Θεωρία Υπολογισμού
Άρτιοι ΑΜ

Διδάσκων: Σταύρος Κολλιόπουλος

eclass.di.uoa.gr

Περιγραφή μαθήματος

Σκοπός του μαθήματος είναι η εισαγωγή στη Θεωρία Υπολογισμού και στη Θεωρία Υπολογιστικής Πολυπλοκότητας (Θεωρία Αλγορίθμων).

Ύλη του μαθήματος

Η ύλη του μαθήματος χωρίζεται σε 3 μεγάλες ενότητες που προσπαθούν να απαντήσουν τα αντίστοιχα ερωτήματα:

- Μοντέλα υπολογισμού. Αυτόματα και γλώσσες.
  Τί είναι υπολογιστής;
- Θεωρία υπολογισιμότητας (computability theory).
  Τί είναι και τί δεν είναι υπολογίσιμο;
- Θεωρία υπολογιστικής πολυπλοκότητας (complexity theory). Τί μπορεί να υπολογιστεί σε μικρό χρόνο (ή χώρο) και τί όχι;

Τί μπορεί να κάνει ένας υπολογιστής;

(Ας υποθέσουμε πως έχουμε συμφωνήσει τί είναι ο υπολογιστής).

Ο υπολογιστής λύνει «προβλήματα». Λύνει όλα τα προβλήματα; Υπάρχουν προβλήματα που δεν μπορεί να λύσει ένας υπολογιστής;

Τί μπορεί να κάνει ένας υπολογιστής;

(Ας υποθέσουμε πως έχουμε συμφωνήσει τί είναι ο υπολογιστής).

Ο υπολογιστής λύνει «προβλήματα». Λύνει όλα τα προβλήματα; Υπάρχουν προβλήματα που δεν μπορεί να λύσει ένας υπολογιστής;

Πώς σχετίζονται τα προβλήματα που λύνει ένας υπολογιστής με τα προβλήματα των Μαθηματικών;

Τί μπορούν να «κάνουν» και τί δεν μπορούν να «κάνουν» τα Μαθηματικά; Από αυτό το ερώτημα στις αρχές του 20ου αιώνα ξεκίνησε κατά κάποιο τρόπο η ιστορία μας.

Η έννοια «πρόβλημα»

1) Υπάρχουν ακέραιοι $x, y, z \geq 1$ και $n > 2$ τέτοιοι ώστε $x^n + y^n = z^n$;

2) Γράψτε ένα πρόγραμμα Pascal που όταν η είσοδος είναι ένα ακέραιο πολυώνυμο p (πολλών μεταβλητών), στην έξοδο απαντά αν το πολυώνυμο p έχει ακέραιες ρίζες.
Π.χ. Αν η είσοδος είναι $p = x^2 + 2y^2 + 3$ πρέπει να απαντά «όχι» (γιατί;).

Βασική διαφορά ανάμεσα στις δύο περιπτώσεις: Στην πρώτη περίπτωση η απάντηση είναι «ναι» ή «όχι», ενώ στη δεύτερη περίπτωση η απάντηση είναι ένα πρόγραμμα Pascal (αλγόριθμος).

Η έννοια «πρόβλημα»

1) [$x^n + y^n = z^n$] είναι το περίφημο Θεώρημα του Fermat που προτάθηκε από τον Fermat.
Παρέμεινε άλυτο για τετρακόσια περίπου χρόνια, ώς το 1994, όταν ο Andrew Wiles κατάφερε να το λύσει (η σωστή απάντηση στην ερώτηση είναι αρνητική).

2) [πρόγραμμα που να λύνει ακέραιες εξισώσεις] προτάθηκε από τον David Hilbert το 1900, είναι το περίφημο δέκατο πρόβλημα του Hilbert.
Απαντήθηκε απο τον Yuri Matiyasevich το 1970, που έδειξε ότι δεν υπάρχει τέτοιο πρόγραμμα Pascal.

Μας ενδιαφέρουν τα προβλήματα της δεύτερης περίπτωσης, όπου το ζητούμενο είναι ένας αλγόριθμος και όχι ένα απλό «ναι» ή «όχι».

Η έννοια «πρόβλημα» II

1) Υπάρχουν ακέραιοι $x, y, z \geq 1$ και $n > 2$ τέτοιοι ώστε $x^n + y^n = z^n$;

2) Γράψτε ένα πρόγραμμα που με είσοδο ακέραιους $x, y, z \geq 1$, να αποφασίζει αν υπάρχει ακέραιος $n > 2$, τέτοιος ώστε $x^n + y^n = z^n$.

3) Γράψτε ένα πρόγραμμα που με είσοδο την πρόταση:
« Για οποιουσδήποτε ακέραιους $x, y, z \geq 1$ δεν υπάρχει ακέραιος $n > 2$, τέτοιος ώστε $x^n + y^n = z^n$»,
να αποφασίζει αν η πρόταση είναι αληθής.

4) Γράψτε ένα πρόγραμμα που με είσοδο μια μαθηματική πρόταση $\mathcal{P}$ (σε κατάλληλο συμβολισμό), να αποφασίζει αν η $\mathcal{P}$ είναι αληθής.

