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

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

31.1.2020

FILA "E"

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

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 $(p \rightarrow q) \wedge (\neg r \rightarrow p)$, e quindi la (i) è vera.

(ii) Poiché la formula $r \vee \neg r$ 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:

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

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 $\neg k$: $\{x, \neg z\},\ \{y, z\},\ \{x, \neg y\}$;

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

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

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

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

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

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

dunque

$$\sigma = (1\ 3\ 7)(4\ 9)(6\ 8) = (1\ 3)(1\ 7)(4\ 9)(6\ 8)\,.$$

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

Esercizio 4

Sia $\mathbb{Z}_{329}$ l'anello delle classi di resto modulo 329. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{329}$ a cui z appartiene.
Per ciascuno dei seguenti elementi di $\mathbb{Z}_{329}$ si stabilisca, motivando la risposta, se è invertibile in $\mathbb{Z}_{329}$ e, se è invertibile, se ne trovi l'inverso:

$$[94]\,; \qquad\qquad [100]\,.$$

Soluzione – Sappiamo che l'elemento $[a]$ è invertibile in $\mathbb{Z}_{329}$ se e soltanto se

$$\mathrm{MCD}(329, a) = 1\,.$$

Poiché

$$329 = 94 \cdot 3 + 47\,; \qquad 94 = 47 \cdot 2 + 0\,;$$

$$329 = 100 \cdot 3 + 29\,; \qquad 100 = 29 \cdot 3 + 13\,; \quad 29 = 13 \cdot 2 + 3\,;$$

$$13 = 3 \cdot 4 + 1\,; \qquad 3 = 1 \cdot 3 + 0$$

si ha che

$$\mathrm{MCD}(329, 94) = 47 \neq 1, \qquad \mathrm{MCD}(329, 100) = 1$$

e pertanto fra i due elementi di $\mathbb{Z}_{329}$ proposti dall'esercizio l'unico invertibile è $[100]$.

Per trovare l'inverso di $[100]$ in $\mathbb{Z}_{329}$ dobbiamo risolvere l'equazione

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

in $\mathbb{Z}_{329}$, che ci riconduce all'equazione diofantina

$$100\,x - 329\,y = 1$$

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 $\mathrm{MCD}(329, 100)$. Si ha dunque

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 = 13 - (29 - 13 \cdot 2) \cdot 4 = 13 \cdot 9 + 29 \cdot (-4) = \\ &= (100 - 29 \cdot 3) \cdot 9 + 29 \cdot (-4) = 100 \cdot 9 + 29 \cdot (-31) = \\ &= 100 \cdot 9 + (329 - 100 \cdot 3) \cdot (-31) = 329 \cdot (-31) + 100 \cdot 102 \end{aligned}$$

cosicché l'inverso di $[100]$ in $\mathbb{Z}_{329}$ è $[102]$.

Esercizio 5

Sia $\mathbb{Z}_{12\,901}$ l'anello delle classi di resto modulo $12\,901$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{12\,901}$ a cui z appartiene.

Per ciascuna delle seguenti equazioni nell'incognita x si dica quante soluzioni ha in $\mathbb{Z}_{12\,901}$:

$$[291] \cdot x = [489]\,; \qquad\qquad [399] \cdot x = [931]\,.$$

Soluzione – Consideriamo in primo luogo l'equazione

$$[291] \cdot x = [489]\,.$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{12\,901}$ se e soltanto se il massimo comun divisore δ fra $12\,901$ e 291 divide 489; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra $12\,901$ e 291:

$$12\,901 = 291 \cdot 44 + 97\,;$$
$$291 = 97 \cdot 3 + 0\,.$$

Il massimo comun divisore fra $12\,901$ e 291 è dunque 97; poiché non si tratta di un divisore di 489 (infatti $489 = 97 \cdot 5 + 4$), l'equazione considerata non ha soluzione (quindi il numero delle soluzioni è zero).

Consideriamo poi l'equazione

$$[399] \cdot x = [931]\,.$$

Sappiamo dalla teoria che essa ha soluzione in $\mathbb{Z}_{12\,901}$ se e soltanto se il massimo comun divisore δ fra $12\,901$ e 399 divide 931; e in tal caso essa ha esattamente δ soluzioni.

Calcoliamo con l'algoritmo di Euclide il MCD fra $12\,901$ e 399:

$$12\,901 = 399 \cdot 32 + 133\,;$$
$$399 = 133 \cdot 3 + 0\,.$$

Il massimo comun divisore fra $12\,901$ e 399 è dunque 133; poiché si tratta di un divisore di 931 ($= 133 \cdot 7$), l'equazione considerata ha 133 soluzioni.

Esercizio 6

Con riferimento all'anello $\mathbb{Z}_{23\,125}$ delle classi di resto modulo $23\,125$, si dica, esprimendo ogni risposta in base *tredici*:

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

Soluzione – Un elemento $[a]$ di $\mathbb{Z}_{23\,125}$ è invertibile se e soltanto se

$$\mathrm{MCD}(a,\, 23\,125) = 1$$

e quindi il numero degli elementi invertibili di $\mathbb{Z}_{23\,125}$ è

$$\varphi(23\,125) = \varphi(5^4 \cdot 37) = \varphi(5^4) \cdot \varphi(37) = 5^3 \cdot (5-1) \cdot (37-1) = 18\,000\,.$$

Scriviamo questo numero in base *tredici*, eseguendo successive divisioni per 13:

$$18\,000 = 13 \cdot 1\,384 + 8\,;$$
$$1\,384 = 13 \cdot 106 + 6\,;$$
$$106 = 13 \cdot 8 + 2\,;$$
$$8 = 13 \cdot 0 + 8\,.$$

Pertanto, *diciottomila* in base *tredici* si scrive 8268.

I divisori dello zero di $\mathbb{Z}_{23\,125}$ sono quegli elementi che sono diversi da zero e non sono invertibili; dunque il loro numero è $23\,125 - 1 - 18\,000 = 5124$.

Scriviamo questo numero in base *tredici*, eseguendo successive divisioni per 13:

$5\,124 = 13 \cdot 394 + 2$;
$394 = 13 \cdot 30 + 4$;
$30 = 13 \cdot 2 + 4$;
$2 = 13 \cdot 0 + 2$.

Pertanto, *cinquemilacentoventiquattro* in base *tredici* si scrive 2442.

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 è un numero dispari multiplo di 18 allora $n^2 - 1$ è multiplo di 11;

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

Soluzione –

(i) Ogni multiplo di 18 è pari, e quindi non è dispari; dunque la condizione "n è un numero dispari multiplo di 18" è certamente falsa, qualunque sia $n \in \mathbb{N}$. Pertanto l'implicazione considerata è certamente vera, qualunque sia $n \in \mathbb{N}$.

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

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 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 $\binom{8}{4} = \frac{8\cdot7\cdot6\cdot5}{4\cdot3\cdot2} = 70$ 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 primo caso sono

$$70\cdot1\,820\cdot70 = 8\,918\,000\,.$$

Consideriamo poi 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 secondo caso sono

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

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

$$8\,918\,000 + 8\,561\,280 = 17\,479\,280\,.$$