το Π_2. Να δείξετε ότι η R είναι μερική διάταξη στο $\mathcal{P}$. Ποια στοιχεία του $\mathcal{P}$ είναι μέγιστα και ποια ελάχιστα; Θεωρήστε ότι το $\mathcal{P}$ είναι μια αυθαίρετη συλλογή των υποσυνόλων του 2^S, τα οποία δεν χρειάζεται να είναι διαμερίσεις του S. Θα ήταν τότε απαραίτητα η R μερική διάταξη;

1.4 ΠΕΠΕΡΑΣΜΕΝΑ ΚΑΙ ΑΠΕΙΡΑ ΣΥΝΟΛΑ

Μία βασική ιδιότητα ενός πεπερασμένου συνόλου είναι το *μέγεθός* του, δηλαδή ο αριθμός των στοιχείων που περιέχει. Κάποια δεδομένα για τα μεγέθη των πεπερασμένων συνόλων είναι τόσο προφανή που δεν χρειάζονται απόδειξη. Για παράδειγμα, αν $A \subseteq B$, τότε το μέγεθος του A είναι μικρότερο ή ίσο από αυτό του B· το μέγεθος του A είναι μηδέν αν και μόνον αν το A είναι το κενό σύνολο.

Ωστόσο, μια επέκταση της έννοιας του «μεγέθους» στα άπειρα σύνολα οδηγεί σε δυσκολίες, αν προσπαθήσουμε να ακολουθήσουμε τη διαίσθησή μας. Υπάρχουν περισσότερα πολλαπλάσια του 17 $(0, 17, 34, 51, 68, \ldots)$ από ό,τι τέλεια τετράγωνα $(0, 1, 4, 9, 16, \ldots)$; Μπορείτε, αν θέλετε, να ερευνήσετε τις εναλλακτικές λύσεις, όμως η εμπειρία έχει δείξει ότι η μοναδική ικανοποιητική σύμβαση είναι να θεωρήσουμε ότι τα δύο αυτά σύνολα έχουν *το ίδιο μέγεθος*.

Ονομάζουμε δύο σύνολα A και B **ισάριθμα** αν υπάρχει αμφιμονοσήμαντη αντιστοιχία $f : A \mapsto B$. Θυμηθείτε ότι αν υπάρχει αμφιμονοσήμαντη αντιστοιχία $f : A \mapsto B$, τότε υπάρχει και αμφιμονοσήμαντη αντιστοιχία $f^{-1} : B \mapsto A$· άρα η σχέση αυτή είναι μια συμμετρική σχέση. Στην πραγματικότητα, όπως εύκολα αποδεικνύεται, είναι και σχέση ισοδυναμίας. Για παράδειγμα, τα $\{8, IAa, \{\emptyset, b\}\}$ και $\{1, 2, 3\}$ είναι ισάριθμα· έστω $f(8) = 1, f(IAa) = 2, f(\{\emptyset, b\} = 3$. Το ίδιο ισχύει και για τα πολλαπλάσια του 17 και τα τέλεια τετράγωνα· υπάρχει αμφιμονοσήμαντη αντιστοιχία $f(17n) = n^2$ για κάθε $n \in \mathbf{N}$.

Γενικά, ονομάζουμε ένα σύνολο **πεπερασμένο**, αν, διαισθητικά, είναι ισάριθμο με το $\{1, 2, \ldots, n\}$ για κάποιο φυσικό αριθμό n. (Για $n = 0$, $\{1, \ldots, n\}$ είναι το κενό σύνολο, και έτσι το $\emptyset$ είναι πεπερασμένο, καθώς είναι ισάριθμο με τον εαυτό του). Αν A και $\{1, \ldots, n\}$ είναι ισάριθμα, τότε λέμε ότι ο πληθικός αριθμός του A (συμβολίζουμε με $|A|$) είναι n. Ο πληθικός αριθμός ενός πεπερασμένου συνόλου είναι επομένως ο αριθμός των στοιχείων του.

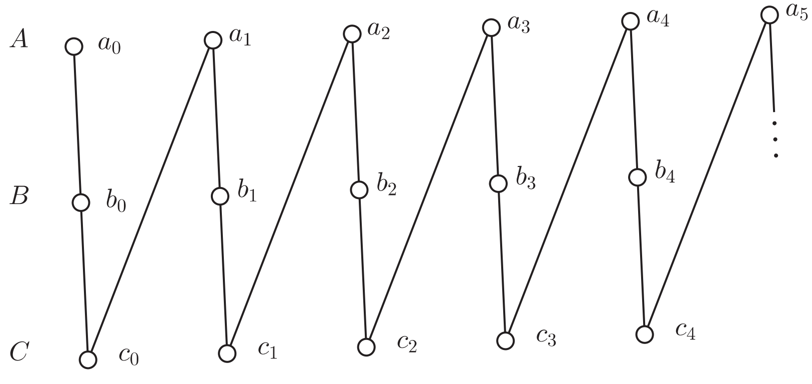
Ένα σύνολο είναι **άπειρο** αν δεν είναι πεπερασμένο. Για παράδειγμα, το σύνολο **N** των φυσικών είναι άπειρο. Το ίδιο και το σύνολο των ακεραίων, των πραγματικών και το σύνολο των τέλειων τετραγώνων. Ωστόσο, *δεν είναι όλα τα άπειρα σύνολα ισάριθμα.*

Ένα σύνολο λέγεται **μετρήσιμα άπειρο** αν είναι ισάριθμο του **N**, και **μετρήσιμο** αν είναι πεπερασμένο ή μετρήσιμα άπειρο. Ένα σύνολο που δεν είναι μετρήσιμο είναι **μη μετρήσιμο**. Για να δείξουμε ότι ένα σύνολο A είναι μετρήσιμα άπειρο πρέπει να παρουσιάσουμε μία αμφιμονοσήμαντη αντιστοιχία ανάμεσα στο A και το **N**· ισοδύναμα, αρκεί να προτείνουμε έναν τρόπο με τον οποίο το A να μπορεί να απαριθμηθεί ως

$$A = \{a_0, a_1, a_2, \ldots\},$$

κ.ο.κ, καθώς μία τέτοια απαρίθμηση συνεπάγεται αυτόματα μία αμφιμονοσήμαντη αντιστοιχία – απλά πάρτε $f(0) = a_0, f(1) = a_1, \ldots$.

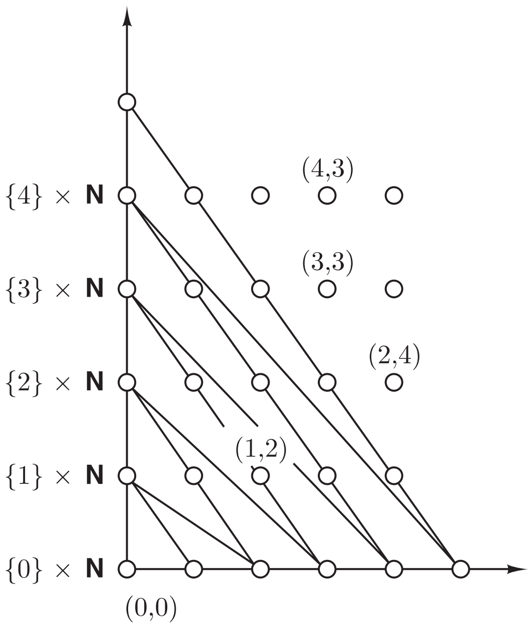
Για παράδειγμα, μπορούμε να αποδείξουμε ότι η ένωση μετρήσιμα άπειρων συνόλων πεπερασμένου αριθμού είναι μετρήσιμα άπειρο σύνολο. Ας εξηγήσουμε την απόδειξη μόνο για τρία, ανά δύο ξένα μεταξύ τους, μετρήσιμα άπειρα σύνολα· παρόμοια είναι η απόδειξη και στη γενική περίπτωση. Έστω τα σύνολα A, B και C. Τα σύνολα μπορούν να παρατεθούν όπως παραπάνω: $A = \{a_0, a_1, \ldots\}$, $B = \{b_0, b_1, \ldots\}$, $C = \{c_0, c_1, \ldots\}$. Τότε η ένωσή τους μπορεί να παρατεθεί ως $A \cup B \cup C = \{a_0, b_0, c_0, a_1, b_1, c_1, a_2 \ldots\}$. Η παράθεση αυτή προσομοιάζει με έναν τρόπο «επίσκεψης» όλων των στοιχείων του $A \cup B \cup C$ κατά την οποία εναλλασσόμαστε ανάμεσα σε διαφορετικά σύνολα, όπως στο Σχήμα 1-7. Αυτή η τεχνική εναλλαγής της απαρίθμησης πολλών συνόλων ονομάζεται «μέθοδος ουράς περιστεριού» (dovetailing), όρος που καθιερώθηκε για αντίστοιχα σχήματα από ξυλουργούς.



Σχήμα 1-7

Η ίδια ιδέα μπορεί να χρησιμοποιηθεί για να δείξουμε ότι η ένωση μιας μετρήσιμα άπειρης συλλογής μετρήσιμα άπειρων συνόλων, είναι μετρήσιμα άπειρο σύνολο. Για παράδειγμα, ας δείξουμε ότι $\mathbf{N} \times \mathbf{N}$ είναι μετρήσιμα άπειρο σύνολο· σημειώστε ότι $\mathbf{N} \times \mathbf{N}$ είναι η ένωση των $\{0\} \times \mathbf{N}$, $\{1\} \times \mathbf{N}$, $\{2\} \times \mathbf{N}$, κ.ο.κ, δηλαδή η ένωση μιας μετρήσιμα άπειρης συλλογής μετρήσιμα άπειρων συνόλων. Εδώ η εφαρμογή της μεθόδου ουράς περιστεριού θα πρέπει να είναι πιο πολύπλοκη από ό,τι στο παραπάνω παράδειγμα: δεν μπορούμε, όπως κάναμε πριν, να επισκεφτούμε ένα στοιχείο από κάθε σύνολο πριν από το δεύτερο στοιχείο του πρώτου συνόλου, διότι εφόσον πρέπει να επισκεφτούμε άπειρο πλήθος συνόλων, δεν θα μπορούσαμε να ολοκληρώσουμε ούτε τον πρώτο γύρο! Αντί γι' αυτό, προχωρούμε ως ακολούθως (βλέπε Σχήμα 1-8).

(1) Στον πρώτο γύρο, επισκεπτόμαστε ένα στοιχείο από το πρώτο σύνολο: $(0, 0)$.
(2) Στο δεύτερο γύρο, επισκεπτόμαστε το επόμενο στοιχείο του πρώτου συνόλου, $(0, 1)$, και επίσης το πρώτο στοιχείο του δεύτερου συνόλου, $(1, 0)$.
(3) Στον τρίτο γύρο, επισκεπτόμαστε το επόμενο στοιχείο του πρώτου και



Σχήμα 1-8

δεύτερου συνόλου, που δεν έχουμε ήδη επισκεφτεί, $(0, 2)$ και $(1, 1)$, καθώς επίσης και το πρώτο στοιχείο του τρίτου συνόλου, $(2, 0)$.

(4) Γενικά, στο n-οστό γύρο, επισκεπτόμαστε το n-οστό στοιχείο του πρώτου συνόλου, το $(n-1)$-οστό στοιχείο του δεύτερου συνόλου και το πρώτο στοιχείο του n-οστού συνόλου.

Ένας άλλος τρόπος θεώρησης της χρήσης της μεθόδου ουράς περιστεριού είναι να παρατηρήσουμε ότι θα επισκεφτούμε το ζεύγος (i, j) μετά από m επισκέψεις, όπου $m = \frac{1}{2}[(i+j)^2 + 3i + j]$· δηλαδή, η συνάρτηση $f(i, j) = \frac{1}{2}[(i+j)^2 + 3i + j]$ είναι *αμφιμονοσήμαντη αντιστοιχία* από το $\mathbf{N} \times \mathbf{N}$ στο $\mathbf{N}$ (βλέπε Πρόβλημα 1.4.4).

Στο τέλος της επόμενης ενότητας θα παρουσιάσουμε μια τεχνική για να δείχνουμε ότι δύο άπειρα σύνολα *δεν* είναι ισάριθμα.

Προβλήματα για την Ενότητα 1.4

1.4.1. Να αποδείξετε ότι τα παρακάτω είναι μετρήσιμα.

(α) Η ένωση τριών μετρήσιμων συνόλων, όχι υποχρεωτικά απείρων ή ξένων μεταξύ τους.

(β) Το σύνολο όλων των πεπερασμένων υποσυνόλων του $\mathbf{N}$.

1.4.2. Να δώσετε ακριβείς αμφιμονοσήμαντες αντιστοιχίες ανάμεσα στο καθένα από τα παρακάτω ζεύγη.

(α) $\mathbf{N}$ και οι περιττοί φυσικοί αριθμοί.

(β) $\mathbf{N}$ και το σύνολο όλων των ακεραίων.

(γ) $\mathbf{N}$ και $\mathbf{N} \times \mathbf{N} \times \mathbf{N}$.

(Ζητάμε τύπους που είναι οι απλούστεροι δυνατοί και περιέχουν μόνο τέτοιες πράξεις όπως η πρόσθεση και ο πολλαπλασιασμός.)

1.4.3. Έστω C ένα σύνολο συνόλων ορισμένο ως εξής:

1. $\emptyset \in C$
2. Αν $S_1 \in C$ και $S_2 \in C$, τότε $\{S_1, S_2\} \in C$.
3. Αν $S_1 \in C$ και $S_2 \in C$, τότε $S_1 \times S_2 \in C$.
4. Τίποτε άλλο, εκτός αυτών που προκύπτουν από τα (1), (2) και (3), δεν ανήκει στο C.

(α) Να εξηγήσετε προσεκτικά γιατί από τα (1) έως (4) συνεπάγεται ότι $\{\emptyset, \{\emptyset\}\} \in C$.

(β) Να δώσετε ένα παράδειγμα ενός συνόλου διατεταγμένων ζευγών S, τέτοιο ώστε $S \in C$ και $|S| > 1$.

(γ) Περιέχει το C άπειρα σύνολα; Να εξηγήσετε.

(δ) Είναι το C μετρήσιμο ή μη μετρήσιμο; Να εξηγήσετε.

1.4.4. Να δείξετε ότι η μέθοδος ουράς περιστεριού του Σχήματος 1-8 επισκέπτεται κάθε ζεύγος (i, j) στο m-οστό γύρο, όπου

$$m = \frac{1}{2}[(i+j)^2 + 3i + j].$$

1.5 ΤΡΕΙΣ ΘΕΜΕΛΙΩΔΕΙΣ ΤΕΧΝΙΚΕΣ ΑΠΟΔΕΙΞΗΣ

Κάθε απόδειξη είναι διαφορετική καθώς σχεδιάζεται για να στηρίξει ένα διαφορετικό αποτέλεσμα. Ωστόσο, σε παιχνίδια όπως το σκάκι ή το μπέιζμπολ, με παρατήρηση πολλών παρτίδων, καταλήγει κανείς στο συμπέρασμα ότι υπάρχουν μοτίβα, τεχνικές και τεχνάσματα που μπορούν να ανακαλυφθούν και να χρησιμοποιηθούν κατ' επανάληψη. Ο κύριος σκοπός της ενότητας αυτής είναι να εισάγει τρεις θεμελιώδεις αρχές που επαναλαμβάνονται με διάφορους τρόπους σε πολλές αποδείξεις: η *μαθηματική επαγωγή*, η *αρχή του περιστεριώνα*, και η *διαγωνιοποίηση*.

