

# Cap 1 Il linguaggio degli insiemi

## 1.1 INSIEMI

Tutta la matematica è un insieme e si compone principalmente di 3 concetti primitivi:

insieme, elemento e appartenenza.

Intuitivamente un insieme è una collezione di oggetti, detti elementi appartenenti all'insieme. Come si scrive:

$$A := \{1, 2, 3\}$$

Oss. In un insieme l'ordine non conta quindi  $\{1, 2\} = \{2, 1\}$

Due insiemi sono uguali se contengono gli stessi elementi.

Oss. In un insieme non ci sono ripetizioni infatti  $\{1, 2, 2\}$  non è un insieme.

L'insieme vuoto si indica con  $\emptyset$  è l'insieme che non ha elementi, si può indicare anche con  $\{\}$ .

Notazione

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Z} := \{0, -1, 1, -2, 2, \dots\}$$

$$\mathbb{Q} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

$$\text{se } a \in \mathbb{N} \text{ allora } [a] := \{0, 1, 2, \dots, a\}$$

$A := \{\dots\}$  oppure  $A \stackrel{\text{def}}{=} \{\dots\}$  sto definendo

$A$  come l'insieme che sta alla sua destra.

Si  $P$  una proprietà che un elemento

può avere o meno. Allora:

$$A := \{x : x \text{ ha } P\}.$$

Ciò significa che  $A$  è l'insieme di tutti gli elementi  $x$  che soddisfano la proprietà  $P$ .

## 1.2 OPERAZIONI TRA INSIEMI

Siano  $A, B$  insiemi,

**Def.** Si dice  $A$  sottoinsieme di  $B$  ( $A \subseteq B$ )

se ogni elemento di  $A$  appartiene anche a  $B$ .

Scriviamo  $A \subsetneq B$  per dire che  $A \subseteq B$

e  $A \neq B$ .

**Oss.**  $A \subseteq B$  e  $B \subseteq C \Rightarrow A \subseteq C$

**Oss.**  $A = B \Leftrightarrow (A \subseteq B \text{ e } B \subseteq A)$

**Def.** L'unione  $A \cup B$  è ancora un insieme e si scrive  $A \cup B$

$$A \cup B := \{x : x \in A \circ x \in B\}$$

Def. L'intersezione  $A \cap B$  è dunque un insieme e si scrive  $A \cap B$

$$A \cap B := \{x : x \in A \text{ e } x \in B\}$$

Prop. 1.2.1.

Siano  $A, B, C$  insiemi allora:  
proprietà distributiva:

$$1) A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$2) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

proprietà associativa:

$$3) (A \cap B) \cap C = A \cap (B \cap C)$$

$$4) (A \cup B) \cup C = A \cup (B \cup C)$$

Per evitare paradossi si assume l'esistenza di un insieme universo ( $U$ ) di cui tutti gli insiemi sono sottoinsiemi. Sia  $A$  un insieme.

Def. Il complementare di  $A$  è l'insieme  $A' := \{x \in U : x \notin A\}$  (si scrive anche  $C.A.$ )

Prop. 1.2.2. Siano  $A, B$  insiemi allora  $(A \cup B)' = (A') \cap (B')$  e  $(A \cap B)' = (A') \cup (B')$ . Queste sono dette le leggi di De Morgan.

Def. La differenza di A e B è la seguente

$$A \setminus B := \{x \in A : x \notin B\}$$

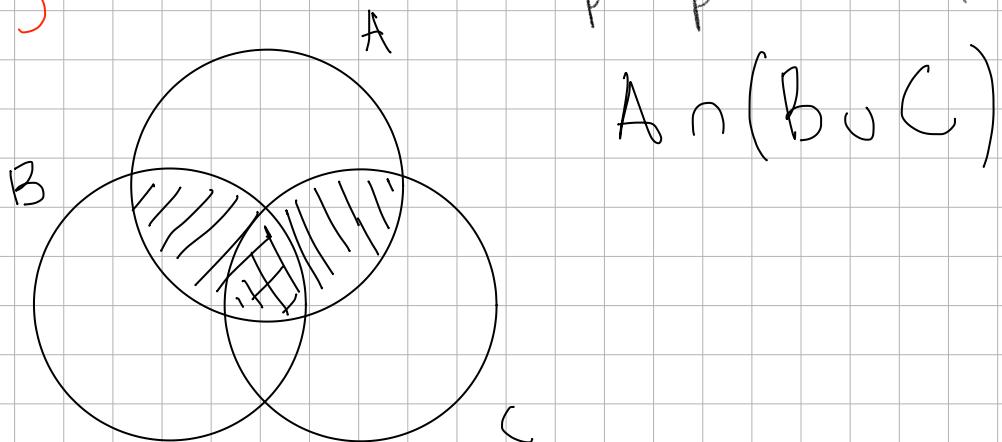
Def. La differenza simmetrica di A e B è la seguente

$$A \Delta B := (A \setminus B) \cup (B \setminus A)$$

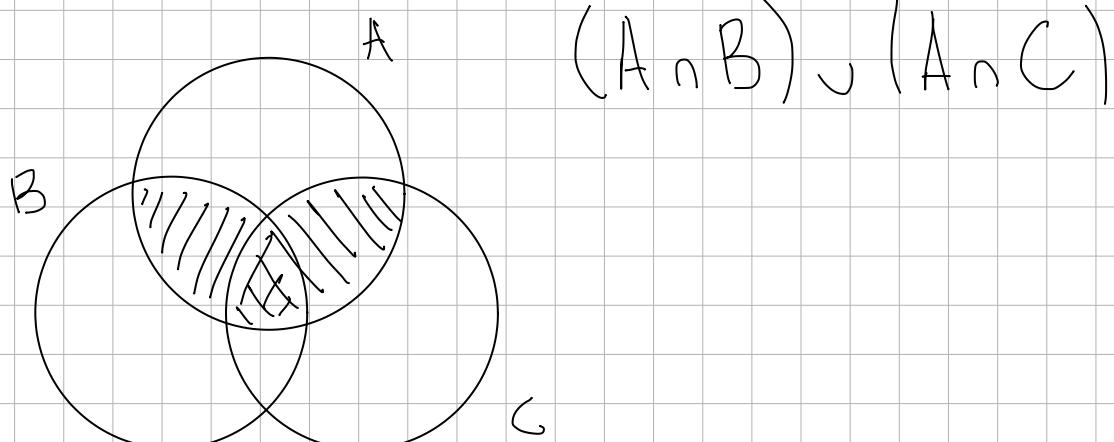
Diagrammi di Venn

Si rappresenta ogni insieme con i punti racchiusi da una curva chiusa

E.g. dimostrazione proprietà distributiva



$$A \cap (B \cup C)$$



$$(A \cap B) \cup (A \cap C)$$

Tavole di Verità

$x \in U$  allora

$0 \times e$	A	$0 \times \notin$	A
$0 \times e$	B	$0 \times \notin$	B
$0 \times e$	C	$0 \times \notin$	C

$$AB \subset A \cap B \quad A \cap C \quad (A \cap B) \cup (A \cap C) \quad B \cup C \quad A \cap (B \cup C)$$

1	1	1	1	1	1	1	1
1	1	0	1	0	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	0	0	0	0
0	1	1	0	0	0	1	0
0	1	0	0	0	0	1	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Le colonne di  $A \cap (B \cup C)$ ,  $(A \cap B) \cup (A \cap C)$  sono uguali; quindi i due insiemi sono uguali.

E' importante notare che Tavoli di Verita', dimostra, non aiuta intuizione. Diagramma di Venn, aiuta intuizione, non dimostra. Ragionamento, dimostra, ma ha bisogno dell'intuizione.

Siano A, B insiemi.

Def. Il prodotto cartesiano di  $A$  e  $B$  è

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

La coppia  $(a, b)$  è una coppia ordinata:

$$\{\{a\}, \{a, b\}\}$$

Oss.  $(1, 2) \neq (2, 1)$

E. g.  $\begin{bmatrix} 2 \\ \text{insieme } J_2 = \{1, 2\} \end{bmatrix} \times \begin{bmatrix} 3 \\ \text{insieme } J_3 = \{1, 2, 3\} \end{bmatrix} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$

Prop 1.2.3.  $A, B, C$  insiemi allora

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

Notazione

$$\mathbb{N} := \{1, 2, 3, \dots\} \text{ numeri interi positivi}$$

Sia  $A$  un insieme

Def. L'insieme delle parti di  $A$  (o insieme potenza) è l'insieme  $P(A) := \{B : B \subseteq A\}$

E. g.

$$P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

insieme i quali elementi sono tutti sottinsiemi

### 1.3 FUNZIONI

Siano  $A, B$  insiemi

Def. Una funzione (o applicazione o mappa)

f da  $A$  in  $B$  (scritto  $f: A \rightarrow B$ ) è un sottinsieme

$f \subseteq A \times B$  (prodotto cartesiano) tale che:

$\forall a \in A \Rightarrow \exists! b \in B$  tale che  $(a, b) \in f$   
Scriviamo allora  $f(a) = b$ .

Intuitivamente è una legge che ad ogni elemento di  $A$ , associa un elemento di  $B$  uno ed uno solo.

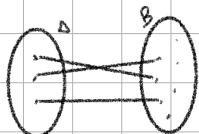
### Notazione

$\forall$  = per ogni,  $\exists$  = esiste,  $\nexists$  = non esiste,  
 $\exists!$  = esiste un unico

Sia  $f: A \rightarrow B$

Def.  $f$  è iniettiva se

$$(x, y) \in A, x \neq y \Rightarrow f(x) \neq f(y)$$

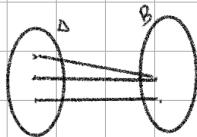


(2 elementi di  $A$  diversi corrispondono elementi di  $B$  diversi)

Def.  $f$  è suriettiva se

$$\forall b \in B \Rightarrow \exists a \in A$$
 tale che  $f(a) = b$

(ogni elemento di  $B$  corrisponde ad almeno un elemento di  $A$ )

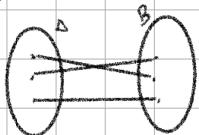


Def.  $f$  è biunivoco se  $f$  è iniettiva e suriettiva

Sia  $X \subseteq A$

Def. L'immagine di  $X$  tramite  $f$  è un insieme:

$$f(X) := \{f(a) : a \in X\}$$
 applico  $f$  a tutti gli elementi di  $X$  - vari elementi di  $B$



S.2  $y \in B$

Def. La controimmagine (o retroimmagine) di  $Y$  tramite  $f$  è:

$$f^{-1}(Y) := \{a \in A : f(a) \in Y\} \text{ elementi di } A \text{ che } f \text{ manda dentro } Y$$

Oss.  $f(\emptyset) = \emptyset, f^{-1}(\emptyset) = \emptyset$

Siano  $A, B, C$  insiemi e  $f: A \rightarrow B$  e  $g: B \rightarrow C$

Def. La composizione di  $f$  e  $g$  è una funzione

$g \circ f: A \rightarrow C$  definita ponendo

$$(g \circ f)(a) := g(f(a)), \forall a \in A$$

Prop 1.3.1. Siano  $A, B, C, f$  e  $g$  come sopra,

allora:

1) se  $f$  e  $g$  iniettive  $\Rightarrow g \circ f$  è iniettiva

2) se  $f$  e  $g$  suriettive  $\Rightarrow g \circ f$  è suriettiva

3) se  $f$  e  $g$  bivinuocche  $\Rightarrow g \circ f$  è bivinuoca

Def. L'identità di un insieme  $A$  è la funzione

$Id_A: A \rightarrow A$  definita ponendo  $Id_A(a) := a$

$\forall a \in A$  (si scrive anche  $I_A$ )

Notazione A' insieme allora

$$\bar{A} := A'$$

S.2  $f: A \rightarrow B$ ,  $f$  bivinuoca

Def. L'inversa di  $f$  è la funzione

$f^{-1}: B \rightarrow A$  definita da

$$f^{-1} := \{ (b, a) \in B \times A : (a, b) \in f \}$$

Oss. quindi

$$f(a) = b \iff f^{-1}(b) = a$$

Siano  $f, g: A \rightarrow B$

Def.  $f$  e  $g$  si dicono uguali, scritto  $f = g$   
se  $f(a) = g(a) \quad \forall a \in A$

Prop. 1.3.2 Siano  $f, g, h: A \rightarrow A$  allora

$$1) f \circ g : A \rightarrow A$$

$$2) (f \circ g) \circ h = f \circ (g \circ h)$$

$$3) f \circ \text{Id}_A = \text{Id}_A \circ f = f$$

$$4) f \text{ biunivoca} \Rightarrow f \circ f^{-1} = f^{-1} \circ f = \text{Id}_A$$

Sia  $n \in \mathbb{N}$

Def. il gruppo simmetrico (di rango  $n$ ) è

$$S_n := \{ f: [n] \rightarrow [n] : f \text{ biunivoca} \}$$

Gli elementi di  $S_n$  si dicono permutazioni

Sia  $f \in S_n$  scriviamo

$$f = a_1, a_2, \dots, a_n \text{ per dire } f(1) = a_1, f(2) = a_2, \dots$$

dove  $a_i := f(c)$   $\forall i \in [n]$

E.g.  $S_3 = \{123, 132, 213, 231, 312, 321\}$

Oss. Se  $f, g \in S_n$ ,  $f = a_1 \dots a_n$ ,  $g = b_1 \dots b_n$  allora  
 $f \circ g = a_{b_1} \dots a_{b_n}$

E.g.  $n=3$ ,  $f = 123436$   $g = 234165$

$$f \circ g \stackrel{\text{indice posizione}}{=} 165234 \quad e \quad g \circ f = 5217436$$

Oss. Se  $f \in S_n$ ,  $f = a_1 \dots a_n$  allora

$f^{-1} = b_1 \dots b_n$  dove  $b_i$  è la posizione di  $i$  in  $a_1 \dots a_n$  ( $\forall i \in [n]$ )

E.g.  $n=3$ ,  $f = 123436$  allora  
 $f^{-1} = 246531$

in effetti:

$$f \circ f^{-1} = 1234567, \quad f^{-1} \circ f = 1234567$$

Prop. 1.3.3 se  $f: A \rightarrow B$  e se  $X, Y \subseteq B$  allora

$$1) f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$$

$$2) f^{-1}(X \cap Y) \subseteq f^{-1}(X) \cap f^{-1}(Y)$$

Oss. sia  $f: A \rightarrow B$ ,  $f$  bivinolare e  $Y \subseteq B$

Allora:

$f^{-1}(Y)$  ha due significati:

controimmagine di  $Y$  tramite  $f$  e immagine di  $Y$  tramite  $f^{-1}$ , ma il risultato non cambia.

## 1.4 RELAZIONI

Siano  $A, B$  insiemi

Def. una relazione tra  $A$  e  $B$  è un sottoinsieme  $R \subseteq A \times B$  se  $(a, b) \in R$

scriviamo  $a R b$  (lettura "2 è in relazione  $R$  con b")

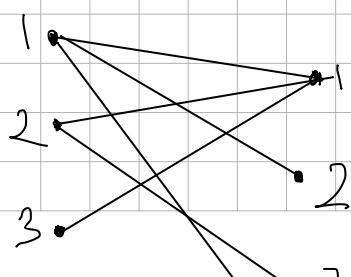
se  $A = B$  si dice che  $R$  è una relazione su  $A$ .

Oss. Una funzione  $f: A \rightarrow B$  è una relazione tra  $A$  e  $B$ .

