Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διακριτά Μαθηματικά

Διδάσκοντες: Δ. Φωτάκης, Δ. Σούλιου

1η Γραπτή Εργασία, Ημ/νια Παράδοσης: 19/4/2022

Θέμα 1 (Διαδικασίες Απαρίθμησης, 2 μον.). (α) 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 n άρτιος;", "είναι ο φυσικός n πρώτος;", κλπ.).
Ένα πρόβλημα απόφασης Π στο $\mathbb{N}$ 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. Ουσιαστικά, κάθε πρόβλημα απόφασης Π αντιστοιχεί σε λογική συνάρτηση $f_\Pi : \mathbb{N} \to \{0, 1\}$.
Η λύση σε ένα τέτοιο πρόβλημα είναι ένα πρόγραμμα σε μία γλώσσα προγραμματισμού, για παράδειγμα στη C++, το οποίο λαμβάνει ως είσοδο έναν φυσικό n, και έπειτα από πεπερασμένο αριθμό βημάτων, τυπώνει στην έξοδο τη σωστή απάντηση στην αντίστοιχη ερώτηση. Να δείξετε ότι υπάρχουν (μη αριθμήσιμα άπειρα) προβλήματα απόφασης στους φυσικούς για τα οποία δεν υπάρχει λύση.

(β) 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. Ποιος ο λόγος που μπορούμε να εγγυηθούμε την ύπαρξη μιας τέτοιας αλγοριθμικής μεθόδου;

Θέμα 2 (Προτασιακή Λογική, 3.5 μον.). (α) 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);

(β) 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.

(γ) Η αρχή της *ανάλυσης* (resolution) είναι ο συντακτικός αποδεικτικός κανόνας:

$$\frac{p \vee \varphi\,,\ \neg p \vee \psi}{\varphi \vee \psi}\,,$$

όπου p προτασιακή μεταβλητή και φ, ψ διαζεύξεις λεκτικών (literals – λεκτικό είναι μια προτασιακή μεταβλητή q ή η άρνηση μιας προτασιακής μεταβλητής $\neg q$). Προσέξτε ότι οι φ, ψ μπορούν να είναι κενοί τύποι. Για διευκόλυνση, σε αυτό το ερώτημα, θεωρούμε πάντα ότι οι προτασιακοί τύποι έχουν τη μορφή διαζεύξεων λεκτικών.

1. Να δείξετε ότι η αρχή της ανάλυσης αποτελεί γενίκευση του αποδεικτικού κανόνα Modus Ponens.
2. Μια *απόδειξη* $T \vdash_{res} \varphi$ με την αρχή της ανάλυσης είναι μια πεπερασμένη ακολουθία τύπων $(\chi_1, \chi_2, \ldots, \chi_n)$ όπου: (i) για κάθε βήμα i, είτε ο τύπος $\chi_i \in T$, είτε ο χ_i προκύπτει από εφαρμογή της αρχής της ανάλυσης σε προηγούμενους τύπους χ_j, χ_k, και (ii) $\chi_n = \varphi$. Χρησιμοποιώντας μαθηματική επαγωγή στο πλήθος των βημάτων της απόδειξης, να δείξετε ότι για κάθε ικανοποιήσιμο σύνολο τύπων $T = \{\psi_1, \ldots, \psi_k\}$ και κάθε τύπο φ, αν $T \vdash_{res} \varphi$, τότε $T \models \varphi$.
3. Η εφαρμογή του κανόνα της ανάλυσης σε συμπληρωματικά λεκτικά $p, \neg p$ (με φ, ψ κενούς) οδηγεί σε αντίφαση $\perp$ (δηλ. έχουμε ότι $\frac{p,\ \neg p}{\perp}$). Να δείξετε ότι για κάθε σύνολο τύπων $T = \{\psi_1, \ldots, \psi_k\}$, αν $T \vdash_{res} \perp$, τότε το T δεν είναι ικανοποιήσιμο.