Αρχή της Μαθηματικής Επαγωγής: *Έστω ένα σύνολο A φυσικών αριθμών τέτοιο ώστε*

(1) $0 \in A$ και

(2) για κάθε φυσικό αριθμό n, αν $\{0, 1, \ldots, n\} \subseteq A$, τότε $n + 1 \in A$.

Τότε $A = \mathbf{N}$.

Λιγότερο αυστηρά, η αρχή της μαθηματικής επαγωγής δηλώνει ότι κάθε σύνολο φυσικών αριθμών που περιέχει το μηδέν και έχει την ιδιότητα να περιέχει το $n + 1$, αν περιέχει όλους τους αριθμούς μέχρι και το n, πρέπει να είναι στην πραγματικότητα το σύνολο όλων των φυσικών αριθμών.

Η αιτιολόγηση της αρχής αυτής θα πρέπει να είναι σαφής διαισθητικά· κάθε φυσικός αριθμός πρέπει να ανήκει στο A, αφού μπορούμε να τον «φτάσουμε» αν ξεκινήσουμε από το μηδέν με πεπερασμένη ακολουθία βημάτων, προσθέτοντας κάθε φορά τη μονάδα. Το ίδιο αποδεικνύεται με αναγωγή σε άτοπο: ας υποθέσουμε ότι ισχύουν τα (1) και (2), αλλά $A \neq \mathbf{N}$. Τότε κάποιος αριθμός λείπει από το A. Πιο συγκεκριμένα, έστω n ο πρώτος αριθμός ανάμεσα στους $0, 1, 2, \ldots$, που λείπει από το $\mathbf{N}$.[3] Τότε ο n δεν μπορεί να είναι το μηδέν, καθώς $0 \in A$ λόγω της (1)· και εφόσον $0, 1, \ldots, n-1 \subseteq A$ λόγω επιλογής του n, τότε $n \in A$ λόγω της (2), που είναι άτοπο.

Στην πράξη, η επαγωγή χρησιμοποιείται για να αποδείξει συμπεράσματα του τύπου: «Για κάθε φυσικό αριθμό n ισχύει η ιδιότητα P». Η παραπάνω αρχή εφαρμόζεται στο σύνολο $A = \{n : P \text{ αληθής για } n\}$ με τον παρακάτω τρόπο.

1. Στο *βασικό βήμα* δείχνουμε ότι $0 \in A$, δηλαδή ότι η P ισχύει για το 0.
2. Η *επαγωγική υπόθεση* είναι η υπόθεση ότι για κάποιο καθορισμένο αλλά αυθαίρετο $n \geq 0$, η P ισχύει για κάθε φυσικό αριθμό $0, 1, \ldots, n$.
3. Στο *επαγωγικό βήμα* δείχνουμε, με χρήση της επαγωγικής υπόθεσης ότι η P ισχύει και για $n+1$. Τότε, σύμφωνα με την αρχή της επαγωγής, το A ισούται με το $\mathbf{N}$, δηλαδή η P ισχύει για κάθε φυσικό αριθμό.

Παράδειγμα 1.5.1: Ας δείξουμε ότι για κάθε $n \geq 0$, $1 + 2 + \cdots + n = \frac{n^2+n}{2}$.

Βασικό βήμα. Έστω $n = 0$. Τότε το άθροισμα στα αριστερά είναι μηδέν, καθώς δεν υπάρχει τίποτα για να προστεθεί. Η έκφραση στα αριστερά είναι επίσης μηδέν.

Επαγωγική υπόθεση. Υποθέτουμε ότι, για κάποιο $n \geq 0$, $1 + 2 + \cdots + m = \frac{m^2+m}{2}$ όταν $m \leq n$.

---

3. Εδώ χρησιμοποιούμε μία άλλη αρχή, η οποία ονομάζεται *αρχή του ελάχιστου αριθμού*, στην πραγματικότητα ισοδύναμη με την αρχή της μαθηματικής επαγωγής. Επομένως, δεν «αποδεικνύουμε» πραγματικά την αρχή της μαθηματικής επαγωγής. Η αρχή του ελάχιστου αριθμού είναι: Αν $A \subseteq \mathbf{N}$ και $A \neq \mathbf{N}$, τότε υπάρχει ένας μοναδικός ελάχιστος αριθμός $n \in \mathbf{N} - A$. Αυτό σημαίνει ότι υπάρχει ένας μοναδικός αριθμός n τέτοιος ώστε $n \notin A$, αλλά $0, 1, \ldots, n-1 \in A$. Ένα κάπως παράξενο παράδειγμα της αρχής του ελάχιστου αριθμού αποτελεί το γεγονός ότι *δεν υπάρχουν μη ενδιαφέροντες αριθμοί*. Διότι, αν υποθέσουμε ότι υπήρχαν, τότε θα έπρεπε να υπάρχει ένας ελάχιστος τέτοιος αριθμός, έστω n. Τότε όμως το n θα είχε την αξιοσημείωτη ιδιότητα να είναι ο ελάχιστος μη ενδιαφέρων αριθμός, που σίγουρα θα έκανε τον n ενδιαφέροντα…

Επαγωγικό βήμα.

$$
\begin{aligned}
1+2+\cdots+n+(n+1) &= (1+2+\cdots+n)+(n+1) \\
&= \frac{n^2+n}{2}+(n+1) \qquad \text{(λόγω της επαγωγικής υπόθεσης)} \\
&= \frac{n^2+n+2n+2}{2} \\
&= \frac{(n+1)^2+(n+1)}{2}
\end{aligned}
$$

αυτό που είχαμε να δείξουμε. $\diamondsuit$

Παράδειγμα 1.5.2: Για κάθε πεπερασμένο σύνολο A, $|2^A| = 2^{|A|}$· δηλαδή, ο πληθικός αριθμός του δυναμοσυνόλου του A είναι το 2 υψωμένο σε δύναμη ίση με τον πληθικό αριθμό του A. Θα αποδείξουμε την πρόταση αυτή *με επαγωγή στον πληθικό αριθμό του* A.

Βασικό βήμα. Έστω A σύνολο με πληθικό αριθμό $n = 0$. Τότε $A = \emptyset$ και $2^{|A|} = 2^0 = 1$· επίσης, $2^A = \{\emptyset\}$ και $|2^A| = |\{\emptyset\}| = 1$.

Επαγωγική υπόθεση. Έστω ότι $n > 0$, και υποθέτουμε ότι $|2^A| = 2^{|A|}$ υπό την προϋπόθεση ότι $|A| \leq n$.

Επαγωγικό βήμα. Έστω A τέτοιο ώστε $|A| = n + 1$. Αφού $n > 0$, το A περιέχει τουλάχιστον ένα στοιχείο a. Έστω $B = A - \{a\}$· τότε $|B| = n$. Λόγω της επαγωγικής υπόθεσης, $|2^B| = 2^{|B|} = 2^n$. Τώρα το δυναμοσύνολο του A μπορεί να διαιρεθεί σε δύο μέρη: σε εκείνα τα σύνολα που περιέχουν το a και σε εκείνα που δεν περιέχουν το a. Το δεύτερο μέρος είναι απλά το 2^B, και το πρώτο προκύπτει όταν εισάγουμε το a σε κάθε μέλος του 2^B. Έτσι

$$2^A = 2^B \cup \{C \cup \{a\} : C \in 2^B\}.$$

Η διαίρεση αυτή ουσιαστικά διαμερίζει το 2^A σε δύο ξένα μεταξύ τους ισάριθμα μέρη, και έτσι τελικά ο πληθικός αριθμός του όλου συνόλου είναι διπλάσιος του $2^{|B|}$, το οποίο, λόγω της επαγωγικής υπόθεσης, είναι $2 \cdot 2^n = 2^{n+1}$, δηλαδή το ζητούμενο. $\diamondsuit$

Στη συνέχεια θα χρησιμοποιήσουμε την επαγωγή για να στηρίξουμε τη δεύτερη θεμελιώδη αρχή, την *αρχή του περιστεριώνα*.

Αρχή του Περιστεριώνα: *Αν A και B είναι πεπερασμένα σύνολα και $|A| > |B|$, τότε δεν υπάρχει ένα προς ένα συνάρτηση από το A στο B.*

Με άλλα λόγια, αν προσπαθήσουμε να σχηματίσουμε ζεύγη των στοιχείων του A (τα «περιστέρια») με τα στοιχεία του B (τους «περιστεριώνες»), αργά ή γρήγορα θα αναγκαστούμε να τοποθετήσουμε περισσότερα από ένα περιστέρια σε έναν περιστεριώνα.

Απόδειξη:

Βασικό βήμα. Υποθέστε ότι $|B| = 0$, δηλαδή $B = \emptyset$. Τότε δεν υπάρχει συνάρτηση $f : A \mapsto B$ έτσι κι αλλιώς, αλλά ούτε και ένα προς ένα συνάρτηση.
Επαγωγική υπόθεση. Υποθέστε ότι η f δεν είναι ένα προς ένα, αν $f : A \mapsto B$, $|A| > |B|$ και $|B| \leq n$, όπου $n \geq 0$.

Επαγωγικό βήμα. Υποθέστε ότι $f : A \mapsto B$ και $|A| > |B| = n + 1$. Διαλέξτε ένα $a \in A$ (αφού $|A| > |B| = n + 1 \geq 1$, το A είναι μη κενό σύνολο, και επομένως μια τέτοια επιλογή είναι δυνατή). Αν υπάρχει ένα άλλο στοιχείο του A, έστω a', τέτοιο ώστε $f(a) = f(a')$, τότε προφανώς η f δεν είναι ένα προς ένα συνάρτηση, και τελειώσαμε. Υποθέστε, λοιπόν, ότι το a είναι το μόνο στοιχείο που απεικονίζεται από την f στο $f(a)$. Θεωρήστε τότε τα σύνολα $A - \{a\}$, $B - \{f(a)\}$, και τη συνάρτηση g από το $A - \{a\}$ στο $B - \{f(a)\}$ που συμφωνεί με την f για όλα τα στοιχεία του $A - \{a\}$. Τώρα η επαγωγική υπόθεση ισχύει, επειδή το $B - \{f(a)\}$ έχει n στοιχεία, και $|A - \{a\}| = |A| - 1 > |B| - 1 = |B - \{f(a)\}|$. Συνεπώς, υπάρχουν δύο διαφορετικά στοιχεία του $A - \{a\}$ που απεικονίζονται από την g (και συνεπώς και από την f) στο ίδιο στοιχείο του $B - \{b\}$, και άρα η f δεν είναι ένα προς ένα. ■

Το απλό αυτό γεγονός χρησιμοποιείται σε μια εντυπωσιακά μεγάλη ομάδα αποδείξεων. Παρουσιάζουμε μία μόνον απλή εφαρμογή εδώ, αλλά θα δούμε και άλλες περιπτώσεις καθώς εμφανίζονται στα επόμενα κεφάλαια.

Θεώρημα 1.5.1: *Έστω R μία δυαδική σχέση ορισμένη σε ένα πεπερασμένο συνόλο A, και έστω $a, b \in A$. Αν υπάρχει μονοπάτι από το a στο b στην R, τότε υπάρχει μονοπάτι μήκους το πολύ $|A|$.*

Απόδειξη:

Υποθέστε πως $(a_1, a_2, \ldots, a_n)$ είναι το ελάχιστο μονοπάτι από το $a_1 = a$ στο $a_n = b$, δηλαδή το μονοπάτι με το μικρότερο μήκος, και υποθέστε πως $n > |A|$. Σύμφωνα με την αρχή του περιστεριώνα, υπάρχει ένα στοιχείο του A το οποίο επαναλαμβάνεται στο μονοπάτι, έστω $a_i = a_j$ για κάποια i, j τέτοια ώστε $1 \leq i < j \leq n$. Τότε όμως $(a_1, a_2, \ldots, a_i, a_{j+1}, \ldots, a_n)$ είναι ένα μικρότερο μονοπάτι από το a στο b, γεγονός που έρχεται σε αντίφαση με την υπόθεσή μας ότι το $(a_1, a_2, \ldots, a_n)$ είναι το ελάχιστο μονοπάτι από το a στο b. ■

Τέλος, φτάνουμε στην τρίτη βασική τεχνική απόδειξης, την *αρχή της διαγωνιοποίησης* (diagonalization principle). Αν και εμφανίζεται σπανιότερα από την επαγωγή ή την αρχή του περιστεριώνα, είναι ιδιαίτερα χρήσιμη για την απόδειξη συγκεκριμένων σημαντικών αποτελεσμάτων στη θεωρία του υπολογισμού.

Η Αρχή της Διαγωνιοποίησης: *Έστω R μία δυαδική σχέση σε ένα σύνολο A, και έστω D το διαγώνιο σύνολο για την $R, \{a : a \in A$ και $(a, a) \notin R\}$. Για κάθε $a \in A$, έστω $R_a = \{b : b \in A$ και $(a, b) \in R\}$. Τότε το D είναι διαφορετικό από όλα τα R_a.*

Αν το A είναι πεπερασμένο σύνολο, τότε η R μπορεί να απεικονιστεί ως ένας τετραγωνικός πίνακας. Οι γραμμές και οι στήλες επιγράφονται με τα ονόματα των στοιχείων του A και υπάρχει ένας σταυρός στη θέση του πίνακα που αντιστοιχεί στη γραμμή που επιγράφεται με a και στη στήλη που επιγράφεται με b, στην περίπτωση όπου $(a, b) \in R$. Το διαγώνιο σύνολο D αντιστοιχεί στο συμπλήρωμα της ακολουθίας των θέσεων κατά μήκος της κύριας διαγωνίου που προκύπτει αν εναλλάξουμε τις θέσεις του πίνακα με σταυρούς σε θέσεις χωρίς σταυρούς, και αντίστροφα. Τα σύνολα R_a αντιστοιχούν στις γραμμές του πίνακα. Η αρχή της διαγωνιοποίησης μπορεί τότε να διατυπωθεί διαφορετικά: το συμπλήρωμα της διαγωνίου διαφέρει από κάθε σειρά.

