LOGICA

Lezione 4: Ultima su Logica Proposizionale

Laura Nenzi

DIA – Università degli Studi di Trieste

Contenuti della Lezione

- Forme normali
- Sostituzioni
- Dualità
- Complessità computazionale dei problemi della logica proposizionale:
  - SAT
  - TAUTOLOGY

Forma Normale Congiuntiva (**FNC**) (CNF in inglese)

- Una fbf P è detta in **forma normale congiuntiva (FNC)** sse:
  - $P = P_1 \wedge P_2 \wedge \ldots \wedge P_n$ con n ≥ 1
  - e $\forall i = 1, \ldots, n \quad P_i$ è una disgiunzione di letterali: $P_i = L_1 \vee L_2 \vee \cdots \vee L_m$

- Es. $(A \vee \neg B \vee C) \wedge B \wedge \neg D \wedge (A \vee D)$

Forma Normale Disgiuntiva (**FND**) (DNF in inglese)

- Una fbf P è detta in **forma normale disgiuntiva (FND)** sse:
  - $P = P_1 \vee P_2 \vee \ldots \vee P_n$ con $n \geq 1$
  - e $\forall i = 1, \ldots, n$ P_i è una congiunzione di letterali: $P_i = L_1 \wedge L_2 \wedge \cdots \wedge L_m$

- Es. $(A \wedge \neg B \wedge C) \vee B \vee \neg D \vee (A \wedge D)$

Trasformazione

- Per ogni fbf P esistono una forma normale congiuntiva P^C e una forma normale disgiuntiva P^D, tali che $P \equiv P^C$ e $P \equiv P^D$ (lo dimostriamo formalmente dopo).

- Per la trasformazione si usano le regole di equivalenza, le formule di De Morgan e le regole distributive.

FNC e FND

- OSS: Per ogni fbf P possono esistere piu` fbf in FNC e in FND equivalenti ad essa

- Esempio:
  - $P = (A \wedge \neg B \wedge C) \vee (\neg(A \rightarrow B) \wedge A) \vee (A \wedge B \wedge C)$
  - $P \equiv (A \wedge C) \vee (\neg B \wedge A)$
  - $P \equiv (\neg B \wedge A) \vee (A \wedge B \wedge C)$
  - $P \equiv (A \wedge \neg B \wedge C) \vee (\neg B \wedge A) \vee (A \wedge B \wedge C)$

Metodo per Trasformazione in FND e FNC

Voglio trovare la FND P^D, risp FNC P^C di una P con prop atomiche $A_1, \dots, A_n$

- **Passo 1** eliminare il connettivo $\rightarrow$:
  - $P \rightarrow Q \equiv \neg P \vee Q$
- **Passo 2** eliminazione di $\bot$:
  - $\bot \equiv \neg A \ \wedge \ A$ (A è una qualsiasi formula atomica)
- **Passo 3** portare le negazione all'interno e eliminare le doppie negazioni:
  - $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ (DeMorgan)
  - $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ (DeMorgan)
  - $\neg\neg P \ \equiv \ P$

Metodo per Trasformazione in FND e FNC

Voglio trovare la FND P^D, risp FNC P^C di una P con prop atomiche $A_1, \dots, A_n$

- **Passo 4 FND** portare le congiunzioni all'interno delle disgiunzioni:
  - $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ (distr.)
  - $(P \vee S) \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R) \vee (S \wedge Q) \vee (S \wedge R)$ (distr.)

- **Passo 4 FNC** portare le disgiunzioni all'interno delle congiunzioni:
  - $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ (distr.)
  - $(P \wedge S) \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) \wedge (S \vee Q) \wedge (S \vee R)$ (distr.)

