



UNIVERSITÀ DI PISA

Dipartimento di Informatica
Corso di Laurea Triennale in Informatica

Corso 1° anno - 9 CFU

Fondamenti di Informatica

Professori:

Prof. Alessio Conte
Prof. Roberto Grossi

Autore:

Matteo Giuntori

Anno Accademico 2020/2021

Contents

1	Insiemi	2
1.1	Notazione	2
1.2	Specificare un insieme	2
1.3	Proprietà degli insiemi	3
1.3.1	Confrontare due insiemi	3
1.3.2	Inclusione fra insiemi	3
1.3.3	Proprietà di uguaglianza ed inclusione	3
1.4	Operazioni su insiemi	4
1.5	Tavola delle leggi	4
1.6	Algebra di Bool	5
1.7	Dimostrazioni	5
1.7.1	Diagramma di Eulero-Venn	5
1.7.2	Argomentazioni sostitutive	6
1.7.3	Argomentazione discorsiva	6
1.8	Prodotto Cartesiano	7
1.9	Insiemi di insiemi	7
2	Relazioni	8
2.1	Identità	8
2.2	Composizione	8
2.3	Relazione opposta	9
2.4	Leggi	9
2.4.1	Dimostrazione proprietà associativa	10
2.5	Proprietà fondamentali	11
2.5.1	Teorema di caratterizzazione	12
2.5.2	Proprietà di chiusura per composizione	12
2.6	Funzione	12
2.6.1	Composizione fra funzioni	13
2.6.2	Proprietà di chiusura per funzioni	13
2.6.3	Caratterizzazione in biezione	13
2.6.4	Insiemi di biezione	14
2.6.5	Proprietà insiemi di biezione	15
2.7	N-upla	15
3	Induzione	16
3.1	Schema generale induttivo	16
3.2	Definizione induttiva dell'insieme \mathbb{N}	16
3.3	Definizione induttiva di funzioni	17
3.4	Dimostrazione induttiva di proprietà	17
3.5	Principio di Induzione forte sui naturali	19
4	Relazioni su un insieme	20
4.1	Proprietà di relazione su un insieme	20
4.1.1	Riflessiva	20
4.1.2	Simmetrica	21
4.1.3	Transitiva	21
4.1.4	Anti-simmetrica	22
4.2	Teorema di caratterizzazione	23
4.3	Chiusure	23
4.3.1	Chiusura riflessiva	23
4.3.2	Chiusura simmetrica	24
4.3.3	Chiusura transitiva	24
4.4	Stella di Kleene	25
4.4.1	Applicazione al While	25
4.4.2	Leggi stella di Kleene	26

4.5	Relazioni di equivalenza	27
4.5.1	Classe di equivalenza	27
4.5.2	Teorema di biiezione	27
4.6	Relazioni di ordinamento	27
4.6.1	Ordinamento parziale	27
4.6.2	Ordinamento	28
4.6.3	Ordinamento lessiografico	28
5	Grafi	29
5.1	Grafo orientato	29
5.1.1	Notazione sui grafi orientati	29
5.1.2	Grafi orientati come relazioni e proprietà TUSI	29
5.1.3	Hand-shaking lemma	30
5.2	Rappresentazione grafi	30
5.2.1	Matrici di adiacenza	31
5.2.2	Liste di adiacenza	31
5.3	Grafi orientati etichettati e pesati	31
5.4	Cammini	32
5.4.1	Walk, trail e path	32
5.4.2	Enunciati sui cammini	32
5.4.3	Walk chiusi, circuiti, cicli	34
5.5	Connettività	35
5.5.1	Componenti connesse e partizioni	35
5.5.2	Proprietà connettività	36
5.6	Grafo orientato aciclico (DAGs)	36
5.6.1	Ordinamento topologico	37
5.7	Grafo non orientato	37
5.7.1	Hand-shaking lemma	38
5.7.2	Rappresentazione grafi non orientati	38
5.7.3	Cammini nei grafi non orientati	38
5.7.4	Cicli e connettività nei grafi non orientati	39
5.8	Cammini Euleriani	39
5.9	Cicli e path Hamiltoniani	40
5.9.1	Il problema del commesso viaggiatore	40
5.10	Distanze	40
5.10.1	Diametro, altezza, profondità	42
5.11	Alberi	43
5.11.1	Albero radicato	44
5.12	Isomorfismo	45
5.13	Grafi notevoli	45
6	Calcolo combinatorio	46
6.1	Cardinalità insiemi	46
6.1.1	Cardinalità di operazioni su insiemi	47
6.1.2	Principio di inclusione-esclusione	47
6.1.3	Cardinalità del prodotto cartesiano	48
6.2	Relazioni e cardinalità	50
6.2.1	Pigeonhole Principle	50
6.2.2	Regola di biiezione	50
6.3	Permutazioni	51
6.3.1	Cardinalità delle biiezioni tra due insiemi	51
6.3.2	Anagrammi e permutazioni con ripetizioni	51
6.4	Disposizioni	52
6.5	Combinazioni	52
6.6	Contare sui grafi	53
6.6.1	Grafi non orientati	53
6.6.2	Grafi orientati	53

Fondamenti d'informatica

Realizzato da: Giuntoni Matteo

A.A 2021-2022

1 Insiemi

Gli insiemi sono definibili come delle correlazioni di elementi e saranno alla base del corso di FDI. ¹

Cardinalità: si rappresenta con n o $|A|$ ed è uno dei parametri di un insieme ed è il numero di elementi nell'insieme.

Gli insiemi possono inoltre essere finiti o infiniti.

Finiti: quando hanno un numero finito di elementi.

Infiniti: quando invece il numero di elementi è infinito.

Esempio 1.1. Esempi insiemi finiti ed infiniti:

- Insieme finito: $A = \{a_1, a_2, a_3, \dots, a_n\} \mid |A| = n$. ²
- Insieme finito: $GS = \{lun, mar, mer, \dots, dom\} \mid |GS| = 7$.
- Insieme infinito: $A = \{\dots, a_i - 1, a_i, a_i + 1, \dots\} \mid |A| = \infty$.

1.1 Notazione

Elementi: Lettere piccole dell'alfabeto. Ess: a, b, c - a_1, a_2, a_3

Insiemi: Lettere maiuscole dell'alfabeto. Ess: A, B, C

Appartiene: $a \in A$ **Non Appartiene:** $a \notin A$ **Tale che:** \mid

Esempio 1.2. Alcuni insiemi infiniti ricorrenti:

\mathbb{N} = num. naturali \mathbb{Z} = num. interi \mathbb{Q} = num. razionali \mathbb{R} = num. reali

1.2 Specificare un insieme

Un insieme può essere scritto sotto due forme, quella estensionale e quella intenzionale.

- **Estensionale** o per enumerazione: si va ad elencare esplicitamente tutti gli oggetti.

Esempio 1.3. Esempi estensionale:

$ore = \{1, 2, 3, \dots, 24\}$ - $vocali = \{a, e, i, o, u\}$

$n = \{0, 1, 2, \dots, n-1\}$ - $\emptyset = \{\}$ (insieme vuoto)

- **Intenzionale** o per proprietà: si va ad elencare implicitamente tutti gli oggetti attraverso una regola che li caratterizza.

Esempio 1.4. Esempi intenzionale:

$ore_1 = \{n \in \mathbb{N} \mid n \geq 1 \text{ and } n \leq 24\}$

$N_d = \{n \in \mathbb{N} \mid n \text{ non è divisibile per } 2\}$

$N_p = \{n \in \mathbb{N} \mid n \text{ è divisibile per } 2\}$

$\mathbb{Q} = \{n/m \mid n \in \mathbb{Z}, m \in \mathbb{N}, \text{ ma } m \neq 0\}$

¹Ricorda che all'interno di un insieme gli elementi possono essere ripetuti, in tal caso per le varie operazioni da fare questi elementi ripetuti andranno considerati come unici

²I tre puntini '...' si utilizzano quando non si è in grado di scrivere tutti gli elementi

1.3 Proprietà degli insiemi

1.3.1 Confrontare due insiemi

$A = B$ se contengono esattamente gli stessi elementi.

$A \neq B$ almeno un elemento di A non occorre in B oppure almeno un elemento di B non occorre in A .

Domanda: Con $A = \{a, e, b, c, o, u\}$ e $B = \{a, b, e, b, c, o, o, u\}$, $A = B$?

Se partiamo dalla definizione di insiemi uguali, cioè che $A = B$ quando A contiene gli stessi elementi di B e viceversa possiamo concludere che SI in questa casistica A e B sono uguali.

Da qui possiamo definire una **proprietà del confronto**: $A = B$ equivale a dire che ogni elemento di $a \in A$ e anche $a \in B$ e ogni elemento $b \in B$ è anche $b \in A$.

Inoltre, continuando su questo ragionamento possiamo anche vedere come la cardinalità di due insiemi uguali non necessariamente è uguale.

1.3.2 Inclusione fra insiemi

Contenuto uguale: $A \subseteq B$ Figura [1]

(Ogni elemento di A è anche elemento di B e possono essere uguali, ma non necessariamente)

$$A \subseteq U \quad A \subseteq B \quad B \subseteq U^3$$

Inclusione impropria e stretta: $A \subset B$

(da usare solo quando vuoi specificare che $A \neq B$)

Proprietà: Per ogni insieme di A si ha che:

$$\emptyset \subseteq A \quad A \subseteq U$$

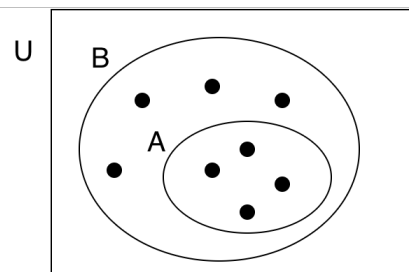


Figure 1: Contenuto uguale

Insiemi disgiunti: A e B si dicono insiemi disgiunti quando non hanno elementi in comune:

$$\{\text{non esiste } x \in U \mid x \in A \text{ and } x \in B\}$$

1.3.3 Proprietà di uguaglianza ed inclusione

Per tutti gli insiemi A, B, C valgono le proprietà scritte in tabella 1.

Riflessiva	$A = A$	$A \subseteq A$
Transitiva	Se $A = B$ e $B = C$ allora $A = C$	Se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$
Simmetrica	Se $A = B$ allora $B = A$	<i>Niente</i>
Antisimmetrica	<i>Niente</i>	Se $A \subseteq B$ e $B \subseteq A$ allora $A = B$

Table 1: Proprietà Uguaglianza ed Inclusione

³con il simbolo "U", chiamato universo, si indicano tutti i possibili elementi che possiamo trovare in un insieme.

1.4 Operazioni su insiemi

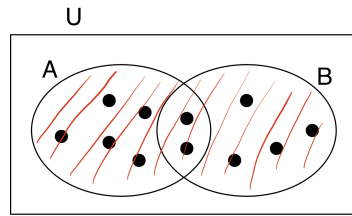
Cardinalità: (solo per insiemi finiti) si indica con $|A|$

Esempio 1.5. Esempi cardinalità:

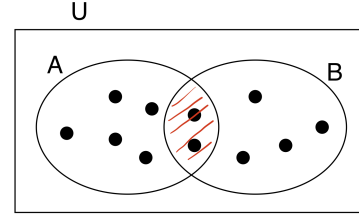
$$|\bar{A}| = |U| - |A| \quad |A \cup B| = |A| + |B| - |A \cap B| \quad |A \setminus B| = |A| - |A \cap B|$$

Unione: $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$

Intersezione: $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$



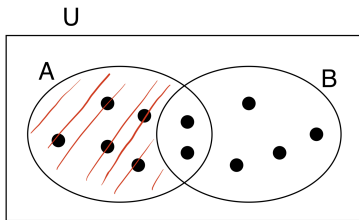
(a) Unione



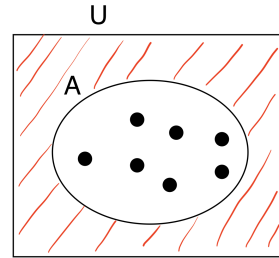
(b) Intersezione

Differenza: $A \setminus B = \{x \in U \mid x \in A \text{ and } x \notin B\}$

Complemento: $\bar{A} = \{x \in U \mid x \notin A\}$



(a) Differenza



(b) Complemento

1.5 Tavola delle leggi

Per tutti gli insiemi A, B, C (dell'universo U) valgono le uguaglianze nella tabella 2

Associazione	$A \cup (B \cap C) = (A \cup B) \cap C$	$A \cap (B \cup C) = (A \cap B) \cup C$
Unità	$A \cup \emptyset = A$	$A \cap U = A$
Commutativa	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Indipendenza	$A \cup A = A$	$A \cap A = A$
Assorbimento	$A \cup U = U$	$A \cap \emptyset = \emptyset$
Distributiva	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Complemento	$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$
De Morgan	$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$
Convoluzione	$\overline{(\bar{A})} = A$	
Assorbimento con \cap e \cup	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$

Table 2: Tavola delle leggi

1.6 Algebra di Bool

L'algebra di bool sta alla base dell'informatica e si compone di solo 2 elementi che possono essere rappresentati in tanti modi: V - F, Vero - Falso, True - False, 1 - 0, \emptyset - U

Su questi elementi possono essere applicate una serie di operazioni che sono:

And, $\&$, \wedge **Or**, $\|$, \vee **Not**, \sim , \neg **Implicazione**:⁴ $A \implies B$, se A allora B

Conseguenza: $A \Leftarrow B$, A se B

Doppia implicazione: $A \iff B$, A se e solo se B

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \implies B$	$A \Leftarrow B$	$A \iff B$
\emptyset	\emptyset	\emptyset	\emptyset	U	U	U	U
\emptyset	U	\emptyset	U	U	U	\emptyset	\emptyset
U	\emptyset	\emptyset	U	\emptyset	\emptyset	U	\emptyset
U	U	U	U	\emptyset	U	U	U

Table 3: Operazioni con algebra booleana

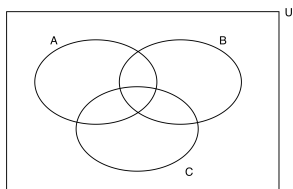
Note 1.6.1. Se nella tabella andiamo a sostituire lo \emptyset con 0 e U con 1 o con qualsiasi altro valore corrispondente nell'algebra di boole il risultato invariato.

1.7 Dimostrazioni

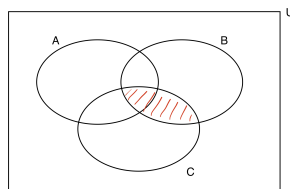
Una **legge** è **valida** se vale per tutte le scelte dell'insieme che prendiamo in considerazione. Una **dimostrazione** indica la validità di una legge. Un **controesempio** mostra che la legge può non essere valida. Ci sono 3 tecniche di dimostrazione: **Diagramma di eulero-venn**, **Argomentazione discorsiva** e **Regole di sostituzione**

1.7.1 Diagramma di Eulero-Venn

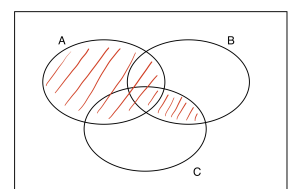
Esempio 1.6. Dimostriamo la legge distributiva mediante i diagrammi di eulero-venn. Legge: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.



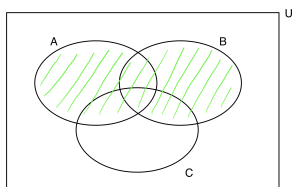
(a) Insiemi di partenza



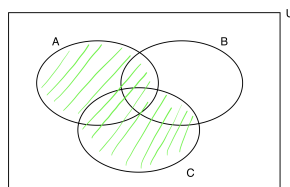
(b) Step 1 - $B \cap C$



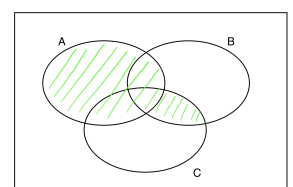
(c) Step 2 - $A \cup (B \cap C)$



(a) Step 3 - $A \cup B$



(b) Step 4 - $A \cup C$



(c) Step 5 - $(A \cup B) \cap (A \cup C)$

Possiamo vedere come lo step 2 (4b), che rappresenta ciò che dovrebbe essere $A \cup (B \cap C)$ con i diagrammi di eulero-venn, e lo step 5 (5b), cioè $(A \cup B) \cap (A \cup C)$, siano uguali e quindi possiamo dire che la proprietà è dimostrata.

⁴La parte a sinistra della freccia si chiama premessa, la parte a destra invece conseguenza

1.7.2 Argomentazioni sostitutive

Questo tipo di dimostrazione si basa sull'utilizzare le leggi sopra riportate per dimostrare un'affermazione, andando a scomporre tale affermazioni in modo che richiami ad un legge fondamentale.

Esempio 1.7. $(A \cup B) \cup C = A \cup (C \cup B)$

1. Commutativa: $(A \cup B) \cup C = A \cup (B \cup C)$

L'ipotesi è vera per la proprietà associativa.

Esempio 1.8. $A \cup (\bar{A} \cap B)$

1. Usando la **Distributiva** possiamo dividere la prima parte: $(A \cup \bar{A}) \cap (A \cup B) = (A \cup B)$
2. Usando la proprietà del **Complemento** $A \cup \bar{A}$ diventa U quindi perché un insieme unito con la sua negazione torna sempre l'universo: $U \cap (A \cup B) = (A \cup B)$
3. Per la proprietà dell'**Unità** un insieme A unito con l'universo U è uguale a l'insieme stesso quindi: $A \cup B = A \cup B$

L'ipotesi è così verificata.

1.7.3 Argomentazione discorsiva

Esempio con dimostrazione della proprietà distributiva: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Teniamo conto che: $X = Y \iff (X \subseteq Y) \wedge (Y \subseteq X)$

Andiamo a questo punto a sostituire X con la prima parte della proprietà distributiva, $A \cup (B \cap C)$ e Y con la seconda $(A \cup B) \cap (A \cup C)$. Applicando la considerazione scritta sopra otteniamo due condizione che devono entrambi essere vere per far sì che la condizione di uguaglianza iniziale $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ sia vera e quindi la proprietà sia verificata. Queste due condizioni sono:

- $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ - Dimostrazione 1°
- $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ - Dimostrazione 2°

Dimostrazione 1°: $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Ricordiamo che un insieme $W \subseteq Z$ per ogni $x \in W$ e $z \in Z$.

Sostituendo la W con la prima parte, $A \cup (B \cap C)$, e la Z con la seconda, $(A \cup B) \cap (A \cup C)$ possiamo scrivere che $y \in A \cup (B \cap C)$. Per la definizione di unione possiamo distinguere in 2 casi.

$$(1a) \ y \in A \quad (1b) \ y \in (B \cap C)$$

Da qui il nostro obiettivo è far valere per entrambi i casi che $y \in (A \cup B) \cap (A \cup C)$.

- **Caso 1a:** $y \in A$

1. Per questo caso possiamo vedere come, per la definizione di unione, aggiungendo qualsiasi cosa all'insieme A l'appartenenza di y rimarrà invariata. Quindi $y \in A \cup B$, $y \in A \cup C$.
2. Da qui per la definizione di intersezione⁵ $y \in (A \cup B) \cap (A \cup C)$. Caso dimostrato. ■

- **Caso 1b:** $y \in (B \cap C)$

1. Siccome $x \in B \cap C$, per definizione di intersezione si ha che $x \in B$ e che $x \in C$.
2. Dato che $x \in B$, a sua volta ha che $x \in A \cup B$.
3. Analogamente, dato che $x \in C$, per definizione di unione si ha che $x \in A \cup C$.
4. Ma allora, visto che x appartiene a entrambi questi insiemi deve appartenere anche alla loro intersezione, ovvero $y \in (A \cup B) \cap (A \cup C)$. Caso dimostrato. ■

⁵ $(y \in W \cap Z, \iff y \in W \text{ e } y \in Z)$

Dimostrazione 2°: $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

Come per la dimostrazione 1° andiamo a prendere qualsiasi elemento $y \in (A \cup B) \cap (A \cup C)$.

Da qui per la definizione di intersezione $y \in (A \cup B)$ e $y \in (A \cup C)$ che ci permette di conseguenza di distinguere 4 casi:

- (1) $y \in A$ e $y \in A$ (2) $y \in A$ e $y \in B$ (3) $y \in C$ e $y \in A$ (4) $y \in B$ e $y \in C$

Però possiamo racchiudere le prime 3 con $y \in A$ e l'ultima come $y \notin A$. Quindi abbiamo due possibilità disgiunti fra loro.

- (2a) $y \in A$ (2b) $y \notin A$

In entrambi i casi bisogna arrivare a dimostrare che $y \in A \cup (B \cap C)$.

• **Caso 2a:** $y \in A$

1. Essendo che $y \in A$ allora per definizione di unione $y \in A \cup (B \cap C)$. Caso dimostrato. ■

• **Caso 2b:** $y \notin A$

1. Dato che $y \in A \cup B$ ma $y \notin A$, allora necessariamente $y \in B$.
2. Analogamente, data che $y \in A \cup C$ ma $y \notin A$, allora $y \in C$.
3. Visto che y appartiene sia a B che a C deve per forza appartenere alla loro intersezione, quindi $y \in (B \cap C)$.
4. A questo punto per definizione di unione $y \in A \cup (B \cap C)$. Caso dimostrato. ■

Non avendo nessun' altro caso da dimostrare abbiamo concluso la dimostrazione. ■

1.8 Prodotto Cartesiano

Prendendo 2 insiemi A, B il loro prodotto cartesiano si definisce come:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Esempio 1.9. Esempio prodotto cartesiano:

$$A = \{501234, 501227, 678980\} \text{ N. matricola} \quad B = \{18, 19, 20, \dots, 30L\} \text{ Voti}$$

$$A \times B = \{(501234, 18), (501234, 19), \dots, (678980, 30L)\}$$

I sotto insiemi che si vanno a creare con il prodotto cartesiano si indicano con le parentesi tonde "(...)" e possono essere di due tipi:

- **Coppia Ordinata:** si tiene conto dell'ordinamento degli elementi. Ess: $(a, b) \neq (b, a)$.
- **Coppia Non Ordinata:** non si tiene conto dell'ordinamento degli elementi. Ess: $(a, b) = (b, a)$.

1.9 Insiemi di insiemi

Definizione 1.1 (Insieme). *Un insieme di insieme è quando uno o più elementi di un insieme è a sua volta un insieme.*

Esempio 1.10. Esempi insiemi di insiemi:

- $X = \{a, \{a, b, c\}, \{a, \{b\}\}, \{\{c\}, d\}\}$
- $N = \{\{\}, \{\{\}\}, \{\{\{\}\}\}, \{\{\{\{\}\}\}\}, \dots\} = \mathbb{N}$

Definizione 1.2 (Insieme delle parti). *L'insieme della parti, per esempio di A , si indica come $P(A)$ e si definisce come tutti i possibili sottoinsiemi di A . $P(A) = \{x \subseteq A\}$. La **cardinalità** nell'insieme delle parti si calcola come: $P(A) = 2^{|A|}$*

Esempio 1.11. Con $A = \{a, b, c\}$, $\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

2 Relazioni

Definizione 2.1 (Relazione). Prendiamo in considerazione un prodotto cartesiano con due insiemi A, B che sia $A \times B = \{(a, b) \mid a \in A, b \in B\} = U$ (Universo).

