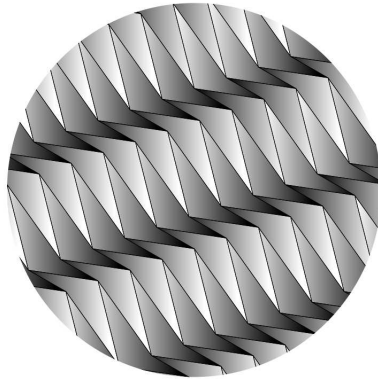


Πανεπιστήμιο Αθηνών

Μαθηματικά Πληροφορικής

Ηλίας Κουτσοπιάς



Αθήνα, Οκτώβριος 2009

Περιεχόμενα

Περιεχόμενα	1
Σύνολα	5
Άλλα Σύμβολα	6
1 Υποθέσεις και Θεωρήματα	9
1.1 Παρατήρηση - Υπόθεση - Απόδειξη	9
1.2 Εικασίες	14
Ασκήσεις	16
2 Αποδείξεις	19
2.1 Εξαντλητική μέθοδος	19
2.2 Μαθηματική επαγωγή	23
Ασκήσεις	31
3 Αναδρομή και Επαγωγή	35
Ασκήσεις	44
4 Αποδείξεις Ύπαρξης	47
4.1 Η Αρχή του Περιστερώνα	50
Ασκήσεις	54
5 Η Μέθοδος της Διαγωνίου	57
5.1 Αριθμήσιμα σύνολα	58
5.2 Η Μέθοδος της Διαγωνίου	61
5.3 Οι πραγματικοί αριθμοί	62
5.4 Υπολογισιμότητα	63
Ασκήσεις	64
6 Διακριτή Πιθανότητα	69
6.1 Δειγματικοί χώροι και πιθανότητα	69
6.2 Τυχαίες μεταβλητές και αναμενόμενη τιμή	74
6.3 Ανεξαρτησία	76
Ασκήσεις	81
7 RSA και πρώτοι αριθμοί	83

7.1	RSA	85
	Ασκήσεις	91
8	Ανάλυση Αλγορίθμων	93
8.1	Ο συμβολισμός O	95
8.2	Οι συμβολισμοί και \mathfrak{fi}	99
	Ασκήσεις	101
9	Γράφοι	103
9.1	Ειδικές κατηγορίες γράφων	105
9.2	Περιγραφή γράφων σε υπολογιστή	109
9.3	Δένδρα και Συνεκτικότητα	111
9.4	Επίπεδοι γράφοι	114
9.5	Κύκλοι του Euler και του Hamilton	118
9.6	Ταιριάσματα	121
	Ασκήσεις	125
A'	Λύσεις επιλεγμένων ασκήσεων	129
B'	Άλλες Πηγές	155

Πρόλογος

Οι σημειώσεις αυτές είναι στα αρχικά στάδια γραφής. Είναι ελλιπείς και περιέχουν τυπογραφικά λάθη, ανακρίβειες, και πιθανώς λάθη ουσίας. Δίνονται σαν βοήθημα στους φοιτητές του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Αθηνών για το ακαδημαϊκό έτος 2009-10. Αν έχετε παρατηρήσεις, σχόλια, ή βρείτε λάθη παρακαλώ να στείλτε email στο elias@di.uoa.gr για να περιληφθούν σε πιθανή πληρέστερη μελλοντική έκδοση.

Το κεφάλαιο ‘Αναδρομικές εξισώσεις’ είναι γραμμένο από τον Ιωάννη Εμίρη, που δίδαξε το μάθημα το ακαδημαϊκό έτος 2008-9.

Ευχαριστώ όσους έστειλαν σχόλια και τυπογραφικά λάθη για προηγούμενες εκδόσεις των σημειώσεων. Ειδικά ευχαριστώ τον Δημήτρη Αραπάκη και τον Ιωάννη Εμίρη.

Αθήνα, Οκτώβριος 2009
Ηλίας Κουτσοπιάς

Συμβολισμός

Σύνολα

Ακόμα και το πιο βασικό σύνολο αριθμών, το σύνολο των φυσικών αριθμών, ορίζεται από μερικούς συγγραφείς σαν $\{1, 2, 3, \dots\}$ και από άλλους σαν $\{0, 1, 2, 3, \dots\}$. Εδώ θα προτιμήσουμε την πρώτη περίπτωση το σύνολο $\mathbb{N} = \{1, 2, 3, \dots\}$ θα το ονομάζουμε σύνολο φυσικών αριθμών και το σύνολο $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ θα το ονομάζουμε σύνολο μη αρνητικών ακεραιών.

Κάποια βασικά σύνολα αριθμών:

Φυσικοί ή θετικοί ακέραιοι (\mathbb{N} ή \mathbb{Z}^+): $1, 2, 3, \dots$

Μη αρνητικοί ακέραιοι (\mathbb{N}_0 ή \mathbb{Z}_0^+): $0, 1, 2, \dots$

Ακέραιοι (\mathbb{Z}): $0, 1, -1, 2, -2, \dots$

Θετικοί ρητοί (\mathbb{Q}^+): $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \dots$

Ρητοί (\mathbb{Q}): $0, \frac{1}{1}, -\frac{1}{1}, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{3}, -\frac{1}{3}, \dots$

Πραγματικοί (\mathbb{R})

Ένας γενικός τρόπος περιγραφής συνόλων είναι να περιγράψουμε τις ιδιότητες των στοιχείων του: $\{x \mid P(x)\}$ όπου $P(x)$ είναι μια ιδιότητα. Για παράδειγμα,

$$\{x \mid x \text{ είναι φυσικός που διαιρείται με το } 3\}$$

ή

$$\{n \mid n \in \mathbb{N} \text{ και υπάρχει } k \in \mathbb{N}: n = k^2 + k + 1\}$$

Ο συμβολισμός $\{x \mid P(x)\}$ ορίζει το σύνολο που περιέχει όλα τα στοιχεία που ικανοποιούν την ιδιότητα $P(x)$. Έτσι, το πρώτο παράδειγμα παραπάνω ορίζει το σύνολο $\{3, 6, 9, \dots\}$. Ένα συνηθισμένο λάθος είναι να αγνοήσουμε τη σύμβαση ότι το σύνολο $\{x \mid P(x)\}$ περιέχει όλα τα στοιχεία που ικανοποιούν την ιδιότητα $P(x)$. Έτσι, είναι λάθος να πούμε πως το πρώτο παράδειγμα ορίζει το σύνολο $\{9, 18, 27, \dots\}$: πράγματι, όλα τα στοιχεία του $\{9, 18, 27, \dots\}$ διαρούνται με το 3, αλλά δεν είναι τα μόνα.

Άλλα Σύμβολα

$\lfloor x \rfloor$: Το ακέραιο μέρος του x . Πιο συγκεκριμένα $\lfloor x \rfloor$ είναι ο ακέραιος που ικανοποιεί $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Π.χ. $\lfloor 3 \rfloor = 3$, $\lfloor 3.4 \rfloor = 3$, $\lfloor -3.4 \rfloor = -4$.

$\lceil x \rceil$: Ο μικρότερος ακέραιος που είναι μεγαλύτερος ή ίσος με x . Πιο συγκεκριμένα, το $\lceil x \rceil$ είναι ο ακέραιος που ικανοποιεί $\lceil x \rceil - 1 < x \leq \lceil x \rceil$. Π.χ. $\lceil 3 \rceil = 3$, $\lceil 3.4 \rceil = 4$, $\lceil -3.4 \rceil = -3$.

$\binom{n}{k}$: Ίσον με $\frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{1 \cdot 2 \cdot \dots \cdot k} = \frac{n!}{k!(n-k)!}$. Όσοι τρόποι υπάρχουν για να διαλέξουμε k στοιχεία από ένα σύνολο n διαφορετικών στοιχείων. Εμφανίζεται επίσης στην ανάπτυξη διωνύμου

$$\begin{aligned} (a + b)^n &= \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \\ &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-k} b^n. \end{aligned}$$

1 Υποθέσεις και Θεωρήματα

Στο Λύκειο, αλλά πολλές φορές και στο Πανεπιστήμιο, τα μαθηματικά μας παρουσιάζονται σαν έτοιμο προϊόν. Βλέπουμε συνήθως τη μια όψη των πραγμάτων, τη φωτεινή πλευρά όπου βρίσκονται τα θεωρήματα που κάποιος έχει διατυπώσει και αποδείξει (πολλές φορές πριν από αιώνες). Δεν βλέπουμε συνήθως την άλλη πλευρά, την αθέατη, που είναι τα θεωρήματα που είτε κανένας δεν τα έχει σκεφτεί και διατυπώσει ακόμα, είτε έχουν μεν διατυπωθεί αλλά δεν έχουν αποδειχτεί ακόμα. Για να κατανοήσουμε όμως σε βάθος τα πράγματα χρειάζεται όχι μόνο να μάθουμε κάποια θεωρήματα, αποδείξεις και τεχνικές, αλλά να γνωρίζουμε ‘τι ξέρουμε’ και ‘τι δεν ξέρουμε’. Αυτή η μεταγνώση μιας επιστημονικής περιοχής είναι καμιά φορά πιο σημαντική από την ίδια τη γνώση. Η ενδιαφέρουσα περιοχή με άλλα λόγια είναι το σύνορο των δυο πλευρών, εκεί που η σημερινή έρευνα προσπαθεί να επεκτείνει τη φωτεινή περιοχή σε βάρος της αθέατης.

1.1 Παρατήρηση - Υπόθεση - Απόδειξη

Παρατηρώντας προσεκτικά τα δεδομένα ενός προβλήματος συνήθως καταλήγουμε να διατυπώσουμε μια ή περισσότερες υποθέσεις. Μια υπόθεση είναι μια λογική πρόταση που πιστεύουμε ότι είναι αληθής. Όταν μια τέτοια πρόταση αποδειχτεί τότε λέγεται *θεώρημα*, *πρόταση*, ή *λήμμα*.

Η διατύπωση σωστών υποθέσεων είναι συνήθως το πιο σημαντικό βήμα για τη μελέτη ενός προβλήματος. Μια καλή υπόθεση πρέπει να είναι καθαρά διατυπωμένη, να είναι απλή και λιτή και να έχει το κατάλληλο επίπεδο αφαίρεσης. Το παρακάτω διάγραμμα δείχνει μια τυπική διαδικασία που αρχίζει με παρατηρήσεις και καταλήγει σε κατάλληλο θεώρημα.

Παρατηρήσεις, δεδομένα \rightarrow Υπόθεση \Leftrightarrow Απόδειξη \rightarrow Λήμμα
 \rightarrow Θεώρημα

Από τα δεδομένα εξάγουμε συνήθως υποθέσεις τις οποίες προσπαθούμε να αποδείξουμε. Αν αποτύχουμε, τροποποιούμε την υπόθεση και επαναλαμβάνουμε. Αλλά ακόμα και αν πετύχουμε να αποδείξουμε την

υπόθεση, η ίδια η απόδειξη συχνά υποδεικνύει κατάλληλες γενικεύσεις ή εξειδικεύσεις της υπόθεσης.

Ας δούμε ένα χαρακτηριστικό παράδειγμα αυτής της διαδικασίας.

ΠΑΡΑΔΕΙΓΜΑ 1.1. Ας πούμε ότι ‘παίζουμε’ με τα ακέραια πολλαπλάσια της χρυσής τομής φ . Η χρυσή τομή $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618 \dots$ είναι η μεγαλύτερη ρίζα της εξίσωσης $\varphi^2 = \varphi + 1$ και έχει πολλές καταπληκτικές ιδιότητες. Σχετίζεται για παράδειγμα με τους αριθμούς Fibonacci και με την αναπαράσταση των αριθμών ως συνεχή κλάσματα.

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

Εμφανίζεται συχνά σε βιολογικές διαδικασίες και φαίνεται να έχει σχέση με την αισθητική αντίληψη μας: λέγεται για παράδειγμα ότι κτήρια με λόγο διαστάσεων ίσο με φ έχουν αισθητική τελειότητα.

Ας παρατηρήσουμε όμως τα πολλαπλάσια του φ και φ^2 :

$1 \cdot \varphi = 1.618 \dots$	$1 \cdot \varphi^2 = 2.618$
$2 \cdot \varphi = 3.236 \dots$	$2 \cdot \varphi^2 = 5.236$
$3 \cdot \varphi = 4.854 \dots$	$3 \cdot \varphi^2 = 7.854$
$4 \cdot \varphi = 6.472 \dots$	$4 \cdot \varphi^2 = 10.472$
$5 \cdot \varphi = 8.090 \dots$	$5 \cdot \varphi^2 = 13.090$
$6 \cdot \varphi = 9.708 \dots$	$6 \cdot \varphi^2 = 15.708$

Τι παρατηρείτε για το ακέραιο μέρος των αριθμών αυτών; Μια παρατήρηση είναι ότι εμφανίζονται οι αριθμοί 1 (αριστερά), 2 (δεξιά), 3, 4 (αριστερά), 5 (δεξιά), 6 (αριστερά) κοκ. Μια φυσική υπόθεση επομένως είναι η ακόλουθη.

Υπόθεση 1. Το ακέραιο μέρος των πολλαπλασίων του φ και φ^2 περιλαμβάνει όλους τους φυσικούς αριθμούς.

Πριν προσπαθήσουμε να αποδείξουμε ότι η υπόθεση ισχύει, ας προσπαθήσουμε να την ελέγξουμε πειραματικά. Γράφουμε ένα σύντομο πρόγραμμα που να ελέγχει την υπόθεση για όλους τους φυσικούς αριθμούς από 1 έως ας πούμε το 1000 ή το 10000. Εναλλακτικά, ελέγχουμε αν η υπόθεση ισχύει για κάποιον (ή κάποιους) μεγάλους τυχαίους αριθμούς ως εξής. Διαλέγουμε, για παράδειγμα, ένα μεγάλο ‘τυχαίο’ αριθμό n , ας πούμε $n = 1000$. Η υπόθεση είναι ότι ο n είναι το ακέραιο μέρος κάποιου πολλαπλασίου του φ . Είναι; Αυτό είναι εύκολο

να το ελέγξουμε ως εξής: Με ποιον ακέραιο k πρέπει να πολλαπλασιάσουμε το φ ώστε το αποτέλεσμα να είναι λίγο μεγαλύτερο από n ; Προφανώς με το $k = \lceil n/\varphi \rceil = \lceil 1000/1.618 \rceil = 619$. Αλλά για $k = 619$ έχουμε $\lfloor k\varphi \rfloor = \lfloor 1001.563 \rfloor = 1001$. Ο 1000 λοιπόν δεν είναι ακέραιο μέρος κάποιου πολλαπλασίου του φ . Ας επαναλάβουμε τους υπολογισμούς για το φ^2 . Βρίσκουμε $k = \lceil n/\varphi^2 \rceil = 382$ για το οποίο ισχύει $\lfloor k\varphi^2 \rfloor = \lfloor 1000.089 \rfloor = 1000$. Η υπόθεση λοιπόν ισχύει για $n = 1000$. Αν επαναλάβουμε την ίδια διαδικασία για πολλά n θα παρατηρήσουμε ότι η υπόθεση ισχύει για όλα.

Ένας τέτοιος πειραματικός έλεγχος μιας υπόθεσης, αν και δεν μας βεβαιώνει απόλυτα ότι η υπόθεση είναι αληθής, μας οπλίζει με αρκετή εμπιστοσύνη στην ορθότητα της ώστε να προσπαθήσουμε να την αποδείξουμε. Εξάλλου σήμερα έχουμε το κατάλληλο εργαλείο για αυτό, τον υπολογιστή. Ο πειραματικός έλεγχος πρέπει να αποτελεί ένα ουσιαστικό συστατικό της αποδεικτικής διαδικασίας. Εκτός της εμπιστοσύνης, μας δίνει συνήθως και αρκετές πληροφορίες για να μας καθοδηγήσουν στην απόδειξη. Αλλά ο πειραματικός έλεγχος μιας υπόθεσης μπορεί να μας οδηγήσει μερικές φορές σε λάθος συμπεράσματα. Μόνο μια αυστηρή απόδειξη θα μας βεβαιώσει για την ορθότητα μιας υπόθεσης. Η ιστορία των μαθηματικών είναι γεμάτη από παραδείγματα υποθέσεων που φαίνονταν αληθείς αλλά αποδείχτηκαν ψευδείς· μερικές φορές δε, η πραγματικότητα αποδείχτηκε διαμετρικά αντίθετη της εικαζόμενης.

Ας προσπαθήσουμε λοιπόν να αποδείξουμε την υπόθεση.

Απόδειξη της υπόθεσης 1. Ας ορίσουμε

$$A = \{\lfloor k\varphi \rfloor : k = 1, 2, \dots\}$$

$$B = \{\lfloor k\varphi^2 \rfloor : k = 1, 2, \dots\}$$

Θέλουμε να δείξουμε ότι $N = A \cup B$. Είναι δύσκολο να επιχειρηματολογήσουμε με απειροσύνολα για αυτό ας επικεντρωθούμε στα υποσύνολα που περιλαμβάνουν μόνο τους αριθμούς $1, 2, \dots, n$.

$$A_n = A \cap \{1, 2, \dots, n\} = \{\lfloor k\varphi \rfloor : \lfloor k\varphi \rfloor \leq n \text{ και } k = 1, 2, \dots\}$$

$$B_n = B \cap \{1, 2, \dots, n\} = \{\lfloor k\varphi^2 \rfloor : \lfloor k\varphi^2 \rfloor \leq n \text{ και } k = 1, 2, \dots\}$$

Θέλουμε να δείξουμε ότι όλοι οι φυσικοί $\{1, 2, \dots, n\}$ ανήκουν στο $A_n \cup B_n$. Βρισκόμαστε σε κομβικό σημείο της απόδειξης. Διαλέξαμε, ελπίζουμε, το σωστό συμβολισμό και οριοθετήσαμε κατάλληλα το πρόβλημα. Πώς προχωράμε όμως στην απόδειξη; Φυσικά, δεν υπάρχει κάποια γενική μέθοδος που να μας βοηθάει σ' αυτό. Η ικανότητα όμως του καθενός μας να βρει μια κατάλληλη προσέγγιση εξαρτάται σε μεγάλο βαθμό από την εξάσκηση και εμπειρία μας. Αν έχουμε λύσει δεκάδες παρόμοιες περιπτώσεις, η λύση εμφανίζεται μαγικά από μόνη της.

Το συγκεκριμένο πρόβλημα είναι ένα καλό παράδειγμα για να δούμε τη δημιουργική διαδικασία των μαθηματικών. Είναι ένα πρόβλημα

εύκολο να το κατανοήσουμε και όπως θα δούμε έχει μια λύση που δεν απαιτεί παρά μόνο γνώσεις Λυκείου. Είναι όμως σχετικά δύσκολο πρόβλημα ακόμα και για έμπειρους μαθηματικούς γιατί έχει μια 'έξυπνη' προσέγγιση. Η 'έξυπνη' ιδέα που θα χρησιμοποιήσουμε είναι να επικεντρώσουμε την προσοχή μας όχι στα στοιχεία του συνόλου A_n αλλά στον αριθμό των στοιχείων του, στον πληθάρηθμό του.

Πόσα στοιχεία, λοιπόν, έχει το A_n ; Τα στοιχεία του A_n είναι της μορφής $[k\varphi]$, όπου $[k\varphi] \leq n$. Σε κάθε k αντιστοιχεί ένα ακριβώς στοιχείο. Αυτό μπορεί να μην ήταν έτσι αν το φ ήταν μικρότερο του 1, αλλά επειδή $\varphi > 1$ ισχύει. Πιο συγκεκριμένα, επειδή τα $(k+1)\varphi - k\varphi = \varphi$, έχουμε είτε $[(k+1)\varphi] = [k\varphi] + 1$ είτε $[(k+1)\varphi] = [k\varphi] + 2$.

Αφού λοιπόν για κάθε k έχουμε διαφορετικό στοιχείο, τα στοιχεία του A_n είναι ακριβώς όσοι οι φυσικοί k για τους οποίους ισχύει $[k\varphi] \leq n$. Αλλά αυτή η σχέση είναι ισοδύναμη με

$$k\varphi < n + 1 \Leftrightarrow k < \frac{n+1}{\varphi} \Leftrightarrow k \leq \lfloor \frac{n+1}{\varphi} \rfloor.$$

Δηλαδή, ο αριθμός των στοιχείων του συνόλου A_n είναι $|A_n| = \lfloor \frac{n+1}{\varphi} \rfloor$. Με τον ίδιο τρόπο βρίσκουμε $|B_n| = \lfloor \frac{n+1}{\varphi^2} \rfloor$. Ο συνολικός αριθμός λοιπόν των στοιχείων και των δυο συνόλων, A_n και B_n , είναι

$$|A_n| + |B_n| = \lfloor \frac{n+1}{\varphi} \rfloor + \lfloor \frac{n+1}{\varphi^2} \rfloor. \quad (1.1)$$

Θα δείξουμε ότι αυτός ο αριθμός είναι ίσος με n . Παρατηρούμε πρώτα ότι $\frac{1}{\varphi} + \frac{1}{\varphi^2} = 1$ (αυτό προκύπτει αν διαιρέσουμε όλους τους όρους της $\varphi^2 = \varphi + 1$ με φ^2). Επομένως

$$\frac{n+1}{\varphi} + \frac{n+1}{\varphi^2} = n + 1.$$

Αφού οι δυο αριθμοί $\frac{n+1}{\varphi}$ και $\frac{n+1}{\varphi^2}$ είναι άρρητοι και έχουν άθροισμα $n+1$, τα ακέραια μέρη τους έχουν άθροισμα n . (Για παράδειγμα $1001/1.618 = 618.652$, $1001/2.618 = 382.348$, $618.652 + 382.348 = 1001$, $\lfloor 618.652 \rfloor + \lfloor 382.348 \rfloor = 1000$.)

Δείξαμε λοιπόν ότι $|A_n| + |B_n| = n$. Από τον ορισμό των A_n και B_n , ξέρουμε πως τα σύνολα $A_{n-1} \cup B_{n-1}$ και $A_n \cup B_n$ μπορούν να διαφέρουν μόνο στο στοιχείο n . Αφού όμως δείξαμε πως $|A_n| + |B_n| = n$ και $|A_{n-1}| + |B_{n-1}| = n-1$, συμπεραίνουμε πως το $A_n \cup B_n$ περιέχει το στοιχείο n . Αυτό ολοκληρώνει την απόδειξη της υπόθεσης αφού κάθε στοιχείο n ανήκει στο $A \cup B$. \square

Αν παρατηρήσουμε προσεκτικά το τελευταίο μέρος της παραπάνω απόδειξης θα διαπιστώσουμε ότι όχι μόνο αποδείξαμε ότι κάθε φυσικός αριθμός γράφεται σαν $[k\varphi]$ ή σαν $[k\varphi^2]$, αλλά και ότι αυτό συμβαίνει με

μοναδικό τρόπο. Ο λόγος είναι το n υπάρχει στα A_n και B_n ακριβώς μια φορά αφού $(|A_n| + |B_n|) - (|A_{n-1}| + |B_{n-1}|) = n - (n - 1) = 1$.

Όταν βλέπουμε μια απόδειξη πρέπει να προσπαθούμε να καταλάβουμε ποια είναι η κεντρική ή οι κεντρικές ιδέες. Για παράδειγμα, μια φυσική ερώτηση για την παραπάνω απόδειξη είναι 'Ποια ακριβώς ιδιότητα του φ χρησιμοποιήσαμε;' Αν διαβάσουμε προσεκτικά την απόδειξη θα παρατηρήσουμε ότι χρησιμοποιήσαμε ακριβώς τις εξής δυο ιδιότητες:

- $\frac{1}{\varphi} + \frac{1}{\varphi^2} = 1$. Από αυτό προκύπτει αμέσως πως $\varphi > 1$, μια ιδιότητα που χρησιμοποιήθηκε και αυτή σε κάποιο σημείο της απόδειξης.
- Ο φ και φ^2 είναι θετικοί άρρητοι. Την ιδιότητα αυτή χρησιμοποιήσαμε όταν βγάλαμε το συμπέρασμα ότι τα ακέραια μέρη των αριθμών $\frac{n+1}{\varphi}$ και $\frac{n+1}{\varphi^2}$ έχουν άθροισμα n , επειδή οι δυο αυτοί αριθμοί έχουν άθροισμα $n + 1$. Αν οι φ και φ^2 ήταν ρητοί τότε για κάποια n οι αριθμοί $\frac{n+1}{\varphi}$ και $\frac{n+1}{\varphi^2}$ θα ήταν ακέραιοι και θα είχαν άθροισμα $n + 1$ αντί για το επιθυμητό n .

Επομένως η ίδια απόδειξη θα ήταν σωστή για οποιουδήποτε θετικούς άρρητους λ και μ που ικανοποιούν την εξίσωση $\frac{1}{\lambda} + \frac{1}{\mu} = 1$. Έτσι μπορούμε να γενικεύσουμε την υπόθεση στο εξής θεώρημα:

Θεώρημα 2. Έστω θετικοί άρρητοι λ και μ που ικανοποιούν $\frac{1}{\lambda} + \frac{1}{\mu} = 1$. Για κάθε φυσικό αριθμό n , υπάρχει μοναδικός ακέραιος k τέτοιος ώστε $n = [k\lambda]$ ή $n = [k\mu]$.

Για παράδειγμα, για $\lambda = \sqrt{2}$ και $\mu = 2 + \sqrt{2}$ έχουμε $\frac{1}{\lambda} + \frac{1}{\mu} = 1$. Άρα κάθε φυσικός αριθμός γράφεται με μοναδικό τρόπο σαν το ακέραιο μέρος κάποιου πολλαπλάσιου του $\sqrt{2}$ ή του $2 + \sqrt{2}$ (δοκιμάστε το!).

ΠΑΡΑΔΕΙΓΜΑ 1.2. Ας δούμε όμως ένα ακόμα παράδειγμα της διαδικασίας υπόθεση-απόδειξη-θεώρημα-γενίκευση. Ας παρατηρήσουμε τις τιμές του πολυώνυμου $n^2 - n + 41$ για $n = 1, 2, \dots$:

$$41, 43, 47, 53, 61, \dots$$

Παρατηρούμε ότι όλοι αυτοί οι αριθμοί είναι πρώτοι. Επομένως είναι φυσικό να κάνουμε την υπόθεση

Υπόθεση 3. Για κάθε φυσικό αριθμό n , ο αριθμός $n^2 - n + 41$ είναι πρώτος.

Δοκιμάζοντας πολλές τιμές για το n διαπιστώνουμε ότι η υπόθεση δεν ισχύει. Ισχύει για $n = 1, 2, \dots, 40$, αλλά για $n = 41$ βλέπουμε ότι το $41^2 - 41 + 41 = 41^2$ διαιρείται προφανώς από το 41.

* *

Όπως διαπιστώσαμε, το πολυώνυμο $n^2 - n + 41$ δεν καταφέρνει να παράγει όλους τους πρώτους αριθμούς και μόνο αυτούς. Υπάρχουν όμως πολυώνυμα που έχουν αυτή την ιδιότητα; Αναπάντεχα, η απάντηση είναι καταφατική (αλλά το πολυώνυμο πρέπει να έχει πολλές μεταβλητές). Π. χ. υπάρχει πολυώνυμο με 26 μεταβλητές που έχει αυτή την ιδιότητα και πιο συγκεκριμένα: το σύνολο των θετικών τιμών αυτού του πολυώνυμου είναι ακριβώς το σύνολο των πρώτων αριθμών.

1.2 Εικασίες

Μερικές φορές παρά τις προσπάθειες μας δεν καταφέρνουμε να αποδείξουμε αλλά ούτε να διαψεύσουμε μια υπόθεση. Μια τέτοια υπόθεση αποκαλείται εικασία. Οι εικασίες είναι η κινητήρια δύναμη των μαθηματικών και της επιστήμης γενικότερα. Προσπαθώντας να αποδείξουμε εικασίες αναγκαζόμαστε να ανακαλύψουμε νέες θεωρίες και τεχνικές. Μερικές διάσημες εικασίες είναι οι ακόλουθες:

Το τελευταίο θεώρημα του Fermat. Η εικασία, που τώρα αποτελεί θεώρημα, είναι ότι η εξίσωση $x^n + y^n = z^n$ δεν έχει λύση για μη μηδενικούς ακέραιους x, y , και z και για ακέραιο $n > 2$. Προτάθηκε από τον Pierre Fermat τον 17ο αιώνα και αποδείχτηκε από τον Andrew Wiles τη δεκαετία του 1990.

Η εικασία του Goldbach. Το 1742 ο Christian Goldbach διατύπωσε την εξής υπόθεση: Κάθε άρτιος αριθμός μεγαλύτερος του 2 μπορεί να γραφτεί σαν άθροισμα 2 πρώτων αριθμών. Π. χ. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$. Η εικασία δεν έχει αποδειχτεί ούτε καταρριφθεί ακόμα. Έχει όμως επιβεβαιωθεί με τη βοήθεια υπολογιστή για όλους τους άρτιους μέχρι 10^{14} .

Το θεώρημα των 4 χρωμάτων. Η εικασία, που και αυτή είναι τώρα πια θεώρημα, είναι ότι κάθε επίπεδος χάρτης μπορεί να χρωματιστεί με 4 χρώματα έτσι ώστε γειτονικές χώρες να έχουν διαφορετικά χρώματα. Η υπόθεση αυτή προτάθηκε πριν από 130 χρόνια περίπου και αποδείχτηκε τελικά το 1976 από τους Kenneth Appel και Wolfgang Haken. Η απόδειξη βασίζεται στον έλεγχο 1936 περιπτώσεων και η κάθε περίπτωση απαιτεί τον έλεγχο πολλών λογικών συνδυασμών. Μόνο με τη βοήθεια υπολογιστή μπορούν να ελεγχθούν όλες οι περιπτώσεις. Παραμένει ανοικτό πρόβλημα αν υπάρχει σύντομη απόδειξη, που δεν απαιτεί τεράστια υπολογιστική ικανότητα.

Η εικασία του $3x + 1$. Πάρε ένα φυσικό αριθμό x . Αν είναι άρτιος διαιρέσε τον με το 2, αλλιώς υπολόγισε το $3x + 1$. Επανάλαβε με το αποτέλεσμα μέχρι να προκύψει το 1. Για παράδειγμα: $7 \rightarrow 22 \rightarrow 11 \rightarrow 34 \rightarrow 17 \rightarrow 52 \rightarrow 26 \rightarrow 13 \rightarrow 40 \rightarrow 20 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$. Η εικασία λέει ότι αν αρχίσουμε από οποιοδήποτε φυσικό αριθμό x θα καταλήξουμε πάντα στο 1. Η εικασία προτάθηκε από διάφορους, γι αυτό και λέγεται επίσης το πρόβλημα του Collatz, το πρόβλημα του Ulam, ο αλγόριθμος του Hasse, κλπ. Η εικασία δεν έχει αποδειχτεί ούτε καταρριφθεί ακόμα. Έχει όμως επιβεβαιωθεί με τη βοήθεια υπολογιστή για αρκετά μεγάλους αριθμούς.

Η εικασία του Riemann. Η συνάρτηση ζ του Riemann ορίζεται ως εξής:

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \dots$$

Για $x > 1$ το άθροισμα συγκλίνει. Η συνάρτηση μπορεί να επεκταθεί και στους μιγαδικούς αριθμούς.

Η εικασία του Riemann λέει ότι οι μόνες ρίζες με θετικό πραγματικό τμήμα της αναλυτικής επέκτασης της συνάρτησης ζ , δηλαδή οι τιμές του x που ικανοποιούν $\zeta(x) = 0$ με $\Re(x) > 0$, είναι μιγαδικοί αριθμοί με πραγματικό τμήμα ίσο με $1/2$. Η εικασία προτάθηκε από τον Riemann πριν από 150 χρόνια περίπου και δεν έχει ακόμα αποδειχτεί ούτε καταρριφθεί.

Η εικασία του Riemann σχετίζεται άμεσα με την πυκνότητα των πρώτων αριθμών. Πόσοι πρώτοι αριθμοί είναι μικρότεροι από 1000; Από n ; Ας ορίσουμε αυτόν τον αριθμό ως $\pi(n)$. Πόσο μεγάλο είναι το $\pi(n)$; Έχει αποδειχτεί ότι το $\pi(n)$ είναι περίπου $n/\ln n$. Αυτό είναι το περίφημο *Θεώρημα των πρώτων αριθμών*. Αλλά πόσο κοντά στο $n/\ln n$ είναι το $\pi(n)$; Η εικασία του Riemann είναι ισοδύναμη με την πρόταση ότι το $\pi(n)$ και το $n/\ln n$ διαφέρουν κατά το πολύ $c\sqrt{n}\ln n$ για κάποια σταθερά c .

Η εικασία του Riemann είναι ένα εξαιρετο παράδειγμα για την ενότητα των μαθηματικών γιατί συνδέει διάφορες περιοχές όπως η Θεωρία Αριθμών και η Ανάλυση. Υπάρχουν για παράδειγμα εικασίες ισοδύναμες με την εικασία του Riemann ακόμα και στην θεωρία σημάτων (σταθερά de Bruijn-Newman). Αποτελεί επίσης εξαιρετο παράδειγμα για το πως θέματα εντελώς 'θεωρητικά' μπορεί με την ανάπτυξη της τεχνολογίας να γίνουν 'πρακτικά'. Η εικασία αυτή για παράδειγμα έχει άμεση σχέση με την κρυπτογραφία δημόσιου κλειδιού.

Η εικασία $P \neq NP$. Η πιο σημαντική εικασία στην πληροφορική και μια από τις σημαντικότερες εικασίες γενικότερα είναι η εικασία $P \neq NP$. Η εικασία λέει ότι υπάρχουν προβλήματα που λύνονται από μη ντετερμινιστικές μηχανές Turing σε πολυωνυμικό χρόνο αλλά απαιτούν περισσότερο από πολυωνυμικό χρόνο σε ντετερμινιστικές μηχανές. Με πιο απλά

λόγια, η εικασία λέει ότι υπάρχουν προβλήματα για τα οποία είναι αρκετά πιο δύσκολο να βρούμε τη λύση τους από το να επιβεβαιώσουμε την ορθότητά της.

Ένα τέτοιο πρόβλημα είναι το πρόβλημα της ικανοποιησιμότητας απλών λογικών προτάσεων που είναι γνωστό σαν SATISFIABILITY. Σ' αυτό το αλγοριθμικό πρόβλημα, δίνεται μια λογική πρόταση, για παράδειγμα,

$$(x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3),$$

και θέλουμε να βρούμε αν υπάρχουν τιμές των μεταβλητών που κάνουν την πρόταση αληθή. Προφανώς, αν κάποιος μας υποδείξει κατάλληλες τιμές μπορούμε εύκολα να επιβεβαιώσουμε αν οι τιμές αυτές έχουν την επιθυμητή ιδιότητα. Αλλά χωρίς κάποια τέτοια υπόδειξη, πόσο δύσκολο είναι να ελέγξουμε αν υπάρχουν τέτοιες τιμές; Η εικασία $P \neq NP$ λέει ότι χωρίς υπόδειξη, το πρόβλημα είναι δύσκολο, και πιο συγκεκριμένα, ότι δεν μπορεί να λυθεί πάντα σε χρόνο πολυωνυμικό ως προς το μήκος της πρότασης.

Ασκήσεις

1.1. Θεωρείστε τα πρώτα $k = 10$ πολλαπλάσια του φ και παρατηρείστε το δεκαδικό τους μέρος: 0.618, 0.236, 0.854, 0.472, 0.090, 0.708 ... Σχεδιάστε τις τιμές στο ευθύγραμμο τμήμα $[0, 1]$ και παρατηρείστε τα διαστήματα που δημιουργούνται. Ισοδύναμα, ταξινομήστε πρώτα τις τιμές αυτές (μαζί με τους αριθμούς 0 και 1) και έπειτα παρατηρείστε τις διαφορές μεταξύ διαδοχικών τιμών. Τι παρατηρείτε; Είναι όλα τα διαστήματα διαφορετικά μεταξύ τους;

Επαναλάβετε για $k = 15$. Διατυπώστε μια πρόταση που αφορά τον πληθάρημο του συνόλου αυτών των διαστημάτων για οποιοδήποτε ακέραιο k .

Γράψτε ένα πρόγραμμα που να ελέγχει την πρότασή σας για μικρά k , π. χ. $k < 1000$.

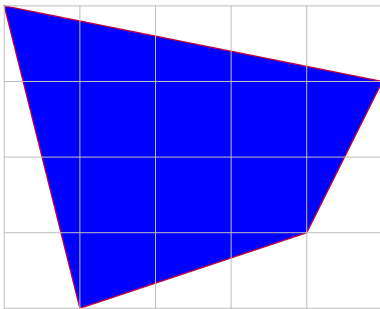
Προαιρετικό και κάπως δύσκολο πρόβλημα: Δοκιμάστε να αποδείξετε την πρόταση αυτή.

Υπάρχει παρόμοιο φαινόμενο για τα πολλαπλάσια του $\sqrt{2}$;

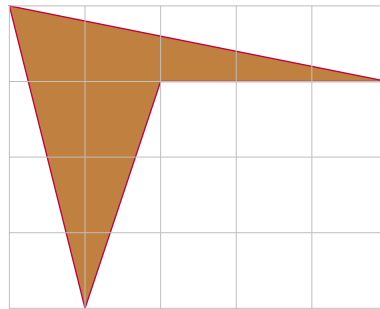
1.2. Στο πρόβλημα του Collatz βρείτε ένα αριθμό n τέτοιο ώστε αν αρχίσουμε από το n θα φτάσουμε σε κάποιο αριθμό μεγαλύτερο του $10n$.

1.3. Η κολλητή σας χτίζει καινούργιο σπίτι. Έχει παραγγείλει πλακάκια και τυχαίνει να είσαστε μαζί όταν παραλαμβάνει τα πλακάκια της κουζίνας. Όταν ανοίγετε όμως τα κουτιά, σας περιμένει μια έκπληξη. Το σχήμα τους δεν είναι ορθογώνιο αλλά το τετράπλευρο του Σχήματος 1.1(a). Η φίλη σας είναι έτοιμη να επικοινωνήσει με την εταιρεία και να τα επιστρέψει, όταν την πείθετε να το σκεφτείτε λίγο. Πόσο 'cool' θα

είναι η κουζίνα αν μπορούσατε να την στρώσετε με τέτοια πλακάκια! Μπορείτε;



(a)



(b)

Σχήμα 1.1: Cool πλακάκια

Την επόμενη ημέρα που θαυμάζετε τα στρωμένα πλακάκια της κουζίνας, καταφθάνουν τα πλακάκια του μπάνιου. Η φίλη σας απελπίζεται μόλις βλέπει το σχήμα τους (Σχήμα 1.1(b)), αλλά εσείς την πείθετε πως είναι ‘way cool’ αν καταφέρετε να στρώσετε το μπάνιο με τέτοια πλακάκια. Μπορείτε;

Η φίλη σας έχει αρχίσει να αναρωτιέται τι είδους πλακάκια θα της φέρουν για το σαλόνι. Όταν όμως επικοινωνείτε με την εταιρία πλακακιών το μόνο που μαθαίνετε είναι πως τα πλακάκια του σαλονιού είναι και αυτά τετράπλευρα. Είναι ανακούφιση που δεν είναι πεντάπλευρα ή επτάπλευρα, αλλά η φίλη σας αναρωτιέται αν θα είναι δυνατό να καλύψει το σαλόνι με αυτά. Θέλετε να την καθησυχάσετε πως κάθε τετράπλευρο μπορεί να το κάνει αυτό, αλλά είστε σίγουροι; Μπορείτε να της το αποδείξετε;

1.4. Ας δοκιμάσουμε να γράψουμε τους φυσικούς αριθμούς σαν άθροισμα τετραγώνων.

$$\begin{aligned}
 1 &= 1^2 \\
 2 &= 1^2 + 1^2 \\
 3 &= 1^1 + 1^2 + 1^2 \\
 4 &= 2^2 \\
 &\vdots \\
 21 &= 4^2 + 2^2 + 1^2 \\
 &\vdots
 \end{aligned}$$

Πόσα τετράγωνα το πολύ χρειάζονται για κάθε φυσικό αριθμό; Διατύπωσε μια κατάλληλη πρόταση. Η απόδειξή της είναι δύσκολη και πέρα από τα πλαίσια του μαθήματος.

1.5. Οι τριγωνικοί αριθμοί είναι οι $1, 3, 6, 10, 15, \dots$. Ο n -οστός τριγωνικός αριθμός είναι ίσος με το άθροισμα $1 + 2 + \dots + n = n(n + 1)/2$. Μπορείτε να καταλάβετε γιατί τους λένε τριγωνικούς; (Πόσες τελείες έχουν τα παρακάτω τρίγωνα;)



Προβληματίζεστε αν είναι δυνατό να γράψετε κάθε φυσικό αριθμό σαν άθροισμα τριγωνικών αριθμών. Μετά από κάποιες δοκιμές φαίνεται να γίνεται. Αλλά αναρωτιέστε πόσοι τριγωνικοί αριθμοί χρειάζονται για κάθε φυσικό αριθμό. Για παράδειγμα:

$$\begin{aligned} 1 &= 1 \\ 2 &= 1 + 1 \\ 3 &= 3 \\ 4 &= 3 + 1 \\ &\vdots \\ 14 &= 10 + 3 + 1 \\ &\vdots \end{aligned}$$

Δοκιμάστε να γράψετε τους φυσικούς αριθμούς μέχρι το 20 σαν άθροισμα όσο το δυνατό λιγότερων τριγωνικών αριθμών. Τι παρατηρείτε; Γενικεύστε και διατυπώστε μια πρόταση για όλους τους φυσικούς¹. Η απόδειξή της πρότασης είναι δύσκολη, πέρα από τα πλαίσια του μαθήματος.

¹Η πρόταση αυτή σημειώθηκε στο ημερολόγιο του Gauss, του Αρχιμήδη των νεωτέρων χρόνων, με το επιφώνημα 'Εύρηκα'.

2 Αποδείξεις

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 αλλά σε μια δομή που ορίζεται αναδρομικά.

Κατασκευαστική απόδειξη ύπαρξης. Δείχνουμε την ύπαρξη ενός στοιχείου δίνοντας ένα αλγόριθμο που το παράγει.

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.

2.1 Εξαντλητική μέθοδος

Αυτή η μέθοδος εφαρμόζεται όταν έχουμε πεπερασμένο αριθμό περιπτώσεων που κάθε μια μπορεί να ελεγχθεί άμεσα. Η μέθοδος συνίσταται στον έλεγχο όλων των περιπτώσεων. Σήμερα που έχουμε στη διάθεση μας ισχυρούς υπολογιστές, αυτή η μέθοδος μπορεί να χρησιμοποιηθεί σε πολλά προβλήματα. Ας δούμε μερικά παραδείγματα αυτής της μεθόδου.

ΠΑΡΑΔΕΙΓΜΑ 2.1 (Σκύλος-κατσίκια-χορτάρι). Ένας βοσκός έχει ένα 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 κατσίκα και η κατσίκα το χορτάρι αν μείνουν χωρίς το βοσκό στην ίδια όχθη. Υπάρχει τρόπος ο βοσκός να μεταφέρει σώα και ασφαλή και τα τρία απέναντι;

Αυτό είναι ένα πρόβλημα που η ουσία του μπορεί να εκφραστεί με πεπερασμένο αριθμό καταστάσεων. Ας ορίσουμε σαν κατάσταση το σύνολο των 4 στοιχείων ($B =$ βοσκός, $\Sigma =$ σκύλος, $K =$ κατσίκα, $X =$ χορτάρι) που βρίσκεται στην αρχική όχθη. Η αρχική κατάσταση είναι $\{B, \Sigma, K, X\}$ και θέλουμε να φτάσουμε στην τελική κατάσταση $\{\}$. Κάθε κατάσταση είναι ένα υποσύνολο του $\{B, \Sigma, K, X\}$, άρα υπάρχουν το πολύ 16 καταστάσεις (Άσκηση 2.5). Επιπλέον μπορούμε να φτιάξουμε ένα γράφο με κόμβους τις καταστάσεις και ακμές που δηλώνουν μετάβαση από μια κατάσταση σε άλλη. Π. χ. ο γράφος έχει μια ακμή από την αρχική κατάσταση $\{B, \Sigma, K, X\}$ στην κατάσταση $\{\Sigma, X\}$, που δηλώνει ότι ο βοσκός πήρε την κατσίκα και τη μετέφερε στην απέναντι όχθη. Από το γράφο αυτό αφαιρούμε όλες τις καταστάσεις/κόμβους που δεν επιτρέπονται από τους περιορισμούς του προβλήματος. Π. χ. η κατάσταση $\{B, \Sigma\}$ δεν επιτρέπεται γιατί στην απέναντι πλευρά βρίσκεται μόνη της η κατσίκα με το χορτάρι. Το πρόβλημα έχει λύση αν και μόνο αν σε αυτό το γράφο υπάρχει διαδρομή που οδηγεί από την αρχική κατάσταση $\{B, \Sigma, K, X\}$ στην τελική $\{\}$.

Αν και η χρήση του γράφου καταστάσεων είναι μάλλον περιττή για το παραπάνω πρόβλημα—πρόκειται για παλιό δημοφιλή γρίφο που έχει απλή λύση—η μέθοδος αυτή έχει γενικότερη εφαρμογή και αξία. Ο προσεγγιστικός υπολογισμός του μεγέθους των καταστάσεων αποτελεί βασικό συστατικό της μεθόδου· ο αριθμός αυτός μας δηλώνει πότε είναι χρήσιμη μια εξαντλητική προσέγγιση του προβλήματος. Για παράδειγμα, υπολογίσαμε παραπάνω ότι ο αριθμός των πιθανών καταστάσεων είναι το πολύ 16. Φανταστείτε μια γενίκευση του προβλήματος όπου ο βοσκός έχει 100 στοιχεία να μεταφέρει απέναντι και ότι κάποιοι συνδυασμοί αυτών δεν επιτρέπονται. Ο συνολικός αριθμός καταστάσεων ανεβαίνει στο 2^{101} , ένας αριθμός απαγορευτικά μεγάλος που δεν επιτρέπει να δοκιμάσουμε όλες τις περιπτώσεις σήμερα, ακόμα και με τον πιο ισχυρό υπολογιστή.

ΠΑΡΑΔΕΙΓΜΑ 2.2 (Ματ σε 3 κινήσεις). Στην κατηγορία των προβλημάτων που λύνονται με την εξαντλητική μέθοδο ανήκουν τα προβλήματα σκακιού της μορφής ‘ματ σε 3 κινήσεις’. Μπορούμε και σ’ αυτή την περίπτωση να δοκιμάσουμε όλες τις περιπτώσεις που είναι πεπερασμένες σε αριθμό. Είναι όμως εφικτό; Αν υποθέσουμε ότι σε μια τυπική κατάσταση ο κάθε παίκτης μπορεί να κάνει περίπου 40 κινήσεις, οι δυνατές περιπτώσεις για ‘ματ σε 3 κινήσεις’ είναι περίπου 40^5 , ένας αριθμός που είναι μέσα στις δυνατότητες των σημερινών υπολογιστών. Αν όμως το πρόβλημα είναι ‘ματ σε 7 κινήσεις’, ο αριθμός των καταστάσεων είναι περίπου 40^{15} , πέρα από τις σημερινές υπολογιστικές δυνατότητες.

Σ' αυτή την περίπτωση χρειάζεται να επιστρατεύσουμε άλλες τεχνικές που εκμεταλλεύονται τη γνώση μας για το σκάκι και βοηθούν ώστε να ελεγχθούν λιγότεροι συνδυασμοί. Τα σημερινά προγράμματα σκακιού μπορούν χρησιμοποιώντας τέτοιες τεχνικές να λύσουν συνήθως τέτοια προβλήματα.

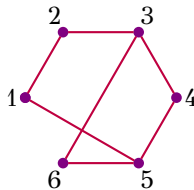
Αλλά θεωρείστε το εξής πρόβλημα σκακιού: μας δίνεται η αρχική σκακιέρα και μας ζητείτε 'ματ σε 137 κινήσεις'. Αυτό είναι πιθανό να έχει λύση και κάποια ημέρα να τη βρούμε, αλλά είναι πολύ πιο πέρα από τις σημερινές υπολογιστικές δυνατότητες. Αν και το πρόβλημα είναι πεπερασμένο, δεν είναι εφικτό—η εξαντλητική μέθοδος δεν δίνει τη λύση.

ΠΑΡΑΔΕΙΓΜΑ 2.3. Σε κάθε ομάδα 6 ατόμων μπορούμε πάντα να βρούμε είτε μια ομάδα 3 ατόμων που γνωρίζονται ανά δυο είτε μια ομάδα 3 αγνώστων μεταξύ τους ατόμων. Ισοδύναμα, μπορούμε να εκφράσουμε το πρόβλημα με την ορολογία των γράφων, αν κάθε άτομο είναι ένας κόμβος και οι ακμές υποδηλώνουν γνωριμία.

Ένα υποσύνολο κόμβων λέγεται *πλήρης υπογράφος* ή *κλίκα* όταν κάθε ζεύγος κόμβων του υποσυνόλου ενώνεται με ακμή. Ένα υποσύνολο κόμβων λέγεται *κενός υπογράφος* ή *ανεξάρτητο σύνολο* όταν κανένα ζεύγος κόμβων του υποσυνόλου δεν ενώνεται με ακμή.

Πρόταση 4. Κάθε γράφος με 6 κόμβους περιέχει ένα πλήρη υπογράφο με 3 κόμβους ή έναν κενό υπογράφο με 3 κόμβους.

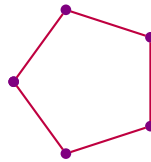
Για παράδειγμα, στο γράφο του Σχήματος 2.1, ο υπογράφος με κόμβους {1, 4, 6} είναι κενός. Αν στο γράφο προσθέσουμε την ακμή [4, 6] που καταστρέφει την ιδιότητα στον υπογράφο {1, 4, 6}, τότε ο υπογράφος {1, 4, 5} γίνεται πλήρης υπογράφος.



Σχήμα 2.1: Ένας γράφος με 6 κόμβους

Για να αποδείξουμε την Πρόταση 4 μπορούμε να ελέγξουμε ένα-προς-ένα όλους τους γράφους 6 κόμβων. Πόσοι γράφοι των 6 κόμβων υπάρχουν; Οι πιθανές ακμές ενός τέτοιου γράφου είναι 15 (Άσκηση 2.6). Κάθε μια από αυτές τις ακμές μπορεί να υπάρχει ή όχι στο γράφο, άρα υπάρχουν 2^{15} γράφοι των 6 κόμβων. Όλοι αυτοί οι γράφοι μπορούν να ελεγχθούν με τη βοήθεια υπολογιστή. Θα δούμε αργότερα, ότι αυτό μπορεί να δείχτεί και με άλλη, εκτός της εξαντλητικής, μέθοδο και πιο συγκεκριμένα με επαγωγή.

Ο αριθμός των κόμβων στην παραπάνω πρόταση δεν μπορεί να μειωθεί από το 6 στο 5. Προσέξτε ότι η πρόταση αναφέρεται σε κάθε γράφο. Άρα αν υπάρχει έστω και ένας γράφος που δεν έχει την ιδιότητα, δηλαδή ένα αντιπαράδειγμα στην πρόταση, τότε η πρόταση δεν ισχύει. Για 5 κόμβους υπάρχει το εξής αντιπαράδειγμα: Ο κύκλος με 5 κόμβους (Σχήμα 2.2) δεν έχει ούτε πλήρη υπογράφο με 3 κόμβους, ούτε κενό υπογράφο με 3 κόμβους.



Σχήμα 2.2: Ο γράφος C_5

Υπάρχουν αντίστοιχες προτάσεις για μεγαλύτερους γράφους:

Πρόταση 5. Κάθε γράφος με 18 κόμβους είτε περιέχει ένα πλήρη υπογράφο με 4 κόμβους είτε ένα κενό υπογράφο με 4 κόμβους.

Πρόταση 6. Κάθε γράφος με 49 κόμβους είτε περιέχει ένα πλήρη υπογράφο με 5 κόμβους είτε ένα κενό υπογράφο με 5 κόμβους.

Πόσους γράφους χρειάζεται να ελέγξουμε για να επιβεβαιώσουμε αυτές τις προτάσεις. Με την ίδια συλλογιστική που χρησιμοποιήσαμε στην Πρόταση 4, ο αριθμός των ακμών ενός γράφου με n κόμβους είναι $\binom{n}{2} = n(n-1)/2$. Υπάρχουν επομένως $2^{n(n-1)/2}$ γράφοι με n κόμβους

Για να δείξουμε την Πρόταση 5 με την εξαντλητική μέθοδο, χρειάζεται να ελέγξουμε $2^{18 \cdot 17/2} = 2^{153}$ γράφους. Αντίστοιχα για την Πρόταση 6 χρειάζεται να ελέγξουμε $2^{49 \cdot 48/2} = 2^{1176}$. Αν και οι προτάσεις αυτές έχουν πεπερασμένο αριθμό περιπτώσεων, δεν μπορούν αν ελεγχθούν εξαντλητικά σήμερα, γιατί ο αριθμός των περιπτώσεων είναι πολύ μεγάλος. Οι προτάσεις έχουν αποδειχθεί, όχι όμως με την εξαντλητική μέθοδο. Η αποδείξεις τέτοιων προτάσεων είναι αρκετά πολύπλοκες. Αυτό υποδηλώνει και το γεγονός ότι δεν γνωρίζουμε αν ο αριθμός 49 στην τελευταία πρόταση είναι ο μικρότερος δυνατός

2.2 Μαθηματική επαγωγή

Η πιο κοινή αποδεικτική μέθοδος είναι η μαθηματική επαγωγή που βασίζεται στην παρακάτω πρόταση.

Πρόταση 7 (Μαθηματική επαγωγή). Έστω $P(n)$ μια λογική πρόταση που αφορά ένα αριθμό n τέτοια ώστε

- η πρόταση ισχύει για $n = 1$ και
- για κάθε φυσικό n , η πρόταση $P(n)$ συνεπάγεται την πρόταση $P(n + 1)$.

Τότε η πρόταση $P(n)$ ισχύει για κάθε φυσικό αριθμό n .

ΠΑΡΑΔΕΙΓΜΑ 2.4. Ας χρησιμοποιήσουμε μαθηματική επαγωγή για να φράξουμε τους αρμονικούς αριθμούς H_k που ορίζονται ως

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

Οι αρμονικοί αριθμοί εμφανίζονται πολλές φορές στην ανάλυση αλγορίθμων και θα ήταν πολύ χρήσιμο να τους εκφράσουμε σε κλειστή μορφή (όχι σαν άθροισμα). Δυστυχώς αυτό είναι ανέφικτο, αλλά για τις εφαρμογές αρκεί συνήθως μια καλή προσέγγιση. Η παρακάτω πρόταση δίνει μια καλή άνω προσέγγιση:

Λήμμα 8. Για κάθε φυσικό n : $H_{2n} \leq 1 + n$.

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 $H_{2^{n+1}} \leq 1 + (n+1)$.

Έχουμε

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

Λαμβάνοντας υπόψη την επαγωγική υπόθεση, για να δείξουμε το λήμμα αρκεί να δείξουμε ότι το άθροισμα μέσα στην παρένθεση είναι το πολύ 1. Αυτό προκύπτει από το γεγονός ότι το άθροισμα μέσα στην παρένθεση έχει 2^n όρους και ο κάθε όρος είναι μικρότερος από $1/2^n$. Έχουμε δηλαδή

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

□

Με παρόμοιο τρόπο μπορούμε να φράξουμε τους αρμονικούς αριθμούς από κάτω: $1 + \frac{n}{2} \leq H_{2^n}$ (Άσκηση 2.8). Αν θέσουμε $k = 2^n$, τότε μπορούμε να ξαναγράψουμε τις προτάσεις ως: $1 + \frac{1}{2} \log k \leq H_k \leq 1 + \log k$ που δείχνουν ότι οι αρμονικός αριθμός είναι της ίδιας τάξης μεγέθους με τον $\log k$.

Θεώρημα 9. Για κάθε φυσικό k : $1 + \frac{1}{2} \log k \leq H_k \leq 1 + \log k$.

Μερικές φορές χρειάζεται η βάση της επαγωγής να είναι κάποιο $n \neq 1$. Αυτό μπορεί να συμβεί για δυο τουλάχιστον λόγους:

- Θέλουμε να δείξουμε ότι μια πρόταση $P(n)$ που αφορά ακέραιους αριθμούς ισχύει για κάθε $n \geq k$, όπου $k \neq 1$ είναι μια σταθερά (για παράδειγμα Άσκηση 2.9).
- Θέλουμε μεν να δείξουμε ότι μια πρόταση $P(n)$ ισχύει για κάθε φυσικό n , αλλά είναι ευκολότερο να δείξουμε το επαγωγικό βήμα

όταν $n \geq k$, όπου $k > 1$ είναι μια σταθερά. Σ' αυτή την περίπτωση αποδεικνύουμε ξεχωριστά τις περιπτώσεις για $n < k$ (για παράδειγμα Άσκηση 2.10).

Σε πολλές περιπτώσεις χρειαζόμαστε πιο ισχυρή επαγωγική υπόθεση: υποθέτουμε ότι η πρόταση ισχύει για $1, 2, \dots, n$ και δείχνουμε ότι ισχύει για $n + 1$.

Οι παραπάνω παραλλαγές της μαθηματικής επαγωγής είναι περιπτώσεις της ισχυρής μαθηματικής επαγωγής (που αποδεικνύεται στην Άσκηση 2.11).

