**ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ**
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
**ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ**
Διδάσκοντες: Δ.Φωτάκης, Θ. Σούλιου
**1η Γραπτή Εργασία, Ημ/νια υποβολής 12/4/2020**

**Θέμα 1 (Προτασιακή Λογική, 2.4 μον.)**

(α) Επισκέπτεσθε ένα νησί όπου κατοικούν δύο είδη ανθρώπων, οι ιππότες που λένε πάντα την αλήθεια, και οι απατεώνες που λένε πάντα ψέματα. (i) Πρώτα συναντάτε δύο κατοίκους του νησιού, τον Α και τον Β. Ο Α λέει ότι "Είμαστε και οι δύο ιππότες". Ο Β λέει ότι "Ο Α είναι απατεώνας". Τι είναι οι Α και Β; (ii) Δύο άλλοι κάτοικοι ο C και ο D σας πλησιάζουν, αλλά μιλάει μόνο ο C και λέει ότι: "Είμαστε και οι δύο απατεώνες". Τι είναι οι C και D; (iii) Στη συνέχεια συναντάτε τους κατοίκους του νησιού Ε και F. Ο Ε λέει ότι "Ο F είναι απατεώνας", και ο F λέει ότι "Ο Ε είναι απατεώνας". Πόσοι από τους Ε και F είναι απατεώνες;

(i) Ο Α δεν μπορεί να λέει αλήθεια γιατί τότε ο Β θα έλεγε αλήθεια και ο Α θα ήταν απατεώνας. Επομένως ο Α είναι απατεώνας. Κατά συνέπεια ο Β είναι ευγενής.
(ii) Η πρόταση είναι ψευδής. Άρα D ιππότης και C απατεώνας
(iii) Ένας από τους δύο θα είναι ιππότης και ένας απατεώνας

(β) Έστω $\varphi$ προτασιακός τύπος. Ορίζουμε την ακολουθία προτασιακών τύπων $\sigma_0, \sigma_1, ..., \sigma_n, ...$ ως εξής: $\sigma_0 \equiv \varphi \to \varphi$, και για κάθε $n \geq 0$, $\sigma_{n+1} \equiv \sigma_n \to \varphi$. Για ποιές τιμές του $n$ ο $\sigma_n$ είναι ικανοποιήσιμος και για ποιές είναι ταυτολογία; Για ποιές τιμές του n αληθεύει ο $\sigma_n \models \sigma_{n+1}$;

$\sigma_n$ ταυτολογία όταν $n$ άρτιος και ικανοποιήσιμος όταν $n$ περιττός

(γ) Η n-οστή πρόταση σε μία λίστα με 100 μαθηματικές προτάσεις δηλώνει ότι "Οι n από τις προτάσεις στη λίστα είναι ψευδείς". (i) Ποιές από τις 100 προτάσεις είναι αληθείς και ποιές ψευδείς; (ii) Ποιές από τις 100 προτάσεις είναι αληθείς και ποιές ψευδείς αν η n-οστή πρόταση δηλώνει ότι "Τουλάχιστον n από τις προτάσεις στη λίστα είναι ψευδείς;" (iii) Τι συμβαίνει αν έχουμε 99 δηλώσεις όπως αυτές στο (ii);

(i) Εφόσον κάθε πρόταση δίνει διαφορετικό πλήθος ψευδών προτάσεων μόνο μία μπορεί να είναι αληθής και 99 ψευδείς. Επομένως η πρόταση 99 είναι αληθής.
(ii) Αν μία πρόταση είναι αληθής τότε όλες οι προηγούμενες πρέπει είναι αληθείς. Άρα οι πρώτες $x$ προτάσεις θα είναι αληθείς και $100 - x$ ψευδείς. Αλλά η $x$ πρόταση λέει πως $100 - x$ προτάσεις είναι ψευδείς. Επομένως $x = 100 - x$. Άρα $x = 50$ προτάσεις αληθείς και 50 ψευδείς.
(iii) Εδώ έχουμε αντίστοιχα $x = 99 - x$ που δεν μπορεί να ισχύει, δεδομένου ότι $1 \leq x \leq 99$ και $x$ ακέραιος.