Θέμα 3 (Κατηγορηματική Λογική, 2.5 μον.). (α) Θεωρούμε μια πρωτοβάθμια γλώσσα με μονομελή κατηγορηματικά σύμβολα P και M και διμελή κατηγορηματικά σύμβολα T και L. Ερμηνεύουμε αυτή τη γλώσσα στο σύμπαν που αποτελείται από την ένωση του συνόλου των καθηγητών και των μαθημάτων της Σχολής, με το $P(x)$ να δηλώνει ότι *"ο x είναι καθηγητής"*, το $M(x)$ να δηλώνει ότι *"το x είναι μάθημα"*, το $T(x, y)$ να δηλώνει ότι *"ο x διδάσκει το y"*, και το $L(x, y)$ να δηλώνει ότι *"ο x συμπαθεί τον y"*. Σε αυτή την ερμηνεία, να γράψετε τύπους που να δηλώνουν ότι:

1. Το ελάχιστο πλήθος μαθημάτων που διδάσκει κάποιος καθηγητής είναι δύο.
2. Ένας καθηγητής συμπαθεί έναν άλλο μόνον αν υπάρχει μάθημα που το διδάσκουν και οι δύο.
3. Αν δυο καθηγητές διδάσκουν τα ίδια ακριβώς μαθήματα, τότε συμπαθούν τους ίδιους ακριβώς καθηγητές.
4. Αν ένας καθηγητής διδάσκει περισσότερα του ενός μαθήματα, τότε τουλάχιστον ένα από αυτά το συνδιδάσκει με όλους τους άλλους καθηγητές που τον συμπαθούν.

(β) Έστω πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο Q. Να διερευνήσετε την λογική εγκυρότητα της παρακάτω πρότασης:

$$\forall x \forall y \Big(Q(x, y) \leftrightarrow Q(y, x) \Big) \rightarrow \exists x Q(x, x)$$

Θέμα 4 (Κατηγορηματική Λογική, 2.0 μον.). (α) Έστω πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Θεωρούμε την πρόταση:

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

1. Να διατυπώσετε (σε φυσική γλώσσα, απλά και κατανοητά) το νόημα του τύπου φ. Αν βοηθάει να θεωρήσετε συγκεκριμένο πλαίσιο ερμηνείας, σκεφτείτε απλά κατευθυνόμενα γραφήματα, όπου το σύμπαν είναι οι κορυφές του γραφήματος και το $P(x, y)$ δηλώνει την ύπαρξη ακμής από την κορυφή x προς την κορυφή y.
2. Χρησιμοποιώντας μαθηματική επαγωγή στον πληθάριθμο του σύμπαντος, να δείξετε ότι ο φ αληθεύει σε κάθε ερμηνεία με πεπερασμένο σύμπαν.

(β) Έστω πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο Q. Θεωρούμε την πρόταση:

$$\xi = \forall x \Big(Q(x, x) \rightarrow \forall y \big(Q(x, y) \vee Q(y, x) \big) \Big) \rightarrow \forall x \forall y \Big(Q(x, y) \vee Q(y, x) \Big)$$

Να διερευνήσετε σε ποιες από τις παρακάτω ερμηνείες αληθεύει η ξ:

1. Σύμπαν $A = \{a, b, c\}$ και το Q ερμηνεύεται με τη σχέση $Q^A = \{(a, b), (b, c)\}$.
2. Σύμπαν $A = \{a, b, c\}$ και το Q ερμηνεύεται με τη σχέση $Q^A = \{(a, a), (b, b), (c, c)\}$.
3. Σύμπαν $A = \{a, b, c\}$ και το Q ερμηνεύεται με τη σχέση $Q^A = \{(a, a), (c, c), (a, b), (a, c), (b, c)\}$.
4. Οποιαδήποτε ερμηνεία όπου το σύμπαν είναι μονοσύνολο.

Παράδοση. Οι εργασίες πρέπει να αναρτηθούν στο https://helios.ntua.gr/course/view.php?id=893 μέχρι τα μεσάνυχτα της Μ. Τρίτης 19 Απριλίου.

Καλή Επιτυχία!