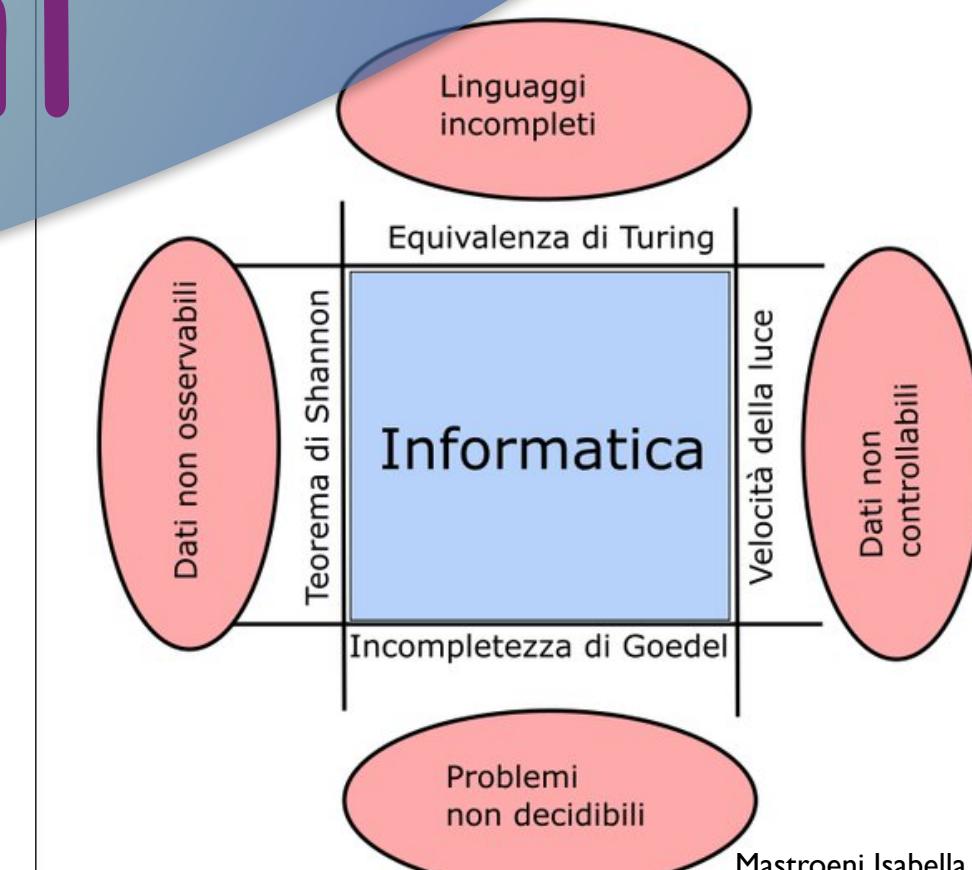
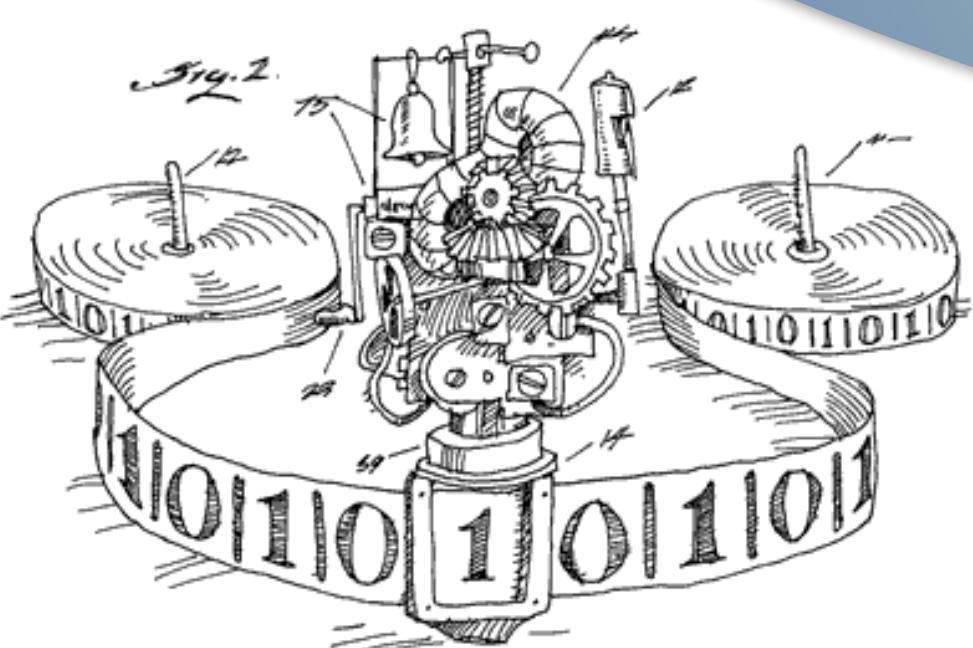


