Αποδοτικοί Αλγόριθμοι

Μέρος 8: Τυχαιοκρατικοί Αλγόριθμοι

Εξάμηνο: 7ο

Κωδικός μαθήματος: 748

Τμήμα Μαθηματικών
Πανεπιστήμιο Ιωαννίνων

Μιχάλης Α. Μπέκος
bekos@uoi.gr

Τυχαιοκρατικοί Αλγόριθμοι

- Κάνουν τυχαίες επιλογές στις εκτελέσεις τους
- Διαφορετικές εκτελέσεις στην ίδια είσοδο μπορεί να οδηγήσουν σε διαφορετικές εξόδους
- Γιατί μελετάμε τυχαιοκρατικούς αλγορίθμους;
  - Απλούστεροι από τους ντετερμινιστικούς
  - Πιο αποδοτικοί από τους ντετερμινιστικούς
  - Δεν υπάρχει ντετερμινιστικός αλγόριθμος

- Δύο κύριες κατηγορίες

	Ορθότητα	Χρόνος εκτέλεσης
Monte Carlo:	Πιθανώς σωστός	Πολυωνυμικός
Las Vegas:	Πάντα σωστός	Πιθανώς πολυωνυμικός

Βασικές γνώσεις

- Ορισμός: Δοθέντος ενός συνόλου γεγονότων Ω , καθένα $\omega \in \Omega$ σχετίζεται με μια πιθανότητα:
  - $0 \leq Pr(\omega) \leq 1$
  - $\sum_{\omega \in \Omega} Pr(\omega) = 1$
- Παράδειγμα: Αν $\Omega = \{1, \ldots, 6\}$, τότε $Pr(\{2, 4, 6\}) = 3 \cdot \frac{1}{6} = \frac{1}{2}$
- Ιδιότητες:
  - $Pr(A_1 \cap A_2) = Pr(A_1) \cdot Pr(A_2|A_1)$
  - $Pr(A_1 \cap \ldots \cap A_k) = Pr(A_1) \cdot Pr(A_2|A_1) \cdots Pr(A_k|A_1 \cap \ldots \cap A_{k-1})$

Αναμενόμενες τιμές

- Ορισμός: Δοθείσας μιας τυχαίας διακριτής μεταβλητής X, η αναμενόμενη τιμή της X (σ.σ., η τιμή που αναμένουμε μεσοσταθμικά) είναι:

$$E[X] = \sum_{j=0}^{\infty} j \cdot Pr(X = j)$$

- 0-1 Ιδιότητα: Αν X είναι μια δυαδική τυχαία μεταβλητή (δηλαδή, παίρνει τιμές 0 ή 1), τότε:

$$E[X] = Pr(X = 1)$$

- Παράδειγμα 1: Ποια είναι η αναμενόμενη τιμή ενός ζαριού, αφού το ρίξει κάποιος μια φορά;

Έστω X η τυχαία διακριτή μεταβλητή που εκφράζει την τιμή του ζαριού. Τότε:

$$X \in \{1, \ldots, 6\} \Rightarrow E[X] = \sum_{j=1}^{6} j \cdot Pr(X = j) = \frac{1}{6} \cdot (1 + \ldots + 6) = 3.5$$

Αναμενόμενες τιμές

- Παράδειγμα 2: Ας υποθέσουμε ότι ρίχνουμε ένα νόμισμα μέχρι να έρθει η κορώνα. Ποιο είναι το αναμενόμενο πλήθος των ρίψεων που θα γίνουν;

  Έστω X η τυχαία διακριτή μεταβλητή που εκφράζει το πλήθος των ρίψεων. Τότε:

  - $X \in \{1, 2, \ldots\} \Rightarrow Pr(X = j) = \frac{1}{2^j}$
  - $E[X] = \sum_{j=1}^{\infty} \frac{j}{2^j}$
  - Παρατήρηση: $E[X] = 1 + \frac{1}{2}E[X] \Rightarrow E[X] = 2$