E.g.  $A = [5]$ ,  $B = [4]$ ,

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

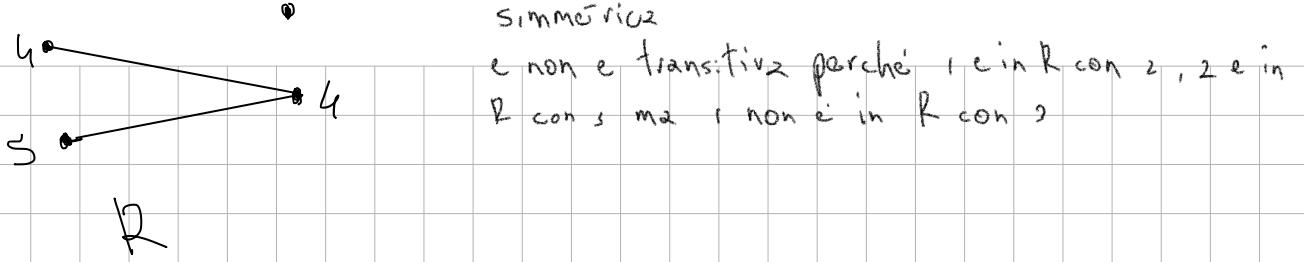
posso rappresentare  $R$  graficamente  
in questo modo



fare finta che  $B$  sia  $[5]$ :

2 non è in relazione con 2 quindi non è riflessiva

3 è in  $R$  con 1 ma 1 non lo è con 3 quindi non è simmetrica



$\exists$ :  $R$  una relazione su  $A$ .

Def.

- 1)  $R$  è riflessiva se  $(a, a) \in R$  per  $\forall a \in A$ ;
- 2)  $R$  è simmetrica se per  $\forall a, b \in A$  vale che  $(a, b) \in R \Rightarrow (b, a) \in R$
- 3)  $R$  è transitiva se per  $\forall a, b, c \in A$  vale che  $(a, b) \in R \text{ e } (b, c) \in R \Rightarrow (a, c) \in R$

Def.  $R$  si dice una relazione di equivalenza

se  $R$  è riflessiva, simmetrica e transitiva.

$\exists$ :  $R$  di equivalenza, sia  $a \in A$ .

Def. La classe di equivalenza di  $a$  rispetto a  $R$  è

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

Prop. 1.4.1.  $\exists$ :  $R$  di equivalenza su  $A$ , e siano  $a, b \in A$ , allora  $[a]_R = [b]_R \Leftrightarrow [a]_R \cap [b]_R = \emptyset$

Def. Una partizione (o partizione insiemistica)

di  $A$  è un insieme:  $\Pi := \{B_1, \dots, B_K\} (K \in \mathbb{P})$

tale che:

- 1)  $B_i \subseteq A$  e  $B_i \neq \emptyset$  per  $\forall i = 1, \dots, K$ ;
- 2)  $B_1 \cup \dots \cup B_K = A$ ;

3)  $B_i \cap B_j = \emptyset$  per  $\forall 1 \leq i, j \leq k, i \neq j$ .

$B_1, \dots, B_k$  si dicono i **blockhi** di  $\Pi$ . e si dice che  $\Pi$  ha  $k$  blockhi.

E.g.  $A = [9]$  allora

$$\Pi = \{\{1, 4\}, \{5\}, \{2, 6, 9\}, \{3, 7, 8\}\}$$

è una partizione di  $[9]$  in 4 blockhi.

Oss. Sia  $\Pi$  una partizione di  $A$ . Definiamo una relazione  $R$  su  $A$  ponendo

$aRb \Leftrightarrow aeb \in$  allo stesso blocco di  $\Pi$   
allora  $R$  è di equivalenza.

Prop. 1.4.2. Sia un insieme  $\mathcal{R}$  una relazione di equivalenza su  $A$  allora le classi di equivalenza rispetto ad  $\mathcal{R}$  sono una partizione di  $A$ .

E.g. Definiamo una relaz. su  $\mathbb{Z}$  ponendo

$$mRn \Leftrightarrow 3 \mid (m-n) \quad \text{cioè } \exists k \in \mathbb{Z} \text{ tale che} \\ \text{divide} \quad m-n = 3 \cdot k$$

$\forall m, n \in \mathbb{Z}$ . Allora  $R$  è di equiv.

Sia  $m \in \mathbb{Z} \Rightarrow m-n=3 \cdot 0 \Rightarrow mRn \Rightarrow R$  è riflessiva

Siano  $m, n \in \mathbb{Z}$  tali che  $mRn \Rightarrow \exists k \in \mathbb{Z}$  tale che

$$m-n=3 \cdot k \Rightarrow n-m=3 \cdot (-k) \text{ e } -k \in \mathbb{Z} \Rightarrow 3 \mid (n-m)$$

$\Rightarrow nRm$ . Quindi è simmetrica

Siano  $m, n, p \in \mathbb{Z}$  tali che  $mRn$  e  $nRp \Rightarrow$   
 $\exists k, l \in \mathbb{Z}$  tali che  $m-n=3k$  e  $n-p=3l \Rightarrow$   
 $m-p=m-n+n-p=3k+3l=3(k+l)$  e  $k+l \in \mathbb{Z} \Rightarrow pRm$ .

Quindi è transitiva.

Che sono le classi di equivalenza?

Abbiamo che

$$\begin{aligned}[0]_R &= \{ m \in \mathbb{Z} : 0Rm \} = \{ m \in \mathbb{Z} : 3 \mid (m-0) \} \\ &= \{ m \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tale che } m=3k \} \\ &= \{ 0, 3, -3, 6, -6, 9, -9, \dots \}\end{aligned}$$

$$\begin{aligned}[1]_R &= \{ m \in \mathbb{Z} : 1Rm \} \\ &= \{ m \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tale che } m-1=3k \} \\ &\approx \{ 3k+1 : k \in \mathbb{Z} \} \\ &\approx \{ 1, 4, -2, 7, -5, \dots \}\end{aligned}$$

$$\begin{aligned}[2]_R &= \{ m \in \mathbb{Z} : 2Rm \} \\ &= \{ m \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tale che } m-2=3k \} \\ &= \{ 3k+2 : k \in \mathbb{Z} \} \\ &= \{ 2, 5, -1, 8, -4, \dots \}\end{aligned}$$

In generale otteniamo

$$[-]_R = \{ 3k+i : k \in \mathbb{Z} \} \quad \text{quindi}$$

$$[0]_R = [3]_R = [-3]_R = [6]_R = [-6]_R$$

$$[1]_R = [4]_R = [-2]_R = [7]_R = [-5]_R$$

$$[2]_R = [5]_R = [-1]_R = [8]_R = [-4]_R$$

$A$  = insieme,  $R$  = relazione di equivalenza su  $A$ .

$a, b \in A$ ,

Oss  $a R b \iff [a]_R = [b]_R$

## Cap 2 Logica

### 2.1 PROPOSIZIONI

Una proposizione è un'affermazione che può essere vera o falsa

E.g.  $2 + 3 = 5$  è una proposizione

$2 \cdot 3 = 5$  è una prop.

Dove vai? non è una prop.

### 2.1 PROPOSIZIONI COMPOSTE

Così vogliono dire esattamente?

Queste prop. sono formate da prop più semplici collegate tra loro da connettivi logici come "e", "o" e "Se ... allora".

Sia  $P$  una prop.

Def. La negazione di  $P$ , è la proposizione

$\neg P$  (lett "non  $P$ ") definita ponendo:

$P$	$\neg P$
V	F
F	V

Siano  $P$  e  $Q$  prop.

Def. La congiunzione di  $P$  e  $Q$  è la prop.

$P \wedge Q$  (lett "P e Q") definita da:

$P$	$Q$	$P \wedge Q$	and
V	V	V	
V	F	F	
F	V	F	
F	F	F	

Def. La disgiunzione di  $P$  e  $Q$  è la prop.

$P \vee Q$  (lett "P o Q") definita da:

$P$	$Q$	$P \vee Q$	or
V	V	V	
V	F	V	
F	V	V	
F	F	F	

Def. La disgiunzione esclusiva di  $P$  e  $Q$  è la prop.

$P \circ Q$  (lett "P per o Q") definita da:

$P$	$Q$	$P \circ Q$	entrambe diverse
V	V	F	
V	F	V	
F	V	V	
F	F	F	

Def. L' implicazione da  $P$  a  $Q$  è la prop.

$P \rightarrow Q$  (lett. "P implica Q" o "se P allora Q") definita da:

P	Q	$P \rightarrow Q$	tranne se P è vera e Q è falsa
V	V	V	1
V	F	F	2
F	V	V	3
F	F	V	4

Def. L'equivalenza logica di P e Q è la prop.

$P \leftrightarrow Q$  (lett. "P se e solo se Q") definita da:

P	Q	$P \leftrightarrow Q$	o entrambe vere o entrambe false Scritto anche $P = Q$ e si dice che P e Q sono logicamente equivalenti
V	V	V	
V	F	F	
F	V	F	
F	F	V	

E.g. le prop. " $x^2 \geq 4$ " e " $|x| \geq 2$ " sono

logicamente equivalenti (non è mai vero che  
una è vera e l'altra è falsa)

E.g. " $P \rightarrow Q$ " e " $\neg Q \rightarrow \neg P$ " sono equiv.?

P	Q	$\neg P$	$\neg Q$	$P \rightarrow Q$	$\neg Q \rightarrow \neg P$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

Le colonne sono uguali

E.g. " $(P \rightarrow Q) \wedge (Q \rightarrow P)$ " e " $P \leftrightarrow Q$ "

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	$P \leftrightarrow Q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

colonne uguali.

## 2.3 LEGGI DISTRIBUTIVE E DI DE MORGAN

Siano  $P$  e  $Q$  prop.

Prop. 2.3.1: Abbiamo che: leggi di De Morgan

$$\neg(P \wedge Q) = (\neg P) \vee (\neg Q) \quad \text{e} \quad \neg(P \vee Q) = (\neg P) \wedge (\neg Q)$$

Sia  $R$  una prop.

Prop. 2.3.2: Abbiamo che

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$$

$$\text{e} \quad P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$$

leggi distributive

## 2.5 PREDICATI

Un predicato è una prop. la cui verità o falsità dipende da una (o più) variabili.

Si scrive:  $P(x, y, \dots)$  dove  $x, y, \dots$  sono le variabili.

Eg.  $P(n) = "n \text{ è primo}"$  ( $n \in \mathbb{P}$ )

$P(u)$  è falso,  $P(s)$  è vero

Eg.  $Q(n) = "n \text{ è un quadrato perfetto}"$  ( $n \in \mathbb{P}$ )

$Q(u)$  è vero,  $Q(s)$  è falso

In logica e informatica (come in matematica)

si usano i simboli:

" $\forall$ " significa "per ogni"

" $\exists$ " significa "esiste"

Quindi

" $\forall n. P(n)$ " significa "per ogni  $n$   $P(n)$  è vera"

" $\exists n. P(n)$ " significa "esiste (almeno) un  $n$  tale che  $P(n)$  è vera"

E' importante rendersi conto che

" $\neg(\forall n. P(n))$ " è equivalente a " $\exists n. \neg P(n)$ "

e " $\neg(\exists n. P(n))$ " è equivalente a " $\forall n. \neg P(n)$ "

### Cap 3. Numeri

#### 3.1 IL PRINCIPIO DI INDUZIONE

In matematica ci sono 3 modi per dimostrare un'implicazione  $A \rightarrow B$ :

1) Dimostrazione diretta

Il ragionamento che mostra che se  $A$  è vero allora necessariamente è vero anche  $B$ .

2) Dimostrazione per assurdo

Supponendo vere  $A$  e  $\neg B$  si deduce una contraddizione

### 3) Il principio di induzione matematica

Sia  $P(n)$  un predicato in cui  $n \in \mathbb{P}$ .

Supponiamo che:

-  $P(1)$  è vero

- se  $n \in \mathbb{P}$  allora  $(P(n) \rightarrow P(n+1))$  è vero

allora  $P(n)$  è vero  $\forall n \in \mathbb{P}$

### Principio di induzione completa

Sia  $P(n)$  come sopra, supponiamo che:

-  $P(1)$  è vero

- se  $n \in \mathbb{P}$  allora  $((P(1) \wedge P(2) \wedge \dots \wedge P(n)) \rightarrow P(n+1))$  è vero

allora  $P(n)$  è vero  $\forall n \in \mathbb{P}$

### Notazione

Siano  $a_0, a_1, \dots, a_n \in \mathbb{R}$  allora:

$$\sum_{i=0}^n a_i \text{ significa } a_0 + a_1 + \dots + a_n$$

E.g. Dimostrare che

$$\sum_{i=1}^n i = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{P}$$

-  $P(1)$  è vero

$$\sum_{i=1}^1 i = \frac{1(1+1)}{2} \Rightarrow P(1) \text{ è vero}$$

$P(n) \rightarrow P(n+1)$  è vero  $\forall n \in \mathbb{R}$ ?

Sia  $n \in \mathbb{P}$ . Sia  $P(n)$  vero allora

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}$$

quindi

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^n i + (n+1) = \text{sostituire } n \text{ con } n+1 \Rightarrow$$

$$\frac{(n+2)(n+1)}{2} \Rightarrow P(n+1) \text{ è vero}$$

quindi  $P(n)$  è vero  $\forall n \in \mathbb{R}$

### 3.2 IL PRINCIPIO DEL BUON ORDINAMENTO

Princípio del buon ordinamento (WOP)

(Well ordered principle)

\* Sia  $S \subseteq \mathbb{P}$  allora  $\exists m \in S$  tale che  $m \leq x \quad \forall x \in S$

Oss. WOP è falso per  $\mathbb{Z} (S = \{-1, -2, -3\})$  non ha un minimo)

Oss. WOP è falso per  $\mathbb{Q}_{>0} (= \{\alpha \in \mathbb{Q} : \alpha > 0\})$

( $S = \left\{ \frac{1}{2}, \frac{1}{3}, \dots \right\}$  non ha un minimo)

\* ogni sottoinsieme degli intui positivi ha un minimo

Teo. 3.2.1

Principio di induzione  $\Leftrightarrow$  NoP  
matematica

### 3.3 NUMERI COMPLESSI

Notazione

$$\mathbb{R} := \{ \text{numeri reali} \}$$

$$\mathbb{C} := \{ \text{numeri complessi} \}$$

$$(= \{ a+ib : a, b \in \mathbb{R} \}) \quad (i := \sqrt{-1})$$

Sia  $z \in \mathbb{C}$ ,  $z = a+ib$  ( $a, b \in \mathbb{R}$ )

Def.  $a$  si dice la parte reale di  $z$ .

$b$  si dice l'immaginaria di  $z$ .

