ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

Victor Shoup

Μια υπολογιστική εισαγωγή στη και την **θεωρία αριθμών άλγεβρα**

Επιμέλεια ελληνικής έκδοσης:
Γιώργος Στεφανίδης, Αναπλ. Καθηγητής Εφ. Πληροφορικής Πανεπ. Μακεδονίας

Περιεχόμενα

7

Πιθανοτικοί αλγόριθμοι

Μερικές φορές είναι χρήσιμο να δώσουμε στον αλγόριθμό μας τη δυνατότητα να παράγει τυχαίους αριθμούς. Για να απλοποιήσουμε τα πράγματα, θεωρούμε μόνο αλγορίθμους που παράγουν τυχαία bit. Από πού προέρχονται πραγματικά αυτά τα τυχαία bit δεν θα μας απασχολήσει και πολύ εδώ. Σε μια πρακτική υλοποίηση, θα χρησιμοποιούσε κάποιος μια ψευδοτυχαία γεννήτρια bit η οποία θα παρήγαγε bit τα οποία "για όλους τους πρακτικούς σκοπούς" θα ήταν "τόσο καλά όσο τα τυχαία". Ενώ υπάρχει μια καλά ανεπτυγμένη θεωρία της παραγωγής ψευδοτυχαίων bit (μέρος της οποίας θεμελιώνεται πάνω στις ιδέες της §6.9), δεν θα ασχοληθούμε εδώ με αυτή. Επιπλέον, οι ψευδοτυχαίες γεννήτριες bit που χρησιμοποιούνται στην πράξη, δεν βασίζονται σ' αυτή τη γενική θεωρία και είναι πολύ περισσότερο βασισμένες ειδικώς στη σχεδίαση. Έτσι, παρόλο που θα παρουσιάσουμε μια αυστηρή επίσημη θεωρία των πιθανοτικών αλγορίθμων, η εφαρμογή αυτής της θεωρίας στην πράξη είναι τελικά λιγάκι ευρετική.

7.1 Βασικοί ορισμοί

Μιλώντας τυπικά, θα προσθέσουμε ένα νέο τύπο εντολής στη μηχανή μας τυχαίας προσπέλασης (που περιγράψαμε στην §3.2):

τυχαίο bit (random bit) Αυτός ο τύπος εντολής (instruction) είναι της μορφής $\alpha \leftarrow \text{RANDOM}$, όπου το α παίρνει την ίδια μορφή όπως στις αριθμητικές εντολές. Η εκτέλεση αυτού του τύπου εντολής αναθέτει στο α μια τιμή που έχει επιλεγεί σαν δείγμα από την ομοιόμορφη κατανομή στο $\{0, 1\}$, ανεξάρτητα από την εκτέλεση όλων των άλλων εντολών τυχαίου bit.

Κατά την περιγραφή των αλγορίθμων σε ένα υψηλό επίπεδο, θα γράφουμε "$b \leftarrow_R \{0, 1\}$" για να συμβολίζουμε την ανάθεση ενός τυχαίου bit στη μεταβλητή b και "$s \leftarrow_R \{0, 1\}^{\times \ell}$" για να συμβολίζουμε την ανάθεση μιας τυχαίας δυαδικής συμβολοσειράς μήκους ℓ στη μεταβλητή s.

Κατά την περιγραφή της συμπεριφοράς ενός τέτοιου **πιθανοτικού** (probabilistic) ή **τυχαιοποιημένου** (randomized) αλγορίθμου A, για οποιαδήποτε δεδομένα εισόδου x, βλέπουμε το χρόνο εκτέλεσής του και την έξοδό του σαν τυχαίες μεταβλητές που συμβολίζονται με $T_A(x)$ και $A(x)$, αντιστοίχως. Ο **αναμενόμενος χρόνος εκτέλεσης** του A με είσοδο x ορίζεται ως η αναμενόμενη τιμή $\mathsf{E}[T_A(x)]$ της τυχαίας μεταβλητής $T_A(x)$. Σημειώστε ότι στον ορισμό του αναμενόμενου χρόνου εκτέλεσης, δεν θεωρούμε την *είσοδο* να επιλέγεται τυχαία από κάποια κατανομή πιθανότητας. Θα μπορούσε κάποιος, φυσικά, να ορίσει μια τέτοια έννοια· όμως, δεν είναι πάντα εύκολο να έχουμε μια κατανομή στο χώρο των δεδομένων εισόδου που να μοντελοποιεί ικανοποιητικά μια συγκεκριμένη κατάσταση του πραγματικού κόσμου. Δεν θα αναφερθούμε περισσότερο σ' αυτό το θέμα εδώ.

Λέμε ότι ένας πιθανοτικός αλγόριθμος A εκτελείται σε **αναμενόμενο πολυωνυμικό χρόνο** αν υπάρχουν σταθερές c, d τέτοιες ώστε για όλα τα $n \geq 0$ και όλες τις εισόδους x μήκους n, να έχουμε $\mathsf{E}[T_A(x)] \leq n^c + d$. Λέμε ότι ο A εκτελείται σε **αυστηρά πολυωνυμικό χρόνο** αν υπάρχουν σταθερές c, d τέτοιες ώστε για όλα τα n και όλες τις εισόδους x μήκους n, ο A *πάντα* τερματίζεται για είσοδο x μέσα σε χρόνο $n^c + d$, ανεξάρτητα από τις τυχαίες επιλογές του.

Το να ορίσουμε τις κατανομές των $T_A(x)$ και $A(x)$ είναι λίγο δύσκολο. Τα πράγματα είναι αρκετά απλά αν ο A τερματίζεται *πάντα* για είσοδο x μετά από ένα πεπερασμένο πλήθος βημάτων, ανεξάρτητα από τα αποτελέσματα των τυχαίων επιλογών του: σε αυτή την περίπτωση, μπορούμε φυσικά να δούμε τις $T_A(x)$ και $A(x)$ σαν τυχαίες μεταβλητές με ομοιόμορφη κατανομή πάνω σε δυαδικές συμβολοσειρές κάποιου συγκεκριμένου μήκους — μια τέτοια τυχαία δυαδική συμβολοσειρά μπορεί να χρησιμοποιηθεί σαν πηγή τυχαίων bit για τον αλγόριθμο. Όμως, αν δεν υπάρχει εκ των προτέρων φράγμα στο πλήθος των βημάτων, τα πράγματα γίνονται πιο σύνθετα: σκεφτείτε έναν αλγόριθμο που παράγει τυχαία bit, ένα κάθε φορά, μέχρι να παράγει, ας πούμε 1 bit — ακριβώς όπως στο Παράδειγμα 6.29, δεν προσπαθούμε να μοντελοποιήσουμε αυτό σαν μια κατανομή πιθανότητας στο μη μετρήσιμο σύνολο των άπειρων δυαδικών συμβολοσειρών, αλλά αντίθετα, ορίζουμε απευθείας μια κατάλληλη διακριτή κατανομή πιθανότητας που μοντελοποιεί την εκτέλεση του A με είσοδο x.

