COL 702 Lecture 6 Aug 9

Primality testing: Given an integer N is N prime?

See for $i = 1$ to $\sqrt{N}$ if i divides N

$O(\sqrt{N})$ Input size: $\log N$ bits $= n$

$\uparrow$

$2^{\frac{n}{2}}$

density of primes: Among n integers $\sim \frac{n}{\ln n}$ are prime

Pick a large random integer K
test if K is prime

Efficient algorithm for primality testing
Rabin-Miller Solovay Strassen

(Monte Carlo) Randomized : $\sim n^2$

AKS algorithm deterministic : n^{12}

Selection Problem

Given n elements from a (totally ordered) set S and an integer $1 \leq k \leq n$, find an element $x \in S$ such that

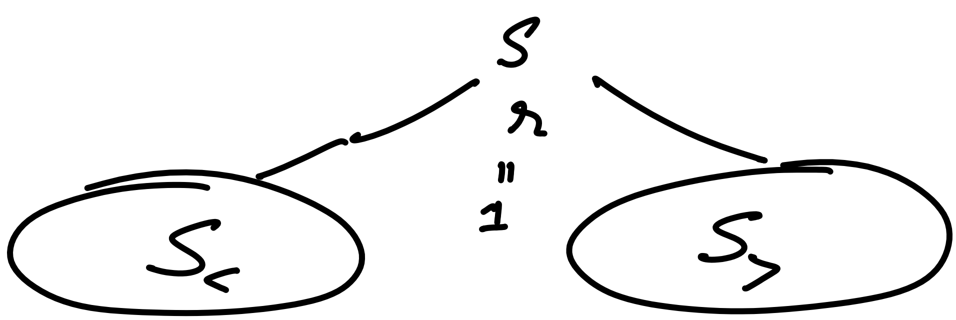
$$\text{rank}(x, S) = k$$

\# elements $y \in S$ s.t. $y < x$

Objective: Design a linear time algorithm for selection

Easy soln: to sort

Pick some element $r \in S$ and partition S using r



Prune and search

Analysis: If the subset containing the rank k element decreases by some constant factor, say $\alpha < 1$

running time: $\sum_{i \geq 0} \alpha^i n = O(n)$

Approximate median: If the rank of r is between $\left[\frac{1}{4}n, \frac{3}{4}n\right]$

r : random element of S

r is an approx median with prob $\geq \frac{1}{2}$

Find rank of r

If rank is in $\left[\frac{1}{4}n, \frac{3}{4}n\right]$

then proceed with the correct partition

else

Expected # of iterations = 2

In each iteration we spend cn time

First recursive call $2cn$ X_1

Sec. " " $2c \cdot \frac{3}{4} n$ X_2

⋮

i " " $2c \left(\frac{3}{4}\right)^i n$ X_m

$m = \log_{4/3} n$

$O(cn)$

X : random variable representing the overall running time

$$E[X] = E\left[cn \cdot X_1 + c\frac{3}{4}n \cdot X_2 + \cdots (\ ) X_m\right]$$

$$= cn\, E[X_1] + \frac{3}{4} cn\, E[X_2] + \cdots (\ ) E[X_m]$$

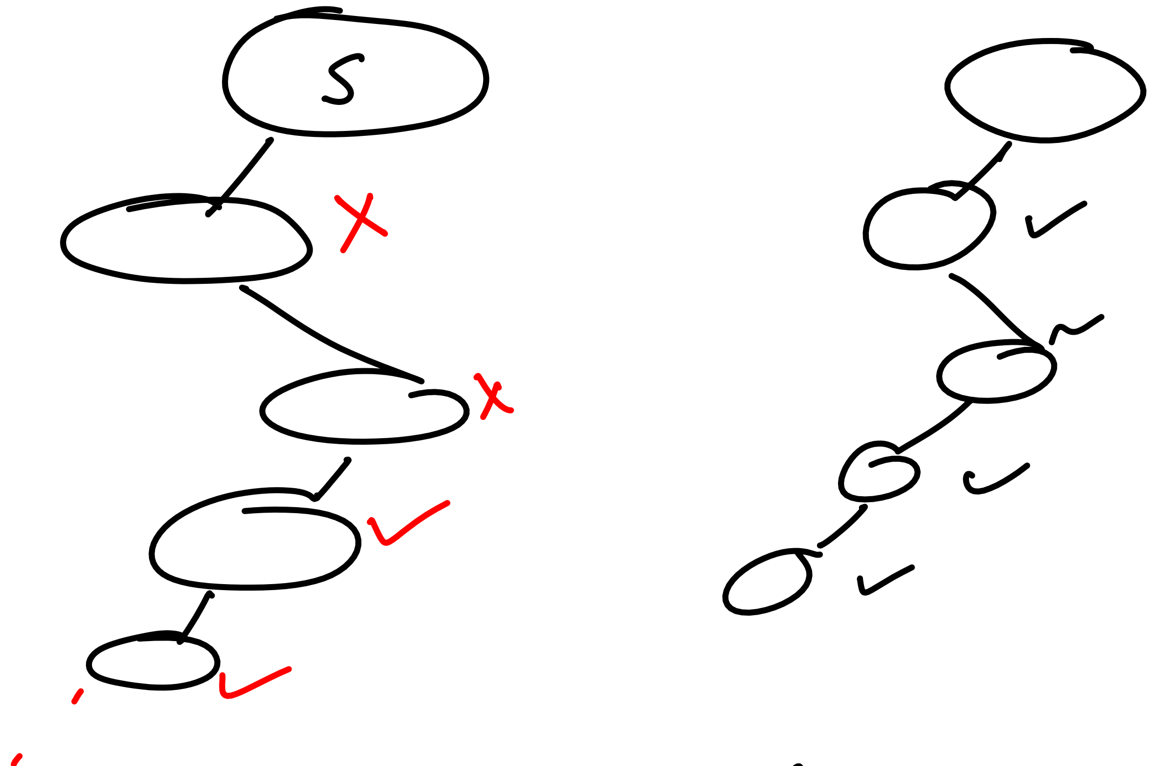
using linearity of expectation

$$E[x+y] = E[x] + E[y]$$

for "any" r.v. x, y (not necessarily independent)