Def.  $i$  ( $i := \sqrt{-1}$ ) si dice l'unità immaginaria

Siano  $w, z \in \mathbb{C}$ ,  $z = a+ib$ ,  $w = c+id$

( $a, b, c, d \in \mathbb{R}$ )

Def. La somma di  $w$  e  $z$  è:

$$w+z := (a+c) + i(b+d)$$

Def. Il prodotto di  $w$  e  $z$  è:

$$\begin{aligned} w \cdot z &:= (a+ib)(c+id) = ac + ibc + ai \cdot d + i^2 bd = \\ &= ac + i(bc + ad) - bd \stackrel{i^2 = -1}{=} (ac - bd) + i(bc + ad) \end{aligned}$$

Def. Il complesso coniugato (o coniugato) di  $z$  è

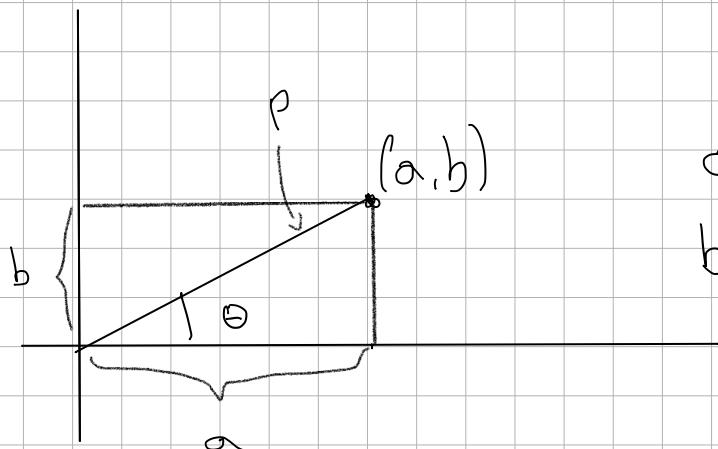
$$\bar{z} := a - bi$$

Possiamo dividere i  $z$  per  $w$ , se  $w \neq 0$   
razionalizzando

E.g.,  $z = 1 + 4i$ ,  $w = 2 + 3i$ , allora

$$\frac{z}{w} = \frac{1+4i}{2+3i} = \frac{(1+4i)(2-3i)}{(2+3i)(2-3i)} = \frac{2-8i-3i+12i^2}{4+6i-6i-9i^2} =$$
$$\frac{-10-11i}{13} = -\frac{10}{13} - i \frac{11}{13}$$

Se  $z = a + bi$



$$a = p \cos \theta$$
$$b = p \sin \theta$$

Def.  $p$  si dice il modulo di  $z$ , scritto  $\|z\|$ .

Def.  $\theta$  si dice l'argomento di  $z$

quindi  $z = p \cos \theta + i p \sin \theta = p(\cos \theta + i \sin \theta)$ ,

«FORMA POLARE DI  $z$ .

Oss.  $\|z\| = \sqrt{a^2 + b^2}$ .

Oss.  $\|z\|^2 = z \cdot \bar{z}$ .

Siano  $z, w \in \mathbb{C}$ ,  $z = p \cos \theta + i p \sin \theta$  e  
 $w = \epsilon \cos \varphi + i \epsilon \sin \varphi$  ( $\Rightarrow p, \epsilon \geq 0$  e  $\theta, \varphi \in \mathbb{R}$ ) allora  
 $zw = (p \cos \theta + i p \sin \theta)(\epsilon \cos \varphi + i \epsilon \sin \varphi) = \dots$   
 $= p\epsilon (\cos(\theta + \varphi) + i \sin(\theta + \varphi))$

### 3.4. NUMERI PRIMI E COMPOSTI

Siano  $a, b \in \mathbb{P}$ .

Def. Si dice che  $a$  divide  $b$  (o che  $b$  è multiplo di  $a$ ) se  $\exists k \in \mathbb{Z}$  tale che  $b = a \cdot k$ . (scritto  $a | b$ ).

Oss.  $a | b \Rightarrow a \leq b$

$$a | b \text{ e } b | c \Rightarrow a | c$$

$$a | b \text{ e } a | c \Rightarrow a | (c \cdot x + b \cdot y) \quad \forall x, y \in \mathbb{Z}.$$

Def. Si dicono primi i numeri  $a \in \mathbb{P}$  tali che se  $a \geq 2$  e  $a | b \Rightarrow b = 1$  o  $b = a$ .  
Altrimenti,  $a$  si dice composto.

Theo. 3.4.1 Si dicono composti i numeri  $n \in \mathbb{P}$ ,  $n \geq 2$  allora  $n$  è prodotto di numeri primi

Def.  $a$  e  $b$  sono coprimi (o primi tra loro) se  $c | a$  e  $c | b \Rightarrow c = 1$

Oss. Si sono  $p, q \in \mathbb{P}, p \neq q$ ,  $p$  e  $q$  primi allora  
 $p$  e  $q$  sono coprimi

Def. n si dice perfetto se è uguale alla  
Somma dei suoi divisori  $\neq n$ .

E.g.  $n=6$  è perfetto ( $1+2+3$ )

$n=9$  non è perfetto ( $1+3 \neq 9$ )

Teo 3.4.2 Esistono infiniti numeri primi

Sia  $n \in \mathbb{P}$  poniamo:

$$\pi(n) := |\{m \in \mathbb{P} : m \leq n, m \text{ è primo}\}|$$

E.g.

$$\pi(8) = |\{2, 3, 5, 7\}| = 4$$

( $|A|$  := numero di elementi di  $A$ )

Teorema dei numeri primi

$$\lim_{n \rightarrow +\infty} \frac{\pi(n)}{\left(\frac{n}{\ln(n)}\right)} = 1$$

### 3.5 ALGORITMO EUCLIDEO

Siano  $a, b \in \mathbb{P}$

Def. Il massimo comune divisore tra  $a$  e  $b$  è

$$\text{MCD}(a, b) := \max \{c \in \mathbb{P}, c | a \text{ e } c | b\}$$

Si scrive anche  $(a, b) \circ \text{MCD}(a, b)$

Come calcolare  $\text{MCD}(a, b)$ ?

Prop 3.5.1 Siano  $a, b \in \mathbb{P}, a \geq b$ , allora

$\exists q, r \in \mathbb{Z}$  tali che  $a = b \cdot q + r$  e  $0 \leq r < b$ .

Algoritmo euclideo

Siano  $a, b \in \mathbb{P}, a \geq b$  allora  $\exists q, r \in \mathbb{Z}$  tali che  
 $a = b \cdot q + r$  e  $0 \leq r < b$ .

Se  $r = 0 \Rightarrow \text{MCD}(a, b) = b$ ,

Se  $r > 0 \Rightarrow \exists q, r \in \mathbb{Z}$  tali che  $b = r \cdot q + r$ ,  $0 \leq r < r$

Se  $r_1 = 0 \Rightarrow \text{MCD}(a, b) = r$

Se  $r_1 > 0 \Rightarrow \exists q_2, r_2 \in \mathbb{Z}$  tali che  $r = r_1 \cdot q_2 + r_2$ ,  $0 \leq r_2 < r_1$

Se  $r_2 = 0 \Rightarrow \text{MCD}(a, b) = r_1$

Se  $r_2 > 0 \Rightarrow \exists q_3, r_3 \in \mathbb{Z}$  tali che  $r = r_2 \cdot q_3 + r_3$ ,  $0 \leq r_3 < r_2$

Se  $r_3 = 0 \Rightarrow \text{MCD}(a, b) = r_2$

Se  $r_3 > 0$  e così via.

Otteniamo quindi due sequenze di numeri

$q_1, q_2, \dots$  e  $r_1, r_2, \dots$  tali che

$b > r > r_1 > r_2 > \dots \geq 0$

Quindi  $\exists k \in \mathbb{Z}$  tale che  $r_k = 0 \Rightarrow \text{MCD}(a, b) = r_{k-1}$

E.g.  $a = 375$   $b = 45$

$$375 = 8 \cdot 45 + 15 \Rightarrow \text{MCD}(375, 45) = 15$$
$$45 = 3 \cdot 15 + 0$$

### 3.6 CONSEGUENZE DELL'A.E.

Oss. Siano  $a, b, q, r \in \mathbb{P}$  tali che

$$a = bq + r$$

e  $r > 0$  allora

$$\text{MCD}(a, b) = \text{MCD}(b, r)$$

Prop. 3.6.1 Siano  $a, b \in \mathbb{P} \Rightarrow \exists x, y \in \mathbb{Z}$  tali che

$$\text{mcd}(a, b) = a \cdot x + b \cdot y \quad \text{identità di Bezout}$$

Prop 3.6.2 Siano  $a, b \in \mathbb{P}$  allora

$$(a, b) = \min(\{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{P})$$

Prop. 3.6.3 Siano  $a, b, p \in \mathbb{P}$  tali che

$p \mid ab$  e  $p$  è primo allora  $\Rightarrow p \mid a$  o  $p \mid b$

Oss. 3.6.3 è falso, in generale se  $p$  non è primo ( $6 \mid 6 \cdot 2$ , ma  $4 \nmid 6$  e  $4 \nmid 2$ )

Oss. Similmente a 3.6.3 si dimostra che:

$$m \mid ab \text{ e } (m, a) = 1 \Rightarrow m \mid b$$

**Teo 3.6.4 (Teorema fondamentale dell'aritmetica)**

Sia  $n \in \mathbb{P}$ ,  $n \geq 2$  allora

$n$  è prodotto di numeri primi, in uno ed un solo modo, a parte l'ordine dei fattori.

E.g.

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$$

### 3.7 EQUAZIONI DIOFANTEE LINEARI

**Teo 3.7.1** Siano  $a, b, n \in \mathbb{P}$  allora  $\exists x, y \in \mathbb{Z}$  tali che:

$$a \cdot x + b \cdot y = n \quad (*)$$

Se e solo se  $(a, b) | n$

**Teo 3.7.2** Siano  $a, b, n \in \mathbb{P}$  tali che  $(a, b) | n$  allora tutte le soluzioni  $x, y \in \mathbb{Z}$  di

$$ax + by = n \leftarrow \text{eq. lineare}$$

sono della forma

$$\begin{cases} x = x_0 - \left( \frac{b}{(a, b)} \right) t \\ y = y_0 + \left( \frac{a}{(a, b)} \right) t \end{cases}$$

dove  $t \in \mathbb{Z}$  e  $x_0, y_0 \in \mathbb{Z}$  è una soluzione di (\*)

### 3.8 LE CLASSI DI RESTO

$$\begin{array}{ccccccccc} -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 \end{array} \text{ colori}$$

$$\begin{array}{ccccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \checkmark$$

3 colori

$$\begin{array}{ccccccccc} -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{array}$$

Le classi di resto sono i numeri che hanno lo stesso colore.

Sia  $n \in \mathbb{P}$ , definiamo la relazione  $\equiv_n$  su  $\mathbb{Z}$

ponendo:  $s \mid 15-10 \quad 10 \equiv_5 15$   
 $a \equiv_n b \iff n \mid (b-a) \quad \forall a, b \in \mathbb{Z}$ .

$\equiv_n$  si dice relazione di congruenza modulo  $n$

Prop 3.8.1. Sia  $n \in \mathbb{P}$ . Allora  $\equiv_n$  è di equivalenza su  $\mathbb{Z}$ .

Sia  $a \in \mathbb{Z}$  la classe di congruenza di  $a$  modulo  $n$  è la classe di equiv. di  $a$  rispetto a  $\equiv_n$ .

Quindi:

$$[a]_n := \{b \in \mathbb{Z} : a \equiv_n b\}$$

(si dice anche classe di resto di  $a$  modulo  $n$ )

$$\text{E.g. } [0]_2 = \{0, 2, -2, 4, -4, \dots\}$$

$$[1]_2 = \{1, 3, -3, -5, 5, \dots\}$$

è contenuta

$$[0]_6, \{0, 6, 12, -6, -12, \dots\} \quad (\Rightarrow [0]_6 \subseteq [0]_2)$$

$$[3]_6 = \{3, 9, 15, -3, -9, \dots\}$$

$$[8]_4 = \{8, 12, 16, -12, -16, \dots\}$$

Dato che 8 è divisibile per 4 l'8 può essere contato come 0.

$$\begin{aligned} ([8]_4 &= \{b \in \mathbb{Z} : b \equiv_4 8\} = \{b \in \mathbb{Z} : 4|(b-8)\} = \\ &= \{b \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ per cui } b-8 = 4 \cdot k\} = \{4 \cdot k + 8 : k \in \mathbb{Z}\}, \\ &= \{4 \cdot k : k \in \mathbb{Z}\} = \{8, 8+4, 8-4, 8+4 \cdot 2, 8-4 \cdot 2, \dots\} \end{aligned}$$

Oss.  $a, b, c, d \in \mathbb{Z}$  e  $n \in \mathbb{P}$ . Allora

$$a \equiv_n c \text{ e } b \equiv_n d \Rightarrow a+b \equiv_n c+d \text{ e } ab \equiv_n cd$$

Questo suggerisce e permette le seguenti definizioni.

Def. Siano  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{P}$ . La somma:

$$[a]_n + [b]_n := [a+b]_n$$

Il prodotto è:

$$[a]_n \cdot [b]_n := [ab]_n$$

$$\text{E.g. } [3]_6 + [3]_6 = [3+3]_6 = [6]_6 = [0]_6$$

$$[4]_6 \cdot [3]_6 = [4 \cdot 3]_6 = [12]_6 = [0]_6$$

$$[2]_6 + [5]_6 = [7]_6 = [1]_6$$

$$[2]_6 \cdot [5]_6 = [10]_6 = [4]_6$$

Sia  $n \in \mathbb{N}$ , si pone  $\mathbb{Z}_n$  come l'insieme delle classi di resto modulo  $n$ . Quindi:

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

Somma e prodotto tra classi di resto si comportano come le operazioni tra numeri.

E.g.  $[a]_n \cdot ([b]_n + [c]_n) = [ab]_n + [ac]_n$

$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

etc...

È presente una differenza:

$$[a]_n \cdot [k]_n = [b]_n \cdot [k]_n \text{ e } [k]_n \neq [0]_n$$

$$\Leftrightarrow [a]_n = [b]_n$$

E.g.  $[4]_6 [3]_6 = [12]_6 = [6]_6$

$$[2]_6 \cdot [3]_6 = [6]_6$$

$$[3]_6 \neq [0]_6 \text{ ma } [4]_6 \neq [2]_6$$

Oss.  $[a]_n \cdot [0]_n = [0]_n \quad \forall a \in \mathbb{Z} \text{ e } n \in \mathbb{P}$

Prop. 3.8.2 Siano  $a, b, k \in \mathbb{Z}$  e  $n \in \mathbb{P}$  tali che  $(k, n) = 1$  allora

$$[k]_n \cdot [a]_n = [k]_n \cdot [b]_n \iff [a]_n = [b]_n$$

si può cancellare  $k$  se solo se  $k$  e  $n$  sono coprimi

Sia  $a \in \mathbb{Z}$  e sia  $n \in \mathbb{P}$

Def. Un' inversa moltiplicativa di  $[a]_n$  è un' classe  $[b]_n$  tale che  $[a]_n \cdot [b]_n = [1]_n$ .

Prop. 3.8.3 Sia  $a \in \mathbb{Z}$  e sia  $n \in \mathbb{P}$  tale che  $(a, n) = 1$  allora esiste un'unica inversa moltiplicativa di  $[a]_n$ .

Siano  $[b]_n, [c]_n \in \mathbb{Z}_n$  tali che

$$[a]_n \cdot [b]_n = [1]_n \stackrel{\text{può essere ogni numero}}{=} [a]_n \cdot [c]_n$$

$$\text{ma } (a, n) = 1 \Rightarrow [b]_n = [c]_n$$

### 3.9 LA FUNZIONE DI EULERO

Sia  $n \in \mathbb{P}$

Def. La funzione di Eulero di  $n$  è

$$\Phi(n) := |\{1 \leq i < n : (i, n) = 1\}|.$$

E identifica il numero di positivi minori di  $n$  coprimi con  $n$ .  
E.g.

$$\Phi(8) = |\{1, 2, 4, 5, 7\}| = 6$$

Oss.  $p \in \mathbb{P}$ ,  $p$  primo  $\Rightarrow \Phi(p) = p - 1$ .