7.1.1 Ορισμός της κατανομής πιθανότητας

Προειδοποίηση στον αναγνώστη: *το υπόλοιπο αυτής της ενότητας είναι λίγο τεχνικό και μπορεί να θελήσετε να περάσετε στην §7.2 κατά την πρώτη ανάγνωση, αν είστε πρόθυμοι να εμπιστευτείτε τη διαίσθησή σας σχετικά με τους πιθανοτικούς αλγορίθμους.*

Για να δικαιολογήσουμε τον ορισμό μας, ο οποίος μπορεί αρχικά να φαίνεται λίγο περίεργος, θεωρούμε ξανά το Παράδειγμα 6.29. Θα μπορούσαμε να δούμε το δειγματικό χώρο εκείνου του παραδείγματος ως το σύνολο όλων των δυαδικών συμβολοσειρών αποτελούμενων από μηδέν ή περισσότερα 0 bit, ακολουθούμενα από ένα 1 bit και σε κάθε

τέτοια δυαδική συμβολοσειρά σ αυτής της ειδικής μορφής, να αναθέσουμε την πιθανότητα $2^{-|\sigma|}$, όπου $|\sigma|$ συμβολίζει το μήκος της σ. Το ″τυχαίο πείραμα″ που έχουμε στο μυαλό μας είναι να παράγουμε τυχαία bit, ένα κάθε φορά, μέχρι να παραχθεί μια από αυτές τις ειδικές συμβολοσειρές ″τερματισμού″. Κατά τη διατύπωση του ορισμού της κατανομής πιθανότητας ενός πιθανοτικού αλγορίθμου, απλά θεωρούμε πιο γενικά σύνολα από συμβολοσειρές ″τερματισμού″, καθορισμένα από τον αλγόριθμο και την είσοδό του.

Για να απλοποιήσουμε τα πράγματα, υποθέτουμε ότι η μηχανή παράγει μια σειρά από τυχαία bit, ένα με κάθε εντολή που εκτελείται και αν η εντολή τυχαίνει να είναι μια εντολή τυχαίου-bit, τότε αυτό είναι το bit που χρησιμοποιεί. Για μια δυαδική συμβολοσειρά σ, μπορούμε να εκτελέσουμε τον A με είσοδο x μέχρι $|\sigma|$ βήματα, χρησιμοποιώντας τη σ για το ρεύμα τυχαίων bit και παρατηρούμε τη συμπεριφορά του αλγορίθμου. Ο αναγνώστης μπορεί να θέλει να απεικονίσει τη σ σαν μια πεπερασμένη διαδρομή σε ένα άπειρο δυαδικό δέντρο, όπου η εκκίνηση γίνεται από τη ρίζα, με μια διακλάδωση προς τα αριστερά αν το επόμενο bit της σ είναι 0 και μια διακλάδωση προς τα δεξιά αν το επόμενο bit της σ είναι ένα 1 bit. Σε αυτά τα πλαίσια, καλούμε τη σ **διαδρομή εκτέλεσης** (execution path). Κάποια επιπλέον ορολογία θα είναι χρήσιμη:

- Αν ο A τερματίζεται σε $|\sigma|$ το πολύ βήματα, τότε καλούμε τη σ **πλήρη διαδρομή εκτέλεσης**·
- αν ο A τερματίζεται σε $|\sigma|$ ακριβώς βήματα, τότε καλούμε τη σ **ακριβή διαδρομή εκτέλεσης**·
- αν ο A δεν τερματίζεται σε λιγότερα από $|\sigma|$ βήματα, τότε καλούμε τη σ **μερική διαδρομή εκτέλεσης**.

Ο δειγματικός χώρος $\mathcal{S}$ της κατανομής πιθανότητας που σχετίζεται με τον A με είσοδο x αποτελείται από όλες τις *ακριβείς* διαδρομές εκτέλεσης. Προφανώς, ο $\mathcal{S}$ είναι **ελεύθερος προθέματος** (prefix free)· δηλαδή, καμιά συμβολοσειρά στον $\mathcal{S}$ δεν είναι ένα γνήσιο πρόθεμα μιας άλλης.

Θεώρημα 7.1. *Αν $\mathcal{S}$ είναι ένα ελεύθερο προθέματος σύνολο δυαδικών συμβολοσειρών, τότε* $\sum_{\sigma\in\mathcal{S}} 2^{-|\sigma|} \le 1$.

Απόδειξη. Αρχικά ισχυριζόμαστε ότι το θεώρημα ισχύει για κάθε πεπερασμένο ελεύθερο προθέματος σύνολο $\mathcal{S}$. Μπορούμε να υποθέσουμε ότι το $\mathcal{S}$ είναι μη κενό, διότι διαφορετικά, ο ισχυρισμός είναι τετριμμένος. Αποδεικνύουμε τον ισχυρισμό με επαγωγή στο άθροισμα των μηκών των στοιχείων του $\mathcal{S}$. Η βασική περίπτωση είναι όταν το $\mathcal{S}$ περιέχει μόνο την κενή συμβολοσειρά, στην οποία περίπτωση ο ισχυρισμός είναι προφανής. Αν το $\mathcal{S}$ περιέχει μη κενές συμβολοσειρές, έστω τ μια συμβολοσειρά του $\mathcal{S}$ μέγιστου μήκους και έστω τ' το πρόθεμα μήκους $|\tau| - 1$ της τ. Τώρα, αφαιρέστε από το $\mathcal{S}$ όλες τις συμβολοσειρές που έχουν το τ' σαν πρόθεμα (υπάρχουν μία ή δύο τέτοιες συμβολοσειρές) και προ-

σθέστε στο $\mathcal{S}$ τη συμβολοσειρά τ'. Είναι εύκολο να δούμε (επαληθεύστε) ότι το σύνολο $\mathcal{S}'$ που παίρνουμε σαν αποτέλεσμα είναι επίσης ελεύθερο προθέματος και ότι

$$\sum_{\sigma\in\mathcal{S}} 2^{-|\sigma|} \le \sum_{\sigma\in\mathcal{S}'} 2^{-|\sigma|}.$$

Ο ισχυρισμός τώρα προκύπτει με επαγωγή.