(δ) Έστω Τ ένα άπειρο σύνολο προτασιακών τύπων, και έστω $\varphi$ αυθαίρετα επιλεγμένος προτασιακός τύπος. Να δείξετε ότι:

1. Αν $T \models \varphi$, τότε υπάρχει πεπερασμένο $T_0 \subseteq T$ τέτοιο ώστε $T_0 \models \varphi$.

Από το θεώρημα της Πληρότητας αν $T \models \varphi \rightarrow T \mid -\varphi$. Η τυπική απόδειξη του $\varphi$ προκύπτει από πεπερασμένα βήματα συνακτικών αντικαταστάσεων και κανόνων παραγωγής, και συνεπώς χρησιμοποιεί ένα πεπερασμένο σύνολο υποθέσεων $T_0$. Έχουμε λοιπόν ότι υπάρχει πεπερασμένο $T_0 \subseteq T$ τέτοιο ώστε $T_0 \vdash \varphi$. Εφαρμόζοντας το Θεώρημα Εγκυρότητας, έχουμε ότι υπάρχει πεπερασμένο $T_0 \subseteq T$ τέτοιο ώστε $T_0 \models \varphi$. Επομένως ένα πεπερασμένο υποσύνολο του $T$ συνεπάγεται ταυτολογικά τον $\varphi$.

2. Αν το $T$ είναι μη ικανοποιήσιμο, τότε υπάρχει πεπερασμένο $T_0 \subseteq T$ που δεν είναι ικανοποιήσιμο.

Εφόσον $T$ μη κανοποιήσιμο, ισχύει $T \models \varphi$ για κάθε προτασιακό τύπο $\varphi$. Σύμφωνα με το προηγούμενο ερώτημα υπάρχει πεπερασμένο υποσύνολο του $T$ έστω $T_0$ που συνεπάγεται ταυτολογικά τον $\varphi$. Αυτό σημαίνει ότι για κάθε προτασιακό τύπο $\varphi$, υπάρχει πεπερασμένο υποσύνολο τύπων $T_0$ τέτοιο ώστε $T_0 \cup \{\neg\varphi\}$ μη ικανοποιήσιμο.. Στην περίπτωση που το $\varphi$ είναι αντίφαση, το $\neg\varphi$ είναι ταυτολογία και κατά συνέπεια το αντίστοιχο πεπερασμένο υποσύνολο $T_0$ είναι μη ικανοποιήσιμο. Σε κάθε περίπτωση μπορούμε να βρούμε πεπερασμένο υποσύνολο τύπων $T_0$ που δεν είναι ικανοποιήσιμο.

**Θέμα 2 (Κατηγορηματική Λογική, 2.0 μον.)**

Έστω ένα σύμπαν που περιλαμβάνει επιστήμονες που είναι μαθηματικοί ή πληροφορικοί (ή και τα δύο) και λειτουργικά συστήματα. Θεωρούμε τα ακόλουθα κατηγορήματα: $CS(x)$ που δηλώνει ότι "ο $x$ είναι πληροφορικός", $M(x)$ που δηλώνει ότι "ο $x$ είναι μαθηματικός", $OS(x)$ που δηλώνει ότι "το $x$ είναι λειτουργικό σύστημα", $L(x,y)$ που δηλώνει ότι "ο $x$ συμπαθεί τον $y$", και $U(x,y)$ που δηλώνει ότι "ο $x$ χρησιμοποιεί το $y$". Σε αυτή την ερμηνεία, να διατυπώσετε τις παρακάτω προτάσεις:

1. Κάθε πληροφορικός συμπαθεί δύο μαθηματικούς.

$$\forall x\left(CS(x) \rightarrow \exists y \exists z\left(\begin{array}{l} M(y) \wedge M(z) \wedge L(x,y) \wedge L(x,z) \wedge y \neq z \wedge \\ \forall w(M(w) \wedge L(x,w) \rightarrow ((w=y) \vee (w=z))) \end{array}\right)\right)$$

2. Υπάρχει λειτουργικό σύστημα που το χρησιμοποιούν όλοι οι πληροφορικοί και κανένας μαθηματικός.