Prop 3.9.1 Siano  $p, q \in \mathbb{P}$ ,  $p, q$  primi,  $p \neq q$   
allora  $\Phi(p \cdot q) = (p-1)(q-1)$

Teo. 3.9.2 Si  $n \in \mathbb{N}$  e  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  la su 2 decomposizione in numeri primi ( $\Rightarrow p_1, \dots, p_r \in \mathbb{P}$ ,  $p_1, \dots, p_r$  primi e distinti e  $\alpha_1, \dots, \alpha_r \in \mathbb{N}$ ) allora

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Prop. 3.9.3 Siano  $a, b \in \mathbb{N}$ , tali che  $(a, b) = 1$   
allora

$$\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$$

E.g.  $n = 100 \Rightarrow n = 2^2 \cdot 5^2 \Rightarrow$

$$\Phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 10 \cdot 4 = 40$$

Sia  $n \in \mathbb{P}$ , poniamo

$$E(n) := \{[a]_n : (a, n) = 1\}$$

Prop. 3.9.4 Sia  $n \in \mathbb{P}$  e sia  $k \in \mathbb{Z}$  tali che  $(k, n) = 1$ . Allora la funzione

$$[a]_n \mapsto [a]_n \cdot [k]_n$$

preso una classe in  $E(n)$  la moltiplico per la classe  $k$  e la classe trovata sarà ancora in  $E(n)$  e la funzione sarà iniettiva e suriettiva.

$\forall [a]_n \in E(n)$ , è una bijezione.

Teo. 3.9.5 (Teorema di Euler)

Siano  $n \in \mathbb{P}$  e  $k \in \mathbb{Z}$  tali che  $(k, n) = 1$  allora

$$K \stackrel{\Phi(n)}{=} \equiv_n 1$$

E.g. Sia  $n = 9$  allora

$$E(9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$$

La cardinalità di  $E(n) = \Phi(n)$

Cor 3.9.6 (piccolo teorema di Fermat)

Siano  $k, p \in \mathbb{N}$ ,  $p$  primo, tali che  $p \nmid k$ . Allora

$$K \stackrel{p-1}{=} \equiv_p 1$$

### 3.10 IL CODICE RSA

Problema fondamentale della crittografia

Spedire un messaggio da A a B in modo  
che solo B possa leggerlo (decrittarlo)

Codice RSA.

- Preparazione: B sceglie 2 primi  $p, q \geq 0$ ,  
 $p \neq q$ , e calcola  $n := pq$ . Quindi trova  $e \in \mathbb{P}$   
t.c.  $\text{MCD}(e, (p-1)(q-1)) = 1$ . Infine B calcola  
l'inversa moltiplicativa  $[d]_{(p-1)(q-1)}$  di  $[e]_{(p-1)(q-1)}$   
(Esiste ed è unica, vedi 3.8). B pubblica  
 $n$ ,  $e$  e tiene segreti  $p, q$  e  $d$

- Codifica: A prende un messaggio  $m \in \mathbb{P}$ ,  
Se un messaggio è un numero  
più grande viene spezzato  
 $1 \leq m \leq n$ , t.c.  $(m, n) = 1$ , calcola  
 $[\tilde{m}]_n := [m^e]_n$ , e spedisce  $\tilde{m}$ .

- Decodifica: B riceve  $\tilde{m}$  e decodifica  
calcolando  $[\tilde{m}^d]_n$

Perché funziona?

$$\text{Poiché } [e]_{(p-1)(q-1)} \cdot [d]_{(p-1)(q-1)} = [1]_{(p-1)(q-1)}$$

$$\Rightarrow e \cdot d \equiv 1 \pmod{\Phi(n)} \Rightarrow \exists k \in \mathbb{Z} \text{ t.c.}$$

$$e \cdot d = k \cdot \Phi(n) + 1. \text{ Pertanto}$$

$$\begin{aligned} [\tilde{m}^d]_n &= [(m^e)^d]_n = [m^{ed}]_n = [m^{k \cdot \varphi(n)+1}]_n = \\ &= [(m^{\varphi(n)})^k]_n \cdot [m]_n = ([m^{\varphi(n)}]_n)^k \cdot [m]_n \stackrel{\substack{\text{Teorema Euler} \\ (m,n)=1}}{=} \\ &= ([1]_n)^k \cdot [m]_n = [m]_n \end{aligned}$$

Oss. A e B non si scambiano niente.

Perché pensiamo che rompere RSA sia difficile?

Per rompere RSA dovremmo o fattorizzare  $n$   
(impossibile se  $n \gg 0$ ) o risolvere

$$[x^e]_n = [\tilde{m}]_n$$

-  $e=2 \Rightarrow$  reciprocità quadratica (GAUSS  $\approx 1810$ )

-  $e=3 \Rightarrow$  reciprocità cubica (EISENSTAIN  $\approx 1930$ )

-  $e \geq 4 \Rightarrow$  ricerche attuali

Così significa "grandi",  $\gg 0$ ?  
(attualmente  $\approx 10^{1000}$ )

### 3.11 NUMERAZIONI IN BASI DIVERSE

Prop. 3.11.1 Siano  $n, b \in \mathbb{P}$ ,  $b \geq 2$  allora esistono

$b_0, \dots, b_k \in \mathbb{N}$  t.c.  $0 \leq b_i \leq b-1 \quad \forall i=0, \dots, k$  e

$$n = b_k \cdot b^k + b_{k-1} \cdot b^{k-1} + \dots + b_1 \cdot b + b_0 \quad \square$$

dove  $k := \max \{ i \in \mathbb{N} : b^i \leq n \}$ . tali  $b_0, \dots, b_k$  sono unici.

Def. Si dice espressione b-aria (o in base b) di n l'espressione:

$$n = b_k \cdot b^k + b_{k-1} \cdot b^{k-1} + \dots + b_1 \cdot b^1 + b_0$$

## Cap 4: Combinatoria e numerativa

### 4.1. IL PROBLEMA FONDAMENTALE DELLA COMBINATORIA ENUMERATIVA

Sia A un insieme.

Def. La cardinalità di A (scritto  $|A|$ , o  $\#A$ ) è il numero di elementi di A.

Problema fondamentale dell'c.e.:

Dato una sequenza  $A_0, A_1, \dots$  di insiemi finiti. calcolare  $\{|A_i|\}$ ,  $i \neq 0$ .

Cosa significa "calcolare"?

3 risposte:

1) una formula (E.g.  $|A_n| = 2^n \quad \forall n \in \mathbb{N}$  o  $|A_n| = \sum_{i=0}^n 2^i$ )

2) una ricorsione (E.g.  $|A_n| = |A_{n-1}| + |A_{n-2}| \quad \forall n \geq 2$ )

3) una funzione generatrice. cioè una funzione  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f$  infinitamente differenziabile in  $x=0$

Tale che lo sviluppo in serie di Taylor di  $f$  in  $x=0$  è  $\sum_{n \geq 0} |A_n| \cdot x^n$  (E.g.  $f(x) = \frac{1}{1-x-x^2}$ )

## 4.2 PROPRIETÀ DI BASE

Oss. Siano  $A$  e  $B$  insiemi e  $f: A \rightarrow B$ ,  
 $f$  biunivoca. Allora  $\Rightarrow |A| = |B|$ .

Def. La potenza di  $A$  alla  $B$  è:

$$A^B := \left\{ f : B \rightarrow A \mid \text{tutte le } f \text{ da } B \text{ in } A \right\}.$$

Prop 4.2.1 Siano  $A$  e  $B$  insiemi finiti allora:

$$1) |A \times B| = |A| \cdot |B|$$

$$2) |A^B| = |A|^{ |B| }$$

$$3) |A \cup B| = |A| + |B| - |A \cap B|$$

## 4.3 COEFFICIENTI BINOMIALI

Sia  $n \in \mathbb{N}$ , ricordiamo che:

$$[n] := \{1, \dots, n\}$$

Prop 4.3.1 Sia  $n \in \mathbb{N}$  allora:

$$|\mathcal{P}([n])| = 2^n.$$

Sia  $A$  un insieme e sia  $n \in \mathbb{N}$ . poniamo:

$$\binom{A}{n} := \{B \subseteq A : |B| = n\} \quad \begin{array}{l} \text{"A binomiale n"} \\ \text{"a eseguire n"} \end{array}$$

E.g.  $A = \{1, 2, 3\}$ ,  $n=3$  allora:

$$\binom{\{1, 2, 3\}}{2} = \left\{ \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\} \right\}$$

Sia  $n \in \mathbb{N}$ .

Def. Il coefficiente binomiale di grado  $n$  è

$$\binom{x}{n} := \frac{x \cdot (x-1) \cdot (x-2) \cdots (x-n+1)}{n!} = \frac{x!}{n!(x-n)!}$$

Se  $n \in \mathbb{P}$ ,  $\binom{x}{0} := 1$ ,  $\binom{x}{n} := 0$  se  $n < 0$

Oss.  $\binom{x}{n} \in \mathbb{Q}[x]$  è un polinomo a coeff. razionali

Oss. Se  $n \in \mathbb{P}$  allora  $\binom{x}{n} = \binom{x-1}{n} + \binom{x-1}{n-1}$

E.g. il numero in riga  $n$  e

$$\begin{array}{ccccccccc} & & 1 & & & & & & \\ & & 1 & 1 & & & & & \\ & & 1 & 2 & 1 & & & & \\ & & 1 & 3 & 3 & 1 & & & \\ & & 1 & 4 & 6 & 4 & 1 & & \\ & & 1 & 5 & 10 & 10 & 5 & 1 & \end{array}$$

posizione  $k+1$  è  $\binom{n}{k}$

Prop. 4.3.2 Sia  $n \in \mathbb{N}$  allora

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$$

Prop 4.3.3 Siano  $n, k \in \mathbb{N}$ ,  $0 \leq k \leq n$ . allora:

$$|\binom{\{1, 2, \dots, n\}}{k}| = \binom{n}{k}$$

Cor. 4.3.4 Sia  $n \in \mathbb{P}$ . allora

$$|\{A \subseteq [n] : |A| \text{ è pari}\}| = |\{A \subseteq [n] : |A| \text{ è dispari}\}|$$

## L.4 IL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Sappiamo che:

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (*)$$

Se  $A$  e  $B$  sono insiemi finiti.

Siano  $A, B, C$  insiemi finiti. Allora

$$\begin{aligned} |A \cup B \cup C| &= |A \cup B| + |C| - |(A \cup B) \cap C| = * \\ &= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| = * \\ &= |A| + |B| + |C| - |A \cap B| - (|A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|) = \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \end{aligned}$$

Siano  $A_1, \dots, A_n$  insiemi finiti ( $n \in \mathbb{P}$ ).

Dato  $T \subseteq [n]$ ,  $T = \{t_1, \dots, t_r\}$  poniamo:

$$A_T := A_{t_1} \cap \dots \cap A_{t_r}.$$

$$\text{E.g. } A_{\{1, 5, 6\}} = (A_1 \cap A_5 \cap A_6)$$

Allo stesso modo che per  $n=3$  si dimostra:

**Teo. 4.4.1 (Il principio di inclusione-esclusione)**

Siano  $A_1, \dots, A_n$  insiemi finiti. Allora:

$$|A_1 \cup \dots \cup A_n| = \sum_{\substack{T \subseteq [n] \\ T \neq \emptyset}} (-1)^{|T|-1} \cdot |A_T|$$

Cap 3

**Teo.** Sia nell'  $\mathbb{P}$  e sia  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  la sua decomposizione in numeri primi.

( $\Rightarrow p_1, \dots, p_r, \alpha_1, \dots, \alpha_r \in \mathbb{P}, p_1, \dots, p_r$  primi distinti)

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

#### 4.5 COMPOSIZIONI

Siano  $n, k \in \mathbb{P}$ .

**Def.** Una **composizione** (di  $n$  in  $k$  parti) è una sequenza  $(\alpha_1, \dots, \alpha_k) \in \mathbb{P}^k$ :  $\alpha_1 + \dots + \alpha_k = n$  (dove  $\mathbb{P}^k := \underbrace{\mathbb{P} \times \dots \times \mathbb{P}}_k$ )

E.g le composizioni di  $n=5$  in  $k=3$  parti sono:

$$(1, 1, 3), (1, 2, 2), (1, 3, 1), (2, 1, 2), (2, 2, 1), (3, 1, 1)$$

Sono 6

**Prop. 4.5.1** Siano  $n, k \in \mathbb{P}$ . Allora ci sono  $\binom{n-1}{k-1}$  composizioni di  $n$  in  $k$  parti

E.g  $n=19, k=5$ , sia  $S = \{1, 7, 9, 12\} \in \binom{[18]}{4}$  allora

$$\{1, 7, 9, 12\} \subseteq [18]$$

$$\begin{array}{ccccccccccccc} \cdot & | & \cdot & \circ & \cdot & \cdot & \cdot & \cdot & | & \cdot & \circ & \cdot & \cdot & \cdot & \cdot \\ & \uparrow & & & & & & & \uparrow & & & & & & & \\ & 1 & & 7 & & 9 & & 12 & & & & & & & & \end{array}$$

spazio      spazio      spazio

$(1, 6, 2, 3, 7)$  c-pallini tra le barre

Def. Una composizione debole (di  $n$  in  $K$  parti) è una sequenza  $(a_1, \dots, a_K) \in \mathbb{N}^K$  :  $a_1 + \dots + a_K = n$ .

Prop. 4.5.2 (i) Sono:

$$\binom{n+K-1}{K-1} \text{ composizioni deboli di } n \text{ in } K \text{ parti}$$

#### 4.6 COEFFICIENTI MULTINOMIALI

Siano  $n, K \in \mathbb{P}$  e sia  $(a_1, \dots, a_K) \in \mathbb{P}^K$  una composizione di  $n$  in  $K$  parti.

Def. Il coefficiente multinomiale  $(a_1, \dots, a_K)$  è il numero di modi di assegnare ogni  $i \in [n]$  ad ogni  $K$  categorie  $J=1 \dots K$ ,  $C_1, \dots, C_K$  in modo che  $a_J$  numeri vengano assegnati a  $C_J$  ( $H_J$ )

Eg.  $n=4, K=3$   $(a_1, a_2, a_3) = (1, 2, 1)$

$$\begin{array}{lll} 1) & \boxed{3} & \boxed{1, 2} \\ 2) & \boxed{4} & \boxed{1, 2} \end{array} \quad \begin{array}{l} C_1, \dots, C_K \text{ scatole} \\ \binom{n}{a_1, \dots, a_K} \end{array}$$

$$\Rightarrow \binom{4}{1, 2, 1} = 12 \text{ possibili combinazioni}$$

Prop. 4.6.1 Sia  $(a_1, \dots, a_K)$  una composizione di  $n$  in  $K$  parti allora:

$$\binom{n}{\alpha_1, \dots, \alpha_k} = \frac{n!}{\alpha_1! \dots \alpha_k!}$$

Sia  $S = \{D_1, D_2, \dots, D_n\}$  un insieme finito

**Def.** Un multinsieme  $n$  su  $S$  è una funzione

$v: S \rightarrow \mathbb{N}$ . Se  $x \in S \Rightarrow v(x)$  si dice  $\lambda_x$

molteplicità di  $x$  in  $n$ . La cardinalità di  $n$  è:

$$|n| := \sum_{x \in S} v(x), \text{ scritto}$$

$$M = \{v(D_1), v(D_2), \dots, v(D_n)\}$$

$$M = \underbrace{\{D_1, \dots, D_1\}}_{v(D_1)}, \underbrace{\{D_2, \dots, D_2\}}_{v(D_2)}, \underbrace{\{D_n, \dots, D_n\}}_{v(D_n)}$$

Intuitivamente, un multinsieme è un insieme con "ripetizioni".

