Μαθηματικά Πληροφορικής

4ο Μάθημα

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

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.
- Δομική επαγωγή. Επαγωγή όχι στους φυσικούς αριθμούς αλλά σε μια δομή που ορίζεται επαγωγικά.

Μορφές αποδείξεων (συνέχεια)

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

Παράδειγμα: Άθροισμα κύβων

- Υπάρχει φυσικός ακέραιος που μπορεί να γραφεί με δύο διαφορετικούς τρόπους σαν άθροισμα δύο κύβων;
- Ισοδύναμα, υπάρχουν δύο διαφορετικά ζεύγη φυσικών αριθμών $\{a_1, b_1\}$ και $\{a_2, b_2\}$ με $a_1^3 + b_1^3 = a_2^3 + b_2^3$;
- Ο 1729 μπορεί να γραφεί σαν $1^3 + 12^3$ και σαν $9^3 + 10^3$.

Κατασκευαστικές ή Όχι;

Γενικά οι αποδείξεις ύπαρξης χωρίζονται σε δύο μεγάλες κατηγορίες:

- Κατασκευαστικές αποδείξεις, στις οποίες η απόδειξη είτε δίνει το στοιχείο που έχει την απαιτούμενη ιδιότητα είτε έναν αλγόριθμο που παράγει ένα τέτοιο στοιχείο.
  - Παράδειγμα: Υπάρχει ακέραιος που γράφεται με δύο τρόπους σαν άθροισμα δύο κύβων. Η απόδειξη $1729 = 1^3 + 12^3 = 9^3 + 10^3$ είναι κατασκευαστική.
- Μη κατασκευαστικές αποδείξεις, στις οποίες δείχνουμε ότι το στοιχείο υπάρχει, αλλά ούτε το στοιχείο δίνεται ούτε αλγόριθμος που να το παράγει.

Παράδειγμα μη Κατασκευαστικής Απόδειξης

ΠΑΡΑΔΕΙΓΜΑ

Να δειχτεί ότι υπάρχουν άρρητοι x και y τέτοιοι ώστε ο x^y είναι ρητός.

Απόδειξη.

- Είτε οι $x_1 = \sqrt{2}$, $y_1 = \sqrt{2}$ έχουν την ιδιότητα είτε οι $x_2 = \sqrt{2}^{\sqrt{2}}$, $y_2 = \sqrt{2}$ την έχουν.
- Γιατί; $x_1^{y_1} = x_2$ και $x_2^{y_2} = 2$. Αν x_2 είναι ρητός τότε το πρώτο ζευγάρι έχει την ιδιότητα, διαφορετικά το δεύτερο ζευγάρι την έχει.
- Η απόδειξη είναι μη κατασκευαστική γιατί δεν μας λέει ποια x και y έχουν την ιδιότητα.

□

Μέγιστος κοινός διαιρέτης

- Ο διαχωρισμός σε κατασκευαστικές ή μη αποδείξεις δεν είναι αυστηρός.
- Θα δούμε ένα παράδειγμα δύο αποδείξεων του ιδίου θεωρήματος, μια κατασκευαστική και μια μη κατασκευαστική.

Θεώρημα

Έστω a και b δύο ακέραιοι με μέγιστο κοινό διαιρέτη δ. Τότε υπάρχουν ακέραιοι x και y τέτοιοι ώστε $ax + by = \delta$.

ΠΑΡΑΔΕΙΓΜΑ

$a = 13 \qquad b = 16 \qquad \gcd(a,b) = 1 \qquad x = 5 \qquad y = -4$

Αλγόριθμος του Ευκλείδη

Ο Αλγόριθμος του Ευκλείδη βρίσκει το μέγιστο κοινό διαιρέτη δύο αριθμών.

Αλγόριθμος του Ευκλείδη

```
function EUCLID(a, b)                      ▷ Υποθέτουμε ότι a > b
    if b = 0 then
        return a                           ▷ gcd(a, 0) = a
    else
        δ ← EUCLID(b, a mod b)             ▷ gcd(a, b) = gcd(b, a mod b)
        return δ
    end if
end function
```

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

Γενικευμένος Αλγόριθμος του Ευκλείδη

Με μικρές αλλαγές ο αλγόριθμος επιστρέφει κατάλληλα x και y.

