

## ΑΠΟΦΑΣΗ

Έγκριση Κανονισμού Διδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών των Τμημάτων Πληροφορικής και Τηλεπικοινωνιών και Μαθηματικών του Ε.Κ.Π.Α. και των Σχολών Ε.Μ.Φ.Ε. και Η.Μ.Μ.Υ. του Ε.Μ.Π., με τίτλο «Αλγόριθμοι, Λογική και Διακριτά Μαθηματικά (Α.Λ.ΜΑ.)»

### Η ΣΥΓΚΛΗΤΟΣ

#### ΤΟΥ ΕΘΝΙΚΟΥ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΘΗΝΩΝ

Λαμβάνοντας υπόψη:

1. Τις διατάξεις του Ν. 4485/17 «Οργάνωση και Λειτουργία της ανώτατης εκπαίδευσης, ρυθμίσεις για την έρευνα και άλλες διατάξεις» (ΦΕΚ Α' 114), και ειδικότερα τα άρθρα 30 έως και 37, 45 και 85
2. την υπ' αριθμ. 163204/Ζ1/29-9-2017 Εγκύκλιο του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων
3. Την υπ' αριθμ. 216772/Ζ1/8-12-2017 Υπουργική Απόφαση (ΦΕΚ 4334/12-12-2017, τ. Β') με τίτλο «Τρόπος κατάρτισης του αναλυτικού προϋπολογισμού λειτουργίας και της έκθεσης βιωσιμότητας των Προγραμμάτων Μεταπτυχιακών Σπουδών»
4. τις παραγράφους 7 και 8 του άρθρου 19 του Ν. 4521/2018 «Ίδρυση Πανεπιστημίου Δυτικής Αττικής και άλλες διατάξεις» (ΦΕΚ Α' 38)
5. τις διατάξεις του Ν.4009/2011 «Δομή, λειτουργία, διασφάλιση της ποιότητας των σπουδών και διεθνοποίηση των ανωτάτων εκπαιδευτικών ιδρυμάτων (ΦΕΚ Α' 195), όπως τροποποιήθηκαν και ισχύουν
6. τις διατάξεις του Ν.4386/2016 «Ρυθμίσεις για την έρευνα και άλλες διατάξεις» (ΦΕΚ Α' 83), όπως τροποποιήθηκαν και ισχύουν
7. το Π.Δ. 85/31-5-2013 (ΦΕΚ Α' 124) «Ίδρυση, μετονομασία, ανασυγκρότηση Σχολών και ίδρυση Τμήματος στο Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών»
8. Τις διατάξεις του Ν. 3374/2005 και ιδίως τα άρθρα 14 και 15 (ΦΕΚ 189, τ. Α', 02-08-2005) «Διασφάλιση της ποιότητας στην ανώτατη εκπαίδευση. Σύστημα μεταφοράς και συσώρευσης πιστωτικών μονάδων - Παράρτημα διπλώματος» όπως τροποποιήθηκε και ισχύει
9. το απόσπασμα πρακτικού της Συνέλευσης του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ (συνεδρίαση 12/3/2018)
10. το απόσπασμα πρακτικού της Συνέλευσης του Τμήματος Μαθηματικών του ΕΚΠΑ (συνεδρίαση 27/4/2018)
11. το απόσπασμα πρακτικού της Συνέλευσης της Σχολής Ε.Μ.Φ.Ε του Εθνικού Μετσόβιου Πολυτεχνείου (συνεδρίαση 3/5/2018)
12. το απόσπασμα πρακτικού της Συνέλευσης της Σχολής Η.Μ.Μ.Υ του Εθνικού Μετσόβιου Πολυτεχνείου (συνεδρίαση 24/4/2018)
13. το Ειδικό Πρωτόκολλο Συνεργασίας των συνεργαζομένων φορέων
14. το απόσπασμα πρακτικού της Επιτροπής Μεταπτυχιακών Σπουδών του ΕΚΠΑ (συνεδρίαση 22/5/2018)
15. το απόσπασμα πρακτικού της Επιτροπής Μεταπτυχιακών Σπουδών του Εθνικού Μετσόβιου Πολυτεχνείου (συνεδρίαση 10/5/2018)
16. το απόσπασμα πρακτικού της Συγκλήτου του ΕΚΠΑ (συνεδρίαση 22/5/2018)

17.το απόσπασμα πρακτικού της Συγκλήτου του Εθνικού Μετσόβιου Πολυτεχνείου (συνεδρίαση 10/5/2018)

18.το γεγονός ότι με την παρούσα δεν προκαλείται δαπάνη εις βάρος του κρατικού προϋπολογισμού

#### **αποφασίζουμε:**

την έγκριση του Κανονισμού του Διδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών (ΔΠΜΣ) των Τμημάτων Πληροφορικής και Τηλεπικοινωνιών και Μαθηματικών του Ε.Κ.Π.Α. και των Σχολών Ε.Μ.Φ.Ε. και Η.Μ.Μ.Υ. του Ε.Μ.Π., με τίτλο «Αλγόριθμοι, Λογική και Διακριτά Μαθηματικά (Α.Λ.ΜΑ.)», από το ακαδημαϊκό έτος 2018-2019, ως ακολούθως:

#### **ΑΡΘΡΟ 1**

##### **ΑΝΤΙΚΕΙΜΕΝΟ-ΣΚΟΠΟΣ**

Αντικείμενο του ΔΠΜΣ είναι οι Αλγόριθμοι, η Λογική και τα Διακριτά Μαθηματικά, περιοχές που αναφέρονται στις επιστήμες της Πληροφορικής και των Μαθηματικών. Με τη σύμπραξη των Σχολών και Τμημάτων που συμμετέχουν στο πρόγραμμα επιδιώκεται:

1. Η εκμετάλλευση του ελληνικού επιστημονικού δυναμικού που εξειδικεύεται στο γνωστικό αντικείμενο του ΔΠΜΣ.
2. Η εκμετάλλευση της υλικοτεχνικής υποδομής των Ιδρυμάτων που συμπράττουν, καθώς και των ερευνητικών ινστιτούτων και κληροδοτημάτων που διασυνδέονται με αυτά.
3. Η αποτελεσματικότερη αλληλεπίδραση επιστήμης και τεχνολογίας με στόχο την ισόρροπη εκπαίδευση νέων επιστημόνων.

Σκοπός του ΔΠΜΣ είναι η παροχή εξειδικευμένων γνώσεων, η ανάπτυξη της έρευνας και η παραγωγή νέας γνώσης στις επιστημονικές περιοχές που σχετίζονται με τους Αλγόριθμους και την αλληλεπίδρασή τους με τη Μαθηματική Λογική και τα Διακριτά Μαθηματικά. Επίσης, το ΔΠΜΣ αποσκοπεί στη βελτίωση της ποιότητας του Ελληνικού επιστημονικού δυναμικού στο πλαίσιο του Ευρωπαϊκού και γενικότερα του διεθνούς χώρου.

Το ΔΠΜΣ οδηγεί στην απονομή Διπλώματος Μεταπτυχιακών Σπουδών (ΔΜΣ) στους «Αλγορίθμους, τη Λογική και τα Διακριτά Μαθηματικά», μετά την πλήρη και επιτυχή ολοκλήρωση των σπουδών με βάση το πρόγραμμα σπουδών. Ο τίτλος απονέμεται από το Τμήμα Πληροφορικής και Τηλεπικοινωνιών με αναφορά όλων των συνεργαζόμενων Τμημάτων και Σχολών.

Τη διοικητική υποστήριξη του Προγράμματος αναλαμβάνει το Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

#### **ΑΡΘΡΟ 2**

##### **ΔΟΜΗ ΚΑΙ ΟΡΓΑΝΑ ΤΟΥ ΠΜΣ**

Αρμόδια όργανα για τη λειτουργία του ΔΠΜΣ σύμφωνα με το νόμο 4485/2017 είναι:

- η **Ειδική Διδρυματική Επιτροπή (ΕΔΕ)**: Η Ειδική Διδρυματική Επιτροπή έχει διετή θητεία, είναι εννεαμελής και συγκροτείται από επτά (7) διδάσκοντες μέλη ΔΕΠ των συνεργαζόμενων Τμημάτων/Σχολών και δύο (2) εκπροσώπους των μεταπτυχιακών φοιτητών του προγράμματος. Η κατανομή των μελών ανά συνεργαζόμενο φορέα και κατ' αναλογία του αριθμού των διδασκόντων τους στο ΔΠΜΣ έχει ως εξής:

- Ένα μέλος ΔΕΠ από το Τμήμα/Σχολή που έχει τη διοικητική υποστήριξη του προγράμματος, ο οποίος και αποτελεί τον **Πρόεδρο της ΕΔΕ**.
- Τρία μέλη ΔΕΠ από τα Τμήματα Πληροφορικής και Τηλεπικοινωνιών, και Μαθηματικών του ΕΚΠΑ.
- Τρία μέλη ΔΕΠ από τις Σχολές ΕΜΦΕ και ΗΜΜΥ του ΕΜΠ.

Σε ειδικές περιπτώσεις που επιβάλλεται για την εύρυθμη λειτουργία του ΔΠΜΣ, ύστερα από αιτιολογημένη απόφαση της ΕΔΕ, Πρόεδρος αναλαμβάνει μέλος ΔΕΠ από άλλο Τμήμα/Σχολή από αυτό που έχει τη διοικητική στήριξη του ΔΠΜΣ (αρ. 31, παρ.4, Ν.4485/17).

Η ΕΔΕ αποφασίζει ως προς την οικονομική διαχείριση και ειδικότερα ως προς την έγκριση των δαπανών του ΠΜΣ και πιστοποιεί τη σχέση εκπαιδευτικών αναγκών του ΠΜΣ με τις εκάστοτε αιτούμενες δαπάνες.

- **η Συντονιστική Επιτροπή (ΣΕ) του ΔΠΜΣ:** Η ΣΕ απαρτίζεται από πέντε (5) μέλη ΔΕΠ των συνεργαζόμενων φορέων, τα οποία έχουν αναλάβει μεταπτυχιακό έργο και εκλέγονται από την ΕΔΕ για διετή θητεία. Τα μέλη της ΣΕ δεν δικαιούνται επιπλέον αμοιβή ή αποζημίωση για τη συμμετοχή τους στην επιτροπή. Πρόεδρος της ΣΕ είναι ο **Διευθυντής του ΔΠΜΣ**, ο οποίος ορίζεται από την ΕΔΕ μεταξύ των μελών της ΣΕ. Η θητεία του Προέδρου της ΣΕ μπορεί να ανανεωθεί μία φορά (παρ.5, αρ.31, Ν.4485/2017). Η ΣΕ είναι αρμόδια για την παρακολούθηση και τον συντονισμό της λειτουργίας του προγράμματος και:

- Εισηγείται στην ΕΔΕ την κατανομή του διδακτικού έργου μεταξύ των διδασκόντων του ΔΠΜΣ.
- Ορίζει τον επιβλέποντα και τα μέλη της τριμελούς επιτροπής εξέτασης διπλωματικών εργασιών, ο ορισμός της οποίας επικυρώνεται από την ΕΔΕ.
- Εξετάζει φοιτητικά θέματα όπως αιτήσεις αναστολής φοίτησης, παράτασης σπουδών, αναγνώρισης μαθημάτων από προηγούμενη μεταπτυχιακή εκπαίδευση, αντικατάστασης μαθημάτων του παρόντος Προγράμματος με μαθήματα άλλων Μεταπτυχιακών Προγραμμάτων, και εισηγείται σχετικά στην ΕΔΕ.