Una relazione è $R \subseteq U$ dove, come scritto sopra, $U = A \times B$. In una relazione A è detto **insieme di partenza** e B è detto **insieme di arrivo**.

In sintesi possiamo definire una relazione come un sottoinsieme del prodotto cartesiano fra due insiemi. L'insieme $rel(A, B)$ è l'insieme di tutte le possibili relazioni fra A e B .

Esempio 2.1. Esempio relazione.

Prendiamo due insiemi e facciamo il prodotto cartesiano.

$S = \{\text{luca, mario, angela, gino, maria}\}$. Insieme degli studenti.

$C = \{\text{PA, LAB, FI, AN}\}$. Insieme dei corsi.

Il prodotto cartesiano fra S e C è uguale a tutte le possibile coppie ordinate che si possono formare fra i due insiemi, quindi: $S \times C = \{(\text{luca, PA}), (\text{luca, LAB}), \dots, (\text{marica, AN})\}$.

In questo caso possiamo creare una relazione del prodotto cartesiano andando appunto a prendere un sottoinsieme di $A \times B$ andando a stabilire una regola o condizione per scegliere quali coppie ordinate vogliamo nella nostra relazione, esempio:

$R \subseteq A \times B$ è una relazione che specifica quali esami sono stati sostenuti dai vari studenti.

2.1 Identità

L'identità è un altro tipo di operazione che è possibile fare sulle relazioni, oltre a quelle insiemistiche.

Definizione 2.2 (Identità). Preso un insieme A , l'identità su A è una relazione con se stessa, e si scrive $Id_A \subseteq A \times A$, quindi si può vedere come nell'identità di un insieme ogni elemento è identico a se stesso. Inoltre l'identità di un insieme si definisce come:

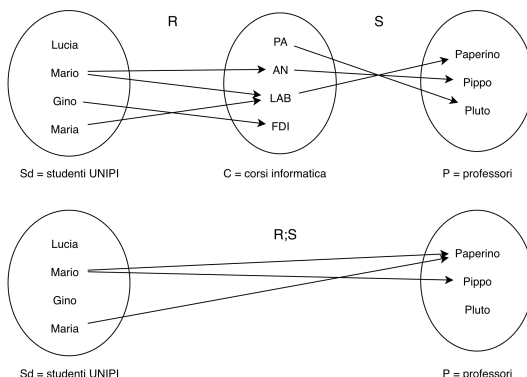
$$Id_A = \{(a, a) \mid a \in A\} \quad (1)$$

2.2 Composizione

Definizione 2.3 (Composizione). La composizione, date due relazioni $R \subseteq A \times B$ e $S \subseteq B \times C$ si scrive $R;S$ e sarebbe una relazione che si sviluppa fra gli elementi degli insiemi diversi di R ed S , in questo caso A e C , che però hanno uno stesso collegamento ad un elemento dell'insieme B . Matematicamente si definisce come:

$$R;S = \{(a, c) \in A \times C \mid \exists b \in B . (a, b) \in R \wedge (b, c) \in S\} \quad (2)$$

NOTA: l'insieme di arrivo di R deve essere uguale all'insieme di partenza di S per effettuare l'operazione di composizione.



Esempio 2.2. Nell'esempio in figura [6] prendiamo in considerazione i seguenti insiemi:

$S_d = \{\text{lucia, mario, gino, maria}\}$

$C = \{\text{PA, LAB, FI, AN}\}$

$P = \{\text{paperino, pippi, pluto}\}$

Effettuiamo un'operazione di composizione. Come possiamo vedere il risultato è un insieme che unisce gli elementi di S_d e P che avevano una relazione con un elemento di C in comune.

Figure 6: Esempio composizione

2.3 Relazione opposta

Definizione 2.4 (Relazione opposta). *Dato un insieme A e B ed una relazione $R \subseteq A \times B$, una relazione opposta è inversione dell'associazione degli elementi degli insiemi A e B da (a,b) a (b,a) e si definisce formalmente come: $R^{op} = \{(b,a) \in B \times A \mid (a,b) \in R\}$*

Esempio 2.3. $A = \{\text{pagine web}\}$ $B = \{\text{parole del vocabolario}\}$ $R \subseteq A \times B$

Si associa ciascuna pagina web con le parole in essa contenute:

- $(a,b) \in R$ dice che nella pagina web "a" è contenuta la parola "b".
- $R^{op} ((b,a) \in R)$ dice per ogni parola "b" quali sono le pagine web che le contengono.

2.4 Leggi

Come per gli insiemi, anche per le relazioni esistono delle utili leggi che regolano il comportamento delle varie operazioni. Le relazioni, essendo di base degli insiemi, valgono le stesse leggi scritte nella sezione degli insiemi, tabella 2.

Per tutti gli insiemi A, B, C, D e per tutte le relazioni $R \subseteq A \times B$, $S \subseteq B \times C$, $T \subseteq C \times D$, valgono le leggi scritte nelle tabelle 4, 5, 6.

Associatività	$(R;S);T = R;(S;T)$
Unità	$Id_A;R = R;Id_B = R$
Assorbimento	$\emptyset;S = S;\emptyset = \emptyset$

Table 4: Leggi composizione

Convoluzione	$(R^{op})^{op} = R$
Opposto-identità	$(Id)^{op} = Id$
Opposto-complemento	$(A \times B)^{op} = (B \times A)$
Opposto-vuoto	$(\emptyset)^{op} = \emptyset$

Table 5: Leggi relazioni opposte

Distributività composizione	$R;(S \cup T) = (R;S) \cup (R;T)$	$(S \cup T); R = (S;R) \cup (T;R)$
Distributività opposto	$(R \cup S)^{op} = S^{op} \cup R^{op}$	$(R \cap S)^{op} = S^{op} \cap R^{op}$
Distributività opposto su negazione	$(\overline{R})^{op} = \overline{(R^{op})}$	
Distributività opposto su composizione	$(R;S)^{op} = S^{op};R^{op}$	

Table 6: Leggi distributività

Spiegazione Associatività:

$R;S \subseteq A \times C$, facendo la composizione con T la prima parte dell'uguaglianza $(R;S);T \subseteq A \times D$. A sua volta, analizzando la seconda parte dell'uguaglianza, $S;T \subseteq B \times D$ che poi se andiamo a comporre con R risulta che $R;(S;T) \subseteq A \times D$. Possiamo così vedere che l'uguaglianza è verificata. Per la dimostrazione discorsiva completa vedere in seguito.

Spiegazione Unità:

Essendo che $Id_A = A \times A$ e $Id_B = B \times B$ vediamo che la prima parte dell'uguaglianza $Id_A;R = A \times B$ e la seconda è $R;Id_B = A \times B$, quindi la prima uguaglianza è verificata. La seconda uguaglianza si verifica in automatico visto che $A \times B$ è uguale a R .

2.4.1 Dimostrazione proprietà associativa

Dimostrazione 2.1. Facciamo una dimostrazione discorsiva della proprietà associativa in tabella 4.

Proprietà associativa: $(R;S);T = R;(S;T)$ Con: $R \subseteq A \times B$, $S \subseteq B \times C$, $T \subseteq C \times D$.

Innanzitutto ricordiamo la proprietà per cui dati 2 insiemi X, Y $X = Y \iff X \subseteq Y \wedge Y \subseteq X$.

Utilizziamo la proprietà sopra scritto andando a sostituire alla X " $(R;S);T$ " e alla Y " $R;(S;T)$ ", troviamo così due condizioni che, per l'operatore logico \wedge , devono essere vere entrambe per far valere l'uguaglianza:

- $(R;S);T \subseteq R;(S;T)$ - Dimostrazione 1°.
- $R;(S;T) \subseteq (R;S);T$ - Dimostrazione 2°.

Dimostrazione 1°: $(R;S);T \subseteq R;(S;T)$

Come prima cosa ricordiamo che un insieme $W \subseteq Z \iff \forall w \in W \exists z \in Z$.

Sostituendo " $(R;S);T$ " a W e " $R;(S;T)$ " a Z troviamo che, per fare in modo che la condizione che un insieme sia sottoinsieme di un altro $\forall (a, d) \in (R;S);T \wedge (a, d) \in R;(S;T)$.⁶

Noi dobbiamo dimostrare che $\forall (a, d) \in (R;S);T$ sia vera:

Prendiamo come prima cosa una generica coppia di valori $(a, d) \in (R;S);T$. Perché esista questa coppia deve esistere per forza un valore " c " che faccia da ponte fra " $(R;S)$ " e " T " (ricordiamo che $R;S \subseteq A \times C$ e $T \subseteq C \times D$). Possiamo scrivere quindi (Colore **nero** nella rappresentazione [7]):

$$(a, d) \in (R;S);T \implies \exists c \in C \bullet (a, c) \in R;S \wedge (c, d) \in T \text{ (Nel disegno freccia NERA)} \quad (3)$$

Ora nella forma scritta sopra [3] abbiamo una parte $(a, c) \in R;S$ che deve essere "scomposta" in maniera specifica per verificare che tutta la composizione di partenza sia vera, infatti deve esistere un valore b che colleghi l'insieme R ed S nell'operazione di composizione $R;S$ (ricordiamolo che $R \subseteq A \times B$ e $S \subseteq B \times C$). Possiamo scrivere quindi (Colore **blu** nella rappresentazione [7]):

$$(a, d) \in (R;S);T \implies \exists b \in B, c \in C \bullet (a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T \text{ (Nel disegno freccia BLU)} \quad (4)$$

Ora per arrivare alla forma che dobbiamo dimostrare, $R;(S;T)$, l'ultima forma [4] è troppo estesa, infatti la parte $(b, c) \in S \wedge (c, d) \in T$ deve essere racchiusa per arrivare alla forma $S;T$. Quindi andiamo a scrivere che (Colore **rosso** nella rappresentazione [7]):

$$(a, d) \in R;(S;T) \implies \exists b \in B \bullet (a, b) \in R \wedge (b, d) \in S;T \text{ (Nel disegno freccia ROSSA)} \quad (5)$$

L'ultima forma raggiunta [5] dimostra che $\forall (a, d) \in R;(S;T)$ è vera e quindi che $(R;S);T \subseteq R;(S;T)$ è verificata. ■

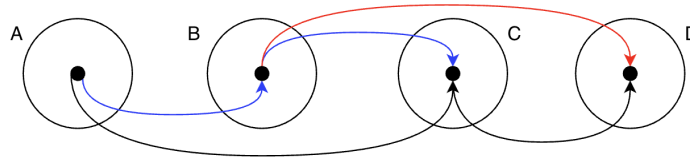


Figure 7: Rappresentazione dimostrazione 1°

⁶Ricordati che $(R;S);T$ ha al suo interno coppie $(a, d) \subseteq A \times D$ per le operazioni di composizione

Dimostrazione 2°: $R;(S;T) \subseteq (R;S);T$

La seconda dimostrazione ha uno svolgimento analogo alla prima. Pure qui andiamo a considerare che: per fare in modo che la prima parte, cioè " $R;(S;T)$ ", sia sottoinsieme della seconda, la seconda deve contenere tutti gli elementi della prima. quindi $\forall (a, d) \in R;(S;T) \wedge (a, d) \in (R;S);T$.

Per fare in modo che ciò scritto sia vero dobbiamo dimostrare che $\forall (a, d) \in (R;S);T$ sia vero:

Come prima cosa dobbiamo capire in che casi i punti appartengono a " $(R;S);T$ ", questo avviene quando esiste un punto " c " che collega " $R;S$ " e " T " ($R;S$ è uguale a $A \times C$ e T è $C \times D$), quindi possiamo scrivere che:

$$(a, d) \in (R;S);T \implies \forall c \in C \bullet (a, c) \in R; S \wedge (c, d) \in T \quad (6)$$

Da questo punto procediamo come nella dimostrazione 1° quindi andiamo a scomporre ulteriormente la forma [6] in $(a, c) \in R; S$ per verificare i casi in cui la composizione esista:

$$(a, d) \in (R;S);T \implies \exists b \in B, c \in C \bullet (a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T \quad (7)$$

L'ultimo passaggio è trasformare la forma [7] in una versione che possa validare $\forall (a, d) \in (R;S);T$, ed essa sarebbe:

$$(a, d) \in R;(S;T) \implies \exists c \in C \bullet (a, c) \in R; S \wedge (c, d) \in T \quad (8)$$

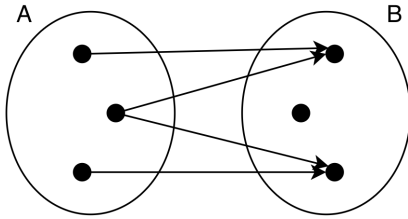
L'ultima forma trovata [8] verifica che $\forall (a, d) \in (R;S);T$ sia vero, di conseguenza pure $R;(S;T) \subseteq (R;S);T$ è verificato. ■

Dato che siamo riusciti a dimostrare entrambe le dimostrazioni la proprietà associativa $((R;S);T = R;(S;T))$ con cui siamo partiti è verificata. ■

2.5 Proprietà fondamentali

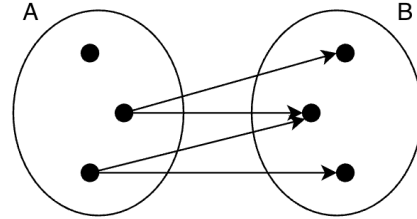
Prendendo in considerazioni due insiemi A e B ed una relazione R, dove $R \subseteq A \times B$, valgono le seguenti proprietà.

Totale: $\forall a \in A \bullet \exists b \in B \bullet (a, b) \in R$



(a) Ogni elem. di A è collegato ad almeno uno di B

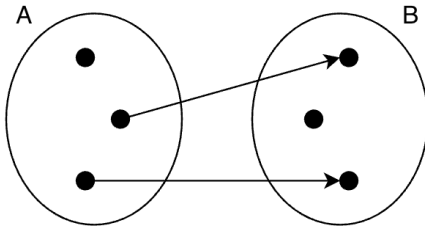
Surgettiva: $\forall b \in B \bullet \exists a \in A \bullet (a, b) \in R$



(b) Ogni elem. di B ha almeno un'entrata da A

Univalente:

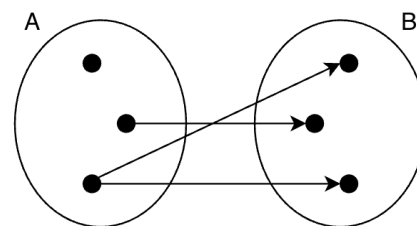
$\forall a \in A \bullet \exists \text{ al più un } b \in B \bullet (a, b) \in R$



(a) Ogni elem. di A deve avere al massimo 1 collegamento con B

Iniettiva:

$\forall b \in B \bullet \exists \text{ al più un } a \in A \bullet (a, b) \in R$



(b) Ogni elem. di B deve avere al massimo un entrante da A

Le proprietà fra di loro sono legate da un rapporto di dualità in particolare totale con surgettiva e univalente con iniettiva, questo vuol dire che:

- $R \subseteq A \times B$ è totale $\iff R^{op} \subseteq B \times A$ è surgettiva.
- $R \subseteq A \times B$ è surgettiva $\iff R^{op} \subseteq B \times A$ è totale.
- $R \subseteq A \times B$ è univalente $\iff R^{op} \subseteq B \times A$ è iniettiva.
- $R \subseteq A \times B$ è iniettiva $\iff R^{op} \subseteq B \times A$ è univalente.

2.5.1 Teorema di caratterizzazione

Prendendo due insiemi A e B ed una relazione R tale che $R \subseteq A \times B$. Possiamo vedere come ogni proprietà fondamentale vale solo se sono soddisfatte delle condizioni che le caratterizzano:

- **R Totale** $\iff Id_A \subseteq R; R^{op}$ - Spiegazione:
La congiunzione fra R che è $A \times B$ e il suo opposto che è $B \times A$ torna un insieme $A \times A$, per questo l'identità di A (Id_A), che sarebbe un insieme $A \times A$, è un sottoinsieme di $R; R^{op}$.
Se R non fosse totale vorrebbe dire che alcuni elementi di $R(A)$ non sono collegati.
- **R Univalente** $\iff R^{op}; R \subseteq Id_B$ - Spiegazione:
La congiunzione fra R^{op} che sarebbe $B \times A$ e R , che è $A \times B$, forma un insieme $B \times B$ che è quindi sottoinsieme di Id_B , che sarebbe $B \times B$.
- **R Surgettiva** $\iff Id_B \subseteq R^{op}; R$ - Spiegazione:
La congiunzione fra R^{op} ed R , che sono rispettivamente $B \times A$ e $A \times B$, torna una relazione $B \times B$, quindi Id_B , che è $B \times B$, è sottoinsieme.
- **R Iniettiva** $\iff R; R^{op} \subseteq Id_A$ - Spiegazione:
La congiunzione fra R ed R^{op} torna $A \times A$, essendo che R è $A \times B$ e l'opposto è $B \times A$, che è sottoinsieme di Id_A che è $A \times A$.

2.5.2 Proprietà di chiusura per composizione

Per tutti gli insiemi A, B, C e per tutte le relazioni, $R \subseteq A \times B$ e $S \subseteq B \times C$ valgono le seguenti proprietà:

1. Se R ed S sono totali allora la loro composizione $R;S$ è totale.
2. Se R ed S sono univalenti allora la loro composizione $R;S$ è univalente.
3. Se R ed S sono surgettive allora la loro composizione $R;S$ è surgettiva.
4. Se R ed S sono iniettive allora la loro composizione $R;S$ è iniettiva.

2.6 Funzione

Una funzione può essere definita utilizzando le proprietà fondamentali delle relazioni.

Definizione 2.5 (Funzione). *Dati due insiemi A, B ed una relazione $R \subseteq A \times B$, tale relazione si definisce funzione quando rispetta la proprietà **totale** e **univalente** quindi tutti gli elementi dell'insieme A hanno uno ed un solo corrispettivo in B .*

Una funzione è inoltre infittiva quando rispetta la proprietà iniettiva e suriettiva quando rispetta quella surgettiva.

Definizione 2.6 (Funzione parziale). *Una funzione si dice parziale se rispetta solamente la proprietà univalente.*

Definizione 2.7 (Biezione). *Dati due insiemi A, B ed una relazione $R \subseteq A \times B$, tale relazione si definisce funzione biettiva quando rispetta tutte e 4 le proprietà.*

Esempio 2.4. Esempio con i booleani:

$\text{bool} = \{\text{True}, \text{False}\}$ $2 = \{0, 1\}$

Questi due insiemi sono biettivi.

Domanda: Se dati due insiemi A, B dove $|A| \neq |B|$ la loro relazione $R \subseteq A \times B$ può essere una biezione?

La risposta è NO visto che avendo cardinalità diverse esisterà sempre un elemento in B che o non ha corrispettivo o ne ha 2.

2.6.1 Composizione fra funzioni

La composizione fra funzioni è una casistica particolare di quella fra relazioni.

Esempio 2.5. Dati due funzioni f e g dove:

$f : A \longrightarrow B$ $g : B \longrightarrow C$ ⁷

La composizione si scrive come $f;g$ e sarebbe $f;g \subseteq A \times C$ ⁸

NOTA: indichiamo con $\text{fun}(A, B) = \{f | f : A \longrightarrow B\}$ l'insieme di tutte le funzioni che vanno da A a B .

2.6.2 Proprietà di chiusura per funzioni

Per tutti gli insiemi A, B, C e per tutte le relazioni, funzioni, $i : A \longrightarrow B$ e $j : B \longrightarrow C$ valgono le seguenti proprietà:

1. Id_A è una biezione, essendo che sarebbe una relazione con se stesso.
2. Se prendiamo $i : A \longrightarrow B$ e $j : B \longrightarrow C$, dove entrambi le funzioni sono biezioni, la loro composizione, $i;j : A \longrightarrow C$ è a sua volta una biezioni.
3. Se prendiamo la funzione $i : A \longrightarrow B$ biettiva, il suo opposto $i^{op} : B \longrightarrow A$ è a sua volta biettiva.

2.6.3 Caratterizzazione in biezione

Definizione 2.8 (Caratterizzazione). *In maniera rigorosa la caratterizzazione, applicata alla biezione, si definisce: $\forall A, B \bullet \forall R \subseteq A \times B, R \text{ è biezione} \iff \text{Id}_A = R; R^{op} \wedge \text{Id}_B = R^{op}; R$.*

Spiegazione: Per definire la proprietà di caratterizzazione per una relazione biettiva bisogna partire da cos'è una relazione biettiva: una relazione è biezione quando è contemporaneamente totale, univalente, surgettiva ed iniettiva.

Da qui capiamo che se una relazione ha tutte e 4 le proprietà a suo volta dovrà rispettare per ciascuna di esse la caratterizzazione associata vista nel paragrafo 2.5.1.

Quindi semplicemente riscriviamo questa quattro proprietà semplificando $\text{Id}_A \subseteq R; R^{op}$ con $R; R^{op} \subseteq \text{Id}_A$ in $\text{Id}_A = R; R^{op}$ e $\text{Id}_B \subseteq R^{op}; R$ con $R^{op}; R \subseteq \text{Id}_B$ con $\text{Id}_B = R^{op}; R$ (possiamo fare questa "semplificazione" perché due insiemi sono uguali quando uno è sottoinsieme dell'altro, come in questo caso).

Esempio 2.6. Come si usa la caratterizzazione:

Dati due insiemi A, B ed una relazione $R \subseteq A \times B$. Se riusciamo a trovare una relazione $S \subseteq B \times A$ tale che venga soddisfatta la definizione sopra scritta per cui $\text{Id}_A = R; S \wedge S; R = \text{Id}_B$ è equivalente a dimostrare che la relazione R è una biezione.

⁷Scrivere una funzione "f" nella forma $f : A \longrightarrow B$ equivale a scrivere $f \subseteq A \times B$

⁸è possibile scrivere la composizione fra funzioni anche come $g \bullet f$ oppure $g(f())$.

2.6.4 Insiemi di biezione

Definizione 2.9 (Insiemi di biezione). *Dati due insiemi A e B , essi sono in biezioni⁹ se esiste una biezione che va da $i: A \rightarrow B$, e si scrive come $A \cong B$ ¹⁰*

Esempio 2.7. Esempi insiemi di biezione:

- Dati gli insiemi $2 = \{0, 1\}$ e $\text{bool} = \{\text{true}, \text{false}\}$ l'insieme di biezione è $2 \cong \text{bool}$
- Dati A e B l'insieme di biezione è $A \times B \cong B \times A$
Altri modi per scriverlo sono: $i: A \times B \rightarrow B \times A - i((a,b)) = (b,a)$ ¹¹
NOTA: $A \times B = B \times A$ sarebbe farlo perché uno crea coppie (a,b) e l'altro coppie (b,a) .
- Dati gli insieme $1 = \{0\}$ ed A l'insieme di biezione è $A \times 1 \cong A$
Altri modi per scriverlo sono: $i: A \times 1 \rightarrow A - i((a,0)) = a$
- $\text{fun}(A \times B, C) \cong \text{fun}(A, (\text{fun}(B, C)))$
Spiegazione esempio: la prima funzione data una coppia (a,b) restituisce un valore c mentre la seconda funzione dando un valore a restituisce una nuova funzione, dove a sua volta se inseriamo un valore b restituisce c . Quindi $f((a,b)) = c$ e $f(a)(b) = c$.

