# Richiami matematici

Corso di Fondamenti di Informatica - modulo 1
Corso di Laurea in Informatica
Università di Roma "Tor Vergata"
a.a. 2020-2021

Giorgio Gambosi

## Insiemi di particolare interesse

| simbolo | descrizione |
|---|---|
| $\mathbb{N}$ | naturali |
| $\mathbb{N}^+$ | naturali positivi |
| $\mathbb{Z}$ | interi |
| $\mathbb{Z}^+$ | interi positivi (coincide con $\mathbb{N}^+$) |
| $\mathbb{Z}^-$ | interi negativi |
| $\mathbb{Q}$ | razionali |
| $\mathbb{Q}^+$ | razionali positivi |
| $\mathbb{Q}^-$ | razionali negativi |
| $\mathbb{R}$ | reali |
| $\mathbb{R}^+$ | reali positivi |
| $\mathbb{R}^-$ | reali negativi |

## Sintassi del calcolo proposizionale

- Insieme non vuoto di elementi denominati *simboli proposizionali* $\mathcal{A} = \{A, B, C, \ldots\}$.
- Costanti proposizionali $\top$ e $\bot$. Per contrapposizione, i simboli proposizionali sono anche denominati *variabili proposizionali*.
- *Connettivi logici* $\neg$, $\vee$ e $\wedge$.
- *Separatori* '(' e ')'.

## Proposizioni

- se $a$ è una variabile o costante proposizionale allora $a$ è una proposizione;
- se $\alpha$ è una proposizione allora $(\neg\alpha)$ è una proposizione;
- se $\alpha$ e $\beta$ sono proposizioni allora $(\alpha \vee \beta)$ e $(\alpha \wedge \beta)$ sono proposizioni;
- tutte le proposizioni sono ottenute mediante le regole descritte.

## Esempi di proposizioni e non

- $((\neg\bot) \vee ((A \vee B) \wedge C))$ è una proposizione.
- $A \vee B$ non è una proposizione

- $(A \wedge B)A \top B$ non è una proposizione

### Semantica del calcolo proposizionale

- Dominio: insieme $\mathcal{B} = \{0, 1\}$, in cui $0$ è associato al valore di verità falso e $1$ al valore vero
- Insieme di operatori $\mathcal{O} = \{o_\neg, o_\vee, o_\wedge\}$, contiene un elemento per ciascuno dei connettivi logici del calcolo proposizionale

#### Negazione logica (*not*)

$o_\neg : \mathcal{B} \mapsto \mathcal{B}$, tale che $o_\neg(0) = 1$ e $o_\neg(1) = 0$

| $a$ | $\neg a$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

#### Congiunzione logica (*and*)

$o_\wedge : \mathcal{B} \times \mathcal{B} \mapsto \mathcal{B}$

Definito dalla seguente tabella di verità

| $a$ | $b$ | $a \wedge b$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

#### Disgiunzione logica (*or*)

$o_\vee : \mathcal{B} \times \mathcal{B} \mapsto \mathcal{B}$

Definito dalla seguente tabella di verità

| $a$ | $b$ | $a \vee b$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

#### Assegnazione booleana $\mathcal{V}$

Funzione $\mathcal{V} : \mathcal{A} \mapsto \mathcal{B}$: un'assegnazione booleana alle variabili proposizionali altro non è che una associazione di valori di verità alle variabili stesse.

#### Valutazione booleana

Prop insieme delle proposizioni, $\mathcal{V}$ assegnazione booleana su $\mathcal{A}$.

- se $A \in \mathcal{A}$, $\mathcal{I}_\mathcal{V}(A) = \mathcal{V}(A)$
- $\mathcal{I}_\mathcal{V}(\top) = 1$
- $\mathcal{I}_\mathcal{V}(\bot) = 0$
- se $\alpha \in$ Prop, $\mathcal{I}_\mathcal{V}(\neg\alpha) = o_\neg(\mathcal{I}_\mathcal{V}(\alpha))$
- se $\alpha, \beta \in$ Prop, $\mathcal{I}_\mathcal{V}(\alpha \vee \beta) = o_\vee(\mathcal{I}_\mathcal{V}(\alpha), \mathcal{I}_\mathcal{V}(\beta))$
- se $\alpha, \beta \in$ Prop, $\mathcal{I}_\mathcal{V}(\alpha \wedge \beta) = o_\wedge(\mathcal{I}_\mathcal{V}(\alpha), \mathcal{I}_\mathcal{V}(\beta))$

#### Soddisfacibilità

Una formula proposizionale $\alpha$ viene detta:

- *soddisfatta* da una valutazione booleana $\mathcal{I}_\mathcal{V}$ se $\mathcal{I}_\mathcal{V}(\alpha) = 1$.