Η έννοια «πρόβλημα» ΙΙ

1) Υπάρχουν ακέραιοι $x, y, z \geq 1$ και $n > 2$ τέτοιοι ώστε $x^n + y^n = z^n$;

2) Γράψτε ένα πρόγραμμα που με είσοδο ακέραιους $x, y, z \geq 1$, να αποφασίζει αν υπάρχει ακέραιος $n > 2$, τέτοιος ώστε $x^n + y^n = z^n$.

3) Γράψτε ένα πρόγραμμα που με είσοδο την πρόταση:
« Για οποιουσδήποτε ακέραιους $x, y, z \geq 1$ δεν υπάρχει ακέραιος $n > 2$, τέτοιος ώστε $x^n + y^n = z^n$»,
να αποφασίζει αν η πρόταση είναι αληθής.

4) Γράψτε ένα πρόγραμμα που με είσοδο μια μαθηματική πρόταση $\mathcal{P}$ (σε κατάλληλο συμβολισμό), να αποφασίζει αν η $\mathcal{P}$ είναι αληθής.

Η Περίπτωση 4 αντιστοιχεί στο περίφημο Entscheidungsproblem του David Hilbert.

Κάποια πρόσωπα της ιστορίας μας

David Hilbert: Έθεσε (μεταξύ άλλων) τα ερωτήματα

(i) αν μπορεί να αποδειχτεί πως τα Μαθηματικά είναι συνεπή (consistent) (*2^o πρόβλημα του H., 1900*).

(ii) αν υπάρχει αλγόριθμος για την επίλυση ακέραιων εξισώσεων (*10^o πρόβλημα του H., 1900*).

(iii) αν τα Μαθηματικά μπορούν να «αυτοματοποιηθούν» (*Entscheidungsproblem, 1928*).

Kurt Gödel: Εδειξε ότι το (i) είναι αδύνατο με το περίφημο «Θεώρημα της μη πληρότητας» (1930).

Alan Turing: Έθεσε τις βάσεις της Θεωρίας Υπολογισμού. Όρισε την έννοια του υπολογιστή (μηχανές Turing) και μελέτησε την έννοια της υπολογισιμότητας (1936). Έδειξε πως ουσιαστικά το (iii) είναι αδύνατο.

Το Θεώρημα της μη πληρότητας του K. Gödel (απλοποιημένο)

Ένα λογικό σύστημα S λέγεται συνεπές (consistent) αν κάθε πρόταση που αποδεικνύουμε εντός του S είναι αληθής.

Το Θεώρημα της μη πληρότητας του K. Gödel (απλοποιημένο)

Ένα λογικό σύστημα S λέγεται συνεπές (consistent) αν κάθε πρόταση που αποδεικνύουμε εντός του S είναι αληθής.

Ο Gödel διατύπωσε, στο φορμαλισμό ενός δεδομένου S, μία πρόταση U που λέει: «Η U δεν μπορεί να αποδειχτεί στο S».

Το Θεώρημα της μη πληρότητας του K. Gödel (απλοποιημένο)

Ένα λογικό σύστημα S λέγεται συνεπές (consistent) αν κάθε πρόταση που αποδεικνύουμε εντός του S είναι αληθής.

Ο Gödel διατύπωσε, στο φορμαλισμό ενός δεδομένου S, μία πρόταση U που λέει: «Η U δεν μπορεί να αποδειχτεί στο S».

Θεώρημα: Αν το S είναι συνεπές τότε

1. Η U είναι αληθής.
2. Η U δεν μπορεί να αποδειχτεί στο S.
3. Η άρνηση της U, την οποία συμβολίζουμε $\overline{U}$, δεν μπορεί να αποδειχτεί στο S.

Το Θεώρημα της μη πληρότητας του K. Gödel (απλοποιημένο)

Ένα λογικό σύστημα S λέγεται συνεπές (consistent) αν κάθε πρόταση που αποδεικνύουμε εντός του S είναι αληθής.

Ο Gödel διατύπωσε, στο φορμαλισμό ενός δεδομένου S, μία πρόταση U που λέει: «Η U δεν μπορεί να αποδειχτεί στο S».

Θεώρημα: Αν το S είναι συνεπές τότε

1. Η U είναι αληθής.
2. Η U δεν μπορεί να αποδειχτεί στο S.
3. Η άρνηση της U, την οποία συμβολίζουμε $\overline{U}$, δεν μπορεί να αποδειχτεί στο S.

Πόρισμα: Δεν μπορούμε να αποδείξουμε εντός του S πως το S είναι συνεπές.

Το Θεώρημα της μη πληρότητας του K. Gödel (απλοποιημένο)

Ένα λογικό σύστημα S λέγεται συνεπές (consistent) αν κάθε πρόταση που αποδεικνύουμε εντός του S είναι αληθής.

Ο Gödel διατύπωσε, στο φορμαλισμό ενός δεδομένου S, μία πρόταση U που λέει: «Η U δεν μπορεί να αποδειχτεί στο S».

Θεώρημα: Αν το S είναι συνεπές τότε

1. Η U είναι αληθής.
2. Η U δεν μπορεί να αποδειχτεί στο S.
3. Η άρνηση της U, την οποία συμβολίζουμε $\overline{U}$, δεν μπορεί να αποδειχτεί στο S.

Πόρισμα: Δεν μπορούμε να αποδείξουμε εντός του S πως το S είναι συνεπές.

