Εθνικό Μετσόβιο Πολυτεχνείο

Πψρφοροσ2.θπεγ

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

1η Σειρά Γραπτών Ασκήσεων

Μάθημα: Διακριτά Μαθηματικά

Όνομα: Παναγιώτης Κωσταπαναγιώτης

Α.Μ: 03115196

Θέμα 1ο

- (α) Αρχικά, είναι σαφές πως μια πολυωνυμική συνάρτηση βαθμού d χαρακτηρίζεται αμφιμονοσήμαντα από το διάνυσμα των συντελεστών της $C^T = (a_0, a_1, ..., a_d)$. Όμως το σύνολο των διανυσμάτων αυτών, δηλαδή το P_d αποτελεί απλά το καρτεσιανό γινόμενο $\mathbb{N}^d$ που είναι αριθμήσιμο ως γινόμενο πεπερασμένου πλήθους αριθμήσιμων συνόλων. Το γεγονός ότι το καρτεσιανό γινόμενο ενός πεπερασμένου πλήθους από αριθμήσιμα σύνολα είναι αριθμήσιμο σύνολο μπορούμε να το δείξουμε εύκολα με επαγωγή. Επιπλέον το σύνολο $P = \cup_{d \in \mathbb{N}} P_d$ είναι αριθμήσιμο ως ένωση αριθμήσιμων συνόλων.

  (β) Θα δείξουμε ότι το σύνολο F όλων των συναρτήσεων $f : \mathbb{N} \to \mathbb{N}$ είναι μη αριθμήσιμο. Θα εφαρμόσουμε διαγωνιοποίηση. Έστω πως το εν λόγω σύνολο είναι αριθμήσιμο και έστω μια αρίθμηση του $f_1, f_2, ..., f_i, ...$, κατασκευάζουμε την συνάρτηση $D : \mathbb{N} \to \mathbb{N}$ με τύπο $D(i) = f_i(i) + 1$. Όμως, είναι $D \notin F$, άτοπο. Συνεπώς το σύνολο F δεν είναι αριθμήσιμο, ενώ το σύνολο P είναι και άρα υπάρχουν άπειρες συναρτήσεις $f : \mathbb{N} \to \mathbb{N}$ που δεν μπορούν να εκφραστούν ως πολυώνυμα.

  (γ) Οι πληροφορίες που περιγράφουν αμφιμονοσήμαντα την διαδικασία παραγωγής κωδικών είναι η τούπλα (x_0, q, P) όπου x_0 ο κωδικός την χρονική στιγμή 0, q ο εν λόγω πρώτος αριθμός και p το πολυώνυμο που αναπαρίσταται από το διάνυσμα συντελεστών του C^T. Επιπλέον, πρέπει να γνωρίζουμε κάθε στιγμή και πόση ώρα έχει περάσει από την εκκίνηση της διαδικασίας. Αν γνωρίζουμε όλες αυτές τις πληροφορίες, έστω πως έχουν περάσει n δευτερόλεπτα, τότε μπορούμε απλά να παράξουμε τον σωστό κωδικό με επαναλαμβανόμενη εφαρμογή του πολυωνύκου στον εαυτό του. Παράγουμε δηλαδή τον κωδικό $x_n = p(...p(p(x_0))...) mod q$.

  Εάν από την άλλη θέλουμε να πιστοποιήσουμε αν μια αυθαίρετη τούπλα (x_0, q, P) είναι σωστή μπορούμε απλά να παράξουμε τον υποψήφιο κωδικό x_n από την τούπλα μας και να ελέγξουμε αν είναι ίδιος με τον κωδικό του συστήματος. Εάν δεν πάρουμε πρόσβαση τότε η τούπλα είναι σίγουρα λάθος ενώ εαν πάρουμε, με μεγάλη πιθανότητα, η τούπλα μας είναι σωστή, ωστόσο αυτό δεν έχει σημασία εφ' όσον καταφέραμε να πάρουμε πρόσβαση.

