PROBLEM SESSION 2024-01-19

1

4.25 Sampling w/o replacement

$x \in [p-1]$ pick k of them w/o replacement

$$P\left(\begin{matrix}\text{no nonresidue found} \\ \text{w repl.}\end{matrix}\right) = \frac{1}{2^k}$$

w/o repl.

$$\frac{\binom{\frac{p-1}{2}}{k}}{\binom{p-1}{k}} \leftarrow \#\text{residues}$$

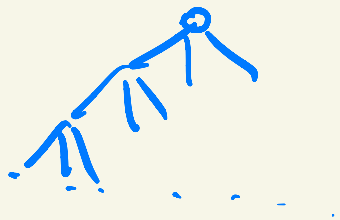
$$= \frac{\frac{p-1}{2}\cdot\left(\frac{p-1}{2}-1\right)\cdots\left(\frac{p-1}{2}-k+1\right)}{(p-1)(p-2)\cdots(p-k)} =$$

$$= \frac{\frac{p-1}{2}}{p-1}\cdot\frac{\frac{p-1}{2}-1}{(p-1)-1}\cdot\frac{\frac{p-1}{2}-2}{(p-1)-2}\cdots\frac{\frac{p-1}{2}-k+1}{p-1-k+1} < \frac{1}{2}\cdots\frac{1}{2} = \frac{1}{2^k}$$

$$> \qquad > \qquad >$$

4.34(a) 14 coins require 3 measurements

(1 fake (heavier / lighter) $\longrightarrow$ 28 outcomes



$28 > 3^3$ # outcomes for ternary decision tree of depth 3

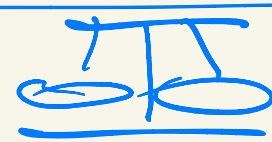
(b) 13 coins 26 outcomes

LEMMA. No benefit to measurement that compare un-equal # coins

Pf: alg. needs to work for case: genuine coins weight 1
fake " $1 \pm \varepsilon$

Case 2: $k \leq 4$
if equal:
5 candidates remain: 10 cases $> 3^2$

1^{st} measurement
k coins vs k coins



Case 1: $k \geq 5$
if unequal:
10 choices $> 3^2$

4.42 (a) find min in $n-1$ comparisons

$x_1 \dots x_n$ ← input

$w := x_1$

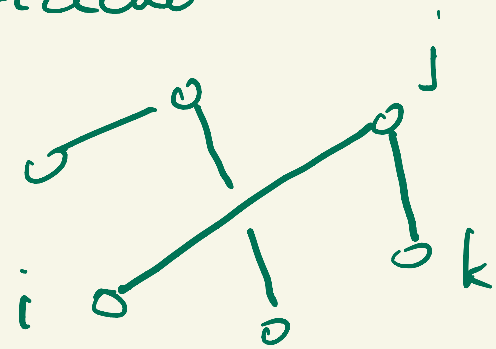
for $i = 2$ to n

  $w := \min(w, x_i)$

endfor

return w

(b) $n-2$ are not sufficient

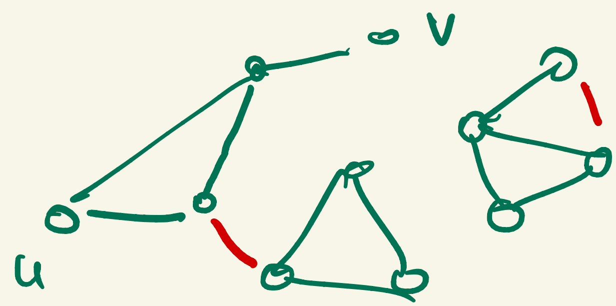


min

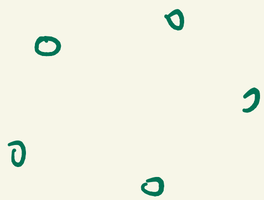
reduce weights of another component to beat purported output

Lemma Connected graph has $\geq n-1$ edges

connected component:



