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

Prova "*in itinere*" per "Matematica Discreta e Logica" – primo appello

31.1.2020

FILA "D"

Esercizio 1

Siano p, q, r, s variabili proposizionali. Per ciascuna delle seguenti affermazioni si dica, motivando la risposta, se è vera o falsa:

(i) $\quad q \wedge \neg q \wedge (p \rightarrow s) \models (r \rightarrow s) \wedge (\neg q \rightarrow r)$;
(ii) $\quad (p \rightarrow q) \wedge (\neg s \rightarrow r) \models p \vee \neg p$.

Soluzione – Esaminiamo separatamente le due affermazioni proposte.

(i) Poiché la formula $q \wedge \neg q$ è insoddisfacibile, anche la formula $q \wedge \neg q \wedge (p \rightarrow s)$ è insoddisfacibile; pertanto qualsiasi valutazione di verità che la soddisfa (non ce ne sono!) soddisfa anche la formula $(r \rightarrow s) \wedge (\neg p \rightarrow q)$, e quindi la (i) è vera.

(ii) Poiché la formula $p \vee \neg p$ è una tautologia, essa è certamente soddisfatta da qualsiasi valutazione di verità soddisfi la formula $(p \rightarrow q) \wedge (\neg s \rightarrow r)$; pertanto, anche la (ii) è vera.

Esercizio 2

Siano h, k, t, w, x, y, z variabili proposizionali. Si stabilisca, motivando la risposta, se il seguente insieme di clausole è soddisfacibile; e nel caso che la risposta sia affermativa si trovi un'interpretazione che lo soddisfa:

$$\{\{x, y\},\ \{k, t\},\ \{h, \neg k, t, z\},\ \{\neg h, \neg w\},\ \{w, z\},\ \{\neg k, \neg y\},\ \{\neg h, k, \neg t, \neg z\},$$
$$\{\neg x, \neg z\},\ \{h, \neg t\},\ \{w, x, \neg y\}\}.$$

Soluzione – 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 $\neg x$: $\{k, t\}, \{h, \neg k, t, z\}, \{\neg h, \neg w\}, \{w, z\}, \{\neg k, \neg y\}, \{\neg h, k, \neg t, \neg z\}, \{h, \neg t\}$;

$\text{Ris}_x(\{x, y\}, \{\neg x, \neg z\}) = \{y, \neg z\}$;
$\text{Ris}_h(\{w, x, \neg y\}, \{\neg x, \neg z\}) = \{w, \neg y, \neg z\}$;

$$\{\{k, t\}, \{h, \neg k, t, z\}, \{\neg h, \neg w\}, \{w, z\}, \{\neg k, \neg y\}, \{\neg h, k, \neg t, \neg z\}, \{h, \neg t\}, \{y, \neg z\}, \{w, \neg y, \neg z\}\}.$$

Pivot k:

clausole non contenenti né k né $\neg k$: $\{\neg h, \neg w\}$, $\{w, z\}$, $\{h, \neg t\}$, $\{y, \neg z\}$, $\{w, \neg y, \neg z\}$;

$\text{Ris}_k(\{k, t\}, \{h, \neg k, t, z\}) = \{h, t, z\}$;
$\text{Ris}_k(\{k, t\}, \{\neg k, \neg y\}) = \{t, \neg y\}$;
$\text{Ris}_k(\{\neg h, k, \neg t, \neg z\}, \{h, \neg k, t, z\}) = \{h, \neg h, t, \neg t, z, \neg z\}$ (si sopprime perché tautologia) ;
$\text{Ris}_k(\{\neg h, k, \neg t, \neg z\}, \{\neg k, \neg y\}) = \{\neg h, \neg t, \neg y, \neg z\}$;

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

.