- **ο Διευθυντής και ο Αναπληρωτής Διευθυντή του ΔΠΜΣ:** Ο Διευθυντής του ΔΠΜΣ και ο Αναπληρωτής του είναι μέλη ΔΕΠ πρώτης βαθμίδας ή της βαθμίδας του αναπληρωτή, και είναι του ίδιου ή συναφούς αντικείμενου με το γνωστικό αντικείμενο του ΔΠΜΣ. Ο Διευθυντής είναι μέλος και Πρόεδρος της ΣΕ. Επιλέγεται από τα εκλεγμένα μέλη της ΣΕ και ορίζεται μαζί με τον Αναπληρωτή του με απόφαση της ΕΔΕ για διετή θητεία. Δεν μπορεί να έχει περισσότερες από δύο συνεχόμενες θητείες. Προγενέστερες της ισχύος του Ν.4485/2017 θητείες δεν λαμβάνονται υπόψη. Ο Διευθυντής του ΔΠΜΣ εισηγείται στα αρμόδια όργανα του Ιδρύματος για κάθε θέμα που αφορά την αποτελεσματική λειτουργία του προγράμματος. Ο Διευθυντής του ΔΠΜΣ προέρχεται από το Τμήμα/Σχολή που έχει τη διοικητική στήριξη του Προγράμματος. Σε ειδικές περιπτώσεις που επιβάλλεται για την εύρυθμη λειτουργία του ΔΠΜΣ, ύστερα από αιτιολογημένη απόφαση της ΕΔΕ, Διευθυντής αναλαμβάνει μέλος ΔΕΠ από άλλο Τμήμα/Σχολή από αυτό που έχει τη διοικητική στήριξη του ΠΜΣ (αρ. 31, παρ.4, Ν.4485/17). Ο Διευθυντής έχει τις ακόλουθες αρμοδιότητες:

- α) Συγκαλεί σε συνεδρίαση τη ΣΕ.
- β) Καταρτίζει την ημερήσια διάταξη των εν λόγω συνεδριάσεων, λαμβάνοντας υπόψη εισηγήσεις των μελών και οργάνων του ΔΠΜΣ.
- γ) Έχει την ευθύνη σύνταξης του προϋπολογισμού και απολογισμού του Προγράμματος, τους οποίους υποβάλλει στην ΕΔΕ για έγκριση.
- δ) Είναι υπεύθυνος για την παρακολούθηση της εκτέλεσης του προϋπολογισμού και για την έκδοση των εντολών πληρωμής των σχετικών δαπανών.

ε) Κατά τη λήξη της θητείας του, καθώς και της ΣΕ, συντάσσει αναλυτικό απολογισμό του ερευνητικού και εκπαιδευτικού έργου του ΔΠΜΣ, καθώς και των λοιπών δραστηριοτήτων του, με στόχο την αναβάθμιση των σπουδών, την καλύτερη αξιοποίηση του ανθρώπινου δυναμικού, τη βελτιστοποίηση των υφιστάμενων υποδομών και την κοινωνικά επωφελή χρήση των διαθέσιμων πόρων του ΔΠΜΣ.

Ο Αναπληρωτής Διευθυντής του ΔΠΜΣ εκπληρώνει τα καθήκοντα του Διευθυντή σε περίπτωση απουσίας του.

Το ΔΠΜΣ «Α.Λ.ΜΑ.» υποστηρίζεται από Γραμματεία του Προγράμματος που είναι εγκατεστημένη στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ και βρίσκεται υπό την επιστολή της Γραμματείας του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ. Η Γραμματεία του ΠΜΣ έχει ως καθήκον τη γραμματειακή υποστήριξη του ΠΜΣ, όπως την προετοιμασία της διαδικασίας εισδοχής υποψηφίων, την τήρηση των οικονομικών στοιχείων του Προγράμματος, τη γραμματειακή υποστήριξη της ΕΔΕ, την καταχώριση βαθμολογιών κλπ.

### **ΑΡΘΡΟ 3**

#### **ΚΑΤΗΓΟΡΙΕΣ ΚΑΙ ΑΡΙΘΜΟΣ ΕΙΣΑΚΤΕΩΝ**

Στο ΔΠΜΣ «Α.Λ.ΜΑ.» γίνονται δεκτοί κάτοχοι τίτλου του Α΄ κύκλου σπουδών ΑΕΙ της ημεδαπής ή ομοταγών, αναγνωρισμένων από τον ΔΟΑΤΑΠ, ιδρυμάτων της αλλοδαπής. Το Πρόγραμμα απευθύνεται κυρίως σε υποψηφίους προερχόμενους από Τμήματα ή Σχολές Μαθηματικών, Πληροφορικής, Πληροφορικής και Τηλεπικοινωνιών, Επιστήμης Υπολογιστών, Μηχανικών Υπολογιστών και Πληροφορικής, Ηλεκτρολόγων Μηχανικών. Εφόσον γίνουν δεκτοί, υποψήφιοι προερχόμενοι από άλλα Τμήματα (και σε ειδικές περιπτώσεις, υποψήφιοι προερχόμενοι από τα προαναφερθέντα Τμήματα) θα περάσουν από ειδικό προπαρασκευαστικό κύκλο προπτυχιακών μαθημάτων ενίσχυσης του υποβάθρου τους. Για τους μεταπτυχιακούς φοιτητές οι οποίοι έγιναν δεκτοί για αρχική φοίτηση στον κύκλο προκαταρκτικών μαθημάτων προκειμένου να γίνουν δεκτοί στον κύκλο μεταπτυχιακών μαθημάτων, ο χρόνος παρακολούθησης των προκαταρκτικών μαθημάτων δεν προσμετράται στο χρόνο φοίτησης για την κτήση του ΔΜΣ.

Γίνονται δεκτοί ως υπεράριθμοι υπότροφοι και μέλη των κατηγοριών ΕΕΠ, ΕΔΙΠ και ΕΤΕΤ σύμφωνα με την παρ. 8 του άρ. 34 του Ν.4485/17.

Ο αριθμός των εισακτέων στο ΔΠΜΣ ορίζεται κατ' ανώτατο όριο σε τριάντα (30) άτομα ανά ακαδημαϊκό έτος και προγραμματίζεται να απασχολεί δεκαπέντε (15) συνολικά διδάσκοντες, από τους οποίους τουλάχιστον το 80% θα είναι από τα Τμήματα/Σχολές που συμμετέχουν στο πρόγραμμα και 20% από Πανεπιστήμια και Ερευνητικά Κέντρα της ημεδαπής και της Αλλοδαπής. Αυτό αντιστοιχεί σε δύο (2) φοιτητές ανά διδάσκοντα.

Σημειώνεται ότι ο αριθμός μεταπτυχιακών φοιτητών στα λειτουργούντα ΠΜΣ του επισπεύδοντος Τμήματος Πληροφορικής και Τηλεπικοινωνιών είναι τριακόσιοι είκοσι πέντε (325), σε σχέση με τον αριθμό των δύο χιλιάδων ενενήντα πέντε (2.095) προπτυχιακών φοιτητών και των σαράντα τριών (43) διδασκόντων του Τμήματος, που αναλύεται ως εξής: 39 μέλη ΔΕΠ και 4 αφυπηρηθέντα μέλη ΔΕΠ. Τα ανωτέρω στοιχεία δίνονται κατά προσέγγιση και ανταποκρίνονται στα δεδομένα του έτους σύνταξης του Κανονισμού.

### **ΑΡΘΡΟ 4**

#### **ΤΡΟΠΟΣ ΕΙΣΑΓΩΓΗΣ**

Η επιλογή των φοιτητών/τριών γίνεται σύμφωνα με το νόμο 4485/2017 και τις προβλέψεις του παρόντος Κανονισμού Μεταπτυχιακών Σπουδών. Δικαίωμα αίτησης έχουν και νυν φοιτητές οι οποίοι βρίσκονται στο τελευταίο εξάμηνο υποχρεωτικής φοίτησης και αναμένεται να αποκτήσουν το πτυχίο τους μέχρι την περίοδο εγγραφών.

Κατά τη διάρκεια του εαρινού εξαμήνου με απόφαση της ΣΕ του ΔΠΜΣ δημοσιεύεται στην ιστοσελίδα του Τμήματος προκήρυξη για την εισαγωγή μεταπτυχιακών φοιτητών στο ΔΠΜΣ. Οι σχετικές αιτήσεις μαζί με τα απαραίτητα δικαιολογητικά κατατίθενται σε προθεσμία που ορίζεται κατά την προκήρυξη και μπορεί να παραταθεί με απόφαση της ΣΕ.

Απαραίτητα δικαιολογητικά είναι:

1. Αίτηση Συμμετοχής.
2. Βιογραφικό σημείωμα.
3. Επικυρωμένο Αντίγραφο πτυχίου ή βεβαίωση περάτωσης σπουδών.
4. Αναλυτική Βαθμολογία για κάθε προσκομιζόμενο τίτλο σπουδών.
5. Δημοσιεύσεις σε περιοδικά ή συνέδρια με κρίση, εάν υπάρχουν.
6. Μία πρόσφατη φωτογραφία.
7. Έως δύο συστατικές επιστολές κατά τα οριζόμενα στην προκήρυξη.
8. Πιστοποιητικό γλωσσομάθειας αγγλικής γλώσσας επιπέδου τουλάχιστον B2.
9. Επιπλέον στοιχεία κατά την κρίση του υποψήφιου, όπως αποδεικτικά επαγγελματικής ή ερευνητικής δραστηριότητας.

Η γνώση της Αγγλικής γλώσσας αποδεικνύεται με βάση όσα ορίζει η από 25/2/2016 σχετική απόφαση του ΑΣΕΠ<sup>1</sup>.

Με απόφαση της ΕΔΕ συγκροτείται Επιτροπή Επιλογής (εφεξής ΕΕ) μεταπτυχιακών φοιτητών. Κατά τη διαδικασία επιλογής οι υποψήφιοι κρίνονται ως προς τρεις άξονες:

Α. Απόδοση. Για τους ήδη αποφοίτους είναι ο βαθμός πτυχίου. Για τους νυν φοιτητές είναι ο μέχρι τότε μέσος όρος βαθμολογίας τους.

Β. Υπόβαθρο. Κρίνεται με βάση τα μαθήματα που έχει πάρει ο υποψήφιος και την υπόλοιπη δραστηριότητά του. Αντιπροσωπεύεται από τον μέσο όρο των 5 καλύτερων βαθμών που έχει πάρει ο υποψήφιος σε μαθήματα που ανήκουν στο συγκεκριμένο σύνολο που έχει οριστεί για κάθε μεταπτυχιακή ειδίκευση.

Γ. Γενική Αξιολόγηση. Περιλαμβάνει επιπρόσθετα στοιχεία που συμπληρώνουν την εικόνα του υποψηφίου, όπως ερευνητική δραστηριότητα, δημοσιεύσεις, συστατικές επιστολές, πτυχιακή εργασία, κ.ο.κ. Κατά την κρίση της ΣΕ ορισμένοι υποψήφιοι μπορεί να κληθούν σε προφορική συνέντευξη ώστε να σχηματιστεί πληρέστερη εικόνα.

Με βάση το σύνολο των κριτηρίων, η ΕΕ αξιολογεί τους υποψήφιους και καταρτίζει εισήγηση προς την ΕΔΕ η οποία αποφασίζει. Οι επιλεγέντες μη πτυχιούχοι οφείλουν να έχουν αποδεδειγμένα ολοκληρώσει τις υποχρεώσεις τους για το πτυχίο πριν το τέλος της περιόδου εγγραφών στο μεταπτυχιακό πρόγραμμα. Σε αντίθετη περίπτωση χάνουν οριστικά το δικαίωμα εγγραφής. Το δικαίωμα εγγραφής χάνουν και οι επιλεγέντες που δεν

---

1

<http://www.asep.gr/webcenter/ShowProperty?nodeId=%2Fucmsserver%2FVDCCMS01.ASEP.004721%2F%2FidcPrimaryFile&revision=latestreleased>

θα καταθέσουν εγκαίρως όλα τα απαραίτητα δικαιολογητικά. Σε περίπτωση μη έγκαιρης εγγραφής ενός ή περισσότερων φοιτητών, θα κληθούν να εγγραφούν στο ΠΜΣ οι επιλαχόντες, εάν υπάρχουν.

Οι εγγραφές στο ΠΜΣ πραγματοποιούνται τον Οκτώβριο κάθε ακαδημαϊκού έτους σε ημερομηνίες που ανακοινώνονται από το Τμήμα.

## **ΑΡΘΡΟ 5**

### **ΔΙΑΡΚΕΙΑ ΦΟΙΤΗΣΗΣ**

Η χρονική διάρκεια φοίτησης στο ΠΜΣ που οδηγεί στη λήψη Διπλώματος Μεταπτυχιακών Σπουδών (ΔΜΣ) ορίζεται σε τρία (3) ακαδημαϊκά εξάμηνα, στα οποία περιλαμβάνεται και ο χρόνος εκπόνησης διπλωματικής εργασίας. Ο ανώτατος επιτρεπόμενος χρόνος ολοκλήρωσης των σπουδών, ορίζεται στα έξι (6) ακαδημαϊκά εξάμηνα.

Ένας μεταπτυχιακός φοιτητής μπορεί, με αιτιολογημένη αίτησή του και για σοβαρούς λόγους, να ζητήσει την αναστολή φοίτησης του για χρονικό διάστημα που δεν υπερβαίνει τα δύο συνεχόμενα εξάμηνα. Τα εξάμηνα αναστολής της φοιτητικής ιδιότητας δεν προσμετρούνται στην προβλεπόμενη ανώτατη διάρκεια κανονικής φοίτησης.

