Υπολογιστικά & Διακριτά Μαθηματικά

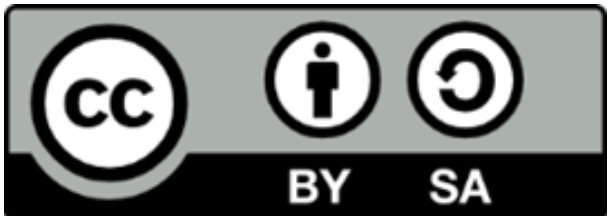
Ενότητα 2:Στοιχεία Μαθηματικής Λογικής

Στεφανίδης Γεώργιος

Τμήμα Εφαρμοσμένης Πληροφορικής

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ισοδυναμία - απλοποίηση προτάσεων

- Θα θεωρήσω ότι είμαστε εξοικειωμένοι με το λεξιλόγιο της Λογικής και τα Σύνολα όπως αναφέρονται στο **Εισαγωγικό Κεφάλαιο (βλέπε αρχείο)** του Σχολικού Βιβλίου (Α' Λυκείου). Χρήσιμο είναι και το Σχολ. β. της Γ' Λυκείου **ΛΟΓΙΚΗ (βλέπε αρχείο)**.
- **1ο Παράδειγμα**

Θεωρούμε δύο τμήματα κώδικα από δύο διαφορετικές εκδοχές του MergeSort. Διαφέρουν μόνο στη γραμμή (1).

```
(1) if (((i+j ≤ p+q) && (i ≤ p) && (j > q))
    || ((i+j ≤ p+q) && (i ≤ p)
        && (List1[i] ≤ List2[j])))
(2)   List3[k] = List1[i]
(3)   i = i+1
(4) else
(5)   List3[k] = List2[j]
(6)   j = j+1
(7) k = k+1
```

```
(1) if ((i+j ≤ p+q) && (i ≤ p) &&
    ((j > q) || (List1[i] ≤ List2[j])))
(2)   List3[k] = List1[i]
(3)   i = i+1
(4) else
(5)   List3[k] = List2[j]
(6)   j = j+1
(7) k = k+1
```

1ο Παράδειγμα[1]

```
(1) ((i+j ≤ p+q) && (i ≤ p) &&
     ((j > q) || (List1[i] ≤ List2[j])))
```

&& = "and"

|| = "or"

```
(1') (((i+j ≤ p+q) && (i ≤ p) && (j > q))
    || ((i+j ≤ p+q) && (i ≤ p)
        && (List1[i] ≤ List2[j])))
```

- **Είναι αυτές οι εκφράσεις ισοδύναμες;**
- **Ας τις ξαναγράψουμε χρησιμοποιώντας μεταβλητές**

$s \sim$ (i+j $\leq$ p+q) $t \sim$ (i$\leq$ p) $u \sim$ (j$>$ q)

$v \sim$ (List[i] $\leq$ List2[j])

(1) s and t and (u or v)

(1') (s and t and u) or (s and t and v)

1ο Παράδειγμα[2]

- Θέτουμε

$$w \sim (s \text{ and } t)$$

οπότε το ερώτημα γίνεται:

$$(1)\ w \text{ and } (u \text{ or } v) \quad \overset{\text{ίσα ;}}{\longleftrightarrow} \quad (1')\ (w \text{ and } u) \text{ or } (w \text{ and } v)$$

- Απλά μετασχηματίσαμε τον κώδικα σε Μπουλιανές (Boolean) εκφράσεις που αντιστοιχούν σε λογικούς τύπους (λ.τ) σύνθετων προτάσεων και θα ανατρέξουμε σε μια θεωρία που θα μας επιτρέψει να διαπιστώσουμε αν δύο τέτοιοι λ.τ είναι ισοδύναμοι, γεγονός που θα μας επιτρέψει στη συνέχεια, να πούμε αν οι δύο εκφράσεις είναι ισοδύναμες.

2ο Παράδειγμα

- *2ο Παράδειγμα*
- Θεωρούμε το ακόλουθο τμήμα κώδικα το οποίο θα μπορούσε να είναι της C, της C++ ή της Java:

```
if (x > 0 || (x <= 0 && y > 10))
…       (πρόσθετες εντολές)
```

- Το σύμβολο `||` σημαίνει "ή" (OR) και το σύμβολο `&&` σημαίνει "και" (AND). Οι *πρόσθετες εντολές* εκτελούνται μόνο αν η πρόταση που ακολουθεί τη (δεσμευμένη) λέξη `if` είναι *αληθής*. Μπορούμε να παρατηρήσουμε ότι αυτή η μεγάλη έκφραση είναι φτιαγμένη από δύο απλούστερες εκφράσεις. Έστω *p* η πρόταση "x > 0" και *q* η πρόταση "y > 10". Τότε μπορούμε να ξαναγράψουμε τη συνθήκη ως εξής:

```
p OR ((NOT p) AND q)
```

- Πρόκειται για τον λ.τ.