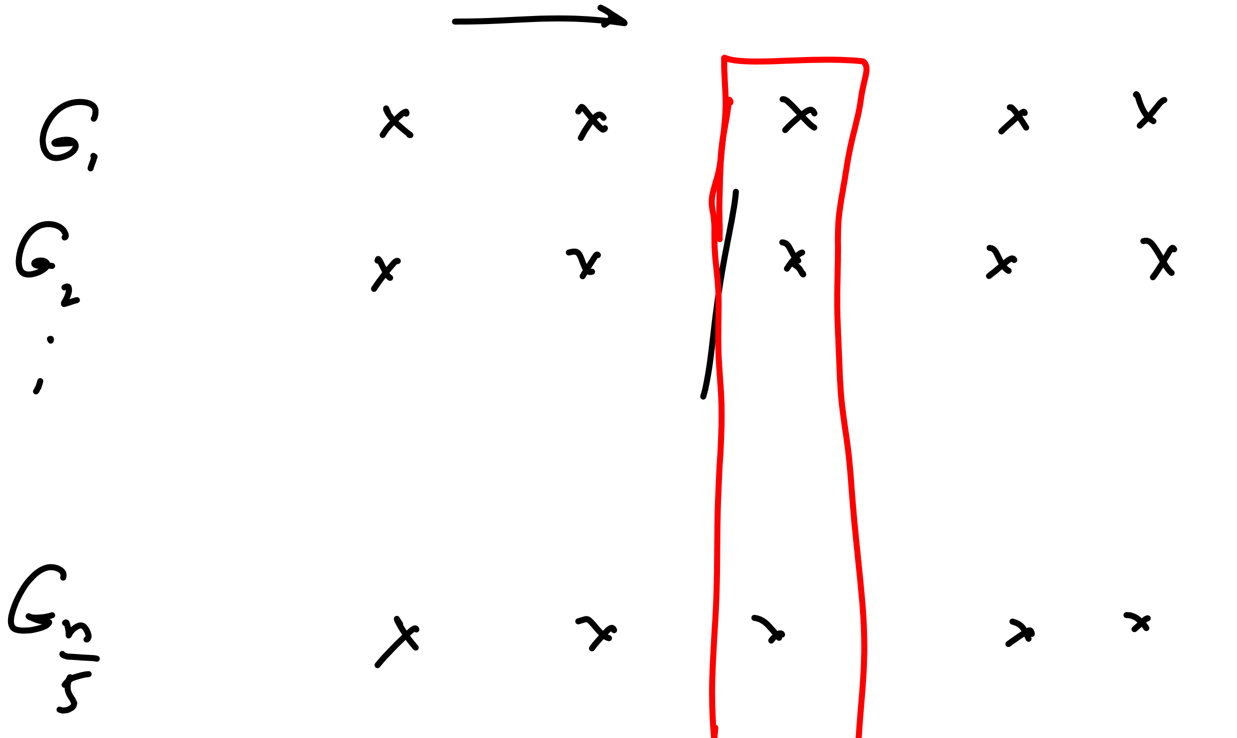
$E[X]$ is $O(cn)$

Not repeating sampling

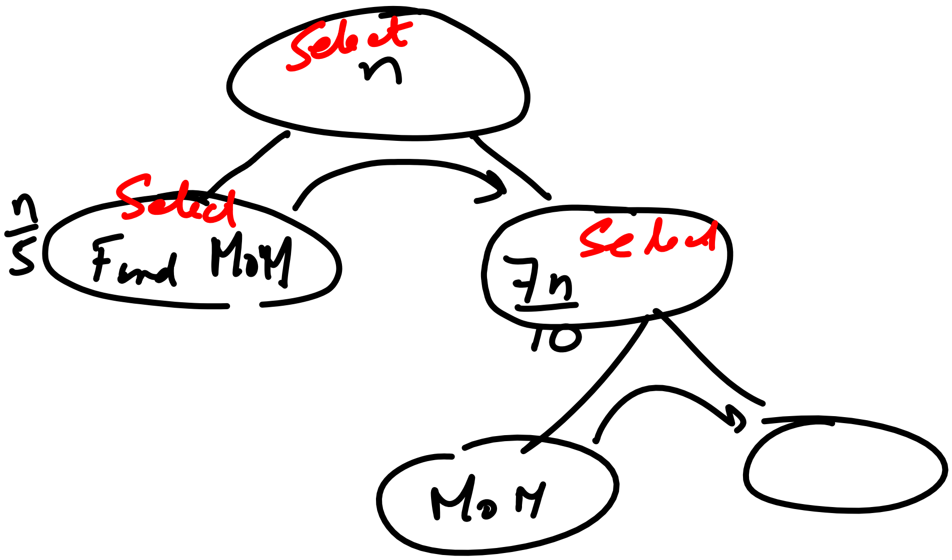


Median-of-median for approximate median

n



Chose the median of medians and that is x



$$T(n) \leq T\left(\frac{n}{5}\right) + T\left(\frac{7n}{10}\right) + O(n)$$

Solve by guessing $T = cn$ for some approp constant c

$\sim \quad c$

$\boxed{\text{Analyse the Space complexity of this algorithm}}$