  Όπως δείξαμε στο ερώτημα (α), το σύνολο των πολυωνύμων P είναι αριθμήσιμο και το σύνολο των εν λόγω τριάδων είναι το καρτεσιανό γινόμενο

$\mathbb{N} \times PRIMES \times \mathbb{P}$ το οποίο είναι με την σειρά του αριθμήσιμο ως το καρτεσιανό γινόμενο τριών αριθμήσιμων συνόλων. Συνεπώς υπάρχει μια διαδικασία απαρίθμησης που παράγει τις εν λόγω τριάδες. Μπορούμε λοιπόν να δοκιμάσουμε κάθε τριάδα με την σειρά μέχρι να βρούμε μια που να μας δώσει πρόσβαση όπως περιγράψαμε παραπάνω. Αυτό θα γίνει σίγουρα διότι το πολυώνυμο και ο πρώτος q του υπολογιστή δεν αλλάζουν και συνεπώς κάποια στιγμή, σε πεπερασμένο βήμα, μέσω της διαδικασίας απαρίθμησης η τριάδα που δοκιμάζουμε με την τριάδα του υπολογιστή θα ταυτιστούν. Η μόνη λεπτομέρεια που μένει είναι πως θα δοκιμάζουμε τριάδες μόνο σε ακέραια πολλαπλάσια των 30 δευτερολέπτων αφού αλλιώς θα έχουμε πρόβλημα με τον συναγερμό.

Θέμα 2ο

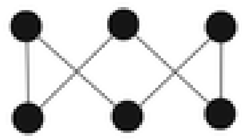
- (α). Ευθύ: Θα δείξουμε ότι αν μια σχέση είναι ανακλαστική και κυκλική, τότε είναι σχέση ισοδυναμίας. Αρκεί να δείξουμε ότι η σχέση είναι ανακλαστική, μεταβατική και αυτοπαθής.

  1. Ανακλαστικότητα: Κατευθείαν από την υπόθεση.
  2. Μεταβατικότητα: Έχουμε, από κυκλικότητα, $\forall x, y, z (x, y) \in R \wedge (y, z) \in R \Rightarrow (z, x) \in R$ Όμως, λόγω ανακλαστικότητας έχουμε $(z, x) \in R \Rightarrow (x, z) \in R$ που είναι και το ζητούμενο.
  3. Αυτοπάθεια: Από ανακλαστικότητα λαμβάνουμε $\forall x, y (x, y) \in R \Rightarrow (y, x) \in R$. Εφαρμόζουμε την ιδιότητα της κυκλικότητας. Είναι $(x, y) \in R \wedge (y, x) \in R \Rightarrow (x, x) \in R$.

  Συνεπώς, η σχέση μας είναι σχέση ισοδυναμίας, που είναι και το ζητούμενο.

  Αντίστροφο: Δεδομένου ότι η σχέση μας είναι σχέση ισοδυναμίας η ανακλαστικότητα προκύπτει τετριμμένα. Αρκεί να δείξουμε ότι είναι και κυκλική. Έχουμε, από μεταβατικότητα, $\forall x, y, z (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$. Με εφαρμογή της ανακλαστικότητας στην παραπάνω σχέση προκύπτει άμεσα το ζητούμενο.

  (β) Το διάγραμμα Hasse απεικονίζεται παρακάτω



(γ) Η σχέση αυτή δεν είναι σχέση μερικής διάταξης διότι δεν είναι αντισυμμετρική. Θεωρούμε τους αριθμούς 2 και 2^{10} είναι προφανώς $2 \neq 2^{10}$ και $(2, 2^{10}) \in R \wedge (2^{10}, 2) \in R$.

