CAP. 2 LOGICA

2.1 PROPOSIZIONI

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

esempio: "$2+3=5$" è una proposizione

"$2*3=5$" è una proposizione

"Dove vai?" non è una proposizione

Nella lingua italiana ci sono delle ambiguità.
Consideriamo le seguenti proposizioni:

"Se i maiali volano, allora capirai il teorema di Cantor"

"Se la luna è bianca, allora è fatta di formaggio"

"Se l'ipotesi di Riemann è vera, allora $x^2 \geq 0$ per $\forall x \in \mathbb{R}$"

Sono vere o false queste proposizioni?
Cosa vogliamo dire esattamente?

2.1 PROPOSIZIONI COMPOSTE

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

Sia P una proposizione

DEF la negazione di P, è la proposizione $\neg P$ (detta "non P") definita ponendo

P	$\neg P$
V	F
F	V

Siano P e Q proposizioni

DEF La congiunzione di P e Q, è la proposizione $P \wedge Q$ (letto "P e Q") definita da:

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

DEF La disgiunzione di P e Q, è la proposizione $P \vee Q$ (letto "P o Q") definita da:

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

DEF La disgiunzione esclusiva di P e Q è la prop. $P \overset{o}{\times} Q$ (letto "P oppure Q") definita da:

P	Q	$P \overset{o}{\times} Q$
V	V	F
V	F	V
F	V	V
F	F	F

DEF L'implicazione da P a Q è la prop. $P \to Q$ (letto "P implica Q" o "se P allora Q") definita da

P	Q	$P \to Q$	
V	V	V	(1)
V	F	F	(2)
F	V	V	(3)
F	F	V	(4)

Quindi la proposizione "Se i maiali volano, allora capirai il teorema di Cantor" è vera perché i maiali non volano ($\Rightarrow$ casi (3) e (4))

La prop. "Se la luna è bianca, allora è fatta di formaggio" è falsa perché è vero che la luna è bianca ma è falso che è fatta di formaggio
($\Rightarrow$ caso (2))

La prop. "Se l'ipotesi di Riemann è vera allora $x^2 \geq 0$ per $\forall x \in \mathbb{R}$" è vera perché nessuno sa se l'ipotesi di Riemann è vera ma è vero che $x^2 \geq 0$ per $\forall x \in \mathbb{R}$
($\Rightarrow$ caso (1) e (3))

<u>DEF</u> L'equivalenza logica di P e Q è la prop. scritta "$P \leftrightarrow Q$" (letta "P se e solo se Q") definita da

P	Q	$P \leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

(Si scrive anche "$P \equiv Q$" e si dice che P e Q sono logicamente equivalenti)

esempio: le ~~prop~~ 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)

esempio: "$P \to Q$" e "$\neg Q \to \neg P$"

Sono equivalenti?

P	Q	$\neg P$	$\neg Q$	$P \to Q$	$\neg Q \to \neg Q$
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 $\Rightarrow$ si

esempio: "$(P \to Q) \wedge (Q \to P)$" e "$P \leftrightarrow Q$"

Sono equivalenti?

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

$\Rightarrow$ si

<u>esercizio</u> Consideriamo 3 relazioni su l'insieme delle ~~pese~~ persone:

$a R_1 b \iff$ a e b hanno la stessa età

$a R_2 b \iff$ a e b hanno gli stessi genitori

$a R_3 b \iff$ a e b hanno una lingua in comune

RIFL? SIMM? TRANS.?

	RIFL	SIMM	TRAN
R_1	✓	✓	✓
R_2	✓	✓	✓
R_3	✓	✓	✗

<u>ESEMPI e CONTROESEMPI</u>

Esempio: Non dimostra

Controesempio: Dimostra che non è sempre vero

<u>es.</u> "Ogni primo è dispari" (P)

ESEMPIO: 3 è primo ed è dispari

CONTROESEMPIO: 2 è primo ed è pari

$(\Rightarrow (P)$ è falsa$)$

esempio Consideriamo la relazione
"$A \supseteq B$" su $\mathcal{P}([S])$
RIFL.? SIMM? TRAN?