Pivot h:

clausole non contenenti né h né $\neg h$: $\{w, z\},\ \{y, \neg z\},\ \{w, \neg y, \neg z\},\ \{t, \neg y\}$;

$\text{Ris}_h(\{\neg h, \neg w\}, \{h, \neg t\}) = \{\neg t, \neg w\}$;
$\text{Ris}_h(\{\neg h, \neg w\}, \{h, t, z\}) = \{t, \neg w, z\}$;
$\text{Ris}_h(\{\neg h, \neg t, \neg y, \neg z\}, \{h, \neg t\}) = \{\neg t, \neg y, \neg z\}$;
$\text{Ris}_h(\{\neg h, \neg t, \neg y, \neg z\}, \{h, t, z\}) = \{t, \neg t, \neg y, z, \neg z\}$ (si sopprime perché tautologia) ;

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

Pivot w:

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

$\text{Ris}_w(\{w, z\}, \{\neg t, \neg w\}) = \{\neg t, z\}$;
$\text{Ris}_w(\{w, z\}, \{t, \neg w, z\}) = \{t, z\}$;
$\text{Ris}_w(\{w, \neg y, \neg z\}, \{\neg t, \neg w\}) = \{\neg t, \neg y, \neg z\}$ (si sopprime perché già presente) ;
$\text{Ris}_w(\{w, \neg y, \neg z\}, \{t, \neg w, z\}) = \{t, \neg y, z, \neg z\}$ (si sopprime perché tautologia) ;

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

Pivot y:

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

$\text{Ris}_y(\{y, \neg z\}, \{t, \neg y\}) = \{t, \neg z\}$;
$\text{Ris}_y(\{y, \neg z\}, \{\neg t, \neg y, \neg z\}) = \{\neg t, , \neg z\}$;

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

Pivot t:

clausole non contenenti né t né $\neg t$: non ce ne sono!

$\text{Ris}_t(\{\neg t, z\}, \{t, z\}) = \{z\}$;
$\text{Ris}_t(\{\neg t, z\}, \{t, \neg z\}) = \{\neg z, z\}$ (si sopprime perché tautologia) ;
$\text{Ris}_t(\{\neg t, \neg z\}, \{t, z\}) = \{z, \neg z\}$ (si sopprime perché tautologia) ;
$\text{Ris}_t(\{\neg t, \neg z\}, \{t, \neg z\}) = \{\neg z\}$;

$$\{\{z\},\ \{\neg z\}\}$$

Pivot z:

clausole non contenenti né z né $\neg z$: non ce ne sono!

$\text{Ris}_z(\{z\}, \{\neg z\}) = [\,]$;

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

Avendo ottenuto la clausola vuota, possiamo concludere che $\mathcal{K}$ non è soddisfacibile.

Esercizio 3

Siano α, β le permutazioni sull'insieme $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ così definite:

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 8 & 1 & 5 & 9 & 4 & 2 & 7 \end{pmatrix}, \quad \beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 6 & 5 & 7 & 1 & 2 & 8 & 9 \end{pmatrix}.$$

e sia σ la permutazione ottenuta applicando prima α e poi β.

Si scriva σ come prodotto di cicli disgiunti e si dica, motivando la risposta, se σ è una permutazione pari oppure una permutazione dispari.

Soluzione – Si ha

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 6 & 8 & 4 & 7 & 9 & 5 & 3 & 2 \end{pmatrix}$$

dunque

$$\sigma = (2\ 6\ 9)(3\ 8)(5\ 7) = (2\ 6)(2\ 9)(3\ 8)(5\ 7)\,.$$

Poiché σ si scrive come prodotto di quattro trasposizioni, σ è una permutazione pari.

Esercizio 4

Sia $\mathbb{Z}_{11\,837}$ l'anello delle classi di resto modulo $11\,837$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{11\,837}$ a cui z appartiene.
Per ciascuna delle seguenti equazioni nell'incognita x si dica quante soluzioni ha in $\mathbb{Z}_{11\,837}$:

$$[267] \cdot x = [449]\,; \qquad\qquad [532] \cdot x = [665]\,.$$

Soluzione – Consideriamo in primo luogo l'equazione

$$[267] \cdot x = [449]\,.$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{11\,837}$ se e soltanto se il massimo comun divisore δ fra $11\,837$ e 267 divide 449 ; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra $11\,837$ e 267 :

$$11\,837 = 267 \cdot 44 + 89\,;$$
$$267 = 89 \cdot 3 + 0\,.$$

Il massimo comun divisore fra $11\,837$ e 267 è dunque 89; poiché non si tratta di un divisore di 449 (infatti $449 = 89 \cdot 5 + 4$), l'equazione considerata non ha soluzione (quindi il numero delle soluzioni è zero).