Θεώρημα 10 (Ισχυρή μαθηματική επαγωγή). Έστω ότι μια πρόταση $P(n)$

- είναι αληθής για κάποιο ακέραιο $n = n_0$ και
- οι προτάσεις $P(n_0), P(n_0+1), \dots, P(n)$ συνεπάγονται την πρόταση $P(n+1)$, για κάθε ακέραιο αριθμό $n \geq n_0$.

Τότε η πρόταση $P(n)$ ισχύει για κάθε ακέραιο αριθμό $n \geq n_0$.

ΠΑΡΑΔΕΙΓΜΑ 2.5. 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 11. Να δείχτεί ότι για κάθε ακέραιο $n \geq 0$,

$$F_n \leq \varphi^n,$$

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

Απόδειξη. Θα χρησιμοποιήσουμε ισχυρή επαγωγή με βάση της επαγωγής το 0. *Βάση της επαγωγής:* Για $n = 0$ και $n = 1$ το λήμμα ισχύει γιατί $F_0 = 1 \leq \varphi^0$ και $F_1 = 1 \leq \varphi^1$.

Επαγωγική υπόθεση: Υποθέτουμε ότι το λήμμα ισχύει για κάθε φυσικό αριθμό $k \leq n$ και ειδικότερα για $n - 1$ και για n .

Επαγωγικό βήμα: Θα δείξουμε ότι ισχύει για $n + 1$: $F_{n+1} \leq \varphi^{n+1}$. Από τον ορισμό των αριθμών Fibonacci, έχουμε

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &\leq \varphi^{n-1} + \varphi^n \\ &= \varphi^{n-1}(1 + \varphi) \\ &= \varphi^{n-1}\varphi^2 \\ &= \varphi^{n+1}. \end{aligned} \quad \square$$

Με παρόμοιο τρόπο μπορούμε να φράξουμε το ρυθμό αύξησης των αριθμών Fibonacci από κάτω. Για παράδειγμα μπορούμε να δείξουμε $\frac{1}{2}\varphi^n \leq F_n$ (Άσκηση 2.12). Προκύπτει λοιπόν ότι ο αριθμός Fibonacci F_n είναι της ίδιας τάξης μεγέθους με το φ^n .

Θεώρημα 12. Για κάθε θετικό ακέραιο n : $\frac{1}{2}\varphi^n \leq F_n \leq \varphi^n$.

ΠΑΡΑΔΕΙΓΜΑ 2.6. Ναδειχτεί ότι για κάθε ακέραιους $n, m \geq 0$, οι αριθμοί Fibonacci ικανοποιούν την

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

Απόδειξη. Και πάλι θα χρησιμοποιήσουμε ισχυρή επαγωγή. Παρατηρήστε αρχικά ότι έχουμε δύο μεταβλητές. Θα χρησιμοποιήσουμε επαγωγή μόνο στο n και το m θα το θεωρούμε σταθερό. Θα δείξουμε ότι για κάθε $n \in \mathbb{N}$ ισχύει:

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

Επαγωγική βάση: Για $n = 1$ η πρόταση $F_{1+m} = F_1 F_m + F_0 F_{m-1} = F_m + F_{m-1}$ ισχύει για κάθε m από τον ορισμό των αριθμών Fibonacci.

Επαγωγικό βήμα: Θεωρούμε ότι η πρόταση που θέλουμε να αποδείξουμε ισχύει για κάθε $k \leq n$. Θα δείξουμε ότι η πρόταση είναι αληθής για $n + 1$ δηλαδή ότι $F_{(n+1)+m} = F_{n+1} F_m + F_n F_{m-1}$. Πράγματι λοιπόν:

$$\begin{aligned} F_{(n+1)+m} &= F_{n+m} + F_{(n-1)+m} \\ &= (F_n F_m + F_{n-1} F_{m-1}) + (F_{n-1} F_m + F_{n-2} F_{m-1}) \\ &= (F_n F_m + F_{n-1} F_m) + (F_{n-1} F_{m-1} + F_{n-2} F_{m-1}) \\ &= (F_n + F_{n-1}) F_m + (F_{n-1} + F_{n-2}) F_{m-1} \\ &= F_{n+1} F_m + F_n F_{m-1}. \end{aligned} \quad \square$$

Η παραπάνω πρόταση μπορεί να χρησιμοποιηθεί για τον υπολογισμό του F_n χωρίς να χρειάζεται να υπολογίσουμε όλους τους ενδιάμεσους

Αλγόριθμος 2.1: Αλγόριθμος του Ευκλείδη

```

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

```

αριθμούς Fibonacci. Πιο συγκεκριμένα, για να υπολογίσουμε τον F_{2k+1} και F_{2k} χρειάζεται να ξέρουμε μόνο τους F_k και F_{k-1} :

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

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

Για παράδειγμα, μπορούμε να υπολογίσουμε τον F_{31} ως εξής:

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

$$F_{15} = F_7^2 + 2F_7F_6$$

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

$$F_7 = F_3^2 + 2F_3F_2$$

$$F_6 = F_3^2 + F_2^2$$

$$F_3 = \dots$$

$$F_2 = \dots$$

ΠΑΡΑΔΕΙΓΜΑ 2.7. Ο μέγιστος κοινός διαιρέτης $\gcd(a, b)$ δυο μη αρνητικών ακεραίων ορίζεται σαν ο μέγιστος ακέραιος που διαιρεί τους a και b . Ο μέγιστος κοινός διαιρέτης μπορεί να βρεθεί με τον αλγόριθμο του Ευκλείδη (Αλγόριθμος 2.1), έναν από τους αρχαιότερους αλγόριθμους. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a \geq b$. Ο αλγόριθμος του Ευκλείδη βασίζεται στο

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

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

Απόδειξη. Με επαγωγή στο a .

Βάση της επαγωγής: Για $a = 2$ και $b = 1, 2$, είναι εύκολο να ελέγξουμε εξαντλητικά ότι ο αλγόριθμος κάνει ακριβώς μια διαίρεση και η πρόταση ισχύει.

Επαγωγικό βήμα: Όταν καλούμε τον αλγόριθμο με a, b , στο επόμενο βήμα γίνονται $b, a \bmod b$. Η επαγωγή θα εφαρμοζόταν εύκολα αν η νέα τιμή της πρώτης παραμέτρου, δηλαδή το b , ήταν ας πούμε το πολύ το μισό του a . Δυστυχώς, όμως αυτό δεν συμβαίνει όταν το b είναι περίπου ίσο με το a . Ευτυχώς όμως σ' αυτή την περίπτωση στη δεύτερη επανάληψη η πρώτη παράμετρος γίνεται ίση με $a \bmod b$.

Η βασική ιδέα λοιπόν της απόδειξης είναι ότι σε δυο επαναλήψεις η τιμή του a μειώνεται κάτω από το μισό της αρχικής τιμής. Πιο συγκεκριμένα, για κάθε $a \geq b$, $a \bmod b < a/2$. Για να το δείξουμε αυτό, διακρίνουμε δυο περιπτώσεις. Αν $b \leq a/2$, τότε $a \bmod b < b \leq a/2$. Αν πάλι $b > a/2$, τότε $a \bmod b = a - b < a/2$.

Ο αριθμός των διαιρέσεων του αλγόριθμου του Ευκλείδη με πρώτη παράμετρο το a είναι 2 συν τον αριθμό των διαιρέσεων όταν η πρώτη παράμετρος είναι $a \bmod b$, το οποίο είναι το πολύ $a/2$. Από την επαγωγική υπόθεση, ο συνολικός αριθμός διαιρέσεων είναι το πολύ $2 + 2 \log(a/2) = 2 + 2(\log a - 1) = 2 \log a$. \square

ΠΑΡΑΔΕΙΓΜΑ 2.8 (Ισχυροποίηση της επαγωγικής υπόθεσης). Μια χρήσιμη τεχνική για να αποδείξουμε μια πρόταση με μαθηματική επαγωγή είναι να ισχυροποιήσουμε την επαγωγική υπόθεση. Για παράδειγμα, θεωρήστε την παρακάτω πρόταση.

Πρόταση 14. Για κάθε φυσικό αριθμό n : $1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2$.

Απόδειξη. Ας προσπαθήσουμε να χρησιμοποιήσουμε επαγωγή για να δείξουμε την πρόταση. Υποθέτουμε ότι η πρόταση ισχύει για 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 λοιπόν

αποτυγχάνει. Τι μπορούμε να κάνουμε; Θα δείξουμε μια ισχυρότερη πρόταση. Πιο συγκεκριμένα θα δείξουμε ότι $1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$. Πράγματι έχουμε

Βάση της επαγωγής: Για $n = 1$, $1 \leq 2 - 1/1$ και η πρόταση ισχύει.

Επαγωγικό βήμα: Έστω ότι η πρόταση ισχύει για κάποιο φυσικό n , δηλαδή $1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$. Προσθέτουμε και στα δύο μέλη το $\frac{1}{(n+1)^2}$. Έτσι έχουμε

$$\begin{aligned} 1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(n+1)^2} &\leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\ &\leq 2 - \frac{1}{n+1} \end{aligned}$$

που δείχνει ότι η πρόταση ισχύει και για $n + 1$. □

Ας δούμε άλλο ένα παράδειγμα όπου η ισχυροποίηση της επαγωγικής υπόθεσης βοηθάει.

ΠΑΡΑΔΕΙΓΜΑ 2.9 (Ramsey theory). Έχουμε ήδη αναφερθεί στο τμήμα των εξαντλητικών αποδείξεων στο θεώρημα ότι κάθε γράφος 6 κόμβων περιέχει είτε ένα πλήρη υπογράφο 3 κόμβων είτε ένα κενό υπογράφο 3 κόμβων. Το θεώρημα αυτό δείχνει ότι ακόμα και σε τυχαίους γράφους υπάρχουν ψήγματα κάποια τάξης ή κανονικότητας. Τα θεωρήματα αυτού του είδους ονομάζονται θεωρήματα Ramsey. Το πιο βασικό θεώρημα Ramsey, είναι η γενίκευση της παραπάνω πρότασης που λέει ότι κάθε γράφος με R_k κόμβους περιέχει είτε ένα πλήρη υπογράφο με k κόμβους είτε ένα κενό υπογράφο με k κόμβους, όπου R_k είναι κάποιος ακέραιος που εξαρτάται από το k . Π. χ. $R_2 = 2$, $R_3 = 6$ και $R_4 = 18$. Δεν γνωρίζουμε ποια είναι ακριβώς τα R_k για $k \geq 5$, αλλά αυτό δεν μας εμποδίζει να αποδείξουμε το θεώρημα:

Θεώρημα 15 (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 χρησιμοποιήσουμε τη μέθοδο της επαγωγής για τη πρόταση αυτή θα διαπιστώσουμε ότι δεν γίνεται. Ο λόγος είναι ότι η πρόταση $P(k)$ δεν συνεπάγεται την πρόταση $P(k + 1)$. Το κόλπο είναι να κάνουμε κάτι που αρχικά φαίνεται οξύμωρο: θα αποδείξουμε μια ισχυρότερη πρόταση. Αν το σκεφτούμε όμως λίγο παύει να είναι οξύμωρο γιατί μια ισχυρότερη επαγωγική υπόθεση $P'(k)$ μπορεί να συνεπάγεται την $P(k + 1)$. Θα δείξουμε λοιπόν την παρακάτω γενικότερη πρόταση.

Θεώρημα 16 (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.

Απόδειξη. Ας δούμε πρώτα πώς μπορούμε να αποδείξουμε την πρόταση για $k = m = 3$, που είναι ίδια με την Πρόταση 4, και μετά θα γενικεύσουμε τη βασική ιδέα για οποιαδήποτε k και m .

Όπως ήδη έχουμε αναφέρει $R_{3,3} = 6$. Ας πάρουμε λοιπόν ένα οποιοδήποτε γράφο με 6 κόμβους και ας θεωρήσουμε ένα κόμβο v . Αν ο v έχει τουλάχιστον 3 ακμές, δηλαδή έχει τουλάχιστον 3 γειτονικούς κόμβους, τότε διακρίνουμε δύο περιπτώσεις:

- Αν δυο από τους γείτονες του v ενώνονται με ακμή, τότε μαζί με τον v κάνουν ένα πλήρη υπογράφο 3 κόμβων.
- Αλλιώς οι γείτονες του v σχηματίζουν ένα κενό υπογράφο μεγέθους (τουλάχιστον) 3.

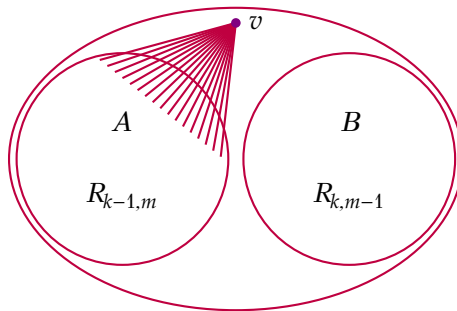
Με πολύ παρόμοιο τρόπο εργαζόμαστε και όταν ο v έχει λιγότερους από 3 γειτονικούς κόμβους. Σ' αυτή την περίπτωση, θεωρούμε τους μη γειτονικούς κόμβους του v . Αν υπάρχουν δυο που δεν ενώνονται, τότε με τον v σχηματίζουν ένα κενό υπογράφο 3 κόμβων, αλλιώς οι μη γειτονικοί κόμβοι του v σχηματίζουν ένα πλήρη υπογράφο με (τουλάχιστον) 3 κόμβους.

Η παραπάνω συλλογιστική επεκτείνεται και στη γενική περίπτωση, την οποία θα αποδείξουμε με επαγωγή στο $k + m$.

Βάση της επαγωγής: Για $k + m = 2$, οι μόνοι θετικοί ακέραιοι που έχουν αυτή την ιδιότητα είναι $k = m = 1$. Ο γράφος με ένα μόνο κόμβο είναι πλήρης (και κενός) γράφος. Άρα η πρόταση ισχύει για $R_{1,1} = 1$.

Επαγωγικό βήμα: Η επαγωγική υπόθεση είναι (α) ότι κάθε γράφος με τουλάχιστον $R_{k-1,m}$ κόμβους περιέχει είτε ένα πλήρη υπογράφο με $k - 1$ κόμβους είτε ένα κενό υπογράφο με m κόμβους, και (β) ότι κάθε γράφος με τουλάχιστον $R_{k,m-1}$ κόμβους περιέχει είτε ένα πλήρη υπογράφο με k κόμβους είτε ένα κενό υπογράφο με $m - 1$ κόμβους.

Για να δείξουμε την πρόταση για κάποια k και m , ας πάρουμε τώρα ένα γράφο με μεγάλο πλήθος κόμβων (που θα τον καθορίσουμε αργότερα). Ας θεωρήσουμε ένα κόμβο v αυτού του γράφου. Οι υπόλοιποι κόμβοι του γράφου χωρίζονται σε δυο σύνολα: το σύνολο A των γειτόνων του v και το σύνολο B των μη γειτόνων (Σχήμα 2.3). Επειδή ο v είναι γείτονας με όλους τους κόμβους του A , σε κάθε πλήρη γράφο A μπορούμε να προσθέσουμε τον v και να έχουμε ένα πλήρη γράφο με ένα περισσότερο κόμβο. Παρόμοια, σε κάθε κενό υπογράφο του B μπορούμε να προσθέσουμε τον κόμβο v .



Σχήμα 2.3: Επαγωγική απόδειξη του Θεωρήματος Ramsey

Αν το σύνολο A των γειτόνων έχει τουλάχιστον $R_{k-1,m}$ κόμβους, τότε, από την επαγωγική υπόθεση, περιέχει είτε ένα πλήρη υπογράφο με $k-1$ κόμβους είτε ένα κενό υπογράφο με m κόμβους. Αν προσθέσουμε τον v , τότε το μέγεθος του πλήρη υπογράφου αυξάνεται κατά ένα. Άρα αν το σύνολο A των γειτόνων έχει τουλάχιστον $R_{k-1,m}$ κόμβους, η πρόταση ισχύει.

Παρόμοια, αν το σύνολο B των μη γειτόνων έχει τουλάχιστον $R_{k,m-1}$ κόμβους, η πρόταση ισχύει. Αν λοιπόν ο γράφος έχει τουλάχιστον $1 + R_{k-1,m} + R_{k,m-1}$, τότε είτε το σύνολο A των γειτόνων έχει τουλάχιστον $R_{k-1,m}$ κόμβους, είτε το σύνολο B των μη γειτόνων έχει τουλάχιστον $R_{k,m-1}$ κόμβους. Άρα η πρόταση ισχύει πάντα. \square

Μπορούμε να εκτιμήσουμε ένα πάνω φράγμα στον αριθμό $R_{k,m}$ από την αναδρομική σχέση $R_{k,m} \leq 1 + R_{k-1,m} + R_{k,m-1}$, όπως προκύπτει από την παραπάνω απόδειξη. Από αυτή τη σχέση και με επαγωγή μπορούμε να δείξουμε ότι $R_{k,m} \leq 2^{k+m-1} - 1$ (Άσκηση 2.18). Για παράδειγμα, για το $R_{5,5}$ έχουμε $R_{5,5} \leq 2^9 - 1 = 511$. Για αυτή την περίπτωση, γνωρίζουμε από άλλες μεθόδους το καλύτερο φράγμα $R_{5,5} \leq 49$, όπως είδαμε παραπάνω στην Πρόταση 6.

Ασκήσεις

2.1. Έχουμε τρία δοχεία με χωρητικότητα 10, 7 και 3 λίτρα. Το δοχείο των 10 λίτρων είναι γεμάτο νερό και τα άλλα δοχεία είναι άδεια. Θέλουμε να μοιράσουμε το νερό σε δυο (ακριβώς) ισόποσα μέρη. Πως μπορούμε να το πετύχουμε; Περιγράψτε τις καταστάσεις του συστήματος και χρησιμοποιείστε την εξαντλητική μέθοδο για να λύσετε το πρόβλημα. Πόσες καταστάσεις έχει το σύστημα; Δώστε ένα χαλαρό πάνω φράγμα.

2.2. Έχουμε 5 μπάλες και μια παλάντζα (μια ζυγαριά χωρίς διαβαθμίσεις που συγκρίνει δυο ποσότητες, αλλά δεν δείχνει ποιο είναι το

βάρος τους). Ξέρουμε ότι μια από τις μπάλες έχει διαφορετικό βάρος από τις υπόλοιπες και θέλουμε να βρούμε ποια είναι. Πόσες ζυγίσσεις χρειάζονται για να το πετύχουμε;

2.3. Δώστε ένα παράδειγμα γράφου με 11 κόμβους που δεν περιέχει ούτε πλήρη ούτε κενό υπογράφο με 4 κόμβους.

2.4. Δώστε ένα παράδειγμα γράφου με 12 κόμβους που δεν περιέχει ούτε πλήρη ούτε κενό υπογράφο με 4 κόμβους.

2.5. Δείξτε με επαγωγή ότι ο αριθμός των υποσυνόλων ενός συνόλου, συμπεριλαμβανομένου του κενού συνόλου και του εαυτού του, με n στοιχεία είναι 2^n .

2.6. Δείξτε με επαγωγή ότι ο αριθμός των ακμών ενός μη κατευθυνόμενου πλήρους γράφου με n κόμβους είναι $n(n-1)/2$.

2.7. Δείξτε με επαγωγή ότι αν p είναι πρώτος αριθμός τότε για κάθε φυσικό αριθμό x : $x^p = x \pmod{p}$.

2.8. Δείξτε ότι για κάθε φυσικό n : $1 + \frac{n}{2} \leq H_{2^n}$.

2.9. Δείξτε ότι για κάθε φυσικό $n \geq 4$: $2^n \geq n^2$.

2.10. Δείξτε ότι για κάθε φυσικό n : $\sum_{i=1}^n \frac{5}{2^i-1} \leq n + \frac{14}{3}$.

2.11. Αποδείξτε το Θεώρημα 10 χρησιμοποιώντας μόνο την Πρόταση 7. Βοήθεια: Για να αλλάξουμε τη βάση της επαγωγής από 1 σε n_0 , θεωρούμε την πρόταση $Q(n) = P(n-1+n_0)$.

2.12. Να δειχτεί ότι για κάθε φυσικό αριθμό n ,

$$F_n \geq \varphi^n / 2,$$

όπου $\varphi = 1.618\dots$ είναι η χρυσή τομή.

2.13. Δείξτε χρησιμοποιώντας Μαθηματική Επαγωγή ότι για κάθε μη αρνητικό ακέραιο n ισχύει:

$$\frac{8}{1 \cdot 3} + \frac{8}{5 \cdot 7} + \dots + \frac{8}{(4n+1) \cdot (4n+3)} \leq 4$$

Που φαίνεται να συγκλίνει αυτό το άθροισμα;

2.14. Θέλουμε να δείξουμε πως το παρακάτω γινόμενο συγκλίνει σε κάποιο θετικό αριθμό και όχι στο 0. Για παράδειγμα σε κάποιο αριθμό μεγαλύτερο του 0.25.

$$Q = \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{2^3}\right) \dots$$

Ένας τρόπος είναι να δείξουμε χρησιμοποιώντας Μαθηματική Επαγωγή ότι για κάθε ακέραιο $n \geq 1$ ισχύει:

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2^2}\right) \dots \left(1 - \frac{1}{2^n}\right) \geq \frac{1}{4} \left(1 + \frac{1}{2^{n-1}}\right),$$

από το οποίο προκύπτει πως $Q \geq 1/4$. Αποδείξτε το.

Μπορείτε να βρείτε και να αποδείξετε ένα καλύτερο (μεγαλύτερο) φράγμα; Υπόδειξη: Με ελάχιστες αλλαγές στην απόδειξή σας μπορείτε να δείξετε την γενικότερη πρόταση: Για κάθε k και $n > k$:

$$\left(1 - \frac{1}{2^{k+1}}\right)\left(1 - \frac{1}{2^{k+2}}\right) \cdots \left(1 - \frac{1}{2^n}\right) \geq \left(1 - \frac{1}{2^k}\right)\left(1 + \frac{1}{2^{n-1}}\right).$$

Χρησιμοποιώντας αυτή την πρόταση, το αρχικό γινόμενο φράσσεται από

$$Q \geq \left[\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2^2}\right) \cdots \left(1 - \frac{1}{2^k}\right)\right]\left(1 - \frac{1}{2^k}\right)$$

για κάθε k . Ειδικά για $k = 2$, το γινόμενο είναι τουλάχιστον $9/32$.

2.15. Αποδείξτε προσεκτικά πως σε κάθε αύξουσα ακολουθία a_1, a_2, \dots, a_n με $a_i \in \{1, 2, \dots, n\}$, υπάρχει κάποιο k τέτοιο ώστε $a_k = k$.

Για παράδειγμα, στην ακολουθία 2, 3, 3, 5, 6, 6, 6, έχουμε $a_3 = 3$ (επίσης $a_6 = 6$).

2.16. Οι κινήσεις του Ίππου στο σκάκι έχουν σχήμα Γ (από τη θέση (x, y) μπορεί να πάει στις θέσεις $(x \pm 2, y \pm 1)$ και $(x \pm 1, y \pm 2)$). Ας θεωρήσουμε μια άπειρη σκακιέρα (που επεκτείνεται μέχρι το άπειρο προς τα δεξιά και πάνω) και ας υποθέσουμε ότι αρχικά ο Ίππος είναι στο κάτω αριστερό άκρο της $(1, 1)$.

Δείξτε με επαγωγή ότι για κάθε θέση (x, y) , με $x, y \in \mathbb{N}$, υπάρχει διαδρομή που ξεκινά από την αρχική θέση και καταλήγει στη θέση (x, y) .

Για ποια n μπορεί να γίνει το ίδιο όταν η σκακιέρα είναι πεπερασμένη και έχει διαστάσεις $n \times n$; Για παράδειγμα, αν $n = 2$ δεν μπορεί να γίνει γιατί ο Ίππος δεν μπορεί καν να κινηθεί από την αρχική θέση και επομένως δεν μπορεί να επισκεφτεί τη θέση $(1, 2)$.

2.17. Δείξτε ότι

1. $R_{k,m} = R_{m,k}$

2. $R_{1,m} = 1$

3. $R_{2,m} = m$

2.18. Δείξτε ότι αν $R_{1,m} = R_{k,1} = 1$ και $R_{k,m} \leq 1 + R_{k-1,m} + R_{k,m-1}$, για κάθε θετικό ακέραιο k και m , τότε $R_{k,m} \leq 2^{k+m-1} - 1$.

2.19. Τριγωνοποίηση πολυγώνου καλείται κάθε υποδιαίρεση του εσωτερικού του σε τρίγωνα που ορίζονται από ευθύγραμμα τμήματα μεταξύ των κορυφών του, τα οποία δεν τέμνονται μεταξύ τους. Αποδείξτε πως για πολυγώνο με $n \geq 3$ κορυφές, κάθε τριγωνοποίησή του περιέχει $n - 2$ τρίγωνα.

3 Αναδρομή και Επαγωγή

Η ιδέα της μαθηματικής επαγωγής μπορεί να επεκταθεί και σε άλλες δομές εκτός από το σύνολο των φυσικών \mathbb{N} . Μπορούμε να μιμηθούμε τον επαγωγικό ορισμό του συνόλου των φυσικών για να ορίσουμε αναδρομικά νέες δομές στις οποίες μπορούμε να κάνουμε επαγωγή. Πριν αναφερθούμε σε λεπτομέρειες ας δούμε ένα παράδειγμα.

ΠΑΡΑΔΕΙΓΜΑ 3.1. Ας ορίσουμε ένα σύνολο S επαγωγικά ως εξής:

Βάση του ορισμού: $3 \in S$

Επαγωγικός ορισμός: Αν $x, y \in S$ τότε και $x + y \in S$

Όπως φαίνεται αρχικά το σύνολο S περιέχει μόνο ένα στοιχείο, το 3. Στο πρώτο βήμα της επαγωγής το σύνολο S έχει επιπλέον το στοιχείο 6. Στο επόμενο επαγωγικό βήμα το σύνολο S έχει επιπλέον τα στοιχεία 9, 12 κ.ο.κ.

Με τη βοήθεια του επαγωγικού ορισμού του συνόλου S μπορούμε να αποδείξουμε ότι περιέχει ακριβώς όλα τα πολλαπλάσια του 3. Έχουμε εδώ δυο σύνολα. Το σύνολο S που ορίζεται επαγωγικά και το σύνολο A των πολλαπλασίων του 3, που ορίζεται περιγραφικά:

$$A = \{3n : n \in \mathbb{N}\}.$$

Θέλουμε να δείξουμε ότι τα δυο σύνολα είναι ίσα, $A = S$. Έτσι πρέπει να δείξουμε δυο προτάσεις.

- $A \subseteq S$, δηλαδή ότι κάθε θετικό πολλαπλάσιο του 3 ανήκει στο S . Θα το κάνουμε με μαθηματική επαγωγή. Πιο συγκεκριμένα θα δείξουμε με μαθηματική επαγωγή ότι για κάθε ακέραιο n : $3n \in S$.
- $S \subseteq A$, δηλαδή ότι κάθε αριθμός που παράγεται με τους παραπάνω κανόνες, είναι πολλαπλάσιο του 3. Θα το κάνουμε με δομική επαγωγή. Στην δομική επαγωγή, δείχνουμε ότι κάθε στοιχείο μια δομής που ορίζεται αναδρομικά έχει κάποια συγκεκριμένη ιδιότητα: στην προκειμένη περίπτωση ότι διαιρείται με το 3.

Απόδειξη του $A \subseteq S$. Θα δείξουμε με μαθηματική επαγωγή ότι για κάθε n ισχύει ότι $3n \in S$.

Βάση της επαγωγής: Επιβεβαιώνουμε ότι $3 \in S$ από τη βάση του ορισμού του συνόλου S .

Επαγωγικό βήμα: Έστω ότι $3n \in S$. Θα δείξουμε ότι $3(n+1) \in S$. Παρατηρούμε ότι $3 \in S$, και $3n \in S$. Από τον επαγωγικό ορισμό του συνόλου S αν δύο στοιχεία ανήκουν σε αυτό, την ίδια ιδιότητα έχει και το άθροισμά τους, δηλαδή $3+3n \in S$ κάτι που ολοκληρώνει την επαγωγή.

Απόδειξη του $S \subseteq A$. Για να αποδείξουμε το δεύτερο εγκλεισμό $S \subseteq A$ πρέπει να εκμεταλλευτούμε τον επαγωγικό ορισμό του S . Θα δείξουμε ότι όλα τα στοιχεία του λοιπόν ότι S είναι πολλαπλάσια του 3. Ποιο συγκεκριμένα, θα δείξουμε ότι και οι δύο κανόνες που παράγουν στοιχεία του S παράγουν πολλαπλάσια του 3.

Βάση δομικής επαγωγής: Η βάση του ορισμού παράγει μόνο ένα στοιχείο, το 3, που είναι πολλαπλάσιο του 3.

Επαγωγικό βήμα: Σε κάποιο στάδιο της κατασκευής του συνόλου S υποθέτουμε ότι αυτό περιέχει πολλαπλάσια του 3. Θα δείξουμε ότι στο επόμενο βήμα όπου νέα στοιχεία εισάγονται στο σύνολο S έχουν την ίδια ιδιότητα. Αν λοιπόν $x, y \in S$ με x, y πολλαπλάσια του 3, αρκεί να δείξουμε ότι και το νέο στοιχείο του S , $x+y$ είναι επίσης πολλαπλάσιο του 3. Πράγματι από την ιδιότητα των x, y έχουμε ότι για κάποιους ακεραίους k_1, k_2 , $x = 3k_1, y = 3k_2$ και άρα $x+y = 3(k_1+k_2)$, που ολοκληρώνει τη δομική επαγωγή.

Το παραπάνω είναι ένα χαρακτηριστικό παράδειγμα αναδρομικού ορισμού και της δομικής επαγωγής. Η ιδέα λοιπόν του επαγωγικού ορισμού εννοιών είναι πολύ βασική και χρησιμοποιείται ευρύτατα στην Πληροφορική για τη δημιουργία και μελέτη νέων δομών. Το πιο χαρακτηριστικό παράδειγμα αποτελεί η θεωρία των δομών δεδομένων. Για να αποδεικνύουμε προτάσεις για δομές που ορίζονται αναδρομικά χρησιμοποιούμε τη δομική επαγωγή.

Ορισμός 17 (Δομική επαγωγή). Έστω σύνολο ή δομή Δ που ορίζεται επαγωγικά. Για να αποδείξουμε μια ιδιότητα P για κάθε στοιχείο του συνόλου Δ αρκεί να ακολουθήσουμε τα επόμενα βήματα:

- *Βάση της επαγωγής:* Αποδεικνύουμε ότι τα στοιχεία του συνόλου Δ που ορίζονται στο βήμα Βάση του ορισμού του έχουν την ιδιότητα.
- *Επαγωγικό βήμα:* Θεωρούμε ότι σε κάποιο βήμα της κατασκευής του Δ , τα στοιχεία του έχουν την ιδιότητα. Αποδεικνύουμε ότι αν τα στοιχεία του Δ έχουν την ιδιότητα P , τότε και τα νέα στοιχεία που ορίζονται στο επαγωγικό βήμα του ορισμού του Δ έχουν την ιδιότητα.

Με τη δομική επαγωγή είμαστε έτοιμοι να ορίσουμε και να μελετήσουμε δομές που ορίζονται με αναδρομικό τρόπο. Θα ασχοληθούμε

με το σύνολο των συμβολοσειρών, το σύνολο των δένδρων με ρίζα, τα δυαδικά δένδρα και τα πλήρη δυαδικά δένδρα. Κάθε μια από αυτές τις δομές θα την ορίσουμε επαγωγικά και θα αποδείξουμε προτάσεις με τη βοήθεια της δομικής επαγωγής.

ΠΑΡΑΔΕΙΓΜΑ 3.2 (Συμβολοσειρές ενός αλφαβήτου). Έστω Σ ένα πεπερασμένο σύνολο που θα το ονομάζουμε αλφάβητο. Παραδείγματα αλφαβήτου είναι το $\{a, b, \dots, \omega\}$ και το $\{0, 1, \dots\}$. Οι συμβολοσειρές ενός αλφαβήτου Σ είναι οι πεπερασμένες ακολουθίες που παράγονται με τα στοιχεία του αλφαβήτου. Για παράδειγμα, η ακολουθία $(\epsilon, v, \rho, \eta, \kappa, a)$ είναι συμβολοσειρά του αλφαβήτου $\{a, b, \dots, \omega\}$. Για απλότητα, στις συμβολοσειρές παραλείπουμε τα κόμματα και τις παρενθέσεις: έτσι για παράδειγμα γράφουμε *ευρηκα* αντί για $(\epsilon, v, \rho, \eta, \kappa, a)$. Επίσης, χρησιμοποιούμε το σύμβολο ϵ για να συμβολίσουμε την κενή συμβολοσειρά, που αντιστοιχεί στην ακολουθία $()$ χωρίς κανένα στοιχείο. Μερικοί συγγραφείς χρησιμοποιούν το σύμβολισμό λ για την κενή συμβολοσειρά.

Το σύνολο των συμβολοσειρών ενός αλφαβήτου Σ , που το συμβολίζουμε με Σ^* , μπορεί να οριστεί αναδρομικά ως εξής:

Ορισμός 18 (Σύνολο συμβολοσειρών Σ^* αλφάβητου Σ).

Βάση του ορισμού: Η κενή συμβολοσειρά ϵ ανήκει στο Σ^* , $\epsilon \in \Sigma^*$.

Επαγωγικός ορισμός: Αν $w \in \Sigma^*$ και $\sigma \in \Sigma$ τότε $w\sigma \in \Sigma^*$.

Για παράδειγμα ας πάρουμε το αλφάβητο που περιέχει τα σύμβολα 0 και 1, $\Sigma = \{0, 1\}$. Σύμφωνα με τη βάση του ορισμού, οι συμβολοσειρές του Σ περιέχουν την κενή υπακολουθία. Μετά την πρώτη εφαρμογή του επαγωγικού βήματος, στις συμβολοσειρές περιλαμβάνονται οι συμβολοσειρές 0, και 1. Μετά το δεύτερο βήμα εφαρμογής του επαγωγικού βήματος παίρνουμε επιπλέον τις συμβολοσειρές 00, 01, 10, 11 κ.ο.κ. Το σύνολο επομένως που παράγεται είναι το $\{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \dots\}$.

ΠΑΡΑΔΕΙΓΜΑ 3.3 (Μήκος και παράθεση συμβολοσειρών). Χρησιμοποιώντας τον παραπάνω επαγωγικό ορισμό των συμβολοσειρών μπορούμε να ορίσουμε με αυστηρό τρόπο το μήκος μιας συμβολοσειράς, ή πράξεις πάνω στις συμβολοσειρές, π. χ. την παράθεση (concatenation) συμβολοσειρών, καθώς και να αποδείξουμε ιδιότητες για αυτές.

Ορισμός 19 (Μήκος ' συμβολοσειράς).

Βάση του ορισμού: Ορίζουμε $'(\epsilon) = 0$.

Επαγωγικός ορισμός: Αν $w \in \Sigma^*$ και $\sigma \in \Sigma$ ορίζουμε $'(w\sigma) = '(w) + 1$.

Ορισμός 20 (Παράθεση δύο συμβολοσειρών).

Βάση του ορισμού: Αν $w \in \Sigma^*$ ορίζουμε $w \cdot \epsilon = w$

Επαγωγικός ορισμός: Αν $w_1, w_2 \in \Sigma^*$ και $\sigma \in \Sigma$ ορίζουμε $w_1 \cdot (w_2\sigma) = (w_1 \cdot w_2)\sigma$

Για παράδειγμα η παράθεση των συμβολοσειρών 011 και 00 είναι 01100.

Είμαστε τώρα έτοιμοι να αποδείξουμε την πρώτη πρόταση που αφορά τις συμβολοσειρές. Η πρόταση είναι προφανώς αληθής και ο μόνος λόγος που την δίνουμε εδώ είναι για να δείξουμε πώς χρησιμοποιούμε τους επαγωγικούς ορισμούς για να αποδείξουμε προτάσεις για επαγωγικές δομές.

Πρόταση 21. Για κάθε συμβολοσειρές $x, y \in \Sigma^*$ ισχύει ότι $\epsilon'(x \cdot y) = \epsilon'(x) + \epsilon'(y)$.

Απόδειξη. Η απόδειξη θα γίνει με δομική επαγωγή. Πιο συγκεκριμένα, για δεδομένο x , ας ορίσουμε την ιδιότητα P_x να είναι η εξής: $P_x(y)$ είναι αληθής αν και μόνο αν $\epsilon'(x \cdot y) = \epsilon'(x) + \epsilon'(y)$. Χρησιμοποιούμε δομική επαγωγή στο y για να δείξουμε την πρόταση $P_x(y)$.

Βάση της επαγωγής: $y = \epsilon$. Σε αυτή την περίπτωση, η πρόταση $P_x(y)$ είναι ισοδύναμη με $\epsilon'(x \cdot \epsilon) = \epsilon'(x) + \epsilon'(\epsilon)$, που ισχύει από τον ορισμό της παράθεσης και τον ορισμό του μήκους συμβολοσειρών.

Επαγωγικό βήμα: Θα δείξουμε ότι η $P_x(y)$ συνεπάγεται την $P_x(y\sigma)$. Έστω λοιπόν $y \in \Sigma^*$ με $\epsilon'(x \cdot y) = \epsilon'(x) + \epsilon'(y)$. Θα δείξουμε ότι για $\sigma \in \Sigma$ ισχύει ότι $\epsilon'(x \cdot (y\sigma)) = \epsilon'(x) + \epsilon'(y\sigma)$. Πράγματι έχουμε:

$$\begin{aligned} \epsilon'(x \cdot (y\sigma)) &= \epsilon'((x \cdot y)\sigma) && \text{από τον ορισμό της παράθεσης} \\ &= \epsilon'(x \cdot y) + 1 && \text{από τον ορισμό του μήκους} \\ &= (\epsilon'(x) + \epsilon'(y)) + 1 && \text{από την επαγωγική υπόθεση} \\ &= \epsilon'(x) + (\epsilon'(y) + 1) \\ &= \epsilon'(x) + \epsilon'(y\sigma) && \text{από τον ορισμό του μήκους.} \end{aligned}$$

□

Με παρόμοιο τρόπο μπορούμε να δείξουμε ότι αν x, y, z είναι συμβολοσειρές τότε $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Αυτό μας επιτρέπει να γράφουμε $x \cdot y \cdot z$, ή ακόμα και xyz , για την παράθεση των συμβολοσειρών χωρίς να δημιουργείται σύγχυση.

ΠΑΡΑΔΕΙΓΜΑ 3.4 (Αναδρομικός ορισμός γλωσσών). Έστω Σ ένα αλφάβητο. Τα υποσύνολα των συμβολοσειρών του Σ ονομάζονται γλώσσες. Παραδείγματα γλωσσών

- Η γλώσσα της δεκαδικής παράστασης των περιττών αριθμών: $\{1, 3, 5, 7, \dots\}$. Το αλφάβητο είναι το $\Sigma = \{0, 1, \dots, 9\}$.
- Η γλώσσα της δυαδικής παράστασης των περιττών αριθμών: $\{1, 11, 101, 111, \dots\}$. Το αλφάβητο είναι το $\Sigma = \{0, 1, \dots, 9\}$ ή το $\Sigma = \{0, 1\}$. Προσέξτε ότι η γλώσσα αυτή είναι διαφορετική από την προηγούμενη. Τα στοιχεία των γλωσσών αυτών είναι συμβολοσειρές, όχι αριθμοί. Άλλο είναι το σύνολο των περιττών αριθμών και άλλο είναι το σύνολο της δεκαδικής παράστασης των περιττών αριθμών.
- Η γλώσσα των λέξεων της Ελληνικής γλώσσας: $\{\alpha\beta\alpha\epsilon\iota\omicron, \alpha\beta\acute{\alpha}\theta\epsilon\iota\alpha, \dots, \omega\delta\eta\varsigma\}$. Το αλφάβητο είναι $\{\alpha, \acute{\alpha}, \dots, \acute{\omega}\}$.
- Η γλώσσα των προτάσεων της Αγγλικής γλώσσας: $\{\dots, \text{Nothing in education is so astonishing as the amount of ignorance it accumulates in the form of inert facts}, \dots\}$. Το αλφάβητο είναι $\{\alpha, \acute{\alpha}, \dots, \acute{\omega}, (\acute{\kappa}\acute{o}\mu\mu\alpha), (\text{space})\}$.
- Η γλώσσα των συντακτικά ορθών προγραμμάτων της γλώσσας C. Το αλφάβητο είναι οι λατινικοί χαρακτήρες και κάποια επιπλέον σύμβολα όπως οι παρενθέσεις, τα σύμβολα των αριθμητικών πράξεων κλπ.

Οι γλώσσες, και ειδικά αυτές που μοιάζουν με το τελευταίο παράδειγμα, παίζουν μεγάλο ρόλο στη Θεωρία Υπολογισμού. Ένα από τα κύρια αντικείμενα της Θεωρίας Υπολογισμού είναι η μελέτη των αναδρομικών ορισμών γλωσσών. Η δομική επαγωγή είναι συχνά πολύ χρήσιμη για να αποδείξουμε ιδιότητες τέτοιων γλωσσών.

Ας δούμε ένα παράδειγμα μια γλώσσας του αλφαβήτου $\{0, 1\}$. Με παρόμοιο τρόπο, αλλά με περισσότερους κανόνες, ορίζονται οι γραμματικές πολλές χρήσιμων γλωσσών· για παράδειγμα η γλώσσα των συντακτικά σωστών προγραμμάτων Java.

Ας θεωρήσουμε λοιπόν τη γλώσσα L που ορίζεται από τους κανόνες:
Βάση του ορισμού: Η κενή συμβολοσειρά ϵ ανήκει στη γλώσσα L .

Επαγωγικός ορισμός: Αν $w, v \in L$ τότε και οι συμβολοσειρές $0w1v$ και $1w0v$ ανήκουν στη γλώσσα L .

Ποιές συμβολοσειρές ανήκουν στην γλώσσα L ; Στην αρχή η L περιέχει μόνο την κενή συμβολοσειρά. Με την πρώτη εφαρμογή του επαγωγικού ορισμού, η L περιέχει τις συμβολοσειρές $\epsilon, 01$, και 10 . Με τη δεύτερη εφαρμογή, η L περιέχει τις συμβολοσειρές $\epsilon, 01, 10, 0011, 0101, 0110, 1001, 1010, 1100, 000111, 001011, 001101, 001110, \dots, 111000$.

Θα δείξουμε ότι η γλώσσα L περιέχει ακριβώς όλες τις συμβολοσειρές που έχουν ίσο αριθμό από 0 και 1. Θα το κάνουμε σε δυο βήματα.

Πρώτα θα δείξουμε ότι οι συμβολοσειρές της γλώσσας L έχουν ίσο αριθμό από 0 και 1. Και μετά θα δείξουμε ότι κάθε συμβολοσειρά με ίσο αριθμό από 0 και 1 ανήκει στη γλώσσα L .

Ισχυρισμός. Κάθε συμβολοσειρά της γλώσσας L έχει ίσο αριθμό από 0 και 1.

Απόδειξη. Θα χρησιμοποιήσουμε δομική επαγωγή. Ας ορίσουμε $n_0(u)$ και $n_1(u)$ τον αριθμό των 0 και 1 μιας συμβολοσειράς u . Θα δείξουμε ότι αν $u \in L$ τότε $n_0(u) = n_1(u)$.

Βάση της επαγωγής: $u = \epsilon$. Προφανώς η πρόταση ισχύει αφού $n_0(u) = n_1(u) = 0$.

Επαγωγικό βήμα: Η επαγωγική υπόθεση είναι ότι το καθένα από τα w και v έχει ίσο αριθμό από 0 και 1, δηλαδή ότι $n_0(w) = n_1(w)$ και $n_0(v) = n_1(v)$. Θέλουμε να δείξουμε ότι το ίδιο ισχύει και για τα $0w1v$ και $1w0v$. Πράγματι για την $0w1v$ έχουμε

$$n_0(0w1v) = n_0(w) + n_0(v) + 1$$

και

$$n_1(0w1v) = n_1(w) + n_0(v) + 1$$

και επομένως $n_0(0w1v) = n_1(0w1v)$. Με τον ίδιο ακριβώς τρόπο προκύπτει ότι το ίδιο ισχύει και για τη συμβολοσειρά $1w0v$. Δηλαδή οι νέες συμβολοσειρές που παράγονται από τον επαγωγικό ορισμό έχουν ίσο αριθμό από 0 και 1. \square

Τώρα θα δείξουμε το ανάποδο.

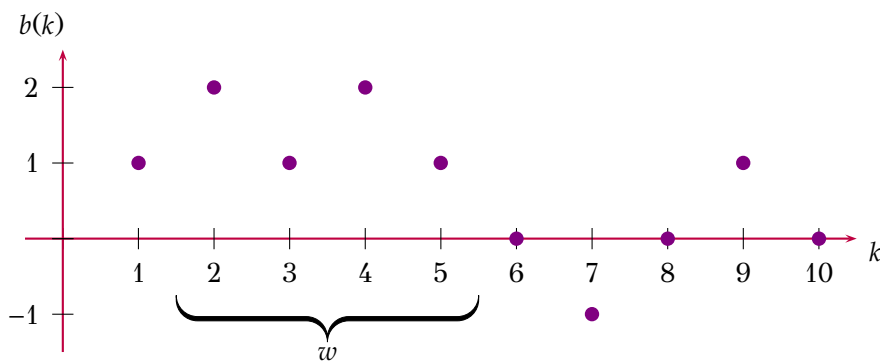
Ισχυρισμός. Κάθε συμβολοσειρά του αλφαβήτου $\{0, 1\}$ με ίσο αριθμό από 0 και 1 ανήκει στη γλώσσα L .

Απόδειξη. Με ισχυρή μαθηματική επαγωγή στο μήκος της συμβολοσειράς.

Βάση της επαγωγής: Αν η συμβολοσειρά έχει μήκος 0, δηλαδή είναι η κενή συμβολοσειρά ϵ , ανήκει στη γλώσσα L .

Επαγωγικό βήμα: Υποθέτουμε ότι κάθε συμβολοσειρά με μήκος το πολύ n που έχει ίσο αριθμό από 0 και 1 ανήκει στη γλώσσα L . Έστω μια συμβολοσειρά u με μήκος $n+1$ και ίσο αριθμό από 0 και 1. Διακρίνουμε δυο περιπτώσεις ανάλογα αν η συμβολοσειρά u αρχίζει με 0 ή με 1.

Ας υποθέσουμε λοιπόν ότι αρχίζει με 0. Αρχεί να δείξουμε ότι υπάρχουν συμβολοσειρές w και v , που μπορεί να είναι και οι κενές συμβολοσειρές, τέτοιες ώστε $u = 0w1v$ και επιπλέον $w, v \in L$. Ας συγκεντρώσουμε την προσοχή μας στο w , γιατί αν υπάρχει τέτοιο w , τότε αυτόματα θα υπάρχει και v . Πώς ξέρουμε ότι τέτοιο w υπάρχει; Ο λόγος είναι απλός: Στην αρχή του u ο αριθμός των 0 υπερτερεί γιατί το πρώτο σύμβολο είναι 0. Καθώς διαβάζουμε το u από αριστερά προς τα δεξιά κάποια στιγμή ο αριθμός των 0 θα γίνει ίσος με τον αριθμό των 1. (Αυτό θα συμβεί γιατί ξέρουμε ότι στο τέλος ο αριθμός των μηδέν είναι ίσος με



Σχήμα 3.1: Η συνάρτηση $b(k)$ για τη συμβολοσειρά 0010111001.

τον αριθμό των 1.) Η πρώτη φορά που ο αριθμός των μηδέν θα γίνει ίσος με τον αριθμό των 1 συμβαίνει μόνο όταν συναντήσουμε κάποιο 1. Ας πάρουμε λοιπόν για w το τμήμα του u μεταξύ του πρώτου 0 και αυτού του 1. Για παράδειγμα αν $u = 0010111001$, ο αριθμός των 0 γίνεται για πρώτη φορά ίσος με τον αριθμό των 1 όταν έχουμε διασχίσει το 001011, οπότε αγνοούμε το πρώτο 0 και το τελευταίο 1 και παίρνουμε $w = 0101$.

Για να κάνουμε την παραπάνω ιδέα πιο αυστηρή, έστω $b(k)$ δηλώνει το πόσα περισσότερα 0 από 1 υπάρχουν στα πρώτα k σύμβολα του u (Σχήμα 3.1). Γνωρίζουμε ότι $b(1) = 1$, δηλαδή το u αρχίζει με 0, και ότι $b(n+1) = 0$, δηλαδή το u έχει ίσο αριθμό από 0 και 1. Επίσης γνωρίζουμε ότι το $|b(k+1) - b(k)| = 1$, δηλαδή ένα σύμβολο αλλάζει τη διαφορά του αριθμού των 0 από τον αριθμό των 1 ακριβώς κατά 1. Έστω k ο μικρότερος αριθμός για τον οποίο συμβαίνει $b(k) = 0$. Προφανώς πριν γίνει μηδέν πρέπει να ήταν 1, δηλαδή $b(k-1) = 1$, που σημαίνει ότι τα πρώτα k σύμβολα του u είναι της μορφής $0w1$ για κάποιο w . Επιπλέον το w έχει ίσο αριθμό από 0 και 1.

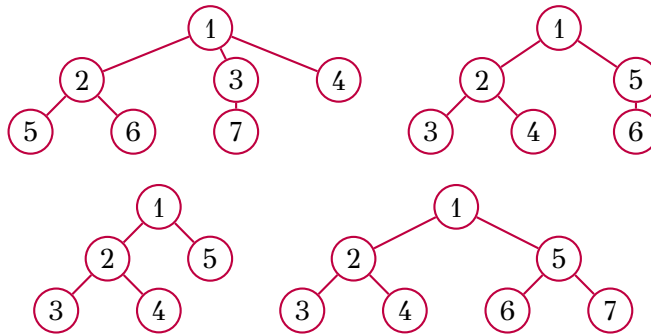
Τέλος, με τον ίδιο ακριβώς τρόπο αντιμετωπίζουμε την περίπτωση που το u αρχίζει με 1. □

Η ιδέα του επαγωγικού ορισμού μπορεί να χρησιμοποιηθεί για να ορίσουμε με αυστηρό τρόπο ποικίλες δομές. Στη συνέχεια θα ασχοληθούμε με μια ειδική κατηγορία γράφων, τα δένδρα. Αν το θεωρήσουμε σαν γράφο, δένδρο είναι κάθε συνεκτικός (δηλαδή ενωμένος) γράφος χωρίς κύκλους. Αλλά αν το θεωρήσουμε σαν δομή δεδομένων, τότε έχει μια ιεραρχική δομή, όπου υπάρχει κάποιος αρχικός κόμβος, η ρίζα του δένδρου, και από αυτή κρέμονται άλλα δένδρα. Εδώ θα μιλήσουμε για τέτοια δένδρα με ιεραρχική δομή.

Τα δένδρα, όπως και οι γράφοι, μπορεί να έχουν επώνυμους ή ανώνυμους κόμβους. Στην πρώτη περίπτωση τα ονομάζουμε δένδρα με ετικέτες (labeled trees) και στη δεύτερη περίπτωση δένδρα χωρίς ετικέτες (unlabeled trees). Για παράδειγμα, το Σχήμα 3.2 δείχνει ένα δένδρο



Σχήμα 3.2: Δένδρο χωρίς ετικέτες και δένδρο με ετικέτες.



Σχήμα 3.3: Δένδρα (γενικό, δυαδικό, κανονικό, πλήρες).

με ετικέτες και ένα δένδρο χωρίς ετικέτες. Εδώ θα θεωρήσουμε μόνο δένδρα με ετικέτες. Οι ετικέτες είναι στοιχεία κάποιου συνόλου U : στο παράδειγμα του Σχήματος 3.2 $U = \{A, B, \dots, Z\}$.

ΠΑΡΑΔΕΙΓΜΑ 3.5 (Δένδρα με ρίζα). Το σύνολο U των ετικετών μπορεί να είναι πεπερασμένο, αλλά εδώ θα υποθέτουμε ότι είναι άπειρο. Θα ορίσουμε τα δένδρα που έχουν σαν κόμβους τα στοιχεία του U .

Ορισμός 22 (Δένδρα με ρίζα).

Βάση τού ορισμού: Κάθε στοιχείο v του U είναι δένδρο. Θα λέμε ότι το δένδρο αυτό έχει ρίζα το v , σύνολο κόμβων το $\{v\}$, και σύνολο ακμών το κενό σύνολο.

Επαγωγικός ορισμός: Έστω T_1, \dots, T_n , για κάποιο $n \geq 0$, είναι δένδρα με σύνολα κόμβων ξένα μεταξύ τους και με ρίζες r_1, \dots, r_n αντίστοιχα. Έστω επίσης r ένα στοιχείο του U , που δεν ανήκει στους κόμβους των δένδρων T_1, \dots, T_n . Τότε ορίζουμε το δένδρο $T = (r, \{T_1, \dots, T_n\})$ με ρίζα το r . Το σύνολο των κόμβων του T είναι όλοι οι κόμβοι των T_1, \dots, T_n μαζί με το r . Το σύνολο των ακμών του T είναι όλες οι ακμές των T_1, \dots, T_n μαζί με τις $(r, r_1), \dots, (r, r_n)$. Τα δένδρα T_1, \dots, T_n θα τα ονομάζουμε υποδένδρα του T και οι κόμβοι r_1, \dots, r_n λέγονται παιδιά του r .

Ο ίδιος ορισμός μπορεί να χρησιμοποιηθεί για να ορίσουμε ειδικές

κατηγορίες δένδρων. Για να ορίσουμε τα *δυναδικά δένδρα*, στον επαγωγικό ορισμό απαιτούμε επιπλέον να ισχύει $n \leq 2$, δηλαδή κάθε κόμβος να έχει το πολύ δυο παιδιά. Αν απαιτήσουμε $n = 2$, τότε παίρνουμε τα *κανονικά ή γεμάτα δυναδικά δένδρα*. Τέλος για να ορίσουμε τα *πλήρη δυναδικά δένδρα*, απαιτούμε όχι μόνο $n = 2$, αλλά επίσης και ότι ο αριθμός των κόμβων των T_1, T_2 να είναι ίσος.

Προσέξτε ότι μαζί με τον ορισμό των δένδρων, ορίσαμε μαζί και το σύνολο των κόμβων και των ακμών. Αυτό θα μπορούσαμε να το κάνουμε με ξεχωριστό ορισμό, αλλά είναι πολλές φορές βολικό να έχουμε ένα κοινό ορισμό. Για παράδειγμα, έτσι μπορούμε να ορίσουμε εύκολα τα πλήρη δυναδικά δένδρα, που ο ορισμός τους χρησιμοποιεί τον αριθμό των κόμβων.

Οι κόμβοι ενός δένδρου που δεν έχουν παιδιά ονομάζονται φύλλα του δένδρου. Οι υπόλοιποι κόμβοι ονομάζονται εσωτερικοί κόμβοι.

ΠΑΡΑΔΕΙΓΜΑ 3.6 (Σχέση ύψους και πλήθος κόμβων δυναδικών δένδρων). Εκτός από τον επαγωγικό ορισμό των δένδρων μπορούμε να εισάγουμε την έννοια του ύψους δένδρων.

Ορισμός 23 (Ύψος δένδρου).

Βάση του ορισμού: Αν ένα δένδρο T αποτελείται μόνο από τη ρίζα του, ορίζουμε το ύψος του $h(T) = 0$.

Επαγωγικός ορισμός: Αν T_1, \dots, T_n είναι τα υποδένδρα ενός δένδρου T , τότε το ύψος του T είναι $h(T) = 1 + \max\{h(T_1), \dots, h(T_n)\}$.

Είμαστε τώρα έτοιμοι να αποδείξουμε ένα άνω φράγμα του αριθμού των κόμβων ενός δυναδικού δένδρου με δεδομένο ύψος.

Πρόταση 24. Για κάθε δυναδικό δένδρο T ισχύει ότι το πλήθος των κόμβων του $n(T)$ είναι το πολύ $2^{h(T)+1} - 1$.

Απόδειξη. Η απόδειξη και πάλι θα γίνει με επαγωγή στη δομή των δυναδικών δένδρων.

Βάση δομικής επαγωγής: Αν το δένδρο αποτελείται μόνο από τη ρίζα του, έχει εξ' ορισμού ύψος 0 και ένα κόμβο· η πρόταση προφανώς ισχύει.

Επαγωγικό βήμα: Έστω δυναδικό δένδρο T με δύο υποδένδρα T_1 και T_2 . Εξ' ορισμού, οι κόμβοι του T είναι οι κόμβοι του T_1 , οι κόμβοι του T_2 , και η ρίζα του T . Άρα ο αριθμός των κόμβων του είναι $n(T) = n(T_1) + n(T_2) + 1$. Επίσης εξ' ορισμού, το ύψος του είναι $h(T) = 1 + \max\{h(T_1), h(T_2)\}$.