## **ΑΡΘΡΟ 6**

### **ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ**

Το ΠΜΣ ξεκινά το χειμερινό εξάμηνο εκάστου ακαδημαϊκού έτους. Για την απόκτηση ΔΜΣ απαιτούνται συνολικά ενενήντα (90) πιστωτικές μονάδες (ECTS). Η διδασκαλία των μαθημάτων γίνεται διά ζώσης αλλά και με μέσα εξ αποστάσεως εκπαίδευσης σε ποσοστό όμως που δεν υπερβαίνει το 35% (παρ. 3, αρ. 30, Ν.4485/2017). Τα μαθήματα οργανώνονται σε εξάμηνα, πραγματοποιούνται σε εβδομαδιαία βάση και διεξάγονται στην Ελληνική γλώσσα. Μετά από απόφαση της ΕΔΕ, μπορούν να προσφερθούν μαθήματα και στην Αγγλική γλώσσα.

**Α.** Στο πλαίσιο του ΔΠΜΣ προσφέρονται οι ακόλουθες κατηγορίες μαθημάτων:

#### **1. Υποχρεωτικό μάθημα**

– Αλγόριθμοι

#### **2. Κατ' επιλογήν υποχρεωτικά μαθήματα**

Τα κατ' επιλογήν υποχρεωτικά μαθήματα χωρίζονται στις παρακάτω 3 ομάδες:

Ομάδα **A** (Αλγόριθμοι):

- Προσεγγιστικοί αλγόριθμοι
- Συνδυαστική βελτιστοποίηση
- Υπολογιστική πολυπλοκότητα

Ομάδα **B** (Λογική):

- Θεωρία αναδρομής
- Θεωρία συνόλων
- Λογική

Ομάδα **Γ** (Διακριτά Μαθηματικά):

- Θεωρία γραφημάτων
- Στοχαστικές διαδικασίες
- Συνδυαστική

#### **3. Μαθήματα επιλογής**

– Ακραία συνδυαστική

- Άλγεβρα και κρυπτογραφία
- Αλγοριθμικά θέματα κοινωνικών δικτύων
- Αλγοριθμική θεωρία γραφημάτων
- Αλγοριθμική θεωρία παιγνίων
- Αλγόριθμοι δικτύων και πολυπλοκότητα
- Αλγόριθμοι στη δομική βιοπληροφορική
- Ανάλυση γεωμετρικών δεδομένων
- Αναλυτική συνδυαστική
- Απεικόνιση γραφημάτων
- Απειροσυνδυαστική
- Διακριτή ανάλυση
- Δομική πολυπλοκότητα
- Δομική θεωρία γραφημάτων
- Δυναμικός προγραμματισμός
- Ειδικά θέματα αλγορίθμων
- Ειδικά θέματα διακριτών μαθηματικών
- Ειδικά θέματα λογικής
- Επιχειρησιακή έρευνα
- Θεωρία αποδείξεων
- Θεωρία γραμμικού προγραμματισμού
- Θεωρία κόμβων και εφαρμογές
- Θεωρία μητροειδών
- Θεωρία μοντέλων
- Θεωρία ουρών αναμονής
- Θεωρία παιγνίων
- Θεωρία πληροφορίας
- Κρυπτογραφία
- Κυρτή ανάλυση
- Λάμδα λογισμός
- Μοντέλα υπολογισμού, τυπικές γλώσσες και αυτόματα
- Παραμετρικοί πολυπλοκότητα και αλγόριθμοι
- Πιθανοτικές μέθοδοι
- Προσθετική συνδυαστική
- Σημασιολογία γλωσσών προγραμματισμού
- Στοχαστικά μοντέλα
- Συστήματα τύπων των γλωσσών προγραμματισμού
- Τροπική λογική
- Τυπικές μέθοδοι
- Τυχαίοι αλγόριθμοι
- Υπολογιστική άλγεβρα
- Υπολογιστική γεωμετρία
- Υπολογιστική επιστήμη και τεχνολογία
- Υπολογιστική κρυπτογραφία

**4. Σεμιναριακά μαθήματα:** αφορούν προχωρημένα θέματα και διδάσκονται συνήθως από επισκέπτες καθηγητές.

**5. Μαθήματα μελέτης:** έχουν ως στόχο τη μελέτη σε βάθος κάποιου συγκεκριμένου ερευνητικού θέματος και προσφέρονται σε φοιτητές που έχουν ολοκληρώσει επιτυχώς τα υποχρεωτικά μαθήματα, υπό την καθοδήγηση ενός διδάσκοντα του προγράμματος.

Το υποχρεωτικό, κάθε κατ' επιλογήν υποχρεωτικό μάθημα και κάθε μάθημα επιλογής διδάσκεται για τέσσερις (4) ώρες εβδομαδιαίως, από τις οποίες η μία (1) μπορεί

να αφορά φροντιστηριακές ή εργαστηριακές ασκήσεις, και αντιστοιχεί σε έξι (6) πιστωτικές μονάδες (ECTS). Κάθε σεμιναριακό μάθημα διδάσκεται για τουλάχιστον είκοσι (20) ώρες ανά εξάμηνο και αντιστοιχεί σε τέσσερις (4) πιστωτικές μονάδες. Κάθε μάθημα μελέτης διδάσκεται για δύο (2) ώρες εβδομαδιαίως και αντιστοιχεί σε τέσσερις (4) πιστωτικές μονάδες.

Κάθε φοιτητής μπορεί, κατόπιν εγκρίσεως της Ε.Δ.Ε.,

α. να συγκεντρώσει μέχρι δώδεκα (12) πιστωτικές μονάδες από επιτυχή παρακολούθηση μαθημάτων άλλων ΠΜΣ συναφούς αντικειμένου και

β. να ζητήσει την αναγνώριση μεταπτυχιακών μαθημάτων που παρακολούθησε επιτυχώς πριν από την εγγραφή του στο ΔΠΜΣ.

Κάθε φοιτητής μπορεί να συγκεντρώσει συνολικά το πολύ τριάντα (30) πιστωτικές μονάδες από μαθήματα των παραπάνω περιπτώσεων (α) και (β).

Για την απονομή του ΔΜΣ κάθε φοιτητής οφείλει να συγκεντρώσει ενενήντα (90) πιστωτικές μονάδες ως εξής:

- εικοσιτέσσερις (24) πιστωτικές μονάδες μέσω επιτυχούς παρακολούθησης του υποχρεωτικού μαθήματος «Αλγόριθμοι» και τριών (3) κατ' επιλογήν υποχρεωτικών μαθημάτων, ένα από κάθε μία από τις Ομάδες Α. Αλγόριθμοι, Β. Λογική και Γ. Διακριτά Μαθηματικά.

- τριαντάξι (36) πιστωτικές μονάδες μέσω επιτυχούς παρακολούθησης λοιπών μαθημάτων.

- τριάντα (30) πιστωτικές μονάδες μέσω επιτυχούς συγγραφής μεταπτυχιακής διπλωματικής εργασίας.

Τα μαθήματα, η κατανομή τους σε εξάμηνα και οι προϋποθέσεις για τη λήψη του διπλώματος μπορούν να τροποποιηθούν με απόφαση της ΕΔΕ. Στις οποιοσδήποτε τροποποιήσεις που αφορούν το υποχρεωτικό, τα κατ' επιλογήν υποχρεωτικά και τα λοιπά μαθήματα θα πρέπει να τηρείται μια ισορροπία μεταξύ των τριών επιστημονικών περιοχών του προγράμματος (Αλγόριθμοι, Λογική, Διακριτά Μαθηματικά), καθώς και να εξασφαλίζεται ο κεντρικός ρόλος των Αλγορίθμων, όπως στο παρόν πρόγραμμα. Επίσης τυχόν τροποποιήσεις θα είναι εφαρμοστέες από το επόμενο ακαδημαϊκό έτος από αυτό κατά το οποίο αποφασίζονται από την ΕΔΕ.

Ο παρακάτω πίνακας εμφανίζει μια ενδεικτική κατανομή μαθημάτων ανά εξάμηνο και ανά κατηγορία, αναφέροντας για κάθε μάθημα τις αντίστοιχες πιστωτικές μονάδες.

Α' ΕΞΑΜΗΝΟ		
ΜΑΘΗΜΑ	Διδακτικές Ώρες	ECTS
ΑΛΓΟΡΙΘΜΟΙ (ΥΠΟΧΡΕΩΤΙΚΟ)	4	6
ΥΠΟΧΡΕΩΤΙΚΟ ΚΑΤ' ΕΠΙΛΟΓΗ ΟΜΑΔΑΣ Α	4	6
ΥΠΟΧΡΕΩΤΙΚΟ ΚΑΤ' ΕΠΙΛΟΓΗ ΟΜΑΔΑΣ Β	4	6
ΥΠΟΧΡΕΩΤΙΚΟ ΚΑΤ' ΕΠΙΛΟΓΗ ΟΜΑΔΑΣ Γ	4	6
ΜΑΘΗΜΑ ΕΠΙΛΟΓΗΣ	4	6



	<b>Σύνολο</b>	20	30
<b>Β' ΕΞΑΜΗΝΟ</b>			
	<b>ΜΑΘΗΜΑ</b>	<b>Διδακτικές Ώρες</b>	<b>ECTS</b>
	ΜΑΘΗΜΑ ΕΠΙΛΟΓΗΣ	4	6
	ΜΑΘΗΜΑ ΕΠΙΛΟΓΗΣ	4	6
	ΜΑΘΗΜΑ ΕΠΙΛΟΓΗΣ	4	6
	ΜΑΘΗΜΑ ΕΠΙΛΟΓΗΣ	4	6
	ΜΑΘΗΜΑ ΕΠΙΛΟΓΗΣ	4	6
	<b>Σύνολο</b>	20	30
<b>Γ' ΕΞΑΜΗΝΟ</b>			
	<b>ΜΑΘΗΜΑ</b>		<b>ECTS</b>
	ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ		30

## **Β. Περιεχόμενο/Περιγραφή μαθημάτων**

Η λεπτομερής περιγραφή του περιεχομένου των προσφερόμενων μαθημάτων του «Α.Λ.ΜΑ.», δίνεται στο παράρτημα του Κανονισμού. Με απόφαση της ΕΔΕ μπορεί κάποιο από τα μαθήματα να διδαχθεί στην αγγλική γλώσσα. Η γλώσσα συγγραφής της μεταπτυχιακής διπλωματικής εργασίας μπορεί να είναι τα Ελληνικά ή τα Αγγλικά, με σύμφωνη γνώμη του επιβλέποντα.

### **ΑΡΘΡΟ 7**

#### **ΕΞΕΤΑΣΕΙΣ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΦΟΙΤΗΤΩΝ**

Το εκπαιδευτικό έργο κάθε ακαδημαϊκού έτους διαρθρώνεται σε δύο εξάμηνα σπουδών, το χειμερινό και το εαρινό, έκαστο εκ των οποίων περιλαμβάνει τουλάχιστον 13 εβδομάδες διδασκαλίας και τρεις εβδομάδες εξετάσεων. Τα μαθήματα εξετάζονται στο τέλος του εξαμήνου κατά το οποίο διδάχτηκαν. Το υποχρεωτικό μάθημα ΑΛΓΟΡΙΘΜΟΙ εξετάζεται και την περίοδο του Σεπτεμβρίου.

Η παρακολούθηση των μαθημάτων είναι υποχρεωτική. Σε περίπτωση κωλύματος διεξαγωγής μαθήματος προβλέπεται η αναπλήρωσή του. Η ημερομηνία και η ώρα αναπλήρωσης αναρτώνται στην ιστοσελίδα του μαθήματος.

Η αξιολόγηση των μεταπτυχιακών φοιτητών και η επίδοσή τους στα μαθήματα που υποχρεούνται να παρακολουθήσουν στο πλαίσιο του ΔΠΜΣ πραγματοποιείται στο τέλος κάθε εξαμήνου με γραπτές ή προφορικές εξετάσεις ή με εκπόνηση εργασιών καθ' όλη τη διάρκεια του εξαμήνου. Ο τρόπος αξιολόγησης ορίζεται από τον διδάσκοντα του κάθε μαθήματος. Η βαθμολόγηση γίνεται στην κλίμακα 1-10.

## **ΑΡΘΡΟ 8**

### **ΥΠΟΧΡΕΩΣΕΙΣ ΚΑΙ ΔΙΚΑΙΩΜΑΤΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΦΟΙΤΗΤΩΝ**

1. Οι μεταπτυχιακοί φοιτητές έχουν όλα τα δικαιώματα και τις παροχές που προβλέπονται για τους φοιτητές του Α΄ κύκλου σπουδών, πλην του δικαιώματος παροχής δωρεάν διδακτικών συγγραμμάτων. Το Ίδρυμα υποχρεούται να εξασφαλίσει στους φοιτητές με αναπηρία ή/και ειδικές ανάγκες προσβασιμότητα στα προτεινόμενα συγγράμματα και τη διδασκαλία (παρ. 3, αρ.34, Ν.4485/2017).