Παράδειγμα 1.5.3: Ας εξετάσουμε τη σχέση $R = \{(a, b), (a, d), (b, b), (b, c), (c, c), (d, b), (d, c), (d, e), (d, f), (e, e), (e, f), (f, a), (f, c), (f, d), (f, e)\}$· Παρατηρήστε ότι $R_a = \{b, d\}$, $R_b = \{b, c\}$, $R_c = \{c\}$, $R_d = \{b, c, e, f\}$, $R_e = \{e, f\}$ και $R_f = \{a, c, d, e\}$. Η R μπορεί να απεικονιστεί ως εξής:

	a	b	c	d	e	f
a		×		×		
b		×	×			
c			×			
d		×	×		×	×
e					×	×
f	×		×	×	×	

Η ακολουθία των θέσεων κατά μήκος της διαγωνίου είναι

	×	×		×	

Το συμπλήρωμά της είναι

×			×		×

που αντιστοιχεί στο διαγώνιο σύνολο $D = \{a, d, f\}$. Πράγματι, το D διαφέρει από κάθε γραμμή του πίνακα· εξαιτίας του τρόπου κατασκευής του, διαφέρει από την πρώτη γραμμή στην πρώτη θέση, από τη δεύτερη γραμμή στη δεύτερη θέση, κ.ο.κ. $\diamondsuit$

Η αρχή της διαγωνιοποίησης ισχύει επίσης και για τα άπειρα σύνολα, για παρόμοιους λόγους: Το διαγώνιο σύνολο D πάντα διαφέρει από το σύνολο R_a ως προς την ερώτηση εάν περιέχει το a, και άρα δεν μπορεί να ταυτίζεται με το R_a για κανένα a.

Παρουσιάζουμε τη χρήση της διαγωνιοποίησης με ένα κλασικό θεώρημα του Georg Cantor (1845-1918).

Θεώρημα 1.5.2: *Το σύνολο $2^{\mathbf{N}}$ είναι μη μετρήσιμο.*

Απόδειξη:

Θεωρήστε ότι το $2^{\mathbf{N}}$ είναι μετρήσιμα άπειρο. Δηλαδή υποθέτουμε ότι υπάρχει τρόπος να απαριθμηθούν τα στοιχεία του $2^{\mathbf{N}}$ ως

$$2^{\mathbf{N}} = \{R_0, R_1, R_2, \ldots\}$$

(προσέξτε ότι αυτά είναι τα σύνολα R_a στη διατύπωση της αρχής της διαγωνοποίησης, από τη στιγμή που θεωρούμε τη σχέση $R = \{(i,j) : j \in R_i\}$). Τώρα θεωρήστε το σύνολο

$$D = \{n \in \mathbf{N} : n \notin R_n\}$$

(αυτό είναι το διαγώνιο σύνολο). Το D είναι ένα σύνολο φυσικών αριθμών, και συνεπώς θα έπρεπε να εμφανίζεται κάπου στην απαρίθμηση $\{R_0, R_1, R_2, \ldots\}$. Το D, όμως, δεν μπορεί να είναι το R_0, επειδή διαφέρει από αυτό στο ότι περιέχει το 0 (το περιέχει αν και μόνον αν το R_0 δεν το περιέχει)· και δεν μπορεί να είναι το R_1, επειδή διαφέρει από αυτό στο ότι περιέχει το 1, κ.ο.κ. Θα πρέπει να συμπεράνουμε, λοιπόν, ότι το D δεν εμφανίζεται καθόλου στην απαρίθμηση, και αυτό είναι άτοπο.

Για να διατυπώσουμε το επιχείρημα αυτό λίγο πιο αυστηρά, θεωρήστε ότι $D = R_k$ για κάποιο $k \geq 0$ (εφόσον το D είναι σύνολο φυσικών αριθμών, και θεωρήσαμε ότι $\{R_0, R_1, R_2, \ldots\}$ είναι μία πλήρης απαρίθμηση όλων των συνόλων αυτού του τύπου, ένα τέτοιο k πρέπει να υπάρχει). Καταλήγουμε σε άτοπο εξετάζοντας εάν $k \in R_k$:

(α) Έστω ότι η απάντηση είναι ναι, $k \in R_k$. Εφόσον $D = \{n \in \mathbf{N} : n \notin R_n\}$, προκύπτει ότι $k \notin D$· όμως $D = R_k$, πράγμα άτοπο.
(β) Έστω ότι η απάντηση είναι όχι, $k \notin R_k$· τότε $k \in D$. Όμως $D = R_k$, οπότε $k \in R_k$, που είναι επίσης άτοπο.

Φτάσαμε σε άτοπο ενώ ξεκινήσαμε από την υπόθεση ότι το $2^{\mathbf{N}}$ είναι μετρήσιμα άπειρο, και συνεχίσαμε κατά τα άλλα με άμεμπτα αυστηρή μαθηματική λογική· θα πρέπει, λοιπόν, να συμπεράνουμε ότι η υπόθεση αυτή είναι λανθασμένη. Άρα το $2^{\mathbf{N}}$ είναι μη μετρήσιμο. ■

Για μια διαφορετική εκδοχή της απόδειξης αυτής, στην περίπτωση που το σύνολο των πραγματικών αριθμών στο διάστημα $[0,1]$ είναι μη μετρήσιμο, δείτε το Πρόβλημα 1.5.11.

Προβλήματα για την Ενότητα 1.5

1.5.1. Να δείξετε με επαγωγή ότι

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n \cdot (n+1) \cdot (n+2) =$$

$$= \frac{n \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4}.$$

1.5.2. Να δείξετε με επαγωγή ότι το $n^4 - 4n^2$ διαιρείται ακριβώς με το 3 για κάθε $n \geq 0$.

1.5.3. Πού βρίσκεται το λάθος στην παρακάτω επαγωγική απόδειξη ότι όλα τα άλογα έχουν το ίδιο χρώμα;
Απόδειξη με επαγωγή στον αριθμό των αλόγων:
Βασικό βήμα. Υπάρχει ένα μόνον άλογο. Τότε προφανώς όλα τα άλογα έχουν το ίδιο χρώμα.
Επαγωγική υπόθεση. Σε κάθε σύνολο μέχρι και n αλόγων, όλα έχουν το ίδιο χρώμα.
Επαγωγικό βήμα. Θεωρήστε ένα σύνολο $n+1$ αλόγων. Αφαιρούμε ένα άλογο. Λόγω της επαγωγικής υπόθεσης, όλα τα υπόλοιπα άλογα έχουν το ίδιο χρώμα. Τώρα προσθέτουμε το άλογο που είχαμε αφαιρέσει και αφαιρούμε ένα άλλο· πάλι όλα τα άλογα έχουν το ίδιο χρώμα. Έτσι όλα τα άλογα έχουν το ίδιο χρώμα με αυτά που δεν είχαν αφαιρεθεί και τις δύο φορές, και έτσι όλα έχουν το ίδιο χρώμα.

1.5.4. Να δείξετε ότι, αν τα A και B είναι πεπερασμένα σύνολα, τότε υπάρχουν $|B|^{|A|}$ συναρτήσεις από το A στο B.

1.5.5. Να αποδείξετε με επαγωγή: Κάθε μερική διάταξη σε ένα μη κενό πεπερασμένο σύνολο έχει τουλάχιστον ένα ελάχιστο στοιχείο. Θα ήταν η πρόταση αυτή αληθής, χωρίς την προϋπόθεση ότι το σύνολο είναι πεπερασμένο;

1.5.6. Να δείξετε ότι σε κάθε σύνολο ανθρώπων υπάρχουν τουλάχιστον δύο που έχουν τον ίδιο αριθμό γνωριμιών μέσα στο σύνολο. (Χρησιμοποιήστε την αρχή του περιστεριώνα).

1.5.7. Υποθέστε ότι προσπαθούμε να αποδείξουμε, με ένα επιχείρημα ανάλογο με την απόδειξη του Θεωρήματος 1.5.2, ότι το σύνολο όλων των πεπερασμένων υποσυνόλων του **N** είναι μη μετρήσιμο. Πού βρίσκεται το λάθος;

1.5.8. Να δώσετε παραδείγματα για να δείξετε ότι η τομή δύο μετρήσιμα άπειρων συνόλων μπορεί να είναι είτε πεπερασμένη είτε μετρήσιμα άπειρη, και ότι η τομή δύο μη μετρήσιμα άπειρων συνόλων μπορεί να είναι είτε πεπερασμένη είτε μετρήσιμα άπειρη ή μη μετρήσιμη.

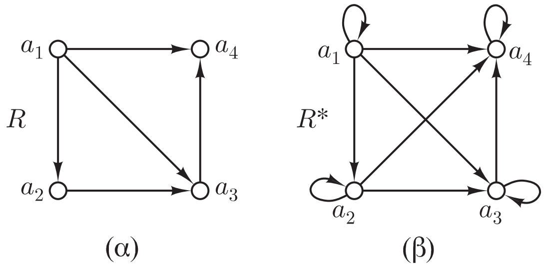
1.5.9. Να δείξετε ότι η διαφορά ενός μετρήσιμου συνόλου από ένα μη μετρήσιμο είναι μη μετρήσιμο σύνολο.

1.5.10. Να δείξετε ότι αν το S είναι ένα οποιοδήποτε σύνολο, τότε υπάρχει ένα προς ένα συνάρτηση από το S στο 2^S, αλλά όχι αντίστροφα.

1.5.11. Να αποδείξετε ότι το σύνολο όλων των πραγματικών αριθμών στο διάστημα $[0, 1]$ είναι μη μετρήσημο. (*Υπόδειξη:* Είναι γνωστό ότι κάθε τέτοιος αριθμός μπορεί να γραφτεί στο δυαδικό σύστημα ως μία άπειρη ακολουθία από 0 και 1 – όπως η 0,0110011100000…. Υποθέστε ότι υπάρχει απαρίθμηση των ακολουθιών αυτών και δημιουργήστε μια «διαγώνια» ακολουθία, «στρίβοντας» το i-οστό διφίο (bit) της i-οστής ακολουθίας.)

1.6 ΚΛΕΙΣΤΟΤΗΤΑ ΚΑΙ ΑΛΓΟΡΙΘΜΟΙ

Θεωρήστε τα δύο κατευθυνόμενα γραφήματα R και R^* στο Σχήμα 1-9(α) και (β). Το R^* περιέχει το R· επίσης, το R^* είναι ανακλαστικό και μεταβατικό (ενώ το R δεν είναι τίποτε από τα δύο). Στην πραγματικότητα, είναι εύκολο να δει κανείς ότι το R^* είναι το *μικρότερο δυνατό κατευθυνόμενο γράφημα* που έχει τις ιδιότητες αυτές – δηλαδή, περιέχει το R, είναι ανακλαστικό, και είναι μεταβατικό (με το χαρακτηρισμό «μικρότερο» εννοούμε αυτό με τις λιγότερες ακμές). Για το λόγο αυτό, το R^* ονομάζεται η *ανακλαστική μεταβατική κλειστότητα του* R. Στη συνέχεια ορίζουμε τη χρήσιμη αυτή έννοια αυστηρά:



Σχήμα 1-9

Ορισμός 1.6.1: Έστω $R \subseteq A^2$ το κατευθυνόμενο γράφημα ορισμένο σε ένα σύνολο A. Η **ανακλαστική μεταβατική κλειστότητα** του R είναι η σχέση

$$R^* = \{(a, b) : a, b \in A \text{ και υπάρχει μονοπάτι από το } a \text{ στο } b \text{ στο } R.\}$$

Προσέξτε την ενδιαφέρουσα αντίθεση μεταξύ του ορισμού «από κάτω», που δομήθηκε στον Ορισμό 1.6.1, και τον άτυπο ορισμό «από πάνω» μέσω του οποίου εισαγάγαμε την ανακλαστική μεταβατική κλειστότητα (τη μικρότερη σχέση που περιέχει το R και είναι ανακλαστική και μεταβατική). Είναι ίσως διαισθητικά σαφές ότι οι δύο ορισμοί είναι ισοδύναμοι. Προς το τέλος της ενότητας αυτής θα μελετήσουμε πιο λεπτομερώς τέτοιους «ορισμούς από πάνω», και το λόγο για τον οποίο πάντα αντιστοιχούν σε έναν εναλλακτικό ορισμό «από κάτω.»

Αλγόριθμοι

Από τον Ορισμό 1.6.1 προκύπτει άμεσα ένας *αλγόριθμος* για τον *υπολογισμό* της ανακλαστικής μεταβατικής κλειστότητας της R^* για κάθε δεδομένη δυαδική σχέση R ως προς ένα πεπερασμένο σύνολο $A = \{a_1, a_2, \ldots, a_n\}$:

Αρχικά $R^* := \emptyset$
for $i = 1, \ldots, n$ do
  για κάθε i*-άδα* $(b_1, \ldots, b_i) \in A^i$ do
  if $(b_1, \ldots, b_i)$ *είναι ένα μονοπάτι στην* R then *πρόσθεσε* (b_1, b_i)
  στην R^*.

Η αυστηρή μελέτη των αλγορίθμων θα μπορούσε να θεωρηθεί το βασικό αντικείμενο του βιβλίου αυτού. Αν όμως δίναμε έναν αυστηρό ορισμό ενός αλγορίθμου στο σημείο αυτό, θα χαλούσε η όμορφη ιστορία που έχουμε να διηγηθούμε. Μέχρι να εισάγουμε ένα αυστηρό γενικό μοντέλο για την περιγραφή αλγορίθμων, θα αντιμετωπίζουμε τους αλγόριθμους άτυπα και κατά κάποιο τρόπο μη σχολαστικά, ενώ θα αυξάνουμε σταδιακά την αντίληψη και την εξοικείωσή μας. Θα γίνει τότε σαφές ότι ο ορισμός μας για τον αλγόριθμο, όταν έρθει η κατάλληλη στιγμή για την παρουσίασή του, πράγματι εκφράζει σωστά τη σημαντική αυτή έννοια. Έτσι, λοιπόν, η ενότητα αυτή περιέχει μόνο μία διαισθητική προσέγγιση των αλγορίθμων και μία άτυπη εισαγωγή στην ανάλυσή τους.

Ευτυχώς, είναι εύκολο να διακρίνει κανείς έναν αλγόριθμο όταν τον συναντήσει. Η διαδικασία που περιγράφηκε παραπάνω για τον υπολογισμό της R^* είναι μια λεπτομερής και σαφής ακολουθία οδηγιών που παράγει ένα αποτέλεσμα – αυτό που αποκαλούμε R^*. Αποτελείται από στοιχειώδη βήματα, τα οποία μπορούμε λογικά να υποθέσουμε ότι είναι εύκολο να πραγματοποιηθούν: Θέτουμε αρχικά την R^* στο $\emptyset$, προσθέτουμε νέα στοιχεία στην R^*, ελέγχουμε εάν $(b_j, b_{j+1}) \in R$ – αυτό το τελευταίο πρέπει να γίνει $i-1$ φορές στην τελευταία γραμμή του αλγορίθμου για να ελέγξουμε εάν το $(b_1, \ldots, b_i)$ είναι μονοπάτι της R. Θεωρούμε ότι με κάποιο τρόπο ο αλγόριθμος αυτός ενεργεί σε στοιχεία του A και της R άμεσα, και έτσι δεν χρειάζεται να προσδιορίσουμε πώς τέτοια σύνολα και σχέσεις *αναπαριστώνται*, ώστε να τα χειριστεί ο αλγόριθμος.