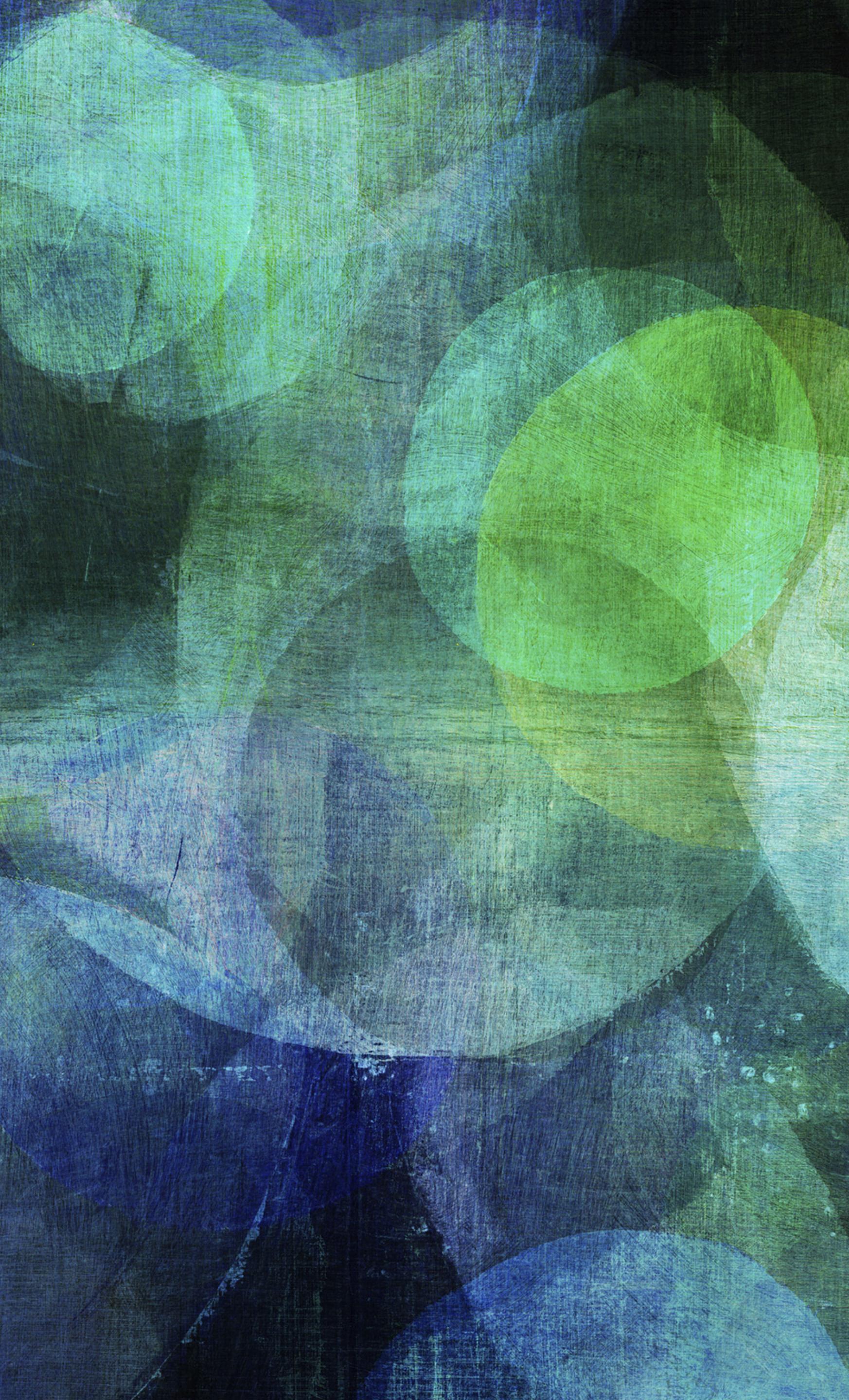


FONDAMENTI DELL'INFORMATICA

Prof.ssa Isabella Mastroeni
Dip. Informatica

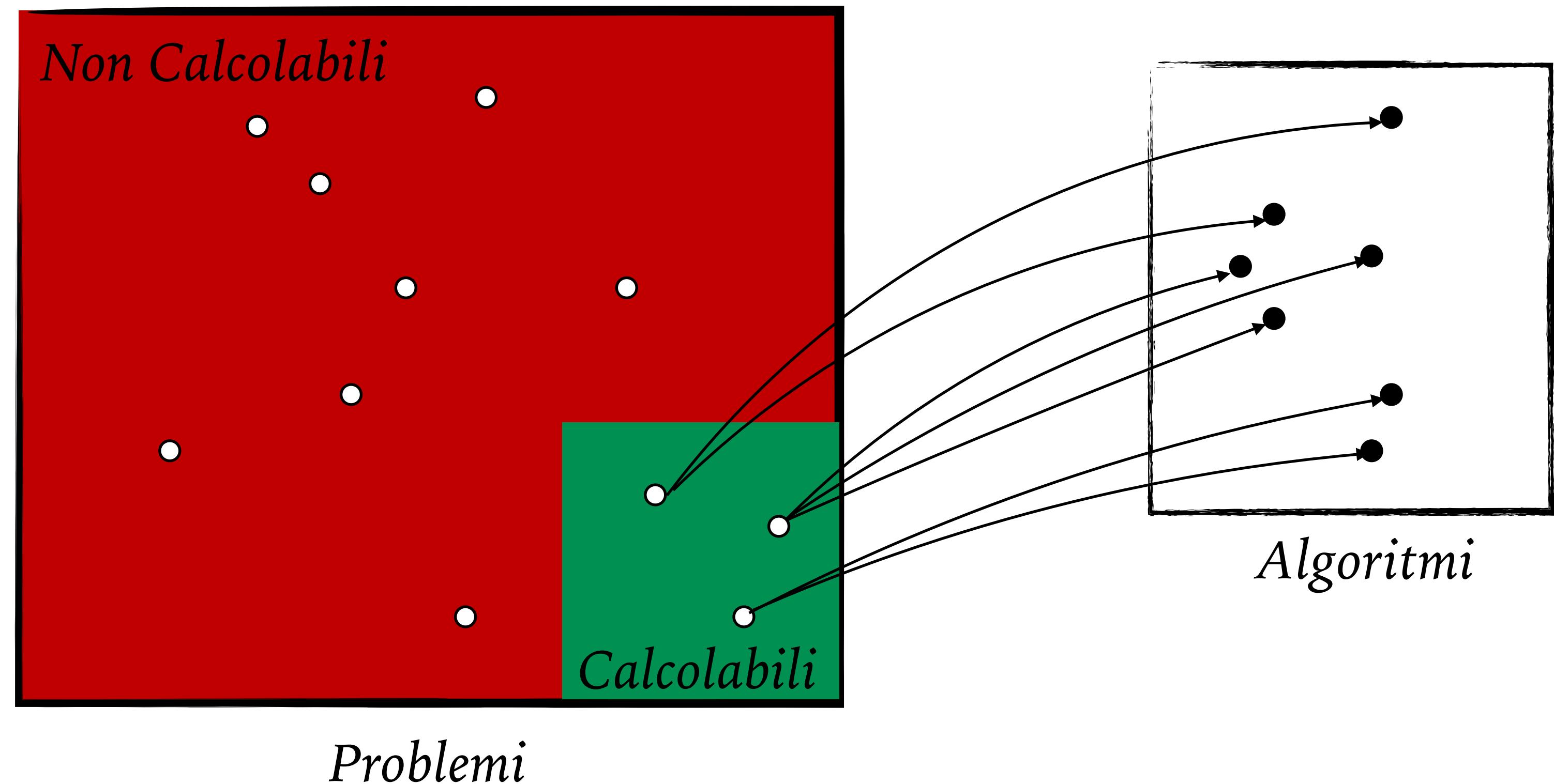


IL PROBLEMA DELL' INFORMATICA



SCIENZA DEL CALCOLARE

- **Problema** = Funzione $f: \mathbb{N} \rightarrow \mathbb{N}$,
- **Problema calcolabile** = funzione calcolabile mediante algoritmo
- **Algoritmo** = Sequenza FINITA di passi discreti (simboli) - programma P nel linguaggio L
- Quale relazione esiste?



QUANTE FUNZIONI CI SONO?

- $f:\mathbb{N} \rightarrow \mathbb{N}$, funzione su \mathbb{N} , è un insieme di coppie dentro \mathbb{N} , $f \subseteq \mathbb{N} \times \mathbb{N}$
- $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ (enumerazione lessicografica delle coppie)