Από την επαγωγική υπόθεση για τα δένδρα T_1 και T_2 , $n(T_1) \leq 2^{h(T_1)+1} - 1$ και $n(T_2) \leq 2^{h(T_2)+1} - 1$. Αν τα βάλουμε όλα μαζί έχουμε

$$\begin{aligned} n(T) &= n(T_1) + n(T_2) + 1 \\ &\leq (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1) + 1 \\ &= 2^{h(T_1)+1} + 2^{h(T_2)+1} - 1 \\ &\leq 2 \cdot \max\{2^{h(T_1)+1}, 2^{h(T_2)+1}\} - 1 \\ &= 2 \cdot 2^{\max\{h(T_1)+1, h(T_2)+1\}} - 1 \\ &= 2 \cdot 2^{\max\{h(T_1), h(T_2)\}+1} - 1 \\ &= 2 \cdot 2^{h(T)} - 1 \\ &= 2^{h(T)+1} - 1 \end{aligned}$$

Με τον ίδιο τρόπο χειριζόμαστε και την περίπτωση που το δένδρο T έχει μόνο ένα υποδένδρο. \square

Ασκήσεις

3.1. Χρησιμοποιήστε δομική επαγωγή για να αποδείξετε ότι σε κάθε πλήρες δυαδικό δένδρο T , το πλήθος των φύλλων του $l(T)$, δηλαδή των κόμβων που δεν έχουν παιδιά, είναι ένα παραπάνω από το πλήθος των εσωτερικών του κόμβων $i(T)$, δηλαδή των κόμβων που έχουν παιδιά.

3.2. Έστω S ένα υποσύνολο του $\mathbb{N} \times \mathbb{N}$ που ορίζεται επαγωγικά ως εξής:

Βάση του ορισμού: $(0, 0) \in S$

Επαγωγικός ορισμός: Αν $(a, b) \in S$ τότε $(a+2, b+3) \in S$ και $(a+3, b+2) \in S$.

α' Καταγράψτε τα στοιχεία του συνόλου S μετά από 4 εφαρμογές του επαγωγικού βήματος του ορισμού του.

β' Χρησιμοποιήστε επαγωγή για να αποδείξετε ότι αν $(a, b) \in S$ τότε το $a + b$ είναι πολλαπλάσιο του 5.

γ' Διατυπώστε με σαφήνεια μια υπόθεση για το ποια ζεύγη αριθμών ανήκουν στο S . Αποδείξτε την υπόθεση σας.

3.3. Έστω S ένα υποσύνολο του $\mathbb{N} \times \mathbb{N}$ που ορίζεται επαγωγικά ως εξής:

Βάση επαγωγικού ορισμού: $(1, 1) \in S$

Επαγωγικό βήμα: Αν $(a, b) \in S$ τότε $(a + b, b) \in S$ και $(a, a + b) \in S$.

α' Καταγράψτε τα στοιχεία του συνόλου S μετά από 3 εφαρμογές του επαγωγικού βήματος.

β' Χρησιμοποιήστε επαγωγή για να αποδείξετε ότι

$$S = \{(x, y) : x, y \in \mathbb{N} \text{ και } \gcd(x, y) = 1\}.$$

3.4. Ορίζουμε αναδρομικά ένα σύνολο Q , που περιέχει ζεύγη από φυσικούς αριθμούς, ως εξής:

1. Το ζεύγος $(1, 1)$ ανήκει στο Q .
2. Αν ένα ζεύγος (a, b) ανήκει στο Q , τότε και το ζεύγος $(b, a+b)$ ανήκει στο Q .

Ποιό είναι το σύνολο Q ; Αποδείξτε προσεκτικά την απάντησή σας.

3.5. Θεωρήστε το σύνολο S που ορίζεται ως εξής:

1. $(1, 1) \in S$
2. Αν $(x, y) \in S$ τότε και $(y, x) \in S$
3. Αν $(x, y) \in S$ τότε και $(x, x + 2y) \in S$

Ποιο είναι το σύνολο S ; Αποδείξτε προσεκτικά την απάντησή σας. Επικεντρωθείτε στο άθροισμα των δυο αριθμών του κάθε ζεύγους.

3.6. Θεωρήστε το σύνολο A των συμβολοσειρών του αλφαβήτου $\{0, 1\}$ που ορίζεται με τον εξής αναδρομικό ορισμό:

- $01 \in A$.
- Αν $w \in A$, τότε $w1w \in A$.

1. Ποιο σύνολο είναι το A ; Περιγράψτε το με μια πρόταση της καθομιλουμένης.
2. Δώστε επίσης μια ακριβή μαθηματική περιγραφή.
3. Αποδείξτε προσεκτικά ότι η μαθηματική περιγραφή που δώσατε εκφράζει το σύνολο A .

3.7. Θεωρήστε το υποσύνολο T των φυσικών αριθμών που ορίζεται με τον εξής αναδρομικό ορισμό:

- $1 \in T$.
- Αν $n \in T$, τότε $2n \in T$.
- Αν $n \in T$, τότε $n + 3 \in T$.

1. Δώστε τα 10 μικρότερα στοιχεία του συνόλου T ;
2. Αποδείξτε προσεκτικά ότι το σύνολο T είναι το

$$\{3k + a : k \in \mathbb{N} \text{ και } a = 1, 2\}.$$

3.8. Ορίζουμε αναδρομικά ένα σύνολο συμβολοσειρών P του αλφαβήτου $\{0, 1\}$ ως εξής :

3. ΑΝΑΔΡΟΜΗ ΚΑΙ ΕΠΑΓΩΓΗ

1. Η κενή συμβολοσειρά ανήκει στο P : $\epsilon \in P$
2. Αν μια συμβολοσειρά w ανήκει στο σύνολο P , τότε και οι συμβολοσειρές $0w0$ και $1w1$ ανήκουν στο P .

Ποιο είναι το σύνολο P ; Αποδείξτε προσεκτικά την απάντησή σας.

4 Αποδείξεις Ύπαρξης

Πολλές φορές χρειάζεται να αποδείξουμε ότι κάποιο σύνολο ή δομή έχει κάποιο στοιχείο με συγκεκριμένες ιδιότητες. Οι αποδείξεις αυτές ονομάζονται αποδείξεις ύπαρξης.

Για παράδειγμα, θέλουμε να δείξουμε ότι υπάρχει φυσικός αριθμός που μπορεί να γραφεί με δύο διαφορετικούς τρόπους σαν άθροισμα δυο κύβων, ή ισοδύναμα, ότι υπάρχουν δυο διαφορετικά ζεύγη φυσικών αριθμών $\{a_1, b_1\}$ και $\{a_2, b_2\}$ με $a_1^3 + b_1^3 = a_2^3 + b_2^3$.

Γενικά οι αποδείξεις ύπαρξης χωρίζονται σε δυο μεγάλες κατηγορίες:

- *Κατασκευαστικές αποδείξεις*, στις οποίες η απόδειξη είτε δίνει το στοιχείο που έχει την απαιτούμενη ιδιότητα είτε δίνει ένα αλγόριθμο που παράγει ένα τέτοιο στοιχείο.
- *Μη κατασκευαστικές αποδείξεις*, στις οποίες δείχνουμε ότι το στοιχείο υπάρχει, αλλά ούτε το στοιχείο δίνεται ούτε αλγόριθμος που να το παράγει.

Ένα καλό παράδειγμα κατασκευαστικής απόδειξης αποτελεί η απόδειξη της παραπάνω πρότασης για το άθροισμα κύβων. Η απόδειξη είναι ουσιαστικά μισή γραμμή: ο 1729 μπορεί να γραφτεί¹ σαν $1^3 + 12^3 = 9^3 + 10^3$.

Ένα καλό παράδειγμα μη κατασκευαστικής απόδειξης είναι η απόδειξη της παρακάτω πρότασης.

Πρόταση 25. *Να δειχτεί ότι υπάρχουν άρρητοι x και y τέτοιοι ώστε ο x^y είναι ρητός.*

¹Υπάρχει μια χαριτωμένη ιστορία που αφορά αυτό το γεγονός και τον μεγάλο Ινδό μαθηματικό Ramanujan. Όταν ο Ramanujan ήταν άρρωστος, τον επισκέφτηκε ο σπουδαίος Άγγλος μαθηματικός Hardy. Ο Hardy είχε πάει με ταξί και ανέφερε στον Ramanujan πως ο αριθμός του ταξί ήταν ο ασήμαντος αριθμός 1729. Ο Ramanujan αμέσως το διαβεβαίωσε πως δεν είναι έτσι, αφού ο 1729 είναι ο μικρότερος φυσικός που γράφεται με δυο διαφορετικούς τρόπους σαν άθροισμα φυσικών κύβων.

Απόδειξη. Έστω $x_1 = \sqrt{2}$, $y_1 = \sqrt{2}$ και $x_2 = \sqrt{2}\sqrt{2}$, $y_2 = \sqrt{2}$. Θα δείξουμε ότι ένα από τα ζευγάρια των αριθμών x_1, y_1 και x_2, y_2 ικανοποιεί την πρόταση.

Έχουμε ότι $x_1^{y_1} = x_2$ και $x_2^{y_2} = 2$. Επιπλέον οι αριθμοί x_1, y_1, y_2 είναι άρρητοι. Το ερώτημα είναι αν ο x_2 είναι ρητός. Αν είναι, τότε το πρώτο ζευγάρι x_1, y_1 ικανοποιεί την πρόταση. Διαφορετικά, τα x_2, y_2 είναι άρρητα, ο $x_2^{y_2} = 2$ είναι ρητός και το δεύτερο ζευγάρι ικανοποιεί την πρόταση.

Αν και δείξαμε ότι ένα από τα ζευγάρια ικανοποιεί την πρόταση, δεν γνωρίζουμε ποιό είναι. \square

Η διάκριση μεταξύ των δυο κατηγοριών, κατασκευαστικής απόδειξης ύπαρξης ή μη, είναι συνήθως υποκειμενική και όχι πάντα ευδιάκριτη, αλλά βοηθάει να έχουμε την κατηγοριοποίηση στο μυαλό μας όταν σκεφτόμαστε για αποδείξεις ύπαρξης.

Θα δούμε ένα ακόμα παράδειγμα για να κατανοήσουμε καλύτερα την ιδέα της κατασκευαστικής ή μη απόδειξης ύπαρξης. Αυτή τη φορά θα δούμε δυο διαφορετικές αποδείξεις του ίδιου θεωρήματος, η μια κατασκευαστική και η άλλη μη κατασκευαστική. Θα αποδείξουμε το παρακάτω βασικό θεώρημα της Θεωρίας Αριθμών.

Θεώρημα 26. Έστω a και b δυο ακέραιοι με μέγιστο κοινό διαιρέτη d . Τότε υπάρχουν ακέραιοι x και y τέτοιοι ώστε $ax + by = d$.

Για παράδειγμα, αν $a = 13$ και $b = 16$, τότε $\gcd(a, b) = 1$ και το θεώρημα εγγυάται ότι υπάρχουν ακέραιοι x και y τέτοια ώστε $13x + 16y = 1$. Πράγματι αυτό ισχύει για $x = 5$ και $y = -4$.

Ας δούμε πρώτα μια κατασκευαστική απόδειξη του Θεωρήματος 26. Θα δείξουμε ότι μια παραλλαγή του αλγόριθμου του Ευκλείδη βρίσκει τέτοια x και y . Αν πάρουμε δηλαδή τον Αλγόριθμο 2.1, μπορούμε να τον αλλάξουμε κατάλληλα στον Αλγόριθμο 4.1 για να επιστρέφει όχι μόνο τον μέγιστο κοινό διαιρέτη d αλλά και ακέραιους x και y τέτοιους ώστε $ax + by = d$. Μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι οι αριθμοί a και b είναι μη αρνητικοί ακέραιοι και ότι $a \geq b$ (διαφορετικά μπορούμε να αλλάξουμε τη σειρά τους και τα πρόσημα των a, b, x και y).

Θα χρησιμοποιήσουμε ισχυρή μαθηματική επαγωγή στο b και θα δείξουμε

Θεώρημα 27. Ο Αλγόριθμος 4.1 επιστρέφει d, x και y τέτοια ώστε (α) ο d είναι ο μέγιστος κοινός διαιρέτης των a και b και (β) $ax + by = d$.

Αλγόριθμος 4.1: Αλγόριθμος του Ευκλείδη

```

1: function EUCLID( $a, b$ )                                ▷Υποθέτουμε ότι  $a > b$ 
2:   if  $b = 0$  then
3:     return ( $a, 1, 0$ )                                  ▷ $a \cdot 1 + b \cdot 0 = a$ 
4:   else
5:      $(\delta, x', y') \leftarrow$  EUCLID( $b, a \bmod b$ )      ▷ $b \cdot x' + (a \bmod b) \cdot y' = \delta$ 
6:     return ( $\delta, y', x' - \lfloor a/b \rfloor y'$ )          ▷ $x = y', y = x' - \lfloor a/b \rfloor y'$ 
7:   end if
8: end function

```

Απόδειξη. Βάση της επαγωγής: Αν $b = 0$, τότε ο μέγιστος κοινός διαιρέτης είναι $\delta = a$. Αφού $a \cdot 1 + b \cdot 0 = \delta$, ο αλγόριθμος σωστά επιστρέφει τις τιμές $\delta = a$, $x = 1$ και $b = 0$.

Επαγωγικό βήμα: Υποθέτουμε ότι ο αλγόριθμος επιστρέφει σωστές τιμές για κάθε $b \leq n$. Θα δείξουμε ότι το ίδιο ισχύει και για $b = n + 1$. Επειδή ο $a \bmod b$ είναι μικρότερος του b , η επαγωγική υπόθεση ισχύει για $a \bmod b$. Η γραμμή 5 λοιπόν επιστρέφει τιμές x' και y' τέτοιες ώστε $b \cdot x' + (a \bmod b) \cdot y' = \delta$, όπου δ είναι ο μέγιστος κοινός διαιρέτης των b και $a \bmod b$. Ο δ είναι επίσης μέγιστος κοινός διαιρέτης και των a και b , όπως προκύπτει από την απλή μορφή του αλγόριθμου του Ευκλείδη 2.1. Λαμβάνοντας υπόψη ότι $a \bmod b = a - \lfloor a/b \rfloor b$, έχουμε:

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

Επομένως αν θέσουμε $x = y'$ και $y = x' - \lfloor a/b \rfloor y'$, τότε έχουμε $ax + by = \delta$. Σωστά λοιπόν επιστρέφει ο αλγόριθμος στη γραμμή 6 τις τιμές αυτές. \square

Ας δούμε τώρα μια άλλη απόδειξη του Θεωρήματος 26, μη κατασκευαστική αυτή τη φορά.

Απόδειξη. Κατ' αρχήν μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι οι αριθμοί a και b είναι μη αρνητικοί (διαφορετικά μπορούμε να τους αλλάξουμε κατάλληλα τα πρόσημα τους καθώς και τα πρόσημα των x και y). Επίσης αν κάποιος είναι 0 τότε είναι εύκολο να δούμε ότι το θεώρημα ισχύει.

Επιπλέον αρκεί να δείξουμε το θεώρημα για θετικούς ακεραίους που είναι πρώτοι μεταξύ τους, δηλαδή έχουν μέγιστο κοινό διαιρέτη 1. Πράγματι, αν ο μέγιστος κοινός διαιρέτης των a και b είναι $\delta > 1$, θεωρούμε τους αριθμούς a/δ και b/δ . Οι αριθμοί αυτοί είναι πρώτοι μεταξύ

τους και αν υπάρχουν x και y με $a/\delta x + b/\delta y = 1$, τότε προκύπτει άμεσα ότι $ax + by = \delta$.

Θα δείξουμε ότι υπάρχει y τέτοιο ώστε $by - 1 = 0 \pmod{a}$. Από αυτό, η πρόταση προκύπτει άμεσα, γιατί τότε υπάρχει ακέραιος x' τέτοιος ώστε $by - 1 = ax'$ ή ισοδύναμα $a(-x') + by = 1$. Πάρε τώρα $x = -x'$ και η πρόταση ισχύει.

Ας περάσουμε λοιπόν στην ουσία της απόδειξης. Για να δείξουμε ότι υπάρχει y τέτοιο ώστε $by - 1 = 0 \pmod{a}$, θεώρησε τους αριθμούς $by - 1 \pmod{a}$ για $y = 1, \dots, a$. Παρατήρησε ότι όλοι αυτοί οι αριθμοί είναι διαφορετικοί μεταξύ τους. Γιατί; Γιατί αν $by_1 - 1 \pmod{a} = by_2 - 1 \pmod{a}$ για κάποια y_1, y_2 , με $y_1 > y_2$, τότε απλοποιώντας θα έχουμε $b(y_1 - y_2) = 0 \pmod{a}$. Αφού όμως οι a και b είναι πρώτοι μεταξύ τους, αυτό μπορεί να ισχύει μόνο αν ο a διαιρεί τον $y_1 - y_2$, αδύνατο αφού $0 < y_1 - y_2 < a$.

Αφού όλοι οι a το πλήθος αριθμοί της μορφής $by - 1 \pmod{a}$ είναι διαφορετικοί και ανήκουν στο σύνολο $\{0, \dots, a-1\}$, κάποιος από αυτούς είναι ίσος με 0. Άρα υπάρχει y τέτοιο ώστε $by - 1 = 0 \pmod{a}$. \square

Προσέξτε ότι η τελευταία γραμμή της απόδειξης αυτής είναι το μη κατασκευαστικό μέρος της. Ξέρουμε ότι τέτοιο y υπάρχει, και ότι ανήκει στο $\{1, \dots, a\}$, αλλά δεν έχουμε καμμία άλλη πληροφορία για αυτό.

Βέβαια, κάποιος θα μπορούσε να ισχυριστεί ότι και αυτή η απόδειξη είναι κατασκευαστική γιατί μας δίνει ένα τρόπο για να βρούμε το y : Δοκίμασε όλες τις τιμές στο $\{1, \dots, a\}$. Όπως αναφέραμε παραπάνω η διάκριση ανάμεσα σε κατασκευαστικές και μη κατασκευαστικές αποδείξεις είναι μερικές φορές δυσδιάκριτη. Αλλά διαισθητικά, ο αλγόριθμος του Ευκλείδη κατασκευάζει ένα κατάλληλο y , ενώ η μη κατασκευαστική απόδειξη απλώς δείχνει ότι υπάρχει. Μια άλλη διαφορά ανάμεσα στις δυο αποδείξεις είναι η εξής: Για να δοκιμάσουμε όλα τα y στο $\{1, \dots, a\}$ χρειαζόμαστε a βήματα, ενώ ο αλγόριθμος του Ευκλείδη βρίσκει ένα τέτοιο y σε χρόνο το πολύ $2 \log a$ (Πρόταση 13). Με άλλα λόγια η κατασκευαστική απόδειξη μας δίνει ένα πολύ πιο αποτελεσματικό αλγόριθμο για να βρούμε το κατάλληλο y .

4.1 Η Αρχή του Περιστερώνα

Πολλές μη κατασκευαστικές αποδείξεις ύπαρξης βασίζονται σε μια απλή αρχή.

Θεώρημα 28. *Αν τοποθετήσουμε n περιστέρια σε $n - 1$ φωλιές, θα υπάρχει μια τουλάχιστον φωλιά με 2 τουλάχιστον περιστέρια.*

ΠΑΡΑΔΕΙΓΜΑ 4.1. Αν έχουμε $n + 1$ ακέραιους αριθμούς που ανήκουν στο διάστημα $1, \dots, n$, τότε δυο τουλάχιστον από τους αριθμούς είναι ίσοι. Εδώ τα ‘περιστέρια’ είναι οι αριθμοί και οι ‘φωλιές’ οι αριθμοί $1, \dots, n$.

Η αλήθεια του Θεωρήματος είναι προφανής και μπορεί να αποδειχτεί με μαθηματική επαγωγή (Άσκηση 4.1). Μερικές φορές χρησιμοποιούμε την παρακάτω γενίκευση της αρχής:

Θεώρημα 29 (Αρχή του Περιστερώνα). *Αν τοποθετήσουμε n περιστέρια σε m φωλιές, θα υπάρξει μια τουλάχιστον φωλιά με $\lceil n/m \rceil$ τουλάχιστον περιστέρια.*

ΠΑΡΑΔΕΙΓΜΑ 4.2. Χρησιμοποιώντας την Αρχή του Περιστερώνα, βρίσκουμε ότι σε κάθε ομάδα 13 ατόμων θα υπάρχουν δυο που γεννήθηκαν τον ίδιο μήνα. Παρόμοια σε κάθε ομάδα 100 ατόμων θα υπάρχουν τουλάχιστον 9 ($= \lceil 100/12 \rceil$) που γεννήθηκαν τον ίδιο μήνα.

ΠΑΡΑΔΕΙΓΜΑ 4.3. Μερικές φορές η Αρχή του Περιστερώνα μπορεί να χρησιμοποιηθεί για να δείξει αναπάντεχα αποτελέσματα, όπως: 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 $11 \dots 100 \dots 0$. Για παράδειγμα, αν $n = 12$ υπάρχει πολλαπλάσιο του αυτής της μορφής: $11100 = 12 \cdot 925$.

Η απόδειξη με χρήση της Αρχής του Περιστερώνα είναι εύκολη: Ας θεωρήσουμε τους $n + 1$ αριθμούς $1, 11, 111, \dots, 11 \dots 1$ και τα υπόλοιπα τους $\pmod n$. Επειδή τα υπόλοιπα ανήκουν στο $\{0, \dots, n - 1\}$, δυο τουλάχιστον από τους παραπάνω αριθμούς έχουν το ίδιο υπόλοιπο. Η διαφορά τους έχει την επιθυμητή μορφή και είναι πολλαπλάσιο του n .

ΠΑΡΑΔΕΙΓΜΑ 4.4. Ας θεωρήσουμε μια ακολουθία αριθμών t_1, \dots, t_m . Κάθε ακολουθία που προκύπτει όταν αγνοήσουμε μηδέν ή περισσότερους όρους της ακολουθίας λέγεται υποακολουθία. Για παράδειγμα, κάποιες από τις υποακολουθίες της ακολουθία 3, 5, 2, 7 είναι η ακολουθία 3, 2, 7, η ακολουθία 5, 2, καθώς και η κενή υποακολουθία.

Μια ακολουθία λέγεται αύξουσα αν κάθε όρος της είναι μεγαλύτερος ή ίσος από τον προηγούμενο του· λέγεται φθίνουσα αν κάθε όρος της είναι μικρότερος ή ίσος από τον προηγούμενό του. Μια ακολουθία λέγεται μονότονη αν είναι αύξουσα ή φθίνουσα. Για παράδειγμα, η ακολουθία 2, 4, 5, 8 είναι μονότονη (αύξουσα), ενώ η 3, 6, 4, 8 δεν είναι μονότονη. Θα δείξουμε το παρακάτω θεώρημα ύπαρξης:

Θεώρημα 30. Κάθε ακολουθία πραγματικών αριθμών με $n^2 + 1$ στοιχεία έχει μια μονότονη υποακολουθία με $n + 1$ στοιχεία.

Για παράδειγμα κάθε ακολουθία 5 ($= 2^2 + 1$) στοιχείων περιέχει μια υποακολουθία με 3 στοιχεία που είναι είτε αύξουσα είτε φθίνουσα.

Το Θεώρημα δεν μπορεί να βελτιωθεί, με την έννοια ότι υπάρχουν ακολουθίες που έχουν n^2 στοιχεία που ουδεμία υποακολουθία τους με $n + 1$ στοιχεία είναι μονότονη· για παράδειγμα για $n = 3$, η ακολουθία 7, 8, 9, 4, 5, 6, 1, 2, 3 (Άσκηση 4.12).

Απόδειξη. Ας αποδείξουμε τώρα το Θεώρημα με χρήση της Αρχής του Περιστερώνα. Έστω t_1, \dots, t_{n^2+1} μια ακολουθία. Για κάθε $i = 1, \dots, n^2 + 1$ ορίζουμε ως a_i να είναι το μήκος της μακρύτερης αύξουσας υποακολουθίας με τελευταίο στοιχείο το t_i . Με τον ίδιο τρόπο ορίζουμε ως φ_i να είναι το μήκος της μακρύτερης φθίνουσας υποακολουθίας με τελευταίο στοιχείο το t_i . Για παράδειγμα, αν η ακολουθία είναι 2, 4, 3, 5, 6, τότε $a_1 = 1$, $a_4 = 3$, και $\varphi_3 = 2$.

Θέλουμε να δείξουμε ότι υπάρχει μονότονη υποακολουθία μήκους $n + 1$ ή ισοδύναμα ότι κάποιο από τα a_i ή τα φ_i έχει τιμή μεγαλύτερη ή ίση με $n + 1$. Η ουσία της απόδειξης είναι ότι τα ζεύγη (a_i, φ_i) είναι διαφορετικά για όλα τα i , δηλαδή $(a_i, \varphi_i) \neq (a_j, \varphi_j)$ όταν $i < j$. Πράγματι, αν $t_i \leq t_j$, τότε $a_i + 1 \leq a_j$ γιατί μπορούμε να επεκτείνουμε την αύξουσα υποακολουθία που τελειώνει με το t_i προσθέτοντας το στοιχείο t_j . Αν πάλι $t_i > t_j$, τότε $\varphi_i + 1 \leq \varphi_j$ για παρόμοιο λόγο.

Για να δείξουμε ότι κάποιο από τα a_i ή τα φ_i έχει τιμή μεγαλύτερη ή ίση με $n + 1$ θα χρησιμοποιήσουμε απαγωγή σε άτοπο. Έστω ότι όλα τα a_i και φ_i είναι μεταξύ 1 και n . Τότε ας θεωρήσουμε για ‘περιστέρια’ τα ζεύγη (a_i, φ_i) και για ‘φωλιές’ τα ζεύγη των αριθμών στο διάστημα $1, \dots, n$. Υπάρχουν $n^2 + 1$ ‘περιστέρια’ και n^2 ‘φωλιές’. Από την Αρχή του Περιστερώνα, δύο ‘περιστέρια’ θα βρισκονται στην ίδια ‘φωλιά’, δηλαδή, υπάρχουν δυο ζεύγη (a_i, φ_i) και (a_j, φ_j) ίδια, που όπως δείξαμε παραπάνω δεν μπορεί να συμβεί. Άρα η υπόθεση ότι τα a_i και φ_i είναι μεταξύ 1 και n είναι εσφαλμένη. \square

ΠΑΡΑΔΕΙΓΜΑ 4.5. Ο Dirichlet χρησιμοποίησε την αρχή του Αρχή του Περιστερώνα για να μελετήσει πόσο καλά μπορούμε να προσεγγίσουμε άρρητους αριθμούς με ρητούς. Για παράδειγμα, ο αριθμός π μπορεί προσεγγιστεί σαν

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

Είναι φυσικό να ρωτήσουμε αν αυτές είναι οι καλύτερες προσεγγίσεις του π με ρητούς. Είναι προφανές ότι αν αυξήσουμε τον παρονομαστή

σε μεγαλύτερη δύναμη του 10 θα πάρουμε καλύτερη προσέγγιση. Το ερώτημα είναι αν μπορούμε να έχουμε καλύτερη προσέγγιση με άλλους παρονομαστές. Ο Αρχιμήδης για παράδειγμα γνώριζε ότι μια καλή προσέγγιση του π είναι το $22/7 = 3.1428\dots$, μια προσέγγιση με μικρό παρονομαστή. Μια ακόμα καλύτερη προσέγγιση είναι το $355/113$ που συμφωνεί με το π μέχρι το 6ο δεκαδικό ψηφίο.

Το ερώτημα που θέλουμε να μελετήσουμε είναι το εξής: Έστω θ ένας άρρητος αριθμός και m ένας θετικός ακέραιος· πόσο καλά μπορούμε να προσεγγίσουμε τον θ με κλάσματα των οποίων ο παρονομαστής είναι το πολύ m ;

Θεώρημα 31 (Dirichlet). Έστω θ ένας πραγματικός αριθμός. Τότε για οποιοδήποτε θετικό ακέραιο m , υπάρχουν ακέραιοι p και q , με $1 \leq q \leq m$, τέτοιοι ώστε

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

Απόδειξη. Ας πάρουμε τα ακέραια πολλαπλάσια $q\theta$, για $q = 0, 1, \dots, m$ και ας θεωρήσουμε το δεκαδικό μέρος τους $q\theta - [q\theta]$. Για παράδειγμα τα ακέραια πολλαπλάσια του $\sqrt{2}$ είναι $0, 1.41\dots, 2.82\dots, 4.24\dots$ κλπ και το δεκαδικό μέρος τους είναι $0, 0.41\dots, 0.82\dots, 0.24\dots$ κλπ. Οι αριθμοί αυτοί είναι της μορφής $q\theta - p$, όπου q και $p = [q\theta]$ είναι ακέραιοι. Για $q = 0, 1, \dots, m$ υπάρχουν $m + 1$ τέτοιοι αριθμοί και όλοι βρίσκονται στο διάστημα $[0, 1)$.

Αν θεωρήσουμε τους αριθμούς αυτούς ως περιστέρια και τα διαστήματα $[0, 1/m), [1/m, 2/m), \dots, [(m-1)/m, 1)$ ως φωλιές, μπορούμε να εφαρμόσουμε την Αρχή του Περιστερώνα. Κάποια φωλιά θα περιέχει δυο περιστέρια, άρα υπάρχουν δυο αριθμοί $q_1\theta - p_1$ και $q_2\theta - p_2$ που διαφέρουν λιγότερο από $1/m$, δηλαδή $|(q_2 - q_1)\theta - (p_2 - p_1)| < 1/m$.

Οι αριθμοί $q = q_2 - q_1$ και $p = p_2 - p_1$ είναι ακέραιοι και επιπλέον $1 \leq q \leq m$. Συμπεραίνουμε δηλαδή ότι υπάρχουν ακέραιοι p και q , με $1 \leq q \leq m$, τέτοιοι ώστε

$$|q\theta - p| < 1/m.$$

Η απόδειξη ολοκληρώνεται αν διαιρέσουμε με το q :

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

□

Η παραπάνω απόδειξη είναι μη κατασκευαστική. Δεν μας δίνει καμία πληροφορία για το πως να βρούμε ένα καλό παρονομαστή q .

* *

Υπάρχει όμως ένας απλός τρόπος για να βρούμε ένα τέτοιο καλό παρονομαστή, τα συνεχή κλάσματα. Π.χ.

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}} \quad \pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \dots}}}$$

Για να βρούμε το συνεχές κλάσμα του $\sqrt{2}$, υπολογίζουμε το ακέραιο μέρος του που είναι ίσο με 1. Γράφουμε λοιπόν $\sqrt{2} = 1 + 1/x$, όπου λύνοντας ως προς x βρίσκουμε $x = 1/(\sqrt{2} - 1)$. Αρκεί τώρα να βρούμε το συνεχές κλάσμα του x , κοκ.

Αποδεικνύεται ότι οι καλύτερες προσεγγίσεις ενός αριθμού προκύπτουν να πάρουμε κάποιους όρους του συνεχούς κλάσματος του αριθμού και το μετατρέψουμε σε απλό κλάσμα. Π.χ. μια καλή προσέγγιση του $\sqrt{2}$ είναι

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5}.$$

Πολλές φορές όμως θέλουμε την κοινή προσέγγιση πολλών άρρητων αριθμών με ρητούς που να έχουν κοινό παρονομαστή ώστε να είναι εύκολη η πρόσθεση και η αφαίρεση τους. Για παράδειγμα, μια κοινή προσέγγιση του $\sqrt{2} = 1.414\dots$ και του $\sqrt{3} = 1.732\dots$ είναι $7/5 = 1.4$ και $9/5 = 1.8$, αντίστοιχα. Το Θεώρημα 31 επεκτείνεται σε πολλούς αριθμούς με παρόμοια απόδειξη:

Θεώρημα 32. Έστω $\theta_1, \dots, \theta_n$ πραγματικοί αριθμοί. Τότε για οποιοδήποτε θετικό ακέραιο m , υπάρχουν ακέραιοι p_1, \dots, p_n και q , με $1 \leq q \leq m^n$, τέτοιοι ώστε

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

για κάθε $i = 1, \dots, n$.

Αν και το θεώρημα εγγυάται την ύπαρξη τέτοιων p_i και q , δεν γνωρίζουμε κανένα αλγόριθμο που να τους βρίσκει ουσιαστικά πιο γρήγορα από το να δοκιμάσουμε όλες τις m^n δυνατές τιμές του q . Με άλλα λόγια, τα συνεχή κλάσματα επιτρέπουν να βρούμε γρήγορα καλές ρητές προσεγγίσεις αλλά δεν έχουμε παρόμοιο τρόπο για δυο ή περισσότερους αριθμούς.

Ασκήσεις

4.1. Αποδείξτε με μαθηματική επαγωγή το Θεώρημα 28.

4.2. Θεωρήστε πέντε διαφορετικούς αριθμούς που επιλέγονται από το σύνολο $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Δείξτε ότι σε αυτούς περιλαμβάνεται τουλάχιστον ένα ζευγάρι που έχει άθροισμα 9.

4.3. Πόσοι αριθμοί πρέπει να επιλεχθούν από το σύνολο $\{1, 3, 5, 7, 9, 11, 13, 15\}$ ώστε σίγουρα να υπάρχει ζευγάρι που να έχει άθροισμα 16;

4.4. Υποθέστε ότι ένα μάθημα διακριτών μαθηματικών παρακολουθείται από εννιά φοιτητές. Αποδείξτε ότι στο μάθημα υπάρχουν σίγουρα τουλάχιστον 5 αγόρια ή τουλάχιστον 5 κορίτσια. Αποδείξτε επίσης ότι στο μάθημα υπάρχουν σίγουρα τουλάχιστον 3 αγόρια ή τουλάχιστον 7 κορίτσια.

4.5. Δείξτε ότι αν υπάρχουν 101 άτομα με διαφορετικό ύψος το καθένα ένα, τα οποία στέκονται σε μια γραμμή, είναι δυνατό να βρεθούν 11 άτομα που στέκονται συνεχόμενα στην γραμμή και που τα ύψη τους αυξάνονται ή μειώνονται.

4.6. Ένα δίκτυο υπολογιστών αποτελείται από 6 υπολογιστές. Κάθε υπολογιστής συνδέεται με μηδέν ή και περισσότερους από τους άλλους υπολογιστές. Δείξτε ότι υπάρχουν δύο υπολογιστές που συνδέονται με το ίδιο πλήθος υπολογιστών.

4.7. Υποθέστε ότι διαθέτουμε καλώδια σύνδεσης υπολογιστών με εκτυπωτές. Βρείτε το μικρότερο αριθμό από καλώδια που εγγυάται ότι με όποιο τρόπο και αν συνδέσουμε 8 υπολογιστές με 4 εκτυπωτές, υπάρχουν τουλάχιστον 4 υπολογιστές που συνδέονται με τέσσερις διαφορετικούς εκτυπωτές. Υπολογίστε επίσης το ελάχιστο πλήθος από καλώδια ώστε να ισχύει το ίδιο για 100 υπολογιστές, 20 εκτυπωτές, και ώστε 20 υπολογιστές να συνδέονται με 20 διαφορετικούς εκτυπωτές.

4.8. Σ' ένα δρόμο με 101 σπίτια οι διευθύνσεις είναι από το 1 έως το 200. Δείξτε ότι υπάρχουν 2 γειτονικά σπίτια με αριθμούς που διαφέρουν κατά 1.

Υποθέστε ότι ο δρόμος έχει μόνο μια πλευρά και ότι αυτή η πλευρά περιέχει άρτιους και περιττούς αριθμούς.

4.9. Έστω ότι διαλέγουμε 101 τυχαίους αριθμούς στο διάστημα $[0, 1)$. Δείξτε ότι υπάρχουν δυο αριθμοί που διαφέρουν κατά το πολύ $1/100$.

4.10. Η Ελλάδα έχει πληθυσμό 11 εκατομμυρίων. Δείξτε ότι υπάρχει κάποια ημέρα του χρόνου που 50 τουλάχιστον κάτοικοι της Ελλάδας έχουν γενέθλια και επιπλέον όλοι έχουν τα ίδια αρχικά γράμματα (ονόματος και επωνύμου).

4.11. Δείξτε, με χρήση της Αρχής του Περιστερώνα, ότι σε κάθε ομάδα n ανθρώπων, όπου $n > 1$, υπάρχουν δυο άνθρωποι που έχουν τον ίδιο αριθμό γνωστών. Υποθέτουμε ότι οι γνωριμίες είναι αμοιβαίες (αν ο X γνωρίζει τον Y , τότε και ο Y γνωρίζει τον X).

4.12. Κατασκευάστε ακολουθία 16 φυσικών αριθμών που δεν έχει αύξουσα ή φθίνουσα υπακολουθία 5 στοιχείων. Γενικεύστε για ακολουθία

n^2 φυσικών αριθμών που δεν έχει αύξουσα ή φθίνουσα υπακολουθία $n + 1$ στοιχείων.

4.13. Ποιο είναι το ελάχιστο πλήθος από φοιτητές του Πανεπιστημίου Αθηνών, κάθε ένας από τους οποίους κατάγεται από έναν από τους 51 νομούς της Ελλάδας, που εγγυάται ότι σίγουρα υπάρχουν 100 φοιτητές που κατάγονται από τον ίδιο νομό.

4.14. Θεωρείστε τη συνάρτηση που ορίζεται από το παρακάτω πρόγραμμα

```
int f(int n)
  int m
  m=(29*n^755+529*n^541+2^(734*n^2+1)+73) mod 2006
  if m>=1000 then m=n
  if m=0 then m=1
  return m
```

Δείξτε ότι υπάρχουν δυο διαφορετικές τιμές n_1, n_2 στο $\{0, 1, \dots, 999\}$ για τις οποίες το πρόγραμμα επιστρέφει την ίδια τιμή, δηλαδή, $f(n_1) = f(n_2)$.

4.15. Δείξτε πως κάθε γράφος που έχει $n > 2$ κόμβους και m ακμές, όπου $m > n(n - 1)/3$, περιέχει ένα τουλάχιστον τρίγωνο K_3 (δηλαδή 3 κόμβους που ενώνονται ανά 2 μεταξύ τους).

5 Η Μέθοδος της Διαγωνίου

Σε αυτό το κεφάλαιο θα ασχοληθούμε με τη Μέθοδο της Διαγωνίου ή Διαγωνοποίηση. Είναι μια μορφή απόδειξης ύπαρξης που μας επιτρέπει να δείξουμε ότι υπάρχουν στοιχεία που δεν ανήκουν σε ένα συγκεκριμένο σύνολο.

Η κλασική χρήση της Μεθόδου της Διαγωνίου, που πρωτοχρησιμοποιήθηκε από τον Georg Cantor, είναι για να δείξουμε ότι το σύνολο των πραγματικών αριθμών είναι ‘μεγαλύτερο’ από το σύνολο των φυσικών αριθμών. Αλλά τι σημαίνει ότι ένα άπειρο σύνολο είναι ‘μεγαλύτερο’ από ένα άλλο άπειρο σύνολο; Πρέπει να είμαστε προσεκτικοί και να ορίσουμε αυστηρά τις έννοιες. Αντί για τη σχέση ‘μεγαλύτερο’ θα επικεντρώσουμε την προσοχή μας στη σχέση ‘ίσο’. Για πεπερασμένα σύνολα είναι εύκολο να πούμε πότε δυο σύνολα έχουν το ίδιο πλήθος στοιχείων, τον ίδιο πληθικό αριθμό, όπως λέμε. Αλλά για άπειρα σύνολα;

Ορισμός 33. Λέμε ότι δυο σύνολα A και B έχουν το ίδιο πλήθος στοιχείων όταν υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των στοιχείων τους. Θα συμβολίζουμε τη σχέση αυτή με $|A| = |B|$.

Έτσι για παράδειγμα το σύνολο των φυσικών αριθμών έχει το ίδιο πλήθος στοιχείων με το σύνολο των άρτιων φυσικών αριθμών, όπως φαίνεται από την αμφιμονοσήμαντη αντιστοιχία $f : \mathbb{N} \rightarrow \{2, 4, 6, \dots\}$ με $f(n) = 2n$:

$$\begin{array}{cccc} 1 & 2 & 3 & \dots \\ \downarrow & \downarrow & \downarrow & \dots \\ 2 & 4 & 6 & \dots \end{array}$$

Αυτό σε πρώτη ματιά ίσως μας προκαλεί εντύπωση γιατί το σύνολο των άρτιων είναι γνήσιο υποσύνολο των φυσικών αριθμών. Πώς γίνεται να έχουν το ίδιο πλήθος στοιχείων; Μια απάντηση είναι ότι η διαίσθησή μας δεν είναι αρκετή για τα άπειρα σύνολα. Η σωστή απάντηση όμως είναι ότι είναι θέμα ορισμού. Ο Ορισμός 33 ορίζει με φυσικό τρόπο την ισότητα μεταξύ του πλήθους των στοιχείων δυο συνόλων. Δεν αναφέρε-

ται στο πότε ένα σύνολο έχει πλήθος στοιχείων μικρότερο ή μεγαλύτερο από κάποιο άλλο.

Ας ορίσουμε λοιπόν ότι ένα σύνολο A έχει πλήθος στοιχείων μικρότερο ή ίσο με το πλήθος στοιχείων ενός συνόλου B αν και μόνο αν το A έχει το ίδιο πλήθος στοιχείων με ένα υποσύνολο του συνόλου B . Θα συμβολίζουμε αυτή τη σχέση με $|A| \leq |B|$. Προσέξτε ότι αυτός είναι ένας απλός συμβολισμός. Η σχέση \leq δεν έχει τις ιδιότητες που έχει στους αριθμούς.

Όταν λοιπόν θα λέμε ότι το σύνολο των πραγματικών αριθμών \mathbb{R} είναι γνήσια 'μεγαλύτερο' από το σύνολο των φυσικών αριθμών \mathbb{N} , θα εννοούμε ότι

1. $|\mathbb{N}| \leq |\mathbb{R}|$, και ότι
2. δεν ισχύει $|\mathbb{N}| = |\mathbb{R}|$

Το πρώτο είναι προφανές αφού το σύνολο των φυσικών είναι υποσύνολο των πραγματικών. Το δεύτερο θα το δείξουμε παρακάτω, αφού πρώτα μελετήσουμε το πλήθος των φυσικών αριθμών.

5.1 Αριθμήσιμα σύνολα

Τα σύνολα που είναι πεπερασμένα ή έχουν τον ίδιο αριθμό στοιχείων με το σύνολο φυσικών αριθμών λέγονται αριθμήσιμα. Ένας εναλλακτικός ορισμός τους είναι ο εξής:

Ορισμός 34. Ένα σύνολο S λέγεται αριθμήσιμο ή μετρήσιμο (countable) αν είτε είναι πεπερασμένο είτε είναι άπειρο και υπάρχει ακολουθία r_1, r_2, \dots στην οποία να εμφανίζονται όλα τα στοιχεία του S .

Τα στοιχεία του S μπορούν να εμφανίζονται πολλές φορές στην ακολουθία r_1, r_2, \dots . Αν υπάρχει τέτοια ακολουθία, τότε θα υπάρχει και μια στην οποία κάθε στοιχείο του S εμφανίζεται ακριβώς μια φορά. Αυτή η ακολουθία προκύπτει αν διαγράψουμε από την r_1, r_2, \dots τις δεύτερες, τρίτες κλπ εμφανίσεις κάθε στοιχείου του S . Αν λοιπόν όλα τα στοιχεία είναι διαφορετικά μεταξύ τους, τότε η συνάρτηση $f(n) = r_n$, από το σύνολο \mathbb{N} στο σύνολο S είναι αμφιμονοσήμαντη (η εικόνα της περιέχει όλα τα στοιχεία του S και όλες οι εικόνες είναι διαφορετικές). Από αυτό προκύπτει ότι ο παραπάνω ορισμός είναι συμβατός με τον Ορισμό 33.

Οι φυσικοί και οι ακέραιοι είναι αριθμήσιμοι. Για να το δείξουμε αυτό αρκεί να βρούμε μια κατάλληλη ακολουθία που περιέχει όλα τα στοιχεία του κάθε συνόλου. Οι παρακάτω ακολουθίες έχουν την επιθυμητή ιδιότητα.

Φυσικοί (\mathbb{N}): 1, 2, 3, ...

Ακέρατοι (Z): $0, 1, -1, 2, -2, \dots$

Είναι αριθμήσιμο το σύνολο των θετικών ρητών \mathbb{Q}^+ , δηλαδή των κλασμάτων p/q με $p, q \in \mathbb{N}$; Ας προσπαθήσουμε να βάλουμε όλα τα κλάσματα σε σειρά ως εξής:

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \dots, \frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \dots, \frac{3}{1}, \dots$$

Δείχνει αυτή η σειρά ότι το σύνολο των θετικών ρητών είναι αριθμήσιμο; Όχι. Ας πάρουμε συγκεκριμένα το κλάσμα $\frac{2}{1}$. Ποια είναι η θέση του στην ακολουθία, ή ισοδύναμα πόσα στοιχεία είναι πριν από αυτό; Η απάντηση είναι 'άπειρα' και αυτό σημαίνει ότι η παραπάνω σειρά δεν είναι ακολουθία στην οποία εμφανίζεται το $\frac{2}{1}$.

Το γεγονός ότι η παραπάνω σειρά δεν είναι κατάλληλη ακολουθία δεν σημαίνει ότι το σύνολο των θετικών ρητών δεν είναι αριθμήσιμο. Θα δείξουμε τώρα ότι υπάρχει κατάλληλη ακολουθία. Για να κατασκευάσουμε μια κατάλληλη ακολουθία πρέπει να φροντίσουμε κάθε στοιχείο να εμφανίζεται στην ακολουθία. Υπάρχουν πολλοί τρόποι να το πετύχουμε, αλλά η βασική ιδέα είναι να βάλουμε πρώτα τα κλάσματα που έχουν μικρό αριθμητή και παρονομαστή (όχι μόνο μικρό αριθμητή, όπως κάναμε στην παραπάνω αποτυχημένη προσπάθεια). Να δυο τρόποι για να το πετύχουμε

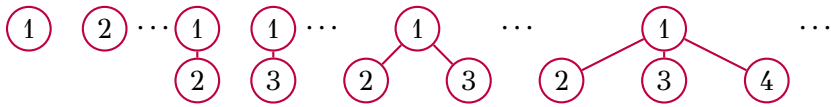
Θετικοί ρητοί (\mathbb{Q}^+): $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \dots$

Θετικοί ρητοί (\mathbb{Q}^+): $\frac{1}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \frac{3}{1}, \frac{3}{2}, \frac{3}{3}, \frac{3}{4}, \frac{4}{1}, \dots$

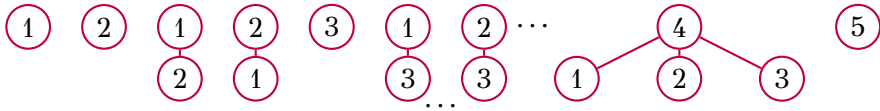
Στην πρώτη ακολουθία, εμφανίζονται πρώτα τα κλάσματα με άθροισμα αριθμητή και παρονομαστή ίσο με 2, μετά τα κλάσματα με άθροισμα αριθμητή και παρονομαστή ίσο με 3, κοκ. Ένα κλάσμα p/q θα εμφανιστεί όταν απαριθμούμε τα κλάσματα με άθροισμα αριθμητή και παρονομαστή ίσο με $p+q$. Επειδή το πλήθος των ζευγαριών των φυσικών αριθμών με άθροισμα το πολύ $p+q$ είναι το πολύ $(p+q)^2$, το κλάσμα p/q , θα εμφανιστεί στα πρώτα $(p+q)^2$ στοιχεία.

Στην δεύτερη ακολουθία, κάθε κλάσμα p/q ακολουθείται από το αντίστροφό του q/p . Αν παρατηρήσουμε μόνο τα κλάσματα στις περιττές θέσεις, διαπιστώνουμε ότι έχουν όλα αριθμητή μικρότερο ή ίσο με τον παρονομαστή και ότι πρώτα είναι τα όλα τα κλάσματα με παρονομαστή 1, μετά όλα τα κλάσματα με παρονομαστή 2, κοκ. Επομένως ένα κλάσμα p/q , με $p \leq q$, θα εμφανιστεί όταν απαριθμούνται τα κλάσματα με παρονομαστές q και ένα κλάσμα p/q , με $p > q$, θα εμφανιστεί αμέσως μετά το q/p .

Προσέξτε ότι κάθε θετικός ρητός εμφανίζεται πολλές φορές στην ακολουθία (για παράδειγμα ο $1/2$ εμφανίζεται και σαν $2/4$, $4/6$ κλπ.), αλλά όπως αναφέρθηκε παραπάνω αυτό είναι συμβατό με τον ορισμό των αριθμήσιμων συνόλων. Δεν είναι δύσκολο να τροποποιήσουμε τις



Σχήμα 5.1: Δένδρα σε σειρά.



Σχήμα 5.2: Μια ακολουθία που περιέχει όλα τα δένδρα με κόμβους στο \mathbb{N} .

παραπάνω ακολουθίες ώστε να περιέχουν και τους αρνητικούς ρητούς. Επομένως από τα παραπάνω συμπεραίνουμε ότι

Θεώρημα 35. Τα σύνολα των φυσικών, ακεραίων και ρητών αριθμών είναι αριθμήσιμα.

ΠΑΡΑΔΕΙΓΜΑ 5.1 (Δένδρα). Ας δούμε ένα ακόμα παράδειγμα αριθμήσιμου συνόλου. Θα δείξουμε ότι το σύνολο των πεπερασμένων δένδρων¹ είναι αριθμήσιμο. Όπως και στο Κεφάλαιο 3, θα θεωρήσουμε δένδρα με κόμβους από το σύνολο των φυσικών αριθμών. Μια πιθανή σειρά των δένδρων φαίνεται στο Σχήμα 5.1.

Αυτή όμως η σειρά των δένδρων δεν συνιστά ακολουθία στην οποία εμφανίζονται όλα τα δένδρα. Ας πάρουμε, για παράδειγμα, ένα δένδρο με 2 κόμβους. Πόσα δένδρα προηγούνται; Η απάντηση είναι ‘άπειρα’ και επομένως η σειρά δεν είναι κατάλληλη. Μια καλύτερη προσέγγιση είναι να κατασκευάσουμε πρώτα όλα τα δένδρα με σύνολο κόμβων το $\{1\}$, μετά όλα τα δένδρα με κόμβους στο $\{1, 2\}$, μετά όλα τα δένδρα με κόμβους στο $\{1, 2, 3\}$, κοκ (Σχήμα 5.2).

Πρόταση 36. Το σύνολο των πεπερασμένων δένδρων με κόμβους στο σύνολο των φυσικών αριθμών \mathbb{N} είναι αριθμήσιμο.

Σαν τελευταίο παράδειγμα αριθμήσιμου συνόλου, θα μελετήσουμε το σύνολο Σ^* των συμβολοσειρών ενός αλφαβήτου Σ .

¹Ένα δένδρο είναι πεπερασμένο αν ο αριθμός των κόμβων του είναι πεπερασμένος. Το βιβλίο αυτό πραγματεύεται μόνο τέτοια δένδρα.

ΠΑΡΑΔΕΙΓΜΑ 5.2 (Συμβολοσειρές). Θυμηθείτε ότι αλφάβητο είναι ένα οποιοδήποτε πεπερασμένο σύνολο. Έστω λοιπόν ένα αλφάβητο Σ και έστω Σ^* το σύνολο των συμβολοσειρών του. Για παράδειγμα, $\Sigma = \{0, 1\}$ και $\Sigma^* = \{\epsilon, 0, 1, 00, 01, 10, 11, \dots\}$. Είναι το σύνολο Σ^* αριθμήσιμο; Ναι, όπως προκύπτει από την ακολουθία που περιέχει πρώτα τις συμβολοσειρές με μήκος 0 (υπάρχει μόνο μια τέτοια συμβολοσειρά, η ϵ), μετά όλες τις συμβολοσειρές με μήκος 1, μετά όλες τις συμβολοσειρές με μήκος 2 κοκ. Για το παραπάνω παράδειγμα, η ακολουθία είναι

$$\epsilon, 0, 1, 00, 01, 10, 11, 000, \dots$$

Επειδή οι συμβολοσειρές με μήκος k είναι πεπερασμένες, μια συμβολοσειρά μήκους k θα εμφανιστεί τελικά στην ακολουθία αυτή.

Αντίθετα η σειρά των λεξικών δεν είναι κατάλληλη. Στα λεξικά εμφανίζονται πρώτα όλες οι συμβολοσειρές που αρχίζουν από α μετά οι συμβολοσειρές που αρχίζουν από β κοκ. Επειδή όμως οι συμβολοσειρές που αρχίζουν από α είναι άπειρες, μια συμβολοσειρά που αρχίζει από β δεν θα εμφανιστεί ποτέ σε αυτή τη σειρά. Στα πραγματικά λεξικά αυτό δεν είναι πρόβλημα, γιατί δεν περιέχουν όλες τις πιθανές συμβολοσειρές, αλλά μόνο ένα πεπερασμένο αριθμό λέξεων.

5.2 Η Μέθοδος της Διαγωνίου

Είναι όλα τα σύνολα αριθμήσιμα; Όπως αναφέραμε παραπάνω το σύνολο των πραγματικών αριθμών δεν είναι αριθμήσιμο. Αλλά πως δείχνουμε ότι ένα σύνολο δεν είναι αριθμήσιμο; Με τη Μέθοδο της Διαγωνίου ή Διαγωνιοποίηση.

Ας πούμε ότι μας δίνονται 5 5-ψηφιοι αριθμοί και μας ζητάνε αν βρούμε ένα 5-ψηφιο αριθμό διαφορετικό από αυτούς. Το πρόβλημα είναι ότι κάθε ψηφίο των 5 αριθμών είναι γραμμένο σε κάρτα που είναι αναποδογυρισμένη και θέλουμε να κοιτάξουμε όσο το δυνατόν λιγότερες κάρτες. Μια λύση είναι να ανοίξουμε τις κάρτες της διαγωνίου. Από αυτές μπορούμε να κατασκευάσουμε ένα νέο αριθμό που διαφέρει από τον 1ο αριθμό στο 1ο ψηφίο, από τον 2ο στο 2ο ψηφίο και γενικά από τον i -οστό στο i -στο ψηφίο. Στο παρακάτω παράδειγμα είμαστε σίγουροι ότι ο αριθμός 43066 δεν είναι ένας από τους 5 αριθμούς.

						3				
					⇒		2			
								9		
									5	
										5

Αυτή είναι η Μέθοδος της Διαγωνίου ή Διαγωνιοποίηση (Diagonalization). Στο παραπάνω παράδειγμα, η μέθοδος αποδεικνύει ότι υπάρχουν περισσότεροι από 5 5-ψηφιοι αριθμοί. Πράγματι, όποια και αν είναι τα

ψηφία της διαγωνίου, μπορούμε να βρούμε ένα 5-ψήφιο αριθμό που διαφέρει στο πρώτο ψηφίο από τον πρώτο αριθμό, στο δεύτερο ψηφίο από τον δεύτερο αριθμό κ.ο.κ. Άρα, όποιοι 5 αριθμοί και να υπάρχουν στις αναποδογυρισμένες κάρτες υπάρχει ένας ακόμα. Βέβαια, η παραπάνω πρόταση ότι υπάρχουν τουλάχιστον 6 5-ψήφιοι αριθμοί δεν μας εντυπωσιάζει, αφού γνωρίζουμε πολύ καλά ότι οι υπάρχουν 10^5 5-ψήφιοι αριθμοί. Αλλά η μέθοδος, που λέγεται Μέθοδος της Διαγωνίου είναι πιο γενική και έχει πολλές εφαρμογές στην Θεωρία Υπολογισμού. Χρησιμοποιήθηκε πρώτη φορά από τον Georg Cantor για να δείξει ότι οι πραγματικοί αριθμοί δεν είναι αριθμήσιμοι.

5.3 Οι πραγματικοί αριθμοί

Το παρακάτω θεώρημα μπορεί να ερμηνευτεί και ως: ‘Οι πραγματικοί αριθμοί είναι περισσότεροι από τους φυσικούς’.

Θεώρημα 37. Το σύνολο των πραγματικών αριθμών \mathbb{R} δεν είναι αριθμήσιμο, δηλαδή δεν υπάρχει ακολουθία r_1, r_2, \dots στην οποία να εμφανίζονται όλοι οι πραγματικοί αριθμοί.

Απόδειξη. Με εις άτοπο απαγωγή. Έστω ότι υπήρχε τέτοια ακολουθία r_1, r_2, \dots . Ας θεωρήσουμε τη δεκαδική παράσταση των αριθμών αυτών και ας κατασκευάσουμε ένα αριθμό που διαφέρει από τον r_1 στο πρώτο δεκαδικό ψηφίο, από τον r_2 στο δεύτερο δεκαδικό ψηφίο, κ.ο.κ. Πιο συγκεκριμένα κατασκευάζουμε τον αριθμό a με δεκαδική παράσταση $0.a_1a_2a_3\dots$ όπου

$$a_i = \begin{cases} 1 & \text{αν το } i\text{-στο δεκαδικό ψηφίο του } r_i \text{ είναι διάφορο του } 1 \\ 2 & \text{αν το } i\text{-στο δεκαδικό ψηφίο του } r_i \text{ είναι ίσο με } 1 \end{cases}$$

Για παράδειγμα, αν

$$r_1 = 0.06542\dots$$

$$r_2 = 1.11287\dots$$

$$r_3 = 3.14159\dots$$

$$r_4 = 1.41421\dots$$

τότε $a = 0.1221\dots$

Ο νέος αριθμός a έχει διαφορετική δεκαδική παράσταση από κάθε αριθμό της ακολουθίας r_1, r_2, \dots . Είναι όμως διαφορετικός από κάθε r_i ; Η απάντηση είναι καταφατική αλλά πρέπει να είμαστε προσεκτικοί γιατί υπάρχουν πραγματικοί αριθμοί που έχουν δυο δεκαδικές

παραστάσεις. Πιο συγκεκριμένα κάποιοι αριθμοί έχουν δυο δεκαδικές παραστάσεις που από κάποιο σημείο και πέρα αποτελούνται από επαναλαμβανόμενα 0 ή από επαναλαμβανόμενα 9. Για παράδειγμα $1.20000\dots = 1.19999\dots$. Αλλά φροντίσαμε τα νέα ψηφία a_i να μην περιέχουν ούτε 0 ούτε 9. Έτσι ο νέος αριθμός a , όχι μόνο έχει διαφορετική δεκαδική παράσταση αλλά είναι και διαφορετικός από κάθε r_i .

