UNIVERSITA' DI FIRENZE – CDL IN INFORMATICA – A. A. 2019-2020

Prova scritta "a distanza" di "Matematica Discreta e Logica" del giorno 18 giugno 2020

Soluzione degli esercizi

Esercizio 1

La password di accesso a una banca dati è composta di sette caratteri alfanumerici anche ripetuti (scelti fra le usuali dieci cifre $\{0,1,2,\dots,9\}$ e le ventuno lettere dell'alfabeto italiano) uno dei quali può essere sostituito dal carattere "#" che in tal caso deve comparire esattamente tre volte.

Si dica, motivando la risposta, in quante di tali password compaiono esattamente tre lettere, non necessariamente adiacenti ma disposte in ordine alfabetico.

Soluzione – Distinguiamo il caso in cui il carattere "#" non compare da quello in cui compare, e (poiché i due casi sono mutuamente esclusivi ed esauriscono tutte le possibilità) applichiamo poi il principio di addizione.

Se il carattere "#" non compare, ci sono tre lettere e quattro cifre. Come prima cosa, scegliamo il posto delle tre lettere (che determinerà automaticamente il posto delle quattro cifre); questo si può fare in

$$\tbinom{7}{3}\ \left(=\tfrac{7\cdot6\cdot5}{3\cdot2}=35\right)$$

modi diversi. Per scegliere le tre lettere basta scegliere tre elementi, anche ripetuti, nell'insieme delle 21 lettere a disposizione (poi andranno sistemate in ordine alfabetico, secondo le condizioni del problema); questo si può fare in

$$\tbinom{21+3-1}{3}\ \left(=\tbinom{23}{3}=\tfrac{23\cdot22\cdot21}{3\cdot2}=23\cdot11\cdot7=1\,771\right)$$

modi diversi. Infine, le quattro cifre si possono scegliere in $10^4=10\,000$ modi diversi. Applicando il principio di moltiplicazione, si trova che, fra le password che soddisfano la condizione posta, quelle in cui il carattere "#" non compare sono

$$35\cdot1\,771\cdot10\,000=619\,850\,000\,.$$

Se invece il carattere "#" compare, esso compare in esattamente tre posizioni che possono essere scelte in

$$\tbinom{7}{3}\ \left(=\tfrac{7\cdot6\cdot5}{3\cdot2}=35\right)$$

modi diversi. Poiché devono comparire tre lettere, ci sarà un'unica cifra la cui posizione (che determina anche quella delle tre lettere) può essere scelta in 4 modi diversi. Per scegliere le tre lettere basta scegliere tre elementi, anche ripetuti, nell'insieme delle 21 lettere a disposizione (poi andranno sistemate in ordine alfabetico, secondo le condizioni del problema); questo (come si è già visto) si può fare in

$$\tbinom{21+3-1}{3}\ \left(=\tbinom{23}{3}=\tfrac{23\cdot22\cdot21}{3\cdot2}=23\cdot11\cdot7=1\,771\right)$$

modi diversi. Infine, l'unica cifra si può scegliere in 10 modi diversi. Applicando il principio di moltiplicazione, si trova che, fra le password che soddisfano la condizione posta, quelle in cui il carattere "#" compare sono

$$35\cdot4\cdot1\,771\cdot10=2\,479\,400\,.$$

La risposta al quesito si ottiene infine applicando il principio di addizione, ed è

$$619\,850\,000+2\,479\,400=622\,329\,400\,.$$

Esercizio 2

Per ciascuno dei seguenti tre enunciati si dica, motivando la risposta, se è vero oppure è falso. Se l'enunciato è vero, si faccia esplicito riferimento ai teoremi (studiati nel corso) dai quali ciò consegue; se l'enunciato è falso, si trovi un controesempio.

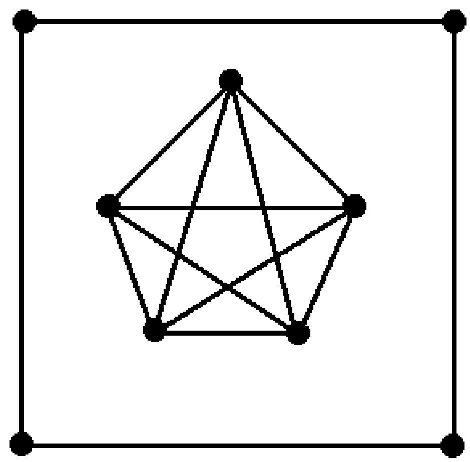
(a) Per ogni grafo finito $\mathcal{G}$ senza orientamento, se $\mathcal{G}$ ha esattamente 9 vertici dei quali 5 hanno grado 4 e i restanti hanno grado 2, allora $\mathcal{G}$ è euleriano.