1) $A \supseteq A$ => RIFLESSIVA
2) $\{2,3,4\} \supseteq \{2\}$ ma $\{2\} \not\supseteq \{2,3,4\}$ => NON È SIMMETRICA
3) Se $A \supseteq B$ e $B \supseteq C$ => $A \supseteq C$ => TRANSITIVA

esempio Consideriamo la relazione
"BATTE" nell'insieme
{CARTA, FORBICE, PIETRA}
nel noto gioco.
RIFL? SIMM? TRAN?

Carta non batte carta => non riflessiva
pietra batte forbice ma forbice mai batte pietra => non è simmetrica
Carta batte pietra
e
pietra batte forbice => mai è transitiva
ma
carta mai batte forbice

esempio Consideriamo la relazione vuota su $\mathbb{R}$
$aRb \iff$ MAI $\forall a,b \in \mathbb{R}$
RIFL? SIMM? TRAN?

- $a \not R a$ => NO RIFLESSIVA
- È vero che "$aRb \Rightarrow bRa$"? Sì (caso (4) di "$P \to Q$")
  => è SIMMETRICA

OSS: Anche "$aRb \leftrightarrow bRa$" è vera
"$(aRb$ e $bRa) \Rightarrow (aRa)$" è vera perché
$(aRb$ e $bRa)$ è falso (caso (4))

ES [1]: Siano P e Q proposizioni. È vero che

"$P \to Q$" e "$(\neg P) \to (\neg Q)$"

sono equivalenti?

2.3 LEGGE DISTRIBUTIVE E DI DE MORGAN

Siano P e Q proposizioni

PROP 2.3.1 : Abbiamo che

Leggi di De Morgan
$$\begin{cases} \neg(P \wedge Q) = (\neg P) \vee (\neg Q) \\ \quad e \\ \neg(P \vee Q) = (\neg P) \wedge (\neg Q) \end{cases}$$

DIM. TAVOLA DI VERITÀ

Sia R una prop.

PROP. 2.3.2 : Abbiamo che

Leggi distrib.
$$\begin{cases} P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R) \\ \quad e \\ P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R) \end{cases}$$

DIM. TAVOLA DI VERITÀ

2.4 LOGICA E PROGRAMMAZIONE

Consideriamo le seguenti linee di codice che potrebbero essere C, C++ o Java:

```
IF (x ≥ 0 || (x<0 && y >100))
   - - - -
   - - - -
```

In questi linguaggi di programmazione

"||" = "$\vee$"

"&&" = "$\wedge$"

le linee di codice vengono eseguite se e solo se l'espressione scritta in parentesi è vera. Questa espressione in parentesi è nella forma

$$A \vee ((\neg A) \wedge B)$$

Dove $A = $ "$x \geq 0$" e $B = $ "$y > 100$"

Questa espressione sembra equivalente a

$$A \vee B$$

In effetti

$$A \vee ((\neg A) \wedge B) = (A \vee (\neg A)) \wedge (A \vee B) = A \vee B$$

Posso quindi riscrivere il programma così:

```
IF (x≥0 || y>100)
   -----
```

Questi due programmi sono equivalenti ma il secondo è più breve $\Rightarrow$ più veloce.
Semplificare prop. composte è importante e non facile (anche nel design di chip, un chip che usa meno connettori logici ("$\wedge$", "$\vee$" e "$\neg$") è più piccolo, costa meno, ha meno errori e consuma meno)

2.5 PREDICATI

Un predicato è una proposizione la cui verità o falsità dipende da una variabile o più.
Si scrive

$$P(x, y, \ldots)$$

Dove $x, y, \ldots$ sono le variabili

esempio: $P(n) =$ "n è primo" $(n \in \mathbb{N})$

$P(4)$ è falso, $P(5)$ è vero

esempio: $Q(n) =$ "n è un quadrato perfetto" $(n \in \mathbb{N})$

$Q(4)$ è vero, $Q(5)$ è falso

In logica e informatica (come in matematica) si usano questi simboli:

