Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διακριτά Μαθηματικά

Διδάσκοντες: Δ. Φωτάκης, Δ. Σούλιου

1η Γραπτή Εργασία, Ημ/νια Παράδοσης: 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 A και τον B. Ο A λέει ότι *"Είμαστε και οι δύο ιππότες."*. Ο B λέει ότι *"Ο A είναι απατεώνας."*. Τι είναι οι A και B; (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 E και F. Ο E λέει ότι *"Ο F είναι απατεώνας"*, και ο F λέει ότι *"Ο E είναι απατεώνας"*. Πόσοι από τους E και F είναι απατεώνες;

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

(γ) Η n-οστή πρόταση σε μία λίστα με 100 μαθηματικές προτάσεις δηλώνει ότι *"Οι n από τις προτάσεις στη λίστα είναι ψευδείς."*. (i) Ποιες από τις 100 προτάσεις είναι αληθείς και ποιες ψευδείς; (ii) Ποιες από τις 100 προτάσεις είναι αληθείς και ποιες 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);

(δ) 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 2 (Κατηγορηματική Λογική, 2.0 μον.). (α) 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.
2. Υπάρχει λειτουργικό σύστημα που το χρησιμοποιούν όλοι οι πληροφορικοί και κανένας μαθηματικός.
3. Υπάρχουν μόνο δύο λειτουργικά συστήματα στο σύμπαν μας και κάθε πληροφορικός χρησιμοποιεί τουλάχιστον ένα από αυτά.
4. Υπάρχει ένα ζευγάρι λειτουργικών συστημάτων που χρησιμοποιούνται από το ίδιο ακριβώς σύνολο μαθηματικών.
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.

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

$$\big\{\forall x Q_1(x), \forall x Q_1(x) \to \forall x Q_2(x), \ldots, \forall x Q_{n-1}(x) \to \forall x Q_n(x)\big\} \models \forall x \big(Q_1(x) \leftrightarrow Q_n(x)\big)$$

Θέμα 3 (Κατηγορηματική Λογική, 2.0 μον.). (α) Έστω πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Θεωρούμε τις προτάσεις:

$$\varphi = \forall x P(x, x) \land \forall x \forall y \Big(P(x, y) \to \forall z \big(P(x, z) \lor P(z, y)\big)\Big) \to \forall x \forall y \big(P(x, y) \lor P(y, x)\big)$$

$$\psi = \forall x P(x, x) \land \forall x \forall y \Big(P(x, y) \to \forall z \big(P(x, z) \lor P(z, y)\big)\Big) \to \exists x \forall y P(x, y)$$

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 4 (Διαδικασίες Απαρίθμησης, 2.4 μον.). (α) Έστω $A = \{a_1, \ldots, a_n\}$ ένα πεπερασμένο σύνολο n στοιχείων. Συμβολίζουμε με A^k, $k \in \mathbb{N}^*$, 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 στοιχεία του A με πεπερασμένο μήκος (δηλ. έχουμε ότι $A^* = \bigcup_{k \in \mathbb{N}^*} A^k$). Να εξετάσετε αν το σύνολο A^* είναι αριθμήσιμο.

(β) Στην Θεωρητική Πληροφορική, ένα (υπολογιστικό) *πρόβλημα απόφασης* ουσιαστικά χαρακτηρίζεται από ένα ερώτημα στο οποίο η απάντηση είναι είτε "ναι" είτε "όχι" (π.χ. "έχει το γράφημα G κύκλο Hamilton;", "είναι ο φυσικός αριθμός n άρτιος;", "είναι ο φυσικός αριθμός n πρώτος;", κλπ.). Έτσι, κάθε πρόβλημα απόφασης στους φυσικούς αριθμούς μπορεί να αναπαρασταθεί από το υποσύνολο των φυσικών για τους οποίους η απάντηση στο αντίστοιχο ερώτημα είναι "ναι". Π.χ. το πρόβλημα της αναγνώρισης των άρτιων αριθμών μπορεί να αναπαρασταθεί από το σύνολο $\{0, 2, 4, 6, \ldots\}$, το πρόβλημα της αναγνώρισης των πρώτων αριθμών μπορεί να αναπαρασταθεί από το σύνολο $\{2, 3, 5, 7, 11, \ldots\}$, κλπ. 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.

(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 $p : \mathbb{N} \rightarrow \mathbb{N}$ 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 5 (Διμελείς Σχέσεις, 1.2 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.

Παράδοση. Οι εργασίες πρέπει να αναρτηθούν στο `courses.corelab.ntua.gr` μέχρι τα μεσάνυχτα της Κυριακής 12 Απριλίου.

Καλή Επιτυχία!