Esempio 2.8. Esempio particolare con dimostrazione

Per tutti gli insiemi A, B, C vale che:

$$(A \times B) \times C \cong A \times (B \times C) \quad (9)$$

Dimostrazione 2.2. Innanzitutto scriviamo questa biezione sotto la seguente forma

$i((a,b),c) = (a,(b,c))$ dove la funzione "i" prende in input una coppia di valori $((a,b),c)$ e restituisce $(a,(b,c))$.

Utilizziamo la proprietà di caratterizzazione scritta nel paragrafo 2.6.3 che dice che:

$$R \iff Id_A = R; R^{op} \wedge Id_B = R^{op}; R.$$

Sfruttiamola applicandola al nostro caso quindi (consideriamo i come una relazione fra due insiemi W e K dove W è $((A \times B) \times C)$ e K è $(A \times (B \times C))$):

$$i \text{ biettiva} \iff Id_W = i; i^{op} \wedge i^{op}; i = Id_K \quad (10)$$

Il nostro obiettivo è quindi trovare i^{op} che soddisfi le due condizioni determinate da \wedge sopra:

- $Id_W = i; i^{op}$ - Dimostrazione 1°
- $Id_K = i^{op}; i$ - Dimostrazione 2°

Dimostrazione 1° - $Id_W = i; i^{op}$ Ricordiamo che l'opposto di "i" è $i^{op}: A \times (B \times C) \rightarrow (A \times B) \times C$ che quindi possiamo vedere come una funzione che prende in ingresso una coppia di valori $(a, (b,c))$ e restituisce $((a,b),c)$.

Ora rappresentiamo la composizione fra i e i^{op} come unione fra funzioni come funzione di una funzione quindi: $i; i^{op} = i^{op}(i(x))$

Ora semplicemente riscriviamo la composizione di funzioni scrivendo i parametri di input ed output:

$$i^{op}(i((a,b),c)) = i^{op}(a, (b,c)) \text{ che restituisce } ((a,b),c) \quad (11)$$

Vediamo così che l'opposto di i restituisce lo stesso valore che restituisce Id_W (Id_W è una relazione fra W e W , visto che W è $(A \times B) \times C$ possiamo scrivere che $Id_W((a,b),c) = ((a,b),c)$).

$\mathcal{P}(A) \cong \text{fun}(A, 2)$ ¹². Questo caso è dimostrato. ■

⁹nota che puoi chiamare due insiemi di biezione anche in corrispondenza, 1-1 o una relazione biunivoca

¹⁰attenzione: usare il simbolo \cong invece che un semplice $=$ vuole dire che non per forza le due parti devono essere uguali, quindi si sopperisce ad un eventuale mancanza di uguaglianza

¹¹questa forma vuol dire che se diamo in input alla funzione i una coppia di valori (a,b) restituirà una coppia (b,a)

¹²Questo insieme è quello dei numeri binari

Dimostrazione 2° - $Id_K = i^{op}; i$ Procediamo in maniera analoga alla dimostrazione 1° quindi andiamo a rappresentare la composizione fra l'opposto i^{op} ed i come funzioni di funzione $i(i^{op})$ andando poi ad inserire i parametri i input ed output:

$$i(i^{op}(a, (b, c))) = i((a, b), c) \text{ che restituisce } (a, (b, c)) \quad (12)$$

Pure in questo caso possiamo vedere che l'opposto di K Id_K restituisce gli stessi valori scritti sopra (anche in questo caso tieni a mente che l'opposto di Id_K è una relazione che associa K con K quindi, ricordando che K è $A \times (B \times C)$, se la scriviamo sotto forma di funzione è $Id_K(a, (b, c)) = (a, (b, c))$. Anche questo caso è dimostrato. ■

Essendo che entrambi le casistiche sono state dimostrate possiamo concludere che l'insieme di biezione $(A \times B) \times C \cong A \times (B \times C)$ è dimostrato. ■

2.6.5 Proprietà insiemi di biezione

Per tutti gli insiemi A, B, C valgono le proprietà scritte nella tabella 7.

Riflessiva	$A \cong A$
Simmetrica	$A \cong B \iff B \cong A$
Transitiva	$A \cong B, B \cong C \implies A \cong C$

Table 7: Proprietà insiemi di biezione

2.7 N-upla

Definizione 2.10 (N-upla). *Una sequenza su A di lunghezza n che è una n -upla $(a_0, a_1, a_2, \dots, a_{n-1})$ dove per tutti gli indici $i \in \{0, 1, \dots, n-1\}$ di $j \in A$ l'insieme A^n di tutte le sequenze è definito come:*

$$A^n = \{(a_0, a_1, \dots, a_{n-1}) \mid \forall i \in \{0, \dots, n-1\} . a_i \in A\} \quad (13)$$

Definizione 2.11 (Sequenza su A di lunghezza arbitraria). *Una sequenza su A di lunghezza arbitraria è una sequenza di lunghezza n per qualsiasi numero naturale $n \in \mathbb{N}$. L'insieme di tutte le sequenze su A di lunghezza arbitraria:*

$$A^* = \bigcup_{n \in \mathbb{N}} A^n$$

3 Induzione

L'induzione è un metodo formale che aiuta a definire in modo rigoroso insiemi, funzioni ma anche serve per dimostrare che una proprietà è vera per tutti gli elementi di un tale insieme. Diventa soprattutto utile quando queste definizioni sono un insieme, funzioni di cardinalità o di lunghezza notevolmente grande (ma sempre finiti).

3.1 Schema generale induttivo

Schema generare induttivo usato per definire un insieme A , e con il quale tramite una regola finita andiamo a rappresentare infinite soluzioni:

1. **Clausola base**, o caso base, che stabilisce che certi oggetti appartengono all'insieme. Questi elementi costituiscono i mattoncini per costruire altri elementi dell'insieme. Nel nostro caso andiamo ad elencare un numero finito di elementi che appartengono ad A .
2. **Clausola induttiva** o passo induttivo, che descrive in che modo gli elementi dell'insieme possono essere usati per produrre altri elementi dell'insieme. Nel nostro caso usiamo elementi di A per costruirne o definirne altri.
3. **Clausola terminale**, che stabilisce che l'insieme che si sta definendo non contiene altri elementi oltre a quelli ottenuti dalle due clausole precedenti. Quindi l'insieme definito è il più piccolo insieme che soddisfa la clausola base e quella induttiva. Nel nostro caso definiamo che gli unici elementi che soddisfano A sono quelli definiti nelle condizioni 1 e 2.¹³

Esempio 3.1. Riscrivendo per intero in nostro esempio con A :

Clausola base: $A_1 \times A_2$ è una n -upla

Clausola induttiva: $A_1 \times A_2 \times A_3$ è una n -upla

Tramite queste due clausole possiamo andare a ricreare ogni n -upla (2-upla, 3-upla, ecc..) andando semplicemente a ripetere la clausola induttiva partendo da quella base. Infatti una 3-upla è clausola base per 1 volta clausola induttiva, mentre una 4-upla è la clausola base più due ripetizioni della clausola induttiva:

3-upla = $A_1 \times A_2 \times A_3$ 4-upla = $A_1 \times A_2 \times A_3 \times A_4$ e così per ogni n -upla

Esempio 3.2. Altri esempi particolari di casi induttivi:

- **Chiusura di kleene** o stella di kleene: $A^* = \bigcup_{n=0}^{\infty} A^n$ $A^n = A \times A \times A \dots$ (n volte).
Parte da 0 perché si considera quella che in informatica sarebbe la stringa vuota, cioè $A^0 = \{\}$, che si rappresenta con ϵ .
- **Chiusura positiva:** $A^+ = \bigcup_{n=1}^{\infty} A^n$ Uguale alla stella di kleene ma senza insieme vuoto.

Entrambi questi casi sono operazioni molto consuete nel mondo dell'informatica, essendo che possiamo vedere A come un insieme di caratteri per esempio $A = \text{unicode}$, e tramite queste operazioni si vanno a creare tutte le possibili sequenze o stringhe con quei caratteri.

3.2 Definizione induttiva dell'insieme \mathbb{N}

Definizione 3.1 (Definizione induttiva insieme \mathbb{N}). *L'insieme N dei numeri naturali è l'insieme di numeri che soddisfa le seguenti clausole:*

1. Clausola base: $0 \in \mathbb{N}$.
2. Clausola induttiva: se $n \in \mathbb{N}$ allora $(n + 1) \in \mathbb{N}$.

Definendo le tre clausole è immediato capire la definizione dell'insieme \mathbb{N} per induzione. Infatti possiamo ricavare qualsiasi numero dell'insieme semplicemente partendo da 0 (che già sappiamo per clausola base appartenere all'insieme) e ripetendo la clausola induttiva tante volte quanto mi serve.

¹³La clausola terminale di solito non viene specificata essendo sotto intesa

Esempio 3.3. Altri esempi analoghi alla definizione dell'insieme \mathbb{N} :

1. Definizione **N. pari**: Base: $2 \in \mathbb{N}^{pari}$ Induttiva: se $n \in \mathbb{N}^{pari}$ allora $n + 2 \in \mathbb{N}^{pari}$
2. Definizione **N. dispari**: Base: $1 \in \mathbb{N}^{dispari}$ Induttiva: se $n \in \mathbb{N}^{dispari}$ allora $n + 2 \in \mathbb{N}^{dispari}$
3. Definizione **Potenze 2**: Base: $1 \in P$ Induttiva: se $p \in P$ allora $2 * p \in P$
 È possibile scrivere anche come: Base: $2^0 \in P$ Induttiva: se $2^n \in P$ allora $2^n + 1 \in P$

3.3 Definizione induttiva di funzioni

Per andare ad effettuare la definizione induttiva di una funzione bisogna andare (1) a stabilire il valore delle funzioni per gli elementi appartenenti alla clausola base e (2) una regola per andare a calcolare il valore della funzione sugli elementi che vi appartengono, stabiliti dalla clausola induttiva. Successivamente tramite la clausola terminale definiamo che i punti (1) e (2) sono sufficienti a definire la funzione per tutti gli elementi dell'insieme. Quindi, prendendo una $f : A \rightarrow B$:

- La **clausola base** sarà il valore di $f(a)$ per alcuni $a \in A$.
- La **clausola induttiva** invece indicherà il valore di $f(a)$ utilizzando valori di f già definiti in precedenza.

Esempio 3.4. Facciamo un primo esempio definendo la funzione dei **numeri triangolari**.

Definizione 3.2 (Numeri triangolari). *Per ogni $n \in \mathbb{N}$ in numero triangolare T_n è uguale alla somma di tutti i numeri minori o uguali a n :*

$$T_n : \mathbb{N} \rightarrow \mathbb{N} \text{ o } T_n = \text{fun}(\mathbb{N}, \mathbb{N}) \quad T_n = \sum_{i=0}^n i \quad (14)$$

1. Clausola base: $T_0 = 0$
2. Passo induttivo: $T_{n+1} = T_n + (n + 1)$

Per andare a dimostrare questa casistica possiamo procedere per casi andando a controllare $n = 1, n = 2, n = 3, \dots$ e dimostrare la validità per questi casi, cosa che però non porta ad un risultato per un generico numero n . Per dimostrare la validità bisogna andare a dimostrare quella che viene chiamata *formula di gauss*.

$$\forall n \in \mathbb{N}. \left(T_n = \frac{n \cdot (n + 1)}{2} \right) \quad (15)$$

3.4 Dimostrazione induttiva di proprietà

Per andare a dimostrare una proprietà bisogna applicare il principio di induzione sui numeri naturali, che, dato una generica proprietà $P(n)$ sui naturali dice:

Definizione 3.3 (Principio di induzione). *Se (caso base) $P(0)$ è vera, e se (passo induttivo) per ogni $n \in \mathbb{N}$ vale che se $P(n)$ è vera allora anche $P(n + 1)$ lo è, allora $P(m)$ è vera per ogni $m \in \mathbb{N}$*

$$\frac{P(0) \quad \forall n \in \mathbb{N}. (P(n) \implies P(n + 1))}{\forall m \in \mathbb{N}. P(m)} \quad (16)$$

Proposizione 3.1 (Formula di gauss). *La formula (15), $T_n = \frac{n(n+1)}{2}$, è valida per ogni $n \in \mathbb{N}$*

Dimostrazione 3.1 (Formula di gauss). Per dimostrare la formula di gauss (15) per induzione è sufficiente dimostrare i seguenti casi:

1. Caso base: $T_0 = 0$, perché per definizione sarebbe $\frac{0 \cdot (0+1)}{2} = 0$, quindi la formula di gauss (15) per $n = 0$ è vera.

2. Passo induttivo: Assumiamo che l'ipotesi $T_n = \frac{n \cdot (n+1)}{2}$ sia vera e dimostriamo che è vera per ogni $n + 1$, cioè che:

$$\begin{aligned} T_{n+1} &= T_n + (n+1) && \text{Possibile per il passo induttivo della definizione dei numeri triangolari} \\ &= \frac{n \cdot (n+1)}{2} + (n+1) && \text{Sostituiamo a } T_n \text{ la clausola induttiva} \\ &= \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} && \text{Sviluppiamo l'equazione} \\ &= \frac{(n+2) \cdot (n+1)}{2} && \text{Dimostrato il caso } T_{n+1} \text{ la formula è dimostrata per induzione.} \quad \blacksquare \end{aligned}$$

Esempio 3.5 (De Morgan). Facciamo un altro esempio andando a dimostrare la proprietà di **De Morgan** per induzione. Tale proprietà dice che:

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$

Noi dobbiamo andare a dimostrare che questa legge può vale per più insiemi utilizzando l'induzione. Quindi dobbiamo far valere la generalizzazione:

$$DM(n) = \forall A_1, \dots, A_n \cdot \left(\overline{\left(\bigcup_{i=1}^n A_i \right)} = \bigcap_{i=1}^n \overline{A_i} \right)$$

Noi a questo punto dobbiamo in particolare andare a dimostrare che per ogni $n \geq 2$ vale $DM(n)$:

$$\forall n. (n \geq 2 \implies DM(n))$$

1. Caso base: $DM(2)$ dice che $\overline{(A_1 \cup A_2)} = \overline{A_1} \cap \overline{A_2}$, ed è dimostrato perché è ciò che dice la legge di De Morgan.
2. Passo induttivo: Assumiamo che $DM(n)$ sia vera e dimostriamo che vale anche $DM(n+1)$. Noi quindi vogliamo dimostrare che la seguente proprietà sia vera:

$$DM(n+1) = \forall A_1, \dots, A_{n+1} \cdot \left(\overline{\left(\bigcup_{i=1}^{n+1} A_i \right)} = \bigcap_{i=1}^{n+1} \overline{A_i} \right)$$

Se prendiamo $n+1$ che è un insieme di $A_1, A_2, \dots, A_n, A_{n+1}$ notiamo che:

$$\begin{aligned} \overline{\left(\bigcup_{i=1}^{n+1} A_i \right)} &= \overline{\left(A_{n+1} \cup \bigcup_{i=1}^n A_i \right)} && \text{Perché possiamo usare la proprietà associativa per } \cup. \\ &= \overline{A_{n+1}} \cap \overline{\left(\bigcup_{i=1}^n A_i \right)} && \text{Utilizzando De Morgan} \\ &= \overline{A_{n+1}} \cap \left(\bigcap_{i=1}^n \overline{A_i} \right) && \text{Per ipotesi induttiva.} \\ &= \left(\bigcap_{i=1}^{n+1} \overline{A_i} \right) && \text{Possiamo racchiudere tutto sotto la concatenazioni di intersezioni.} \end{aligned}$$

Vediamo quindi che anche il $DM(n+1)$ è dimostrato, quindi che tutte le sequenze $DM(n)$ sono dimostrate. \blacksquare

Esempio 3.6 (Numeri di Fibonacci). La successione dei numeri di Fibonacci può essere definita induttivamente come:

1. $f_1 = 1$
2. $f_2 = 1$
3. $f_n = f_{n-1} + f_{n-2}$ se $n > 2$

Dimostrazione 3.2 (Numeri di Fibonacci). Proviamo a dimostrare questa successione numerica. Sia f_i l' i -esimo numero di Fibonacci, noi dobbiamo dimostrare per induzione che:

$$\forall n \in \mathbb{N}^+ . \left(\sum_{i=1}^n f_i^2 = f_n \cdot f_{n+1} \right) \quad (17)$$

1. Caso base: Poiché noi dobbiamo dimostrare per tutti gli n tale che $n \in \mathbb{N}^+$ per il caso base dobbiamo considerare $n = 1$, quindi il nostro caso base sarà $\sum_{i=1}^1 f_i^2 = f_1 \cdot f_2$. questo caso è dimostriamo immediatamente dalla definizione di f_i
2. Passo induttivo: Assumiamo per ipotesi induttiva che valga $\sum_{i=1}^n f_i^2 = f_n \cdot f_{n+1}$

Una volta assunto per vero il passo induttivo possiamo dimostrare il caso $n + 1$, ciò porta a dimostrare che:

$$\begin{aligned} \sum_{i=1}^{n+1} f_i^2 &= \sum_{i=1}^n f_i^2 + f_{n+1}^2 && \text{Togliamo l'ultimo termine dalla sommatoria e scriviamolo esplicitamente.} \\ &= f_n^2 \cdot f_{n+1} + f_{n+1}^2 && \text{Applichiamo l'ipotesi induttiva} \\ &= (f_n^2 + f_{n+1}^2) \cdot f_{n+1} && \text{Proprietà distributiva} \\ &= f_{n+2}^2 \cdot f_{n+1} && \text{Sviluppiamo l'equazione} \end{aligned}$$

Vediamo come $f_{n+2}^2 \cdot f_{n+1}$ sia la causala induttiva che volevamo dimostrare. Possiamo dire dunque che la formula di Fibonacci è dimostrata. ■

3.5 Principio di Induzione forte sui naturali

Il Principio di Induzione Forte sui naturali ci permette di rafforzare le ipotesi del passo induttivo e portare avanti la dimostrazione in modo più semplice.

Definizione 3.4 (Induzione Forte). *Se per ogni $n \in \mathbb{N}$ vale che se $P(0), P(1), \dots, P(n-1)$ sono vere allora anche $P(n)$ lo è, allora $P(m)$ è vera per ogni $m \in \mathbb{N}$.*

$$\frac{\forall n. (P(0) \wedge P(1) \wedge \dots \wedge P(n-1) \rightarrow P(n))}{\forall m. P(m)} \quad (18)$$

4 Relazioni su un insieme

Definizione 4.1 (Relazioni su un insieme). *Dato un insieme A , una relazione su un insieme A è un sottoinsieme $A \times A$, cioè un elemento di $\text{rel}(A, A)$, dove $\text{rel}(A, A)$ è l'insieme delle possibili relazioni $A \times A$. Quindi una relazione $R \subseteq A \times A$.*

Le relazioni su insiemi sono caratterizzate dal fatto che si sviluppano fra due insiemi uguali. Infatti non è una relazione su un insieme un $R \subseteq A \times B$.

Esempio 4.1. Alcuni esempi generali di relazioni su un insieme:

- $\text{Succ} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y = x + 1\}$
- $\text{id}_A \in \text{rel}(A, A)$ è una relazione su A
- S è l'insieme degli studenti. $\text{CompagnoDiClasse} \in \text{rel}(S, S)$
- $\text{Somma} \in \text{rel}((\mathbb{Z}, \mathbb{Z}), \mathbb{Z})$ Somma non è una relazione su in insieme.

4.1 Proprietà di relazione su un insieme

4.1.1 Riflessiva

Dato un insieme A , una relazione $R : A \longleftrightarrow A$ possiamo definirla come:

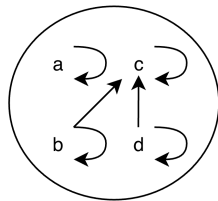
Definizione 4.2 (Riflessiva). *R è una relazione **riflessiva** se per tutti gli $a \in A$ vale che $(a, a) \in R$*

$$\forall a \in A. (a, a) \in R$$

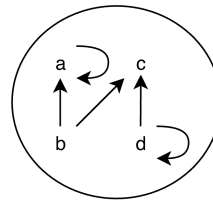
Rappresentiamo **graficamente** ora una relazione riflessiva.

Dato un insieme A di partenza dove $A = \{a, b, c, d\}$:

- Il caso [10a] è riflessivo perché ogni elemento è collegato a se stesso ¹⁴.
- Il caso [10b] non è riflessivo perché gli elementi c e b non sono collegati con loro stesso.



(a) Relazione riflessiva



(b) Relazione non riflessiva

Esempio 4.2. Alcuni esempi di relazioni riflessive:

- L'Identità di A $\text{Id}_A : A \longleftrightarrow A$ è riflessiva.
- La relazione completa $A \times A : A \longleftrightarrow A$ è riflessiva.
- La relazione vuota $\emptyset : A \longleftrightarrow A$ non è riflessiva perché non ci sono relazioni fra elementi.
- La relazione minore $< : \mathbb{N} \longleftrightarrow \mathbb{N}$ ¹⁵ non è riflessiva perché un numero non è minore di se stesso.
- La relazione minore-uguale $\leq : \mathbb{N} \longleftrightarrow \mathbb{N}$ ¹⁶ è riflessiva.
- La relazione madre: $\text{EU} \longleftrightarrow \text{EU}$ non è riflessiva.

¹⁴Il collegamento di un elemento a se stesso viene anche chiamata cappio

¹⁵La relazione minore è definita come: $< = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x < y\}$

¹⁶La relazione minore-uguale è definita come: $\leq = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$

4.1.2 Simmetrica

Dato un insieme A , una relazione $R : A \longleftrightarrow A$ possiamo definirla come:

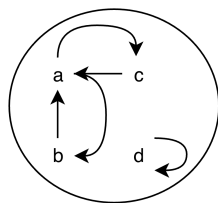
Definizione 4.3 (Simmetrica). R è una relazione **simmetrica** se per tutti gli $a, b \in A$ vale che se $(a, b) \in R$ allora $(b, a) \in R$.

$$\forall a, b \in A. (a, b) \in R \implies (b, a) \in R$$

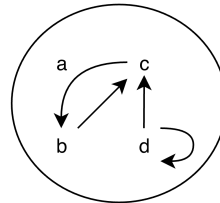
Rappresentiamo **graficamente** ora una relazione simmetrica.

Dato un insieme A di partenza dove $A = \{a, b, c, d\}$:

- Il caso [11a] è simmetrica perché ogni elemento esiste la coppia inversa di ogni collegamento.
- Il caso [11b] non è simmetrica perché gli elementi c e d hanno un collegamento sono in un verso.



(a) Relazione simmetrica



(b) Relazione non simmetrica

Esempio 4.3. Alcuni esempi di relazioni simmetrica:

- L'Identità di A $Id_A : A \longleftrightarrow A$ è simmetrica.
- La relazione completa $A \times A : A \longleftrightarrow A$ è simmetrica.
- La relazione vuota $\emptyset : A \longleftrightarrow A$ è simmetrica.
- La relazione minore $< : \mathbb{N} \longleftrightarrow \mathbb{N}$ non è simmetrica perché se un elemento a è minore di un elemento b non può essere che esista l'inverso.
- La relazione minore-uguale $\leq : \mathbb{N} \longleftrightarrow \mathbb{N}$ non è riflessiva perché ci sono casi in cui a è minore di un elemento b che non permettono l'inverso.
- La relazioni di amicizia su facebook $FbFreind : FB \longleftrightarrow FB$ è simmetrica.
- La relazioni di follow su instagram $IGFollow : IG \longleftrightarrow IG$ non è simmetrica perché se te sei follow di un utente questo utente non necessariamente lo è di te.

