Μαθηματικά Πληροφορικής

1ο Μάθημα

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

Υποθέσεις - Θεωρήματα

- Στα μαθηματικά και στις άλλες επιστήμες κάνουμε συχνά υποθέσεις. Όταν δείξουμε ότι μια υπόθεση είναι αληθής, τότε την ονομάζουμε θεώρημα ή πρόταση.
- Τα μαθηματικά που διδασκόμαστε στο σχολείο και στο Πανεπιστήμιο, αποτελούνται συνήθως από ορισμούς, θεωρήματα και αποδείξεις που μας δίνονται έτοιμες.
- Η πιο ενδιαφέρουσα πλευρά των μαθηματικών είναι όταν εξερευνούμε τα σύνορα της γνώσης. Εκεί πρέπει να κάνουμε υποθέσεις και μετά να τις αποδείξουμε ή να τις καταρρίψουμε.
- Υπόθεση $\rightleftharpoons$ Απόδειξη $\rightleftharpoons$ Θεώρημα

Υποθέσεις - Εικασίες

- Πολλές φορές, όταν δεν μπορούμε να αποδείξουμε μια υπόθεση, την αναθεωρούμε.
- Άλλες φορές, όταν καταφέρνουμε να αποδείξουμε μια υπόθεση, η ίδια η απόδειξη μας βοηθάει να γενικεύσουμε την πρόταση.

Η χρυσή τομή

Η χρυσή τομή είναι ο αριθμός $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$. Ισχύει $\phi^2 = \phi + 1$. Ας πολλαπλασιάσουμε το ϕ και το ϕ^2 με τους φυσικούς αριθμους.

$$
\begin{aligned}
1 \cdot \phi &= 1.618\ldots & \qquad 1 \cdot \phi^2 &= 2.618\ldots \\
2 \cdot \phi &= 3.236\ldots & \qquad 2 \cdot \phi^2 &= 5.236\ldots \\
3 \cdot \phi &= 4.854\ldots & \qquad 3 \cdot \phi^2 &= 7.854\ldots \\
4 \cdot \phi &= 6.472\ldots & \qquad 4 \cdot \phi^2 &= 10.472\ldots \\
5 \cdot \phi &= 8.090\ldots & \qquad 5 \cdot \phi^2 &= 13.090\ldots \\
6 \cdot \phi &= 9.708\ldots & \qquad 6 \cdot \phi^2 &= 15.708\ldots
\end{aligned}
$$

Η χρυσή τομή

- Παρατηρήστε πως στα ακέραια μέρη των γινομένων φαίνεται ότι εμφανίζονται όλοι οι φυσικοί αριθμοί $1, 2, 3, \ldots$ από μία φορά ο καθένας.
- Είναι όμως αλήθεια; Για να απαντήσουμε πρέπει πρώτα να διατυπώσουμε με σαφήνεια την υπόθεση και μετά να προσπαθήσουμε να την αποδείξουμε ή καταρρίψουμε.
- *Υπόθεση: Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor k\phi \rfloor$ ή $n = \lfloor k\phi^2 \rfloor$.*

Η χρυσή τομή

- Ας δοκιμάσουμε να καταρρίψουμε την υπόθεση με υπολογιστή. Ας πάρουμε ένα μεγάλο 'τυχαίο' n, π.χ. $n = 1000$, και ας δοκιμάσουμε τα k που είναι κοντά στα n/ϕ και n/ϕ^2. Βρίσκουμε ότι η υπόθεση ισχύει για αυτό το n.
- Αν έχουμε πειστεί αρκετά για την αλήθεια της υπόθεσης ας προσπαθήσουμε να την αποδείξουμε.