**E.g.**  $M = \{1^4, 2^0, 3^2, 4^4\}$   $M = \{1, 1, 1, 1, 3, 3, 4, 4, 4, 4\}$   
 è un multinsieme su  $[4]$  di cardinalità 10 ( $4+0+2+4$ )  
 (definita da  $v_{(1)}=4, v_{(2)}=0, v_{(3)}=2, v_{(4)}=4$ )

Siano  $n \in \mathbb{P}$  e  $k \in \mathbb{N}$

**Def.** Il coefficiente binomiale rigirato (o storto)  
 è il numero di multinsiemi di  $[n]$  di cardinalità  
 $k$ , scritto  $\binom{n}{k}$

Oss. La funzione

$\{1^{\alpha_1}, 2^{\alpha_2}, 3^{\alpha_3}, \dots, n^{\alpha_n}\} \mapsto (\alpha_1, \alpha_2, \dots, \alpha_n)$  è  
una bijezione fra (multinsieme su  $[n]$  di  
cardinalità  $K$ ) e (composizioni deboli di  $K$  in  
 $n$  parti) Quindi per 4.5.2

$$\left(\begin{array}{c} n \\ K \end{array}\right) = \left(\begin{array}{c} K+n-1 \\ n-1 \end{array}\right)$$

Prop 4.6.2 Sia  $n \in \mathbb{P}$  allora

$$\frac{1}{(1-x)^n} = \sum_{K \geq 0} \left(\begin{array}{c} n \\ K \end{array}\right) x^K$$

Sia  $M = \{1^{\alpha_1}, \dots, n^{\alpha_n}\}$  un multinsieme su  $[n]$

Def. Una permutazione di  $M$  è un ordinamento  
lineare degli elementi di  $M$ . Poniamo

$$S(M) = \{ \text{permutazioni di } M \}$$

E.g. Sia  $M = \{1^2, 2^2, 3^1\} = \{1, 1, 2, 2, 3\}$ . Allora

$$S(M) = \{1223, 1232, 1322, 2123, 2132, 2213, 2231, \\ 2312, 2321, 3122, 3212, 3221\}$$

Prop 4.6.3 Sia

$M = \{1^{\alpha_1}, \dots, n^{\alpha_n}\}$  un multinsieme su  $[n]$ . Allora

$$|S(M)| = \binom{N}{\alpha_1, \dots, \alpha_n} \text{ dove } N := \alpha_1 + \dots + \alpha_n$$

E.g. Sia  $M = \{1^5, 2^3, 3^1, 4^2, 5^5\}$  e sia

$1534112451251255 \in S(M)$

↓

$\boxed{1, 5, 6, 10, 13}$	$\boxed{7, 11, 14}$	$\boxed{}$	$\boxed{3}$	$\boxed{}$	$\boxed{4, 8, }$	$\boxed{}$	$\boxed{2, 9, 12, 15, 16}$	$\checkmark$ posiz. ← numero
1	2		3		4		5	

## 4.7 ENUMERAZIONE PRATICA

52 carte: 4 semi . 13 valori

$$= =$$

$$\left\{ C, Q, F, P \right\} \quad \left\{ 1, 2, \dots, K \right\}$$

Quante mani ci sono? (5 carte , mano)

$$\binom{52}{5} = \frac{26 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2} = 26 \cdot 51 \cdot 10 \cdot 49 \cdot 4 = 2598960$$

Quante mani sono un full?

full  $\leftrightarrow$  (valore del tris, valore della coppia)  
seme mancante, semi della coppia

$$\Rightarrow 13 \cdot 4 \cdot 12 \cdot \binom{4}{2} = 13 \cdot 4 \cdot 12 \cdot 6 = 3744$$

Quante mani sono un poker?

poker  $\leftrightarrow$  (valore del poker, valore carta rimanente)  
seme del poker, seme carta rimanente

$$\Rightarrow 13 \cdot 12 \cdot 1 \cdot 4 = 624$$

Quante mani sono un colore?

Colore  $\leftrightarrow$  (valore del colore,  
seme del colore)

$$\Rightarrow \binom{13}{5} \cdot 4 = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2} \cdot 4 = 5148$$

Quante mani sono una doppia coppia?

Doppia coppia  $\leftrightarrow$  (valore 1° coppia, 12° coppia, valore carta rim.  
seme 1° coppia, 12° coppia, seme carta rim.)

$$\Rightarrow 13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{2} \cdot 11 \cdot 4 = \frac{13 \cdot 4 \cdot 3 \cdot 12 \cdot 6 \cdot 3 \cdot 11 \cdot 4}{2 \cdot 2} = 247104$$

non corretto perché non è una biezione

E.g.

$$(2c, 2Q, 4P, 4F, 7c) \leftrightarrow (2, \{C, Q\}, 4, \{P, F\}, 7, C)$$

↑  
sono due seq diverse

$(4, \{P, F\}, 2, \{C, Q\}, 3, C)$  anche se la mano è una  
pertanto la vera codifica è:

Doppia coppia  $\leftrightarrow$  (valori delle 2 coppie, carta rimanente  
semi coppia valore più alto  
" " " " più basso, semi carta "

$$\Rightarrow \binom{13}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot 11 \cdot 4 =$$

$$= \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{2 \cdot 2 \cdot 2} = 123552$$

## 4.8 RICORSIONI LINEARI E COEFFICIENTI COSTANTI

**Teo 4.8.1 (Teorema fondamentale dell'algebra)**

Siano  $a_0, \dots, a_d \in \mathbb{R}$  ( $d \in \mathbb{P}$ ),  $a_d \neq 0$ . Allora

$\exists \alpha_1, \dots, \alpha_r \in \mathbb{C}$ , e  $\exists d_1, \dots, d_r \in \mathbb{P}$  tali che

$$d_1 + \dots + d_r = d \text{ e } a_0 + a_1 x + \dots + a_d x^d = \\ = a_d (x - \alpha_1)^{d_1} \cdots (x - \alpha_r)^{d_r}.$$

**Def.** I numeri  $\alpha_1, \dots, \alpha_r$  si dicono radici di  $a_0 + a_1 x + \dots + a_d x^d$ . Il numero  $d_i$  si dice la molteplicità di  $\alpha_i$  ( $\forall i = 1, \dots, r$ )

**Prop. 4.8.2 (Ruffini)** Sia  $P(x) \in \mathbb{R}[x]$  e  $\alpha \in \mathbb{C}$

Allora  $P(\alpha) = 0 \iff (x - \alpha) \mid P(x)$

Sia  $f: \mathbb{N} \rightarrow \mathbb{R}$

$$(A(x) \mid B(x) \iff \exists C(x) \in \mathbb{R}[x]. B(x) = A(x)C(x))$$

**Def.**  $f$  soddisfa una ricorsione lineare a

coefficienti costanti Se  $\exists a_0, \dots, a_d \in \mathbb{R}$  ( $d \in \mathbb{P}$ )

tali che  $f(n+d) = a_{d-1} \cdot f(n+d-1) + \dots + a_1 f(n+1) + a_0 f(n)$

$\forall n \in \mathbb{N}$



**Euristica (e idee):** Calcolando i primi valori

si nota che  $f(n)$  cresce esponenzialmente.

Sia  $\lambda \in \mathbb{C}$ :  $f(n) = \lambda^n \quad \forall n \in \mathbb{N}$ . Abbiamo che



$f(n) = \lambda^n$  è soluzione di (\*) se e solo se  
 $\lambda^{n+d} = a_{d-1}\lambda^{n+d-1} + \dots + a_1\lambda^{n+1} + a_0\lambda^n$  cioè sse:

$$\lambda^d = a_{d-1}\lambda^{d-1} + \dots + a_1\lambda + a_0.$$

cioè sse  $\lambda$  è radice di

$$\lambda^d - a_{d-1}\lambda^{d-1} - \dots - a_1\lambda - a_0 = 0 \quad (**)$$

Def.  $(**)$  si dice l'**equazione caratteristica**  
della ricorsione (\*)

**Teo 4.8.3** Sia  $f: \mathbb{N} \rightarrow \mathbb{R}$  e siano  $a_0, \dots, a_{d-1} \in \mathbb{R}$   
( $d \in \mathbb{P}$ ) tali che:

$$f(n+d) = a_{d-1}f(n+d-1) + \dots + a_1f(n+1) + a_0f(n) \quad (*)$$

per  $\forall n \in \mathbb{N}$ . allora  $\exists P_1(x), \dots, P_r(x) \in \mathbb{C}[x]$

tali che  $\deg(P_i) \leq d_i - 1 \quad \forall i = 1, \dots, r$  e

$$f(n) = \sum_{i=1}^r P_i(n) \cdot (\gamma_i)^n$$

$\forall n \in \mathbb{N}$ , dove  $\gamma_1, \dots, \gamma_r \in \mathbb{C}$  sono le radici  
dell'equazione caratteristica di (\*) e  $d_1, \dots, d_r \in \mathbb{P}$   
sono le molteplicità di  $\gamma_1, \dots, \gamma_r$  rispettivamente

## CAP 5: SOMME E APPROXIMAZIONI

### S.1 ANNUITÀ

Avete vinto al superenalotto e avete una scelta  
1000000 euro subito o 50000 euro l'anno  
per 30 anni, cosa conviene scegliere?

Sia  $x = 50000$  e sia  $p = \text{inflazione}$ . Allora in 30 anni riceveremo:

$$x + x(1-p) + x(1-p)^2 + \dots + x(1-p)^{29} = \\ x \sum_{i=0}^{29} (1-p)^i = x \cdot \frac{(1-p)^{30} - 1}{(1-p) - 1} =$$

Se  $p = 0,03$  allora otteniamo:

$$x \cdot \frac{(0,97)^{30} - 1}{0,97 - 1} = x \cdot \frac{(0,40) - 1}{-0,03} = \frac{-0,60}{-0,03} = 20x = 1000000$$

e se infiniti anni?

$$x + x(1-p) + x(1-p)^2 + \dots = x \sum_{i=0}^{\infty} (1-p)^i = \\ x \cdot \frac{1}{1-(1-p)} = x \cdot \frac{1}{0,03} = 33,3x = 1666666$$

Abbiamo usato il seguente

Lemma S.1.1 Sia  $n \in \mathbb{N}$  e sia  $x \in \mathbb{R}$ . Allora

$$\sum_{i=0}^n x^i = \frac{x^{n+1} - 1}{x - 1} \quad \text{somma geometrica}$$

Metodo della perturbazione (per trovare la somma geometrica)

Sia  $S := 1 + x + x^2 + \dots + x^n \Rightarrow$

$$xS = x + x^2 + x^3 + \dots + x^{n+1} = x^{n+1} + (S - 1).$$

## 5.2 SOMME POLINOMICHE

Sappiamo che:

$$\sum_{i=1}^n i = \binom{n+1}{2} \quad \forall n \in \mathbb{N}$$

Come trovare una simile formula?

$$1 + 2 + \dots + n + 1 + 2 + \dots + n = (1+n) + (2+(n-1)) + \dots + (n+1) = \\ n \cdot (n+1)$$

Come calcolare

$$\sum_{i=1}^n i^2 = ?$$

**Teo 5.2.1** Sia  $f(x) \in \mathbb{R}[x]$ . allora

$\exists g(x) \in \mathbb{R}[x]: \deg(g(x)) \leq \deg(f(x) + 1)$  e

$$\sum_{i=0}^n f(i) = g(n) \quad \forall n \in \mathbb{N}$$

**Def.** Si dice che  $g(n)$  è una formula chiusa

per  $\sum_{i=0}^n f(i)$

E.g. Calcolare  $\sum_{i=0}^n i^2$

poiche  $i^2 = f(i)$  con  $f(x) = x^2 \in \mathbb{R}[x] \Rightarrow$  per S.Z.1

$$\exists g(x) \in \mathbb{R}[x] : \sum_{i=0}^n i^2 = g(n) \quad \forall n \in \mathbb{N}$$

e  $\deg(g(x)) \leq 3$ . pertanto

$\exists a, b, c, d \in \mathbb{R}$  tali che  $g(x) = ax^3 + bx^2 + cx + d$ .

quindi:

$$\sum_{i=0}^n i^2 = a \cdot n^3 + b \cdot n^2 + cn + d \quad \forall n \in \mathbb{N} \quad (*)$$

$m_2$  oppure

$$\begin{cases} 0 = d & (\star \text{ per } n=0) \\ 1 = a+b+c+d & (\star \text{ per } n=1) \\ 5 = 8a+4b+2c+d & (\star \text{ per } n=2) \\ 14 = 27a+9b+3c+d & (\star \text{ per } n=3) \end{cases}$$

pertanto

$$\begin{cases} a+b+c = 1 \\ 8a+4b+2c = 5 \\ 27a+9b+3c = 14 \end{cases} \quad c = 1 - a - b$$

$$\begin{cases} 8a + 4b + 2(1-a-b) = 5 \\ 27a + 9b + 3(1-a-b) = 14 \end{cases}$$

$$\begin{cases} 6a + 2b = 3 \\ 2a + 6b = 11 \end{cases} \quad b = \frac{3 - 6a}{2}$$

$$24a + 6\left(\frac{3 - 6a}{2}\right) = 11 \quad \rightarrow \quad 6a = 2 \quad a = \frac{1}{3}$$

$$a = \frac{1}{3}$$

$$b = \frac{3 - 6a}{2} = \frac{3 - \frac{6}{3}}{2} = \frac{1}{2} \quad b = \frac{1}{2}$$

$$c = 1 - a - b = 1 - \frac{1}{3} - \frac{1}{2} = \frac{1}{6} \quad \text{pertanto}$$

$$\sum_{i=0}^n i^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \quad \forall n \in \mathbb{N}$$

### 5.3 SOMME NON POLINOMIALI

$$\sum_{i=1}^n \sqrt{i} = ?$$

**Teo 5.3.1** Si  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f$  continua e monotona in  $\mathbb{R}_{>0}$ . Allora

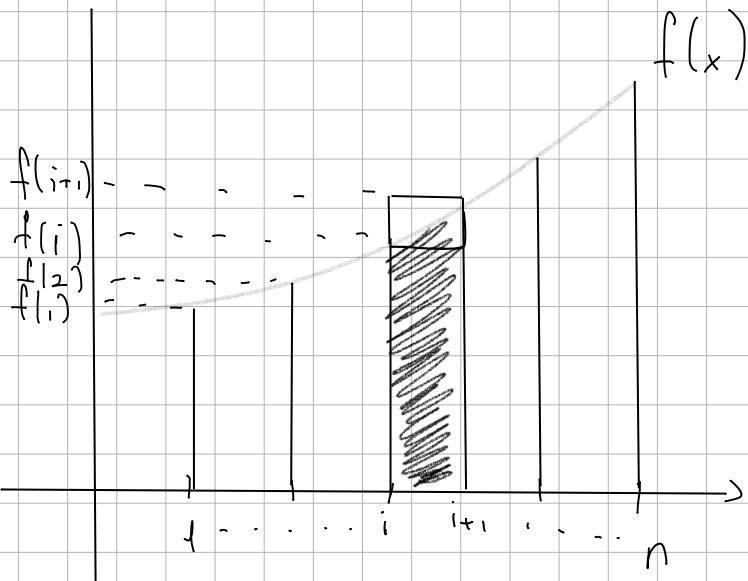
$$f(1) + \int_1^n f(x) dx \leq \sum_{i=1}^n f(i) \leq f(n) + \int_1^n f(x) dx \quad \forall n \in \mathbb{N}$$

se  $f$  è crescente, e

$$f(1) + \int_1^n f(x) dx \geq \sum_{i=1}^n f(i) \geq f(n) + \int_1^n f(x) dx \quad \forall n \in \mathbb{N}$$

se  $f$  è decrescente

Geometricamente:



$$f(1) \leq \int_1^{i+1} f(x) dx \leq f(i+1)$$

AREA SOTTOINTESA ENDENZIALE

E.g. Calcolare o stimare

$$\sum_{i=1}^n \sqrt{i}$$

poiché  $f(x) := \sqrt{x}$  è continua e monotona crescente in  $\mathbb{R}_{>0} \Rightarrow$  per S.S.I.  $\Rightarrow$

$$f(1) + \int_1^n f(x) dx \leq \sum_{i=1}^n f(i) \leq f(n) + \int_1^n f(x) dx.$$

M2

$$\int_1^n \sqrt{x} dx = \frac{2}{3} \times \left[ \frac{3}{2} x^{\frac{3}{2}} \right]_1^n = \frac{2}{3} n^{\frac{3}{2}} - \frac{2}{3}$$

quindi

$$\underbrace{\left( \frac{2}{3} n^{\frac{3}{2}} - \frac{2}{3} \right)}_{\text{1}} \leq \sum_{i=1}^n \sqrt{i} \leq \underbrace{\sqrt{n} + \frac{2}{3} n^{\frac{3}{2}} - \frac{2}{3}}_{\text{2}}$$

$\forall n \in \mathbb{N}$

Def.  $f$  e  $g$  sono asintoticamente equivalenti.