4.1.3 Transitiva

Dato un insieme A , una relazione $R : A \longleftrightarrow A$ possiamo definirla come:

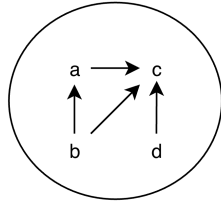
Definizione 4.4 (Transitiva). R è una relazione **transitiva** se per tutti gli $a, b, c \in A$ vale che se $(a, b) \in R$ e $(b, c) \in R$ allora $(a, c) \in R$

$$\forall a, b, c \in A. (a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$$

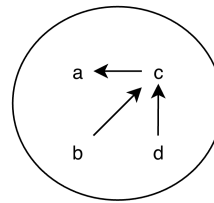
Rappresentiamo **graficamente** ora una relazione transitiva.

Dato un insieme A di partenza dove $A = \{a, b, c, d\}$:

- Il caso [12a] è transitiva perché ogni caso in cui un elemento che si trova "nel mezzo" fra due altri elementi prevede un collegamento fra questi due elementi.
- Il caso [12b] non è transitiva perché esiste (d, c) e (c, a) ma non (a, c) .



(a) Relazione transitiva



(b) Relazione non transitiva

Esempio 4.4. Alcuni esempi di relazioni transitive:

- L'Identità di A $Id_A : A \longleftrightarrow A$ è transitiva.
- La relazione completa $A \times A : A \longleftrightarrow A$ è transitiva.
- La relazione vuota $\emptyset : A \longleftrightarrow A$ è transitiva.
- La relazione minore $< : \mathbb{N} \longleftrightarrow \mathbb{N}$ è transitiva.
- La relazione minore-uguale $\leq : \mathbb{N} \longleftrightarrow \mathbb{N}$ è transitiva.
- La relazioni di amicizia su facebook $FbFreind : FB \longleftrightarrow FB$ non è transitiva perché se te sei amico di una persona e questa persona ha amico un altro utente non necessariamente te sei amico di quest'altro utente.
- La relazioni di follow su instagram $IGFollow : IG \longleftrightarrow IG$ non è transitiva perché se te hai come follow una persona e questa persona ha come follow un altro utente non necessariamente te sei come follow di quest'altro utente.

4.1.4 Anti-simmetrica

Dato un insieme A , una relazione $R : A \longleftrightarrow A$ possiamo definirla come:

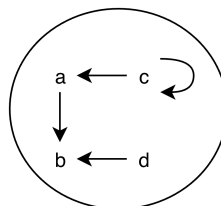
Definizione 4.5 (Anti-simmetrica). R è una relazione **Anti-simmetrica** se per tutti gli $a, b \in A$ vale che se $(a, b) \in R$ e $(b, a) \in R$ allora $a = b$

$$\forall a, b \in A. (a, b) \in R \wedge (b, a) \in R \implies a = b$$

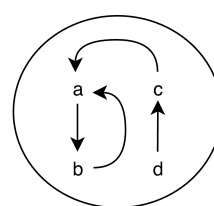
Rappresentiamo **graficamente** ora una relazione anti-simmetrica.

Dato un insieme A di partenza dove $A = \{a, b, c, d\}$:

- Il caso [13a] è anti-simmetrica perché la premessa è negata, quindi per le varie coppie di valori non esistono coppie simmetriche.
- Il caso [13b] non è anti-simmetrica perché esiste sia la coppia (a, b) e (b, a) ma a è diverso da b .



(a) Relazione anti-simmetrica



(b) Rel. non anti-simmetrica

Esempio 4.5. Alcuni esempi di relazioni anti-simmetrica:

- L'Identità di A $Id_A : A \longleftrightarrow A$ è anti-simmetrica.
- La relazione completa $A \times A : A \longleftrightarrow A$ non è anti-simmetrica perché sicuramente esisterà sia (a, b) che (b, a) ma non necessariamente $a = b$.

- La relazione vuota $\emptyset : A \longleftrightarrow A$ è anti-simmetrica.
- La relazione minore $< : \mathbb{N} \longleftrightarrow \mathbb{N}$ è anti-simmetrica ¹⁷.
- La relazione minore-uguale $\leq : \mathbb{N} \longleftrightarrow \mathbb{N}$ è anti-simmetrica.

4.2 Teorema di caratterizzazione

Teorema 4.1 (Teorema di caratterizzazione). *Pero tutti gli insiemi A e per tutte le relazioni $R : A \longleftrightarrow A$ vale che:*

1. R è **riflessiva** $\iff Id_A \subseteq R$.
2. R è **simmetrica** $\iff R \subseteq R^{op}$ (o anche $R^{op} \subseteq R, R = R^{op}$).
3. R è **transitiva** $\iff R; R \subseteq R$.
4. R è **anti-simmetrica** $\iff R \cap R^{op} \subseteq Id_A$.

Dimostrazione 4.1 (Simmetrica). Proviamo a dimostrare il punto 2 quindi che R è **simmetrica** $\iff R \subseteq R^{op}$ (o anche $R^{op} \subseteq R, R = R^{op}$).

Per effettuare questa dimostrazione andiamo a dimostrare i due sensi dell'implicazione (in due sensi della freccia \iff).

- $\forall (a, b) \in R \implies (b, a) \in R \implies R \subseteq R^{op}$.
Noi sappiamo che per la proprietà simmetrica che per ogni coppia di valori (a, b) dovrà esistere (b, a) , quindi l'insieme R sarà composto da una serie di coppie e i loro opposti. Da qui deduciamo come se $(b, a) \in R$ e $(a, b) \in R$ e l'opposto di R , R^{op} , conterrà ugualmente tutte le coppie di R soltanto invertite (per la definizione di opposto), farà sì che, essendo già presenti le coppie di valori invertite in R , $R \subseteq R^{op}$. In maniera più formale: $\forall (a, b) \in R$ sarà presente un $\forall (a, b) \in R^{op}$ e $\forall (b, a) \in R$ sarà presente un $\forall (b, a) \in R^{op}$ per la definizione di op e di simmetria.
- $R \subseteq R^{op} \implies \forall (a, b) \in R \implies (b, a) \in R$.
Per dimostrare la proprietà simmetrica partendo da $R \subseteq R^{op}$ consideriamo che: $(a, b) \in R$ per assunzione $(a, b) \in R^{op}$ ma per definizione di opposto, per far in modo che $(a, b) \in R$ allora $(b, a) \in R$, è così dimostrato anche questo senso dell'implicazione.

4.3 Chiusure

Le chiusure servono per rendere una relazione in un determinato modo tra riflessiva, simmetrica transitiva, applicando delle operazioni fra insiemi.

4.3.1 Chiusura riflessiva

La chiusura riflessiva di R è il modo "minimale" per rendere R riflessiva.

Definizione 4.6 (Chiusura riflessiva). *Sia $R : A \longleftrightarrow A$ una relazione su in insieme A , la chiusura riflessiva di R è la relazione $R \cup Id_A$*

Esempio 4.6. Alcuni esempi di chiusure riflessive:

$$Id_A : A \longleftrightarrow A = Id_A \quad A : A \longleftrightarrow A = A \times A \quad \emptyset : A \longleftrightarrow A = Id_A$$

$$< : \mathbb{N} \longleftrightarrow \mathbb{N} = \leq \quad \leq : \mathbb{N} \longleftrightarrow \mathbb{N} = \leq$$

Note 4.3.1. *Nota che per ogni $S : A \longleftrightarrow A$, se $R \subseteq S$ ed R è riflessiva, allora $R \cup Id_A \subseteq S$*

¹⁷Ricorda che se cade la premessa allora la conclusione è sempre vera per le leggi logiche sugli operatori

4.3.2 Chiusura simmetrica

La chiusura simmetria di R è un metodo "minimale" per rendere R simmetrica. Sia $R : A \longleftrightarrow A$ una relazione su in insieme A :

Definizione 4.7 (Chiusura simmetrica). *Sia $R : A \longleftrightarrow A$ una relazione su in insieme A , la chiusura simmetrica di R è la relazione $R \cup R^{op}$*

Esempio 4.7. Alcuni esempi di chiusure riflessive:

$$Id_A : A \longleftrightarrow A = Id_A \quad A : A \longleftrightarrow A = A \times A \quad \emptyset : A \longleftrightarrow A = \emptyset$$

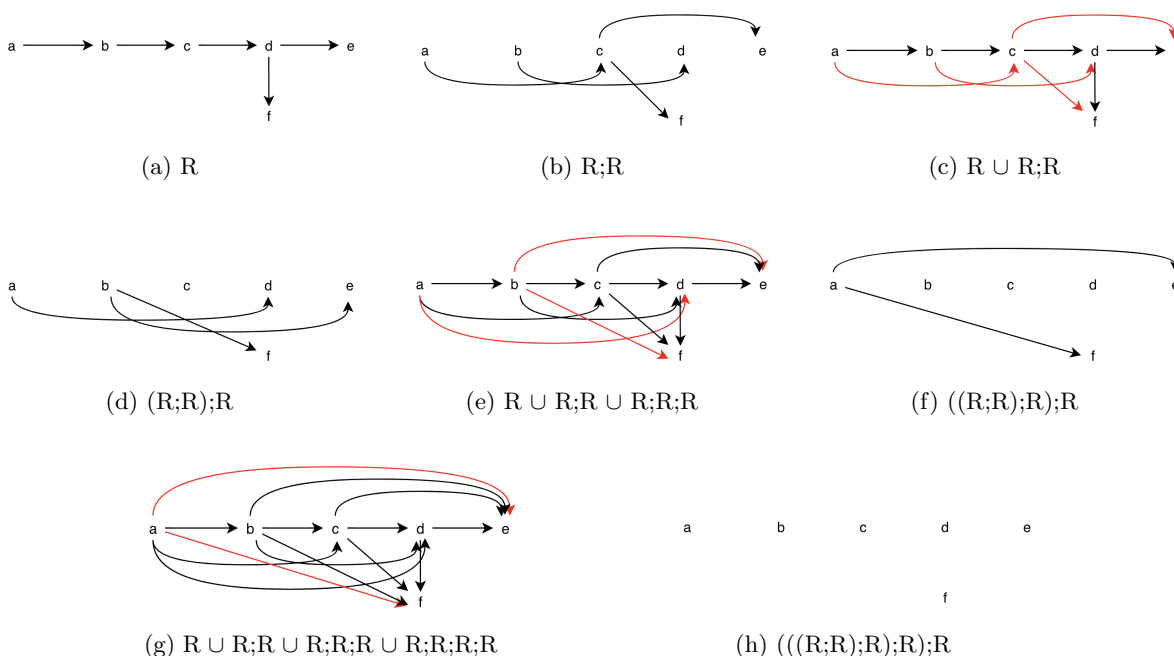
$$< : \mathbb{N} \longleftrightarrow \mathbb{N} = \neq \quad \leq : \mathbb{N} \longleftrightarrow \mathbb{N} = \mathbb{N} \times \mathbb{N}$$

Note 4.3.2. Nota che per ogni $S : A \longleftrightarrow A$, se $R \subseteq S$ ed R è simmetria, allora $R \cup R^{op} \subseteq S$

4.3.3 Chiusura transitiva

Per arrivare a capire la chiusura transitiva come opera bisogna partire da un'intuizione. La proprietà transitiva intanto dice in maniera informale che $\forall x, y \in A \exists(x, y)$ se x "può raggiungere" y in R ; capiamo dunque come la chiusura transitiva arricchisce R con tutte le coppie (x, y) tali che y è raggiungibile da x seguendo degli archi.

Sia data dunque una relazione $R : A \longleftrightarrow A$ dove $R = \{(a, b), (b, c), (c, d), (d, e), (d, f)\}$, e rappresentiamo graficamente i vari "passaggi per rendere tale relazione transitiva.



Come si vede nelle sequenza di passi sopra, il metodo per fra diventare una relazione transitiva si basa sul ripetere una serie di composizioni ed unirle fra loro finché non si raggiunge uno stato o di vuoto (come in questo caso) o di loop. Questo genere di operazione può essere definita in modo più formale tramite la composizione n-aria di relazione.

Definizione 4.8 (Composizione n-aria di relazione). *Sia A u insieme e $R : A \longleftrightarrow A$ una relazione su A , $\forall n \in \mathbb{N}$, la composizione n-aria della relazione R , R^n è definita induttivamente come:*

$$1. \text{ Caso base: } R^0 = Id_A$$

$$2. \text{ Passo induttivo: } R^{n+1} = R; R^n$$

Esempio 4.8. $R^0 = Id_A$ $R^1 = R; Id_A = R$ $R^2 = R; R$ $R^3 = R; R; R$ e così via.

Ora possiamo chiaramente definire la chiusura transitiva.

Definizione 4.9 (Chiusura transitiva). Sia $R : A \longleftrightarrow A$ una relazione su in insieme A , la chiusura transitiva di R è la relazione definita come $R^+ = \bigcup_{n \in \mathbb{N}^+} R^n$ con $\emptyset \notin R^+$.

Esempio 4.9. Alcuni esempi di chiusure transitive:

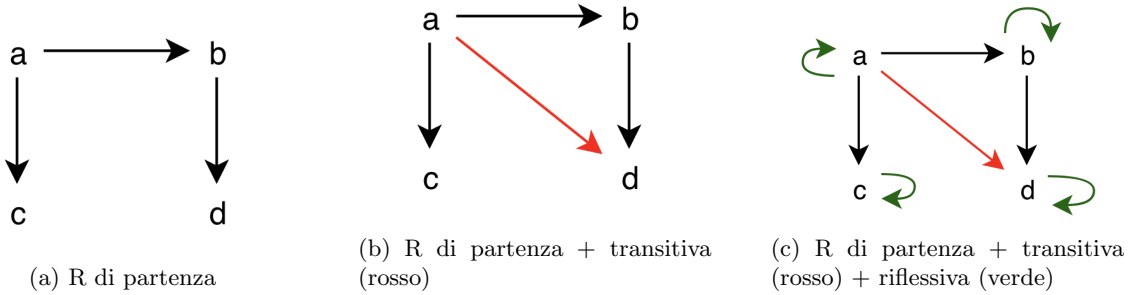
$$Id_A^+ = Id_A \quad (A : A \longleftrightarrow A)^+ = A \times A \quad (\emptyset : A \longleftrightarrow A)^+ = \emptyset$$

4.4 Stella di kleene

Definizione 4.10 (Stella di kleene). Sia A un insieme ed $R : A \longleftrightarrow A$ una relazione su A . La chiusura di kleene (o stella di kleene) è la combinazione della chiusura riflessiva e transitiva di R ed è definita come:

$$R^* = \bigcup_{n \in \mathbb{N}} R^n \quad \text{quindi} \quad R^* = (R^+) \cup (Id_A)$$

Esempio 4.10. Facciamo un esempio in cui consideriamo l'insieme $A = \{a, b, c, d\}$ ed applichiamo la stella di kleene alla relazione $R = \{(a, b), (a, d), (b, c)\}$.



4.4.1 Applicazione al While

Prendiamo come esempio questo pezzo di codice while:

```
while (x ≥ 2) do {x = x - 2}
```

Andiamo ora a definire i 3 componenti di questo ciclo.

- $C = \{(x, x-2) \mid x \in \mathbb{Z}\} : \mathbb{Z} \longleftrightarrow \mathbb{Z}$. Identifica il **corpo** del while, cioè $x = x - 2$, che è la parte che viene eseguita ad ogni iterazione.
- $G = \{(x, x) \mid x \in \mathbb{Z} \wedge x \geq 2\} : \mathbb{Z} \longleftrightarrow \mathbb{Z}$. Identifica la **guardia**, cioè $x \geq 2$. Si può notare che $G \subseteq Id_{\mathbb{Z}}$ essendo che associa coppie di valori uguali, l'unica cosa che contraddistingue G dall'identità è che i valori devono soddisfare la condizione $x \geq 2$.
- $\overline{G} = \{(x, x) \mid x \in \mathbb{Z} \wedge x < 2\}$. Identifica la **negazione della guardia** che sarebbe $\overline{G} = Id_{\mathbb{Z}} \setminus G$ cioè tutti i valori che non rispettano la condizione del while.

Utilizziamo i 3 componenti appena scritti per andare a definire il pezzo di programma sopra come una relazione.

$$W = (G; C)^*; \overline{G} \quad (19)$$

Spieghiamo velocemente la forma scritta sopra [19]. L'obiettivo è ottenere una relazione che associ un valore consentito dalla guardia al valore finale che uscirà dal while.

La prima composizione che troviamo $(G; C)$ è una relazione che dato un qualsiasi numero che rispetti le regole scritte nella guardia restituisce quel numero meno 2 ($x = x - 2$); andando poi ad applicare la stella di kleene su quella relazione, $(G; C)^*$ stiamo semplicemente aggiungendo la proprietà transitiva e riflessiva all'insieme, quindi per qualsiasi numero che rispetta le condizioni della guardia esisteranno delle coppie per tutti i "cicli" che il while permette, facciamo un esempio: prendiamo $x = 6$, il valore di x rispetta la guardia perché $x \in \mathbb{Z}$ e $x \geq 2$, inoltre, per la prima composizione, esisterà anche la coppia $(x, x - 2)$ e cioè $(6, 4)$; ora, visto che la relazione è composta da tutti i numeri appartenenti a \mathbb{Z} esisterà anche la coppia con partenza $x = 4$ e quindi formata da $(4, 2)$ e così anche le coppie $(2, 2)$ e

(2,0); se applichiamo quindi la proprietà transitiva si andranno allora a creare le coppie (6,4), (6,2) e (6,0) che possiamo vedere che sono i vari passaggi del while.

Arrivati a questo punto però noi vogliamo ottenere una relazione che dano un valore restituisca il risultato finale del ciclo, quindi, riferendosi all'esempio di prima, basterà "eliminare" tutte le coppie "intermedie, e questo si fa con l'ultima composizione, $(G; C)^*; \bar{G}$ dove \bar{G} permette di creare coppie fra i valori di partenza e il valore che non rispetta più la condizione del while, quindi (6,0), (4,0) ecc.

Dimostrazione 4.2. Andiamo ora a dimostrare che per ogni coppia $(a, b) \in \mathbb{Z} \times \mathbb{X}$, $(a, b) \in W$ se e solo se il programma while eseguito a partite da uno stato in cui $x = a$ termina in uno stato in cui $x = b$.

Caso 1° ($x \leq 2$) - Quello che dobbiamo dimostrare in questo caso è che le coppie $(a, a) \in W$ perché dati dei valori inferiori a 2 il ciclo non parte e quindi restituirà lo stesso valore.

In questo caso teoricamente per la legge con cui è costruita la relazione G , $(a, a) \neq G$ e per cioè si verifica anche la condizione $(a, a) \neq G; C$, però nel caso $(G; C)^*$ si aggiunge all'insieme anche tutta $Id_{\mathbb{Z}}$ per la proprietà della stella di Kleene, $Id_{\mathbb{Z}} \subseteq (G; C)^*$, allora arriviamo a vedere che $(a, a) \in (G; C)^*$ e che $(a, a) \in \bar{G}$ (questo perché a sono i valori minori di 2 e quindi rispettano la legge della relazione \bar{G}) quindi di conseguenza $(a, a) \in (G; C)^*; \bar{G}$ come desiderato. ■

Caso 2° ($x \geq 2$) - In questo caso dobbiamo invece dimostrare l'appartenenza all'insieme W di tutte le coppie con un x di partenza valido per l'attivazione del ciclo while.

Questa seconda casistica si dimostra in maniera intuitiva. Vediamo come prima cosa che $(a, a) \in G$ e $(a, a - 2) \in C$ quindi $(a, a - 2) \in (G; C)$, quindi per ogni $a \geq 2$ si andranno a costruire i vari passaggi del while, descrivibile come $(G; C)^n$ con $n \in \mathbb{N}^+$ dove n è l' n -esima iterazione. Ad esempio:

$$\begin{array}{ll} (6, 4) \in (G; C)^1 & (7, 5) \in (G; C)^1 \\ (6, 2) \in (G; C)^2 & (7, 3) \in (G; C)^2 \\ (6, 0) \in (G; C)^3 & (7, 1) \in (G; C)^3 \end{array}$$

Note 4.4.1. Nota che nell'esempio sopra $(6, -2) \notin (G; C)^4$ in quanto $(0, -2) \notin G; C$

Ora per concludere la dimostrazione basta considerare che la composizione $(G; C)^*; \bar{G}$ va ad associare ogni interazione valida all'interno di while $(a, a - 2)$ con i valori che non la validano (che si trovano nella relazione \bar{G}) quindi seguendo l'esempio sopra $(7, 1) \in W$ e $(6, 0) \in W$. Poiché questo ragionamento può essere applicato ag ogni numero pari o dispari maggiore o uguale a 2, questo conclude anche questo caso della dimostrazione. ■

4.4.2 Leggi stella di Kleene

Per tutti gli insiemi A e le relazioni $R : A \longleftrightarrow A$ e $S : A \longleftrightarrow A$ valgono le seguenti uguaglianze.

Riflessività	$Id_A \subseteq R^*$
Transitività	$R^*; R^* \subseteq R^*$
Chiusura	$R \subseteq R^*$
Indempotenza	$(R^*)^* = R^*$
-id	$Id_A^ = Id_A$
-compl	$(A \times A)^ = A \times A$
-vuoto	$\emptyset_{A;A}^ = Id_A$
Distributività di * su \cup	$R^* \cup S^* \subseteq (R \cup S)^*$
Distributività di * su \cap	$(R \cap S)^* \subseteq R^* \cap S^*$
Distributività di * su $.^{op}$	$(R^*)^{op} = (R^{op})^*$

Table 8: Leggi stella di Kleene

4.5 Relazioni di equivalenza

Definizione 4.11 (Relazioni di equivalenza). *Sia A un insieme $R : A \longleftrightarrow A$ una relazione su A , si dice che R è una relazione di equivalenza se **riflessiva**, **simmetrica**, **transitiva**.*

Esempio 4.11. Alcuni esempi di relazioni di equivalenza:

$$Id_A : A \longleftrightarrow A \text{ SI} \quad A : A \longleftrightarrow A \text{ SI} \quad \emptyset : A \longleftrightarrow A \text{ NO}$$

$$< : \mathbb{N} \longleftrightarrow \mathbb{N} \text{ NO perché non riflessiva} \quad \leq : \mathbb{N} \longleftrightarrow \mathbb{N} \text{ NO perché non simmetrica}$$

4.5.1 Classe di equivalenza

Definizione 4.12 (Classe di equivalenza). *Data $R : A \longleftrightarrow A$ una relazione di equivalenza, ed $a \in A$, la classe di equivalenza di a si definisce come l'insieme:*

$$[a]_R = \{b \in A \mid (a, b) \in R\} \quad (20)$$

La definizione vuol dire che, una classe di equivalenza di un determinato insieme di relazioni è un insieme di elementi appartenenti a questa relazione il quale, questi elementi, sono legati fra di loro da una relazione.