Ο a είναι πραγματικός αριθμός αλλά δεν ανήκει στην ακολουθία r_1, r_2, \dots , άτοπο. \square

5.4 Υπολογισιμότητα

Πολλά από τα αποτελέσματα της Θεωρίας Υπολογισμού δείχνονται με τη Μέθοδο της Διαγωνίου. Εδώ θα δείξουμε ότι δεν υπάρχει πρόγραμμα Pascal ή C ή οποιασδήποτε γενικής γλώσσας υπολογισμού που να μπορεί να αναλύει τον πηγαίο κώδικα προγραμμάτων της γλώσσας και να απαντά αν τερματίζει ή όχι όταν εκτελεστεί.

Ο πηγαίος κώδικας ενός προγράμματος για μας εδώ δεν θα είναι παρά μια συμβολοσειρά (δηλαδή ένα κείμενο) κάποιου αλφάβητου Σ . Θα θεωρήσουμε προγράμματα που παίρνουν για είσοδο μια συμβολοσειρά του Σ . Έστω P_1, P_2, \dots τα προγράμματα αυτά. Προσέξτε, ότι τα προγράμματα είναι συμβολοσειρές, άρα είναι αριθμήσιμα, δηλαδή μπορούν να μπου σε σειρά P_1, P_2, \dots (π.χ. πρώτα τα προγράμματα με 1 σύμβολο, μετά τα προγράμματα με 2 σύμβολα κοκ).

Ένα τέτοιο πρόγραμμα μπορεί να τερματίζει ή όχι. Τι θα κάνουν τα προγράμματα αν τους δώσουμε για είσοδο τους πηγαίους κώδικες;

Ας ορίσουμε την συνάρτηση

$$g(P_i, P_j) = \begin{cases} \text{true} & \text{αν το πρόγραμμα } P_i \text{ τερματίζει με είσοδο} \\ & \text{τη συμβολοσειρά } P_j \\ \text{false} & \text{σε κάθε άλλη περίπτωση} \end{cases}$$

και ας γεμίσουμε με τις τιμές της τον παρακάτω άπειρο πίνακα

	P_1	P_2	P_3	P_4	P_5
P_1	$g(P_1, P_1)$	$g(P_1, P_2)$	$g(P_1, P_3)$	$g(P_1, P_4)$	
P_2	
P_3	$g(P_3, P_4)$	
P_4	
P_5	

Χρησιμοποιώντας τώρα τη Μέθοδο της Διαγωνίου θεωρούμε τη γραμμή που έχει αντίστροφες τιμές από αυτές της διαγωνίου (από true σε false και το αντίστροφο). Η γραμμή που κατασκευάζεται με αυτό τον τρόπο, έχει στην i -οστή θέση true αν και μόνο αν $g(P_i, P_i) = \text{false}$. Η γραμμή αυτή δεν υπάρχει στον πίνακα γιατί διαφέρει από την 1η γραμμή στην 1η θέση, από τη 2η γραμμή στη 2η θέση κοκ. Δηλαδή, δεν

υπάρχει πρόγραμμα που να υπολογίζει το " $\text{not } g(P_i, P_i)$ ". Ισοδύναμα, δεν υπάρχει πρόγραμμα H τέτοιο ώστε για κάθε συμβολοσειρά P_i

το H με είσοδο P_i τερματίζει
αν και μόνο αν
το πρόγραμμα P_i με είσοδο P_i δεν τερματίζει.

Αυτό είναι το βασικό συμπέρασμα που η Μέθοδος της Διαγωνίου μας επιτρέπει να δείξουμε με τόσο εύκολο τρόπο. Από αυτό συμπεραίνουμε ότι δεν υπάρχει αλγόριθμος για το πρόβλημα:

Δίνεται πρόγραμμα P και είσοδος w . Τερματίζει το P με είσοδο w ;

Πράγματι αν υπήρχε αλγόριθμος γι' αυτό, θα μπορούσαμε να υπολογίσουμε αν το P_i τερματίζει με είσοδο τον πηγαίο κώδικά του, $w = P_i$.

Είναι ενδιαφέρον να παρατηρήσουμε ότι δεν χρησιμοποιήσαμε καμία ιδιότητα της έννοιας 'τερματίζει' στην απόδειξη. Η απόδειξη, για παράδειγμα, δουλεύει και αν αντικαταστήσουμε τη λέξη 'τερματίζει' με την έκφραση 'τυπώνει 17'.

Εναλλακτικά, αντί για τη Μέθοδο της Διαγωνίου, θα μπορούσαμε άμεσα να δούμε γιατί δεν υπάρχει πρόγραμμα H τέτοιο ώστε για κάθε συμβολοσειρά P_i

το H με είσοδο P_i τυπώνει 17
αν και μόνο αν
το πρόγραμμα P_i με είσοδο P_i δεν τυπώνει 17

αν αναρωτηθούμε τι θα έκανε ένα τέτοιο πρόγραμμα H αν του δίνουμε για είσοδο τον πηγαίο κώδικά του, αν δηλαδή αντικαταστήσουμε το P_i με H στην παραπάνω ισοδυναμία. Τότε,

το H με είσοδο H τυπώνει 17
αν και μόνο αν
το πρόγραμμα H με είσοδο H δεν τυπώνει 17.

Άτοπο, άρα τέτοιο πρόγραμμα H δεν υπάρχει.

Η Μέθοδος της Διαγωνίου μας επιτρέπει να κάνουμε μια άμεση απόδειξη, χωρίς να χρειάζεται να ανακαλύψουμε τέτοια 'παράδοξα' σχήματα.

Ασκήσεις

5.1. Δείξτε ότι κάθε υποσύνολο ενός αριθμήσιμου συνόλου είναι αριθμήσιμο.

5.2. Έστω δυο αριθμήσιμα σύνολα A και B . Δείξτε ότι το σύνολο $A \cup B$ είναι επίσης αριθμήσιμο.

5.3. Δείξτε ότι αν δυο σύνολα A_1 και A_2 είναι αριθμήσιμα, τότε και το καρτεσιανό γινόμενο τους

$$A = \{(a_1, a_2) : a_1 \in A_1 \text{ και } a_2 \in A_2\}$$

είναι επίσης αριθμήσιμο.

5.4. Θεωρείστε τα υποσύνολα των φυσικών αριθμών με πληθικό αριθμό 3: για παράδειγμα $\{1, 2, 3\}$ ή $\{4, 6, 10\}$. Δείξτε ότι το σύνολο όλων αυτών των υποσυνόλων είναι αριθμήσιμο.

5.5. Θεωρείστε το σύνολο όλων των υποσυνόλων των φυσικών αριθμών

$$P(\mathbb{N}) = \{S : S \subset \mathbb{N}\}.$$

Χρησιμοποιείστε τη Μέθοδο της Διαγωνίου για να δείξετε ότι το σύνολο $P(\mathbb{N})$ δεν είναι αριθμήσιμο.

Ποια η διαφορά με την προηγούμενη άσκηση;

5.6. Έστω F το σύνολο των συναρτήσεων με πεδίο ορισμού το σύνολο των φυσικών αριθμών και με πεδίο τιμών επίσης το σύνολο των φυσικών αριθμών. Δείξτε ότι το σύνολο F δεν είναι αριθμήσιμο.

5.7. Είναι τα παρακάτω σύνολα αριθμήσιμα ή όχι; Αποδείξτε την απάντησή σας.

1. Το σύνολο των συναρτήσεων με πεδίο ορισμού τους φυσικούς \mathbb{N} και πεδίο τιμών το $\{0, 1\}$.
2. Το σύνολο των συναρτήσεων με πεδίο ορισμού το $\{0, 1\}$ και πεδίο τιμών τους φυσικούς \mathbb{N} .

5.8. Θεωρείστε το σύνολο των υποσυνόλων των φυσικών αριθμών που έχουν πληθικό αριθμό 3: $S_3 = \{\{x, y, z\} : x, y, z \in \mathbb{N} \text{ και } x < y < z\}$. (Οι ανισότητες εγγυώνται ότι τα x, y, z είναι διαφορετικά μεταξύ τους.).

1. Δείξτε ότι το σύνολο S_3 είναι αριθμήσιμο.
2. Εξηγήστε προσεκτικά που βρίσκεται το λάθος στην παρακάτω απόδειξη:

Απόδειξη. Θα χρησιμοποιήσουμε τη μέθοδο της Διαγωνίου για να δείξουμε ότι το σύνολο S_3 δεν είναι αριθμήσιμο. Έστω ότι ήταν αριθμήσιμο. Τότε θα υπήρχε ακολουθία A_1, A_2, \dots που περιέχει κάθε σύνολο που αποτελείται από 3 φυσικούς αριθμούς. Θα κατασκευάσουμε ένα νέο υποσύνολο B με 3 στοιχεία που διαφέρει από κάθε A_i . Πιο συγκεκριμένα, το B θα περιέχει το στοιχείο i αν και μόνο αν το A_i δεν περιέχει το στοιχείο i . Έτσι, το σύνολο B διαφέρει από το σύνολο A_i στο στοιχείο i . Αφού το B διαφέρει από κάθε A_i δεν ανήκει στην ακολουθία A_1, A_2, \dots . Άτοπο. Επομένως η υπόθεση ότι το S_3 είναι αριθμήσιμο δεν ισχύει. \square

5.9. Δείξτε ότι το σύνολο των γλωσσών ενός αλφαβήτου Σ δεν είναι αριθμήσιμο. Θυμηθείτε πως γλώσσες ονομάζονται τα υποσύνολα του συνόλου των συμβολοσειρών του Σ .

5.10. Είναι τα παρακάτω σύνολα αριθμήσιμα ή όχι; Αποδείξτε προσεκτικά τις απαντήσεις σας.

1. $P = \{a : a \text{ είναι αριθμητική ακολουθία φυσικών αριθμών}\}$
2. $Q = \{a : a \text{ είναι αύξουσα ακολουθία φυσικών αριθμών}\}$
3. $Q = \{a : a \text{ είναι εναλλασόμενη ακολουθία φυσικών αριθμών}\}$

Αριθμητική ακολουθία: Για κάθε i , $a_{i+1} - a_i = c$ για κάποια σταθερά c .
Π.χ. 2, 5, 8, 11, 14, ..., όπου $c = 3$.

Εναλλασόμενη ακολουθία: Για κάθε i , $(a_{i+2} - a_{i+1})(a_{i+1} - a_i) < 0$. Π.χ. 3, 2, 4, 1, 6, 2, ...

5.11. Είναι τα παρακάτω σύνολα αριθμήσιμα ή όχι; Αποδείξτε προσεκτικά τις απαντήσεις σας.

1. $I = \{f : f \text{ είναι αύξουσα συνάρτηση από το } \mathbb{Z}_0^+ \text{ στο } \mathbb{Z}_0^+\}$
Παράδειγμα: Η συνάρτηση

$$f(n) = \begin{cases} n & \text{αν } n \text{ είναι περιττός} \\ n+1 & \text{αν } n \text{ είναι άρτιος} \end{cases}$$

ανήκει στο I .

2. $D = \{f : f \text{ είναι φθίνουσα συνάρτηση από το } \mathbb{Z}_0^+ \text{ στο } \mathbb{Z}_0^+\}$
Παράδειγμα: Η συνάρτηση

$$f(n) = \left\lceil \frac{10}{n+1} \right\rceil$$

ανήκει στο D .

5.12. Δείξτε ότι τα σύνολα των πραγματικών αριθμών δυο διαστημάτων $[a, b]$ με $b > a$ και $[c, d]$ με $d > c$ έχουν το ίδιο πλήθος στοιχείων. Δώστε μια κατάλληλη αμφιμονοσήμαντη αντιστοιχία.

5.13. Δώστε μια 1-1 συνάρτηση f από το σύνολο των σημείων του τετραγώνου $S = \{(x, y) : x, y \in [0, 1)\}$ στο σύνολο των σημείων του διαστήματος $I = \{z : z \in [0, 1)\}$. Προσέξτε ότι η συνάρτηση f δεν χρειάζεται να είναι επί του I αλλά μόνο 1-1, δηλαδή αρκεί να έχουμε

$$x \neq x' \text{ είτε } y \neq y' \implies f(x, y) \neq f(x', y').$$

Από αυτό συμπεραίνουμε ότι το (τετράγωνο) S έχει πλήθος στοιχείων ίσο με ένα υποσύνολο του (διαστήματος) I . Αυτό μπορεί να επεκταθεί, αν και δεν είναι ζητούμενο της άσκησης, στο ότι το επίπεδο έχει το ίδιο πλήθος στοιχείων με τη γραμμή. Σαν συνέπεια αυτού, το σύνολο μιγαδικών αριθμών \mathbb{C} έχει το ίδιο πλήθος στοιχείων με το σύνολο των πραγματικών αριθμών \mathbb{R} .

6 Διακριτή Πιθανότητα

Η Θεωρία Πιθανοτήτων έχει άμεση σχέση με την επιστήμη της Πληροφορικής. Φαντάζει αντιφατική αυτή η παρατήρηση δεδομένου ότι οι υπολογισμοί έχουν νομοτελειακή φύση σε αντίθεση με τις πιθανότητες. Αλλά είναι τέτοια στενή η σχέση των δυο περιοχών, που η πλειοψηφία των επιστημονικών δημοσιεύσεων στην περιοχή των αλγορίθμων και της υπολογιστικής πολυπλοκότητας προσεγγίζουν τα θέματα τους σε μικρό ή μεγάλο βαθμό πιθανοτικά (ή όπως αλλιώς λέμε, στοχαστικά).

Οι πιθανότητες παίζουν πολύ μεγάλο ρόλο στη θεωρία πληροφορίας, στην τεχνητή νοημοσύνη, στη θεωρία παιγνίων και σε πολλές άλλες περιοχές. Στη θεωρία αλγορίθμων και υπολογισμού, η θεωρία πιθανοτήτων αποτελεί τη βάση των πιθανοτικών ή στοχαστικών αλγορίθμων. Αυτοί οι αλγόριθμοι υπερτερούν των ντετερμινιστικών αλγορίθμων γιατί είναι συνήθως πιο γρήγοροι και πιο απλοί. Τελευταία, υπάρχει έντονο ενδιαφέρον για την ειδική κατηγορία πιθανοτικών αλγορίθμων, τους κβαντικούς αλγόριθμους, που εκμεταλλεύονται κβαντικά φαινόμενα. Αν και έχουμε μακρύ δρόμο μέχρι να κατασκευάσουμε κβαντικούς υπολογιστές και να υλοποιήσουμε τέτοιους αλγόριθμους, η έρευνα προς αυτή την κατεύθυνση έχει ενταθεί μετά τη εφεύρεση γρήγορων κβαντικών αλγορίθμων που σπάνε πολλά σημερινά κρυπτογραφικά συστήματα (μέσω της γρήγορης παραγοντοποίησης ακεραίων).

6.1 Δειγματικοί χώροι και πιθανότητα

Εδώ θα μελετήσουμε κυρίως στοχαστικές διαδικασίες που αφορούν πεπερασμένους χώρους, π.χ. όταν ρίχνουμε ένα ζάρι 100 φορές. Για τέτοιες διαδικασίες οι πιο κοινές ερωτήσεις που θέλουμε να απαντήσουμε είναι της μορφής

- Ποιά η πιθανότητα να συμβεί το δεινό γεγονός;
- Ποιά η αναμενόμενη τιμή της τάδε τυχαίας μεταβλητής;

Η απάντηση στην πρώτη ερώτηση είναι μία πιθανότητα (ένας αριθμός στο διάστημα $[0, 1]$) και στη δεύτερη περίπτωση ένας πραγματικός αριθμός. Γενικά, οι ερωτήσεις του δευτέρου είδους είναι πιο εύκολες από τις ερωτήσεις του πρώτου είδους.

Οι πιθανότητες πεπερασμένων χώρων, οι διακριτές πιθανότητες όπως αλλιώς τις λέμε, ορίζονται σε ένα πεπερασμένο δειγματικό χώρο Δ . Ο δειγματικός χώρος είναι όλα τα πιθανά αποτελέσματα ενός πειράματος. Σε κάθε δείγμα δ , δηλαδή σε κάθε στοιχείο $\delta \in \Delta$, αντιστοιχούμε μια πιθανότητα, δηλαδή ένα μη αρνητικό αριθμό $\Pr(\delta)$. Το άθροισμα των πιθανοτήτων όλων των δειγμάτων είναι ίσο με 1: $\sum_{\delta \in \Delta} \Pr(\delta) = 1$. Το ζεύγος $(\Delta, \Pr : \Delta \mapsto [0, 1])$ ορίζει απόλυτα το στοχαστικό πείραμα.

Τα υποσύνολα του δειγματικού χώρου τα ονομάζουμε γεγονότα. Ορίζουμε την πιθανότητα ενός γεγονότος $\Gamma \subseteq \Delta$ σαν το άθροισμα των πιθανοτήτων των δειγμάτων του: $\Pr(\Gamma) = \sum_{\delta \in \Gamma} \Pr(\delta)$.

Σε αντίθεση με τους παραπάνω απλούς και διαισθητικούς ορισμούς της διακριτής πιθανότητας, ο ορισμός της πιθανότητας άπειρων δειγματικών χώρων κρύβει παγίδες και γι' αυτό μόλις σχετικά πρόσφατα (το 1930) βρέθηκε μια ικανοποιητική αξιωματικοποίησή της, από τον Kolmogorov.

Όταν έχουμε να αντιμετωπίσουμε ένα πρόβλημα πιθανοτήτων, η παρακάτω διαδικασία βοηθά να το απλοποιήσουμε και να αποφύγουμε τις παγίδες.

1. Βρίσκουμε το δειγματικό χώρο.

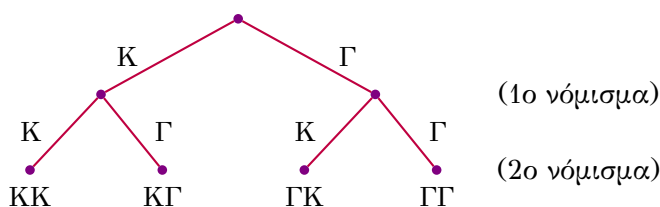
Για παράδειγμα, αν έχουμε το πρόβλημα της μορφής 'Ρίχνουμε 2 νομίσματα, το καθένα με πιθανότητα p να φέρει K (κεφαλή) και $1 - p$ να φέρει Γ (γράμματα). Ποια η πιθανότητα ...;' Ποιος είναι ο δειγματικός χώρος, δηλαδή το σύνολο όλων των πιθανών αποτελεσμάτων του πειράματος;

Μπορούμε να τον προσδιορίσουμε σαν το σύνολο $\{KK, K\Gamma, \Gamma K, \Gamma\Gamma\}$, όπου το πρώτο σύμβολο είναι το αποτέλεσμα του πρώτου νομίσματος και το δεύτερο σύμβολο το αποτέλεσμα του δεύτερου νομίσματος. Ή μήπως ο δειγματικός χώρος είναι το σύνολο $\{KK, K\Gamma, \Gamma\Gamma\}$; Σ' αυτή την περίπτωση δεν ξεχωρίζουμε τα νομίσματα σε πρώτο και δεύτερο, αλλά βλέπουμε μόνο το σύνολο τους.

Ποιός είναι λοιπόν ο δειγματικός χώρος; Και οι δύο απαντήσεις είναι αποδεκτές σαν δειγματικοί χώροι. Αλλά, μόνο ο πρώτος δειγματικός χώρος αντανακλά με ακρίβεια το πείραμα. Ο δεύτερος δειγματικός χώρος θα μας βάλει σε μελάδες αν δεν είμαστε προσεκτικοί. Ποια είναι για παράδειγμα η πιθανότητα του δείγματος $K\Gamma$ στο δεύτερο δειγματικό χώρο; Για να αποφύγουμε τέτοια προβλήματα, αναλύουμε τα πειράματα σε βήματα. Για παράδειγμα, χωρίς βλάβη της γενικότητας, το παραπάνω πείραμα γίνεται ως εξής: πρώτα ρίχνουμε το ένα νόμισμα και μετά το άλλο. Αυτή η διαδικασία δείχνεται στο δένδρο του Σχήματος 6.1.

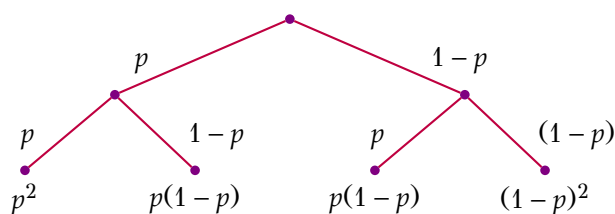
Ο δειγματικός χώρος αντιστοιχεί στα φύλλα του δένδρου.

2. Αποδίδουμε πιθανότητες σε κάθε δείγμα.



Σχήμα 6.1: Ο δειγματικός χώρος δυο νομισμάτων

Οι πιθανότητες του παραπάνω παραδείγματος φαίνονται στο δένδρο του Σχήματος 6.2.



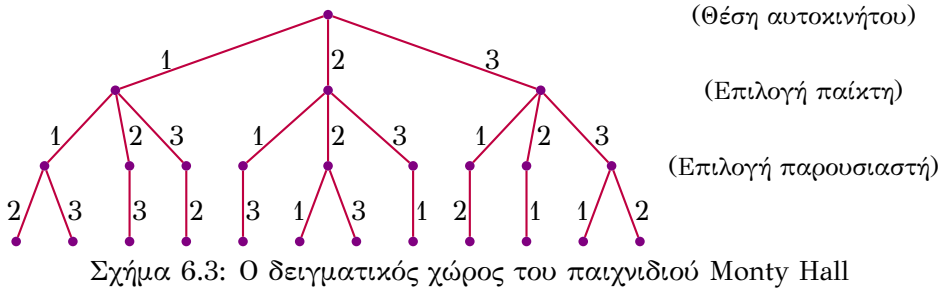
Σχήμα 6.2: Πιθανότητες δυο νομισμάτων

3. Προσδιορίζουμε ποιό γεγονός μας ενδιαφέρει. Για παράδειγμα, αν η ερώτηση είναι 'Ποιά η πιθανότητα ότι τα δύο νομίσματα είναι ίσα;', τότε το γεγονός είναι $\{ΚΚ, ΓΓ\}$ και η πιθανότητά του είναι $p^2 + (1-p)^2$.

ΠΑΡΑΔΕΙΓΜΑ 6.1 (Το Monty Hall πρόβλημα). Σε ένα τηλεπαιχνίδι υπάρχουν 3 πόρτες. Πίσω από τη μια πόρτα βρίσκεται ένα αυτοκίνητο ενώ πίσω από τις άλλες δυο μια κατσίκα. Ο παίκτης θέλει να διαλέξει την πόρτα με το αυτοκίνητο αλλά δεν γνωρίζει ποιά είναι αυτή. Διαλέγει λοιπόν μια πόρτα. Τότε ο παρουσιαστής του παιχνιδιού ανοίγει μια από τις άλλες δυο πόρτες που έχει από πίσω της κατσίκα και δίνει την δυνατότητα στον παίκτη να αλλάξει επιλογή αν θέλει. Τι πρέπει να κάνει ο παίκτης; Να επιμείνει στην αρχική του επιλογή ή να προτιμήσει τη τρίτη πόρτα;

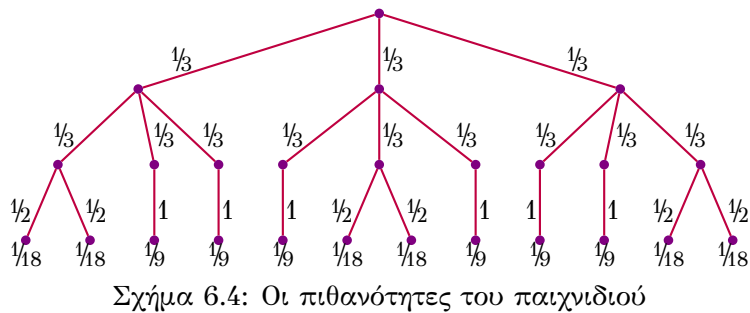
Για να απαντήσουμε, ας κάνουμε μερικές υποθέσεις που απλοποιούν τους υπολογισμούς. Η απάντηση δεν επηρεάζεται από αυτές τις απλοποιήσεις αλλά είναι πιο πολύπλοκο να επιχειρηματολογήσουμε χωρίς τις απλοποιήσεις. Υποθέτουμε λοιπόν ότι

- το αυτοκίνητο βρίσκεται πίσω από μια τυχαία πόρτα
- ο παίκτης στην αρχή διαλέγει μια τυχαία πόρτα.
- ο παρουσιαστής διαλέγει μια τυχαία πόρτα με κατσίκα από πίσω (όταν υπάρχουν δυο τέτοιες πόρτες).



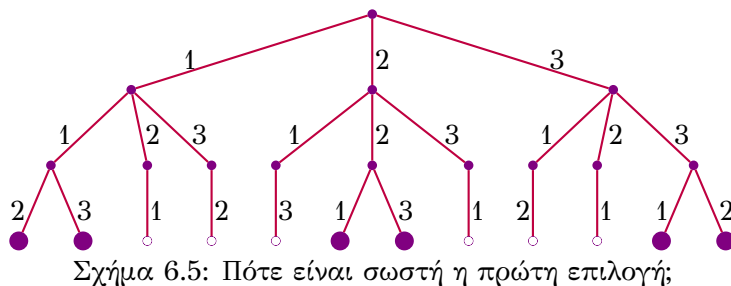
Χρησιμοποιώντας την παραπάνω μεθοδολογία ορίζουμε τον δειγματικό χώρο με το δένδρο του Σχήματος 6.3.

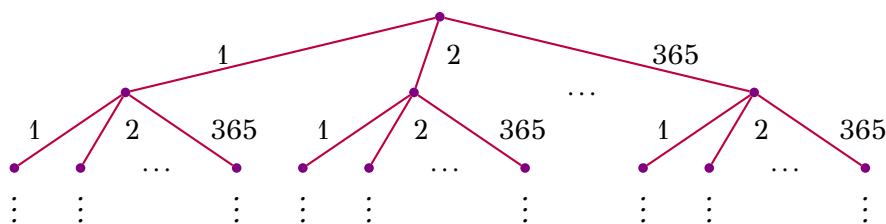
Ορίζουμε τώρα τις πιθανότητες κάθε δείγματος όπως στο Σχήμα 6.4.



Η ερώτηση που θέλουμε να απαντήσουμε είναι ποιά η πιθανότητα να κερδίσει ο παίκτης αν επιμείνει στην πρώτη του επιλογή. Το γεγονός αυτό φαίνεται στο Σχήμα 6.5, όπου τα δείγματα του γεγονότος σημειώνονται πιο έντονα.

Παρατηρούμε ότι η πιθανότητα να κερδίσει αν επιμείνει στην πρώτη του επιλογή είναι μόνο $6 \cdot \frac{1}{18} = \frac{1}{3}$. Αυτή είναι βέβαια η ίδια πιθανότητα που είχε πριν ο παρουσιαστής ανοίξει την άλλη πόρτα! Επομένως η καλύτερη στρατηγική για τον παίκτη είναι να διαλέξει την άλλη πόρτα, με πιθανότητα επιτυχίας $\frac{2}{3}$.





Σχήμα 6.6: Ο δειγματικός χώρος των γενεθλίων

Το αποτέλεσμα αυτό έρχεται σε αντίθεση με τη διαίσθηση πολλών ανθρώπων. Ίσως βοηθάει να πειστούμε ότι η καλύτερη στρατηγική είναι να διαλέξουμε την άλλη πόρτα, ας θεωρήσουμε το ίδιο παιχνίδι με 10 αντί για 3 πόρτες. Όπως και στο αρχικό παιχνίδι, ο παίκτης διαλέγει μια πόρτα. Τώρα όμως ο παρουσιαστής ανοίγει όλες τις άλλες πόρτες εκτός από μία. Τι πρέπει να κάνει ο παίκτης; Αν επιμένει στην αρχική του επιλογή, η πιθανότητα επιτυχίας είναι $1/10$ (τόση είναι η πιθανότητα να πετύχει την σωστή πόρτα αρχικά και αυτό δεν αλλάζει από το πως εξελίσσεται το παιχνίδι). Αν διαλέξει την άλλη πόρτα, η πιθανότητα επιτυχίας είναι βέβαια $1 - 1/10 = 9/10$.

ΠΑΡΑΔΕΙΓΜΑ 6.2 (Το πρόβλημα των γενεθλίων). Ας θεωρήσουμε μια ομάδα με n ανθρώπους. Ποιά η πιθανότητα να υπάρχουν τουλάχιστον δυο με κοινά γενέθλια;

Για να έχει νόημα η ερώτηση χρειάζεται να κάνουμε κάποιες υποθέσεις για την κατανομή των μελών της ομάδας. Για να απλοποιήσουμε τους υπολογισμούς υποθέτουμε

- Κάθε έτος έχει 365 ημέρες. Ισοδύναμα, υποθέτουμε ότι κανένα μέλος της ομάδας δεν έχει γενέθλια την 29 Φεβρουαρίου.
- Όλες οι ημέρες είναι το ίδιο πιθανές¹.
- Τα μέλη της ομάδας δεν έχουν καμμία σχέση μεταξύ τους, έτσι ώστε τα γενέθλια τους είναι ανεξάρτητα μεταξύ τους.

Κατασκευάζουμε τώρα το δειγματικό χώρο όπως στο Σχήμα 6.6.

Ο δειγματικός χώρος είναι πολύ μεγάλος και η παραπάνω αναπαράσταση δεν βοηθάει πολύ. Μας δίνει όμως αρκετή πληροφορία για να συμπεράνουμε πως ο δειγματικός χώρος είναι

$$\{(1, 1, \dots, 1), (1, 1, \dots, 1, 365), \dots, (365, 365, \dots, 365)\},$$

¹Αυτό δεν είναι αλήθεια όπως δείχνουν τα στατιστικά στοιχεία. Για παράδειγμα, κάποιοι γονείς και γιατροί καθυστερούν τον τοκετό την 31η Δεκεμβρίου, ώστε το παιδί να γεννηθεί μετά τα μεσάνυχτα. Επίσης, ελάχιστα από τα παιδιά που γεννιούνται με καισαρική έχουν γενέθλια την 25η Δεκεμβρίου.

όπου κάθε δείγμα αποτελείται από μια ακολουθία n στοιχείων του συνόλου $\{1, 2, \dots, 365\}$. Όλοι οι συνδυασμοί των 365 αριθμών ανήκουν στον δειγματικό χώρο. Υπάρχουν 365^n δείγματα και είναι όλα ισοπίθανα. Επομένως η πιθανότητα κάθε δείγματος είναι $1/365^n$. Το γεγονός που μας ενδιαφέρει είναι το σύνολο των δειγμάτων στα οποία δυο τουλάχιστον μέλη έχουν κοινά γενέθλια, ή ισοδύναμα αυτά που περιέχουν δυο ίδιους αριθμούς.

Πόσα δείγματα περιέχει το γεγονός; Συχνά στον υπολογισμό πιθανοτήτων η απάντηση φαίνεται πολύ πιο απλή αν θεωρήσουμε το συμπληρωματικό γεγονός. Έτσι ας ρωτήσουμε ‘Ποιά η πιθανότητα να έχουν όλοι διαφορετικά γενέθλια;’ Ο πρώτος μπορεί να έχει τα γενέθλια του οποιαδήποτε ημέρα του χρόνου. Ο δεύτερος οποιαδήποτε ημέρα εκτός από τα γενέθλια του πρώτου. Ο τρίτος εκτός οποιαδήποτε ημέρα εκτός από τα γενέθλια του πρώτου και του δεύτερου κ.ο.κ. Δηλαδή ο αριθμός των δειγμάτων είναι $365 \cdot 364 \cdot 363 \cdots (366 - n)$. Αφού το κάθε δείγμα έχει πιθανότητα $1/365^n$, η πιθανότητα να έχουν όλοι διαφορετικά γενέθλια είναι

$$\frac{365 \cdot 364 \cdot 363 \cdots (366 - n)}{365^n}.$$

Μόλις προσδιορίσουμε το πλήθος n των ανθρώπων, μπορούμε να υπολογίσουμε ακριβώς την πιθανότητα αυτή. Αλλά όπως συμβαίνει στην ανάλυση των στοχαστικών φαινομένων, μας ενδιαφέρει μια απλή απάντηση ακόμα και αν πρέπει να εγκαταλείψουμε την ακρίβεια και να αρκεστούμε με μια προσεγγιστική απάντηση. Για να απλοποιήσουμε την παραπάνω έκφραση χρησιμοποιούμε την προσέγγιση $e^x \approx 1 + x$ για μικρά (θετικά ή αρνητικά) x . Ξαναγράφουμε λοιπόν την παραπάνω πιθανότητα σαν

$$\begin{aligned} \frac{365 \cdots (366 - n)}{365^n} &\approx \left(1 - \frac{0}{365}\right) \cdot \left(1 - \frac{1}{365}\right) \cdots \left(1 - \frac{n-1}{365}\right) \\ &= e^{-\frac{0}{365}} \cdot e^{-\frac{1}{365}} \cdots e^{-\frac{n-1}{365}} \\ &= e^{-\frac{n(n-1)}{2 \cdot 365}} \\ &\approx e^{-\frac{n^2}{730}} \end{aligned}$$

Αν ο αριθμός των ανθρώπων είναι $n = 23$ η πιθανότητα να έχουν διαφορετικά γενέθλια είναι περίπου $e^{-23^2/730} \approx 0.5$. Άρα σε μια τυχαία ομάδα 23 ανθρώπων η πιθανότητα να υπάρχουν δυο με κοινά γενέθλια είναι περίπου 0.5.

6.2 Τυχαίες μεταβλητές και αναμενόμενη τιμή

Πολλές φορές σε προβλήματα που έχουν πιθανότητες μας ενδιαφέρει η αριθμητική τιμή μιας ποσότητας. Για να μοντελοποιήσουμε τέτοιες

ερωτήσεις, το κατάλληλο μέσο είναι οι τυχαίες μεταβλητές. Μια τυχαία μεταβλητή δεν είναι τίποτα άλλο παρά η απόδοση τιμών σε κάθε δείγμα ενός δειγματικού χώρου Δ . Πιο συγκεκριμένα, μια τυχαία μεταβλητή X είναι απλά μια συνάρτηση $X: \Delta \mapsto \mathbb{R}$. Συνήθως, από σύμβαση, χρησιμοποιούμε κεφαλαία γράμματα για να συμβολίσουμε τυχαίες μεταβλητές.

Για παράδειγμα, όταν ρίχνουμε ένα αμερόληπτο (τίμιο) νόμισμα, ο δειγματικός χώρος είναι $\{K, \Gamma\}$. Σ' αυτό το δειγματικό χώρο μπορούμε να ορίσουμε πολλές τυχαίες μεταβλητές ανάλογα με το ποια ποσότητα μας ενδιαφέρει. Αν, για παράδειγμα, κερδίζουμε ή χάνουμε ένα ευρώ ανάλογα αν έρθει K ή Γ , τότε μια τυχαία μεταβλητή Y που εκφράζει το κέρδος μας παίρνει δυο τιμές, 1 και -1. Αν ακολουθήσουμε πιστά τον ορισμό της τυχαίας μεταβλητής σαν συνάρτηση από τον δειγματικό χώρο στους πραγματικούς αριθμούς, έχουμε $Y(K) = 1$ και $Y(\Gamma) = -1$. Επιπλέον, η πιθανότητα η τυχαία μεταβλητή Y να πάρει την τιμή 1 ή -1 είναι ακριβώς η πιθανότητα του γεγονότος K ή Γ . Έτσι $\Pr(Y = 1) = 1/2$ και $\Pr(Y = -1) = 1/2$.

Μια κατηγορία τυχαίων μεταβλητών, που είναι συνήθως πολύ χρήσιμες, είναι οι χαρακτηριστικές μεταβλητές του κάθε δείγματος. Αν δ είναι ένα δείγμα, τότε η τυχαία μεταβλητή X που δηλώνει αν θα συμβεί το γεγονός δ λέγεται χαρακτηριστική τυχαία μεταβλητή. Η τυχαία αυτή μεταβλητή παίρνει τιμή 1 για το δ ($X(\delta) = 1$) και 0 διαφορετικά. Για το παράδειγμα με το ένα νόμισμα, η τυχαία μεταβλητή X με $X(K) = 1$ και $X(\Gamma) = 0$ είναι η χαρακτηριστική τυχαία μεταβλητή του δείγματος K .

Ας δούμε ένα ακόμα παράδειγμα τυχαίας μεταβλητής όταν ρίχνουμε ένα νόμισμα 10 φορές και μας ενδιαφέρει ο αριθμός των κεφαλών που θα έρθουν. Ορίζουμε την τυχαία μεταβλητή X να είναι ακριβώς ο αριθμός των κεφαλών σε κάθε δείγμα. Το κάθε δείγμα σε αυτή την περίπτωση είναι μια ακολουθία από 10 σύμβολα K και Γ . Έτσι, για παράδειγμα, $X(KKKK\Gamma\Gamma KKKK\Gamma) = 7$.

Η αναμενόμενη ή μέση τιμή $E[X]$ μιας τυχαίας μεταβλητής X ορίζεται σαν

$$E[X] = \sum_{\delta \in \Delta} \Pr(\delta) \cdot X(\delta).$$

Από τον ορισμό μπορούμε αμέσως αν συμπεράνουμε ένα απλό αλλά πανίσχυρο θεώρημα.

Θεώρημα 38. Για οποιεσδήποτε τυχαίες μεταβλητές X_1, \dots, X_n

$$E[X_1 + \dots + X_n] = E[X_1] + \dots + E[X_n].$$

Απόδειξη. Έστω $X = X_1 + \dots + X_n$. Έχουμε

$$\begin{aligned} E[X] &= \sum_{\delta \in \Delta} \Pr(\delta) \cdot X(\delta) \\ &= \sum_{\delta \in \Delta} \Pr(\delta) \cdot (X_1(\delta) + \dots + X_n(\delta)) \\ &= \sum_{\delta \in \Delta} \Pr(\delta) \cdot X_1(\delta) + \dots + \sum_{\delta \in \Delta} \Pr(\delta) \cdot X_n(\delta) \\ &= E[X_1] + \dots + E[X_n] \end{aligned}$$

□

ΠΑΡΑΔΕΙΓΜΑ 6.3 (Αθροισμα ζαριών). Ρίχνουμε δυο ζάρια; Ποιά είναι η αναμενόμενη τιμή του αθροίσματος τους;

Ορίζουμε τις τυχαίες μεταβλητές X_1, X_2 να είναι ίσες με το αποτέλεσμα του πρώτου και του δεύτερου ζαριού. Μας ενδιαφέρει η αναμενόμενη τιμή της τυχαίας μεταβλητής $X = X_1 + X_2$.

Βρίσκουμε πρώτα την αναμενόμενη τιμή της X_1 .

$$E[X_1] = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \dots + \frac{1}{6} \cdot 6 = \frac{7}{2}.$$

Προφανώς η X_2 έχει την ίδια αναμενόμενη τιμή και επομένως η τιμή του αθροίσματος είναι $E[X] = 7/2 + 7/2 = 7$.

6.3 Ανεξαρτησία

Δυο ή περισσότερες τυχαίες μεταβλητές λέγονται ανεξάρτητες αν η πιθανότητα η μια τυχαία μεταβλητή να πάρει κάποια συγκεκριμένη τιμή δεν επηρεάζεται από την τιμή που παίρνουν οι άλλες τυχαίες μεταβλητές. Πιο συγκεκριμένα:

Ορισμός 39. Οι τυχαίες μεταβλητές X_1, \dots, X_n λέγονται ανεξάρτητες αν για κάθε $v_1, \dots, v_n \in \mathbb{R}$:

$$\Pr(X_1 = v_1 \wedge \dots \wedge X_n = v_n) = \Pr(X_1 = v_1) \cdots \Pr(X_n = v_n).$$

Η ανεξαρτησία παίζει πολύ μεγάλο ρόλο γιατί διευκολύνει τους υπολογισμούς. Χωρίς την έννοια της ανεξαρτησίας οι διακριτές πιθανότητες δεν θα διέφεραν ουσιαστικά από την συνδυαστική ανάλυση. Το παρακάτω θεώρημα βοηθά συχνά στον υπολογισμό αναμενόμενων τιμών.

Θεώρημα 40. Αν οι τυχαίες μεταβλητές X_1, \dots, X_n είναι ανεξάρτητες τότε

$$E[X_1 \cdots X_n] = E[X_1] \cdots E[X_n].$$

Για να αποδείξουμε το θεώρημα θα χρησιμοποιήσουμε το επόμενο λήμμα που υπολογίζει την αναμενόμενη τιμή μιας τυχαίας μεταβλητής X , όχι ως άθροισμα ως προς το πεδίο ορισμού της ($E[X] = \sum_{\delta \in \Delta} \Pr(\delta) \cdot X(\delta)$), αλλά ως άθροισμα ως προς το πεδίο τιμών της ($E[X] = \sum_{v \in X(\Delta)} \Pr(X = v) \cdot v$), όπου $X(\Delta) = \{X(\delta) : \delta \in \Delta\}$ συμβολίζει το πεδίο τιμών της τυχαίας μεταβλητής X (που ας μην ξεχνάμε, πρόκειται για συνάρτηση). Αφού το Δ το θεωρούμε πεπερασμένο, το $X(\Delta)$ είναι επίσης πεπερασμένο.

Λήμμα 41. Για κάθε τυχαία μεταβλητή X : $E[X] = \sum_{v \in X(\Delta)} \Pr(X = v) \cdot v$.

Η απόδειξη του λήμματος αφήνεται για άσκηση (Άσκηση 6.1). Μπορούμε τώρα να αποδείξουμε το Θεώρημα 40.

Απόδειξη Θεωρήματος 40. Για απλότητα θα δείξουμε το θεώρημα για δυο τυχαίες μεταβλητές. Με τον ίδιο τρόπο μπορούμε να το δείξουμε για περισσότερες τυχαίες μεταβλητές.

Έστω $X = X_1 \cdot X_2$. Από το Λήμμα 41 έχουμε

$$\begin{aligned} E[X] &= \sum_{v \in X(\Delta)} \Pr(X = v) \cdot v \\ &= \sum_{v_1 \in X_1(\Delta), v_2 \in X_2(\Delta)} \Pr(X_1 = v_1 \wedge X_2 = v_2) \cdot v_1 \cdot v_2 \\ &= \sum_{v_1 \in X_1(\Delta), v_2 \in X_2(\Delta)} \Pr(X_1 = v_1) \cdot \Pr(X_2 = v_2) \cdot v_1 \cdot v_2 \\ &= \left(\sum_{v_1 \in X_1(\Delta)} \Pr(X_1 = v_1) \cdot v_1 \right) \cdot \left(\sum_{v_2 \in X_2(\Delta)} \Pr(X_2 = v_2) \cdot v_2 \right) \\ &= E[X_1] \cdot E[X_2]. \end{aligned}$$

□

ΠΑΡΑΔΕΙΓΜΑ 6.4 (Ρίψεις νομίσματος). Ένα από τα πιο απλά αλλά πολύ σημαντικά πειράματα είναι να ρίξουμε n φορές ένα νόμισμα, με πιθανότητα p να φέρει Κ(εφαλή) και πιθανότητα $1-p$ να φέρει Γ(ράμματα). Οι ερωτήσεις που μας ενδιαφέρουν είναι της μορφής:

1. Ποιος ο αναμενόμενος αριθμός των K;
2. Ποιά η πιθανότητα να έρθει K ακριβώς m φορές;
3. Ποιά η πιθανότητα να έρθει K τουλάχιστον k φορές;

Η πρώτη ερώτηση είναι πράγματι εύκολη αλλά ας την εκφράσουμε πρώτα πιο αυστηρά. Έστω X_1, \dots, X_n είναι τυχαίες μεταβλητές. Η X_i παίρνει τιμή 1 αν στην i -οστή ρίψη έρθει K και τιμή 0 αν έρθει Γ.

$$X_i = \begin{cases} 1 & \text{αν η } i\text{-στή ρίψη είναι K} \\ 0 & \text{αν η } i\text{-στή ρίψη είναι Γ} \end{cases}$$

Υποθέτουμε ότι οι ρίψεις δεν επηρεάζουν η μια την άλλη, δηλαδή ότι οι τυχαίες μεταβλητές X_1, \dots, X_n είναι ανεξάρτητες. Η πρώτη ερώτηση είναι ισοδύναμη με 'ποια είναι η αναμενόμενη τιμή της τυχαίας μεταβλητής $X_1 + \dots + X_n$;

Για να βρούμε την αναμενόμενη τιμή $E[X_1 + \dots + X_n] = E[X_1] + \dots + E[X_n]$ αρκεί να βρούμε την αναμενόμενη τιμή της X_1 , αφού $E[X_1] = \dots = E[X_n]$. Από τον ορισμό της αναμενόμενης τιμής, έχουμε $E[X_1] = p \cdot 1 + (1-p) \cdot 0 = p$. Άρα η απάντηση στην πρώτη ερώτηση, δηλαδή ο αναμενόμενος αριθμός των K, είναι np .

Η απάντηση στην δεύτερη ερώτηση είναι επίσης εύκολη αν χρησιμοποιήσουμε λίγη συνδυαστική ανάλυση. Τα δείγματα του πειράματος είναι όλες οι ακολουθίες από n σύμβολα K ή Γ. Υπάρχουν $\binom{n}{m}$ τέτοιες ακολουθίες με ακριβώς m K. Κάθε τέτοιο δείγμα έχει πιθανότητα $p^m(1-p)^{n-m}$. Επομένως η απάντηση στο δεύτερο ερώτημα, η πιθανότητα να έρθει K ακριβώς m φορές, είναι $\binom{n}{m}p^m(1-p)^{n-m}$.

Όπως αναφέραμε παραπάνω, στις πιθανότητες και ιδιαίτερα στις εφαρμογές τους στην πληροφορική, μας ενδιαφέρει η απάντηση να έχει απλή (κλειστή) μορφή ακόμα και αν χρειαστεί να μην είναι ακριβής αλλά προσεγγιστική. Χρησιμοποιώντας μεθόδους του απειροστικού λογισμού μπορούμε να προσεγγίσουμε την πιθανότητα πολύ καλά:

$$\binom{n}{m}p^m(1-p)^{n-m} \approx \frac{e^{-\frac{(m-np)^2}{2p(1-p)n}}}{\sqrt{\pi} \sqrt{2p(1-p)n}}.$$

Ειδικά για αμερόληπτα νομίσματα, δηλαδή αν $p = 1/2$, η παραπάνω έκφραση γίνεται $\frac{e^{-\frac{2(m-n/2)^2}{n}}}{\sqrt{\pi n/2}}$. Για παράδειγμα, αν ρίξουμε το νόμισμα $n = 100$ φορές η ακριβής πιθανότητα να έρθουν $m = 60$ K είναι $\binom{100}{60}2^{-100} = 0.010844 \dots$, όχι πολύ διαφορετική από την παραπάνω προσέγγιση που δίνει $\frac{e^{-2}}{\sqrt{50\pi}} = 0.010798 \dots$

Η ακριβής έκφραση δεν είναι τόσο σημαντική όσο η παρατήρηση ότι ο έκθετης $(m - n/2)^2/n$ χαρακτηρίζει την πιθανότητα. Αν ο αριθμός των K είναι πολύ μακριά από την αναμενόμενη τιμή, δηλαδή αν το $|m - n/2|$

είναι πολύ μεγαλύτερο από \sqrt{n} , τότε ο εκθέτης του e στον αριθμητή είναι ένας μεγάλος αρνητικός αριθμός και η πιθανότητα είναι πάρα πολύ μικρή. Με άλλα λόγια, όταν ρίχνουμε ένα αμερόληπτο νόμισμα n φορές, με μεγάλη πιθανότητα ο αριθμός των κεφαλών βρίσκεται στο διάστημα $[n/2 - c\sqrt{n}, n/2 + c\sqrt{n}]$, όταν το c είναι κάποια σταθερά. Καθώς το c μεγαλώνει, η πιθανότητα πέφτει εκθετικά. Για παράδειγμα, για $c = 1$ η πιθανότητα είναι 0.95 και για $c = 2$ η πιθανότητα είναι περίπου 0.9999.

Το παραπάνω απαντάει επίσης την τρίτη ερώτηση, δηλαδή ποιά η πιθανότητα να έρθουν τουλάχιστον k Κ. Αν μας ενδιέφερε η ακριβής τιμή, τότε η απάντηση είναι $\sum_{m=k}^n \binom{n}{m} p^m (1-p)^{n-m}$.

ΠΑΡΑΔΕΙΓΜΑ 6.5 (Πιθανοτικοί αλγόριθμοι). Οι πιθανοτικοί αλγόριθμοι χρησιμοποιούν τυχαία bits ή τυχαίους αριθμούς. Θεωρητικά δεν διαφέρουν από τους ντετερμινιστικούς αλγορίθμους παρά μόνο στο ότι, εκτός από την είσοδό τους, τους δίνεται επιπλέον μια μεγάλη (ουσιαστικά άπειρη) ακολουθία από bits. Υπάρχουν διάφορων ειδών πιθανοτικοί αλγόριθμοι. Εδώ θα ασχοληθούμε με τους Monte Carlo αλγόριθμους. Ένας αλγόριθμος λέγεται Monte Carlo (α) αν είναι αλγόριθμος απόφασης, δηλαδή που η έξοδος του είναι 0 (όχι) ή 1 (ναι), και (β) κάνει λάθη μόνο προς μια κατεύθυνση. Πιο συγκεκριμένα, αν η σωστή απάντηση είναι 1, τότε ο αλγόριθμος απαντάει πάντα σωστά, αλλά αν η σωστή απάντηση είναι 0 τότε απαντάει σωστά με πιθανότητα $1/2$, τουλάχιστον.

Για να κάνουμε πιο συγκεκριμένο τον ορισμό και να ‘απομυθοποιήσουμε’ την έννοια ‘πιθανοτικός’ αλγόριθμος ας δώσουμε ένα ακριβή ορισμό. Έστω $A(x, r)$ ένας ντετερμινιστικός αλγόριθμος, όπου x είναι η είσοδος και r μια ακολουθία από bits. Ο αλγόριθμος $A(x, r)$ λέγεται ένας αλγόριθμος Monte Carlo που υπολογίζει τη συνάρτηση $f(x)$ αν για κάθε x :

α') αν $f(x) = 1$, τότε για κάθε r : $A(x, r) = 1$

β') αν $f(x) = 0$, τότε για τουλάχιστον τα μισά r : $A(x, r) = 0$.

Προσέξτε ότι σ' αυτόν τον ορισμό δεν υπάρχει τίποτα πιθανοτικό. Οι πιθανότητες μπαίνουν στο παιχνίδι όταν εμείς διαλέγουμε ένα τυχαίο r για να τρέξουμε τον αλγόριθμο. Προσέξτε επίσης ότι αν τρέξουμε πολλές φορές τον αλγόριθμο με την ίδια είσοδο x και ανεξάρτητα τυχαία r , οι απαντήσεις θα είναι ανεξάρτητες.

Είναι χρήσιμος ένας τέτοιος αλγόριθμος; Γιατί δεν ζητάμε να είναι η πιθανότητα λάθους μικρότερη από $1/2$; Η απάντηση είναι ότι αν τρέξουμε τον αλγόριθμο αρκετές φορές μπορούμε να κάνουμε την πιθανότητα λάθους πολύ μικρή (πρακτικά 0).

Πράγματι, έστω ότι τρέχουμε ένα αλγόριθμο Monte Carlo n φορές. Αν απαντήσει έστω και μία φορά 0 τότε είμαστε σίγουροι ότι η σωστή απάντηση είναι 0. Διαφορετικά, δηλαδή όταν όλες οι n απαντήσεις είναι 1, δεχόμαστε σαν απάντηση το 1, αλλά υπάρχει η πιθανότητα λάθους. Πόσο μεγάλη είναι η πιθανότητα λάθους; Επειδή οι n απαντήσεις είναι

ανεξάρτητες, η πιθανότητα λάθους είναι $1/2^n$. Για $n = 100$, η πιθανότητα είναι τόσο μικρή που πρακτικά μπορούμε να την αγνοήσουμε (είναι ας πούμε πολύ μικρότερη από την πιθανότητα να καταστραφεί ο υπολογιστής στη διάρκεια εκτέλεσης του αλγορίθμου).

ΠΑΡΑΔΕΙΓΜΑ 6.6 (Το πρόβλημα των κουπονιών). Οι περισσότεροι από μας μάλλον έχουν συμμετάσχει σε ‘παιχνίδια’ συλλογής κουπονιών: Υπάρχουν n είδη κουπονιών και ο σκοπός είναι να μαζέψεις ένα από κάθε είδος. Πολλές φορές επίσης έχουμε την εντύπωση ότι το παιχνίδι δεν είναι τίμιο, δηλαδή ότι τα κουπόνια δεν έχουν ομοιόμορφη κατανομή, αφού το τελευταίο ή προτελευταίο κουπόνι δεν φαίνεται να υπάρχει. Είναι όμως έτσι; Ας αναλύσουμε αυτό το πείραμα, που εμφανίζεται πολλές φορές σε προβλήματα πιθανοτικών αλγορίθμων.

Το πείραμα λοιπόν είναι το εξής: Υπάρχουν n είδη και κάθε φορά διαλέγουμε τυχαία και ομοιόμορφα ένα είδος. Το ερώτημα είναι πόσες φορές πρέπει να επαναλάβουμε τη διαδικασία ώστε να βρούμε όλα τα είδη. Πιο συγκεκριμένα, ο αριθμός των κουπονιών είναι μια τυχαία μεταβλητή X . Μπορούμε να ρωτήσουμε

- Ποιά είναι η αναμενόμενη τιμή $E[X]$ της X ;
- Ποιά η πιθανότητα ότι η X είναι μεγαλύτερη από κάποιο δεδομένο φράγμα c , δηλαδή $\Pr(X \geq c)$;

Θα υπολογίσουμε την απάντηση στην πρώτη ερώτηση, αλλά υπάρχει ένα γενικότερο θέμα εδώ. Αν ξέραμε την απάντηση στην πρώτη ερώτηση, τι μπορούμε να πούμε για τη δεύτερη ερώτηση; Με άλλα λόγια, υπάρχει τρόπος να φράξουμε την πιθανότητα στη δεύτερη ερώτηση αν γνωρίζουμε την αναμενόμενη τιμή; Η απάντηση είναι καταφατική και μας πηγαίνει κατευθείαν στην καρδιά της ανάλυσης πολλών στοχαστικών διαδικασιών. Υπάρχουν τέτοια φράγματα, όπως η Ανισότητα του Markov και η Ανισότητα του Chebyshev.

Αλλά ας γυρίσουμε στο πρώτο ερώτημα. Για να βρούμε τον αναμενόμενο αριθμό χωρίζουμε τη διαδικασία σε φάσεις. Έστω X_1, \dots, X_n τυχαίες μεταβλητές, όπου X_i εκφράζει τον αριθμό των βημάτων για να βρούμε το i -στο κουπόνι. Μας ενδιαφέρει ο συνολικός αριθμός βημάτων $X = X_1 + \dots + X_n$. Διαισθητικά, όσο περισσότερα κουπόνια έχουμε, τόσο πιο πολύ παίρνει να βρούμε το επόμενο νέο κουπόνι, δηλαδή $E[X_{i+1}] > E[X_i]$.

Το $E[X_i]$ είναι η αναμενόμενη τιμή των βημάτων του πειράματος: Υπάρχουν n είδη κουπονιών από τα οποία $i - 1$ έχουν ήδη βρεθεί. Η πιθανότητα να πετύχουμε ένα νέο κουπόνι είναι $p_i = (n - (i - 1))/n$. Αν πετύχουμε σταματάμε· αν αποτύχουμε επαναλαμβάνουμε το ίδιο πείραμα. Επομένως $E[X_i] = 1 + (1 - p_i)E[X_i]$ που έχει τη λύση $E[X_i] = 1/p_i$ (αν θέλουμε να είμαστε αυστηροί πρέπει επίσης να δείξουμε ότι η $E[X_i]$ υπάρχει, δηλαδή ότι δεν είναι άπειρη). Αυτό είναι από τα πιο κοινά πειράματα και λέμε ότι η X_i ακολουθεί τη γεωμετρική κατανομή.

Ο αναμενόμενος αριθμός βημάτων για να βρούμε το πρώτο κουπόνι είναι $1/p_1 = 1$, το δεύτερο κουπόνι $1/p_2 = n/(n-1) \approx 1$, αλλά το προτελευταίο κουπόνι $1/p_2 = n/2$ και το τελευταίο κουπόνι $1/p_n = n$. Αυτό εξηγεί μερικώς γιατί έχουμε την αίσθηση ότι τα παιχνίδια κουπονιών δεν είναι πάντα τίμια.

Μπορούμε τώρα να υπολογίσουμε τον συνολικό αναμενόμενο αριθμό βημάτων

$$E[X] = \frac{n}{n} + \frac{n}{n-1} + \dots + \frac{n}{1} = n\left(\frac{1}{n} + \frac{1}{n-1} + \dots + \frac{1}{1}\right) = nH_n \approx n \ln n.$$

Ασκήσεις

6.1. Αποδείξτε το Λήμμα 41.