(b) Per ogni grafo finito $\mathcal{G}$ senza orientamento, se $\mathcal{G}$ ha esattamente 28 vertici dei quali 19 hanno grado 6 e i restanti hanno grado 5, allora $\mathcal{G}$ è hamiltoniano.

(c) Per ogni grafo finito $\mathcal{G}$ senza orientamento, se $\mathcal{G}$ è $2-$connesso allora $\mathcal{G}$ è hamiltoniano.

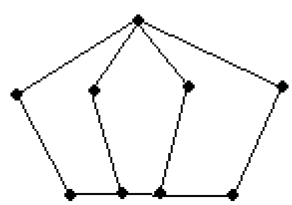
Soluzione – Gli enunciati (a) e (c), sono falsi, mentre l'enunciato (b) è vero.

Mostriamo con un controesempio che l'enunciato (a) è falso. Nel seguente grafo ogni vertice ha grado 2 oppure 4, ma il grafo non è euleriano (non ci può essere un circuito euleriano perché il grafo non è connesso!):



Ora dimostriamo che l'enunciato (b) è vero. L'enunciato consiste in un'implicazione, che come sappiamo è vera ogni volta che la premessa è falsa. Ma qui la premessa è certamente falsa per ogni grafo senza orientamento: essa afferma infatti che ci sono esattamente 9 vertici di grado 5; e noi sappiamo (teorema 1.3.2 degli "Appunti di teoria dei grafi" disponibili nella pagina e-learning di questo insegnamento) che in qualsiasi grafo finito senza orientamento il numero dei vertici di grado dispari è pari!

Mostriamo infine con un controesempio che un grafo $2-$connesso può essere hamiltoniano:



(Questo è l'esempio 6.3.4 degli "Appunti di teoria dei grafi").

Esercizio 3

Nell'anello $\mathbb{Z}_{20\,923}$ delle classi di resto modulo $20\,923$ ci sono più elementi invertibili o divisori dello zero?

Soluzione – Per il corollario 11.2.3 degli appunti di algebra, ogni elemento diverso da $[0]$ di $\mathbb{Z}_{20\,923}$ è invertibile oppure (qui la disgiunzione è esclusiva!) è un divisore dello zero. Se indichiamo con k il numero degli elementi invertibili di $\mathbb{Z}_{20\,923}$, il numero dei divisori dello zero di $\mathbb{Z}_{20\,923}$ è dunque $20\,923 - k - 1$.

Per il teorema 11.2.1 degli appunti di algebra, il numero degli elementi invertibili di $\mathbb{Z}_{20\,923}$ è $\varphi(20\,923)$ (dove φ è la funzione di Euler). Per calcolare quanti sono gli elmeneti invertibili e quanti sono i divisori dello zero di $\mathbb{Z}_{20\,923}$ dobbiamo dunque calcolare $\varphi(20\,923)$ e a questo scopo ci serve una scomposizione di $20\,923$ in fattori primi.

Per i noti criteri di divisibilità per 2, per 3 e per 5, $20\,923$ non è divisibile né per 2 né per 3 né per 5. Si ha però

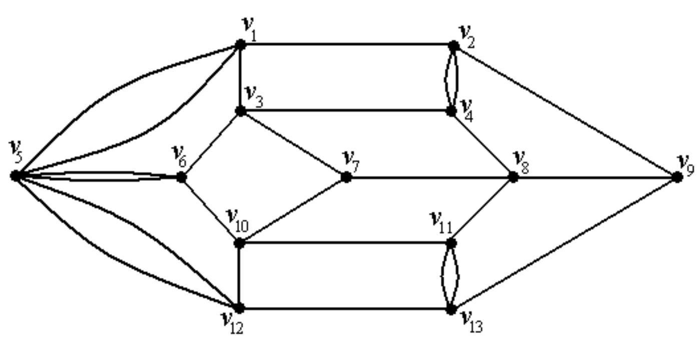
$$20\,923 = 7 \cdot 2\,989\,;$$
$$2\,989 = 7 \cdot 427\,;$$
$$427 = 7 \cdot 61\,;$$

con 61 numero primo (perché non è divisibile né per 2, né per 3, né per 5, né per 7, mentre ogni altro numero primo ha il quadrato che supera 61).