- *soddisfacibile* se è soddisfatta da *almeno* una valutazione booleana
- *tautologia* se è soddisfatta da *ogni* valutazione booleana
- *contraddizione* se non è soddisfatta da *nessuna* valutazione booleana

Implicazione

$o_{\rightarrow} : \mathcal{B} \times \mathcal{B} \mapsto \mathcal{B}$

Definito dalla seguente tabella di verità

| $a$ | $b$ | $a \rightarrow b$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

$a \rightarrow b$ equivalente a $\neg a \vee b$

Equivalenza

$o_{\leftrightarrow} : \mathcal{B} \times \mathcal{B} \mapsto \mathcal{B}$

Definito dalla seguente tabella di verità

| $a$ | $b$ | $a \leftrightarrow b$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

$a \leftrightarrow b$ equivalente a $(a \leftrightarrow b) \wedge (b \leftrightarrow a)$

Operatori $k$-ari

Dato $k$, esistono $2^{2^k}$ operatori differenti $\mathcal{B}^k \mapsto \mathcal{B}$.

Se $k = 2$:

| $a$ | $b$ | zero | and ($\wedge$) | n-implicazione ($\not\rightarrow$) | operando-1 | n-implicato ($\not\leftarrow$) | operando-2 | ex-or ($\oplus$) | or ($\vee$) | nor ($\dot{\vee}$) | equivalenza ($\leftrightarrow$) | n-operando-2 | implicato ($\leftarrow$) | n-operando-1 | implicazione ($\rightarrow$) | nand ($\dot{\wedge}$) | uno |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

Completezza di $\{\neg, \vee, \wedge\}$

Ogni operatore binario è equivalente ad una opportuna composizione degli operatori $\{\neg, \vee, \wedge\}$

### Proprietà degli operatori 1

| | |
|---|---|
| *idempotenza* | $\alpha \wedge \alpha \equiv \alpha$<br>$\alpha \vee \alpha \equiv \alpha$ |
| *associatività* | $\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$<br>$\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$<br>$\alpha \leftrightarrow (\beta \leftrightarrow \gamma) \equiv (\alpha \leftrightarrow \beta) \leftrightarrow \gamma$ |
| *commutatività* | $\alpha \wedge \beta \equiv \beta \wedge \alpha$<br>$\alpha \vee \beta \equiv \beta \vee \alpha$<br>$\alpha \leftrightarrow \beta \equiv \beta \leftrightarrow \alpha$ |
| *distributività* | $\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$<br>$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$ |

### Proprietà degli operatori 2

| | |
|---|---|
| *assorbimento* | $\alpha \wedge (\alpha \vee \beta) \equiv \alpha$<br>$\alpha \vee (\alpha \wedge \beta) \equiv \alpha$ |
| *doppia negazione* | $\neg\neg\alpha \equiv \alpha$ |
| *leggi di De Morgan* | $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$<br>$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$ |
| *terzo escluso* | $\alpha \vee \neg\alpha \equiv \top$ |
| *contrapposizione* | $\alpha \to \beta \equiv \neg\beta \to \neg\alpha$ |
| *contraddizione* | $\alpha \wedge \neg\alpha \equiv \bot$ |

### Quantificatori

Calcolo dei predicati

- *quantificatore universale*, indicato con il simbolo $\forall$
  $\forall x P(x)$, $P$ è vero per qualunque valore di $x$
- *quantificatore esistenziale*, indicato con il simbolo $\exists$
  $\exists x P(x)$, $P$ è vero per almeno un valore di $x$

### Relazioni

- Prodotto cartesiano di $A$ e $B$, denotato con $C = A \times B$

  $$C = \{\langle x, y\rangle \mid x \in A \ \wedge y \in B\},$$

- $A^n$ indica il prodotto cartesiano di $A$ con se stesso, ripetuto $n$ volte

  $$\underbrace{A \times \cdots \times A}_{n \text{ volte}}.$$

- Relazione $n$-aria $R$ su $A_1, A_2, \ldots, A_n$ è un sottoinsieme del prodotto cartesiano $A_1 \times \cdots \times A_n$

  $$R \subseteq A_1 \times \cdots \times A_n.$$

### Relazione d'ordine

Una relazione $R \subseteq A^2$ si dice relazione d'ordine se per ogni $x, y, z \in A$ valgono le seguenti proprietà

1. $\langle x, x\rangle \in R$ (riflessività),
2. $\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \iff x = y$ (antisimmetria),
3. $\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \iff \langle x, z\rangle \in R$ (transitività).

