

Διακριτά Μαθηματικά

Πύρρος Χάιδος
Γιάννης Χαμόδρακας

Τμήμα Πληροφορικής & Τηλεπικοινωνιών, ΕΚΠΑ
<http://eclass.uoa.gr/courses/D268/>

Οκτώβριος 2026

Διαφάνειες: Γ. Εμίρης, Γ. Χαμόδρακας, Π. Χάιδος

Οργάνωση και περιεχόμενα Μαθήματος

Λογική και Αποδείξεις

Οργάνωση Μαθήματος

Σύγγραμμα: "Διακριτά Μαθηματικά και Εφαρμογές",
του **Kenneth Rosen**, 8η έκδοση (εκδ. Τζιόλα).



- ▶ Αμφιθέατρο: Δευτέρα και Τετάρτη 11 πμ – 1 μμ
- ▶ Φροντιστήρια (Γιάννης Χαμόδρακας).

Ξεκινούν **τη 2η βδομάδα (θα ανακοινωθεί στο eclass)**:

Δευτέρα 1-3, $AM \bmod 4 = 1$,

Δευτέρα 3-5 μμ, $AM \bmod 4 = 3$,

Τετάρτη 3-5 μμ, $AM \bmod 4 = 0$,

Πέμπτη 1-3, $AM \bmod 4 = 2$.

Βαθμολόγηση

- ▶ 2 πρόοδοι με ~ 1 μήνα διαφορά μεταξύ τους
- ▶ Βαθμός Εξέτασης Φεβρουαρίου =
 $\text{Max} \{ \text{Βαθμός τελικής εξέτασης},$
 $70\% \text{Τελικής} + 15\% \text{Πρόοδος1} + 15\% \text{Πρόοδος2} \}$
- ▶ Εξέταση Σεπτεμβρίου: Ομοίως.

Τι είναι τα Διακριτά Μαθηματικά;

Είναι η μελέτη **διακριτών** μαθηματικών αντικειμένων:

- ▶ σύνολα, π.χ. $\{\alpha, \epsilon, \eta, \iota, \omicron, \upsilon, \omega\}$,
- ▶ ακέραιοι αριθμοί και υποσύνολά τους: $\{0, 2, 4, 8, 16, \dots\}$,
- ▶ αριθμητικές συναρτήσεις: με πεδίο ορισμού τους ακεραίους,
- ▶ πρώτοι αριθμοί $2, 3, 5, 7, 11, 13, \dots$,
- ▶ γραφήματα.

Αναπαρίστανται με **απόλυτη ακρίβεια** στον Υπολογιστή!

Τι **ΔΕΝ** εξετάζουμε; Συνεχή αντικείμενα, Αριθμητική ανάλυση.

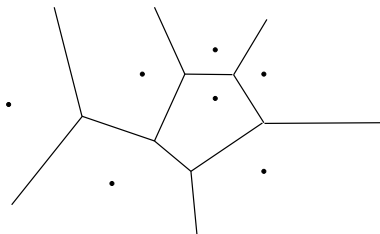
Αντιστοιχία διακριτών/συνεχών αντικειμένων

Διακριτά αντικείμενα	Συνεχή αντικείμενα
$\mathbb{Z}, \mathbb{Q}$	$\mathbb{R}, \mathbb{C}$
σύνολο $\{0, 1, 2, 3\}$, ακολουθία $(0, 1, 2, 3)$	διάστημα $[0, 3]$ ή $(0, 3)$
άθροισμα $\sum_{k=0}^N k = \frac{N(N+1)}{2} = \frac{N^2}{2} + \frac{N}{2}$	ολοκλήρωμα $\int_0^N t \, dt = \frac{t^2}{2} \Big _0^N = \frac{N^2}{2}$
διακριτή πιθανότητα γεγονός $\in$ δειγματικό χώρο $\Delta = \{K, \Gamma\}$	συνεχής πιθανότητα $\Delta = [0, 1]$

Γιατί μελετάμε τα Διακριτά Μαθηματικά ;

A. Αλγόριθμοι και Πολυπλοκότητα:

- ▶ ανάλυση πολυπλοκότητας μέσω αριθμητικών συναρτήσεων,
- ▶ πιθανοκρατικοί αλγόριθμοι:
αποφεύγουν χειρίστη περίπτωση,
- ▶ βελτιστοποίηση στην επιχειρησιακή έρευνα,
π.χ. δρομολόγια αεροπορικών εταιριών,
- ▶ γεωμετρικοί αλγόριθμοι,
π.χ. κυρτό περίβλημα, διάγραμμα Voronoi.
- ▶ δομές και βάσεις δεδομένων.



Γιατί μελετάμε τα Διακριτά Μαθηματικά;

Β. Κρυπτογραφία, κωδικοποίηση, ασφάλεια:

- ▶ υπολογιστικών προβλήματα: υπολογισμός ρίζας σε ομάδες **RSA**, διακριτός λογάριθμος, **Lattices**.
- ▶ **Https**, ψηφιακές υπογραφές, **VPN**, κρυπτονομίσματα.
- ▶ **RAID**, συμπίεση δεδομένων, διόρθωση σφαλμάτων σε δίσκους,

Γ. Τηλεπικοινωνιακά δίκτυα:

- ▶ αλγόριθμοι σε γραφήματα,
- ▶ συνδυαστική και πιθανότητες.
- ▶ διασφάλιση ακεραιότητας, διόρθωση σφαλμάτων

Δ. Λογική σχεδίαση και Γλώσσες προγραμματισμού / μεταγλωττιστές

- ▶ λογικές προτάσεις, θεωρία συνόλων.