Pertanto, $\varphi(20\,923) = \varphi(7^3 \cdot 61) = \varphi(7^3) \cdot \varphi(61) = 7^2 \cdot 6 \cdot 60 = 17\,640$ e nell'anello $\mathbb{Z}_{20\,923}$ delle classi di resto modulo $20\,923$ ci sono $17\,640$ elementi invertibili e $3\,282$ $(= 20923 - 17640 - 1)$ divisori dello zero. Ci sono dunque più elementi invertibili che divisori dello zero.

Esercizio 4

Sia $\mathcal{G}$ il (multi)grafo con 13 vertici qui disegnato:



Si dica, motivando ciascuna risposta:

(i) quanti lati ha $\mathcal{G}$;

(ii) se $\mathcal{G}$ è euleriano; se $\mathcal{G}$ non è euleriano ma in $\mathcal{G}$ c'è un cammino euleriano;

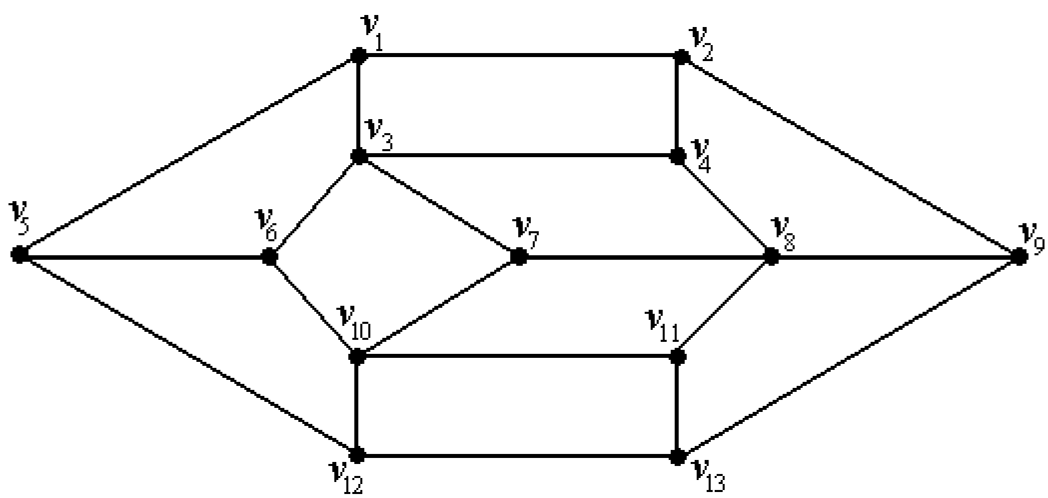
(iii) se $\mathcal{G}$ è hamiltoniano.

Soluzione – Per contare il numero dei lati è comodo guardare che grado ha ciascun vertice (questa informazione infatti è facile da ricavarsi senza errori, e ci consentirà poi di rispondere immediatamente alla domanda del punto (ii)).

I vertici $v_1, v_2, v_3, v_4, v_6, v_8, v_{10}, v_{11}, v_{12}$ e v_{13} hanno grado 4; il vertice v_5 ha grado 6; i vertici v_7 e v_9 hanno grado 3. Pertanto la somma dei gradi di tutti i vertici è 52, e il grafo $\mathcal{G}$ ha 26 lati.

Il grafo $\mathcal{G}$ è connesso; poiché due vertici di $\mathcal{G}$ hanno grado dispari e tutti gli altri vertici hanno grado pari, $\mathcal{G}$ non è euleriano ma ha un cammino euleriano.

Poiché $\mathcal{G}$ è disegnato nel piano senza sovrapposizione di lati, possiamo cercare di utilizzare il teorema di Grinberg per dimostrare che $\mathcal{G}$ non è hamiltoniano. Conviene ragionare sul sostegno di $\mathcal{G}$, cioè sul grafo $\mathcal{G}^*$ qui disegnato:



Nel grafo $\mathcal{G}^*$ ci sono 9 facce col bordo formato da 4 lati e una faccia (certamente esterna ad un eventuale ciclo hamiltoniano) col bordo formato da 6 lati.