- $|\wp(\mathbb{N})| = |\mathbb{N} \rightarrow \mathbb{N}|$
- $|\wp(\mathbb{N})| = |\mathbb{N} \rightarrow \{0,1\}|$: Per ogni insieme S posso fornire la funzione caratteristica, ovvero $f(x) = 1$ se $x \in S$, $f(x) = 0$ altrimenti, e viceversa.
- $|\mathbb{N} \rightarrow \{0,1\}| = |\mathbb{N} \rightarrow \mathbb{N}|$: $\{0,1\} \subseteq \mathbb{N}$, quindi $f:\mathbb{N} \rightarrow \{0,1\}$ è tale che $f:\mathbb{N} \rightarrow \mathbb{N}$, ma se $f:\mathbb{N} \rightarrow \mathbb{N}$ posso costruire la funzione caratteristica dal suo grafico, ovvero esiste unica $g:\mathbb{N} \rightarrow \{0,1\}$
- **L'insieme delle funzioni su \mathbb{N} è equipotente all'insieme dei sottoinsiemi di \mathbb{N} ,**

QUANTI PROBLEMI CALCOLABILI CI SONO?

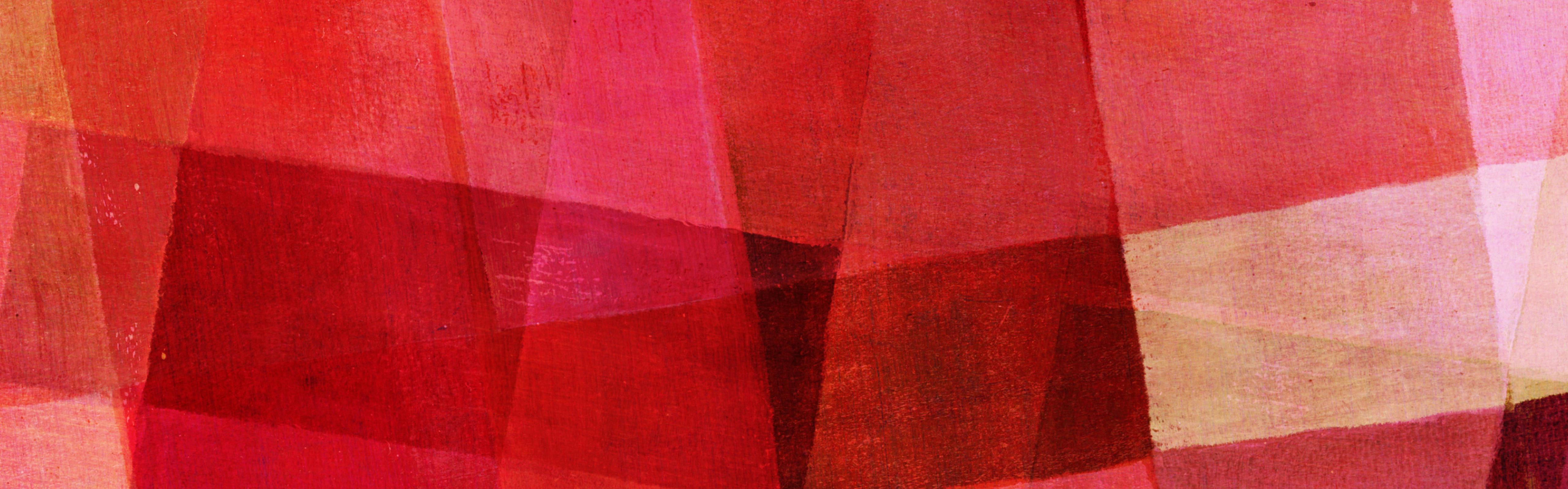
- Sia Σ l'alfabeto con cui possiamo scrivere i nostri programmi, allora un programma non è altro che una sequenza finita di simboli di Σ : $s_1s_2s_3 \dots s_n$
- Gli algoritmi o programmi che possiamo descrivere sono quindi tanti quanti le sequenze finite di simboli di Σ : $|Alg| = |\Sigma^*| = |\mathbb{N}|$
- $|Alg| = |\mathbb{N}|$: Supponiamo inoltre che i dati manipolabili dai programmi siano anch'essi numerabili, ovvero siano numeri, quindi $Alg \subseteq \mathbb{N} \rightarrow \mathbb{N}$:
 - Problemi calcolabili = $\{f:\mathbb{N} \rightarrow \mathbb{N} \mid f=[P], P \in Alg\} = Alg$
 - **L'insieme delle funzioni descrivibili mediante algoritmi Alg è equipotente all'insieme dei numeri naturali \mathbb{N}**