Γενικευμένος Αλγόριθμος του Ευκλείδη

```
function EUCLID(a, b)                              ▷ Υποθέτουμε ότι a > b
    if b = 0 then
        return (a, 1, 0)                           ▷ a·1 + b·0 = a
    else
        (δ, x', y') ← EUCLID(b, a mod b)           ▷ b·x' + (a mod b)·y' = δ
        return (δ, y', x' − ⌊a/b⌋y')               ▷ x = y', y = x' − ⌊a/b⌋y'
    end if
end function
```

$$\begin{aligned}\delta &= bx' + (a \bmod b)y' = bx' + (a - b\lfloor \frac{a}{b} \rfloor)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y').\end{aligned}$$

Μη κατασκευαστική απόδειξη

Δόθηκε στην τάξη όταν παρουσιάσαμε τον αλγόριθμο του Ευκλείδη. Για την ακρίβεια δείξαμε την παρακάτω ισχυρότερη πρόταση, γνωστή ως Λήμμα του Bézout:

$$\text{Αν } a^2 + b^2 > 0, \quad \gcd(a,b) = \min_{\delta > 0}\{\delta = ax + by \mid x, y \in \mathbb{Z}\}.$$

Αρχή του Περιστερεώνα

Πολλές μη κατασκευαστικές αποδείξεις ύπαρξης βασίζονται στο

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε $n-1$ φωλιές, θα υπάρχει μία τουλάχιστον φωλιά με 2 τουλάχιστον περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Αν έχουμε $n+1$ φυσικούς αριθμούς που ανήκουν στο διάστημα $1, \ldots, n$, τότε δύο τουλάχιστον από τους αριθμούς είναι ίσοι. Εδώ τα «περιστέρια» είναι οι αριθμοί και οι «φωλιές» οι αριθμοί $1, \ldots, n$.

Αρχή του Περιστερεώνα

Πολλές μη κατασκευαστικές αποδείξεις ύπαρξης βασίζονται στο

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε $n-1$ φωλιές, θα υπάρχει μία φωλιά με 2 τουλάχιστον περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Αν έχουμε $n+1$ φυσικούς αριθμούς που ανήκουν στο διάστημα $1, \ldots, n$, τότε δύο τουλάχιστον από τους αριθμούς είναι ίσοι. Εδώ τα «περιστέρια» είναι οι αριθμοί και οι «φωλιές» οι αριθμοί $1, \ldots, n$.

Αρχή του Περιστερεώνα

Μερικές φορές χρησιμοποιούμε την πιο γενική μορφή:

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε m φωλιές, θα υπάρχει μία τουλάχιστον φωλιά με τουλάχιστον $\lceil n/m \rceil$ περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 13 ατόμων θα υπάρχουν δύο που γεννήθηκαν τον ίδιο μηνα.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 100 ατόμων θα υπάρχουν τουλάχιστον 9 $(= \lceil 100/12 \rceil)$ που γεννήθηκαν τον ίδιο μήνα.

Μορφές αποδείξεων Αποδείξεις ύπαρξης Αρχή του Περιστερεώνα

Αρχή του Περιστερεώνα

Μερικές φορές χρησιμοποιούμε την πιο γενική μορφή:

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε m φωλιές, θα υπάρχει μία φωλιά με τουλάχιστον $\lceil n/m \rceil$ περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 13 ατόμων θα υπάρχουν δύο που γεννήθηκαν τον ίδιο μηνα.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 100 ατόμων θα υπάρχουν τουλάχιστον 9 $(= \lceil 100/12 \rceil)$ που γεννήθηκαν τον ίδιο μήνα.

Εφαρμογές της Αρχής του Περιστερεώνα

Πρόταση

Κάθε φυσικός αριθμός n έχει ένα ακέραιο πολλαπλάσιο που η δεκαδική του παράσταση αποτελείται από μια σειρά από 1 ακολουθούμενη από μια σειρά από 0, είναι δηλαδή της μορφής $11\ldots100\ldots0$.

ΠΑΡΑΔΕΙΓΜΑ

Για $n = 12$ υπάρχει πολλαπλάσιο αυτής της μορφής: $11100 = 12 \cdot 925$.

Απόδειξη.