Esempio: Trasformare in FND $\neg(A \land (B \to \bot))$

- Passo 1
  - $\neg(A \land (\neg B \lor \bot))$
- Passo 2
  - $\neg(A \land (\neg B \lor (\neg A \land A)))$
- Passo 3
  - $\neg A \lor \neg(\neg B \lor (\neg A \land A))$
  - $\neg A \lor (\neg\neg B \land \neg(\neg A \land A))$
  - $\neg A \lor (B \land \neg(\neg A \land A))$

Esempio: Trasformare in FND $\neg(A \wedge (B \rightarrow \bot))$

- Passo 3
  - $\neg A \vee (B \wedge \neg(\neg A \wedge A))$
  - $\neg A \vee (B \wedge (\neg\neg A \vee \neg A))$
  - $\neg A \vee (B \wedge (A \vee \neg A))$
- Passo 4
  - $\neg A \vee ((B \wedge A) \vee (B \wedge \neg A))$
  - $\neg A \vee (B \wedge A) \vee (B \wedge \neg A)$ in forma FND

Esempio: Trasformare in FNC $\neg(A \wedge (B \rightarrow (\neg A \wedge B)))$

- Passo 1
  - ¬(A∧(¬B∨(¬A∧B)))
- Passo 3
  - $\neg A \vee \neg(\neg B \vee (\neg A \wedge B))$
  - $\neg A \vee (\neg\neg B \wedge \neg(\neg A \wedge B))$
  - $\neg A \vee (B \wedge \neg(\neg A \wedge B))$
  - $\neg A \vee (B \wedge (\neg\neg A \vee \neg B))$
  - $\neg A \vee (B \wedge (A \vee \neg B))$
- Passo 4
  - $(\neg A \vee B) \wedge (\neg A \vee A \vee \neg B)$ in forma FNC

Proprietà

- **Thm 1.33:** Per ogni fbf P esistono una FNC P^C e una FND P^D, tali che

$$P \equiv P^C \text{ e } P \equiv P^D$$

- **Dim** Per costruzione. Basta utilizzare le equivalenze semantiche e seguire lo schema degli algoritmi:
  - Si eliminano i connettivi diversi da $\neg, \vee, \wedge$ utilizzando le equivalenze semantiche: $P \rightarrow Q \equiv \neg P \vee Q$, e $\bot \equiv \neg A \wedge A$
  - Si utilizza ripetutamente la legge di De Morgan per portare le negazioni davanti alle proposizioni atomiche
  - Si utilizza la distributività per convertire P in P^C o P^D

Costruzione **FND** (risp. **FNC**) **completa**

- Siano $A_1, \dots, A_n$ le formule atomiche di P
- Si costruisce la tabella di verità di P
- La FND è la disgiunzione di ogni riga dove $v_i(P) = 1$.
  - Ogni riga (con $v_i(P) = 1$) è una congiunzione di letterali così definita:
    - $j \in \{1, \dots n\}$ se $v_i(A_j) = 1$ allora viene inserito A_j altrimenti $\neg A_j$
- La FNC è la congiunzione di ogni riga che ha $v_i(P) = 0$
  - Ogni riga (con $v_i(P) = 0$) è una disgiunzione di letterali così definita:
    - $\forall j \in \{1, \dots n\}$ se $v_i(A_j) = 0$ allora viene inserito A_j altrimenti $\neg A_j$

Esempio FND completa

- Trasformare $\neg(A \wedge (B \rightarrow (\neg A \wedge B)))$ nella FNC completa:

int	A	B	$\neg(A \wedge B)$	$B \rightarrow (\neg A \wedge B)$	$A \wedge (B \rightarrow (\neg A \wedge B))$	$\neg(A \wedge (B \rightarrow (\neg A \wedge B)))$
v_1	0	0	1	1	0	1
v_2	0	1	1	1	0	1
v_3	1	0	1	1	1	0
v_4	1	1	0	0	0	1

- FND completa: $(\neg A \wedge \neg B) \vee (\neg A \wedge B) \vee (A \wedge B)$

Esempio FNC completa

- Trasformare $\neg(A \ \wedge \ (B \rightarrow \ (\neg A \ \wedge \ B)))$ nella FND completa:

int	A	B	$\neg(A \wedge B)$	$B \rightarrow (\neg A \wedge B)$	$A \wedge (B \rightarrow (\neg A \wedge B))$	$\neg(A \wedge (B \rightarrow (\neg A \wedge B)))$
v_1	0	0	1	1	0	1
v_2	0	1	1	1	0	1
v_3	1	0	1	1	1	0
v_4	1	1	0	0	0	1

