Θεωρία Υπολογισμού

Δημήτρης Φωτάκης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Διαδικαστικά

- 4 ώρες **θεωρία** (Δ. Φωτάκης, **Τετάρτη 19-21** και **Πέμπτη 11-13**):
- **2 εργασίες** (σύνολα ασκήσεων): ανακοίνωση 2ο δεκαήμερο Μαΐου, 1ο δεκαήμερο Ιουνίου.
  - **Υποχρεωτικές**: 30% βαθμού (ΒΕργ), **ΒΕργ** ≥ 5
  - **6 - 8 ασκήσεις** / εργασία, **1 εβδομάδα**, παράδοση στο μάθημα.
  - **Καμία παράταση** στην παράδοση των εργασιών!
- **Γραπτή πρόοδος**: αρχές Ιουνίου, 20% βαθμού (ΒΠ);;;
- **Τελική εξέταση**: τέλος Ιουνίου, 50% βαθμού (ΒΤΕ), **ΒΤΕ** ≥ 5
- **Τελικός βαθμός**: $0.5 \times$ ΒΤΕ $+ 0.2 \times$ ΒΠ $+ 0.3 \times$ ΒΕργ εφόσον ΒΕργ ≥ 5 **και** ΒΤΕ ≥ 5.

Βιβλιογραφία - Ύλη

- Lewis και Παπαδημητρίου, Στοιχεία Θεωρίας Υπολογισμού, Prentice Hall , 1998. Ελληνική μετάφραση Π. Αντωνιάδης και Μ. Σιδέρη, Κριτική, 2005.
- M. Sipser, Introduction to the Theory of Computation, PWS, 1997.
- C. Papadimitriou, Computational Complexity, Addison Wesley, 1994.
- **Διαφάνειες** διδάσκοντα (για επισκόπηση ύλης).
- **Οτιδήποτε** άλλο (ασκήσεις, παραδείγματα, εφαρμογές) αναφέρεται στις **διαλέξεις**.
- Σημειώσεις, ανακοινώσεις, άλλο υλικό: http://www.icsd.aegean.gr/lectures/fotakis/toc.html
- **Παρακολούθηση** διαλέξεων και ενεργή **συμμετοχή**.
- **Μηδενική ανοχή** σε θέματα αντιγραφής, αθέμιτης συνεργασίας.

Θεωρία Υπολογισμού

- **Σκοπός**: Εισαγωγή στη Θεωρία Υπολογισμού και στη Θεωρία Υπολογιστικής Πολυπλοκότητας.
- Γιατί προβλήματα είναι **δύσκολο ή αδύνατο** να λυθούν από υπολογιστές; Θεμελιώδεις **δυνατότητες** και **περιορισμοί** των υπολογιστών;
- **Hilbert** (1900): **πληρότητα** και **αυτοματοποίηση** των μαθηματικών.
- 10ο πρόβλημα : **Αλγόριθμος** για λύση Διοφαντικών εξισώσεων: Έχει $x^2 - 2y^2 + 3 = 0$ **ακέραιες** ρίζες;
- **Αλγόριθμος**: Διατύπωση και απόδειξη.
- **Όχι αλγόριθμος**: Υπολογιστικό μοντέλο και απόδειξη ότι “αλγόριθμος $\Rightarrow$ αντίφαση στο μοντέλο”.
- **Gödel**: Μαθηματικά **δεν είναι πλήρη**!
- **Turing**: Μαθηματικά **δεν αυτοματοποιούνται**!
- **Matijasevic** (1970): Δεν υπάρχει αλγόριθμος για Διοφαντικές εξισώσεις! Για κάθε αλγόριθμο $\mathcal{A}$, υπάρχει εξίσωση που ο $\mathcal{A}$ δίνει **λάθος απάντηση**!

(Υπολογιστική) Πολυπλοκότητα

- Το σύνολο των πρώτων αριθμών είναι πιο πολύπλοκο από το σύνολο των περιττών αριθμών.
- Ερώτημα "x πρώτος;" πιο δύσκολο από "x άρτιος;".
- Πρόγραμμα για "x πρώτος;" πιο σύνθετο από πρόγραμμα για "x άρτιος;".
- Πρόγραμμα που τυπώνει πρώτους $\leq n$ πιο σύνθετο από πρόγραμμα που τυπώνει άρτιους $\leq n$.
- Η συμβολοσειρά 101000101101 πιο πολύπλοκη από την 111111000000.
- Χρειαζόμαστε έναν **ακριβή** ορισμό του **πιο πολύπλοκου**.
- Βάση η έννοια του **προγράμματος** που απαντάει (σωστά) ένα ερώτημα. Πρόγραμμα δίνει μια **μορφή απόδειξης** για την απάντησή του.
- Χωρισμός των προβλημάτων σε **κλάσεις πολυπλοκότητας** που περιλαμβάνουν προβλήματα περίπου ίδιας πολυπλοκότητας.