Consideriamo poi l'equazione

$$[532] \cdot x = [665]\,.$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{11\,837}$ se e soltanto se il massimo comun divisore δ fra $11\,837$ e 532 divide 665 ; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra $11\,837$ e 532 :

$$11\,837 = 532 \cdot 22 + 133\,;$$
$$532 = 133 \cdot 4 + 0\,.$$

Il massimo comun divisore fra $11\,837$ e 532 è dunque 133 ; poiché si tratta di un divisore di 665 ($= 133 \cdot 5$), l'equazione considerata ha 133 soluzioni.

Esercizio 5

Sia $\mathbb{Z}_{287}$ l'anello delle classi di resto modulo 287. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{287}$ a cui z appartiene.

Per ciascuno dei seguenti elementi di $\mathbb{Z}_{287}$ si stabilisca, motivando la risposta, se è invertibile in $\mathbb{Z}_{287}$ e, se è invertibile, se ne trovi l'inverso:

$$[82]\,; \qquad\qquad [100]\,.$$

Soluzione – Sappiamo che l'elemento $[a]$ è invertibile in $\mathbb{Z}_{287}$ se e soltanto se

$$\mathrm{MCD}(287, a) = 1\,.$$

Poiché

$$287 = 82 \cdot 3 + 41\,; \qquad 82 = 41 \cdot 2 + 0\,;$$

$$287 = 100 \cdot 2 + 87\,; \qquad 100 = 87 \cdot 1 + 13\,; \qquad 87 = 13 \cdot 6 + 9\,;$$
$$13 = 9 \cdot 1 + 4\,; \qquad 9 = 4 \cdot 2 + 1\,;$$
$$4 = 1 \cdot 4 + 0$$

si ha che

$$\mathrm{MCD}(287, 82) = 41 \neq 1, \qquad \mathrm{MCD}(287, 100) = 1$$

e pertanto fra i due elementi di $\mathbb{Z}_{287}$ proposti dall'esercizio l'unico invertibile è $[100]$.

Per trovare l'inverso di $[100]$ in $\mathbb{Z}_{287}$ dobbiamo risolvere l'equazione

$$[100] \cdot [x] = [1]$$

in $\mathbb{Z}_{287}$, che ci riconduce all'equazione diofantina

$$100\,x - 287\,y = 1$$

della quale vogliamo trovare una soluzione nella x. A tale scopo basta scrivere l'identità di Bezout, che si ricava dai calcoli già fatti per trovare il $\mathrm{MCD}(287, 100)$. Si ha dunque

$$1 = 9 - 4 \cdot 2 = 9 - (13 - 9) \cdot 2 = 9 \cdot 3 + 13 \cdot (-2) = (87 - 13 \cdot 6) \cdot 3 + 13 \cdot (-2) =$$
$$= 87 \cdot 3 + 13 \cdot (-20) = 87 \cdot 3 + (100 - 87) \cdot (-20) =$$
$$= 100 \cdot (-20) + 87 \cdot 23 = 100 \cdot (-20) + (287 - 100 \cdot 2) \cdot 23 = 100 \cdot (-66) + 287 \cdot 23$$

cosicché l'inverso di $[100]$ in $\mathbb{Z}_{287}$ è $[-66]$ $(= [221])$.

Esercizio 6

Con riferimento all'anello $\mathbb{Z}_{26\,875}$ delle classi di resto modulo $26\,875$, si dica, esprimendo ogni risposta in base *quindici*:

- quanti sono gli elementi invertibili;
- quanti sono i divisori dello zero.

Soluzione – Un elemento $[a]$ di $\mathbb{Z}_{26\,875}$ è invertibile se e soltanto se

$$\mathrm{MCD}(a, 26\,875) = 1$$

e quindi il numero degli elementi invertibili di $\mathbb{Z}_{26\,875}$ è

$$\varphi(26\,875) = \varphi(5^4 \cdot 43) = \varphi(5^4) \cdot \varphi(43) = 5^3 \cdot (5 - 1) \cdot (43 - 1) = 21\,000\,.$$

Scriviamo questo numero in base *quindici*, eseguendo successive divisioni per 15:

$$21\,000 = 15 \cdot 1\,400 + 0\,;$$
$$1\,400 = 15 \cdot 93 + 5\,;$$
$$93 = 15 \cdot 6 + 3\,;$$
$$6 = 15 \cdot 0 + 6\,.$$

Pertanto, *ventunomila* in base *quindici* si scrive 6350.