(δ) Αρχικά ορίζουμε το γενικευμένο κατηγόρημα P^* που εκφράζει την ύπαρξη μονοπατιών συσχέτισης στο διάγραμα Hasse της σχέσης που εκφράζουμε μέσω του κατηγορήματος P. Είναι δηλαδή $P^*(x,y) = \exists z : P^*(x,z) \wedge P(z,y)$. Χρησιμοποιώντας τον παραπάνω ορισμό θα εκφράσουμε τις δύο συνθήκες που είναι αναγκαίες και ικανές για να είναι η σχέση μας lattice , δηλαδή κάθε ζεύγος στοιχείων να έχει μοναδικό infimum και supremum . Για το infimum έχουμε: $\forall x, y \exists z : P^*(z,x) \wedge P^*(z,y) \wedge [\forall z' : (P^*(z',x) \wedge P^*(z',y)) \rightarrow P^*(z',z)]$. Εντελώς ανάλογα έχουμε για το supremum : $\forall x, y \exists z : P^*(y,z) \wedge P^*(z,y) \wedge [\forall z' : (P^*(y,z') \wedge P^*(x,z')) \rightarrow P^*(z,z')]$. Συνολικά, λαμβάνοντας την τομή των δύο προτάσεων έχουμε την ακόλουθη έκφραση: $\forall x, y \{\exists z : P^*(z,x) \wedge P^*(z,y) \wedge [\forall z' : (P^*(z',x) \wedge P^*(z',y)) \rightarrow P^*(z',z)]\} \wedge \{\exists z : P^*(y,z) \wedge P^*(z,y) \wedge [\forall z' : (P^*(y,z') \wedge P^*(x,z')) \rightarrow P^*(z,z')]\}$.

Θέμα 3ο

- (α) (ι) Αν ο Β είναι απατεώνας, τότε ο Α είναι ευγενής και άρα συνεπώς, λόγω της δήλωσης του Α, ο Β είναι ευγενής, άτοπο. Συνεπώς ο Β είναι ευγενής και ο Α απατεώνας.

  (ιι) Αν και οι 2 είναι απατεώνες προκύπτει πως και οι 2 πρέπει να είναι ευγενείς. Αντίστροφα αν κανένας από τους 2 δεν είναι απατεώνας τότε και οι 2 είναι απατεώνες. Συνεπώς συμπαιρένουμε πως ακριβώς ένας εκ των 2 είναι απατεώνας.
  (ιιι) Ο Χ απαντάει στην ερώτηση πως κανένας από τους δύο δεν είναι

ευγενής. Αν λέει αλήθεια τότε δημιουργείται παράδοξο, συνεπώς ο Χ πρέπει να λέει ψέμματα. Εφ' όσον λέει ψέμματα τότε προκύπτουν τα εξής:

– Ο Χ είναι απατεώνας

– Ένας από τους Χ, Υ είναι ευγενής

Συμπαιρένουμε λοιπόν πως ο Χ πρέπει να είναι απατεώνας, ενώ ο Υ ευγενής.

(β) Αρχικά, γνωρίζουμε πως ο Β και ο Γ λένε αλήθεια αφού δηλώνουν κάτι τετριμμένα αληθές. Συνεπώς κάποιος από τους δύο είναι κατάσκοπος και ο άλλος είναι ευγενής. Οπότε ανεξάρτητα του τι θα δηλώσει ο Α γνωρίζουμε εκ των προτέρων πως είναι απατεώνας. Έστω πως ο Α δήλωσε πως ο Γ είναι απατεώνας, σε αυτή την περίπτωση ο ανακριτής δεν θα μπορούσε να αποφανθεί για το ποιός είναι ο κατάσκοπος. Συνεπώς γνωρίζουμε πως ο Α δήλωσε ότι ο Γ είναι κατάσκοπος. Όμως, ο Α είναι απατεώνας και άρα ο Γ δεν μπορεί να είναι κατάσκοπος. Συμπαιρένουμε λοιπόν πως ο Γ είναι απατεώνας και ο Β είναι κατάσκοπος.

Θέμα 4ο

- 1.$\exists x : C(x) \wedge \forall y : S(y) \rightarrow E(y, x)$
  2.$(\nexists y, z, w : T(x, y) \wedge T(x, z) \wedge T(x, w)) \wedge (\exists y, z : T(x, y) \wedge T(x, z))$
  3.$\forall x \forall y F(x, y) \rightarrow \exists z : C(z) \wedge E(x, z) \wedge E(y, z)$
  4.Συμβολίζουμε με x το μάθημα των διακριτών μαθηματικών και με y το μάθημα της αριθμητικής Ανάλυσης. Έχουμε τότε: $\forall z : S(z) \rightarrow (E(z, x) \rightarrow \neg E(z, y))$
  5.$\forall x, y : P(x) \wedge S(y) \rightarrow [(\forall z T(x, z) \rightarrow E(y, z)) \rightarrow F(x, y)]$