Στη συνέχεια θα επιχειρηματολογήσουμε ότι η σχέση R^*, που υπολογίζει ο αλγόριθμος αυτός, είναι πραγματικά η ανακλαστική μεταβατική κλειστότητα της R (δηλαδή, ο αλγόριθμος είναι *ορθός*). Ο λόγος είναι ότι ο αλγόριθμός μας είναι απλώς μια απευθείας *υλοποίηση* του Ορισμού 1.6.1. Προσθέτει στην R^*, η οποία αρχικά είναι κενή, όλα τα ζεύγη στοιχείων του A που συνδέονται μέσω ενός μονοπατιού της R. Τα πιθανά μονοπάτια ελέγχονται ένα προς ένα, σε αύξουσα σειρά μήκους. Σταματάμε σε ακολουθίες μήκους n γιατί, σύμφωνα με το Θεώρημα 1.5.1, αν δύο κόμβοι του A συνδέονται μέσω ενός μονοπατιού, τότε υπάρχει μονοπάτι μήκους n ή μικρότερου που τους συνδέει.

Είναι, λοιπόν, προφανές ότι ο αλγόριθμός μας θα τερματίσει κάποτε με τη σωστή απάντηση. Μία ερώτηση που θα αποδειχθεί ιδιαίτερα σημαντική και σχετική με τα θέματα που μας απασχολούν στο βιβλίο αυτό είναι: *μετά από πόσα βήματα θα τερματίσει;* Στο τελευταίο τμήμα του βιβλίου θα αναπτύξουμε μια ολόκληρη θεωρία για το πώς υπολογίζεται η απάντηση σε τέτοια ερωτήματα, και πότε το αποτέλεσμα θεωρείται ικανοποιητικό. Ας συνεχίσουμε, όμως, άτυπα προς το παρόν.

Αυτό που χρειαζόμαστε είναι μία ένδειξη για το πόσα βασικά βήματα, πόσο «χρόνο», απαιτεί ο αλγόριθμος όταν του δίνεται η σχέση R ως είσοδος. Είναι λογικό να περιμένει κανείς ότι ο αλγόριθμος θα χρειαστεί περισσότερο χρόνο για σχέσεις εισόδου με μεγαλύτερο μεγέθος, και όντως η απάντηση εξαρτάται από το πόσο μεγάλη είναι η σχέση εισόδου – πιο συγκεκριμένα, από τον αριθμό n των στοιχείων του συνόλου A. Έτσι, αναζητούμε μια συνάρτηση $f: \mathbf{N} \mapsto \mathbf{N}$, τέτοια ώστε, για κάθε $n \geq 1$, αν στον αλγόριθμο δίνεται ως είσοδος μια δυαδική σχέση $R \subseteq A \times A$ με $|A| = n$, θα τερματίσει μετά από το πολύ $f(n)$ βήματα. Είναι τυπικό στην ανάλυση αλγορίθμων να επιτρέπουμε η $f(n)$ να είναι μια πρόχειρη υπερεκτίμηση, αρκεί να έχει το σωστό *ρυθμό αύξησης*. Οι ρυθμοί αύξησης είναι, λοιπόν, το επόμενο θέμα μας.

Ρυθμός αύξησης συναρτήσεων

Ποια από τις τρεις αυτές συναρτήσεις από το συνόλο των φυσικών συναρτήσεων στον εαυτό του είναι η μεγαλύτερη;

$$f(n) = 1.000.000 \cdot n^{\cdot} \quad g(n) = 10 \cdot n^{3\cdot} \quad h(n) = 2^n$$

Αν και για μικρές τιμές του n ισχύει ότι $f(n) > g(n) > h(n)$, θα πρέπει να είναι διαισθητικά σαφές ότι η σωστή κατάταξη είναι η ακριβώς αντίθετη. Για *αρκετά μεγάλα* n θα έχουμε τελικά $f(n) < g(n) < h(n)$. Στην υποενότητα αυτή θα αναπτύξουμε τις κατάλληλες έννοιες για την κατάταξη τέτοιων συναρτήσεων ανάλογα με τη μέγιστη δυνατότητά τους για παραγωγή μεγάλων τιμών.

Ορισμός 1.6.2:
Έστω $f: \mathbf{N} \mapsto \mathbf{N}$ μία συνάρτηση από τους φυσικούς αριθμούς στους φυσικούς αριθμούς. Η **τάξη της** f, συμβολίζεται $\mathcal{O}(f)$, είναι το σύνολο όλων των συναρτήσεων $g: \mathbf{N} \mapsto \mathbf{N}$ με την ιδιότητα ότι υπάρχουν θετικοί φυσικοί αριθμοί $c > 0$ και $d > 0$ τέτοιοι ώστε, για κάθε $n \in \mathbf{N}$, $g(n) \leq c \cdot f(n) + d$. Αν στην πραγματικότητα η ανισότητα αυτή ισχύει για όλα τα n, λέμε ότι $g(n) \in \mathcal{O}(f(n))$ **με σταθερές** c **και** d.

Αν για δύο συναρτήσεις $f, g: \mathbf{N} \mapsto \mathbf{N}$ ισχύει ότι $f \in \mathcal{O}(g)$ και $g \in \mathcal{O}(f)$, τότε γράφουμε $f \asymp g$. Είναι φανερό ότι η σχέση $\asymp$ ορισμένη για συναρτήσεις είναι σχέση ισοδυναμίας: Είναι ανακλαστική (επειδή πάντα $f \in \mathcal{O}(f)$, με σταθερές 1 και 0) και είναι συμμετρική (επειδή οι ρόλοι των f και g είναι δυνατόν να αντιμετατεθούν στον ορισμό του $\asymp$). Τέλος, είναι μεταβατική. Γιατί υποθέστε ότι $f \in \mathcal{O}(g)$ με σταθερές c, d, και $g \in \mathcal{O}(h)$ με σταθερές c', d'. Τότε για όλα τα n,

$$f(n) \leq c \cdot g(n) + d \leq c \cdot (c' \cdot h(n) + d') + d = (c \cdot c')h(n) + (d + c \cdot d').$$

Συνεπώς, $f \in \mathcal{O}(h)$ με σταθερές $c \cdot c'$ και $d + c \cdot d'$.

Συνεπώς, όλες οι συναρτήσεις από το σύνολο των φυσικών αριθμών στον εαυτό του ομαδοποιούνται μέσω της $\asymp$ σε κλάσεις ισοδυναμίας. Η κλάση ισοδυναμίας της f ως προς την $\asymp$ ονομάζεται **ρυθμός αύξησης** της f.

Παράδειγμα 1.6.1: Θεωρήστε το *πολυώνυμο* $f(n) = 31n^2 + 17n + 3$. Ισχυριζόμαστε ότι $f(n) \in \mathcal{O}(n^2)$. Για να το δείτε, παρατηρήστε ότι $n^2 \geq n$, και έτσι $f(n) \leq 48n^2 + 3$, και επομένως $f(n) \in \mathcal{O}(n^2)$ με σταθερές 48 και 3. Φυσικά, επίσης $n^2 \in \mathcal{O}(f(n))$ –με σταθερές 1 και 0. Άρα $n^2 \asymp 31n^2 + 17n + 3$, και οι δύο συναρτήσεις έχουν τον ίδιο ρυθμό αύξησης.

Ομοίως, για κάθε πολυώνυμο βαθμού d με μη αρνητικούς συντελεστές

$$f(n) = a_d n^d + a_{d-1} n^{d-1} + \cdots + a_1 n + a_0$$

όπου $a_i \geq 0$ για κάθε i, και $a_d > 0$, είναι εύκολο να αποδείξουμε ότι $f(n) \in \mathcal{O}(n^d)$ – με σταθερές $\sum_{i=1}^{d} a_i$ και a_0. *Όλα τα πολυώνυμα του ίδιου βαθμού έχουν τον ίδιο ρυθμό αύξησης.*

Θεωρήστε, λοιπόν, δύο πολυώνυμα με διαφορετικούς βαθμούς· έχουν επίσης τον ίδιο ρυθμό αύξησης; Η απάντηση εδώ είναι αρνητική. Εφόσον όλα τα πολυώνυμα με τον ίδιο βαθμό έχουν τον ίδιο ρυθμό αύξησης, αρκεί να εξετάσουμε τους δύο πιο απλούς αντιπροσώπους, δηλαδή δύο πολυώνυμα της μορφής n^i και n^j, με $0 < i < j$. Προφανώς, $n^i \in \mathcal{O}(n^j)$ με σταθερές 1 και 0. Θα αποδείξουμε ότι $n^j \notin \mathcal{O}(n^i)$.

Ας θεωρήσουμε, λοιπόν, ότι πράγματι $n^j \in \mathcal{O}(n^i)$ με σταθερές c και d, με σκοπό να οδηγηθούμε σε άτοπο. Δηλαδή, για κάθε $n \in \mathbf{N}$ $n^j \leq cn^i + d$. Είναι εύκολο, όμως, να δείξουμε ότι αυτό είναι παράλογο αν δοκιμάσουμε $n = c + d$:

$$c(c+d)^i + d < (c+d)^{i+1} \leq (c+d)^j.$$

Ανακεφαλαιώνοντας, αν οποιαδήποτε δύο πολυώνυμα f και g έχουν τον ίδιο βαθμό, τότε $f \asymp g$. Διαφορετικά, αν το g έχει μεγαλύτερο βαθμό από το f, τότε $f \in \mathcal{O}(g)$ αλλά $g \notin \mathcal{O}(f)$· δηλαδή, *το g έχει μεγαλύτερο ρυθμό αύξησης* από το f. $\diamondsuit$

Παράδειγμα 1.6.2: Από το προηγούμενο παράδειγμα προκύπτει ότι ο ρυθμός αύξησης ενός πολυωνύμου εξαρτάται από το βαθμό του. Όσο μεγαλύτερος ο βαθμός του f, τόσο μεγαλύτερος είναι ο ρυθμός αύξησής του. Υπάρχουν, όμως, συναρτήσεις με ρυθμό αύξησης μεγαλύτερο από αυτόν οποιουδήποτε πολυωνύμου. Ένα απλό παράδειγμα είναι η *εκθετική* συνάρτηση 2^n.

Ας εξασφαλίσουμε αρχικά ότι, για όλα τα $n \in \mathbf{N}$, $n \leq 2^n$. Θα χρησιμοποιήσουμε επαγωγή στο n. Το ζητούμενο ασφαλώς ισχύει για $n = 0$. Υποθέστε, λοιπόν, ότι ισχύει για όλους τους φυσικούς μέχρι και το n. Τότε έχουμε

$$n + 1 \leq 2^n + 1 \leq 2^n + 2^n = 2^{n+1},$$

όπου στην πρώτη ανισότητα χρησιμοποιήσαμε την επαγωγική υπόθεση, και στη δεύτερη χρησιμοποιήσαμε το γεγονός ότι $1 \leq 2^n$ για όλα τα n.

Τώρα θα επεκτείνουμε το προφανές αυτό γεγονός για όλα τα πολυώνυμα. Θα δείξουμε ότι για κάθε $i \geq 1$, $n^i \in \mathcal{O}(2^n)$· δηλαδή,

$$n^i \leq c2^n + d \tag{1}$$

για κατάλληλες σταθερές c και d. Παίρνουμε $c = (2i)^i$ και $d = (i^2)^i$. Υπάρχουν δύο περιπτώσεις: Αν $n \leq i^2$, η ανισότητα ισχύει διότι $n^i \leq d$. Αν αντίθετα $n \geq i^2$, θα δείξουμε ότι η ανισότητα (1) συνεχίζει να ισχύει διότι τώρα $n^i \leq c2^n$. Για την απόδειξη, θεωρήστε m το πηλίκο της διαίρεσης του n με το i – το μοναδικό ακέραιο για τον οποίο $im \leq n < im + i$. Τότε θα έχουμε

$$\begin{aligned}
n^i &\leq (im + i)^i && \text{κατά τον ορισμό του } m \\
&= i^i(m + 1)^i && \\
&\leq i^i(2^{m+1})^i && \text{κατά την ανισότητα } n \leq 2^n \text{ για } n = m + 1 \\
&\leq c2^{mi} && \text{θυμηθείτε ότι } c = (2i)^i \\
&\leq c2^n && \text{επίσης κατά τον ορισμό του } m.
\end{aligned}$$

Συνεπώς, ο ρυθμός αύξησης οποιουδήποτε πολυωνύμου δεν είναι γρηγορότερος από αυτόν του 2^n. Μπορεί ένα πολυώνυμο να έχει τον ίδιο ρυθμό αύξησης με το 2^n; Αν ναι, τότε κάθε πολυώνυμο μεγαλύτερου βαθμού θα έχει επίσης τον ίδιο ρυθμό αύξησης· και είδαμε στο προηγούμενο παράδειγμα ότι πολυώνυμα διαφορετικών βαθμών έχουν διαφορετικούς ρυθμούς αύξησης. Συμπεραίνουμε ότι *το 2^n έχει μεγαλύτερο ρυθμό αύξησης από οποιοδήποτε πολυώνυμο.* Άλλες εκθετικές συναρτήσεις, όπως οι 5^n, n^n, $n!$, 2^{n^2}, ή χειρότερα η 2^{2^n}, έχουν ακόμα μεγαλύτερους ρυθμούς αύξησης. $\diamondsuit$

Ανάλυση αλγορίθμων

Πολυωνυμικοί και εκθετικοί ρυθμοί αύξησης προκύπτουν πολύ φυσικά στην *ανάλυση αλγορίθμων*. Για παράδειγμα, ας κάνουμε μια πρόχειρη εκτίμηση για τον αριθμό βημάτων που χρειάζεται να κάνει ένας αλγόριθμος για την ανακλαστική μεταβατική κλειστότητα που εισαγάγαμε στην αρχή αυτής της ενότητας.

Ο αλγόριθμος εξετάζει κάθε ακολουθία $(b_1, \ldots, b_i)$, μήκους μέχρι n, για να αποφασίσει εάν είναι μονοπάτι της R, και, αν η απάντηση είναι «ναι», προσθέτει την $(b_1, \ldots, b_i)$ στην R^*. Κάθε τέτοια επανάληψη μπορεί οπωσδήποτε να ολοκληρωθεί σε n ή λιγότερες «στοιχειώδεις λειτουργίες» – εξετάζουμε εάν $(a, b) \in R$ και προσθέτουμε το (a, b) στην R^*. Άρα, ο συνολικός αριθμός λειτουργιών δεν μπορεί να είναι μεγαλύτερος από

$$n \cdot (1 + n + n^2 + \cdots + n^n),$$

ο οποίος ανήκει στο $\mathcal{O}(n^{n+1})$. Έχουμε δείξει, επομένως, ότι ο ρυθμός αύξησης των *χρονικών απαιτήσεων* του αλγορίθμου αυτού είναι $\mathcal{O}(n^{n+1})$.

Το αποτέλεσμα αυτό είναι αρκετά απογοητευτικό διότι είναι μία *εκθετική* συνάρτηση, με ρυθμό αύξησης ακόμα μεγαλύτερο από 2^n. Ο αλγόριθμος αυτός δεν είναι καθόλου αποδοτικός!