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

Μπορεί να απλοποιηθεί χρησιμοποιώντας *λογικές ισοδυναμίες*;

Προτάσεις και Λογική

- Ο θεμέλιος λίθος της τυπικής λογικής είναι η πρόταση. *Πρόταση* είναι μια δηλωτική φράση η οποία έχει μια τιμή αληθείας: είναι είτε *αληθής*, συμβολικά T (True), είτε *ψευδής*, συμβολικά F (False).
- Χρησιμοποιούμε μεταβλητές *p*, *q*, *r*, … προκειμένου να συμβολίζουμε τις προτάσεις.
- Νέες προτάσεις μπορούν να κατασκευαστούν από άλλες χρησιμοποιώντας *λογικούς τελεστές*, όπως οι $\neg$ (NOT - όχι), $\vee$ (OR - ή) και $\wedge$ (AND - και) για να παραγάγουμε μια *σύνθετη* πρόταση.
- Εκφράζουμε κάθε μία από τις σύνθετες προτάσεις σε συμβολική μορφή, δηλαδή γράφουμε τον λογικό τύπο (λ.τ) τους.
- Για να προσδιορίσουμε την τιμή αληθείας μιας σύνθετης πρότασης χρειάζεται να ξέρουμε τα αποτελέσματα της δράσης των λογικών τελεστών. Αυτά συνοψίζονται απλά με τη βοήθεια ενός *πίνακα αληθείας*.

Πίνακες αληθείας

AND

s	t	$s \wedge t$
T	T	T
T	F	F
F	T	F
F	F	F

OR

s	t	$s \vee t$
T	T	T
T	F	T
F	T	T
F	F	F

XOR

s	t	$s \oplus t$
T	T	F
T	F	T
F	T	T
F	F	F

NOT

s	$\neg s$
T	F
F	T

- Αν *s* και *t* είναι δύο προτάσεις, η ***σύζευξη*** των *s* και *t* είναι η πρόταση ($s \wedge t$). Είναι αληθής μόνον όταν *s* και *t* είναι και οι δύο αληθείς.
- Αν *s* και *t* είναι δύο προτάσεις, η ***διάζευξη*** των *s* και *t* είναι η πρόταση ($s \vee t$). Είναι αληθής όταν μία τουλάχιστον από τις *s*, *t* είναι αληθής.
- Αν *s* και *t* είναι δύο προτάσεις, η ***αποκλειστική διάζευξη*** των *s* και *t* είναι η πρόταση ($s \oplus t$). Είναι αληθής όταν μία ακριβώς από τις *s*, *t* είναι αληθής.
- Αν *s* συμβολίζει μια οποιαδήποτε πρόταση, η **άρνηση** της *s* είναι η πρόταση ($\neg s$). Είναι αληθής όταν η *s* είναι ψευδής.
- Ένας λ.τ. ονομάζεται **ταυτολογία** αν έχει σταθερή τιμή αληθείας Τ ανεξάρτητα από τις τιμές των μεταβλητών του και η πρόταση της οποίας ο λ. τ. είναι μια ταυτολογία λέγεται **ταυτολογική πρόταση**.
- Ο λ.τ. του οποίου η τιμή είναι πάντα F ονομάζεται **αντίφαση** και η πρόταση της οποίας ο λ.τ. είναι μια αντίφαση λέγεται **αντιφατική πρόταση**.

Ισοδυναμία προτάσεων – λ.τ

- Δύο προτάσεις οι οποίες έχουν δημιουργηθεί από τις ίδιες βασικές προτάσεις με διαφορετικούς τρόπους μπορούν στην πραγματικότητα να έχουν την ίδια τιμή αληθείας για κάθε δυνατό σύνολο τιμών αληθείας των προτάσεων που τις απαρτίζουν. Τέτοιες προτάσεις λέμε ότι είναι (*λογικά*) *ισοδύναμες*.
- Για να διαπιστώσουμε την ισοδυναμία των προτάσεων κατασκευάζουμε τον πίνακα αληθείας της κάθε μιας σύνθετης πρότασης και εξετάζουμε αν ταυτίζονται οι τελικές στήλες των πινάκων αληθείας.
- Χρησιμοποιώντας μεταβλητές στη θέση των προτάσεων μελετάμε τους λ.τ που προκύπτουν και την ισοδυναμία τους τη διαπιστώνουμε από τους αντίστοιχους πίνακες αληθείας τους.