Για τη γενική περίπτωση, έστω σ_1, σ_2, … μια συγκεκριμένη απαρίθμηση του $\mathcal{S}$ και θεωρούμε τα μερικά αθροίσματα $S_i = \sum_{j=1}^{i} 2^{-|\sigma_j|}$ για $i = 1, 2, \ldots$. Από τον παραπάνω ισχυρισμό, καθένα από αυτά τα μερικά αθροίσματα είναι το πολύ 1, από το οποίο έπεται ότι $\lim_{i\to\infty} S_i \le 1$. □

Από το παραπάνω θεώρημα, αν $\mathcal{S}$ είναι ένας δειγματικός χώρος που σχετίζεται με τον αλγόριθμο A με είσοδο x, έχουμε

$$S := \sum_{\sigma\in\mathcal{S}} 2^{-|\sigma|} \le 1 .$$

Υποθέτουμε ότι $S = 1$. Τότε λέμε ότι ο A **τερματίζεται με πιθανότητα** 1 **για είσοδο** x και ορίζουμε την κατανομή $\mathbf{D}_{A,x}$ που σχετίζεται με τον A με είσοδο x να είναι η κατανομή στο $\mathcal{S}$ που αναθέτει την πιθανότητα $2^{-|\sigma|}$ σε κάθε δυαδική συμβολοσειρά $\sigma \in \mathcal{S}$. Ορίζουμε επίσης τις $T_A(x)$ και $A(x)$ σαν τυχαίες μεταβλητές στην κατανομή $\mathbf{D}_{A,x}$ με το φυσικό τρόπο: για κάθε $\sigma \in \mathcal{S}$, ορίζουμε την $T_A(x)$ να είναι $|\sigma|$ και την $A(x)$ να είναι η έξοδος που παράγεται από τον A με είσοδο x χρησιμοποιώντας τη σ να οδηγεί την εκτέλεσή του.

Όλοι οι παραπάνω ορισμοί υπέθεσαν ότι ο A τερματίζεται με πιθανότητα 1 για είσοδο x και όντως, θα ενδιαφερθούμε μόνο για αλγορίθμους που τερματίζουν με πιθανότητα 1 για όλες τις εισόδους. Όμως, για να αναλύσουμε έναν δεδομένο αλγόριθμο, πρέπει ακόμη να αποδείξουμε ότι τερματίζεται με πιθανότητα 1 για όλες τις εισόδους πριν χρησιμοποιήσουμε αυτούς τους ορισμούς και να εξασκήσουμε όλα τα μέσα της θεωρίας της διακριτής πιθανότητας. Τέλος, είναι χρήσιμο να μελετήσουμε διάφορες κατανομές πεπερασμένης πιθανότητας που σχετίζονται με την εκτέλεση του A με είσοδο x. Για κάθε ακέραιο $k \ge 0$, ας θεωρήσουμε την ομοιόμορφη κατανομή στις δυαδικές συμβολοσειρές μήκους k και για κάθε $j = 0, \ldots, k$, ορίζουμε το $\mathcal{H}_j^{(k)}$ να είναι το ενδεχόμενο ότι μια τέτοια τυχαία k-bit συμβολοσειρά έχει σαν αποτέλεσμα ο A με είσοδο x να τερματίζεται μέσα σε j βήματα.

Παραθέτουμε ορισμένες παρατηρήσεις. Πρώτον, αν $\mathcal{S}$ είναι το σύνολο όλων των ακριβών διαδρομών εκτέλεσης του A με είσοδο x, τότε έχουμε (επαληθεύστε)

$$\mathsf{P}[\mathcal{H}_j^{(k)}] = \sum_{\substack{\sigma\in\mathcal{S}\\ |\sigma|\le j}} 2^{-|\sigma|} .$$

Από αυτό προκύπτει ότι για όλους τους μη αρνητικούς ακεραίους j, k, k' με $j \le \min\{k, k'\}$, έχουμε

$$\mathsf{P}[\mathcal{H}_j^{(k)}] = \mathsf{P}[\mathcal{H}_j^{(k')}].$$

Ορίζοντας $H_k := \mathsf{P}[\mathcal{H}_k^{(k)}]$, προκύπτει επίσης ότι η ακολουθία $\{H_k\}_{k\geq 0}$ είναι μη-φθίνουσα και άνω φραγμένη από το 1, και ότι ο A τερματίζεται με πιθανότητα 1 για είσοδο x, αν και μόνο αν

$$\lim_{k\to\infty} H_k = 1.$$

Μια απλή αναγκαία συνθήκη για το σταμάτημα με πιθανότητα 1 για δοθείσα είσοδο είναι ότι για όλες τις μερικές διαδρομές εκτέλεσης, υπάρχει κάποια επέκταση που είναι μια ολοκληρωμένη διαδρομή εκτέλεσης. Διαισθητικά, αν αυτό δεν ισχύει, τότε με κάποια μη-μηδενική πιθανότητα, ο αλγόριθμος πέφτει σε έναν ατέρμονα βρόχο. Πιο επίσημα, αν υπάρχει μια μερική διαδρομή εκτέλεσης μήκους j που δεν μπορεί να επεκταθεί σε μια ολοκληρωμένη διαδρομή εκτέλεσης, τότε για όλα τα $k \geq j$ έχουμε

$$H_k \leq 1 - 2^{-j}.$$

Αυτό, όμως, δεν εγγυάται το σταμάτημα με πιθανότητα 1. Μια απλή ικανή συνθήκη είναι η εξής:

> *Υπάρχει ένα φράγμα ℓ (ενδεχομένως εξαρτώμενο από την είσοδο) τέτοιο, ώστε για κάθε μερική διαδρομή εκτέλεσης σ, να υπάρχει μια πλήρης διαδρομή εκτέλεσης που επεκτείνει την σ και της οποίας το μήκος είναι το πολύ $|\sigma| + \ell$.*

Για να δούμε γιατί αυτή η συνθήκη συνεπάγεται ότι ο A τερματίζεται με πιθανότητα 1, παρατηρούμε ότι αν ο A εκτελείται για $k\ell$ βήματα χωρίς να τερματίζεται, τότε η πιθανότητα ότι δεν τερματίζεται μέσα σε $(k + 1)\ell$ βήματα είναι το πολύ $1 - 2^{-\ell}$. Πιο επίσημα, ας ορίσουμε $\bar{H}_k := 1 - H_k$ και σημειώστε ότι για όλα τα $k \geq 0$, έχουμε

$$\begin{aligned}
\bar{H}_{(k+1)\ell} &= \mathsf{P}[\bar{\mathcal{H}}_{(k+1)\ell}^{((k+1)\ell)} \mid \bar{\mathcal{H}}_{k\ell}^{((k+1)\ell)}] \cdot \mathsf{P}[\bar{\mathcal{H}}_{k\ell}^{((k+1)\ell)}] \\
&\leq (1 - 2^{-\ell})\mathsf{P}[\bar{\mathcal{H}}_{k\ell}^{((k+1)\ell)}] \\
&= (1 - 2^{-\ell})\bar{H}_{k\ell}
\end{aligned}$$

και συνεπώς (με επαγωγή στο k), έχουμε

$$\bar{H}_{k\ell} \leq (1 - 2^{-\ell})^k,$$

από το οποίο προκύπτει ότι

$$\lim_{k\to\infty} H_k = 1.$$

Είναι συνήθως αρκετά απλό να επαληθεύσουμε την ιδιότητα αυτή για έναν συγκεκριμένο αλγόριθμο "δια παρατηρήσεως".