Γραμμικότητα των αναμενόμενων τιμών

- Θεώρημα: Δοθέντων δύο τυχαίων διακριτών μεταβλητών X και Y: $E[X+Y] = E[X] + E[Y]$

  Απόδειξη:

$$
\begin{aligned}
E[X+Y] &= \sum_{x=0}^{\infty}\sum_{y=0}^{\infty}(x+y)Pr(X=x, Y=y) \\
&= \sum_{x=0}^{\infty}\sum_{y=0}^{\infty} x \cdot Pr(X=x, Y=y) + \sum_{y=0}^{\infty}\sum_{x=0}^{\infty} y \cdot Pr(X=x, Y=y) \\
&= \sum_{x=0}^{\infty} x \cdot Pr(X=x) + \sum_{y=0}^{\infty} y \cdot Pr(Y=y) \\
&= E[X] + E[Y]
\end{aligned}
$$

Η ανισότητα Markov

- Θεώρημα: Για μια τυχαία διακριτή μεταβλητή X και μια σταθερά $a \geq 0$: $Pr(X \geq a) \leq \frac{E[X]}{a}$

  Απόδειξη:

$$
\begin{aligned}
E[X] &= \sum_{j=0}^{\infty} j \cdot Pr(X = j) \\
&= \sum_{j<a}^{\infty} j \cdot Pr(X = j) + \sum_{j \geq a}^{\infty} j \cdot Pr(X = j) \\
&\geq \sum_{j \geq a}^{\infty} j \cdot Pr(X = j) \\
&\geq a \sum_{j \geq a}^{\infty} Pr(X = j) \\
&= a \cdot Pr(X \geq a)
\end{aligned}
$$

Το πρόβλημα της επαλήθευσης πολυωνυμικών ταυτοτήτων

- Είσοδος: Δύο πολυώνυμα $P(x)$ και $Q(x)$
- Έξοδος: Είναι τα P και Q ισοδύναμα; (σ.σ., $P(x) = Q(x), \forall x \in \mathbb{R}$)

- Παράδειγμα: $P(x) = (x+1)(x-2)(x+3)(x-4)(x+5)(x-6)$

  $Q(x) = x^6 - 7x^3 + 25$

- Σημείωση: Το πρόβλημα μπορεί να λυθεί σε πολυωνυμικό χρόνο φέρνοντας τα P και Q σε μια κανονική μορφή (π.χ. άθροισμα μονωνύμων)

  Αυτό απαιτεί $O(d^2)$ πολλαπλασιασμούς συντελεστών, όπου d είναι ο μέγιστος βαθμός των P και Q

Μερικές απλές παρατηρήσεις

- Παρατηρήσεις: Για δύο πολυώνυμα P και Q ισχύουν τα εξής:

  (i) $\exists x_0 \in \mathbb{R}$ έτσι ώστε $P(x_0) \neq Q(x_0) \Rightarrow P \not\equiv Q$

  (ii) $\exists x_0 \in \mathbb{R}$ έτσι ώστε $P(x_0) = Q(x_0) \not\Rightarrow P \equiv Q$

  (iii) $P \equiv Q \Longleftrightarrow F \equiv 0$, όπου $F = P - Q$

Ένας απλός τυχαιοκρατικός αλγόριθμος

- `Let d be the maximum degree of F=P-Q`

  `Pick at random an integer r from [1,2,…,100d]`

  `If F(r)=0, then report P≡Q else report P≢Q`

- Πολυπλοκότητα: $O(d)$

- Σημείωση 1: Σύμφωνα με την Παρ.(ii) ο αλγόριθμος μπορεί να αναφέρει λανθασμένη απάντηση

- Σημείωση 2: Η πιθανότητα αναφοράς λανθασμένης απάντησης είναι το πολύ $\frac{d}{100d} = 0.01$
  αφού το F έχει το πολύ d ρίζες.

