Metodi Matematici per l'Informatica - Dispensa 13
(a.a. 22/23, I canale)

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

1 Relazioni di equivalenza e partizioni

Il concetto di relazione di equivalenza è una generalizzazione della relazione di identità.

Consideriamo la relazione di identità numerica su $\mathbf{N}$. Ovviamente gode delle seguenti proprietà:

1. Per ogni $n \in \mathbf{N}$, $n = n$.
2. Per ogni $n, m \in \mathbf{N}$: Se $n = m$ allora $m = n$.
3. Per ogni $n, m, q \in \mathbf{N}$: Se $n = m$ e $m = q$ allora $n = q$.

La definizione di relazione di equivalenza è modellata esattamente su queste tre proprietà.

Definizione 1 (Relazione di Equivalenza)**.** *Una relazione R su un insieme A è una* relazione di equivalenza *se e solo se gode delle seguenti tre proprietà:*

1. *(Riflessività) Per ogni $a \in A$, aRa.*
2. *(Simmetria) Per ogni $a, b \in A$: Se aRb allora bRa.*
3. *(Transitività) Per ogni $a, b, c \in A$: Se aRb e bRc allora aRc.*

In breve una relazione $R \subseteq A \times A$ se e solo è riflessiva, simmetrica e transitiva.

Esempio 1. La realzione aRb se e solo se a e b hanno la stessa età è una relazione di equivalenza.

Esempio 2. La relazione tra segmenti nel piano definita ponendo: sRt se e solo se s e t hanno la stessa lunghezza è una relazione di equivalenza.

Osservazione 1. In generale, se definisco una relazione R su A come aRb se e solo se a e b hanno un certo valore assenato identico, quello che ottengo è una relazione di equivalenza. Più formalmente: se $v : A \to X$ è una funzione che associa valori in X agli elementi di A, e pongo aRb se e solo se $v(a) = v(b)$, la relazione che ottengo è di equivalenza. Le proprietà di riflessività, simmetria e transitività vengono ereditate immediatamente dall'identità.

Esempio 3. Non tutte le relazioni di equivalenza si ottengono imponendo una identità di valori associati agli elementi. Per esempio la relazione aRb se e solo se a è parente di b è una relazione di equivalenza. Quali sono le sue classi di equivalenza?

Esempio 4. Consideriamo gli interi $\mathbf{Z}$ e stabiliamo: aRb se e solo se a e b hanno lo stesso resto nella divisione per 2. Per esempio $(-4)R18$ perché sia -4 che 18 hanno resto 0 nella divisione per 2. Analogamente $(-111)R1$. Invece $(-8, 3) \notin R$. Si tratta di una relazione di equivalenza, per l'osservazione di sopra (il valore in questione associato a un intero p è il suo resto nella divisione per 2). Si può anche verificare direttamente che R così definita è una relazione di equivalenza.

Dato che i possibili resti della divisione per 2 di un intero sono 0 e 1, è facile osservare che un arbitrario intero sarà in relazione R con 0 oppure con 1!

Sia p un intero e consideriamo l'insieme degli interi in relazione R con p:

$$[p]_R = \{q \in \mathbf{Z} \,:\, pRq\}$$

Questa viene detta la classe di equivalenza di p modulo R. Si osserva facilmente che per ogni intero p, si ha $p \in [0]_R$ oppure $p \in [1]_R$ a seconda che p sia pari o dispari. Si osserva pure facilmente che se $p \in [0]_R$, ossia p è divisibile per 2 con resto 0, allora $[p]_R = [0]_R$: ogni altro numero che ha lo stesso resto di p nella divisione per 2 ha anche lo stesso resto di 0, ossia resto 0. Se $p \in [1]_R$, ossia p ha resto 1 se diviso per 2 (ossia p è dispari), allora $[p]_R = [1]_R$.

Visto in un altro modo: presi due interi p, q, le loro classi di equivalenza o coincidono oppure sono completamente disgiunte. In particolare: se p e q sono pari allora $[p]_R = [q]_R = [0]_R$, se p e q sono dispari allora $[p]_R = [q]_R = [1]_R$; mentre se p e q sono l'uno pari e l'altro dispari, le loro classi di equivalenza non hanno elementi in comune: $[p]_R \cap [q]_R = \emptyset$. Un elemento in comune dovrebbe essere sia pari che dispari.