Ας θεωρήσουμε τους $n+1$ αριθμούς 1, 11, 111, $\ldots$, $11\ldots1$ και τα υπόλοιπα τους $\mod n$.
Τα υπόλοιπα ανήκουν στο $\{0, \ldots, n-1\}$, άρα από την Αρχή του Περιστερεώνα δύο από τους αριθμούς έχουν το ίδιο υπόλοιπο. Η διαφορά τους είναι πολλαπλάσιο του n. □

Μονότονες υποακολουθίες

- Έστω μια ακολουθία αριθμών, π.χ. 6,2,4,3,7,5.
- Κάθε ακολουθία που προκύπτει όταν αγνοήσουμε μηδέν ή περισσότερους όρους της ακολουθίας λέγεται υποακολουθία. Παράδειγμα: 6,4,3,5.
- Μια ακολουθία λέγεται *μονότονη* αν είναι είτε αύξουσα είτε φθίνουσα. Για παράδειγμα, η 6,4,3 είναι μονότονη, η 6,4,7 δεν είναι μονότονη. Η 6,6,6,6 είναι μονότονη.

Θεώρημα

Κάθε ακολουθία πραγματικών αριθμών με n^2+1 στοιχεία περιέχει μια μονότονη υποακολουθία με $n+1$ στοιχεία.

Μονότονες υποακολουθίες

- Έστω $t_1, \ldots, t_{n^2+1}$ μια ακολουθία. Παράδειγμα: 5,3,4,1,2.
- Ορίζουμε ως α_i να είναι το μήκος της μακρύτερης αύξουσας υποακολουθίας με τελευταίο στοιχείο το t_i. Παράδειγμα: $\alpha_2 = 1$, $\alpha_3 = 2$.
- Ορίζουμε ως ϕ_i να είναι το μήκος της μακρύτερης φθίνουσας υποακολουθίας με τελευταίο στοιχείο το t_i. Παράδειγμα: $\phi_2 = 2$, $\phi_4 = 3$.
- Αν $t_i \le t_j$ για $i < j$, τότε $\alpha_i + 1 \le \alpha_j$. Παράδειγμα: $3 < 4$, άρα $\alpha_2 + 1 \le \alpha_3$.
- Αν $t_i \ge t_j$ για $i < j$, τότε $\phi_i + 1 \le \phi_j$. Παράδειγμα: $3 > 1$, άρα $\phi_2 + 1 \le \phi_4$.
- Αρα, τα ζεύγη (α_i, ϕ_i) είναι όλα διαφορετικά.
- Αν κάθε α_i και ϕ_i είναι το πολύ n, τότε τα $n^2 + 1$ ζεύγη (α_i, ϕ_i) παίρνουν τις n^2 τιμές $(1,1)$, ..., (n,n).
- Από την Αρχή του Περιστερεώνα δύο από τα ζεύγη είναι ίδια, άτοπο.

Προσέγγιση αρρήτων με ρητούς

- ο αριθμός π μπορεί προσεγγιστεί σαν

$$\frac{3}{1}, \quad \frac{31}{10}, \quad \frac{314}{100}, \quad \frac{3141}{1000}, \ldots$$

- Υπάρχει καλύτερη προσέγγιση με άλλους παρονομαστές (όχι απαραίτητα δυνάμεις του 10);
- Ναι. $22/7 = 3.1428\ldots$ ή ακόμα καλύτερα $355/113 = 3.141592\ldots$
- Έστω θ ένας άρρητος αριθμός και m ένας φυσικός αριθμός· πόσο καλά μπορούμε να προσεγγίσουμε τον θ με κλάσματα των οποίων ο παρονομαστής είναι το πολύ m;

Προσέγγιση άρρητου με ρητούς

Θεώρημα (Dirichlet)

Έστω θ ένας πραγματικός αριθμός. Τότε για οποιονδήποτε φυσικό m, υπάρχουν ακέραιοι p και q, με $1 \le q \le m$, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Απόδειξη.

- Ας πάρουμε τα ακέραια πολλαπλάσια $q\theta$, για $q = 0, 1, \ldots, m$ και ας θεωρήσουμε το δεκαδικό μέρος τους $q\theta - \lfloor q\theta \rfloor$.
- Για παράδειγμα τα ακέραια πολλαπλάσια του $\sqrt{2}$ είναι 0, $1.41\ldots$, $2.82\ldots$, $4.24\ldots$ κλπ και το δεκαδικό μέρος τους είναι 0, $0.41\ldots$, $0.82\ldots$, $0.24\ldots$ κλπ.

$\square$

Προσέγγιση άρρητου με ρητούς

Θεώρημα (Dirichlet)

Έστω θ ένας πραγματικός αριθμός. Τότε για οποιονδήποτε φυσικό m, υπάρχουν ακέραιοι p και q, με $1 \le q \le m$, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Απόδειξη.