Μπορεί να μειωθεί η πιθανότητα;
(χωρίς αύξηση του $[1, \ldots, 100d]$)

Μείωση της πιθανότητας αναφοράς λανθασμένης απάντησης

(χωρίς αύξηση του $[1, \ldots, 100d]$)

- Ιδέα: Να εκτελέσουμε τον προηγούμενο αλγόριθμο k φορές

  $\Rightarrow$ Η πιθανότητα αναφοράς λανθασμένης απάντησης είναι το πολύ $\left(\frac{d}{100d}\right)^k = 0.01^k$

- Σημείωση: Ο ίδιος ακέραιος αριθμός μπορεί να επιλεγεί πολλές φορές.

- Ερώτηση: Τι γίνεται αν κάθε ακέραιος μπορεί να επιλεγεί το πολύ μία φορά;

- Διαίσθηση: Αν $k = d + 1$, τότε μπορούμε να αποφασίσουμε αν $P \equiv Q$

  ↑ Ωστόσο, θα προτιμούσαμε $k < d + 1$, για λόγους αποδοτικότητας.

Κάθε ακέραιος μπορεί να επιλεγεί το πολύ μία φορά

- $A_i \leftarrow$ το ενδεχόμενο αναφοράς λανθασμένης απάντησης μετά την i-οστή επανάληψη

- Η πιθανότητα αναφοράς λανθασμένης απάντησης είναι το πολύ:

$$Pr(\cap_{i=1}^{k} A_i) = Pr(A_1) \cdot Pr(A_2|A_1) \cdots Pr(A_k|A_1 \cap \cdots \cap A_{k-1})$$
$$= \frac{d}{100d} \cdot \frac{d-1}{100d-1} \cdot \frac{d-2}{100d-2} \cdots \frac{d-(k-1)}{100d-(k-1)}$$

Η πιθανότητα εύρεσης μιας ρίζας

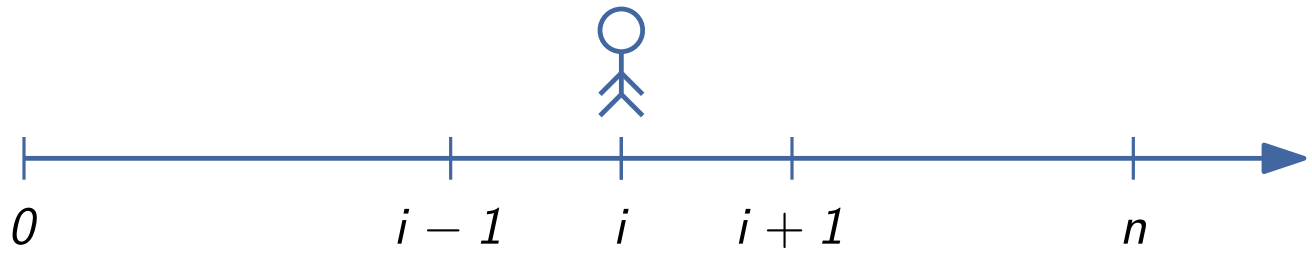
Η πιθανότητα εύρεσης επόμενης ρίζας

- Πολυπλοκότητα: $O(kd)$

- Τύπος αλγορίθμου: Monte Carlo

Τυχαίοι περίπατοι

- Έστω $\mathcal{P}$ ένα άτομο κατά μήκος μιας γραμμής



  - Setup:
    - Το $\mathcal{P}$ βρίσκεται αρχικά στη θέση 0 (και δεν μπορεί να μετακινηθεί στο -1)
    - Το $\mathcal{P}$ κινείται προς τα αριστερά με πιθανότητα p
    - Το $\mathcal{P}$ κινείται προς τα δεξιά με πιθανότητα $1 - p$
  - Για λόγους απλότητας: υποθέτουμε $p = \frac{1}{2}$
  - Ερώτηση: Ποιος είναι το αναμενόμενο πλήθος κινήσεων του $\mathcal{P}$ για να φτάσει στη θέση n;