IL PROBLEMA DI CARDINALITÀ

- Teorema di Cantor. Sia S un insieme. $|S| < |\wp(S)|$
- Per assurdo assumiamo esista una funzione $f : S \rightarrow \wp(S)$ biiettiva (iniettiva e suriettiva). Sia $A = \{x \in S \mid x \notin f(x)\}$. Poiché $A \in \wp(S)$ e f è per ipotesi suriettiva, deve esistere $a \in S$ tale che $f(a) = A$. Ora, chiediamoci se a appartenga o meno ad A :
 - se $a \in A$ allora, per definizione di A , $a \notin f(a) = A$;
 - se $a \notin A = f(a)$ allora, per definizione di A , $a \in A$.
- In entrambi i casi si giunge ad una contraddizione: l'unica ipotesi che abbiamo fatto è quella dell'esistenza di una f biettiva, che pertanto non può essere vera.
- Quindi: $|\text{Alg}| = |\mathbb{N}| < |\wp(\mathbb{N})| = |\mathbb{N} \rightarrow \mathbb{N}|$

E LA ENUMERABILITÀ?

- Diciamo che un insieme S è numerabile se $|S| = |\mathbb{N}|$
- Il numero di funzioni calcolabili mediante algoritmo è numerabile
- Ipotesi del continuo (CH): Ogni sottoinsieme di \mathbb{R} è o numerabile o di cardinalità $|\wp(\mathbb{N})|$ (Godel-Cohen)
 - Teorema: $|\mathbb{R}| = |\wp(\mathbb{N})|$
 - Un insieme A è non-numerabile se $|\wp(\mathbb{N})| \geq |A| > |\mathbb{N}|$.
- Il numero di funzioni su \mathbb{N} ($|\mathbb{N} \rightarrow \mathbb{N}|$) è non numerabile



QUALCHE NOZIONE DI BASE

2024/2025

QUALCHE NOZIONE... DI LOGICA

- Linguaggio del primo ordine:
 - Simboli relazionali (p, q, \dots)
 - Simboli funzionali (f, g, \dots)
 - Simboli costanti (c, d, \dots)
 - Simboli logici
 - Parentesi (,) e virgola
 - Insieme numerabile di variabili (v, x, \dots)
 - Insieme di connettivi logici: $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$
 - Quantificatori: \forall (per ogni) e \exists (esiste)
 - Alcuni quantificati sono superflui per equivalenze e leggi di De Morgan