- FNC completa: $(\neg A \vee B)$

Proprietà

- Data una fbf P, la FND completa e la FNC completa di P sono **uniche**.
  - Vero per costruzione utilizzando la tabella di verità.
- **Corollario** L'insieme dei connettivi $\{\neg,\wedge,\vee\}$ è funzionalmente completo
- **Corollario** Gli insiemi di connettivi $\{\neg,\vee\}$ e $\{\neg,\wedge\}$ sono funzionalmente completi
  - $A \wedge B \equiv \neg(\neg A \vee \neg B)$
  - $A \vee B \equiv \neg(\neg A \wedge \neg B)$

Sostituzione

- Siano P e R due fbf e A una formula atomica. La **sostituzione** $(\boldsymbol{R[P/A]})$ di P al posto di A in R si definisce in modo ricorsivo nel seguente modo:
  - Se R è una formula atomica diversa da A allora $R[P/A] = R$
  - Se $R \equiv A$ allora $R[P/A] = P$
  - Se $R \equiv \neg Q$ allora $(\neg Q)[P/A] = \neg Q[P/A]$
  - Se $R \equiv Q_1 \vee Q_2$ allora $(Q_1 \vee Q_2)[P/A] = Q_1[P/A] \vee Q_2[P/A]$
  - Se $R \equiv Q_1 \wedge Q_2$ allora$(Q_1 \wedge Q_2)[P/A] = Q_1[P/A] \wedge Q_2[P/A]$
  - Se $R \equiv Q_1 \rightarrow Q_2$ allora $(Q_1 \rightarrow Q_2)[P/A] = Q_1[P/A] \rightarrow Q_2[P/A]$

Esempio

- $R = \neg(A \wedge (B \rightarrow (\neg A \wedge B)))$
- $P = (A \vee B)$

- $R[P/A] = \neg((A \vee B) \wedge (B \rightarrow (\neg (A \vee B) \wedge B)))$
- $P[R/A] = ((\neg(A \wedge (B \rightarrow (\neg A \wedge B)))) \vee B)$

Proprietà

- **Thm 1.23**: Sia v un'interpretazione t.c. $v(P) = v(Q)$ allora:
  - per ogni R, $v(R[P/A]) = v(R[Q/A])$
- **Dim** per induzione strutturale (per esercizio, c'e` sul libro ma provate a farlo voi ☺))

Teorema di Sostituzione

- Thm 1.24 (**di Sostituzione**) Sia $P \equiv Q$ allora R[P/A] ≡ R[Q/A]
- **Dim**
  - Sia v una interpretazione.
  - Per ipotesi $P \equiv Q$ quindi $v(P) = v(Q)$, per ogni v
  - Per la proprietà di prima: $v(R[P/A]) = v(R[Q/A])$, per ogni v
  - Per def. di equivalenza si ha R[P/A] ≡ R[Q/A]

Sostituzione Simultanea

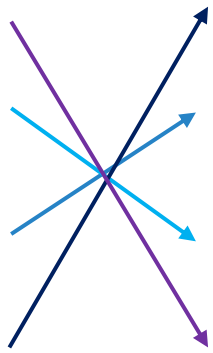
- $R[P_1, \dots P_n/A_1, \dots A_n]$ si ottiene sostituendo P_i al posto di A_i per tutti gli i **simultaneamente**.

- Esempio
  - $R = \neg\Big(A \wedge \big(B \rightarrow (\neg A \wedge B)\big)\Big)$,
  - $P = (A \vee B)$
  - $Q = (\neg A \wedge B)$
  - $R[P, Q/A, B] = \neg((A \vee B) \wedge ((\neg A \wedge B) \rightarrow (\neg(A \vee B) \wedge (\neg A \wedge B))))$

Dualità

- $A \wedge B = 1$ sse $A = B = 1$
- $A \vee B = 0$ sse $A = B = 0$
- Sono operatori **duali** ovvero ognuno deriva dall'altro rovesciando il ruolo di 0 e 1.