"$\forall$" = "per ogni"

"$\exists$" = "esiste"

esempio "$\forall n.\, P(n)$" = "Per ogni n $P(n)$ è vera"

(è un separatore)

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

È importante rendersi conto che

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

Similmente

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

2.6. IL PROBLEMA SAT

Problema SAT: Data una proposizione composta formata da n proposizioni $P_{1,2} \dots P_n$ e "$\vee$", "$\wedge$", "$\neg$", e ")", "(", decidere in un tempo "ragionevole" se esiste un'assegnazione di valori di verità a $P_1, \dots P_n$ che rende vera la proposizione data composta

SAT = SATISFIABILITY

Una soluzione affermativa implica la rottura di (quasi) tutti i sistemi di crittografia attualmente in uso.

SAT è uno dei "problemi del millennio" dell'Istituto Fields

TABELLA DELLA VERITÀ

P	Q	R	$P \leftrightarrow Q$	$Q \leftrightarrow R$	$(P \leftrightarrow Q) \land (Q \leftrightarrow R)$
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	F	F	F
V	F		F	V	F
F	V		F	V	F
F	V		F	F	F
F	F		V	F	F
F	F		V	V	V

$P \leftrightarrow R$	$((Q \leftrightarrow R) \land (P \leftrightarrow Q)) \rightarrow (P \leftrightarrow R)$
V	V
F	V
V	V
F	V
F	V
V	V
F	V
V	V

$\Rightarrow$ è Transitiva $\Rightarrow$ Quindi "$\leftrightarrow$" è una relazione di equivalenza

esercizio

Siano P, Q, R proposizioni. è vero che

"$\neg(P \wedge (Q \wedge R))$" e "$(\neg P) \vee ((\neg Q) \vee (\neg R))$"

sono equivalenti?

P	Q	R	$Q \wedge R$	$\neg P$	$\neg Q$	$\neg R$	$P \wedge (Q \wedge R)$
V	V	V	V	F	F	F	V
V	V	F	F	F	F	V	F
V	F	V	F	F	V	F	F
V	F	F	F	F	V	V	F
F	V	V	V	V	F	F	F
F	V	F	F	V	F	V	F
F	F	V	F	V	V	F	F
F	F	F	F	V	V	V	F

$\neg(P \wedge (Q \wedge R))$	$(\neg Q) \vee (\neg R)$	$(\neg P) \vee ((\neg Q \vee (\neg R))$
F	F	F
V	V	V
V	V	V
V	V	V
V	F	V
V	V	V
V	V	V
V	V	V

le colonne sono uguali ⇒ sono equivalenti

esercizio In pratica è più comodo usare le "NAND" (not and) invece di "$\vee$", "$\wedge$" e "$\neg$".

La definizione è:

P	Q	$P \,\square\, Q$
V	V	F
V	F	V
F	V	V
F	F	V

Esprimere "$\vee$", "$\wedge$" e "$\neg$" in funzione di NAND ($\square$)

Mi pare che $A \square B$ è $\neg(A \wedge B)$. In effetti:

A	B	$A \wedge B$	$\neg(A \wedge B)$	$A \square B$
V	V	V	F	F
V	F	F	V	V
F	V	F	V	V
F	F	F	V	V

Pertanto

$$A \square B = \neg(A \wedge B)$$

$$\Downarrow$$

$$A \wedge B = \neg(A \square B)$$

$$A \square A = \neg(A \wedge A) = \neg A$$

$$A \square B = (\neg A) \vee (\neg B)$$

$$\Downarrow$$

$$\neg A = A \square A$$

$$A \wedge B = (A \square B) \square (A \square B)$$

$$(\neg A) \square (\neg B) = A \vee B$$

Concludendo

$$A \wedge B = (A \square B) \square (A \square B)$$

$$A \vee B = (A \square A) \square (B \square B)$$

$$\neg A = A \square A$$

es.: C'è stato un delitto e Poirot ha determinato che:

