1))!}}{\frac{n!}{r!(n-r)!}} = \frac{r!(n-r)!}{(r+1)!(n-(r+1))!} = \frac{r!(n-r)(n-(r+1))!}{(r+1)r!(n-(r+1))!} = \frac{n-r}{r+1}$$

e dunque il simbolo binomiale è crescente se $n - r > r + 1$, cioè $n > 2r + 1$ ovvero $r < \frac{n-1}{2}$, e decrescente se $r > \frac{n-1}{2}$. In altri termini,

$$\binom{n}{0} \leq \binom{n}{1} \leq \ldots \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} \geq \ldots \geq \binom{n}{n-1} \geq \binom{n}{n}$$

[1] Dal nome dei tre matematici (Lubell, Yamamoto e Meshalkin) che l'hanno dimostrata o riscoperta.

Dal Teor. 3 segue subito il:

Teorema 4. (SPERNER 1928) *Se $\mathcal{F}$ è una famiglia di Sperner di sottoinsiemi di un insieme con n elementi allora*:

$$|\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}. \tag{8}$$

Dim. Poiché il massimo valore di $\binom{n}{k}$ si ha per $k = \lfloor \frac{n}{2} \rfloor$, $\binom{n}{|I|}$ è minore di $\binom{n}{\lfloor \frac{n}{2} \rfloor}$, e quindi $\frac{1}{\binom{n}{|I|}}$ maggiore di $\frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}$. Se sostituiamo $\lfloor \frac{n}{2} \rfloor$ ad ogni $|I|$ nella somma che compare nella (7) abbiamo:

$$|\mathcal{F}| \cdot \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \leq \sum_{I \in \mathcal{F}} \frac{1}{\binom{n}{|I|}} \leq 1,$$

da cui il risultato. ◊

In altri termini, il Teor. 4 afferma che se si prendono $\binom{n}{\lfloor \frac{n}{2} \rfloor}+1$ sottoinsiemi di un insieme con n elementi si trovano necessariamente due sottoinsiemi uno contenuto nell'altro. Si osservi che, per n grande, il numero $\binom{n}{\lfloor \frac{n}{2} \rfloor} + 1$ è molto minore di $2^{n-1} + 1$, cioè della metà più uno dei sottoinsiemi (v. inizio di questo paragrafo). Si osservi altresì che se n è pari vi è una sola famiglia di Sperner $\mathcal{F}$ che contiene $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ sottoinsiemi, il massimo possibile, ed è quella in cui i sottoinsiemi sono tutti di cardinalità $\frac{n}{2}$ (è l'unico modo di avere uguaglianza nella (8)). Se n è dispari ve ne sono due, quella dei sottoinsiemi con $\frac{n-1}{2}$ elementi, e quella dei sottoinsiemi con $\frac{n+1}{2}$ elementi; la dimostrazione che queste due famiglie sono le uniche per le quali si raggiunge il massimo è un po' più complicata.

Esempio. Sia M una matrice $m \times n$ di interi positivi e sia $c_1, c_2, \ldots, c_n$, o semplicemente $[n] = \{1, 2, \ldots, n\}$, l'insieme delle colonne di M. Un sottoinsieme K di colonne (quindi di $[n]$) si dice una *chiave* se due righe che sono uguali sulle colonne di K sono uguali dovunque. Una chiave si dice *minimale* se non contiene alcun'altra chiave. È chiaro allora che l'insieme delle chiavi minimali forma un sistema di Sperner, e dunque, per il Teor. 4, vi sono al più $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ chiavi minimali per una matrice a n colonne. Ad esempio, per $n = 4$, nella matrice 5×4:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 3 & 1 & 3 & 3 \\ 4 & 4 & 1 & 4 \\ 5 & 5 & 5 & 1 \end{pmatrix}$$

due qualunque colonne costituiscono una chiave, e questa è minimale. Queste coppie di colonne sono in numero di 6, e formano quindi un sistema di Sperner di cardinalità massima ($\binom{4}{\lfloor \frac{4}{2} \rfloor} = \binom{4}{2} = 6$). La maggiorazione data dal teorema di Sperner è la migliore possibile, nel senso che per ogni n è possibile trovare un intero m e una matrice $m \times n$ che ammette $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ chiavi minimali.

Nota. Supponiamo che in un database vi siano i dati di m persone costituiti da n attributi (nome, luogo e data di nascita, ecc). Utilizzando un opportuno codice possiamo supporre che questi attributi siano i numeri interi $1, 2, \ldots, n$, e costruire quindi una matrice intera $m \times n$ che nel posto (i, j) ha l'attributo j dell'$i-$esima persona. Conoscendo i valori di una riga che stanno sulle colonne di una chiave, la riga resta determinata (in altre parole, di una persona basta conoscere gli attributi appartenenti a una chiave per individuarla); di qui il nome di "chiave".