Supponiamo che in $\mathcal{G}$ (e quindi in $\mathcal{G}^*$) esista un ciclo hamiltoniano $\mathcal{C}$; sia e_4 il numero delle facce di $\mathcal{G}^*$ col bordo di 4 lati esterne a $\mathcal{C}$ e sia i_4 il numero delle facce di $\mathcal{G}^*$ col bordo di 4 lati interne a $\mathcal{C}$; per il teorema di Grinberg deve essere

$$2(e_4 - i_4) + 4 = 0$$

ossia

$$e_4 - i_4 = -2$$

ma questo è assurdo perché sarebbe

$$e_4 + i_4 = 9$$
$$e_4 - i_4 = -2$$

e quindi, sommando membro a membro,

$$2e_4 = 7$$

impossibile perché il primo membro dell'uguaglianza è pari mentre il secondo membro è dispari.

Dunque in $\mathcal{G}$ non può esistere un ciclo hamiltoniano, cioè $\mathcal{G}$ non è hamiltoniano.

Esercizio 5

Siano x, y, z, t variabili proposizionali, e siano

$$\varphi_1 := x \to (y \wedge (t \vee z)); \qquad \varphi_2 := (t \wedge y) \to x\,; \qquad \varphi_3 := (t \wedge z) \to x\,;$$

$$\varphi_4 := x \vee y \vee (\neg z)\,; \qquad \varphi_5 := t \vee x \vee y\,.$$

Si dica, motivando la risposta, se la formula

$$\varphi_0 := (t \vee x \vee z) \to (y \wedge z)$$

è o non è conseguenza logica di $\{\varphi_1,\ \ \varphi_2,\ \ \varphi_3,\ \ \varphi_4,\ \ \varphi_5\}$.

Soluzione – Si ha

$$\{\varphi_1,\ \ \varphi_2,\ \ \varphi_3,\ \ \varphi_4,\ \ \varphi_5\} \models \varphi_0$$

se e soltanto se la formula $\varphi := \varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4 \wedge \varphi_5 \wedge (\neg\varphi_0)$ non è soddisfacibile.

Scriviamo φ in forma normale congiuntiva che poi trasformiamo in un insieme di clausole:

$$\varphi \equiv ((\neg x) \vee (y \wedge (t \vee z))) \wedge (\neg(t \wedge y) \vee x) \wedge (\neg(t \wedge z) \vee x) \wedge (x \vee y \vee (\neg z)) \wedge$$
$$\wedge\, (t \vee x \vee y) \wedge ((t \vee x \vee z) \wedge \neg(y \wedge z)) \equiv$$
$$\equiv ((\neg x \vee y) \wedge (\neg x \vee t \vee z)) \wedge ((\neg t) \vee (\neg y) \vee x) \wedge ((\neg t) \vee (\neg z) \vee x) \wedge (x \vee y \vee (\neg z)) \wedge$$
$$\wedge\, (t \vee x \vee y) \wedge ((t \vee x \vee z) \wedge ((\neg y) \vee (\neg z)))\ .$$

L'insieme di clausole corrispondente è

$$\mathcal{K} = \{\{\neg x, y\}, \{t, \neg x, z\}, \{\neg t, x, \neg y\}, \{\neg t, x, \neg z\}, \{x, y, \neg z\}, \{t, x, y\}, \{t, x, z\}, \{\neg y, \neg z\}\}\ .$$

Applichiamo l'algoritmo di Davis e Putnam, scegliendo come primo *pivot* una variabile proposizionale che compare in una clausola di lunghezza 2, ad esempio la x .

Pivot x:

clausole non contenenti né x né $\neg x$: $\{\neg y, \neg z\}$;

$\mathrm{Res}_x(\{\neg x, y\},\ \{\neg t, x, \neg y\}) = \{\neg t, y, \neg y\}$ (si sopprime perché tautologia) ;

$\mathrm{Res}_x(\{\neg x, y\},\ \{\neg t, x, \neg z\}) = \{\neg t, y, \neg z\}$;

$\mathrm{Res}_x(\{\neg x, y\},\ \{x, y, \neg z\}) = \{y, \neg z\}$;

$\mathrm{Res}_x(\{\neg x, y\},\ \{t, x, y\}) = \{t, y\}$;

$\mathrm{Res}_x(\{\neg x, y\},\ \{t, x, z\}) = \{t, y, z\}$;

$\mathrm{Res}_x(\{t, \neg x, z\},\ \{\neg t, x, \neg y\}) = \{t, \neg t, \neg y, z\}$ (si sopprime perché tautologia) ;

$\mathrm{Res}_x(\{t, \neg x, z\},\ \{\neg t, x, \neg z\}) = \{t, \neg t, z, \neg z\}$ (si sopprime perché tautologia) ;

$\mathrm{Res}_x(\{t, \neg x, z\},\ \{x, y, \neg z\}) = \{t, y, z, \neg z\}$ (si sopprime perché tautologia) ;