Scritto  $f \approx g$ , se

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} = 1$$

pertanto

$$\sum_{i=1}^n \sqrt{i} \approx \frac{2}{3} n^{\frac{3}{2}} \quad \text{se } n \rightarrow +\infty$$

Per  $n \in \mathbb{N}$  poniamo

$$H_n := \sum_{i=1}^n \frac{1}{i}$$

Def.  $H_n$  si dice l'<sup>l</sup> n-esimo numero armonico.

Quanto è grande  $H_n$ ?

La funzione  $f(x) = \frac{1}{x}$  è continua e monotona  
decrecente per  $x \in \mathbb{R}_{>0}$ . Quindi per S.3.1.

$$f(1) + \int_1^n f(x) dx \geq \sum_{i=1}^n f(i) \geq f(n) + \int_1^n f(x) dx$$

abbiamo

$$\int_1^n \frac{1}{x} dx = \left[ \ln(x) \right]_1^n = \ln(n)$$

quindi

$$1 + \ln(n) \geq \sum_{i=1}^n \frac{1}{i} \geq \frac{1}{n} + \ln(n) \quad \forall n \in \mathbb{N}$$

pertanto

$$\frac{1}{\ln(n)} \geq \frac{\sum_{i=1}^n \frac{1}{i}}{\ln(n)} \geq \frac{1}{n \ln(n)}$$

↓      ↓  
1      1

quindi per il Teorema del confronto,

$$\lim_{n \rightarrow +\infty} \frac{\sum_{i=1}^n \frac{1}{i}}{\ln(n)} = 1$$

$$H_n \approx \ln(n) \quad \text{per } n \rightarrow +\infty$$

#### B.4 SOMME DOPPIE

Quant'è grande  $\sum_{i=1}^n H_i$ ?

abbiamo che

$$\sum_{i=1}^n H_i = ?$$

abbiamo che

$$\sum_{i=1}^n H_i = \sum_{i=1}^n \sum_{j=1}^i \frac{1}{j}$$

Cos'è stiamo sommando realmente?

Stiamo sommando i numeri nella tabella:

i	1	2	3	..	n
1	$\frac{1}{1}$				
2	$\frac{1}{1}$	$\frac{1}{2}$			
3	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$		
.	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$		
n	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	..	$\frac{1}{n}$

possiamo sommare questi numeri per colonne

otteniamo

quantità colonna

$$\sum_{i=1}^n \sum_{j=1}^i \frac{1}{j} = n \cdot 1 + (n-1) \cdot \frac{1}{2} + (n-2) \cdot \frac{1}{3} + \dots + 1 \cdot \frac{1}{n} =$$

$$= \sum_{k=1}^n \frac{1}{k} (n+1-k) = \sum_{k=1}^n \left( \frac{n}{k} + \frac{1}{k} - 1 \right) =$$

$$= \sum_{k=1}^n \frac{n}{k} + \sum_{k=1}^n \frac{1}{k} - \sum_{k=1}^n 1 = n \cdot H_n + H_n - n =$$

$$(n+1)(H_n - n) =$$

$$\sum_{i=1}^n H_i = (n+1)(H_n - n) \quad \forall n \in \mathbb{P}$$

in particolare

$$\sum_{i=1}^n \approx (n+1) \ln(n) \quad \text{per } n \rightarrow +\infty$$

## 5.5 PRODOTTI

Si  $f : \mathbb{N} \rightarrow \mathbb{R}_{>0}$  quanto è grande

$$\prod_{i=1}^n f(i) ?$$

Allora

$$\ln\left(\prod_{i=1}^n f(i)\right) = \sum_{i=1}^n \ln(f(i)) =$$

quindi

$$\prod_{i=1}^n f(i) = e^{\sum_{i=1}^n \ln(f(i))}$$

Quanto è grande  $n!$ ?

abbiamo che

$$\ln(n!) = \sum_{i=1}^n \ln(i)$$

quindi

$$n! = \exp\left(\sum_{i=1}^n \ln(i)\right) \quad \forall n \in \mathbb{P}$$

stimiamo  $\sum_{i=1}^n \ln(i)$ . Poiché  $\ln(x)$  è continua e monotona crescente in  $\mathbb{R}_{>0}$ . Abbiamo per s.b. che

$$\ln(1) + \int_1^n \ln(x) dx \leq \sum_{i=1}^n \ln(i) \leq \ln(n) + \int_1^n \ln(x) dx$$

$\forall n \in \mathbb{P}$  m2

$$\int_1^n \ln(x) dx = \left[ x \ln(x) - x \right]_1^n = n \ln(n) - n + 1$$

quindi

$$n \ln(n) - n + 1 \leq \sum_{i=1}^n \ln(i) \leq \ln(n) + n \cdot \ln(n) - n + 1 \quad \forall n \in \mathbb{P}$$

pertanto

$$e^{n \ln(n) - n + 1} \leq n! \leq e^{(\ln(n) + n) \ln(n) - n + 1} \quad \forall n \in \mathbb{P}$$

quindi

$$\frac{e^{\ln(n^n)}}{e^{n-1}} \leq n! \leq \frac{e^{\ln(n^{n+1})}}{e^{n-1}}$$

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{n^{n+1}}{e^{n-1}}$$

in realtà vale che

**Teo S.S.1 (stirling)** esiste una funzione  
 $\varepsilon: \mathbb{N} \rightarrow \mathbb{R}$  tale che

$$\overset{\text{epsilon}}{n!} = \sqrt{2\pi n} \left( \frac{n}{e} \right)^n \cdot e^{\varepsilon(n)}$$

dove

$$\frac{1}{12n+1} \leq \varepsilon(n) \leq \frac{1}{12n}$$

## 5.6 NOTAZIONI ASINTOTICHE

Siano  $f, g: \mathbb{N} \rightarrow \mathbb{R}$

Def. Si dice che  $f$  è asintoticamente più piccola (o che è un  $o$ -piccolo) di  $g$ , scritto  $f = o(g)$ , se

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} = 0.$$

Prop 5.6.1 Siano  $a, b \in \mathbb{R}$ ,  $a < b$ . Allora

$$x^a = o(x^b)$$

Prop 5.6.2 Sia  $b \in \mathbb{R}$ ,  $b > 0$ . Allora

$$\ln(x) = o(x^b)$$

Prop 5.6.3. Siano  $a, b \in \mathbb{R}$ ,  $b > 1$ . Allora

$$x^a = o(b^x)$$

Sia  $f, g: \mathbb{N} \rightarrow \mathbb{R}$ . Sia  $g(n) \in \mathbb{R}_{>0}$   $\forall n \in \mathbb{N}$ .

Def. Si dice che  $f$  è un  $O$ -grande di  $g$ , scritto  $f = O(g)$ , se  $\exists c \in \mathbb{R}_{>0}$  e  $\exists N \in \mathbb{P}$  tali che

$$|f(n)| \leq c \cdot g(n) \quad \text{Se } n \geq N$$

E.g. Si  $f(x) = 5x^3 - 4x + 2$  allora

$$\lim_{x \rightarrow +\infty} \frac{5x^3 - 4x + 2}{x^3} = 5$$

Per  $N \in \mathbb{P}$  tale che  $4 \leq \frac{5x^3 - 4x + 2}{x^3} \leq 6$  se  $x > N$   
quindi

$$\frac{|5x^3 - 4x + 2|}{x^3} \leq 6 \quad \text{se } x > N$$

pertanto  $|5x^3 - 4x + 2| = O(x^3)$ .

Con lo stesso ragionamento si dimostra che

Prop 5.6.4. Siano  $f, g: \mathbb{N} \rightarrow \mathbb{R}$  tali che  $g(n) > 0$

$\forall n \in \mathbb{N}$ , e

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} = c \quad \text{per qualche } c \in \mathbb{R}. \text{ allora } f = O(g)$$

Cor. 5.6.5 Siano  $a_0, \dots, a_d \in \mathbb{R}$ ,  $a_d > 0$  allora

$$a_d x^d + \dots + a_1 x + a_0 = O(x^d)$$

Cor 5.6.6. Siano  $f: \mathbb{N} \rightarrow \mathbb{R}$  e  $g: \mathbb{N} \rightarrow \mathbb{R}_{>0}$

allora

$$f = o(g) \stackrel{\text{quoziente } v_d > 0}{\Rightarrow} f = O(g) \quad \text{e} \quad f \underset{\substack{\text{quoziente } v_d = 1 \\ \text{oppure}}} \approx g \Rightarrow f = O(g)$$

Siano  $f: \mathbb{N} \rightarrow \mathbb{R}_{>0}$  e  $g: \mathbb{N} \rightarrow \mathbb{R}$

Def. Si dice che  $f$  è un **omega** di  $g$ , scritto  
 $f = \Omega(g)$  se  $\exists c \in \mathbb{R}_{>0}$  e  $\exists N \in \mathbb{P}$  tali che

$$f(n) \geq c \cdot g(n) \quad \text{se } n \geq N$$

Prop 5.6.7 Siano  $f, g: \mathbb{N} \rightarrow \mathbb{R}_{>0}$  allora

$$f = O(g) \iff g = \Omega(f)$$

Oss. Se  $f = o(g)$  allora non è detto che  $g = O(f)$

(per es se  $f(x) = x$  e  $g(x) = x^2 \Rightarrow f = o(g)$  ma  
 $g \neq O(f)$  (se  $\exists c \in \mathbb{R}_{>0}$  e  $N \in \mathbb{P}$  tali che  
 $n^2 \leq cn \quad \forall n \geq N \Rightarrow$  assurdo))

Def. Siano  $f, g: \mathbb{N} \rightarrow \mathbb{R}_{>0}$  diciamo che  $f$  è  
un **teza** di  $g$ , scritto  $f = \Theta(g)$ , se  $f = O(g)$  e  
 $g = O(f)$

E.g. Sia  $f: \mathbb{N} \rightarrow \mathbb{R}_{>0}$  tale che  $f = \Theta(n^3)$

$\Rightarrow \exists c_1, c_2 \in \mathbb{R}_{>0}$  e  $\exists N \in \mathbb{P}$  tali che  $c_1 \cdot n^3$   
 $\leq f(n) \leq c_2 \cdot n^3 \quad \forall n > N$ . Quindi se  $n$   
si doppia  $\Rightarrow f(n)$  si moltiplica per 8.

## 5.7 QUANTO E' GRANDE L'INFINITO?

Siano  $A$  e  $B$  insiemi.

**Def.** Diciamo che  $|A| = |B|$  se  
 $\exists f: A \rightarrow B$ ,  $f$  biunivoca

**Teo 5.7.1 (Zntor)**

Sia  $A$  un insieme allora  $|A| \neq |\mathcal{P}(A)|$   
(dove  $\mathcal{P}(A) := \{S : S \subseteq A\}$ )

tutti i sottinsiemi di  $A$

Siano  $A$  e  $B$  insiemi.

**Def.** diciamo che  $|A| \leq |B|$  se  $\exists f: A \rightarrow B$ ,  
 $f$  iniettiva

**Oss.** è chiaro che  $|A| \leq |\mathcal{P}(A)|$ , quindi

$$|A| \subsetneq |\mathcal{P}(A)| \subsetneq |\mathcal{P}(\mathcal{P}(A))| \subsetneq \dots$$

quindi ci sono infiniti infiniti.

**Ipotesi del continuo** Non esiste nessun insieme  
 $A$  tale che

$$|\mathbb{N}| \subsetneq |A| \subsetneq |\mathcal{P}(\mathbb{N})|.$$

## CAP 6. GRAFI

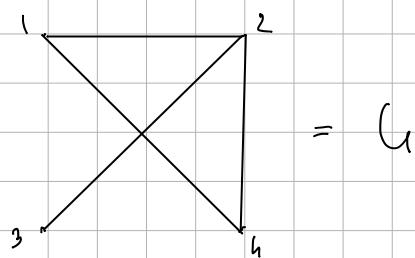
### 6.1 DEFINIZIONI

Def. Un grafo  $G$  è una coppia  $(V, E)$  dove  $V$  è un insieme e  $E \subseteq \binom{V}{2}$  (dove  $\binom{V}{k} := \{A \subseteq V : |A| = k\}$ ).  $V$  si dice insieme dei vertici di  $G$ ,  $E$  si dice insieme dei lati (o spigoli, o edges) di  $G$ .

Si rappresenta graficamente un grafo  $G = (V, E)$  disegnando un punto per ogni elemento di  $V$  e collegando due punti con un segmento (anche curvilineo) se e solo se i vertici corrispondenti sono un lato.

E.g.

$$G = ([4], \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\})$$



Sia  $G = (V, E)$  un grafo

Def. Un cammino in  $G$  è una sequenza  $(v_0, v_1, \dots, v_k) \in V^{k+1}$  tale che  $\{v_{i-1}, v_i\} \in E \quad \forall i = 1, \dots, k$

seq. di vertici  $\rightarrow$

collegati da un lato

La lunghezza del cammino è  $k$

Def. Un sentiero in  $G$  è un cammino tale che  
 $v_i \neq v_j \quad \forall 0 \leq i, j \leq k, i \neq j.$

un cammino con vertici distinti (non torna su un suo  
vertice già passato.)