La relazione R su $\mathbf{Z}$ determina soltanto due classi di equivalenza: $[0]_R$ e $[1]_R$.

Esempio 5. Definiamo R sugli interi ponendo: aRb se e solo se a e b hanno lo stesso resto nella divisione per 3. Come sopra si dimostra che è un relazione di equivalenza. In questo caso i resti possibili sono tre: 0, 1, 2. Come sopra si osserva facilmente che per ogni intero p si ha $pR0$ oppure $pR1$ oppure $pR2$. In termini di classi di equivalenza questo significa che esistono solo le tre classi di equivalenza: $[0]_R, [1]_R, [2]_R$ contenenti, rispettivamente, gli interi divisibili per 3, gli interi di forma $3 \cdot k + 1$ e gli interi di forma $3 \cdot k + 2$.

La costruzione si generalizza facilmente fissando un intero n qualunque e ponendo aRb se e solo se a e b hanno lo stesso resto nella divisione per n (si dice a e b sono *congruenti modulo* n. Le classi di equivalenza in questo caso sono n e determinano una partizione di $\mathbf{Z}$.

Le osservazioni negli esempi precedenti si generalizzano a relazioni di equivalenza arbitrarie: Ogni relazione di equivalenza determina una partizione dell'insieme su cui è definita. Basta considerare le classi di equivalenza $[a]_R$ al variare di a in A.

Teorema 1. *Sia $R \subseteq A \times A$ una relazione di equivalenza. Per $a \in A$ definiamo*

$$R[a] = \{b \in A \,:\, aRb\}$$

detta classe di equivalenza di a. Valgono i seguenti punti:

1. *Per ogni $a \in A$, $R[a] \neq \emptyset$.*
2. *Per ogni $a, b \in A$ si ha che $R[a] \cap R[b] = \emptyset$ oppure $R[a] = R[b]$.*

Dimostrazione Dato che R è riflessiva, per ogni $a \in A$ vale aRa. Dunque $a \in R[a]$. Questo dimostra il primo punto.

Siano $a, b \in A$. O aRb oppure no. Ragioniamo per casi.

(Caso 1) aRb. Dimostriamo che $R[a] = R[b]$. Cominciamo dimostrando che $R[a] \subseteq R[b]$. Sia $c \in R[a]$. Per definizione vale aRc. Per simmetria vale cRa. Dato che per ipotesi del caso vale aRb, per transitività abbiamo cRb. Per simmetria vale bRc e dunque per definizione $c \in R[b]$. L'inclusione $R[b] \subseteq R[a]$ si dimostra analogamente.

(Caso 2) Non vale aRb. Supponiamo per assurdo che valga $R[a] \cap R[b] \neq \emptyset$. Sia c nell'intersezione di $R[a]$ e $R[b]$. Per definizione di $R[a]$ segue che cRa e per definizione di $R[b]$ segue che bRc. Per simmetria da cRa segue aRc; e da bRc segue cRb. Per transitività, da aRc e cRb segue aRb, contro l'ipotesi del caso. **Q.E.D.**

Il risultato appena dimostrato mostra che ogni relazione di equivalenza su A determina una cosidetta *partizione* di A, ossia una scomposizione di A come unione di sottinsiemi di A due a due disgiunti.

Vale anche il viceversa: ogni partizione determina una relazione di equivalenza.

Definizione 2 (Partizione)**.** *Una partizione di un insieme A è una famiglia $\{C_i : i \in I\}$ di insiemi non vuoti $C_i \subseteq A$, dove I è un insieme qualunque (anche infinito, detto insieme di indici), tali che*

1. *per ogni $a \in A$ esiste un $i \in I$ tale che $a \in C_i$, e*
2. *per $i, j \in I$ se $i \neq j$ allora $C_i \cap C_j = \emptyset$ (ossia le classi C_i sono due a due disgiunte).*

Si osserva che $\bigcup_{i\in I} C_i \subseteq A$ dato che ogni C_i è sottinsieme di A; dal primo punto della definizione di partizione segue invece che $A \subseteq \bigcup_{i\in I} C_i$. Dunque $A = \bigcup_{i\in I} C_i$. (La notazione $\bigcup_{i\in I} C_i$ generalizza la notazione di unione e indica l'insieme che contiene tutti e soli gli elementi x per cui esiste (almeno) un $i \in I$ tale che $x \in C_i$). Il Teorema 1 dimostrato sopra può riformularsi così: se R è una relazione di equivalenza du A, l'insieme delle classi di equivalenza dei suoi elementi (ossia $\{[a]_R : a \in A\}$) sono una partizione di A.