Απόδειξη

- Ορίζουμε τα σύνολα $A = \{\lfloor k\phi \rfloor \, : \, k = 1, 2, \ldots\}$ και $B = \{\lfloor k\phi^2 \rfloor \, : \, k = 1, 2, \ldots\}$.
- Για κάθε φυσικό n ορίζουμε τα υποσύνολα A_n και B_n να είναι τα στοιχεία των A και B που δεν ξεπερνούν το n.
- Πόσα στοιχεία έχει το A_n; Όσοι είναι οι φυσικοί k για τους οποίους ισχύει

$$\lfloor k\phi \rfloor \leq n \Leftrightarrow k\phi < n+1 \Leftrightarrow k < \frac{n+1}{\phi} \Leftrightarrow k \leq \left\lfloor \frac{n+1}{\phi} \right\rfloor.$$

Δηλαδή, ο αριθμός των στοιχείων του σύνολου A_n είναι $|A_n| = \left\lfloor \frac{n+1}{\phi} \right\rfloor$. Με τον ίδιο τρόπο βρίσκουμε $|B_n| = \left\lfloor \frac{n+1}{\phi^2} \right\rfloor$.

Απόδειξη

- Ο αριθμός λοιπόν των στοιχείων και του A_n και του B_n είναι

$$\left\lfloor \frac{n+1}{\phi} \right\rfloor + \left\lfloor \frac{n+1}{\phi^2} \right\rfloor.$$

- Ισχύει ότι $A_n \cap B_n = \varnothing$. (Γιατί;) Άρα η αρχική υπόθεση ισχύει αν και μόνο αν $|A_n| + |B_n| = n$, δηλαδή:

$$\left\lfloor \frac{n+1}{\phi} \right\rfloor + \left\lfloor \frac{n+1}{\phi^2} \right\rfloor = n.$$

Απόδειξη

- Παρατηρούμε ότι το ϕ έχει την ιδιότητα

$$\frac{n+1}{\phi} + \frac{n+1}{\phi^2} = n+1.$$

- Οι δυο αριθμοί $\frac{n+1}{\phi}$ και $\frac{n+1}{\phi^2}$ έχουν άθροισμα $n+1$ και δεν είναι ακέραιοι. Άρα τα ακέραια μέρη τους έχουν άθροισμα n (γιατί;).

Εκκρεμότητα

Γιατί $A_n \cap B_n = \varnothing$; Θα δείξουμε κάτι γενικότερο: $A \cap B = \varnothing$.
Προς άτοπο έστω ότι υπάρχουν $j, k, m \in \mathbb{N}$ τ. ώ.

$$j = \lfloor k\phi \rfloor = \lfloor m\phi^2 \rfloor \Leftrightarrow$$
$$j \leq k\phi < j+1 \text{ και } j \leq m\phi^2 < j+1.$$

Επειδή $k\phi, m\phi^2 \notin \mathbb{Q}$

$$j < k\phi < j+1 \text{ και } j < m\phi^2 < j+1 \Rightarrow$$
$$j/\phi < k < (j+1)/\phi \text{ και } j/\phi^2 < m < (j+1)/\phi^2$$

Προσθέτοντας κατά μέλη:

$$j\left(\frac{1}{\phi} + \frac{1}{\phi^2}\right) < k + m < (j+1)\left(\frac{1}{\phi} + \frac{1}{\phi^2}\right) \Rightarrow$$
$$j < k + m < j + 1.$$

Γενίκευση

- Ποια ιδιότητα του ϕ και του ϕ^2 χρησιμοποιήσαμε στην παραπάνω απόδειξη;
- Μόνο ότι
$$\frac{1}{\phi} + \frac{1}{\phi^2} = 1$$
και ότι είναι άρρητοι.
- Η ίδια απόδειξη μπορεί να χρησιμοποιηθεί για το πιο γενικό θεώρημα:

Θεώρημα

Έστω δύο οποιοιδήποτε θετικοί άρρητοι r και s που ικανοποιούν $\frac{1}{r} + \frac{1}{s} = 1$. Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor kr \rfloor$ ή $n = \lfloor ks \rfloor$.

Γενίκευση

- Ποια ιδιότητα των ϕ και ϕ^2 χρησιμοποιήσαμε στην παραπάνω απόδειξη;
- Μόνο ότι

$$\frac{1}{\phi} + \frac{1}{\phi^2} = 1$$

και ότι είναι άρρητοι.