$$\exists x[OS(x) \wedge \forall y(CS(y) \rightarrow U(y,x)) \wedge \forall z(M(z) \rightarrow \neg U(z,x))]$$

3. Υπάρχουν μόνο δύο λειτουργικά συστήματα στο σύμπαν μας και κάθε πληροφορικός χρησιμοποιεί τουλάχιστον ένα από αυτά.

$$\exists x \exists y[OS(x) \wedge OS(y) \wedge x \neq y \wedge \forall w(OS(w) \rightarrow w=x \vee w=y) \wedge \forall z(CS(z) \rightarrow U(z,x) \vee U(z,y))]$$

4. Υπάρχει ένα ζευγάρι λειτουργικών συστημάτων που χρησιμοποιούνται από το ίδιο ακριβώς σύνολο μαθηματικών.

$$\exists x \exists y[OS(x) \wedge OS(y) \wedge x \neq y \wedge \forall z(M(z) \rightarrow (U(z,x) \leftrightarrow U(z,y)))]$$

5. Αν ένας μαθηματικός χρησιμοποιεί περισσότερα του ενός λειτουργικά συστήματα, τότε τουλάχιστον το ένα από αυτά το χρησιμοποιούν όσοι άλλοι μαθηματικοί τον συμπαθούν και όλοι οι πληροφορικοί.

$$\forall x\forall y\forall z\begin{Bmatrix}[M(x)\wedge OS(y)\wedge OS(z)\wedge y\neq z\wedge U(x,y)\wedge U(x,z)]\rightarrow\\ \forall w[(M(w)\wedge L(w,x))\rightarrow(U(w,y)\vee U(w,z))]\wedge\\ \forall u[CS(u)\rightarrow(U(u,y)\vee U(u,z))]\end{Bmatrix}$$

(β) Έστω πρωτοβάθμια γλώσσα με $n\geq 3$ μονομελή κατηγορηματικά σύμβολα $Q_1,...,Q_n$. Να διερευνήσετε την εγκυρότητα της παρακάτω λογικής συνεπαγωγής:

$$\{\forall xQ_1(x),\forall xQ_1(x)\rightarrow\forall xQ_2(x),...,\forall xQ_{n-1}(x)\rightarrow\forall xQ_n(x)\}\models\forall x(Q_1(x)\leftrightarrow Q_n(x))$$

Αρκεί να εστιάσουμε στην περίπτωση που η υπόθεση είναι αληθής. Συνεπώς, δεχόμαστε ότι οι τύποι $\forall xQ_1(x),\forall xQ_2(x),\ \ldots\ ,\forall xQ_n(x)$ αληθεύουν και θέλουμε να αποδείξουμε πως αληθεύει η ισοδυναμία $\forall x(Q_1(x)\leftrightarrow Q_n(x))$, η οποία λέει πως κάθε στοιχείο του σύμπαντος που έχει την ιδιότητα $Q_1$ αν και μόνο αν έχει την ιδιότητα $Q_n$. Δεδομένου πως όλα τα στοιχεία του σύμπαντος έχουν τις ιδιότητες $Q_1$, $Q_2$, … και $Q_n$ τόσο η $Q_1$ όσο και η $Q_n$ αληθεύουν για όλα τα στοιχεία του σύμπαντος και επομένως η πρόταση αληθεύει.

**Θέμα 3 (Κατηγορηματική Λογική, 2.0 μον.)**

(α) Έστω πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο $P$. Θεωρούμε τις προτάσεις:

$$\varphi=\forall xP(x,x)\wedge\forall x\forall y(P(x,y)\rightarrow\forall z(P(x,z)\vee P(z,y)))\rightarrow\forall x\forall y(P(x,y)\vee P(y,x))$$
$$\psi=\forall xP(x,x)\wedge\forall x\forall y(P(x,y)\rightarrow\forall z(P(x,z)\vee P(z,y)))\rightarrow\exists x\forall yP(x,y)$$

1. Να διερευνήσετε τη λογική εγκυρότητα της $\varphi$.