***Παράδειγμα* 7.1.** Θεωρούμε τον εξής αλγόριθμο:

repeat
  $b \leftarrow_R \{0, 1\}$
until $b = 1$

Αφού κάθε βρόχος είναι απλά ένα σταθερό πλήθος εντολών και αφού υπάρχει περίπτωση να τερματίζεται με κάθε επανάληψη του βρόχου, ο αλγόριθμος τερματίζεται με πιθανότητα 1. □

***Παράδειγμα* 7.2.** Θεωρούμε τον εξής αλγόριθμο:

$i \leftarrow 0$
repeat
  $i \leftarrow i + 1$
  $s \leftarrow_R \{0,1\}^{\times i}$
until $s = 0^{\times i}$

Για θετικό ακέραιο n, θεωρούμε την πιθανότητα p_n της εκτέλεσης τουλάχιστον n επαναλήψεων βρόχου (κάθε p_n ορίζεται χρησιμοποιώντας μια κατάλληλη πεπερασμένη κατανομή πιθανότητας). Έχουμε

$$p_n = \prod_{i=1}^{n-1}(1-2^{-i}) \geq \prod_{i=1}^{n-1} e^{-2^{-i+1}} = e^{-\sum_{i=0}^{n-2} 2^{-i}} \geq e^{-2},$$

όπου έχουμε κάνει χρήση της εκτίμησης (iii) της §A1. Αφού η p_n δεν τείνει στο μηδέν καθώς $n \to \infty$, μπορούμε να συμπεράνουμε ότι ο αλγόριθμος δεν τερματίζεται με πιθανότητα 1.

Σημειώστε ότι κάθε μερική διαδρομή εκτέλεσης μπορεί να επεκταθεί σε πλήρη διαδρομή εκτέλεσης, αλλά το μήκος της επέκτασης δεν είναι φραγμένο. □

Οι παρακάτω τρεις ασκήσεις αναπτύσσουν εργαλεία τα οποία απλοποιούν την ανάλυση των πιθανοτικών αλγορίθμων.

ΑΣΚΗΣΗ 7.1. Θεωρούμε έναν πιθανοτικό αλγόριθμο A που τερματίζεται με πιθανότητα 1 για είσοδο x και θεωρούμε την κατανομή πιθανότητας $\mathbf{D}_{A,x}$ στο σύνολο $\mathcal{S}$ των ακριβών διαδρομών εκτέλεσης. Έστω τ μια σταθερή, μερική διαδρομή εκτέλεσης και έστω $\mathcal{B} \subseteq \mathcal{S}$ το ενδεχόμενο που αποτελείται από όλες τις ακριβείς διαδρομές εκτέλεσης που επεκτείνουν την τ. Δείξτε ότι $\mathsf{P}[\mathcal{B}] = 2^{-|\tau|}$.

ΑΣΚΗΣΗ 7.2. Θεωρούμε έναν πιθανοτικό αλγόριθμο A που τερματίζεται με πιθανότητα 1 για είσοδο x και θεωρούμε την κατανομή πιθανότητας $\mathbf{D}_{A,x}$ στο σύνολο $\mathcal{S}$ των ακριβών

διαδρομών εκτέλεσης. Για μια δυαδική συμβολοσειρά σ και έναν ακέραιο $k \geq 0$, έστω ότι με $\{\sigma\}_k$ συμβολίζουμε την τιμή της σ αποκομμένη στα πρώτα k bit. Υποθέτουμε ότι $\mathcal{B} \subseteq \mathcal{S}$ είναι ένα ενδεχόμενο της μορφής

$$\mathcal{B} = \{\sigma \in \mathcal{S} : \phi(\{\sigma\}_k)\}$$

για κάποιο κατηγόρημα ϕ και κάποιον ακέραιο $k \geq 0$. Διαισθητικά, αυτό σημαίνει ότι το $\mathcal{B}$ είναι τελείως προσδιορισμένο από τα πρώτα k bit της διαδρομής εκτέλεσης. Τώρα θεωρούμε την ομοιόμορφη κατανομή στο $\{0,1\}^{\times k}$. Ας ορίσουμε ένα ενδεχόμενο $\mathcal{B}'$ σε αυτή την κατανομή ως εξής. Για $\sigma \in \{0,1\}^{\times k}$, ας εκτελέσουμε τον A με είσοδο x χρησιμοποιώντας τη διαδρομή εκτέλεσης σ για k βήματα ή μέχρι ο A να τερματίσει (όποιο από τα δύο συμβεί πρώτο). Αν το πλήθος των βημάτων που θα εκτελεστούν είναι t (όπου $t \leq k$), τότε βάζουμε τη σ στο $\mathcal{B}'$, αν και μόνο αν $\phi(\{\sigma\}_t)$. Δείξτε ότι η πιθανότητα ότι το ενδεχόμενο $\mathcal{B}$ πραγματοποιείται (ως προς την κατανομή $\mathbf{D}_{A,x}$) είναι η ίδια με την πιθανότητα ότι το $\mathcal{B}'$ πραγματοποιείται (ως προς την ομοιόμορφη κατανομή $\{0,1\}^{\times k}$). Υπόδειξη: χρησιμοποιήστε την Άσκηση 7.1.

Η παραπάνω άσκηση είναι πολύ χρήσιμη στην απλοποίηση της ανάλυσης των πιθανοτικών αλγορίθμων. Τυπικά, μπορεί κάποιος να ανάγει την ανάλυση ενός ενδεχομένου που μας ενδιαφέρει στην ανάλυση μιας συλλογής ενδεχομένων, καθένα από τα οποία προσδιορίζεται από τα πρώτα k bit της διαδρομής εκτέλεσης για κάποιο σταθερό k. Η πιθανότητα ενός ενδεχομένου το οποίο προσδιορίζεται από τα πρώτα k bit της διαδρομής εκτέλεσης μπορεί μετά να υπολογιστεί αναλύοντας τη συμπεριφορά του αλγορίθμου σε μια τυχαία k-bit διαδρομή εκτέλεσης.

ΑΣΚΗΣΗ 7.3. Υποθέτουμε ότι ο αλγόριθμος A καλεί τον αλγόριθμο B σαν μια υπορουτίνα. Στην κατανομή πιθανότητας $\mathbf{D}_{A,x}$, θεωρούμε μια συγκεκριμένη μερική διαδρομή εκτέλεσης τ που οδηγεί τον A σε ένα σημείο όπου ο A καλεί τον αλγόριθμο B με μια συγκεκριμένη είσοδο y (καθορισμένη από τα x και τ). Θεωρούμε τη δεσμευμένη κατανομή πιθανότητας με δεδομένο ότι τ είναι ένα πρόθεμα της πραγματικής διαδρομής εκτέλεσης του A. Μπορούμε να ορίσουμε μια τυχαία μεταβλητή X σε αυτή τη δεσμευμένη κατανομή της οποίας η τιμή είναι η υποδιαδρομή που ακολουθείται από την κλήση της υπορουτίνας B. Δείξτε ότι η κατανομή της X είναι η ίδια με την $\mathbf{D}_{B,y}$. Υπόδειξη: χρησιμοποιήστε την Άσκηση 7.1.

Η παραπάνω άσκηση είναι επίσης πολύ χρήσιμη στην απλοποίηση της ανάλυσης των πιθανοτικών αλγορίθμων, με το ότι μας επιτρέπει να αναλύσουμε μια υπορουτίνα απομονωμένη και να χρησιμοποιήσουμε τα αποτελέσματα στην ανάλυση ενός αλγορίθμου που καλεί την υπορουτίνα αυτή.

