Advanced Algorithmics

Strategies for Tackling Hard Problems

Sebastian Wild

Markus Nebel

Lecture 9

2017-05-18

4 Randomized Algorithms and Data Structures

Computational Models

We consider deterministic TM,
with an additional input tape (read-only, unidirectional)
containing an infinite sequence of random 0s and 1s.

$\rightsquigarrow$ Algorithms can use random bits to decide on branching.

$\Rightarrow$ Randomized algorithm A defines a random experiment on input x

probability space $(S_{A,x}, \mathrm{Prob})$

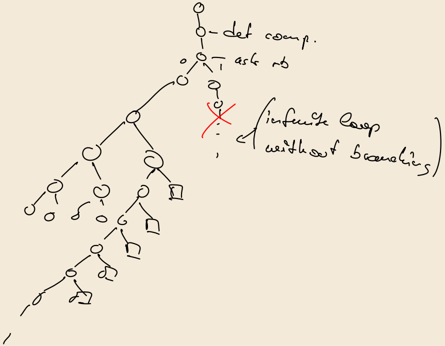
$S_{A,x} = \{ c \mid c$ randomly controlled computation of A on $x \}$

Prob = probability distribution on $S_{A,x}$ induced by $0/1$ sequences

What Can Go Wrong in RA?

- computation can go to df. inf loop
- computation can go to branch inf loop.
- $\forall n \; \exists c \quad |c| \geq n$

$\hookrightarrow$ ξ_{max}



Warmup: Rejection Sampling

We assume only random *bits*. How to simulate a fair (6-sided) die?

```
procedure rollDie:
    do
        Draw 3 random bits b_2, b_1, b_0
        n = Σ_{i=0}^{2} 2^i b_i    // Interpret as binary representation of a number in [0 : 7]
    while (n = 0 ∨ n = 7)
    return n
```

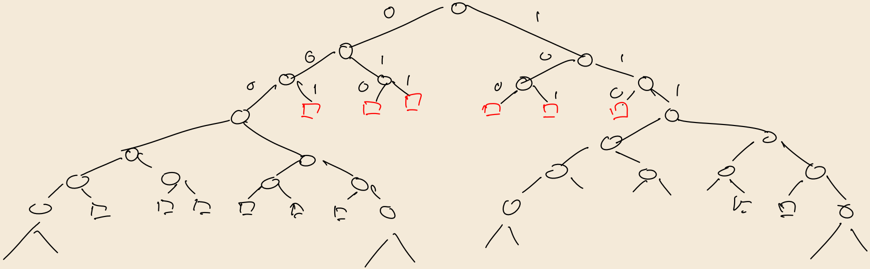
Correctness: Every output $1, \ldots, 6$ equally likely by construction.

Termination: *Infinite* runs possible! *Is that a problem?*

Expected Running Time: Leave loop with probability $\frac{6}{8} = \frac{3}{4}$ in each iteration

$\rightsquigarrow$ in expectation, only $\dfrac{4}{3} = \displaystyle\sum_{i \ge 1} i \cdot \left(\frac{1}{4}\right)^{i-1} \frac{3}{4}$ repetitions.

rollDie is a correct and practically efficient algorithm.



$\{000, 111\}^{\omega}$ = set of sequences that correspond to infinite run?

represent $\omega \in \{0,1\}^{\mathbb{N}}$ $\quad 0.\omega \rightsquigarrow$ real number $x \in [0,1]$

0.011111...

0.100...

Cantor set

$\mathbb{Q} \cap [0,1)$

good news: measurable set, has measure 0

How to define the random length of a computation?

Worst-Case Time

$$\mathrm{time}_A(x) = \begin{cases} \infty & \text{if } \exists c \text{ on } x \text{ that is infinite} \\ (\infty & \text{if } \forall n\, \exists c\ |c| \geq n\ ) \quad \text{Kőnig's lemma} \\ \max\{ |c| : c \text{ comp. on } x \} & \text{else} \end{cases}$$

$$\mathrm{time}_A(n) = \max\{ \mathrm{time}_A(x) : |x| = n \}$$

a) Complexity Measure

$$\mathrm{Random}_A(n) = \begin{cases} \infty & \text{if } \exists c \text{ with infinite \# rb} \\ \max\{\mathrm{Random}_A(x) \mid x \text{ with } |x| = n\} \end{cases}$$

$$\mathrm{Random}_A(x) = \max\{\text{random bits used by } c \;:\; c \text{ computation of } A \text{ on } x\}$$

4.1 Recap of Probability Theory

Discrete probability space $(\Omega, \Pr)$:

- $\Omega = \{\omega_1, \omega_2, \ldots\}$ a (finite or) *countable* set
- $\Pr : 2^\Omega \to [0,1]$ a discrete probability measure, i.e.,
  - $\Pr[\Omega] = 1$
  - $\Pr[A] = \sum_{\omega \in A} \Pr[\omega] \quad \rightsquigarrow \quad \Pr$ determined by $\underbrace{w_i}$ $= \Pr[\omega_i]$.