Esempio 4.12. Prendiamo $A = \{a, b, c, d\}$ ed $R = \{(a, b), (b, a), (a, a), (b, b), (c, c), (d, d)\}$

Le classi di equivalenza saranno per ogni elemento di A le seguenti:

$$[a]_R = \{a, b\} \quad [b]_R = \{a, b\} \quad [c]_R = \{c\} \quad [d]_R = \{d\}$$

Esempio 4.13. Altri esempi di classi di equivalenza. Dato un insieme A si considerino le relazioni Id_A e la relazione $A \times A$, per tutti gli $a \in A$ vale che: $[a]_{Id_A} = \{a\}$ $[a]_{A \times A} = A$

4.5.2 Teorema di biiezione

Definizione 4.13 (Partizione). *Dato un $F = A_1, A_2, A_3, \dots, A_k$, F è una partizione di A se:*

1. $\forall i A_i \neq \emptyset$
2. $\bigcup_{i=1}^m A_i = A$
3. $\forall i, j A_i \cap A_j = \emptyset$ con $i \neq j$

Ora con la definizione di partizione e di classe di equivalenza possiamo osservare che:

- L'insieme di tutte le classi di equivalenza di R definisce una partizione dell'insieme A .

$$EC_R = \{[a]_r \mid a \in A\}$$

- Viceversa, ogni partizione di A definisce una relazione di equivalenza.

$$R_f = \{(a, b) \in A \times A \mid \exists i a, b \in A_i\}$$

Teorema 4.2 (Teorema di biiezione). *Sia A un insieme, $ERel(A)$ l'insieme di tutte le relazioni di equivalenza su A , $Part(A)$ l'insieme di tutte le partizioni su A . Allora:*

$$ERel(A) \cong Part(A) \quad (21)$$

4.6 Relazioni di ordinamento

4.6.1 Ordinamento parziale

Definizione 4.14 (Ordinamento parziale). *Sia A un insieme e $R : A \longleftrightarrow A$ una relazione su A . Si dice che R è una relazione di ordinamento parziale se è **riflessiva**, **transitiva** e **anti-simmetrica**.*

Note 4.6.1. *Nota che gli ordinamenti si scrivono utilizzando o il simbolo \prec , \preceq oppure \sqsubset , \sqsubseteq .*

Esempio 4.14. Alcuni esempi di ordinamento parziale:

$Id_A : A \longleftrightarrow A$ SI $A : A \longleftrightarrow A$ NO $\emptyset : A \longleftrightarrow A$ NO

$< : \mathbb{N} \longleftrightarrow \mathbb{N}$ NO perché non riflessiva $\leq : \mathbb{N} \longleftrightarrow \mathbb{N}$ SI.

Proposizione 4.1. Per ogni insieme A , l'inclusione $\mathcal{P}(X)$ è una relazione di ordinamento parziale, e si scrive come:

$$\{(X, Y) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid X \subseteq Y\}$$

Per capire se la proposizione scritta sopra è vera dobbiamo verificare che la relazione creata abbia le proprietà riflessiva, transitiva ed anti-simmetrica.

Innanzitutto capiamo cosa crea questo insieme. Essendo il prodotto cartesiano fra due insiemi della parti su un insieme A sarà formato da coppie ordinate costituite da insiemi (essendo che l'insieme $\mathcal{P}(X)$ è un insieme di insiemi che contiene tutti i possibili insiemi creabili con A), non è però un prodotto cartesiano "completo" ma verranno prese solo le coppie di valori che rispettano la legge $X \subseteq Y$ che vuol dire che in una coppia ordinata (A, B) dove A e B sono due insiemi $A \subseteq B$. Ora che abbiamo capito da cos'è costituita questa relazione verifichiamo le varie proprietà.

1. **Riflessiva:** la relazione sarà riflessiva perché al suo interno esisteranno tutte le coppie (A, A) , (B, B) , (C, C) visto che un insieme è sempre sotto insieme uguale a se stesso.
2. **Transitiva:** la relazione sarà anche transitiva visto che se prendiamo due coppie ordinate (A, B) e (B, C) dove per le regole della relazione $A \subseteq B$ e $B \subseteq C$ esisterà anche (A, C) visto che se $A \subseteq B \subseteq C$ allora $A \subseteq C$.
3. **Anti-simmetrica:** in fine la relazione sarà anche anti-simmetrica perché se esistono coppie (A, B) dove $A \subseteq B$ non potrà mai esistere una coppia (B, A) perché se $A \subseteq B$ e $A \subseteq B$, l'insieme B avrà obbligatoriamente elementi in più di A (non in meno perché in quel caso A non sarebbe sotto insieme) quindi, per le regole della relazione, non potrà esistere la coppia (B, A) quindi la premessa è falsa e quindi la conseguenza, per le regole dell'implicazione, è vera. Mentre nel caso in cui $A = B$ la condizione di anti-simmetria è valida per sua stessa definizione.

4.6.2 Ordinamento

Definizione 4.15 (Ordinamento). Sia $R : A \longleftrightarrow A$ una relazione di ordinamento parziale su un insieme A , si dice che R è ordinamento se R soddisfa le seguenti proprietà (totalità). Per tutti gli $(a, b) \in A \times A$ vale che $(b, a) \in R$ oppure $(b, a) \in R$. Formalmente:

$$\forall (a, b) \in A \times A \mid (a, b) \in R \vee (b, a) \in R \quad (22)$$

Esempio 4.15. Alcuni esempi di ordinamento:

$Id_A : A \longleftrightarrow A$ NO $A : A \longleftrightarrow A$ Non è un ordinamento parziale $< : \mathbb{N} \longleftrightarrow \mathbb{N}$ SI

$< : \mathbb{N} \longleftrightarrow \mathbb{N}$ Non è un ord. parziale $\emptyset : A \longleftrightarrow A$ Non è un ord. parziale.

4.6.3 Ordinamento lessiografico

Definizione 4.16 (Ordinamento lessiografico). Dato un ordinamento $\sqsubseteq_A : A \longleftrightarrow A$, l'**ordinamento lessiografico** è: $a_0 a_1 \dots a_n \sqsubseteq_{A^*} b_0 b_1 \dots b_m$ se esiste $i \in \mathbb{N}$ tale che:

1. $a_j = b_j$ per tutti $j < i$
2. $a_i \sqsubseteq_A b_i$ e $a_i \neq b_i$ oppure $i = n + 1$ e $n < m$

Questo tipo di ordinamento è usato per le parole nei dizionari o negli elenchi. Si usa se dato un insieme A e un ordinamento $\sqsubseteq_A : A \longleftrightarrow A$ (ordinamento sui caratteri), si vuole definire un ordinamento $\sqsubseteq_{A^*} : A^* \longleftrightarrow A^*$ (ordinamento sulle stringhe) sull'insieme delle stringhe su A . Noi conosciamo l'ordinamento dei caratteri (l'alfabeto), dato questo possiamo, tramite l'ordinamento lessiografico, ordinare le stringhe.

Esempio 4.16. Dato un $A = \{a, b, c, \dots, z\}$ con $a \sqsubseteq_A b \sqsubseteq_A c \sqsubseteq_A \dots \sqsubseteq_A z$.

Allora tramite l'ordinamento lessiografico $alessandro \sqsubseteq_A anna \sqsubseteq_A annarella \sqsubseteq_A \dots$

5 Grafi

5.1 Grafo orientato

Definizione 5.1 (Grafo orientato). *Un grafo orientato è una relazione $E : V \leftrightarrow V$ su un insieme finito V . In un grafo V è l'insieme di nodi o vertici, E è l'insieme di archi o lati. Chiamiamo G (o G^1 , G_1 , G_2) e scriviamo $G = (V, E)$*

Esempio 5.1. Qui di seguito un esempio di un grafo:

Dati i due insiemi V e E :

$$V = \{0, 1, 2, 3, 4, 5\}$$

$$E = \{(0, 0), (0, 1), (0, 5), (1, 3), (1, 5), (2, 1), (3, 4), (3, 5), (5, 3), (5, 4)\}$$

Quello rappresentato nell'immagine 16 è un grafo orientato.

In questo esempio $n = 6$ e $m = 10$ mentre l'arco $(0, 0)$ è un cappio.

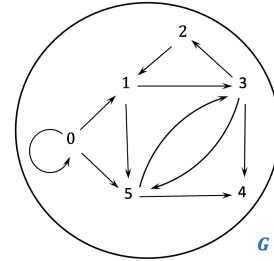


Figure 16: Grafo G

5.1.1 Notazione sui grafi orientati

Alcune punti di notazione e definizioni sui grafi (Esempi riferiti a immagine 16):

- **Cardinalità nodi:** $n = |V|$. **Cardinalità archi:** $m = |E|$.
 $V = |V| = \{0, 1, \dots, |V| - 1\}$
- **Cappio:** Un arco $(1, 1)$ quindi che parte e ritorna allo stesso nodo lo chiamiamo **cappio**.
- **Nodi adiacenti:** Nodi $x, y \in V$ sono detti **adiacenti** se $(x, y) \in E \vee (y, x) \in E$
- **Vicinato in uscita** di $x \in V$: $N^+(x) = \{y \mid (x, y) \in E\}$.
Esempio 5.2. $N^+(1) = \{3, 5\}$.
- **Vicinato in ingresso** di $x \in V$: $N^-(x) = \{y \mid (y, x) \in E\}$.
Esempio 5.3. $N^-(1) = \{0, 2\}$.

- **Grado di uscita:** dato un nodo $x \in V$: $d_x^+ = |N^+(x)|$.
Esempio 5.4. $d_0^+ = 3$, $d_4^+ = 0$.

- **Grado di ingresso:** dato un nodo $x \in V$: $d_x^- = |N^-(x)|$.
Esempio 5.5. $d_5^+ = 3$.

Definizione 5.2 (Pozzo, sorgente, isolato). *Definiamo un nodo si dice **sorgente** se non ha archi entrati, si dice **pozzo** se non ha archi uscenti e si definisce **isolato** se non ha ne archi uscenti ne entrati.*

5.1.2 Grafi orientati come relazioni e proprietà TUSI

Vediamo ora le quattro proprietà viste per le relazioni (Totale, univalente, surgettiva, iniettiva) come si applicano ai grafi. Dato un grafo orientato $E : V \leftrightarrow V$ possiamo dire che:

1. $E : V \leftrightarrow V$ è **totale** \iff per ogni nodo $x \in V$ vale $d_x^+ \geq 1$.
2. $E : V \leftrightarrow V$ è **univalente** \iff per ogni nodo $x \in V$ vale $d_x^+ \leq 1$.
3. $E : V \leftrightarrow V$ è **iniettiva** \iff per ogni nodo $x \in V$ vale $d_x^- \geq 1$.
4. $E : V \leftrightarrow V$ è **surgettiva** \iff per ogni nodo $x \in V$ vale $d_x^- \leq 1$.

5.1.3 Hand-shaking lemma

Proposizione 5.1 (Hand-shaking lemma). *Per ogni grafo orientato $G = (V, E)$, vale che:*

$$\sum_{x \in V} d_x^- = \sum_{x \in V} d_x^+ = |E| \quad (23)$$

Questo lemma può essere dimostrando intuitivamente. Se infatti prendiamo un qualsiasi arco fra esso per forza avrà un nodo di partenza ed uno di fine, quindi si dovrà per forza fare un "+1" sia alla somma degli archi entrati, alla somma degli uscenti, che alla somma di tutti gli archi, se questa cosa la estendiamo a tutti gli archi di un grafo possiamo scrivere allora scrivere che $\sum_{x \in V} d_x^- = \sum_{x \in V} d_x^+ = |E|$.

Dimostrazione 5.1. Andiamo a dimostrare questa proprietà in modo più formale per induzione:

1. Caso base: Se $|E| = 0$ non ci sono archi quindi il grado di uscita di ogni nodo sarà per forza 0, e quindi anche la somma di tutti i gradi in uscita sarà 0.

$$\sum_{x \in V} d_x^+ = 0 = |E|$$

2. Passo induttivo: Supponiamo che la proprietà valga per tutti i grafi con m archi, noi dobbiamo dimostrare il caso $m + 1$.

Prendiamo ora un grafo $G = (V, E)$ con $|E| = m + 1$, essendo che $|E| > 0$ esiste per forza almeno un arco. Ora rimuoviamo da questo grafo un arco casuale $(i, j) \in E$ tale che si vada a creare un nuovo grafo $G' = (V, E')$ con $E' = E \setminus \{(i, j)\}$, inoltre possiamo anche vedere che in questo nuovo grafo $|E'| = |E| - 1$ che è uguale a $|E'| = m$.

Avendo supposto che la proprietà per ogni m sia vera abbiamo che $\sum_{x \in V} d_x'^+ = |E'|$. Ora noi sappiamo che se escludiamo per esempio i dai nodi abbiamo che $d_x^+ = d_x'^+$ per ogni $x \in V \setminus \{i\}$, mentre $d_i^+ = d_i'^+ + 1$ perché in d_i^+ consideriamo un uscente in più che in $d_i'^+$ non abbiamo e quindi dobbiamo aggiungere. Risulta che quindi se sommiamo i gradi in uscita di G in risultato sarà uguale alla somma dei gradi uscenti di G' + il numero di archi di differenza (in questo caso 1) quindi:

$$\sum_{x \in V} d_x^+ = \sum_{x \in V} d_x'^+ + 1 = |E'| + 1 = |E|$$

E così dimostrata questa proposizioni tramite induzione. ■

5.2 Rappresentazione grafi

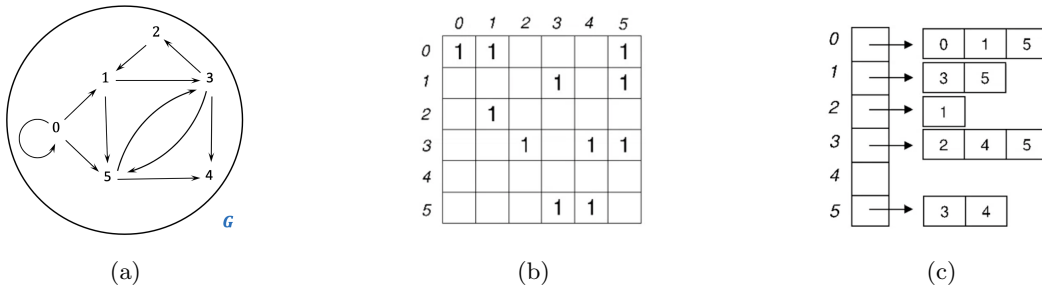


Figure 17: In (a) il grafo, in (b) la matrice di adiacenza ed in (c) la lista di adiacenza

5.2.1 Matrici di adiacenza

Una delle tecniche di rappresentazione di un grafo è quella tramite una matrice di adiacenza.

Definizione 5.3 (Matrice di adiacenza). *La matrice di adiacenza di G è una matrice quadrata A con n righe e n colonne, numerate da 0 a $n-1$, dove l'elemento di A_{ij} (in riga i e colonna j) assume un valore in $\{0, 1\}$ se $(i, j) \notin E$ e 1 se $(i, j) \in E$.*

Questo tipo di rappresentazione è molto utile per sfruttare tecniche di algebra lineare, ma non conviene in termine di spazio occupato se ci sono pochi archi da rappresentare.

Alcune proprietà dei grafi viste tramite le matrici di adiacenza:

- Dato $x \in V$, $N^+(x)$ si ottiene guardando tutti gli 1 nella riga x .
- Dato $x \in V$, $N^-(x)$ si ottiene guardando tutti gli 1 nella colonna x .
- Per ottenere $|E|$ si sommano tutti gli 1 nella matrice.
- d_x^+ si ottiene sommando gli 1 di una riga.
- d_x^- si ottiene sommando gli 1 di una colonna.

5.2.2 Liste di adiacenza

Un metodo alternativo alle matrici di adiacenza sono le liste di adiacenza.

Definizione 5.4 (Liste di adiacenza). *Le rappresentazioni con liste di adiacenza di un grafo orientato $G = (V, E)$ è costituita da un array di A di $n = |V|$ insiemi in cui l'elemento i -esimo è il vicinato in uscita del nodo $i \in V$, cioè $A[i] = N^+(i)$.*

Questo tipo di rappresentazione occupa meno memoria delle matrici di adiacenza se $|E|$ è molto minore di $|V|^2$. Questo perché se prendiamo per esempio una $|E| = 10^{11}$ ed una $|V| = 10^9$ la rappresentazioni di una matrice occuperà $|V|^2$ spazi che sono uguali a 10^{18} mentre le liste occuperanno spazi uguali a $|V| + |E|$ che in questo caso sarebbero $10^9 + 10^{11}$ che è minore di della rappresentazione della matrice.

Alcune proprietà dei grafi viste tramite le matrici di adiacenza:

- Dato $x \in V$, $N^+(x)$ si ottiene leggendo semplicemente la lista di adiacenza ad x .
- Dato $x \in V$, $N^-(x)$ si ottiene leggendo tutte le liste di adiacenza e cercando occorrenze di x .

5.3 Grafi orientati etichettati e pesati

Definizione 5.5 (Grafo etichettato, grafo pesato). *Un grafo orientato etichettato o pesato è una tripla $G = (V, E, L)$ dove L è una funzione $L : (V \cup E) \rightarrow D$ che associa ad ogni nodo e arco una etichetta presa da un certo dominio D di valori. Nel caso che D sia un valore numeri il grado si chiama anche pesato.*

La rappresentazioni di etichettate su grafi orientati è simile a quella per grafi normali, quindi si possono usare le tecniche di matrici di adiacenza e di liste di adiacenza andando però nel primo caso ad aggiungere l'etichetta al posto del numero 1, mentre nelle liste di adiacenza gli elementi dell'array non conterranno una coppia di valori con il nodo a cui è collegati e il valore dell'etichetta.

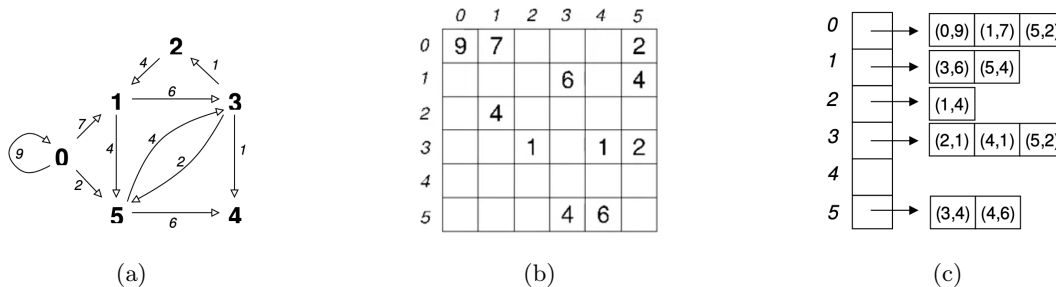


Figure 18: In (a) il grafo pesato, in (b) la matrice pesata ed in (c) la lista pesata

5.4 Cammini

Definizione 5.6 (Cammino). Un **cammino** è una sequenza di nodi collegati da archi (nella stessa direzione).

5.4.1 Walk, trail e path

Esistono 3 tipi di cammini: il **walk**, il **trail** ed il **path**

Definizione 5.7 (Walk). Dato un grafo orientato $G = (V, E)$ un **walk** è una sequenza di nodi.

$$P = v_0, v_1, \dots, v_k \text{ tale che } (v_i, v_{i+1}) \in E \text{ per ogni } i \in K$$

Vediamo che la **lunghezza** di P è uguale a k mentre gli estremi di un walk P sono v_0 e v_k , e si dice che P inizia con v_0 e termina con v_k .

Note 5.4.1. Nota che un walk di lunghezza 0 è un semplice nodo.

Definizione 5.8 (Trail e path). Un walk P è detto **trail** se attraversa ogni arco in E al più una volta. Un trail è detto **path** se attraversa ogni nodo in V al più una volta.

Esempio 5.6. Prendendo come esempio l'immagine 16 vediamo che:

- La sequenza "0, 0, 1, 3, 2, 1, 3, 2" è un walk ma non è un trail.
- Mentre la sequenza "0, 0, 1, 3, 4, 3, 4" è un trail ma non è un path.
- In fine la sequenza "0, 1, 3, 4" è un path.

5.4.2 Enunciati sui cammini

Proposizione 5.2. Sia $G = (V, E)$ un grafo orientato e siano $x, y \in V$ due nodi. Allora vale che:

$$^{18} \text{Esiste un walk di lunghezza } n \in \mathbb{N} \text{ da } x \text{ a } y \iff (x, y) \in E^n$$

Dimostrazione 5.2. Dimostrammo la proposizione 5.2 per induzione.

1. Caso base: con $n = 0$ può esistere un solo walk di lunghezza 0 e sarebbe un walk (x, x) con il nodo $x \in V$. Questo caso si dimostra facilmente visto che $E^0 = Id_E$ e per definizione di identità $(x, x) \in Id_E$.

¹⁸Ricorda che E^n è una composizione di E per n volte, quindi con $n = 3$ è $E; E; E$

2. Passo induttivo: Per ipotesi induttiva assumiamo che il caso per un walk di lunghezza n sia vero, dimostriamo ora che vale anche quello di lunghezza $n + 1$.

Noi sappiamo che esista un walk di lunghezza $n + 1$ fra x e y :

- (a) $\iff \exists$ un walk $x, v_1, v_2, \dots, v_n, y$ che a sua volta esiste.
- (b) $\iff (x, v_1) \in E$ ed esiste un walk v_1, v_2, \dots, v_n, y , che esiste.
- (c) $\iff (x, v_1) \in E$ e $(v_1, y) \in E^n$.
- (d) $\iff (x, y) \in E^{n+1}$

Nel (c) il primo passaggio del walk deve esistere già in E (E senza ulteriori composizioni E^n), il resto del walk invece è $(v_1, y) \in E^n$ e non in $n + 1$ perché avendo "tolto" e messo a se il primo passo ($(x, v_1) \in E$) ci rimane un cammino di lunghezza n . Se quindi facciamo la composizione fra E ed E^n ($E; E^n$) torna che è uguale a dire E^{n+1} , quindi arriviamo al punto (d) che dimostra il passo induttivo. ■

Lemma 5.1. Sia $G = (V, E)$ un grafo orientato e siano $x, y \in V$ due nodi. Allora vale che:

1. Se esiste un walk da x a $y \implies$ esiste un trail da x a y .
2. Se il walk ha lunghezza > 0 , allora anche il trail ha lunghezza > 0 .

Dimostrazione 5.3. Questo lemma può essere dimostrato intuitivamente in entrambi i suoi punti.

Caso 1: Innanzitutto partiamo da un walk $P = 1, 2, 3, 4, 1, 2, 6, 5$ dove c'è almeno una ripetizione dello stesso arco (in questo caso si passa 2 volte fra 1,2) che quindi non lo rende un trail.

Possiamo però rendere questo walk un trail rimuovendo tutti i collegamenti da una all'altra coppia ripetuta (in questo caso si rimuove "3,4,1,2") visto che se 2 è connesso a 6 possiamo connetterlo direttamente senza passare per 3,4,1,2. Eseguendo questa operazione per tutte le ripetizioni otteniamo un trail.