QUALCHE NOZIONE.. DI LOGICA

- Termine
 - Variabili
 - Costanti
 - f simbolo di funzione m -ario, t_1, t_2, \dots, t_m termini, allora $f(t_1, t_2, \dots, t_m)$ è termine
- Formula atomica: p simbolo di relazione n -ario, t_1, t_2, \dots, t_m termini, allora $p(t_1, t_2, \dots, t_m)$ è formula atomica
- Formula
 - Formula atomica
 - φ formula, allora $(\neg\varphi)$ formula
 - φ e ψ formule, allora $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$ sono formule
 - φ formula, v variabile, allora $\forall x(\varphi)$ e $\exists x(\varphi)$ sono formule

QUALCHE NOZIONE.. DI LOGICA

► Equivalenze

- $\neg(\neg\varphi) = \varphi$
- $\neg(\varphi \wedge \psi) = (\neg\varphi) \vee (\neg\psi)$ e $\neg(\varphi \vee \psi) = (\neg\varphi) \wedge (\neg\psi)$. De Morgan
- $(\varphi \Rightarrow \psi) = (\neg\varphi) \vee \psi = ((\neg\psi) \Rightarrow (\neg\varphi))$ Controvariante
- $\neg(\exists x(\varphi)) = \forall x(\neg\varphi)$ e $\neg(\forall x(\varphi)) = \exists x(\neg\varphi)$

► Abbreviazioni

- $(\exists x \in S. \varphi) = \exists x(x \in S \wedge \varphi)$
- $(\forall x \in S. \varphi) = \forall x(x \in S \Rightarrow \varphi)$

QUALCHE NOZIONE.. SUGLI INSIEMI

- $x \in A$ significa che x è un elemento dell'insieme A
- $\{x \mid P(x)\}$ si identifica l'insieme costituito dagli x che soddisfano (rendono vera) una dato predicato P (Rappresentazione intensionale)
- $A \subseteq B$ indica che A è un sottoinsieme di B , ovvero che $\forall x. x \in A \Rightarrow x \in B$. $A \subset B$ denota l'inclusione stretta ovvero $A \subseteq B$ e A diverso da B
- $\wp(S)$ denota l'insieme delle parti (dei sottoinsiemi) di S , $\{X \mid X \subseteq S\}$
- $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$, $A \cup B = \{x \mid x \in A \vee x \in B\}$, $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- $|A|$ denota la cardinalità (ovvero il numero di elementi) di A
- \bar{A} denota il complemento di A , ovvero $x \in \bar{A} \Leftrightarrow x \notin A$

QUALCHE NOZIONE.. SULLE RELAZIONI

- **PRODOTTO CARTESIANO:** $A_1 \times A_2 \times \cdots \times A_n = \{\langle x_1, \dots, x_n \rangle \mid x_1 \in A_1, \dots, x_n \in A_n\}$
- Una RELAZIONE (binaria) è un sottoinsieme del prodotto cartesiano di (due) insiemi; dati A e B , $R \subseteq A \times B$ è una relazione su A e B
 - **riflessiva:** $\forall a \in S$ si ha che aRa ,
 - **simmetrica:** $\forall a, b \in S$ si ha che $aRb \Rightarrow bRa$
 - **antisimmetrica:** se $\forall a, b \in S$ si ha che $(aRb \wedge bRa) \Rightarrow a=b$
 - **transitiva:** $\forall a, b, c \in S$ si ha che $(aRb \wedge bRc) \Rightarrow aRc$.
- Per ogni relazione $R \subseteq S \times S$, la *chiusura transitiva* di R è il più piccolo insieme R^* tale che: $\langle a, b \rangle \in R^* \wedge \langle b, c \rangle \in R^* \Rightarrow \langle a, c \rangle \in R^*$

QUALCHE NOZIONE.. SULLE RELAZIONI

- Una relazione R è detta *totale* su S se $\forall a,b \in S$ si ha che $(aRb \vee bRa)$
- Una relazione R di *equivalenza* è una relazione binaria riflessiva, simmetrica e transitiva
- Una relazione binaria $R \subseteq S \times S$ è un *pre-ordine* se essa è riflessiva e transitiva.
- R è un *ordine parziale* se è un pre-ordine ed è *anti-simmetrica*
- $x \in S$ è *minimale* rispetto a R se $\forall y \in S$. $y \not R x$ (ovvero $\neg(yRx)$).
- $x \in S$ è *minimo* se $\forall y \in S$. $x R y$
- $x \in S$ è *massimale* rispetto a R se $\forall y \in S$. $x \not R y$ (ovvero $\neg(xRy)$).
- $x \in S$ è *massimo* se $\forall y \in S$. $y R x$