2. Προκειμένου να επιτευχθεί η ολοκλήρωση της ακαδημαϊκής προσωπικότητας και της εκπαίδευσης τους, οι μεταπτυχιακοί φοιτητές προετοιμάζονται σχετικά με την Άσκηση Ακαδημαϊκής Εμπειρίας η οποία διενεργείται εντός των δομών και διαδικασιών των Τμημάτων/Σχολών που συμμετέχουν στο πρόγραμμα. Η Άσκηση Ακαδημαϊκής Εμπειρίας αποτελείται από τρεις ενότητες: 1) Παρακολούθηση και παρουσίαση επιστημονικών διαλέξεων. Το ΔΠΜΣ στηρίζει την ερευνητική προσπάθεια των μεταπτυχιακών φοιτητών μέσω της διοργάνωσης σεμιναρίων στα οποία συμμετέχουν είτε ως ακροατές είτε ως ομιλητές, 2) Ερευνητική ενασχόληση, Συγγραφή Επιστημονικών Εργασιών και Ακαδημαϊκή Δεοντολογία. Κατά τη διάρκεια της φοίτησής τους, οι μεταπτυχιακοί φοιτητές εξοικειώνονται με την διαδικασία της έρευνας και της συγγραφής ερευνητικών εργασιών, τηρώντας την ακαδημαϊκή ηθική, και 3) Το ΔΠΜΣ παρέχει Βιωματική Απόκτηση Ακαδημαϊκής Εμπειρίας των μεταπτυχιακών φοιτητών μέσω της συμμετοχής τους στην εκπαιδευτική διαδικασία υπό την καθοδήγηση και επίβλεψη μελών ΔΕΠ. Η ΕΔΕ του προγράμματος προσδιορίζει επιμέρους ζητήματα της Άσκησης Ακαδημαϊκής Εμπειρίας.

3. Η ΕΔΕ μετά την εισήγηση της ΣΕ, δύναται να αποφασίσει τη διαγραφή μεταπτυχιακών φοιτητών εάν:

- έχουν αποτύχει στην εξέταση μαθήματος ή μαθημάτων και δεν έχουν ολοκληρώσει επιτυχώς το πρόγραμμα,
- υπερβούν τη μέγιστη χρονική διάρκεια φοίτησης στο ΠΜΣ, όπως ορίζεται στον παρόντα Κανονισμό,
- έχουν παραβιάσει τις κείμενες διατάξεις όσον αφορά την αντιμετώπιση πειθαρχικών παραπτώματων από τα αρμόδια πειθαρχικά Όργανα,
- αυτοδίκαια κατόπιν αιτήσεως τους,
- υποπέσουν σε παράπτωμα που εμπίπτει στο δίκαιο περί πνευματικής ιδιοκτησίας (Ν.2121/93) κατά τη συγγραφή των προβλεπομένων εργασιών τους.

4. Στο τέλος κάθε εξαμήνου πραγματοποιείται αξιολόγηση κάθε μαθήματος και κάθε διδάσκοντος από τους μεταπτυχιακούς φοιτητές (παρ. 1., αρ.44, Ν.4485/2017). Τα αποτελέσματα της αξιολόγησης κοινοποιούνται στους διδάσκοντες.

5. Η καθομολόγηση γίνεται στο πλαίσιο της Συνέλευσης του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ και σε χώρο του ΕΚΠΑ, παρουσία του Διευθυντή του ΔΠΜΣ ή του Αναπληρωτή του, του Προέδρου του Τμήματος ή του Αναπληρωτή του και, κατά τις δυνατότητες, ενδεχομένως εκπροσώπου του Πρυτάνεως.

Πιο συγκεκριμένα στο πλαίσιο του ΠΜΣ «Α.Λ.Μ.Α.» απονέμεται Δίπλωμα Μεταπτυχιακών Σπουδών στους «Αλγορίθμους, τη Λογική και τα Διακριτά Μαθηματικά».

6. Δίπλωμα Μεταπτυχιακών Σπουδών δεν απονέμεται σε φοιτητή του οποίου ο τίτλος σπουδών πρώτου κύκλου από ίδρυμα της αλλοδαπής δεν έχει αναγνωρισθεί από το Διεπιστημονικό Οργανισμό Αναγνώρισης Τίτλων Ακαδημαϊκών και Πληροφόρησης (Δ.Ο.Α.Τ.Α.Π.), σύμφωνα με το ν. 3328/2005 (Α΄ 80).

7. Οι μεταπτυχιακοί φοιτητές μπορούν να αιτηθούν την έκδοση παραρτήματος διπλώματος.

8. Για τη συμμετοχή τους στο ΔΠΜΣ «Α.Λ.ΜΑ.» οι μεταπτυχιακοί φοιτητές δεν καταβάλλουν τέλη φοίτησης.

## **ΑΡΘΡΟ 9**

### **ΥΠΟΔΟΜΗ ΠΜΣ**

1. Για την εύρυθμη λειτουργία του ΠΜΣ θα διατεθούν αίθουσες διδασκαλίας και σεμιναρίων, αμφιθέατρα εξοπλισμένα με οπτικοακουστικά μέσα και εργαστήρια σε όλα τα Τμήματα/Σχολές που συμμετέχουν στο πρόγραμμα.

2. Η διοικητική και γραμματειακή υποστήριξη του ΠΜΣ γίνεται από τη Γραμματεία του ΠΜΣ, η οποία βρίσκεται στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ.

3. Η χρηματοδότηση του ΠΜΣ μπορεί να προέρχεται από:

α) τον προϋπολογισμό του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών και των συνεργαζόμενων για την οργάνωσή του φορέων σύμφωνα με το άρθρο 43,

β) τον προϋπολογισμό του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων,

γ) δωρεές, παροχές, κληροδοτήματα και κάθε είδους χορηγίες φορέων του δημόσιου τομέα, όπως οριοθετείται στην περίπτωση α' της παρ. 1 του άρθρου 14 του ν. 4270/2014 (Α' 143), ή του ιδιωτικού τομέα,

δ) πόρους από ερευνητικά προγράμματα,

ε) πόρους από προγράμματα της Ευρωπαϊκής Ένωσης ή άλλων διεθνών οργανισμών,

στ) μέρος των εσόδων των Ειδικών Λογαριασμών Κονδυλίων Έρευνας (Ε.Λ.Κ.Ε.)

ζ) κάθε άλλη νόμιμη πηγή.

4. Κατά τη λήξη της θητείας της ΣΕ, με ευθύνη του απερχόμενου Διευθυντή, συντάσσεται αναλυτικός απολογισμός του ερευνητικού και εκπαιδευτικού έργου και των λοιπών δραστηριοτήτων του ΠΜΣ, ο οποίος κατατίθεται στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ (παρ. 2, άρ.44, Ν.4485/2017). Ο εν λόγω απολογισμός με ευθύνη της Κοσμητείας αποστέλλεται αμελλητί στα μέλη της ΕΣΕ (παρ. 5, άρ.44, Ν.4485/2017).

5. Η εσωτερική και εξωτερική αξιολόγηση του ΠΜΣ θα γίνεται σύμφωνα με τις διατάξεις του άρθρου 44 του Ν.4485/2017.

## **ΑΡΘΡΟ 10**

### **ΑΝΑΘΕΣΗ ΔΙΔΑΣΚΑΛΙΑΣ/ΔΙΔΑΣΚΟΝΤΕΣ ΣΤΟ ΠΜΣ**

Οι διδάσκοντες του ΠΜΣ, προέρχονται, τουλάχιστον κατά 80%, από:

- μέλη Δ.Ε.Π. των συνεργαζόμενων Τμημάτων/Σχολών,

- μέλη Ε.Ε.Π., Ε.ΔΙ.Π. και Ε.Τ.Ε.Π. των συνεργαζόμενων Τμημάτων/Σχολών, κατόχους διδακτορικού διπλώματος εκτός κι αν το γνωστικό τους αντικείμενο είναι εξαιρετικής και αδιαμφισβήτητης ιδιαιτερότητας για το οποίο δεν είναι δυνατή ή συνήθης η εκπόνηση διδακτορικής διατριβής,

- ομότιμους καθηγητές (άρ. 69, Ν.4386/2016) και αφυπηρητήσαντα μέλη Δ.Ε.Π. των Τμημάτων/Σχολών που συμμετέχουν στο ΔΠΜΣ.

- διδάσκοντες σύμφωνα με το π.δ. 407/1980 (Α' 112),

- επιστήμονες αναγνωρισμένου κύρους είτε κάτοχους διδακτορικού διπλώματος είτε

υποψήφιους διδάκτορες είτε εξαιρετικής τεχνικής εμπειρίας, οι οποίοι μπορεί να απασχολούνται ως ακαδημαϊκοί υπότροφοι με απόφαση της Συνέλευσης και πράξη του Προέδρου του οικείου Τμήματος για τη διεξαγωγή διδακτικού και ερευνητικού έργου, καθοριζόμενου με τη σύμβαση που υπογράφεται μεταξύ του ακαδημαϊκού υποτρόφου και του Πρύτανη του οικείου ΑΕΙ. (παρ. 7, άρ. 29, Ν. 4009/2011).

Με αιτιολογημένη απόφαση της ΕΔΕ ανατίθεται διδασκαλία σε:

- μέλη ΔΕΠ άλλων Τμημάτων του ίδιου ή άλλου ΑΕΙ,
- ερευνητές από ερευνητικά κέντρα του αρ. 13Α, Ν. 4310/2014, της Ακαδημίας Αθηνών και του Ιδρύματος Ιατροβιολογικών Ερευνών της Ακαδημίας Αθηνών,
- επισκέπτες καταξιωμένους επιστήμονες από την ημεδαπή ή την αλλοδαπή, που έχουν θέση ή προσόντα καθηγητή ή ερευνητή σε ερευνητικό κέντρο, ή επιστήμονες αναγνωρισμένου κύρους με εξειδικευμένες γνώσεις ή σχετική εμπειρία στο γνωστικό αντικείμενο του ΔΠΜΣ,
- επισκέπτες μεταδιδακτορικούς ερευνητές, Έλληνες ή αλλοδαπούς νέους επιστήμονες, κάτοχους διδακτορικού διπλώματος (παρ. 7, άρ. 16, Ν.4009/2011)

ή γίνονται νέες προσλήψεις/συμβάσεις σύμφωνα με τα ανωτέρω (παρ. 1, 2, 5 & 6, αρ. 36, Ν.4485/2017).

Η ανάθεση διδασκαλίας μαθημάτων, σεμιναρίων και ασκήσεων του ΠΜΣ γίνεται ύστερα από εισήγηση της ΣΕ και έγκριση της ΕΔΕ.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Ο Πρύτανης

Μελέτιος-Αθανάσιος Δημόπουλος

## ΠΑΡΑΡΤΗΜΑ: Περιεχόμενο/Περιγραφή μαθημάτων

### - Αλγόριθμοι

Τεχνικές για ασυμπτωτική εκτίμηση υπολογιστικής πολυπλοκότητας, κριτήρια για επιλογή αλγορίθμων, πολυωνυμικοί αλγόριθμοι. Ουρές προτεραιότητας, σωροί, διαχείριση ξένων συνόλων, union-find. Επεξεργασία δεδομένων (ταξινόμηση, επιλογή, αναζήτηση). Μέθοδοι σχεδιασμού αποδοτικών αλγορίθμων: «διαίρει και βασίλευε», άπληστοι αλγόριθμοι, δυναμικός προγραμματισμός. Εφαρμογές σε προβλήματα γραφημάτων: αναζήτηση κατά βάθος, αναζήτηση κατά πλάτος, ελάχιστο συνδυαστικό δένδρο, συντομότερα μονοπάτια, μέγιστη ροή και ελάχιστη τομή. Πιθανοτικοί και προσεγγιστικοί αλγόριθμοι. Υπολογισιμότητα και πολυπλοκότητα. Κλάσεις υπολογιστικής πολυπλοκότητας και αναγωγές. Οι κλάσεις P και NP, NP-πλήρη προβλήματα. Κλάσεις χωρικής πολυπλοκότητας. Μαντεία και ιεραρχίες.

### - Προσεγγιστικοί αλγόριθμοι

Άπληστοι προσεγγιστικοί αλγόριθμοι. Τυχαιοκρατική στρογγυλοποίηση. Η μέθοδος του πρωτεύοντος-δυσικού. Επαναληπτική στρογγυλοποίηση. Γεωμετρικές εμβάπτισεις. Εφαρμογές σε προβλήματα όπως: Set Cover, Steiner Tree, Sparsest Cut. Ημιορισμένος Προγραμματισμός.