Ο A. Turing και το Entscheidungsproblem

Πρόταση $Q(P, x)$: «Αν το πρόγραμμα P πάρει είσοδο τη συμβολοσειρά x, τότε το P θα τερματίσει».

Θεώρημα: Υπάρχουν P_0 και x_0, για τα οποία δεν μπορεί να γραφτεί πρόγραμμα που να αποφασίζει, αν η πρόταση $Q(P_0, x_0)$ είναι αληθής.

Ο Turing έδειξε ακόμη πως η $Q(P_0, x_0)$ μπορεί να εκφραστεί σαν λογική πρόταση.

Από το Θεώρημα έπεται πως δεν μπορεί να γραφτεί πρόγραμμα που να αποδεικνύει τη λογική πρόταση $Q(P_0, x_0)$ (ή το συμπλήρωμα της).

Δεν μπορούμε λοιπόν να αυτοματοποιήσουμε τα Μαθηματικά. Δεν μπορούμε να γράψουμε ένα πρόγραμμα που να αποφασίζει ποιες μαθηματικές προτάσεις είναι αληθείς!

Το Entscheidungsproblem του Hilbert είναι μη επιλύσιμο!

Η έννοια «πρόβλημα» ΙΙΙ

Ζητάμε αλγορίθμους για τα ακόλουθα ερωτήματα.

Π1: Δίνεται γράφημα $G = (V, E)$, και κορυφές $s, t \in V$. Να βρεθεί στον G ένα μονοπάτι από το s στο t.

Π2: Δίνεται γράφημα $G = (V, E)$, και κορυφές $s, t \in V$. Υπάρχει στον G μονοπάτι από το s στο t;

Το Π1 είναι πρόβλημα εύρεσης. Το Π2 είναι πρόβλημα απόφασης, δηλ. απαντιέται με ΝΑΙ ή ΟΧΙ.

Το Π2 ανάγεται στο πρόβλημα Π1: αν λύσω το πρόβλημα εύρεσης έχω λύσει και το πρόβλημα απόφασης. Το αντίστροφο δεν ισχύει απαραίτητα.

Χάριν κομψότητας και ευκολίας θα ασχοληθούμε κυρίως με προβλήματα απόφασης.

Προβλήματα απόφασης και γλώσσες

Όρισε ενα κατάλληλο πεπερασμένο αλφάβητο Σ. (Π.χ. $\Sigma = \{0, 1\}$).

Κάθε πρόβλημα απόφασης κωδικοποιείται με μια γλώσσα, δηλ. ένα υποσύνολο του συνόλου όλων των δυνατών συμβολοσειρών Σ.

Π.χ.
Π2: Δίνεται γράφημα $G = (V, E)$, και κορυφές $s, t \in V$. Υπάρχει στον G μονοπάτι από το s στο t;

Αντίστοιχη γλώσσα
L:= { δυαδικές συμβολοσειρές w, τ.ω. $w =< G = (V, E), s, t >$ και ο G περιέχει μονοπάτι από το s στο t }.

Προβλήματα απόφασης και γλώσσες

Όρισε ενα κατάλληλο πεπερασμένο αλφάβητο Σ. (Π.χ. $\Sigma = \{0, 1\}$).

Κάθε πρόβλημα απόφασης κωδικοποιείται με μια γλώσσα, δηλ. ένα υποσύνολο του συνόλου όλων των δυνατών συμβολοσειρών Σ.

Π.χ.
Π2: Δίνεται γράφημα $G = (V, E)$, και κορυφές $s, t \in V$. Υπάρχει στον G μονοπάτι από το s στο t;

Αντίστοιχη γλώσσα
L:= { δυαδικές συμβολοσειρές w, τ.ω. $w =< G = (V, E), s, t >$ και ο G περιέχει μονοπάτι από το s στο t }.

Λύνω το Π2 ισοδύναμο με «δεδομένης συμβολοσειράς w, ανήκει η w στην L;»

Συμβολοσειρές και γλώσσες

Αλφάβητο: Αλφάβητο είναι κάθε πεπερασμένο μη κενό σύνολο. Τα μέλη του τα ονομάζουμε σύμβολα ή γράμματα.

Π.χ. $\Sigma_1 = \{0, 1\}$, $\Sigma_2 = \{a, b, \ldots, w\}$.**Συμβολοσειρά (string):** Συμβολοσειρά ενός αλφάβητου Σ είναι μια πεπερασμένη ακολουθία συμβόλων του Σ.

Π.χ. 0101101 είναι συμβολοσειρά του αλφάβητου $\Sigma = \{0, 1, 2\}$.

Συμβολοσειρές και γλώσσες

Αλφάβητο: Αλφάβητο είναι κάθε πεπερασμένο μη κενό σύνολο. Τα μέλη του τα ονομάζουμε σύμβολα ή γράμματα.

Π.χ. $\Sigma_1 = \{0, 1\}$, $\Sigma_2 = \{a, b, \ldots, w\}$.**Συμβολοσειρά (string):** Συμβολοσειρά ενός αλφάβητου Σ είναι μια πεπερασμένη ακολουθία συμβόλων του Σ.

Π.χ. 0101101 είναι συμβολοσειρά του αλφάβητου $\Sigma = \{0, 1, 2\}$.