Ε. Διατύπωση Προδιαγραφών

- ▶ λογικές ισοδυναμίες, συνεπαγωγές, αποδείξεις

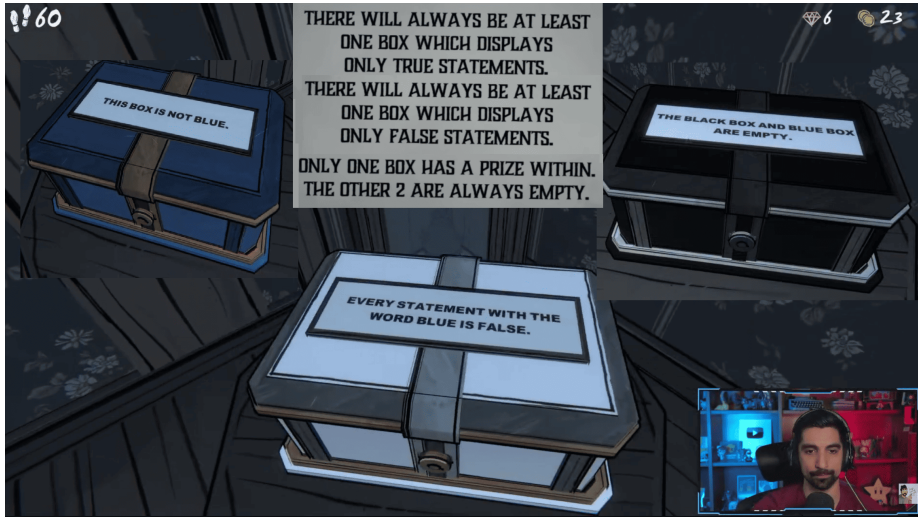
Στην καθημερινότητα

- ▶ Πώς θα υπολογίσω το $AM \bmod 4$;
- ▶ Πώς θα μάθω την αλήθεια χωρίς να ξέρω αν αυτός που απαντά είναι ψεύτης ή όχι;
- ▶ Ποιος είναι ο αποδοτικότερος αλγόριθμος ώστε να αντιμετωπίσει μαζικά δεδομένα;
- ▶ Ποια η πιθανότητα δύο τυχαίοι φοιτητές του μαθήματος να έχουν την ίδια ημέρα γενέθλια;

Στην καθημερινότητα: Υπολογισμός $N \bmod 4$

- ▶ Κρατάμε τα 2 τελευταία ψηφία μόνο.
 $100 = 25 \cdot 4$ άρα αφαιρώντας ακέραιες εκατοντάδες δεν αλλάζει το υπόλοιπο.
- ▶ Από κάθε ψηφίο ≥ 4 αφαιρούμε 4 μέχρι να γίνει < 4 . Αφαιρώντας ακέραιες σαραντάδες ή τετράδες δεν αλλάζει το υπόλοιπο.
- ▶ Προσθέτουμε 2 φορές το ψηφίο των δεκάδων στις μονάδες. Μια δεκάδα $= 8 + 2$. Παραλείπω το 8 ως πολλαπλάσιο του 4, προσθέτω το 2.
- ▶ Αν το άθροισμα ≥ 4 αφαιρούμε 4 μέχρι να γίνει < 4 .

Στην καθημερινότητα: Blue Prince¹



Περιεχόμενα μαθήματος

1. Λογική, Προτάσεις
2. Σύνολα
3. Απαρίθμηση, εγκλεισμός-αποκλεισμός
4. Μεταθέσεις, συνδυασμοί,
5. Επαγωγή
6. Ασυμπτωτική πολυπλοκότητα αλγορίθμων

Οργάνωση και περιεχόμενα Μαθήματος

Λογική και Αποδείξεις

Προτασιακή Λογική

Κατηγορήματα και ποσοδείκτες

Συνεπαγωγή (συμπερασμός)

Αποδείξεις

Οργάνωση και περιεχόμενα Μαθήματος

Λογική και Αποδείξεις

Προτασιακή Λογική

Κατηγορήματα και ποσοδείκτες

Συνεπαγωγή (συμπερασμός)

Αποδείξεις

Προτασιακή Λογική

Rosen, Κεφ. 1

Μαθηματικές / λογικές προτάσεις [Rosen 1.1, 1.2]

Ορισμός (Πρόχειρος).

(Μαθηματική ή λογική) **πρόταση** είναι μια δήλωση η οποία είναι είτε αληθής είτε ψευδής, αλλά όχι και τα δύο.

Παράδειγμα.

Η Ουάσιγκτον είναι η πρωτεύουσα των Η.Π.Α.

Παράδειγμα.

$$2 + 2 = 3$$

Παράδειγμα.

Θα βρέξει αύριο.

Μη παράδειγμα.

Τι ώρα γίνεται το μάθημα των Διακριτών;

Μη παράδειγμα.

Ο n είναι άρτιος

Πράξεις και Πίνακες Αληθείας

- ▶ **άρνηση** της p : $\bar{p}$ ή $\neg p$,
- ▶ **διάζευξη** (ή): $p \vee q$ αληθής αν μία ή 2 προτάσεις ισχύουν,
- ▶ **αποκλειστική διάζευξη** (είτε-είτε, xor, $\oplus$): $p \underline{\vee} q$ αληθής αν ακριβώς μία αρχική πρόταση αληθεύει,
- ▶ **σύζευξη** (και): $p \wedge q$ αληθής αν και οι 2 προτάσεις ισχύουν,
- ▶ **ισοδυναμία** (αν και μόνον αν, ανν, iff): $p \leftrightarrow q$ είναι αληθής αν οι δυο προτάσεις έχουν τους ίδιους πίνακες αληθείας,

p	q	$p \vee q$	$p \underline{\vee} q$	$p \wedge q$	$p \leftrightarrow q$
F	F	F	F	F	T
F	T	T	T	F	F
T	F	T	T	F	F
T	T	T	F	T	T

Ειδικές περιπτώσεις προτάσεων

Ορισμός.

Ταυτολογία καλείται κάθε πρόταση που είναι πάντα αληθής (συμβολίζεται $1, A$ ή T).

Ορισμός.

Αντίφαση καλείται κάθε πρόταση που είναι πάντα ψευδής (συμβολίζεται $0, \Psi$ ή F).

Κάτω από το καπό

Τυπικά, μια πρόταση μπορεί να είναι:

- ▶ Μια προτασιακή μεταβλητή: ατομική (απλή) πρόταση
- ▶ Συνδυασμός προτάσεων μέσω μιας πράξης: σύνθετη πρόταση



Σύνθετες προτάσεις: Συνεπαγωγή

Αν p τότε q : $p \rightarrow q$.

Παράδειγμα.

Αν κάποιος είναι επισκέπτης, τότε φοράει κονκάρδα.

p	q	$p \rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

Παράδειγμα.

Αν αντιγράψεις από τον διπλανό σου, τότε μηδενίζεσαι.

Άσκηση.

Δείξτε την ισοδυναμία συνεπαγωγής με μια κατάλληλη διάζευξη.

Σύνθετες προτάσεις: Αντιθετοαναστροφή

Έστω η σύνθετη πρόταση $p \rightarrow q$.

