# *Fondamenti di Informatica*

# *per la Sicurezza*

# *a.a. 2003/04*

# ◇ *Algebre booleane* ◇

Stefano Ferrari

Università degli Studi di Milano

Dipartimento di Tecnologie dell'Informazione



## *Algebre booleane*

Sono algebre booleane:

| **Boole** | **insiemistica** | **proposizioni** | **commutazione** |
|---|---|---|---|
| $K$ | $\wp(\mathcal{U})$ | $\{V, F\}$ ($\{\top, \bot\}$) | {aperto, chiuso} |
| $\cdot$ | $\cap$ | $\wedge$ (*e*) | serie |
| $+$ | $\cup$ | $\vee$ (*o*) | parallelo |
| $^-$ | $^-$ | $\neg$ (*non*) | invertitore |
| $0$ | $\emptyset$ | $F$ ($\bot$) | aperto |
| $1$ | $\mathcal{U}$ | $V$ ($\top$) | chiuso |

Esempio:

- Idempotenza ($a + a = a$): mettere in parallelo due interrutori abbinati, equivale a usarne uno solo.

## Algebra di commutazione

- Shannon (1938): una circuito dotato di interrutori (*switch*) si comporta secondo le leggi dell'algebra Booleana.
- Logica pneumatica: le stesse leggi descrivono il comportamento di meccanismi simili, anche se basati su una differente tecnologia.



## Algebra delle proposizioni

L'*algebra delle proposizioni* o *calcolo proposizionale*:

- si occupa di stabilire la verità o la falsità di asserzioni (espressioni linguistiche) ottenute componendo proposizioni semplici.

Una *proposizione semplice* (o *atomica*) è un'affermazione che

- non dipende da variabili
- può essere *vera* o *falsa*

Una *proposizione composta* può essere:

- sempre vera
- sempre falsa
- vera o falsa a seconda dei componenti

## Connettivi logici

Le proposizioni semplici sono composte per mezzo dei seguenti operatori detti *connettivi logici*:

- congiunzione logica: $\wedge$, *et*, AND, e
  $a \wedge b$ è vera se lo è sia $a$ che $b$
- disgiunzione logica: $\vee$, *vel*, OR, o
  $a \vee b$ è vera quando le è almeno uno fra $a$ e $b$
- negazione logica: $\neg$, *non*, NOT, non
  $\neg a$ è vera quando $a$ è falsa



## Esempi

- proposizioni semplici
  - la somma degli angoli interni di un triangolo è 180°
    *vera*
  - Roma è in Francia
    *falsa*
- proposizioni composte
  - la formica è un insetto $\wedge$ il quadrato è un rombo
    *vera*
  - *oggi* piove $\vee$ *questo* pavimento è di marmo
    *variabile*

**NB** non interessa il significato delle proposizioni, solo se sono vere o false

## Precedenze

**Simboli ausiliari** parentesi $(, )$

**Precedenze** $\neg$ precede $\wedge$ precede $\vee$

Esempi:

- $((\neg a) \vee a)$ si può scrivere $\neg a \vee a$
- $(a \vee (b \wedge c))$ si può scrivere $a \vee b \wedge c$
- $(a \wedge (b \vee c))$ si può scrivere $a \wedge (b \vee c)$



## Altri connettivi

A partire da $\wedge$, $\vee$ e $\neg$, possono essere definiti altri connettivi:

- implicazione: $a \rightarrow b$, se $a$ allora $b$
  $a \rightarrow b \equiv \neg a \vee b$
- biimplicazione: $a \leftrightarrow b$, $a$ se e solo se $b$
  $a \leftrightarrow b \equiv (a \rightarrow b) \wedge (b \rightarrow a) \equiv (a \wedge b) \vee (\neg a \wedge b)$

| $a$ | $b$ | $a \rightarrow b$ |
|---|---|---|
| F | F | V |
| F | V | V |
| V | F | F |
| V | V | V |

| $a$ | $b$ | $a \leftrightarrow b$ |
|---|---|---|
| F | F | V |
| F | V | F |
| V | F | F |
| V | V | V |

*Nota:* $\rightarrow$ segue gli altri connettivi e precede $\leftrightarrow$

## Proposizioni

- *tautologia*: se è sempre vera
  - esempio: $a \rightarrow a$
- *contraddizione*: se è sempre falsa
  - esempio: $a \wedge \neg a$
- soddisfacibile: se viene resa vera almeno da una configurazione dei valori delle variabili che la compongono
  - esempio: $a \wedge b \rightarrow b$