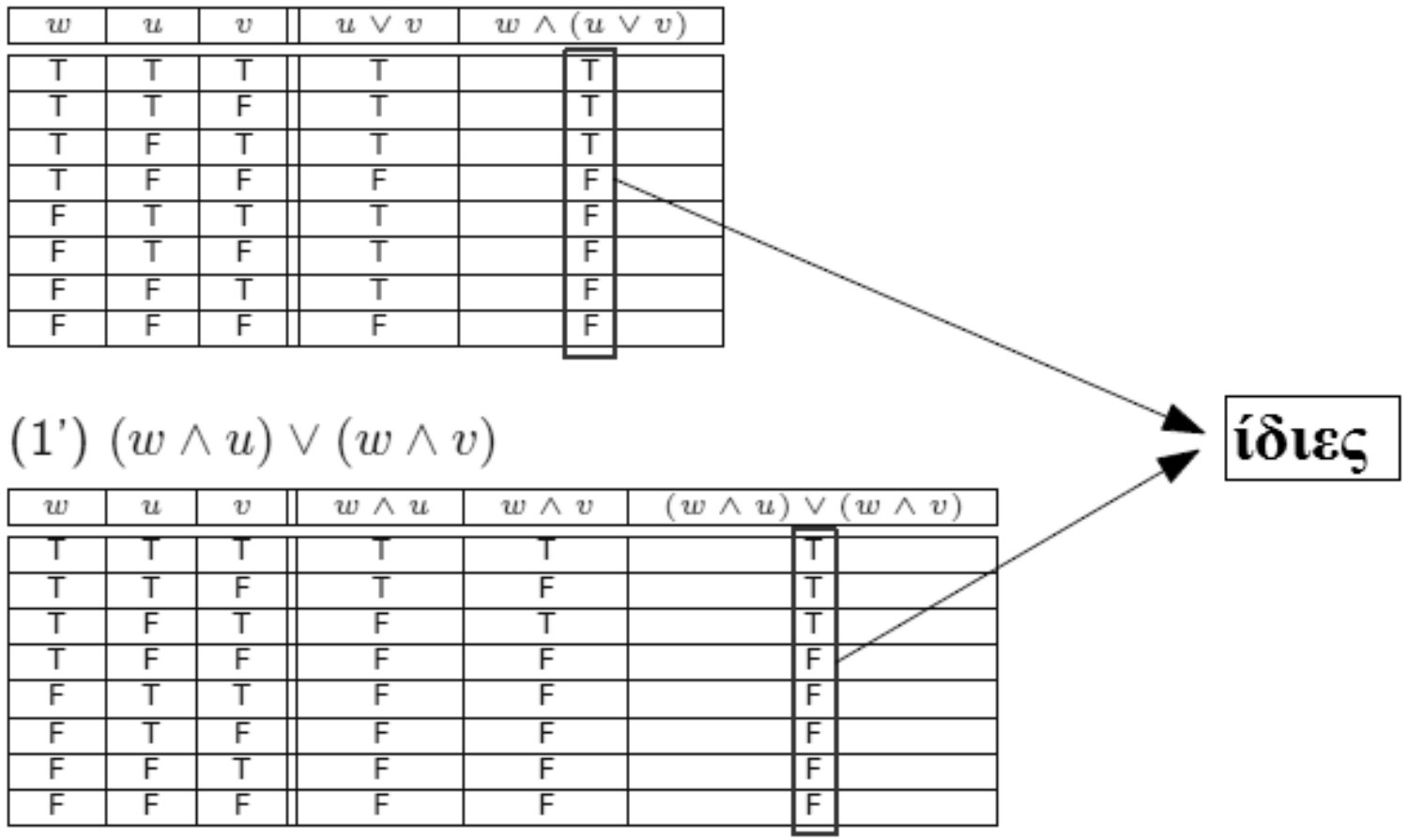
Απάντηση στο 1ο Παράδειγμα

(1) $w \wedge (u \vee v)$

w	u	v	$u \vee v$	$w \wedge (u \vee v)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

(1') $(w \wedge u) \vee (w \wedge v)$

w	u	v	$w \wedge u$	$w \wedge v$	$(w \wedge u) \vee (w \wedge v)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F



Λογικές ισοδυναμίες

- $(p \vee c) \equiv p$
  $(p \wedge t) \equiv p$ (νόμοι ταυτότητας)
- $(p \vee \neg p) \equiv t$
  $(p \wedge \neg p) \equiv c$ (νόμοι άρνησης)
- $(p \vee q) \equiv (q \vee p)$
  $(p \wedge q) \equiv (q \wedge p)$ (αντιμεταθετικότητα)
- $[(p \vee q) \vee r] \equiv [p \vee (q \vee r)]$
  $[(p \wedge q) \wedge r] \equiv [p \wedge (q \wedge r)]$ (προσεταιριστικότητα)
- $[p \vee (q \wedge r)] \equiv [(p \vee q) \wedge (p \vee r)]$
  $[p \wedge (q \vee r)] \equiv [(p \wedge q) \vee (p \wedge r)]$ (επιμεριστικότητα)
- $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$
  $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ (νόμοι De Morgan)