Θέμα 5ο

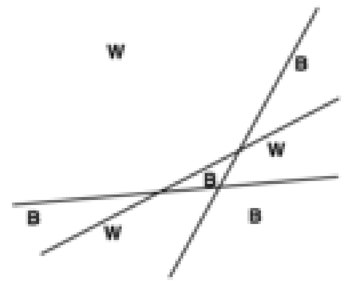
- 1. Η πρόταση $y1$ είναι λογικά έγκυρη διότι περιγράφει πως αν μια σχέση είναι ανακλαστική, μεταβατική και δεν υπάρχει στοιχείο που να μην σχετίζεται με κανένα άλλο τότε είναι και αυτοπαθής. Οι προτάσεις $y2, y3$ από

την άλλη δεν περιγράφουν κάτι που ισχύει εν γένει για κάθε σχέση και η εγκυρότητα τους εξαρτάται από την ερμηνεία των συμβόλων τους.
2. Μπορούμε να δώσουμε την εξής ερμηνεία στα σύμβολα P, R. Ορίζουμε το $P(q)$ ως: ¨Το χ είναι άρτιος' και το $R(q, y)$ ως: ¨Το χ είναι μεγαλύτερο ή ίσο του ψ¨. Σε αυτήν την περίπτωση η πρόταση ψ2 λέει πως υπάρχει ένας άρτιος που είναι μικρότερος από όλους τους υπόλοιπους ενώ η πρόταση ψ3 λέει πως αν δύο άρτιοι αριθμοί είναι άνισοι τότε υπάρχει τουλάχιστον ένας φυσικός αριθμός ανάμεσά τους.
3. Σύμφωνα με την δεδομένη ερμηνεία η πρόταση $y3$ είναι λογικά έγκυρη αφού δηλώνει πως αν δύο πεπερασμένα σύνολα q, y είναι άνισα και το χ είναι υποσύνολο του ψ τότε υπάρχει ένα σύνολο που δεν είναι υπερσύνολο του ψ και δεν είναι υποσύνολο του χ. Ωστόσο η πρόταση 2 δεν είναι έγκυρη αφού δηλώνει πως υπάρχει ένα χ για το οποίο κάθε πεπερασμένο σύνολο ψ είναι υποσύνολό του.

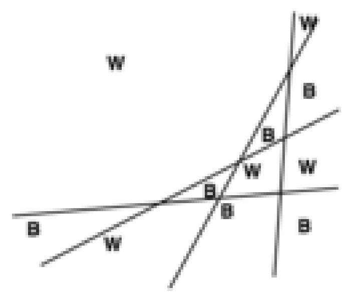
Θέμα 6ο

- (α) Θα δείξουμε το ζητούμενο χρησιμοποιώντας μαθηματική επαγωγή. Αρχικά, η περίπτωση όπου έχουμε μια ευθεία είναι τετριμμένη αφού το επίπεδο χωρίζεται σε δύο ημιεπίπεδα και μπορούμε προφανώς να τα χρωματίσουμε με 2 χρώματα. Έστω πως μπορούμε να χρωματίσουμε κάθε σύνολο k ευθειών με έγκυρο τρόπο χρησιμοποιώντας ακριβώς 2 χρώματα, θα δείξουμε πως μπορούμε να χρωματίσουμε έγκυρα το επίπεδο για κάθε σύνολο ευθειών μεγέθους $k + 1$. Έστω $A = \{e_1, e_2, ..., e_k\}$ κάποιο αυθαίρετο σύνολο ευθειών και έστω e_{k+1} κάποια ευθεία. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε πως η ευθεία e_{k+1} είναι ευθεία μεγαλύτερης κλίσης από όλες τις ευθείες του συνόλου A αφού, αν δεν είναι μπορούμε να την ανταλλάξουμε με την ευθεία μεγαλύτερης κλίσης του συνόλου A. Έστω κάποιος έγκυρος χρωματισμός του A, θα δείξουμε πως μπορούμε από τον εν λόγω χρωματισμό να παράξουμε έναν έγκυρο χρωματισμό για το σύνολο $B = A \cup \{e_{k+1}\}$. Με την εισαγωγή της ευθείας e_{k+1} ορίζονται κάποιες νέες περιοχές που παραβιάζουν την συνθήκη όπως φαίνεται στο σχήμα.