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1



A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Trasformazione: $^{\perp}$

- La funzione $^{\perp} : \mathrm{FBF} \rightarrow \mathrm{FBF}$ soddisfa:
  - $P^{\perp} = \neg P$ se P è una formula atomica
  - $(P \wedge Q)^{\perp} = P^{\perp} \vee Q^{\perp}$
  - $(P \vee Q)^{\perp} = P^{\perp} \wedge Q^{\perp}$
  - $(\neg P)^{\perp} = \neg P^{\perp}$

- Esempio: $\big((A \wedge \neg \mathrm{B}) \vee C\big)^{\perp} =$
  - $((A \wedge \neg B)^{\perp} \wedge C^{\perp} =$
  - $(A^{\perp} \vee (\neg B)^{\perp}) \wedge \neg C =$
  - $\big(\neg A \vee (\neg\neg B)\big) \wedge \neg C =$
  - $(\neg A \vee B) \wedge \neg C$

Proprietà

- **Lemma:** $P^{\perp} \equiv \neg P$
- **Dim** $P^{\perp} \equiv \neg P$ se $\forall v, v(P^{\perp}) = v(\neg P) = 1 - v(P)$, proviamo per induzione
  - (Caso Base) P atomica, $v(P^{\perp}) = v(\neg P) = 1 - v(P)$
  - (Caso Induttivo) vero per P, Q,
    - $v\big((P \vee Q)^{\perp}\big) = v(P^{\perp} \wedge Q^{\perp})$
    - $= \min(v(P^{\perp}), v(Q^{\perp}))$
    - $= \min\big(1 - v(P), 1 - v(Q)\big)$
    - $= 1 - \max\big(v(P), v(Q)\big)$
    - $= 1 - v(P \vee Q)$

- La trasformazione ha l'effetto di: $(A \vee B)^{\perp} \equiv A^{\perp} \wedge B^{\perp} \equiv \neg A \wedge \neg B$
- **Non è la funzione di dualità!**

Funzione di dualità

- La funzione $^{d} : \mathrm{FBF} \rightarrow \mathrm{FBF}$ soddisfa:
  - $P^d = P$ se P è una formula atomica
  - $(P \wedge Q)^d = P^d \vee Q^d$
  - $(P \vee Q)^d = P^d \wedge Q^d$
  - $(\neg P)^{\perp} = \neg P^d$

Esempio Funzione di Dualità

- $(A \wedge B)^d =$
  - $A^d \vee B^d =$
  - $A \vee B$

- È la funzione giusta!!!
- **Osservazione:** la funzione di dualità consiste nello scambiare gli operatori $\wedge$ e $\vee$.

- **Lemma 1.40**, Per ogni insieme $A_1 \, , \ldots A_n$ di simboli proposizionali atomici che compaiono in una proposizione R si ha:
  $R^d[\neg\neg A_1, \ldots, \neg\neg A_n \, / A_1, \ldots, A_n \,] \; = R^{\perp}[\neg A_1, \ldots, \neg A_n \, / A_1, \ldots, A_n \,]$

- **Dim** esercizio.

Teorema di Dualità

$$P \equiv Q \Leftrightarrow P^d \equiv Q^d$$

Dim.

- (1) ⇒ (2):
  - Siano $A_1, \ldots, A_n$ i simboli proposizionali atomici in P e Q
  - $P^d \equiv P^{\perp}[\neg A_1, \ldots, \neg A_n / A_1, \ldots, A_n]$
  - $Q^d \equiv Q^{\perp}[\neg A_1, \ldots, \neg A_n / A_1, \ldots, A_n]$
  - $\neg P \equiv \neg Q$
  - ma $P^{\perp} \equiv \neg P$ e quindi $P^{\perp} \equiv Q^{\perp}$
  - $P^d \equiv P^{\perp}[\neg A_1, \ldots, \neg A_n / A_1, \ldots, A_n] \equiv Q^{\perp}[\neg A_1, \ldots, \neg A_n / A_1, \ldots, A_n] \equiv Q^d$
- (1) ⇐ (2) deriva immediatamente dal fatto che $P^{d^d} = P$