Νόμοι De Morgan

- i) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- Ii) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- Απόδειξη
- i)

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

- ii) Δίνεται ως άσκηση

Παράδειγμα

- $p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$

  Απόδειξη

p	q	$p \oplus q$	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
T	T	F	T	T	F	F
T	F	T	T	F	T	T
F	T	T	T	F	T	T
F	F	F	F	F	T	F

Απάντηση στο 2ο Παράδειγμα

- Μπορούμε να απλοποιήσουμε τον λ.τ

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

χρησιμοποιώντας λογικές ισοδυναμίες, ως εξής:

$$\begin{aligned} p \vee (\neg p \wedge q) &\equiv (p \vee \neg p) \wedge (p \vee q) && \text{(επιμεριστικότητα)} \\ &\equiv t \wedge (p \vee q) && \text{(ν. άρνησης)} \\ &\equiv p \vee q && \text{(ν. ταυτότητας)} \end{aligned}$$

- Αυτό σημαίνει ότι μπορούμε να απλοποιήσουμε το τμήμα κώδικα χωρίς να επηρεαστεί η ροή ελέγχου του προγράμματος:

```
if (x > 0 || y > 10)
```

… (*πρόσθετες εντολές*)

Συνεπαγωγές [1]

- Η **υποθετική** ή **υπό συνθήκη πρόταση**, «*αν p τότε q*», συμβολικά «$p \rightarrow q$» χαρακτηρίζεται ως ψευδής αν η υπόθεση *p* είναι αληθής και το συμπέρασμα *q* είναι ψευδής, και αληθής σε κάθε άλλη περίπτωση.
- Συχνά διαβάζεται, p συνεπάγεται q, ή p είναι ικανή για q, ή q είναι αναγκαία για p.
- Πίνακας αληθείας της ($p \rightarrow q$)

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

- Η πρόταση $q \rightarrow p$ λέγεται **αντίστροφη** της πρότασης $p \rightarrow q$ και είναι διαφορετική από την πρόταση $p \rightarrow q$ (έχει διαφορετικό πίνακα αληθείας).
- η $p \rightarrow q$ είναι αληθής στις περιπτώσεις που η *p* είναι ψευδής ή η *q* είναι αληθής
- οι αντίστροφες συνεπαγωγές $p \rightarrow q$ και $q \rightarrow p$ *συναληθεύουν* μόνο στην περίπτωση που οι προτάσεις *p*, *q* είναι ομότιμες.

Συνεπαγωγές [2]

- Όταν δίνεται η πρόταση $p \to q$ τότε η πρόταση $\neg p \to \neg q$ λέγεται **αντίθετή** της και η $\neg q \to \neg p$ λέγεται ότι είναι η **αντιθετοαντίστροφή** της.
- Εύκολα μπορεί να διαπιστώσει κανείς ότι οι τελικές στήλες των πινάκων αληθείας των προτάσεων $p \to q$ και $\neg q \to \neg p$ είναι ίδιες.
- Πράγματι, αν κάνουμε τους πίνακες αληθείας τους, έχουμε

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

- Τέλος, έχουμε τη σύζευξη δύο αντίστροφων υποθετικών προτάσεων: Αν p, q είναι δύο προτάσεις, η πρόταση «$p \to q$ και $q \to p$», συμβολικά «$p \leftrightarrow q$», διαβάζεται «p, αν και μόνο αν q», ονομάζεται **αμφίδρομη υπό συνθήκη** πρόταση των p, q.
- Ο πίνακας αληθείας της $p \leftrightarrow q$ προκύπτει ότι είναι ο ακόλουθος:

Συνεπαγωγές [3]

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

- Όπως προκύπτει από τον παραπάνω πίνακα αληθείας της, χαρακτηρίζεται ως αληθής, αν οι προτάσεις *p*, *q* είναι ομότιμες, και ψευδής, αν οι προτάσεις *p*, *q* είναι ετερότιμες.
- Επειδή ο λ.τ. $P \leftrightarrow Q$ έχει τιμές αληθείας Τ ακριβώς όταν οι τιμές αληθείας των *P* και *Q* συμφωνούν, προκύπτει ότι:

  $P \Leftrightarrow Q$, *αν και μόνο αν ο λ.τ* $P \leftrightarrow Q$ είναι μια ταυτολογία.
- Δεδομένων δύο λ.τ. *P* και *Q*, λέμε ότι ο *P* συνεπάγεται (λογικά) τον *Q*, συμβολικά $P \Rightarrow Q$, εάν ο *Q* έχει τιμή αληθείας Τ όποτε ο *P* έχει τιμή Τ. Να σημειώσουμε ότι

