Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διακριτά Μαθηματικά

Διδάσκοντες: Δ. Φωτάκης, Δ. Σούλιου

1η Γραπτή Εργασία, Ημ/νια Παράδοσης: 28/4/2017

Θέμα 1 (Διαδικασίες Απαρίθμησης, 2.0 μον.). (α) Μια συνάρτηση $p : \mathbb{N} \to \mathbb{N}$ είναι *πολυωνυμική βαθμού* d όταν υπάρχουν φυσικοί $(a_d, a_{d-1}, \ldots, a_0)$ τέτοιοι ώστε $p(n) = \sum_{\ell=0}^{d} a_\ell n^\ell$, για κάθε $n \in \mathbb{N}$. Συμβολίζουμε με $\mathcal{P}_d$ το σύνολο όλων των πολυωνυμικών συναρτήσεων βαθμού d στους φυσικούς και με $\mathcal{P} = \bigcup_{d\in\mathbb{N}} \mathcal{P}_d$ το σύνολο όλων των πολυωνυμικών συναρτήσεων. Να εξετάσετε αν τα σύνολα $\mathcal{P}_d$ και $\mathcal{P}$ είναι αριθμήσιμα.

(β) Χρησιμοποιώντας το (α), να δείξετε ότι υπάρχουν (άπειρες) συναρτήσεις $f : \mathbb{N} \to \mathbb{N}$ που δεν ανήκουν στο $\mathcal{P}$, δηλ. που δεν μπορούν να εκφραστούν ως πολυωνυμικές συναρτήσεις;

(γ) Ο κωδικός πρόσβασης ενός υπερυπολογιστή είναι ένας φυσικός αριθμός που αλλάζει κάθε δευτερόλεπτο, για λόγους ασφαλείας. Η αλλαγή γίνεται με βάση μια πολυωνυμική συνάρτηση $p : \mathbb{N} \to \mathbb{N}$ 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 $(a_d, a_{d-1}, \ldots, a_0)$ 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 ασφάλειας: αν δοκιμάζετε έναν κωδικό κάθε 30 (ή περισσότερα) δευτερόλεπτα, αυτό δεν πρόκειται πότε να προκαλέσει συναγερμό ή κλείδωμα του συστήματος (όσες φορές και αν αποτύχετε). Να διατυπώσετε μία αλγοριθμική μέθοδο που παράγει κωδικούς συστηματικά και εγγυάται ότι θα αποκτήσετε πρόσβαση στον υπερυπολογιστή σε πεπερασμένο χρόνο. Να αποδείξετε την ορθότητα της μεθόδου.

Θέμα 2 (Διμελείς Σχέσεις, 2.0 μον.). (α) Μια 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 το διάγραμμα Hasse ενός μερικώς διατεταγμένου συνόλου το οποίο έχει τρία minimal και τρία maximal στοιχεία, και είναι τέτοιο ώστε κάθε στοιχείο είναι είτε μεγαλύτερο είτε μικρότερο από (ακριβώς) δύο άλλα στοιχεία.

(γ) Ορίζουμε μια σχέση R στο σύνολο των θετικών φυσικών ως εξής: Για κάθε $m, n \in \mathbb{N}_+$, $(n, m) \in R$ 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 μια πρόταση που να δηλώνει ότι (η διμελής σχέση με την οποία ερμηνεύουμε) το P είναι lattice.

Θέμα 3 (Προτασιακή Λογική, 1.2 μον.). (α) Επισκέπτεσθε ένα νησί όπου κατοικούν δύο είδη ανθρώπων: οι ευγενείς, που λένε πάντα την αλήθεια, και οι απατεώνες, που λένε πάντα ψέματα. (i) Πρώτα συναντάτε δύο κατοίκους του νησιού, τον A και τον B. Ο A λέει ότι *"Είμαστε και οι δύο ευγενείς."*. Ο B λέει ότι *"Ο A είναι απατεώνας."*. Τι είναι οι A και B; (ii) Στη συνέχεια συναντάτε τους C και D. Ο C λέει ότι *"Ο D είναι απατεώνας"*, και ο D λέει ότι *"Ο C είναι απατεώνας"*. Πόσοι από τους D και C είναι απατεώνες; (iii) Λίγο παρακάτω συναντάτε τους X και Y. Ρωτάτε τον X: *"Υπάρχει κάποιος ευγενής μεταξύ σας;"*. Αυτός αποκρίνεται, και η απάντησή του είναι τέτοια ώστε να μπορείτε να αποφανθείτε με σιγουριά για τους X και Y. Τι απάντησε ο X, και τι είναι οι X και Y;

(β) Ένας ανακριτής προσπαθεί να ξεχωρίσει έναν κατάσκοπο μεταξύ τριών υπόπτων (ας τους ονομάσουμε Α, Β και Γ). Ο ανακριτής γνωρίζει πως ένας από τους τρεις είναι ευγενής (και λέει πάντα αλήθεια), ένας είναι απατεώνας (και λέει πάντα ψέματα) και ένας είναι κατάσκοπος (μπορεί να λέει είτε αλήθεια είτε ψέματα). Ο Α δήλωσε είτε ότι *"Ο Γ είναι απατεώνας"* είτε ότι *"Ο Γ είναι κατάσκοπος"*. Εμείς δεν γνωρίσουμε τι από τα δύο δήλωσε ο Α, γιατί δεν ακούσαμε καλά, αλλά ο ανακριτής άκουσε και κατέγραψε τη δήλωσή του. Ο Β δήλωσε ότι *"Είτε ο Α είναι κατάσκοπος είτε ο Α είναι απατεώνας είτε ο Α είναι ευγενής"*. Ο Γ δήλωσε ότι *"Είτε ο Β είναι κατάσκοπος είτε ο Β είναι απατεώνας είτε ο Β είναι ευγενής"*. Ο ανακριτής συνέλαβε τον κατάσκοπο. Ποιος ήταν ο κατάσκοπος; Ποια ήταν η δήλωση του Α;