### Relazione d'equivalenza

Una relazione $R \subseteq A^2$ si dice relazione d'equivalenza se, per ogni $x, y, z \in A$, valgono le seguenti proprietà

1. $\langle x, x\rangle \in R$ (riflessività),
2. $\langle x, y\rangle \in R \iff \langle y, x\rangle \in R$ (simmetria),
3. $\langle x, y\rangle \in R \land \langle y, z\rangle \in R \iff \langle x, z\rangle \in R$ (transitività).

### Relazione d'equivalenza

- Un insieme $A$ su cui sia definita una relazione d'equivalenza $R$ si può partizionare in sottoinsiemi, detti classi d'equivalenza, ciascuno dei quali è un sottoinsieme massimale che contiene solo elementi tra loro equivalenti.
- Dati un insieme $A$ ed una relazione d'equivalenza $R$ su $A^2$, l'insieme delle classi d'equivalenza di $A$ rispetto a $R$ è detto insieme quoziente $A/_R$.
- I suoi elementi vengono denotati con $[a]$, dove $a \in A$ è un "rappresentante" della classe d'equivalenza: $[a]$ indica cioè l'insieme degli elementi equivalenti ad $a$.

### Operazioni tra relazioni

- Unione: $R_1 \cup R_2 = \{\langle x, y\rangle \mid \langle x, y\rangle \in R_1 \lor \langle x, y\rangle \in R_2$
- Intersezione: $R_1 \cup R_2 = \{\langle x, y\rangle \mid \langle x, y\rangle \in R_1 \land \langle x, y\rangle \in R_2$
- Complementazione: $\overline{R} = \{\langle x, y\rangle \mid \langle x, y\rangle \notin R\}$
- Chiusura transitiva:

$$\begin{aligned} R^+ = &\{\langle x, y\rangle \mid \exists y_1, \ldots, y_n \in A, n \geq 2, y_1 = x, y_n = y, \\ &\langle y_i, y_{i+1}\rangle \in R, i = 1, \ldots, n-1\} \end{aligned}$$

- Chiusura transitiva e riflessiva: $R^* = R^+ \cup \{\langle x, x\rangle \mid x \in A\}$

### Funzioni

$R \subseteq X_1 \times \ldots \times X_n$ ($n \geq 2$) è una relazione funzionale tra una $(n-1)$-pla di elementi e l'$n$-esimo elemento, se $\forall \langle x_1, \ldots, x_{n-1}\rangle \in X_1 \times \ldots \times X_{n-1}$ esiste al più[1] un elemento $x_n \in X_n$ tale che $\langle x_1, \ldots, x_n\rangle \in R$

$$f : X_1 \times \cdots \times X_{n-1} \mapsto X_n.$$

$$f(x_1, \ldots, x_{n-1}) = x_n.$$

### Funzioni

- $X_1 \times \cdots \times X_{n-1}$, dominio della funzione, $\mathrm{dom}(f)$
- $X_n$, codominio $\mathrm{cod}(f)$
- dominio di definizione:

$$\begin{aligned} \mathrm{def}(f) = \big\{&\langle x_1, \ldots, x_{n-1}\rangle \in \mathrm{dom}(f) \mid \\ &\exists x_n \in \mathrm{cod}(f) : \ f(x_1, \ldots, x_{n-1}) = x_n\big\} \end{aligned}$$

- immagine $\text{imm}(f)$:

$$\text{imm}(f) = \{x_n \in \text{cod}(f) \mid \exists\langle x_1, \ldots, x_{n-1}\rangle \in \text{dom}(f) : \ f(x_1, \ldots, x_{n-1}) = x_n\}$$

Funzioni

- $f$ totale se $\text{def}(f) = \text{dom}(f)$, parziale altrimenti
- $f$ suriettiva se $\text{imm}(f) = \text{cod}(f)$
- $f$ iniettiva o uno-ad-uno (1:1) se

$$\forall\langle x'_1, \ldots, x'_{n-1}\rangle, \langle x''_1, \ldots, x''_{n-1}\rangle \in X_1 \times \ldots \times X_{n-1},$$
$$\langle x'_1, \ldots, x'_{n-1}\rangle \neq \langle x''_1, \ldots, x''_{n-1}\rangle \Longleftrightarrow$$
$$f(x'_1, \ldots, x'_{n-1}) \neq f(x''_1, \ldots, x''_{n-1})$$

- $f$ biiettiva se suriettiva e iniettiva

Pigeonhole principle

Dati due insiemi finiti $A$ e $B$, tali che

$$0 < |B| < |A|,$$

non esiste alcuna funzione iniettiva totale $f : A \mapsto B$

Strutture algebriche

Dato un insieme non vuoto $S \subseteq U$, si definisce operazione binaria $\circ$ su $S$ una funzione $\circ : S \times S \mapsto U$.

Un insieme non vuoto $S$ si dice chiuso rispetto ad una operazione binaria $\circ$ su $S$ se $\text{imm}(\circ) \subseteq S$.

