Metodi Matematici per l'Informatica - Dispensa 11
(a.a. 22/23, I canale)

Docente: Lorenzo Carlucci (`lorenzo.carlucci@uniroma1.it`)

1 Estensioni totali di ordini parziali

Gli ordni totali permettono di confrontare gli elementi di un insieme finito in modo del tutto lineare, partendo dal minimo e procedendo seguendo l'ordine. Questo risulta comodo anche dal punto di vista informatico/algoritmico. Gli ordini parziali sono in linea di massima più complicati perché rendono necessario seguire i diversi "percorsi" ramificati che collegano i punti. Risulta dunque interessante osservare che è sempre possibile estendere un ordine parziale a un ordine totale sullo stesso insieme.

Teorema 1. *Sia $A = \{a_1, a_2, \ldots, a_n\}$ un insieme finito ordinato da una relazione R di ordine parziale. Allora esiste una relazione $R^* \subseteq A \times A$ che è un ordine totale ed estende R, ossia per ogni $a, b \in A$, se aRb allora aR^*b.*

Per dimostrare il Teorema è sufficiente dimostrare la seguente proposizione.

Proposizione 1. *Sia $R \subseteq A \times A$ una relazione di ordine parziale. Siano $a, b \in A$ due elementi incomparabili relativamente a R, ossia tali che $(a, b) \notin R$ e $(b, a) \notin R$. Esiste una relazione $R' \subseteq A \times A$ tale che*

1. $R \subseteq R'$,
2. $(a, b) \in R'$.

Dimostrazione. Consideriamo i seguenti due insiemi: Definiamo la relazione R' aggiungendo la coppia (a, b) e tutte le coppie (x, y) per x, y tali che xRa e bRy. Intuitivamente stiamo considerando tutti gli elementi minori o uguali ad a e sitamo imponendo che siano tutti minori o uguali (nella nuova relazione R') a tutti gli elementi maggiori o uguali a b.

In termini insiemistici poniamo:

$$X = \{x \in A \,:\, xRa\}$$

$$Y = \{y \in A \,:\, bRy\}$$

La relazione R' è definita come $R \cup (X \times Y)$.

Dimostriamo che R' è un ordine parziale su A.

Si osserva facilmente che X e Y sono disgiunti: se esistesse un $x \in X \cap Y$ avremmo xRa e bRx e dunque, per transitività di R, anche bRa, contro l'ipotesi che a e b sono incomparabili in R.

R' è riflessiva perché R è riflessiva.

Supponiamo $xR'y$ e $yR'x$. Dimostriamo che $x = y$. Da $xR'y$ abbiamo che xRy oppure $(x, y) \in X \times Y$. Da $yR'x$ abbiamo yRx oppure $(y, x) \in X \times Y$. Abbiamo dunque a priori quattro casi da analizzare:

Caso 1: $(x, y) \in X \times Y$ e $(y, x) \in X \times Y$. Dunque $x \in X \cap Y$, contro il fatto che $X \cap Y = \emptyset$. Questo caso è dunque impossibile.

Caso 2: xRy e yRx. Allora $x = y$ perché R è antisimmetrica.

Caso 3: xRy e $(y, x) \in X \times Y$. Da $y \in X$ segue yRa. Da yRa e xRy segue xRa dunque $x \in X$. Ma per ipotesi $x \in Y$ contro il fatto che $X \cap Y = \emptyset$. Questo caso è dunque impossibile. Si può anche ragionare così:

da $x \in Y$ segue bRx. Da $y \in X$ segue yRa. Da bRx, yRa e xRy segue, per transività di R, anche bRa, contro l'ipotesi che a e b sono incomparabili.

Caso 4: $(x, y) \in X \times Y$, e yRx. Da $x \in X$ segue xRa. Da $y \in Y$ segue bRy. Da xRa e bRy e yRx segue, per transitività di R, bRa, contro l'ipotesi che a e b sono incomparabili.

Dimostriamo ora la transitività di R'. Supponiamo $xR'y$ e $yR'z$ e dimostriamo $xR'z$. Da $xR'y$ abbiamo che xRy oppure $(x, y) \in X \times Y$. Da $yR'z$ abbiamo yRz oppure $(y, z) \in X \times Y$. Abbiamo dunque a priori quattro casi da analizzare:

Caso 1: $(x, y) \in X \times Y$ e $(y, z) \in X \times Y$. Dunque $y \in X \cap Y$, contro il fatto che $X \cap Y = \emptyset$. Questo caso è dunque impossibile.