Τυχαίοι περίπατοι

- Θεώρημα: Το αναμενόμενο πλήθος κινήσεων του $\mathcal{P}$ για να φτάσει στη θέση n είναι n^2

  Απόδειξη:

  $X_i \leftarrow$ πλήθος κινήσεων του $\mathcal{P}$ για να φτάσει στη θέση i

  $T[i] \leftarrow E[X_i]$

  Ενδιαφερόμαστε για τον όρο $T[n]$:

  - $T[0] = 0$
  - $T[1] = 1 + \frac{1}{2}T[0] + \frac{1}{2}T[2]$

    $\ldots$
  - $T[i] = 1 + \frac{1}{2}T[i-1] + \frac{1}{2}T[i+1]$

    $\ldots$
  - $T[n] = 1 + T[n-1]$

Για να φτάσει στη θέση 1, είτε:
- βρίσκεται στη θέση 0 και εκτελεί μια κίνηση προς τα δεξιά με πιθανότητα $\frac{1}{2}$ είτε
- βρίσκεται στη θέση 2 και εκτελεί μια κίνηση προς τα αριστερά με πιθανότητα $\frac{1}{2}$

Ο μόνος τρόπος για να φτάσει στη θέση n είναι να να βρίσκεται στη θέση $n-1$ και να κινηθεί προς τα δεξιά

Προς τα πίσω αντικαταστάσεις

- $T[n-1] = 1 + \frac{1}{2}T[n-2] + \frac{1}{2}T[n]$
  $= 1 + \frac{1}{2}T[n-2] + \frac{1}{2}(1 + T[n-1])$

$\Rightarrow T[n-1] = 3 + T[n-2]$

- $T[n-2] = 1 + \frac{1}{2}T[n-3] + \frac{1}{2}T[n-1]$
  $= 1 + \frac{1}{2}T[n-3] + \frac{1}{2}(3 + T[n-2])$

$\Rightarrow T[n-2] = 5 + T[n-3]$

$\ldots$

- $T[n-i] = 2i + 1 + T[n-i-1]$

$\ldots$

- $T[1] = 2(n-1) + 1 + \cancel{T[0]}^{0}$

Προς τα εμπρός αντικαταστάσεις

- $T[1] = 2(n-1) + 1$
- $T[2] = 1 + 2(n-2) + \overbrace{2(n-1)+1}^{T[1]}$
- $T[3] = 1 + 2(n-3) + \overbrace{1 + 2(n-2) + 2(n-1) + 1}^{T[2]}$

  $\ldots$

- $$\begin{aligned} T[n] &= 1 + 2(n-n) + \ldots + 1 + 2(n-2) + 2(n-1) + 1 \\ &= n + 2(1 + 2 + \ldots + (n-2) + (n-1)) \\ &= n + n(n-1)) = n^2 \end{aligned}$$

Το πρόβλημα 2SAT

- Είσοδος: Ένας λογική πρόταση φ με n μεταβλητές και m συνθήκες, καθεμία με δύο τελεστέους
- Έξοδος: Μια ανάθεση τιμών αλήθειας στις μεταβλητές της φ που την καθιστά ικανοποιήσιμη (αν υπάρχει)

- Παράδειγμα: $\phi = (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee \neg x_3) \wedge (x_1 \vee x_2) \wedge (\neg x_3 \vee \neg x_4)$

  Λύση: $x_1 = x_2 = \texttt{true}, x_3 = x_4 = \texttt{false}$

Ένας απλός τυχαιοκρατικός αλγόριθμος

- Start with an arbitrary assignment (e.g., x_i = false, i=1,…,n)