Esempio: Applicazione Thm di Dualita`

- Esempio: Leggi di De Morgan
- Prima legge:
  - $\neg(\boldsymbol{P} \vee \boldsymbol{Q}) \equiv \neg\boldsymbol{P} \wedge \neg\boldsymbol{Q}$
  - $\big(\neg(P \vee Q)\big)^d \equiv (\neg P \wedge \neg Q)^d$
- Seconda legge:
  - $\neg(\boldsymbol{P} \wedge \boldsymbol{Q}) \equiv \neg\boldsymbol{P} \vee \neg\boldsymbol{Q}$
  - $\big(\neg(P \wedge Q)\big)^d \equiv (\neg P \vee \neg Q)^d$

SAT (Boolean Satisfiability Problem)

- Problema **SAT**: la fbf proposizionale P è soddisfacibile?
- Con una tabella di verità è possibile decidere se una fbf. è soddisfacibile.
- Se P ha n formule atomiche distinte, la tabella di verità di P ha 2^n righe (una per ogni interpretazione) L'algoritmo per SAT basato sulla tabella di verità ha complessità al caso pessimo $O(2^n)$.

È possibile fare meglio?

- Esiste un algoritmo polinomiale
  - che stabilisca se una fbf proposizionale è soddisfacibile?
  - ovvero che risolva il problema SAT?
- La risposta per ora non esiste:
- SAT è un problema NP-completo! (Teorema di Cook visto con Luca)
- Tutti gli algoritmi conosciuti per SAT hanno complessità esponenziale

Tautologia

- Problema **TAUTOLOGY**: la fbf proposizionale P è una tautologia?

- Sembrerebbe più difficile di SAT perché
  - non ci possiamo accontentare di trovare un modello di P (come per SAT)
  - ma dobbiamo verificare che tutte le 2^n interpretazioni siano modelli di P

Tautologia

- **OSS**: Una formula P è una tautologia se e solo se la sua negata è insoddisfacibile
  - ovvero se e solo se $\neg P$ non è soddisfacibile
- TAUTOLOGY è il problema complementare di SAT

Conclusioni

- Nonostante stiamo utilizzando un linguaggio logico molto limitato: SAT è un problema NP-completo TAUTOLOGY è un problema in co-NP

- Gli algoritmi di calcolo che vedremo hanno complessità esponenziale al caso pessimo.

Esercizi

A	B	C	D	$A \wedge \neg B \rightarrow C$	$C \rightarrow D \vee B$	$\neg D \rightarrow A$	$\neg B$	P	$P \rightarrow D$
0	0	0	0	1	1	0	1	0	1
0	0	0	1	1	1	1	1	1	1
0	0	1	0	1	0	0	1	0	1
0	0	1	1	1	1	1	1	1	1
0	1	0	0	1	1	0	0	0	1
0	1	0	1	1	1	1	0	0	1
0	1	1	0	1	1	0	0	0	1
0	1	1	1	1	1	1	0	0	1
1	0	0	0	0	1	1	1	0	1
1	0	0	1	0	1	1	1	0	1
1	0	1	0	1	0	1	1	0	1
1	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	0	0	1
1	1	0	1	1	1	1	0	0	1
1	1	1	0	1	1	1	0	0	1
1	1	1	1	1	1	1	0	0	1

A	B	C	D	$A \wedge \neg B \rightarrow C$	$C \rightarrow D \vee B$	$\neg D \rightarrow A$	$\neg B$	P	$P \rightarrow D$
0	0	0	0	1	1	0	1	0	1
0	0	0	1	1	1	1	1	1	1
0	0	1	0	1	0	0	1	0	1
0	0	1	1	1	1	1	1	1	1
0	1	0	0	1	1	0	0	0	1
0	1	0	1	1	1	1	0	0	1
0	1	1	0	1	1	0	0	0	1
0	1	1	1	1	1	1	0	0	1
1	0	0	0	0	1	1	1	0	1
1	0	0	1	0	1	1	1	0	1
1	0	1	0	1	0	1	1	0	1
1	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	0	0	1
1	1	0	1	1	1	1	0	0	1
1	1	1	0	1	1	1	0	0	1
1	1	1	1	1	1	1	0	0	1