Caso 2: xRy e yRz. Allora xRz perché R è transitiva. Dunque anche $xR'z$ perché $R \subseteq R'$.

Caso 3: xRy e $(y, z) \in X \times Y$. Da $y \in X$ segue yRa. Da xRy e yRa segue xRa per transitività di R. Dunque $(x, z) \in X \times Y$ e dunque $x \in X$. Questo contraddice che $X \times Y = \emptyset$.

Caso 4: $(x, y) \in X \times Y$, e yRz. Esercizio.

2 Ordini totali e sottosuccessioni monotone

Supponiamo di scegliere a caso una sequenza di k numeri interi distinti, in ordine arbitrario $(a_1, \dots, a_k)$. ù Siamo sicuri di trovare in essa un numero a_i tale che esiste un successivo a_j $(i < j)$ che è maggiore di a_i oppure minore di a_j. Siamo anche sicuri di trovare $1 \leq i < j < h \leq k$ tali che $a_i < a_j < a_h$ oppure $a_i > a_j > a_h$? E se volessimo trovare una successione di questo tipo di lunghezza 4? In generale ci stiamo chiedendo se possiamo trovare "sotto-successioni" strettamente crescenti o strettamente decrescenti all'interno della successione casuale di partenza.

Il seguente teorema ci dice che se vogliamo essere sicuri di trovare, all'interno di una successione arbitraria di numeri naturali, sottosuccessioni lunghe $n + 1$ crescenti o decrescenti, è sufficiente scegliere $n^2 + 1$ numeri.

Teorema 2. *Sia $n \geq 1$. Sia $(x_1, \dots, x_{n^2+1})$ una successione di elementi distinti scelti in insieme X su cui $\preceq$ è un ordine totale. Allora esiste una sottosuccessione strettamente crescente lunga $n + 1$ oppure esiste una sottosuccessione strettamente decrescente lunga $n + 1$.*

NB X non è necessariamente un insieme di numeri ma è un insieme arbitrario! La relazione denotata con $\preceq$ è un arbitrario ordine totale su X. Le sottosuccessioni sono ordinate rispetto all'ordine $\preceq$. Denotiamo con $\prec$ l'ordine stretto ottenuto da $\preceq$ (ossia $x \prec y$ sse $x \preceq y$ e $x \neq y$). Una sottosuccessione strettamente crescente di lunghezza $\ell \leq n^2+1$ è una sequenza $(x_{a_1}, x_{a_2}, \dots, x_{a_\ell})$ con $x_{a_1} \prec x_{a_2} \prec \dots \prec x_{a_\ell}$, per qualche $a_1 < \dots < a_\ell$ in $\{1, \dots, n^2 + 1\}$. Analogamente una sottosuccessione strettamente decrescente di lunghezza $\ell \leq n^2 + 1$ è una sequenza $(x_{a_1}, x_{a_2}, \dots, x_{a_\ell})$ con $x_{a_\ell} \prec x_{a_\ell} \prec \dots \prec x_{a_1}$, per qualche $a_1 < \dots < a_\ell$ in $\{1, \dots, n^2 + 1\}$.

Per capire la dimostrazione può essere utile pensare a un ordine totale famigliare, per es. l'ordine $\leq$ sui naturali, e a valori concreti di n.

Dimostrazione Ragioniamo per assurdo. La Supponiamo quindi che non esista **né** una sottosuccessione strettamente crescente di lunghezza $n+1$ **né** una sottosuccessione strettamente decrescente di lunghezza $n+1$. Consideriamo la funzione

$$f : \{1, \dots, n^2 + 1\} \to \{1, \dots n\}$$

definita ponendo $f(i) =$ lunghezza massima di una successione strettamente crescente che termina con x_i. La funzione f ha dominion $\{1, \dots, n^2 + 1\}$ e, per l'ipotesi per assurdo, codominio $\{1, \dots, n\}$.

Dato che il dominio è più grande del codominio, diversi elementi del dominio assumeranno lo stesso valore tramite f. In particolare almeno $n + 1$ elementi del dominio assumono lo stesso valore. Altrimenti ognuno degli n valori del codominio viene assunto al massimo da n elementi del dominio. Ma dunque al massimo $n + \dots + n = n \times n = n^2$ elementi di $\{1, 2, \dots, n^2 + 1\}$ ricevono un valore. Contraddizione.