- ▶ Ανάστροφη: $q \rightarrow p$
- ▶ Αντιθετοανάστροφη: $\neg q \rightarrow \neg p$
- ▶ Αντίστροφη: $\neg p \rightarrow \neg q$

Ισοδύναμες με την αρχική;

p	q	$p \rightarrow q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$	$\neg p \rightarrow \neg q$
0	0	1	1	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	1	1	1	1	1

Σύνθετες προτάσεις: διπλή συνεπαγωγή

Ορισμός.

Ο συμβολισμός $p \leftrightarrow q$ εκφράζει την πρόταση p αν και μόνο αν q .

Άσκηση.

Η πρόταση $(p \leftrightarrow q)$ είναι ισοδύναμη με τη σύνθετη πρόταση $[(p \rightarrow q) \wedge (q \rightarrow p)]$.

ΑΠΟΔΕΙΞΗ:

Σύνθετες προτάσεις: διπλή συνεπαγωγή

Ορισμός.

Ο συμβολισμός $p \leftrightarrow q$ εκφράζει την πρόταση p αν και μόνο αν q .

Άσκηση.

Η πρόταση $(p \leftrightarrow q)$ είναι ισοδύναμη με τη σύνθετη πρόταση $[(p \rightarrow q) \wedge (q \rightarrow p)]$.

ΑΠΟΔΕΙΞΗ:

p	q	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$[\dots \wedge \dots]$
F	F	T	T	T	T
F	T	F	T	F	F
T	F	F	F	T	F
T	T	T	T	T	T

Παράδειγμα

Μπορείτε να έχετε πρόσβαση στο ίντερνετ αν σπουδάζετε πληροφορική ή αν δεν είστε νέοι φοιτητές:

$$(q \vee \bar{r}) \rightarrow p.$$

p	Πρόσβαση στο ίντερνετ
q	Σπουδάζω πληροφορική
r	Είμαι νέος φοιτητής

Μπορείτε να έχετε πρόσβαση στο ίντερνετ μόνο αν σπουδάζετε πληροφορική ή αν δεν είστε νέοι φοιτητές:

$$p \rightarrow (q \vee \bar{r}) \equiv p \rightarrow (r \rightarrow q)$$

Προτασιακές Ισοδυναμίες [Rosen 1.3]

Ορισμός.

Λογικά ισοδύναμες είναι **2** προτάσεις με τον ίδιο πίνακα αλήθειας

Όταν δυο προτάσεις α, β είναι ισοδύναμες, χρησιμοποιούμε τον συμβολισμό $\alpha \Leftrightarrow \beta$ ή το σύμβολο $\equiv$. Διαβάζεται “αν και μόνο αν” και το γράφουμε “ανν” (if and only if ή iff).

Όταν ισχύει η ισοδυναμία $\alpha \equiv \beta$ ισχύουν τα εξής:

- ▶ το α είναι επαρκής συνθήκη για το β , δηλ. « β εάν α »: $\alpha \Rightarrow \beta$.
- ▶ το α είναι αναγκαία συνθήκη για το β , δηλ. « β μόνο αν α »: $\alpha \Leftarrow \beta$.
- ▶ το $\alpha \leftrightarrow \beta$ είναι ταυτολογία.

Ιδιότητες

Ιδιότητες όπως οι παρακάτω (των οποίων η απόδειξη αφήνεται ως άσκηση) απλοποιούν τις αποδείξεις και αποφεύγουν την κατασκευή ενός εξαντλητικού πίνακα αληθείας.

- ▶ Ταυτολογίες: $x \vee \neg x \equiv T$, $x \leftrightarrow x \equiv T$.
- ▶ Προσεταιριστική ιδιότητα: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$,
 $(p \vee q) \vee r \equiv p \vee (q \vee r)$ και $(p \leftrightarrow q) \leftrightarrow r \equiv p \leftrightarrow (q \leftrightarrow r)$.
- ▶ Επιμεριστική ιδιότητα: $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$
και $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$.

Άσκηση

Ν.δ.ό. $[(p \wedge q) \vee (\neg p \wedge \neg q)] \equiv [(p \vee \neg q) \wedge (\neg p \vee q)]$.

Απόδειξη.

$$\begin{aligned} [(p \wedge q) \vee (\neg p \wedge \neg q)] &\equiv \\ &\equiv [(p \wedge q) \vee \neg p] \wedge [(p \wedge q) \vee \neg q] && : \text{επιμεριστικότητα} \\ &\equiv [(p \vee \neg p) \wedge (q \vee \neg p)] \wedge [(p \vee \neg q) \wedge (q \vee \neg q)] && : \text{επιμεριστ.} \\ &\equiv (p \vee \neg p) \wedge (q \vee \neg p) \wedge (p \vee \neg q) \wedge (q \vee \neg q) && : \text{προσεταιρ.} \\ &\equiv (q \vee \neg p) \wedge (p \vee \neg q) && : \text{ταυτολογία } X \vee \neg X \end{aligned}$$

Ιδιότητες De Morgan

Να δείχτεί ότι:

- ▶ $\neg(p \wedge q) \equiv \neg p \vee \neg q$,
- ▶ $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Απόδειξη ($\neg(p \wedge q) \equiv \neg p \vee \neg q$).

Πίνακες Αληθείας

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Άσκηση

Νδó: $p \vee q \equiv [((p \wedge q) \vee (\neg p \wedge \neg q)) \rightarrow p]$.

Απόδειξη.

p	q	$p \vee q$	$p \wedge q$	$(\neg p \wedge \neg q)$	$\vee$	$\vee \rightarrow p$
0	0	0	0	1	1	0
0	1	1	0	0	0	1
1	0	1	0	0	0	1
1	1	1	1	0	1	1

Γρίφος

Υπάρχουν δύο ομάδες στο χωριό, η μία λέει πάντα αλήθεια (ιππότες), η άλλη ποτέ (πότες).

- ▶ Ερώτηση 1 (μη χρήσιμη): Λες την αλήθεια;
Απάντηση κατοίκου Κ: «Λεω την αλήθεια». (δεν είμαι πότης).
- ▶ (κακή) Ερώτηση 2 (μη χρήσιμη): Υπάρχει χρυσός στο χωριό;
Απάντηση κατοίκου Κ: «Υπάρχει».

Γρίφος

Υπάρχουν δύο ομάδες στο χωριό, η μία λέει πάντα αλήθεια (ιππότες), η άλλη ποτέ (πότες).