$\mathrm{Res}_x(\{t, \neg x, z\},\ \{t, x, y\}) = \{t, y, z\}$ (si sopprime perché già ottenuta) ;

$\mathrm{Res}_x(\{t, \neg x, z\},\ \{t, x, z\}) = \{t, z\}$;

$$\{\{\neg y, \neg z\},\ \ \{\neg t, y, \neg z\},\ \ \{y, \neg z\},\ \ \{t, y\},\ \ \{t, y, z\},\ \ \{t, z\}\}$$

Alcune delle clausole ottenute si possono eliminare perché includono altre clausole ottenute. Poiché $\{y, \neg z\} \subset \{\neg t, y, \neg z\}$, si può eliminare la clausola $\{\neg t, y, \neg z\}$; poiché $\{t, y\} \subset \{t, y, z\}$, si può eliminare la clausola $\{t, y, z\}$. Siamo dunque ricondotti a considerare il seguente insieme di clausole:

$$\{\{\neg y, \neg z\},\ \ \{y, \neg z\},\ \ \{t, y\},\ \ \{t, z\}\}\ .$$

Pivot t:

clausole non contenenti né t né $\neg t$: $\{\neg y, \neg z\}$, $\{y, \neg z\}$;
Non ci sono risolventi da calcolare!

$$\{\{\neg y, \neg z\},\ \{y, \neg z\}\}\ .$$

Pivot z:

clausole non contenenti né z né $\neg z$: non ce ne sono!
Non ci sono risolventi da calcolare!

$$\{\ \}.$$

Avendo ottenuto l'insieme che non ha clausole, possiamo concludere che $\mathcal{K}$ è soddisfacibile e dunque φ_0 non è conseguenza logica di $\{\varphi_1,\ \ \varphi_2,\ \ \varphi_3,\ \ \varphi_4,\ \ \varphi_5\}$.

Esercizio 6

Si stabilisca se dalle premesse

(i) Qualche scimmia è un gorilla;
(ii) nessun pesce è un gorilla;

si può dedurre logicamente che

(iii) qualche scimmia non è un pesce.

Soluzione – Introduciamo tre simboli di predicato unario (S, G, P), che interpretiamo come segue per tradurre le premesse date:

$\mathrm{S}(x) := x$ è una scimmia;

$\mathrm{G}(x) := x$ è un gorilla;

$\mathrm{P}(x) := x$ è un pesce.

In questo linguaggio della logica dei predicati, le premesse diventano:

(i) $\quad (\exists x)\big(\mathrm{S}(x) \wedge \mathrm{G}(x)\big)$;

(ii) $\quad \neg(\exists x)\big(\mathrm{P}(x) \wedge \mathrm{G}(x)\big)$;

e la supposta conclusione diventa

(iv) $\quad (\exists x)\big(\mathrm{S}(x) \wedge \neg\mathrm{P}(x)\big)$.

Dobbiamo pertanto vedere se

$$(\exists x)\big(\mathrm{S}(x) \wedge \mathrm{G}(x)\big) \wedge \neg(\exists x)\big(\mathrm{P}(x) \wedge \mathrm{G}(x)\big) \models (\exists x)\big(\mathrm{S}(x) \wedge \neg\mathrm{P}(x)\big)$$

ossia se la formula ben formata φ definita da

$$(\exists x)\big(\mathrm{S}(x) \wedge \mathrm{G}(x)\big) \wedge \neg(\exists x)\big(\mathrm{P}(x) \wedge \mathrm{G}(x)\big) \wedge \neg\big((\exists x)\big(\mathrm{S}(x) \wedge \neg\mathrm{P}(x)\big)\big)$$

è o non è soddisfacibile.

Scriviamo φ in forma normale prenessa:

