

Μαθηματικά Πληροφορικής 2ο Μάθημα

Ηλίας Κουτσοπιάς

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών
elias@di.uoa.gr

Γενικό πλάνο

Αποδείξεις

Μορφές αποδείξεων

Υπάρχουν πολλά είδη αποδείξεων. Εδώ θα δούμε τα πιο κοινά:

- ▶ **Εξαντλητική μέθοδος ή μέθοδος επισκόπησης.** Όταν το πρόβλημα έχει πεπερασμένο αριθμό περιπτώσεων, τις εξετάζουμε όλες.
- ▶ **Μαθηματική επαγωγή.** Έστω μια πρόταση $P(n)$ που ισχύει για $n = 1$. Αν η $P(n)$ συνεπάγεται την $P(n + 1)$, τότε η πρόταση ισχύει για όλους τους φυσικούς.
- ▶ **Αναδρομική επαγωγή.** Επαγωγή όχι στους φυσικούς αριθμούς αλλά σε μια δομή που ορίζεται αναδρομικά.

Μορφές αποδείξεων (συνέχεια)

- ▶ **Κατασκευαστική απόδειξη ύπαρξης.** Δείχνουμε την ύπαρξη ενός στοιχείου δίνοντας ένα αλγόριθμο που το παράγει. Στην ίδια κατηγορία ανήκει και η απόδειξη με αντιπαράδειγμα.
- ▶ **Μη κατασκευαστική απόδειξη ύπαρξης.** Τέτοιες αποδείξεις χρησιμοποιούν
 - ▶ την αρχή του περιστερώνα και τις γενικεύσεις του
 - ▶ κατάλληλη καταμέτρηση
 - ▶ την πιθανοτική μέθοδο που βασίζεται στο ότι ένα στοιχείο υπάρχει όταν έχει μη μηδενική πιθανότητα ύπαρξης.
 - ▶ την διαγωνιοποίηση του Cantor.

Εξαντλητική μέθοδος

- ▶ Σε αυτό το είδος απόδειξης θεωρούμε όλες τις δυνατές περιπτώσεις και τις ελέγχουμε όλες. Αν ο αριθμός των περιπτώσεων είναι πεπερασμένος (και σχετικά μικρός) τότε αυτή είναι συνήθως η πιο κατάλληλη μέθοδος. Σήμερα που έχουμε στη διάθεση μας ισχυρούς υπολογιστές, αυτή η μέθοδος μπορεί να χρησιμοποιηθεί σε πολλά προβλήματα.
- ▶ Ας δούμε μερικά παραδείγματα τέτοιων αποδείξεων.

Σκύλος-κατσίκια-χορτάρι

- ▶ Ένας βοσκός έχει ένα άγριο σκύλο, μια κατσίκια και ένα δεμάτι χορτάρι και θέλει να χρησιμοποιήσει μια βάρκα για να διασχίσει ένα ποτάμι. Το πρόβλημα είναι ότι η βάρκα είναι μικρή και χωράει μόνο το βοσκό και ένα από τα 3 πράγματα ή ζώα που θέλει να μεταφέρει απέναντι. Επιπλέον ο σκύλος θα φάει την κατσίκια και η κατσίκια το χορτάρι αν μείνουν χωρίς το βοσκό στην ίδια όχθη.
- ▶ Υπάρχει λύση;
- ▶ Ναι. Μπορούμε να τη βρούμε αν δοκιμάσουμε όλους τους συνδυασμούς.

Σκάκι

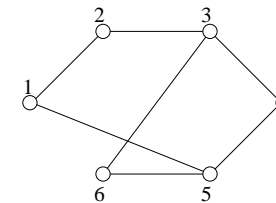
- ▶ Στα προβλήματα 'Ματ σε 3 κινήσεις' μπορούμε να δοκιμάσουμε όλες τις περιπτώσεις.
- ▶ Είναι εφικτά σήμερα τα προβλήματα της μορφής 'Ματ σε 7 κινήσεις';
- ▶ Δίνεται η αρχική σκακιέρα. Ματ σε 137 κινήσεις. Αυτό το πρόβλημα είναι πεπερασμένο, αλλά όχι υπολογιστικά εφικτό.

Ramsey numbers

Πρόταση

Σε κάθε ομάδα 6 ατόμων

- ▶ είτε υπάρχουν 3 που γνωρίζονται ανά δυο
- ▶ είτε υπάρχουν 3 που είναι άγνωστοι ανά δυο.



- ▶ Απόδειξη: Δοκίμασε όλες τις περιπτώσεις.
- ▶ Το παραπάνω δεν ισχύει για κάθε ομάδα 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.