Δεδομένου ότι κάθε στοιχείο του σύμπαντος σχετίζεται με τον εαυτό του (υπάρχει βελάκι που από το $x$ "δείχνει" στο $x$) ο δεύτερος όρος του λογικού συνδέσμου "$\wedge$" για $y=x$ λέει πως για κάθε στοιχείο $x$, κάθε στοιχείο του σύμπαντος σχετίζεται με το $x$ προς τη μία ή την άλλη κατεύθυνση. Σε αυτή την περίπτωση κάθε ζευγάρι στοιχείων του σύμπαντος σχετίζονται προς τη μία ή την άλλη κατεύθυνση. Επομένως είναι λογικά έγκυρη.

2. Χρησιμοποιώντας μαθηματική επαγωγή στον πληθάριθμο του σύμπαντος, να δείξετε ότι κάθε ερμηνεία σε πεπερασμένο σύμπαν αποτελεί μοντέλο της $\psi$.

Η πρόταση λέει πως ΑΝ κάθε στοιχείο του σύμπαντος έχει την ανακλαστική ιδιότητα και ΑΝ για κάθε ζεύγος στοιχείων $(a,b)$ που σχετίζονται ισχύει πως για κάθε στοιχείο του σύμπαντος υπάρχει συσχέτιση του $a$ με αυτό ή αυτού με το $b$ τότε υπάρχει στοιχείο που σχετίζεται με όλα τα στοιχεία του σύμπαντος (ελάχιστο).

Για σύμπαν με ένα στοιχείο ισχύει. Έστω πως ισχύει για σύμπαν με $k$ στοιχεία και έστω $a$ το ελάχιστο στοιχείο. Συμβολίζουμε με $x_i$ τα στοιχεία με τα οποία συσχετίζεται το $a$. Θα αποδείξουμε πως ισχύει για σύμπαν με $k+1$ στοιχεία. Αν το $a$ σχετίζεται με το τελευταίο στοιχείο που προσθέσαμε έστω $b$ τότε το $a$ εξακολουθεί να παίζει το ρόλο του ελάχιστου στοιχείου. Αν όχι τότε η συχέτιση θα υπάρχει προς την αντίθετη κατεύθυνση δηλ το $b$ σχετίζεται με το $a$. Σε αυτή την περίπτωση ισχύει $P(a,x_i)\to P(a,b)\vee P(b,x_i)$ και επειδή $P(a,b)$ δεν είναι αληθής θα είναι η $P(b,x_i)$ για όλα τα $x_i$. Επομένως το $b$ θα παίξει το ρόλο του ελάχιστου στοιχείου.

3. Να διατυπώσετε ερμηνεία που δεν αποτελεί μοντέλο της $\psi$.

Σύμπαν οι φυσικοί αριθμοί και κατηγορηματικό σύμβολο $P(x,y)=x\le y$

(β) Θεωρούμε μια πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο $P$. Να διερευνήσετε τη λογική εγκυρότητα της παρακάτω πρότασης:

$$\xi=\begin{pmatrix}\forall x\neg P(x,x)\wedge\exists x\forall y\neg P(x,y)\wedge\\ \forall x\forall y\forall z(P(x,y)\wedge P(x,z)\to y=z)\wedge\\ \forall x\forall y\forall z(P(y,x)\wedge P(z,x)\to y=z)\end{pmatrix}\to\exists x\forall y\neg P(x,y)$$

Η πρόταση λέει πως ΑΝ κανένα στοιχείο δεν σχετίζεται με τον εαυτό του και ΑΝ υπάρχει minimal και ΑΝ κάθε στοιχείο σχετίζεται με ένα στοιχείο το πολύ και το πολύ ένα στοιχείο σχετίζεται με αυτό τότε υπάρχει maximal. Είναι προφανές πως σε πεπερασμένο σύμπαν αυτό ισχύει (ουσιαστικά έχω πεπερασμένες αλυσίδες που δεν έχουν κοινά στοιχεία). Σε άπειρο σύμπαν όπως αυτό των φυσικών αριθμών και με ερμηνεία του κατηγορηματικού συμβόλου $P(a,b)=a<b$ δεν υπάρχει maximal. Επομένως η $\xi$ δεν είναι λογικά έγκυρη.