- ▶ Ερώτηση 1 (μη χρήσιμη): Λες την αλήθεια;
Απάντηση κατοίκου K: «Λεω την αλήθεια». (δεν είμαι πότης).
- ▶ (κακή) Ερώτηση 2 (μη χρήσιμη): Υπάρχει χρυσός στο χωριό;
Απάντηση κατοίκου K: «Υπάρχει».

Λύση. Πρόταση **A**: "ο K λέει αλήθεια", πρόταση **X**: " $\exists$ χρυσός".

Ο κάτοικος απάντησε, **A** και **X** όμως εμείς ξέρουμε ότι οι απαντήσεις είναι αλήθεια μόνο αν **A**.

A	X	Απάντηση 1 $A \leftrightarrow A$	Απάντηση 2: $X \leftrightarrow A$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	1	1

Γρίφος II

Υπάρχουν δύο ομάδες στο χωριό, η μία λέει πάντα αλήθεια (ιππότες), η άλλη ποτέ (πότες).

- Ερώτηση 3: Η πρόταση «Υπάρχει ανν λέω την αλήθεια» ισχύει για εσένα;

Απάντηση κατοίκου K: ...

Λύση. Πρόταση **A**: "ο K λέει αλήθεια", πρόταση **X**: " $\exists$ χρυσός".

Ο κάτοικος απάντησε, **A**, **X** και **A** $\leftrightarrow$ **X** αντίστοιχα.

A	X	πραγματική απάντ. $A \leftrightarrow X$	δοθείσα απ. $A \leftrightarrow (A \leftrightarrow X)$
0	0	1	0
0	1	0	1
1	0	0	0
1	1	1	1

Γρίφος II

Υπάρχουν δύο ομάδες στο χωριό, η μία λέει πάντα αλήθεια (ιππότες), η άλλη ποτέ (πότες).

- Ερώτηση 3: Η πρόταση «Υπάρχει ανν λέω την αλήθεια» ισχύει για εσένα;

Απάντηση κατοίκου K: ...

Λύση. Πρόταση A: "ο K λέει αλήθεια", πρόταση X: " $\exists$ χρυσός".

Ο κάτοικος απάντησε, A, X και $A \leftrightarrow X$ αντίστοιχα.

A	X	πραγματική απάντ. $A \leftrightarrow X$	δοθείσα απ. $A \leftrightarrow (A \leftrightarrow X)$
0	0	1	0
0	1	0	1
1	0	0	0
1	1	1	1

Αφού η δοθείσα απάντηση είναι 1, υπάρχει χρυσός (περιπτώσεις 2,4).



Γρίφος (Εναλλακτικές)

Συντομότερη διερεύνηση.

Η δοθείσα απάντηση είναι: $A \leftrightarrow (A \leftrightarrow X)$.

Όμως: $A \leftrightarrow (A \leftrightarrow X) \equiv (A \leftrightarrow A) \leftrightarrow X \equiv 1 \leftrightarrow X \equiv X$.

Το $1 \leftrightarrow X \equiv X$ δεν το έχουμε δείξει, αλλά αποδεικνύεται εύκολα.

Άρα, υπάρχει χρυσός.

Γρίφος (Εναλλακτικές)

Συντομότερη διερεύνηση.

Η δοθείσα απάντηση είναι: $A \leftrightarrow (A \leftrightarrow X)$.

Όμως: $A \leftrightarrow (A \leftrightarrow X) \equiv (A \leftrightarrow A) \leftrightarrow X \equiv 1 \leftrightarrow X \equiv X$.

Το $1 \leftrightarrow X \equiv X$ δεν το έχουμε δείξει, αλλά αποδεικνύεται εύκολα.

Άρα, υπάρχει χρυσός.

Εναλλακτικά θέτουμε την ερώτηση σε κάποιον κάτοικο:

"Τι θα απαντήσει ένας κάτοικος της άλλης ομάδας ως προς την ύπαρξη χρυσού;"

Άσκηση.

Δείξτε πως υπάρχει χρυσός αν η απάντηση είναι ΟΧΙ.

Και εδώ, μαθαίνω για τον χρυσό χωρίς να ανακαλύπτω την ομάδα του κατοίκου.

Ιδιότητες προτασιακής λογικής

Άσκηση.

$p \wedge p$	$\equiv$	p
$q \vee q$	$\equiv$	q
$p \rightarrow q$	$\equiv$	$\neg p \vee q$
$p \rightarrow q$	$\equiv$	$\neg q \rightarrow \neg p$
$p \vee q$	$\equiv$	$\neg p \rightarrow q$
$p \wedge q$	$\equiv$	$\neg(p \rightarrow \neg q)$
$p \leftrightarrow q$	$\equiv$	$(p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q$	$\equiv$	$\neg p \leftrightarrow \neg q$

Πλήρεις πίνακες ιδιοτήτων στην Ενότητα 1.2 του Rosen.

Παράδοξα

Η θεωρία μας των προτάσεων (και συνόλων) δεν περιγράφει κάθε δυνατό σύστημα.

Π.χ. Έστω άνθρωποι που λένε είτε αλήθεια είτε ψέμματα.

"Όλοι οι Κρητικοί είναι ψεύτες", είπε ο Κ ο Κρητικός.

Πρόβλημα αυτοαναφοράς (επιλύσιμο;) [Επιμενίδης].

Π.χ. Ο Χ λέει: "Είμαι ψεύτης".

Η πρόταση δεν είναι ούτε Α ούτε Ψ. [Ευβουλίδης]

Παράδοξο του **Russell**: Έστω $\mathcal{R}$ το σύνολο των συνόλων που δεν ανήκουν στον εαυτό τους. Αδύνατον να αποφασίσουμε αν $\mathcal{R} \in \mathcal{R}$.

Οργάνωση και περιεχόμενα Μαθήματος

Λογική και Αποδείξεις

Προτασιακή Λογική

Κατηγορήματα και ποσοδείκτες

Συνεπαγωγή (συμπερασμός)

Αποδείξεις

Κατηγορήματα και ποσοδείκτες [Rosen 1.4]

Ορισμός.

Μια προτασιακή συνάρτηση (ή **κατηγορήμα**) είναι μια δήλωση της οποίας η λογική τιμή εξαρτάται από την τιμή μίας ή περισσότερων **μεταβλητών**.

Παράδειγμα.

Η προτασιακή συνάρτηση

$$P(x) : x > 3$$

Και οι προτάσεις

$$P(2) \text{ (ψευδής), } P(4) \text{ (αληθής)}$$

Ποσοδείκτες

Εστω μεταβλητή x σε ένα πεδίο ορισμού (ή πεδίο).