ΑΣΚΗΣΗ 7.4. Έστω A ένας πιθανοτικός αλγόριθμος και για μια είσοδο x και ακέραιο $k \geq 0$, θεωρούμε το πείραμα στο οποίο επιλέγουμε μια τυχαία διαδρομή εκτέλεσης μήκους k και εκτελούμε τον A με είσοδο x μέχρι k βήματα χρησιμοποιώντας την επιλεγμένη δια-

δρομή εκτέλεσης. Αν ο A τερματίζεται μέσα σε k βήματα, ορίζουμε $A_k(x)$ να είναι η έξοδος που παράγεται από τον A και $T_{A_k}(x)$ να είναι το πραγματικό πλήθος βημάτων που εκτελούνται από τον A· διαφορετικά, ορίζουμε $A_k(x)$ να είναι η διακεκριμένη τιμή "$\perp$" και $T_{A_k}(x)$ να είναι ο k.

(α) Δείξτε ότι αν ο A τερματίζεται με πιθανότητα 1 για είσοδο x, τότε για όλες τις δυνατές εξόδους y,

$$\mathsf{P}[A(x) = y] = \lim_{k\to\infty} \mathsf{P}[A_k(x) = y] .$$

(β) Δείξτε ότι αν ο A τερματίζεται με πιθανότητα 1 για είσοδο x, τότε

$$\mathsf{E}[T_A(x)] = \lim_{k\to\infty} \mathsf{E}[T_{A_k}(x)] .$$

ΑΣΚΗΣΗ 7.5. Μπορεί κάποιος να γενικεύσει την έννοια μιας διακριτής, στοχαστικής διαδικασίας, ως εξής. Έστω Γ ένα πεπερασμένο ή μετρήσιμα άπειρο σύνολο. Έστω f μια συνάρτηση που απεικονίζει ακολουθίες ενός ή περισσοτέρων στοιχείων του Γ στο [0, 1], έτσι ώστε να ισχύει η παρακάτω ιδιότητα:

> για όλες τις πεπερασμένες ακολουθίες $(\gamma_1, \ldots, \gamma_{i-1})$, όπου $i \geq 1$, η $f(\gamma_1, \ldots, \gamma_{i-1}, \gamma)$ είναι μη μηδενική για το πολύ ένα πεπερασμένο πλήθος από $\gamma \in \Gamma$ και
>
> $$\sum_{\gamma\in\Gamma} f(\gamma_1,\ldots,\gamma_{i-1},\gamma) = 1.$$

Θεωρούμε τώρα ένα ελεύθερο προθέματος σύνολο $\mathcal{S}$ των πεπερασμένων ακολουθιών στοιχείων του Γ. Για $\sigma = (\gamma_1, \ldots, \gamma_n) \in \mathcal{S}$, ορίζουμε

$$\mathsf{P}[\sigma] := \prod_{i=1}^{n} f(\gamma_1,\ldots,\gamma_i) .$$

Δείξτε ότι $\sum_{\sigma\in\mathcal{S}} \mathsf{P}[\sigma] \leq 1$. Έτσι μπορούμε να ορίσουμε μια κατανομή πιθανότητας στο $\mathcal{S}$ χρησιμοποιώντας τη συνάρτηση πιθανότητας $\mathsf{P}[\cdot]$ αν αυτό το άθροισμα είναι 1. Η ιδέα είναι ότι μοντελοποιούμε μια διαδικασία κατά την οποία αρχίζουμε με "κενή" διαμόρφωση (configuration)· σε κάθε βήμα, αν είμαστε στη διαμόρφωση $(\gamma_1, \ldots, \gamma_{i-1})$, τερματίζουμε αν αυτή είναι μια διαμόρφωση "τερματισμού", δηλαδή ένα στοιχείο του $\mathcal{S}$ και διαφορετικά, προχωράμε στη διαμόρφωση $(\gamma_1, \ldots, \gamma_{i-1}, \gamma)$ με πιθανότητα $f(\gamma_1, \ldots, \gamma_{i-1}, \gamma)$.

7.2 Προσέγγιση συναρτήσεων

Υποθέτουμε ότι f είναι μια συνάρτηση που απεικονίζει δυαδικές συμβολοσειρές σε δυαδικές συμβολοσειρές. Μπορεί να έχουμε έναν αλγόριθμο A που **υπολογίζει προσεγγιστικά** την f

με την εξής έννοια: υπάρχει μια σταθερά ϵ, με $0 \leq \epsilon < 1/2$, τέτοια, ώστε για όλες τις εισόδους x, $\mathsf{P}[A(x) = f(x)] \geq 1 - \epsilon$. Η τιμή ϵ είναι ένα φράγμα στην **πιθανότητα σφάλματος** η οποία ορίζεται ως $\mathsf{P}[A(x) \neq f(x)]$.

7.2.1 Ελάττωση της πιθανότητας σφάλματος

Υπάρχει ένα καθιερωμένο "τρικ" με το οποίο μπορεί κάποιος να κάνει την πιθανότητα σφάλματος πολύ μικρή· δηλαδή, εκτελεί τον A με είσοδο x ένα πλήθος, ας πούμε, t φορών και παίρνει την πλειοψηφούσα έξοδο σαν απάντηση. Χρησιμοποιώντας το φράγμα Chernoff (Θεώρημα 6.13), η πιθανότητα σφάλματος για την επαναλαμβανόμενη εκδοχή του A είναι φραγμένη από το $\exp[-(1/2 - \epsilon)^2 t/2]$ και έτσι η πιθανότητα σφάλματος μειώνεται εκθετικά ως προς το πλήθος των επαναλήψεων. Αυτό το φράγμα παράγεται ως εξής. Για $i = 1, \ldots, t$, έστω X_i μια τυχαία μεταβλητή που αναπαριστά το αποτέλεσμα της i-οστής επανάληψης του A· ακριβέστερα, $X_i = 1$ αν $A(x) \neq f(x)$ στην i-οστή επανάληψη και $X_i = 0$, διαφορετικά. Έστω ϵ_x η πιθανότητα ότι $A(x) \neq f(x)$. Η πιθανότητα ότι η πλειοψηφούσα έξοδος είναι εσφαλμένη είναι ίση με την πιθανότητα ότι ο μέσος δείγματος των $X_1, \ldots, X_t$ υπερβαίνει τον μέσο ϵ_x τουλάχιστον κατά $1/2 - \epsilon_x$. Το τμήμα (i) του Θεωρήματος 6.13 λέει ότι αυτό συμβαίνει με πιθανότητα το πολύ

$$\exp\left[\frac{-(1/2 - \epsilon_x)^2 t}{2(1 - \epsilon_x)}\right] \leq \exp\left[\frac{-(1/2 - \epsilon)^2 t}{2}\right].$$