6.2. Δώστε ένα παράδειγμα δυο τυχαίων μεταβλητών για τις οποίες δεν ισχύει $E[X_1 \cdot X_2] = E[X_1] \cdot E[X_2]$.

Άσκηση 1. Έστω X μια τυχαία μεταβλητή που παίρνει μόνο τιμές στους φυσικούς αριθμούς, δηλαδή για κάθε δείγμα δ , $X(\delta) \in \mathbb{N}$. Δείξτε ότι για κάθε θετικό αριθμό $a > 1$: $\Pr(X \geq a) \leq \frac{E[X]-1}{a} - 1$.

6.3. Έστω ότι έχετε ένα πιθανοτικό αλγόριθμο A για ένα πρόβλημα απόφασης (δηλαδή ένα πρόβλημα που οι απαντήσεις είναι ‘ναι’ και ‘όχι’) που για κάθε είσοδο δίνει τη σωστή απάντηση με πιθανότητα τουλάχιστον $3/4$.

1. Θέλουμε να τρέξουμε τον αλγόριθμο πολλές φορές ώστε να αυξήσουμε την πιθανότητα σωστής απάντησης σε $15/16$; Εξηγήστε με ακρίβεια πως θα το κάνουμε αυτό και πόσες φορές πρέπει να τρέξουμε τον αλγόριθμο A .
 2. Γενικεύστε την προηγούμενη απάντηση για την περίπτωση που θέλουμε να αυξήσουμε την πιθανότητα σωστής απάντησης στο $1-\epsilon$, για κάποιο μικρό θετικό ϵ .
- 6.4. Έστω ότι έχουμε ένα πιθανοτικό αλγόριθμο A που για κάθε είσοδο x :

- Αν η σωστή απάντηση για την είσοδο x είναι ‘ναι’, τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά ‘ναι’) με πιθανότητα $1/2$.
- Αν η σωστή απάντηση για την είσοδο x είναι ‘όχι’, τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά ‘όχι’) με πιθανότητα $9/10$.

Πως μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο A ώστε να κατασκευάσουμε ένα αλγόριθμο που δίνει την σωστή απάντηση—ανεξάρτητα αν η σωστή απάντηση είναι ‘ναι’ ή ‘όχι’—με πιθανότητα τουλάχιστον $3/4$;

6.5. Κατασκευάζουμε ένα τυχαίο κανονικό δυαδικό δένδρο ξεκινώντας από μια ρίζα και επαναλαμβάνοντας τον εξής κανόνα:

Σε κάθε νέο κόμβο u του δένδρου, με πιθανότητα p προσθέτουμε 2 παιδιά στον u , ενώ με πιθανότητα $1-p$ ο u παραμένει για πάντα φύλλο.

Στην αρχή βέβαια υπάρχει μόνο ένας νέος κόμβος του δένδρου, η ρίζα του.

Αν $p < 1/2$, υπολογίστε τον αναμενόμενο αριθμό των κόμβων του δένδρου (σαν συνάρτηση του p).

6.6. Έστω ότι ρίχνουμε b μπαλάκια σε n δοχεία. Το κάθε μπαλάκι ρίχνεται με ομοιόμορφη κατανομή στα δοχεία και ανεξάρτητα από τα υπόλοιπα μπαλάκια. Υπολογίστε την πιθανότητα ότι κανένα δοχείο δεν περιέχει δυο ή περισσότερα μπαλάκια όταν

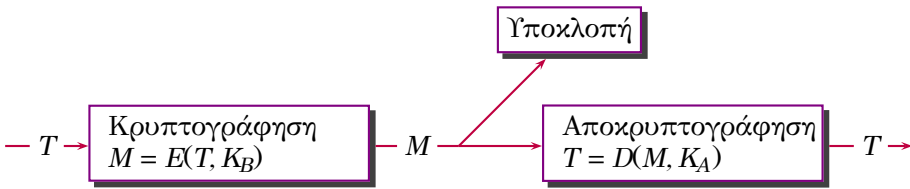
1. $b = 2$
2. $b = n$.
3. $b = n + 1$.

7 RSA και πρώτοι αριθμοί

Η σημασία της κρυπτογραφίας έχει αυξηθεί δραματικά τα τελευταία χρόνια. Η κρυπτογραφία ήταν μια στρατιωτική κυρίως εφαρμογή αλλά έχει εξελιχθεί σε βασικό παράγοντα της οικονομικής ζωής.

Το τυπικό σκηνικό έχει ως εξής: Έστω ότι ο Βασίλης θέλει να στείλει ένα μυστικό μήνυμα T στην Αλίκη και έστω ότι κάποιος κρυφακούει στη γραμμή επικοινωνίας τους και μπορεί να μάθει όλα τα μηνύματα που ανταλλάσσουν ο Βασίλης και η Αλίκη. Για να μην μπορεί κάποιος ενδιάμεσος να βρει το μήνυμα T , ο Βασίλης θα το κρυπτογραφήσει. Θα χρησιμοποιήσει μια συνάρτηση κρυπτογράφησης K και θα υπολογίσει την τιμή $K(T)$. Την τιμή αυτή $K(T)$, που θα τη συμβολίσουμε με M , τη στέλνει στην Αλίκη. Όταν η Αλίκη πάρει το μήνυμα M , θα υπολογίσει την αντίστροφη συνάρτηση $A(M)$ για να βρει το αρχικό μήνυμα $T = A(M)$. Επειδή το μήνυμα M μπορεί να το διαβάσει και κάποιος τρίτος, που προσπαθεί να υποκλέψει την πληροφορία που ανταλλάσσουν η Αλίκη και ο Βασίλης, πρέπει η συνάρτηση κρυπτογράφησης K να έχει κάποιες επιθυμητές ιδιότητες. Η πιο βασική ιδιότητα είναι να μην μπορεί κάποιος να υπολογίσει το T από το $M = K(T)$. Υπάρχουν και άλλες επιθυμητές ιδιότητες, όπως για παράδειγμα να μην μπορεί κάποιος να υποκριθεί ότι είναι ο Βασίλης ή να πλαστογραφήσει μηνύματα, αλλά δεν θα μας απασχολήσουν σ' αυτό το κεφάλαιο.

Το βασικό πρόβλημα στην κρυπτογραφία είναι να βρεθεί κατάλληλη οικογένεια συναρτήσεων κρυπτογράφησης, και κατά συνέπεια κατάλληλη οικογένεια συναρτήσεων αποκρυπτογράφησης. Για να απλοποιηθεί αλλά και για να συγκεκριμενοποιηθεί αυτή η αναζήτηση, περιορίζουμε τις οικογένειες συναρτήσεων σε παραμετρικές οικογένειες. Δηλαδή, μια συνάρτηση κρυπτογράφησης έχει την μορφή $E(T, K_B)$, όπου K_B μια παράμετρος που λέγεται κλειδί κρυπτογράφησης. Παρόμοια, η συνάρτηση αποκρυπτογράφησης έχει τη μορφή $T = D(M, K_A)$, όπου K_A μια παράμετρος που λέγεται κλειδί αποκρυπτογράφησης. Στο Σχήμα 7.1 φαίνεται ένα τυπικό περιβάλλον κρυπτογράφησης-αποκρυπτογράφησης. Οι συναρτήσεις E και D καθορίζουν τις οικογένειες των συναρτήσεων κρυπτογράφησης και αποκρυπτογράφησης. Στην ανάλυση των κρυπτογραφικών συστημάτων θεωρούμε ότι οι E και D θεωρούνται γνωστές σε όλους, με βάση τη επιχειρήμα ότι οι καλές οικογένειες συναρτήσεων κρυπτογράφησης και αποκρυπτογράφησης είναι λίγες και γνωστές σε όλους.



Σχήμα 7.1: Κρυπτογράφηση και αποκρυπτογράφηση

Φυσικά, αυτό που πρέπει να είναι μυστικό είναι το κλειδί K_A , διαφορετικά ένας ενδιαμέσος μπορεί να υπολογίσει το μήνυμα T με τον ίδιο τρόπο που το κάνει η Αλίχη.

Η πιο απλή και πιο ασφαλής κρυπτογραφία είναι η κρυπτογραφία μιας φοράς. Σε αυτό το σύστημα ο Βασίλης και η Αλίχη έχουν ένα κοινό μυστικό κλειδί K που κανένας άλλος δεν γνωρίζει. Υποθέτουμε ότι το μήνυμα T καθώς και το μυστικό κλειδί K είναι ακολουθίες από δυαδικά ψηφία και ότι έχουν το ίδιο μήκος. Ο Βασίλης κρυπτογραφεί το μήνυμα σαν $M = T \oplus K$ και η Αλίχη αποκρυπτογραφεί το μήνυμα σαν $T = M \oplus K$, όπου η πράξη \oplus (xor) εφαρμόζεται σε κάθε δυαδικό ψηφίο. Για παράδειγμα

$$T = 01100100$$

$$K = 11000100$$

$$M = 10100000$$

Κάποιος ενδιαμέσος βλέπει μόνο το M . Με την υπόθεση ότι το κλειδί K είναι μυστικό, το σύστημα αυτό είναι απόλυτα ασφαλές. Πράγματι, αν ένας ενδιαμέσος μπορούσε να υπολογίσει το T τότε θα μπορούσε να υπολογίσει το μυστικό κλειδί σαν $K = T \oplus M$, άτοπο.

Αν και αυτό το σύστημα είναι απόλυτα ασφαλές, το μεγάλο μειονέκτημα του είναι η υπόθεση ότι ο Βασίλης και η Αλίχη έχουν ένα κοινό μυστικό κλειδί με μήκος ίσο με το μήνυμα. Έτσι αν θέλουν να επικοινωνήσουν ξανά, πρέπει να χρησιμοποιήσουν κάποιο νέο κλειδί. Στην πράξη το ίδιο κλειδί χρησιμοποιείται επανειλημμένα, αλλά τότε το παραπάνω σύστημα δεν είναι πολύ ασφαλές.

Σε πολλές όμως από τις σύγχρονες εφαρμογές της κρυπτογραφίας, η Αλίχη και ο Βασίλης μπορεί να μην έχουν ποτέ συναντηθεί (όπως για παράδειγμα συμβαίνει όταν κατεβάζουμε ιστοσελίδες που έχουν κρυπτογραφηθεί, που το όνομα τους δηλαδή τελειώνει σε .shtml). Σε αυτή την περίπτωση, χρησιμοποιούμε κρυπτογραφία δημόσιου κλειδιού. Στην κρυπτογραφία ιδιωτικού κλειδιού το κλειδί κρυπτογράφησης K_B είναι μυστικό, αλλά στην κρυπτογραφία δημόσιου κλειδιού είναι γνωστό σε όλους. Όπως αναφέραμε παραπάνω το κλειδί αποκρυπτογράφησης πρέπει οπωσδήποτε να είναι μυστικό. Στη κρυπτογραφία δημόσιου

κλειδιού, αυτό που εμποδίζει κάποιον ενδιάμεσο να βρει το μήνυμα T είναι ότι απαιτούνται πολλοί υπολογισμοί για να βρεθεί το T . Αν δηλαδή κάποιος είχε πανίσχυρους υπολογιστές ή ήταν διατεθειμένος να περιμένει για αρκετό χρόνο θα μπορούσε να βρει πάντα το μήνυμα T .

7.1 RSA

Εδώ θα μελετήσουμε το κρυπτογραφικό σύστημα RSA (το όνομα προέρχεται από τα αρχικά των εφευρετών του Rivest, Shamir, Adleman) που προτάθηκε το 1978 και αποτελεί σήμερα το πιο διαδεδομένο σύστημα δημόσιου κλειδιού.

Εστω ότι ο Βασίλης θέλει να στείλει ένα κείμενο στην Αλίκη. Το χωρίζει σε τμήματα των 1022 δυαδικών ψηφίων και στέλνει το κάθε τμήμα T με το RSA. Το πρωτόκολλο είναι το εξής:

1. Η Αλίκη επιλέγει δυο μεγάλους τυχαίους πρώτους αριθμούς p και q (με 512 δυαδικά ψηφία ο καθένας).
2. Υπολογίζει το $n = p \cdot q$. Το n πρέπει να έχει περισσότερα δυαδικά ψηφία από το T .
3. Υπολογίζει το $\varphi(n) = (p - 1) \cdot (q - 1)$ και επιλέγει ένα τυχαίο αριθμό e (με 1024 δυαδικά ψηφία) που είναι σχετικά πρώτος με τον $\varphi(n)$. Υπολογίζει ένα d τέτοιο ώστε $e \cdot d = 1 \pmod{\varphi(n)}$.
4. Δημοσιεύει τα n , e κρατώντας μυστικά τα p , q και d . Το ζεύγος (n, e) αποτελεί το δημόσιο κλειδί της Αλίκης.
5. Ο Βασίλης υπολογίζει και στέλνει στην Αλίκη το $M = T^e \pmod{n}$.
6. Η Αλίκη αποκρυπτογραφεί το μήνυμα υπολογίζοντας $T = M^d \pmod{n}$.

Η πραγματική κρυπτογράφηση και αποκρυπτογράφηση γίνεται στα βήματα 5 και 6. Τα τέσσερα πρώτα βήματα αποτελούν την προεργασία και μπορούν να γίνουν μια φορά για όλα τα μηνύματα που θα στείλει ο Βασίλης στην Αλίκη. Ή μπορεί ακόμα η Αλίκη να υπολογίσει το δημόσιο κλειδί της (n, e) μια φορά, να το δημοσιεύσει και να το χρησιμοποιεί στις επικοινωνίες της για ολόκληρη τη ζωή της.

Τα ερωτήματα που προκύπτουν είναι αν το πρωτόκολλο είναι σωστό, αν είναι υπολογιστικά εφικτό και τέλος αν είναι ασφαλές. Η σύντομη απάντηση είναι καταφατική ως προς την ορθότητα και την υπολογιστικότητα αλλά η ασφάλεια του RSA παραμένει ένα σπουδαίο ανοικτό πρόβλημα. Πιο συγκεκριμένα θέλουμε να απαντήσουμε στα παρακάτω:

Ερωτήματα Ορθότητας

1. Υπάρχουν μεγάλοι πρώτοι αριθμοί; (Βήμα 1)
2. Υπάρχει πάντα d τέτοιο ώστε $e \cdot d = 1 \pmod{\varphi(n)}$; (Βήμα 3)

3. Είναι αλήθεια ότι το $M^d \pmod n$ είναι ισο με το αρχικό T ; (Βήμα 6)

Ερωτήματα Υπολογισμού

4. Μπορούμε να βρούμε γρήγορα δυο μεγάλους τυχαίους πρώτους; Μπορούμε να επιβεβαιώσουμε γρήγορα αν ένας αριθμός είναι πρώτος; (Βήμα 1)
5. Μπορούμε να βρούμε γρήγορα d τέτοιο ώστε $e \cdot d = 1 \pmod{\varphi(n)}$; (Βήμα 3)
6. Μπορούμε να υπολογίσουμε γρήγορα δυνάμεις $\pmod n$ και πιο συγκεκριμένα το $M = T^e \pmod n$ και $T = M^d \pmod n$; (Βήματα 5 και 6)

Ερωτήματα Ασφάλειας

7. Μπορεί κάποιος ενδιάμεσος να υπολογίσει σε εφικτό χρόνο το T αν γνωρίζει το n , e και M ;

1. Υπάρχουν μεγάλοι πρώτοι αριθμοί; Η απάντηση είναι καταφατική. Ο Ευκλείδης απέδειξε ότι υπάρχουν άπειροι πρώτοι αριθμοί. Στην πραγματικότητα το πλήθος $\pi(n)$ των πρώτων αριθμών μικρότερων ενός ακέραιου n είναι περίπου $n/\ln n$ με την έννοια ότι

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln n} = 1$$

Αυτο είναι το Θεώρημα των Πρώτων Αριθμών και συνδέεται άμεσα με την εικασία του Riemann (Κεφάλαιο 1). Διαισθητικά η παραπάνω σχέση μπορεί να ερμηνευτεί και ως εξής: Ένας τυχαίος ακέραιος n είναι πρώτος με πιθανότητα $1/\ln n$.

2. Υπάρχει πάντα d τέτοιο ώστε $e \cdot d = 1 \pmod{\varphi(n)}$; Ναι, αλλά μόνο αν ο e και ο $\varphi(n)$ είναι πρώτοι μεταξύ τους. Γι' αυτό η Αλίκη πρέπει να διαλέξει το e να είναι πρώτο με το $\varphi(n)$.

Η απόδειξη βασίζεται στο παρακάτω γενικότερο λήμμα:

Λήμμα 42. Η ακέραια εξίσωση $ax = c \pmod b$ έχει λύση αν ο μέγιστος κοινός διαιρέτης των a και b διαιρεί τον c .

Απόδειξη. Η απόδειξη λήμματος προκύπτει από τον αλγόριθμο του Ευκλείδη. Όπως δείξαμε στο Κεφάλαιο 4, για κάθε ακέραιους a και b με μέγιστο κοινό διαιρέτη δ , υπάρχουν πάντα ακέραιοι x και y τέτοιοι ώστε $ax + by = \delta$. Προφανώς αν πολλαπλασιάσουμε όλους τους όρους

με τον ίδιο ακέραιο, η ισότητα ισχύει. Ειδικά αν πολλαπλασιάσουμε με τον c/δ (που από την υπόθεση είναι ακέραιος), παίρνουμε ότι υπάρχουν ακέραιοι $x' = xc/\delta$ και $y' = yc/\delta$ τέτοιοι ώστε $ax' + by' = c$. Αυτό σημαίνει ότι η εξίσωση $ax' = c \pmod{b}$ έχει πάντα ακέραια λύση. \square

Προφανώς ισχύει και το αντίστροφο: Αν ο μέγιστος κοινός διαιρέτης δ των a και b δεν διαιρεί τον c , η εξίσωση $ax = c \pmod{b}$ δεν έχει λύση.

Για το RSA αρκεί τώρα να πάρουμε $a = e$, $b = \varphi(n)$, $c = 1$ και τότε d είναι η λύση της εξίσωσης $ax = c \pmod{b}$.

3. Είναι αλήθεια ότι το $M^d \pmod{n}$ είναι ίσο με το αρχικό T ; Η απάντηση είναι καταφατική και σ' αυτό κεντρικό ρόλο παίζει η ιδιότητα $ed = 1 \pmod{\varphi(n)}$. Η απόδειξη βασίζεται στα δυο παρακάτω γενικότερα θεωρήματα της θεωρίας αριθμών.

Θεώρημα 43 (Μικρό Θεώρημα του Fermat). Για κάθε πρώτο p και κάθε a σχετικά πρώτο με τον p : $a^{p-1} = 1 \pmod{p}$.

Για παράδειγμα $3^6 = 1 \pmod{7}$. Μια απόδειξη βασίζεται στην εξής ιδέα: Οι αριθμοί $a \cdot 1 \pmod{p}$, $a \cdot 2 \pmod{p}$, \dots , $a \cdot (p-1) \pmod{p}$ είναι σχετικά πρώτοι με τον p και είναι όλοι διαφορετικοί μεταξύ τους. Πράγματι αν $a \cdot j = a \cdot i \pmod{p}$ τότε $a(j-i) = 0 \pmod{p}$, άτοπο αφού και ο a και ο $j-i$ είναι σχετικά πρώτοι με τον p .

Επομένως το σύνολο των αριθμών $\{a \cdot 1 \pmod{p}, a \cdot 2 \pmod{p}, \dots, a \cdot (p-1) \pmod{p}\}$ είναι ίσο με το σύνολο $\{1, 2, \dots, p-1\}$.

Αλλά τότε το γινόμενο των $a \cdot 1$, $a \cdot 2$, \dots , $a \cdot (p-1)$ είναι ίσο με $a^{p-1} \cdot 1 \cdot 2 \cdot (p-1)$, αλλά και ίσο με $1 \cdot 2 \cdot (p-1) \pmod{p}$. Αυτό μπορεί να συμβαίνει μόνο αν $a^{p-1} = 1 \pmod{p}$.

Αυτό που θα χρειαστούμε εμείς εδώ είναι το εξής πόρισμα του Μικρού Θεωρήματος του Fermat:

Πόρισμα 44. Για κάθε πρώτο p και κάθε a (όχι υποχρεωτικά πρώτοι μεταξύ τους): $a^k = a \pmod{p}$ για κάθε $k = 1 \pmod{p-1}$.

Πράγματι αν $a = 0 \pmod{p}$, το πόρισμα ισχύει γιατί $0^k = 0 \pmod{p}$. Ας υποθέσουμε τώρα ότι $a \neq 0 \pmod{p}$. Αν γράψουμε $k = 1 + \lambda(p-1)$ για κάποιο ακέραιο λ , έχουμε

$$a^k = a^{1+\lambda(p-1)} = a(a^{p-1})^\lambda = a(1)^\lambda = a \pmod{p}.$$

Το δεύτερο θεώρημα που χρειαζόμαστε είναι:

Θεώρημα 45 (Το Κινέζικο Θεώρημα των Υπολοίπων). Έστω n_1, \dots, n_k θετικοί ακέραιοι, πρώτοι ανά δυο μεταξύ τους και έστω a_1, \dots, a_k είναι φυσικοί τέτοιοι ώστε $a_i < n_i$. Τότε υπάρχει ένας και μοναδικός ακέραιος a στο διάστημα $[0, n_1 \cdots n_k)$ τέτοιος ώστε $a = a_i \pmod{n_i}$.

Για παράδειγμα, ας πάρουμε $n_1 = 5$, $n_2 = 6$ και $a_1 = 3$, $a_2 = 5$. Οι αριθμοί που έχουν υπόλοιπο 3 (mod 5) στο διάστημα $[0, 24]$ είναι οι 3, 8, 13, 18, 23. Αντίστοιχα, οι αριθμοί που αφήνουν υπόλοιπο 5 (mod 6) είναι οι 5, 11, 17, 23. Παρατηρούμε ότι ο $a = 23$ ανήκει και στις δυο ακολουθίες.

Ειδικά εδώ θα χρειαστούμε το εξής πόρισμα του Κινέζικου Θεωρήματος των Υπολοίπων:

Πόρισμα 46. Έστω p και q πρώτοι. Το μοναδικό a στο διάστημα $[0, pq)$ που ικανοποιεί τις ισότητες $a = T \pmod{p}$, $a = T \pmod{q}$ είναι ο $a = T$.

Πράγματι, αν πάρουμε $n_1 = p$, $n_2 = q$ και $a_1 = a_2 = T$, ο $a = T$ προφανώς ικανοποιεί το $a = T \pmod{p}$ και $a = T \pmod{q}$ και σύμφωνα με το Κινέζικο Θεώρημα των Υπολοίπων είναι ο μοναδικός τέτοιος αριθμός στο $[0, pq)$.

Ας δούμε τώρα πως μπορούμε να χρησιμοποιήσουμε τα παραπάνω δυο πορίσματα για να δείξουμε ότι η αποκρυπτογράφηση παράγει το αρχικό μήνυμα T .

Πράγματι αφού $M = T^e \pmod{n}$, έχουμε

$$M^d \pmod{n} = (T^e)^d \pmod{n} = T^{ed} \pmod{n}$$

Το d επιλέχθηκε έτσι ώστε $ed = 1 \pmod{(p-1)(q-1)}$. Από αυτό προκύπτει ότι $ed = 1 \pmod{p-1}$ και $ed = 1 \pmod{q-1}$. Το Πόρισμα 44 δίνει

$$T^{ed} = T \pmod{p} \quad \text{και} \quad T^{ed} = T \pmod{q}$$

Μπορούμε τώρα να χρησιμοποιήσουμε το Πόρισμα 46 και να συμπεράνουμε ότι T είναι ο μοναδικός αριθμός στο διάστημα $[0, pq)$ που ικανοποιεί τα παραπάνω.

Προσέξτε ότι πρέπει να διαλέξουμε τον αριθμό των δυαδικών ψηφίων ώστε το $n = pq$ να είναι σίγουρα μεγαλύτερο από το T για να έχουμε μοναδική λύση. Αν τα p και q έχουν k δυαδικά ψηφία, τότε ο n είναι τουλάχιστον $2^{k-1}2^{k-1}$ και μπορούν να κρυπτογραφηθούν $2(k-1)$ δυαδικά ψηφία σε κάθε μήνυμα M .

4. Μπορούμε να επιβεβαιώσουμε γρήγορα αν ένας αριθμός είναι πρώτος; Μπορούμε να βρούμε γρήγορα δυο μεγάλους τυχαίους πρώτους; Η απάντηση είναι καταφατική και στις δυο ερωτήσεις. Όπως είδαμε παραπάνω οι πρώτοι αριθμοί είναι αρκετά πυκνοί. Αν επιλέξουμε ένα τυχαίο αριθμό x , η πιθανότητα να είναι πρώτος είναι περίπου $1/\ln n$. Για παράδειγμα αν επιλέξουμε ένα τυχαίο αριθμό με 512 δυαδικά ψηφία, η πιθανότητα να είναι πρώτος είναι περίπου $1/(512 \ln 2) \approx 1/355$. Για να βρούμε ένα τυχαίο πρώτο αριθμό με 512 δυαδικά ψηφία, επιλέγουμε ένα τυχαίο αριθμό και ελέγχουμε αν είναι πρώτος. Αν είναι τελειώσαμε, αλλιώς επαναλαμβάνουμε τη διαδικασία. Περιμένουμε ο αναμενόμενος αριθμός βημάτων αυτής της διαδικασία να είναι 355 (ή πιο γενικά $\ln n$).

Η παραπάνω διαδικασία μπορεί να υλοποιηθεί πρακτικά μόνο αν μπορούμε να ελέγξουμε γρήγορα αν ένας αριθμός είναι πρώτος. Πώς ελέγχουμε αν ένας αριθμός m είναι πρώτος;

Μια απλή μέθοδος είναι το κόσκινο του Ερατοσθένους που βρίσκει όλους τους πρώτους μεταξύ 1 και m . Παρόμοιος είναι ο αλγόριθμος: Έλεγε αν ο m διαιρείται με τους $2, 3, \dots, \lfloor \sqrt{m} \rfloor$. Αν ο m δεν διαιρείται με κανένα από αυτούς, είναι πρώτος. Το πρόβλημα με αυτό τον αλγόριθμο είναι ότι ο αριθμός των βημάτων του είναι περίπου \sqrt{m} . Για $m \approx 2^{1024}$, $\sqrt{m} = 2^{512}$ είναι υπερβολικά μεγάλος αριθμός.

Υπάρχουν όμως πιο γρήγοροι τρόποι να ελέγξουμε αν ένας αριθμός m είναι πρώτος, χωρίς να χρειάζεται να βρούμε τους πρώτους παράγοντες του. Μια τέτοια μέθοδος βασίζεται στο Μικρό Θεώρημα του Fermat. Υπολογίζουμε το $2^{m-1} \pmod{m}$. Αν ο m είναι πρώτος, το Μικρό Θεώρημα του Fermat εγγυάται ότι το αποτέλεσμα είναι ίσο με 1. Αν λοιπόν $2^{m-1} \not\equiv 1 \pmod{m}$, τότε είμαστε σίγουροι ότι ο m δεν είναι πρώτος. Αν όμως $2^{m-1} \equiv 1 \pmod{m}$, τότε ο m μπορεί να είναι πρώτος, αλλά δεν είμαστε σίγουροι γιατί η ισότητα ισχύει και για κάποιους μη πρώτους m . Τέτοιοι αριθμοί όμως είναι λίγοι και η πιθανότητα να συμβαίνει αυτό είναι πολύ μικρή. Για πρακτικούς λόγους, το παραπάνω είναι ικανοποιητικό τεστ, αφού η πιθανότητα να αποτύχει είναι πρακτικά μηδέν. Υπάρχει όμως τρόπος να επεκτείνουμε αυτή την ιδέα και να κατασκευάσουμε πιθανοτικούς αλγόριθμους που ελέγχουν γρήγορα και με εξαιρετικά μεγάλη πιθανότητα αν ένας αριθμός είναι πρώτος.

Επίσης, πολύ πρόσφατα εφευρέθηκε ένας ντετερμινιστικός αλγόριθμος που μπορεί να ελέγξει γρήγορα και με σιγουριά αν ένας αριθμός είναι πρώτος.

5. Μπορούμε να βρούμε γρήγορα d τέτοιο ώστε $e \cdot d = 1 \pmod{\phi(n)}$; Όπως αναφέραμε παραπάνω μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο του Ευκλείδη για να βρούμε γρήγορα ένα τέτοιο d .

6. Μπορούμε να υπολογίσουμε γρήγορα $x^k \pmod{n}$; Χρειάζεται να μπορούμε να υπολογίσουμε γρήγορα $x^k \pmod{n}$ για δεδομένα

x, k, n . Για τους πρακτικούς σκοπούς της κρυπτογραφίας, αυτοί οι αριθμοί είναι πολύ μεγάλοι (της τάξης των 1024 δυαδικών ψηφίων ο καθένας).

Ο προφανής τρόπος είναι να υπολογίσουμε τα $x, x^2, x^3, \dots, x^k \pmod{n}$ με επανειλημμένους πολλαπλασιασμούς με το x . Δυστυχώς αυτός ο αλγόριθμος απαιτεί τουλάχιστον $k - 1$ πολλαπλασιασμούς (στην πραγματικότητα χρειάζονται και ανάλογες διαιρέσεις για να υπολογίσουμε το αποτέλεσμα \pmod{n}).

Ευτυχώς όμως υπάρχει ταχύτερη μέθοδος για να υπολογίσουμε το $x^k \pmod{n}$. Υπολογίζουμε $x, x^2, x^4, x^8, \dots \pmod{n}$. Ο κάθε όρος αυτής της ακολουθίας είναι το τετράγωνο του προηγούμενου (π.χ. $x^8 = (x^4)^2$). Για να βρούμε τώρα το x^k πολλαπλασιάζουμε κάποια από τα μέλη της ακολουθίας.

Για παράδειγμα, αν θέλουμε να υπολογίσουμε το x^{11} , υπολογίζουμε πρώτα τα x, x^2, x^4, x^8 και μετά $x \cdot x^2 \cdot x^8 = x^{1+2+8} = x^{11}$. Η δυαδική παράσταση του 11 είναι 1011. Πολλαπλασιάσαμε τα x, x^2 και x^8 που αντιστοιχούν στα 1 της δυαδικής παράστασης.

Γενικότερα, από την δυαδική παράσταση του έχθετη k έχουμε $k = 2^{i_1} + 2^{i_2} + \dots + 2^{i_t}$ για κάποια i_1, \dots, i_t . Υπολογίζουμε το $x^k = x^{2^{i_1}} x^{2^{i_2}} \dots x^{2^{i_t}}$.

Πόσοι πολλαπλασιασμοί συνολικά; Το πολύ $\log k$ πολλαπλασιασμούς για να βρούμε τα $x, x^2, x^4, x^8, \dots, x^{2^{\lfloor \log k \rfloor}}$ και το πολύ άλλους τόσους για να υπολογίσουμε το $x^k = x^{2^{i_1}} x^{2^{i_2}} \dots x^{2^{i_t}}$. Συνολικά το πολύ $2 \log k$ πολλαπλασιασμούς. Χρειαζόμαστε επίσης άλλες τόσες διαιρέσεις για να βρούμε τους αριθμούς αυτούς \pmod{n} . Για παράδειγμα, για κρυπτογραφία με 1024 δυαδικά ψηφία όπως παραπάνω, ο αριθμός των πολλαπλασιασμών είναι περίπου 2048.

Μια σημαντική λεπτομέρεια στους υπολογισμούς είναι ότι μετά από κάθε πολλαπλασιασμό πρέπει να βρίσκουμε το αποτέλεσμα \pmod{n} , έτσι ώστε όλοι οι αριθμοί να παραμένουν σχετικά μικροί. Αν δεν το κάνουμε αυτό ο αριθμός $x^{2^{\lfloor \log k \rfloor}}$ θα έχει περίπου k δυαδικά ψηφία (δηλαδή περίπου 2^{1024} δυαδικά ψηφία!)

7. Μπορεί κάποιος ενδιάμεσος να υπολογίσει σε εφικτό χρόνο το T αν γνωρίζει το n, e και M ; Δεν το γνωρίζουμε. Αυτό είναι το πιο σημαντικό ανοικτό πρόβλημα στην κρυπτογραφία σήμερα.

Αν υπάρχει γρήγορος αλγόριθμος που παραγοντοποιεί ακέραιους, τότε μπορούμε να 'σπάσουμε' το RSA. Με τον αλγόριθμο αυτό θα παραγοντοποιούσαμε τον n , θα βρίσκαμε τους p και q που είναι το μυστικό της Αλίκης. Από τους p και q θα βρίσκαμε το $\varphi(n)$ και το d με τον ίδιο τρόπο που τα υπολογίζει η Αλίκη.

Προσέξτε ότι υπάρχουν δυο προβλήματα που μοιάζουν παρόμοια:

Έλεγχος: Δίνεται ακέραιος. Είναι πρώτος ή σύνθετος;

Παραγοντοποίηση: Δίνεται ακέραιος. Βρείτε τους πρώτους παράγοντες του.

Το σύστημα RSA όμως βασίζεται στο ότι το πρώτο πρόβλημα έχει γρήγορο αλγόριθμο, ενώ το δεύτερο (μάλλον) δεν έχει.

Η παραγοντοποίηση είναι σίγουρα της ίδιας δυσκολίας ή μεγαλύτερης από τον έλεγχο, γιατί αν μπορούμε να βρούμε τους πρώτους παράγοντες ενός αριθμού μπορούμε αμέσως να δούμε αν είναι πρώτος ή σύνθετος. Από την άλλη, γνωρίζουμε, όπως είδαμε παραπάνω, γρήγορους αλγόριθμους για τον έλεγχο (που δεν βασίζονται στην παραγοντοποίηση), αλλά δεν γνωρίζουμε κανένα γρήγορο αλγόριθμο για παραγοντοποίηση. Ο καλύτερος αλγόριθμος που γνωρίζουμε για παραγοντοποίηση παίρνει περίπου $e^{(\ln n)^{1/3}}$ βήματα. Με τις σημερινές υπολογιστικές δυνατότητες μπορούμε να παραγοντοποιούμε ακέραιους με περίπου 100 δεκαδικά ψηφία.

Ασκήσεις

7.1. Θεωρείστε το σύστημα RSA με παραμέτρους

$$p = 71, \quad q = 83, \quad e = 3.$$

1. Ποιο είναι το d ;
2. Ποια είναι η ημερομηνία γέννησή σας;
3. Έστω g η ημέρα γέννησής σας (αν για παράδειγμα γεννηθήκατε 1988/02/17, τότε $g = 17$). Έστω ότι χρησιμοποιούμε το RSA για να κρυπτογραφήσουμε το g . Ποιο μήνυμα θα σταλεί;
4. Έστω ότι κάποιος κρυπτογράφησε ένα μήνυμα T με το παραπάνω σύστημα και το αποτέλεσμα είναι ο μήνας γέννησής σας (ένας ακέραιος στο $\{1, \dots, 12\}$). Ποιο είναι το T ;

Αυτή η άσκηση απαιτεί πολλούς υπολογισμούς και ο καλύτερος τρόπος είναι να γράψετε κατάλληλο πρόγραμμα.

7.2. Κάποιος που θέλει να 'σπάσει' ένα σύστημα RSA κατάφερε να βρει ένα κατάσκοπο και με πολλές προσπάθειες να αποκτήσει ένα αποκρυπτογραφημένο μήνυμα του συστήματος. Έχει λοιπόν στη διάθεση του ένα μήνυμα στην κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή. Ελπίζει ότι με αυτή την πληροφορία θα καταφέρει να 'σπάσει' το σύστημα και να μπορεί να αποκρυπτογραφεί κάθε μήνυμα γρήγορα χωρίς τη βοήθεια του κατασκόπου φυσικά. Τι λέτε, μπορεί; Εξηγείστε.

Υποθέστε βέβαια ότι το σύστημα RSA χρησιμοποιεί πάντα τα ίδια ιδιωτικά και δημόσια κλειδιά.

8 Ανάλυση Αλγορίθμων

Η σχεδίαση και ανάλυση αλγορίθμων είναι ακρογωνιαίος λίθος της Επιστήμης της Πληροφορικής. Εδώ θα μελετήσουμε βασικές τεχνικές ανάλυσης αλγορίθμων καθώς και της υπολογιστικής πολυπλοκότητας προβλημάτων. Δεν θα καλύψουμε όμως καθόλου τεχνικές σχεδίασης αλγορίθμων καθώς αποτελούν ένα βαθύτερο και πολύ εκτεταμένο επιστημονικό χώρο.

Οι κλασικοί αλγόριθμοι έχουν αρχή και τέλος με είσοδο και έξοδο αντίστοιχα. Σήμερα όμως μια άλλη κατηγορία αλγορίθμων, οι ατέρμονες αλγόριθμοι που δεν τερματίζουν ποτέ, αποκτά όλο και μεγαλύτερη αξία. Παραδείγματα τέτοιων αλγορίθμων είναι τα λειτουργικά συστήματα, οι δομές και βάσεις δεδομένων, τα πρωτόκολλα επικοινωνίας στο Διαδίκτυο, παιχνίδια εικονικής πραγματικότητας με χιλιάδες χρήστες. Εδώ θα μελετήσουμε μόνο κλασικούς αλγόριθμους γιατί η ανάλυση τους είναι απλούστερη, αλλά κυρίως γιατί το αντικείμενο είναι ξεκάθαρο. Το αντικείμενο της ανάλυσης των κλασικών αλγορίθμων είναι συνήθως ο χρόνος εκτέλεσης τους. Μας ενδιαφέρει ένας αλγόριθμος να τρέχει γρήγορα, δηλαδή, να έχει μικρό χρόνο εκτέλεσης. Όμως στους ατέρμονες αλγόριθμους δεν υπάρχει αντίστοιχο απλό κριτήριο, αφού ο χρόνος εκτέλεσης είναι άπειρος. Συνεπώς η ανάλυση των ατερομόνων αλγορίθμων απαιτεί άλλη προσέγγιση.

Ο χρόνος εκτέλεσης ενός αλγορίθμου (προγράμματος) εξαρτάται κυρίως από την είσοδο. Αλλά και για δεδομένη είσοδο εξαρτάται από πολλούς άλλους εξωγενείς παράγοντες: τη γλώσσα προγραμματισμού, τον επεξεργαστή, το υπολογιστικό περιβάλλον και άλλα. Έτσι όταν μιλάμε για χρόνο εκτέλεσης ενός αλγορίθμου πρέπει

- να ξεκαθαρίσουμε ποια χαρακτηριστικά της εισόδου επηρεάζουν το χρόνο του αλγορίθμου και
- να εξαλείψουμε με κάποιο τρόπο τους εξωγενείς παράγοντες.

Για τους εξωγενείς παράγοντες, η λύση είναι απλή. Αυτοί οι παράγοντες λειτουργούν κυρίως πολλαπλασιαστικά. Αν για παράδειγμα ο χρόνος εκτέλεσης ενός προγράμματος με κάποια δεδομένη είσοδο παίρνει χρόνο t σε ένα υπολογιστή, παίρνει χρόνο περίπου at σε κάποιον άλλο, για κάποια σταθερά a που εκφράζει πόσο ταχύτερος ή βραδύτερος είναι ο

δεύτερος υπολογιστής σε σχέση με τον πρώτο. Έτσι όταν αναλύουμε ένα αλγόριθμο, αρκεί να εξαλείψουμε ένα (άγνωστο) παράγοντα που εκφράζει την ταχύτητα. Ο τρόπος που το κάνουμε αυτό είναι χρησιμοποιώντας το συμβολισμό O , που θα ορίσουμε παρακάτω.

Από τα χαρακτηριστικά της εισόδου που επηρεάζουν το χρόνο εκτέλεσης ενός αλγορίθμου, συνήθως το μόνο που εξετάζουμε είναι το μήκος της. Σχεδόν για όλους τους αλγόριθμους που μας ενδιαφέρουν, ο χρόνος εκτέλεσης αυξάνει όταν αυξήσουμε το μήκος της εισόδου. Μια βασική παραδοχή της ανάλυσης αλγορίθμων είναι ότι ο χρόνος είναι συνάρτηση $T(n)$ του μήκους n της εισόδου. Μήκος εισόδου θεωρείται ο αριθμός των δυαδικών ψηφίων της παράστασης της εισόδου. Ας δούμε μερικά παραδείγματα:

- Αν η είσοδος είναι μια συμβολοσειρά του αλφαβήτου $\{0, 1\}$, τότε το μήκος της εισόδου n είναι ο αριθμός των συμβόλων της συμβολοσειράς. Για παράδειγμα, η είσοδος '010011001101' έχει μήκος 12.
- Αν η είσοδος είναι μια συμβολοσειρά του αλφαβήτου $\{0, 1, \dots, 9\}$ τότε το μήκος εισόδου είναι 4 επί τον αριθμό των συμβόλων της εισόδου, γιατί η παράσταση των δεκαδικών ψηφίων γίνεται με 4 δυαδικά ψηφία. Για παράδειγμα, η είσοδος '0043445190' έχει μήκος 40 ($= 10 \cdot 4$).
- Πιο ενδιαφέρον παράδειγμα αποτελεί η περίπτωση που η είσοδος είναι ένας φυσικός αριθμός a . Το μήκος της εισόδου είναι ίσο με $\lceil \log a \rceil$, όσα και τα ψηφία της δυαδικής παράστασης του a . Για παράδειγμα, η είσοδος 1040 έχει μήκος 11, γιατί η δυαδική παράσταση του 1040 είναι 10000010000.
- Αν η είσοδος είναι μια ακολουθία a_1, a_2, \dots, a_k φυσικών αριθμών, τότε το μήκος της εισόδου είναι $c(k-1) + \lceil \log a_1 \rceil + \lceil \log a_2 \rceil + \dots + \lceil \log a_k \rceil$, όπου $c(k-1)$ εκφράζει τα επιπλέον δυαδικά ψηφία που απαιτούνται για την παράσταση των κομμάτων (';').

Είναι προφανές από τα παραπάνω παραδείγματα ότι ακόμα και το μήκος της εισόδου παρουσιάζει επιπλοκές και δυσκολίες. Ευτυχώς στη θεωρία ανάλυσης αλγορίθμων οι επιπλοκές αποφεύγονται, πάλι με τη χρήση του συμβολισμού O . Μερικές φορές πάλι, οι επιπλοκές αγνοούνται εσκεμμένα. Για παράδειγμα, για τους περισσότερους αλγορίθμους που παίρνουν για είσοδο μια ακολουθία από k φυσικούς αριθμούς, όπως στο τελευταίο παράδειγμα παραπάνω, το μήκος εισόδου εκλαμβάνεται απλά ως k .

Όπως αναφέρθηκε παραπάνω, ο χρόνος εκτέλεσης είναι μια συνάρτηση $T(n)$ του μήκους n της εισόδου. Αλλά υπάρχουν πολλές εισοδοί που έχουν μήκος n (για την ακρίβεια, υπάρχουν 2^n τέτοιες εισοδοί). Για κάποιες από αυτές ο αλγόριθμος μπορεί να έχει μικρό χρόνο εκτέλεσης

και για κάποιες άλλες μεγάλο χρόνο εκτέλεσης. Ποιο χρόνο λοιπόν θεωρούμε σαν $T(n)$; Από παραδοχή, χρησιμοποιούμε τον μεγαλύτερο από αυτούς τους χρόνους, τη χειρίστη δηλαδή περίπτωση. Η ανάλυση της χειρίστης περίπτωση (worst-case analysis) χρησιμοποιείται συχνά στην Πληροφορική γιατί παρέχει κάποιο είδος εγγύησης: Όταν λέμε ότι ο χρόνος εκτέλεσης είναι $T(n)$, αυτό σημαίνει ότι ο χρόνος εκτέλεσης δεν θα ξεπεράσει το $T(n)$ για καμία είσοδο μήκους n .

8.1 Ο συμβολισμός O

Ορισμός 47. Έστω f και g δυο συναρτήσεις από τους μη αρνητικούς ακέραιους στο σύνολο των πραγματικών αριθμών. Θα λέμε ότι $f(n) = O(g(n))$ αν υπάρχουν θετικές σταθερές c και n_0 τέτοιες ώστε

$$f(n) \leq c \cdot g(n)$$

για κάθε $n \geq n_0$.

ΠΑΡΑΔΕΙΓΜΑ 8.1 (Πολυώνυμα).

Ισχυρισμός. $10n + 7 = O(n)$

Απόδειξη. Εδώ έχουμε $f(n) = 10n + 7$ και $g(n) = n$. Αρκεί να βρούμε τις δυο σταθερές c και n_0 του ορισμού και να επιβεβαιώσουμε τη σχέση $f(n) \leq c \cdot g(n)$. Στις περισσότερες περιπτώσεις αρκεί να πάρουμε $n_0 = 1$ και αυτό θα κάνουμε εδώ. Ποιο c θα διαλέξουμε; Ας μαντέψουμε: $c = 17$.

Για $n \geq n_0 = 1$, έχουμε

$$f(n) = 10n + 7 \leq 10n + 7n \leq 17n = cn = cg(n).$$

Άρα οι σταθερές $n_0 = 1$ και $c = 17$ ικανοποιούν τις υποθέσεις του ορισμού και ο ισχυρισμός είναι αληθής. \square

Μπορούμε να γενικεύσουμε το παραπάνω παράδειγμα για όλα τα πολυώνυμα:

Θεώρημα 48. Αν $p(n)$ είναι πολυώνυμο βαθμού d , τότε $p(n) = O(n^d)$.

Απόδειξη. Η απόδειξη είναι όμοια με την παραπάνω. Το πολυώνυμο $p(n)$ γράφεται σαν $p(n) = a_d n^d + \dots + a_1 n + a_0$, όπου a_d, a_{d-1}, \dots, a_0 είναι

σταθερές. Διαλέγουμε $n_0 = 1$ και $c = |a_d| + \dots + |a_1| + |a_0|$ και έχουμε

$$\begin{aligned} p(n) &= a_d n^d + \dots + a_1 n + a_0 \\ &\leq |a_d n^d + \dots + a_1 n + a_0| \\ &\leq |a_d n^d| + \dots + |a_1 n| + |a_0| \\ &\leq |a_d| n^d + \dots + |a_1| n + |a_0| \\ &\leq |a_d| n^d + \dots + |a_1| n^d + |a_0| n^d \\ &= c n^d. \end{aligned}$$

Γιατί δεν πήραμε σαν $c = a_d + \dots + a_1 + a_0$, χωρίς τις απόλυτες τιμές; Αυτό το c δεν δουλεύει, όπως φαίνεται από το αντιπαράδειγμα $p(n) = 10n - 10$, όπου $c = 0$, και για το οποίο προφανώς δεν ισχύει $p(n) = O(0)$. Σε ποιο σημείο θα κατέρρευε η παραπάνω απόδειξη αν δεν παίρναμε απόλυτες τιμές; \square

Ο συμβολισμός O επιτρέπει να χρησιμοποιούμε απλές και κατανοητές συναρτήσεις όταν αναφερόμαστε στο χρόνο ενός αλγορίθμου. Για παράδειγμα, αντί να λέμε ότι ο χρόνος ενός αλγορίθμου είναι $5n^3 + 13n + 1$, μπορούμε απλά να πούμε ότι είναι $O(n^3)$. Αλλά, αυτή η απλοποίηση δεν πρέπει να οδηγεί σε αντιφάσεις. Το επόμενο θεώρημα δείχνει ότι είναι πράγματι έτσι και πιο συγκεκριμένα ότι μπορούμε να 'ταξινομήσουμε' τις συναρτήσεις από μικρές προς μεγάλες.

Θεώρημα 49. Αν $f(n) = O(g(n))$ και $g(n) = O(h(n))$ τότε $f(n) = O(h(n))$.

Απόδειξη. Από τη σχέση $f(n) = O(g(n))$ προκύπτει ότι υπάρχουν σταθερές n_0 και c τέτοιες ώστε

$$f(n) \leq c g(n)$$

για $n \geq n_0$. Παρόμοια από τη σχέση $g(n) = O(h(n))$ προκύπτει ότι υπάρχουν σταθερές n'_0 και c' τέτοιες ώστε

$$g(n) \leq c' h(n)$$

για $n \geq n'_0$. Πολλαπλασιάζοντας τις σχέσεις παρατηρούμε ότι

$$f(n) \leq c c' h(n)$$

για $n \geq \max\{n_0, n'_0\}$. Άρα υπάρχουν σταθερές $n''_0 = \max\{n_0, n'_0\}$ και $c'' = c c'$ και η σχέση $f(n) = O(h(n))$ ισχύει. \square

Το επόμενο θεώρημα είναι επίσης πολύ βασικό γιατί δείχνει ότι ο συμβολισμός O μπορεί να χρησιμοποιηθεί για να απλοποιηθεί εκφράσεις από το άθροισμα δυο συναρτήσεων αρκεί να κρατήσουμε τη μεγαλύτερη. Από αυτό για παράδειγμα προκύπτει άμεσα ότι $2^n + n = O(2^n)$.

Θεώρημα 50. Αν $f_1(n) = O(g_1(n))$ και $f_2(n) = O(g_2(n))$ τότε $f_1(n) + f_2(n) = O(\max\{g_1(n), g_2(n)\})$.

Η απόδειξη του θεωρήματος είναι παρόμοια με αυτή του Θεωρήματος 49 και αφήνεται για άσκηση.

Στις παραπάνω αποδείξεις χρησιμοποιήσαμε άμεσα τον ορισμό του συμβολισμού O . Για τις περισσότερες κοινές συναρτήσεις όμως, υπάρχει ένας απλούστερος τρόπος για να επιχειρηματολογήσουμε για τον συμβολισμό O . Συγκεκριμένα, έχουμε

Θεώρημα 51. Για θετικές συναρτήσεις $f(n)$ και $g(n)$, αν το όριο $\lambda = \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)}$ υπάρχει, τότε $f(n) = O(g(n))$ αν και μόνο αν το όριο λ είναι κάποια σταθερά (δεν είναι άπειρο δηλαδή).

Απόδειξη. Έστω ότι το όριο $\lambda = \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)}$ υπάρχει. Θα δείξουμε πρώτα ότι αν δεν είναι άπειρο, τότε $f(n) = O(g(n))$. Τι σημαίνει ότι $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \lambda$, για κάποιο σταθερό λ ; Ότι για κάθε $\epsilon > 0$, υπάρχει m_ϵ τέτοιο ώστε για κάθε $n \geq m_\epsilon$:

$$\left| \frac{f(n)}{g(n)} - \lambda \right| < \epsilon$$

Ας πάρουμε $\epsilon = \lambda$. Τότε για κάθε $n \geq m_\lambda$:

$$\left| \frac{f(n)}{g(n)} - \lambda \right| < \lambda \quad \Rightarrow \quad \frac{f(n)}{g(n)} < 2\lambda \quad \Rightarrow \quad f(n) < 2\lambda g(n).$$

Η πρώτη συνεπαγωγή προκύπτει γιατί $\frac{f(n)}{g(n)} - \lambda \leq \left| \frac{f(n)}{g(n)} - \lambda \right|$. Στη δεύτερη χρησιμοποιήσαμε την υπόθεση ότι $g(n)$ είναι θετική. Αρκεί τώρα να πάρουμε $n_0 = m_\lambda$ και $c = 2\lambda$ για να συμπεράνουμε ότι $f(n) = O(g(n))$.

Τώρα θα δείξουμε το αντίστροφο με απαγωγή σε άτοπο. Ας υποθέσουμε λοιπόν ότι $f(n) = O(g(n))$ και ότι $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty$ και θα καταλήξουμε σε άτοπο. Αφού $f(n) = O(g(n))$, υπάρχουν σταθερές n_0 και c τέτοιες ώστε

$$f(n) \leq cg(n) \quad \text{για κάθε } n \geq n_0.$$

Αλλά, επειδή $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty$, για κάθε $\epsilon > 0$, υπάρχει m_ϵ τέτοιο ώστε: για κάθε $n \geq m_\epsilon$, $\frac{f(n)}{g(n)} > \epsilon$. Ας διαλέξουμε τιμή για το ϵ ίση με c . Τότε έχουμε ότι

$$f(n) > cg(n) \quad \text{για κάθε } n \geq m_c.$$

Για $n \geq \max\{n_0, m_c\}$, οι παραπάνω ανισότητες είναι αντιφατικές και οδηγούν σε άτοπο. \square

ΠΑΡΑΔΕΙΓΜΑ 8.2. Για παράδειγμα, επειδή το όριο $\lim_{n \rightarrow \infty} \frac{n}{n^2}$ υπάρχει και είναι 0, προκύπτει από το θεώρημα ότι $n = O(n^2)$.

Επίσης επειδή το όριο $\lim_{n \rightarrow \infty} \frac{n^3}{n^2}$ υπάρχει και είναι ∞ , προκύπτει από το θεώρημα ότι δεν είναι αλήθεια πως $n^3 = O(n^2)$.

Προσοχή χρειάζεται στη χρήση του παραπάνω θεωρήματος. Το θεώρημα ισχύει μόνο αν το όριο υπάρχει. Για παράδειγμα, το θεώρημα δεν μπορεί να εφαρμοστεί για τις συναρτήσεις

$$f(n) = \begin{cases} 2 & \text{αν } n \text{ είναι περιττός} \\ 1 & \text{αλλιώς} \end{cases}$$

και

$$g(n) = \begin{cases} 3 & \text{αν } n \text{ είναι περιττός} \\ 1 & \text{αλλιώς} \end{cases}$$

γιατί το όριο δεν υπάρχει. Εύκολα όμως μπορεί ναδειχτεί, με άμεση χρήση του ορισμού, ότι υπάρχουν κατάλληλα c και n_0 τέτοια ώστε $f(n) = O(g(n))$.

ΜΕΘΟΔΟΣ 8.1. Πως αποδεικνύουμε ότι $f(n) = O(g(n))$;

Οι δυο πιο βασικές μέθοδοι είναι:

- Βρίσκουμε κατάλληλα c και n_0 .

Για παράδειγμα, για να δείξουμε ότι $n^2 = O(2^n)$, βρίσκουμε $c = 1$ και $n_0 = 4$ και επιβεβαιώνουμε με μαθηματική επαγωγή ότι $n^2 \leq c2^n$ για $n \geq n_0$.

- Για θετικές συναρτήσεις $f(n)$ και $g(n)$, δείχνουμε ότι το όριο

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)}$$

υπάρχει και είναι κάποια σταθερά (δεν είναι ∞ δηλαδή).

Για παράδειγμα, για να δείξουμε πως $2n + 5 = O(n)$, βρίσκουμε ότι το όριο $\lim_{n \rightarrow \infty} (2n + 5)/n$ υπάρχει και είναι ίσο με 2 που είναι σταθερά.

ΜΕΘΟΔΟΣ 8.2. Πως αποδεικνύουμε το αντίστροφο, δηλαδή ότι δεν ισχύει $f(n) = O(g(n))$;

Οι δυο πιο βασικές μέθοδοι είναι πάλι:

- Δείχνουμε με απαγωγή σε άτοπο ότι δεν υπάρχουν κατάλληλα c και n_0 .
Για παράδειγμα, ας δείξουμε με απαγωγή σε άτοπο ότι δεν ισχύει $n^2 = O(n)$. Έστω ότι υπήρχαν κατάλληλες σταθερές c και n_0 . Ας θεωρήσουμε την τιμή $n = \lceil \max\{n_0, c + 1\} \rceil$. Αφού $n \geq n_0$, θα πρέπει να έχουμε $n^2 \leq cn$. Ισοδύναμα $n \leq c$, άτοπο.
- Για θετικές συναρτήσεις $f(n)$ και $g(n)$, δείχνουμε ότι το όριο

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)}$$

υπάρχει και είναι ∞ .

Για παράδειγμα, για να δείξουμε πως δεν ισχύει $n^2 = O(n \log n)$, βρίσκουμε ότι το όριο $\lim_{n \rightarrow \infty} \frac{n^2}{n \log n}$ υπάρχει και είναι ίσο με ∞ .

8.2 Οι συμβολισμοί και Ω

Η σχέση $f(n) = O(g(n))$ σημαίνει πως για μεγάλα n , το $f(n)$ φράσσεται από ένα πολλαπλάσιο του $g(n)$. Το αντίστροφο φυσικά, δεν ισχύει πάντα. Για παράδειγμα, ενώ ισχύει $n = O(n^2)$, το αντίστροφο $n^2 = O(n)$ δεν ισχύει. Ανάλογα λοιπόν με τον συμβολισμό O που βάζει κάποιο άνω φράγμα στο ρυθμό αύξησης μιας συνάρτησης, χρησιμοποιείται και ο συμβολισμός Ω που βάζει κάποιο κάτω φράγμα στο ρυθμό αύξησης μιας συνάρτησης.

Ορισμός 52. Έστω f και g δυο συναρτήσεις από τους μη αρνητικούς ακέραιους στο σύνολο των πραγματικών αριθμών. Θα λέμε ότι $f(n) = \Omega(g(n))$ αν υπάρχουν μη αρνητικές σταθερές c και n_0 τέτοιες ώστε

$$f(n) \geq c \cdot g(n)$$

για κάθε $n \geq n_0$.

Κάθε πρόταση για το συμβολισμό O έχει την ανάλογή τους στο συμβολισμό Ω . Το παρακάτω θεώρημα δείχνει τη σχέση των συμβολισμών O και Ω .