QUALCHE NOZIONE.. SULLE FUNZIONI

- Una relazione $f \subseteq C \times D$ è una funzione se $\forall x \in C \ \exists$ uno ed un solo $y \in D$ tale che $(x,y) \in f$, in tal caso scriviamo $f(x)=y$ e $f: C \rightarrow D$, $f=\{(x,f(x))|x \in C\} \subseteq C \times D$
- **C dominio e D co-dominio di f. Il range di f è l'insieme $\{f(x) \in D | x \in C\}$**
- f iniettiva se $f(x)=f(y) \Rightarrow x=y$, f suriettiva se $\forall y \in D. \exists x \in C$ tale che $y=f(x)$
- Se $f:C \rightarrow D$ è sia infettiva che suriettiva, è detta *biettiva* e descrive una corrispondenza biunivoca tra C e D
- *Immagine:* Sia $X \subseteq C$, $f(X)=\{f(x)|x \in X\} \subseteq D$
- *Immagine inversa:* Sia $Y \subseteq D$, $f^{-1}(Y)=\{x | f(x) \in Y\} \subseteq C$

QUALCHE NOZIONE.. L'INDUZIONE

- Dato un dominio A e una relazione su esso $<$: $(A, <)$
- *Induzione matematica*: $A = \text{Nat}$
- *Induzione strutturale*: $A = L(G)$ ($L(G)$ linguaggio generato dalla grammatica G)

Una relazione binaria $< \subseteq A \times A$ è ben fondata se non esistono catene discendenti infinite. In tal caso si dice che A è ben fondato.

- NB: Una relazione riflessiva non è mai ben fondata!

Un elemento $b \in A$ è minimale se $\forall b_i < b$, allora $b_i \notin A$.

Th: Una relazione $<$ su A è ben fondata sse $\forall B \subseteq A$, B ha un elemento minima

QUALCHE NOZIONE.. L'INDUZIONE

Dato un insieme ben fondato $A (<)$. Sia π una proprietà definita sugli elementi di A , allora

$$\forall a \in A. \pi(a) \text{ sse } \forall a \in A. ([\forall b < a. \pi(b)] \Rightarrow \pi(a))$$

Ipotesi induttiva

Passo induttivo

Base induttiva

Per applicare il principio dobbiamo prima dimostrare π per ogni elemento minima: *Base induttiva*

Dato un insieme ben fondato $A (<)$.

Sia $\text{Base}_A = \{a \in A \mid a \text{ minima}\}$

$$\forall a \in A. \pi(a) \text{ sse }$$

$$\forall a \in \text{Base}_A. \Pi(a) \wedge \forall a \in A \setminus \text{Base}_A. ([\forall b < a. \pi(b)] \Rightarrow \pi(a))$$

QUALCHE NOZIONE.. L'INDUZIONE: DIMOSTRAZIONE

(\Rightarrow) Banale.

(\Leftarrow) Supponiamo che $\forall a \in A \setminus \text{Base}_A. ([\forall b < a. \pi(b)] \Rightarrow \pi(a))$ sia vero, dimostriamo per assurdo. Suppongo esista a_i tale che $\neg\pi(a_i)$, prendiamo $C = \{a_i \in A | \neg\pi(a_i)\} \subseteq A$, poiché A è ben fondato C ha elemento minimale \underline{a} , quindi $\neg\pi(\underline{a})$.

Ora per ipotesi induttiva $\forall b < \underline{a}. \pi(b)$, questo perché \underline{a} è minimale in C , quindi $b \notin C$ implica $\pi(b)$, ma allora per ipotesi abbiamo che vale $\pi(\underline{a})$, che è assurdo.

Esempio: Induzione matematica.