Def. Un cammino chiuso in  $G$  è un cammino  
( $v_0, \dots, v_k$ ) tale che  $v_0 = v_k$  ritorna all'inizio

Def. Un ciclo in  $G$  è un cammino chiuso  
tale che  $v_0, \dots, v_k$  è un sentiero

Sia  $n \in \mathbb{P}$

Def. Il grafo vuoto (di ordine  $n$ ) è

$$N_n := ([n], \emptyset)$$

senza lati

Def. Il grafo completo (di ordine  $n$ ) è

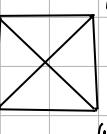
$$K_n := ([n], \binom{[n]}{2})$$

tutti i lati

E.g.

$$N_4 = \begin{matrix} & 1 & 2 \\ 1 & & & \\ 3 & & 4 \end{matrix}$$

$$K_4 = \begin{matrix} & 1 & 2 \\ 1 & & & \\ 3 & & 4 \end{matrix}$$



Def.  $G$  è连通的 se  $\forall x, y \in V, x \neq y \Rightarrow$   
Esiste un cammino tale che  $v_0 = x$  e  $v_k = y$ .

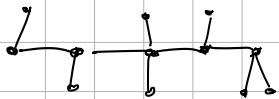
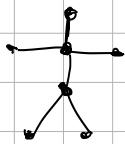
Def.  $G$  è aciclico (o una foresta) se  $G$  non

ha cicli

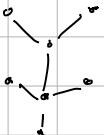
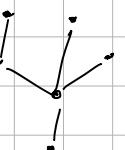
Def.  $G$  è un albero se  $G$  è aciclico e connesso

E.g.

alberi:



foreste:



Sia  $S \subseteq V$

Def.  $S$  è indipendente se

$$\begin{array}{l} x, y \in S \\ x \neq y \end{array} \stackrel{\text{implicaz}}{\Rightarrow} \{x, y\} \notin E$$

Def.  $S$  è completo (o una clique) se

$$\begin{array}{l} x, y \in S \\ x \neq y \end{array} \Rightarrow \{x, y\} \in E$$

Sia  $v \in V$

Def. Il grado di  $v$  è

$$d(v) := |\{u \in V : \{u, v\} \in E\}|$$



Lem. 6.1.1 Sia  $G = (V, E)$  un grafo allora

$$\sum_{v \in V} d(v) = 2 |E|$$

## 6.2 ACCOPPIAMENTI

Sia  $P$  una proprietà che un grafo può avere o no.

Def. Si dice che  $P$  è invariante per isomorfismi se vale che

$$(G \cong H) \Rightarrow ((G \text{ ha } P) \Leftrightarrow (H \text{ ha } P)) \quad \forall G, H$$

E. g.

$P = \text{"\'e connesso"}$   $\Rightarrow$  è invariante per isom.

$P = \text{"ha un ciclo di lunghezza 4"}$   $\Rightarrow$  // //

$P = \text{"se cambio nome a un vertice non \'e pi\'u un vertice"}$

$P = \text{"\'e un vertice"}$   $\Rightarrow$  non è //

E. g.

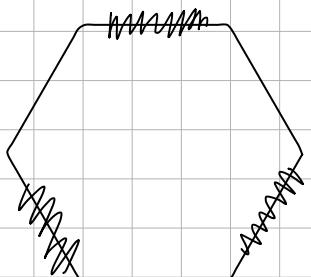


$(G \text{ ha un vertice di grado 4, ma } H \text{ no; } H \text{ ha un ciclo di lunghezza 4, ma } G \text{ no})$  ultima in dubbio

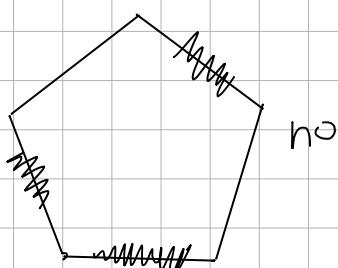
Def.  $M$  è un accoppiamento (o matching) se

$$\left( \{x, y\} \in M, \{u, v\} \in M \right) \stackrel{\text{implica}}{\rightarrow} \left\{ \begin{array}{l} \text{diversi} \\ \{x, y\} \cap \{u, v\} = \emptyset \end{array} \right. \quad \text{(f)} \quad \text{tra loro}$$

E.g.



si

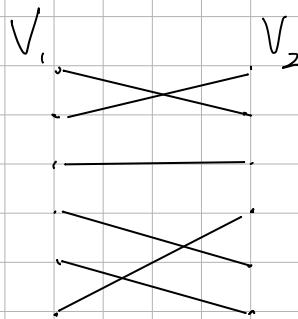


(hanno un  $v$  in comune)

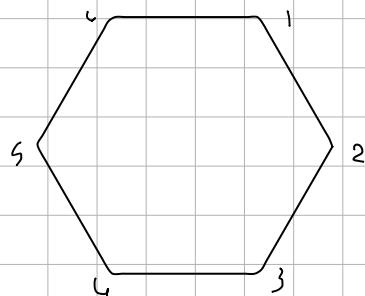
Sia  $G = (V, E)$  un grafo

Def.  $G$  si dice bipartito se  $\exists V_1, V_2 \subseteq V$ ,  $V_1$  e  $V_2$  indipendenti, tali che  $V = V_1 \cup V_2$ . unione con intersezione vuota soli lati di  $V_1$  e  $V_2$

E.g.



è bipartito

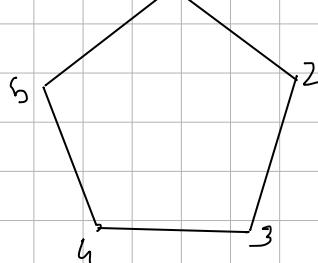


$$V_1 = \{1, 3, 5\} \quad V_2 = \{2, 4, 6\}$$

è bipartito

$$V_1 = \{1, 3, 5\} \quad V_2 = \{2, 4\}$$

non è bipartito

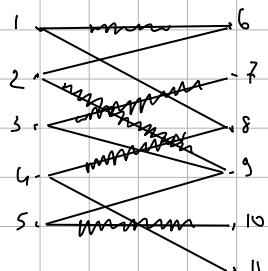


Sia  $G = (V, E)$  un grafo bipartito e sia  $M$  un accoppiamento di  $G$

**Def.** Si dice che  $M$  è un **accoppiamento** di  $V_1$  e  $V_2$  se  $\forall u \in V_1 \Rightarrow \exists v \in V_2$  tale che  $\{u, v\} \in M$

$v \in V_2$  accoppiato a qualche  $u$  di  $V_1$

E.g.



è un accoppiamento di  $V_1$  in  $V_2$

Sia  $S \subseteq V_1$  poniamo

$$N_G(S) := \{v \in V_2 : \exists u \in S \text{ con } \{u, v\} \in E\}$$

$$S = \{1, 3, 4\} \Rightarrow N_G(S) = \{6, 7, 8, 9, 11\}$$

**Teo 6.2.1 (Teorema di Hall, del matrimonio)**

Sia  $G = (V, E)$  un grafo bipartito allora esiste un accoppiamento di  $V_1$  in  $V_2$  se solo se

$$|S| \leq |N_G(S)| \quad \forall S \subseteq V_1$$

Sia  $G = (V, E)$  un grafo bipartito

**Def.** Si dice che  $G$  è **legato nei gradi** (o costretto nei gradi) da  $V_1$  a  $V_2$  se  $d(x) \geq d(y) \quad \forall x \in V_1 \text{ e } \forall y \in V_2$ .

**Prop 6.2.2** Sia  $G = (V, E)$  un grafo bipartito legato nei gradi da  $V_1$  e  $V_2$ . Allora esiste un accoppiamento da  $V_1$  in  $V_2$ .

Sia  $G = (V, E)$  un grafo.

**Def.**  $G$  si dice regolare (di grado  $r$ ) ( $r \in \mathbb{P}$ ) se  $d(x) = r \quad \forall x \in V$

**Cor 6.2.3.** Sia  $G = (V, E)$  un grafo bipartito e regolare. Allora  $\exists$  un accoppiamento di  $V_1$  in  $V_2$  e  $\exists$  un accoppiamento di  $V_2$  in  $V_1$ .

### 6.3 COLORAZIONI

Sia  $G = (V, E)$  un grafo e sia  $K \in \mathbb{P}$ .

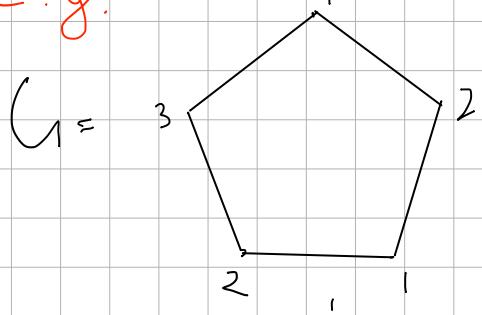
**Def.**  $G$  si dice colorabile in al più  $K$  colori se  $\exists f: V \rightarrow [K]$  tale che  $f(x) \neq f(y) \quad \text{se } \{x, y\} \in E$ .

Ad ogni vertice associo un numero con la proprietà che se due vertici sono collegati da 1 lato i numeri devono essere diversi.

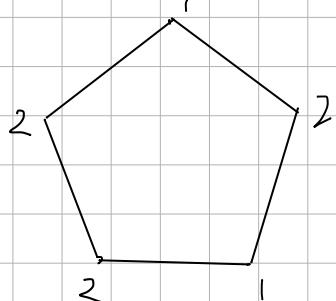
**Def.** Il numero cromatico di  $G$ , scritto

$\chi(G)$ , è il più piccolo  $K \in \mathbb{P}$  tale che  $G$  è colorabile in al più  $K$  colori.

E.g.



è una colorazione



non è una colorazione

$$\chi_6(G) = 3$$

Prop 6.3.1 Sia  $G = (V, E)$  un grafo allora

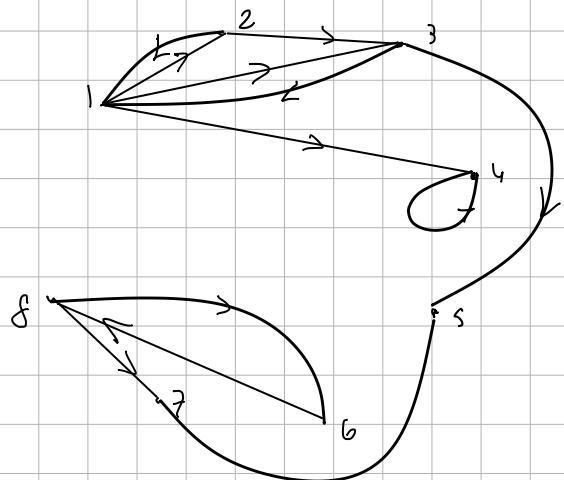
$$\chi(G) \leq \max_{v \in V} \{d(v)\} + 1.$$

## 6.4 GRAFI DIRETTI

Def. Un grafo diretto è una coppia  $D = (V, A)$  dove  $V$  è un insieme e  $A \subseteq V \times V$ . Si dice insieme dei vertici,  $A$  si dice insieme dei lati diretti (o spigoli diretti, o frecce).

Si rappresenta graficamente un grafo diretto disegnando un punto per ogni vertice e una freccia (anche curvilinea) da  $v_1$  a  $v_2$  se  $(v_1, v_2)$  appartiene ad  $A$ .

E.g.  $V = \{8\}$ ,  $A = \{(1,2), (1,3), (1,4), (2,3), (3,5), (3,1), (2,1), (4,4), (6,8), (8,7), (8,6), (7,5)\}$



E.g. Twitter è un grafo diretto

Sia  $D = (V, A)$  un digrafo

Def. Un cammino diretto in  $D$  è una sequenza  $(x_0, \dots, x_k) \in V^{k+1}$  tale che  $(x_i, x_{i+1}) \in A \quad \forall i = 0, \dots, k-1$

Def. Un sentiero diretto in  $D$  è un cammino diretto tale che  $x_i \neq x_j$  se  $0 \leq i < j \leq k$ .

Def. Un cammino diretto chiuso in  $D$  è un cammino diretto chiuso tale che  $x_0 = x_k$ .

Def. Un ciclo diretto in  $D$  è un cammino diretto chiuso tale che  $(x_0, \dots, x_{k-1})$  è un sentiero diretto.

Si dicono  $x, y \in V$ .

Def. Si dice che  $y$  è raggiungibile da  $x$  se

Esiste un cammino diretto  $T = (x_0, \dots, x_k)$  tale che  
 $x_0 = x$  e  $x_k = y$ . (si dice anche che  $T$  va da  $x$  a  $y$ ).

Def.  $x$  e  $y$  sono comparabili se o  $x$  è raggiungibile  
da  $y$  o viceversa. Altrimenti si dicono incomparabili.

Sia  $S \subseteq V$

Def. Si dice una catena se

$x, y \in S \Rightarrow x$  e  $y$  sono  
 $x \neq y$  comparabili

Def. Si dice una anticatena se

$x, y \in S \Rightarrow x$  e  $y$  sono  
 $x \neq y$  incomparabili

Sia  $v \in V$

Def. Il grado interno di  $v$  è (in-degree)

$$d_-(v) := |\{u \in V : (u, v) \in A\}|$$

Def. Il grado esterno di  $v$  è (out-degree)

$$d_+(v) := |\{u \in V : (v, u) \in A\}|$$

Def.  $D$  è ciclico se non ha cicli diretti.

## 6.5 RETI DI COMUNICAZIONE

Def. Una rete di comunicazione è una terna  $(R, I, O)$  dove  $R = (V, A)$  è un grafo diretto,  $I \subseteq V$ ,  $O \subseteq V$ ,  $I \cap O = \emptyset$  e  $|I| = |O| = N$ . Gli elementi di  $I$  si dicono nodi di input, quelli di  $O$  nodi di output

Def. Un problema di smistamento è una permutazione  $\pi \in S_N$ .

Sia  $\pi \in S_N$  come sopra.

Def. Uno smistamento per  $\pi$  è una  $(P_1, P_2, \dots, P_N)$  dove  $P_j$  è un sentiero diretto che va da  $i_j$  a  $\pi(i_j)$   $\forall j = 1, \dots, N$  dove  $I = \{i_1, i_2, \dots, i_N\}$  e  $O = \{\pi(i_1), \pi(i_2), \dots, \pi(i_N)\}$

Sia  $(P_1, \dots, P_N)$  uno smistamento per  $\pi$

Def. La latenza di  $(P_1, \dots, P_N)$  è  $\max \{ \text{lung}(P_1), \dots, \text{lung}(P_N) \}$ .

Def. La congestione di  $(P_1, \dots, P_N)$  è

$$c(P_1, \dots, P_N) = \max_{x \in V} \left\{ \left| \left\{ j \in [N] : x \in P_j \right\} \right| \right\}$$

massimo su tutti i vertici di numero di  $j$  che va da 1 a  $N$  tale che il vertice appartiene a  $P_j$

smistamento non è altro che una collezione di cammini che vanno dall'input all'output, la congestione guarda quanti cammini passano su di esso il max è la congestione

Siano  $x, y \in V$ ,  $x \neq y$

Def. La distanza da  $x$  a  $y$  è

$d(x, y) := \min \{ \text{lung}(P) : P \text{ è un sentiero diretto che va da } x \text{ a } y \}$

Def. Il diametro della rete di comunicazione è:

$\max \{ d(i_j, o_k) : j, k \in [N] \}$ .