- I sospettati sono 9: 1, 2 ... 9
- I colpevoli sono almeno 3

a) 1 o 2 sono innocenti

b) se (3 o 4 sono colpevoli) => tutti sono colpevoli

c) se 1 è colpevole => 2 è colpevole

d) se 5 è colpevole => 3 è colpevole

e) se 6 o 7 sono colpevoli => 8 è innocente

f) se 6 o 2 sono colpevoli => 9 è innocente

Scrivere una prop. composta che esprima queste affermazioni e trovare i colpevoli

DEFINIAMO LE PROP

- 1 = "1 è colpevole"

9 = "9 è colpevole"

- $\exists x \exists y \exists z. ((x \neq y) \wedge (x \neq z) \wedge ((y \neq z) \wedge x \wedge y \wedge z)$

a) $(\neg 1) \vee (\neg 2)$

b) $(3 \vee 4) \longrightarrow (1 \wedge 2 \wedge 3 \wedge 4 \wedge 5 \wedge 6 \wedge 7 \wedge 8 \wedge 9)$

c) $(1 \to 2)$

d) $(5 \to 3)$

e) $(6 \vee 7) \to \neg 8$

f) $(6 \vee 2) \to \neg 9$

Se 1 è colpevole → 2 è colpevole → entrambi colpevoli → contraddice a) (c osservazioni)

INOLTRE...

Se 3 o 4 sono colpevoli $\xrightarrow{b)}$ tutti sono colpevoli → 6 e 7 sono colpevoli $\xrightarrow{e)}$ 8 è innocente → assurdo

PERTANTO...

Non è vero che 3 o 4 sono colpevoli ☐

INOLTRE 5 è innocente □

(se 5 è colpevole $\xrightarrow{d)}$ 3 è colpevole → assurdo vedi sopra)

NOTIAMO CHE

Se 9 è colpevole → non è vero che 6 o 2 sono colpevoli → 6 e 2 sono innocenti

INOLTRE...

2 innocente $\xrightarrow{c)}$ 1 innocente

Quindi 1 è innocente ⇒ 3 e 4 sono innocenti ⇒
⇒ 5 è innocente

Se 2 è innocente ⇒ 6 o 7 sono ~~innocen~~ colpevoli
(se entrambi innocenti ⇒ 7 innocenti, ASSURDO) ⇒
⇒ 8 è innocente ⇒ 6, 7 e 9 sono colpevoli ⇒
⇒ 9 è innocente, assurdo.
Quindi 2 è colpevole ⇒ 9 è innocente ⇒ 6 o 7 sono colpevoli (altrimenti ci sono 7 innocenti, ASSURDO)
⇒ 8 innocente ⇒ 6 innocenti ⇒ i rimanenti sono colpevoli (2,6,7)

2ª soluzione: USIAMO LA LOGICA PROPOSIZIONALE

Poirot dice che la seguente prop. è vera:

$$((\neg 1) \vee (\neg 2)) \wedge ((3 \vee 4) \to (1 \wedge 2 \wedge \ldots \wedge 9)) \wedge (1 \to 2) \wedge (5 \to 3) \wedge ((6 \vee 7) \to \neg 8) \wedge (6 \vee 2) \to \neg 9)$$

$$=$$

$$((\neg 1) \vee (\neg 2)) \wedge (\neg(3 \vee 4) \vee (1 \wedge 2 \wedge \ldots \wedge 9)) \wedge ((\neg 1) \vee 2) \wedge ((\neg 5) \vee 3) \wedge (\neg(6 \vee 7)) \vee \neg 8) \wedge ((\neg(6 \vee 2)) \vee \neg 9) =$$

$$\overbrace{((\neg 1) \vee (\neg 2))}^{=A} \wedge (((\neg 3) \wedge (\neg 4)) \vee (1 \wedge 2 \wedge \ldots \wedge 9)) \wedge \underbrace{((\neg 1) \vee 2)}_{=B} \wedge ((\neg 5 \vee 3) \wedge (((\neg 6) \vee (\neg 7)) \vee \neg 8) \wedge ((\neg 6 \wedge \neg 2) \vee \neg 9) =$$