**Θέμα 4 (Διαδικασίες Απαρίθμησης 2.4 μον.)**

(α) Έστω $A=\{a_1,...,a_n\}$ ένα πεπερασμένο σύνολο $n$ στοιχείων. Συμβολίζουμε με $A^k$, $k\in N^*$, το σύνολο όλων των ακολουθιών από στοιχεία του $A$ με μήκος $k$ (π.χ. για $n=2$, $A^2=\{a_1a_1,a_1a_2,a_2a_1,a_2a_2\}$ και
$A^3=\{a_1a_1a_1,a_1a_1a_2,a_1a_2a_1,a_1a_2a_2,a_2a_1a_1,a_2a_1a_2,a_2a_2a_1,a_2a_2a_2\}$).
Συμβολίζουμε με $A^*$ το σύνολο όλων των ακολουθιών από τα στοιχεία του $A$ με πεπερασμένο μήκος (δηλαδή έχουμε ότι $A^*=\bigcup_{k\in N^*}A^k$). Να εξετάσετε αν το σύνολο $A^*$ είναι αριθμήσιμο.

Ας υποθέσουμε πως $n=l$ όπου $l$ πεπερασμένος φυσικός αριθμός.
$A=\{a_1,a_2,...a_l\}$. Σχηματίζουμε τα $A^k$
$A^1=\{a_1,a_2,...,a_l\}$ το πλήθος των στοιχείων του είναι $|A^1|=l$
$A^2=\{a_1a_1,a_1a_2,...,a_la_l\}$ το πλήθος των στοιχείων του είναι $|A^2|=l*l=l^2$
$A^3=\{a_1a_1a_1,a_1a_1a_2,...,a_la_la_l\}$ το πλήθος των στοιχείων του είναι $|A^3|=l*l*l=l^3$
...

$A^k = \left\{ \overbrace{a_1 a_1 \ldots a_1}^{k}, \ldots, \overbrace{a_l a_l \ldots a_l}^{k} \right\}$ το πλήθος των στοιχείων του είναι $\left|A^k\right| = l^k$

Εφόσσον το $k$ είναι πεπερασμένο γνωρίζουμε σε ποιό βήμα θα μετρηθεί κάθε συμβολοσειρά.
Αριθμήσιμα άπειρη ένωση πεπερασμένων στοιχείων.

(β) Στη Θεωρητική Πληροφορική, ένα (υπολογιστικό) *πρόβλημα απόφασης* ουσιαστικά χαρακτηρίζεται από ένα ερώτημα στο οποίο η απάντηση είναι είτε "ναί" είτε "όχι" (π.χ. " έχει το γράφημα G κύκλο Hamilton; ", "είναι ο φυσικός αριθμός $n$ άρτιος; ", "είναι ο φυσικός αριθμός $n$ πρώτος; ", κ.λπ.). Έτσι, κάθε πρόβλημα απόφασης στους φυσικούς αριθμούς μπορεί να αναπαρασταθεί από το υποσύνολο των φυσικών για τους οποίους η απάντηση στο αντίστοιχο ερώτημα είναι "ναί". Π.χ. το πρόβλημα της αναγνώρισης των άρτιων αριθμών μπορεί να αναπαρασταθεί από το σύνολο $\{0,2,4,6,...\}$, το πρόβλημα της αναγνώρισης των πρώτων αριθμών μπορεί να αναπαρασταθεί από το σύνολο $\{2,3,5,7,11,...\}$, κ.λπ. Η λύση σε ένα τέτοιο πρόβλημα είναι ένα πρόγραμμα σε μία γλώσσα προγραμματισμού, για παράδειγμα στην C, το οποίο λαμβάνει ως είσοδο έναν φυσικό αριθμό $n$, και έπειτα από πεπερασμένο αριθμό βημάτων, τυπώνει στην έξοδο τη σωστή απάντηση στην αντίστοιχη ερώτηση. Να δείξετε ότι υπάρχουν άπειρα προβλήματα απόφασης στους φυσικούς για τα οποία δεν υπάρχει λύση.