- Ας πάρουμε τα ακέραια πολλαπλάσια $q\theta$, για $q = 0, 1, \ldots, m$ και ας θεωρήσουμε το δεκαδικό μέρος τους $q\theta - \lfloor q\theta \rfloor$.
- Οι αριθμοί αυτοί είναι της μορφής $q\theta - p$, όπου q και $p = \lfloor q\theta \rfloor$ είναι ακέραιοι.

$\square$

Προσέγγιση αρρήτου με ρητούς

Συνέχεια.

- Για $q = 0, 1, \ldots, m$ υπάρχουν $m + 1$ τέτοιοι αριθμοί και όλοι βρίσκονται στο διάστημα $[0, 1)$.
- Αν θεωρήσουμε τους αριθμούς αυτούς ως περιστέρια και τα διαστήματα $[0, 1/m)$, $[1/m, 2/m)$, $\ldots$, $[(m-1)/m, 1)$ ως φωλιές, μπορούμε να εφαρμόσουμε την Αρχή του Περιστερεώνα.
- Κάποια φωλιά θα περιέχει δύο περιστέρια. Άρα υπάρχουν δύο αριθμοί $q_1\theta - p_1$ και $q_2\theta - p_2$ που διαφέρουν λιγότερο από $1/m$, δηλαδή $|(q_2 - q_1)\theta - (p_2 - p_1)| < 1/m$.
- Ας θέσουμε $q = q_2 - q_1$ και $p = p_2 - p_1$. Οι p και q είναι ακέραιοι στο διάστημα $1 \leq q \leq m$.

$$|q\theta - p| < 1/m \Rightarrow |\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Σχόλια στο Θ. του Dirichlet

Θεώρημα (Dirichlet)

Έστω θ ένας πραγματικός αριθμός. Τότε για οποιονδήποτε φυσικό m, υπάρχουν ακέραιοι p και q, με $1 \leq q \leq m$, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Παρατηρήστε ότι $1 \leq q \leq m \Rightarrow \left[\frac{1}{mq} \leq 1/m \text{ και } \frac{1}{mq} \leq 1/q^2\right]$.

Δύο τρόποι να ερμηνεύσουμε το θεώρημα:

1. Δοθέντος m, υπάρχει ρητή προσέγγιση του θ με απόκλιση μικρότερη από $1/m$.
2. Υπάρχει ρητή προσέγγιση p/q του θ με απόκλιση μικρότερη από $1/q^2$.

Πόσοι ρητοί με τη δεύτερη ιδιότητα υπάρχουν; Το επόμενο πόρισμα μας λέει: άπειροι.

Πόρισμα του Θ. του Dirichlet

Πόρισμα

Έστω θ ένας άρρητος αριθμός. Υπάρχουν άπειροι ρητοί p/q, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{q^2}. \tag{1}$$

Απόδειξη.

Έστω ότι μόνο οι ρητοί $\frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}$ ικανοποιούν την (2).
Αν $\delta = \min_{1 \leq i \leq k} |\theta - \frac{p_i}{q_i}|$, τότε $\delta > 0$. Έστω $M \in \mathbb{Z}_{>0}$ τ. ώ. $1/M < \delta$. Από το Θ. Dirichlet υπάρχει p/r, $1 \leq r \leq M$, τ. ώ.

$$|\theta - \frac{p}{r}| < \frac{1}{Mr} < \delta.$$

Άρα $\frac{p}{r} \notin \{\frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}\}$, άτοπο. □

Πόρισμα του Θ. του Dirichlet

Πόρισμα

Έστω θ ένας άρρητος αριθμός. Υπάρχουν άπειροι ρητοί p/q, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{q^2}. \tag{2}$$

Αν αντικαταστήσουμε το $1/q^2$ με $1/q^a$, $a > 2$, αποδεικνύεται (δύσκολα!) ότι ο αριθμός των λύσεων μπορεί να είναι πεπερασμένος. Για την ακρίβεια, ο αριθμός των λύσεων είναι πάντα πεπερασμένος για αλγεβρικούς αριθμούς $a > 2$.

Προσέγγιση αρρήτων με κοινό παρονομαστή

Η προσέγγιση πολλών άρρητων αριθμών με ρητούς που έχουν κοινό παρονομαστή διευκολύνει την πρόσθεση και την αφαίρεση τους. Π.χ., μια κοινή προσέγγιση του $\sqrt{2} = 1.414\ldots$ και του $\sqrt{3} = 1.732\ldots$ είναι $7/5 = 1.4$ και $9/5 = 1.8$, αντίστοιχα.