- Η ίδια απόδειξη μπορεί να χρησιμοποιηθεί για το πιο γενικό θεώρημα:

Θεώρημα

Έστω δύο οποιοιδήποτε θετικοί άρρητοι r και s που ικανοποιούν $\frac{1}{r} + \frac{1}{s} = 1$. Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor kr \rfloor$ ή $n = \lfloor ks \rfloor$.

Γενίκευση

Η προηγούμενη διατύπωση περιείχε μία περιττή λέξη:

Θεώρημα

Έστω δυο θετικοί άρρητοι r και s που ικανοποιούν $\frac{1}{r} + \frac{1}{s} = 1$. Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor kr \rfloor$ ή $n = \lfloor ks \rfloor$.

Γενίκευση

Θεώρημα

Έστω δυο θετικοί άρρητοι r και s που ικανοποιούν $\frac{1}{r} + \frac{1}{s} = 1$. Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor kr \rfloor$ ή $n = \lfloor ks \rfloor$.

Υπάρχουν άπειρα τέτοια ζευγάρια (r, s). Για κάθε άρρητο $r > 1$ $s = r/(r-1)$ είναι θετικός άρρητος (γιατί;) τ. ώ. $\frac{1}{r} + \frac{1}{s} = 1$.

Π.χ., $(\sqrt{2},\ 2+\sqrt{2})$, $(\pi,\ \pi/(\pi-1))$.

Υπόθεση - Κατάρριψη

- Ας παρατηρήσουμε τους αριθμούς της μορφής $n^2 + n + 41$ για $n = 0, 1, 2, \ldots$:

$$41, 43, 47, 53, 61, \ldots.$$

- Όλοι αυτοί οι αριθμοί είναι πρώτοι.
- *Υπόθεση: Για κάθε φυσικό αριθμό n, ο αριθμός $n^2 + n + 41$ είναι πρώτος.*
- Δοκιμάζοντας πολλές τιμές για το n διαπιστώνουμε ότι η υπόθεση δεν ισχύει. Ισχύει για $n = 0, 1, 2, \ldots, 39$, άλλα για $n = 40$ βλέπουμε ότι το $40^2 + 40 + 41 = 40 \cdot (40 + 1) + 41$ διαιρείται από το 41.

Υπόθεση - Κατάρριψη

Για την κατάρριψη μιας υπόθεσης με καθολικό ποσοδείκτη, αρκεί ένα αντιπαράδειγμα.

Υπόθεση: Για κάθε φυσικούς αριθμούς n, k,

$$\lfloor \frac{n+k}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{k}{2} \rfloor.$$

Εικασίες

- Μια υπόθεση που δεν μπορούμε να την καταρρίψουμε ή να την αποδείξουμε την ονομάζουμε εικασία.
- Οι εικασίες είναι η κινητήρια δύναμη των Μαθηματικών αλλά και της Θεωρητικής Πληροφορικής. Προσπαθώντας να αποδείξουμε εικασίες αναγκαζόμαστε να ανακαλύψουμε νέες θεωρίες και τεχνικές.

Το Θεώρημα του Φερμά

- Το Θεώρημα του Fermat είναι ίσως η πιο γνωστή πρώην εικασία: *Η εξίσωση* $x^n + y^n = z^n$ *δεν έχει λύση για μη μηδενικούς ακέραιους* x, y, *και* z *και για ακέραιο* $n > 2$.
- Προτάθηκε από τον Pierre Fermat τον 17ο αιώνα και αποδείχτηκε από τον Andrew Wiles το 1995.

Η εικασία του Goldbach

- Το 1742 ο Christian Goldbach διατύπωσε την εξής υπόθεση: *«Κάθε άρτιος αριθμός μεγαλύτερος του 2 μπορεί να γραφτεί σαν άθροισμα 2 πρώτων αριθμών.»* Π.χ. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $100 = 53 + 47$.
- Η εικασία δεν έχει αποδειχτεί ούτε καταρριφθεί.
- Έχει επιβεβαιωθεί με τη βοήθεια υπολογιστή για όλους τους αριθμούς μέχρι το 10^{17}.