7.2.2 Αυστηρά πολυωνυμικός χρόνος

Αν έχουμε έναν αλγόριθμο A που εκτελείται σε αναμενόμενο πολυωνυμικό χρόνο και ο οποίος υπολογίζει προσεγγιστικά μια συνάρτηση f, τότε μπορούμε εύκολα να τον μετατρέψουμε σε έναν νέο αλγόριθμο A' που εκτελείται σε *αυστηρά* πολυωνυμικό χρόνο και επίσης, προσεγγίζει την f, ως εξής. Υποθέτουμε ότι $\epsilon < 1/2$ είναι ένα φράγμα στην πιθανότητα σφάλματος και $T(n)$ είναι ένα πολυωνυμικό φράγμα στον αναμενόμενο χρόνο εκτέλεσης για εισόδους μήκους n. Τότε ο A' εκτελεί τον A για το πολύ $tT(n)$ βήματα, όπου t είναι μια σταθερά επιλεγμένη έτσι ώστε $\epsilon + 1/t < 1/2$ — αν ο A δεν τερματίζεται μέσα σ' αυτό το φράγμα χρόνου, τότε ο A' απλά τερματίζεται με μια αυθαίρετη έξοδο. Η πιθανότητα ότι ο A' σφάλλει είναι το πολύ η πιθανότητα ότι ο A σφάλλει συν την πιθανότητα ότι ο A εκτελείται για περισσότερα από $tT(n)$ βήματα. Από την ανισότητα του Markov (Θεώρημα 6.11), η τελευταία πιθανότητα είναι το πολύ $1/t$ και συνεπώς ο A' προσεγγίζει την f επίσης, αλλά με μια πιθανότητα σφάλματος φραγμένη από το $\epsilon + 1/t$.

7.2.3 Αναγνώριση Lagrange

Μια σημαντική ειδική περίπτωση προσεγγιστικού υπολογισμού συνάρτησης είναι όταν η έξοδος της συνάρτησης f είναι 0 ή 1 (ή ισοδύναμα *false* ή *true*). Στην περίπτωση αυτή, μπορούμε να δούμε την f σαν τη χαρακτηριστική συνάρτηση της γλώσσας $L := \{x : f(x) = 1\}$. (Είναι παράδοση της θεωρίας της υπολογιστικής πολυπλοκότητας να καλούμε ″γλώσσες″ σύνολα δυαδικών συμβολοσειρών.) Υπάρχουν διάφορες «αποχρώσεις» πιθανοτικών αλγορίθμων για τον προσεγγιστικό υπολογισμό της χαρακτηριστικής συνάρτησης f μιας γλώσσας L που θεωρούνται παραδοσιακά — για τους σκοπούς αυτών των ορισμών, μπορούμε να περιοριστούμε στους αλγορίθμους που έχουν έξοδο 0 ή 1:

- Καλούμε έναν πιθανοτικό αλγόριθμο αναμενόμενου πολυωνυμικού χρόνου, **αλγόριθμο Atlantic City** για την αναγνώριση της L αν υπολογίζει προσεγγιστικά την f με πιθανότητα σφάλματος φραγμένη από μια σταθερά $\epsilon < 1/2$.
- Καλούμε έναν πιθανοτικό αλγόριθμο αναμενόμενου πολυωνυμικού χρόνου, **αλγόριθμο Monte Carlo** για την αναγνώριση της L αν για κάποια σταθερά $\delta > 0$, έχουμε:
  - για κάθε $x \in L$, $\mathsf{P}[A(x) = 1] \geq \delta$ και
  - για κάθε $x \notin L$, $\mathsf{P}[A(x) = 1] = 0$.
- Καλούμε έναν πιθανοτικό αλγόριθμο αναμενόμενου πολυωνυμικού χρόνου, **αλγόριθμο Las Vegas** για την αναγνώριση της L αν υπολογίζει την f σωστά για όλες τις εισόδους x.

Λέει επίσης κάποιος ότι ένας αλγόριθμος Atlantic City έχει **αμφίπλευρο σφάλμα** (two-sided error), ένας αλγόριθμος Monte Carlo έχει **μονόπλευρο σφάλμα** (one-sided error) και ένας αλγόριθμος Las Vegas έχει **μηδενικό-πλευρο σφάλμα** (zero-sided error).

ΑΣΚΗΣΗ 7.6. Δείξτε ότι κάθε γλώσσα που αναγνωρίζεται από έναν αλγόριθμο Las Vegas, αναγνωρίζεται επίσης από έναν αλγόριθμο Monte Carlo και ότι κάθε γλώσσα που αναγνωρίζεται από έναν αλγόριθμο Monte Carlo, αναγνωρίζεται επίσης από έναν αλγόριθμο Atlantic City.

ΑΣΚΗΣΗ 7.7. Δείξτε ότι αν η L αναγνωρίζεται από έναν αλγόριθμο Atlantic City που εκτελείται σε αναμενόμενο πολυωνυμικό χρόνο, τότε αναγνωρίζεται από έναν αλγόριθμο Atlantic City που εκτελείται σε αυστηρά πολυωνυμικό χρόνο και του οποίου η πιθανότητα σφάλματος είναι το πολύ 2^{-n} με δεδομένα εισόδου μήκους n.

ΑΣΚΗΣΗ 7.8. Δείξτε ότι αν η L αναγνωρίζεται από έναν αλγόριθμο Monte Carlo που εκτελείται σε αναμενόμενο πολυωνυμικό χρόνο, τότε αναγνωρίζεται από έναν αλγόριθμο Monte Carlo που εκτελείται σε αυστηρά πολυωνυμικό χρόνο και του οποίου η πιθανότητα σφάλματος είναι το πολύ 2^{-n} με δεδομένα εισόδου μήκους n.

ΑΣΚΗΣΗ 7.9. Δείξτε ότι μια γλώσσα αναγνωρίζεται από έναν αλγόριθμο Las Vegas, αν και μόνο αν η γλώσσα και το συμπλήρωμά της αναγνωρίζονται από αλγορίθμους Monte Carlo.

ΑΣΚΗΣΗ 7.10. Δείξτε ότι αν μια γλώσσα αναγνωρίζεται από έναν αλγόριθμο Las Vegas που εκτελείται σε αυστηρά πολυωνυμικό χρόνο, τότε η L μπορεί να αναγνωρίζεται σε ντετερμινιστικό πολυωνυμικό χρόνο.

ΑΣΚΗΣΗ 7.11. Υποθέτουμε ότι για μια δεδομένη γλώσσα L, υπάρχει πιθανοτικός αλγόριθμος A που εκτελείται σε αναμενόμενο πολυωνυμικό χρόνο και πάντα έχει έξοδο 0 ή 1. Επιπλέον, υποθέτουμε ότι για κάποιες σταθερές α και c, όπου

- α είναι ένας ρητός αριθμός με $0 \leq \alpha < 1$, και
- c είναι ένας θετικός ακέραιος,

και για όλους τους αρκούντως μεγάλους n και όλα τα δεδομένα εισόδου x μήκους n, έχουμε

- αν $x \notin L$, τότε $\mathsf{P}[A(x) = 1] \leq \alpha$, και
- αν $x \in L$, τότε $\mathsf{P}[A(x) = 1] \geq \alpha + 1/n^c$.