### - Συνδυαστική βελτιστοποίηση

Μαθηματική μοντελοποίηση προβλημάτων συνδυαστικής βελτιστοποίησης που εμφανίζονται σε πρακτικές εφαρμογές όπως των τηλεπικοινωνιακών δικτύων, των δικτύων υπολογιστών ή οδικών δικτύων, χρονοπρογραμματισμού, διαχείρισης πόρων, τοποθέτησης εξυπηρετητών και μεταφοράς. Γενικές τεχνικές επίλυσης προβλημάτων συνδυαστικής βελτιστοποίησης. Μέθοδοι διαχώρισης και αποτίμησης (Branch and Bound), ευριστικοί αλγόριθμοι, μεταευριστικοί αλγόριθμοι. Ανάδειξη των ορίων των αλγορίθμων και ανάπτυξη των πρόσφατων ερευνητικών εξελίξεων στο πεδίο. Δυναμικός Προγραμματισμός και προσεγγιστικοί αλγόριθμοι. Πολυωνυμικού χρόνου προσεγγιστικά σχήματα (PTAS, FPTAS). Μέθοδοι τοπικής αναζήτησης, PLS-completeness, δομές γειτονιών, εκθετικές γειτονίες αναζητούμενες πολυωνυμικά, προσεγγισσιμότητα. Σύνδεση των μεθόδων τοπικής αναζήτησης με τη θεωρία παιγνίων και τη θεωρία τοπίων .

### - Υπολογιστική πολυπλοκότητα

Ορισμός κλάσεων πολυπλοκότητας με βάση τις ακόλουθες παραμέτρους: α) Το υπολογιστικό μοντέλο (προγράμματα σε γλώσσα υψηλής βαθμίδος, μηχανές Turing κτλ.), β) Τον τρόπο υπολογισμού (ντετερμινιστικό, μη ντετερμινιστικό, πιθανοτικό κτλ.), γ) Τον περιορισμό των πόρων (πολυωνυμικός χρόνος, λογαριθμικός χώρος, σταθερός αριθμός επεξεργαστών, κτλ.). Μελέτη κλάσεων πολυπλοκότητας και των μεταξύ τους σχέσεων. Σχέσεις μεταξύ κλάσεων πολυπλοκότητας. Ιεραρχίες, αναγωγές και πληρότητα, NP - πλήρη προβλήματα, Co-NP και κλάσεις συναρτήσεων. Πιθανοτικοί υπολογισμοί και πολυπλοκότητα κυκλωμάτων, κρυπτογραφία, μονόδρομες συναρτήσεις. Πρωτόκολλα, προσεγγισσιμότητα και μη προσεγγισσιμότητα, P vs. NP. Ισομορφισμός, μαντεία, μονότονα κυκλώματα, παράλληλοι υπολογισμοί. Κλάσεις NC και RNC, λογαριθμικός χώρος, κλάση L. Προσεγγιστικοί αλγόριθμοι. Η πολυωνυμική ιεραρχία. Προβλήματα βελτιστοποίησης, μετρητικές κλάσεις, η κλάση #P. Πολυωνυμικός χώρος, PSPACE. Παίγνια και διαλογικά πρωτόκολλα, εκθετικός χρόνος κ.α.

### - Θεωρία αναδρομής

Σχέσεις, Συναρτήσεις, Γλώσσες, Προβλήματα, Επαγωγή, Αποδεικτικές τεχνικές. Μηχανές Turing. Turing Απαριθμήσιμες Γλώσσες. Παραλλαγές/Επεκτάσεις Μηχανών Turing. Γενικές γραμματικές. Πρωτογενώς Αναδρομικές Συναρτήσεις. Καθολικές Μηχανές Turing. Αυτοαναφορά, το θεώρημα της αναδρομής. Βαθμοί μη-αποφασισιμότητας.

– Θεωρία συνόλων

Επανάληψη βασικών εννοιών, αξιώματα της ZFC, διατακτικοί αριθμοί, υπερπεπερασμένη αναδρομή και επαγωγή. Πληθάριθμοι και πληθική αριθμητική. Το Αξίωμα της Επιλογής και το Αξίωμα της Θεμελίωσης. Το σύμπαν  $V$  των καλώς θεμελιωμένων συνόλων. Σχετικοποίηση και απολυτότητα πρωτοβάθμιων τύπων, το Θεώρημα της Ανάκλασης. Το κατασκευάσιμο σύμπαν  $L$  του Godel. Η (σχετική) συνέπεια του Αξιώματος της Επιλογής και της Υπόθεσης του Συνεχούς με τα υπόλοιπα αξιώματα της ZFC συνολοθεωρίας.

– Λογική

Σύντομη ανασκόπηση Προτασιακής Λογικής. Πρωτοτάξια Λογική. Αλήθεια και μοντέλα. Τυπικές αποδείξεις (συναγωγές). Θεώρημα αξιοπιστίας και πληρότητας. Ερμηνείες (στοιχειώδης θεωρία μοντέλων). Μη συμβατική ανάλυση. Μη-διαγνωσιμότητα και μη πληρότητα. Αναδρομικές συναρτήσεις. Αριθμητικοποίηση σύνταξης. Θεωρία αριθμών. Πρώτο και δεύτερο θεώρημα μη πληρότητας.

– Θεωρία γραφημάτων

Ισομορφισμοί, αυτομορφισμοί, ομάδες αυτομορφισμών. Μετασχηματισμοί και σχέσεις σε γραφήματα. Βαθμοί, πυκνότητα, ελαχιστομέγιστο θεώρημα εκφυλισμού. Μονοπάτια, κύκλοι, διάμετρος, ακτίνα, κέντρο, απόκεντρο, περιφέρεια, περίμετρος. Συνεκτικότητα, δισυνεκτικά γραφήματα, το Θεώρημα του Menger, Το Θεώρημα του Tutte για την 3-συνεκτικότητα. Δάση και δέντρα, δεντροπαράγοντες. Επίπεδα γραφήματα, τοπολογικός ισομορφισμός, δυικά γραφήματα, πυκνότητα και επιπεδότητα, Το θεώρημα του Kuratowski. Χρωματισμοί γραφημάτων, Χρωματικότητα και εκφυλισμός, Το θεώρημα του Heawood, Το θεώρημα του Erdős για την περιφέρεια και τον χρωματικό αριθμό. Η εικασία του Hadwiger. Κλίκες, ανεξάρτητα σύνολα, Αριθμοί Ramsey. Καλύμματα, ταιριάσματα, Τέλεια γραφήματα. Το θεώρημα του Lovasz για τα τέλεια γραφήματα, Το θεώρημα του Dilworth. Μονοπάτια Euler και Hamilton. Η πιθανοτική τεχνική, τυχαία γραφήματα. Ακραία γραφοθεωρία, τοπολογική θεωρία γραφημάτων. Η θεωρία των ελασσόνων γραφημάτων.

– Στοχαστικές διαδικασίες

Μαρκοβιανές αλυσίδες διακριτού χρόνου: Βασικοί ορισμοί. Υπολογισμοί για τις μεταβατικές κατανομές. Κατάταξη καταστάσεων και οριακή συμπεριφορά αδιαχώριστων αλυσίδων. Υπολογισμοί στάσιμων κατανομών. Αντιστρεψιμότητα Μαρκοβιανών αλυσίδων και εφαρμογές. Πιθανότητες και μέσοι χρόνοι απορρόφησης για διαχωρίσιμες Μαρκοβιανές αλυσίδες. Η στοχαστική διαδικασία Poisson: Υπολογισμοί και ιδιότητες. Μη-ομογενής και σύνθετη διαδικασία Poisson. Μαρκοβιανές αλυσίδες συνεχούς χρόνου: Βασικοί ορισμοί. Υπολογισμοί για τις μεταβατικές κατανομές. Κατάταξη καταστάσεων και οριακή συμπεριφορά αδιαχώριστων αλυσίδων. Υπολογισμοί στάσιμων κατανομών. Αντιστρεψιμότητα Μαρκοβιανών αλυσίδων και εφαρμογές. Πιθανότητες και μέσοι χρόνοι απορρόφησης για διαχωρίσιμες Μαρκοβιανές αλυσίδες. Ανανεωτική Θεωρία: Εισαγωγή, στοιχειώδεις ανανεωτικό θεώρημα, ανανεωτική συνάρτηση και ανανεωτική εξίσωση, βασικό ανανεωτικό θεώρημα. Υπολειπόμενος και παρελθών χρόνος ανανέωσης. Εφαρμογές. Martingales διακριτού χρόνου: Βασικές ιδιότητες. Θεώρημα επιλεκτικής στάσης. Σύγκλιση martingales. Εφαρμογές. Κλαδωτές διαδικασίες. Τυχαίοι περίπατοι.

- Συνδυαστική

Απαρίθμηση και γεννήτριες συναρτήσεις, μεταθέσεις και πολυώνυμα Euler, εκθετικές γεννήτριες συναρτήσεις, ο εκθετικός τύπος, ο τύπος αντιστροφής του Lagrange και εφαρμογές στην απαρίθμηση δένδρων. Η αρχή εγκλεισμού-αποκλεισμού και εφαρμογές. Μερικώς διατεταγμένα σύνολα, η συνάρτηση του Möbius, αντιστροφή Möbius, semimodular και γεωμετρικοί σύνδεσμοι, το θεώρημα NBC του Rota, το χαρακτηριστικό πολυώνυμο, εφαρμογές σε παρατάγματα υπερεπιπέδων και χρωματισμούς γραφημάτων, το πολυώνυμο ζήτα μιας μερικής διάταξης. Στοιχεία τοπολογικής συνδυαστικής, το σύμπλεγμα μιας μερικής διάταξης και η χαρακτηριστική Euler, μονοπλεκτικά και κυτταρικά συμπλέγματα, αποφλοιώσιμα (shellable) και Cohen-Macaulay συμπλέγματα και μερικώς διατεταγμένα σύνολα, μερικές διατάξεις του Euler και οι εξισώσεις Dehn-Sommerville. Ρητές γεννήτριες συναρτήσεις, θεωρία των P-διαμερίσεων και P-πολυώνυμα Euler, quasi-συμμετρικές συναρτήσεις.

- Ακραία συνδυαστική

Θεωρήματα αποκλεισμού γραφημάτων, η εικασία του Hadwiger, το λήμμα κανονικότητας του Szemerédi, το θεώρημα Erdős-Ko-Rado, το θεώρημα του Turán, το θεώρημα του Sperner, Θεωρήματα Ramsey, το λήμμα Sauer-Shelah, το θεώρημα Kruskal-Katona, ισοπεριμετρικές ανισότητες.

- Άλγεβρα και κρυπτογραφία:

Μεταθετικοί Δακτύλιοι και ομάδες Κρυπτοσυστήματα βασισμένα σε μεταθετικούς Δακτυλίους και ομάδες. Κρυπτανάλυση Μη-μεταθετικές ομάδες, ελεύθερες ομάδες, παραστάσεις ομάδων. Μη-μεταθετική κρυπτογραφία.

- Αλγοριθμικά θέματα κοινωνικών δικτύων

Βασικές έννοιες, παραδείγματα, εφαρμογές. Αναζήτηση στον παγκόσμιο ιστό, σύγκλιση σε γραμμικά συστήματα. Τυχαία δίκτυα και φαινόμενα κατωφλίου, μοντέλα δημιουργίας κοινωνικών δικτύων, κατανομή βαθμών κορυφών σε κοινωνικά δίκτυα. Μοντέλα διάχυσης πληροφορίας, μοντέλα επίδρασης από γείτονες, μεγιστοποίηση επίδρασης, τιμολόγηση προϊόντων σε κοινωνικά δίκτυα, επιδημικά φαινόμενα, γραμμικές και συνεξελικτικές (coevolutionary) δυναμικές διαμόρφωσης απόψεων (opinion dynamics). Φαινόμενα «μικρού κόσμου», κατανεμημένη αναζήτηση και δρομολόγηση με χρήση τοπικής πληροφορίας. Βασικές έννοιες θεωρίας παιγνίων και αλγοριθμικής θεωρίας παιγνίων, ισορροπία Nash, σύγκλιση σε ισορροπία, τμήμα της αναρχίας και τμήμα της σταθερότητας. Μοντέλα σχηματισμού δικτύων από ιδιοτελείς οντότητες. Αγορές, διαπραγμάτευση και ισχύς σε ένα κοινωνικό δίκτυο, externalities σε αγορές αγαθών και σε δημοπρασίες διαφημιστικού χώρου στο διαδίκτυο. Διάχυση πληροφορίας και μάθηση σε κοινωνικά δίκτυα.