Ramsey numbers

Μπορούμε να γενικεύσουμε την πρόταση

Θεώρημα

Σε κάθε σύνολο 18 ατόμων είτε υπάρχουν 4 που γνωρίζονται ανά δυο είτε υπάρχουν 4 που είναι άγνωστοι ανά δυο.

Απόδειξη.

Δοκίμασε όλες τις περιπτώσεις. Όμως τώρα οι περιπτώσεις είναι πάρα πολλές. \square

Θεώρημα

Σε κάθε σύνολο 49 ατόμων είτε υπάρχουν 5 που γνωρίζονται ανά δυο είτε υπάρχουν 5 που είναι άγνωστοι ανά δυο.

Απόδειξη.

Η εξαντλητική μέθοδος δεν μπορεί να χρησιμοποιηθεί γιατί σήμερα είναι υπολογιστικά ανέφικτη. \square

Μαθηματική επαγωγή

Έστω $P(n)$ μια υπόθεση που αφορά τους φυσικούς αριθμούς.

Για να αποδείξουμε την υπόθεση με επαγωγή

- ▶ Δείχνουμε ότι ισχύει για $n = 1$: $P(1)$
- ▶ Δείχνουμε για κάθε n : αν ισχύει για n τότε θα ισχύει για $n + 1$:

$$P(n) \Rightarrow P(n + 1)$$

Παράδειγμα - H_k

- ▶ Ο αρμονικός αριθμός H_k ορίζεται σαν

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k}$$

- ▶ Τι μεγέθους είναι ο H_k ;

Παράδειγμα - H_k

Λήμμα

Να δειχτεί ότι για κάθε φυσικό n : $H_{2^n} \leq 1 + n$.

Απόδειξη.

Βάση της επαγωγής: Για $n = 1$ έχουμε $H_{2^1} = H_2 = 3/2$ και $1 + n = 2$ και επομένως το λήμμα ισχύει: $3/2 \leq 2$.

Επαγωγική υπόθεση: Υποθέτουμε ότι το λήμμα ισχύει για κάποιο φυσικό αριθμό n : $H_{2^n} \leq 1 + n$.

Επαγωγικό βήμα: Θα δείξουμε ότι ισχύει για $n + 1$, δηλαδή ότι $H_{2^{n+1}} \leq 1 + (n + 1)$. \square

Παράδειγμα - H_k

Απόδειξη (συνέχ.)

Έχουμε

$$\begin{aligned}H_{2^{n+1}} &= 1 + \frac{1}{2} + \cdots + \frac{1}{2^{n+1}} \\ &= \left(1 + \frac{1}{2} + \cdots + \frac{1}{2^n}\right) + \left(\frac{1}{2^n} + \cdots + \frac{1}{2^{n+1}}\right) \\ &= H_{2^n} + \left(\frac{1}{2^n} + \cdots + \frac{1}{2^{n+1}}\right) \\ &\leq (1+n) + \left(\frac{1}{2^n} + \cdots + \frac{1}{2^n}\right) \\ &= (1+n) + 2^n \frac{1}{2^n} = (1+n) + 1 = 1 + (n+1).\end{aligned}$$

□

Μαθηματική επαγωγή - γενικεύσεις

Κάποιες κοινές παραλλαγές της επαγωγής

- ▶ Η βασική περίπτωση δεν είναι πάντα για $n = 1$. Για παράδειγμα για θεωρήματα της μορφής 'Για κάθε φυσικό αριθμό $n \geq 4$: ...' η βάση είναι $n = 4$.
- ▶ Η επαγωγική υπόθεση είναι ότι η πρόταση ισχύει για **όλους** τους μικρότερους αριθμούς:

$$P(1), \dots, P(n) \Rightarrow P(n+1)$$

Οι αριθμοί Fibonacci

Οι αριθμοί Fibonacci ορίζονται ως εξής:

$$F_0 = 1, \quad F_1 = 1,$$

και για κάθε $n \geq 2$:

$$F_n = F_{n-1} + F_{n-2}.$$

Λήμμα

Να δειχτεί ότι για κάθε ακέραιο $n \geq 0$,

$$F_n \leq \phi^n,$$

όπου $\phi = \frac{1+\sqrt{5}}{2} = 1.618\dots$ είναι η χρυσή τομή.

Θεώρημα

Για κάθε θετικό ακέραιο n : $\frac{1}{2}\phi^n \leq F_n \leq \phi^n$.