Το Θεώρημα των 4 χρωμάτων

- *«Κάθε χάρτης μπορεί να χρωματιστεί με τέσσερα χρώματα έτσι ώστε γειτονικές χώρες να έχουν διαφορετικά χρώματα».*
- Η υπόθεση αυτή προτάθηκε πριν από 130 χρόνια
- Αποδείχτηκε τελικά το 1976 από τους Kenneth Appel και Wolfgang Haken. Η απόδειξη αυτή βασίζεται στον έλεγχο 1936 περιπτώσεων και η κάθε περίπτωση απαιτεί τον έλεγχο πολλών λογικών συνδυασμών. Μόνο με τη βοήθεια υπολογιστή μπορούν να ελεγχθούν όλες οι περιπτώσεις.
- Παραμένει ανοικτό αν υπάρχει σύντομη απόδειξη, που δεν απαιτεί υπολογιστική βοήθεια.

Η εικασία του $3x + 1$

- Πάρε ένα φυσικό αριθμό x. Αν είναι άρτιος διαίρεσε τον με το 2, αλλιώς υπολόγισε το $3x + 1$. Επανέλαβε με το αποτέλεσμα μέχρι να προκύψει το 1.
- $7 \to 22 \to 11 \to 34 \to 17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$
- Εικασία: *Αν ξεκινήσουμε από οποιονδήποτε φυσικό αριθμό x θα φτάσουμε πάντα στο 1.*
- Προτάθηκε από διάφορους, γι αυτό και λέγεται επίσης το πρόβλημα του Collatz, το πρόβλημα του Ulam, ο αλγόριθμος του Hasse, κλπ.
- Παραμένει ανοικτό. Έχει ελεγχθεί υπολογιστικά για όλες τις τιμές του x μέχρι το 2^{68}.

P≠NP

- Η πιο σημαντική εικασία στην πληροφορική και μια από τις σημαντικότερες γενικότερα είναι η εικασία P≠NP.
- Η εικασία λέει ότι υπάρχουν προβλήματα που λύνονται από μη ντετερμινιστικές μηχανές Turing σε πολυωνυμικό χρόνο αλλά απαιτούν περισσότερο από πολυωνυμικό χρόνο σε ντετερμινιστικές μηχανές.
- Πιο απλά: υπάρχουν προβλήματα για τα οποία είναι σημαντικά πιο δύσκολο να βρούμε τη λύση τους από το να επαληθεύσουμε την ορθότητα μιας δυνητικής λύσης που μας δίνουν ως είσοδο.

Satisfiability

- Το πρόβλημα της ικανοποιησιμότητας Boolean λογικών προτάσεων είναι γνωστό σαν Satisfiability (SAT). Η *είσοδος* δίνεται ως σύξευξη διαζεύξεων, π.χ.,

$$(x_1 \vee \overline{x}_2) \wedge (\overline{x}_1 \vee x_2 \vee \overline{x}_3) \wedge (x_1 \vee \overline{x}_2 \vee \overline{x}_3) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3)$$

  και θέλουμε να βρούμε *αν υπάρχουν boolean τιμές των μεταβλητών που κάνουν την πρόταση αληθή.*
- Κάθε διάζευξη την ονομάζουμε όρο (clause). Η παραπάνω πρόταση έχει τρεις μεταβλητές και τέσσερεις όρους.

Αλγόριθμος για το SAT;

$$(x_1 \vee \overline{x}_2) \wedge (\overline{x}_1 \vee x_2 \vee \overline{x}_3) \wedge (x_1 \vee \overline{x}_2 \vee \overline{x}_3) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3)$$

Αν κάποιος μας υποδείξει μια δυνητική λύση, δηλαδή n Boolean τιμές για τις n μεταβλητές μπορούμε γρήγορα να επαληθεύσουμε αν ικανοποιούν τη λογική πρόταση.