I divisori dello zero di $\mathbb{Z}_{26\,875}$ sono quegli elementi che sono diversi da zero e non sono invertibili; dunque il loro numero è $26\,875 - 1 - 21\,000 = 5\,874$.

Scriviamo questo numero in base *quindici*, eseguendo successive divisioni per 15:

$$5\,874 = 15 \cdot 391 + 9\,;$$
$$391 = 15 \cdot 26 + 1\,;$$
$$26 = 15 \cdot 1 + 11\,;$$
$$1 = 15 \cdot 0 + 1\,.$$

Pertanto, *cinquemilaottocentosettantaquattro* in base *quindici* si scrive $1\mathrm{B}19$.

Esercizio 7

Per ciascuna delle due seguenti affermazioni si dica se è vera per ogni $n \in \mathbb{N}$ (richiamando esplicitamente il motivo per cui lo è) oppure è falsa per qualche $n \in \mathbb{N}$ (presentando in questo caso un controesempio):

(i) se n divide un prodotto ab (con $a, b \in \mathbb{N}$), allora n divide a oppure n divide b;

(ii) se n è un numero dispari multiplo di 6 allora $n^2 - 1$ è multiplo di 7.

Soluzione –

(i) L'affermazione è falsa, come si vede considerando $n := 6$, $a := 4$ e $b := 9$.

(ii) Ogni multiplo di 6 è pari, e quindi non è dispari; dunque la condizione "n è un numero dispari multiplo di 6" è certamente falsa, qualunque sia $n \in \mathbb{N}$. Pertanto l'implicazione considerata è certamente vera, qualunque sia $n \in \mathbb{N}$.

Esercizio 8

La password di accesso a una banca dati è una sequenza ordinata di otto lettere dell'alfabeto italiano (21 caratteri) che soddisfa tutte le seguenti condizioni:

– le consonanti sono tre o quattro, tutte diverse fra loro e disposte, da sinistra a destra, in ordine alfabetico;

– le vocali possono essere anche ripetute ma anch'esse devono essere disposte, da sinistra a destra, in ordine alfabetico.

Si dica, motivando la risposta, quante sono in tutto le possibili password.

Soluzione – Conviene distinguere tra il caso in cui le consonanti sono tre e il caso in cui le consonanti sono quattro: essi si escludono a vicenda, quindi possiamo contare separatamente le password che rientrano nel primo caso e quelle che rientrano nel secondo caso e poi applicare il principio di addizione.

Consideriamo il caso in cui le consonanti sono tre. Il loro posto si può scegliere in $\binom{8}{3} = \frac{8\cdot7\cdot6}{3\cdot2} = 56$ modi diversi (e determina automaticamente il posto delle cinque vocali); le tre consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{3} = \frac{16\cdot15\cdot14}{3\cdot2} = 8\cdot5\cdot14 = 560$ modi diversi; le cinque vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+5-1}{5} = \frac{9\cdot8\cdot7\cdot6}{4\cdot3\cdot2} = 9\cdot2\cdot7 = 126$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel primo caso sono

$$56\cdot560\cdot126 = 3\,951\,360\,.$$

Consideriamo poi il caso in cui le consonanti sono quattro. Il loro posto si può scegliere in $\binom{8}{4} = \frac{8\cdot7\cdot6\cdot5}{4\cdot3\cdot2} = 70$ modi diversi (e determina automaticamente il posto delle quattro vocali); le quattro consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{4} = \frac{16\cdot15\cdot14\cdot13}{4\cdot3\cdot2} = 2\cdot5\cdot14\cdot13 = 1\,820$ modi diversi; le quattro vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+4-1}{4} = \frac{8\cdot7\cdot6\cdot5}{4\cdot3\cdot2} = 7\cdot2\cdot5 = 70$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel secondo caso sono

$$70\cdot1\,820\cdot70 = 8\,910\,000\,.$$

Applicando infine il principio di addizione, si ottiene che il numero totale delle possibili password è

$$3\,951\,360 + 8\,910\,000 = 12\,869\,360\,.$$