Θεώρημα 53. Αν $f(n) = O(g(n))$ τότε $g(n) = \Omega(f(n))$

Απόδειξη. Με άμεση εφαρμογή του ορισμού. Ένα σημαντικό στοιχείο της απόδειξης είναι ότι η σταθερά c στον ορισμό των συμβολισμών O και Ω είναι θετική.

Πιο συγκεκριμένα, αφού $f(n) = O(g(n))$, υπάρχουν θετικές σταθερές c και n_0 , τέτοιες ώστε $f(n) \leq c \cdot g(n)$. Από αυτό, και το γεγονός πως η σταθερά c είναι θετική, προκύπτει άμεσα ότι $g(n) \geq \frac{1}{c}f(n)$. Συνεπώς υπάρχουν θετικές σταθερές $c' = 1/c$ και $n'_0 = n_0$, τέτοιες ώστε $g(n) \geq c'f(n)$ για κάθε $n \geq n'_0$. \square

Ορισμός 54. Αν για δυο συναρτήσεις $f(n)$ και $g(n)$ ισχύει $f(n) = O(g(n))$ και $f(n) = \Omega(g(n))$, τότε λέμε πως $f(n) = \Theta(g(n))$.

Η σχέση $f(n) = \Theta(g(n))$ δείχνει ότι οι δυο συναρτήσεις έχουν τον ίδιο ρυθμό αύξησης. Για παράδειγμα, αν $f(n)$ και $g(n)$ είναι πολυώνυμα του ίδιου βαθμού, τότε $f(n) = \Theta(g(n))$.

Όταν αναλύουμε ένα αλγόριθμο είναι προτιμότερο να εκφράζουμε το χρόνο εκτέλεσης με Θ αντί με O , γιατί η σχέση Θ είναι πιο ακριβής από τη σχέση O . Έτσι όταν λέμε πως ένας αλγόριθμος έχει χρόνο εκτέλεσης $O(n^2)$, ο χρόνος εκτέλεσης μπορεί να είναι πολύ μικρότερος του n^2 , π.χ. $n \log n$. Αντίθετα, όταν λέμε πως ένας αλγόριθμος έχει χρόνο εκτέλεσης $\Omega(n^2)$, ο χρόνος εκτέλεσης δεν μπορεί να είναι $n \log n$.

Το επόμενο θεώρημα χαρακτηρίζει το ρυθμό αύξησης των χρόνων των πιο κοινών αλγορίθμων.

Θεώρημα 55. Οι παρακάτω συναρτήσεις είναι σε αύξουσα σειρά (από αριστερά προς τα δεξιά και από πάνω προς τα κάτω) με την έννοια ότι αν μια συνάρτηση $f(n)$ είναι πριν από μια συνάρτηση $g(n)$, τότε ισχύει $f(n) = O(g(n))$ και δεν ισχύει $f(n) = \Theta(g(n))$.

Σταθερές:	1					
Υπολογαριθμικές:	$\log \log n$					
Λογαριθμικές:	$\log n$	$\log^2 n$				
Πολυωνυμικές:	\sqrt{n}	n	$n \log n$	n^2		
Υποεκθετικές:	$n^{\log n}$					
Εκθετικές:	$2^{\sqrt{n}}$	2^n	3^n	$n!$	n^n	2^{n^2}
Υπερεκθετικές:	2^{2^n}					

Η απόδειξη του θεωρήματος αφήνεται για άσκηση (Άσκηση 8.12). αρκεί να δείχτεί ότι για κάθε δυο συνεχόμενες συναρτήσεις της σειράς $f(n)$ και $g(n)$ ισχύει $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$.

Ασκήσεις

8.1. Δείξτε τις παρακάτω σχέσεις βρίσκοντας κατάλληλες σταθερές c και n_0 του ορισμού του συμβολισμού O :

1. $n = O(2n + \log n)$.

2. $4n^2 = O(n^2 - 10)$

3. $n^3 2^n = O(4^n)$

8.2. Δείξτε τις παρακάτω σχέσεις χρησιμοποιώντας το Θεώρημα 51:

1. $n = \Omega(2n + \log n)$

2. $4n^2 = \Theta(n^2 - 10)$

3. $n^3 2^n = O(4^n)$

8.3. Δείξτε ότι οι παρακάτω σχέσεις δεν ισχύουν:

1. $n^3 + n^2 = O(n^2 \log n)$

2. $(\log n)^{\log n} = \Theta(n)$

3. $f(n) = \Omega(g(n))$ όπου

$$f(n) = \begin{cases} n & \text{αν } n \text{ είναι περιττός} \\ n^2 & \text{αν } n \text{ είναι άρτιος} \end{cases}$$

και

$$g(n) = \begin{cases} n^2 & \text{αν } n \text{ είναι περιττός} \\ n & \text{αν } n \text{ είναι άρτιος} \end{cases}$$

8.4. Η παρακάτω απόδειξη είναι λανθασμένη. Πού είναι το λάθος;

Θα δείξουμε με μαθηματική επαγωγή πως $n^2 = O(n)$. Για τη βάση της επαγωγής $n = 1$, ισχύει $n^2 = 1 \cdot n$. Έστω ότι η πρόταση ισχύει για κάποιο n , δηλαδή $n^2 = O(n)$. Θα δείξουμε πως η πρόταση ισχύει για $n + 1$. Πράγματι,

$$(n+1)^2 = n^2 + 2n + 1 = O(n) + n + 1 = O(n+1) + n + 1 = O(2(n+1)) = O(n+1).$$

8.5. Η παρακάτω απόδειξη είναι λανθασμένη. Πού είναι το λάθος;

Θα δείξουμε με μαθηματική επαγωγή πως $n^2 = O(n)$. Ας διαλέξουμε $n_0 = 1$. Θα δείξουμε πως για κάθε $n \geq n_0$ υπάρχει σταθερά c τέτοια ώστε $n^2 \leq cn$.

Για τη βάση της επαγωγής $n = 1$, υπάρχει η σταθερά $c = 1$ γιατί $n^2 = 1 \cdot n$. Έστω ότι η πρόταση ισχύει για κάποιο n , δηλαδή ότι υπάρχει σταθερά c τέτοια ώστε $n^2 \leq cn$. Θα δείξουμε πως η πρόταση ισχύει για $n + 1$. Πράγματι,

$$(n + 1)^2 = n^2 + 2n + 1 \leq cn + 2n + 1 \leq cn + 2n + n \leq (c + 3)n.$$

Από την επαγωγική υπόθεση η c είναι σταθερά και επομένως η $c + 3$ είναι σταθερά. Δείξαμε λοιπόν ότι υπάρχει κατάλληλη σταθερά και για $n + 1$.

8.6. Δεν είναι αλήθεια πως όλες οι συναρτήσεις από το σύνολο των μη αρνητικών ακεραίων στο σύνολο των πραγματικών αριθμών μπορούν να διαταχθούν με το συμβολισμό O . Δώστε ένα παράδειγμα δυο θετικών συναρτήσεων $f(n)$ και $g(n)$ για τις οποίες δεν ισχύει ούτε $f(n) = O(g(n))$ ούτε $g(n) = O(f(n))$.

8.7. Αποδείξτε προσεκτικά το Θεώρημα 50.

8.8. Δείξτε πως αν δυο συναρτήσεις $f(n)$ και $g(n)$ είναι θετικές με $f(n) = \Theta(g(n))$, τότε $(f(n))^2 = \Theta((g(n))^2)$. Δείξτε επίσης ότι αυτό δεν ισχύει για όλες τις συναρτήσεις, αν δηλαδή αφαιρέσουμε τον περιορισμό πως οι συναρτήσεις είναι θετικές.

8.9. Αυτή η άσκηση είναι γενίκευση της προηγούμενης. Δείξτε πως για θετικές συναρτήσεις αν $f_1(n) = \Theta(g_1(n))$ και $f_2(n) = \Theta(g_2(n))$, τότε $f_1(n)f_2(n) = \Theta(g_1(n)g_2(n))$.

8.10. Δώστε συναρτήσεις $f(n)$ και $g(n)$ για τις οποίες ισχύει $f(n) = O(g(n))$ αλλά δεν ισχύει $2^{f(n)} = O(2^{g(n)})$.

8.11. Δείξτε πως αν για δυο συναρτήσεις $f(n)$ και $g(n)$ με $g(n) \geq 2$ ισχύει $f(n) = O(g(n))$, τότε θα ισχύει και $\log f(n) = O(\log g(n))$.

Ο περιορισμός $g(n) \geq 2$, εγγυάται πως $\log g(n) \geq 1$. Ισχύει η πρόταση αν αφαιρέσουμε τον περιορισμό $g(n) \geq 2$;

8.12. Αποδείξτε το Θεώρημα 55.

9 Γράφοι

Θα ασχοληθούμε με το πολύ σημαντικό θέμα των γράφων. Κάποιοι συγγραφείς τους ονομάζουν γραφήματα, άλλα εμείς εδώ θα προτιμήσουμε τη λιτή μορφή ‘γράφοι’. Στα επόμενα σχήματα βλέπουμε κάποια χαρακτηριστικά παραδείγματα γράφων.

Οι γράφοι παίζουν πολύ σημαντικό ρόλο στην Πληροφορική αλλά και σε άλλες επιστήμες. Υπάρχουν πολλοί λόγοι για τους οποίους συμβαίνει αυτό: Ο πιο σημαντικός φαίνεται να είναι πως έχουμε πολλή καλή αντίληψη για τους γράφους, τους ‘καταλαβαίνουμε’. Σε αυτό βοηθάει πολύ η εποπτική δυνατότητα που μας δίνει η σχεδιάσή τους στο χαρτί ή στην οθόνη. Αυτός ο λόγος σε συνδυασμό με τις πολλές εφαρμογές τους, τούς καθιστά κεντρικό αντικείμενο της Πληροφορικής. Αλλά γιατί οι γράφοι έχουν πολλές εφαρμογές; Ουσιαστικά οι γράφοι συσχετίζουν ζεύγη στοιχείων ενός συνόλου και αυτό μας επιτρέπει να εκφράσουμε πολλές έννοιες σαν ιδιότητες γράφων¹.

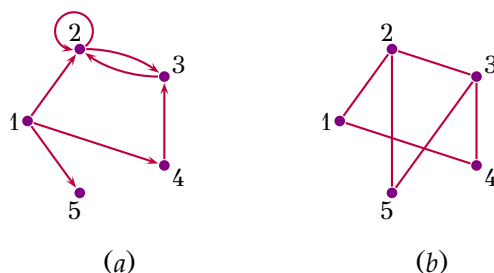
Δυο είναι τα συστατικά στοιχεία ενός γράφου, το σύνολο των κόμβων του, που συνήθως το συμβολίζουμε με V , και το σύνολο των ακμών του, που συνήθως το συμβολίζουμε με E . Υπάρχουν δυο είδη γράφων, οι κατευθυνόμενοι και οι μη κατευθυνόμενοι γράφοι. Στο Σχήμα 9.1, ο πρώτος γράφος είναι κατευθυνόμενος και ο δεύτερος μη κατευθυνόμενος.

Στους κατευθυνόμενους γράφους, η κάθε ακμή έχει ένα αρχικό κόμβο και ένα τελικό κόμβο. Αλλά στους μη κατευθυνόμενους γράφους, οι δυο κόμβοι κάθε ακμής δεν διαφοροποιούνται.

Ορισμός 56. Κατευθυνόμενος γράφος είναι ένα σύνολο V , του οποίου τα στοιχεία ονομάζονται κόμβοι, και ένα σύνολο E που είναι υποσύνολο του $V \times V$ και του οποίου τα στοιχεία ονομάζονται ακμές:

$$E \subseteq \{(u, v) : u, v \in V\}$$

¹Αν αντί να συσχετίσουμε ζεύγη, συσχετίζαμε τριάδες, τετράδες κλπ. θα παίρναμε αυτό που ονομάζουμε υπεργράφο. Είναι ίσως άξιο απορίας γιατί τόσο μεγάλος αριθμός εφαρμογών χρησιμοποιεί απλούς γράφους αντί για υπεργράφους, που έχουν πολύ πλουσιότερη εκφραστική ικανότητα. Ίσως γιατί δεν έχουμε την ίδια εποπτική αντίληψη γι’ αυτούς.



Σχήμα 9.1: Παραδείγματα κατευθυνόμενου και μη κατευθυνόμενου γράφου

Συνήθως συμβολίζουμε τον γράφο σαν $G(V, E)$.

Μια ακμή ενός κατευθυνόμενου γράφου που έχει τον ίδιο αρχικό και τελικό κόμβο ονομάζεται βρόχος (για παράδειγμα, στο Σχήμα 9.1 ο κόμβος 2 έχει βρόχο). Συνήθως ενδιαφερόμαστε για γράφους χωρίς βρόχους.

Οι μη κατευθυνόμενοι γράφοι είναι η ειδική κατηγορία κατευθυνόμενων γράφων που

- δεν έχουν βρόχους
- είναι συμμετρικοί, δηλαδή για κάθε ακμή (u, v) υπάρχει και η αντίθετη της (v, u) .

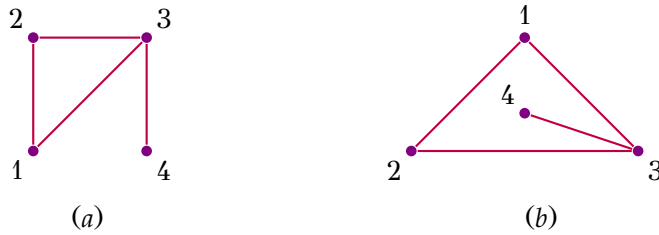
Εναλλακτικά, ένας μη κατευθυνόμενος γράφος $G(V, E)$ ορίζεται από το σύνολο των κόμβων του V και το σύνολο των ακμών του E . Κάθε ακμή είναι ένα υποσύνολο του V με δυο κόμβους.

$$E \subset \{\{u, v\} : u, v \in V\}$$

Από σύμβαση μια ακμή ενός μη κατευθυνόμενου γράφου με κόμβους u και v τη συμβολίζουμε με $[u, v]$.

Ο πρώτος ορισμός ενός μη κατευθυνόμενου γράφου, σαν ειδική περίπτωση των κατευθυνόμενων γράφων, είναι μερικές φορές πολύ χρήσιμος. Κάθε πρόταση που ισχύει για τους κατευθυνόμενους γράφους ισχύει φυσικά και για τους μη κατευθυνόμενους γράφους. Το αντίθετο βέβαια δεν ισχύει πάντα.

Όταν αναφερόμαστε απλά σε γράφους, χωρίς επιθετικό προσδιορισμό ‘κατευθυνόμενος’ και ‘μη κατευθυνόμενος’, συνήθως εννοούμε μη κατευθυνόμενους γράφους και αυτή τη σύμβαση θα κρατήσουμε εδώ.



Σχήμα 9.2: Γραφικές παραστάσεις του ίδιου γράφου

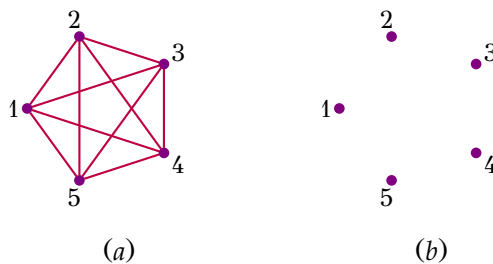
Ένα μεγάλο πλεονέκτημα των γράφων είναι πως μπορούν να σχεδιαστούν με απλό τρόπο σε μια επίπεδη επιφάνεια (χαρτί, οθόνη). Αν και οι γράφοι είναι, με βάση τον παραπάνω ορισμό τους, στην ουσία αλγεβρικά αντικείμενα, εν τούτοις συχνά τους ταυτίζουμε με το σχέδιό τους.

ΠΑΡΑΔΕΙΓΜΑ 9.1 (Σχεδίαση Γράφων). Ο γράφος $G(V, E)$ με σύνολο κόμβων $V = \{1, 2, 3, 4\}$ και σύνολο ακμών $E = \{[1, 2], [1, 3], [2, 3], [3, 4]\}$ σχεδιάζεται όπως φαίνεται στο Σχήμα 9.2(a). Δεν πρέπει να συγχέουμε τον γράφο με τη σχεδίασή του. Εξ' άλλου, ένας γράφος έχει πολλές σχεδιάσεις. Για παράδειγμα, στο Σχήμα 9.2(b) βλέπουμε μια άλλη σχεδίαση του ίδιου γράφου.

9.1 Ειδικές κατηγορίες γράφων

Κάποιοι γράφοι χρησιμοποιούνται συχνά και γι' αυτό τους έχουμε δώσει ονόματα. Μερικοί από αυτούς είναι:

Πλήρης Είναι ο γράφος που περιέχει όλες τις ακμές μεταξύ n κόμβων. Τον ονομάζουμε επίσης κλίκα και τον συμβολίζουμε με K_n . Στο Σχήμα 9.3(a) βλέπουμε τον K_5 .

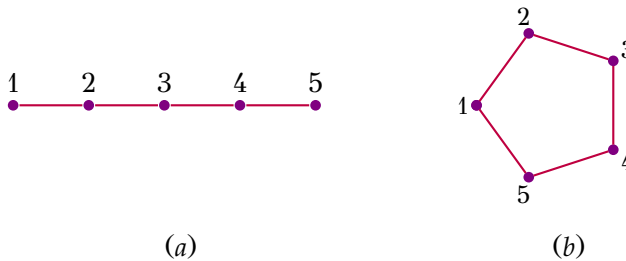


Σχήμα 9.3: Οι γράφοι K_5 και $\overline{K_5}$

Κενός Είναι ο συμπληρωματικός του πλήρους γράφου. Δεν έχει καμία ακμή. Τον ονομάζουμε και ανεξάρτητο σύνολο κόμβων και τον συμβολίζουμε με $\overline{K_n}$, όπου n είναι ο αριθμός των κόμβων. Στο Σχήμα 9.3(b) βλέπουμε τον $\overline{K_5}$.

Προσέξτε ότι σε ένα γράφο δεν χρειάζεται όλοι οι κόμβοι του να είναι ενωμένοι. Ειδικά, ο κενός γράφος έχει τη μικρότερη συνεκτικότητα από όλους τους γράφους, σε αντίθεση με τον πλήρη γράφο που έχει τη μεγαλύτερη συνεκτικότητα. Θα αναφερθούμε παρακάτω εκτενέστερα στη συνεκτικότητα των γράφων.

Μονοπάτι Αποτελείται από n κόμβους ενωμένους ένας μετά τον άλλο. Πιο συγκεκριμένα, το σύνολο των κόμβων είναι $\{1, 2, \dots, n\}$ και σύνολο ακμών $\{[i, i + 1] : i = 1, 2, \dots, n - 1\}$. Τον συμβολίζουμε με P_n . Στο Σχήμα 9.4(b) βλέπουμε τον P_5 .



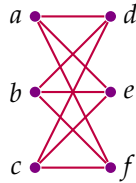
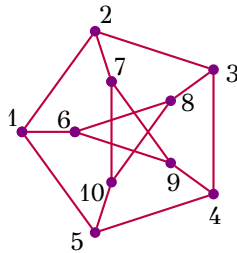
Σχήμα 9.4: Οι γράφοι P_5 και C_5

Κύκλος Είναι σαν το μονοπάτι με την επιπλέον ακμή $[1, n]$, που ενώνει τις άκρες του μονοπατιού. Τον συμβολίζουμε με C_n . Στο Σχήμα 9.4(b) βλέπουμε τον C_5 .

Πλήρης διμερής Αποτελείται από δυο ομάδες κόμβων A και B . Κάθε κόμβος της ομάδας A ενώνεται με κάθε κόμβο της ομάδας B . Τον συμβολίζουμε με $K_{a,b}$, όπου a και b είναι ο αριθμός των κόμβων των ομάδων A και B . Στο Σχήμα 9.5 βλέπουμε τον $K_{3,3}$.

Πέτερσεν (Petersen) Ο γράφος του Πέτερσεν εικονίζεται στο Σχήμα 9.6. Αποτελείται από 10 κόμβους και 15 ακμές. Έχει πολύ ενδιαφέρουσες ιδιότητες και αποτελεί το μικρότερο αντιπαράδειγμα σε πολλές αληθοφανείς εικασίες για γράφους. Θα μπορούσε κάποιος να πει, με μικρή μόνο δόση υπερβολής, πως αν μια πρόταση για γράφους είναι αληθοφανής και ο γράφος του Πέτερσεν δεν αποτελεί αντιπαράδειγμα, τότε είναι πολύ πιθανό η πρόταση να ισχύει για όλους τους γράφους.

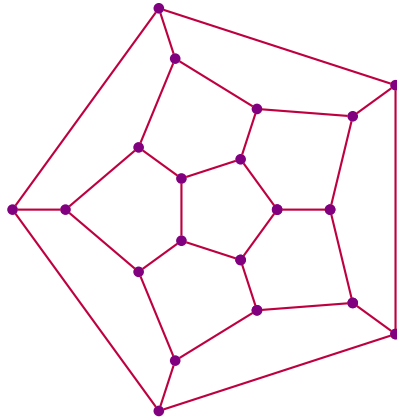
Δωδεκάεδρο Ο γράφος του δωδεκάεδρου. Εικονίζεται στο Σχήμα 9.7.

Σχήμα 9.5: Ο γράφος $K_{3,3}$ 

Σχήμα 9.6: Ο γράφος του Petersen

Η Θεωρία Γράφων είναι εκτενής με βαθιά αποτελέσματα. Είναι επίσης από τις περιοχές των Μαθηματικών που κάποια βασικά θεωρήματα μπορούν να γίνουν αντιληπτά από κάποιον μη ειδικό. Αλλά όπως όλες οι σημαντικές περιοχές των Μαθηματικών, με εξαίρεση ίσως τη Θεωρία Αριθμών, απαιτεί από το σπουδαστή να απομνημονεύσει αρκετούς ορισμούς πριν αρχίσει να βλέπει ‘ψαχνό’. Πολλοί από αυτούς τους ορισμούς δεν χρησιμοποιούνται σχεδόν καθόλου σε ένα εισαγωγικό βιβλίο ή μάθημα. Έτσι ένα βιβλίο ή μάθημα Μαθηματικών που πρέπει να δώσει έμφαση στην ουσία, στο ψαχνό, που δεν είναι παρά μόνο οι ουσιαστικές προτάσεις, τα θεωρήματα, οι τεχνικές και τα λήμματα, αναλύσεται σε φαινομενικά ανούσιες περιγραφές και ορισμούς. Χαρακτηριστικό παράδειγμα, είναι η αναφορά παραπάνω στον γράφο του Πέτερσεν. Αν και το κείμενο ανακοινώνει στον αναγνώστη πως πρόκειται για γράφο με σημαντικές ιδιότητες, καμία τέτοια ιδιότητα δεν έχει αναφερθεί ακόμα. Για να γίνει όμως αυτό χρειάζεται να εισάγουμε επιπλέον έννοιες, όπως χρωματισμός γράφου, κύκλος του Hamilton και άλλες.

Ευτυχώς υπάρχουν κάποια αποτελέσματα της Θεωρίας Γράφων που μπορούν να εκφραστούν με ελάχιστη ορολογία. Θα δούμε ένα τέτοιο αμέσως μόλις ορίσουμε την πολύ απλή έννοια του βαθμού ενός κόμβου:



Σχήμα 9.7: Το δωδεκάεδρο

Ο βαθμός ενός κόμβου είναι ο αριθμός των γειτόνων του. Για παράδειγμα, στο γράφο του Σχήματος 9.2, οι κόμβοι 1, 2, 3, 4 έχουν βαθμούς 2, 2, 3, 1 αντίστοιχα. Αν προσθέσουμε τους βαθμούς, το άθροισμα $2+2+3+1=8$ είναι άρτιο. Αυτό δεν είναι σύμπτωση, αλλά ισχύει σε κάθε γράφο, όπως δηλώνει το παρακάτω θεώρημα.

Θεώρημα 57. Σε κάθε γράφο, το άθροισμα των βαθμών όλων των κόμβων είναι άρτιο.

Απόδειξη. Ο λόγος που ισχύει το θεώρημα είναι απλός: κάθε ακμή συνεισφέρει στον βαθμό δυο κόμβων. Εναλλακτικά μπορούμε να αποδείξουμε το θεώρημα με επαγωγή στον αριθμό των ακμών ενός γράφου.

Βάση της επαγωγής: Αν ο γράφος δεν έχει καμία ακμή, ο βαθμός όλων των κόμβων είναι 0. Επομένως, το άθροισμα των βαθμών όλων των κόμβων είναι 0, που είναι άρτιος αριθμός.

Επαγωγικό Βήμα: Η επαγωγική υπόθεση είναι πως κάθε γράφος m ακμών έχει άρτιο άθροισμα βαθμών. Ας θεωρήσουμε ένα γράφο με $m+1$ ακμές. Έστω $[u, v]$ μια ακμή του γράφου. Ας αφαιρέσουμε την ακμή $[u, v]$. Από την επαγωγική υπόθεση ο γράφος που προκύπτει έχει άρτιο άθροισμα βαθμών. Πώς αλλάζει το άθροισμα των βαθμών όταν ξαναπροσθέσουμε την ακμή $[u, v]$; Αυξάνει κατά 2, γιατί αλλάζουν μόνο οι βαθμοί των κόμβων u και v και ο καθένας από αυτούς αυξάνεται κατά μια μονάδα. Άρα το άθροισμα των βαθμών παραμένει άρτιο. \square

Αυτό το απλό και φαινομενικά ‘αθώο’ θεώρημα έχει πολλές επιπτώσεις. Μπορούμε αμέσως να συμπεράνουμε αμέσως τη παρακάτω

ισοδύναμη πρόταση.

Πόρισμα 58. Σε κάθε γράφο, ο αριθμός των κόμβων περιττού βαθμού είναι άρτιος.

Πως προκύπτει το πόρισμα αυτό; Από το γεγονός πως όταν το άθροισμα n αριθμών είναι άρτιο, τότε ο αριθμός των περιττών όρων πρέπει να είναι άρτιος. Για το γράφο του Σχήματος 9.2, το άρτιο άθροισμα $2 + 2 + 3 + 1$ έχει δυο περιττούς όρους που αντιστοιχούν στους δυο κόμβους με περιττό βαθμό, τους κόμβους 3 και 4.

Το παραπάνω θεώρημα και πόρισμα μπορούν να χρησιμοποιηθούν σε περιπτώσεις που δεν φαίνεται από την πρώτη ματιά να σχετίζονται με τη Θεωρία Γράφων. Για παράδειγμα, η επόμενη πρόταση ισχύει για κάθε ομάδα με περιττό αριθμό μελών: Υπάρχει πάντα κάποιος που έχει άρτιο αριθμό γνωστών. Υποθέτουμε βέβαια πως η σχέση γνωριμίας είναι συμμετρική: Αν ο u γνωρίζει τον v τότε και ο v γνωρίζει τον u . Για να δείξουμε την παραπάνω πρόταση, ας θεωρήσουμε το γράφο με κόμβους τα μέλη της ομάδας και ακμές μεταξύ των ζευγών γνωστών. Δηλαδή, η ακμή $[u, v]$ υπάρχει αν και μόνο αν ο u και ο v γνωρίζονται. Σε αυτό το γράφο, ο βαθμός κάθε κόμβου είναι ίσος με τον αριθμό των γνωστών του. Αφού όμως από την υπόθεση ο γράφος έχει περιττό αριθμό κόμβων, δεν μπορεί με βάση το πόρισμα όλοι οι κόμβοι να έχουν περιττό βαθμό: κάποιος κόμβος έχει άρτιο βαθμό. Το γεγονός πως ο αριθμός των μελών είναι περιττός παίζει κεντρικό ρόλο στην απόδειξη. Εξάλλου, η πρόταση δεν ισχύει για ομάδες με άρτιο αριθμό μελών, όπως μπορούμε εύκολα να διαπιστώσουμε.

9.2 Περιγραφή γράφων σε υπολογιστή

Η μελέτη των τρόπων με τους οποίους μπορούμε να περιγράψουμε μια κλάση αντικειμένων στον υπολογιστή δεν έχει μόνο την προφανή αξία, να μας βοηθάει δηλαδή στην σύνταξη κατάλληλων προγραμμάτων, αλλά και μια βαθύτερη, πιο μαθηματική χρησιμότητα. Μας κάνει να σκεφτούμε πια χαρακτηριστικά των αντικειμένων προς περιγραφή.

Για παράδειγμα, μπορεί ένας γράφος να περιγραφεί μόνο με το σύνολο των ακμών του; Αν σας φαίνεται πως η απάντηση είναι προφανώς καταφατική, σκεφτείτε το ξανά. Πως θα περιγράψουμε τον κενό γράφο των 10 κόμβων; των 100 κόμβων; Το σύνολο των δυο αυτών γράφων είναι κενό, αλλά οι δυο γράφοι διαφέρουν. Συμπεραίνουμε λοιπόν πως η περιγραφή ενός γράφου πρέπει να περιέχει άμεσα ή έμμεσα τον αριθμό των κόμβων του.

Δυο είναι οι συνηθισμένοι τρόποι περιγραφής γράφων σε υπολογιστή: με τις λίστες γειτνίασης ή με τον πίνακα γειτνίασης.

Λίστες γειτνίασης: Παραθέτουμε τη λίστα των γειτόνων κάθε κόμβου, συμπεριλαμβανομένων των κόμβων με κανένα γείτονα. Για παράδειγμα, ο γράφος του Σχήματος 9.1(a) έχει την εξής περιγραφή:

1: 2, 4, 5
 2: 2, 3
 3: 2
 4: 3
 5:

Στον υπολογιστή, το σύνολο των γειτόνων κάθε κόμβου αποθηκεύεται σε λίστα. Η περιγραφή αυτή σαν δομή δεδομένων είναι ένας πίνακας από λίστες.

Η περιγραφή αυτή έχει το πλεονέκτημα πως είναι οικονομική για γράφους με λίγες ακμές. Πιο συγκεκριμένα, για ένα γράφο με V κόμβους και E ακμές, η περιγραφή έχει μήκος περίπου $V + E$. Η περιγραφή με λίστες γειτνίασης είναι επίσης κατάλληλη για κάποιους αλγορίθμους γράφων. Το βασικό μειονέκτημα της περιγραφής αυτής είναι πως απαιτεί πολύ χρόνο να ελέγξουμε αν μια συγκεκριμένη ακμή ανήκει στο γράφο. Πιο συγκεκριμένα, αν θέλουμε να βρούμε αν η ακμή (u, v) ανήκει στο γράφο, χρειάζεται να διασχίσουμε τη λίστα του κόμβου u , που μπορεί να πάρει V βήματα στη χειρότερη περίπτωση.

Πίνακας γειτνίασης: Αυτή την περιγραφή γίνεται με ένα πίνακα G μεγέθους $V \times V$, όπου $G_{u,v}$ έχει τιμή 1 αν η ακμή (u, v) υπάρχει στον γράφο, αλλιώς έχει τιμή 0. Η περιγραφή αυτή σαν δομή δεδομένων είναι ένας δισδιάστατος πίνακας. Για παράδειγμα, ο γράφος του Σχήματος 9.1(a) έχει την περιγραφή

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

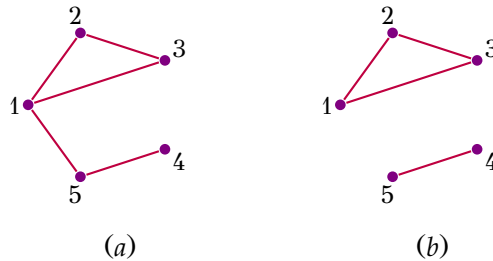
Το πλεονέκτημα αυτής της περιγραφής είναι πως μπορούμε αμέσως να βρούμε αν μια συγκεκριμένη ακμή ανήκει στο γράφο κοιτάζοντας την κατάλληλη θέση στον πίνακα. Ένα άλλο πλεονέκτημα της είναι πως γενικεύεται πολύ εύκολα σε γράφους που έχουν βάρη στις ακμές. σε αυτή την περίπτωση, ο πίνακας δεν περιέχει 0 και 1 αλλά τα βάρη των ακμών.

Το βασικό μειονέκτημα της είναι πως για γράφους με λίγες ακμές, η περιγραφή έχει πολύ μεγαλύτερο μέγεθος από την παράσταση με λίστες γειτνίασης. Η περιγραφή αυτή απαιτεί ακριβώς V^2 δυαδικά ψηφία. Για παράδειγμα, ο γράφος του παγκόσμιου ιστού (με κόμβους τις σελίδες και ακμές τα links μεταξύ αυτών) έχει σήμερα κάπου 10 δισεκατομμύρια κόμβους. Αν τον περιγράφαμε με πίνακα γειτνίασης θα χρειαζόταν περίπου 10^{20} δυαδικά ψηφία, που είναι αδύνατο να χωρέσουν σε κάποιο σημερινό σκληρό δίσκο.

Οι παραπάνω περιγραφές γράφων είναι ίδιες για τους κατευθυνόμενους και μη κατευθυνόμενους γράφους. Αλλά τους μη κατευθυνόμενους γράφους κάθε ακμή εμφανίζεται δυο φορές στη δομή δεδομένων. Αυτό όχι μόνο διπλασιάζει τον απαιτούμενο αποθηκευτικό χώρο, αλλά εισάγει και προβλήματα συνέπειας της περιγραφής. Για παράδειγμα, αν ένα πρόγραμμα προσθέσει μια ακμή στη λίστα γειτνίασης, πρέπει να το κάνει σε δυο μέρη.

9.3 Δένδρα και Συνεκτικότητα

Μια σημαντική ιδιότητα γράφων είναι η συνεκτικότητα. Ένας γράφος ονομάζεται συνεκτικός αν όλοι οι κόμβοι του είναι ενωμένοι. Για παράδειγμα, στο Σχήμα 9.8 ο γράφος (a) είναι συνεκτικός ενώ ο γράφος (b) δεν είναι. Ο ορισμός όμως που δώσαμε για συνεκτικούς γράφους δεν είναι αυστηρός. Για να τον κάνουμε αυστηρό, ας ορίσουμε πρώτα μια νέα έννοια:



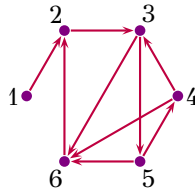
Σχήμα 9.8: Παραδείγματα συνεκτικού και μη συνεκτικού γράφου

Ορισμός 59. Σε ένα κατευθυνόμενο γράφο, θα ονομάζουμε μονοπάτι από τον κόμβο s στον κόμβο t μια ακολουθία κόμβων u_0, u_1, \dots, u_k με πρώτο στοιχείο τον κόμβο $s = u_0$, τελευταίο στοιχείο τον κόμβο $t = u_k$ και τέτοια ώστε τα (u_{i-1}, u_i) για $i = 1, \dots, k$ να είναι ακμές του γράφου.

Το μήκος του μονοπατιού είναι ο αριθμός των ακμών του, δηλαδή k . Το μονοπάτι ονομάζεται απλό αν οι κόμβοι της ακολουθίας δεν επαναλαμβάνονται.

Για παράδειγμα, το μονοπάτι $(1, 2, 3, 5)$ στον γράφο του Σχήματος 9.9 είναι απλό, αλλά το μονοπάτι $(2, 3, 5, 4, 3, 6)$ δεν είναι. Συνήθως όταν αναφερόμαστε στα μονοπάτια εννοούμε τα απλά μονοπάτια.

Προσέξτε πως οι περισσότεροι ορισμοί, όπως ο παραπάνω ορισμός, αφορά τους κατευθυνόμενους γράφους. Αφού οι μη κατευθυνόμενοι



Σχήμα 9.9: Μονοπάτια σε γράφους

γράφοι αποτελούν ειδική κατηγορία κατευθυνόμενων γράφων, οι οποίοι εφαρμόζονται άμεσα και σε αυτούς.

Όταν ένα μονοπάτι έχει κοινή αρχή και τέλος, το ονομάζουμε κύκλο. Για παράδειγμα στο γράφο του Σχήματος 9.9, η ακολουθία κόμβων $(2, 3, 5, 4, 6, 2)$ είναι κύκλος. Το μήκος ενός κύκλου είναι ο αριθμός των ακμών του. Για παράδειγμα ο κύκλος του παραδείγματος έχει μήκος 5. Ειδικά για τους μη κατευθυνόμενους γράφους όταν αναφερόμαστε σε κύκλους, υποθέτουμε ότι έχουν τουλάχιστον 3 διαφορετικούς κόμβους (για να αποφύγουμε την τετριμμένη περίπτωση των κύκλων μήκους 2, δηλαδή της μορφής (u, v, u)).

Οι κύκλοι παίζουν μεγάλο ρόλο στη μελέτη της δομής των γράφων. Οι γράφοι που δεν περιέχουν κύκλους περιττού μήκους ονομάζονται διμερείς. Οι κόμβοι ενός διμερούς γράφου μπορούν να χωριστούν σε δυο ομάδες L και R έτσι ώστε οι ακμές να ενώνουν κόμβους του L με κόμβους του συνόλου R . Τους διμερείς γράφους τους συμβολίζουμε με $G(L+R, E)$.

Τώρα μπορούμε να ορίσουμε με ακρίβεια ποιοι είναι οι συνεκτικοί γράφοι.

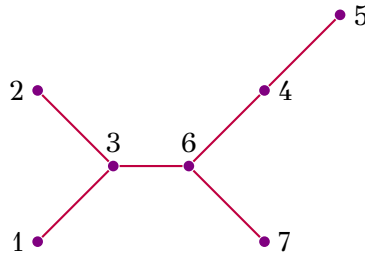
Ορισμός 60. Ένα μη κατευθυνόμενος γράφος ονομάζεται συνεκτικός αν για κάθε ζεύγος κόμβων του u και v υπάρχει μονοπάτι από το u στο v .

Ένας κατευθυνόμενος γράφος που έχει την ιδιότητα αυτή ονομάζεται ισχυρά συνεκτικός.

Η συνεκτικότητα είμαι μια βασική ιδιότητα των γράφων και ικανοποιεί κάποιο είδος μονοτονικότητας, με την έννοια πως αν προσθέσουμε μια ακμή σε ένα συνεκτικό γράφο, ο γράφος παραμένει συνεκτικός. Προς την άλλη κατεύθυνση, αν αρχίσουμε να αφαιρούμε ακμές από κάποιο συνεκτικό γράφο, για πόσο αυτός θα παραμείνει συνεκτικός; Προκύπτει λοιπόν η εξής ενδιαφέρουσα ερώτηση: Ποιοι γράφοι είναι

συνεκτικοί και χάνουν την συνεκτικότητα τους αν αφαιρέσουμε οποιαδήποτε ακμή τους;² Η απάντηση στην ερώτηση αυτή είναι: τα δένδρα. Αλλά τι είναι τα δένδρα;

Ορισμός 61. Δένδρα ονομάζονται οι συνεκτικοί γράφοι που δεν περιέχουν κύκλους.



Σχήμα 9.10: Δένδρο

Για παράδειγμα, ο γράφος του Σχήματος 9.10 είναι δένδρο. Τα δένδρα είναι μια πολύ σημαντική κατηγορία γράφων με πολλές ενδιαφέρουσες ιδιότητες. Είναι εύκολο να παρατηρήσουμε, για παράδειγμα, πως ένα δένδρο δεν περιέχει κύκλους. Πράγματι, αν ένας γράφος περιέχει κάποιο κύκλο και αφαιρέσουμε μια ακμή $[u, v]$ του κύκλου, η συνεκτικότητα του γράφου δεν αλλάζει, αφού οι κόμβοι u και v παραμένουν ενωμένοι μέσω του τμήματος του κύκλου που παραμένει.

Με παρόμοιο τρόπο μπορούμε να δείξουμε πολλές ιδιότητες των δένδρων, που τις παραθέτουμε στο επόμενο θεώρημα. Η απόδειξή τους αφήνεται για άσκηση.

Θεώρημα 62. Οι παρακάτω προτάσεις είναι όλες ισοδύναμες με τον ορισμό των δένδρων:

1. Δένδρα είναι οι συνεκτικοί γράφοι που αν αφαιρέσουμε οποιαδήποτε ακμή τους παύουν να είναι συνεκτικοί. Θα μπορούσαμε δηλαδή να πούμε πως τα δένδρα είναι ελάχιστοι γράφοι ως προς της συνεκτικότητα.

²Τέτοια είδη ερωτήσεων αποτελούν ολόκληρη περιοχή στη Θεωρία Γράφων, την Ακραία Θεωρία Γράφων *Extremal Graph Theory*. Η μελέτη αυτής της περιοχής στρέφεται σε ερωτήσεις της μορφής: Για δεδομένη ιδιότητα γράφων ποιοι είναι οι ελάχιστοι (ή οι μέγιστοι) γράφοι που έχουν αυτή την ιδιότητα; Για παράδειγμα ποιοι είναι οι μέγιστοι γράφοι με n κόμβους που δεν περιέχουν τον K_3 , δηλαδή που καμία τριάδα κόμβων τους δεν σχηματίζει κλίκα;

2. Δένδρα είναι οι γράφοι που δεν έχουν κανένα κύκλο, αλλά αν προσθέσουμε οποιαδήποτε νέα ακμή αποκτούν κάποιο κύκλο. Θα μπορούσαμε να πούμε πως είναι μέγιστοι γράφοι που δεν περιέχουν κύκλους.
3. Δένδρα είναι οι συνεκτικοί γράφοι με $n - 1$ ακμές, όπου n είναι ο αριθμός των κόμβων τους.
4. Δένδρα είναι οι γράφοι που για κάθε ζεύγος κόμβων u και v υπάρχει ένα και μοναδικό μονοπάτι από τον u στον v .

Μια άλλη βασική ιδιότητα των δένδρων είναι η ακόλουθη:

Θεώρημα 63. Σε κάθε δένδρο υπάρχει ένας τουλάχιστον κόμβος με βαθμό 1.

Απόδειξη. Θα δώσουμε δυο αποδείξεις.

Η πρώτη είναι με απαγωγή σε άτοπο και βασίζεται στην ιδιότητα πως ο αριθμός των ακμών ενός δένδρου είναι $n - 1$. Έστω λοιπόν ένα δένδρο του οποίου κάθε κόμβος έχει βαθμό τουλάχιστον 2. Τότε το σύνολο των ακμών του δένδρου είναι τουλάχιστον n , γιατί κάθε κόμβος συνεισφέρει 2 τουλάχιστον ακμές και κάθε ακμή τη μετράμε δυο φορές (μια φορά για κάθε κόμβο της). Αυτό όμως είναι άτοπο, γιατί κάθε δένδρο έχει ακριβώς $n - 1$ ακμές. Μια μικρή παραλλαγή της απόδειξης δείχνει πως υπάρχουν τουλάχιστον 2 κόμβοι με βαθμό 1.

Η δεύτερη απόδειξη είναι η εξής: Σε ένα δένδρο, ας θεωρήσουμε ένα απλό μονοπάτι u_1, \dots, u_k με όσο το δυνατό μεγαλύτερο μήκος (για παράδειγμα, στο δένδρο του Σχήματος 9.10 θεωρούμε το μονοπάτι $(2, 3, 6, 4, 5)$). Το επιχείρημα είναι πως τα άκρα αυτού του μονοπατιού, u_1 και u_k είναι κόμβοι με βαθμό 1. Πράγματι, έστω ότι κάποιο από τα άκρα του μονοπατιού, ας πούμε το u_1 , έχει βαθμό μεγαλύτερο από 1. Θα έχει τότε, εκτός από τον u_2 , κάποιον δεύτερο γείτονα v . Ο v δεν μπορεί να είναι κάποιος από τους κόμβους του μονοπατιού γιατί αυτό θα δημιουργούσε κύκλο. Αφού όμως ο v είναι ένας άλλος κόμβος, θα μπορούσαμε να επεκτείνουμε το μονοπάτι σε (v, u_1, \dots, u_k) . Άτοπο αφού υποθέσαμε πως το μονοπάτι (u_1, \dots, u_k) έχει μέγιστο μήκος. \square

9.4 Επίπεδοι γράφοι

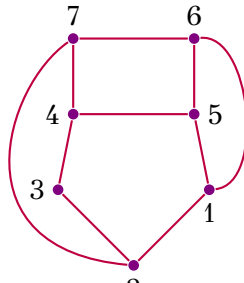
Μια ειδική κατηγορία γράφων με πολλές εφαρμογές είναι οι επίπεδοι γράφοι. Ένας γράφος λέγεται επίπεδος αν υπάρχει τρόπος να σχεδιαστεί στο επίπεδο με τέτοιο τρόπο ώστε οι ακμές του να μην τέμνονται. Για παράδειγμα, ο γράφος του Σχήματος 9.7 είναι επίπεδος, ενώ όπως θα

δούμε παρακάτω ο γράφος K_5 (Σχήμα 9.3(a)) δεν είναι επίπεδος. Άλλοι γράφοι που θα δούμε πως δεν είναι επίπεδοι είναι ο γράφος του Petersen και ο $K_{3,3}$.

Ο Leonard Euler ήταν από τους πρώτους μαθηματικούς που μελέτησαν τις ιδιότητες των γράφων και ειδικότερα των επίπεδων γράφων. Διατύπωσε τον Τύπο του Euler που συσχετίζει τα στοιχεία των επίπεδων γράφων. Στη συνέχεια θα διατυπώσουμε και θα αποδείξουμε τον Τύπο του Euler.

Ας ξεκινήσουμε με την διαισθητική διαπίστωση πως αν ένας γράφος με n κόμβους έχει πάρα πολλές ακμές, τότε δεν θα είναι επίπεδος. Πόσο πολλές; Θα απαντήσουμε σύντομα σε αυτή την ερώτηση. Αλλά υπάρχουν γράφοι που έχουν λίγες σχετικά ακμές, όπως ο γράφος του Petersen, αλλά δεν είναι επίπεδοι. Αν και διαισθητικά φαίνεται να υπάρχει κάποια σχέση μεταξύ των ακμών και των κόμβων ενός επίπεδου γράφου, ο αριθμός των ακμών δεν είναι ο μόνος που καθορίζει αν ένας γράφος είναι επίπεδος. Σαν ένα άλλο παράδειγμα, θεωρείστε ένα γράφο που περιέχει ένα K_5 και άλλους 1000 ανεξάρτητους κόμβους που δεν συνδέονται με κανένα άλλο. Αυτός ο γράφος έχει 1005 κόμβους και μόνο 10 ακμές (όσες και ο K_5) αλλά δεν είναι επίπεδος.

Αυτό που είδε ο Euler είναι πως υπάρχει ακόμα μια παράμετρος που παίζει μεγάλο ρόλο: Ο αριθμός των περιοχών. Πιο συγκεκριμένα, ας θεωρήσουμε τη σχεδίαση ενός επίπεδου γράφου. Οι ακμές της σχεδίασης χωρίζουν το επίπεδο σε περιοχές. Πιο συγκεκριμένα, θα ονομάζουμε περιοχή ένα μέγιστο σύνολο σημείων που δεν περιέχουν σημεία ακμών. Για παράδειγμα, ο γράφος του Σχήματος 9.11 έχει 5 περιοχές, αυτές που περικλείονται από τους κύκλους (1, 2, 3, 4, 5), (1, 5, 6), (2, 3, 4, 7), (4, 5, 6, 7) και (1, 2, 7, 6) (η τελευταία περιοχή είναι η εξωτερική περιοχή στο σχήμα).



Σχήμα 9.11: Επίπεδος γράφος

Θεώρημα 64. (Τύπος του Euler) Σε κάθε συνεκτικό επίπεδο γράφο ο αριθμός των κόμβων n , των ακμών m και των περιοχών f συνδέονται με τη σχέση

$$n - m + f = 2.$$

Απόδειξη. Θα αποδείξουμε το θεώρημα με επαγωγή στον αριθμό των ακμών.

Η βάση της επαγωγής είναι για δένδρα (αφού τα δένδρα είναι οι ελάχιστοι συνεκτικοί γράφοι). Είναι εύκολο να δούμε πως όλα τα δένδρα είναι επίπεδοι γράφοι (αν και αυτό δεν το χρειαζόμαστε στην απόδειξη). Ένα δένδρο με αριθμό κόμβων n έχει αριθμό ακμών $m = n - 1$ και μια μόνο περιοχή, $f = 1$. Προφανώς ο Τύπος του Euler ισχύει για τα δένδρα.

Για το επαγωγικό βήμα, αρκεί να παρατηρήσουμε πως κάθε νέα ακμή σε ένα συνεκτικό γράφο χωρίζει μια περιοχή ακριβώς σε δυο περιοχές. Δηλαδή, όταν το m αυξάνεται κατά 1 τότε και το f αυξάνεται κατά 1, και ο Τύπος του Euler ισχύει. \square

Ο Τύπος του Euler μας δίνει μια ακριβή σχέση μεταξύ κόμβων, ακμών και περιοχών. Αλλά πόσο πυκνός μπορεί να είναι επίπεδος γράφος; Δηλαδή πόσες πολλές ακμές μπορεί να έχει ένας γράφος n κόμβων;

Θεώρημα 65. Σε κάθε συνεκτικό επίπεδο γράφο ο αριθμός των κόμβων n και των ακμών m ικανοποιεί

$$m \leq 3n - 6.$$

Απόδειξη. Η απόδειξη βασίζεται σε δυο παρατηρήσεις:

1. Κάθε ακμή συνορεύει με (το πολύ) δυο περιοχές.
2. Κάθε περιοχή συνορεύει με 3 τουλάχιστον ακμές.

Η βασική ιδέα τώρα είναι να μετρήσουμε με δυο τρόπους τα ζεύγη που περιέχουν μια ακμή και μια γειτονική περιοχή. Για παράδειγμα, στο Σχήμα 9.11 έχουμε τα ζεύγη ακμών-περιοχών ($[1, 2]$, $(1, 2, 3, 4, 5)$), ($[1, 2]$, $(1, 2, 7, 6)$), ..., ($[6, 7]$, $(1, 2, 7, 6)$). Από την πρώτη παρατήρηση προκύπτει πως ο αριθμός των ζευγών είναι το πολύ $2m$ (το πολύ δυο ζεύγη ανά ακμή), ενώ από τη δεύτερη παρατήρηση αυτός ο αριθμός είναι τουλάχιστον $3f$ (τουλάχιστον 3 ζεύγη ανά περιοχή). Άρα πρέπει να έχουμε

$$2m \leq 3f.$$

Αν εξαλείψουμε το f από τον Τύπο του Euler χρησιμοποιώντας αυτή τη σχέση, προκύπτει πως $m \leq 3n - 6$. \square

Το θεώρημα αυτό μπορεί να χρησιμοποιηθεί για ναδειχθεί πως ο K_5 δεν είναι επίπεδος. Προσπαθήστε να σχεδιάσετε τον K_5 στο επίπεδο. Θα παρατηρήσετε πως δεν γίνεται. Αλλά είναι αυτό απόδειξη πως δεν υπάρχει τρόπος; Δεν είναι. Χρησιμοποιώντας όμως το παραπάνω

θεώρημα μπορούμε εύκολα να το αποδείξουμε. Ο K_5 έχει $n = 5$ κόμβους και $m = 10$ ακμές. Δεν ισχύει επομένως πως $m \leq 3n - 6$, άρα δεν είναι επίπεδος.

Ένας άλλος γράφος που παίζει, όπως θα δούμε, μεγάλο ρόλο στο χαρακτηρισμό των επίπεδων γράφων είναι ο $K_{3,3}$. Θέλουμε να δείξουμε πως ο $K_{3,3}$ δεν είναι επίπεδος. Ας προσπαθήσουμε να δείξουμε πως δεν είναι επίπεδος με τη ίδια μέθοδο που χρησιμοποιήσαμε για τον K_5 . Ο $K_{3,3}$ έχει $n = 6$ κόμβους και $m = 9$ ακμές. Παρατηρούμε δηλαδή πως η σχέση $m \leq 3n - 6$ ισχύει και το παραπάνω θεώρημα δεν είναι αρκετό για να δείξουμε πως ο $K_{3,3}$ δεν είναι επίπεδος. Τι συμβαίνει λοιπόν; Αν παρατηρήσουμε προσεκτικά, ο $K_{3,3}$ δεν μπορεί να έχει περιοχές με 3 ακμές. Ο λόγος είναι πως ο $K_{3,3}$ δεν έχει κανένα κύκλο με 3 ακμές. Άρα για τον $K_{3,3}$ οι παρατηρήσεις της απόδειξης του παραπάνω θεωρήματος γίνονται:

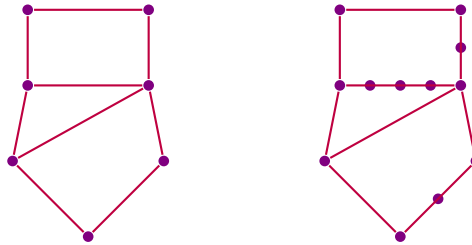
1. Κάθε ακμή συνορεύει με (το πολύ) δυο περιοχές.
2. Κάθε περιοχή συνορεύει με 4 τουλάχιστον ακμές.

Μπορούμε να διαπιστώσουμε πως οι παρατηρήσεις αυτές ισχύουν για όλους τους διμερείς γράφους, οι οποίοι εξ' ορισμού δεν περιέχουν κύκλους με περιττό μήκος και ειδικότερα δεν περιέχουν κύκλους μήκους 3. Με παρόμοια απόδειξη με αυτή του παραπάνω θεωρήματος μπορούμε λοιπόν να δείξουμε:

Θεώρημα 66. Σε κάθε συνεκτικό διμερή επίπεδο γράφο ο αριθμός των κόμβων n και των ακμών m ικανοποιεί

$$m \leq 2n - 4.$$

Με αυτό το θεώρημα τώρα βλέπουμε πως ο $K_{3,3}$ δεν είναι επίπεδος. Δείξαμε λοιπόν πως ούτε ο K_5 , ούτε ο $K_{3,3}$ είναι επίπεδοι. Θέλουμε να γενικεύσουμε αυτές τις παρατηρήσεις. Ένα βασικό δηλαδή ερώτημα είναι 'ποιοι είναι οι επίπεδοι γράφοι'; Στο ερώτημα αυτό απαντά το Θεώρημα του Kuratowski. Για να το διατυπώσουμε θα χρειαστούμε την έννοια της υποδιαίρεσης: Υποδιαίρεση ενός γράφου είναι κάθε γράφος που προκύπτει αν αντικαταστήσουμε τις ακμές του με μονοπάτια, αν δηλαδή παρεμβάλλουμε στις ακμές του νέους κόμβους. Για παράδειγμα, στο Σχήμα 9.12 ο δεύτερος γράφος αποτελεί υποδιαίρεση του πρώτου. Προφανώς ένας γράφος είναι επίπεδος αν και μόνο αν οι υποδιαίρεσεις του είναι επίπεδοι γράφοι. Επίσης είναι προφανές πως αν από ένα επίπεδο γράφο αφαιρέσουμε κόμβους και ακμές παραμένει επίπεδος.



Σχήμα 9.12: Ένας γράφος και μια υποδιαίρεσή του

Θεώρημα 67. (Kuratowski, 1930) Ένας γράφος είναι επίπεδος αν και μόνο αν δεν περιέχει κάποια υποδιαίρεση του K_5 και του $K_{3,3}$.

Η απόδειξη του Θεωρήματος του Kuratowski είναι αρκετά πολύπλοκη και ξεφεύγει από τα πλαίσια του βιβλίου.

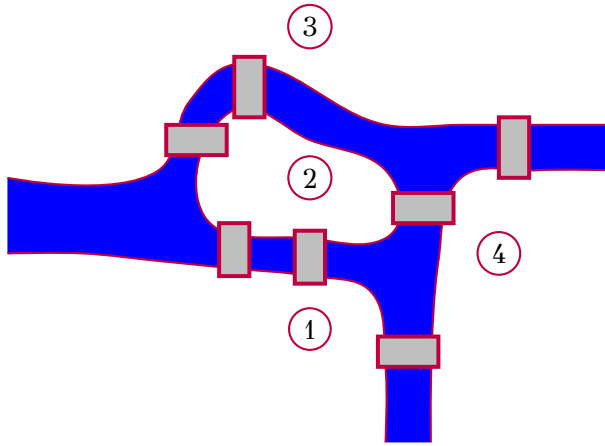
9.5 Κύκλοι του Euler και του Hamilton

Η γέννηση της Θεωρίας Γράφων αποδίδεται συνήθως στην ανάλυση του πρόβληματος των Γεφυρών του Königsberg από τον Leonard Euler. Το Königsberg, μια πόλη της παλιάς Πρωσίας που σήμερα ονομάζεται Καλίνιγγραντ και ανήκει στη Ρωσία, διασχίζεται από ένα ποταμό. Στον ποταμό υπήρχαν δυο νησιά που ενώνονταν με γέφυρες όπως στο Σχήμα 9.13. Στους κατοίκους της πόλης άρεσε η βόλτα στις γέφυρες και προσπαθούσαν ανεπιτυχώς να βρουν μια διαδρομή που περνάει από όλες τις γέφυρες ακριβώς μια φορά.

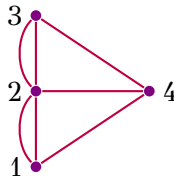
Ο Euler έκανε πρώτα τη διαπίστωση πως μόνο η τοπολογία της περιοχής παίζει ρόλο και πως το πρόβλημα είναι ισοδύναμο με το αν υπάρχει μονοπάτι που διασχίζει κάθε ακμή του Σχήματος 9.14. Στο σχήμα αυτό απεικονίζεται ένας γράφος με πολλαπλές ακμές. Αυτοί οι γράφοι αποτελούν μια γενίκευση των απλών γράφων, αλλά εδώ θα περιοριστούμε στους απλούς γράφους. Ο Euler γενίκευσε το πρόβλημα των γεφυρών στους γενικούς γράφους:

Ορισμός 68. (Μονοπάτι και κύκλος του Euler) Μονοπάτι του Euler θα λέμε ένα μονοπάτι που διασχίζει κάθε ακμή του γράφου ακριβώς μια φορά.