  While (there is unsatisfied clause or tired to flip coins) {

  c ← some clause that is unsatisfied in φ

  choose a variable of c at random by flipping a coin

  and change its value

  }

- $S \leftarrow$ μια ανάθεση των τιμών αλήθειας στη φ

  $A_j \leftarrow$ οι τιμές των μεταβλητών της φ μετά την επανάληψη j

  $X_j \leftarrow$ το πλήθος των μεταβλητών με την ίδια τιμή στις S και A_j

- Πίσω στο παράδειγμα: $S = \{x_1 = x_2 = \texttt{true}, x_3 = x_4 = \texttt{false}\}$

$$A_0 = \{x_1 = x_2 = x_3 = x_4 = \texttt{false}\} \Rightarrow X_0 = 2$$

Ένας απλός τυχαιοκρατικός αλγόριθμος: Ανάλυση

- Λήμμα: Αν S είναι μια ανάθεση τιμών αλήθειας στις μεταβλητές της φ, ο αλγόριθμος αναμένεται να βρει την S μετά από n^2 επαναλήψεις

  Απόδειξη:

  Υποθέστε χ.β.τ.γ. ότι $X_0 = 0$ (σ.σ., τη χειρότερη περίπτωση)

  Ερμηνεύστε τις επαναλήψεις του αλγορίθμου ως τυχαίο περίπατο

  Ερώτηση: Ποια είναι η πιθανότητα να απομακρυνθούμε / πλησιάσουμε την S στην επανάληψη j;

  $Pr(X_{j+1} = k-1 | X_j = k)$ ↑ ↑ $Pr(X_{j+1} = k+1 | X_j = k)$

  $(x_k \vee x_\ell)$ ← η συνθήκη στην επανάληψη j ⇒ Τουλάχιστον μια από τις x_k και x_ℓ έχει διαφορετική τιμή στις A_j και S

  - Και οι δύο έχουν διαφορετικές τιμές:
    $Pr(X_{j+1} = k+1 | X_j = k) = 1$
  - Μόνο μια έχει διαφορετική τιμή:
    $Pr(X_{j+1} = k+1 | X_j = k) = \frac{1}{2}$

  ⇒ Ο αναμενόμενος αριθμός επαναλήψεων για την εύρεση της S είναι το πολύ n^2

Ένας απλός τυχαιοκρατικός αλγόριθμος: Ανάλυση

- Θεώρημα: Αν η φ είναι ικανοποιήσιμη, τότε η πιθανότητα να μην βρεθεί η λύση της μετά από $2n^2$ επαναλήψεις είναι μικρότερη από $\frac{1}{2}$

  Απόδειξη:

  $X \leftarrow$ το πλήθος των επαναλήψεων για την εύρεση μιας ανάθεσης τιμών αλήθειας που καθιστά τη φ ικανοποιήσιμη

  Χρησιμοποιώντας την ανισότητα Markov:

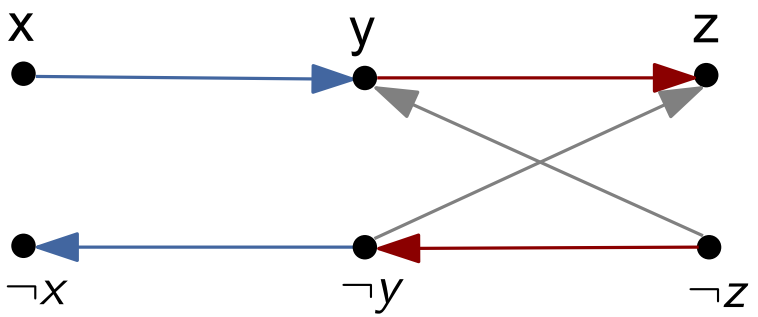
  $Pr(\text{μη εύρεση λύσης μετά από } 2n^2 \text{ επαναλήψεις}) = Pr(X \geq 2n^2) \leq \frac{E[X]}{2n^2} \leq \frac{1}{2}$