Τη (μοναδική) συμβολοσειρά μήκους 0, την ονομάζουμε κενή και τη συμβολίζουμε με ε. Το σύνολο των συμβολοσειρών μήκους k το συμβολίζουμε με Σ^k, π.χ. $\{0, 1\}^2 = \{00, 01, 10, 11\}$.

Συμβολοσειρές και γλώσσες

Αλφάβητο: Αλφάβητο είναι κάθε πεπερασμένο μη κενό σύνολο. Τα μέλη του τα ονομάζουμε σύμβολα ή γράμματα.

Π.χ. $\Sigma_1 = \{0, 1\}$, $\Sigma_2 = \{a, b, \ldots, w\}$.**Συμβολοσειρά (string):** Συμβολοσειρά ενός αλφάβητου Σ είναι μια πεπερασμένη ακολουθία συμβόλων του Σ.

Π.χ. 0101101 είναι συμβολοσειρά του αλφάβητου $\Sigma = \{0, 1, 2\}$.

Τη (μοναδική) συμβολοσειρά μήκους 0, την ονομάζουμε κενή και τη συμβολίζουμε με ε. Το σύνολο των συμβολοσειρών μήκους k το συμβολίζουμε με Σ^k, π.χ. $\{0, 1\}^2 = \{00, 01, 10, 11\}$.

Το σύνολο όλων των συμβολοσειρών του Σ το συμβολίζουμε με Σ^*. Π.χ. $\{0, 1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$.

Πράξεις με συμβολοσειρές

Παράθεση (concatenation): Η παράθεση δύο συμβολοσειρών x και y είναι η συμβολοσειρά xy που τη συμβολίζουμε xy ή $x \circ y$.

Π.χ. Η παράθεση του $x = 011$ και του $y = 1001$ είναι $x \circ y = 0111001$.

Επανάληψη: Αν w είναι μια συμβολοσειρά, τότε w^k αποτελείται από την παράθεση k αντιγράφων του w.

Π.χ. $(01)^3 = 010101$.

Αντίστροφη: Η αντίστροφη μιάς συμβολοσειράς w συμβολίζεται με w^R και προκύπτει αν διαβάσουμε το w από το τέλος προς την αρχή.

Π.χ. $01011^R = 11010$.

Άσκηση: Δείξε ότι για οποιεσδήποτε συμβολοσειρές x και y: $(x \circ y)^R = y^R \circ x^R$.

Γλώσσες (Languages)

Γλώσσα: Έστω Σ ένα αλφάβητο. Οποιοδήποτε υποσύνολο του Σ^* ονομάζεται γλώσσα του Σ.

Π.χ. Έστω $\Sigma = \{0, 1, \ldots, 9\}$. Τα παρακάτω σύνολα είναι γλώσσες του Σ:

- $L_1 = \{23, 044, 9999\}$ (πεπερασμένη γλώσσα).
- $L_2 = \{\varepsilon, 1, 11, 111, 1111, \ldots\}$.
- $L_3 = \{w : w$ είναι πρώτος αριθμός (η δεκαδική παράσταση του)$\} = \{2, 3, 5, 7, 11, 13, \ldots\}$.
- $L_4 = \{w : w$ είναι πρώτος αριθμός (η δυαδική παράσταση του)$\} = \{10, 11, 101, 111, 1011, 1101, \ldots\}$.
- $L_5 = \{\} = \emptyset$ (κενή γλώσσα).
- $L_6 = \{\varepsilon\}$.
- $L_7 = \{w : w$ είναι πρόγραμμα της C++ χωρίς input που δεν τελειώνει ποτέ (κωδικοποιημένο στο δυαδικό σύστημα)$\}$.
- $L_8 = \{w : w$ είναι πρόγραμμα της C++ χωρίς input που **κάποτε τελειώνει** (κωδικοποιημένο στο δυαδικό σύστημα)$\}$.

Πράξεις με γλώσσες

Αφού οι γλώσσες είναι σύνολα, ορίζεται η **ένωση** $L_1 \cup L_2$ και η **τομή** τους $L_1 \cap L_2$ όπως και το συμπλήρωμα:

Συμπλήρωμα: Το συμπλήρωμα μιας γλώσσας L του αλφαβήτου Σ συμβολίζεται με $\bar{L}$ και είναι η γλώσσα $\Sigma^* - L$ που αποτελείται από τις συμβολοσειρές του Σ που **δεν** ανήκουν στην L.

Επιπλέον μπορούμε να ορίσουμε τις παρακάτω πράξεις σε γλώσσες:

Παράθεση: Αν L_1 και L_2 είναι δυο γλώσσες του αλφαβήτου Σ, τότε η παράθεσή τους συμβολίζεται $L_1 \circ L_2$ ή $L_1 L_2$ και ορίζεται σαν $L_1 \circ L_2 = \{w : w = xy \text{ για κάποιο } x \in L_1 \text{ και κάποιο } y \in L_2\}$.

Π.χ. αν $L_1 = \{0, 1, 00\}$ και $L_2 = \{\varepsilon, 00\}$ τότε
$L_1 \circ L_2 = \{0, 1, 00, 000, 100, 0000\}$.