Strutture algebriche

Dato un insieme $S$ chiuso rispetto ad un'operazione binaria $\circ$.

La coppia $\langle S, \circ\rangle$ viene denominata semigruppo se l'operazione binaria $\circ$ soddisfa la proprietà associativa:

$$\forall x \forall y \forall z \in S \ \ (x \circ (y \circ z)) = (x \circ y) \circ z).$$

Se inoltre vale la proprietà commutativa:

$$\forall x \forall y \in S \ \ (x \circ y) = (y \circ x)$$

il semigruppo è detto commutativo.

La coppia $\langle \mathbf{N}, +\rangle$, dove $+$ è l'usuale operazione di somma, è un semigruppo commutativo,

Strutture algebriche

La terna $\langle S, \circ, e\rangle$ viene detta monoide se $\langle S, \circ\rangle$ è un semigruppo, e se $e \in S$ è tale che:

$$\forall x \in S \ \ (e \circ x) = (x \circ e) = x$$

L'elemento $e$ viene detto elemento neutro o unità del monoide. Se $\circ$ è anche commutativa, il monoide viene detto commutativo.

Le terne $\langle \mathbf{N}, +, 0\rangle$ e $\langle \mathbf{N}, *, 1\rangle$, dove $+$ e $*$ sono le usuali operazioni di somma e prodotto, sono monoidi commutativi.

Strutture algebriche

Dati un insieme $S$ ed una operazione associativa $\circ$, definiamo semigruppo libero sulla coppia $\langle S, \circ\rangle$ il semigruppo $\langle S^+, \circ^+\rangle$, dove:

1. $S^+$ è l'insieme di tutte le espressioni $x = x_1 \circ x_2 \circ \ldots \circ x_n$, per ogni $n \geq 1$, con $x_1, \ldots, x_n \in S$;
2. l'operazione $\circ^+$ è definita nel modo seguente: se $x = x_1 \circ \ldots \circ x_n$ e $y = y_1 \circ \ldots \circ y_n$, allora $x \circ^+ y = x_1 \circ \ldots \circ x_n \circ y_1 \circ \ldots \circ y_n$.

Strutture algebriche

Se estendiamo $S^+$ introducendo un elemento aggiuntivo $\varepsilon$, detto parola vuota, possiamo definire sull'insieme risultante $S^* = S^+ \cup \{\varepsilon\}$ l'operazione $\circ^*$, estensione di $\circ^+$, tale che, $\forall x, y \in S^+ \; x \circ^* y = x \circ^+ y$ e $\forall x \in S^* \; (\varepsilon \circ^* x = x \circ^* \varepsilon = x)$.

La terna $\langle S^*, \circ^*, \varepsilon \rangle$ è allora un monoide e viene detto monoide libero.

Strutture algebriche

La terna $\langle S, \circ, e \rangle$ viene detta gruppo se $\langle S, \circ, e \rangle$ è un monoide ed inoltre l'operazione $\circ$ ammette inverso, cioè se

$$\forall x \in S \; \exists y \in S \;\; (x \circ y) = (y \circ x) = e.$$

L'elemento $y$ viene detto inverso di $x$, e si denota come $x^{-1}$.

Se il monoide $\langle S, \circ, e \rangle$ è commutativo il gruppo viene detto commutativo (o abeliano).

Le terne $\langle \mathbf{N}, +, 0 \rangle$ e $\langle \mathbf{N}, *, 1 \rangle$ non sono gruppi, in quanto l'insieme $\mathbf{N}$ non è chiuso rispetto all'inverso di $+$ e di $*$. Al contrario, le terne $\langle \mathbb{Z}, +, 0 \rangle$ e $\langle \mathbb{Q}, *, 1 \rangle$ sono gruppi abeliani.

Strutture algebriche

Dato un semigruppo $\langle S, \circ \rangle$, una congruenza $\equiv$ è una relazione d'equivalenza su $S$ che soddisfa la seguente proprietà:

$$\forall x, y \in S \;\; x \equiv y \Longleftrightarrow \forall z \in S \; \big((x \circ z \equiv y \circ z) \wedge (z \circ x \equiv z \circ y)\big).$$

La relazione d'equivalenza $\equiv_k$ delle classi resto rispetto alla divisione per $k$ è una congruenza rispetto al semigruppo commutativo $\langle \mathbf{N}, + \rangle$: infatti, se $n \equiv_k m$, abbiamo che $\forall l \; (n + l \equiv_k m + l)$ e, chiaramente, anche $l + n \equiv_k l + m$. Viceversa, se $\forall l \; (n + l \equiv_k m + l)$ allora abbiamo, nel caso particolare $l = 0$, $n \equiv_k m$