Πανεπιστημιο Κρητης – Τμημα Μαθηματικων
Λεωφ. Κνωσου, 714 09 Ηρακλειο. Τηλ: +30 2810393801, Fax +30 2810393881

Μιχαλης Κολουντζακης, Καθηγητής

Μεταπτυχιακό μάθημα

"ΠΙΘΑΝΟΘΕΩΡΗΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ"

http:/fourier.math.uoc.gr/~mk/ralg0708

Ημερίδα Ομιλιών

Αίθουσα Ζ301, Δευτέρα 11/2/2008

Στο πλαίσιο του μεταπτυχιακού μαθήματος "Πιθανοθεωρητικοί Αλγόριθμοι" θα γίνουν 45-λεπτες ομιλίες από τους φοιτητές που συμμετείχαν στο μάθημα. Οι ομιλίες θα γίνουν το απόγευμα της Δευτέρας 11/2/08 στην αίθουσα Ζ301. Τα θέματα είναι αρκετά διαφορετικά μεταξύ τους και καλύπτουν το φάσμα από την εφαρμογή ως την πράξη.

Οι ομιλίες είναι ανοιχτές στο κοινό. Δεν χρειάζεται να έχει κάποιος παρακολουθήσει το μάθημα για να παρακολουθήσει τις ομιλίες, οι οποίες είναι αυτοτελείς και προϋποθέτουν σχετικά στοιχειώδεις γνώσεις.

Πρόγραμμα ομιλιών

14:15–15:00	Α. Χόνδρος	Martingales και εφαρμογές
15:15–16:00	Μ. Γιακουμάκης	Η μέθοδος Monte Carlo και οι εφαρμογές της
16:15–17:00	Κ. Περογιαννάκη	Η επίλυση γεωμετρικών προβλημάτων με τη χρήση πιθανοτήτων
17:15–17:45	ΔΙΑΛΛΕΙΜΑ	
17:45–18:30	Γ. Κωνσταντούλας	Ένα φράγμα για το discrepancy ως προς 2-χρωματισμούς
18:45–19:30	Ε. Κουτάκη-Παντερμάκη	Πρωτόκολλα μηδενικής γνώσης

Περιλήψεις

Α. Χόνδρος, *Martingales και εφαρμογές*

Martingales: Πώς πρωτοεμφανίστηκαν και κάποια παραδείγματα.
Stopping Time: Ορισμός και αναφορά του Stopping time theorem καθώς και παράδειγμα.
Wald's Equation: Αναφορά της εξίσωσης του Wald, η απόδειξη και κάποια παραδείγματα.
Azuma's Inequality: Αναφορά της ανισότητας του Azuma και η απόδειξή της καθώς και η Generalized Azuma's Inequality. Εφαρμογές της ανισότητας του Azuma.

Μ. Γιακουμάκης, *Η μέθοδος Monte Carlo και οι εφαρμογές της*

1. Εισαγωγή. Παρουσίαση της μεθόδου Monte Carlo ως διαδικασία για την εύρεση ζητούμενης τιμής, μέσω δειγματοληψίας και προσομοίωσης. Σύνδεση της ζητούμενης τιμής με υπολογίσιμη πιθανότητα.

2. Εφαρμογή της μεθόδου για τον υπολογισμό του π. Παρουσίαση των μεθόδου μέσα από το παράδειγμα. Ανάδειξη προβλημάτων που ενδέχεται να παρουσιαστούν. Έννοια πιθανοθεωρητικής προσέγγισης αποτελέσματος δειγματοληψίας σε ζητούμενη τιμή Έννοια πολυωνυμικού χρόνου πιθανοθεωρητικού αγορίθμου

3. Το πρόβλημα της DNF formula. Έλεγχος επιλυσιμότητας. Η πρώτη προσέγγιση. Ανάδειξη του προβλήματος ελέγχου επιλυσιμότητας σε πολυωνυμικό χρόνο. Η δεύτερη προσέγγιση. Προσπάθεια παράκαμψης του προηγούμενου προβήματος.

Κ. Περογιαννάκη, *Η επίλυση γεωμετρικών προβλημάτων με τη χρήση πιθανοτήτων*

Η ομιλία περιλαμβάνει τα παρακάτω γεωμετρικά προβλήματα καθώς και τις αποδείξεις τους. Το πρώτο πρόβλημα είναι το θεώρημα του Wendel και η απόδειξή του. Το θεώρημα αυτό υπολογίζει την πιθανότητα το κέντρο ενός δεδομένου κύκλου να βρίσκεται στο εσωτερικό της κυρτής θήκης που σχηματίζεται από ανεξάρτητα και ομοιόμορφα επιλεγμένα σημεία του κύκλου και εξαρτάται από το πλήθος των επιλεγμένων σημείων. Στη συνέχεια θα παρουσιαστεί το δεύτερο θεώρημα των Erdős και Füredi και η απόδειξή του. Το θεώρημα αυτό αναφέρει ότι υπάρχει ένα υποσύνολο του Ευκλείδειου Χώρου ($d \geq 1$) με "πολλά" σημεία για το οποίο ισχύει ότι οποιαδήποτε τριάδα από τα στοιχεία του σχηματίζει οξεία γωνία.

Γ. Κωνσταντούλας, *Ένα φράγμα για το discrepancy ως προς 2-χρωματισμούς*

Η έννοια του discrepancy δίνει ένα μέτρο των ανισορροπιών στην κατανομή αντικειμένων ως προς μια δοθείσα δομή (συνδυαστική, τοπολογική, μετρική κτλ.). Στην παρούσα διάλεξη θα μελετήσουμε 2-χρωματισμούς πεπερασμένων συνόλων και πόσο ακανόνιστα κατανέμονται αυτοί ως προς μια οικογένεια υποσυνόλων. Αποδεικνύοντας ένα φράγμα για το discrepancy θα δούμε πόσο περιορίζεται αυτή η έλλειψη κανονικότητας. Τέλος θα αναφέρουμε συσχετισμένα και ισοδύναμα προβλήματα καθώς και εφαρμογές.

Ε. Κουτάκη-Παντερμάκη, *Πρωτόκολλα μηδενικής γνώσης*

Θα γίνει παρουσίαση μιας περιοχής της κρυπτογραφίας, η οποία πρωτοπαρουσιάστηκε το 1985. Αφορά τα πρωτόκολλα μηδενικής γνώσης, τα οποία είναι διαδραστικές αποδείξεις που δεν αποκαλύπτουν παρά μόνο την ορθότητα της προς απόδειξη δήλωσης. Θα παρουσιαστούν τα χαρακτηριστικά των πρωτοκόλλων αυτών, ένα σημαντικό θεώρημα που τα συνδέει με την κλάση NP (προβλήματα που η απόδειξή τους επιβεβαιώνεται σε πολυωνυμικό χρόνο), και ένα παράδειγμα της εφαρμογής τους σε ένα τέτοιο πρόβλημα. Τέλος θα φανεί πώς τέτοιου είδους αποδείξεις εφαρμόζονται σε πραγματικές διαδικασίες πιστοποίησης ταυτότητας, με την παρουσίαση του Fiat-Shamir πρωτοκόλλου.

Ηράκλειο, 8 Φεβρουαρίου 2008