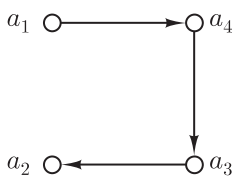
Προκύπτει, λοιπόν, η ερώτηση, υπάρχει γρηγορότερος αλγόριθμος για τον υπολογισμό της ανακλαστικής μεταβατικής κλειστότητας; Θεωρήστε τον παρακάτω:

> *Αρχικά* $R^* := R \cup \{(a_i, a_i) : a_i \in A\}$
> while *υπάρχουν τρία στοιχεία* $a_i, a_j, a_k \in A$ *τέτοια ώστε*
> $(a_i, a_j), (a_j, a_k) \in R^*$ *αλλά* $(a_i, a_k) \notin R^*$ do
>   *πρόσθεσε το* (a_i, a_k) *στην* R^*.

Ο αλγόριθμος αυτός είναι ίσως ακόμα πιο προφανής και διαισθητικά σωστός από τον πρώτο. Αρχίζει προσθέτοντας στην R^* όλα τα ζεύγη της R και όλα τα ζεύγη της μορφής (a_i, a_i) – εξασφαλίζοντας έτσι ότι η R^* περιέχει την R και είναι ανακλαστική. Τότε εξετάζει διαδοχικά για παραβιάσεις της μεταβατικής ιδιότητας. Ενδεχομένως, αυτή η αναζήτηση παραβιάσεων προχωράει με κάποιο οργανωμένο τρόπο που δεν περιγράφεται ακριβώς στον αλγόριθμο, για παράδειγμα διατρέχει όλες τις τιμές του a_i, για καθεμία από αυτές διατρέχει όλες τις τιμές του a_j, και τελικά του a_k. Αν ανακαλύψουμε μια τέτοια παραβίαση, τότε τη διορθώνουμε προσθέτοντας το κατάλληλο ζεύγος στην R^*, και η αναζήτηση παραβιάσεων πρέπει να ξεκινήσει από την αρχή. Αν σε κάποιο σημείο όλες οι τριάδες έχουν εξεταστεί και καμία παραβίαση δεν έχει βρεθεί, ο αλγόριθμος τερματίζει.

Όταν ο αλγόριθμος τερματίσει, η R^* θα περιέχει σίγουρα την R, και θα είναι ανακλαστική· επιπλέον, εφόσον καμία παραβίαση δεν βρέθηκε στην τελευταία επανάληψη του βρόχου while, η R^* πρέπει να είναι μεταβατική. Ακόμα, η R^* είναι η μικρότερη σχέση που έχει όλες τις ιδιότητες αυτές (και είναι επομένως η ζητούμενη ανακλαστική μεταβατική κλειστότητα της R). Για να δείτε γιατί, υποθέστε ότι υπάρχει ένα κατάλληλο υποσύνολο της R^*, το ονομάζουμε R_0, που περιέχει την R, και είναι ανακλαστικό και μεταβατικό. Θεωρήστε το πρώτο ζεύγος που δεν ανήκει στην R_0, αλλά είχε προστεθεί στην R^* από τον αλγόριθμο. Δεν μπορεί να είναι ζεύγος της R, ή ζεύγος της μορφής (a_i, a_i), διότι όλα τα ζεύγη αυτά ανήκουν στην R_0. Συνεπώς, πρέπει να είναι ένα ζεύγος (a_i, a_k) τέτοιο ώστε τα (a_i, a_j) και (a_j, a_k) να ανήκουν και τα δύο στην R^* σε εκείνο το σημείο – και έτσι και στην R_0, καθώς το (a_i, a_k) ήταν το πρώτο ζεύγος ως προς το οποίο διαφέρουν οι δύο σχέσεις. Τότε όμως η R_0, σύμφωνα με την υπόθεσή μας μια μεταβατική σχέση, πρέπει να περιέχει επίσης το (a_i, a_k) – πράγμα άτοπο. Συνεπώς, το αποτέλεσμα θα είναι η ανακλαστική μεταβατική κλειστότητα της R, και ο αλγόριθμος είναι σωστός.

Πότε όμως θα τερματίσει ο αλγόριθμος; Η απάντηση είναι *μετά από το πολύ n^2 επαναλήψεις του βρόχου while*. Και αυτό γιατί μετά από κάθε επιτυχημένη επανάληψη προσθέτουμε στην R^* ένα ζεύγος (a_i, a_k) που δεν υπήρχε εκεί πριν, και υπάρχουν το πολύ n^2 ζεύγη να προστεθούν. Άρα ο αλγόριθμος θα τερματίσει μετά από το πολύ n^2 επαναλήψεις. Και αφού κάθε επανάληψη μπορεί να ολοκληρωθεί σε χρόνο $\mathcal{O}(n^3)$ (πρέπει να αναζητήσουμε όλες τις τριάδες στοιχείων του A), η πολυπλοκότητα του νέου αλγορίθμου είναι $\mathcal{O}(n^2 \times n^3) = \mathcal{O}(n^5)$ – ένας *πολυωνυμικός* ρυθμός αύξησης, και επομένως μια αξιοθαύμαστη βελτίωση σε σύγκριση με την εκθετική πρώτη μας προσπάθεια.



Σχήμα 1-10

Παράδειγμα 1.6.3: Ας εξετάσουμε την απόδοση του νέου αλγορίθμου για το γράφημα στο Σχήμα 1-10. Ξεκινάμε στην πρώτη γραμμή με το γράφημα στο οποίο προσθέτουμε όλες τις μεταβάσεις από έναν κόμβο στον εαυτό του, τις οποίες ονομάζουμε αυτομεταβάσεις. Υποθέστε ότι η αναζήτηση τριάδων (a_i, a_j, a_k) που παραβιάζουν τη μεταβατικότητα πραγματοποιείται με τη «φυσική» σειρά

$$(a_1, a_1, a_1), (a_1, a_1, a_2), \ldots, (a_1, a_1, a_4), (a_1, a_2, a_1), (a_1, a_2, a_2), \ldots, (a_4, a_4, a_4).$$

Η πρώτη παραβίαση που ανακαλύπτουμε επομένως είναι η (a_1, a_4, a_3), και έτσι προσθέτουμε την ακμή (a_1, a_3). Στη συνέχεια ξεκινάμε τον έλεγχο όλων των τριάδων από την αρχή – επειδή η εισαγωγή τής (a_1, a_3) μπορεί να έχει προκαλέσει την παραβίαση της μεταβατικότητας σε μια τριάδα που εξετάστηκε στην προηγούμενη επανάληψη. Πράγματι, η επόμενη παραβίαση βρίσκεται στην (a_1, a_3, a_2), και έτσι προσθέτουμε την ακμή (a_1, a_2). Ξεκινάμε και πάλι από την αρχή, αυτή τη φορά για να ανακαλύψουμε παραβίαση για την τριάδα (a_4, a_3, a_2) – προσθέτουμε την ακμή (a_4, a_2). Στην επόμενη επανάληψη εξετάζουμε όλες τις τριάδες χωρίς να βρεθεί παραβίαση, και έτσι συμπεραίνουμε ότι έχουμε υπολογίσει την ανακλαστική μεταβατική κλειστότητα του γραφήματος. $\diamondsuit$

Το παράδειγμα αυτό καταδεικνύει την αιτία της σχετικά χαμηλής αποδοτικότητας του αλγορίθμου μας, η οποία αντανακλάται στην απότομη (n^5) αύξηση της πολυπλοκότητάς του: Μία τριάδα (a_i, a_j, a_k) πρέπει να εξεταστεί κατ' επανάληψη για πιθανή παραβίαση της μεταβατικότητας, καθώς ένα νεοεισαχθέν ζεύγος μπορεί να προκαλέσει νέες παραβιάσεις *σε τριάδες που έχουν ήδη ελεγχθεί.*

Μπορούμε να κάνουμε κάτι καλύτερο; Πιο συγκεκριμένα, υπάρχει τρόπος να διατάξουμε τις τριάδες έτσι ώστε τα νεοεισαχθέντα ζεύγη να μην προκαλούν ποτέ παραβιάσεις μεταβατικότητας σε τριάδες που έχουν ήδη εξεταστεί; Μια τέτοια διάταξη θα απέφερε έναν $\mathcal{O}(n^3)$ αλγόριθμο, καθώς στην περίπτωση αυτή κάθε τριάδα θα έπρεπε να εξεταστεί μία και μοναδική φορά.

Όπως προκύπτει, μια τέτοια διάταξη είναι δυνατή: Διατάσσουμε όλες τις τριάδες (a_i, a_j, a_k) ώστε να εξεταστούν σε *αύξουσα σειρά ως προς το* j – το μεσαίο δείκτη! Πρώτα κοιτάμε συστηματικά για παραβιάσεις μεταβατικότητας της μορφής (a_i, a_1, a_k)· για όσες βρίσκουμε, προσθέτουμε τα κατάλληλα ζεύγη, και η αναζήτηση συνεχίζει από το σημείο που σταμάτησε. Όταν όλες οι τριάδες της μορφής (a_i, a_1, a_k) έχουν εξεταστεί, κοιτάμε όλες τις τριάδες της μορφής (a_i, a_2, a_k), στη συνέχεια τις (a_i, a_3, a_k), κ.ο.κ. Η ακριβής σειρά με την οποία εξετάζουμε τις τριάδες της κάθε ομάδας δεν έχει σημασία. Αφού εξετάσουμε και την τελευταία ομάδα, όλες τις τριάδες της μορφής (a_i, a_n, a_k), σταματάμε, έχοντας υπολογίσει την ανακλαστική μεταβατική κλειστότητα. Ο πλήρης αλγόριθμος είναι ο εξής:

Αρχικά $R^* := R \cup \{(a_i, a_i) : a_i \in A\}$
for $j = 1, 2, \ldots, n$ do
for $i = 1, 2, \ldots, n$ *και* $k = 1, 2, \ldots, n$ do
if $(a_i, a_j), (a_j, a_k) \in R^*$ *αλλά* $(a_i, a_k) \notin R^*$ then *πρόσθεσε το* (a_i, a_k) *στην* R^*.

Γιατί η ιδέα αυτή λειτουργεί σωστά; Θεωρήστε ένα μονοπάτι $(a_{i_0}, a_{i_1}, \ldots, a_{i_{k-1}}, a_{i_k})$ από το a_{i_0} στο a_{i_k}, όπου $1 \leq i_j \leq n$ για κάθε j. Ορίζουμε ως *βαθμό* του μονοπατιού το μεγαλύτερο ακέραιο ανάμεσα στους $i_1, \ldots, i_{k-1}$· δηλαδή, το μεγαλύτερο δείκτη που εμφανίζεται σε κάποιον ενδιάμεσο κόμβο. Τετριμμένα μονοπάτια, όπως ακμές και αυτομεταβάσεις, έχουν βαθμό μηδέν, καθώς δεν έχουν ενδιάμεσους κόμβους.

Με την ορολογία αυτή μπορούμε να επιχειρηματολογήσουμε για την ορθότητα του τελευταίου αλγορίθμου μας. Πιο συγκεκριμένα, μπορούμε να αποδείξουμε την παρακάτω πρόταση: *Για κάθε $j = 0, \ldots, n$, αμέσως μετά την j-οστή εκτέλεση του εξωτερικού βρόχου, η R^* περιέχει όλα τα ζεύγη (a_i, a_k) έτσι ώστε να υπάρχει μονοπάτι βαθμού j ή μικρότερου από το a_i στο a_k, στην R.* Παρατηρήστε ότι, εφόσον όλα τα μονοπάτια έχουν βαθμό n το πολύ, συνεπάγεται ότι στο τέλος όλα τα ζεύγη που συνδέονται μέσω οποιουδήποτε μονοπατιού θα έχουν προστεθεί στην R^*.

Η πρόταση αυτή αποδεικνύεται με επαγωγή στο j. Το ζητούμενο ασφαλώς ισχύει όταν $j = 0$ – δεν έχουν γίνει επαναλήψεις, και έτσι η R^* περιέχει μόνο ζεύγη που συνδεόνται με τετριμμένα μονοπάτια, βαθμού 0. Για την επαγωγική υπόθεση, υποθέστε ότι το ζητούμενο ισχύει για j μέχρι κάποια τιμή, έστω $m < n$, και θεωρήστε την $m + 1$-οστή επανάληψη. Πρέπει να αποδείξουμε ότι η $m + 1$-οστή επανάληψη προσθέτει στην R^* ακριβώς αυτά τα ζεύγη που συνδέονται στην R με μονοπάτια βαθμού ίσου με $m + 1$, δηλαδή, αυτά για τα οποία ο κόμβος με το μεγαλύτερο δείκτη είναι ο a_{m+1}. Αν δύο κόμβοι a_i και a_k συνδέονται με ένα τέτοιο μονοπάτι, ο κόμβος a_{m+1} θα εμφανίζεται ακριβώς μία φορά στο μονοπάτι αυτό –αν εμφανίζεται παραπάνω από μία φορά, τότε αγνοήστε το τμήμα του μονοπατιού ανάμεσα στην πρώτη και την τελευταία εμφάνιση– ενώ όλοι οι υπόλοιποι ενδιάμεσοι κόμβοι θα έχουν δείκτη m ή μικρότερο. Και ένα τέτοιο μονοπάτι θα αποτελείται από ένα μονοπάτι βαθμού m ή μικρότερου από το a_i στο a_{m+1}, ακολουθούμενο από ένα μονοπάτι βαθμού m ή μικρότερου από το a_{m+1} στο a_k. Λόγω της επαγωγικής υπόθεσης, και τα δύο ζεύγη (a_i, a_{m+1}) και (a_{m+1}, a_k) πρέπει να ανήκουν στην R^* στο σημείο αυτό. Επομένως, ο αλγόριθμος θα ανακαλύψει ότι $(a_i, a_{m+1}), (a_{m+1}, a_k) \in R^*$, αλλά $(a_i, a_k) \notin R^*$, και θα προσθέσει το ζεύγος (a_i, a_k) στην R^*. Αντίστροφα, η $m+1$-οστή επανάληψη θα προσθέσει στην R^* μόνο ζεύγη (a_i, a_j) που συνδέονται με μονοπάτι βαθμού ακριβώς $m+1$. Ο αλγόριθμος είναι σωστός.

Παράδειγμα 1.6.3 (συνέχεια): Αν εφαρμόσουμε αυτό τον αλγόριθμο στο γράφημα του Σχήματος 1-10, καμία ακμή δεν θα προστεθεί όταν $j = 1$ και $j = 2$. Έτσι, όταν $j = 3$ προστίθεται η ακμή (a_4, a_2), και όταν $j = 4$ προστίθενται οι ακμές (a_1, a_3) και (a_1, a_2). $\diamondsuit$

Ιδιότητες κλειστότητας και κλειστότητες

Η μεταβατική κλειστότητα μιας σχέσης είναι απλώς ένα παράδειγμα ενός σημαντικού τρόπου ορισμού μεγαλύτερων συνόλων (ή σχέσεων) ξεκινώντας από μικρότερα.