Kleene star: Η Kleene star L^* μια γλώσσας L είναι η γλώσσα των συμβολοσειρών που προκύπτουν από παράθεση μηδέν ή περισσοτέρων συμβολοσειρών της L:

$$L^* = \{w \mid w = w_1 \circ w_2 \circ \cdots \circ w_n \text{ για } n \geq 0 \text{ και } w_1, \ldots, w_n \in L\}.$$

Π.χ. Αν $L = \{0, 11\}$ τότε
$L^* = \{\varepsilon, 0, 00, 11, 000, 011, 110, 0000, 0011, 0110, 1100, 1111, \ldots\}$.

Π.χ. Αν $L = \{\varepsilon\}$ τότε $L^* = \{\varepsilon\}$.

Π.χ. Αν $L = \{\}$ τότε $L^* = \{\varepsilon\}$ (άρα για κάθε L: $\varepsilon \in L^*$).

L^+: Ορίζουμε επίσης $L^+ = LL^*$.

Άσκηση: Για ποιές γλώσσες έχουμε $L^* \neq L^+$;

Πόσες συμβολοσειρές και γλώσσες υπάρχουν;

Θεώρησε ένα αλφάβητο Σ (εξ ορισμού πεπερασμένο).

Πόσες συμβολοσειρές του Σ υπάρχουν; Άπειρες.

Πόσες γλώσσες του Σ υπάρχουν; Άπειρες.

Αλλά υπάρχουν πολλών ειδών «άπειρα».

Πόσες συμβολοσειρές και γλώσσες υπάρχουν;

Θεώρησε ένα αλφάβητο Σ (εξ ορισμού πεπερασμένο).

Πόσες συμβολοσειρές του Σ υπάρχουν; Άπειρες.
Πόσες γλώσσες του Σ υπάρχουν; Άπειρες.
Αλλά υπάρχουν πολλών ειδών «άπειρα».

Όπως θα δούμε, υπάρχουν «περισσότερες» γλώσσες από συμβολοσειρές...

Πεπερασμένα και άπειρα σύνολα

Ισάριθμα σύνολα: Δύο σύνολα A και B λέγονται ***ισάριθμα*** αν υπάρχει αμφιμονοσήμαντη αντιστοιχία $f : A \to B$.

Πεπερασμένα και άπειρα σύνολα

Ισάριθμα σύνολα: Δύο σύνολα A και B λέγονται ***ισάριθμα*** αν υπάρχει αμφιμονοσήμαντη αντιστοιχία $f : A \to B$.

Ένα σύνολο A λέγεται πεπερασμένο αν υπάρχει $n \in \mathbb{N}$ έτσι ώστε τα A και $\{1, 2, \ldots, n\}$ να είναι ισάριθμα. Ως πληθικός αριθμός του A ορίζεται το n (συμβολίζεται με $|A|$).

Πεπερασμένα και άπειρα σύνολα

Ισάριθμα σύνολα: Δύο σύνολα A και B λέγονται ***ισάριθμα*** αν υπάρχει αμφιμονοσήμαντη αντιστοιχία $f : A \to B$.

Ένα σύνολο A λέγεται πεπερασμένο αν υπάρχει $n \in \mathbb{N}$ έτσι ώστε τα A και $\{1, 2, \ldots, n\}$ να είναι ισάριθμα. Ως πληθικός αριθμός του A ορίζεται το n (συμβολίζεται με $|A|$).

Ένα σύνολο A λέγεται άπειρο αν δεν είναι πεπερασμένο. Π.χ. το $\mathbb{N}$ είναι άπειρο (αποδείξτε το).

Αριθμήσιμα Σύνολα

Ισάριθμα σύνολα: Δύο σύνολα A και B λέγονται ***ισάριθμα*** αν υπάρχει αμφινοσήμαντη αντιστοιχία $f : A \to B$.

Αριθμήσιμα Σύνολα

Ισάριθμα σύνολα: Δύο σύνολα A και B λέγονται ***ισάριθμα*** αν υπάρχει αμφινοσήμαντη αντιστοιχία $f : A \to B$.

Ένα σύνολο A λέγεται αριθμήσιμα άπειρο αν το A είναι ισάριθμο του $\mathbb{N}$.

Ένα σύνολο A λέγεται αριθμήσιμο αν είναι πεπερασμένο ή αριθμήσιμα άπειρο. (Ένα σύνολο που δεν είναι αριθμήσιμο λέγεται μη αριθμήσιμο).

Αριθμήσιμα Σύνολα

Ισάριθμα σύνολα: Δύο σύνολα A και B λέγονται ***ισάριθμα*** αν υπάρχει αμφινοσήμαντη αντιστοιχία $f : A \to B$.

Ένα σύνολο A λέγεται αριθμήσιμα άπειρο αν το A είναι ισάριθμο του $\mathbb{N}$.

Ένα σύνολο A λέγεται αριθμήσιμο αν είναι πεπερασμένο ή αριθμήσιμα άπειρο. (Ένα σύνολο που δεν είναι αριθμήσιμο λέγεται μη αριθμήσιμο).

Διαισθητικά, το A είναι αριθμήσιμο αν υπάρχει τρόπος να «λιστάρουμε» τα στοιχεία του, δηλ. να τα γράψουμε υπό μορφή ακολουθίας.