Το σύνολο όλων των προβλημάτων αντιστοιχεί στο δυναμοσύνολο του N (κάθε υποσύνολο και πρόβλημα) το οποίο είναι μη αριθμήσιμο.

Αυτό μπορούμε να το αποδείξουμε και απευθείας, με διαγωνοποίηση. Βάζουμε στις στήλες όλους τους φυσικούς (αντιστοιχούν στα προγράμματα, που είναι γνωστό ότι είναι αριθμήσιμα) και στις γραμμές όλα τα προβλήματα (υποσύνολα του N), και παίρνουμε τον παρακάτω πίνακα:

| Προβλήματα\ $N$ | 1 | 2 | 3 | 4 | 5 | ... |
|---|---|---|---|---|---|---|
| Πρόβλημα 1 | 0 | 1 | 1 | 1 | 1 | |
| Πρόβλημα 2 | 1 | 1 | 0 | 0 | 0 | |
| Πρόβλημα 3 | 0 | 0 | 0 | 1 | 1 | |
| Πρόβλημα 4 | 1 | 1 | 1 | 0 | 1 | |
| ... | | | | | | |

Πάντα θα υπάρχει κάποιο πρόβλημα που θα έχει διαφορετικές τιμές στη διαγώνιο, και άρα δεν αντιστοιχεί σε κάποιο πρόγραμμα.

Αποδείξαμε πως τα προβλήματα απόφασης είναι μη αριθμήσιμα. Από την άλλη, το σύνολο των προγραμμάτων είναι αριθμήσιμο, επειδή είναι υποσύνολο του συνόλου των συμβολοσειρών. Επομένως το σύνολο των προβλημάτων για τα οποία υπάρχει λύση (αντιστοιχούν στα προγράμματα) είναι αριθμήσιμο και το σύνολο των προβλημάτων για το οποίο δεν υπάρχει λύση είναι μη αριθμήσιμα άπειρο. Διότι αν ήταν αριθμήσιμο, τότε η ένωσή των δύο συνόλων, αυτού των προβλημάτων που έχουν λύση και αυτή των προβλημάτων που δεν έχουν λύση, θα έδινε αριθμήσιμο σύνολο, ως ένωση αριθμήσιμων συνόλων.

Το ίδιο επιχείρημα εφαρμόζεται και όταν θέλουμε να αποδείξουμε πως το $R-N$ είναι μη αριθμήσιμο. Αφού το $(R-N)\cup N=R$ είναι μη αριθμήσιμο και το $N$ είναι αριθμήσιμο, άρα $R-N$ είναι μη αριθμήσιμα άπειρο.

(γ) Ο κωδκός πρόσβασης ενός υπερυπολογιστή είναι ένας φυσικός αριθμός που αλλάζει κάθε δευτερόλεπτο, για λόγους ασφαλείας. Η αλλαγή γίνεται με βάση μια πολυωνυμική συνάρτηση $p:N\to N$ βαθμού $d$ και έναν (πολυψήφιο) πρώτο αριθμό $q$. Αν ο κωδικός τη χρονική στιγμή $t$ είναι $x_t$, ο κωδικός την επόμενη χρονική στιγμή είναι $x_{t+1}=p(x_t)\bmod q$. Ο αρχικός κωδικός $x_0$, οι συντελεστές $(a_d,a_{d-1},...,a_0)$ της πολυωνυμικής συνάρτησης $p$, και ο πρώτος αριθμός $q$ είναι γνωστά μόνο στον διαχειριστή του συστήματος. Γνωρίζετε όμως πόσα δευτερόλεπτα έχουν περάσει από το τελευταίο *reset* και έχετε εντοπίσει ένα κρίσιμο κενό ασφαλείας: αν δοκιμάζετε έναν κωδικό κάθε 30 (ή περισσότερα) δευτερόλεπτα, αυτό δεν πρόκειται ποτέ να προκαλέσει συναγερμό ή κλείδωμα του συστήματος (όσες φορές και αν αποτύχετε). Να διατυπώσετε μια αλγοριθμική μέθοδο που παράγει κωδικούς συστηματικά και εγγυάται ότι θα αποκτήσετε πρόσβαση στον υπερυπολογιστή σε πεπερασμένο χρόνο. Να αποδείξετε την ορθότητα της μεθόδου.