Ορισμός 1.6.3: Έστω D ένα σύνολο, $n \geq 0$, και $R \subseteq D^{n+1}$ μία $(n+1)$-αδική σχέση στο D. Τότε ένα υποσύνολο B του D ονομάζεται **κλειστό ως προς την** R αν $b_{n+1} \in B$ όποτε $b_1, \ldots, b_n \in B$ και $(b_1, \ldots, b_n, b_{n+1}) \in R$. Κάθε ιδιότητα του τύπου «το σύνολο B είναι κλειστό ως προς τις σχέσεις $R_1, R_2, \ldots, R_m$» ονομάζεται **ιδιότητα κλειστότητας** του B.

Παράδειγμα 1.6.4: Το σύνολο των προγόνων ενός ανθρώπου είναι κλειστό ως προς τη σχέση

$$\{(a, b) : a \text{ και } b \text{ είναι άνθρωποι, και } b \text{ είναι ο πατέρας του } a\},$$

καθώς ο πατέρας ενός προγόνου είναι επίσης πρόγονος. $\diamondsuit$

Παράδειγμα 1.6.5: Έστω A ένα συγκεκριμένο σύνολο. Λέμε ότι το σύνολο S ικανοποιεί την *ιδιότητα υποσυνόλου ως προς το* A αν $A \subseteq S$. Κάθε ιδιότητα υποσυνόλου είναι ιδιότητα κλειστότητας, αν πάρουμε τη σχέση R να είναι η μοναδιαία σχέση $\{(a) : a \in A\}$ (παρατηρήστε ότι πρέπει να θέσουμε $n = 0$ στον Ορισμό 1.6.3) $\diamondsuit$

Παράδειγμα 1.6.6: Θα λέμε συχνά ότι ένα σύνολο $A \subseteq D$ είναι κλειστό ως προς μια *συνάρτηση* $f : D^k \mapsto D$. Δεν θα έπρεπε να υπάρχει απορία για τη σημασία της πρότασης αυτής, καθώς μια συνάρτηση είναι ένα ειδικό είδος σχέσης. Για παράδειγμα, μπορούμε να πούμε ότι οι φυσικοί αριθμοί είναι *κλειστοί ως προς την πρόσθεση*. Αυτό σημαίνει ότι για κάθε $m, n \in \mathbf{N}$ έχουμε επίσης $m + n \in \mathbf{N}$ – αφού $(m, n, m + n)$ είναι μια τριάδα ως προς τη «σχέση πρόσθεση» στους φυσικούς αριθμούς. Το $\mathbf{N}$ είναι επίσης κλειστό ως προς τον πολλαπλασιασμό, αλλά δεν είναι κλειστό ως προς την αφαίρεση. $\diamondsuit$

Παράδειγμα 1.6.7: Εφόσον οι σχέσεις είναι σύνολα, μπορούμε, όταν μιλάμε για μία σχέση, να λέμε ότι είναι κλειστή ως προς μία ή περισσότερες άλλες σχέσεις. Έστω D ένα σύνολο, και έστω Q η τριαδική σχέση ως προς το D^2 (δηλαδή το υποσύνολο του $(D \times D)^3$) τέτοιο ώστε

$$Q = \{((a, b), (b, c), (a, c)) : a, b, c \in D\}.$$

Τότε μια σχέση $R \subseteq D \times D$ είναι κλειστή ως προς την Q αν και μόνον αν είναι μεταβατική. Συμπεραίνουμε ότι η μεταβατικότητα είναι ιδιότητα κλειστότητας. Εξάλλου, η ανακλαστικότητα είναι ιδιότητα κλειστότητας, επειδή αποτελεί την ιδιότητα υποσυνόλου του συνόλου $\{(d, d) : d \in D\}$. $\diamondsuit$

Ένας συνηθισμένος τρόπος μαθηματικής κατασκευής είναι η μετάβαση από ένα σύνολο A στο *ελάχιστο σύνολο B που περιέχει το A και έχει την ιδιότητα P*. Όταν λέμε «ελάχιστο σύνολο B», εννοούμε «ένα σύνολο B που δεν περιέχει γνήσια κανένα άλλο σύνολο B' που επίσης περιέχει το A και έχει την ιδιότητα P». Μεγάλη προσοχή χρειάζεται όταν χρησιμοποιούνται ορισμοί αυτής της μορφής, έτσι ώστε το σύνολο B να είναι σαφώς ορισμένο, δηλαδή, να υπάρχει ένα μοναδικό τέτοιο ελάχιστο σύνολο. Εφόσον ένα σύνολο συνόλων μπορεί να έχει πολλά ελάχιστα στοιχεία ή και κανένα, εάν το B είναι σαφώς ορισμένο εξαρτάται από τη φύση της ιδιότητας P. Για παράδειγμα, αν P είναι η ιδιότητα «έχει είτε το b είτε το c ως στοιχείο» και $A = \{a\}$, τότε το B δεν είναι σαφώς ορισμένο καθώς και τα δύο σύνολα $\{a, b\}$ και $\{a, c\}$ είναι ελάχιστα σύνολα με το A υποσύνολο και με την ιδιότητα P.

Ωστόσο, όπως το ακόλουθο αποτέλεσμα εγγυάται, αν η P είναι ιδιότητα κλειστότητας, τότε το B είναι πάντα σαφώς ορισμένο.

Θεώρημα 1.6.1: *Έστω P μία ιδιότητα κλειστότητας ορισμένη από σχέσεις ενός συνόλου D, και έστω $A \subseteq D$. Τότε υπάρχει ένα μοναδικό ελάχιστο σύνολο B το οποίο περιέχει το A και έχει την ιδιότητα P.*

Απόδειξη:

Θεωρήστε το σύνολο όλων των υποσυνόλων του D που είναι κλειστά ως προς τις σχέσεις $R_1, \ldots, R_m$ και το A είναι υποσύνολό τους. Ονομάζουμε αυτό το σύνολο των συνόλων $\mathcal{S}$. Θα πρέπει να δείξουμε ότι το $\mathcal{S}$ έχει ένα μοναδικό ελάχιστο στοιχείο B. Είναι εύκολο να δείτε ότι το $\mathcal{S}$ είναι μη κενό, αφού περιέχει το «σύμπαν» D – ενώ το ίδιο είναι προφανώς κλειστό ως προς κάθε R_i, και σίγουρα περιέχει το A.

Τώρα έστω το σύνολο B, το οποίο είναι η τομή όλων των συνόλων στο $\mathcal{S}$,

$$B = \bigcap \mathcal{S}.$$

Κατ' αρχάς, το B είναι καλά ορισμένο γιατί είναι η τομή μιας μη κενής συλλογής συνόλων. Επίσης, είναι εύκολο να δει κανείς ότι περιέχει το A – αφού αυτό ισχύει για όλα τα σύνολα στο $\mathcal{S}$. Στη συνέχεια ισχυριζόμαστε ότι το B είναι κλειστό ως προς όλες τις R_i. Υποθέστε ότι $a_1, \ldots, a_{n_i-1} \in B$, και $(a_1, \ldots, a_{n_i-1}, a_{n_i}) \in R_i$. Εφόσον το B είναι η τομή όλων των συνόλων στο $\mathcal{S}$, έπεται ότι όλα τα σύνολα στο $\mathcal{S}$, περιέχουν τις $a_1, \ldots, a_{n_i-1}$. Εφόσον, όμως, όλα τα σύνολα στο $\mathcal{S}$ είναι κλειστά ως προς R_i, όλα περιέχουν τις a_{n_i} επίσης. Συνεπώς, το B πρέπει να περιέχει το a_{n_i}, και άρα το B είναι κλειστό ως προς R_i. Τέλος, το B είναι ελάχιστο, επειδή δεν μπορεί να υπάρχει κατάλληλο υποσύνολο του B, B', που να έχει τις ιδιότητες αυτές (να περιέχει το A και να είναι κλειστό ως προς τις R_i). Γιατί το B' θα ήταν στοιχείο του $\mathcal{S}$, και επομένως θα περιείχε το B. ■

Ονομάζουμε το B του Θεωρήματος 1.6.1 **κλειστότητα** του A ως προς τις σχέσεις $R_1, \ldots, R_m$.

Παράδειγμα 1.6.8: Το σύνολο όλων των προγόνων σας (όπου υποθέτουμε ότι καθένας είναι πρόγονος του εαυτού του) είναι η κλειστότητα του μονομελούς συνόλου το οποίο περιέχει μόνο τον εαυτό σας ως προς τη σχέση $\{(a, b) : a$ και b άνθρωποι, και b είναι ο πατέρας του $a\}$.$\diamondsuit$

Παράδειγμα 1.6.9: Το σύνολο των φυσικών αριθμών $\mathbf{N}$ είναι η κλειστότητα ως προς την πρόσθεση του συνόλου $\{0, 1\}$. Το $\mathbf{N}$ είναι κλειστό ως προς την πρόσθεση και τον πολλαπλασιασμό, αλλά όχι ως προς την αφαίρεση. Το σύνολο των ακεραίων (θετικοί, αρνητικοί και το μηδέν) είναι η κλειστότητα του $\mathbf{N}$ ως προς την αφαίρεση. $\diamondsuit$

Παράδειγμα 1.6.10: Η ανακλαστική, μεταβατική κλειστότητα μιας δυαδικής σχέσης R ως προς κάποιο πεπερασμένο σύνολο A, ορισμένη ως

$$R^* = \{(a, b) : \text{ υπάρχει μονοπάτι στην } R \text{ από το } a \text{ στο } b\}$$

(θυμηθείτε τον Ορισμό 1.6.1) έχει δικαιολογημένα αυτό το όνομα: Προκύπτει ότι είναι η κλειστότητα της R ως προς τη μεταβατικότητα και την ανακλαστικότητα – και τις δύο ιδιότητες κλειστότητας.

Κατ' αρχάς, η R^* είναι ανακλαστική και μεταβατική· γιατί υπάρχει τετριμμένο μονοπάτι από το a στο a για κάθε στοιχείο a, και υπάρχει μονοπάτι από το a στο b, και μονοπάτι από το b στο c, και έτσι υπάρχει μονοπάτι από το a στο c. Επίσης, προφανώς $R \subseteq R^*$, γιατί υπάρχει μονοπάτι από το a στο b όποτε $(a, b) \in R$.

Τέλος, η R^* είναι ελάχιστη. Γιατί έστω $(a, b) \in R^*$. Εφόσον $(a, b) \in R^*$, υπάρχει μονοπάτι $(a = a_1, \ldots, a_k = b)$ από το a στο b. Προκύπτει με επαγωγή στο k ότι το (a, b) πρέπει να ανήκει σε οποιαδήποτε σχέση που περιέχει την R και είναι μεταβατική και ανακλαστική.

Η ανακλαστική, μεταβατική κλειστότητα μιας δυαδικής σχέσης είναι μία μόνον από αρκετές πιθανές κλειστότητες. Για παράδειγμα, η *μεταβατική κλειστότητα* μιας σχέσης R, συμβολίζεται R^+, είναι το σύνολο όλων των (a, b) τέτοιο ώστε να υπάρχει ένα *μη τετριμμένο* μονοπάτι από το a στο b στην R – δεν χρειάζεται να είναι ανακλαστική. Και η *ανακλαστική, συμμετρική, μεταβατική κλειστότητα* οποιασδήποτε σχέσης (δεν υπάρχει ειδικό σύμβολο) είναι πάντα μία σχέση ισοδυναμίας. Όπως θα δούμε στη συνέχεια, υπάρχουν πολυωνυμικοί αλγόριθμοι για τον υπολογισμό όλων αυτών των κλειστοτήτων. $\diamondsuit$

Κάθε ιδιότητα κλειστότητας ως προς ένα πεπερασμένο σύνολο μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο! Υποθέστε ότι μας δίνονται σχέσεις $R_1 \subseteq D^{r_1}, \ldots, R_k \subseteq D^{r_k}$ με διάφορες πολλαπλότητες ως προς ένα πεπερασμένο σύνολο D, και ένα σύνολο $A \subseteq D$· μας ζητείται να υπολογίσουμε την κλειστότητα A^* του A ως προς $R_1, \ldots, R_k$. Αυτό μπορεί να πραγματοποιηθεί σε πολυωνυμικό χρόνο από μια απλή γενίκευση του $\mathcal{O}(n^5)$ αλγορίθμου που επινοήσαμε για το πρόβλημα της μεταβατικής κλειστότητας στην προηγούμενη υποενότητα:

Αρχικά $A^* := A$
while *υπάρχει δείκτης* i, $1 \leq i \leq k$, *και* r_i *στοιχεία* $a_{j_1}, \ldots, a_{j_{r_i - 1}} \in A^*$
  και $a_{j_{r_i}} \in D - A^*$ *τέτοιο ώστε* $(a_{j_1}, \ldots, a_{j_{r_i}}) \in R_i$ do
    πρόσθεσε το $a_{j_{r_i}}$ *στο* A^*.

Είναι μια απλή επέκταση του επιχειρήματός μας για τον αλγόριθμο μεταβατικής κλειστότητας, την οποία αφήνουμε ως άσκηση (Πρόβλημα 1.6.9), το να δείξουμε ότι ο παραπάνω αλγόριθμος είναι σωστός, και ότι τερματίζει μετά από $\mathcal{O}(n^{r+1})$ βήματα, όπου $n = |D|$ και r είναι ο μεγαλύτερος ακέραιος ανάμεσα στους $r_1, \ldots, r_k$. Προκύπτει ότι η κλειστότητα οποιουδήποτε δεδομένου συνόλου ως προς κάθε ιδιότητα κλειστότητας ορισμένη με τη χρήση δεδομένων σχέσεων *προκαθορισμένης πολλαπλότητας* μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο. Μάλιστα, στο Κεφάλαιο 7 θα αποδείξουμε μια πολύ ενδιαφέρουσα *αντίστροφη* πρόταση: *Κάθε* αλγόριθμος πολυωνυμικού χρόνου μπορεί να θεωρηθεί ως ο υπολογισμός της κλειστότητας ενός συνόλου ως προς κάποιες σχέσεις προκαθορισμένης πολλαπλότητας. Με άλλα λόγια, ο παραπάνω πολυωνυμικός αλγόριθμος για την κλειστότητα είναι *η μητέρα όλων των πολυωνυμικών αλγορίθμων*.

Προβλήματα για την Ενότητα 1.6

1.6.1. Είναι τα παρακάτω σύνολα κλειστά ως προς τις παρακάτω πράξεις; Αν όχι, ποιες είναι οι αντίστοιχες κλειστότητες;
(α) Οι περιττοί ακέραιοι ως προς τον πολλαπλασιασμό.
(β) Οι θετικοί ακέραιοι ως προς τη διαίρεση.
(γ) Οι αρνητικοί ακέραιοι ως προς την αφαίρεση.
(δ) Οι αρνητικοί ακέραιοι ως προς τον πολλαπλασιασμό.
(ε) Οι περιττοί ακέραιοι ως προς τη διαίρεση.