Η εικασία P≠NP λέει ότι χωρίς υπόδειξη, το πρόβλημα είναι δύσκολο: δεν υπάρχει αλγόριθμος που να τρέχει στη χειρότερη περίπτωση σε χρόνο πολυωνυμικό ως προς το μέγεθος της πρότασης.

- Δεν γνωρίζουμε αλγόριθμο για το SAT που να τρέχει σε χρόνο καλύτερο από $2^{(1-o(1))n}$.

P vs. NP

Ας περιοριστούμε σε υπολογιστικά προβλήματα απόφασης, στα οποία η απάντηση είναι «ΝΑΙ» ή «ΟΧΙ».

Ένα πρόβλημα απόφασης Π ανήκει στην κλάση P αν υπάρχει αλγόριθμος $\mathcal{A}$ έ. ώ:
(1) $\forall$ είσοδο x, $\mathcal{A}(x)$ επιστρέφει ορθά «ΝΑΙ» ή «ΟΧΙ».
(2) Ο $\mathcal{A}$ τρέχει σε χρόνο πολυωνυμικό στο μέγεθος του x.

Ένα πρόβλημα απόφασης Π ανήκει στην κλάση NP αν υπάρχει αλγόριθμος-Επαληθευτής $\mathcal{A}$ έ. ώ:
(1) $\forall$ είσοδο x για την οποία η απάντηση είναι «ΝΑΙ»,
$\exists$ υπόδειξη y για την οποία $\mathcal{A}(x, y) =$ «ΝΑΙ».
(2) Ο $\mathcal{A}$ τρέχει σε χρόνο πολυωνυμικό στο μέγεθος του x.

Προφανώς P $\subseteq$ NP. Το μεγάλο ερώτημα είναι αν P $\neq$ NP.

SAT $\in$ NP

Ένα πρόβλημα απόφασης Π ανήκει στην κλάση NP αν υπάρχει αλγόριθμος-Επαληθευτής $\mathcal{A}$ έ. ώ:

1. $\forall$ είσοδο x για την οποία η απάντηση είναι «ΝΑΙ»,
   $\exists$ υπόδειξη y για την οποία $\mathcal{A}(x, y) =$ «ΝΑΙ».
2. Ο $\mathcal{A}$ τρέχει σε χρόνο πολυωνυμικό στο μέγεθος του x.

Πρόταση

SATISFIABILITY $\in$ NP.

Σκεφτείτε πρόβλημα που να μην ανήκει στο NP!

Planar 3-Coloring

- Δίνεται χάρτης. Μπορεί να χρωματιστεί με τρία χρώματα ώστε γειτονικές χώρες να έχουν διαφορετικά χρώματα;
- Γνωρίζουμε από το Θεώρημα των Τεσσάρων Χρώματων, πως τέσσερα χρώματα είναι πάντα αρκετά.

Πρόταση

Planar 3-Coloring (P3C) $\in$ NP.

▶ Το SAT και το P3C συλλαμβάνουν τη δυσκολία όλης της κλάσης NP.

Θεώρημα

Εάν βρεθεί πολυωνυμικός αλγόριθμος για το Sat *ή το* P3C*, τότε* P = NP*.*

▶ Τα SAT και το P3C χαρακτηρίζονται ως NP-πλήρη.

Αναγωγές Ι

Τί σημαίνει ότι ένα πρόβλημα B «συλλαμβάνει τη δυσκολία» μιας ολόκληρης κλάσης προβλημάτων;

Διαισθητικά σημαίνει ότι το B είναι εξίσου δύσκολο (υπολογιστικά), όσο οποιοδήποτε άλλο πρόβλημα της κλάσης.

Αν βρούμε έναν αποδοτικό αλγόριθμο για το B, θα υπάρχουν αποδοτικοί αλγόριθμοι για όλα τα προβλήματα της κλάσης.