Η λίστα μας είναι σωστή, αν για κάθε $x \in A$, μπορούμε να απαντήσουμε στην ερώτηση «ποια είναι η θέση του x στη λίστα;», δίνοντας έναν συγκεκριμένο αριθμό.

Σχετικά με την ορολογία

- Αγγλικός όρος: countable.
- Στην ελληνική μετάφραση των Lewis-Papadimitriou: μετρήσιμο.
- Μια καλύτερη μετάφραση: αριθμήσιμο.

Μετρώντας (συνέχεια)

Παραδείγματα αριθμήσιμων συνόλων:

- Το σύνολο των ζυγών αριθμών (αντιστοιχία: $f(n) = n/2$. Ακολουθία: $0, 2, 4, \ldots$).
- Το σύνολο των ακεραίων (Ακολουθία: $0, 1, -1, 2, -2, 3, -3, \ldots$).
- Το σύνολο των θετικών ρητών (Ακολουθία: $1/1, 1/2, 2/1, 1/3, 2/2, 3/1, 1/4, 2/3, 3/2, 4/1, \ldots$).

Θεώρημα: Το σύνολο Σ^* των συμβολοσειρών ενός αλφαβήτου Σ είναι αριθμήσιμο.

Θεώρημα: Το σύνολο Σ^* των συμβολοσειρών ενός αλφαβήτου Σ είναι αριθμήσιμο.

Απόδειξη: Εξ ορισμού το Σ είναι πεπερασμένο. Δημιουργούμε ακολουθία που περιέχει όλες τις συμβολοσειρές του Σ:

Θεώρημα: Το σύνολο Σ^* των συμβολοσειρών ενός αλφαβήτου Σ είναι αριθμήσιμο.

Απόδειξη: Εξ ορισμού το Σ είναι πεπερασμένο. Δημιουργούμε ακολουθία που περιέχει όλες τις συμβολοσειρές του Σ:

Πρώτη η συμβολοσειρά μήκους 0, μετά όλες οι συμβολοσειρές μήκους 1 (ταξινομημένες), μετά όλες οι συμβολοσειρές μήκους 2 (ταξινομημένες), κοκ.

Θεώρημα: Το σύνολο Σ^* των συμβολοσειρών ενός αλφαβήτου Σ είναι αριθμήσιμο.

Απόδειξη: Εξ ορισμού το Σ είναι πεπερασμένο. Δημιουργούμε ακολουθία που περιέχει όλες τις συμβολοσειρές του Σ:

Πρώτη η συμβολοσειρά μήκους 0, μετά όλες οι συμβολοσειρές μήκους 1 (ταξινομημένες), μετά όλες οι συμβολοσειρές μήκους 2 (ταξινομημένες), κοκ.

Αυτή είναι η λεξικογραφική διάταξη των συμβολοσειρών του Σ. Π.χ. Αν $\Sigma = \{0, 1\}$, η ακολουθία είναι $\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots$.

Θεώρημα: Το σύνολο των γλωσσών ενός αλφαβήτου Σ είναι **μη αριθμήσιμο**.

Απόδειξη: Με εις άτοπο απαγωγή. Έστω ότι το σύνολο των γλωσσών του Σ είναι αριθμήσιμο. Τότε θα υπάρχει μια ακολουθία $S_1, S_2, \ldots$ των γλωσσών του Σ τέτοια ώστε κάθε γλώσσα του Σ να εμφανίζεται μία φορά σε αυτή. Θα κατασκευάσουμε γλώσσα T του Σ που διαφέρει απο κάθε S_i, $i = 1, 2, \ldots$.

Έστω $w_1, w_2, \ldots$ η λεξικογραφική ακολουθία όλων των συμβολοσειρών του Σ Θα φροντίσουμε ώστε η T να διαφέρει από την S_i στη θέση του w_i. Η T *περιέχει* τη συμβολοσειρά w_i αν και μόνο αν η S_i *δεν περιέχει* τη συμβολοσειρά w_i.

$$T = \{w_i : w_i \notin S_i,\ i = 1, 2, \ldots\}.$$

Θεώρημα: Το σύνολο των γλωσσών ενός αλφαβήτου Σ είναι **μη αριθμήσιμο**.

Απόδειξη: Με εις άτοπο απαγωγή. Έστω ότι το σύνολο των γλωσσών του Σ είναι αριθμήσιμο. Τότε θα υπάρχει μια ακολουθία $S_1, S_2, \ldots$ των γλωσσών του Σ τέτοια ώστε κάθε γλώσσα του Σ να εμφανίζεται μία φορά σε αυτή. Θα κατασκευάσουμε γλώσσα T του Σ που διαφέρει απο κάθε S_i, $i = 1, 2, \ldots$.

Έστω $w_1, w_2, \ldots$ η λεξικογραφική ακολουθία όλων των συμβολοσειρών του Σ Θα φροντίσουμε ώστε η T να διαφέρει από την S_i στη θέση του w_i. Η T *περιέχει* τη συμβολοσειρά w_i αν και μόνο αν η S_i *δεν περιέχει* τη συμβολοσειρά w_i.

$$T = \{w_i : w_i \notin S_i,\ i = 1, 2, \ldots\}.$$

Συνεπώς η ακολουθία $S_1, S_2, \ldots$ δεν περιέχει όλες τις γλώσσες του Σ. Άρα το σύνολο των γλωσσών του Σ είναι μη αριθμήσιμο.