Esistono dunque indici $i_1 < \dots < i_{n+1}$ in $\{1, \dots, n^2 + 1\}$ tali che

$$f(i_1) = f(i_2) = \dots = f(i_{n+1}).$$

Sia ℓ il valore comune in $\{1, \ldots, n\}$ assunto dagli elementi $x_{i_1}, \ldots, x_{i_{n+1}}$.

Consideriamo i primi due elementi x_{i_1} e x_{i_2}. Dato che $\preceq$ è un ordine totale, abbiamo che $x_{i_1} \prec x_{i_2}$ oppure $x_{i_2} \prec x_{i_1}$. Dimostriamo che deve essere $x_{i_2} \prec x_{i_1}$. Supponiamo che valga $x_{i_1} \prec x_{i_2}$. Dato che $f(x_{i_1}) = \ell$, esiste una sottosuccessione strettamente crescente lunga ℓ con ultimo termine x_{i_1}. Ossia esistono $j_1 < \cdots < j_{\ell-1} < i_1$ tali che

$$x_{j_1} \prec x_{j_2} \prec \cdots \prec x_{j_{\ell-1}} \prec x_{i_1}.$$

Ma allora la successione

$$x_{j_1} \prec x_{j_2} \prec \cdots \prec x_{j_{\ell-1}} \prec x_{i_1} \prec x_{i_2}$$

è una sottosuccessione strettamente crescente di lungezza $\ell + 1$ che termina con x_{i_2}, contraddicendo l'ipotesi che la massima sottosuccessione di questo tipo è lunga ℓ.

Lo stesso ragionamento dimostra che $x_{i_3} \prec x_{i_2}$, $x_{i_4} \prec x_{i_3}$ etc. fino a $x_{i_{n+1}} \prec x_{i_n}$. Dunque la successione $(x_{i_1}, x_{i_2}, \ldots, x_{i_{n+1}})$ è una sottosuccessione strettamente decrescente (rispetto all'ordine $\prec$) di lunghezza $n+1$. Contro l'ipotesi per assurdo che ogni successione di questo tipo ha lunghezza al più n. **Q.E.D.**

3 Cicli ed elementi minimali in un ordine parziale

Sia R un ordine parziale su un insieme A. Allora R non ha cicli eccetto quelli di tipo aRa. Si ricorda che un ciclo è un cammino che inizia e finisce nello stesso punto, ossia

$$a_1 R a_2 R \ldots R a_1$$

con $a_1, \ldots, a_n R a_1 \in A$.

Supponiamo che esista un ciclo:

$$a_1 R a_2 R \ldots R a_m R a_1$$

con $a_1, \ldots, a_m$ tutti distinti. Per transitività di R abbiamo che

$$a_1 R a_2 R a_3 \text{ implica } a_1 R a_3$$

e analogamente

$$a_1 R a_3 R a_4 \text{ implica } a_1 R a_4.$$

Ripetendo questo argomento otteniamo

$$a_1 R a_m.$$

Ma abbiamo anche, per ipotesi,

$$a_m R a_1.$$

Per antisimmetria di R questo implica $a_1 = a_m$. Questa contraddizione ci dice che non esistono cicli di lunghezza $m \geq 2$ (i cicli di lunghezza 1 esistono per riflessività di R: per ogni $a \in A$ vale aRa).

Proposizione 2. *In un ordine (parziale) esistono solo cicli di lunghezza* 1*, ossia di tipo* (a, a).

Osserviamo che in un ordine parziale su un insieme finito non esiste necessariamente un elemento minimo. Per esempio, la relazione R su $\{1, 2, 3, 4, 5\}$ definita come segue non ha un minimo:

$$\{(1,3), (3,4), (4,5), (1,4), (1,5), (2,3), (2,4), (2,5), (1,1), (2,2), (3,3), (4,4), (5,5)\}.$$

Qui intendiamo per minimo di un ordine R un elemento $a \in A$ tale che per ogni $b \in A$ vale aRb. Nell'ordine qui sopra esistono però elementi "quasi minimi" nel senso che non esistono altri elementi più piccoli di loro. Questo è vero di 1 e di 2, dato che non c'è in R nessuna coppia di tipo $(x, 1)$ con $x \neq 1$ o di tipn o $(x, 2)$ con $x \neq 2$.