General probability space $(\Omega, \mathcal{F}, \Pr)$:

- Ω is a set of points (the universe)
- $\mathcal{F} \subseteq 2^\Omega$ is a σ-algebra, i.e., (in discrete case: $\mathcal{F} = 2^\Omega$)
  - $\emptyset \in \mathcal{F}$ $\quad \Omega \in \mathcal{F}$
  - closed under complementation: $A \in \mathcal{F} \implies \overline{A} = \Omega \setminus A \in \mathcal{F}$
  - closed under *countable* union: $A_1, A_2, \ldots \in \mathcal{F} \implies \bigcup_{i=1}^\infty A_i \in \mathcal{F}$
- $\Pr : \mathcal{F} \to [0,1]$ is a probability measure, i.e.,
  - $\Pr[\Omega] = 1$
  - If $A_1, A_2, \ldots \in \mathcal{F}$ are pairwise *disjoint* then $\Pr\left[\bigcup_{i=1}^\infty A_i\right] = \sum_{i=1}^\infty \Pr[A_i]$

die $\quad \Omega = [6]$

$A =$ "even" $= \{2, 4, 6\}$

$\Pr[\omega] = \frac{1}{6} \quad \omega \in [6]$

$\Omega = \mathbb{N}$

$\Pr[i] = \left(\frac{1}{4}\right)^{i-1} \cdot \frac{3}{4}$

$\Omega = [0,1]$

$\mathcal{F}$ = Borel set

$(a,b) \in \mathcal{F}$

closure

Lesbesgue

$\lambda((a,b)) = b - a$

Probability Space for Nonterminating RA

$\Omega = \{0,1\}^{\mathbb{N}}$

$\Pi_x = \{ x\omega : \omega \in \{0,1\}^{\mathbb{N}} \} \quad \hat{=} \quad [a, a + 2^{-|x|}]$

$x \in \{0,1\}^*$

closure $\rightsquigarrow \mathcal{F}$

a dyadic number

$= a \cdot 2^n \in \mathbb{N}$ for some n

$\Pr[\Pi_x] = 2^{-|x|}$

$\Pi_\varepsilon = \Omega$

$\omega \in \{0,1\}^{\mathbb{N}}$ $\quad \Pr[\{\omega\}] = 0$

$\Pr[\{\omega\}]$ $\quad \{\omega\} \in \mathcal{F}$? $\quad \Pr[A \cap B] = \Pr[A] \cdot \Pr[B \mid A]$

$\{\omega\} = \bigcap_i \Pi_{\omega_{1:i}}$

$$\Pr[\{\omega\}] = \Pr[\bigcap_i \Pi_{\omega_{1:i}}] = \Pr[\Pi_\varepsilon] \cdot \prod_i \underbrace{\Pr[\Pi_{\omega_{1:i}} \mid \overbrace{\Pi_{\omega_{1,1}} \cap \cdots \cap \Pi_{\omega_{1:i-1}}}^{\Pi_{\omega_{1:i-1}}}]}_{1/2} = 0$$

Events

$A \in \mathcal{F}$ is called an *event* of $(\Omega, \mathcal{F}, \Pr)$; also a *measurable set*.

Basic properties

- $\Pr\left[\overline{A}\right] = 1 - \Pr[A]$ counter-probability
- $\Pr\left[\bigcup A_i\right] \le \sum_i \Pr[A]$ the *union bound* (a.k.a. Boole's inequality a.k.a. σ-subadditivity)
- $\{A_1, \ldots, A_k\}$ *(mutually) independent* $\iff$ $\Pr\left[\bigcap_i A_i\right] = \prod_i \Pr[A_i]$
  An infinite set of events is mutually independent if every finite subset is so.
  k-wise independence means that only all size-k subsets are independent.
- *conditional probability* for A given B: $\Pr[A \mid B] = \Pr[A \cap B] \big/ \Pr[B]$
  generally undefined if $\Pr[B] = 0$.
- *law of total probability*: If $\Omega = B_1 \dot\cup B_2 \dot\cup \cdots$ is a partition of Ω, then holds

$$\Pr[A] \quad = \sum_{\substack{i \\ \Pr[B_i] \neq 0}} \Pr[A \mid B_i] \cdot \Pr[B_i].$$

Random Variables

Random variables (r.v.) $X : \Omega \to \mathcal{X}$; often $\mathcal{X} = \mathbb{R}$ (in general spaces: only *measurable* functions)

Basic properties and conventions:

- event $\{X = x\}$ is defined as $\{\omega \in \Omega : X(\omega) = x\}$.
- For event A define the indicator r.v. $\mathbb{1}_A$ via $\mathbb{1}_A(\omega) = [\omega \in A]$
- $F_X(x) = \Pr[X \le x]$ is the *cumulative distribution function (CDF)*.
- X is *discrete* if $X(\Omega) = \{X(\omega) : \omega \in \Omega\}$ is countable.
- for discrete r.v. X define $f_X(n) = \Pr[X = n]$ the *probability mass function (PMF)*.
- If F_X is everywhere differentiable, X is *continuous*.
  Then $f_X = F'_X$ is its *probability density function*.

Independence:

- Consider *vector* $\vec{X} = (X_1, \ldots, X_k)$ as one function from Ω to $\mathbb{R}^k$. $= \mathcal{X}$
  CDF/PMF/PDF of $\vec{X}$ is called *joint CDF/PMF/PDF* of $X_1, \ldots, X_k$.
- r.v.s *independent* $\iff$ joint PMF/PDF factors:
  X and Y independent $\iff \Pr[X = x \wedge Y = y] = \Pr[X = x] \cdot \Pr[Y = y]$ for all x, y.

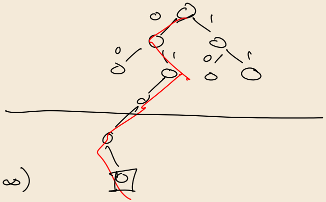
Is Random Runtime Well-defined?

T random runtime

$T : \{0,1\}^{\mathbb{N}} \to \mathbb{N} \cup \{\infty\} =: \mathbb{N}_\infty$

↳ T discrete r.v.

is T measurable?



require that if $M \subseteq \mathbb{N}_\infty$ $\quad M = [k : \infty)$

$$T^{-1}(M) = \{\omega : T(\omega) \in M\} \quad \text{measurable}$$

$$\{r \in \{0,1\}^{\mathbb{N}} : T(r) \geq k\} = \overline{\bigcup_{\substack{w \in \{0,1\}^{<k};\\ v(w) \text{ is terminating}}} \Pi_w} \in \mathcal{F}$$

to show $\Uparrow$ $\mathcal{F}$

$\mathrm{Prob}_{A,x}(c)$ = prob. of sequence of random bits read by A on input x during computation c.

$$\mathrm{Prob}(A(x)=y) = \sum_{c} \mathrm{Prob}_{A,x}(c)$$

// probability of output x

c outputs y

$$\mathbb{E}\text{-}\mathrm{Time}_A(x) = \begin{cases} \infty & \text{if } \exists c \text{ inf. with } \mathrm{Prob} > 0 \\ \sum_c \mathrm{Prob}_{A,x}(c) \cdot \mathrm{Time}(c) \end{cases}$$

need not exist or if can ∞

$$\mathbb{E}\text{-}\mathrm{Time}_A(n) = \max\{\mathbb{E}\text{-}\mathrm{Time}_A(x)\}$$

while (rbit() == 1) { }

usually well-defined even if infinite runs are possible

but hard to determine

Expectations

Expectation of a $\mathcal{X}$-valued r.v. X, written $\mathbb{E}[X]$, is given by

- $\mathbb{E}[X] = \sum_{x \in \mathcal{X}} x \cdot f_X(x)$ for *discrete* X,
- $\mathbb{E}[X] = \int_{x \in \mathcal{X}} x \cdot f_X(x)\, dx$ for *continuous* X.
- undefined if sum does not converge / integral does not exist.

Properties:

- *linearity*: $\mathbb{E}[aX + bY] = a\mathbb{E}[X] + b\mathbb{E}[Y]$ (X, Y r.v. and a, b constants)
  even if X and Y are not independent
  only for *finite* sums / linear combinations!
- X and Y *independent* $\implies \mathbb{E}[X \cdot Y] = \mathbb{E}[X] \cdot \mathbb{E}[Y]$.

Conditional Expectation

Similar to conditional probability, we can define condition expectation.

- *conditional expectation* on event $\mathbb{E}[X \mid A] \;=\; \sum_x^{x\cdot} \Pr[X = x \mid A]$ for *discrete* X.
  for general A, continuous definition problematic
- *conditional expectation* on $\{Y = y\}$, written $\mathbb{E}[X \mid Y = y]$.
  - for *discrete* X and Y

$$\mathbb{E}[X \mid Y = y] \;=\; \sum_{x \in \mathcal{X}} x \cdot \Pr\big[X = x \mid \{Y = y\}\big]$$

  - for *continuous* X and Y, use the joint density $f_{(X,Y)}$ and define the *marginal density* of Y as $f_Y(y) = \int_{\mathcal{X}} f(x, y)\, dx$. Then

$$\mathbb{E}[X \mid Y = y] \;=\; \int_{\mathcal{X}} x \cdot f_{X|Y}(x, y)\, dx \qquad \text{with} \qquad f_{X|Y}(x, y) = \frac{f_{(X,Y)}(x, y)}{f_Y(y)}$$

$P \stackrel{\mathcal{D}}{=} \mathcal{U}(0,1)$

- With $g(y) := \mathbb{E}[X \mid Y = y]$ we obtain a *new r.v.* $\mathbb{E}[X \mid Y] = g(Y)$.

$X \stackrel{\mathcal{D}}{=} \mathcal{B}(P)$

$\mathcal{B}(p) = \begin{cases} 1 & \text{prob } p \\ 0 & \text{other} \end{cases}$

- *law of total expectation*: $\mathbb{E}[X] \;=\; \mathbb{E}\big[E[X \mid Y]\big]$.

$\mathbb{E}[X]$