Δεχόμαστε ότι ο βαθμός $d$ της πολυωνυμικής συνάρτησης $p$ είναι γνωστός (αν δεν ήταν, θα εργαζόμαστε αντίστοιχα). Κάθε 30 secs "μαντεύω" τα $a_d,a_{d-1},...,a_0,x_0,q$ και υπολογίζω το $x_t$ για τη χρονική στιγμή $t$, την οποία γνωρίζω.

$x_1=p(x_0)\bmod q$

$x_2=p(x_1)\bmod q$

...

$x_t=p(x_{t-1})\bmod q$

Αν δεν βρω το password συνεχίζω "μαντεύοντας" το επόμενο σύνολο $a_d,a_{d-1},...,a_0,x_0,q$.

Τα $a_d,a_{d-1},...,a_0,x_0,q$ παίνουν τιμές από το σύνολο των φυσικών και επομένως αν εφαρμόσω μια σωστή διαδικασία απαρίθμησης για το N × … × N (d+3 φορές), θα απαριθμήσουμε τα σωστά $a_d,a_{d-1},...,a_0,x_0,q$ σε κάποια πεπερασμένη χρονική στιγμή.

**Θέμα 5 (Διμελείς Σχέσεις 1.2 μον.)**

(α) Μία διμελής σχέση $R$ είναι *κυκλική* αν για κάθε τριάδα στοιχείων $x,y,z$, $(x,y)\in R\wedge(y,z)\in R\Rightarrow(z,x)\in R$. Να δείξετε ότι μια σχέση $R$ είναι ανακλαστική και κυκλική αν και μόνο αν η $R$ είναι σχέση ισοδυναμίας.

**κυκλική και ανακλαστική $\Rightarrow$ ισοδυναμίας**

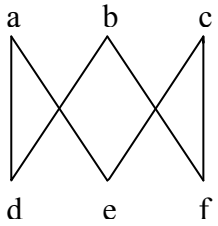
$\forall a(a,a)\in R$, άρα για κάθε ζεύγος $(a,b)\in R\ \Rightarrow(b,a)\in R$ (εφαρμογή της κυκλικής ιδιότητας). Επομένως $R$ συμμετρική.

$\forall a,b,c((a,b)\in R\wedge(b,c)\in R\to(c,a)\in R)$ και επειδή $R$ συμμετρική $(a,c)\in R$. Επομένως $R$ μεταβατική.

**ισοδυναμίας $\Rightarrow$ κυκλική και ανακλαστική**

Επειδή η $R$ είναι μεταβατική για κάθε τριάδα $x,y,z$, λόγω της μεταβατικής ιδιότητας ισχύει πως $(x,y)\in R\wedge(y,z)\in R\Rightarrow(x,z)\in R$. Η $R$ όμως είναι και συμμετρική επομένως $(z,x)\in R$.

(β) Να σχεδιάσετε το διάγραμμα Hasse ενός μερικώς διατεταγμένου συνόλου το οποίο έχει 3 minimal και 3 maximal στοιχεία, και είναι τέτοιο ώστε κάθε στοιχείο είναι είτε μεγαλύτερο είτε μικρότερο από (ακριβώς) δύο άλλα στοιχεία.




(γ) Ορίζουμε μία σχέση $R$ στο σύνολο των θετικών φυσικών ως εξής: Για κάθε $m,n \in N_+, (n,m) \in R$ αν και μόνο αν κάθε πρώτος παράγοντας του $n$ είναι και πρώτος παράγοντας του $m$. Είναι η $R$ σχέση διάταξης; Να αιτιολογήσετε κατάλληλα τον ισχυρισμό σας.

Για να είναι σχέση διάταξης θα πρέπει να ισχύει η αντισυμμετρική ιδιότητα. Το 6 και το 12 έχουν τους ίδιους πρώτους παράγοντες και επομένως $(6,12) \in R$ και $(12,6) \in R$ αλλά το 6 δεν είναι ίσο με το 12.