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

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

**31.1.2020**

FILA "F"

Esercizio 1

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

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

*Soluzione* – Esaminiamo separatamente le due affermazioni proposte.

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

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

*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 $h$.

Pivot $h$:

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

$\mathrm{Ris}_h(\{h, x\}, \{\neg h, \neg z\}) = \{x, \neg z\}$;
$\mathrm{Ris}_h(\{h, x\}, \{\neg h, w, x\}) = \{w, x\}$;

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

Pivot $t$:

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

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

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

Pivot $w$:

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

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

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

Pivot $k$:

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

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

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

Pivot $x$:

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

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

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

Le clausole $\{\neg y,\ z\}$ e $\{\neg y,\ \neg z\}$ si possono sopprimere perché contengono l'altra clausola $\{\neg y\}$, quindi si considera l'insieme di clausole

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

Pivot $y$:

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

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

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

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

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

e sia $\sigma$ la permutazione ottenuta applicando prima $\alpha$ e poi $\beta$.

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

*Soluzione* – Si ha

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

dunque

$$\sigma = (1\ 5)(2\ 4\ 8)(7\ 9) = (1\ 5)(2\ 4)(2\ 8)(7\ 9)\,.$$

Poiché $\sigma$ si scrive come prodotto di quattro trasposizioni, $\sigma$ è una permutazione pari.

Esercizio 4

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

$$301 = 86 \cdot 3 + 43\,; \qquad 86 = 43 \cdot 2 + 0\,;$$

$$301 = 90 \cdot 3 + 31\,; \qquad 90 = 31 \cdot 2 + 28\,; \qquad 31 = 28 \cdot 1 + 3\,;$$
$$28 = 3 \cdot 9 + 1\,; \qquad 3 = 1 \cdot 3 + 0$$

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

$$1 = 28 - 3 \cdot 9 = 28 - (31 - 28) \cdot 9 = 28 \cdot 10 + 31 \cdot (-9) =$$
$$= (90 - 31 \cdot 2) \cdot 10 + 31 \cdot (-9) = 90 \cdot 10 + 31 \cdot (-29) =$$
$$= 90 \cdot 10 + (301 - 90 \cdot 3) \cdot (-29) = 301 \cdot (-29) + 90 \cdot 97$$

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

Esercizio 5

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 $\delta$ fra $10\,507$ e $266$ divide $931$; e in tal caso essa ha esattamente $\delta$ 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 $\delta$ fra $10\,507$ e $237$ divide $396$; e in tal caso essa ha esattamente $\delta$ 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 6

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

- 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 *tredici*, eseguendo successive divisioni per $13$:

$$15\,000 = 13 \cdot 1\,153 + 11\,;$$
$$1\,153 = 13 \cdot 88 + 9\,;$$
$$88 = 13 \cdot 6 + 10\,;$$
$$6 = 13 \cdot 0 + 6\,.$$

Pertanto, *quindicimila* in base *tredici* si scrive $6\mathrm{A}9\mathrm{B}$.

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 *tredici*, eseguendo successive divisioni per $13$:

$4\,374 = 13 \cdot 336 + 6$;
$336 = 13 \cdot 25 + 11$;
$25 = 13 \cdot 1 + 12$;
$1 = 13 \cdot 0 + 1$.

Pertanto, *quattromilatrecentosettantaquattro* in base *tredici* si scrive $1\mathrm{CB}6$.

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 $24$ allora $n^2 - 1$ è multiplo di $17$.

*Soluzione* –

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

($ii$) Ogni multiplo di $24$ è pari, e quindi non è dispari; dunque la condizione "$n$ è un numero dispari multiplo di $24$" 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 cinque o sei, 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 cinque e il caso in cui le consonanti sono sei: 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 cinque. Il loro posto si può scegliere in $\binom{8}{5} = \frac{8\cdot7\cdot6}{3\cdot2} = 56$ modi diversi (e determina automaticamente il posto delle tre vocali); le cinque consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{5} = \frac{16\cdot15\cdot14\cdot13\cdot12}{5\cdot4\cdot3\cdot2} = 2\cdot14\cdot13\cdot12 = 4\,368$ modi diversi; le tre vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+3-1}{3} = \frac{7\cdot6\cdot5}{3\cdot2} = 7\cdot5 = 35$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel primo caso sono

$$56\cdot4\,368\cdot35 = 8\,561\,280\,.$$

Consideriamo poi il caso in cui le consonanti sono sei. Il loro posto si può scegliere in $\binom{8}{6} = \frac{8\cdot7}{2} = 28$ modi diversi (e determina automaticamente il posto delle due vocali); le sei consonanti (il cui ordine è determinato dalle condizioni del problema) possono essere scelte in $\binom{16}{6} = \frac{16\cdot15\cdot14\cdot13\cdot12\cdot11}{6\cdot5\cdot4\cdot3\cdot2} = 4\cdot14\cdot13\cdot11 = 8\,008$ modi diversi; le due vocali (il cui ordine è anch'esso determinato dalle condizioni del problema) possono essere scelte in $\binom{5+2-1}{2} = \frac{6\cdot5}{2} = 3\cdot5 = 15$ modi diversi. Applicando il principio di moltiplicazione, si trova che le password che rientrano nel secondo caso sono

$$28\cdot8\,008\cdot15 = 3\,363\,360\,.$$

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

$$8\,561\,280 + 3\,363\,360 = 11\,924\,640\,.$$