Esercizio 1.8

- Stabilire se le seguenti affermazioni sono equivalenti:
  - (1) $\mathrm{P} \vDash Q$
  - (2) se $\vDash P$ allora $\vDash Q$
- Risouzione: dobbiamo dimostrare che:
  - (1) $\Rightarrow$ (2)
  - (1) $\Leftarrow$ (2)
- Dim ($\Rightarrow$) $\mathrm{P} \vDash Q$ implica (se $\vDash P$ allora $\vDash Q$)
  - Dobbiamo dimostrare che se P e` una tautologia lo è anche Q
  - Per hp $\mathrm{P} \vDash Q$, ho che $\forall v, t.c.\, v(P) = 1$, ho che $v(Q) = 1$
  - Ma se $\vDash P$ allora $v(P) = 1, \forall P$ e quindi $v(Q) = 1, \forall v$ e quindi $\vDash Q$

Esercizio 1.8

- Dim ($\Leftarrow$) (se $\vDash P$ allora $\vDash Q$) implica $\mathrm{P} \vDash Q$
  - Dobbiamo dimostrare che ogni modello di P è anche un modello di Q
  - L'hp (se $\vDash P$ allora $\vDash Q$) è vera in due casi da analizzare:
    - P e Q sono tautologie e segue direttamente che ogni modello di P è modello di Q
    - P non è una tautologia
  - Se P non è una tautologia l'ipotesi è vera ma non ho ipotesi su Q
  - Posso costruire un controesempio in cui P e $\mathrm{P} \quad Q$, cioe` in cui P non è una tautologia e Q non è conseguenza semantica di P?
  - $P = A$ e $Q = A \wedge B$
  - A non è una tautologia e $A \vDash A \wedge B$ è falsa, esiste $v, v(A) = 1, v(A \wedge B) = 0$

Esercizio 1.19

- Trovare un criterio affinché:
  - una formula in FNC sia una tautologia
  - una formula in FND sia una tautologia (per esercizio)

Esercizio 1.19

- Trovare un criterio affinché una formula in FNC sia una tautologia
  - $P = P_1 \wedge P_2 \wedge \cdots \wedge P_n$
  - P_i è una disgiunzione di letterali: $P_i = L_1 \vee L_2 \vee \cdots \vee L_m$
- $P = P_1 \wedge P_2 \wedge \cdots \wedge P_n \equiv \neg\bot$
- sse $P_1 \equiv P_2 \equiv \cdots \equiv P_n \equiv \neg\bot$
- sse ogni P_i contiene un letterale e il suo negato
- ovvero ogni P_i contiene $A_i \vee \neg A_i$

- Esempio:
  - $P = (A \vee B \vee \neg A) \wedge (\neg B \vee B \vee \neg A) \wedge (A \vee C \vee \neg A \vee \neg D)$

Esercizio 1.22

- Si definisca il connettivo duale del connettivo di implicazione, dandone la tabella di verità
- Si esprima in funzione di $\{\wedge, \sim\}$ (hint FND)
- Si estenda la funzione $\perp$ a formule composte anche dai connettivi implicazione ed il suo duale (hint def di $\perp$)
- Sii dimostri che per ogni P: $v(P^{\perp}) = 1 - v(P)$ (per induzione strutturale)

Esercizio 1.15

- Mostrare che l'insieme di connettivi $\{\wedge, \leftrightarrow, \underline{\vee}\}$ è funzionalmente completo e che nessuno dei suoi sottoinsiemi propri lo è.
  - Mostrare che i connettivi di un insieme funzionalmente completo possono essere scritti in funzione di $\{\wedge, \leftrightarrow, \underline{\vee}\}$
  - Per ogni sottoinsiemie proprio di $\{\wedge, \leftrightarrow, \underline{\vee}\}$, mostrare che almeno uno dei connettivi di un insieme funzionalmente completo non può essere scritto in funzione del sottoinsieme