Θεωρία Υπολογισμού

- **Υπολογιστικά Μοντέλα**: Αυτόματα και γλώσσες. Μηχανές Turing.
- **Υπολογισιμότητα**: Τι είναι και τι δεν είναι υπολογίσιμο.
- **Υπολογιστική Πολυπλοκότητα**: Τι υπολογίζεται γρήγορα και τι όχι.
- Γιατί κάποια προβλήματα είναι εύκολο και άλλα δύσκολο ή αδύνατο να λυθούν από υπολογιστή.
- **Υπολογιστικό Μοντέλο**: Αυτόματα, Μηχανές Turing.
- **Μη-επιλύσιμα** προβλήματα: Αναγνώριση (Halting Problem).
- **Επιλύσιμα** προβλήματα: Υπολογιστικοί πόροι;
  - Εύλογοι υπολογιστικοί πόροι $\Rightarrow$ **ευεπίλυτα** (tractable) προβλήματα.
    Πολλαπλασιασμός Πινάκων, Κλασματικό Σακίδιο, Ελάχιστο Επικαλύπτον Δέντρο, Συντομότερα Μονοπάτια.
  - Διαφορετικά, **δυσεπίλυτα** (intractable).
    Ακέραιο Σακίδιο, Περιοδεύων Πωλητής, Κάλυψη Συνόλων, Δρομολόγηση, Χρωματισμός, Συντομότερα Μονοπάτια με Περιορισμούς, κλπ.
  - Επίδραση **υπολογιστικού μοντέλου** στους υπολογιστικούς πόρους.

Προβλήματα και Αλγόριθμοι

- **Αλγόριθμος** είναι λεπτομερής περιγραφή μεθόδου επίλυσης προβλήματος.
  υπολογιστική μηχανή ειδικού σκοπού.
- **Υπολογιστικό πρόβλημα** αποτελείται από άπειρο σύνολο στιγμιοτύπων.
  αποτελεί αντικείμενο μελέτης.
- **Στιγμιότυπο** είναι μαθηματικό αντικείμενο για το οποίο ρωτάμε **ερώτηση** και περιμένουμε **απάντηση**.
- Δύο είδη προβλημάτων:
  - **Απόφασης**: απαντήσεις **ΝΑΙ** ή **ΟΧΙ**.
  - **Βελτιστοποίησης**: καλύτερη εφικτή **λύση**.

Παραδείγματα Προβλημάτων

- **Πρόβλημα Προσπελασιμότητας**:
  - **Στιγμιότυπο**: Κατευθυνόμενο γράφημα $G(V, E)$ και διακεκριμένες κορυφές s και t.
  - **Ερώτηση**: Υπάρχει μονοπάτι από s στο t;
- **Πρόβλημα Συντομότερου Μονοπατιού**:
  - **Στιγμιότυπο**: Κατευθυνόμενο γράφημα με μήκη στις ακμές $G(V, E, w)$ και διακεκριμένες κορυφές s και t.
  - **Ερώτηση**: Ποιο είναι το συντομότερο $s - t$ μονοπάτι;

Παραδείγματα Προβλημάτων

- **Πρόβλημα κύκλου Hamilton**:
  - **Στιγμιότυπο**: Γράφημα $G(V, E)$.
  - **Ερώτηση**: Υπάρχει κύκλος Hamilton στο G (κύκλος που διέρχεται από κάθε κορυφή ακριβώς μία φορά);
- **Πρόβλημα Περιοδεύοντος Πωλητή**:
  - **Στιγμιότυπο**: Σύνολο $= \{1, \ldots, n\}$ σημείων και αποστάσεις $d(i, j)$ μεταξύ κάθε ζεύγους διαφορετικών σημείων.
  - **Ερώτηση**: Ποια μετάθεση π του N ελαχιστοποιεί