- Αλγοριθμική θεωρία γραφημάτων

Επισκόπηση βασικών εννοιών της θεωρίας γραφημάτων. Βασικοί αλγόριθμοι δέντρων και αποστάσεων σε γραφήματα. Άπληστοι αλγόριθμοι σε γραφήματα. Ταιριάσματα. Ειδικές κλάσεις γραφημάτων: δομικές ιδιότητες και αλγόριθμοι. Διαχωριστές σε γραφήματα, δυναμικός προγραμματισμός. Δενδροπλάτος και Μοναδική Δευτεροβάθμια λογική. Τεχνικές σχεδιασμού παραμετρικών αλγόριθμων σε γραφήματα. Προσεγγιστικοί

αλγόριθμοι σε γραφήματα. Πιθανοτικοί αλγόριθμοι σε γραφήματα, τεχνικές αποτυχαίωσης.

#### - Αλγοριθμική θεωρία παιγνίων

Ισορροπία Nash σε παίγνια μηδενικού αθροίσματος και σε παίγνια μη-μηδενικού αθροίσματος, θεωρήματα σταθερού σημείου, υπολογισμός ισορροπίας Nash, η κλάση PPAD, προσεγγιστικοί αλγόριθμοι για τον υπολογισμό ισορροπίας Nash. Παίγνια συμφόρησης και ιδιοτελής δρομολόγηση, αμιγείς ισορροπίες Nash και συναρτήσεις δυναμικού, η κλάση PLS, τίμημα της αναρχίας και τίμημα της σταθερότητας, άνω και κάτω φράγματα, βελτίωση του τιμήματος της αναρχίας (διόδια, πολιτικές Stackelberg, μηχανισμοί συντονισμού, το παράδοξο του Braess). Σχεδιασμός μηχανισμών, κοινωνική επιλογή, θεωρήματα Arrow και Gibbard-Satterthwaite, φιλαλήθεις μηχανισμοί. Μηχανισμοί χωρίς χρηματικά ανταλλάγματα, παίγνια χωροθέτησης, ο χαρακτηρισμός Moulin, ευσταθή ταιριάσματα, top-trading-cycles. Δρομολόγηση σε ιδιοτελείς μηχανές. Δημοπρασίες, θεώρημα Myerson, μηχανισμός VCG, συνδυαστικές δημοπρασίες, multiplicative weight updates και μηχανισμοί με posted prices, άμεσοι μηχανισμοί και το πρόβλημα επιλογής γραμματέως. Φιλαλήθεια και πολυωνυμική προσεγγισσιμότητα για προβλήματα μεγιστοποίησης κοινωνικής ωφέλειας. Μη φιλαλήθεις μηχανισμοί, smooth μηχανισμοί και το τίμημα της αναρχίας, επικοινωνιακή πολυπλοκότητα συνδυαστικών δημοπρασιών, κάτω φράγματα στο τίμημα της αναρχίας από υπολογιστικά κάτω φράγματα στην προσεγγισσιμότητα.

#### - Αλγόριθμοι δικτύων και πολυπλοκότητα

Το αντικείμενο του μαθήματος είναι η μελέτη αλγοριθμικών μεθόδων και η ανάλυση πολυπλοκότητας για υπολογιστικά προβλήματα και θεμελιώδεις διαδικασίες που σχετίζονται με δίκτυα, κυρίως υπολογιστών και επικοινωνιών. Ορισμένα από τα θέματα που θα καλυφθούν: Αποδοτικοί αλγόριθμοι (ακριβείς, προσεγγιστικοί, πιθανοτικοί) για γραφοθεωρητικά προβλήματα βελτιστοποίησης δικτύων: Vertex Cover, Traveling Salesman Problem, Steiner tree, Maximum Flow, Matching, Edge Coloring, Multicommodity Flow, Facility Location, Multicut, k-Center, Clustering, Scheduling. Κατανεμημένα πρωτόκολλα: εκλογήαρχηγού, broadcasting, gossiping, byzantine agreement, secretsharing. Ασύρματα ad hoc δίκτυα. Συγχρονισμένοι και ασύγχρονοι αλγόριθμοι. Fault tolerance. Προβλήματα αυτόνομων οντοτήτων, εξερεύνηση δικτύων, προβλήματα συνάντησης (rendezvous), εντοπισμός βλαβών σε δίκτυα. Πρωτόκολλα δρομολόγησης, compact routing, geometric routing. Ειδικά θέματα: χρονοδρομολόγηση (scheduling), δρομολόγηση και ανάθεση συχνοτήτων σε οπτικά δίκτυα, αλγόριθμοι πλοήγησης, προγραμματισμός δρομολογίων οχημάτων. Στοιχεία θεωρίας παιγνίων: σημεία ισορροπίας Nash, "κόστος της αναρχίας". Εγχειριστική δρομολόγηση σε κλασικά, ασύρματα και οπτικά δίκτυα. Παίγνια συμφόρησης. Σύγκλιση σε ισορροπίες Nash και σχεδίαση μηχανισμών.

#### - Αλγόριθμοι στη δομική βιοπληροφορική

Γονιδίωμα και πρωτεΐνες, πρωτοταγής, δευτεροταγής και τριτοταγής μοριακή δομή. Πειραματικά δεδομένα NMR και κρυσταλλογραφίας ακτίνων X. Σύγκριση και στοίχιση ακολουθιών, στοίχιση με κενά. Δυναμικός προγραμματισμός. Αναζήτηση και χώρος μοριακών διαμορφώσεων (C-space). Γεωμετρία των αποστάσεων. Κινηματική των μορίων, Ευκλείδειοι μετασχηματισμοί Ομοιότητες και αναγνώριση μοριακών δομών, πρόσδεση (docking) μορίου σε υποδοχέα: μοριακές επιφάνειες (α-σχήματα, τριγωνοποίηση Delaunay), δομές γεωμετρικών δεδομένων, γεωμετρικός κατακερματισμός Εξόρυξη δεδομένων, αναζήτηση και συσταδοποίηση μοριακών δεδομένων.



– Ανάλυση Γεωμετρικών δεδομένων

Το μάθημα εστιάζει σε γεωμετρικούς πιθανοκρατικούς, προσεγγιστικούς, και ευριστικούς αλγόριθμους σε υψηλή διάσταση που αντιμετωπίζουν την "κατάρα της διάστασης" (curse of dimensionality). Δειγματοληψία μέσω τυχαίων περιπάτων σε κυρτές και μη-κυρτές περιοχές. Υπολογισμός όγκου κυρτού σώματος. Αναπαράσταση γεωμετρικών αντικειμένων. Δομές γεωμετρικών δεδομένων σε γενική διάσταση, αναζήτηση περιοχής, εύρεση πλησιέστερου γείτονα με δενδρικές δομές, πιθανοκρατικούς πίνακες κατακερματισμού, και τυχαιοκρατική εμβύθιση δεδομένων. Εξόρυξη δεδομένων και αλγόριθμοι συσταδοποίησης (clustering). Εφαρμογές στη βιοπληροφορική και την επεξεργασία εικόνας.

– Αναλυτική συνδυαστική

Συνδυαστικές δομές και εισαγωγή στην Συμβολική Μέθοδο, ετικετωμένες δομές και εκθετικές γεννήτριες συναρτήσεις, συνδυαστικές παράμετροι και πολυμεταβλητές γεννήτριες συναρτήσεις, μιγαδική ανάλυση και μερομορφική ασυμπτωτική, ανάλυση ιδιομορφιών γεννητριών συναρτήσεων, το θεώρημα Flajolet-Odlitzko και εφαρμογές, ασυμπτωτική σαγματικών σημείων.

– Απεικόνιση γραφημάτων

Απεικόνιση γραφημάτων και εφαρμογές. Απεικόνιση επιπέδων γραφημάτων. Απεικόνιση δένδρων και Series-Parallel γραφημάτων. Απεικόνιση βασιζόμενη σε νόμους της φυσικής. Ιεραρχική απεικόνιση γραφημάτων. Ορθογώνια απεικόνιση γραφημάτων. Τρισδιάστατη απεικόνιση γραφημάτων. Δυναμική απεικόνιση γραφημάτων. Πακέτα λογισμικού.

– Απειροσυνδυαστική

Άπειρα γραφήματα και δέντρα, Θεωρία Ramsey σε άπειρα σύνολα, Συνδυαστική του συνεχούς, Εφαρμογές στους χώρους Banach.

– Διακριτή ανάλυση

Διακριτή αρμονική ανάλυση: αναπτύγματα Fourier-Walsh, επιρροές μεταβλητών, ανισότητες τύπου Sobolev και ισοπεριμετρικές ανισότητες, ανισότητες συγκέντρωσης. Ανάλυση Boolean συναρτήσεων. Εμφυτεύσεις πεπερασμένων μετρικών χώρων σε χώρους με νόρμα. Johnson-Lindenstrauss. Ευκλείδειες εμφυτεύσεις: άνω και κάτω φράγματα. Expanders και το θεώρημα Linial-London-Rabinovich. Θεωρήματα τύπου Ramsey: σχεδόν ισομετρικές εμφυτεύσεις και το μη γραμμικό θεώρημα Dvoretzky. Θεώρημα επέκτασης του Kirsbraum. Επέκταση Lipschitz συναρτήσεων με τιμές σε χώρους Banach. Φασματική θεωρία γραφημάτων. Αγωγιμότητα, Λαπλασιανή και ανισότητα Cheeger. Τυχαίοι περίπατοι σε γραφήματα. Expanders: κατασκευές και ιδιότητες. Φασματική αραιοποίηση – η μέθοδος των διαπλεκόμενων οικογενειών. Άλλα θέματα: Διάσταση Varnik-Chervonenkis και θεωρία μάθησης. Αραιή ανακατασκευή. Θεωρία ανισοκατανομής.

– Δομική πολυπλοκότητα

Διαδραστικές αποδείξεις. Πιθανοτικά ελέγξιμες συναρτήσεις. Το θεώρημα PCP. Το θεώρημα του Razboron. Πολυπλοκότητα προβλημάτων μέτρησης. Τα θεωρήματα των Valliant και Toda. Προσεγγιστική μέτρηση. Μέτρο και διάσταση σε κλάσεις πολυπλοκότητας. Ψευδοτυχειότητα. Γραφήματα εξαπλωτές. Μονόδρομες συναρτήσεις. Αποτυχειοποίηση (ομοιόμορφη και μη). Πολυπλοκότητα και υπολογισμός σε πραγματικούς αριθμούς, πολυπλοκότητα αποδείξεων, επικοινωνιακή πολυπλοκότητα, παραμετρική πολυπλοκότητα, πολυπλοκότητα μέσου όρου.

– Δομική θεωρία γραφημάτων

Τέλεια γραφήματα. Ασθενές και ισχυρό θεώρημα τέλειων γραφημάτων. Αποσυνθέσεις τέλειων γραφημάτων. Το λήμμα κανονικότητας του Szemerédi και οι εφαρμογές του. Θεωρία καλής διάταξης σε γραφήματα. Δενδροπλάτος. Θεωρήματα δέσμωσης. Δομικά θεωρήματα αποκλεισμού ελασσόνων. Ασθενές και ισχυρό διμικό θεώρημα των ελασσόνων γραφημάτων. Το θεώρημα Roberson και Seymour. Παράμετροι πλάτους. Θεωρήματα αραιότητας. Ιδιότητες Erdős–Rósa. Παρεμποδίσεις και ελαχιστο μέγιστα θεωρήματα. Παίγνια ανίχνευσης σε γραφήματα. Αλγοριθμικές εφαρμογές της δομικών θεωρημάτων της γραφοθεωρίας.

– Δυναμικός προγραμματισμός

Εισαγωγή στο στοχαστικό δυναμικό προγραμματισμό. Το μοντέλο της Μαρκοβιανής Διαδικασίας Αποφάσεων. Προβλήματα πεπερασμένου ορίζοντα. Αναδρομική επίλυση. Προβλήματα άπειρου ορίζοντα με το κριτήριο του συνολικού αποπληθωρισμένου κόστους. Προβλήματα άπειρου ορίζοντα με το κριτήριο του συνολικού κόστους (θετικός και αρνητικός δυναμικός προγραμματισμός). Προβλήματα βέλτιστου σταματήματος. Προβλήματα άπειρου ορίζοντα με το κριτήριο του μέσου κόστους.

– Ειδικά θέματα αλγορίθμων

Στο μάθημα αυτό θα διδάσκονται σύγχρονα θέματα αλγορίθμων που δεν καλύπτονται από τα υπόλοιπα μαθήματα του προγράμματος.

– Ειδικά θέματα διακριτών μαθηματικών

Στο μάθημα αυτό θα διδάσκονται σύγχρονα θέματα διακριτών μαθηματικών που δεν καλύπτονται από τα υπόλοιπα μαθήματα του προγράμματος.