Teorema 2. *Sia $\{C_i : i \in I\}$ una partizione di A. Allora la relazione $R \subseteq A \times A$ definita ponendo aRb sse esiste un $i \in I$ tale che $a, b \in C_i$ è una relazione di equivalenza su A.*

Dimostrazione Dimostriamo che R è riflessiva simmetrica e transitiva. Per ogni a esiste un $i \in I$ tale che $a \in C_i$. Per definizione di R questo implica aRa. Siano $a, b \in A$ tali che aRb. Per definizione di R esiste $i \in I$ tale che $a, b \in C_i$, che implica anche che bRa. Siano $a, b, c \in A$ tali che aRb e bRc. Da aRb segue che esiste $i \in I$ tale che $a, b \in C_i$. Da bRc segue che esiste $j \in C_j$ tale che $b, c \in C_j$. Dall'ipotesi che C_i e C_j sono disgiunte per $i \neq j$, deve essere $i = j$ dunque $a, c \in C_i$ e dunque aRc. **Q.E.D.**

Si vede facilmente che le classi di equivalenza della relazione definita in base alla partizione sono classi della partizione. Si osserva che se $R \subseteq A \times A$ e $S \subseteq A \times A$ determinano le stesse classi di equivalenza allora sono la stessa relazione (esercizio).

2 Relazioni d'ordine

Una relazione d'ordine è una relazione che gode di alcune proprietà fondamentali della relazione di ordine numerico $\leq$ sui naturali.

Consideriamo la relazione di ordine numerico $\leq$ su $\mathbf{N}$. Ovviamente gode delle seguenti proprietà:

1. Per ogni $n \in \mathbf{N}$, $n \leq n$.
2. Per ogni $n, m \in \mathbf{N}$: Se $n \leq m$ e $m \leq n$ allora $m = n$.
3. Per ogni $n, m, q \in \mathbf{N}$: Se $n \leq m$ e $m \leq q$ allora $n \leq q$.
4. Per ogni $n, m \in \mathbf{N}$: O $n \leq m$ oppure $m \leq n$.

La definizione di relazione d'ordine totale è modellata esattamente su queste quattro proprietà.

Definizione 3 (Relazione di Ordine Totale)**.** *Una relazione R su un insieme A è una* relazione di ordine totale *se e solo se gode delle seguenti tre proprietà:*

1. *(Riflessività) Per ogni $a \in A$, aRa.*
2. *(Anti-simmetria) Per ogni $a, b \in A$: Se aRb e bRa allora $a = b$.*
3. *(Transitività) Per ogni $a, b, c \in A$: Se aRb e bRc allora aRc.*
4. *(Totalità) Per ogni $a, b \in A$ vale $a \leq b$ oppure $b \leq a$.*

In breve una relazione $R \subseteq A \times A$ è un ordine totale (o ordine lineare) se e solo è riflessiva, antisimmetrica, transitiva e totale.

La nozione generalizza l'idea fondamentale di un ordine *lineare* ossia i cui elementi possono essere disegnati su una linea in ordine di precedenza e siano tutti confrontabili tra loro.

Siamo soliti usare relazioni che permettono di stabilire un ordine di precedenza tra elementi ma che non soddisfano la proprietà di totalità. Consideriamo per esempio l'inclusione insiemistica $\subseteq$.

1. (Riflessività) Per ogni insieme X, $X \subseteq X$.
2. (Anti-simmetria) Per ogni coppia di insiemi X, Y: Se $X \subseteq Y$ e $Y \subseteq X$ allora $X = Y$.
3. (Transitività) Per ogni tripla di insiemi X, Y, Z: Se $X \subseteq Y$ e $Y \subseteq Z$ allora $X \subseteq Z$.