$$\varphi \equiv (\exists x)(\mathrm{S}(x) \wedge \mathrm{G}(x)) \wedge \neg(\exists x)(\mathrm{P}(x) \wedge \mathrm{G}(x)) \wedge \neg((\exists x)(\mathrm{S}(x) \wedge \neg\mathrm{P}(x))) \equiv$$
$$\equiv (\exists x)(\mathrm{S}(x) \wedge \mathrm{G}(x)) \wedge (\forall x)(\neg(\mathrm{P}(x) \wedge \mathrm{G}(x))) \wedge (\forall x)(\neg(\mathrm{S}(x) \wedge \neg\mathrm{P}(x))) \equiv$$
$$\equiv (\exists x)(\mathrm{S}(x) \wedge \mathrm{G}(x)) \wedge (\forall x)((\neg\mathrm{P}(x)) \vee (\neg\mathrm{G}(x))) \wedge (\forall x)((\neg\mathrm{S}(x)) \vee \mathrm{P}(x)) \equiv$$
$$\equiv (\exists x)(\mathrm{S}(x) \wedge \mathrm{G}(x)) \wedge (\forall y)((\neg\mathrm{P}(y)) \vee (\neg\mathrm{G}(y))) \wedge (\forall y)((\neg\mathrm{S}(y)) \vee \mathrm{P}(y)) \equiv$$
$$\equiv (\exists x)(\forall y)((\mathrm{S}(x) \wedge \mathrm{G}(x)) \wedge ((\neg\mathrm{P}(y)) \vee (\neg\mathrm{G}(y))) \wedge ((\neg\mathrm{S}(y)) \vee \mathrm{P}(y))) \equiv$$
$$\equiv (\exists x)(\forall y)(\mathrm{S}(x) \wedge \mathrm{G}(x) \wedge ((\neg\mathrm{P}(y)) \vee (\neg\mathrm{G}(y))) \wedge ((\neg\mathrm{S}(y)) \vee \mathrm{P}(y)))\,.$$

Per ridurla in forma di Skolem, basta introdurre un simbolo di costante c e sostituirlo alla variabile individuale x, ottenendo:

$$(\forall y)(\mathrm{S}(c) \wedge \mathrm{G}(c) \wedge ((\neg\mathrm{P}(y)) \vee (\neg\mathrm{G}(y))) \wedge ((\neg\mathrm{S}(y)) \vee \mathrm{P}(y)))\,.$$

A questa formula resta associato il seguente schema di clausole:

$$\{\{\mathrm{S}(c)\},\quad \{\mathrm{G}(c)\},\quad \{\neg\mathrm{P}(y), \neg\mathrm{G}(y)\},\quad \{\neg\mathrm{S}(y), \mathrm{P}(y)\}\}\,.$$

Poiché l'universo di Herbrandt consiste della sola costante c, assegniamo direttamente alla y il valore c e otteniamo questo insieme di clausole:

$$\{\{\mathrm{S}(c)\},\quad \{\mathrm{G}(c)\},\quad \{\neg\mathrm{P}(c), \neg\mathrm{G}(c)\},\quad \{\neg\mathrm{S}(c), \mathrm{P}(c)\}\}\,.$$

Possiamo applicare l'algoritmo di Davis-Putnam!

Pivot $\mathrm{S}(c)$:

clausole non contenenti né $\mathrm{S}(c)$ né $\neg\mathrm{S}(c)$: $\{\mathrm{G}(c)\}, \{\neg\mathrm{P}(c), \neg\mathrm{G}(c)\}$;

$\mathrm{Ris}_{\mathrm{S}(c)}(\{\mathrm{S}(c)\}, \{\neg\mathrm{S}(c), \mathrm{P}(c)\}) = \{\mathrm{P}(c)\}$;

$$\{\{\mathrm{G}(c)\},\quad \{\neg\mathrm{P}(c), \neg\mathrm{G}(c)\},\quad \{\mathrm{P}(c)\}\}\,.$$

Pivot $\mathrm{G}(c)$:

clausole non contenenti né $\mathrm{T}(c)$ né $\neg\mathrm{T}(c)$: $\{\mathrm{P}(c)\}$;

$\mathrm{Ris}_{\mathrm{G}(c)}(\{\mathrm{G}(c)\}, \{\neg\mathrm{P}(c), \neg\mathrm{G}(c)\}) = \{\neg\mathrm{P}(c)\}$;

$$\{\{\mathrm{P}(c)\},\quad \{\neg\mathrm{P}(c)\}\}\,.$$

Pivot $\mathrm{P}(c)$:

clausole non contenenti né $\mathrm{P}(c)$ né $\neg\mathrm{P}(c)$: non ce ne sono!

$\mathrm{Ris}_{\mathrm{P}(c)}(\{\mathrm{P}(c)\}, \{\neg\mathrm{P}(c)\}) = [\,]$;

$$\{[\,]\}\,.$$

Poiché abbiamo ottenuto la clausola vuota, l'insieme di clausole considerato non è soddisfacibile; dunque nemmeno la formula φ è soddisfacibile, ed abbiamo dimostrato che la (iii) è effettivamente conseguenza logica delle (i) e (ii).