Συμπεράσματα για την αναπαράσταση των γλωσσών με πεπερασμένες περιγραφές.

- Οποιαδήποτε αναπαράσταση και αν διαλέξουμε, θα υπάρχουν γλώσσες που δεν περιγράφονται.
- Π.χ., υπάρχει κάποια γλώσσα L τέτοια ώστε κανένα πρόγραμμα C++ δεν μπορεί να τυπώσει όλες τις συμβολοσειρές της (ακόμα και αν το αφήσουμε να τρέχει για πάντα). Γιατί; Το σύνολο των προγραμμάτων είναι αριθμήσιμο, ενώ το σύνολο των γλωσσών δεν είναι.

Συμπεράσματα για την αναπαράσταση των γλωσσών με πεπερασμένες περιγραφές.

- Οποιαδήποτε αναπαράσταση και αν διαλέξουμε, θα υπάρχουν γλώσσες που δεν περιγράφονται.
- Π.χ., υπάρχει κάποια γλώσσα L τέτοια ώστε κανένα πρόγραμμα C++ δεν μπορεί να τυπώσει όλες τις συμβολοσειρές της (ακόμα και αν το αφήσουμε να τρέχει για πάντα). Γιατί; Το σύνολο των προγραμμάτων είναι αριθμήσιμο, ενώ το σύνολο των γλωσσών δεν είναι.

Οι γλώσσες που μας ενδιαφέρουν είναι αυτές που μπορούν να περιγραφούν (αυτές που έχουν πεπερασμένη περιγραφή). Υπάρχει πρόγραμμα C++ για αυτές τις γλώσσες; Αυτό είναι ένα κεντρικό θέμα του μαθήματος.

Για να το μελετήσουμε πρέπει πρώτα να συμφωνήσουμε για το τί εννοούμε με τον όρο «πεπερασμένη περιγραφή».

Μέθοδος Διαγωνιοποίησης

Πώς αποδείξαμε ότι το σύνολο των γλωσσών δεν είναι αριθμήσιμο; Η μέθοδος που χρησιμοποιήσαμε λέγεται *διαγωνιοποίηση* και είναι πολύ απλή.

Μέθοδος Διαγωνιοποίησης

Πώς αποδείξαμε ότι το σύνολο των γλωσσών δεν είναι αριθμήσιμο; Η μέθοδος που χρησιμοποιήσαμε λέγεται *διαγωνιοποίηση* και είναι πολύ απλή.

Μέθοδος Διαγωνιοποίησης: Έστω R μια διμελής σχέση ενός συνόλου A, δηλαδή R είναι ένα υποσύνολο του Καρτεσιανού γινομένου $A \times A$: $R \subseteq \{(a_1, a_2) : \ a_1, a_2 \in A\}$. Τότε το διαγώνιο σύνολο $\Delta = \{(a : \ (a, a) \notin R\}$ διαφέρει από κάθε γραμμή $R_a = \{b : \ (a, b) \in R\}$

Π.χ. $A = \{1, 2, 3, 4, 5\}$ και $R = \{(1, 3), (1, 5), (2, 2), (2, 4), (2, 6), (3, 3), (3, 5), (4, 2), (4, 5), (5, 1), (5, 2), (5, 3), (5, 5)\}$.

	1	2	3	4	5
1			X		X
2		X		X	X
3			X		X
4		X			X
5	X	X	X		X

Οι γραμμές της R είναι $R_1 = \{3, 5\}$, $R_2 = \{2, 4, 5\}$, $R_3 = \{3, 5\}$, $R_4 = \{2, 5\}$, και $R_5 = \{1, 2, 3, 5\}$.

Το διαγώνιο σύνολο είναι το $\Delta = \{1, 4\}$ και είναι διαφορετικό από κάθε γραμμή της R.

Π.χ. $A = \{1, 2, 3, 4, 5\}$ και $R = \{(1, 3), (1, 5), (2, 2), (2, 4), (2, 6), (3, 3), (3, 5), (4, 2), (4, 5), (5, 1), (5, 2), (5, 3), (5, 5)\}$.

	1	2	3	4	5
1	X		X		X
2		X		X	X
3			X		X
4		X		X	X
5	X	X	X		X

Οι γραμμές της R είναι $R_1 = \{3, 5\}$, $R_2 = \{2, 4, 5\}$, $R_3 = \{3, 5\}$, $R_4 = \{2, 5\}$, και $R_5 = \{1, 2, 3, 5\}$.

Το διαγώνιο σύνολο είναι το $\Delta = \{1, 4\}$ και είναι διαφορετικό απο κάθε γραμμή της R.

X			X	

Πραγματικοί αριθμοί

Την μέθοδο διαγωνιοποίησης την εισήγαγε ο Georg Cantor στα 1891. Την χρησιμοποίησε για να δείξει ότι το σύνολο των πραγματικών αριθμών $\mathbb{R}$ είναι «μεγαλύτερο» από το σύνολο των φυσικών αριθμών $\mathbb{N}$.