Θέμα 4 (Κατηγορηματική Λογική, 1.6 μον.). Έστω πρωτοβάθμια γλώσσα με κατηγορηματικά σύμβολα τα $C(x)$, $S(x)$, $P(x)$, $T(x,y)$, $E(x,y)$ και $F(x,y)$, τα οποία ερμηνεύουμε ως "το x είναι μάθημα" (για το $C(x)$), "ο x είναι φοιτητής" (για το $S(x)$), "ο x είναι καθηγητής" (για το $P(x)$), "ο καθηγητής x διδάσκει το μάθημα y" (για το $T(x,y)$), "ο φοιτητής x παρακολουθεί το μάθημα y" (για το $E(x,y)$), και "οι x και y είναι φίλοι μεταξύ τους" (για το $F(x,y)$). Σε αυτή την ερμηνεία, να διατυπώσετε ότι:

1. Υπάρχει μάθημα που το παρακολουθούν όλοι οι φοιτητές.
2. Ο καθηγητής x διδάσκει ακριβώς 2 μαθήματα.
3. Όταν δύο φοιτητές είναι φίλοι, τότε παρακολουθούν τουλάχιστον ένα μάθημα μαζί.
4. Όσοι φοιτητές παρακολουθούν το μάθημα "Διακριτά Μαθηματικά" δεν παρακολουθούν το μάθημα "Αριθμητική Ανάλυση".
5. Αν ένας φοιτητής παρακολουθεί όλα τα μαθήματα ενός καθηγητή, τότε αυτοί είναι φίλοι.

Θέμα 5 (Κατηγορηματική Λογική, 2.4 μον.). Έστω πρωτοβάθμια γλώσσα με ένα μονομελές κατηγορηματικό σύμβολο P και ένα διμελές κατηγορηματικό σύμβολο R. Θεωρούμε τις παρακάτω προτάσεις:

$$\psi_1 \equiv [\forall x \forall y \forall z (R(x,y) \land R(y,z) \to R(x,z)) \land \forall x \forall y (R(x,y) \to R(y,x)) \land \forall x \exists y R(x,y)] \to \forall x R(x,x)$$
$$\psi_2 \equiv \exists x [\forall y (P(y) \to R(y,x)) \land \forall y (\forall z (P(z) \to R(z,y)) \to R(x,y))]$$
$$\psi_3 \equiv \forall x \forall y [P(x) \land R(x,y) \land P(y) \land \neg R(y,x) \to \exists z (\neg R(z,x) \land \neg R(y,z)))]$$

1. Να διερευνήσετε αν οι προτάσεις ψ_1, ψ_2 και ψ_3 είναι λογικά έγκυρες.
2. Να δώσετε μια ερμηνεία των κατηγορηματικών συμβόλων P και R στο σύνολο $\mathbb{N}$ των φυσικών αριθμών ώστε να ικανοποιούνται οι προτάσεις ψ_2 και ψ_3.
3. Να διερευνήσετε αν οι προτάσεις ψ_2 και ψ_3 ικανοποιούνται στην ερμηνεία με σύμπαν το δυναμοσύνολο του $\mathbb{N}$, με το $P(x)$ να δηλώνει ότι "*το x είναι πεπερασμένο σύνολο*" και το $R(x,y)$ να δηλώνει ότι "*το x είναι υποσύνολο του y*".

Θέμα 6 (Μαθηματική Επαγωγή, 1.8 μον.). (α) Θεωρούμε n ευθείες που διαιρούν το επίπεδο σε περιοχές. Με μαθηματική επαγωγή στο n, να δείξετε ότι αυτές οι περιοχές μπορούν να χρωματισθούν με δύο χρώματα ώστε αν δύο περιοχές είναι γειτονικές, αυτές να έχουν διαφορετικό χρώμα (δύο περιοχές θεωρούνται γειτονικές αν το "σύνορό" τους είναι ένα ευθύγραμμο τμήμα, όχι μόνο ένα σημείο).

(β) Θεωρούμε μια 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. Να δείξετε, χρησιμοποιώντας μαθηματική επαγωγή, ότι σε κάθε τέτοια χώρα, υπάρχει μια μετάθεση $t_1, \ldots, t_n$ των πόλεων ώστε κάθε πόλη (εκτός της τελευταίας) να συνδέεται απευθείας με την επόμενή της στη μετάθεση, δηλ. για κάθε $i = 1, \ldots, n-1$, να υπάρχει απευθείας οδική σύνδεση από την πόλη t_i στην πόλη t_{i+1}.

Παράδοση. Οι εργασίες θα παραδοθούν στο μάθημα της Παρασκευής 28/4.

Καλή Επιτυχία!