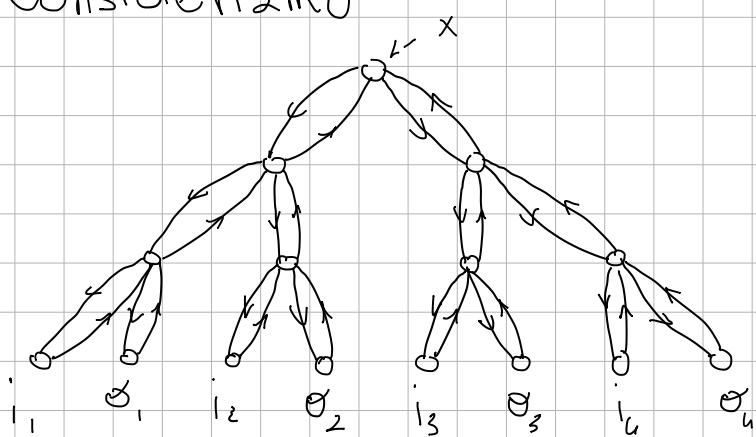
Sia  $(R, I, O)$  come sopra

Def. La congestione di  $(R, I, O)$  è

$\max_{\pi \in S_N} (\min_{(P_1, \dots, P_N)} C(P_1, \dots, P_N))$

(quindi  $\forall \pi \in S_N$ , prendiamo uno smistamento di congestione minima, e poi prendiamo il massimo di tutti questi minimi).

E.g. Consideriamo

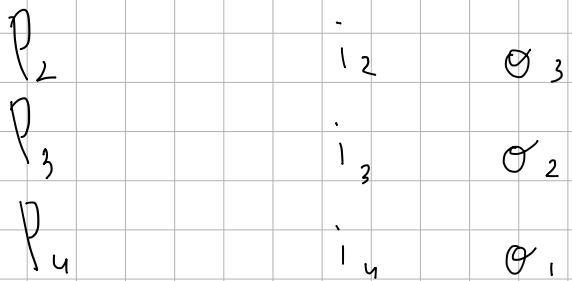


$\pi = 2bc$  collego  $i_1$  con  $x$ ,  $i_2$  con  $b$  e così via

$$\text{diametro} = d(i, \sigma_u) = 6$$

$\text{Si} z \pi = 4321 \quad \text{Si} z (P_1, \dots, P_6)$  uno smistamento

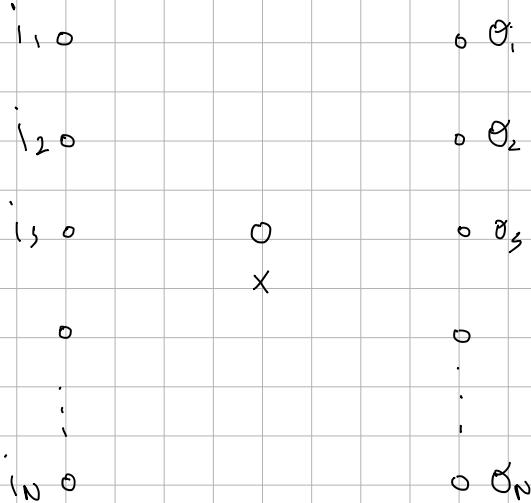
per  $\pi \Rightarrow P_i$  vede  $\delta_2$  i, 2  $\sigma_u$



$\Rightarrow x \in P_1 \cap P_2 \cap P_3 \cap P_4 \Rightarrow c(P_1, \dots, P_4) = 4$   
passano tutti per  $x$

$\Rightarrow \delta_2$  congestione della rete è 4

E.g. Il "mostro" di ordine N



$\delta_2$  congestione è N, il numero di vertici è  $2N+1$

$\text{Si} z (L, I, O)$  come sopra.

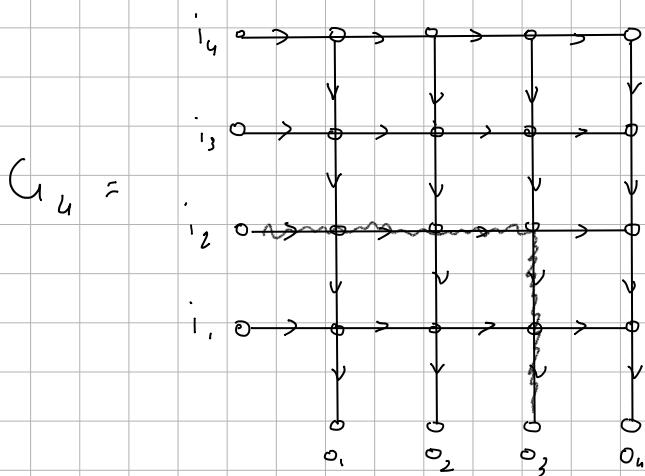
(I vertici si dicono anche switch)

Def. La grandezza di  $v \in V$  è  $(d_+(v), d_-(v))$

(anche detto che  $v$  è uno switch  $d_+(v) \times d_-(v)$ )

Obiettivo: bassa congestione, pochi switch e switch piccoli

L<sub>2</sub> griglia



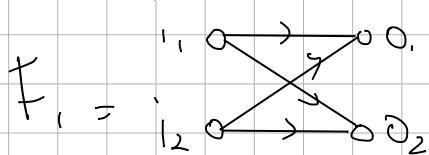
P<sub>j</sub> v<sub>2</sub> d<sub>2</sub> i<sub>j</sub> 2 o<sub>π(j)</sub>

Teo 6.5.1

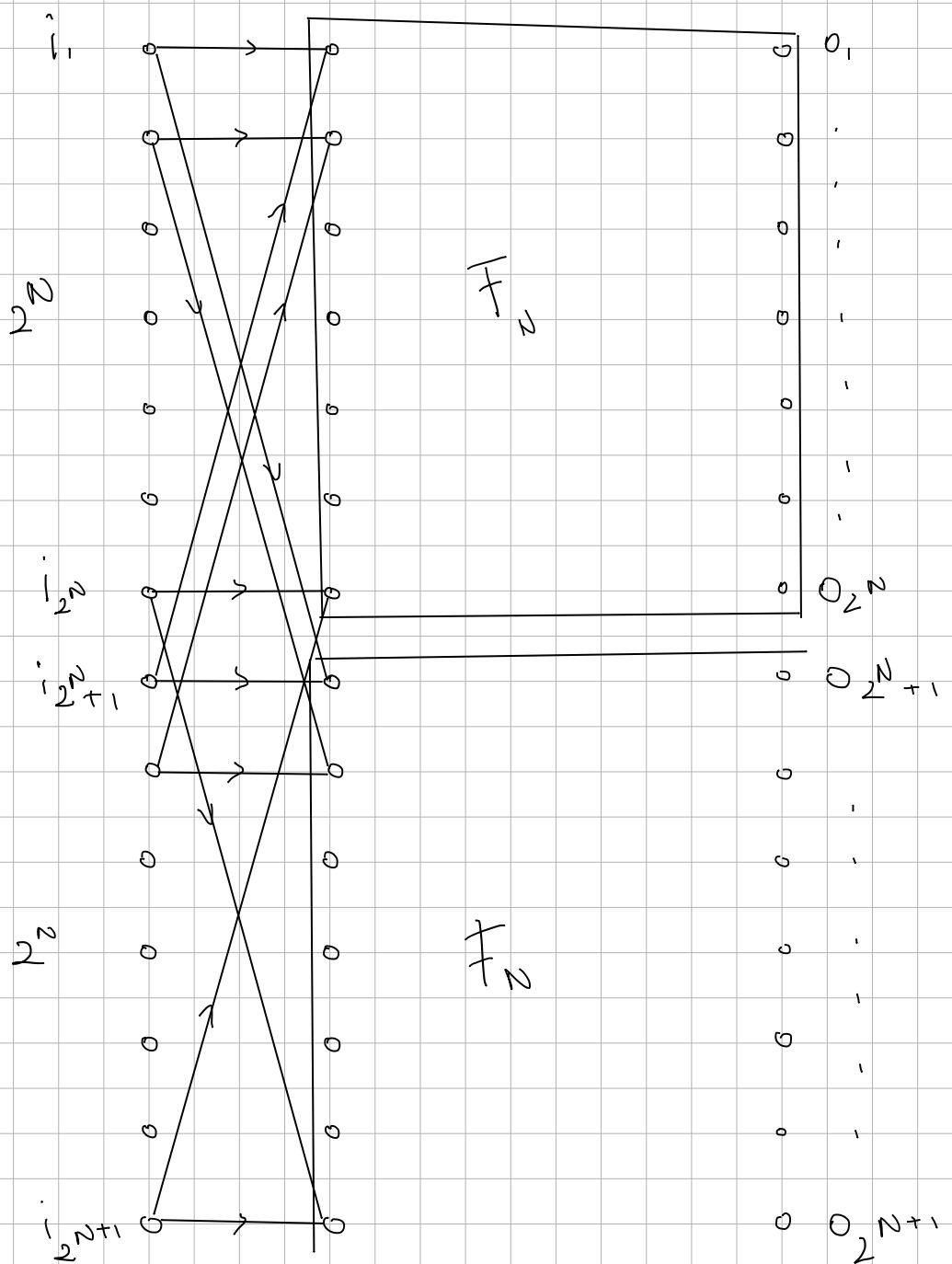
L<sub>2</sub> griglia  $G_N$  ( $\Rightarrow |I| = N$ ) ha  $N^2 + 2N$  vertici, switch più grande  $2 \cdot 2$  e congestione 2

L<sub>2</sub> farfalla

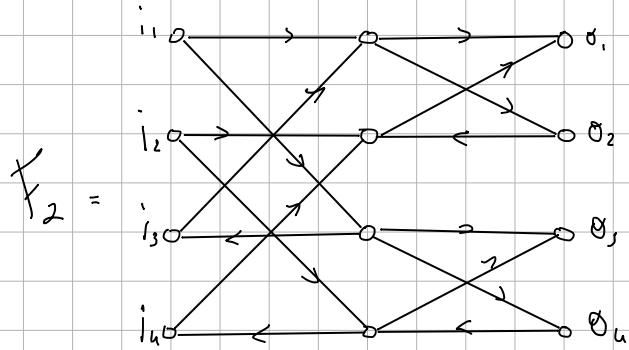
L<sub>2</sub> farfalla con  $|I| = 2^n$ ,  $F_N$ , è definita  
induttivamente come segue

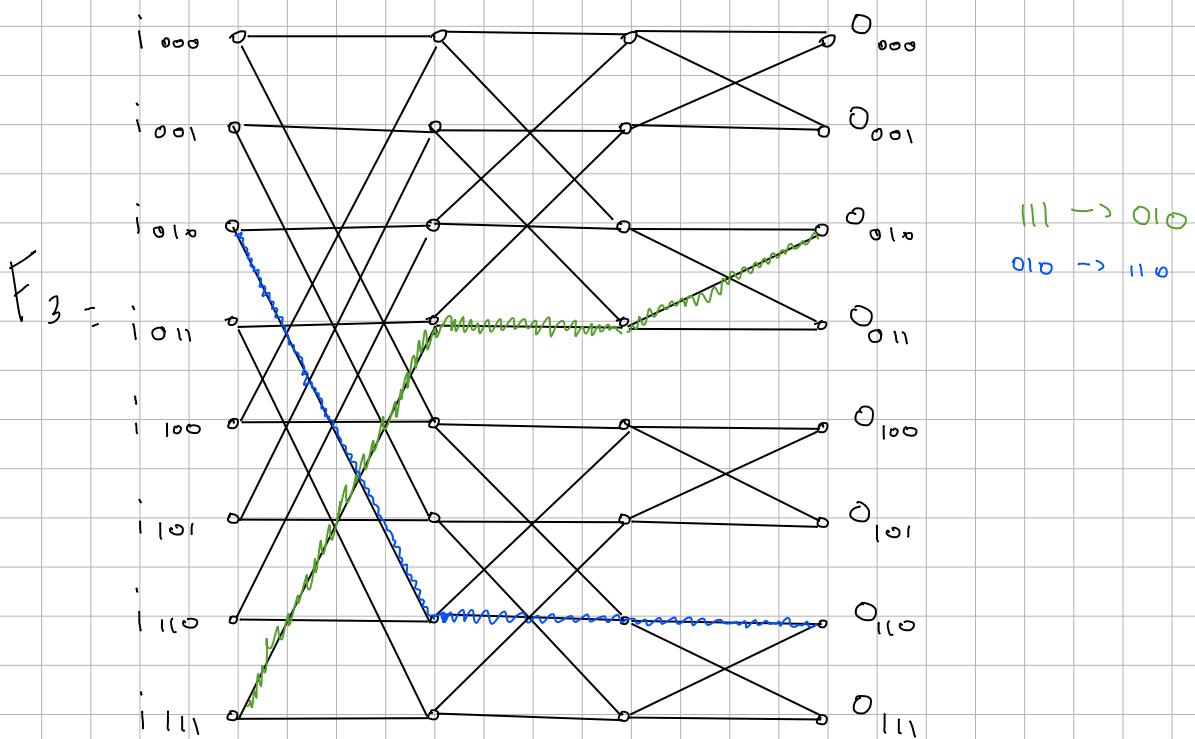


Sia  $F_N$  definita. Allora  $F_{N+1}$  è definita come  
segue:



Quindi





Formalmente  $F_K = (R, I, O)$  dove  $R = (V, E)$  e

$$V := \left\{ (\varepsilon_1, \dots, \varepsilon_{K+1}) \in \underbrace{\{0,1\} \times \dots \times \{0,1\}}_{K+1} \times \{0,1\} \right\}$$

$$\text{e } (\varepsilon_1, \dots, \varepsilon_{K+1}) \xrightarrow{\text{meta}} (\eta_1, \dots, \eta_{K+1}) \text{ se } j = i+1 \text{ e } \varepsilon_r = \eta_r \quad \forall r \in [K] \setminus \{i\}$$

$$\text{e } I := \left\{ (\varepsilon_1, \dots, \varepsilon_{K+1}) \in \{0,1\} \times \dots \times \{0,1\} \times \{1\} \right\}$$

$$\text{e } O := \left\{ (\varepsilon_1, \dots, \varepsilon_{K+1}) \in \{0,1\} \times \dots \times \{0,1\} \times \{K+1\} \right\}$$

E.g. Qual' è  $c(F_3)$ ?

Notiamo che presi  $(\varepsilon_1, \dots, \varepsilon_{K+1}) \in I$  e

$(\eta_1, \dots, \eta_{K+1}) \in O \Rightarrow \exists!$  cammino diretto dal primo

al secondo, in  $F_K$

(per es.  $F(u)$ )

$$\left( \begin{smallmatrix} 0 & 1 & 0 & 1 & 1 \\ \downarrow & & & & \\ 0 & 1 & 0 & 1 & 2 \end{smallmatrix} \right) \xrightarrow{\text{n^a colonna}} \left( \begin{smallmatrix} 1 & 1 & 0 & 1 & 2 \\ \downarrow & & & & \\ 1 & 1 & 0 & 1 & 3 \end{smallmatrix} \right) \xrightarrow{\text{n^a colonna}} \left( \begin{smallmatrix} 1 & 1 & 0 & 1 & 4 \\ \downarrow & & & & \\ 1 & 1 & 0 & 1 & 5 \end{smallmatrix} \right)$$

Quanti cammini passano per  $(0, 1, 1, 2)$ ? al massimo 2

per  $(1, 0, 0, 3)$ ? al massimo 2

$$\Rightarrow c(F_3) = 2$$

con lo stesso ragionamento si dimostra che

**Teo 6.5.2**

La congestione di  $F_k$  ( $k \in \mathbb{P}$ ) è

$$c(F_k) = \begin{cases} \sqrt{\frac{N}{2}} & \text{se } k \equiv 1 \pmod{2} \text{ e dispari} \\ \sqrt{N} & \text{se } k \equiv 0 \pmod{2} \text{ e pari} \end{cases}$$

$$\text{dove } N = |I| = |O| = 2^k$$