1.6.2. Ποια είναι η ανακλαστική μεταβατική κλειστότητα R^* της $R = \{(a, b), (a, c), (a, d), (d, c), (d, e)\}$; Να σχεδιάσετε ένα κατευθυνόμενο γράφημα που να αναπαριστά την R^*.

1.6.3. Είναι η μεταβατική κλειστότητα της συμμετρικής κλειστότητας μιας δυαδικής σχέσης αναγκαστικά ανακλαστική; Να το αποδείξετε ή να δώσετε αντιπαράδειγμα.

1.6.4. Έστω $R \subseteq A \times A$ μία δυαδική σχέση.
(α) Έστω $Q = \{(a, b) : a, b \in A$ και υπάρχουν μονοπάτια της R από το a στο b και από το b στο $a\}$. Να δείξετε ότι η Q είναι μία σχέση ισοδυναμίας στο A.
(β) Έστω Π μία διαμέριση του A που αντιστοιχεί στη σχέση ισοδυναμίας Q. Έστω $\mathcal{R}$ η σχέση $\{(S, T) : S, T \in \Pi$ και υπάρχει

μονοπάτι στην R από κάποιο από τα στοιχεία του S προς κάποιο από τα στοιχεία του $T\}$. Να δείξετε ότι η $\mathcal{R}$ είναι σχέση μερικής διάταξης στο Π.

1.6.5. Να δώσετε ένα παράδειγμα δυαδικής σχέσης που δεν είναι ανακλαστική, αλλά που έχει μεταβατική κλειστότητα που είναι ανακλαστική.

1.6.6. Θυμηθείτε τις τρεις συναρτήσεις στην αρχή της υποενότητας για τους ρυθμούς αύξησης:

$$f(n) = 1.000.000 \cdot n \cdot \quad g(n) = 10 \cdot n^3 \cdot \quad h(n) = 2^n.$$

Ποιες είναι οι κατάλληλες σταθερές c και d για τις σχέσεις $f(n) \in \mathcal{O}(g(n))$, $f(n) \in \mathcal{O}(h(n))$, και $g(n) \in \mathcal{O}(h(n))$; Ποιος είναι ο μικρότερος ακέραιος n τέτοιος ώστε $f(n) \leq g(n) \leq h(n)$;

1.6.7. Να διατάξετε τις παρακάτω συναρτήσεις σε αύξουσα σειρά ρυθμού αύξησης. Να εντοπίσετε ποιες από αυτές έχουν τον ίδιο ρυθμό αύξησης:

$$n^2, 2^n, n\lceil \log n \rceil, n!, 4^n, n^n, n^{\lceil \log n \rceil}, 2^{2^n}, 2^{2n}, 2^{2^{n+1}}.$$

1.6.8. Έχετε πέντε αλγορίθμους για ένα πρόβλημα με τους παρακάτω χρόνους εκτέλεσης:

$$10^6 n, \quad 10^4 n^2, \quad n^4, \quad 2^n, \quad n!$$

(α) Ο υπολογιστής σας εκτελεί 10^8 βήματα το δευτερόλεπτο. Ποιο είναι το μεγαλύτερο μέγεθος n για το οποίο ο κάθε αλγόριθμος μπορεί να λύσει το πρόβλημα σε ένα δευτερόλεπτο;
(β) Σε μία μέρα; (Υποθέστε ότι μία μέρα έχει 10^5 δευτερόλεπτα).
(γ) Πώς θα άλλαζαν οι αριθμοί που βρήκατε στα (α) και (β) αν αγοράζατε έναν υπολογιστή 10 φορές πιο γρήγορο;

1.6.9. Να δείξετε ότι ο αλγόριθμος στο τέλος αυτής της ενότητας υπολογίζει σωστά την κλειστότητα του συνόλου $A \subseteq D$ ως προς τις σχέσεις $R_1 \subseteq D^{r_1}, \ldots, R_k \subseteq D^{r_k}$ σε χρόνο $\mathcal{O}(n^r)$, όπου $n = |D|$, και r είναι η μέγιστη από τις πολλαπλότητες $r_1, \ldots, r_k$.
(*Υπόδειξη:* Το επιχείρημα είναι μια απλή γενίκευση του επιχειρήματος για τον $\mathcal{O}(n^5)$ αλγόριθμο μεταβατικής κλειστότητας.)

1.7 ΑΛΦΑΒΗΤΑ ΚΑΙ ΓΛΩΣΣΕΣ

Η μη αυστηρή μελέτη των αλγορίθμων στην προηγούμενη ενότητα έχει αφήσει πολλά σημεία ασαφή. Για παράδειγμα, δεν έχουμε προσδιορίσει πώς ακριβώς οι σχέσεις R και R^*, τις οποίες χρειάζεται να προσπελαύνουμε και να τροποποιούμε, αναπαριστώνται και αποθηκεύονται. Στην πρακτική του υπολογισμού, τέτοια *δεδομένα* κωδικοποιούνται στη μνήμη του υπολογιστή ως ακολουθίες διφίων (bits) ή άλλων συμβόλων κατάλληλων για επεξεργασία από έναν υπολογιστή. Για τη μαθηματική μελέτη της θεωρίας υπολογισμού θα πρέπει συνεπώς πρώτα να κατανοήσουμε *τα μαθηματικά των ακολουθιών συμβόλων*.

Αρχίζουμε με την έννοια του **αλφαβήτου**: ένα πεπερασμένο σύνολο **συμβόλων**. Ένα παράδειγμα είναι, φυσικά, το Λατινικό αλφάβητο $\{a, b, \ldots, z\}$. Ένα αλφάβητο που είναι ιδιαίτερα συμβατό με τη θεωρία υπολογισμού είναι το **δυαδικό αλφάβητο** $\{0, 1\}$. Στην πραγματικότητα, οποιοδήποτε αντικείμενο μπορεί να ανήκει σε ένα αλφάβητο. Αυστηρά, αλφάβητο είναι απλά ένα πεπερασμένο σύνολο οποιουδήποτε είδους αντικειμένων. Για λόγους απλότητας, όμως, χρησιμοποιούμε ως σύμβολα μόνο γράμματα, αριθμούς και άλλους συνηθισμένους χαρακτήρες όπως \$, ή $\#$.

Μία **συμβολοσειρά** (string) ενός αλφαβήτου είναι μια πεπερασμένη ακολουθία συμβόλων του αλφαβήτου. Αντί να γράφουμε τις συμβολοσειρές με παρενθέσεις και κόμματα, όπως κάναμε με τις άλλες ακολουθίες, απλά παραθέτουμε τα σύμβολα. Έτσι $watermelon$ είναι συμβολοσειρά του αλφαβήτου $\{a, b, \ldots, z\}$ και 0111011 είναι συμβολοσειρά του αλφαβήτου $\{0, 1\}$. Επίσης, χρησιμοποιώντας το φυσικό ισομορφισμό, ταυτίζουμε μια συμβολοσειρά ενός συμβόλου με το ίδιο το σύμβολο· επομένως το σύμβολο a είναι το ίδιο με τη συμβολοσειρά a. Μία συμβολοσειρά μπορεί να μην έχει καθόλου σύμβολα, και στην περίπτωση αυτή ονομάζεται **κενή συμβολοσειρά** και συμβολίζεται με e. Γενικά χρησιμοποιούμε τα u, v, w, x, y, z και ελληνικά γράμματα για να συμβολίσουμε τις συμβολοσειρές. Για παράδειγμα, θα χρησιμοποιούσαμε το w ως όνομα για τη συμβολοσειρά abc. Φυσικά, για να αποφύγουμε τη σύγχυση, είναι καλό να αποφεύγουμε να χρησιμοποιούμε ως σύμβολα γράμματα που χρησιμοποιούνται επίσης ως ονόματα συμβολοσειρών. Το σύνολο όλων των συμβολοσειρών, συμπεριλαμβανομένης και της κενής, ενός αλφάβητου Σ συμβολίζεται με Σ^*.

Το **μήκος** μιας συμβολοσειράς, είναι το μήκος της ως ακολουθία· έτσι το μήκος της συμβολοσειράς $acrd$ είναι 4. Συμβολίζουμε το μήκος μιας συμβολοσειράς w με $|w|$· έτσι $|101| = 3$ και $|e| = 0$. Εναλλακτικά (μέσω ενός φυσικού ισομορφισμού), μια συμβολοσειρά $w \in \Sigma^*$ μπορεί να θεωρηθεί ως συνάρτηση $w : \{1, \ldots, |w|\} \mapsto \Sigma$. Η τιμή του $w(j)$, όπου $1 \leq j \leq |w|$, είναι το σύμβολο της w στη θέση j. Για παράδειγμα, αν $w = accordion$, τότε $w(3) = w(2) = c$, και $w(1) = a$. Η εναλλακτική αυτή θεώρηση παρουσιάζει και ένα πιθανό σημείο σύγχυσης. Βέβαια, το σύμβολο c στη δεύτερη θέση είναι το ίδιο με το c της τρίτης θέσης. Αν όμως χρειάζεται να ξεχωρίζουμε όμοια σύμβολα σε διαφορετικές θέσεις μιας συμβολοσειράς, θα αναφερόμαστε σε αυτά ως διαφορετικές *εμφανίσεις* του συμβόλου. Δηλαδή, το σύμβολο $\sigma \in \Sigma$ εμφανίζεται στην j-οστή θέση της συμβολοσειράς $w \in \Sigma^*$ αν $w(j) = \sigma$.

Δύο συμβολοσειρές ενός αλφαβήτου μπορούν να συνδυαστούν για να σχηματίσουν μία τρίτη, με την πράξη της **παράθεσης** (concatenation). Η παράθεση δύο συμβολοσειρών x και y, που γράφεται $x \circ y$ ή απλά xy, είναι η συμβολοσειρά x ακολουθούμενη από την y. Αυστηρά, $w = x \circ y$ αν και μόνον αν $|w| = |x| + |y|$, $w(j) = x(j)$ για $j = 1, \ldots, |x|$, και $w(|x| + j) = y(j)$ για $j = 1, \ldots, |y|$. Για παράδειγμα, $01 \circ 001 = 01001$ και $beach \circ boy = beachboy$. Φυσικά, $w \circ e = e \circ w = w$ για κάθε συμβολοσειρά w. Και η παράθεση είναι προσεταιριστική: $(wx)y = w(xy)$ για όλες τις συμβολοσειρές w, x και y. Μία συμβολοσειρά v είναι **υποσυμβολοσειρά** μιας συμβολοσειράς w αν και μόνον αν υπάρχουν συμβολοσειρές x και y τέτοιες ώστε $w = xvy$. Και το x και το y μπορούν να είναι e, άρα κάθε συμβολοσειρά είναι υποσυμβολοσειρά του εαυτού της· και αν πάρουμε $x = w$ και $v = y = e$, βλέπουμε ότι το e είναι υποσυμβολοσειρά κάθε συμβολοσειράς. Αν $w = xv$ για κάποιο x, τότε το v λέγεται **κατάληξη** (suffix) του w. Αν $w = vy$ για κάποιο y, τότε το v λέγεται **πρόθεμα** (prefix) του w. Έτσι, η $road$ είναι πρόθεμα της $roadrunner$, κατάληξη της $abroad$ και υποσυμβολοσειρά και των δύο αυτών και της $broader$. Μία συμβολοσειρά μπορεί να έχει πολλές εμφανίσεις της ίδιας υποσυμβολοσειράς. Για παράδειγμα, η $ababab$ έχει τρεις εμφανίσεις της ab και δύο της $abab$.

Για κάθε συμβολοσειρά w και κάθε φυσικό αριθμό i, η συμβολοσειρά w^i ορίζεται ως

$$w^0 = e, \text{ η κενή συμβολοσειρά}$$
$$w^{i+1} = w^i \circ w \text{ για κάθε } i \geq 0.$$

Έτσι $w^1 = w$ και $(do)^2 = dodo$.

Με τον ορισμό αυτό συναντάμε για πρώτη φορά έναν πολύ κοινό τύπο ορισμού: τον **ορισμό με επαγωγή**. Έχουμε ήδη δει *αποδείξεις* με επαγωγή, και η βασική ιδέα είναι η ίδια. Υπάρχει μια βασική περίπτωση του ορισμού που εδώ είναι ο ορισμός της w^i για $i = 0$· έπειτα, όταν το οριζόμενο αντικείμενο έχει οριστεί για κάθε $j \leq i$, ορίζεται και για $j = i + 1$. Στο παραπάνω παράδειγμα, η w^{i+1} ορίζεται με τη βοήθεια της w^i. Για να δείτε ακριβώς πώς οποιαδήποτε περίπτωση του ορισμού μπορεί να αναχθεί πίσω στη βασική περίπτωση, εξετάστε το παράδειγμα του $(do)^2$. Σύμφωνα με τον ορισμό (με $i = 1$) $(do)^2 = (do)^1 \circ do$. Και πάλι σύμφωνα με τον ορισμό (με $i = 0$) $(do)^1 = (do)^0 \circ do$. Τώρα, η βασική περίπτωση εφαρμόζεται: $(do)^0 = e$. Έτσι $(do)^2 = (e \circ do) \circ do = dodo$.

Η **αντίστροφη** μίας συμβολοσειράς w, συμβολίζεται με w^R, και είναι η συμβολοσειρά «διαβασμένη από το τέλος προς την αρχή»: για παράδειγμα, $reverse^R = esrever$. Ένας αυστηρός ορισμός μπορεί να δοθεί με επαγωγή στο μήκος της συμβολοσειράς:

(1) Αν w είναι συμβολοσειρά μήκους 0, τότε $w^R = w = e$.
(2) Αν w είναι συμβολοσειρά μήκους $n + 1 > 0$, τότε $w = ua$ για κάποιο $a \in \Sigma$ και $w^R = au^R$.

Ας χρησιμοποιήσουμε τον ορισμό αυτό για να εξηγήσουμε πώς μια επαγωγική απόδειξη μπορεί να βασίζεται σε έναν επαγωγικό ορισμό. Θα δείξουμε ότι για όλες τις συμβολοσειρές w και x, $(wx)^R = x^R w^R$. Για παράδειγμα, $(dogcat)^R = (cat)^R (dog)^R = tacgod$. Θα το δείξουμε με επαγωγή στο μήκος του x.

Βασικό βήμα. $|x| = 0$. Τότε $x = e$, και $(wx)^R = (we)^R = w^R = ew^R = e^R w^R = x^R w^R$.

Επαγωγική υπόθεση. Αν $|x| \leq n$, τότε $(wx)^R = x^R w^R$.