- ▶ **Υπαρξιακή πρόταση:** $\exists x : P(x)$ (υπάρχει x τέτοιο ώστε το κατηγορημα P να είναι αληθές για το x).
Π.χ. " $\exists x \in \mathbb{R} : x \notin \mathbb{Q}$ ", ισχύει για $x = \pi$.
- ▶ **Καθολική πρόταση:** $\forall x : P(x)$.
Αποδεικνύεται ανδειχθεί $P(a)$ για όλα τα a στο πεδίο ορισμού της x .
Π.χ. $\forall n : n^2 > n$ (ψευδής)
Π.χ. $\forall n : n^2 + 1 > n$ (αληθής) (Γιατί;)

Αρνηση ποσοτικοποιημένων εκφράσεων

Οι κανόνες De Morgan για ποσοδείκτες:

Αρνηση	Ισοδύναμη πρόταση
$\neg(\exists x : P(x))$	$\forall x : \neg P(x)$
$\neg (\Upsilon\acute{\alpha}\rho\chi\epsilon\iota \text{ ελεύθερη θέση στο } 250)$	Κάθε θέση στο 250 είναι πιασμένη
$\neg(\forall x : P(x))$	$\exists x : \neg P(x)$

Άρνηση ποσοτικοποιημένων συνεπαγωγών

$A(x)$: Το x είναι ακριβό

$P(x)$: Το x βγάζει προβλήματα

- ▶ **Καθολική πρόταση:** «Τα ακριβά ΙΧ βγάζουν προβλήματα»
 $\forall x : A(x) \rightarrow P(x)$.
- ▶ **Πιθανή Άρνηση 1:** «τα φτηνά ΙΧ βγάζουν προβλήματα»
- ▶ **Πιθανή Άρνηση 2:** «τα ακριβά ΙΧ δεν βγάζουν προβλήματα»
- ▶ **Πιθανή Άρνηση 3:** «το ακριβό ΙΧ της κουμπάρας του ξαδέρφου μου βγήκε καλό»

Άρνηση ποσοτικοποιημένων συνεπαγωγών

$A(x)$: Το x είναι ακριβό

$P(x)$: Το x βγάζει προβλήματα

- ▶ **Καθολική πρόταση:** «Τα ακριβά ΙΧ βγάζουν προβλήματα»
 $\forall x : A(x) \rightarrow P(x)$.
 - ▶ **Πιθανή Άρνηση 1:** «τα φτηνά ΙΧ βγάζουν προβλήματα»
 - ▶ **Πιθανή Άρνηση 2:** «τα ακριβά ΙΧ δεν βγάζουν προβλήματα»
 - ▶ **Πιθανή Άρνηση 3:** «το ακριβό ΙΧ της κουμπάρας του ξαδέρφου μου βγήκε καλό»
 - ▶ **1:** Ασχέτο από τα ακριβά ΙΧ $\forall x : \neg A(x) \rightarrow P(x)$.
 - ▶ **2:** Υπερβολικά ισχυρό $\forall x : A(x) \rightarrow \neg P(x)$.
 - ▶ **3:** Σωστό $\exists x : A(x) \wedge \neg P(x)$.
- Σημειωση. $p \rightarrow q \equiv \neg p \vee q$ άρα $\neg(p \rightarrow q) \equiv \neg(\neg p \vee q)$.
Από De Morgan $\neg(\neg p \vee q) \equiv (\neg\neg p) \wedge (\neg q) \equiv p \wedge \neg q$

Άρνηση ποσοτικοποιημένων συνεπαγωγών II

- Καθολική πρόταση: $\forall x : Y(x) \rightarrow P(x)$.

Καταρρίπτεται με **αντιπαράδειγμα** $x = a : Y(a) \equiv T, P(a) \equiv F$

Π.χ. " $\forall n \in \mathbb{N}$, αν n άρτιος τότε $n^2 > 3$ " ψευδής: $n = 0, 0^2 < 3$.

Η άρνηση είναι η υπαρξιακή πρόταση: $\exists x : Y(x) \wedge \neg P(x)$.

Άρνηση ποσοτικοποιημένων συνεπαγωγών II

- Καθολική πρόταση: $\forall x : Y(x) \rightarrow P(x)$.

Καταρρίπτεται με **αντιπαράδειγμα** $x = a : Y(a) \equiv T, P(a) \equiv F$

Π.χ. " $\forall n \in \mathbb{N}$, αν n άρτιος τότε $n^2 > 3$ " ψευδής: $n = 0, 0^2 < 3$.

Η άρνηση είναι η υπαρξιακή πρόταση: $\exists x : Y(x) \wedge \neg P(x)$.

- Υπαρξιακή πρόταση συνεπαγωγής: $\exists x : Y(x) \rightarrow P(x)$.

Καταρρίπτεται αν $\forall x$: και ισχύει $Y(x)$ και ισχύει $\neg P(x)$.

Άρνηση της υπαρξιακής πρότασης είναι η καθολική:

" $\forall x : Y(x) \wedge \neg P(x)$ ".

Άρνηση ποσοτικοποιημένων συνεπαγωγών II

- Καθολική πρόταση: $\forall x : Y(x) \rightarrow P(x)$.

Καταρρίπτεται με **αντιπαράδειγμα** $x = a : Y(a) \equiv T, P(a) \equiv F$

Π.χ. " $\forall n \in \mathbb{N}$, αν n άρτιος τότε $n^2 > 3$ " ψευδής: $n = 0, 0^2 < 3$.

Η άρνηση είναι η υπαρξιακή πρόταση: $\exists x : Y(x) \wedge \neg P(x)$.

- Υπαρξιακή πρόταση συνεπαγωγής: $\exists x : Y(x) \rightarrow P(x)$.

Καταρρίπτεται αν $\forall x$: και ισχύει $Y(x)$ και ισχύει $\neg P(x)$.

Άρνηση της υπαρξιακής πρότασης είναι η καθολική:

" $\forall x : Y(x) \wedge \neg P(x)$ ".