Caso 2: Se esiste un walk di lunghezza maggiore di 0 fra x e y , come visto sopra, esisterà anche un trail fra x e y , ma è immediato dire che se esiste un trail fra questi due nodi deve esistere almeno un arco che li collega e che quindi dimostra che la lunghezza è > 0 . ■

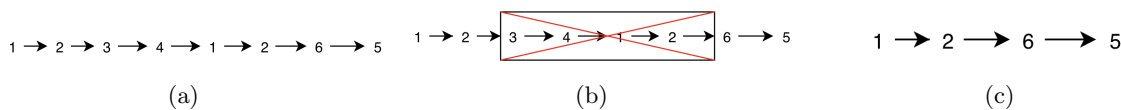


Figure 19: Steps di trasformazione di un walk in un trail

Lemma 5.2. Sia $G = (V, E)$ un grafo orientato e siano $x, y \in V$ due nodi. Allora vale che:

Se esiste un trail da x a y , allora esiste un path da x a y .

Dimostrazione 5.4. Pure questo lemma si dimostra in maniera abbastanza intuitiva. Se prendiamo infatti un trail $P = 4, 5, 6, 7, 6, 9$ che avendo una ripetizione di un nodo (il 6) non è un path, possiamo però farlo diventare andando a costruire un path rimuovendo il nodo ripetuto insieme a tutti i nodi intermedi (fra i due nodi doppi) e connettere il collegamento del nodo ripetuto al nodo mantenuto, riportato a questo esempio rimuoviamo 7,6 e connettiamo 9 a 4,5,6, questo fa uscire un path 4,5,6,9. Nel caso che con questa operazioni non sia ancora uscito un path basta ri-eseguirla per tutti i nodi ripetuti che rimangono. ■

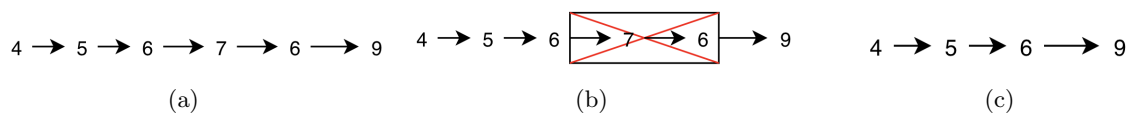


Figure 20: Steps di trasformazione di un trail in un path

5.4.3 Walk chiusi, circuiti, cicli

Quando in un walk si parte e si termina sullo stesso nodo possiamo andare a definire tale cammino in uno di questi 3 modi.

Definizione 5.9 (Walk chiuso, circuito e ciclo). Dato un walk P esso si definisce **walk chiuso** se gli estremi sono lo stesso nodo. Un walk chiuso che è un trail si definisce **circuito**, mentre un circuito che è un path viene chiamato **ciclo** (Senza considerare gli estremi).

Definizione 5.10 (Grafo ciclico). Un grafo G si dice **ciclico** se esiste almeno un ciclo in G , in caso contrario si dice **aciclico**.

Proposizione 5.3. Sia $G = (V, E)$ un grafo orientato e x un nodo in V . Le seguenti affermazioni sono equivalenti:

1. Esiste un walk chiuso da x a x .
2. Esiste un circuito da x a x .
3. Esiste un ciclo da x a x .
4. $(x, x) \in E^*$

Dimostrazione 5.5. Anche questa proposizione si dimostra intuitivamente applicando gli enunciati visti prima. Innanzitutto partiamo a dimostrare che se (1) allora (2). Questa affermazione è vera per la proposizione 5.1. Dimostriamo ora che se (2) allora (3). Questo si dimostra rapidamente come prima applicando una proposizione vista in precedenza, in questo caso la 5.2. In fine per la proposizione 5.2 (1) se e solo se (4). E così dimostrato che queste 4 affermazioni si equivalgono. ■

5.5 Connettività

Definizione 5.11 (Fortemente connesso). Dato un grafo orientato $G = (V, E)$ si dice che questo grafo è **fortemente connesso** se per ogni coppia di nodi $x, y \in V$ esiste un walk da x a y .

Definizione 5.12 (Componente fortemente connessa). Una componente fortemente connessa (SCC) di G è un sottoinsieme non vuoto di nodi $U \subseteq V$ tale che:

1. Per ogni coppia di nodi $x, y \in U$ esiste un walk da x a y .
2. Se esiste un $U' \subseteq V$ che soddisfa la 1 e $U \subseteq U'$, allora $U = U'$ ¹⁹.

Esempio 5.7. Prendiamo per esempio l'immagine 21:

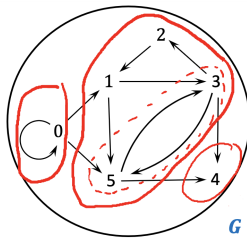


Figure 21: Grafo con i suoi SCC

In questa immagine vediamo che se prendiamo un sottoinsieme $U = \{5, 4\}$ esso non è un SCC perché non è validato il punto (2) visto che esiste un sottoinsieme $U' = \{1, 3, 5\}$ che lo contiene.

Anche U' non è un SCC mentre se prendiamo come $U = \{1, 2, 3, 5\}$ questo è un SCC visto che c'è un walk per ogni elemento ed è il sottoinsieme massimale.

In questo esempio risulta che i SCC sono:

$$\{1, 2, 3, 5\}, \{4\}, \{0\}$$

5.5.1 Componenti connesse e partizioni

Proposizione 5.4. Dato un grafo $G=(V, E)$, l'insieme delle componenti fortemente connesse di G è una partizione di V .

Dimostrazione 5.6. Andiamo ora a dimostrare questa proposizione. Innanzitutto ricordiamo che $P = \{A_i\}_{i \in I}$ è una partizione dell'insieme A se rispetta queste 3 condizioni:

1. $\forall i A_i \neq \emptyset$
2. $\bigcup_{i=1}^m A_i = A$
3. $\forall i, j A_i \cap A_j = \emptyset$ con $i \neq j$

Quello che noi dobbiamo dimostrare è che l'insieme $SCC = \{C_1, C_2, \dots, C_k\}$ è una partizione di G .

¹⁹ U si definisce sottoinsieme massimale

1. La prima si dimostra immediatamente, perché un componente fortemente connesso non può essere vuoto per la sua definizione 5.12.
2. Il secondo punto si dimostra prendendo una $x \in V$ e un insieme $U = \{x\}$, il quale rispetta la condizione (1) della definizione 5.12. Ora questo insieme può o essere una partizione, oppure esser contenuto in una componete fortemente connesso; capiamo dunque che se ripetiamo questa operazione per ogni elemento dell'insieme V avremo una serie di SCC che alla peggio saranno tutti insiemi di un elemento o al meglio sarà tutto V , in ogni caso comunque ogni elemento apparterrà alla fine ad un SCC che se andiamo ad unire tutti insieme avremo V .
3. Andiamo a dimostra il terzo punto per assurdo.
Supponiamo che $\exists C_i, C_j$ partizioni distinte $| C_i \cap C_j \neq \emptyset$. Se questa condizione è vera allora $\exists x \in C_i \cap C_j$ e $\exists y \in C_i \setminus C_j$ e anche $\exists z \in C_j \setminus C_i$ per definizione di intersezione.

Se però la condizione che abbiamo posto per assurdo è vera allora $\forall y \in C_i$ e $\forall z \in C_j \implies C_i \cup C_j$ soddisfa la proprietà (1) della definizione 5.12, e quindi che:

$\exists \text{ walk } y \dots x, \exists \text{ walk } x \dots z \implies \exists \text{ walk } y \dots z$

$\exists \text{ walk } z \dots x, \exists \text{ walk } x \dots y \implies \exists \text{ walk } z \dots y$

e questo dovrebbe avvenire perché se $C_i \cap C_j \neq \emptyset$ vuol dire che c'è un elemento in comune in entrambi gli insiemi che per la proprietà (1) dovrà avere un walk con gli altri elementi sia di C_i che di C_j . Ma se ciò accadesse gli insiemi stessi C_i e C_j non sarebbero più partizioni perché sarebbe violata la proprietà (2) della definizione esistendo un insieme $C_i \cup C_j$ che li contiene. ■

5.5.2 Proprietà connettività

Proposizione 5.5. Per tutti i grafi orientati $G = (V, E)$ e tutti gli $x, y \in V$ vale che:

1. G è fortemente connesso $\iff V \times V \subseteq E^*$.
2. $(x, y) \in E^* \cap (E^*)^{op} \iff x$ ed y appartengono alla stessa componente fortemente connessa.

Dimostrazione 5.7. Questo due proprietà sono vere perché:

1. Nella prima dire di avere un grafo fortemente connesso vuol dire avere un grafo che per ogni $x, y \in V \times V$ nodi esiste un walk fra essi, ma ciò è vero se e solo se (per la proposizione 5.2) per ogni $x, y \in V \times V$ val che $(x, y) \in E^{*20}$, ma se ogni (x, y) appartengono sia a $V \times V$ che a E^* possiamo scrivere che $V \times V \subseteq E^*$ (non il viceversa perché la stella di kleene include anche la proprietà riflessiva).
2. Per dimostrare la seconda consideriamo che se esiste un walk fra x e y e viceversa vuol dire che x e y fanno parte della stessa componente fortemente connessa e quindi $(x, y) \in E^*$ per la dimostrazione vista sopra, e $(x, y) \in (E^*)^{op}$, e questo perché: se lo vediamo come $(x, y) \in (E^{op})^*$ (possibile per le proprietà della stella di kleene) quello che facciamo è andare ad invertire tutti gli archi in E e poi aggiungere la chiusura di kleene che, aggiungendo la proprietà transitiva all'insieme, fa sì che esista un walk fra (x, y) ; quindi in conclusione visto che (x, y) appartiene ad entrambi gli insiemi apparterrà anche alla loro composizione $(x, y) \in E^* \cap (E^*)^{op}$. ■

5.6 Grafo orientato aciclico (DAGs)

Definizione 5.13 (DAG, Sorgenti, Pozzi). Un grafo orientato senza cicli si chiama **Directed Acyclic Graph (DAG)**. Al suo interno possono esistere uno o più nodi di grado di ingresso 0 detto **sorgenti** e uno o più nodi di grado di uscita 0 detti **pozzi**.

Proposizione 5.6. Se $G = (V, E)$ è un DAG, allora E^* è un ordinamento parziale.

Dimostrazione 5.8. Per andare a dimostrare che se prendiamo un grafo è un DAG, allora la stella di kleene sugli archi (E^*) è un ordinamento parziale bisogna dimostrare le 3 proprietà che rendono una relazione su un insieme un ordinamento parziale, e cioè la **transitiva**, la **anti-simmetrica** e la **riflessiva**.

²⁰Ricorda che la stella di kleene applica la chiusura transitiva per rendere appunto transitivo l'insieme, quindi applica una sequenza di composizioni, che è lo stesso di E^n

- **Dimostrazione transitiva e riflessiva:** Queste due proprietà si dimostrano velocemente visto che la stella di Kleene aggiunge sia la proprietà transitiva che riflessiva all'insieme.
- **Dimostrazione anti-simmetrica:** Per dimostrare questa proprietà basta, per il punto (4) del teorema di caratterizzazione 2.5.1, andare a dimostrare che $E^* \cap (E^*)^{op} \subseteq Id_V$. Ora noi sappiamo che se $(x, y) \in E^* \cap (E^*)^{op}$ esiste un walk fra x e y e viceversa per la proposizione 5.2 (questo perché come anche descritto nella dimostrazione 5.7 la stella di Kleene aggiunge una concatenazione di composizioni). Se poniamo per assurdo che $x \neq y$ quello che risulterebbe sarebbe un walk chiuso che attraversa entrambi, perché se esiste un walk (x, y) ed uno (y, x) esso crea un ciclo, ma questo non può essere possibile perché abbiamo supposto per ipotesi che G sia un DAG. Quindi risulta che $x = y$. ■

5.6.1 Ordinamento topologico

Definizione 5.14. Dato un DAG $G = (V, E)$ un ordinamento topologico di G è una biiezione $\eta : V \rightarrow n$ con $n = \{0, 1, 2, \dots, n-1\}$ ²¹ tale che:

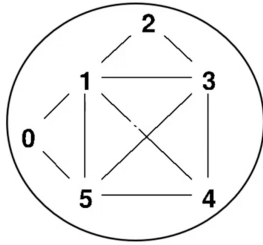
$$\text{per ogni arco } (u, v) \in E \text{ vale } \eta(u) < \eta(v) \quad (24)$$

In altre parole, se disponiamo i vertici lungo una linea orizzontale in base alla loro numerazione η , in ordine crescente, otteniamo che gli archi risultano tutti orientati da sinistra verso destra.

Proposizione 5.7. Ogni DAG ha almeno un ordinamento topologico, e ne possono esistere di più.

5.7 Grafo non orientato

Definizione 5.15 (Grafo non orientato). Un grafo non orientato $G = (V, E)$ ha un insieme finito di nodi V e un insieme di archi $E = P_2(V)$ dove $P_2(V) = \{X \subseteq V \mid |X| = 2\}$



La caratteristica principale dei grafi non orientati che gli archi non hanno una direzione, quindi sono sottoinsiemi di nodi di cardinalità 2. Scriviamo anche un arco fra x ed y come $xy \in E$, che corrisponderebbe a dire $\{x, y\} \in E$. Un grafo orientato inoltre non può avere cappi.

Quello in figura 22 è un esempio di grafo non orientato.

Figure 22: Grafo G non orientato

Notazione. Alcune definizioni e notazioni sui grafi non orientati. Dato un grafo $G = (V, E)$ non orientato si dice che:

- Il **vicinato** di un nodo $x \in V$: $N(x) = \{y \in V \mid xy \in E\}$
- Il **grado** di un nodo $x \in V$: $d_x = |N(x)|$.

Definizione 5.16 (Universale, Isolato). Un nodo x si dice *Univalente* se è vicino di tutti i nodi quindi $N(x) \cup \{x\} = V$, mentre un nodo si dice *isolato* se non ha vicinato, quindi $N(x) = \emptyset$

Definizione 5.17 (Grafo orientato associato). Dato un grafo non orientato $G = (V, E)$, quindi un grafo con $E \subseteq P_2(V)$, il **grafo orientato associato** a G è il grafo orientato $\tilde{G} = (V, \tilde{E})$, dove la relazione \tilde{E} è definita come:

$$\tilde{E} = \{(x, y) \in V \times V \mid \{x, y\} \in E\} : V \leftrightarrow V$$

²¹Si ricorda che per la definizione vista nel capitolo 1 ogni numero naturale n denota un insieme



Figure 23: In (a) il grafo non orientato ed in (b) il rispettivo grafo non associato

5.7.1 Hand-shaking lemma

L'hand-shaking lemma vari per i grafi non orientati rispetto a come era definito per i grafi orientati.

Lemma 5.3 (Hand-shaking lemma). *Per ogni grafo non orientato $G = (V, E)$, vale che:*

$$\sum_{x \in V} d_x = 2|E|$$

Esso dice infatti che la somma dei gradi di tutti i nodi è uguale a 2 volte il numero di archi del grafo.

Il lemma è valido perché: osservando che con l'aggiunta di un arco in un grafo si va a incrementare di 1 il grado di 2 nodi differenti, visto che un arco dovrà per forza connettere due nodi che non possono essere lo stesso (non esistendo il cappio), quindi aumenterà di 2 volte la somma di tutti i gradi, mentre aumenterà solo di 1 il numero di archi, avendo aggiunto un solo arco, basta dunque andare a moltiplicare per 2 il numero di archi per ottenere la somma dei gradi.

5.7.2 Rappresentazione grafi non orientati

Le rappresentazioni per i grafi non orientati sono simili a quelle dei grafi orientati. Esiste infatti sia la rappresentazione tramite **matrice di adiacenza** che tramite **lista di adiacenza**; le uniche differenze sono che, non esistendo un verso per gli archi, verranno riscritti 2 volte i collegamenti, uno per ogni direzione, questo sia nelle matrici che nelle liste.

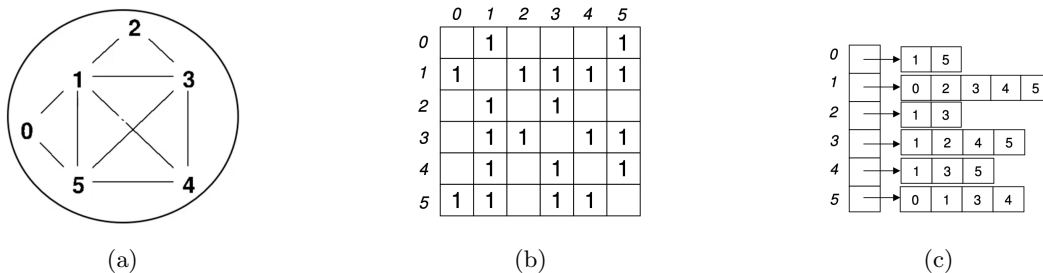


Figure 24: In (a) il grafo non orientato, in (b) la matrice ed in (c) la lista di adiacenza

5.7.3 Cammini nei grafi non orientati

Definizione 5.18 (Walk). *In un grafo non orientato $G = (V, E)$, un walk è una sequenza di nodi*

$$P = v_0, \dots, v_k \text{ tale che } \{v_i, v_{i+1}\} \in E \text{ per ogni } i \in K$$

La lunghezza del walk P è uguale a k .

Definizione 5.19 (Trail, path). *Si definisce un trail un walk che non attraversa due volte lo stesso arco. Un path è un walk (o trail) che non attraversa due volte lo stesso nodo.*

Le proposizioni 5.2, 5.3 e i lemmi 5.1, 5.2 sono validi in ugual modo per i grafi non orientati, bisogna solo tenere in considerazioni il fatto che in questo tipo di grafi gli archi non hanno verso (in pratica bisogna sostituire la E con \tilde{E}), le dimostrazioni sono simili.

5.7.4 Cicli e connettività nei grafi non orientati

Per i grafi non orientati le definizioni di **walk chiuso**, **circuiti** e **cicli** sono uguali a quelli visti nei grafi orientati (Definizione 5.9).

Note 5.7.1. *Un walk chiuso (da x a x) non implica un circuito (da x a x), ma circuito implica ciclo*

Ugualmente le definizioni di grafo **fortemente connesso** e di **componente fortemente connesso** sono analoghe a quelle viste per i grafi orientati (Definizioni 5.11, 5.12).

Pure qui, la proposizione 5.5 vale anche per i grafi non orientati (bisogna sostituire la E con \tilde{E}).

5.8 Cammini Euleriani

Definizione 5.20 (Circuito e trail euleriano). *Dato un grafo non orientato connesso $G = (V, E)$, un **circuito euleriano** è un circuito che passa esattamente una volta per tutti gli archi del grafo. Analogamente un **trail euleriano**. (conosciuto anche come percorso euleriano)*

Questa definizione parte del problema dei sette ponti di Königsberg.

Teorema 5.1 (Il teorema di Eulero). *Dato un grafo $G = (V, E)$ non orientato e connesso:*

1. *Esiste un circuito euleriano \iff tutti i nodi hanno grado pari.*
2. *Esiste un trail euleriano da x a y , con $x \neq y$ \iff x a y sono gli unici nodi di grado dispari.*

Dimostrazione 5.9. Ora calma, un bel respiro, e dimostriamo i due punti del teorema di Eulero.

Punto (1): Per andare a dimostrare questo punto dobbiamo dimostrare i due sensi della freccia.

- Se esiste un circuito euleriano \implies tutti i nodi hanno grado pari.
Questo caso è facilmente dimostrabile perché: possiamo notare che ogni volta che in un circuito euleriano noi passiamo per un nodo ($x \rightarrow y \rightarrow z$) attraversiamo 2 archi mai attraversati, questo vuol dire che il numero di archi incidenti²² in un nodo è il doppio delle volte in cui il circuito ci passa, inoltre non può verificarsi una casistica in cui un nodo ha solo un arco perché in quel modo non ci verificherebbe un circuito.
Essendo che il numero di archi incidenti ad un nodo è il doppio non potrà mai essere un numero dispari.
- Se tutti i nodi hanno grado pari \implies esiste un circuito euleriano.
Innanzitutto prendiamo un nodo r ed iniziamo a creare un percorso in G marcando ogni arco in cui passiamo in modo da non passarci una seconda volta, a questo punto solamente r avrà un solo arco incidente marcato all'inizio, mentre ogni nodo in cui passiamo avrà due archi marcati (un per arrivarci ed uno per andare), continueremo finché non ritorneremo nel nodo r creando un circuito, non potrà essere altrimenti perché se il nodo finale $u \neq r$ allora vorrebbe dire che ha un numero di archi incidenti dispari (avendo un arco per arrivarci e non uno per uscirci) e questo non è possibile per ipotesi.

A questo punto chiamiamo il circuito trovato C , se C passa per tutti gli archi allora è euleriano ed abbiamo finito, in caso contrario dobbiamo utilizzare l'ipotesi che G sia connesso per così dedurre che esista un nodo r' in C che ha un arco incidente non marcato.

Prendiamo ora r' e ripetiamo l'operazione vista prima andando a ricreare un nuovo circuito C' , notiamo che C' e C sono disgiunti sugli archi (perché marchiamo man mano gli archi che passiamo), inoltre C e C' si incontreranno in r' .

A questo punto avremo due circuiti C e C' che coincidono in un nodo r' e con tutti archi disgiunti, se quindi andiamo ad unire questi due circuiti prendendo come nodo di partenza e di arrivo r' avremo un circuito che o è euleriano o avrà un nodo r'' con un arco non segnato, vediamo dunque che possiamo nuovamente ripetere l'operazione precedentemente vista altre n volte, andando volta volta a combinare i circuiti trovati fino a che non si creerà un circuito euleriano. ■

²²Ricorda che gli archi incidenti sono gli archi che escono/entrano in un nodo, in un grafo non orientato

Punto (2): Anche qui bisogna dimostrare i due sensi della freccia per dimostrare la sua veridicità.

- Se esiste un trail euleriano da x a y , con $x \neq y \implies x$ e y sono gli unici nodi di grado dispari.
Questo verso lo dimostriamo vedendo che ogni volta che attraverso un nodo v utilizzo 2 archi, uno per entrare ed uno per uscire, le uniche eccezioni sono per il nodo di partenza e per quello di arrivo che avranno grado uguale a $2k + 1$ dove k è il numero di volte in cui si passa per quel nodo (esclusa la partenza o l'arrivo) ed il $+1$ indica appunto la partenza nel caso di x e l'arrivo nel caso di y . Abbiamo così dimostrato il primo verso.
- Se x e y sono gli unici nodi di grado dispari \implies esiste un trail euleriano da x a y .
Prendiamo per dimostrare questo caso un grafo $G = (V, E)$ che sia un grafo connesso con $x, y \in V$ di grado dispari e $\forall v \in V . v \notin \{x, y\}$ siano di grado pari (queste condizioni sono vere per l'ipotesi).
Ora creiamo un nuovo grafo G' uguale a G solo introducendo un nuovo nodo z con due archi $\{z, x\}$ e $\{z, y\}$ (questo nuovo nodo rispetta le condizioni poste nell'ipotesi).
 G' è connesso visto che il nodo z è connesso ad almeno un nodo il quale, appartenendo anche al grafo G che era connesso per ipotesi, è collegabile a tutti gli altri nodi, dunque che z lo sarà, e quindi G' è connesso.
Essendo che G' è connesso tutti, tutti i nodi hanno grado pari \exists circuito euleriano per il punto (1) di questo teorema. Ma visto che esiste un circuito euleriano z, x, \dots, y, z esisterà allora un trail x, \dots, y che sarà euleriano nel caso si consideri il grafo G (quindi senza z e i suoi archi). Così dimostriamo anche questa implicazione. ■

5.9 Cicli e path Hamiltoniani

Definizione 5.21 (Cicli e path Hamiltoniani). *Dato un grafo connesso (orientato o non orientato), un **ciclo hamiltoniano** è un ciclo che passa esattamente una volta per tutti i nodi del grafo. Analogamente, path hamiltoniano.*

Questo tipo di cammino non prevede una caratterizzazione semplice come per i circuiti euleriani. Equivale inoltre a cercare una permutazione dei nodi che formano un path.