– Ειδικά θέματα λογικής

Στο μάθημα αυτό θα διδάσκονται σύγχρονα θέματα λογικής που δεν καλύπτονται από τα υπόλοιπα μαθήματα του προγράμματος.

– Επιχειρησιακή έρευνα

Εισαγωγή στο Γραμμικό Προγραμματισμό. Μέθοδος Simplex – Δυϊκότητα. Εισαγωγή στον Ακέραιο Προγραμματισμό, Μοντελοποιήσεις. Εισαγωγή στο μη-Γραμμικό Προγραμματισμό. Συνθήκες βελτιστοποίησης. Εφαρμογές: Προβλήματα βελτιστοποίησης σε δίκτυα, θεωρία ελέγχου αποθεμάτων

– Θεωρία αποδείξεων

Αποδεικτικά συστήματα: φυσική απαγωγή, συστήματα Hilbert, συστήματα ακολουθητών του Gentzen. Η έννοια της τομής, θεωρήματα απαλοιφής των τομών και εφαρμογές. Κανονικοποίηση και αριθμητικά φράγματα στην απαλοιφή των τομών, δομή των αποδείξεων χωρίς τομές. Ισοδυναμία Curry-Howard-de Bruijn. Κανονικοποίηση στη φυσική απαγωγή. Εισαγωγή στη Γραμμική Λογική. Αριθμητική του Peano και ανάλυση των αποδείξεων με διατακτικούς αριθμούς.

– Θεωρία γραμμικού προγραμματισμού

Κυρτά σύνολα, πολύεδρα, κώνοι. Θεώρημα Minkowski-Weyl. Λήμματα Farkas, δυϊκότητα. Όψεις και έδρες πολυέδρων. Διάσταση. Ελαχιστικές αναπαραστάσεις. Total unimodularity. Ολική Δυϊκή Ακεραιότητα. Τα πολύτοπα των ταιριασμάτων και των συνδετικών δένδρων. Εκτεταμένες Διατυπώσεις.

– Θεωρία κόμβων και εφαρμογές

Κόμβοι και σύνδεσμοι, διαγράμματα και προσανατολισμοί, δράσες Reidemeister, συμμετρίες, χρωματισμοί κόμβων, πολυώνυμα Alexander, bracket και Jones, συνθέσεις προσανατολισμένων κόμβων, κοτσίδες και πλεξούδες, κουβαριάσματα, γένος, ομάδες κόμπων, εφαρμογές στην τοπολογία πολλαπλοτήτων, στην μοριακή βιολογία και στη Φυσική.

– Θεωρία μητροειδών

Η έννοια της ανεξαρτησίας σε γραφήματα, σε διανυσματικούς χώρους και στην θεωρία διαπεράσεων. Ορισμός μητροειδούς. Βάσεις και Κυκλώματα. Δυϊκότητα. Τάξη μητροειδούς. Κρυπτομορφισμοί. Άπληστοι αλγόριθμοι. Αναπαραστασιμότητα. Ελάσσονα μητροειδή. Είδη συνεκτικότητας μητροειδών. Θεωρήματα αποσύνθεσης μητροειδών (θεώρημα Tutte και θεώρημα Seymour). Αλγόριθμοι σε μητροειδή. Μητροειδή προσεσημασμένων γραφημάτων.

– Θεωρία μοντέλων

Εισαγωγικές έννοιες της θεωρίας μοντέλων. Απαλοιφή ποσοδεικτών. Πληρότητα, συμπάγεια. Θεώρημα Παράλειψης Τύπων. Θεώρημα Παρεμβολής του Craig. Στοιχειώδεις επεκτάσεις. Στοιχειώδεις αλυσίδες. Συναρτήσεις Skolem. Indiscernibles (αδιάκριτα). Model completeness (μοντελοθεωρητική πληρότητα). Υπεργινόμενα. Κορεσμένα μοντέλα. Ειδικά μοντέλα. Θεωρήματα διατήρησης.

– Θεωρία ουρών αναμονής

Περιγραφή, βασικές έννοιες και γενικά αποτελέσματα. Απλές Μαρκοβιανές ουρές (τύπου γέννησης-θανάτου). Μαρκοβιανές ουρές και η μέθοδος των φάσεων. Συμμετρικές ουρές. Ανοικτά και κλειστά δίκτυα Μαρκοβιανών ουρών (Δίκτυα Jackson, δίκτυα με γενικές διαδρομές). Δίκτυα σχεδόν αντιστρέψιμων ουρών. Οι M/G/1 και GI/M/1 ουρές και παραλλαγές και οι επεκτάσεις τους. Η GI/G/1 ουρά. Προσεγγιστικές μέθοδοι.

– Θεωρία παιγνίων

Βασικά στοιχεία θεωρίας: Θεώρημα Minimax, εξισωτικές στρατηγικές, Θεώρημα Nash και Nikaido-Isoda. Μη πεπερασμένα παιχνίδια, συνεχή παιχνίδια πάνω σε συμπαγή σύνολα. (Στοχαστικά παιχνίδια 0-αθροίσματος. Δι-πινακοπαιχνίδια (αλγόριθμος Lemke-Howson). Εξελικτική ευστάθεια). Εφαρμογές στα οικονομικά (ολιγοπώλια, παιχνίδια αγοραπωλησιών). Μπεϋζιανά παιχνίδια. (Συσχετισμένη ισορροπία. Αρχή της αποκάλυψης. Επαναλαμβανόμενα παιχνίδια πεπερασμένου και άπειρου ορίζοντα.)

– Θεωρία πληροφορίας

Μέτρα πληροφορίας. Εντροπία διακριτών πηγών. Κυρτότητα. Μονότονες και συνεχεία ιδιότητες. Αμοιβαία πληροφορία. Απόσταση KL. Πίνακες Toeplitz και το θεώρημα του Szego. Χωρητικότητα διαύλου. Δίαυλοι Gauss. Συμπύεση πληροφορίας. Θεωρήματα Shannon-McMillan και Birkhoff-Khinchine. Θεωρία κωδικοποίησης. Κώδικες Shannon. Κώδικες Huffman. Κωδικοποίηση Lempel-Ziv.

– Κρυπτογραφία

Μελέτη σύγχρονων κρυπτογραφικών πρωτοκόλλων με έμφαση στην τεκμηρίωση ιδιοτήτων ασφάλειας. Η ύλη περιλαμβάνει σχήματα δέσμευσης, coin flipping, ανταλλαγή κλειδιού Diffie-Hellman, ψηφιακές υπογραφές, μηδενική γνώση, κρυπτογραφία δημόσιου κλειδιού (RSA, ElGamal), secret sharing, κρυπτονομίσματα.

– Κυρτή ανάλυση

Κυρτά σύνολα. Κυρτές και κοίλες συναρτήσεις, Συνδυαστική γεωμετρία: θεωρήματα Καραθεοδωρή, Helly, Radon και Εφαρμογές. Μετρική προβολή. Φέροντα υπερεπίπεδα. Διαχωριστικά θεωρήματα. Διϊσμός. Ακραία και εκτεθειμένα σημεία. Το θεώρημα των Minkowski-Krein-Milman. Εφαρμογές. Απόσταση Banach-Mazur. Το θεώρημα του John. Ανισότητα Brunn-Minkowski. Ισοπεριμετρικά προβλήματα. Συμμετρικοποίηση κατά Steiner. Γεωμετρικές ανισότητες. Όγκος στις μεγάλες διαστάσεις. Ανισότητα Brascamp-Lieb και γεωμετρικές εφαρμογές. Ειδικά θέματα: γεωμετρία των αριθμών, χώροι πεπερασμένης διάστασης με νόρμα, αλγοριθμική κυρτή γεωμετρία, γεωμετρικές πιθανότητες.

– Λάμδα λογισμός

Καθαρός λ-λογισμός: β-αναγωγή, η-αναγωγή, θεώρημα Church-Rosser. Αναπαράσταση των μερικών αναδρομικών συναρτήσεων στο λ-λογισμό, θεωρήματα σταθερού σημείου, θεώρημα αναποκρισιμότητας Scott-Curry. λ-λογισμός με τύπους: Τυποποίηση των όρων του λ-λογισμού, το σύστημα Corro-Dezani. Θεωρήματα της κανονικοποίησης, τυποποίηση κανονικοποιήσιμων όρων, πεπερασμένες αναπτύξεις, standard αναγωγή. Θεώρημα του Bohm, δέντρα του Bohm. Συνδυαστική Λογική, ισοδυναμία με λ-λογισμό. Μοντέλα του λ-λογισμού (κατασκευή του μοντέλου του Scott). Το σύστημα F του Girard. Ρητές αντικαταστάσεις.

– Μοντέλα υπολογισμού, τυπικές γλώσσες και αυτόματα

Υπολογισιμότητα: Λογική θεμελίωση πληροφορικής. Ιστορική αναδρομή στο πρόβλημα αποκρισιμότητας μαθηματικών προτάσεων, επιλυσιμότητας ή υπολογισιμότητας προβλημάτων με μηχανιστικό, δηλαδή αλγοριθμικό, τρόπο. Απλά ισοδύναμα υπολογιστικά μοντέλα: μηχανές Turing, προγράμματα WHILE. Επαγωγή και αναδρομή, κωδικοποίηση και σημασιολογία. Θεωρία σταθερού σημείου. Μαντεία και Αριθμητική ιεραρχία. Θεωρία αυτομάτων και τυπικών γραμματικών: Πεπερασμένα αυτόματα. Κανονικά σύνολα και ισοδύναμοι χαρακτηρισμοί. Ιεραρχία Chomsky. Αποδείξεις για το εάν  $LEC$  ή  $L \notin C$ . Εφαρμογές στο συντακτικό γλωσσών προγραμματισμού. Πολυπλοκότητα: Σχέσεις μεταξύ κλάσεων πολυπλοκότητας. Αναγωγές και Πληρότητα. Πολυωνυμική ιεραρχία. Πιθανοτικές, διαλογικές και μετρητικές κλάσεις. Παραμετρική πολυπλοκότητα. Κβαντική πολυπλοκότητα.

– Παραμετρική πολυπλοκότητα και αλγόριθμοι

Εισαγωγή στην παραμετρική πολυπλοκότητα, ισοδυναμίες μέτρων πολυπλοκότητας. Αλγοριθμικές τεχνικές: φραγμένα δέντρα αναζήτησης, επαναληπτική συμπίεση, άπληστος εντοπισμός, αναδρομική κατανόηση, σημαντικοί διαχωριστές, κανόνες αναγωγής, η τεχνική της ασήμαντης κορυφής. Πιθανοτικές μέθοδοι, πυρηνοποίηση, πυρηνοποίηση Turing. Δεντροπλάτος, το θεώρημα του Courcelle, δυναμικός προγραμματισμός, διδιαστατότητα, εναλλακτικές παράμετροι πλάτους, παραμετρικές αναγωγές, μετααλγοριθμικά θεωρήματα. Οι κλάσεις para-NP και XP, η W-ιεραρχία: FPT,  $W[1], W[2], \dots, W[SAT], W[P]$  και ορισμοί της μέσω κυκλωμάτων, λογικών τύπων και μοντέλων μηχανών Turing. Κάτω φράγματα και

υπόθεση εκθετικού χρόνου, ισχυρή υπόθεση εκθετικού χρόνου, παραμετρική πολυπλοκότητα πολυωνυμικά επιλύσιμων προβλημάτων.

– Πιθανοτικές μέθοδοι

Εισαγωγή στην τυχαιότητα, Η πιθανοτική μέθοδος: η πρώτη ροπή, η μέθοδος της δεύτερης ροπής. Προβλήματα τοποθέτησης σφαιρών σε δοχεία. Φράγματα Chernoff. Το τοπικό λήμμα του Lovász, Martingales και εφαρμογές. Τυχαία γραφήματα. Οι ανισότητες Janson. Η ανισότητα του Azuma. Τυχαίο περίπατο. Αλυσίδες Markov. Τυχαίο πίνακες, κατωφλικές συμπεριφορές, οριακά θεωρήματα.

– Προσθετική συνδυαστική

Η προσθετική συνδυαστική συνδυάζει στοιχεία εργοδικής θεωρίας, αρμονικής ανάλυσης, θεωρίας αριθμών, και θεωρίας πιθανοτήτων. Σε γενικές γραμμές προσπαθεί να ταξινομήσει υποσύνολα ενός δεδομένου πεδίου με καλή συμπεριφορά σε σχέση με κάποιο δυαδικό τελεστή. Η ύλη περιλαμβάνει: το θεώρημα του Roth, το θεώρημα των Freiman-Ruzsa-Sanders, το θεώρημα του Gowers, θεωρήματα αποσύνθεσης και συνδυαστικοί παράγοντες, το θεώρημα των Green-Tao, φόρμουλες αθροισμάτων-γινομένων, το θεώρημα του Szemerédi για αριθμητικές προόδους.