- Τεστ κατανόησης:

$\exists n : (n \text{ άρτιος} \rightarrow n^2 = 25)$

1. Όταν $n \in [0, 2, 4, 6, 8, \dots]$
2. Όταν $n \in [1, 3, 5, 7, \dots]$
3. Όταν $n \in \mathbb{N}$

Ποσοτικοποίηση δύο μεταβλητών [Rosen 1.5]

- ▶ Πρόταση: $\forall x \forall y : P(x, y)$ ισοδύναμη με: $\forall y \forall x : P(x, y)$.
Αληθής αν η $P(x, y)$ αληθεύει για κάθε ζεύγος x, y .
Ψευδής αν υπάρχει ζεύγος x, y για το οποίο η $P(x, y)$ είναι ψευδής.
- ▶ Πρόταση: $\forall x \exists y : P(x, y)$.
Αληθής αν, για κάθε x , υπάρχει y για το οποίο η $P(x, y)$ αληθεύει.
Ψευδής αν υπάρχει x τ.ώ. η $P(x, y)$ είναι ψευδής για κάθε y , δηλαδή:
 $\exists x \forall y : \neg P(x, y)$.

Φωλιασμένοι ποσοδείκτες

Αν υπάρχουν ποσοδείκτες δύο ειδών, η **σειρά** τους έχει σημασία.

Εστω $x, y, z \in \mathbb{R}$.

$\forall x, \exists y, z : x = y + z$: αληθής, διότι $z = x - y$.

$\exists y, z : \forall x, x = y + z$: ψευδής, διότι $\forall y, z, \exists x = y + z + 1 \neq y + z$

Π.χ. $\forall n \in \mathbb{N}^*, \exists$ πρώτος p τ.ώ. $n < p \leq n! + 1$.

Απόδειξη.

Αν ο $n! + 1$ είναι πρώτος, η απόδειξη έληξε με $p = n! + 1$.

Αλλιώς, $\exists$ πρώτος $q \mid n! + 1$, $2 \leq q < n! + 1$.

Αν $q > n$, θέτω $p = q$.

Αλλιώς $2 \leq q \leq n$, τότε $q \mid n!$. Επίσης $q \mid n! + 1$: άτοπο.

Ψευδές: $\exists$ πρώτος $p : \forall n \in \mathbb{N}^*, n < p \leq n! + 1$.

Οργάνωση και περιεχόμενα Μαθήματος

Λογική και Αποδείξεις

Προτασιακή Λογική

Κατηγορήματα και ποσοδείκτες

Συνεπαγωγή (συμπερασμός)

Αποδείξεις

Συνεπαγωγή και ισοδυναμία

$\alpha \Leftrightarrow \beta$ σημαίνει: α αν και μόνον αν β ,
δηλ. η α είναι αναγκαία και επαρκής συνθήκη για την β ,
δηλ. ισχύουν τα εξής:

- ▶ Επαρκής συνθήκη: $\alpha \Rightarrow \beta$ (ισχύει β όταν / εάν ισχύει α).

Π.χ. $x = 3 \Rightarrow x^2 = 9$. Δεν είναι όμως και αναγκαία!
($x = 3 \nRightarrow x^2 = 9$).

Ισοδύναμα $\neg\beta \Rightarrow \neg\alpha$.

- ▶ Αναγκαία συνθήκη: $\alpha \Leftarrow \beta$ (ισχύει β μόνο αν ισχύει α).

Π.χ. $x^2 > 4 \Leftarrow x > 2$. Δεν είναι όμως και επαρκής!
($x^2 > 4 \nRightarrow x > 2$).

Ισοδύναμα $\neg\alpha \Rightarrow \neg\beta$.

- ▶ Αν η α είναι επαρκής συνθήκη για τη β , τότε η β είναι αναγκαία για την α

Κανόνες συμπερασμού [Rosen 1.6]

Ορισμός.

Επιχείρημα καλείται μια ακολουθία προτάσεων: όλες εκτός της τελευταίας καλούνται υποθέσεις, ενώ η τελευταία καλείται συμπέρασμα.

Ενα επιχείρημα είναι ορθό αν η αλήθεια των υποθέσεων συνεπάγεται την αλήθεια του συμπεράσματος.

Ορθά επιχειρήματα / Κανόνες / Ταυτολογίες:

- ▶ **Modus ponens:** $(p \wedge (p \rightarrow q)) \Rightarrow q$ Μέθοδος της επιβεβαίωσης.
- ▶ **Modus tollens:** $(\neg q \wedge (p \rightarrow q)) \Rightarrow \neg p$. Μέθοδος της διάψευσης
- ▶ **Υποθετικός συλλογισμός:** $((p \rightarrow q) \wedge (q \rightarrow r)) \Rightarrow (p \rightarrow r)$.
- ▶ **Διαζευτικός συλλογισμός:** $((p \vee q) \wedge \neg p) \Rightarrow q$.
- ▶ **Επίλυση:** $((p \vee q) \wedge (\neg p \vee r)) \Rightarrow (q \vee r)$.
- ▶ **Πρόσθεση:** $p \Rightarrow (p \vee q)$.
- ▶ **Απλοποίηση:** $(p \wedge q) \Rightarrow p$.

Παράδειγμα συμπερασμού

Παράδειγμα.

Έστω p η πρόταση «Μελετώ διακριτά» και q : «Περνάω τα διακριτά», και η πρόταση $p \rightarrow q$ «Αν διαβάσω διακριτά θα περάσω».

Εξετάζουμε τα επιχειρήματα:

1. Η ακολουθία $(p, p \rightarrow q, q)$ ή ισοδύναμα «Αν $(p \rightarrow q)$ και διαβάσω τότε περνάω».
2. Αν $(p \rightarrow q)$ και δεν διαβάσω τότε δεν περνάω.
3. Αν $(p \rightarrow q)$ και περάσω τότε είχα διαβάσει.
4. Αν $(p \rightarrow q)$ και δεν περάσω τότε δεν είχα διαβάσει.

Παράδειγμα συμπερασμού

Παράδειγμα.

Έστω p η πρόταση «Μελετώ διακριτά» και q : «Περνάω τα διακριτά», και η πρόταση $p \rightarrow q$ «Αν διαβάσω διακριτά θα περάσω».

Εξετάζουμε τα επιχειρήματα:

1. Η ακολουθία $(p, p \rightarrow q, q)$ ή ισοδύναμα «Αν $(p \rightarrow q)$ και διαβάσω τότε περνάω».
2. Αν $(p \rightarrow q)$ και δεν διαβάσω τότε δεν περνάω.
3. Αν $(p \rightarrow q)$ και περάσω τότε είχα διαβάσει.
4. Αν $(p \rightarrow q)$ και δεν περάσω τότε δεν είχα διαβάσει.