  $P \Rightarrow Q$, *αν και μόνο αν ο λ.τ.* $P \rightarrow Q$ *είναι μια ταυτολογία.*

Κατηγορήματα και Ποσοδείκτες [1]

- Η προτασιακή λογική εφαρμόζεται σε απλές σχετικά δηλωτικές προτάσεις όπου οι βασικές προτάσεις είναι είτε αληθείς είτε ψευδείς. Οι προτάσεις που περιέχουν μία ή περισσότερες μεταβλητές μπορεί να είναι αληθείς για κάποιες τιμές των μεταβλητών αλλά ψευδείς για κάποιες άλλες.
- Στη γραμματική η λέξη κατηγόρημα αναφέρεται στο τμήμα της φράσης που δίνει πληροφορία για το υποκείμενο. Με άλλα λόγια το κατηγόρημα είναι το τμήμα της φράσης από την οποία έχει απαλειφθεί το υποκείμενο.
- Στη μαθηματική λογική **κατηγόρημα** (predicate) είναι μια φράση που περιέχει ορισμένες μεταβλητές και η οποία μετατρέπεται σε μια πρόταση όταν οι μεταβλητές αντικατασταθούν με συγκεκριμένες τιμές.
- Κατηγόρημα, δηλαδή, είναι μια φράση που περιέχει μεταβλητές, η οποία είναι αληθής είτε ψευδής ανάλογα με τις τιμές που ανατίθενται στις μεταβλητές.
- Παραδείγματος χάριν, «*x είναι ένας ακέραιος που ικανοποιεί την* $x = x^2$» είναι ένα κατηγόρημα διότι είναι αληθής για $x = 0$ ή 1, και είναι ψευδής για όλες τις άλλες τιμές του x.

Κατηγορήματα και Ποσοδείκτες [2]

- Μπορούν τώρα να εφαρμοστούν λογικές πράξεις σε κατηγορήματα. Γενικά, η αλήθεια ενός σύνθετου κατηγορήματος, σε τελευταία ανάλυση, εξαρτάται από τις τιμές που ανατίθενται στις εμπλεκόμενες μεταβλητές.
- Υπάρχουν όμως και άλλοι λογικοί τελεστές, γνωστοί ως **ποσοδείκτες**, οι οποίοι όταν εφαρμόζονται σε ένα κατηγόρημα παράγουν είτε μια αληθή πρόταση είτε μια ψευδή πρόταση.

❑ **Παράδειγμα**

Ποιες από τις παρακάτω προτάσεις είναι αληθείς και ποιες είναι ψευδείς;

(α) Όλα τα τρίγωνα έχουν το άθροισμα των γωνιών τους ίσο με 180^o.

(β) Όλες οι γάτες έχουν ουρές.

(γ) Υπάρχει ακέραιος x που ικανοποιεί την $x^2 = 2$.

(δ) Υπάρχει πρώτος αριθμός ο οποίος δεν είναι περιττός.

Κατηγορήματα και Ποσοδείκτες [3]

- ***Λύση***

  (α) Αληθής.

  (β) Ψευδής. Οι γάτες Manx δεν έχουν ουρά.

  (γ) Ψευδής.

  (δ) Αληθής. Ο αριθμός 2 είναι πρώτος και άρτιος.

- Στο παράδειγμα έχουμε συλλογές αντικειμένων και ισχυριζόμαστε ότι κάποια ιδιότητα ισχύει **για κάθε** ένα από (ή **για όλα**) τα σχετικά αντικείμενα, ή ότι **υπάρχει** τουλάχιστον ένα αντικείμενο για το οποίο ισχύει η δοσμένη ιδιότητα.
- Οι δύο ποσοδείκτες κατηγορημάτων, **για κάθε** (ή **για όλα**) και **υπάρχει**, συμβολίζονται αντίστοιχα με τα σύμβολα $\forall$ και $\exists$. Η ποσοτικοποίηση ενός κατηγορήματος δημιουργεί μια πρόταση και συνεπώς ένα ποσοτικοποιημένο κατηγόρημα είναι είτε αληθές είτε ψευδές.

Κατηγορήματα και Ποσοδείκτες [4]

- **Παράδειγμα**

  Έστω $P(x)$ το κατηγόρημα, *x είναι ακέραιος και* $x^2 = 16$.

  Ας διατυπώσουμε την πρόταση, $\exists x\,(P(x))$, με λόγια και ας προσδιορίσουμε την τιμή αληθείας της.