Θεώρημα

Έστω $\theta_1, \ldots, \theta_n$ πραγματικοί αριθμοί. Τότε για οποιοδήποτε θετικό ακέραιο m, υπάρχουν ακέραιοι $p_1, \ldots, p_n$ και q, με $1 \leq q \leq m^n$, τέτοιοι ώστε

$$|\theta_i - \frac{p_i}{q}| < \frac{1}{mq}$$

για κάθε $i = 1, \ldots, n$.

Ο μόνος αλγόριθμος που έχουμε για να βρίσκει τέτοιους p_i και q, είναι να δοκιμάσουμε όλες τις m^n δυνατές τιμές του q.

Μονοχρωματικό ορθογώνιο

Θεώρημα

Αν χρωματίσουμε κάθε σημείο του επιπέδου με ακέραιες συντεταγμένες κόκκινο ή μπλε, θα υπάρχει πάντα ορθογώνιο του οποίου οι κορυφές έχουν το ίδιο χρώμα.

Απόδειξη.

Θεωρούμε τις τομές των ευθειών $y = 0, 1, 2$ με τις ευθείες $x = i$, $i = 1, 2, \ldots, 9$. Σε κάθε ευθεία $x = i$ υπάρχουν 3 χρωματισμένα σημεία. Οι διαφορετικοί χρωματισμοί τους είναι $2^3 = 8$, άρα από την ΑτΠ δύο από τις 9 κάθετες ευθείες $x = j$ και $x = k$, $j \neq k$, έχουν τον ίδιο χρωματισμό (δηλ. το χρώμα του (j, y) είναι ίδιο με του (k, y) για $y = 0, 1, 2$.)

Πάλι από την ΑτΠ, δύο από τα σημεία $(j, 0), (j, 1), (j, 2)$ πρέπει να έχουν το ίδιο χρώμα, έστω τα $(j, y_1), (j, y_2)$. Το ορθογώνιο με κορυφές $(j, y_1), (j, y_2), (k, y_1), (k, y_2)$ είναι μονοχρωματικό. □

Χρωματική διατύπωση του Θεωρήματος του Ramsey

Το Θεώρημα του Ramsey μπορεί να ιδωθεί ως μια εκλέπτυνση της ΑτΠ, όπου εγγυώμαστε όχι μόνο ότι πολλά στοιχεία συμπίπτουν σε μια φωλιά, αλλά κι ότι έχουν μια ιδιαίτερη σχέση μεταξύ τους.

Ορισμός

Ένας χρωματισμός των ακμών ενός γραφήματος $G = (V, E)$ είναι μια ανάθεση χρωμάτων στα στοιχεία του E.

Με K_n συμβολίζουμε την κλίκα (πλήρες γράφημα) με n κορυφές.

Θεώρημα (Ramsey)

Για κάθε θετικούς ακέραιους $k, m \geq 2$ υπάρχει φυσικός $R = R(k, m)$ τέτοιος ώστε κάθε χρωματισμός των ακμών του πλήρους γραφήματος K_R με τα χρώματα μπλε και κόκκινο ενάγει ως υπογραφήματα ένα μπλε K_k ή ένα κόκκινο K_m.

Άλλα μη κατασκευαστικά θεωρήματα ύπαρξης

- Θεώρημα Robertson-Seymour για ύπαρξη αλγορίθμου ο οποίος αποφασίζει αν ένα γράφημα G ανήκει σε μια κλειστή ως προς ελάσσονα οικογένεια γραφημάτων.
- Θεώρημα Brouwer. Fixed point theorem.
- Θεώρημα Nash στη Θεωρία Παιγνίων.

Θεωρήματα Brouwer

Ορισμός

Δίνεται συνάρτηση $f : K \to K$. Το $x_0 \in K$ καλείται σταθερό σημείο (fixed point) της f αν $f(x_0) = x_0$.

Θεώρημα

Κάθε συνεχής συνάρτηση $f : [a, b] \to [a, b]$ έχει σταθερό σημείο.

Γενικότερα:

Θεώρημα

Κάθε συνεχής συνάρτηση $f : K \to K$ όπου το K κλειστό, φραγμένο και κυρτό *έχει σταθερό σημείο.*

Παράδειγμα: το K κλειστός δίσκος στον Ευκλείδειο χώρο.