Το πρόβλημα 2SAT είναι πολυωνυμικά επιλυσιμο

- Δοθέντος μιας 2SAT πρότασης φ, κατασκευάζουμε γράφημα G_φ ως εξής:
  - για κάθε μεταβλητή x της φ, δημιουργούμε δύο κορυφές στο G_φ: x και $\neg x$
  - για κάθε συνθήκη $(a \vee b)$ της φ, δημιουργούμε δύο ακμές στο G_φ: $(\neg a, b)$ και $(\neg b, a)$

↑ Διαίσθηση: $(x \vee y) \iff \neg x \Rightarrow y$ and $\neg y \Rightarrow x$

- Παράδειγμα: $\phi = (\neg x \vee y) \wedge (\neg y \vee z) \wedge (z \vee y)$



- Παρατήρηση: Αν υπάρχει μονοπάτι από το a στο b στο G_φ, τότε υπάρχει και από το $\neg b$ στο $\neg a$.

↑ Απόδειξη: $(a, b) \in G_\varphi \Rightarrow (\neg b, \neg a) \in G_\varphi$

Το πρόβλημα 2SAT είναι πολυωνυμικά επιλυσιμο

- Θεώρημα: Η φ είναι μη ικανοποιήσιμη $\iff$ υπάρχει μεταβλητή x της φ έτσι ώστε στο G_φ υπάρχουν δύο κατευθυνόμενα μονοπάτια: $P_1 : x \to \neg x$ $P_2 : \neg x \to x$

  Απόδειξη ($\Rightarrow$):

  Έστω ότι η φ μη ικανοποιήσιμη και υποθέστε ότι δεν υπάρχουν τέτοια μονοπάτια

  ```
  Repeat until all variables of φ has been assigned {
      a ← unassigned literal with no path from a to ¬a
      set a and all vertices reachable by a in G_φ to true
      set all vertices reachable by ¬a in G_φ to false
  }
  ```

  Ισχυρισμός: Ο αλγόριθμος είναι σωστός (άρα η φ είναι ικανοποιήσιμη, άτοπο)

  Απόδειξη: Αν υπάρχουν μονοπάτι από τον a στον $\neg b$, τότε υπάρχει και από τον b στον $\neg a$
  Αρα, μονοπάτι από τον a στον $\neg a$, άτοπο

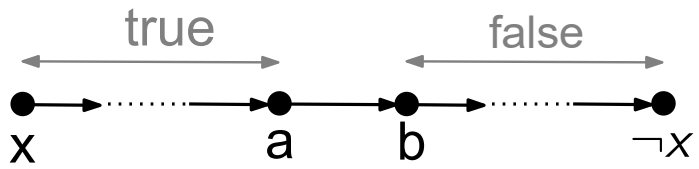
Το πρόβλημα 2SAT είναι πολυωνυμικά επιλυσιμο

- Θεώρημα: Η φ είναι μη ικανοποιήσιμη $\iff$ υπάρχει μεταβλητή x της φ έτσι ώστε στο G_φ υπάρχουν δύο κατευθυνόμενα μονοπάτια:
  - $P_1 : x \to \neg x$
  - $P_2 : \neg x \to x$

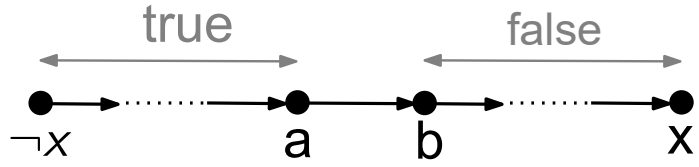
  Απόδειξη ($\Leftarrow$):

  Ας υποθέσουμε ότι η φ είναι ικανοποιήσιμη

  - `x = true`:



  - `x = false`:



  Και στις δύο περιπτώσεις, $(a, b) \in G_\varphi \Rightarrow (\neg a \vee b) \in \varphi$, άτοπο