Οι αριθμοί Fibonacci

Θεώρημα

Να δειχτεί ότι για κάθε ακέραιους $n, m \geq 0$, οι αριθμοί Fibonacci ικανοποιούν την

$$F_{n+m} = F_n F_m + F_{n-1} F_{m-1}.$$

Το Θεώρημα αυτό μας επιτρέπει να υπολογίσουμε ένα αριθμό Fibonacci χωρίς να υπολογίσουμε όλους τους προηγούμενους.

$$F_{2k+1} = F_{k+1} F_k + F_k F_{k-1} = (F_k + F_{k-1}) F_k + F_k F_{k-1} = F_k^2 + 2F_k F_{k-1}$$

$$F_{2k} = F_k F_k + F_{k-1} F_{k-1} = F_k^2 + F_{k-1}^2$$

Παράδειγμα:

$$F_{31} = F_{15}^2 + 2F_{15} F_{14}$$

$$F_{15} = F_7^2 + 2F_7 F_6$$

$$F_{14} = F_7^2 + F_6^2$$

$$F_7 = \dots$$

Μέγιστος Κοινός Διαιρέτης

$$\gcd(a, b) = \begin{cases} a & \text{αν } b = 0 \\ \gcd(b, a \bmod b) & \text{αν } b > 0. \end{cases}$$

Αλγόριθμος του Ευκλείδη

```
1: function EUCLID(a, b)           ▷ Υποθέτουμε ότι  $a \geq b$ 
2:   if  $b = 0$  then
3:     return a                       ▷  $\gcd(a, 0) = a$ 
4:   else
5:      $\delta \leftarrow \text{EUCLID}(b, a \bmod b)$    ▷
6:      $\gcd(a, b) = \gcd(b, a \bmod a)$ 
7:   end if
8: end function
```

Ανάλυση του Αλγορίθμου του Ευκλείδη

- ▶ Πόσα βήματα κάνει ο αλγόριθμος για να υπολογίσει τον μέγιστο κοινό διαιρέτη δυο αριθμών; Εξαρτάται από τους αριθμούς φυσικά, αλλά θέλουμε να έχουμε μια εκτίμηση για τη χειρότερη περίπτωση.
- ▶ Το Θεώρημα του Lamé λέει ότι ο αριθμός των διαιρέσεων, ή ισοδύναμα οι φορές που υπολογίζουμε το $a \bmod b$, είναι το πολύ 5 φορές ο αριθμός των δεκαδικών ψηφίων του b .
- ▶ Εδώ θα δείξουμε ένα παραπλήσιο αποτέλεσμα.

Θεώρημα

Για κάθε θετικούς ακέραιους a, b με $a \geq 2$ και $a \geq b$, ο αριθμός των διαιρέσεων του αλγορίθμου του Ευκλείδη δεν ξεπερνά το $2 \log a$.

Ισχυροποίηση της επαγωγικής υπόθεσης

Μια χρήσιμη τεχνική για να αποδείξουμε μια πρόταση με μαθηματική επαγωγή είναι να ισχυροποιήσουμε την επαγωγική υπόθεση. Παράδειγμα:

Πρόταση

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2.$$

Απόδειξη.

Ας χρησιμοποιήσουμε επαγωγή και ας υποθέσουμε ότι η πρόταση ισχύει για κάποιο n . Προσθέτουμε και στα δυο μέλη το $\frac{1}{(n+1)^2}$. Αλλά, τώρα το δεξί μέλος είναι $2 + \frac{1}{(n+1)^2}$ που δεν είναι μικρότερο του 2. Η προσέγγιση αυτή αποτυγχάνει.

Είναι εύκολο όμως να δείξουμε την πιο ισχυρή πρόταση

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}. \quad \square$$

Ramsey theory

Θεώρημα (Ramsey)

Για κάθε φυσικό k , υπάρχει φυσικός R_k τέτοιος ώστε κάθε γράφος με R_k ή περισσότερους κόμβους περιέχει είτε ένα πλήρη υπογράφο με k κόμβους είτε ένα κενό υπογράφο με k κόμβους.

Αν προσπαθήσουμε να αποδείξουμε το θεώρημα με επαγωγή δεν θα τα καταφέρουμε γιατί η πρόταση για κάποιο k δεν συνεπάγεται την πρόταση για κάποιο $k + 1$.

Αν όμως γενικεύσουμε το θεώρημα, τότε μπορούμε να το αποδείξουμε με επαγωγή.

Θεώρημα (Ramsey)

Για κάθε θετικούς ακέραιους k, m υπάρχει φυσικός $R_{k,m}$ τέτοιος ώστε κάθε γράφος με $R_{k,m}$ ή περισσότερους κόμβους περιέχει είτε ένα πλήρη υπογράφο με k κόμβους είτε ένα κενό υπογράφο με m κόμβους.