1. $p \wedge (p \rightarrow q) \Rightarrow q$
2. $\neg p \wedge (p \rightarrow q) \Rightarrow \neg q$
3. $q \wedge (p \rightarrow q) \Rightarrow p$
4. $\neg q \wedge (p \rightarrow q) \Rightarrow \neg p$

Παράδειγμα συμπερασμού

Παράδειγμα.

Έστω p η πρόταση «Μελετώ διακριτά» και q : «Περνάω τα διακριτά», και η πρόταση $p \rightarrow q$ «Αν διαβάσω διακριτά θα περάσω».

Εξετάζουμε τα επιχειρήματα:

1. Η ακολουθία $(p, p \rightarrow q, q)$ ή ισοδύναμα «Αν $(p \rightarrow q)$ και διαβάσω τότε περνάω».
2. Αν $(p \rightarrow q)$ και δεν διαβάσω τότε δεν περνάω.
3. Αν $(p \rightarrow q)$ και περάσω τότε είχα διαβάσει.
4. Αν $(p \rightarrow q)$ και δεν περάσω τότε δεν είχα διαβάσει.

$$1. p \wedge (p \rightarrow q) \Rightarrow q$$

$$2. \neg p \wedge (p \rightarrow q) \Rightarrow \neg q$$

$$3. q \wedge (p \rightarrow q) \Rightarrow p$$

$$4. \neg q \wedge (p \rightarrow q) \Rightarrow \neg p$$

Παράδειγμα σύνθετου συμπερασμού

Παράδειγμα.

Δείξτε ότι οι προτάσεις "Δεν έχει ήλιο σήμερα και ο καιρός είναι κρύος" και "Θα πάμε για μπάνιο μόνο αν έχει ήλιο" συνεπάγονται την πρόταση "Δεν θα πάμε για μπάνιο".

Παράδειγμα σύνθετου συμπερασμού

Παράδειγμα.

Δείξτε ότι οι προτάσεις "Δεν έχει ήλιο σήμερα και ο καιρός είναι κρύος" και "Θα πάμε για μπάνιο μόνο αν έχει ήλιο" συνεπάγονται την πρόταση "Δεν θα πάμε για μπάνιο".

Λύση.

Θέτουμε τις εξής προτάσεις:

$H \equiv$ "Έχει ήλιο σήμερα"

$K \equiv$ "Ο καιρός είναι κρύος"

$M \equiv$ "Θα πάμε για μπάνιο"

Ισχύουν οι $\neg H \wedge K$ και $M \rightarrow H$ από υπόθεση. Ζητούμενο το $\neg M$.

Ισοδύναμα, θέλουμε νδο:

$((\neg H \wedge K) \wedge (M \rightarrow H) \rightarrow \neg M)$ είναι ταυτολογία

Παράδειγμα συμπερασμού, συνέχεια

Ισχύουν οι $\neg H \wedge K$ και $M \rightarrow H$ από υπόθεση.

Απλοποίηση($\neg H \wedge K$): έχουμε $\neg H \wedge K \Rightarrow \neg H$

Αφού δώσαμε ένα σωστό επιχείρημα για το $\neg H$ μπορούμε πλέον να το χρησιμοποιούμε σε επόμενα επιχειρήματα σαν ήταν ανάμεσα στις υποθέσεις μας.

Modus tollens($\neg H, M \rightarrow H$): έχουμε $(\neg H \wedge (M \rightarrow H)) \Rightarrow \neg M$.

Κανόνες συμπερασμού με ποσοδείκτες

- ▶ Καθολική εφαρμογή: $\forall xP(x)$ άρα ισχύει $P(c)$, όπου c ένα οποιοδήποτε συγκεκριμένο μέλος του πεδίου ορισμού.
- ▶ Καθολική γενίκευση / απόδειξη πρότασης: αν ισχύει $P(c)$ για c **αυθαίρετο**², τότε ισχύει $\forall xP(x)$.
- ▶ Υπαρξιακή εφαρμογή: αν $\exists xP(x)$ τότε ισχύει $P(c)$ για κάποιο συγκεκριμένο c (που όμως δεν γνωρίζω ποιο είναι).
- ▶ Υπαρξιακή γενίκευση / απόδειξη πρότασης: αν ισχύει $P(c)$ για κάποιο c τότε ισχύει η πρόταση: $\exists xP(x)$.

² Δεν μπορούμε να «διαλέξουμε» να έχει κάποια ιδιότητα. □ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ↺ ↻ ↻

Κανόνες συμπερασμού με ποσοδείκτες

Παράδειγμα.

Οι προτάσεις "Όσοι είναι 1ο έτος Πληροφορικής παρακολουθούν Διακριτά" και "Η Μ είναι πρωτοετής φοιτήτρια Πληροφορικής" οδηγούν στο συμπέρασμα "Η Μ παρακολουθεί Διακριτά".

Λύση.

Κανόνες συμπερασμού με ποσοδείκτες

Παράδειγμα.

Οι προτάσεις "Όσοι είναι 1ο έτος Πληροφορικής παρακολουθούν Διακριτά" και "Η Μ είναι πρωτοετής φοιτήτρια Πληροφορικής" οδηγούν στο συμπέρασμα "Η Μ παρακολουθεί Διακριτά".

Λύση.

Εστω $p(x)$: "ο x είναι πρωτοετής", $q(x)$: "ο x παρακολουθεί Διακριτά" και $P(x) : p(x) \rightarrow q(x)$.

Κανόνες συμπερασμού με ποσοδείκτες

Παράδειγμα.

Οι προτάσεις "Όσοι είναι 1ο έτος Πληροφορικής παρακολουθούν Διακριτά" και "Η Μ είναι πρωτοετής φοιτήτρια Πληροφορικής" οδηγούν στο συμπέρασμα "Η Μ παρακολουθεί Διακριτά".

Λύση.

Εστω $p(x)$: "ο x είναι πρωτοετής", $q(x)$: "ο x παρακολουθεί Διακριτά" και $P(x) : p(x) \rightarrow q(x)$.

Κανόνας καθολικής εφαρμογής: Από υπόθεση $\forall x(p(x) \rightarrow q(x))$, τότε $p(M) \rightarrow q(M)$.