## Definizioni

**implicazione logica** $a$ *implica logicamente* $b$ se e solo se $a \rightarrow b$ è una tautologia

**equivalenza logica** $a$ è *logicamente equivalente* a $b$ se e solo se $a \leftrightarrow b$ è una tautologia

## Esempi

- apro l'ombrello $\rightarrow$ piove
- piove $\rightarrow$ apro l'ombrello
- piove $\leftrightarrow$ apro l'ombrello



## Linguaggio formale

- **alfabeto** (vocabolario): elementi del linguaggio
- **sintassi**: regole per combinare gli elementi
- **semantica**: significato da attribuire alle frasi

## Logica proposizionale

- **alfabeto** (vocabolario):
  - simboli enunciativi (e.g., $a$, $b$)
  - frasi in italiano (*oggi piove*)
  - simboli logici (e.g., $\vee$, $\rightarrow$)
  - simboli ausiliari (“(”, “)”)
- **sintassi**: regole induttive per le *formule*:
  - caso base: ogni simbolo enunciativo è una formula
  - passo: ogni composizione di simboli enunciativi è una formula
  - nient’altro è una formula
- **semantica**: tabelle di verità



## Logica proposizionale (2)

Insiemi sufficienti di connettivi: sottoinsieme delle funzioni booleane a partire dalle quali si possono costruire tutte le altre. Per esempio:

- $\{\neg, \wedge\}$
- $\{\neg, \vee\}$
- NAND
- NOR

- Ogni formula può essere riscritta usando solo NAND o solo NOR.
- Non è detto che soddisfino gli assiomi dell’algebra booleana: né NAND né NOR sono associativi!

## Dimostrazione

Una dimostrazione può essere formulata come segue:

- siano $a_1, \ldots, a_k$ degli enunciati veri, detti *assunzioni*
- una dimostrazione è una sequenza di formule vere $F_0, \ldots, F_n$, dove $F_j, 0 \leq j \leq n$:
  - è un'assunzione
  - è un principio logico (tautologia)
  - per applicazione delle seguenti regole:
    **Modus ponens** dato che sia $a \rightarrow b$ che $a$ sono vere, si deduce che anche $b$ è vera
    **Modus tollens** dato che sia $a \rightarrow b$ che $\neg b$ sono vere, si deduce che anche $\neg a$ è vera



## Dimostrazione — esempio

Assumiamo che le seguenti proposizioni siano vere:

- se è vacanza sto a casa o vado in montagna
- oggi sono al lavoro

Date le precedenti assunzioni, dimostrare che oggi è un giorno lavorativo.

## Dimostrazione (2)

Dato un teorema (ipotesi $\rightarrow$ tesi)

- sapere che la tesi è vera, non dice nulla sul valore dell'ipotesi
- sapere che l'ipotesi è falsa, non dice nulla sul valore della tesi



## Regole di dimostrazione

**Dimostrazione per casi** $((a \rightarrow b) \wedge (\neg a \rightarrow b)) \rightarrow b$

**Dimostrazione per assurdo** $(\neg b \rightarrow a \wedge \neg a) \rightarrow b$

**Contrapposizione** $a \rightarrow b \leftrightarrow \neg b \rightarrow \neg a$

**De Morgan**

- $\neg(a \wedge b) \leftrightarrow (\neg a \vee \neg b)$
- $\neg(a \vee b) \leftrightarrow (\neg a \wedge \neg b)$

**Sillogismo ipotetico**

- $((a \rightarrow b) \wedge (b \rightarrow c)) \rightarrow (a \rightarrow c)$
- $(a \rightarrow b) \rightarrow ((b \rightarrow c) \rightarrow (a \rightarrow c))$

## Esercizio

**Assunzioni**

- Mario è un architetto oppure è geometra.
- Se Mario fosse architetto, allora Mario sarebbe laureato.
- Mario non è laureato.

**Tesi** Mario è geometra.



## Esercizi

- Dimostrare tramite la tabella di verità che le seguenti formule sono tautologie:
  - $((a \vee b) \rightarrow c) \rightarrow ((a \rightarrow c) \vee (b \rightarrow c))$;
  - $a \rightarrow (a \rightarrow \neg a)$;
  - $(a \rightarrow b) \vee (b \rightarrow c) \vee (c \rightarrow a)$;
- Sono corrette le seguenti inferenze?
  - se 3 è pari oppure è primo, e 3 non è primo, allora 3 è pari
  - 3 è pari oppure 3 è primo; 3 non è primo; dunque 3 è pari

# Regole di dimostrazione (2)

**Sillogismo disgiuntivo** $(a \vee b) \wedge \neg b \rightarrow a$

***Ex falso sequitur quodlibet*** $\neg a \rightarrow (a \rightarrow b)$

***Verum sequitur a quodlibet*** $a \rightarrow (b \rightarrow a)$

**Terzo escluso** $a \vee \neg a$

**Non contraddizione** $\neg(a \wedge \neg a)$