5.9.1 Il problema del commesso viaggiatore

Il problema del commesso viaggiatore consiste, in un grafo pesato non orientato, di trovare un ciclo hamiltoniano di peso minimo, dove il peso è la somma dei pesi degli archi attraversati.

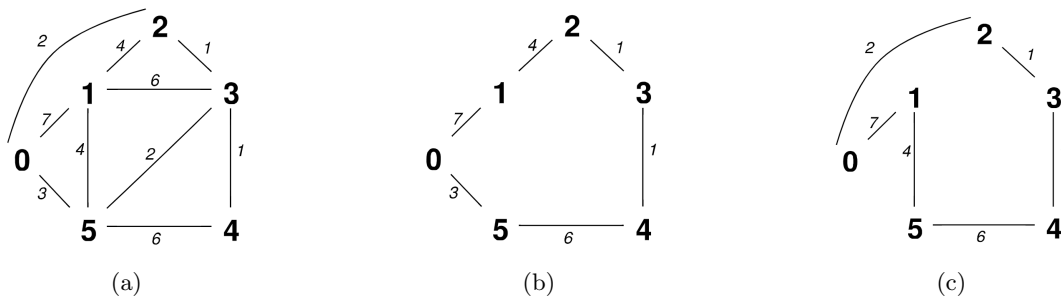


Figure 25: (a) il grafo pesato, (b) ciclo hamiltoniano in (c) un ciclo hamiltoniano di peso minimo

5.10 Distanze

Definizione 5.22 (Distanza). *Una **distanza** (o **metrica**) su un insieme A è una funzione $d : A \times A \rightarrow \mathbb{R}$ che soddisfa le seguenti proprietà per ogni $x, y, z \in A$.*

1. $d(x, y) \geq 0$.
2. $d(x, y) = 0 \iff x = y$.
3. $d(x, y) = d(y, x)$ (simmetria).

4. $d(x, y) \leq (x, z) + d(z, y)$ (disuguaglianza triangolare)

Si può notare che tutte queste condizioni sono soddisfatte dalla distanza euclidea²³, infatti (1) la distanza euclidea è sempre maggiore o uguale a 0, e se è 0 è perché abbiamo preso due punti uguali (2), inoltre (3) la distanza fra due elementi non cambia, indipendentemente da quale punto prendiamo per prima, ed in fine in un triangolo la somma delle lunghezze di due lati maggiore o uguale a quella del terzo lato (4).

Definizione 5.23 (Distanza su un grafo non orientato). *Sia $G = (V, E)$ un grafo non orientato connesso. Dati due nodi $x, y \in V$, la loro **distanza** $d(x, y)$ è la lunghezza del walk più breve tra x e y (il cammino minimo).*

Possiamo vedere che in quest'ultima definizione sono rispettate i quattro punti della definizione di distanza.

1. La distanza fra x e y è sempre maggiore o uguale a 0 perché in caso contrario vorrebbe dire che non esiste, e ciò non è possibile per la definizione stessa (nella definizione diciamo che il grafo è connesso).
2. Se la distanza fra due nodi è 0 allora il nodo è lo stesso.
3. Se esiste un cammino da x a y con una certa distanza, questo cammino può essere percorso anche da y a x e quindi mantiene la stessa distanza.
4. Essendo la distanza la lunghezza del walk più breve la distanza fra x e y sarà per forza minore o uguale di quella fra x e z sommata con quella fra z e y .

Definizione 5.24 (Distanza su grafo induttivamente). *Sia $G = (V, E)$ un grafo non orientato connesso. Dati due nodi $x, y \in V$, al loro distanza $d(x, y)$ può essere definita induttivamente:*

- Caso base: $d(x, y) = 0$, se $x = y$.
- Passo induttivo: $d(x, y) = 1 + \min\{d(z, y) \mid z \in N(x)\}$. Dove $N(x)$ è il vicinato di x

La definizione di distanza (come lunghezza del cammino minimo) si può applicare anche a grafi orientati fortemente connessi, ma in questo caso non vengono rispettate tutte le proprietà:

1. $d(x, y) \geq 0$ è vera per la definizione di grafo fortemente connesso.
2. $d(x, y) = 0$ se e solo se $x = y$ è vera perché l'unico cammino di lunghezza 0 è quello fra un nodo e se stesso.
3. $d(x, y) = d(y, x)$ invece non è rispettata perché essendoci un verso negli archi possono esistere percorsi più brevi differenti.
4. Visto che il punto (3) non è verificato non è necessario verificare il (4).

Nel caso di grafi fortemente orientati definiamo la funzione della distanza una quasi-metrica.

Proposizione 5.8. *Sia $G = (V, E)$ un grafo orientato connesso e x un nodo. Si y un nodo a distanza massima da x , allora $G \setminus \{y\}$ è connesso.*

Dimostrazione 5.10. Dimostriamo la proposizione scritta sopra, essa dice che:

$$\forall v \in V, d(x, y) \geq d(x, v) \implies \forall v \in V \setminus \{y\} \exists \text{ path } P = x, \dots, v. \text{ che non include } y.$$

I path $P = x, \dots, v$ non devono includere y perché se lo includesse allora $\exists P' = x, \dots, y$ più corto di P e questo contraddice che $d(x, y) \geq d(x, v)$.

Se dal nostro grafo rimuovo y segue per quanto detto prima che $\forall v \in V \setminus \{y\}$ esiste ancora un path $P = x, \dots, v$. Allora vediamo che $\forall v, w \exists \text{ walk } W = v, \dots, x, \dots, w \implies G \setminus \{y\}$ è connesso. ■

²³Ricorda che la distanza euclidea è la distanza fra due punti in un piano cartesiano

5.10.1 Diametro, altezza, profondità

Definizione 5.25 (Diametro di grafo). *Il diametro di un grafo G (orientato o meno) è la massima distanza tra coppie di nodi:*

$$\text{diam}(g) = \max_{x,y \in V} d(x,y)$$

Definizione 5.26 (Profondità, altezza di nodi, albero pieno). *Dato un albero radicato, la **profondità** di un nodo x è la distanza $d(x,t)$ dalla radice r , e **l'altezza** di x è la massima distanza tra x e le sue foglie discendenti. L'altezza dell'albero è l'altezza della radice. Inoltre definiamo un albero cardinale **pieno** se è completo e le foglie sono tutte alla stessa distanza dalla radice.*

5.11 Alberi

Definizione 5.27 (Albero, foglia). Un **albero** è un grafo non orientato connesso, aciclico e non vuoto (con almeno 1 nodo). I nodi interni hanno quindi grado > 1 mentre i nodi di grado 1 sono detti **foglie**.

Definizione 5.28 (Foresta). Una **foresta** è un grafo non orientato, aciclico e non vuoto dove ogni componente connessa è un albero assestante.

Da queste definizioni possiamo dedurre alcune proprietà relative agli alberi.

- Il numero di path possibili fra due nodi è sempre uno, perché se esistessero due path distinti la concatenazione di questi due path sarebbe un walk chiuso e quindi il grafo avrebbe cicli (ricorda la proposizioni 5.3 che ci dice che dire walk chiuso o ciclo è analogo).
- Se andiamo a togliere un arco in un albero si andrà a creare una foresta con 2 alberi.
- Se invece andiamo ad aggiungere un arco quello che uscirà non sarà più un albero perché si creerà un ciclo.

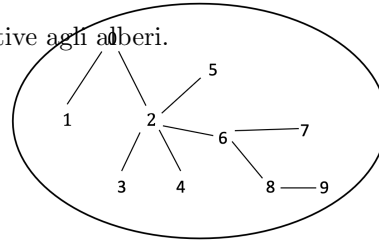


Figure 26: Esempio di albero

Proposizione 5.9. Dato un albero $G = (V, E)$ con $n = |V|$ nodi, valgono le seguenti proprietà:

1. Se $n \geq 2$ (ovvero l'albero ha almeno due nodi), allora G ha almeno una foglia (ovvero un nodo di grado 1).
2. G ha esattamente $n - 1$ archi, cioè $|E| = n - 1$.
3. Per ogni coppia di nodi distinti $x, y \in V$, esiste un unico path da x a y .
4. Per ogni arco $xy \in E$, la rimozione di xy rende il grafo non connesso.
5. Per ogni coppia di nodi distinti $x, y \in V$ tale che $xy \notin E$, l'aggiunta dell'arco xy crea un ciclo, cioè $G' = (V, E \cup xy)$ è un ciclo.

Dimostrazione 5.11. Andiamo ora a dimostrare ogni punto della proposizione sopra.

1. Per dimostrare il primo punto prendiamo innanzitutto un albero $T = (V, E)$ con almeno 2 nodi, per la proposizione 5.8 $\exists y \in V \mid T \setminus \{y\}$ è connesso $\implies T \setminus \{y\}$ rimane connesso quindi rimane un albero. Ora, se re-introduciamo y possiamo vedere 2 casi:
 - O $|N(y)| = 1$ (il vicinato di y è 1), quindi y è una foglia di T e la proprietà è verificata.
 - Oppure $|N(y)| \geq 2$ (il vicinato di y è maggiore o uguale a 2), in questo caso però \exists path $P = w, \dots, z$ in $T \setminus \{y\}$ e $\exists \{z, y\}, \{y, w\} \in E$ (queste due condizioni sono previste visto che un albero è connesso), ma ciò porterebbe ad un ciclo che è impossibile.

Vediamo dunque che solo la prima casistica è possibile, e quindi abbiamo dimostrato questo punto. ■

2. Per andare a dimostrare questo punto procediamo per induzione su n .

- Caso base: Se $n=1$ allora l'albero ha un solo nodo e quindi nessun arco, la proprietà in questo caso è quindi dimostrata perché $n - 1 = 0$, e $m = 0$.
- Passo induttivo: Assumiamo per ipotesi induttiva che la proprietà valga per tutti gli n nodi, dimostriamo che vale anche per gli $n + 1$ nodi. Un albero in questo caso ha almeno 1 nodo quindi $n \geq 1$ mentre nel caso $n + 1$ gli alberi avranno come minimo 2 nodi ($n + 1 > 1$ che è uguale a dire $n + 1 \geq 2$), per la proprietà (1) G ha almeno una foglia y .

Prendiamo ora un albero $G' = G \setminus \{y\}$, togliamo dunque una foglia ed un arco (l'unico arco connesso a y) ed otteniamo che in G' il numero di nodi $n = (n + 1) - 1$ che quindi è $n = n$ ed il numero di archi è $m = (n + 1) - 1$ quindi $m = n$. Visto che G' ha n archi e G ne ha $n + 1$ abbiamo dimostrato l'ipotesi induttiva. ■

3. Dimostriamo questa proprietà per assurdo, quindi supponiamo che esistano due path distinti P_1 e P_2 da x a y .

Prendiamo un nodo z che sia l'ultimo nodo in comune fra P_1 e P_2 prima che P_1 e P_2 divergano in due percorsi distinti, e prendiamo un w che sia invece il primo nodo dopo z in P_1 attraversato anche da P_2 (l'esistenza di questi due nodi è obbligatoria perché P_1 e P_2 partono ed arrivano sugli stessi nodi, alla peggio $z = x$ e $w = y$).

Essendo un albero un grafo connesso esisterà un cammino fra z e w che però sarà un ciclo perché partendo da z andiamo a w passando per i nodi di P_1 e da w posso tornare a z per i nodi in P_2 ; questa però è una contraddizione, è quindi verificata la proprietà. ■

4. Questa proprietà si dimostra in modo veloce vedendo innanzitutto che se prendiamo un albero G con al suo interno due nodi x e y esisterà un unico path $P = xy$, perché in caso c'è ne fossero di più l'albero avrebbe un ciclo e quindi non sarebbe più un albero (meno di un path non è possibile per definizione di albero). Se andiamo a rimuovere P allora \nexists path fra x e y e quindi il grafo non è connesso. ■
5. Anche l'ultima proprietà si dimostra velocemente, visto che se abbiamo un albero G con due nodi x e y allora per definizione di albero \exists path $P = x...y$ (che non sarà xy per ipotesi), se aggiungiamo un arco xy allora si otterrà un ciclo. ■

5.11.1 Albero radicato

Definizione 5.29 (Albero radicato). Un **albero radicato** $G=(V,E,r)$ è costituito da un albero $G=(V,E)$ e da un nodo $r \in V$ chiamato **radice**.

Definizione 5.30 (Antenato, genitore, discendente, figlio). Dato un albero radicato $G=(V,E,r)$ e dato un nodo $y \in V$ e $y \neq r$ possiamo dare le seguenti definizioni.

- I nodi lungo l'unico cammino che collega y a r si chiamano **antenati**.

- Il primo nodo fra gli antenati (quello adiacente a y) è detto il **genitore** di y .
- Simmetricamente y viene detto **discendente** dei suoi antenati e **figlio** del nodo genitore.

Definizione 5.31 (Sottoalbero). Dato un albero radicato $G = (V, E, r)$ e dato un nodo $r' \in V$ il **sottoalbero** di G con radice r' è l'albero radicato $G' = (V', E', r')$ in cui $V' \subseteq V$ contiene r' e tutti i suoi discendenti in G , e $E' \subseteq E$ contiene tutti gli archi di G tra i nodi di V' .

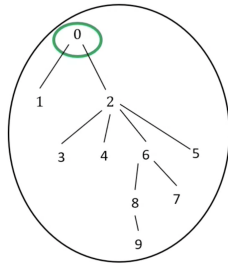


Figure 27: Albero radicato con radice r

Se prendiamo l'immagine 27 vediamo che la radice $r = 0$. La radice ha come figli 1 e 2 mentre 2 ha come antenato solo la radice.

Se prendiamo il nodo 8 questo nodo è padre di 9 e ha come fratello 7.

Il nodo 9 invece è un discendente di 2 essendo che 2 è un suo antenato.

Definizione 5.32 (Albero ordinale, albero cardinale). Un albero radicato si dice **albero ordinale** se per ciascun nodo interno è definito un ordinamento totale tra i suoi figli. Un albero radicato si dice **albero cardinale** o k -ario se ogni nodo interno ha esattamente k figli, alcuni dei quali possono essere vuoti.

Definizione 5.33 (Albero completo, binario). Un albero cardinale è **completo** se ogni nodo interno ha tutti e k i figli non vuoti. Un caso speciale di albero cardinale è quello con $k=2$, esso si dice infatti **albero binario**; in esso il primo figlio viene chiamato figlio sinistro ed il secondo figlio viene chiamato figlio destro.

5.12 Isomorfismo

Definizione 5.34 (Isomorfismo). Dati due qualunque grafi $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ dove $|V_1| = |V_2|$ e $|E_1| = |E_2|$, un isomorfismo fra questi due grafi è una biezione $f : V_1 \mapsto V_2$ tra i loro nodi tale che:

$$\forall u, v \in V_1 \text{ vale che } uv \in E_1 \iff f(u)f(v) \in E_2.$$

Possiamo definire due grafi isomorfi se esiste un isomorfismo fra di loro. Essere isomorfi è una relazione di equivalenza visto che sono presenti le proprietà riflessiva, simmetrica, transitiva.

Intuitivamente due grafi sono isomorfi se posso renderli identici "rinominando" i vertici, infatti la biezione ci dice come rinominare.

Da aggiungere è una condizione necessaria ma non sufficiente cioè che: i nodi devono avere gli stessi gradi, infatti posso subito dire che due grafi non sono isomorfi se la sequenza dei gradi (in ordine decrescente o crescente) non è identica.

5.13 Grafi notevoli

Esistono una serie di grafi, detti grafi notevoli, che per la loro struttura particolare hanno preso dei nomi specifici, essi possono essere anche ritrovati di frequente in differenti casistiche in cui si utilizzano grafi.

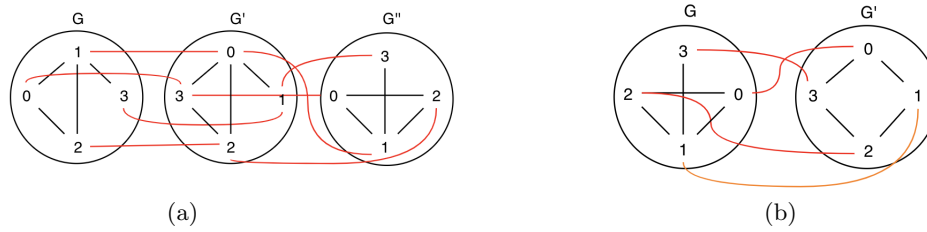


Figure 28: (a) Esempio Isomorfismo, (b) Esempio non isomorfismo

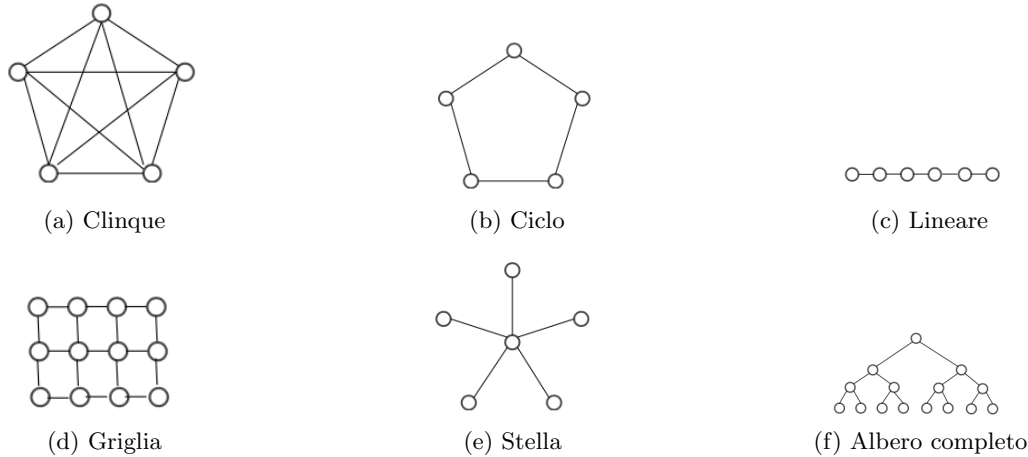


Figure 29: Serie di grafi notevoli

6 Calcolo combinatorio

6.1 Cardinalità insiemi

Il calcolo combinatorio serve per dare delle risposte a domande come: quanti sono? In quanti modi? Quante possibili combinazioni? Per questa forma di calcolo si fa molto utilizzo del concetto di cardinalità di un insieme.

Definizione 6.1 (Cardinalità). La **cardinalità** di un insieme (finito) A è il numero dei suoi elementi e si indica con $|A|$.

Esempio 6.1. $|\{a, e, i, o, u\}| = |\{i, i, i, o, u, e, a, a\}| = 5$ (Le ripetizioni non si contano)
 $|\emptyset| = 0 \quad |n| = |\{0, 1, 2, \dots, n-1\}| = n \quad |2| = |\{0, 1\}| = 2$

Lemma 6.1 (Lemma-x). Dato un insieme A , sia $P = \{A_i\}_{i \in I}$ una partizione di A quindi:

- $\bigcup_{i \in I} A_i = A$ (Punto (2) della definizione di partizione)
- $\forall i, j \in I. i \neq j \implies A_i \cap A_j = \emptyset$ (Punto (3) della definizione di partizione)

Allora vale che $|A| = \sum_{i \in I} |A_i|$.

Note 6.1.1. Notare che nella proposizione sopra non è necessario che valga la condizione (1) di una partizione quindi che $(\forall i \in I. A_i \neq \emptyset)$, e ciò perché se consideriamo una partizione vuota essa non andrà ad influire sulla somma delle cardinalità avendo valore 0.

Dimostrazione 6.1. Per dimostrare questa proposizione supponiamo che $|A| \neq \sum_{i \in I} |A_i|$, quindi $|A|$ sarà o maggiore o minore della sommatoria delle sue partizioni:

- $|A| > \sum_{i \in I} |A_i|$: questo caso contraddice il secondo punto della definizione di partizioni infatti fosse vero questo caso dovrebbe esistere un $a \in A$ che però $a \notin \forall i A_i$

- $|A| < \sum_{i \in I} |A_i|$: questa casistica invece contraddice il terzo punto delle partizioni, infatti per far sì che la cardinalità di A sia inferiore alla somma delle cardinalità delle partizioni dovrebbe esistere un $a \in A$ che contiamo due volte (ed è quindi presente in due partizioni distinte) ma questo farebbe sì che $\exists A_i \neq A_j$ dove $A_i \cap A_j \neq \emptyset$. ■

6.1.1 Cardinalità di operazioni su insiemi

Proposizione 6.1. Per tutti gli insiemi A e B valgono i seguenti fatti:

1. $|A| = |A \setminus B| + |A \cap B|$
2. $|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A|$

Dimostrazione 6.2. Dimostrazione con i diagrammi di eulero-vann della proprietà (1).

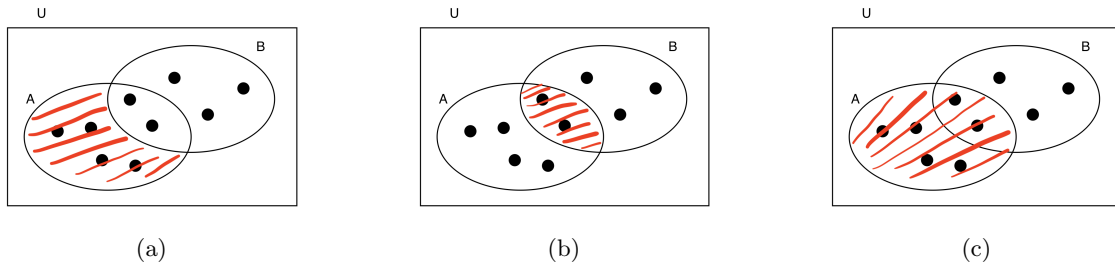


Figure 30: In (a) $|A \setminus B|$, in (b) $|A \cap B|$, in (c) la somma di (a) e (b) uguale a $|A|$

Corollario 6.1. Per tutti gli insiemi A e B valgono i seguenti fatti:

1. $|A \setminus B| = |A| - |A \cap B|$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $|A \cup B| \leq |A| + |B|$ e sono uguali $\iff A$ e B sono disgiunti (lemma 6.1)
4. Se $B \subseteq A$ allora $|B| \leq |A|$

6.1.2 Principio di inclusione-esclusione

La cardinalità dell'unione fra due insiemi si può definire come:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Questa formula può essere generalizzata a 3 insiemi, essa si scrive come:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Dimostrazione 6.3. Scriviamo $|A \cup B \cup C|$ come $|(A \cup B) \cup C|$ e prendiamo $(A \cup B)$ come fosse un unico insieme ed applichiamo la formula base.

