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

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

31.1.2020

FILA "B"

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

Soluzione – Esaminiamo separatamente le due affermazioni proposte.

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

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

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

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 k .

Pivot k:

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

$\text{Ris}_k(\{k, y\}, \{\neg k, \neg x\}) = \{\neg x, y\}$;
$\text{Ris}_k(\{k, w, \neg y\}, \{\neg k, \neg x\}) = \{w, \neg x, \neg y\}$;

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

Pivot t:

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

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

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

Pivot h:

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

Ris$_h(\{\neg h, \neg w\}, \{h, z\}) = \{\neg w, z\}$;
Ris$_w(\{\neg h, \neg w\}, \{h, x, \neg z\}) = \{\neg w, x, \neg z\}$;
Ris$_h(\{\neg h, \neg x, z\}, \{h, z\}) = \{\neg x, z\}$;
Ris$_w(\{\neg h, \neg x, z\}, \{h, x, \neg z\}) = \{x, \neg x, z, \neg z\}$ (si sopprime perché tautologia) ;

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

Pivot w:

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

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

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

Pivot y:

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

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

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

Pivot x:

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

Ris$_x(\{\neg x, z\}, \{x, z\}) = \{z\}$;
Ris$_k(\{\neg x, z\}, \{x, \neg z\}) = \{z, \neg z\}$ (si sopprime perché tautologia) ;
Ris$_x(\{\neg x, \neg z\}, \{x, z\}) = \{z, \neg z\}$ (si sopprime perché tautologia) ;
Ris$_k(\{\neg x, \neg z\}, \{x, \neg z\}) = \{\neg z\}$;

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

Pivot z:

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

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

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

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:

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

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

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

dunque

$$\sigma = (1\ 6)(3\ 5)(4\ 7\ 9) = (1\ 6)(3\ 5)(4\ 7)(4\ 9)\,.$$

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

Esercizio 4

Sia $\mathbb{Z}_{10\,507}$ l'anello delle classi di resto modulo $10\,507$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{10\,507}$ a cui z appartiene.
Per ciascuna delle seguenti equazioni nell'incognita x si dica quante soluzioni ha in $\mathbb{Z}_{10\,507}$:

$$[266] \cdot x = [931]\,; \qquad\qquad [237] \cdot x = [396]\,.$$

Soluzione — Consideriamo in primo luogo l'equazione

$$[266] \cdot x = [931]\,.$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{10\,507}$ se e soltanto se il massimo comun divisore δ fra $10\,507$ e 266 divide 931 ; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra $10\,507$ e 266 :

$$10\,507 = 266 \cdot 39 + 133\,;$$
$$266 = 133 \cdot 2 + 0\,.$$

Il massimo comun divisore fra $10\,507$ e 266 è dunque 133 ; poiché si tratta di un divisore di 931 ($= 133 \cdot 7$), l'equazione considerata ha 133 soluzioni.

Consideriamo poi l'equazione

$$[237] \cdot x = [396]\,.$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{10\,507}$ se e soltanto se il massimo comun divisore δ fra $10\,507$ e 237 divide 396 ; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra $10\,507$ e 237 :

$$10\,507 = 237 \cdot 44 + 79\,;$$
$$237 = 79 \cdot 3 + 0\,.$$

Il massimo comun divisore fra $10\,507$ e 237 è dunque 79 ; poiché non si tratta di un divisore di 396 (infatti $396 = 79 \cdot 5 + 1$), l'equazione considerata non ha soluzione (quindi il numero delle soluzioni è zero).

Esercizio 5

Sia $\mathbb{Z}_{301}$ l'anello delle classi di resto modulo 301. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{301}$ a cui z appartiene.
Per ciascuno dei seguenti elementi di $\mathbb{Z}_{301}$ si stabilisca, motivando la risposta, se è invertibile in $\mathbb{Z}_{301}$ e, se è invertibile, se ne trovi l'inverso:

$$[86]\,; \qquad\qquad [90]\,.$$

Soluzione $-$ Sappiamo che l'elemento $[a]$ è invertibile in $\mathbb{Z}_{301}$ se e soltanto se

$$\mathrm{MCD}(301, a) = 1\,.$$

Poiché

$$\begin{aligned} &301 = 86 \cdot 3 + 43\,; && 86 = 43 \cdot 2 + 0\,; && \\ &301 = 90 \cdot 3 + 31\,; && 90 = 31 \cdot 2 + 28\,; && 31 = 28 \cdot 1 + 3\,; \\ & && 28 = 3 \cdot 9 + 1\,; && 3 = 1 \cdot 3 + 0 \end{aligned}$$

si ha che

$$\mathrm{MCD}(301, 86) = 43 \neq 1, \qquad \mathrm{MCD}(301, 90) = 1$$

e pertanto fra i due elementi di $\mathbb{Z}_{301}$ proposti dall'esercizio l'unico invertibile è $[90]$.