Οργάνωση και περιεχόμενα Μαθήματος

Λογική και Αποδείξεις

Προτασιακή Λογική

Κατηγορήματα και ποσοδείκτες

Συνεπαγωγή (συμπερασμός)

Αποδείξεις

Αποδείξεις [Rosen 1.7]

Απόδειξη μιας (μαθηματικής) πρότασης P
καλείται η τεκμηρίωση της αλήθειας της P ,
η οποία στηρίζεται σε αξιώματα ή υποθέσεις Y και χρησιμοποιεί λογικούς
συλλογισμούς για να καταδείξει την ισχύ της P δηλ. τεκμηριώνει τη
συνεπαγωγή $Y \rightarrow P$.

Στρατηγικές Αποδείξεων [Rosen 1.8]

1. Ευθέως/άμεσα με: $Y \rightarrow Q \rightarrow P$,
ή με "αντίστροφο" συλλογισμό $P \leftrightarrow Q, Y \rightarrow Q$,
όπου αρκούσε να δειχθεί $P \leftarrow Q \leftarrow Y$.
2. Έμμεση απόδειξη: Απαγωγή σε άτοπο δηλ. μέσω
αντιθετοαντίστροφου $\neg P \rightarrow \neg Y$.
3. Υπαρξιακή απόδειξη, ή απόδειξη με αντιπαράδειγμα.
4. Επαγωγικά, εφόσον η πρόταση $P(n), n \geq n_0$ είναι συνάρτηση του
 $n \in \mathbb{N}$: Δείχνουμε την $P(n_0)$ και την $P(n)$ υποθέτοντας $P(k), k < n$.
[Rosen, κεφ. 5]

Στρατηγική 1α: Απαρίθμηση περιπτώσεων / Εξαντλητικές αποδείξεις

$$[(p_1 \vee \cdots \vee p_n) \rightarrow q] \equiv [(p_1 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

Παράδειγμα.

$$n \in \mathbb{Z} \Rightarrow n^2 \geq n.$$

Απόδειξη.

Τρεις (μη-επικαλυπτόμενες) περιπτώσεις:

- Περίπτωση 0. $n = 0$ τότε $0 \geq 0$ ισχύει.
- Περίπτωση 1. $n > 0$ τότε $n \geq 1 \Rightarrow n^2 \geq n$ ισχύει: $n \cdot (n - 1) \geq 0$.
- Περίπτωση 2. $n < 0$ τότε $n \leq -1 \Rightarrow n^2 \geq 1$ και $n < 0$ άρα $n^2 \geq 1 > 0 > n$.

Στρατηγική 1β. Αντίστροφος συλλογισμός

Παράδειγμα.

Για δύο διαφορετικούς θετικούς ακέραιους, ο αριθμητικός μέσος είναι μεγαλύτερος του γεωμετρικού μέσου:

$$\forall x \neq y \in \mathbb{N}^*, (x + y)/2 > \sqrt{xy}.$$

Απόδειξη.

Χρήση ισοδυναμίας:

$$\begin{aligned}(x + y)/2 > \sqrt{xy} &\Leftrightarrow (x + y)^2/4 > xy \\ &\Leftrightarrow x^2 + 2xy + y^2 > 4xy \\ &\Leftrightarrow (x - y)^2 > 0.\end{aligned}$$

Στρατηγική 2. Εις άτοπον απαγωγή

Παράδειγμα.

Σε μια ομάδα **37** ατόμων υπάρχουν τουλάχιστον **4** που έχουν γεννηθεί τον ίδιο μήνα.

Απόδειξη.

Έστω ότι για κάθε ένα μήνα, κατά τη διάρκειά του, έχουν γεννηθεί το πολύ **3** μέλη της ομάδας. Άρα η ομάδα μπορεί να αποτελείται από το πολύ $12 \times 3 = 36$ άτομα. Άτοπο διότι η ομάδα έχει **37**.

Στρατηγική 2. Εις άτοπον απαγωγή (2)

Παράδειγμα.

Δεν υπάρχει ρητός αριθμός x τ.ω. $x^2 = 2$.

Απόδειξη.

Έστω ότι υπάρχει τέτοιος αριθμός. Τότε γράφεται ως ανάγωγο (μη απλοποιήσιμο) κλάσμα $x = a/b$. Άρα

$$(a/b)^2 = 2 \Rightarrow a^2 = 2b^2,$$

δλδ ο a είναι άρτιος (ελέγχουμε περιπτώσεις), οπότε $\exists k, a = 2k$.

Όμως $(2k/b)^2 = 2 \Rightarrow 2k^2 = b^2$, άρα και ο b άρτιος. Άτοπο, καθώς υποθέσαμε την ύπαρξη ανάγωγου κλάσματος.

Στρατηγική 3α: Υπαρξιακή απόδειξη

Για προτάσεις τύπου $\exists x P(x)$: κατασκευαστικές ή μη.

Παράδειγμα.

$\exists x \in \mathbb{N}$ που γράφεται ως άθροισμα κύβων με δύο τρόπους.

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \text{ (ελάχιστος).}$$

Παράδειγμα.

Νδó. $\exists x, y \in \mathbb{R} - \mathbb{Q} : x^y \in \mathbb{Q}$.

Γνωρίζουμε πως $\sqrt{2} \notin \mathbb{Q}$. Εστω ο $\sqrt{2}^{\sqrt{2}}$.

– Αν είναι ρητός, αποδείχθηκε η πρόταση.

– Αλλιώς $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}, x^y = 2$.

Στρατηγική 3β: Αντιπαράδειγμα

Παράδειγμα.

$\forall x \in \mathbb{N}$ γράφεται ως άθροισμα τριών τετραγώνων;

Απόδειξη.

Παρατηρώ πως $1 = 0 + 0 + 1, 2 = 0 + 1 + 1$ κλπ. Όμως ο 7 δεν γράφεται ως άθροισμα τριών τετραγώνων (εκ των 0, 1, 4.)

Στρατηγική 4: Εξαντλητική Απόδειξη

Παράδειγμα.

Ν.δ.ο. $\nexists n \in \mathbb{Z}_{\geq 0}$ τέτοιο ώστε $n^2 + n^3 = 100$

Απόδειξη.

► Αν $n \leq 5$, τότε

$$n = 0 \rightarrow 0^2 + 0^3 = 0$$

$$\vdots$$

$$n = 4 \rightarrow 4^2 + 4^3 = 16 + 64 = 80$$

$$n = 5 \rightarrow 5^2 + 5^3 = 25 + 125 = 150$$

► Αν $n > 5$, τότε

$$n^2 + n^3 > 5^2 + 5^3 > 100$$