Non è vero però che presi due insiemi X e Y arbitrari, debba sempre valere $X \subseteq Y$ oppure $Y \subseteq X$.

Esempio 6. $A = \{1, 2, 3\}$, consideriamo

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Si osserva facilmente che né $\{a\} \subseteq \{b\}$ né $\{b\} \subseteq \{a\}$. In questo caso diciamo che $\{a\}$ e $\{b\}$ sono *incomparabili* relativamente alla relazione di inclusione. Analogamente, $\{a, b\}$ e $\{b, c\}$ sono incomparabili. (Esercizio: trovare tutte le coppie di incomparabili). L'ordine $\subseteq$ su $\mathcal{P}(A)$ è dunque un ordine parziale non totale.

Esempio 7. Un altro ordine parziale non totale molto naturale è quello indotto dalla relazione di divisibilità. Consdieriamo $A = \{1, 2, 3, \ldots, 10\}$ e $R \subseteq A \times A$ definita come segue: aRb se e soltanto se b è divisibile per a con resto 0 (divisione perfetta). Per esempio $(1, 2), (1, 3), \ldots$ sono in R; anche $(2, 6), (3, 6), (6, 6)$ sono in R. Si vede facilmente che R è una relazione di ordine paziale:

1. Riflessività: per ogni $a \in A$ vale aRa: ovviamente a divide a senza resto.
2. Anti-simmetria: per ogni $a, b \in A$ vale: Se aRb e bRa allora $a = b$. Infatti aRb significa che $b = a \cdot k$; bRa significa che $a = b \cdot h$, dunque $a = a \cdot k \cdot h$ e dunque $h = k$ e dunque $a = b$.
3. Transitività: Siano $a, b, c \in A$ tali che aRb e bRc. Dunque $b = a \cdot k$ e $c = b \cdot h$. Dunque $c = a \cdot k \cdot h$ e vale aRc.

Si vede anche facilmente che l'ordine non è totale: infatti né 3 divide 5 senza resto né 5 divide 3 senza resto.

Si possono rappresentare gli ordinii parziali finiti con diagrammi di Hasse. L'idea è semplicemente di non indicare le frecce riflessive e quelle che seguono per transitività e di indicare l'orientamento della relazione usando la direzione dal basso verso l'alto. Alcuni esempi:

Diagramma dei sottinsiemi di $\{a, b, c\}$ ordinati per inclusione.

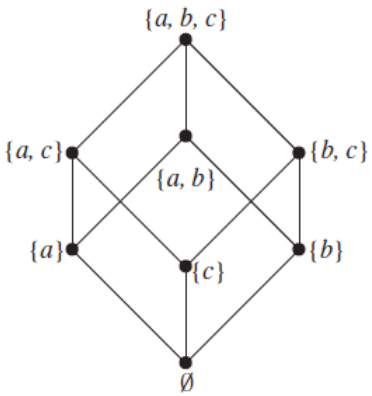
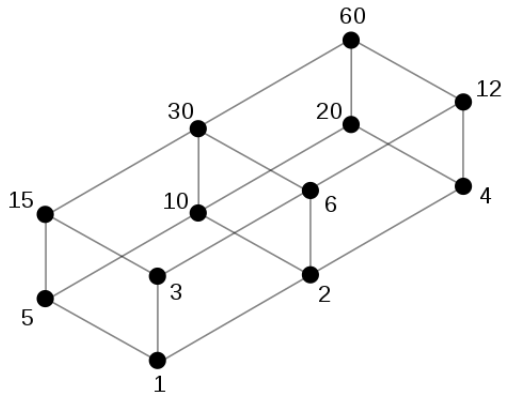


Diagramma dei divisori di 60:



Esempio 8. Abbiamo considerato l'ordine da dizionario su parole italiane, osservando che si tratta di un ordine totale (ammettendo che ogni parola preceda sé stessa). L'ordine delle parole nel dizionario si basa ovviamente sull'ordine alfabetico delle lettere.