QUALCHE NOZIONE.. L'INDUZIONE: ESEMPIO

Dimostrare che $\sum_{i=1}^m i = \frac{m(m+1)}{2} \quad m \geq 1$

BASE : $m=1 \quad \sum_{i=1}^1 i = 1 = \frac{1(1+1)}{2} \quad \checkmark$

Dimostriamo per $m+1$: $\sum_{i=1}^{m+1} i = \frac{(m+1)(m+2)}{2}$

PASSO INDUTTIVO :

Supponiamo vero per m

(Ipotesi induttiva $\sum_{i=1}^m i = \frac{m(m+1)}{2}$)

$$\sum_{i=1}^{m+1} i = \sum_{i=1}^m i + (m+1) = \underbrace{\frac{m(m+1)}{2}}_2 + m+1 =$$

per definizione
di \sum

per ipotesi
induttiva

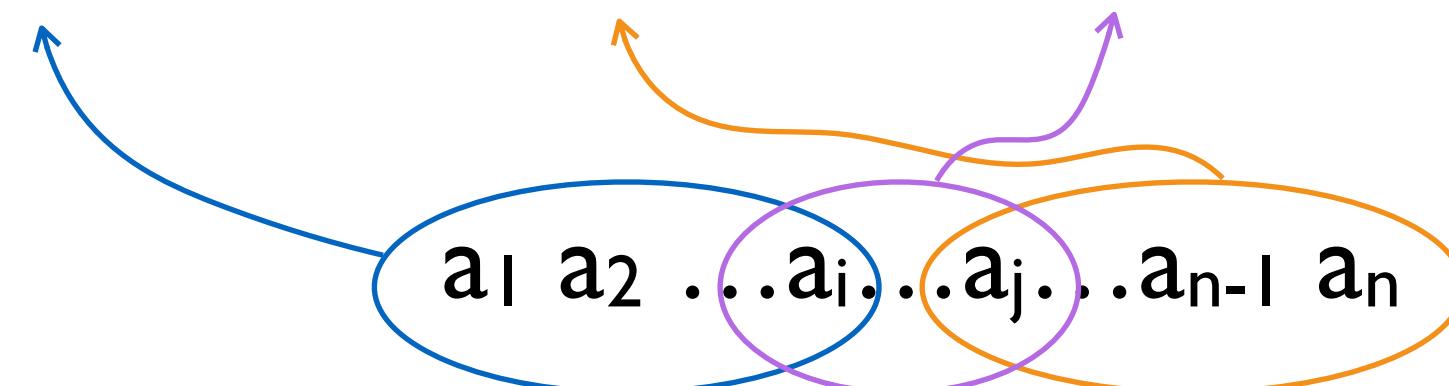
$$= \frac{m(m+1) + 2m+2}{2} = \frac{m^2 + m + 2m + 2}{2} =$$

$$= \frac{(m+1)m + (m+1)2}{2} = \frac{(m+1)(m+2)}{2} \quad \checkmark$$

QUALCHE NOZIONE.. SULLE STRINGHE

- **SIMBOLO**: entità primitiva (lettere, caratteri)
- **STRINGA/PAROLA**: sequenza di simboli
- **LUNGHEZZA**: la lunghezza di una stringa x è $|x|$ ed è il numero di occorrenze di simboli in x
- NB: è sbagliato dire il numero di simboli

- **PREFISSO**, **SUFFISSO** e **SOTTOSTRINGA**



QUALCHE NOZIONE.. SULLE STRINGHE

- **CONCATENAZIONE:** di due stringhe u e v è la stringa ottenuta facendo seguire alla prima stringa u la seconda v , uv . La stringa vuota ϵ è l'elemento neutro.
- **ALFABETO:** insieme finito di simboli Σ
- **LINGUAGGIO (FORMALE):** insieme di stringhe composte da simboli in un alfabeto Σ
 - \emptyset e $\{\epsilon\}$ sono linguaggi e sono indipendenti dall'alfabeto
 - Σ^* denota il linguaggio di tutte le stringhe sull'alfabeto Σ , se Σ non è vuoto allora Σ^* è sempre infinito numerabile
 - Un linguaggio formale è $L \subseteq \Sigma^*$