Κύκλο του Euler θα λέμε ένα μονοπάτι του Euler με κοινή αρχή και τέλος.



Σχήμα 9.13: Οι γέφυρες του Königsberg



Σχήμα 9.14: Ο γράφος των 7 γεφυρών

Για απλότητα θα αναφερθούμε σε κύκλους του Euler, αλλά οι προτάσεις επεκτείνονται με φυσικό τρόπο και στα μονοπάτια του Euler.

Ο Euler παρατήρησε πως η νότια πλευρά του ποταμού έχει 3 γέφυρες. Αυτό σημαίνει πως δεν υπάρχει διαδρομή που να περνάει από όλες τις γέφυρες ακριβώς μια φορά και να επιστρέφει στο σημείο εκκίνησης, δηλαδή δεν υπάρχει κύκλος Euler. Πράγματι κάθε φορά που ο κύκλος περνά από την νότια πλευρά χρησιμοποιεί 2 γέφυρες (με τη μια έρχεται και την άλλη φεύγει). Επειδή ο αριθμός των γεφυρών είναι περιττός δεν μπορεί να υπάρχει κύκλος του Euler. Με παρόμοια λογική ο Euler έδειξε πως δεν υπάρχει μονοπάτι. Επειδή η νότια πλευρά έχει 3 γέφυρες, ένα μονοπάτι του Euler θα πρέπει να αρχίζει ή να τελειώνει σ' αυτή. Αλλά για τον ίδιο λόγο, ένα μονοπάτι του Euler θα πρέπει είτε να αρχίζει είτε να τελειώνει στη βόρεια πλευρά και σε κάθε νησί. Αλλά δεν είναι δυνατό το μονοπάτι να έχει περισσότερη από μια αρχή και ένα τέλος.

Την παρατήρηση για τον κύκλο μπορούμε να τη γενικεύσουμε σε οποιοδήποτε γράφο.

Λήμμα 69. Ένας γράφος έχει κύκλο του Euler μόνο αν όλοι οι κόμβοι του έχουν άρτιο βαθμό.

Το λήμμα αυτό δίνει κάποια αναγκαία συνθήκη για να έχει ένας γράφος κύκλο Euler. Είναι όμως η συνθήκη αναγκαία; Δηλαδή, είναι αλήθεια πως κάθε γράφος που όλοι του οι κόμβοι έχουν άρτιο βαθμό έχει κύκλο Euler; Ο Euler έδειξε πως η συνθήκη είναι πράγματι ικανή και αναγκαία.

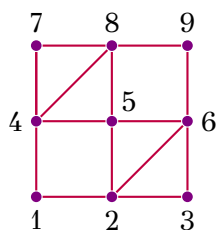
Θεώρημα 70. Ένας συνεκτικός γράφος έχει κύκλο του Euler μόνο αν και μόνο αν όλοι οι κόμβοι του έχουν άρτιο βαθμό.

Απόδειξη. Έχουμε ήδη παρατηρήσει πως η συνθήκη είναι αναγκαία. Θα δείξουμε πως είναι και ικανή. Έστω λοιπόν ένας γράφος που κάθε κόμβος του έχει άρτιο βαθμό. Θα δείξουμε πως έχει κάποιο κύκλο του Euler. Πώς; Κατασκευαστικά. Δηλαδή θα δώσουμε μια μέθοδο, ένα αλγόριθμο, που παράγει ένα κύκλο του Euler. Η απόδειξη αυτή είναι τυπική στη Θεωρία Γράφων, όπου πολλές προτάσεις αποδεικνύονται κατασκευαστικά.

Ο αλγόριθμος κατασκευής ενός κύκλου Euler έχει ως εξής: Ξεκινάμε από οποιονδήποτε κόμβο u και κατασκευάζουμε ένα μονοπάτι ακολουθώντας ακμές από τις οποίες δεν έχουμε ξαναπεράσει. Συνεχίζουμε όσο αυτό είναι δυνατό. Υποστηρίζουμε τώρα πως αυτό το μονοπάτι μπορεί να καταλήξει μόνο στον αρχικό κόμβο u . Πράγματι αν το μονοπάτι αυτό καταλήξει σε κάποιο άλλο κόμβο v , ο v πρέπει να έχει περιττό βαθμό. Γιατί αν το μονοπάτι επισκεφτεί k φορές τον κόμβο v , αυτός πρέπει να έχει βαθμό $2k - 1$ (δυο ακμές για κάθε επίσκεψη, εκτός από την τελευταία επίσκεψη που το μονοπάτι τερματίζει στον κόμβο v). Αλλά αυτό αντιβαίνει στην υπόθεση πως όλοι οι κόμβοι του γράφου έχουν άρτιο βαθμό. Άρα το μονοπάτι μπορεί μόνο να τερματίσει στον κόμβο u , είναι δηλαδή κύκλος.

Για παράδειγμα, στο γράφο του Σχήματος 9.15 έστω ότι ξεκινάμε στον κόμβο $u = 1$ και ακολουθούμε το μονοπάτι $(1, 2, 3, 6, 5, 4, 1)$. Καταλήξαμε στον αρχικό κόμβο u .

Αν ο κύκλος που δημιουργήσαμε ξεκινώντας από το u περιλαμβάνει όλες τις ακμές τελειώσαμε, γιατί αποτελεί κύκλο του Euler. Αλλά τι γίνεται αν μερικές ακμές δεν περιέχονται στον κύκλο αυτό; Επειδή ο γράφος είναι συνεκτικός θα υπάρχει κάποιος κόμβος u' πάνω στον κύκλο που κάποιες από τις ακμές του δεν ανήκουν στον κύκλο. Επαναλαμβάνουμε τώρα τη διαδικασία ξεκινώντας από τον κόμβο u' .



Σχήμα 9.15: Γράφος με κύκλο του Euler

Ακολουθούμε ακμές που δεν έχουμε επισκεφτεί όσο αυτό είναι δυνατό. Για τον ίδιο λόγο το νέο μονοπάτι μπορεί να καταλήξει μόνο στον κόμβο u' . Τώρα μπορούμε να ενώσουμε τους δυο κύκλους αφού έχουν κοινό κόμβο τον u' (πρώτα διασχίζουμε τον αρχικό κύκλο ξεκινώντας από τον u' και όταν τελειώσει συνεχίζουμε στον δεύτερο κύκλο). Αν υπάρχουν ακμές που δεν ανήκουν στον διευρυμένο αυτό κύκλο, επαναλαμβάνουμε τη διαδικασία.

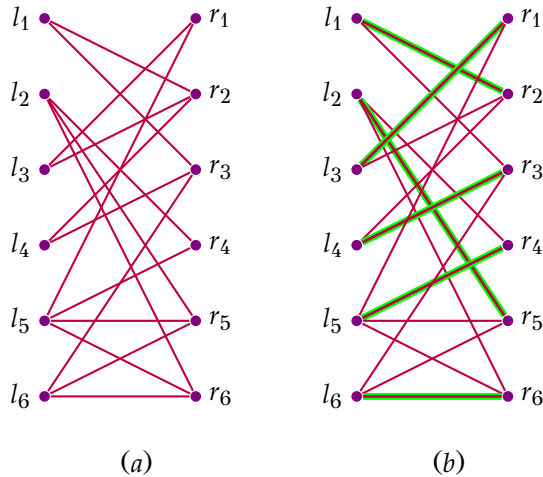
Στο παραπάνω παράδειγμα, ας υποθέσουμε πως διαλέγουμε τον κόμβο $u' = 2$ και δημιουργούμε τον κύκλο $(2, 6, 9, 8, 5, 2)$. Ενώνουμε τώρα τους δυο κύκλους: $(2, 3, 6, 5, 4, 1, 2, 6, 9, 8, 5, 2)$. Η διαδικασία συνεχίζεται από τον κόμβο $u'' = 4$ που κατασκευάζει τον κύκλο $(4, 7, 8, 4)$, τον οποίο κολλάμε στον προηγούμενο κύκλο, παίρνοντας τελικά τον κύκλο του Euler $(4, 1, 2, 6, 9, 8, 5, 2, 3, 6, 5, 4, 7, 8, 4)$.

Αυτή η διαδικασία θα τελειώσει γιατί χρησιμοποιεί πάντα νέες ακμές και ο αριθμός των ακμών είναι πεπερασμένος. Στο τέλος όλες οι ακμές θα ανήκουν στον κύκλο και επομένως θα έχουμε ένα κύκλο Euler. \square

9.6 Ταιριάσματα

Πολλές σημαντικές εφαρμογές της θεωρίας των γράφων σχετίζονται με το πρόβλημα του ταιριάσματος ή αντιστοίχησης. Το πρόβλημα μπορεί να περιγραφεί με την εξής 'πρακτική' και χαριτωμένη εφαρμογή: Σε μια κοινωνία υπάρχουν n ανύπαντρα κορίτσια και ίσος αριθμός ανύπαντρων αγοριών. Θέλουμε να παντρέψουμε κάθε κορίτσι και κάθε αγόρι, αλλά υπάρχουν κάποια από τα ζευγάρια μεταξύ κοριτσιών και αγοριών που δεν είναι εφικτά λόγω των προτιμήσεων τους. Μπορούμε να μοντελοποιήσουμε την κατάσταση με ένα διμερή γράφο, όπου οι κόμβοι του ενός μέρους αντιπροσωπεύουν τα κορίτσια, οι κόμβοι του άλλου μέρους τα αγόρια και οι ακμές αντιπροσωπεύουν επιτρεπτά ζευγάρια. Για παράδειγμα, ο γράφος του Σχήματος 9.16 δείχνει μια κοινωνία 6 κοριτσιών (αριστεροί κόμβοι) και 6 αγοριών (δεξιοί κόμβοι) και τα επιτρεπτά ζευγάρια (π.χ. το τρίτο κορίτσι μπορεί να παντρευτεί μόνο με κάποιο από τα 2 πρώτα αγόρια).

Το πρόβλημα του ταιριάσματος για μια δεδομένη κοινωνία κοριτσιών



Σχήμα 9.16: Διμερής γράφος (a) και ένα πλήρες ταίριασμα (b)

και αγοριών είναι αν υπάρχει ταίριασμα στο οποίο παντρεύονται όλοι. Ένα τέτοιο ταίριασμα ονομάζεται *πλήρες ταίριασμα*. Το ισοδύναμο γραφοθεωρητικό πρόβλημα είναι:

Ορισμός 71 (Πρόβλημα πλήρους ταιριάσματος). Δοθέντος ενός γράφου, υπάρχει υποσύνολο των ακμών του τέτοιο ώστε κάθε κόμβος του γράφου να ανήκει σε μια ακριβώς ακμή;

Ο γράφος του Σχήματος 9.16 έχει πλήρες ταίριασμα, (π.χ. οι έντονες ακμές

$$\{[l_1, r_2], [l_2, r_5], [l_3, r_1], [l_4, r_3], [l_5, r_4], [l_6, r_6]\}$$

αποτελούν πλήρες ταίριασμα). Αν όμως αφαιρέσουμε την ακμή $[l_3, r_1]$, ο γράφος που προκύπτει δεν έχει πλήρες ταίριασμα. Μπορούμε να το διαπιστώσουμε αυτό δοκιμάζοντας όλα τα δυνατά ταιριάσματα, αλλά υπάρχει κάποιος πιο άμεσος τρόπος: αρκεί να παρατηρήσουμε πως τα κορίτσια l_1, l_3 , και l_4 μπορούν να παντρευτούν μόνο τα αγόρια r_2 και r_3 : αλλά είναι αδύνατο να ταιριάξουμε 3 κορίτσια με 2 αγόρια.

Το ερώτημα που ανακύπτει είναι πως μπορούμε να ελέγξουμε αν ένας διμερής γράφος έχει τέλει ταίριασμα. Ποια είναι ικανή και αναγκαία συνθήκη για την ύπαρξη τέλει ταιριάσματος; Το παραπάνω παράδειγμα υποδεικνύει πως αναγκαία συνθήκη είναι κάθε υποσύνολο κοριτσιών να μπορεί να ταιριάξει με ίσο ή μεγαλύτερο αριθμό αγοριών. Πιο συγκεκριμένα, για κάθε υποσύνολο κοριτσιών S , ας συμβολίσουμε με $\Gamma(S)$ το

υποσύνολο των αγοριών που μπορεί να παντρευτούν με κάποιο κορίτσι στο S . Για παράδειγμα, στο γράφο του Σχήματος 9.16 αν $S = \{l_1, l_3, l_4\}$ τότε $\Gamma(S) = \{r_1, r_2, r_3\}$. Η αναγκαία συνθήκη είναι πως για κάθε S , το $\Gamma(S)$ πρέπει να έχει ίσο ή μεγαλύτερο αριθμό στοιχείων από το S . Είναι πολύ ενδιαφέρον πως η συνθήκη αυτή δεν είναι μόνο ικανή αλλά είναι και αναγκαία. Αυτό είναι το περίφημο Θεώρημα του Hall, ένα από τα βασικότερα θεωρήματα της Συνδυαστικής Ανάλυσης.

Θεώρημα 72 (Hall). Ένας διμερής γράφος $G(L+R, E)$ με ίσο αριθμό κόμβων στα δυο μέρη L και R , έχει τέλει ταίριασμα αν και μόνο αν κάθε υποσύνολο S του L έχει μεγαλύτερο ή ίσο αριθμό γειτονικών του κόμβων, δηλαδή

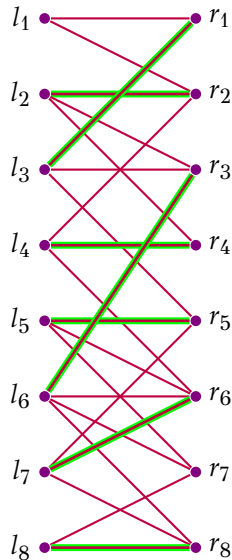
$$|S| \leq |\Gamma(S)|.$$

Απόδειξη. Είναι προφανές πως η συνθήκη $|S| \leq |\Gamma(S)|$ είναι αναγκαία για κάθε S .

Το ερώτημα είναι πως θα δείξουμε το αντίθετο. Πιο συγκεκριμένα, έστω πως η ανισότητα ισχύει για κάθε υποσύνολο S . Πως θα δείξουμε ότι ο γράφος έχει ένα τέλει ταίριασμα; Η απάντηση σε τέτοιες περιπτώσεις είναι συνήθως αλγοριθμική: Θα δώσουμε ένα αλγόριθμο που παίρνει ένα οποιοδήποτε μερικό ταίριασμα και επιστρέφει ένα καλύτερο ταίριασμα που έχει ένα επιπλέον ζευγάρι.

Έστω λοιπόν ένα μερικό ταίριασμα, όπως για παράδειγμα το ταίριασμα του Σχήματος 9.17. Ας θεωρήσουμε ένα κορίτσι u που δεν ανήκει στο ταίριασμα, όπως για παράδειγμα το κορίτσι l_1 στο Σχήμα 9.17. Θέλουμε να βρούμε τρόπο να παντρέψουμε το κορίτσι u . Αυτό θα ήταν εύκολο αν ένας από τους γείτονες της δεν ανήκε στο ταίριασμα, αλλά κάτι τέτοιο γενικά μπορεί να μην είναι δυνατό. Στο παράδειγμα, όλοι οι γείτονες του κοριτσιού u είναι ταιριασμένοι. Η βασική ιδέα της απόδειξης είναι να βρούμε ένα τρόπο για να αλλάξουμε τα ζευγάρια των ταιριασμένων κοριτσιών ώστε κάποιος γείτονας του u να μείνει αδέσμευτος.

Για το σκοπό αυτό ‘ξετυλίγουμε’ τον γράφο ξεκινώντας από τον κόμβο u , όπως στο Σχήμα 9.18a. Πιο συγκεκριμένα, ενώνουμε το u με όλα τα γειτονικά αγόρια. Αν κάποιο από αυτά τα αγόρια είναι ελεύθερο η διαδικασία σταματάει. Στο παράδειγμα, όλα τα γειτονικά αγόρια είναι δεσμευμένα. Σε αυτή την περίπτωση, παίρνουμε για κάθε τέτοιο αγόρι το κορίτσι με το οποίο είναι παντρεμένοι. Επαναλαμβάνουμε τη διαδικασία από αυτά τα κορίτσια: δηλαδή βρίσκουμε όλα τα γειτονικά τους αγόρια που δεν έχουμε εξετάσει μέχρι τώρα, εξετάζουμε να κάποιο από αυτά είναι ελεύθερο, κοκ. Προσέξτε πως η διαδικασία είναι διαφορετική για τα αγόρια και τα κορίτσια. Πιο συγκεκριμένα, για τα κορίτσια παίρνουμε όλα τα γειτονικά αγόρια που δεν έχουμε εξετάσει

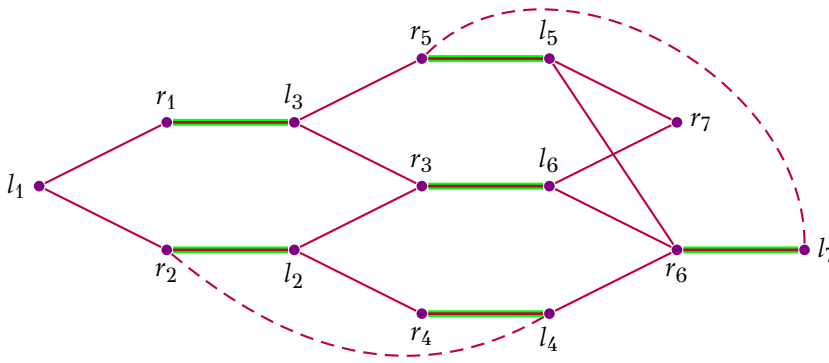


Σχήμα 9.17: Ένα μερικό ταίριασμα

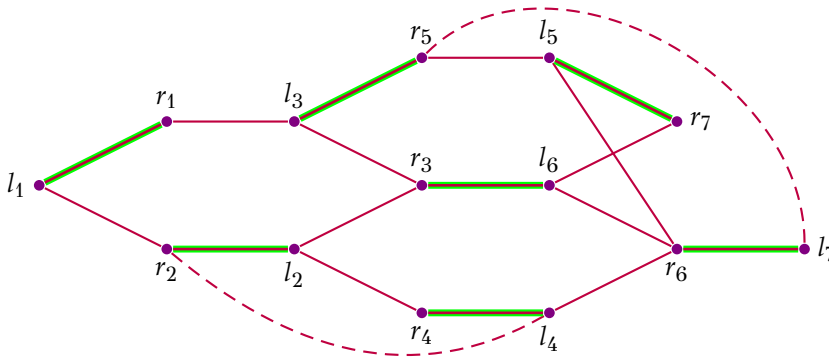
μέχρι τώρα, ενώ για τα αγόρια παίρνουμε μόνο το κορίτσι με το οποίο είναι παντρεμένο.

Αν σε αυτή τη διαδικασία βρεθεί κάποιο αγόρι v που είναι ελεύθερο, όπως το αγόρι r_7 στο παράδειγμά μας, τότε έχουμε βρει ένα μονοπάτι από το ελεύθερο κορίτσι u στο ελεύθερο αγόρι v , που είναι εναλλασσόμενο: οι ακμές που ανήκουν και δεν ανήκουν στο ταίριασμα εναλλάσσονται. Στο παράδειγμα, στο μονοπάτι $(l_1, r_1, l_3, r_5, l_5, r_7)$ οι ακμές $[l_1, r_1], [l_3, r_5], [l_5, r_7]$ δεν ανήκουν στο ταίριασμα ενώ οι $[r_1, l_3], [r_5, l_5]$ ανήκουν στο ταίριασμα. Προσέξτε πως οι ακμές του μονοπατιού που δεν ανήκουν στο ταίριασμα είναι περισσότερες από τις ακμές που ανήκουν στο ταίριασμα. Αυτό συμβαίνει γιατί τα δυο άκρα του μονοπατιού u και v είναι ελεύθερα. Βγάζουμε λοιπόν τις ακμές που ανήκουν στο ταίριασμα και προσθέτουμε αυτές που δεν ανήκουν. Έτσι παίρνουμε ένα ταίριασμα με περισσότερες ακμές, όπως στο Σχήμα 9.18b.

Τι κάνουμε όμως όταν η διαδικασία δεν βρει ελεύθερο αγόρι; Δεν χρειάζεται να μας απασχολεί αυτό το ερώτημα γιατί: Αν η συνθήκη του Hall $|S| \leq |\Gamma(S)|$ ισχύει για κάθε σύνολο κοριτσιών S , τότε πάντα θα βρεθεί κάποιο ελεύθερο αγόρι. Για να το δούμε αυτό, προσέξτε πως στη διαδικασία, εκτός από το αρχικό κορίτσι u , τα υπόλοιπα αγόρια και κορίτσια σχηματίζουν ζευγάρια. Έστω S το σύνολο των κοριτσιών που εμφανίζονται σε αυτή τη διαδικασία. Το σύνολο των αγोरών που εμφανίζονται σε αυτή τη διαδικασία είναι όλα τα γειτονικά αγόρια του S , δηλαδή το $\Gamma(S)$. Αν η διαδικασία τελειώσει χωρίς να βρεθεί ελεύθερο



(a)



(b)

Σχήμα 9.18: (a) Ξεδιπλώνουμε το γράφο από το l_1 . (b) Παίρνουμε ένα καλύτερο ταιρίασμα εναλλάσσοντας τις ακμές στο μονοπάτι $(l_1, r_1, l_3, r_5, r_7)$.

αγόρι, ο αριθμός $|S|$ των κοριτσιών θα είναι κατά 1 μεγαλύτερος του αριθμού $|\Gamma(S)|$ των αγοριών, που αντιβαίνει στην υπόθεση. Αν στο παράδειγμά μας οι ακμές $[l_5, r_7]$ και $[l_6, r_7]$ δεν υπήρχαν, τότε η διαδικασία δεν θα έβρισκε ελεύθερο αγόρι. Αλλά τότε ο γράφος δεν θα ικανοποιούσε τη συνθήκη του Hall γιατί το σύνολο $S = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7\}$ (με 7 κορίτσια) θα είχε γείτονες το σύνολο $\Gamma(S) = \{r_1, r_2, r_3, r_4, r_5, r_6\}$ (με 6 αγόρια). \square

Ασκήσεις

9.1. Υπάρχουν γράφοι με 6 κόμβους που οι κόμβοι τους έχουν τους εξής βαθμούς;

- 3,3,3,3,3,3

- 3,4,4,4,4,4
- 1,2,2,4,4,5

9.2. Δείξτε πως για κάθε γράφο G είτε ο G είτε ο συμπληρωματικός του \overline{G} είναι συνεκτικός. Υπενθυμίζεται πως ο συμπληρωματικός γράφος \overline{G} είναι αυτός που έχει ακριβώς τις ακμές που λείπουν από τον G .

9.3. Αποδείξτε το Θεώρημα 62.

9.4. Δείξτε πως ο γράφος του Petersen δεν είναι επίπεδος χρησιμοποιώντας την ιδέα της απόδειξης των Θεωρημάτων 65 και 66.

9.5. Δείξτε πως ο γράφος του Petersen δεν είναι επίπεδος χρησιμοποιώντας το Θεώρημα του Kuratowski. Δείξτε δηλαδή πως ο γράφος του Petersen περιέχει μια υποδιαίρεση του K_5 ή του $K_{3,3}$.

9.6. Δείξτε πως κάθε δένδρο είναι επίπεδος γράφος.

9.7. Βρείτε ένα κύκλο του Hamilton στον γράφο του δωδεκαέδρου (Σχήμα 9.7).

9.8. Δείξτε πως ο γράφος του Petersen δεν περιέχει κύκλο του Hamilton.

9.9. Διατυπώστε και αποδείξτε μια κατάλληλη συνθήκη Euler ώστε ένας κατευθυνόμενος γράφος να έχει κύκλο Euler.

9.10. Έστω ένας διμερής γράφος $G(L+R, E)$ με ίσο αριθμό κόμβων στα δυο μέρη L και R για τον οποίο ισχύει πως κάθε υποσύνολο S του L έχει αριθμό γειτόνων μεγαλύτερο ή ίσο με τον αριθμό των κόμβων του S , δηλαδή $|S| \leq \Gamma(S)$. Δείξτε πως το ίδιο ισχύει και για δεξιό μέρος: Κάθε υποσύνολο T του R έχει αριθμό γειτόνων μεγαλύτερο ή ίσο με τον αριθμό των κόμβων του T , δηλαδή $|T| \leq \Gamma(T)$.

Δώστε δυο αποδείξεις: μια με χρήση του Θεωρήματος του Hall και μια βασισμένη μόνο σε απλές αρχές που να μην χρησιμοποιεί τα αποτελέσματα της θεωρίας ταιριάσματος.

Λύσεις επιλεγμένων ασκήσεων

Α΄ Λύσεις επιλεγμένων ασκήσεων

Στο τμήμα αυτό παρουσιάζονται λύσεις για κάποιες ασκήσεις. Ο αναγνώστης όμως πρέπει να λάβει υπόψη πως η συγγραφή κάποιων λύσεων υπολείπεται σημαντικά της επιθυμητής ποιότητας.

Κεφάλαιο 1

Άσκηση (1.2). Στο πρόβλημα του Collatz ($3x + 1$), βρείτε ένα αριθμό n τέτοιο ώστε αν αρχίσουμε από το n θα φτάσουμε σε κάποιο αριθμό μεγαλύτερο του $10n$.

Λύση. Ένας τέτοιος αριθμός είναι το 15, ξεκινώντας από τον οποίο και εφαρμόζοντας τον αλγόριθμο, εμφανίζονται οι ακόλουθοι αριθμοί:

$$15 \rightarrow 46 \rightarrow 23 \rightarrow 70 \rightarrow 35 \rightarrow 106 \rightarrow 53 \rightarrow 160 \rightarrow \dots$$

Γενικότερα στη διαδικασία Collatz, αν αρχίσουμε με αριθμό της μορφής $2^k - 1$, οι αρχικοί αριθμοί αυξάνουν σταθερά. Γιατί;

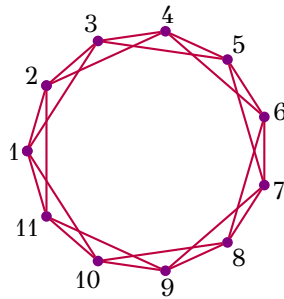
Κεφάλαιο 2

Άσκηση (2.3). Δώστε ένα παράδειγμα γράφου με 11 κόμβους που δεν περιέχει ούτε πλήρη ούτε κενό υπογράφο με 4 κόμβους.

Λύση. Θα δείξουμε πως ο γράφος του Σχήματος Α΄.1 έχει την επιθυμητή ιδιότητα. Παρατηρούμε πρώτα πως ο γράφος έχει κυκλική συμμετρία.

Θα δείξουμε:

- Δεν υπάρχει πλήρης υπογράφος με 4 κόμβους: Οι μόνοι πλήρη υπογράφοι με 3 κόμβους αποτελούνται από 3 συνεχόμενους κόμβους στον κύκλο. Άρα μόνο 4 συνεχόμενοι κόμβοι μπορεί να συνιστούν πλήρη υπογράφο, που δεν ισχύει όπως είναι προφανές από τον υπογράφο με κόμβους 1,2,3,4.
- Δεν υπάρχει κενός υπογράφος με 4 κόμβους: Έστω τώρα ότι υπάρχει ένας κενός υπογράφος με κόμβους v_1, v_2, v_3, v_4 με $v_1 \leq v_2 \leq$



Σχήμα Α.1: Γράφος 11 κόμβων χωρίς K_4 και χωρίς $\overline{K_4}$

$v_3 \leq v_4$. Λόγω συμμετρίας μπορούμε να πάρουμε τον πρώτο κόμβο $v_1 = 1$. Για να είναι κενός πρέπει να έχουμε $v_{i+1} - v_i \geq 3$. Συνεπώς $v_4 - v_1 = (v_4 - v_3) + (v_3 - v_2) + (v_2 - v_1) \geq 3 + 3 + 3 = 9$. Αφού $v_1 = 1$ το οποίο δίνει ότι $v_4 \leq 10$, αλλά τότε ο v_4 συνδέεται με τον v_1 και ο υπογράφος δεν είναι κενός.

Αξίζει να αναφερθεί ότι υπάρχουν πολλοί άλλοι γράφοι που έχουν την ιδιότητα.

Άσκηση (2.13). Δείξτε χρησιμοποιώντας Μαθηματική Επαγωγή ότι για κάθε μη αρνητικό ακέραιο n ισχύει:

$$\frac{8}{1 \cdot 3} + \frac{8}{5 \cdot 7} + \dots + \frac{8}{(4n+1) \cdot (4n+3)} \leq 4$$

Που φαίνεται να συγκλίνει αυτό το άθροισμα;

Λύση. Θα αποδείξουμε κάτι πιο ισχυρό. Ότι για κάθε μη αρνητικό ακέραιο n ισχύει:

$$\frac{8}{1 \cdot 3} + \frac{8}{5 \cdot 7} + \dots + \frac{8}{(4n+1) \cdot (4n+3)} \leq 4 - \frac{1}{n+1}$$

Βάση της Επαγωγής: για $n = 0$ ισχύει αφού $\frac{8}{3} \leq 3$.

Επαγωγικό Βήμα: Υποθέτουμε ότι η πρόταση μας ισχύει για μη αρνητικό ακέραιο k , και θα δείξουμε ότι ισχύει για $k+1$. Έχουμε λοιπόν ότι ισχύει:

$$\frac{8}{1 \cdot 3} + \dots + \frac{8}{(4k+1) \cdot (4k+3)} \leq 4 - \frac{1}{k+1}$$

προσθέτουμε και στα δύο μέλη τον όρο

$$\frac{8}{[4(k+1)+1] \cdot [4(k+1)+3]}$$

και παίρνουμε:

$$\frac{8}{1 \cdot 3} + \dots + \frac{8}{(4k+1) \cdot (4k+3)} + \frac{8}{(4k+5) \cdot (4k+7)} \leq 4 - \frac{1}{k+1} + \frac{8}{(4k+5) \cdot (4k+7)}$$

Σε αυτό το σημείο αρκεί να αποδείξουμε ότι:

$$\begin{aligned}
 4 - \frac{1}{k+1} + \frac{8}{(4k+5) \cdot (4k+7)} &\leq 4 - \frac{1}{k+2} \Leftrightarrow \\
 \frac{8}{(4k+5) \cdot (4k+7)} &\leq \frac{1}{k+1} - \frac{1}{k+2} \Leftrightarrow \\
 \frac{8}{(4k+5) \cdot (4k+7)} &\leq \frac{1}{(k+1) \cdot (k+2)} \Leftrightarrow \\
 8 \cdot (k+1) \cdot (k+2) &\leq (4k+5) \cdot (4k+7) \Leftrightarrow \\
 8k^2 + 24k + 16 &\leq 16k^2 + 48k + 35 \Leftrightarrow \\
 8k^2 + 24k + 19 &\geq 0.
 \end{aligned}$$

Το τελευταίο προφανώς ισχύει και, λόγω της ισοδυναμίας, ισχύει και η αρχική πρόταση.

Το άθροισμα συγκλίνει στο π , αλλά η απόδειξη αυτής της πρότασης είναι πέρα από τα ενδιαφέροντα του βιβλίου.

Μια άλλη ενδιαφέρουσα παρατήρηση είναι ότι μπορούμε να σπάσουμε κάθε όρο αυτού του αθροίσματος και να πάρουμε το άθροισμα

$$\frac{4}{1} - \frac{4}{3} + \frac{4}{5} - \frac{4}{7} + \frac{4}{9} - \dots$$

που είναι πολύ απλούστερο άθροισμα και που επίσης συγκλίνει στο π .

Άσκηση (2.15). Αποδείξτε προσεκτικά πως σε κάθε αύξουσα ακολουθία a_1, a_2, \dots, a_n με $a_i \in \{1, 2, \dots, n\}$, υπάρχει κάποιο k τέτοιο ώστε $a_k = k$.

Για παράδειγμα, στην ακολουθία 2, 3, 3, 5, 6, 6, 6, έχουμε $a_3 = 3$ (επίσης $a_6 = 6$).

Λύση. Με επαγωγή στο n . Η βάση για $n = 1$ είναι προφανής, γιατί $a_1 = 1$. Έστω ότι η πρόταση ισχύει για n . Θα τη δείξουμε για $n+1$. Διακρίνουμε δυο περιπτώσεις:

- Αν $a_{n+1} = n+1$, τότε η πρόταση ισχύει για $k = n+1$.
- Διαφορετικά, $a_{n+1} \leq n$. Επομένως $a_n \leq n$ και η πρόταση ισχύει για τα στοιχεία a_1, a_2, \dots, a_n από την επαγωγική υπόθεση.

Άσκηση (2.16). Οι κινήσεις του Ίππου στο σκάκι έχουν σχήμα Γ (από τη θέση (x, y) μπορεί να πάει στις θέσεις $(x \pm 2, y \pm 1)$ και $(x \pm 1, y \pm 2)$). Ας θεωρήσουμε μια άπειρη σκακιέρα (που επεκτείνεται μέχρι το άπειρο προς τα δεξιά και πάνω) και ας υποθέσουμε ότι αρχικά ο Ίππος είναι στο κάτω αριστερό άκρο της $(1, 1)$.

Δείξτε με επαγωγή ότι για κάθε θέση (x, y) , με $x, y \in \mathbb{N}$, υπάρχει διαδρομή που ξεκινά από την αρχική θέση και καταλήγει στη θέση (x, y) .

Για ποια n μπορεί να γίνει το ίδιο όταν η σκακιέρα είναι πεπερασμένη και έχει διαστάσεις $n \times n$; Για παράδειγμα, αν $n = 2$ δεν μπορεί να γίνει γιατί ο Ίππος δεν μπορεί καν να κινηθεί από την αρχική θέση και επομένως δεν μπορεί να επισκεφτεί τη θέση $(1, 2)$.

Λύση. Θα χρησιμοποιήσουμε την εξής απλή ιδέα: Αν ο Ίππος μπορεί να επισκεφτεί τη θέση (x, y) , τότε μπορεί να επισκεφτεί και τη θέση $(x+1, y)$ (και λόγω συμμετρίας) τη θέση $(x, y+1)$. Πώς; Ως εξής:

$$(x, y) \rightarrow (x+2, y+1) \rightarrow (x, y+2) \rightarrow (x+1, y)$$

Για να είναι η παραπάνω διαδρομή μέσα στη σκακιέρα πρέπει οι παραπάνω συντεταγμένες να είναι θετικές. Πράγματι αν x και y είναι θετικά, τότε και τα $x+1, x+2, y+1, y+2$ είναι επίσης θετικά.

Θα χρησιμοποιήσουμε επαγωγή για να δείξουμε την πρόταση

$$P(n) = \text{Υπάρχει διαδρομή του Ίππου που ξεκινά στο } (1, 1) \text{ και καταλήγει στο } (x, y) \text{ για κάθε } x \text{ και } y \text{ με } x+y = n,$$

δηλαδή θα χρησιμοποιήσουμε επαγωγή στο άθροισμα των x και y .

Βάση της επαγωγής: Η $P(n)$ ισχύει φυσικά για $n = 2$ αφού σ' αυτή την περίπτωση $(x, y) = (1, 1)$.

Επαγωγικό βήμα: Έστω ότι η πρόταση ισχύει για κάποιο $n \geq 2$. Θα δείξουμε πως ισχύει για $n+1$. Πράγματι, έστω x και y τέτοια ώστε $x+y = n+1$. Θα δείξουμε ότι ο Ίππος μπορεί να επισκεφτεί το (x, y) . Επειδή $x+y \geq 3$, ένα τουλάχιστον από τα x και y είναι μεγαλύτερο ή ίσο με 2. Ας υποθέσουμε λοιπόν ότι $x \geq 2$ (ανάλογα εργαζόμαστε όταν $y \geq 2$). Επομένως το $x-1$ είναι θετικό. Επειδή $(x-1)+y = n$, από την επαγωγική υπόθεση, ο Ίππος μπορεί να επισκεφτεί τη θέση $(x-1, y)$. Αλλά τότε μπορεί να επισκεφτεί και τη θέση $((x-1)+1, y) = (x, y)$.

Εναλλακτική απόδειξη: Μια δεύτερη απόδειξη με επαγωγή είναι να κάνουμε διπλή επαγωγή στα x και y . Ας το κάνουμε αναλυτικά γιατί η διπλή επαγωγή απαιτεί πολλές φορές λεπτούς χειρισμούς.

Έστω οι προτάσεις, μια για κάθε y ,

$$Q_y(x) = \text{Υπάρχει διαδρομή του Ίππου που ξεκινά στο } (1, 1) \text{ και καταλήγει στο } (x, y)$$

και

$$R(y) = \text{Η πρόταση } Q_y(x) \text{ είναι αληθής για κάθε } x.$$

Θέλουμε να δείξουμε την $R(y)$ με επαγωγή στο y . Στη βάση της επαγωγής και στο επαγωγικό βήμα θα δείξουμε κάποια $Q_y(x)$ με επαγωγή στο x .

Βάση της επαγωγής: Θα δείξουμε πως η $R(1)$ είναι αληθής. Ισοδύναμα, θα δείξουμε με απαγωγή στο x πως η $Q_1(x)$ ισχύει για κάθε x .

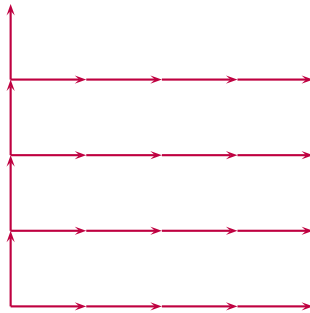
Βάση της επαγωγής: Η $Q_1(1)$ είναι αληθής (ο Ίππος μπορεί να επισκεφτεί το $(1, 1)$).

Επαγωγικό βήμα: Έστω ότι η $Q_1(x)$ είναι αληθής, δηλαδή ο Ίππος μπορεί να επισκεφτεί το $(x, 1)$. Αλλά τότε μπορεί να επισκεφτεί και το $(x+1, 1)$, άρα και η $Q_1(x+1)$ είναι αληθής.

Επαγωγικό βήμα: Έστω πως η $R(y)$ είναι αληθής. Θα δείξουμε πως η $R(y+1)$ είναι επίσης αληθής. Ισοδύναμα, αν η $Q_y(x)$ ισχύει για κάθε x , τότε η $Q_{y+1}(x)$ ισχύει επίσης για κάθε x . Στην παρακάτω απόδειξη, με επαγωγή στο x , μόνο ότι $Q_y(x)$ ισχύει για $x = 1$ θα χρησιμοποιήσουμε.

Βάση της επαγωγής: Η $Q_{y+1}(1)$, δηλαδή ο Ίππος μπορεί να επισκεφτεί το $(1, y+1)$, είναι αληθής. Γιατί; Γιατί από την επαγωγική υπόθεση η $Q_y(1)$ είναι αληθής, δηλαδή ο Ίππος μπορεί να επισκεφτεί το $(1, y)$, και επομένως μπορεί να επισκεφτεί και το $(1, y+1)$.

Επαγωγικό βήμα: Έστω ότι η $Q_{y+1}(x)$ είναι αληθής, δηλαδή ο Ίππος μπορεί να επισκεφτεί το $(x, y+1)$. Αλλά τότε μπορεί να επισκεφτεί και τη θέση $(x+1, y+1)$ και επομένως η $Q_{y+1}(x+1)$ είναι αληθής.



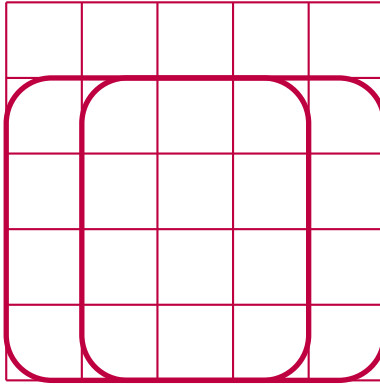
Στο σχήμα φαίνεται η σειρά με την οποία δείχνεται η πρόταση στην παραπάνω απόδειξη. Πρώτα δείχνεται η πρόταση για την κάτω οριζόντια γραμμή (η βάση της εξωτερικής επαγωγής), μετά για την δεύτερη οριζόντια γραμμή κ.ο.κ. Τα κατακόρυφα βέλη αντιστοιχούν στη βάση της δεύτερης εσωτερικής επαγωγής.

Θα δείξουμε πως εκτός από την περίπτωση $n = 2$ και $n = 3$, για όλες τις άλλες περιπτώσεις όλες οι θέσεις μιας $n \times n$ σκακιέρας είναι επισκέψιμες. Για $n = 2$ ο Ίππος δεν μπορεί να κάνει καμία κίνηση. Για $n = 3$ δεν μπορεί να επισκεφτεί το κεντρικό τετράγωνο. Για τα υπόλοιπα n χρησιμοποιούμε επαγωγή στο n .

Βάση της επαγωγής: Για $n = 4$ μπορούμε να το επιβεβαιώσουμε εξαντλητικά.

Επαγωγικό βήμα: Έστω ότι ο Ίππος μπορεί να επισκεφτεί κάθε τετράγωνο μιας σκακιέρας $n \times n$, όπου $n \geq 4$. Θα δείξουμε ότι το ίδιο ισχύει και για σκακιέρες μεγέθους $(n+1) \times (n+1)$. Πράγματι, το τμήμα της σκακιέρας με κορυφές $(1, 1)$ και (n, n) μπορεί να καλυφθεί από την επαγωγική υπόθεση. Για τις υπόλοιπες θέσεις, σκεφτόμαστε ως εξής: Αφού ο Ίππος μπορεί να επισκεφτεί τη θέση $(1, 2)$, αν θεωρήσουμε αυτή τη θέση για αρχική και χρησιμοποιήσουμε την επαγωγική υπόθεση στο τμήμα της σκακιέρας με κορυφές $(1, 2)$ και $(n, n+1)$, συμπεραίνουμε πως

ο Ίππος μπορεί να επισκεφτεί κάθε θέση με $y \leq n$ (όπως φαίνεται στο σχήμα).



Με την ίδια συλλογιστική μπορούμε να δείξουμε ότι ο Ίππος μπορεί να επισκεφτεί και τις υπόλοιπες θέσεις. Πιο συγκεκριμένα, ο Ίππος μπορεί να επισκεφτεί τη θέση $(1, 2)$ και θεωρώντας αυτή για αρχική θέση, όλες τις θέσεις με $2 \leq y \leq n + 1$.

Κεφάλαιο 3

Άσκηση (3.1). Χρησιμοποιήστε δομική επαγωγή για να αποδείξετε ότι σε κάθε πλήρες δυαδικό δένδρο T , το πλήθος των φύλλων του $l(T)$, δηλαδή των κόμβων που δεν έχουν παιδιά, είναι ένα παραπάνω από το πλήθος των εσωτερικών του κόμβων $i(T)$, δηλαδή των κόμβων που έχουν παιδιά.

Λύση. Αρκεί να δείξουμε με δομική επαγωγή ότι τα κανονικά δένδρα έχουν την ιδιότητα, αφού κάθε πλήρες δένδρο είναι κανονικό.

Βάση της επαγωγής: Το δένδρο με ένα μονο κόμβο έχει ένα φύλλο και μηδέν εσωτερικούς κόμβους, δηλαδή $l(T) = 1$ και $i(T) = 0$. Η πρόταση προφανώς ισχύει.

Επαγωγικό βήμα: Έστω ένα δένδρο με ρίζα r και υποδένδρα T_1, T_2 . Από την επαγωγική υπόθεση, η πρόταση ισχύει για τα δένδρα T_1, T_2 , δηλαδή $l(T_1) = i(T_1) + 1$ και $l(T_2) = i(T_2) + 1$.

Ο αριθμός των φύλλων του δένδρου T είναι ίσος με το άθροισμα του αριθμού των φύλλων του T_1 και T_2 , δηλαδή $l(T) = l(T_1) + l(T_2)$. Ο δε αριθμός των εσωτερικών κόμβων του δένδρου T είναι ίσος με το άθροισμα του αριθμού των εσωτερικών κόμβων του T_1 και T_2 συν 1 (για τη ρίζα r), δηλαδή $i(T) = i(T_1) + i(T_2) + 1$. Αν τα βάλουμε όλα μαζί έχουμε

$$l(T) = l(T_1) + l(T_2) = (i(T_1) + 1) + (i(T_2) + 1) = (i(T_1) + i(T_2) + 1) + 1 = i(T) + 1$$

που αποδεικνύει την πρόταση για το δένδρο T .

Άσκηση (3.2). Έστω S ένα υποσύνολο του $\mathbb{N} \times \mathbb{N}$ που ορίζεται επαγωγικά ως εξής:

Βάση επαγωγικού ορισμού: $(0, 0) \in S$.

Επαγωγικό βήμα: Αν $(a, b) \in S$ τότε $(a + 2, b + 3) \in S$ και $(a + 3, b + 2) \in S$.

α' Καταγράψτε τα στοιχεία του συνόλου S μετά από 4 εφαρμογές του επαγωγικού βήματος του ορισμού του.

β' Χρησιμοποιήστε δομική επαγωγή για να αποδείξετε ότι αν $(a, b) \in S$ τότε το $a + b$ είναι πολλαπλάσιο του 5.

γ' Διατυπώστε με σαφήνεια μια υπόθεση για το ποιά ζεύγη αριθμών ανήκουν στο S . Αποδείξτε την υπόθεση σας.

Λύση. α' Οι τιμές που παίρνουμε με τις 4 πρώτες εφαρμογές του επαγωγικού κανόνα είναι οι εξής:

$$\begin{aligned} &(0,0) \\ &(2,3) (3,2) \\ &(4,6) (5,5) (6,4) \\ &(6,9) (7,8) (8,7) (9,6) \\ &(8,12) (9,11) (10,10) (11,9) (12,8) \end{aligned}$$

β' Βάση της επαγωγής: Για $(0, 0)$ η πρόταση προφανώς ισχύει, αφού το $0 + 0$ είναι πολλαπλάσιο του 5.

Επαγωγικό βήμα: Η επαγωγική υπόθεση της δομικής επαγωγής είναι ότι αν το (a, b) ανήκει στο S τότε $a + b$ είναι πολλαπλάσιο του 5. Αρκεί να δείξουμε ότι το $(a + 2, b + 3)$ και το $(a + 3, b + 2)$ έχει την ιδιότητα. Αλλά αφού $(a + 2) + (b + 3) = (a + b) + 5$, και ο $a + b$ είναι πολλαπλάσιο του 5, τότε και το $(a + 2) + (b + 3)$ είναι πολλαπλάσιο του 5. Παρόμοια και το $(a + 3) + (b + 2)$ είναι πολλαπλάσιο του 5.

γ' Παρατηρώντας την απάντηση του πρώτου μέρους της άσκησης καθώς και τον τρόπο παραγωγής των νέων στοιχείων του συνόλου S , βλέπουμε ότι αν (a, b) είναι στοιχείο του S , τότε το a δεν μπορεί να είναι πολύ μικρότερο ή πολύ μεγαλύτερο από το b και πιο συγκεκριμένα ότι $2a \leq 3b$ και αντίστοιχα $2b \leq 3a$. Κάνουμε λοιπόν την εξής υπόθεση:

Υπόθεση 73. Το σύνολο S είναι ακριβώς το σύνολο

$$\{(a, b) : a, b \in \mathbb{N} \text{ και } a + b = 0 \pmod{5} \text{ και } 2a \leq 3b \text{ και } 2b \leq 3a\}.$$

Απόδειξη. Ας ορίσουμε την ιδιότητα

$$P(a, b) = 'a + b = 0 \pmod{5} \text{ και } 2a \leq 3b \text{ και } 2b \leq 3a'$$

και έστω A το σύνολο των φυσικών (a, b) που έχουν την ιδιότητα P :

$$A = \{(a, b) : a, b \in \mathbb{N} \text{ και } P(a, b) \text{ είναι αληθής}\}.$$

Θέλουμε να δείξουμε ότι $A = S$. Θα δείξουμε με δομική επαγωγή ότι $S \subseteq A$ και με μαθηματική επαγωγή ότι $A \subseteq S$.

$S \subseteq A$: Στο πρώτο μέρος, δηλαδή $S \subseteq A$, θέλουμε να δείξουμε ότι αν (a, b) παράγεται με τους κανόνες του S τότε το (a, b) έχει την ιδιότητα P . Το ότι το $a + b$ είναι πολλαπλάσιο του 5 το δείξαμε στο δεύτερο τμήμα της άσκησης. Το $2a \leq 3b$ και $2b \leq 3a$ δείχνεται με τον ίδιο ακριβώς τρόπο:

Βάση της επαγωγής: Για $(0, 0)$ η πρόταση προφανώς ισχύει, αφού $2 \cdot 0 \leq 3 \cdot 0$.

Επαγωγικό βήμα: Η επαγωγική υπόθεση της δομικής επαγωγής είναι ότι αν το (a, b) ανήκει στο S τότε $2a \leq 3b$ και $2b \leq 3a$. Αρκεί να δείξουμε ότι το $(a + 2, b + 3)$ και το $(a + 3, b + 2)$ έχει την ιδιότητα. Για το $(a + 2, b + 3)$ έχουμε

$$\begin{aligned} 2(a + 2) &= 2a + 4 \\ &\leq 3b + 4 && \text{από την επαγωγική υπόθεση} \\ &\leq 3(b + 3) \end{aligned}$$

και

$$\begin{aligned} 2(b + 3) &= 2b + 6 \\ &\leq 3a + 6 && \text{από την επαγωγική υπόθεση} \\ &\leq 3(a + 2) \end{aligned}$$

Λόγω συμμετρίας ή με την ίδια ακριβώς μέθοδο, η πρόταση θα ισχύει και για $(a + 3, b + 2)$.

$A \subseteq S$: Με μαθηματική επαγωγή στο a θα δείξουμε ότι αν (a, b) ικανοποιεί την πρόταση ιδιότητα P , δηλαδή το $a + b$ είναι πολλαπλάσιο του 5 και $2a \leq 3b$ και $2b \leq 3a$, τότε το ζεύγος (a, b) μπορεί να παραχθεί με τους κανόνες του S .

Βάση της επαγωγής: Η βάση θα είναι οι τιμές του $a = 0, 1, 2, 3, 4$. Με την εξαντλητική μέθοδο ελέγχουμε ότι οι μόνες τιμές του b που ικανοποιούν την ιδιότητα P είναι οι $(0, 0), (2, 3), (3, 2), (4, 6)$, οι όποιες ανήκουν στο S όπως προκύπτει από την απάντηση της πρώτης ερώτησης της άσκησης. Για ποιο λόγο θέλουμε η βάση να περιλαμβάνει τις τιμές του a μέχρι και το 4 θα το δούμε στη συνέχεια.

Επαγωγικό βήμα: Υποθέτουμε ότι η πρόταση ισχύει για κάθε $a \leq n$ και θα δείξουμε ότι ισχύει για $a = n + 1 \geq 5$. Έστω λοιπόν ότι το (a, b) έχει την ιδιότητα P . Για να δείξουμε ότι μπορεί να παραχθεί με τους κανόνες του S , αρκεί να δείξουμε ότι το $(a - 2, b - 3)$ έχει την ιδιότητα P . Γιατί τότε από την επαγωγική υπόθεση έχουμε ότι $(a - 3, b - 2) \in S$

και συνεπώς (με μια εφαρμογή του επαγωγικού ορισμού) $(a, b) \in S$. Εναλλακτικά, αρκεί να δείξουμε ότι το $(a - 3, b - 2)$ έχει την ιδιότητα P .

Για παράδειγμα, το $(7, 8)$ έχει την ιδιότητα P . Το $(7 - 2, 8 - 3) = (5, 5)$ έχει επίσης την ιδιότητα P . Αν το $(5, 5)$ ανήκει στο S (που βέβαια ανήκει), τότε και το $(7, 8)$ θα ανήκει στο S .

Αλλά ας επαναλάβουμε το παράδειγμα για το $(6, 9)$ αντί για το $(7, 8)$. Σ' αυτή την περίπτωση $(6 - 3, 9 - 2) = (3, 7)$ δεν ικανοποιεί την ιδιότητα P (γιατί παραβιάζει τη συνθήκη $2b \leq 3a$). Εντούτοις το $(6, 9)$ ανήκει στο S γιατί μπορεί να παραχθεί από το $(6 - 2, 9 - 3) = (4, 6)$.

Ας αναλύσουμε πότε το $(a - 3, b - 2)$ έχει την ιδιότητα P όταν ξέρουμε ότι το (a, b) έχει την ιδιότητα P . Προφανώς το $(a - 3) + (b - 2) = a + b - 5$ διαιρείται με το 5. Επίσης

$$2(a - 3) \leq 3(b - 2) \Leftrightarrow 2a \leq 3b$$

ισχύει. Άρα το $(a - 3, b - 2)$ έχει την ιδιότητα P αν και μόνο αν $2(b - 2) \leq 3(a - 3)$ ή ισοδύναμα $2b + 5 \leq 3a$. Αυτό δεν ισχύει πάντα όπως είδαμε παραπάνω στο παράδειγμα $(a, b) = (6, 9)$.

Με ανάλογους υπολογισμούς (ή λόγω συμμετρίας) βρίσκουμε ότι το $(a - 2, b - 3)$ έχει την ιδιότητα P αν και μόνο αν $2a + 5 \leq 3b$. Συμπερασματικά, πρέπει να δείξουμε ότι αν (a, b) έχει την ιδιότητα P τότε ένα τουλάχιστον από τα δυο πρέπει να συμβαίνει: Είτε $2b + 5 \leq 3a$ είτε $2a + 5 \leq 3b$.

Εδώ είναι που η βάση της επαγωγής είναι χρήσιμο να ισχύει για όλες τις τιμές $a < 5$. Υποθέτουμε λοιπόν ότι $5 \leq a$. Τότε όταν $b \leq a$ ισχύει το $2b + 5 \leq 3a$ και όταν $a \leq b$ ισχύει το $2a + 5 \leq 3b$. Δηλαδή, ένα τουλάχιστον από τα $2b + 5 \leq 3a$ είτε $2a + 5 \leq 3b$ ισχύει και αυτό ολοκληρώνει την απόδειξη. \square

Η παραπάνω απόδειξη με μαθηματική επαγωγή είναι σχετικά μακροσκελής αλλά βασίζεται σε απλές ιδέες. Υπάρχει όμως μια δεύτερη απόδειξη που επίσης βασίζεται σε απλές ιδέες. Ένα (a, b) που παράγεται με k εφαρμογές του κανόνα $(a + 2, b + 3)$ και m εφαρμογές του κανόνα $(a + 3, b + 2)$ θα είναι της μορφής $(2k + 3m, 3k + 2m)$. Άρα μπορούμε να πούμε ότι το S είναι το σύνολο

$$\{(a, b) : \text{Υπάρχουν φυσικοί } k \text{ και } m \text{ τέτοιοι ώστε } (a, b) = (2k + 3m, 3k + 2m)\}.$$

Είναι καλός αυτός ο χαρακτηρισμός του S ; Το θέμα είναι υποκειμενικό αφού δεν έχουμε ορίσει με σαφήνεια τι σημαίνει καλός ορισμός και τι όχι. Αλλά ας θεωρήσουμε τους εξής 3 ορισμούς του S :

α') Το S είναι το σύνολο που παράγεται από το επαγωγικό ορισμό της άσκησης.

β') $S = \{(a, b) : \text{Υπάρχουν φυσικοί } k \text{ και } m \text{ τέτοιοι ώστε } (a, b) = (2k + 3m, 3k + 2m)\}$.

γ') $\{(a, b) : a, b \in \mathbb{N} \text{ και } a + b = 0 \pmod{5} \text{ και } 2a \leq 3b \text{ και } 2b \leq 3a\}$.

Και οι 3 τρόποι ορίζουν το S αλλά ο τελευταίος είναι ο πιο άμεσος. Αν για παράδειγμα μας δοθεί το $(a, b) = (1023, 1417)$, πώς θα ελέγξουμε αν ανήκει στο S ;

- Με τον τρίτο ορισμό η απάντηση είναι εύκολη γιατί $1023 + 1417 = 2440$ διαιρείται με το 5, και επιπλέον $2 \cdot 1023 \leq 3 \cdot 1417$ και $2 \cdot 1417 \leq 3 \cdot 1023$.
- Με τον δεύτερο ορισμό, πρέπει να βρούμε κατάλληλα k και m : Λύνουμε το σύστημα $2k + 3m = 1023$ και $3k + 2m = 1417$ και βρίσκουμε $k = 451$ και $m = 119$. Αφού αυτοί είναι φυσικοί αριθμοί, το $(1023, 1417)$ ανήκει στο S .
- Με τον πρώτο ορισμό δεν είναι σαφές πως να απαντήσουμε αν το $(1023, 1417)$ ανήκει στο S .

Το πλεονέκτημα όμως του δεύτερου ορισμού είναι ότι είναι εύκολο να δείξουμε ότι ορίζει το σύνολο S . Πώς;

Άσκηση (3.3). Έστω S ένα υποσύνολο του $\mathbb{N} \times \mathbb{N}$ που ορίζεται επαγωγικά ως εξής:

Βάση επαγωγικού ορισμού: $(1, 1) \in S$

Επαγωγικό βήμα: Αν $(a, b) \in S$ τότε $(a + b, b) \in S$ και $(a, a + b) \in S$.