Αναγωγές (κατά Cook) II

Η έννοια της αναγωγής μας επιτρέπει να ιεραρχήσουμε τα προβλήματα ως προς την υπολογιστική τους δυσκολία.

Ένα πρόβλημα A ανάγεται σε πολυωνυμικό χρόνο στο πρόβλημα B αν η ύπαρξη αλγορίθμου πολυωνυμικού χρόνου για το B συνεπάγεται ότι και το A μπορεί να λυθεί σε πολυωνυμικό χρόνο.

Συμβολικά: $A \leq_p B$.

Αν $A \leq_p B$, το B είναι υπολογιστικά τουλάχιστον τόσο δύσκολο όσο και το A. Ισοδύναμα, αν ξέρουμε ότι το A δεν μπορεί να λυθεί αποδοτικά, το ίδιο θα ισχύει και για το B.

Παράδειγμα Αναγωγής

0/1 ΑΚΕΡΑΙΟΣ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ (IntProg):
Είσοδος: *Δίνονται* m *γραμμικές ανισότητες με ρητούς συντελεστές, πάνω σε* n *μεταβλητές* $u_1, \ldots, u_n$.
Ερώτημα: *Υπάρχει λύση του συστήματος με* $u_i \in \{0, 1\},\ i = 1, \ldots, n$;

Λήμμα

$\mathrm{SAT} \leq_p$ IntProg.

Απόδειξη: Για κάθε όρο στην είσοδο του SAT κατασκευάζουμε μια ανισότητα. Π.χ.

$$x_1 \vee \overline{x}_2 \vee \overline{x}_3 \ \rightsquigarrow\ u_1 + (1 - u_2) + (1 - u_3) \geq 1$$

Για οποιαδήποτε Boolean έκφραση ϕ κατασκευάζουμε (σε πολυων. χρόνο) σύστημα ανισοτήτων $f(\phi)$ τ. ώ. η ϕ είναι ικανοποιήσιμη αν και μόνο αν υπάρχει $\{0, 1\}$-λύση για το $f(\phi)$.

NP-completeness

Ένα πρόβλημα απόφασης B καλείται NP-πλήρες (NP-complete) αν

1. $B \in$ NP.
2. Για κάθε $A \in$ NP, $A \leq_p B$.

[Ιδιότητα 2] $\Rightarrow$ αν μπορούμε να λύσουμε το B σε πολυωνυμικό χρόνο, το ίδιο ισχύει και για κάθε άλλο πρόβλημα $A \in$ NP.

Το B είναι εξίσου δύσκολο όσο οποιοδήποτε πρόβλημα στο NP.

Δεν είναι προφανές a priori ούτε καν ότι υπάρχουν NP-complete προβλήματα.

▶ Έχει αποδειχθεί για χιλιάδες προβλήματα ότι είναι NP-complete. Μεταξύ αυτών και τα SAT, $\mathrm{P3C}$.

Εφαρμογές;

- Αν και τέτοια θέματα φαίνονται να μην έχουν εφαρμογές, πολλές φορές η τεχνολογία ακολουθεί (με καθυστέρηση) και μεταφέρει τη θεωρία στο πεδίο των εφαρμογών.
- Η επίλυση του προβλήματος του Collatz μπορεί να χρειαστεί τόσο προχωρημένες τεχνικές που είναι δύσκολο να προβλέψει κανείς αν και ποιες θα μπορούσαν να είναι οι πρακτικές εφαρμογές.
- Εάν αποδειχθεί ότι P=NP, αλλάζει δραματικά η έννοια του δύσβατου (intractable) υπολογιστικού προβλήματος. Καταρρέει όλη η κρυπτογραφία όπως την ξέρουμε.
- Εάν αποδειχθεί ότι P=NP, φαντάζει εφικτός ένας αλγόριθμος που θα βρίσκει σε εύλογο χρόνο αποδείξεις για όλες τις μαθηματικές εικασίες.
- Εάν αποδειχθεί ότι P≠NP, παραμένει το καθήκον της (ίσως κατά προσέγγιση) επίλυσης δύσβατων προβλημάτων.