– Σημασιολογία γλωσσών προγραμματισμού

Δηλωτική, αξιωματική και μηχανική σημασιολογία. Ρόλος της σημασιολογίας στη σχεδίαση και ανάπτυξη σύγχρονων γλωσσών προγραμματισμού. Σημασιολογία διαδικαστικών γλωσσών. Πλήρεις σχέσεις μερικής διάταξης (cpos). Μονοτονικές και Συνεχείς Συναρτήσεις. Θεώρημα Σταθερού Σημείου του Kleene. Σημασιολογία συναρτησιακών γλωσσών με αναδρομικούς ορισμούς και συναρτήσεις υψηλής τάξης. Σημασιολογία λογικών προγραμμάτων. Μοντέλα Herbrand. Πλήρη πλέγματα και θεώρημα σταθερού σημείου των Knaster-Tarski. Θεώρημα ελάχιστου μοντέλου Herbrand. Σημασιολογία της Άρνησης στο Λογικό Προγραμματισμό. Στρωματοποιημένα και τοπικά στρωματοποιημένα προγράμματα. Καλώς-θεμελιωμένη σημασιολογία (well-founded semantics). Σημασιολογία σταθερού μοντέλου (stable model semantics). Λογικός προγραμματισμός υψηλής τάξης. Θεωρία άπειρων παιγνίων και εφαρμογές στη σημασιολογία γλωσσών προγραμματισμού.

– Στοχαστικά μοντέλα

Ανανεωτικές διαδικασίες με κόστη: Ορισμοί και παραδείγματα. Μέσος ρυθμός κόστους και υπολογισμοί με το στοιχειώδες ανανεωτικό θεώρημα με κόστη. Αναγεννητικές διαδικασίες και υπολογισμοί μέσου ρυθμού κόστους. Εφαρμογές. Μαρκοβιανές αλυσίδες με κόστη: Ορισμοί και παραδείγματα. Υπολογισμοί μέσους ρυθμούς κόστους. Εφαρμογές. Εισαγωγή στο Δυναμικό προγραμματισμό: Βασική θεωρία για προβλήματα πεπερασμένου ορίζοντα. Εφαρμογές με επαγωγικά επιχειρήματα. Εφαρμογές με το επιχείρημα της ανταλλαγής. Προβλήματα βέλτιστου σταματήματος. Εισαγωγή στις Ουρές Αναμονής: Περιγραφή, ονοματολογία και μέτρα απόδοσης. Βασικά αποτελέσματα. Ανάλυση μέσης τιμής. Μαρκοβιανές ουρές. Βέλτιστος σχεδιασμός συστημάτων. Εισαγωγή στη Στοχαστική Θεωρία Ελέγχου Αποθεμάτων: Το μοντέλο του εφημεριδοπώλη, μοντέλα πολλών περιόδων. Στοιχεία Θεωρίας Παιγνίων: Παιχνίδια σε κανονική μορφή. Σημείο στρατηγικής ισορροπίας (ΣΣΙ ή σημείο Nash). Πεπερασμένα παιχνίδια δύο παικτών μηδενικού αθροίσματος (πινακοπαιχνίδια) και θεώρημα Minimax. Εξισωτικές στρατηγικές και αλγόριθμοι επίλυσης πινακοπαιχνιδιών. Απλοποιήσεις.

– Συστήματα τύπων των γλωσσών προγραμματισμού

Το μάθημα αυτό έχει ως σκοπό τη μελέτη των συστημάτων τύπων (type systems) που χρησιμοποιούνται στις σύγχρονες γλώσσες προγραμματισμού. Μέσω των συστημάτων τύπων μελετώνται σε βάθος τα κυριότερα χαρακτηριστικά των προστακτικών και συναρτησιακών γλωσσών προγραμματισμού: βασικοί τύποι, συναρτήσεις, αναδρομή, αναφορές, εξαιρέσεις, υποτύποι, αναδρομικοί τύποι, αντικείμενα, πολυμορφισμός, υπαρξιακοί και εξαρτώμενοι τύποι. Έμφαση δίνεται στη συνεισφορά των συστημάτων τύπων για τον τυπικό ορισμό των γλωσσών καθώς και για τη μελέτη ιδιοτήτων ασφάλειας των προγραμμάτων. Για την περιγραφή της σημασιολογίας των υπό μελέτη γλωσσών χρησιμοποιείται η προσέγγιση της δομημένης λειτουργικής σημασιολογίας (structural operational semantics).

#### – Τροπική λογική

Εισαγωγή στη βασική τροπική λογική: συντακτικό, σημασιολογία (σχεσιακά μοντέλα ή μοντέλα και πλαίσια (frames) Kripke), σημαντικές ερμηνείες του τροπικού τελεστή (epistemic/doxastic logic, deontic logic, temporal logic, provability logic). Ερμηνεία της Τροπικής Λογικής: βασική θεωρία μοντέλων και πλαισίων, κατασκευές που προστατεύουν αλήθεια και εγκυρότητα, σχέση με την κλασική λογική, πρωτοβάθμια ορισμότητα, θεωρία αντιστοιχίας (correspondence theory). Βασική Θεωρία Αποδείξεων και Θεωρία Πληρότητας (completeness theory): φυσικές λογικές (normal modal logics), κανονιστικά μοντέλα και πληρότητα, χρήση του κανονιστικού μοντέλου, κανονιστικές λογικές (canonical logics) και φαινόμενα μη-πληρότητας (frame incompleteness results), ανάλυση λογικών με “μεταβατικά” πλαίσια (Cluster analysis of transitive logics). Διηθήσεις (filtrations) και αποδείξεις αποκρισμότητας. Αποδεικτικά συστήματα tableaux και υπολογιστική πολυπλοκότητα. Προχωρημένα θέματα: πλούσιες τροπικές γλώσσες και εφαρμογές τους. Δυναμική Λογική (Propositional Dynamic Logic, PDL), Χρονικές Λογικές Γραμμικού και Διακλαδιζόμενου Χρόνου (Temporal Logics of Linear and Branching Time), Λογική της Αποδειξιμότητας (Provability Logic).

#### – Τυπικές μέθοδοι

Εισαγωγή στις τυπικές μεθόδους. Το λογικό σύστημα της εξισωτικής λογικής (equational logic). Το λογικό σύστημα της χρονικής λογικής (temporal logic). Προδιαγραφές (specification) και επαλήθευση (verification) προγραμμάτων. Εφαρμογές στην τεχνολογία λογισμικού. Αλγεβρικές προδιαγραφές (algebraic specifications). Αποδεικτική θεωρημάτων (theorem proving). Model checking. Εφαρμογές στη βιομηχανία.

#### – Τυχαιοποιημένοι αλγόριθμοι.

Μοντέλα τυχαίου υπολογισμού (Las Vegas και Monte Carlo). Δομές δεδομένων. Συναρτήσεις κατάτμησης. Δειγματοληψία. Η εντροπική μέθοδος. Τυχαιοποιημένοι αλγόριθμοι σε γραφήματα. Τυχαιοποιημένοι γεωμετρικοί αλγόριθμοι. Τυχαιοποιημένοι αλγόριθμοι για κατά προσέγγιση μέτρηση. Τυχαιοποιημένοι παράλληλοι αλγόριθμοι. Τεχνικές αποτυχαίωσης. Εργαλεία για την πιθανοτική ανάλυση αλγορίθμων.

#### – Υπολογιστική άλγεβρα

Πολύωνυμα πολλών μεταβλητών: Ιδεώδη, ποικιλότητες (varieties), βάσεις Groebner, αλγόριθμος Buchberger. Μελέτη συστημάτων, καταμέτρηση ριζών (φράγμα Bezout, Μικτός όγκος), επίλυση με μεθόδους γραμμικής άλγεβρας. Απαλοίφουσα (resultant). Κλασική και αραιή απαλοίφουσα. Κατασκευή πινάκων απαλοίφουσας (Sylvester, Macaulay, αραιή απαλοίφουσα). Εφαρμογές: Κινηματική των ρομπότ και γράφοι αποστάσεων. Γεωμετρική σχεδίαση. Υπολογιστική θεωρία Παιγνίων.

#### – Υπολογιστική γεωμετρία

Κυρτό περίβλημα σε 2, 3 και μεγαλύτερες διάστασεις, αλγόριθμος περιτύλιξης (πολυπλοκότητα ευαίσθητη εξόδου) και αυξητικός αλγόριθμος. Αθροισμα Minkowski. Τριγωνοποίηση πολυγώνου. Εκφυλισμένα δεδομένα, διαταραχή. Γραμμικός Προγραμματισμός, αλγόριθμος Simplex και αντίστροφη αναζήτηση, δυϊσμός και πόλωση. Διάγραμμα Voronoi, αναγωγή σε ΚΠ. Τριγωνοποίηση Delaunay,  $\alpha$ -σχήματα και εφαρμογές στην δομική βιοπληροφορική, στην κίνηση ρομπότ ανάμεσα σε εμπόδια. Διατάξεις ευθυγράμμων τμημάτων, ευθειών. Δομές γεωμετρικών δεδομένων. Εντοπισμός και εξόρυξη δεδομένων, ορθογώνια αναζήτηση, kd-δένδρα, δένδρα περιοχών. Προσεγγιστική εύρεση πλησιέστερου γείτονα με δενδρικές δομές ή πίνακες κατακερματισμού σε μεγάλες διαστάσεις και γενικούς μετρικούς χώρους. Locality-sensitive Hashing για την αντιμετώπιση της "κατάρτας της διάστασης". Μείωση διάστασης με τυχαιοκρατικές προβολές και το Λήμμα Johnson-Lindenstrauss. Εφαρμογές στη συσταδοποίηση. Υλοποίηση σε Python και στην C++ βιβλιοθήκη γεωμετρικού λογισμικού CGAL.

#### – Υπολογιστική επιστήμη και τεχνολογία

Προσομοίωση, σφάλματα, αριθμητική υπολογιστών. Ιεραρχίες μνήμης, οι πυρήνες BLAS. Αλγόριθμοι εφαρμοσμένης γραμμικής άλγεβρας, LAPACK. Μέθοδοι Monte Carlo. Προβλήματα αρχικών τιμών και συνοριακά προβλήματα για συνήθεις διαφορικές εξισώσεις. Μη-γραμμικές εξισώσεις πολλών μεταβλητών. Υπολογισμοί με αραιούς πίνακες και εφαρμογές σε μερικές διαφορικές εξισώσεις και σε επίλυση γραμμικών συστημάτων. Επαναληπτικές μέθοδοι Krylov, πολυπλεγματικές μέθοδοι.

#### – Υπολογιστική κρυπτογραφία

Κλασική κρυπτογραφία: κρυπτοσυστήματα αντικατάστασης, Καίσαρα, Vigenere, μέθοδοι κρυπτανάλυσης. Τέλειαμυστικότητα (Shannon), one-time pad. Semantic security, CPA, CCA, PCPA. Συμμετρική κρυπτογραφία. Ψευδοτυχειότητα, κρυπτοσυστήματα ροής. Κρυπτοσυστήματα τμήματος: δίκτυα Feistel, DES, AES. Τρόποι λειτουργίας. Κώδικες πιστοποίησης γνησιότητας (MACs). Συναρτήσεις κατακερματισμού (hash functions). Στοιχεία θεωρίας αριθμών: διαιρετότητα, αριθμητική υπολοίπων, τετραγωνικά υπόλοιπα, Κινέζικο Θεώρημα Υπολοίπων. Στοιχεία θεωρίας ομάδων, θεώρημα Legendre, συνάρτηση  $\phi$  του Euler. Έλεγχος πρώτων αριθμών. Κρυπτογραφία δημοσίου κλειδιού. Κρυπτοσυστήματα RSA και Rabin, σχέση με πρόβλημα παραγοντοποίησης. Το πρόβλημα του διακριτού λογαρίθμου, σύστημα El Gamal. Ανταλλαγή κλειδιού Diffie – Hellman. Ψηφιακές Υπογραφές: RSA, DSS, τυφλές υπογραφές. Κρυπτογραφικά πρωτόκολλα: διαμοιρασμός μυστικού, σχήματα αναγνώρισης, e-voting, ασφαλής υπολογισμών πολλών μερών, Bitcoin. Αποδείξεις μηδενικής γνώσης. Στοιχεία θεωρίας πολυπλοκότητας, μονόδρομες συναρτήσεις. Προχωρημένα θέματα: ελλειπτικές καμπύλες, κρυπτογραφία βασισμένη σε lattices, κρυπτογραφία συζεύξεων, συσκότιση κώδικα, μετα-κβαντική κρυπτογραφία.