$$d(\pi(n), \pi(1)) + \sum_{i=1}^{n-1} d(\pi(i), \pi(i+1))$$

Κωδικοποίηση Προβλημάτων σε Τυπικές Γλώσσες

- Πρόβλημα βελτιστοποίησης $\rightarrow$ πρόβλημα απόφασης με φράγμα B.
  - Ελαχιστοποίηση: Υπάρχει εφικτή λύση με κόστος $\leq B$;
  - Μεγιστοποίηση: Υπάρχει εφικτή λύση με κέρδος $\geq B$;
- Πρόβλημα απόφασης $\rightarrow$ τυπική γλώσσα με κωδικοποίηση.
  - Στιγμιότυπο $\rightarrow$ συμβολοσειρά σε αλφάβητο Σ.
  - Πρόβλημα $\rightarrow$ γλώσσα, υποσύνολο του Σ^*.
- Πρόβλημα Π και κωδικοποίηση e: Γλώσσα $\mathcal{L}(\Pi, e)$ αποτελείται από $x \in \Sigma^*$ που προκύπτουν από την e-κωδικοποίηση των ΝΑΙ-στιγμιοτύπων του Π.

$$\mathcal{L}(\Pi, e) = \{e(x) \in \Sigma^* : x \in \Pi\}$$

Υπόβαθρο

- Σύνολα και πράξεις συνόλων (ένωση, τομή, διαφορά).
  - Δυναμοσύνολο 2^A: Σύνολο όλων των υποσυνόλων του A.
  - Διαμέριση: Μη-κενά, ξένα μεταξύ τους υποσύνολα με ένωση A.
- Ασυμπτωτικός συμβολισμός, γραφήματα, συναρτήσεις, σχέσεις.
- Τεχνικές απόδειξης:
  - Απαγωγή σε Άτοπο: Ν.δ.ο το $\sqrt{2}$ είναι άρρητος (Πυθαγόρας).
    Έστω $\sqrt{2} = \frac{a}{b}$, a, b φυσικοί, ένας τουλάχιστον περιττός.
    Τότε $2b^2 = a^2 \Rightarrow a$ άρτιος. Άρα $a = 2k$.
    Όμως τότε $2b^2 = 4k^2 \Rightarrow b^2 = 2k^2 \Rightarrow b$ άρτιος. Άτοπο.
  - Μαθηματική Επαγωγή
  - Αρχή Περιστερώνα: Αν A και B είναι πεπερασμένα σύνολα και $|A| > |B|$, τότε κάθε συνάρτηση από το A στο B δίνει σε κάποια στοιχεία του A την ίδια εικόνα.
  - Αρχή Διαγωνιοποίησης

Ιδιότητες Συναρτήσεων

- Συνάρτηση $f : A \mapsto B$ (στοιχεία έχουν μοναδική εικόνα):
  - Ένα-προς-ένα: $\forall a, a' \in A, f(a) \neq f(a')$ (διαφορετικά στοιχεία $\rightarrow$ διαφορετικές εικόνες).
  - Επί: $\forall b \in B, \exists a \in A : f(a) = b$ (κάθε στοιχείο του B αποτελεί εικόνα κάποιου στοιχείου του A).
  - Αμφιμονοσήμαντη αντιστοιχία: Ένα-προς-ένα και επί.
  - Αντίστροφη συνάρτηση $f^{-1} : B \mapsto A$. Αν f αμφιμονοσήμαντη, τότε $\forall a \in A, \forall b \in B, f(a) = b \Leftrightarrow f^{-1}(b) = a$.

Ιδιότητες Διμελών Σχέσεων

- Διμελής σχέση $R \subset A \times A$ (κατευθυνόμενο γράφημα στο A):
  - Ανακλαστική: $\forall a \in A,\ (a, a) \in R$ (ανακύκλωση)
  - Συμμετρική: $(a, b) \in R \Rightarrow (b, a) \in R$ (μη-κατευθυνόμενο γράφημα)
  - Αντισυμμετρική: $(a, b) \in R \land a \neq b \Rightarrow (b, a) \notin R$.
  - Μεταβατική: $(a, b) \in R \land (b, c) \in R \Rightarrow (a, c) \in R$.
  - Σχέση Ισοδυναμίας: Ανακλαστική, συμμετρική, και μεταβατική.
    Ορίζει διαμέριση A σε κλάσεις ισοδυναμίας.
  - Μερική διάταξη: Ανακλαστική, αντίσυμμετρική, και μεταβατική.
  - Ολική διάταξη: Μερική διάταξη και $\forall a, b \in A,\ (a, b) \in R \lor (b, a) \in R$.