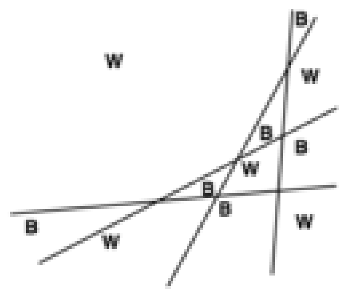
  Αρχικός χρωματισμός ευθειών:



Παραβίαση συνθήκης μετά από εισαγωγή επιπλέον ευθείας:



Προκειμένου να διορθώσουμε την παραβίαση αλλάζουμε το χρώμα των περιοχών στο δεξιά ημιεπιπέδου που ορίζει η ευθεία e_{k+1} στο συμπληρωματικό της παράγοντας έναν έγκυρο χρωματισμό.



Συνεπώς κατασκευάσαμε έναν έγκυρο χρωματισμό για το σύνολο των κ+1 ευθειών και συνεπώς η απόδειξη έχει ολοκληρωθεί.

(β) Θα δείξουμε ότι σε έναν οποιονδήποτε γράφο με την ιδιότητα της εκφώνησης υπάρχει μονοπάτι Ηαμιλτον. Θα χρησιμοποιήσουμε επαγωγή. Για κάθε γράφο με 2 κόμβους θα υπάρχει ακμή που τους συνδέει και συνεπώς έχουμε ένα μονοπάτι $Hamilton$ μεγέθους 1. Έστω πως κάθε γράφος με $k \geqslant 2$ κόμβους έχει μονοπάτι Ηαμιλτον, θα δείξουμε ότι και κάθε γράφος με $k+1$ κόμβους έχει μονοπάτι Ηαμιλτον. Έστω G ο γράφος με κ + 1 κορυφές και έστω ότι αφαιρούμε μια κορυφή από τον γράφο, ας πούμε την u, παράγοντας τον γράφο G'. Ο γράφος G' έχει κ κορυφές και συνεπώς έχει μονοπάτι $Hamilton$, έστω $P = (t_1, ..., t_k)$ όπου $t_i \in V_G$. Διακρίνουμε τις εξής περιπτώσεις, δεδομένου ότι ο γράφος μας έχει την ιδιότητα που περιγράφεται στην εκφώνηση:

- Υπάρχουν κορυφές t_i και t_{i+1} για τις οποίες υπάρχουν οι ακμές (t_i, u) και (u, t_{i+1}). Σε αυτή την περίπτωση εισάγουμε αυτές τις δύο ακμές στο προηγούμενο μονοπάτι του G' , αφαιρούμε την ακμή (t_i, t_{i+1}) και παράγουμε έτσι ένα μονοπάτι $Hamilton$ για τον γράφο G.
- Για κάθε ζεύγος κορυφών t_i και t_{i+1} υπάρχουν οι ακμές (t_i, u) και (t_{i+1}, u). Σε αυτή την περίπτωση δεν μπορούμε να εφαρμόσουμε την κατασκευή της προηγούμενης περίπτωσης αλλά μπορούμε να εισάγουμε την ακμή (t_k, u) στο μονοπάτι μας και έτσι να παράξουμε ένα μονοπάτι $Hamilton$ για τον γράφο G. Βάζοντας δηλαδή τον κόμβο u στο τέλος του υπάρχοντος μονοπατιού

– Για κάθε ζεύγος κορυφών t_i και t_{i+1} υπάρχουν οι ακμές (u, t_i) και (u, t_{i+1}). Εντελώς ανάλογα με την προηγούμενη περίπτωση εισάγουμε την ακμή (u, t_1) παράγοντας έτσι ένα μονοπάτι $Hamilton$ στον γράφο G.

Σε όλες τις περιπτώσεις μπορούμε να κατασκευάσουμε μονοπάτι $Hamilton$ για τον γράφο με $k+1$ κορυφές. Έτσι, δείξαμε ότι η υπόθεση ισχύει για γράφους με οποιονδήποτε αριθμό κορυφών, που είναι και το ζητούμενο.