- Η πρόταση, $\exists x\,(P(x))$, λέει ότι υπάρχει ακέραιος x που ικανοποιεί την εξίσωση $x^2 = 16$.
- Αυτή η πρόταση είναι αληθής διότι, για παράδειγμα, η $x^2 = 16$ ισχύει για $x = 4$.
- Είναι επίσης αληθής όταν $x = -4$, αλλά είναι αρκετό να καθορίσουμε μία μόνον τιμή του x για την οποία η αντίστοιχη $P(x)$ είναι αληθής, προκειμένου να δείξουμε ότι η πρόταση, $\exists x\,(P(x))$, είναι αληθής.

Μέθοδοι απόδειξης

- Οι συνηθέστεροι τύποι αποδείξεων είναι αυτές στις οποίες θέλουμε να εδραιώσουμε την αλήθεια μιας πρότασης της μορφής ($P \rightarrow Q$). Υπάρχουν αρκετές καθιερωμένες μέθοδοι απόδειξης, συμπεριλαμβανομένων των παρακάτω.
- **Ευθεία μέθοδος απόδειξης** (Ευθύ επιχείρημα)

➢ Υποθέτουμε ότι η *P* είναι αληθής και δείχνουμε ότι η *Q* είναι αληθής. Αυτό εξαιρεί την περίπτωση στην οποία η *P* είναι αληθής και η *Q* ψευδής, που είναι η μόνη περίπτωση όπου η ($P \rightarrow Q$) είναι ψευδής.

- **Απόδειξη με αντιθετοαντιστροφή** (Αντιθετοαντίστροφο επιχείρημα)

➢ Υποθέτουμε ότι η *Q* είναι ψευδής και δείχνουμε ότι η *P* είναι ψευδής. Αυτό καταδεικνύει ότι $((\neg Q) \rightarrow (\neg P))$ είναι αληθής, που, όπως έχουμε δει, είναι το ίδιο με το να δείξουμε ότι η ($P \rightarrow Q$) είναι αληθής.

- **Απόδειξη με εις άτοπο απαγωγή** (Απόδειξη με αντίφαση)

➢ Υποθέτουμε ότι η *P* είναι αληθής και η *Q* ψευδής και καταλήγουμε σε αντίφαση (άτοπο). Αυτό πάλι εξαιρεί την περίπτωση στην οποία η *P* είναι αληθής και η *Q* ψευδής, που είναι η μόνη περίπτωση όπου η ($P \rightarrow Q$) είναι ψευδής.

Παραδείγματα [1]

- **Παράδειγμα 1.**

❑ Ας χρησιμοποιήσουμε μια ευθεία μέθοδο απόδειξης για να δείξουμε ότι **αν** x και y είναι περιττοί ακέραιοι **τότε** το γινόμενο xy είναι επίσης περιττός ακέραιος.

➢ Κατ' αρχήν, να παρατηρήσουμε ότι αν x είναι περιττός ακέραιος τότε $x = 2m + 1$, όπου m είναι ακέραιος. Ομοίως, $y = 2n + 1$ για κάποιον ακέραιο n. Έτσι,

$$xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$$

που είναι ένας περιττός ακέραιος.

- **Παράδειγμα 2.**

❑ Έστω n θετικός ακέραιος. Ας αποδείξουμε, με αντιθετοαντιστροφή, ότι **αν** n^2 είναι περιττός, **τότε** ο n είναι περιττός.

➢ Η άρνηση της πρότασης, *n^2 είναι περιττός*, είναι η πρόταση, *n^2 είναι άρτιος* και η άρνηση της πρότασης, *n είναι περιττός*, είναι η πρόταση, *n είναι άρτιος*. Αφού ο n είναι άρτιος, μπορούμε να γράψουμε $n = 2m$, για κάποιον ακέραιο m.
Τότε, $n^2 = 4m^2 = 2(2m^2)$, που είναι άρτιος.

Παραδείγματα [2]

- **Παράδειγμα 3.**

❑ Ας χρησιμοποιήσουμε την εις άτοπο απαγωγή για να δείξουμε ότι **αν** $x^2 = 2$, **τότε** ο x δεν είναι ρητός.

➢ Έστω ότι ο x είναι ρητός, δηλ. $x = m/n$, όπου m και n ακέραιοι με $n \neq 0$ και τέτοιοι ώστε να μην έχουν κοινούς παράγοντες.

Αφού $x^2 = 2$, έχουμε $(m/n)^2 = 2$. Επομένως, $m^2 = 2n^2$.

