Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διακριτά Μαθηματικά

Διδάσκοντες: Δ. Φωτάκης, Δ. Σούλιου

1η Γραπτή Εργασία, Ημ/νια Παράδοσης: 15/4/2019

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 (Προτασιακή Λογική, 1.6 μον.). (α) Συμβολίζουμε με $p \,|\, q$ το "ούτε p ούτε q".

1. Να αποδείξετε ότι για κάθε προτασιακό τύπο φ, υπάρχει ταυτολογικά ισοδύναμος προτασιακός τύπος φ^* που χρησιμοποιεί μόνο τον λογικό σύνδεσμο "$|$".
2. Είναι κάποια από τις εκφράσεις που ακολουθούν αντίφαση ή ταυτολογία; Εξηγήστε την απάντησή σας.

$$\Big(\big((p \,|\, q) \,|\, (p \,|\, q)\big) \wedge (p \,|\, p) \Big) \to q$$

$$\Big((p \,|\, p) \,|\, \big((p \to q) \,|\, (p \to q)\big) \Big) \wedge \Big(\big((p \,|\, p) \,|\, (q \,|\, q)\big) \,|\, \big((p \,|\, p) \,|\, (q \,|\, q)\big) \Big)$$

(β) Ο Ηρακλής Πουαρό ανακρίνει 4 υπόπτους για ένα έγκλημα. Από τις ιστορίες των αυτοπτών μαρτύρων, ο Ηρακλής έχει καταλήξει στα εξής: (i) αν ο μπάτλερ λέει αλήθεια, τότε και ο μάγειρας λέει αλήθεια, (ii) ο μάγειρας και ο κηπουρός δεν μπορεί να λένε και οι δύο αλήθεια, (iii) ο κηπουρός και ο μάστορας δεν μπορεί να λένε και οι δύο ψέματα, και (iv) αν ο μάστορας λέει αλήθεια, τότε ο μάγειρας λέει ψέματα. Μπορεί ο Ηρακλής να καταλάβει ποιος λέει αλήθεια και ποιος ψέματα;

(γ) Έστω T ένα άπειρο σύνολο προτασιακών τύπων, και έστω φ αυθαίρετα επιλεγμένος προτασιακός τύπος. Να δείξετε ότι:

1. Αν $T \models \varphi$, τότε υπάρχει *πεπερασμένο* $T_0 \subseteq T$ τέτοιο ώστε $T_0 \models \varphi$.
2. Αν το T είναι μη ικανοποιήσιμο, τότε υπάρχει *πεπερασμένο* $T_0 \subseteq T$ που δεν είναι ικανοποιήσιμο.

Θέμα 3 (Κατηγορηματική Λογική, 2.1 μον.). Θέλουμε να εκφράσουμε ιδιότητες που μπορεί να έχει ένας πίνακας $A \in \mathbb{N}^{20 \times 30}$. Θεωρούμε μια πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο $P(x, y)$, δύο διθέσια συναρτησιακά σύμβολα $f(x, y)$ και $g(x, y)$, και τέσσερις σταθερές c_1, c_2, c_3, και c_4. Θεωρούμε ως σύμπαν το σύνολο των θετικών ακεραίων αριθμών, και ερμηνεύουμε το $P(x, y)$ ως "$x \leq y$", το $f(x, y)$ ως "$x + y$", το $g(x, y)$ ως "$A[x, y]$", και τις σταθερές ως $c_1 = 1$, $c_2 = 20$, $c_3 = 30$ και $c_4 = 40$.

(α) Σε αυτή την ερμηνεία να διατυπώσετε:

1. Τύπο $\varphi_1(x)$ που δηλώνει ότι τα στοιχεία της x-οστής γραμμή του πίνακα A είναι ταξινομημένα σε αύξουσα σειρά.

2. Τύπο $\varphi_2(x, y)$ που δηλώνει ότι το στοιχείο στη θέση (x, y) του πίνακα A έχει τιμή διαφορετική από αυτές των στοιχείων που βρίσκονται στην ίδια στήλη ή στην ίδια γραμμή με αυτό.
3. Πρόταση που δηλώνει ότι σε κάθε γραμμή του A υπάρχει στοιχείο που η τιμή του ξεπερνά το 40.
4. Πρόταση που δηλώνει ότι η τιμή κάθε στοιχείου του πίνακα A μπορεί να γραφτεί σαν άθροισμα των τιμών δύο στοιχείων του A, ένα στην ίδια γραμμή και ένα στην ίδια στήλη με το αρχικό.
5. Πρόταση που δηλώνει ότι η τιμή κάθε στοιχείου του πίνακα A είναι μικρότερη ή ίση της τιμής κάθε στοιχείου που βρίσκεται σε μεγαλύτερη στήλη ή σε μεγαλύτερη γραμμή από αυτό.

(β) Αν δεν υπήρχαν οι σταθερές c_2, c_3 και c_4, θα μπορούσαμε να τις εκφράσουμε με κάποιον τρόπο χρησιμοποιώντας τα υπόλοιπα σύμβολα (δηλ. τη σταθερά c_1, το κατηγορηματικό σύμβολο P και τα συναρτησιακά σύμβολα f και g);

Θέμα 4 (Κατηγορηματική Λογική, 2.5 μον.). (α) Έστω πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Θεωρούμε τις προτάσεις:

$$\varphi = \forall x P(x,x) \wedge \forall x \forall y \Big(P(x,y) \rightarrow \forall z \big(P(x,z) \vee P(z,y) \big) \Big) \rightarrow \forall x \forall y \big(P(x,y) \vee P(y,x) \big)$$

$$\psi = \forall x P(x,x) \wedge \forall x \forall y \Big(P(x,y) \rightarrow \forall z \big(P(x,z) \vee P(z,y) \big) \Big) \rightarrow \exists x \forall y P(x,y)$$

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.

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

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

Θέμα 5 (Διμελείς Σχέσεις, 1.5 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 διάταξης; Να αιτιολογήσετε κατάλληλα τον ισχυρισμό σας.

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) Έστω $S = \{a_1, \ldots, a_n\}$ ένα σύνολο $n \geq 1$ διαφορετικών δυαδικών συμβολοσειρών μήκους $\ell \geq 1$. Να δείξετε (με μαθηματική επαγωγή στο ℓ) 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 $\{00, 01\}$, $\{00, 10\}$, $\{01, 11\}$, και $\{10, 11\}$. Αντίστοιχα, το σύνολο $S = \{000, 001, 010, 100\}$, περιέχει 3 τέτοια ζευγάρια, τα $\{000, 001\}$, $\{000, 010\}$, και $\{000, 100\}$.

Παράδοση. Οι εργασίες πρέπει είτε να παραδοθούν στο μάθημα της Δευτέρας 15/4 είτε να αναρτηθούν στο `courses.corelab.ntua.gr` μέχρι τα μεσάνυχτα της ίδιας ημέρας.

Καλή Επιτυχία!