- $|(A \cup B) \cup C| = |(A \cup B)| + |C| - |(A \cup B) \cap C|$ (Ri-applichiamo la formula base su $(A \cup B)$).
- $= |A| + |B| - |A \cap B| + |C| - |(A \cup B) \cap C|$ (Scriviamo $|(A \cup B) \cap C|$ usando le proprietà degli insiemi).
- $= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)|$ (Usiamo lo stesso ragionamento iniziale su $|(A \cap C) \cup (B \cap C)|$).
- $= |A| + |B| - |A \cap B| + |C| - ((A \cap C) + (B \cap C)) - |(A \cap C) \cap (B \cap C)|$ (Riscriviamo $(A \cap C) \cap (B \cap C)$).
- $= |A| + |B| - |A \cap B| + |C| - |(A \cap C) + (B \cap C)| - |A \cap B \cap C|$ ■

Possiamo generalizzare ulteriormente questa formula estendendola su n insiemi.

Definizione 6.2 (Principio di inclusione-esclusione). *Presi r insiemi S_1, S_2, \dots, S_r , abbiamo la seguente uguaglianza, dove $(-1)^i$ vale 1 se i è un numero pari e vale -1 se i è dispari:*

$$\left| \bigcup_{j=1}^r S_j \right| = \sum_{I \subseteq \{1, 2, \dots, r\}, I \neq \emptyset} (-1)^{|I|+1} \left| \bigcap_{i \in I} S_i \right| \quad (25)$$

Questa formula spiegata a parole più semplici dice che:

- Per ogni possibile sottoinsieme non vuoti $I \subseteq \{1, 2, \dots, r\}$ consideriamo tutti gli insiemi S_i tali che $i \in I$, e calcoliamo la cardinalità n_I della loro intersezione.
- Sommiamo tutti i valori n_I così calcolati per cui la cardinalità di I è un numero dispari, e sottraiamo tutti i valori n_I per cui la cardinalità di I è un numero pari.

Esempio 6.2. Facciamo un esempio vedendo come si va a ricreare la stessa formula vista in precedenza con il caso $|A \cup B \cup C|$. Prendiamo come $I \subseteq \{1, 2, 3\}$ prima $I = \{1\}$ poi $I = \{2\}$ e poi $I = \{3\}$ essi fanno sì che $(-1)^{|I|+1} = 1$ quindi abbiamo che $|A| + |B| + |C|$ (Perché $\left| \bigcap_{i \in I} S_i \right|$ con $I = \{1\}$, $I = \{2\}$, $I = \{3\}$ fa $|A|$ per il primo caso, $|B|$ per il secondo e $|C|$ per il terzo).

Continuiamo prendendo ora $I = \{1, 2\}$ poi $I = \{2, 3\}$ e poi $I = \{1, 3\}$, in questo caso $(-1)^{|I|+1} = (-1)^{2+1} = -1$ quindi aggiungiamo le intersezioni ed otteniamo $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$.

Prendiamo ora l'ultimo sottoinsieme che ci manca e cioè $I = \{1, 2, 3\}$, questo fa sì che $(-1)^{|I|+1} = (-1)^{3+1} = 1$ e così otteniamo $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ che è la formula a vista in precedenza

Dal principio di inclusione-esclusione seguano come corollari il lemma 6.1 visto sopra, la formula $|A \cup B| = |A| + |B| - |A \cap B|$, e come visto nell'esempio anche la formula $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

6.1.3 Cardinalità del prodotto cartesiano

Proposizione 6.2. *Per tutti gli insiemi A, B vale che $|A \times B| = |A| \cdot |B|$.*

Dimostrazione 6.4. Per dimostrare questa proposizione usiamo il lemma 6.1. Innanzitutto definiamo $\forall a \in A$ una partizioni $S_a = \{(a, b) | b \in B\}$ in modo che $S_a \subseteq A \times B$. Vediamo anche che $|S_a| = |B|$. Ora se verifichiamo i due punti della lemma-x per vedere se possiamo applicare il lemma.

1. $\bigcup_{a \in A} S_a = A \times B$ è vera visto che S_a si forma di coppie $(a_1, b_1), (a_1, b_2) \dots$ per tutti gli elementi di B quindi andando ad unire tutti gli S_a (cioè le varianti con tutte le $a \in A$) abbiamo $A \times B$.
2. $\forall a \neq a' S_a \cap S_{a'} = \emptyset$ perché se cambiamo le a avremo due insiemi completamente diversi.

Vediamo dunque che l'insieme $S = \{S_a\}_{a \in A}$ (l'insieme di sotto insiemi) è una partizione di $A \times B$. Quindi per il lemma-x abbiamo che:

$$|A \times B| = \sum_{a \in A} |S_a| = \sum_{a \in A} |B| = |A| \cdot |B|. \blacksquare$$

Proposizione 6.3. *Per ogni $n \geq 1$, per tutti gli insiemi $A_1, A_2, \dots, A_{n-1}, A_n$ vale che:*

$$|A_1 \times A_2 \times \dots \times A_{n-1} \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_{n-1}| \cdot |A_n|$$

Dimostrazione 6.5. Dimostriamo questa proprietà per induzione.

1. Caso base: prendiamo $n = 1$, quindi $|A_1| = |A_1|$ verifica quindi la proprietà. Mentre se prendiamo $n = 2$, abbiamo che $|A_1 \times A_2| = |A_1| \cdot |A_2|$ che anche è dimostrata perché $|A_1| \cdot |A_n| = |A_1| \cdot |A_2|$.

2. Passo induttivo: Ora per induzione prendiamo come vera $P(n)$ e dimostriamo $P(n+1)$. Per dimostrare il passo induttivo ricordiamo che (a) $A \times B \times C \cong (A \times B) \times C$ e che (b) due insiemi hanno una biezione se e solo se hanno la stessa cardinalità.

$P(n+1) = |A_1 \times A_2 \times \dots \times A_n \times A_{n+1}|$ applicando la proprietà (a) e (b) riscritte sopra otteniamo $|(A_1 \times A_2 \times \dots \times A_n) \times A_{n+1}|$ se poi scriviamo che $B = (A_1 \times A_2 \times \dots \times A_n)$ abbiamo che $|B \times A_{n+1}|$ che per caso base è uguale a $|B| \cdot |A_{n+1}| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_{n+1}|$. Abbiamo così concluso la dimostrazione ■.

Esempio 6.3. Un esempio di cardinalità di prodotti cartesiani sono le targhe delle macchine italiane. Le targhe hanno un formato XXCCCXX dove X è l'alfabeto (esclusi I,O,Q,U) e C sono le 10 cifre decimali. Quindi $|X| = 22$ e $|C| = 10$. L'insieme delle possibili targhe di calcola dunque facendo $X \cdot X \cdot C \cdot C \cdot C \cdot X \cdot X = 22 \cdot 22 \cdot 10 \cdot 10 \cdot 10 \cdot 22 \cdot 22$.

Corollario 6.2. Sia A^n l'insieme delle sequenze di lunghezza n su un insieme A . La sua cardinalità è $|A^n| = |A|^n$

Esempio 6.4. Esempio con la sequenza di caratteri ASCII esteso, di lunghezza n : con $A = 256$, quindi $|A^n| = 256^n$.

Esempio 6.5. Esempio con sequenza binaria di lunghezza n : con $A = \{0, 1\} = 2$, abbiamo $|2^n| = 2^n$. Possiamo calcolare $|2^n|$ anche induttivamente. Sia $B(n)$ il numero di sequenze binarie di lunghezza n .

- Caso base: $B(0) = 1$, la sequenza vuota.
- Passo induttivo: Ogni sequenza binaria di lunghezza $n+1$ è ottenuta aggiungendo 0 o 1 a una sequenza di lunghezza n , quindi: $B(n+1) = 2 \cdot B(n)$.

6.2 Relazioni e cardinalità

Proposizione 6.4. Per tutti gli insiemi A, B e per tutte le relazioni $R : A \leftrightarrow B$ (quindi $R \subseteq A \times B$ e $0 \geq |R|$ ed anche $|R| \leq |A| \cdot |B|$) vale che:

- Se R è **totale** allora $|A| \leq |R|$.
Perché se è totale tutti gli elementi dell'insieme di partenza hanno almeno un collegamento con l'insieme di arrivo, perciò in R dovranno esserci almeno $|A|$ coppie ordinate o più (una per ciascun elemento di A che indica un collegamento).
- Se R è **univalente** allora $|R| \leq |A|$.
Perché sia univalente tutti gli elementi di A devono collegarsi al più con uno di B dunque al massimo ci saranno $|A|$ coppie ordinate in R e non di più (sennò ci saranno per forza ripetizioni di elementi di A).
- Se R è **surgettiva** allora $|B| \leq |R|$. Per surgettività discorso simili a quello del totale solo riferito agli elementi dell'insieme di arrivo.
- Se R è **iniettiva** allora $|R| \leq |B|$. Anche per iniettività discorso simili a quello di univalenza solo riferito all'insieme B .

Note 6.2.1. Nota anche che per far sì che la relazione R sia una funzione $|R| = |A|$ e per far sì che R sia biiezione allora $|R| = |A| \wedge |R| = |B|$ quindi $|A| = |B|$.

6.2.1 Pigeonhole Principle

Se abbiamo n piccioni e li vogliamo collocare nelle m caselle di una piccionaia, se $n > m$ allora almeno una casella conterrà due piccioni. Possiamo formalizzare questo enunciato nel seguente modo.

Definizione 6.3 (Pigeonhole Principle). Dati due insiemi P e C , se $|P| > |C|$ allora non esiste nessuna relazione $R : P \leftrightarrow C$ che sia totale e iniettiva. Infatti se esistesse una tale R , per la proposizione 6.4 avremo $|P| \leq |R|$ (R totale) e $|R| \leq |C|$ (R iniettiva), da cui $|P| \leq |C|$ per transitività, contraddicendo l'ipotesi $|P| > |C|$.

6.2.2 Regola di biiezione

Possiamo formalizzare quello scritto nella nota 6.2.1 riguardante la biiezione nel seguente corollario.

Corollario 6.3 (Regola di biiezione). Per tutti gli insiemi A, B vale che se esiste una biiezione $R : A \leftrightarrow B$ allora $|A| = |B|$.

Proposizione 6.5. Per ogni coppia di insiemi A e B vale che $|Fun(A, B)| = |B|^{|A|} = |B|^{|A|}$

Dimostrazione 6.6. Per dimostrare che $|Fun(A, B)| = |B|^{|A|}$ dimostriamo che esiste una biiezione fra $|Fun(A, B)|$ e $|B|^{|A|}$.

Fun è totale e univalente, questo vuol dire che $\forall a \in A$ f assegna esattamente 1 elemento di B .

Possiamo scrivere $f : A \rightarrow B$ come $f : a_1, a_2, a_3, \dots, a_{|A|}$ e $|B|^{|A|}$ come $b_1, b_2, b_3, \dots, b_{|A|}$.

Vediamo così che i due insiemi contengono lo stesso numero di elementi quindi può esistere una biiezione fra i due insiemi. ■

Proposizione 6.6. Per tutti gli insiemi A e per tutti i numeri naturali $n \in \mathbb{N}$ vale che; se $|A| = n$ allora $A \cong n$.

Questa proposizione è vera perché se consideriamo n come un insieme di n elementi (esempio $2 = \{0, 1\}$) avendo A la stessa cardinalità di n (ricorda che $|n| = n$) esisterà una biiezione fra i due insiemi.

Teorema 6.1. Per tutte le coppie di insiemi A e B vale che:

$$A \cong B \text{ se e solo se } |A| = |B|$$

Dimostrazione 6.7. Per dimostrare il teorema, trattandosi di un se e solo se, dobbiamo dimostrare i due versi della freccia:

- $A \cong B \implies |A| = |B|$ immediato dal corollario 6.3.
- $A \cong B \longleftarrow |A| = |B|$ assumiamo che $|A| = |B| = n$. Per la proposizione 6.6 $A \cong n$ e $B \cong n$ quindi per le proprietà della biiezione $A \cong B$. ■

6.3 Permutazioni

Fra i classici problemi del calcolo combinatorio abbiamo il caso in cui dato un insieme di n oggetti, determinare quanti "raggruppamenti" diversi si possono avere disponendoli su k posti. Da qui si possono usare formule diverse a seconda che l'ordine abbia importanza oppure no, ci possano essere ripetizioni oppure no.

Definizione 6.4 (Permutazione). *Sia A un insieme con $|A| = n$. Una **permutazione** di A è una sequenza ordinata di tutti gli elementi di A : a_0, a_1, \dots, a_{n-1} .*

Possiamo definire in maniera alternativa una permutazione di A come una funzione (una biiezione):

$$\pi : A \rightarrow n \text{ con } n = |A|$$

Infatti π mappa ogni elemento di A con la posizione in cui si trova nella permutazione, è biiezione perché le permutazioni non ammettono ripetizioni e perché le permutazioni prevedono tutti gli elementi.

Esempio 6.6. Facciamo un esempio delle possibili permutazioni di $A = \{a, b, c, d\}$, $Perm(A)$ sono: abcd - abdc - acbd - acdb - adbc - adcb - bacd - badc - bcad - bcda - bdac - bdca - ecc...

Il loro numero si calcola con $4! = 24$.

Se prendiamo un insieme $B = \{1, 2, 3, 4\}$ o $S = \{\text{cuori, quadri, fiori, picche}\}$ il numero di permutazione è sempre $4! = 24$.

Note 6.3.1. Possiamo notare dall'esempio precedente che il numero di permutazioni dipende sola dal numero di elementi. Formalmente:

$$|A| = |B| \implies |Perm(A)| = |Perm(B)|$$

E questo perché $Perm(A) \cong Bii(A, |A|) \cong Bii(B, |B|) \cong Perm(B)$

Proposizione 6.7. *Sia A un insieme di cardinalità $n > 0$. Allora ci sono esattamente*

$$P(n) = n!$$

La dimostrazione per induzione è uguale a quella del fattoriale.

6.3.1 Cardinalità delle biiezioni tra due insiemi

Come visto in precedenza le permutazioni possono essere viste come una biiezione, da questa considerazione possiamo dimostrare che:

$$Bii(A, B) = \begin{cases} 0 & \text{se } |A| \neq |B| \\ |A|! & \text{se } |A| = |B| \end{cases}$$

Possiamo infatti immaginare che partendo dal primo elemento di A , a_1 esso avrà $|A|$ possibili scelte nell'insieme di partenza con cui essere in biiezione, l'elemento a_2 invece ne avrà $|A|$ meno l'elemento scelto per a_1 quindi $|A| - 1$ e così per tutti gli elementi:

$$a_1 \rightarrow |A|, a_2 \rightarrow |A| - 1, a_3 \rightarrow |A| - 2, \dots, a_{|A|} \rightarrow 1 \quad \text{Quindi } |Bii(A, B)| = |A| \cdot |A| - 1 \cdot \dots \cdot 1 = |A|!$$

6.3.2 Anagrammi e permutazioni con ripetizioni

Esempio 6.7. Esempio di un anagramma: CERTOSA è anagramma di COSTARE.

CERTOSA ha $7! = 5040$ possibili anagrammi.

Se prendiamo invece ANNA ha 6 anagrammi:

AANN ANAN ANNA NAAN NANA NNAA

Possiamo vedere dunque che non possiamo usare la normale formula delle permutazioni, infatti $6 \neq 4! = 24$, avendo ANNA 2 caratteri ripetuti.²⁴

Proposizione 6.8 (Permutazioni con ripetizioni). *Sia $S = s_1, s_2, \dots, s_k$ una sequenza di elementi di un insieme $A = \{a_1, a_2, \dots, a_n\}$ di cardinalità n , ogni elemento di A può comparire 0 o più volte. Inoltre per ogni $i \in \{1, 2, \dots, n\}$ sia c_i il numero di volte che l'elemento a_i compare nella sequenza S . Il numero di **permutazioni con ripetizioni** della sequenza è dato da:*

$$\frac{k!}{c_1! \cdot c_2! \cdot \dots \cdot c_n!} \quad (26)$$

²⁴Ricorda che una parola non è un insieme ma è una sequenza di lettere, e può quindi contenere ripetizioni

6.4 Disposizioni

Definizione 6.5 (Disposizioni). Dato un insieme finito A con $|A| = n$ e un intero $k \leq n$, una **disposizione** degli elementi di A in k posti è una sequenza ordinata a_1, \dots, a_k .

Esempio 6.8. Se per esempio prendiamo $A = \{a, b, c, d, e\}$ e $k = 2$ (quindi 2 posti dove disporre gli elementi dell'insieme) abbiamo 20 possibili disposizioni:

ab, ae, bd, cb, da, de, ec, ac, ba, be, cd, db, ea, ed, ad, bc, ca, ce, dc, eb

Proposizione 6.9. Sia A un insieme di cardinalità $n > 0$ e k tale che $0 < k \leq n$. Allora ci sono esattamente:

$$D(n, k) = \frac{n!}{(n-k)!} \quad (27)$$

disposizioni degli elementi di A in k posti.

Questa formula è semplicemente ricavata da una permutazione al numeratore (che però da sola conterrebbe potenzialmente anche elementi in posizioni extra) e da le posizione da non conteggiare al denominatore.

Dimostrazione 6.8. Dimostriamo per induzione su k questa proprietà.

1. Caso base: Per $k = 1$ abbiamo $D(n, 1) = n = \frac{n \cdot (n-1)!}{(n-1)!}$.
2. Passo induttivo: Assumiamo vero $P(k)$ e dimostriamo $P(k+1)$. Quindi $D(n, k) = \frac{n!}{(n-k)!}$ la consideriamo vera mentre noi dobbiamo dimostrare: $D(n, k+1) = \frac{n!}{(n-(k+1))!}$

$$D(n, k+1) = \frac{n!}{(n-k)!} \cdot (n-k) = \frac{n!}{(n-(k+1))!}.$$

(Perché andando ad aggiungere un posto "k+1" dovremo mantenere una posizione in più nella permutazione nel quale si sceglierà fra n-k elementi).■

6.5 Combinazioni

Definizione 6.6 (Combinazioni). Sia A un insieme di cardinalità n e sia $k \leq n$ un numero naturale. Una **combinazione** di k elementi di A è un k -insieme di A , cioè un sottoinsieme di A di cardinalità k . L'insieme di tutte le combinazioni di k elementi di A è quindi denotato con $\mathcal{P}_k(A)$.

Esempio 6.9. Prendiamo per esempio l'insieme $A = \{a, b, c, d, e\}$, le 10 combinazioni possibili sono: abc, abe, ace, bcd, bde, abd, acd, ade, bce, cde.

Note 6.5.1. Nota che nelle combinazioni non ci interessa l'ordine degli elementi $\{a, b, c\} = \{c, b, e\}$.

Definizione 6.7 (Coefficiente binomiale). Dato un insieme A di cardinalità n , il numero di combinazioni di k elementi è chiamato **coefficiente binomiale**.

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \quad (28)$$

Per giustificare questa formula partiamo dal fatto che per disporre n elementi in k posti si deve applicare una disposizione del tipo $D(n, k) = \frac{n!}{(n-k)!}$, essendo una disposizioni però teniamo conto della posizione degli elementi, andando così a creare più possibilità rispetto alle combinazioni dove non teniamo conto delle posizioni. Per eliminare dunque le possibilità extra andiamo a dividere per le permutazioni degli n elementi $P(n) = n!$ otteniamo dunque:

$$\binom{n}{k} = \frac{D(n, k)}{P(n)} = \frac{\frac{n!}{(n-k)!}}{n!} = \frac{n!}{k! \cdot (n-k)!}$$

Dimostrazione 6.9. Dimostrazione per induzione del coefficiente binomiale:

1. Caso base: Definiamo due casi base.

$$\binom{n}{0} = \frac{n!}{0! \cdot n!} = 1 \quad \text{e} \quad \binom{n}{n} = \frac{n!}{n! \cdot 0!} = 1$$

2. Passo induttivo: Prendiamo come vera l'ipotesi induttiva $P(k)$ e dimostriamo $P(k+1)$. Dobbiamo dunque dimostrare la validità della formula:

$$\begin{aligned} & \frac{n!}{(k+1)! \cdot (n-(k+1))!} \\ \binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \text{ (Spiegazioni della formula usata su dispense).} \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \left(\frac{1}{k} + \frac{1}{n-k} \right) \text{ (Raccogliamo le due frazioni).} \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \frac{n}{k(n-k)} = \frac{n!}{k!(n-k)!} \text{ (Risolviamo l'equazione). } \blacksquare \end{aligned}$$

Esempio 6.10. Calcoliamo le combinazioni di 3 elementi di $A = \{a, b, c, d, e\}$.

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5!}{3!2!} = \frac{20}{2} = 10$$

6.6 Contare sui grafi

6.6.1 Grafi non orientati

Partiamo ponendoci una domanda. Dati i nodi $\{1, 2, \dots, n\}$, quanti grafi diversi possiamo comporre? Chiamiamo G_n l'insieme di grafi con n nodi, quindi quello che cerchiamo è la sua cardinalità. Per riuscire a contare tutte le possibilità dobbiamo considerare quanti grafi possono esistere dando un numero di archi.

Esempio 6.11. Prendiamo $n = 3$ nodi e calcoliamo:

Quanti grafi esistono con 0 archi? Esiste 1 grafo.

Se invece vogliamo quanti grafi esistono con 1 arco questi sono 3.

Possiamo continuare fino ad il caso con 3 archi perché andando a tutti le casistiche con archi > 3 abbiamo che non esistono grafi.

Possiamo notare che nel caso di $n = 3$ nodi e 0 archi il calcolo si basa su fare $\binom{n}{0}$ mentre per $n = 3$ e 3 archi abbiamo $\binom{n}{1}$, così anche per tutti i casi con numero di archi minori o uguali a n . Vediamo dunque che il modo di calcolare il numero di grafi con n nodi è:

$$|G_n| = \sum_{i \in \{0, \dots, m_{max}\}} \binom{m_{max}}{i} \text{ con } m_{max} = \frac{n(n-1)}{2} \text{ il numero massimo di archi}$$

Esiste però un metodo alternativo per contare i grafi dati n nodi, e si passa su valutare, per ogni arco se includerlo oppure no, infatti da questo ragionamento vediamo che per ogni arco abbiamo due scelte, da qui possiamo vedere che per calcolare tutte i grafi possibili basta fare 2^m con $m = \frac{n(n-1)}{2}$.

Il conteggio di tutti i possibili sottoinsiemi di m elementi è anche noto come insieme delle parti, questo ci aiuta anche a dimostrare che:

$$\mathcal{P}(m_{max}) = \sum_{i \in \{0, \dots, m_{max}\}} \binom{m_{max}}{i} = 2^{m_{max}}$$

Come conseguenza possiamo notare che c'è una biezione fra $\mathcal{P}(m_{max}) \cong \text{fun}(m_{max}, 2) \cong \{0, 1\}^{m_{max}}$. E vediamo anche due proprietà del coefficiente binomiale che vengono di conseguenza:

$$\sum_{i \in \{0, \dots, k\}} \binom{k}{i} = 2^k, \text{ e quindi } \forall k > 0, i \geq 0 \binom{k}{i} < 2^k$$

6.6.2 Grafi orientati

Per i grafi orientati possiamo usare la stessa logica, l'unica cosa è che dobbiamo contare ogni arco due volte, avendo per ogni 2 nodi due possibili archi che li collegano, e dobbiamo anche considerare i cappi; questo vuol dire che abbiamo n^2 possibili archi.

Teorema 6.2. Esistono $2^{\frac{n(n-1)}{2}}$ grafi non orientati su n nodi, e 2^{n^2} grafi orientati su n nodi.