(α) Δείξτε ότι υπάρχει αλγόριθμος Atlantic City για την L.

(β) Δείξτε ότι αν $\alpha = 0$, τότε υπάρχει αλγόριθμος Monte Carlo για την L.

7.3 Ρίψη νομίσματος μέχρι να εμφανιστεί κορώνα

Σε αυτή και τις επόμενες ενότητες του κεφαλαίου αυτού εξετάζουμε ένα πλήθος συγκεκριμένων πιθανοτικών αλγορίθμων.

Ας αρχίσουμε με τον εξής απλό αλγόριθμο (ο οποίος ήδη παρουσιάστηκε στο Παράδειγμα 7.1) που ουσιαστικά ρίχνει ένα νόμισμα μέχρι να εμφανιστεί κορώνα:

repeat
    $b \leftarrow_R \{0, 1\}$
until $b = 1$

Έστω X μια τυχαία μεταβλητή που αναπαριστά το πλήθος των επαναλήψεων βρόχου που κάνει ο αλγόριθμος. Θα πρέπει να είναι αρκετά εμφανές ότι η X έχει γεωμετρική κατανομή, όπου η σχετική πιθανότητα επιτυχίας είναι 1/2 (βλ. Παράδειγμα 6.30). Όμως, ας παράγουμε αυτό το γεγονός από πιο βασικές αρχές. Ορίζουμε τυχαίες μεταβλητές $B_1, B_2, \ldots$, όπου B_i αναπαριστά την τιμή του bit που ανατέθηκε στο b στην i-οστή επανάληψη του βρόχου, αν $X \geq i$ και $\star$ διαφορετικά. Είναι φανερό ότι ακριβώς ένα B_i θα πάρει την τιμή 1, στην οποία περίπτωση η X παίρνει την τιμή i.

Προφανώς, για κάθε $i \geq 1$, αν ο αλγόριθμος στην πραγματικότητα εισέρχεται στην i-οστή επανάληψη του βρόχου, τότε η B_i κατανέμεται ομοιόμορφα πάνω στο $\{0, 1\}$ και διαφορετικά $B_i = \star$. Δηλαδή:

$$\mathsf{P}[B_i = 0 \mid X \geq i] = 1/2, \ \mathsf{P}[B_i = 1 \mid X \geq i] = 1/2,$$

$$\mathsf{P}[B_i = \star \mid X < i] = 1.$$

Από αυτό βλέπουμε ότι

$$\mathsf{P}[X \geq 1] = 1, \mathsf{P}[X \geq 2] = \mathsf{P}[B_1 = 0 \mid X \geq 1]\mathsf{P}[X \geq 1] = 1/2,$$

$$\mathsf{P}[X \geq 3] = \mathsf{P}[B_2 = 0 \mid X \geq 2]\mathsf{P}[X \geq 2] = (1/2)(1/2) = 1/4,$$

και με επαγωγή στο i βλέπουμε ότι

$$\mathsf{P}[X \geq i] = \mathsf{P}[B_{i-1} = 0 \mid X \geq i - 1]\mathsf{P}[X \geq i - 1] = (1/2)(1/2^{i-2}) = 1/2^{i-1},$$

από το οποίο προκύπτει (βλ. Άσκηση 6.54) ότι η X έχει γεωμετρική κατανομή με σχετική πιθανότητα επιτυχίας 1/2.

Τώρα θεωρούμε την αναμενόμενη τιμή $\mathsf{E}[X]$. Από όσα είπαμε στο Παράδειγμα 6.35, έχουμε $\mathsf{E}[X] = 2$. Αν Y συμβολίζει το συνολικό χρόνο εκτέλεσης του αλγορίθμου, τότε $Y \leq cX$ για κάποια σταθερά c και συνεπώς

$$\mathsf{E}[Y] \leq c\mathsf{E}[X] = 2c$$

και καταλήγουμε ότι ο αναμενόμενος χρόνος εκτέλεσης του αλγορίθμου είναι μια σταθερά, η ακριβής τιμή της οποίας εξαρτάται από τις λεπτομέρειες της υλοποίησης.

[Οι αναγνώστες που προσπέρασαν την §7.1.1 μπορεί να θέλουν να προσπεράσουν και την παράγραφο αυτή.] Όπως είπαμε στο Παράδειγμα 7.1, ο παραπάνω αλγόριθμος τερματίζεται με πιθανότητα 1. Για να κάνουμε το παραπάνω επιχείρημα τελείως αυστηρό, θα πρέπει τυπικά να δικαιολογήσουμε τον ισχυρισμό ότι η δεσμευμένη κατανομή της B_i, με δεδομένο ότι $X \geq i$, είναι ομοιόμορφη στο $\{0, 1\}$. Δεν θέλουμε να υποθέσουμε ότι οι τιμές της B_i τοποθετούνται σε προκαθορισμένες θέσεις της διαδρομής εκτέλεσης· αντιθέτως, θα υιοθετήσουμε μια πιο εφαρμόσιμη γενικά τακτική. Για $i \geq 1$, θα δεσμεύσουμε σε μια συγκεκριμένη μερική διαδρομή εκτέλεσης τ που οδηγεί τον αλγόριθμο στο σημείο όπου είναι απλά να δειγματίσουμε για το bit B_i και θα δείξουμε ότι σε αυτή τη δεσμευμένη κατανομή πιθανότητας η B_i κατανέμεται ομοιόμορφα πάνω στο $\{0, 1\}$. Για να το κάνουμε αυτό αυστηρά, στο τυπικό πλαίσιό μας, ας ορίσουμε το ενδεχόμενο $\mathcal{A}_\tau$ να είναι το ενδεχόμενο ότι τ είναι ένα πρόθεμα της διαδρομής εκτέλεσης. Αν $|\tau| = \ell$, τότε τα ενδεχόμενα $\mathcal{A}_\tau$, $\mathcal{A}_\tau \wedge (B_i = 0)$ και $\mathcal{A}_\tau \wedge (B_i = 1)$ προσδιορίζονται από τα πρώτα $\ell + 1$ bit της διαδρομής εκτέλεσης. Μπορούμε τότε να θεωρήσουμε αντίστοιχα ενδεχόμενα σε ένα πιθανοτικό πείραμα στο οποίο παρατηρούμε τη συμπεριφορά του αλγορίθμου σε μια τυχαία $(\ell + 1)$-bit διαδρομή εκτέλεσης (βλ. Άσκηση 7.2). Στο τελευταίο πείραμα, είναι προφανές ότι η δεσμευ-

μένη κατανομή πιθανότητας της B_i, με δεδομένο ότι τα πρώτα ℓ bit της πραγματικής διαδρομής εκτέλεσης σ συμφωνούν με το τ, είναι ομοιόμορφη στο $\{0, 1\}$, και έτσι, το ίδιο ισχύει για την αρχική κατανομή πιθανότητας. Αφού αυτό ισχύει για όλα τα σχετικά τ, έπεται (από μια διακριτή εκδοχή της Άσκησης 6.13) ότι ισχύει με τη δέσμευση ότι $X \geq i$.