Επαγωγικό βήμα. Έστω $|x| = n + 1$· τότε $x = ua$ για κάποιο $u \in \Sigma^*$ και $a \in \Sigma$ έτσι ώστε $|u| = n$.

$$
\begin{aligned}
(wx)^R &= (w(ua))^R && \text{καθώς } x = ua \\
&= ((wu)a)^R && \text{καθώς η παράθεση είναι προσεταιριστική} \\
&= a(wu)^R && \text{κατά τον ορισμό της αντίστροφης της } (wu)a \\
&= au^R w^R && \text{λόγω της επαγωγικής υπόθεσης} \\
&= (ua)^R w^R && \text{κατά τον ορισμό της αντίστροφης της } ua \\
&= x^R w^R && \text{καθώς } x = ua
\end{aligned}
$$

Τώρα περνάμε από τη μελέτη των μεμονωμένων συμβολοσειρών στη μελέτη των πεπερασμένων και άπειρων *συνόλων* συμβολοσειρών. Τα απλά μοντέλα των υπολογιστικών μηχανών που θα μελετήσουμε σύντομα θα χαρακτηρίζονται σύμφωνα με κανονικότητες στον τρόπο με τον οποίο χειρίζονται πολλές διαφορετικές συμβολοσειρές, και έτσι είναι σημαντικό να κατανοήσει κανείς τους γενικούς τρόπους περιγραφής και συνδυασμού κλάσεων συμβολοσειρών.

Κάθε σύνολο από συμβολοσειρές ενός αλφαβήτου Σ –δηλαδή κάθε υποσύνολο του Σ^*– θα ονομάζεται **γλώσσα**. Έτσι Σ^*, $\emptyset$ και Σ είναι γλώσσες. Εφόσον μία γλώσσα είναι απλά ένα ειδικό είδος συνόλου, μπορούμε να ορίσουμε μια πεπερασμένη γλώσσα παραθέτοντας όλες τις συμβολοσειρές της. Για παράδειγμα, $\{aba, car, d, f\}$ είναι μία γλώσσα του $\{a, b, c, \ldots, z\}$. Ωστόσο, οι περισσότερες ενδιαφέρουσες γλώσσες είναι άπειρες, και έτσι δεν μπορούμε να παραθέσουμε όλες τις συμβολοσειρές τους. Γλώσσες που θα μπορούσαμε να θεωρήσουμε είναι οι $\{0, 01, 011, 0111, ...\}$, $\{w \in \{0,1\}^* :$ η w έχει ίσο πλήθος 1 και 0$\}$, και $\{w \in \Sigma^* :$ η $w = w^R\}$. Επομένως θα ορίσουμε άπειρες γλώσσες σύμφωνα με το σχήμα:

$$L = \{w \in \Sigma^* : \text{η } w \text{ έχει την ιδιότητα } P\},$$

ακολουθώντας το γενικό τρόπο που χρησιμοποιήσαμε για να ορίσουμε τα άπειρα σύνολα.

Αν Σ είναι ένα πεπερασμένο αλφάβητο, τότε το Σ^* είναι σίγουρα άπειρο· αλλά είναι ένα μετρήσιμα άπειρο σύνολο; Δεν είναι δύσκολο να δούμε ότι αυτό πράγματι ισχύει. Για να κατασκευάσουμε την αμφιμονοσήμαντη αντιστοιχία $f : \mathbf{N} \mapsto \Sigma^*$, πρέπει πρώτα να διατάξουμε το αλφάβητο. Έστω $\Sigma = \{a_1, \ldots, a_n\}$, όπου τα $a_1, \ldots, a_n$ είναι διαφορετικά. Τα στοιχεία του Σ^* μπορούν τότε να απαριθμηθούν με τον εξής τρόπο:

(1) Για κάθε $k \geq 0$, όλες οι συμβολοσειρές μήκους k απαριθμούνται πριν από όλες τις συμβολοσειρές που έχουν μήκος $k+1$.
(2) Οι n^k συμβολοσειρές μήκους ακριβώς k απαριθμούνται **λεξικογραφικά**, δηλαδή η $a_{i_1} \ldots a_{i_k}$ προηγείται της $a_{j_1} \ldots a_{j_k}$, υπό την προϋπόθεση ότι για κάποιο m, $0 \leq m \leq k-1$, $i_\ell = j_\ell$ για $\ell = 1, \ldots, m$, και $i_{m+1} < j_{m+1}$.

Για παράδειγμα, αν $\Sigma = \{0, 1\}$, η σειρά θα ήταν ως εξής:

$$e, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots$$

Αν Σ είναι το Λατινικό αλφάβητο και η διάταξη του Σ είναι η συνηθισμένη $\{a, \ldots, z\}$, τότε η λεξικογραφική σειρά για τις ίσου μήκους συμβολοσειρές είναι η σειρά που χρησιμοποιείται στα λεξικά· ωστόσο, η διάταξη που περιγράφηκε με τα (1) και (2) για όλες τις συμβολοσειρές του

Σ^* διαφέρει από τη σειρά του λεξικού στο ότι οι μικρότερες συμβολοσειρές παρατίθενται πριν από τις μεγαλύτερες. Εφόσον οι γλώσσες είναι σύνολα, μπορούν να συνδυαστούν με τις πράξεις συνόλων, ένωση, τομή και διαφορά. Όταν κάποιο αλφάβητο γίνεται κατανοητό από τα συμφραζόμενα, τότε θα γράφουμε $\overline{A}$ –το **συμπλήρωμα** του A– αντί για τη διαφορά $\Sigma^* - A$.

Επιπλέον, ορισμένες πράξεις έχουν έννοια μόνο στις γλώσσες. Η πρώτη από αυτές είναι η **παράθεση των γλωσσών**. Αν L_1 και L_2 είναι γλώσσες του Σ, η παράθεσή τους είναι $L = L_1 \circ L_2$, ή απλά, $L = L_1L_2$ όπου

$$L = \{w \in \Sigma^* : w = x \circ y \text{ για κάποιο } x \in L_1 \text{ και } y \in L_2\}.$$

Για παράδειγμα, αν $\Sigma = \{0, 1\}$, $L_1 = \{w \in \Sigma^* : w \text{ έχει άρτιο αριθμό } 0\}$, και $L_2 = \{w : w \text{ αρχίζει από } 0 \text{ και τα υπόλοιπα σύμβολα είναι } 1\}$, τότε $L_1 \circ L_2 = \{w : w \text{ έχει περιττό αριθμό από } 0\}$.

Μία άλλη πράξη σε γλώσσες, είναι η **Kleene star** μιας γλώσσας L, και συμβολίζεται με L^*. L^*, είναι το σύνολο όλων των συμβολοσειρών που προκύπτουν από την παράθεση μηδέν ή περισσότερων συμβολοσειρών της L (η παράθεση μηδέν συμβολοσειρών είναι η e και η παράθεση μιας συμβολοσειράς είναι η ίδια η συμβολοσειρά). Έτσι

$$\begin{aligned} L^* = \{w \in \Sigma^* : w = w_1 \circ \cdots \circ w_k \ \text{ για κάποιο } k \geq 0 \\ \text{και κάποια } w_1, \ldots, w_k \in L\}. \end{aligned}$$

Για παράδειγμα, αν $L = \{01, 1, 100\}$, τότε $110001110011 \in L^*$, καθώς $110001110011 = 1 \circ 100 \circ 01 \circ 1 \circ 100 \circ 1 \circ 1$, και καθεμία από τις συμβολοσειρές αυτές ανήκει στην L.

Σημειώστε ότι η χρήση του Σ^* για το συμβολισμό του συνόλου όλων των συμβολοσειρών του Σ είναι σύμφωνη με το συμβολισμό του Kleene star του Σ, αν το θεωρήσουμε ως πεπερασμένη γλώσσα. Δηλαδή, αν $L = \Sigma$ και εφαρμόσουμε τον παραπάνω ορισμό, τότε Σ^* είναι το σύνολο όλων των συμβολοσειρών που μπορούν να γραφτούν ως $w_1 \circ \cdots \circ w_k$ για κάποιο $k \geq 0$ και κάποια $w_1, \ldots, w_k \in \Sigma$. Εφόσον τα w_i είναι τότε απλά σύμβολα του Σ, προκύπτει ότι το Σ^* είναι, όπως αρχικά ορίστηκε, το σύνολο όλων των πεπερασμένων συμβολοσειρών των οποίων τα σύμβολά ανήκουν στο Σ.

Ως ένα άλλο ακραίο παράδειγμα, παρατηρήστε ότι $\emptyset^* = \{e\}$. Γιατί έστω $L = \emptyset$ στον παραπάνω ορισμό. Η μοναδική δυνατή παράθεση $w_1 \circ w_2 \circ \cdots \circ w_k$ με $k \geq 0$ και $w_1, \ldots, w_k \in L$ είναι αυτή με $k = 0$, δηλαδή η παράθεση μηδέν συμβολοσειρών· έτσι το μοναδικό στοιχείο του L^* είναι στην περίπτωση αυτή το e!

Ως τελευταίο παράδειγμα θα δείξουμε ότι αν L είναι η γλώσσα $\{w \in \{0,1\}^* : w$ έχει άνισο αριθμό 0 και 1$\}$, τότε $L^* = \{0,1\}^*$. Για να βεβαιωθούμε, αρχικά παρατηρούμε ότι για οποιεσδήποτε γλώσσες L_1 και L_2, αν $L_1 \subseteq L_2$, τότε $L_1^* \subseteq L_2^*$, όπως είναι προφανές από τον ορισμό της Kleene star. Έπειτα $\{0,1\} \subseteq L$, καθώς καθένα από τα 0 και 1, τα οποία τα θεωρούμε συμβολοσειρές, έχει άνισο αριθμό από 0 και 1. Άρα $\{0,1\}^* \subseteq L^*$. Εξ ορισμού, όμως, $L^* \subseteq \{0,1\}^*$ και συνεπώς $L^* = \{0,1\}^*$.

Γράφουμε L^+ για τη γλώσσα LL^*. Ισοδύναμα, L^+ είναι η γλώσσα

$$\{w \in \Sigma^* : w = w_1 \circ w_2 \circ \cdots \circ w_k \text{ για κάποιο } k \geq 1$$
$$\text{και κάποια } w_1, \ldots, w_k \in L\}.$$

Προσέξτε ότι η L^+ μπορεί να θεωρηθεί η *κλειστότητα* της L ως προς τη συνάρτηση της παράθεσης. Δηλαδή, η L^+ είναι η μικρότερη γλώσσα που περιέχει την L και όλες τις συμβολοσειρές που είναι παραθέσεις των συμβολοσειρών της L.

Προβλήματα για την Ενότητα 1.7

1.7.1. (α) Να αποδείξετε, με χρήση του ορισμού της παράθεσης που δόθηκε στο κείμενο, ότι η παράθεση των συμβολοσειρών είναι προσεταιριστική.

(β) Να δώσετε έναν επαγωγικό ορισμό της παράθεσης των συμβολοσειρών.

(γ) Χρησιμοποιώντας τον επαγωγικό ορισμό του (β), να αποδείξετε ότι η παράθεση των συμβολοσειρών είναι προσεταιριστική.

1.7.2. Να αποδείξετε τα παρακάτω χρησιμοποιώντας τον επαγωγικό ορισμό της αντιστροφής που δόθηκε στο κείμενο.

(α) $(w^R)^R = w$ για κάθε συμβολοσειρά w.

(β) Αν v είναι υποσυμβολοσειρά της w, τότε v^R είναι υποσυμβολοσειρά της w^R.

(γ) $(w^i)^R = (w^R)^i$ για κάθε συμβολοσειρά w και κάθε $i \geq 0$.

1.7.3. Έστω $\Sigma = \{a_1, \ldots, a_{26}\}$ το Λατινικό αλφάβητο. Να ορίσετε προσεκτικά τη δυαδική σχέση $<$ στο Σ^* έτσι ώστε $x < y$ αν και μόνον αν το x θα προηγούνταν του y σε ένα συνηθισμένο λεξικό.

1.7.4. Να δείξετε καθένα από τα παρακάτω.

(α) $\{e\}^* = \{e\}$

(β) Για κάθε αλφάβητο Σ και κάθε $L \subseteq \Sigma^*$, $(L^*)^* = L^*$.
(γ) Αν τα a και b είναι διαφορετικά σύμβολα, τότε $\{a,b\}^* = \{a\}^*(\{b\}\{a\}^*)^*$.
(δ) Αν Σ οποιοδήποτε αλφάβητο, $e \in L_1 \subseteq \Sigma^*$ και $e \in L_2 \subseteq \Sigma^*$, τότε $(L_1\Sigma^*L_2)^* = \Sigma^*$.
(ε) Για κάθε γλώσσα L, $\emptyset L = L\emptyset = \emptyset$.

1.7.5. Να δώσετε μερικά παραδείγματα συμβολοσειρών που ανήκουν ή δεν ανήκουν στα παρακάτω σύνολα, όπου $\Sigma = \{a,b\}$.
(α) $\{w : \text{για κάποιο } u \in \Sigma\Sigma, w = uu^Ru\}$.
(β) $\{w : ww = www\}$.
(γ) $\{w : \text{για κάποια } u, v \in \Sigma^*, uvw = wvu\}$
(δ) $\{w : \text{για κάποιο } u \in \Sigma^*, www = uu\}$.

1.7.6. Κάτω από ποιες προϋποθέσεις είναι $L^+ = L^* - \{e\}$;

1.7.7. Ως προς ποιες σχέσεις είναι η Kleene star της γλώσσας L η κλειστότητα της L;

1.8 ΠΕΠΕΡΑΣΜΕΝΗ ΑΝΑΠΑΡΑΣΤΑΣΗ ΤΩΝ ΓΛΩΣΣΩΝ

Ένα κεντρικό θέμα στη θεωρία υπολογισμού είναι η αναπαράσταση των γλωσσών με πεπερασμένες περιγραφές. Βέβαια, κάθε πεπερασμένη γλώσσα μπορεί να περιγραφεί μέσω μιας πεπερασμένης αναπαράστασης, με εξαντλητική απαρίθμηση όλων των συμβολοσειρών της γλώσσας. Το θέμα αυτό αποτελεί πρόκληση μόνον όταν πρόκειται για άπειρες γλώσσες.

Ας γίνουμε κάπως πιο συγκεκριμένοι σχετικά με την έννοια της «πεπερασμένης αναπαράστασης μιας γλώσσας». Το πρώτο σημείο που πρέπει να τονιστεί είναι ότι κάθε τέτοια αναπαράσταση πρέπει να είναι και η ίδια μια συμβολοσειρά, μια πεπερασμένη ακολουθία συμβόλων ενός αλφαβήτου Σ. Έπειτα, θέλουμε οπωσδήποτε διαφορετικές γλώσσες να έχουν διαφορετικές αναπαραστάσεις, αλλιώς δεν θα ήταν κατάλληλος ο όρος *αναπαράσταση*. Αυτές οι δύο απαιτήσεις, όμως, ήδη υποδηλώνουν ότι οι δυνατότητες για πεπερασμένη αναπαράσταση μειώνονται σημαντικά. Εφόσον το σύνολο Σ^* των συμβολοσειρών ενός αλφαβήτου Σ είναι μετρήσιμα άπειρο, έτσι και ο αριθμός των αναπαραστάσεων των γλωσσών είναι μετρήσιμα άπειρος. (Αυτό θα ίσχυε ακόμα και αν δεν είμαστε αναγκασμένοι να χρησιμοποιήσουμε ένα συγκεκριμένο αλφάβη-