Αυτό όμως συνεπάγεται ότι m^2 είναι ένας άρτιος ακέραιος. Επομένως, με βάση γνωστή άσκηση της θεωρίας αριθμών, ο m είναι άρτιος. Συνεπώς, $m = 2p$, όπου p ακέραιος. Αντικαθιστώντας στην εξίσωση $m^2 = 2n^2$ μας δίνει $n^2 = 2p^2$. Τότε όμως, ο n είναι επίσης ένας άρτιος. Έτσι έχουμε δείξει ότι οι m και n έχουν κοινό παράγοντα (το 2) το οποίο αντιφάσκει με την αρχική μας υπόθεση ότι οι m και n δεν έχουν κοινούς παράγοντες.

Μαθηματική επαγωγή

- Η **απλή** αρχή της μαθηματικής επαγωγής

  Έστω $P(n)$ ένα κατηγόρημα το οποίο ορίζεται για κάθε φυσικό αριθμό $n \geq \rho$ ($\rho \in \mathbb{N}$).

  Αν

1. $P(\rho)$ αληθής, και
2. $\forall k \geq \rho\ (P(k) \rightarrow P(k+1))$ αληθής,

  τότε $P(n)$ αληθής για κάθε $n \geq \rho$.

- Η **ισχυρή** αρχή της μαθηματικής επαγωγής

  Έστω $P(n)$ ένα κατηγόρημα το οποίο ορίζεται για κάθε φυσικό αριθμό $n \geq \rho$ ($\rho \in \mathbb{N}$).

  Αν

1. $P(\rho)$ αληθής, και
2. $\forall k > \rho\ ((P(\rho+1) \wedge P(\rho+2) \wedge \ldots \wedge P(k)) \rightarrow P(k+1))$ αληθής,

  τότε $P(n)$ αληθής για κάθε $n \geq \rho$.

Παραδείγματα [3]

- **Παράδειγμα 1.**

❑ Μια ακολουθία ακεραίων $x_1, x_2, \ldots, x_n$ ορίζεται αναδρομικά ως εξής:

$x_1 = 1$

$x_{k+1} = x_k + 8k$ για $k \geq 1$.

Δείξτε ότι, $x_n = (2n - 1)^2$ για κάθε $n \geq 1$.

➢ *Απόδειξη:*

- Έστω $P(n)$ το κατηγόρημα, $x_n = (2n - 1)^2$.

1. Αν $n = 1$, τότε $(2n - 1)^2 = 1$ που ισχύει. Επομένως, $P(1)$ αληθής.
2. Υποθέτουμε τώρα ότι, $x_k = (2k - 1)^2$ για κάποιο $k \geq 1$.

- Τότε
- $x_{k+1} = x_k + 8k$
  $= (2k - 1)^2 + 8k$
  $= 4k^2 + 4k + 1$
  $= (2k + 1)^2$.
- Συνεπώς, $x_{k+1} = [2(k + 1) - 1]^2$ και έτσι, $\forall k \geq 1\ (P(k) \rightarrow P(k + 1))$ αληθής. Επομένως, δια της επαγωγής, $P(n)$ αληθής για κάθε $n \geq 1$.

Παραδείγματα [4]

- **Παράδειγμα 2.**

❑ Κάθε ακέραιος n μεγαλύτερος του 1 μπορεί να γραφτεί ως γινόμενο πρώτων.

➢ *Απόδειξη:*

- Έστω $P(n)$ το κατηγόρημα, "ο ακέραιος $n > 1$ μπορεί να γραφτεί ως γινόμενο πρώτων".

1. Η $P(2)$ αληθής γιατί $2 = 2$.
2. Έστω ότι $P(k)$ αληθής για όλους τους θετικούς ακεραίους k με $k \leq n$. Πρέπει να δείξουμε ότι $P(k + 1)$ αληθής.

- $1^{η}$ περίπτωση: $k + 1$ πρώτος. Τότε $P(k + 1)$ προφανής.
- $2^{η}$ περίπτωση: $k + 1$ σύνθετος. Τότε $k + 1 = a \cdot b$ με $2 \leq a \leq b < n + 1$, αλλά οι a και b από την υπόθεση μπορούν να γραφτούν ως γινόμενο πρώτων.

Ο αλγόριθμος ΠΡΧ

- Ο αλγόριθμος ΠΡΧ υπολογίζει, όπως έχουμε αναφέρει, το γινόμενο δύο αριθμών *M* και *N*, όπου *N* είναι ένας θετικός ακέραιος.
- Σε μορφή ψευδοκώδικα ο αλγόριθμος έχει ως εξής:

Αλγόριθμος ΠΡΧ

```
Begin
  Total ← 0; A ← M; B ← N;
  While ( B > 1 ) Do
    If (B MOD 2 = 1) Then Total ← Total + A End;
    A ← A × 2; B ← B DIV 2;
  End;
  Return ( Total + A );
End.
```

// δεν χρειάζεται να κρατά όλες τις ενδιάμεσες τιμές των *A* και *B*

// Προσθέτει την τρέχουσα τιμή-*A* στη μεταβλητή Total όταν

// η τιμή-*B* είναι περιττός αριθμός

- Βλέπε: **Άσκηση 1**
- Γνωρίζουμε ότι μετά από $k = \lfloor \lg N \rfloor$ επαναλήψεις, η *B*-τιμή πρέπει να γίνει 1 και ο βρόχος While θα **τερματίσει**.