Per trovare l'inverso di $[90]$ in $\mathbb{Z}_{301}$ dobbiamo risolvere l'equazione

$$[90] \cdot [x] = [1]$$

in $\mathbb{Z}_{301}$, che ci riconduce all'equazione diofantina

$$90\,x - 301\,y = 1$$

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 $\mathrm{MCD}(301, 90)$. Si ha dunque

$$\begin{aligned} 1 &= 28 - 3 \cdot 9 = 28 - (31 - 28) \cdot 9 = 28 \cdot 10 + 31 \cdot (-9) = \\ &= (90 - 31 \cdot 2) \cdot 10 + 31 \cdot (-9) = 90 \cdot 10 + 31 \cdot (-29) = \\ &= 90 \cdot 10 + (301 - 90 \cdot 3) \cdot (-29) = 301 \cdot (-29) + 90 \cdot 97 \end{aligned}$$

cosicché l'inverso di $[90]$ in $\mathbb{Z}_{301}$ è $[97]$.

Esercizio 6

Con riferimento all'anello $\mathbb{Z}_{19\,375}$ delle classi di resto modulo $19\,375$, si dica, esprimendo ogni risposta in base *quindici*:

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

Soluzione $-$ Un elemento $[a]$ di $\mathbb{Z}_{19\,375}$ è invertibile se e soltanto se

$$\mathrm{MCD}(a, 19\,375) = 1$$

e quindi il numero degli elementi invertibili di $\mathbb{Z}_{19\,375}$ è

$$\varphi(19\,375) = \varphi(5^4 \cdot 31) = \varphi(5^4) \cdot \varphi(31) = 5^3 \cdot (5-1) \cdot (31-1) = 15\,000\,.$$

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

$$15\,000 = 15 \cdot 1\,000 + 0\,;$$
$$1\,000 = 15 \cdot 66 + 10\,;$$
$$66 = 15 \cdot 4 + 6\,;$$
$$4 = 15 \cdot 0 + 4\,.$$

Pertanto, *quindicimila* in base *quindici* si scrive $46\mathrm{A}0$.

I divisori dello zero di $\mathbb{Z}_{19\,375}$ sono quegli elementi che sono diversi da zero e non sono invertibili; dunque il loro numero è $19\,375 - 1 - 15\,000 = 4\,374$.

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

$$4\,374 = 15 \cdot 291 + 9\,;$$
$$291 = 15 \cdot 19 + 6\,;$$
$$19 = 15 \cdot 1 + 4\,;$$
$$1 = 15 \cdot 0 + 1\,.$$

Pertanto, *quattromilatrecentosettantaquattro* in base *quindici* si scrive 1469 .

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 10 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 10 è pari, e quindi non è dispari; dunque la condizione "n è un numero dispari multiplo di 10" 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 sette lettere dell'alfabeto italiano (21 caratteri) che soddisfa tutte le seguenti condizioni:

$-$ le consonanti sono quattro o cinque, 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 quattro e il caso in cui le consonanti sono cinque: 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 quattro. Il loro posto si può scegliere in $\binom{7}{4} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35$ modi diversi (e determina automaticamente il posto delle tre vocali); le quattro consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{4} = \frac{16 \cdot 15 \cdot 14 \cdot 13}{4 \cdot 3 \cdot 2} = 2 \cdot 5 \cdot 14 \cdot 13 = 1\,820$ modi diversi; le tre vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+3-1}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 7 \cdot 5 = 35$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel primo caso sono

$$35 \cdot 1\,820 \cdot 35 = 2\,229\,500\,.$$

Consideriamo poi il caso in cui le consonanti sono cinque. Il loro posto si può scegliere in $\binom{7}{5} = \frac{7 \cdot 6}{2} = 21$ modi diversi (e determina automaticamente il posto delle due vocali); le cinque consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{5} = \frac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12}{5 \cdot 4 \cdot 3 \cdot 2} = 2 \cdot 14 \cdot 13 \cdot 12 = 4\,368$ modi diversi; le due vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+2-1}{2} = \frac{6 \cdot 5}{2} = 3 \cdot 5 = 15$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel secondo caso sono

$$21 \cdot 4\,368 \cdot 15 = 1\,375\,920\,.$$

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

$$2\,229\,500 + 1\,375\,920 = 3\,605\,420\,.$$