ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ
Διδάσκοντες: Δ.Φωτάκης, Θ. Σούλιου
1η Γραπτή Εργασία, Ημ/νια παράδοσης 15/4/2018

Θέμα 1 (Διαδικασίες Απαρίθμησης 2.0 μον.)

(α) Μια συνάρτηση $p : N \to N$ είναι πολυωνυμική βαθμού d όταν υπάρχουν φυσικοί $(a_d, a_{d-1}, ..., a_0)$ τέτοιοι ώστε $p(n) = \sum_{l=0}^{d} a_l n^l$, για κάθε $n \in N$. Συμβολίζουμε με P_d το σύνολο των πολυωνυμικών συναρτήσεων βαθμού d στους φυσικούς και με $P = \bigcup_{d \in N} P_d$ το σύνολο των πολυωνυμικών συναρτήσεων. Να εξετάσετε αν τα σύνολα P_d και P είναι αριθμήσιμα.
(β) Χρησιμοποιώντας το (α), να δείξετε ότι υπάρχουν (άπειρες) συναρτήσεις $f : N \to N$ που δεν ανήκουν στο P, δηλ. που δεν μπορούν να εκφραστούν ως πολυωνυμικές συναρτήσεις.
(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 να παράγει κωδικούς συστηματικά και εγγυάται ότι θα αποκτήσετε πρόσβαση στον υπερυπολογιστή σε πεπερασμένο χρόνο. Να αποδείξετε την ορθότητα της μεθόδου.

Θέμα 2 (Προτασιακή Λογική 1.2 μον.)

1. Συμβολίζουμε με $p \mid q$ το "ούτε p ούτε q".
(α) Ορίστε τον αληθοπίνακα του plq ,
Χρησιμοποιώντας ως μόνο λογικό σύνδεσμο τον "|" βρείτε έκφραση για τα:
(i) $\neg p$, (ii) $p \wedge q$, (iii) $p \vee q$ και (iv) $p \to q$

(β) Είναι κάποια από τις εκφράσεις που ακολουθούν αντίφαση ή ταυτολογία; Εξηγήστε την απάντησή σας.
(i) $\{[(p \mid q) \mid (p \mid q)] \wedge (p \mid p)\} \to q$
(ii) $\{(p \mid p) \mid [(p \to q) \mid (p \to q)]\} \wedge \{[(p \mid p) \mid (q \mid q)] \mid [(p \mid p) \mid (q \mid q)]\}$

2. Ο Ηρακλής Πουαρό ανακρίνει 4 υπόπτους για ένα έγκλημα. Από τις ιστορίες των αυτόπτων μαρτύρων ο Ηρακλής έχει καταλήξει στα εξής:

(α) αν ο μπάτλερ λέει αλήθεια, τότε και ο μάγειρας λέει αλήθεια,
(β) ο μάγειρας και ο κηπουρός δεν μπορεί να λένε και οι δύο αλήθεια,
(γ) ο κηπουρός και ο μάστορας δεν μπορεί να λένε και οι δύο ψέματα,
(δ) αν ο μάστορας λέει αλήθεια τότε ο μάγειρας λέει ψέματα,
Μπορεί ο Ηρακλής να καταλάβει ποιος λέει αλήθεια και ποιός ψέματα;

3. Τέσσερις φίλοι είναι ύποπτοι για παράνομο κατέβασμα ταινιών και ο κάθε ένας έχει δώσει μια κατάθεση. Ο Νίκος είπε "Το έκανε ο Βασίλης", ο Αλέξανδρος είπε "Εγώ δεν το έκανα", ο Βασίλης είπε "Η Ευαγγελία το έκανε" και η Ευαγγελία είπε "Ο Βασίλης είπε ψέματα όταν είπε ότι το έκανα εγώ".
(α) Αν ξέρουμε ότι ακριβώς ένας από τους 4 λέει την αλήθεια, τότε ποιός το έκανε;
(β) Αν ξέρουμε ότι ακριβώς ένας λέει ψέματα, τότε ποιός το έκανε;

Θέμα 3 (Κατηγορηματική Λογική 2.5 μονάδες)