Έχουμε αναλύσει τον παραπάνω αλγόριθμο με πολύ λεπτομέρεια. Καθώς προχωράμε, πολλές από αυτές τις λεπτομέρειες θα συντμηθούν, αφού όλες μπορούν να αντιμετωπιστούν με πολύ παρόμοια (και εντελώς συνηθισμένα) επιχειρήματα.

7.4 Παραγωγή τυχαίου αριθμού από ένα δεδομένο διάστημα

Υποθέτουμε ότι θέλουμε να παραγάγουμε έναν αριθμό n στην τύχη ομοιόμορφα από το διάστημα $\{0, \ldots, M-1\}$, για δεδομένο ακέραιο $M \geq 1$.

Αν ο M είναι μια δύναμη του 2, ας πούμε $M = 2^k$, τότε αυτό μπορούμε να το κάνουμε απευθείας ως εξής: παράγουμε μια τυχαία k-bit συμβολοσειρά s και μετατρέπουμε την s στον ακέραιο $I(s)$ του οποίου η αναπαράσταση ως προς βάσης 2 είναι s· δηλαδή, αν $s = b_{k-1}b_{k-2}\cdots b_0$, όπου τα b_i είναι bit, τότε

$$I(s) := \sum_{i=0}^{k-1} b_i 2^i \ .$$

Στη γενική περίπτωση, δεν έχουμε ευθύ τρόπο για να το κάνουμε αυτό, αφού απευθείας μπορούμε μόνο να παράγουμε τυχαία bit. Όμως, υποθέτουμε ότι ο M είναι ένας k-bit αριθμός, έτσι ώστε $2^{k-1} \leq M < 2^k$. Τότε ο παρακάτω αλγόριθμος μας εξυπηρετεί:

Αλγόριθμος RN:
repeat
    $s \leftarrow_R \{0,1\}^{\times k}$
    $n \leftarrow I(s)$
until $n < M$
έξοδος n

Έστω ότι με X συμβολίζουμε το πλήθος των επαναλήψεων βρόχου αυτού του αλγορίθμου, με Y το χρόνο εκτέλεσής του και με N την έξοδό του.

Σε κάθε επανάληψη του βρόχου, ο n κατανέμεται ομοιόμορφα πάνω στο $\{0, \ldots, 2^k - 1\}$ και το ενδεχόμενο $n < M$ πραγματοποιείται με πιθανότητα $M/2^k$· επιπλέον, δεσμεύοντας στο τελευταίο ενδεχόμενο, ο n είναι ομοιόμορφα κατανεμημένος πάνω στο $\{0, \ldots, M-1\}$. Έπεται ότι η X έχει γεωμετρική κατανομή με μια σχετική πιθανότητα επιτυχίας $p := M/2^k \geq 1/2$ και ότι ο N είναι ομοιόμορφα κατανεμημένος πάνω στο $\{0, \ldots, M-1\}$. Έχουμε $\mathsf{E}[X] = 1/p \leq 2$ (βλ. Παράδειγμα 6.35) και $Y \leq ckX$ για κάποια ανεξάρτητη της υλοποίησης σταθερά c, από το οποίο προκύπτει ότι

Η θεωρία αριθμών και η άλγεβρα διαδραματίζουν έναν εξαιρετικά σημαντικό ρόλο στους υπολογισμούς και τις επικοινωνίες, όπως αποδεικνύεται από τις εντυπωσιακές εφαρμογές αυτών των αντικειμένων σε τέτοια πεδία όπως η κρυπτογραφία και η θεωρία κωδικοποίησης. Αυτό το εισαγωγικό βιβλίο δίνει έμφαση σε αλγορίθμους και εφαρμογές, όπως είναι η κρυπτογραφία και οι κώδικες διόρθωσης σφαλμάτων, και είναι προσιτό σε ένα ευρύ κοινό. Τα μαθηματικά προαπαιτούμενα είναι ελάχιστα: δεν προϋποτίθεται γνώση ύλης πέρα από αυτήν που διδάσκεται σε ένα τυπικό προπτυχιακό μάθημα διαφορικού και ολοκληρωτικού λογισμού, παρά μόνο κάποια μικρή πείρα στην ανάγνωση και συγγραφή μαθηματικών αποδείξεων. Οτιδήποτε άλλο αναπτύσσεται "από το μηδέν".

Η παρουσίαση εναλλάσσεται μεταξύ θεωρίας και εφαρμογών: κεφάλαια σε ένα ειδικό σύνολο αμιγώς μαθηματικών εννοιών ακολουθούνται από αντίστοιχα κεφάλαια σε αλγορίθμους και εφαρμογές. Τα μαθηματικά παρέχουν τα θεωρητικά εφόδια για τις εφαρμογές, ενώ οι εφαρμογές αποτελούν συγχρόνως το κίνητρο και την επεξήγηση των μαθηματικών. Η κάλυψη των μαθηματικών περιλαμβάνει τα βασικά της θεωρίας αριθμών και της αφηρημένης άλγεβρας, καθώς και τη θεωρία της διακριτής πιθανότητας (η οποία χρειάζεται για την ανάλυση των πιθανοτικών αλγορίθμων και για κρυπτογραφικές εφαρμογές). Ένα σημαντικό χαρακτηριστικό είναι ότι συμπεριλαμβάνονται πολλοί αλγόριθμοι από τους βασικούς έως τους πρόσφατους, συμπεριλαμβανομένου του εντυπωσιακού, νέου ντετερμινιστικού ελέγχου για πρώτο πολυωνυμικού χρόνου των Agrawal, Kayal και Saxena. Επιπροσθέτως, ο συγγραφέας έχει εφοδιάσει το βιβλίο με 500 περίπου ασκήσεις, από απλές έως προκλητικά δύσκολες, οι οποίες εμπλουτίζουν την ύλη που καλύπτεται στο κυρίως σώμα του βιβλίου, αναπτύσσουν περαιτέρω τη θεωρία, και παρουσιάζουν νέες εφαρμογές.

Επομένως, το βιβλίο μπορεί να εξυπηρετήσει διάφορους σκοπούς. Μπορεί να χρησιμοποιηθεί ως βιβλίο αναφοράς και για ατομική μελέτη από αναγνώστες που επιθυμούν να μάθουν τα θεμελιώδη μαθηματικά της σύγχρονης κρυπτογραφίας. Είναι επίσης ιδανικό ως εγχειρίδιο για εισαγωγικά μαθήματα στη θεωρία αριθμών και την άλγεβρα, ειδικά εκείνων που απευθύνονται σε σπουδαστές της επιστήμης των υπολογιστών.

εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ
Στουρνάρα 37, 10682 Αθήνα, Τηλ. 210-3829629

Επισκεφθείτε μας στο Internet:
www.klidarithmos.gr

ISBN 978-960-209-990-2