LOGICA E ALGEBRA
28 GIUGNO 2017
Parte di Logica

Esercizio 1

Sia f (A,B,C) una f.b.f. avente la seguente tavola di verità:

A	B	C	f (A,B,C)
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

a) Scrivere f(A,B,C) utilizzando solo i connettivi ~ e $\Rightarrow$.
b) Dire se la formula

$$\sim (\sim A \Rightarrow C) \Rightarrow (B \Rightarrow f(A,B,C))$$

è un teorema di L.
c) Provare il risultato ottenuto al punto b) utilizzando la risoluzione.

TRACCIA DI SOLUZIONE

a) $f(A,B,C)\equiv(A\wedge B\wedge\sim C)\vee(\sim A\wedge B\wedge C)\equiv B\wedge((A\wedge\sim C)\vee(\sim A\wedge C))\equiv\sim(((A\wedge\sim C)\vee(\sim A\wedge C))\Rightarrow \sim B)\equiv \sim(((A\wedge\sim C)\vee(\sim A\wedge C))\Rightarrow\sim B)\equiv\sim(((A\Rightarrow C)\Rightarrow\sim(C\Rightarrow A))\Rightarrow\sim B)$
b) Per il teorema di correttezza e completezza la formula è un teorema di L se e solo se è una tautologia. Se o A o C valgono 1, l'antecedente della formula è falso e quindi la formula è vera. Quando B vale 0, il conseguente della formula è vero in quanto il suo antecedente è falso e la formula è quindi vera. Resta da considerare il caso v(A)=v(C)=0 e v(B)=1 in cui l'antecedente è vero e l'antecedente del conseguente è vero. In tal caso il conseguente del conseguente è falso e la formula è falsa, pertanto non è una tautologia e non è un teorema di L.
c) La formula è una tautologia se e solo se la sua negazione è insoddisfacibile e quindi se e solo se si può, dalla forma a clausole della sua negazione, ricavare per risoluzione la clausola vuota.
Trasformiamo la negazione della nostra formula in forma a clausole. Si ha:
$\sim(\sim(\sim A\Rightarrow C)\Rightarrow(B\Rightarrow f(A,B,C)))\equiv\sim((A\vee C)\vee(\sim B\vee f(A,B,C))\equiv\sim A\wedge\sim C\wedge B\wedge\sim f(A,B,C)\equiv \sim A\wedge\sim C\wedge B\wedge\sim((A\wedge B\wedge\sim C)\vee(\sim A\wedge B\wedge C))\equiv\sim A\wedge\sim C\wedge B\wedge(\sim A\vee\sim B\vee C)\wedge(A\vee\sim B\vee\sim C))$ da cui $\sim(\sim(\sim A\Rightarrow C)\Rightarrow(B\Rightarrow f(A,B,C)))^c=\{\{\sim A\},\{\sim C\},\{B\},\{\sim A,\sim B,C\},\{A,\sim B,\sim C\}\}$.
Le ultime due clausole, contenendo rispettivamente la prima e la seconda, sono superflue e non ci sono risolventi delle tre clausole rimaste, per cui non è possibile ricavare la clausola vuota per risoluzione e la formula non è un teorema.

Esercizio 2

Usando la risoluzione verificare se, date le seguenti regole di un protocollo su messaggi:

1. Se un messaggio è certificato e crittografato, allora è approvato.

2. Esiste un messaggio certificato.

3. Se un messaggio non è crittografato, allora è approvato.

4. Se esiste un messaggio approvato, allora nessun messaggio è certificato.

sia possibile dedurre:

5. Tutti i messaggi sono approvati.

TRACCIA DI SOLUZIONE
Codifichiamo in logica del primo ordine le formule date usando le lettere predicative C, Cr, A, tutte di arità 1, per indicare rispettivamente "essere certificato", "essere criptato", "essere approvato" e la variabile x per indicare il generico messaggio. Si ha

1. $\forall x(C(x)\wedge Cr(x)\Rightarrow A(x))$
2. $\exists xC(x)$
3. $\forall x(\sim Cr(x)\Rightarrow A(x))$
4. $\exists xA(x)\Rightarrow\forall x\sim C(x)$
5. $\forall xA(x)$

Se dall'insieme di clausole costituite dalle clausole di 1.,2.,3.,4., e della negazione di 5. si ricava la clausola vuota, la formula 5. si deduce dalle prime quattro. Scriviamo quindi 1.,2.,3.,4., e la negazione di 5. in forma di Skolem e poi in forma a clausole La 1. e la 3. sono in forma di Skolem, la 2. diventa C(a) dove a è una costante di Skolem, la 4. diventa $\forall x\forall y(A(x)\Rightarrow\sim C(y))$, la negazione della 5. diventa allora ~A(b) dove b è una nuova costante di Skolem. Le clausole diventano quindi {{~C(x),~Cr(x),A(x)},{C(a)}, {Cr(x),A(x)},{~A(x),~C(y)},{~A(b)}}.
Usando la prima e la seconda clausola con l'unificatore {a/x}si trova per risoluzione la clausola {~Cr(a),A(a)}; da questa per risoluzione con la terza clausola, sempre facendo uso dell'unificatore {a/x}, si trova la clausola {A(a)}; da questa con la quarta clausola si trova sempre tramite l'unificatore {a/x} la clausola {~C(y)} che con la seconda tramite l'unificatore {a/y} genera la clausola vuota.
Dunque 5. è deducibile da 1,2,3,4, più precisamente 1,2,3,4, sono un insieme insoddisfacibile di formule, da cui quindi possiamo dedurre una qualsiasi formula.
Osservate inoltre che non è stata fatta la separazioni di variabili, perché nella risoluzione non si sono mai usate coppie di clausole con variabili comuni e quindi i cambio risultava superfluo.