Θέλουμε να εκφράσουμε ιδιότητες που μπορεί να έχει ένας πίνακας $A \in N^{20\times 30}$.
Είμαστε στο σύμπαν των θετικών ακεραίων εφοδιασμένο με το διμελές κατηγορηματικό σύμβολο P, δύο συναρτησιακά σύμβολα $f(x,y)$ και $g(x,y)$, και τέσσερις σταθερές c_1, c_2, c_3 και c_4. Ερμηνεύουμε το $P(x,y) \equiv x \le y$, το $f(x,y) = x + y$, το $g(x,y) = A[x,y]$, τις σταθερές $c_1 = 1$, $c_2 = 20$, $c_3 = 30$ και $c_4 = 40$.
α) Σε αυτή την ερμηνεία να διατυπώσετε:
1. Τύπο $\varphi_1(x)$ που να αληθεύει για τις γραμμές του πίνακα που είναι ταξινομημένες σε αύξουσα σειρά.
2. Τύπο $\varphi_2(x,y)$ που να αληθεύει για κάθε θέση του πίνακα που η τιμή της είναι διαφορετική από τις τιμές των θέσεων που βρίσκονται στην ίδια στήλη ή στην ίδια γραμμή με αυτήν.
3. Πρόταση που δηλώνει πως όλα τα στοιχεία του Α είναι μεταξύ 20 και 40.
4. Πρόταση που δηλώνει πως υπάρχει γραμμή με όλα τα στοιχεία ίσα με τη μονάδα.
5. Πρόταση που δηλώνει πως σε κάθε γραμμή του Α υπάρχει στοιχείο που ξεπερνά το 40.
6. Πρόταση που δηλώνει πως κάθε στοιχείο του πίνακα μπορεί να γραφτεί σαν άθροισμα δύο στοιχείων, ένα από την ίδια γραμμή και ένα από την ίδια στήλη.
7. Πρόταση που δηλώνει πως σε κάθε θέση του πίνακα βρίσκεται στοιχείο μικρότερο ή ίσο από όλα τα στοιχεία σε θέσεις μικρότερης ή ίσης γραμμής και στήλης.

β) Αν δεν υπήρχαν οι σταθερές c_2, c_3 και c_4 θα μπορούσαμε να τις εκφράσουμε με τα υπόλοιπα σύμβολα (σταθερές, συναρτησιακά σύμβολα);

Θέμα 4 (Κατηγορηματική Λογική 1.5 μονάδες)

Έστω μία πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Θεωρούμε τις προτάσεις:

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

1. Να διερευνήσετε τη λογική εγκυρότητα της φ.

2. Χρησιμοποιώντας μαθηματική επαγωγή στον πληθάριθμο του σύμπαντος, να δείξετε ότι κάθε ερμηνεία σε πεπερασμένο σύμπαν αποτελεί μοντέλο της ψ.
3. Να διατυπώσετε ερμηνεία που δεν αποτελεί μοντέλο της ψ.

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.
(β) Να σχεδιάσετε διάγραμμα Hasse ενός μερικώς διατεταγμένου συνόλου το οποίο έχει 3 minimal και 3 maximal στοιχεία, και κάθε στοιχείο του 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 μερικής διάταξης; Να αιτιολογήσετε κατάλληλα τον ισχυρισμό σας.
(δ) Θεωρούμε μια πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Να διατυπώσετε μία πρόταση που να δηλώνει ότι (η διμελής σχέση με την οποία ερμηνεύουμε) το P είναι lattice.

Θέμα 6 (Μαθηματική Επαγωγή, 1.6 μον.)

α. Θεωρούμε μία χώρα με $n \geq 2$ πόλεις, όπου για κάθε ζευγάρι διαφορετικών πόλεων (x, y) υπάρχει απευθείας οδική σύνδεση (μονής κατεύθυνσης) είτε από την x στην y είτε από την y στην x. Χρησιμοποιώντας μαθηματική επαγωγή, να δείξετε ότι υπάρχει πόλη στην οποία μπορούμε να φτάσουμε από κάθε άλλη πόλη είτε απευθείας είτε μέσω (ακριβώς) μίας ενδιάμεσης πόλης.

β. Έστω $S = \{a_1, a_{2,}, ..., a_n\}$ ένα σύνολο $n \geq 1$ διαφορετικών δυαδικών συμβολοσειρών μήκους $k \geq 1$. Να δείξετε (με μαθηματική επαγωγή στο μήκος k των συμβολοσειρών) ότι το S περιέχει το πολύ $\frac{n}{2}\log_2 n$ (μη διατεταγμένα) ζευγάρια διαφορετικών συμβολοσειρών που διαφέρουν μεταξύ τους σε ένα δυαδικό ψηφίο. Π.χ. το σύνολο $S = \{00,01,10,11\}$ περιέχει 4 τέτοια ζευγάρια, τα $(00,01), (00,10), (01,11), (10,11)$. Αντίστοιχα, το σύνολο $S = \{000,001,010,100\}$ περιέχει 3 τέτοια ζευγάρια, τα $(000,001), (000,010), (000,100)$.