Πραγματικοί αριθμοί

Την μέθοδο διαγωνιοποίησης την εισήγαγε ο Georg Cantor στα 1891. Την χρησιμοποίησε για να δείξει ότι το σύνολο των πραγματικών αριθμών $\mathbb{R}$ είναι «μεγαλύτερο» από το σύνολο των φυσικών αριθμών $\mathbb{N}$.

Θα δείξουμε κάτι ισχυρότερο.

Θεώρημα: Το διάστημα $(0, 1] \subseteq \mathbb{R}$ είναι μη αριθμήσιμο.

Κατ' επέκταση και το $\mathbb{R}$ αποκλείεται να είναι αριθμήσιμο.

Πραγματικοί αριθμοί

Κάθε $x \in (0,1]$, μπορεί να γραφτεί στο δεκαδικό σύστημα. Έστω το $(0,1]$ αριθμήσιμο. Τότε υπάρχει λίστα των στοιχείων του $(0,1]$ π.χ.

$$
\begin{aligned}
&0.\mathbf{0}000001\ldots\\
&0.0\mathbf{0}10000\ldots\\
&0.01\mathbf{1}0030\ldots\\
&0.080\mathbf{5}000\ldots\\
&\quad\vdots
\end{aligned}
$$

Ας κατασκευάσουμε τώρα έναν αριθμό που διαφέρει απο τον πρώτο στο πρώτο δεκαδικό ψηφίο, απο το δεύτερο στο δεύτερο δεκαδικό ψηφίο κοκ.

$$0.\mathbf{0}000001\ldots$$
$$0.0\mathbf{0}10000\ldots$$
$$0.01\mathbf{1}0030\ldots$$
$$0.080\mathbf{5}000\ldots$$
$$\vdots$$

Προσθέτουμε 1 στο iστο ψηφίο του iστου αριθμού στη λίστα. Παίρνουμε

$$0.1126\ldots$$

που διαφέρει από όλους τους αριθμούς. Καταλήγουμε πως δεν μπορεί να υπάρχει λίστα όλων των πραγματικών αριθμών, άτοπο.

Υπάρχει όμως ένα πρόβλημα με την απόδειξη αυτη. Γιατί;

Το πρόβλημα με την απόδειξη είναι ότι η δεκαδική παράσταση ενος αριθμού δεν είναι μοναδική!

Π.χ. $0.10000\ldots = 0.09999\ldots$

Αριθμοί που από «συντακτική» άποψη φαίνονται διαφορετικοί μπορεί να είναι ίδιοι. Άρα μπορεί ο αριθμός που κατασκευάζουμε να ανήκει στη λίστα.

Λύνεται αν κατασκευάσουμε σωστά το νέο αριθμό (π.χ. αν τα k-στο ψηφίο του αριθμού που κατασκευάζουμε διαφέρει κατά τουλάχιστον 2 από το αντίστοιχο ψηφίο του k-στού αριθμού).

Η Υπόθεση του Συνεχούς

Παρεμπιπτόντως, ένα από τα μεγαλύτερα προβλήματα της Λογικής στον 20ο αιώνα είναι η «Υπόθεση του Συνεχούς».

Συνεχές (continuum) είναι ένα όνομα που χρησιμοποιείται για να δηλώσει το $\mathbb{R}$.

Υπόθεση του Συνεχούς: Δεν υπάρχει κανένα σύνολο «μεγαλύτερο» από τους φυσικούς $\mathbb{N}$ και «μικρότερο» από τους πραγματικούς $\mathbb{R}$. Με άλλα λόγια, κάθε μη αριθμήσιμο σύνολο περιέχει ένα υποσύνολο ισάριθμο με το $\mathbb{R}$.

Η διαλεύκανση της Υπόθεσης είναι γνωστή ως το πρώτο πρόβλημα του Hilbert.

Η Υπόθεση του Συνεχούς

Υπόθεση του Συνεχούς: Δεν υπάρχει κανένα σύνολο «μεγαλύτερο» από τους φυσικούς $\mathbb{N}$ και «μικρότερο» από τους πραγματικούς $\mathbb{R}$. Με άλλα λόγια, κάθε μη αριθμήσιμο σύνολο περιέχει ένα υποσύνολο ισάριθμο με το $\mathbb{R}$.

Η Υπόθεση του Συνεχούς

Υπόθεση του Συνεχούς: Δεν υπάρχει κανένα σύνολο «μεγαλύτερο» από τους φυσικούς $\mathbb{N}$ και «μικρότερο» από τους πραγματικούς $\mathbb{R}$. Με άλλα λόγια, κάθε μη αριθμήσιμο σύνολο περιέχει ένα υποσύνολο ισάριθμο με το $\mathbb{R}$.

- Ο Gödel έδειξε το 1937 ότι η Υπόθεση του Συνεχούς είναι συμβατή με τα αξιώματα της συνολοθεωρίας (άρα δεν υπάρχει απόδειξη ότι η υπόθεση δεν ισχύει).
- Ο Cohen έδειξε το 1963 ότι η άρνηση της Υπόθεσης του Συνεχούς είναι επίσης συμβατή με τα αξιώματα της συνολοθεωρίας (άρα δεν υπάρχει απόδειξη ότι η υπόθεση ισχύει).

Συνεπώς η Υπόθεση του Συνεχούς δεν μπορεί ούτε να αποδειχτεί ούτε να καταρριφθεί!!!