α' Καταγράψτε τα στοιχεία του συνόλου S μετά από 3 εφαρμογές του επαγωγικού βήματος.

β' Χρησιμοποιήστε επαγωγή για να αποδείξετε ότι

$$S = \{(x, y) : x, y \in \mathbb{N} \text{ και } \gcd(x, y) = 1\}.$$

Λύση.

α' Τα στοιχεία του S που παράγονται με 3 εφαρμογές του επαγωγικού βήματος: $(1,1) \rightarrow (2,1), (1,2) \rightarrow (3,1), (2,3), (3,2), (1,3) \rightarrow (4,1), (3,4), (5,3), (2,5), (5,2), (3,5), (4,3), (1,4)$.

β' Θα δείξουμε πρώτα ότι όλα τα στοιχεία (x, y) που παράγονται έχουν την ιδιότητα $\gcd(x, y) = 1$. Με επαγωγή:

Βάση της επαγωγής: Το στοιχείο της βάσης $(1,1)$ έχει προφανώς αυτή την ιδιότητα.

Επαγωγικό βήμα: Αν το (x, y) έχει την ιδιότητα, τότε και τα $(x + y, y)$ και $(x, y + x)$ έχουν την ιδιότητα: Πράγματι $\gcd(x + y, y) = \gcd(x, y) = 1$ και $\gcd(x, x + y) = \gcd(x, y) = 1$.

Τώρα θα δείξουμε το αντίστροφο. Αν για κάποια x και y ισχύει $\gcd(x, y) = 1$, τότε ανήκει στο S (δηλαδή παράγεται από τους κανόνες). Με ισχυρή επαγωγή στο άθροισμα $x + y$.

Βάση της επαγωγής: Για $x + y = 2$, πρέπει να έχουμε $x = y = 1$ (επειδή $x, y \in \mathbb{N}$). Η πρόταση ισχύει αφού $(1, 1) \in S$ από τη βάση του επαγωγικού ορισμού.

Επαγωγικό βήμα: Έστω ότι κάθε ζεύγος x, y με $\gcd(x, y) = 1$ και $x + y \leq n$ ανήκει στο S . Θα δείξουμε ότι το ίδιο ισχύει και για κάθε ζεύγος x, y με $\gcd(x, y) = 1$ και $x + y = n + 1$.

Ας υποθέσουμε πως $x < y$ (ανάλογα εργαζόμαστε όταν $x > y$: η περίπτωση $x = y$ δεν υπάρχει γιατί θα είχαμε $\gcd(x, y) = x > 1$). Ας θεωρήσουμε τους αριθμούς $x' = x$ και $y' = y - x$. Για αυτούς ισχύει $x' + y' = y < x + y = n + 1$, δηλαδή $x + y \leq n$. Επίσης $\gcd(x', y') = \gcd(x, y - x) = \gcd(x, y) = 1$. Από την επαγωγική υπόθεση $(x', y') \in S$. Αλλά τότε με μια εφαρμογή του επαγωγικού βήματος του ορισμού, θα έχουμε πως $(x', x' + y') \in S$, δηλαδή πως $(x, y) \in S$.

Άσκηση (3.6). Θεωρήστε το σύνολο A των συμβολοσειρών του αλφαβήτου $\{0, 1\}$ που ορίζεται με τον εξής αναδρομικό ορισμό:

- $01 \in A$.
 - Αν $w \in A$, τότε $w1w \in A$.
1. Ποιο σύνολο είναι το A ; Περιγράψτε το με μια πρόταση της καθομιλουμένης.
 2. Δώστε επίσης μια ακριβή μαθηματική περιγραφή.
 3. Αποδείξτε προσεκτικά ότι η μαθηματική περιγραφή που δώσατε εκφράζει το σύνολο A .

Λύση. Οι συμβολοσειρές του συνόλου A αποτελούνται από 2^n διαδοχικά 011 από τις οποίες έχουμε αφαιρέσει το τελευταίο 1. Ισοδύναμα, κάθε συμβολοσειρά περιέχει $2^n - 1$ διαδοχικά 011 ακολουθούμενα από ένα 01. Πιο συγκεκριμένα, αν $(011)^k$ συμβολίζει τη συμβολοσειρά αποτελούμενη από την παράθεση k αντιγράφων του 011, τότε

$$A = \{(011)^{2^n-1}01 : n \in \mathbb{N}\}$$

Θα δείξουμε τώρα ότι αυτό είναι πράγματι το σύνολο A . Για να το δείξουμε αυτό πρέπει να δείξουμε δυο προτάσεις: Πρώτα ότι κάθε συμβολοσειρά που ανήκει στο A , δηλαδή κάθε συμβολοσειρά που παράγεται με τους παραπάνω κανόνες, έχει τη μορφή $(011)^{2^n-1}01$ για κάποιον φυσικό αριθμό n . Και το αντίστροφο, ότι δηλαδή κάθε συμβολοσειρά που είναι της μορφής $(011)^{2^n-1}01$ μπορεί να παραχθεί με τους παραπάνω κανόνες.

Για το πρώτο θα χρησιμοποιήσουμε δομική επαγωγή και για το δεύτερο μαθηματική επαγωγή στο n .

Πρόταση 74. Κάθε στοιχείο του συνόλου A είναι της μορφής $(011)^{2^n-1}01$ για κάποιο φυσικό αριθμό n .

Απόδειξη. Με δομική επαγωγή.

Βάση δομικής επαγωγής: Το 01 είναι της μορφής $(011)^{2^n-1}01$ γιατί για $n = 0$: $(011)^{2^0-1}01 = (011)^0 01 = 01$.

Επαγωγικό βήμα: Έστω $w \in A$. Από την επαγωγική υπόθεση υπάρχει n τέτοιο ώστε $w = (011)^{2^n-1}01$. Θα δείξουμε ότι το $w1w$ είναι της ίδιας μορφής. Πράγματι

$$w1w = (011)^{2^n-1}011(011)^{2^n-1}01 = (011)^{2^n-1+1+2^n-1} = (011)^{2^{n+1}-1}01$$

είναι της ίδιας μορφής. \square

Πρόταση 75. Κάθε συμβολοσειρά της μορφής $(011)^{2^n-1}01$, όπου n φυσικός αριθμός, παράγεται με τους κανόνες που ορίζουν το σύνολο A .

Απόδειξη. Με μαθηματική επαγωγή στο n .

Βάση της επαγωγής: Αν $n = 0$, τότε η συμβολοσειρά $(011)^{2^n-1}01 = (011)^0 01 = 01$ ανήκει στο σύνολο A , σύμφωνα με τον πρώτο κανόνα.

Επαγωγικό βήμα: Έστω ότι η πρόταση είναι αληθής για κάποιο n , δηλαδή $(011)^{2^n-1}01 \in A$. Θα δείξουμε ότι η πρόταση είναι αληθής για $n + 1$, δηλαδή ότι το $(011)^{2^{n+1}-1}01$ μπορεί να παραχθεί με τους παραπάνω κανόνες. Πράγματι, αν θέσουμε $w = (011)^{2^n-1}01$, τότε σύμφωνα με τον δεύτερο κανόνα, το $w1w$ ανήκει στο A και είναι ίσο με $w1w = (011)^{2^{n+1}-1}01$. \square

Άσκηση (3.7). Θεωρήστε το υποσύνολο T των φυσικών αριθμών που ορίζεται με τον εξής αναδρομικό ορισμό:

- $1 \in T$.
- Αν $n \in T$, τότε $2n \in T$.
- Αν $n \in T$, τότε $n + 3 \in T$.

1. Δώστε τα 10 μικρότερα στοιχεία του συνόλου T ;

2. Αποδείξτε προσεκτικά ότι το σύνολο T είναι το

$$\{3k + a : k \in \mathbb{N} \text{ και } a = 1, 2\}.$$

Λύση. Τα 10 μικρότερα στοιχεία του συνόλου T είναι 1,2,4,5,7,8,10,11,13,14.

Ας ορίσουμε το σύνολο $S = \{3k + a : k \in \mathbb{N} \text{ και } a = 1, 2\}$. Θέλουμε να δείξουμε ότι $T = S$. Για να το δείξουμε αυτό θα δείξουμε ότι $T \subseteq S$ και ότι $S \subseteq T$.

Πρόταση 76. Κάθε στοιχείο του συνόλου T είναι της μορφής $3k + 1$ ή της μορφής $3k + 2$, για κάποιο φυσικό αριθμό k . Ισοδύναμα, τα στοιχεία του συνόλου T δεν διαιρούνται με το 3.

Απόδειξη. Με δομική επαγωγή.

Βάση δομικής επαγωγής: Το 1 προφανώς δεν διαιρείται με το 3 (είναι της μορφής $3k + 1$).

Επαγωγικό βήμα: Έστω $m \in T$. Από την επαγωγική υπόθεση το m δεν διαιρείται με το 3. Αρκεί να δείξουμε ότι τα $2m$ και $m+3$ δεν διαιρούνται με το 3. Αλλά αυτό είναι σχεδόν προφανές (γιατι $\gcd(2m, 3) = \gcd(m, 3)$ και $\gcd(m+3, 3) = \gcd(m, 3)$).

Η απόδειξη τελειώσε αλλά αν θέλουμε μια εξαντλητική λύση μπορούμε να σκεφτούμε ως εξής:

- αν $m = 3k + 1$ τότε $2m = 3(2k) + 2$ και $m + 3 = 3(k + 1) + 1$ που είναι της κατάλληλης μορφής.
- αν $m = 3k + 2$ τότε $2m = 3(2k + 1) + 1$ και $m + 3 = 3(k + 1) + 1$ που είναι επίσης της κατάλληλης μορφής.

□

Θα δείξουμε τώρα το αντίστροφο:

Πρόταση 77. Κάθε φυσικός που δεν διαιρείται με το 3 μπορεί να παραχθεί με τους κανόνες που ορίζουν το σύνολο T .

Απόδειξη. Ας θεωρήσουμε ένα φυσικό αριθμό m της μορφής $3k+1$. Αυτός μπορεί να παραχθεί με μια εφαρμογή του πρώτου κανόνα (που μας δίνει 1) και στη συνέχεια k εφαρμογές του τρίτου κανόνα (που μας δίνει $1 + 3 + 3 + \dots + 3 = 1 + 3k$).

Ας θεωρήσουμε τώρα ένα φυσικό αριθμό m της μορφής $3k+2$. Αυτός μπορεί να παραχθεί με μια εφαρμογή του πρώτου κανόνα (που μας

δίνει 1), μια εφαρμογή του δεύτερου κανόνα (που μας δίνει 2) και στη συνέχεια k εφαρμογές του τρίτου κανόνα (που μας δίνει $2+3+3+\dots+3 = 2 + 3k$).

Στη συνέχεια δίνω μια εναλλακτική απόδειξη με μαθηματική επαγωγή.

Βάση επαγωγής: Το 1 και το 2 παράγονται με τους κανόνες (το 1 με τον πρώτο κανόνα και το 2 με χρήση του δεύτερου κανόνα).

Επαγωγικό βήμα: Ας θεωρήσουμε τώρα ένα φυσικό $m > 3$ που δεν διαιρείται με το 3. Η επαγωγική υπόθεση λέει ότι κάθε φυσικός μικρότερος του m που δεν διαιρείται με το 3 μπορεί να παραχθεί από τους κανόνες που ορίζουν το σύνολο T . Ειδικότερα ο $m-3$ είναι φυσικός γιατί $m-3 \geq 0$ και δεν διαιρείται με το 3, αφού υποθέσαμε ότι ο m δεν είναι πολλαπλάσιο του 3. Άρα μπορεί να παραχθεί με του κανόνες. Αλλά τότε με εφαρμογή του τρίτου κανόνα και ο $(m-3) + 3 = m$ παράγεται με τους κανόνες. \square

Άσκηση (3.8). Ορίζουμε αναδρομικά ένα σύνολο συμβολοσειρών P του αλφαβήτου $\{0, 1\}$ ως εξής :

1. Η κενή συμβολοσειρά ανήκει στο P : $\epsilon \in P$
2. Αν μια συμβολοσειρά w ανήκει στο σύνολο P , τότε και οι συμβολοσειρές $0w0$ και $1w1$ ανήκουν στο P .

Ποιο είναι το σύνολο P ; Αποδείξτε προσεκτικά την απάντησή σας.

Δύση. Το σύνολο $P = \{\epsilon, 00, 11, 0000, 0110, 1001, 1111, 000000, \dots\}$ είναι το σύνολο των συμβολοσειρών του αλφαβήτου $\{0, 1\}$ με άρτιο μήκος που είναι παλίνδρομες, δηλαδή παραμένουν ίδιες αν διαβαστούν από δεξιά προς τα αριστερά.

Έστω S το σύνολο των άρτιων παλίνδρομων του αλφαβήτου $\{0, 1\}$. Θα δείξουμε ότι $P = S$.

$P \subseteq S$: Θα δείξουμε δηλαδή πώς κάθε συμβολοσειρά που παράγεται με τους κανόνες είναι άρτιο παλίνδρομο. Με δομική επαγωγή:

Βάση της επαγωγής: Η κενή συμβολοσειρά έχει άρτιο μήκος (0) και διαβάζεται το ίδιο από δεξιά προς αριστερά.

Επαγωγικό βήμα: Αν w είναι άρτιο παλίνδρομο, τότε είναι σαφές και πως η $0w0$ είναι επίσης άρτιο παλίνδρομο. Το ίδιο και η $1w1$.

$S \subseteq P$: Θα δείξουμε δηλαδή πώς κάθε άρτιο παλίνδρομο παράγεται από του κανόνες. Με επαγωγή στο μήκος του.

Βάση της επαγωγής: Υπάρχει ένα μόνο παλίνδρομο μήκους 0, η κενή συμβολοσειρά ϵ η οποία παράγεται από τον πρώτο κανόνα.

Επαγωγικό βήμα: Έστω ότι κάθε παλίνδρομο μήκους $2k$ παράγεται από τους κανόνες. Θα δείξουμε πως κάθε παλίνδρομο μήκους $2(k+1)$ παράγεται από τους κανόνες. Πράγματι, έστω v ένα παλίνδρομο μήκους $2(k+1)$. Αν το πρώτο σύμβολο του v είναι 0, τότε αφού πρόκειται για παλίνδρομο, και το τελευταίο σύμβολό του θα είναι 0. Επιπλέον τα υπόλοιπα σύμβολα θα σχηματίζουν παλίνδρομο. Άρα η v είναι της

μορφής $0w0$, όπου w είναι παλίνδρομο και έχει μήκος $2k$. Από την επαγωγική υπόθεση, το w μπορεί να παραχθεί από τους κανόνες. Αλλά τότε με μια ακόμα εφαρμογή του δεύτερου κανόνα μπορούμε να παράγουμε το v . Με τον ίδιο ακριβώς τρόπο αντιμετωπίζουμε και την περίπτωση που το v ξεκινά με 1.

Κεφάλαιο 4

Άσκηση (4.8). Σ' ένα δρόμο με 101 σπίτια οι διευθύνσεις είναι από το 1 έως το 200. Δείξτε ότι υπάρχουν 2 γειτονικά σπίτια με αριθμούς που διαφέρουν κατά 1.

Υποθέστε ότι ο δρόμος έχει μόνο μια πλευρά και ότι αυτή η πλευρά περιέχει άρτιους και περιττούς αριθμούς.

Λύση. Με την Αρχή του Περιστερώνα όπου τα περιστέρια είναι οι αριθμοί των σπιτιών και οι φωλιές είναι τα σύνολα $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$, ..., $\{199, 200\}$. Υπάρχουν 101 περιστέρια και εκατό φωλιές. Κάποια φωλιά περιέχει 2 περιστέρια. Ισοδύναμα υπάρχουν δύο σπίτια με αριθμούς $2k - 1$ και $2k$ για κάποιο k .

Άσκηση (4.9). Έστω ότι διαλέγουμε 101 τυχαίους αριθμούς στο διάστημα $[0, 1)$. Δείξτε ότι υπάρχουν δυο αριθμοί που διαφέρουν κατά το πολύ $1/100$.

Λύση. Με την Αρχή του Περιστερώνα. Ας πάρουμε το διαστήμα $[0, 1)$ και ας το χωρίσουμε σε εκατό ίσα διαστήματα:

$$[0, 1/100), [1/100, 2/100), \dots, [99/100, 1).$$

Σύμφωνα με την Αρχή του Περιστερώνα, αν ρίξουμε 101 αριθμούς (περιστέρια) στα 100 αυτά διαστήματα (φωλιές), κάποιο διάστημα θα περιέχει δυο τουλάχιστον αριθμούς. Οι αριθμοί αυτοί διαφέρουν κατά το πολύ $1/100$ (όσο είναι το μήκος του διαστήματος).

Σημείωση: το γεγονός πως οι αριθμοί είναι τυχαίοι δεν παίζει κανένα ρόλο. Οποιοδήποτε σύνολο 101 αριθμών στο διάστημα $[0, 1)$ έχει την ιδιότητα¹

Άσκηση (4.11). Δείξτε, με χρήση της Αρχής του Περιστερώνα, ότι σε κάθε ομάδα n ανθρώπων, όπου $n > 1$, υπάρχουν δυο άνθρωποι που έχουν τον ίδιο αριθμό γνωστών. Υποθέτουμε ότι οι γνωριμίες είναι αμοιβαίες (αν ο X γνωρίζει τον Y , τότε και ο Y γνωρίζει τον X).

Λύση. Ο αριθμός των γνωστών ενός μέλους της ομάδας είναι ένας ακέραιος στο $\{0, 1, \dots, n - 1\}$ (δεν μετράμε τον εαυτό του στους γνωστούς). Δεν μπορούμε να εφαρμόσουμε άμεσα την Αρχή του Περιστερώνα γιατί υπάρχουν n άνθρωποι και n τιμές στο $\{0, 1, \dots, n - 1\}$. Το κόλπο είναι

¹Στην καθομιλουμένη μπερδεύουμε συχνά το 'τυχαίο' με το 'οποιοδήποτε'. (Λέμε, για παράδειγμα, 'έστω τυχαίος αριθμός' ενώ εννοούμε 'έστω κάποιος αριθμός επιλεγμένος με οποιοδήποτε τρόπο'.)

ότι αν υπάρχει άνθρωπος που έχει $n - 1$ γνωστούς τότε όλοι οι άνθρωποι τον γνωρίζουν και έχουν ένα τουλάχιστον γνωστό. Με άλλα λόγια, οι τιμές που μπορεί να πάρει ο αριθμός των γνωστών είναι είτε στο $\{1, 2, \dots, n - 1\}$ (όταν υπάρχει κάποιος που έχει $n - 1$ γνωστούς) είτε $\{1, \dots, n - 2\}$ (όταν κανένας δεν έχει $n - 1$ γνωστούς). Και στις δυο περιπτώσεις υπάρχουν n άνθρωποι και $n - 1$ τιμές, άρα από την Αρχή του Περιστερώνα δυο από τους ανθρώπους έχουν ίσο αριθμό γνωστών.

Άσκηση (4.9). Έστω ότι διαλέγουμε 101 τυχαίους αριθμούς στο διάστημα $[0, 1)$. Δείξτε ότι υπάρχουν δυο αριθμοί που διαφέρουν κατά το πολύ $1/100$.

Λύση. Με την Αρχή του Περιστερώνα. Ας πάρουμε το διάστημα $[0, 1)$ και ας το χωρίσουμε σε εκατό ίσα διαστήματα:

$$[0, 1/100), [1/100, 2/100), \dots, [99/100, 1).$$

Σύμφωνα με την Αρχή του Περιστερώνα, αν ρίξουμε 101 αριθμούς (περιστέρια) στα 100 αυτά διαστήματα (φωλιές), κάποιο διάστημα θα περιέχει δυο τουλάχιστον αριθμούς. Οι αριθμοί αυτοί διαφέρουν κατά το πολύ $1/100$ (όσο είναι το μήκος του διαστήματος).

Σημείωση: το γεγονός πως οι αριθμοί είναι τυχαίοι δεν παίζει κανένα ρόλο. Οποιοδήποτε σύνολο 101 αριθμών στο διάστημα $[0, 1)$ έχει την ιδιότητα².

Άσκηση (4.15). Δείξτε πως κάθε γράφος που έχει $n > 2$ κόμβους και m ακμές, όπου $m > n(n - 1)/3$, περιέχει ένα τουλάχιστον τρίγωνο K_3 (δηλαδή 3 κόμβους που ενώνονται ανά 2 μεταξύ τους).

Λύση. Με την Αρχή του Περιστερώνα. Φωλιές είναι οι τριάδες κόμβων του γράφου. Ένας γράφος με n κόμβους έχει $\binom{n}{3} = \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3}$ τριάδες διαφορετικών κόμβων. Τα περιστέρια είναι οι ακμές, αλλά πρέπει να λάβουμε υπόψη πως κάθε ακμή του γράφου ανήκει σε $n - 2$ τριάδες, μια τριάδα για κάθε κόμβο εκτός από τους δυο κόμβους της ακμής.

Επομένως έχουμε $f = \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3}$ φωλιές και s αυτές τοποθετούμε $p = m(n - 2)$ περιστέρια. Για $m > n(n - 1)/3$, ο αριθμός των περιστεριών p είναι μεγαλύτερος από $n(n - 1)(n - 2)/3$. Από την Αρχή του Περιστερώνα, υπάρχει φωλιά που έχει τουλάχιστον $\lceil p/f \rceil$ περιστέρια. Υπολογίζουμε το λόγο p/f και βρίσκουμε πως $p/f > 2$. Άρα κάποια φωλιά έχει τουλάχιστον 3 περιστέρια ή, ισοδύναμα, κάποια τριάδα έχει 3 ακμές και επομένως δημιουργεί τρίγωνο.

² Στην καθομιλουμένη μπερδεύουμε συχνά το 'τυχαίο' με το 'οποιοδήποτε'. (Λέμε, για παράδειγμα, 'έστω τυχαίος αριθμός' ενώ εννοούμε 'έστω κάποιος αριθμός επιλεγμένος με οποιοδήποτε τρόπο'.)

Κεφάλαιο 5

Άσκηση (5.3). Δείξτε ότι αν δυο σύνολα A_1 και A_2 είναι αριθμήσιμα, τότε και το καρτεσιανό γινόμενό τους

$$A = \{(a_1, a_2) : a_1 \in A_1 \text{ και } a_2 \in A_2\}$$

είναι επίσης αριθμήσιμο.

Λύση. Αφού τα A_1 και A_2 είναι αριθμήσιμα, μπορούμε να βάλουμε τα στοιχεία τους στη σειρά:

$$A_1 = \{x_1, x_2, \dots\}$$

$$A_2 = \{y_1, y_2, \dots\}$$

Αλλά τότε μπορούμε να βάλουμε τα στοιχεία του καρτεσιανού τους γινομένου στη σειρά με το ίδιο 'κόλπο' που χρησιμοποιήσαμε για τους ρητούς. Δηλαδή πρώτα τα στοιχεία με άθροισμα δεικτών 2, μετά αυτά με άθροισμα δεικτών 3 κοκ

$$A = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_1, y_3), (x_2, y_2), (x_3, y_1), (x_1, y_4), \dots\}.$$

Άσκηση (5.5). Θεωρήστε το σύνολο όλων των υποσυνόλων των φυσικών αριθμών

$$P(\mathbb{N}) = \{S : S \subset \mathbb{N}\}.$$

Χρησιμοποιείστε τη Μέθοδο της Διαγωνίου για να δείξετε ότι το σύνολο $P(\mathbb{N})$ δεν είναι αριθμήσιμο.

Λύση. Απόδειξη με εις άτοπον απαγωγή. Έστω ότι το σύνολο $P(\mathbb{N})$ είναι αριθμήσιμο. Τότε μπορούμε να βάλουμε τα στοιχεία του (δηλαδή τα υποσύνολα του \mathbb{N} , στη σειρά S_1, S_2, \dots . Θα κατασκευάσουμε ένα σύνολο S που διαφέρει από το καθένα από αυτά. Πιο συγκεκριμένα, το S θα διαφέρει από το S_1 στο αν περιέχει ή όχι τον αριθμό 1, από το S_2 στο αν περιέχει ή όχι τον αριθμό 2 κοκ. Δηλαδή

$$S = \{i : i \in \mathbb{N} \text{ και } i \notin S_i\}$$

Από την κατασκευή του το S διαφέρει από κάθε σύνολο της ακολουθίας S_1, S_2, \dots και επομένως δεν ανήκει σ' αυτή την ακολουθία. Αλλά το S είναι υποσύνολο του \mathbb{N} και θα έπρεπε να εμφανίζεται στην ακολουθία. Άτοπο.

Άσκηση (5.6). Έστω F το σύνολο των συναρτήσεων με πεδίο ορισμού το σύνολο των φυσικών αριθμών και με πεδίο τιμών επίσης το σύνολο των φυσικών αριθμών. Δείξτε ότι το σύνολο F δεν είναι αριθμήσιμο.

Λύση. Με χρήση της Μεθόδου της Διαγωνίου. Έστω ότι το σύνολο F είναι αριθμήσιμο. Τότε μπορούμε να βάλουμε τα στοιχεία του σε σειρά f_1, f_2, \dots έτσι ώστε όλα τα στοιχεία του να εμφανίζονται στην ακολουθία

αυτή. Το κάθε στοιχείο f_i είναι μία συνάρτηση με πεδίο ορισμού και πεδίο τιμών το σύνολο των φυσικών αριθμών. Θα κατασκευάσουμε τώρα ένα στοιχείο f του συνόλου F που διαφέρει από τα f_1, f_2, \dots :

$$f(n) = f_n(n) + 1$$

Η συνάρτηση f διαφέρει από την f_1 στην τιμή $f(1)$, από την f_2 στην τιμή $f(2)$ κοκ. Η f είναι συνάρτηση από τους φυσικούς στους φυσικούς, είναι δηλαδή στοιχείο του F , και διαφέρει από κάθε όρο της ακολουθίας f_1, f_2, \dots . Άτοπο, αφού υποθέσαμε ότι όλα τα στοιχεία του F εμφανίζονται στην ακολουθία.

Άσκηση (5.7). Είναι τα παρακάτω σύνολα αριθμήσιμα ή όχι; Αποδείξτε την απάντησή σας.

1. Το σύνολο των συναρτήσεων με πεδίο ορισμού τους φυσικούς \mathbb{N} και πεδίο τιμών το $\{0, 1\}$.
2. Το σύνολο των συναρτήσεων με πεδίο ορισμού το $\{0, 1\}$ και πεδίο τιμών τους φυσικούς \mathbb{N} .

Λύση. 1. Μη αριθμήσιμο. Μια συνάρτηση f από το \mathbb{N} στο $\{0, 1\}$ καθορίζεται από το υποσύνολο των φυσικών με εικόνα το 1, δηλαδή από το $\{k : f(k) = 1\}$. Από αυτό παρατηρούμε πως το σύνολο των συναρτήσεων με πεδίο ορισμού τους φυσικούς \mathbb{N} και πεδίο τιμών το $\{0, 1\}$ είναι ισοδύναμο με το σύνολο των υποσυνόλων των φυσικών αριθμών. Το τελευταίο όμως είναι γνωστό πως δεν είναι αριθμήσιμο.

Εναλλακτική λύση με τη Μέθοδο της Διαγωνίου: Έστω ότι ήταν αριθμήσιμο και έστω f_1, f_2, \dots μια απαρίθμηση των συναρτήσεων. Τότε η συνάρτηση g με $g(n) = 1 - f_n(n)$ διαφέρει από όλες τις συναρτήσεις και ανήκει στο σύνολο των συναρτήσεων, άτοπο.

2. Αριθμήσιμο. Το σύνολο των συναρτήσεων αυτό είναι ισοδύναμο με το σύνολο των ζευγών $\{f(0), f(1)\}$ των φυσικών αριθμών, που είναι γνωστό πως είναι αριθμήσιμο.

Εναλλακτική λύση: Μπορούμε να βάλουμε τις συναρτήσεις αυτές στη σειρά. Πρώτα τις συναρτήσεις f με $f(0) + f(1) = 0$, μετά τις συναρτήσεις με $f(0) + f(1) = 1$, μετά τις συναρτήσεις με $f(0) + f(1) = 2$ κοκ.

Άσκηση (5.8). Θεωρείστε το σύνολο των υποσυνόλων των φυσικών αριθμών που έχουν πληθικό αριθμό 3: $S_3 = \{\{x, y, z\} : x, y, z \in \mathbb{N} \text{ και } x < y < z\}$. (Οι ανισότητες εγγυώνται ότι τα x, y, z είναι διαφορετικά μεταξύ τους.)

1. Δείξτε ότι το σύνολο S_3 είναι αριθμήσιμο.
2. Εξηγήστε προσεκτικά που βρίσκεται το λάθος στην παρακάτω απόδειξη:

Απόδειξη. Θα χρησιμοποιήσουμε τη μέθοδο της Διαγωνίου για να δείξουμε ότι το σύνολο S_3 δεν είναι αριθμήσιμο. Έστω ότι ήταν αριθμήσιμο. Τότε θα υπήρχε ακολουθία A_1, A_2, \dots που περιέχει κάθε σύνολο που αποτελείται από 3 φυσικούς αριθμούς. Θα κατασκευάσουμε ένα νέο υποσύνολο B με 3 στοιχεία που διαφέρει από κάθε A_i . Πιο συγκεκριμένα, το B θα περιέχει το στοιχείο i αν και μόνο αν το A_i δεν περιέχει το στοιχείο i . Έτσι, το σύνολο B διαφέρει από το σύνολο A_i στο στοιχείο i . Αφού το B διαφέρει από κάθε A_i δεν ανήκει στην ακολουθία A_1, A_2, \dots . Άτοπο. Επομένως η υπόθεση ότι το S_3 είναι αριθμήσιμο δεν ισχύει. \square

Λύση. Η μέθοδος που παράγει το B δεν εγγυάται ότι αυτό θα έχει ακριβώς 3 στοιχεία.

Άσκηση (5.11). Είναι τα παρακάτω σύνολα αριθμήσιμα ή όχι; Αποδείξτε προσεκτικά τις απαντήσεις σας.

1. $I = \{f : f \text{ είναι αύξουσα συνάρτηση από το } \mathbb{Z}_0^+ \text{ στο } \mathbb{Z}_0^+\}$

Παράδειγμα: Η συνάρτηση

$$f(n) = \begin{cases} n & \text{αν } n \text{ είναι περιττός} \\ n+1 & \text{αν } n \text{ είναι άρτιος} \end{cases}$$

ανήκει στο I .

2. $D = \{f : f \text{ είναι φθίνουσα συνάρτηση από το } \mathbb{Z}_0^+ \text{ στο } \mathbb{Z}_0^+\}$

Παράδειγμα: Η συνάρτηση

$$f(n) = \left\lfloor \frac{10}{n+1} \right\rfloor$$

ανήκει στο D .

Λύση. Θα δείξουμε με τη μέθοδο της Διαγωνίου ότι το σύνολο I δεν είναι αριθμήσιμο. Έστω ότι ήταν αριθμήσιμο. Τότε θα μπορούσαμε να βάλουμε στη σειρά τις αύξουσες συναρτήσεις από το \mathbb{Z}_0^+ στο \mathbb{Z}_0^+ . Έστω f_1, f_2, \dots αυτή η σειρά. Θα κατασκευάσουμε τώρα μια αύξουσα συνάρτηση από το \mathbb{Z}_0^+ στο \mathbb{Z}_0^+ που διαφέρει από κάθε συνάρτηση f_i στην i -οστή τιμή, δηλαδή $f(i) \neq f_i(i)$. Μια τέτοια συνάρτηση είναι η

$$f(i) = \begin{cases} i & \text{αν } f_i(i) \neq i \\ i+1 & \text{αν } f_i(i) = i \end{cases}$$

Είναι προφανές ότι για κάθε i , $f(i) \neq f_i(i)$, αλλά είναι η συνάρτηση f αύξουσα; Ναι, γιατί από τον ορισμό της $i \leq f(i) \leq i+1$. Η σχέση αυτή για $i+1$ είναι $i+1 \leq f(i+1) \leq i+2$ και επομένως $f(i) \leq i+1 \leq f(i+1)$.

Μια άλλη λύση, δηλαδή μια διαφορετική f , είναι η εξής:

$$\begin{aligned} f(1) &= 1 + f_1(1) \\ f(2) &= 1 + f_1(1) + f_2(2) \\ &\vdots \\ f(i) &= 1 + f_1(1) + \dots + f_i(i) \\ &\vdots \end{aligned}$$

Αντίθετα με το I , το σύνολο D είναι αριθμήσιμο! Θα δείξουμε πως μπορούμε να βάλουμε στη σειρά τις φθίνουσες συναρτήσεις από το \mathbb{Z}_0^+ στο \mathbb{Z}_0^+ . Η βασική διαφορά με το σύνολο I είναι πως μια φθίνουσα συνάρτηση γίνεται σταθερή από κάποιο σημείο και πέρα. Οι τιμές της δεν μπορεί να μικραίνουν συνεχώς αφού πρέπει να είναι θετικοί ακέραιοι. Πιο συγκεκριμένα, για κάθε φθίνουσα συνάρτηση f του συνόλου D , υπάρχει κάποιος θετικός ακέραιος, που θα τον συμβολίσουμε με m_f , τέτοιος ώστε $f(i) = f(m_f)$ για κάθε $i \geq m_f$.

Αν μας δοθεί η αρχική τιμή $f(0)$ και η τιμή m_f πέρα από την οποία η συνάρτηση είναι σταθερή, υπάρχει πεπερασμένος αριθμός διαφορετικών τέτοιων συναρτήσεων του D . Μια τέτοια συνάρτηση χαρακτηρίζεται από τις τιμές $f(0), f(1), \dots, f(m_f)$ και όλες αυτές οι τιμές είναι στο διάστημα $\{0, 1, \dots, f(0)\}$. Δηλαδή υπάρχουν το πολύ $f(0)^{m_f}$ διαφορετικές συναρτήσεις του D με αρχική τιμή $f(0)$ και σταθερές μετά από το σημείο m_f .

Μπορούμε τώρα να βάλουμε τις φθίνουσες συναρτήσεις στη σειρά. Επειδή υπάρχουν δυο παράμετροι, οι $f(0)$ και m_f , κάνουμε το ίδιο κόλπο όπως και με τους ρητούς αριθμούς και θεωρούμε το αθροισμά τους: Πρώτα βάζουμε όλες τις συναρτήσεις f με $f(0) + m_f = 0$ (με οποιαδήποτε, π.χ. λεξικογραφική, σειρά), μετά τις συναρτήσεις με $f(0) + m_f = 1$, μετά τις συναρτήσεις με $f(0) + m_f = 2$, κοκ. Επειδή κάθε τέτοια ομάδα περιέχει πεπερασμένο αριθμό συναρτήσεων, και επειδή κάθε συνάρτηση f του D ανήκει σε μια τέτοια ομάδα, η f θα εμφανιστεί στην ακολουθία μετά από πεπερασμένο αριθμό συναρτήσεων.

Κεφάλαιο 6

Άσκηση (6.3). Έστω ότι έχετε ένα πιθανοτικό αλγόριθμο A για ένα πρόβλημα απόφασης (δηλαδή ένα πρόβλημα που οι απαντήσεις είναι 'ναι' και 'όχι') που για κάθε είσοδο δίνει τη σωστή απάντηση με πιθανότητα τουλάχιστον $\frac{3}{4}$.

1. Θέλουμε να τρέξουμε τον αλγόριθμο πολλές φορές ώστε να αυξήσουμε την πιθανότητα σωστής απάντησης σε $\frac{15}{16}$; Εξηγήστε με ακρίβεια πως θα το κάνουμε αυτό και πόσες φορές πρέπει να τρέξουμε τον αλγόριθμο A .

2. Γενικεύστε την προηγούμενη απάντηση για την περίπτωση που θέλουμε να αυξήσουμε την πιθανότητα σωστής απάντησης στο $1-\epsilon$, για κάποιο μικρό θετικό ϵ .

Λύση. Ένας τρόπος για να βελτιώσουμε την πιθανότητα σωστής απάντησης είναι να τρέξουμε τον αλγόριθμο A 3 φορές και να επιστρέψουμε την απάντηση που πλειοψηφεί. (Δεν είναι σαφές αν κερδίζουμε όταν τον τρέξουμε 2 φορές μόνο, γιατί τι θα απαντήσουμε όταν η μια απάντηση είναι 'ναι' και η άλλη 'όχι';) Για να υπολογίσουμε την πιθανότητα επιτυχίας όταν τον τρέχουμε 3 φορές, μπορούμε χωρίς βλάβη της γενικότητας, λόγω της συμμετρίας, να θεωρήσουμε ότι η σωστή απάντηση είναι 'ναι'. Ποια η πιθανότητα ότι θα δώσουμε τη σωστή απάντηση ή ισοδύναμα ότι 2 τουλάχιστον φορές θα πάρουμε την απάντηση 'ναι'; Ας πάρουμε όλα τα δυνατά ενδεχόμενα και ας υπολογίσουμε τις πιθανότητες του καθενός (όπου συμβολίζουμε το 'ναι' με 1 και το 'όχι' με 0):

Απαντήσεις	Πλειοψηφία	Πιθανότητα
000	0	$\left(\frac{1}{4}\right)^3$
001	0	$\left(\frac{1}{4}\right)^2 \frac{3}{4}$
010	0	$\left(\frac{1}{4}\right)^2 \frac{3}{4}$
100	0	$\left(\frac{1}{4}\right)^2 \frac{3}{4}$
110	1	$\left(\frac{3}{4}\right)^2 \frac{1}{4}$
101	1	$\left(\frac{3}{4}\right)^2 \frac{1}{4}$
011	1	$\left(\frac{3}{4}\right)^2 \frac{1}{4}$
111	1	$\left(\frac{3}{4}\right)^3$

Η πιθανότητα επιτυχίας προκύπτει από τις 4 τελευταίες περιπτώσεις:

$$\left(\frac{3}{4}\right)^3 + 3 \cdot \left(\frac{3}{4}\right)^2 \frac{1}{4} = \frac{27}{32}$$

Αυτή η πιθανότητα είναι καλύτερη από $3/4$ αλλά δεν είναι μεγαλύτερη από $15/16$. Για να αυξήσουμε και άλλο την πιθανότητα επιτυχίας, μπορούμε να τρέξουμε τον αλγόριθμο 5 φορές, ή 7 φορές, ή γενικά $2k+1$ φορές και να πάρουμε την απάντηση που πλειοψηφεί.

Ποια η πιθανότητα επιτυχίας; Με τον ίδιο τρόπο που υπολογίσαμε παραπάνω για 3 φορές υπολογίζουμε την απάντηση για $2k+1$ φορές. Η πιθανότητα είναι

$$\begin{aligned} & \left(\frac{3}{4}\right)^{2k+1} + \binom{2k+1}{1} \left(\frac{3}{4}\right)^{2k} \frac{1}{4} + \dots + \binom{2k+1}{k} \left(\frac{3}{4}\right)^{k+1} \left(\frac{1}{4}\right)^k \\ &= \sum_{i=0}^k \binom{2k+1}{i} \left(\frac{3}{4}\right)^{2k+1-i} \left(\frac{1}{4}\right)^i \end{aligned} \tag{A.1}$$

Θέλουμε να βρούμε το ελάχιστο ακέραιο k για το οποίο αυτή η πιθανότητα είναι τουλάχιστον $15/16$. Υπολογίζουμε την πιθανότητα για $k = 2, 3, 4$ και παρατηρούμε ότι για $k = 4$ η πιθανότητα γίνεται μεγαλύτερη από $15/16$. Άρα αν τρέξουμε τον αλγόριθμο 9 φορές και επιστρέψουμε την απάντηση που πλειοψηφεί, η πιθανότητα επιτυχίας είναι μεγαλύτερη από $15/16$.

Αν θέλουμε να βρούμε τη σωστή απάντηση με πιθανότητα τουλάχιστον $1 - \epsilon$, τότε πρέπει να τρέξουμε τον αλγόριθμο $2k + 1$ φορές, όπου k ο ελάχιστος ακέραιος για τον οποίο η πιθανότητα (Α'.1) είναι τουλάχιστον $1 - \epsilon$. Το ελάχιστο τέτοιο k είναι δύσκολο να υπολογιστεί αναλυτικά με ακρίβεια, άλλα μπορούμε να χρησιμοποιήσουμε κατάλληλες προσεγγίσεις για να βρούμε ένα κάπως μεγαλύτερο k που εγγυάται πιθανότητα επιτυχίας $1 - \epsilon$.

Άσκηση (6.4). Έστω ότι έχουμε ένα πιθανοτικό αλγόριθμο A που για κάθε είσοδο x :

- Αν η σωστή απάντηση για την είσοδο x είναι 'ναι', τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά 'ναι') με πιθανότητα $1/2$.
- Αν η σωστή απάντηση για την είσοδο x είναι 'όχι', τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά 'όχι') με πιθανότητα $9/10$.

Πως μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο A ώστε να κατασκευάσουμε ένα αλγόριθμο που δίνει την σωστή απάντηση—ανεξάρτητα αν η σωστή απάντηση είναι 'ναι' ή 'όχι'—με πιθανότητα τουλάχιστον $3/4$;

Λύση. Η απάντηση είναι πολύ απλή: Τρέχουμε τον αλγόριθμο A με είσοδο x δυο φορές: Απαντάμε 'όχι' αν και μόνο αν η απάντηση που πήραμε και τις δυο φορές είναι 'όχι'. Αλλιώς απαντάμε 'ναι'.

Γιατί είναι σωστή αυτή η λύση; Ας εισάγουμε λίγο συμβολισμό για να είμαστε πιο σαφείς. Θα χρησιμοποιήσουμε την αντιστοιχία

$$0 = \text{όχι} \quad 1 = \text{ναι}.$$

Έστω $f(x)$ συμβολίζει τη σωστή απάντηση για την είσοδο x , και έστω ότι $A_1(x)$ και $A_2(x)$ συμβολίζουν τα αποτελέσματα που παίρνουμε όταν τρέχουμε τον αλγόριθμο A με είσοδο x δυο φορές. Οι $A_1(x)$ και $A_2(x)$ είναι τυχαίες μεταβλητές.

Τότε από την εκφώνηση έχουμε

$$\Pr[A_1(x) = 0] = \Pr[A_2(x) = 0] = \begin{cases} 9/10 & \text{αν } f(x) = 0 \\ 1/2 & \text{αν } f(x) = 1 \end{cases}$$

και

$$\Pr[A_1(x) = 1] = \Pr[A_2(x) = 1] = \begin{cases} 1/10 & \text{αν } f(x) = 0 \\ 1/2 & \text{αν } f(x) = 1 \end{cases}$$

Στον παρακάτω πίνακα η πρώτη στήλη έχει το αποτέλεσμα των δυο εκτελέσεων του αλγόριθμου A . Η δεύτερη και τρίτη στήλη έχει την πιθανότητα να συμβεί το αντίστοιχο γεγονός της πρώτης στήλης όταν η σωστή απάντηση είναι 0 και 1 αντίστοιχα.

$A_1(x)A_2(x)$	$f(x) = 0$	$f(x) = 1$
00	$\frac{9}{10} \frac{9}{10}$	$\frac{1}{2} \frac{1}{2}$
01	$\frac{9}{10} \frac{1}{10}$	$\frac{1}{2} \frac{1}{2}$
10	$\frac{1}{10} \frac{9}{10}$	$\frac{1}{2} \frac{1}{2}$
11	$\frac{1}{10} \frac{1}{10}$	$\frac{1}{2} \frac{1}{2}$

Αν η σωστή απάντηση είναι 0 (δηλαδή αν $f(x) = 0$) τότε η πιθανότητα να δώσουμε απάντηση 0 είναι $81/100 \geq 3/4$ (αυτή είναι η πιθανότητα να έρθουν δυο 0). Αν η σωστή απάντηση είναι 1 (δηλαδή αν $f(x) = 1$) τότε η πιθανότητα να δώσουμε απάντηση 1 είναι $1/4 + 1/4/1/4 \geq 3/4$ (αυτή είναι η πιθανότητα να μην έρθουν δυο 0). Και στις δυο περιπτώσεις η πιθανότητα ορθής απάντησης είναι τουλάχιστον $3/4$.

Άσκηση (6.5). Κατασκευάζουμε ένα τυχαίο κανονικό δυαδικό δένδρο ξεκινώντας από μια ρίζα και επαναλαμβάνοντας τον εξής κανόνα:

Σε κάθε νέο κόμβο u του δένδρου, με πιθανότητα p προσθέτουμε 2 παιδιά στον u , ενώ με πιθανότητα $1-p$ ο u παραμένει για πάντα φύλλο.

Στην αρχή βέβαια υπάρχει μόνο ένας νέος κόμβος του δένδρου, η ρίζα του.

Αν $p < 1/2$, υπολογίστε τον αναμενόμενο αριθμό των κόμβων του δένδρου (σαν συνάρτηση του p).

Λύση. Έστω X η τυχαία μεταβλητή που εκφράζει τον αριθμό των κόμβων του δένδρου. Με πιθανότητα p η τιμή της X είναι 1 και με πιθανότητα $1-p$ η τιμή της είναι $1 + X_l + X_r$, όπου X_l και X_r είναι τυχαίες μεταβλητές που εκφράζουν τον αριθμό των κόμβων του αριστερού υποδένδρου και του δεξιού υποδένδρου αντίστοιχα. Αφού η ίδια διαδικασία παράγωγης του δένδρου εφαρμόζεται στο κύριο δένδρο και στο κάθε παιδί, προκύπτει αμέσως ότι ο αναμενόμενος αριθμός των κόμβων των δένδρων αυτών είναι ίσος, δηλαδή,

$$E[X] = E[X_l] = E[X_r]$$

Επομένως ο αναμενόμενος αριθμός κόμβων είναι ίσος με $E[X] = p \cdot 1 + (1-p) \cdot (1 + E[X_l] + E[X_r]) = p + (1-p)(1 + 2E[X]) = 1 + 2pE[X]$.

Αν λύσουμε ως προς $E[X]$, βρίσκουμε ότι ο αναμενόμενος αριθμός κόμβων είναι $E[X] = 1/(1-2p)$.

Η απάντηση αυτή είναι μεν σωστή, αλλά ο τρόπος δεν είναι απόλυτα σωστός. Ο λόγος είναι ότι υπάρχει και δεύτερη λύση της εξίσωσης $E[X] = 1 + 2pE[X]$, η λύση $E[X] = \infty$. Με άλλα λόγια, αν κάποιος μας

εγγυηθεί ότι η μεταβλητή X έχει πεπερασμένη αναμενόμενη τιμή, τότε η τιμή της είναι πράγματι $1/(1-2p)$. Αλλά αυτό δεν το ξέρουμε από πριν. Για να υπολογίσουμε την αναμενόμενη τιμή χωρίς αυτή την υπόθεση, το κάνουμε ως εξής: $E[X] = 1 + 2pE[X] = 1 + 2p(1 + 2pE[X]) = 1 + 2p + (2p)^2 E[X] = \dots = 1 + 2p + (2p)^2 + \dots$. Δηλαδή, η αναμενόμενη τιμή των κόμβων σε βάθος ένα είναι $2p$, σε βάθος 2 $(2p)^2$, και γενικά σε βάθος k $(2p)^k$. Αλλά τότε έχουμε ότι η αναμενόμενη τιμή είναι $1 + 2p + (2p)^2 + \dots = 1/(1-2p)$.

Άσκηση (6.6). Έστω ότι ρίχνουμε b μπαλάκια σε n δοχεία. Το κάθε μπαλάκι ρίχνεται με ομοιόμορφη κατανομή στα δοχεία και ανεξάρτητα από τα υπόλοιπα μπαλάκια. Υπολογίστε την πιθανότητα ότι κανένα δοχείο δεν περιέχει δυο ή περισσότερα μπαλάκια όταν

1. $b = 2$
2. $b = n$.
3. $b = n + 1$.

Λύση. Υπάρχουν n^b διαφορετικοί τρόποι να τοποθετήσουμε b (αριθμημένα) μπαλάκια σε n δοχεία (το πρώτο μπαλάκι μπορεί να πάει σε n δοχεία, το δεύτερο σε n δοχεία κοκ). Από αυτούς τους τρόπους, οι $n(n-1)\dots(n-b+1)$ έχουν το κάθε μπαλάκι σε διαφορετικό δοχείο (το πρώτο μπαλάκι μπορεί να πάει σε n δοχεία, το δεύτερο σε $n-1$ δοχεία γιατί το ένα είναι ήδη κατειλημμένο, κοκ: το b -οστό μπαλάκι μπορεί να πάει σε $n-(b-1) = n-b+1$ δοχεία γιατί $b-1$ δοχεία είναι ήδη κατειλημμένα). Άρα η πιθανότητα τα b μπαλάκια να καταλήξουν σε διαφορετικά δοχεία είναι

$$p_b = \frac{n(n-1)\dots(n-b+1)}{n^b}$$

1. Για $b = 2$ η πιθανότητα αυτή είναι $p_2 = \frac{n(n-1)}{n^2} = (n-1)/n$.
2. Για $b = n$ η πιθανότητα είναι $p_n = n!/n^n$.
3. Για $b = n + 1$ η πιθανότητα είναι $p_{n+1} = 0$, αφού ο τελευταίος πολλαπλασιαστής του αριθμητή είναι $n - b + 1 = 0$. Το τελευταίο αποτέλεσμα προκύπτει άμεσα και από την Αρχή του Περιστερώνα: Δεν μπορούμε να βάλουμε $n+1$ μπαλάκια σε n δοχεία χωρίς κάποιο δοχείο να περιέχει τουλάχιστον 2 μπαλάκια.

Κεφάλαιο 7

Άσκηση (7.2). Κάποιος που θέλει να 'σπάσει' ένα σύστημα RSA κατάφερε να βρει ένα κατάσκοπο και με πολλές προσπάθειες να αποκτήσει ένα αποκρυπτογραφημένο μήνυμα του συστήματος. Έχει λοιπόν στη

διάθεση του ένα μήνυμα στην κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή. Ελπίζει ότι με αυτή την πληροφορία θα καταφέρει να 'σπάσει' το σύστημα και να μπορεί να αποκρυπτογραφεί κάθε μήνυμα γρήγορα: χωρίς τη βοήθεια του κατασκόπου φυσικά. Τι λέτε, μπορεί; Εξηγήστε.

Υποθέστε βέβαια ότι το σύστημα RSA χρησιμοποιεί πάντα τα ίδια ιδιωτικά και δημόσια κλειδιά.

Λύση. Το γεγονός ότι γνωρίζει ένα μήνυμα στην κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή δεν βοηθάει. Ο κατάσκοπος έδωσε κάποια πληροφορία που μπορούσε να αποκτήσει οποιοσδήποτε: ο τρόπος κωδικοποίησης είναι δημόσιος, γνωστός δηλαδή σε όλους. Θα μπορούσε λοιπόν κάποιος να πάρει οποιοδήποτε μήνυμα και να το κρυπτογραφήσει. Έτσι θα γνωρίζει και την κρυπτογραφημένη και την αποκρυπτογραφημένη μορφή του.

Ας σημειωθεί ότι η απάντηση ισχύει για κάθε σύστημα δημόσιου κλειδιού, όχι μόνο για το RSA.

Κεφάλαιο 8

Άσκηση (8.1). Δείξτε τις παρακάτω σχέσεις βρίσκοντας κατάλληλες σταθερές c και n_0 του ορισμού του συμβολισμού O :

1. $n = O(2n + \log n)$

2. $4n^2 = O(n^2 - 10)$

3. $n^3 2^n = O(4^n)$

Λύση. 1. Θα πάρουμε $n_0 = 1$, για να έχουμε $\log n \geq 0$. Επομένως $2n + \log n \geq 2n \geq n$. Αρκεί λοιπόν να πάρουμε $c = 1$ και $n_0 = 1$.

2. Θέλουμε να έχουμε $4n^2 \leq c(n^2 - 10)$. Ισοδύναμα $10 \leq (1 - 4/c)n^2$. Για να ισχύει αυτό πρέπει το $1 - 4/c$ να είναι θετικό, ας πούμε $1/2$. Παίρνουμε λοιπόν $c = 8$ και βρίσκουμε πως πρέπει να έχουμε $10 \leq n^2/2$. Αυτό ισχύει για $n \geq 5$. Επομένως η πρόταση ισχύει για $c = 8$ και $n_0 = 5$.

3. Παρατηρούμε πως το 4^n είναι για μεγάλα n πολύ μεγαλύτερο από το n^3 και το 2^n . Θα πάρουμε λοιπόν $c = 1$. Θέλουμε να έχουμε $n^3 2^n \leq 4^n$ που είναι ισοδύναμο με $n^3 \leq 2^n$. Αυτό ισχύει για $n \geq 3$. Παίρνουμε λοιπόν $c = 1$ και $n_0 = 3$.

Άσκηση (8.10). Δώστε συναρτήσεις $f(n)$ και $g(n)$ για τις οποίες ισχύει $f(n) = O(g(n))$ αλλά δεν ισχύει $2^{f(n)} = O(2^{g(n)})$.

Λύση. Ας πάρουμε $f(n) = 2n$ και $g(n) = n$. Έχουμε $2n = O(n)$, αλλά δεν ισχύει $2^{2n} = O(2^n)$, γιατί $2^{2n} = 4^n$.

Κεφάλαιο 9

Άσκηση (9.2). Δείξτε πως για κάθε γράφο G είτε ο G είτε ο συμπληρωματικός του \bar{G} είναι συνεκτικός. Υπενθυμίζεται πως ο συμπληρωματικός γράφος \bar{G} είναι αυτός που έχει ακριβώς τις ακμές που λείπουν από τον G .

Λύση. Με απαγωγή σε άτοπο. Έστω ότι υπάρχει γράφος G που ούτε αυτός ούτε ο \bar{G} είναι συνεκτικοί. Αφού ο G δεν είναι συνεκτικός, οι κόμβοι του θα μπορούν να χωριστούν σε δυο τμήματα A και B τέτοια ώστε δεν υπάρχει καμία ακμή μεταξύ των κόμβων του A και B . Αλλά τότε όλες αυτές οι ακμές θα πρέπει να υπάρχουν στον συμπληρωματικό του G . Δηλαδή ο \bar{G} περιέχει τον πλήρη διμερή γράφο με πλευρές τα A και B , και ίσως περιέχει επιπλέον ακμές. Αλλά ο πλήρης διμερής γράφος είναι συνεκτικός αφού κάθε δυο κόμβοι ενώνονται είτε με μια ακμή είτε με ένα μονοπάτι δυο ακμών. Άρα ο \bar{G} είναι συνεκτικός. Άτοπο.

Άσκηση (9.5). Δείξτε πως ο γράφος του Petersen δεν είναι επίπεδος χρησιμοποιώντας το Θεώρημα του Kuratowski. Δείξτε δηλαδή πως ο γράφος του Petersen περιέχει μια υποδιαίρεση του K_5 ή του $K_{3,3}$.

Λύση. Θα δείξουμε πως ο γράφος του Petersen περιέχει μια υποδιαίρεση του $K_{3,3}$. Στο Σχήμα 9.6 η μια πλευρά του $K_{3,3}$ θα περιέχει τους κόμβους 1, 3, 7 και η άλλη πλευρά τους κόμβους 2, 9, 10. Αν αφαιρέσουμε τις ακμές $[4, 5]$ και $[6, 8]$, παρατηρούμε πως ο γράφος που απομένει είναι μια υποδιαίρεση του $K_{3,3}$. Για παράδειγμα, η ακμή $[1, 9]$ αντιστοιχεί στο μονοπάτι $(1, 6, 9)$.

Β΄ Άλλες Πηγές

Υπάρχουν πολύ καλά βιβλία με παρόμοιο περιεχόμενο και προσανατολισμό:

- Kenneth H. Rosen. Discrete Mathematics and its Applications.
- Lazlo Lovasz, Jozsef Pelikan, Katalin Vesztergombi. Discrete Mathematics.
- Eric Lehman and Tom Leighton. Mathematics for Computer Science. Αυτό κυκλοφορεί σε ελεύθερη online έκδοση.

Για μια βαθύτερη προσέγγιση κάποιων θεμάτων:

- Για τον συμβολισμό O και γενικότερα την ανάλυση αλγορίθμων προτείνω τα:
 - S. Dasgupta, C.H. Papadimitriou, and U.V. Vazirani. Algorithms. Αυτό κυκλοφορεί σε ελεύθερη online έκδοση.
 - J. Kleinberg and E. Tardos. Algorithm Design.
 - Cormen, Leiserson, Rivest, and Stein. Introduction to Algorithms.
- Για πιθανότητες στην πληροφορική προτείνω τα
 - M. Mitzenmacher and E. Upfal. Probability and Computing : Randomized Algorithms and Probabilistic Analysis.
 - R. Motwani and P. Raghavan. Randomized Algorithms.
- Για τη Μέθοδο της Διαγωνίου και γενικότερα τη Θεωρία Υπολογισμού προτείνω τα:
 - John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman. Introduction to Automata Theory, Languages, and Computation.
 - Michael Sipser. Introduction to the Theory of Computation.
 - Christos Papadimitriou and Harry Lewis. Elements of the theory of computation.
 - Christos Papadimitriou. Computational Complexity

- Για βιβλία λογοτεχνίας σχετικά με τα μαθηματικά προτείνω τα:
 - Απόστολος Δοξιάδης. Ο θείος Πέτρος και η εικασία του Γκόλντμπαχ.
 - Χρίστος Παπαδημητρίου. Το χαμόγελο του Τούρινγκ.

Κάποια από τα παραπάνω βιβλία κυκλοφορούν και μεταφρασμένα στα Ελληνικά.