Proposizione 3. *Un ordine (parziale) non ha necessariaente un elemento minimo.*

Definizione 1. *Diciamo che un elemento $a \in A$ è* minimale *se per ogni $b \in A\{a\}$ non vale bRa.*

Ogni ordine parziale su un insieme finito ha un elemento minimale. Consideriamo un cammino di lunghezza massima in A, ossia una scelta di elementi $a_1, \ldots, a_m$ in A tali che

$$a_1 R a_2 R \ldots a_{m-1} R a_m$$

e non esista un cammino di lunghezza più grande.

Si osserva allora facilmente che, se prendo un $a \in A$ diverso da tutti gli $a_1, \ldots, a_m$, non può valere aRa_1, altrimenti avremmo un cammino più lungo di quello scelto sopra, ossia:

$$a R a_1 R a_2 R \ldots a_{m-1} R a_m.$$

Si osserva altrettanto facilmente che se prendo un a_i con $2 \leq i \leq m$ non può valere $a_i R a_1$. Se valesse, avremmo che il cammino contiene un ciclo. Ma questo è impossibile.

Abbiamo dimostrato la seguente proposizione.

Proposizione 4. *Un ordine (parziale) ha necessariaente (almeno) un elemento minimale.*

4 Dimostrazione per Induzione

Siamo ora pronti a dare una dimostrazione alternativa dell'estendibilità di ogni ordine parziale su un insieme finito a un ordine totale.

La nostra tesi è: Ogni ordine parziale su un insieme finito si può estendere a un ordine totale sullo stesso insieme. Possiamo riformularla più esplicitamente come segue:

Per ogni possibile cardinalità n, per ogni insieme A di cardinalità n, per ogni ordine parziale R su A, esiste un ordine totale R^* su A tale che $R \subseteq R^*$.

Proponiamo il seguente argomento per stabilire la tesi.

Caso Base. Dimostriamo che la tesi vale per insiemi di cardinalità $n = 1$. Consideriamo un insieme generico di questo tipo, ossia $A = \{a\}$. L'unico ordine parziale R su un insieme di questo tipo è $R = \{(a, a)\}$. Questo ordine è anche totale. Dunque la tesi è verificata: l'estensione totale di R è R stesso.

Passo Induttivo. *Assumiamo* ora che la tesi sia vera fino a insiemi di cardinalità n, dove n è un generico intero ≥ 1. *Dimostriamo* che in questo caso possiamo stabilire la tesi anche per insiemi di cardinalità $n + 1$.

A questo scopo consideriamo un generico insieme A con $n + 1$ elementi. Come sopra osservato A contiene almeno un elemento minimale. Sia a un tale minimale. L'insieme $A \setminus \{a\}$ ha n elementi. Inoltre la relazione R^- su $A \setminus \{a\}$ ottenuta cancellando da R tutte le coppie che contengono a è un ordine parziale.

Ma abbiamo assunto di saper dimostrare la tesi per insiemi di cardinalità n. In particolare possiamo farlo per l'ordine R^- sull'insieme $A \setminus \{a\}$. Esiste dunque un ordine totale, sia esso R_T^- su $A \setminus \{a\}$ che estende R^-. Definiamo un ordine R_T su A come segue:

$$R_T = R_T^- \cup \{(a, x) \,:\, a \in A\}.$$

Si dimostra facilmente che R_T è un ordine totale su A che estende R.

Conclusione. La tesi è vera per ogni cardinalità $n \geq 1$.

L'argomento esposto qui sopra consta di due parti fondamentali: vogliamo stabilire una tesi di tipo universale, ossia che per ogni $n \geq 1$ vale una certa proprietà $P(n)$. Lo facciamo stabilendo i due passi seguenti:

1. **Base**: Verifichiamo/dimostriamo che la proprietà P vale per $n = 1$.

2. **Passo Induttivo**: Consideriamo un generico $n \geq 1$. Assumendo che la proprietà P valga per n, dimostriamo che vale per $n + 1$. Ossia dimostriamo che vale l'implicazione:

$$\text{Se } P(n) \text{ allora } P(n + 1).$$

Nel Passo Induttivo, l'ipotesi che valga P per n viene detta *ipotesi induttiva*.

Questo è un esempio del metodo di dimostrazione per Induzione (o *induzione completa*, o *induzione matematica*) sui numeri naturali. Si tratta di un metodo estremamente generale applicabile in una grandissima quantità di casi in cui vogliamo dimostrare che una certa proprietà P vale di tutti i numeri naturali (o di tutti i numeri naturali maggiori di un certo valore di base).