Αναλλοίωτη βρόχου

- Θέλουμε έναν τυπικό μηχανισμό περιγραφής της δράσης ενός βρόχου από επανάληψη σε επανάληψη· κάτι που να μπορούμε να χρησιμοποιούμε για την απόδειξη της ορθότητας ενός αλγορίθμου που περιέχει βρόχους (επανάληψης).

➢ **Αναλλοίωτη βρόχου** (loop invariant) είναι μια πρόταση που περιγράφει τις μεταβλητές που περιλαμβάνονται στον βρόχο και η οποία είναι αληθής (έχει τιμή αληθείας Τ) **μετά από κάθε** επανάληψη του βρόχου.

✓ και επομένως, πρέπει να είναι αληθής (Τ) όταν ο βρόχος τερματίζει.

✓ Η τιμή αληθείας μιας αναλλοίωτης βρόχου δεν αλλάζει (μεταβάλλεται) με τις επαναλήψεις του βρόχου. Μια αναλλοίωτη βρόχου πρέπει να είναι Τ (αληθής) πριν την εισαγωγή στον βρόχο.

- Οι αναλλοίωτες βρόχου μας παρέχουν μια πολύ ισχυρή τεχνική σχεδίασης και ανάλυσης αλγορίθμων οι οποίοι περιέχουν βρόχους.
- Για τον βρόχο, για παράδειγμα, του αλγόριθμου ΠΡΧ μπορούμε να αποδείξουμε ότι η ισότητα

$$AB + \text{Total} = MN$$

είναι μια αναλλοίωτη βρόχου.

Παραδείγματα [5]

- **Πρόταση**: Για οποιονδήποτε μη αρνητικό ακέραιο *n*, μετά από *n* επαναλήψεις του βρόχου στον ΠΡΧ, είναι *AB* + Total = *MN*.

Απόδειξη (με τη μέθοδο της Μαθηματικής Επαγωγής)

- Έστω *P*(*n*) (το κατηγόρημα): «Αν $n \in \mathbb{N}$, μετά από *n* επαναλήψεις του βρόχου στον ΠΡΧ, *AB* + Total = *MN*»

➢ Βήμα 1. Μετά από *n* = 0 επαναλήψεις του βρόχου,

AB + Total = *MN* + 0 = *MN* // *P*(0) αληθής (Τ)

// Υποθέτουμε ότι αυτή η ισότητα είναι αληθής για μερικές πρώτες επαναλήψεις

➢ Βήμα 2. Υποθέτουμε ότι μετά από $k > 0$ επαναλήψεις του βρόχου,

AB + Total = *MN*

// Τώρα, τι θα συμβεί στην επόμενη επανάληψη, αν υπάρξει μια τέτοια;

➢ Βήμα 3. Υποθέτουμε ότι υπάρχει η $(k+1)$-οστή επανάληψη //δηλ. $B \geq 2$

Η τιμή του *B* στην αρχή αυτής της επόμενης επανάληψης του βρόχου μπορεί να γραφεί ως $2Q + R$, όπου $R = 0$ ή 1. Έστω A^*, B^* και Total^* οι τιμές αυτών των μεταβλητών μετά από αυτή την επόμενη επανάληψη. Τότε,

$\text{Total}^* = \text{Total} + RA$ // $R = 1 \Leftrightarrow B$ είναι περιττός

$A^* = 2A$

$B^* = Q$ // $Q = \lfloor B/2 \rfloor = B$ DIV 2

Άρα,

Παραδείγματα [6]

A^*B^* + Total* = (2A)(Q) + (Total + RA)

= A[2Q + R] + Total

= AB + Total

= MN // από το Βήμα 2

Επομένως, $\forall\, n \in \mathbb{N}$, μετά από n επαναλήψεις του βρόχου,

AB + Total = MN .

Όταν ο βρόχος τερματίζει τελικά, B = 1 και

MN = AB + Total // όπως ήδη δείξαμε

= $A \times 1$ + Total = Total + A.

- Έτσι, η τιμή που επιστρέφει ο αλγόριθμος **είναι** το γινόμενο των δύο τιμών, στην είσοδο, M και N. **Ο αλγόριθμος ΠΡΧ είναι ορθός**. Αν ο N είναι θετικός ακέραιος, τότε ο αλγόριθμος υπολογίζει σωστά το γινόμενο MN.

Τέλος Ενότητας

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης