Tutorial 2

01 March 2023 14:06

RQUICKSORT – complexity proof

$f(n) \geq E(\#\text{ comparisons with input size } n)$

$f(n) \in O(n \cdot \log n)$

S – input of size n

$\forall i,j \in S$ define S_{ij}

$S_{ij} = 1$ iff i and j get compared during the run algorithm

$S_{ij} = 0$ otherwise

$$X = \sum_{i<j} S_{ij}$$

$$E(X) = E\left(\sum_{i<j} S_{ij}\right) = \sum_{i<j} E(S_{ij}) = \sum_{i<j} Pr(S_{ij} = 1)$$

1.) What is the probability to compare i and j in the round of the protocol? $\frac{2}{|S|}$

Step 2 $|S_1|, S, |S_2|$

What is the probability to compare i and j?

$Pr(i \text{ and } j \text{ are compared} \mid i < z < j) = 0$

$Pr(\text{—} \mid i < j < z) = \frac{2}{|S_1|}$

$Pr(\text{—} \mid s < i < j) = \frac{2}{|S_2|}$

$\frac{1}{|S_k|}$

Step k Hard combinatorics

P_r (i and j get compared in step k | no pivot $j < y < j$ was got chosen in the run (they are in set S_k))

$= \frac{2}{|S_k|} < \frac{2}{j-i+1}$

$S_{ij} = 1$ iff i and j got compared in some round

$P_r[S_{ij}] = \sum_k P_r$ (i and j get compared in round k | no pivot $i \le y \le j$ was chosen)

$\cdot P_r$ (no pivot was chosen $i \le y \le j$ in previous rounds) < 0

The theorem of total Probability

$+ P_r$ (i and j get compared in round k | pivot $i \le y \le j$ was chosen in previous rounds)

$\cdot P_r$ (Pivot $i \le y \le j$ was chosen in previous rounds

$$\le \sum_k \frac{2}{j-i+1} \cdot \left(\frac{n-(j-i+1)}{n}\right)^k \le \frac{2}{j-i+1} \cdot \sum_k \left(1 - \frac{(j-i+1)}{n}\right)^k$$

$$\sum_{i=0}^{\infty} q^i = \frac{1}{1-q} \qquad 0 < q < 1$$

$$\le \frac{2}{j-i+1} \cdot \frac{n}{(j-i+1)}$$

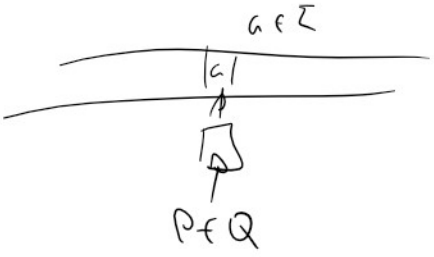
---

n

$$\sum_{i<j} \frac{2}{(j-i+1)} < \dots < n \sum_{i=1}^{n} \frac{1}{i}$$

[c]

TURING MACHINE



$$Q \times \Sigma \to Q \times \{\leftarrow, \rightarrow, \downarrow\}$$

$$Acc \subseteq Q$$

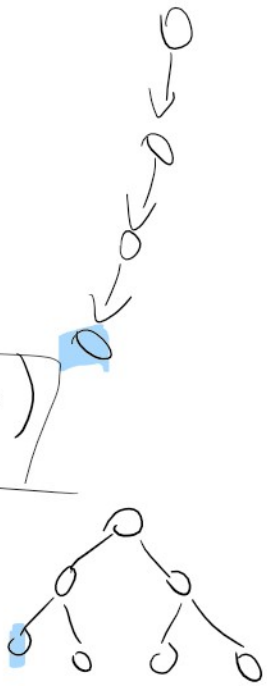
Decision problems $x \in \Sigma^*$ input x belongs to a language

$$L \subseteq \Sigma^*$$

DTM ends in an accepting state $x \in L$

DTM ends outside of accepting states $x \notin L$

NTM $(Q \times \Sigma) \times (Q \times \{\rightarrow, \leftarrow, \downarrow\})$



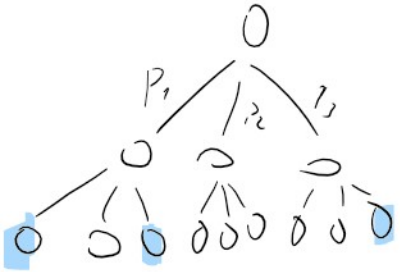
$x \in L \Rightarrow$ } accepting state

PTM → probabilistic TM

multiple rules for (state, input pair) but they are assigned probabilities

()

assigned probabilities



RP — random polynomial

contains problems for which there is PTM

s.t.

$x \in L$: $Pr(TM(x) \text{ accepts}) \geq 1/2 \geq \varepsilon > 0$

$x \notin L$: $Pr(TM(x) \text{ accepts}) = 0$

Problems in RP have 1-sided MC algorithm with NO-bias

co-RP contains problems s.t. $\exists$ TM

$x \in L$: $Pr(TM(x) \text{ accepts}) = 1$

$x \notin L$: $Pr(TM(x) \text{ accepts}) \leq 1/2 \leq \varepsilon < 1$

1 sided MC algorithm with YES-bias

PROBABILITY AMPLIFICATION

RP- NO-Sing

Run the algorithm k times

1.) If there is a single YES answer, answer YES

2.) answer NO otherwise

if for the original algorithm the probability of error is $(1-\varepsilon)$

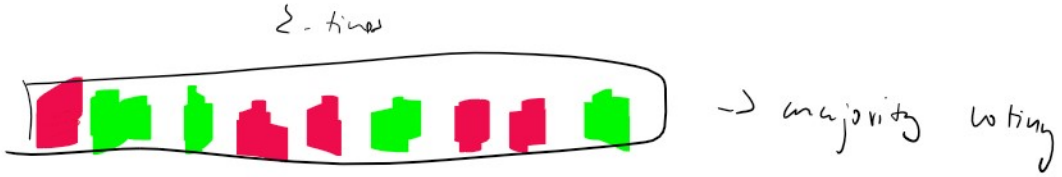
If for the original algorithm the probability of error is $(1-\varepsilon)$

the probability of an error in the new algorithm is $\delta = (1-\varepsilon)^k$

BPP

$x \in L$: $Pr(TM(x) \text{ accepts}) \geq 3/4$

$x \notin L$ $Pr(TM(x) \text{ accepts}) < 1/2$



→ majority voting

(Chernoff - bound (next week))

PP probabilistic polynomial

$x \in L$: $Pr(TM(x) \text{ accepts}) > 1/2$ $\quad (1/2 + 1/2^n)$

$x \notin L$: $Pr(TM(x) \text{ accepts}) < 1/2$

ZPP → associated with Las Vegas algorithms