Come osservato l'esempio si può generalizzare a un generico alfabeto $A = a_1, \ldots, a_n$ di "lettere" o "simboli" e all'insieme delle stringhe finite su A. Assumendo un ordine totale $<_A$ di precedenza sulle lettere di A – poniamo $a_1 < a_2 < \cdots < a_n$, possiamo definire l'ordine di dizionario – detto ordine lessicografico – come segue: una stringa σ precede una stringa τ se e solo se, conrontandole lettera per lettera da sinistra a destra, nel primo punto in cui differiscono la lettera in σ precede la corrispondente lettera in τ, oppure se il confronto termina perché tutte le lettere di σ si trovano in τ nella stessa posizione ma τ contiene anche altre lettere.

Più formalmente, definiamo l'ordine $\leq_{lex}$ sulle stringhe finite di A come segue. Sia $\sigma = s_1 s_2 \ldots s_n$ e $\tau = t_1 t_2 \ldots t_m$. $\sigma \leq_{lex} tau$ se e solo se o esiste un i tale che per ogni $x < i$ $s_x = t_x$, ma $s_i < t_i$, oppure per ogni $1 \leq x \leq n$, $s_x = t_x$.

Si verifica facilmente che si tratta di un ordine totale.

Esempio 9. Un esempio particolare di precedenza nell'ordine lessicografico è quello di sottostringa iniziale, per esempio AMO e AMORE o ASSO e ASSONE. Abbiamo osservato che si tratta di un ordine parziale.

Rilassando le condizioni si può definire la relazione di sottostringa, che cattura l'idea che tutte le lettere di una parola si trovino, nello stesso ordine, in un'altra parola, possibilmente in posizioni non contigue; per esempio come ASSO e ASSISTO, oppure CENA e CREATININA.

Abbiamo dato la seguente definizione, per stringhe finite σ e τ su un qualunque insieme A: $\sigma \preceq \tau$ se e solo se $\sigma = s_1 s_2 \ldots s_n$, $\tau = t_1 t_2 \ldots t_m$ ed esistono indici $1 \leq i_1 < i_2 < \cdots < i_n \leq m$ tali che $s_1 = t_{i_1}, s_2 = t_{i_2}$, $\ldots$, $s_n = t_{i_n}$.

Abbiamo osservato che si tratta di un ordine parziale. L'antisimmetria si verifica così: siano σ e τ tali che $\sigma \preceq \tau$ e $\tau \preceq \sigma$. Si osserva che questi due fatti implicano che σ e τ hanno stessa lunghezza (ossia $n = m$). Ma allora, dato che $\sigma \preceq \tau$, le due stringhe devono coincidere: la scelta degli n indici in τ non può che essere $1, 2, \ldots, n$, ossia tutte le posizioni in τ.

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.

Esempio 10. Abbiamo considerato il caso dell'ordine parziale $\subseteq$ sull'insieme potenza di $A = \{1, 2, 3\}$. Come osservato, il seguente ordine è una estensione totale di questo ordine parziale:

$$\emptyset < \{1\} < \{2\} < \{3\} < \{1, 2\} < \{1, 3\} < \{2, 3\} < \{1, 2, 3\}.$$

Ma anche la scelta seguente è corretta:

$$\emptyset < \{2\} < \{1\} < \{3\} < \{2,3\} < \{1,3\} < \{1,2\} < \{1,2,3\}.$$

Come procedere nel caso generale?

Esempio 11. Abbiamo osservato che ogni successione di 2 naturali distinti contiene (o meglio coincide con) una sottosuccessione lunga 2 decrescente o una sottosuccessione lunga 2 decrescente.

Abbiamo osservato che non è vero che ogni successione di 3 naturali distinti contiene o una sottosuccessione crescente lunga 3 o una sottosuccessione decrescente lunga 3, e analogamente questo non è vero di successioni di lunghezza 4. Per esempio $(22, 4, 12)$ non ha sottosuccessioni decrescenti o crescenti di lunghezza 3, e così non ne ha $(40, 4, 83, 8)$.

Abbiamo formulato la seguente ipotesi: Ogni successione di naturali distinti di lunghezza 5 o contiene una sottosuccessione crescente di lunghezza 3 o una sottosuccessione decrescente di lunghezza 3.