Start:



empty graph — no edges

connected components: $k = n$

at each step # comp's $k \leftarrow \begin{cases} k \\ k-1 \end{cases}$

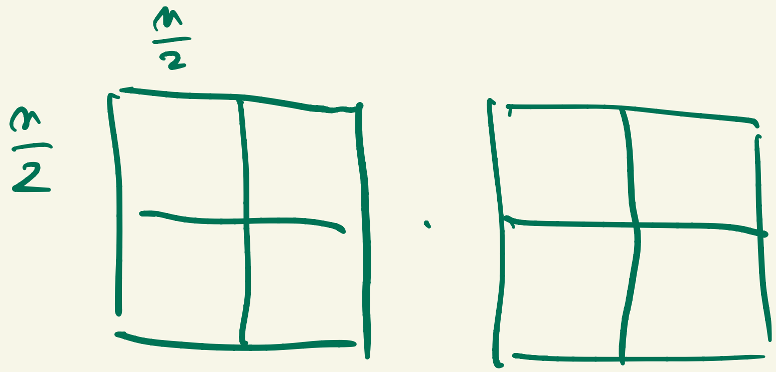
$\therefore$ to make it connected ($k=1$) requires $\geq k-1$ edges

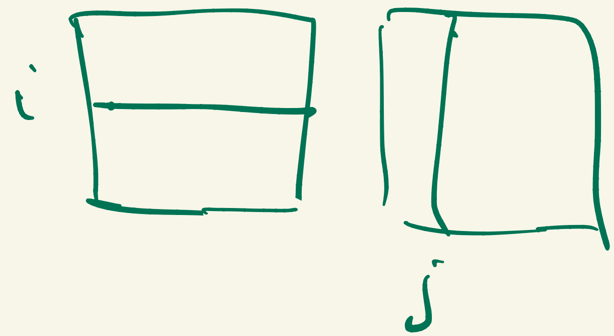
k: potential function

4.55 Strassen's algorithm

real

trivial alg. requires n^3 scalar multiplications





$n = 2^k$

$$M(n) \le 7 \cdot M\left(\frac{n}{2}\right)$$

prove by induction on k: $M(n) \le n^\beta$

$$\beta = \log_2 7$$

$$2^\beta = 7$$

ind. step: $M(n) \le 7 \cdot M\left(\frac{n}{2}\right) \le 7 \cdot \left(\frac{n}{2}\right)^\beta = n^\beta$

$$T(n) \le 7 \cdot T\left(\frac{n}{2}\right) + O(n^2)$$

$$T(n) \le 7T\left(\frac{n}{2}\right) + Cn^2$$

Strategy: guess $g(n) \ge 7g\left(\frac{n}{2}\right) + Cn^2$ and $g(1) \ge T(1)$

then by induction on k: $(\forall n = 2^k)(g(n) \ge T(n))$

$$g(n) := An^\beta - Bn^2$$

Need to guarantee: ① $g(n) \overset{?}{\ge} 7g\left(\frac{n}{2}\right) + Cn^2$

$$\underline{An^\beta} - Bn^2 \overset{?}{\ge} \underline{7A\left(\frac{n}{2}\right)^\beta} - 7B\frac{n^2}{4} + Cn^2$$

$$-B \overset{?}{\ge} -\frac{7}{4}B + C$$

$$\frac{3}{4}B \overset{?}{\ge} C$$

$\boxed{B := \frac{4}{3}C}$ $\xleftarrow{\text{choose}}$

② $g(1) \ge T(1) = 1$

$$A - B \ge 1$$

$\boxed{A := B+1}$

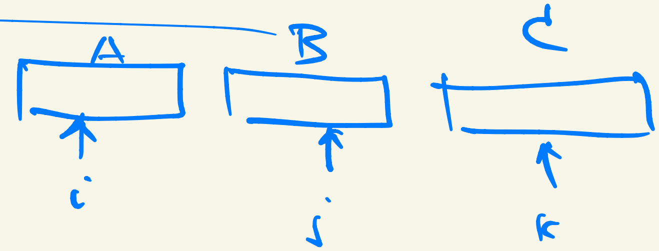
$$g(n) = \left(\frac{4}{3}C+1\right)n^\beta - \frac{4}{3}C \cdot n^2 = O(n^\beta)$$

04.61 MERGE $A[1..m]$ $B[1..n]$ ← input sorted arrays

$C[1..m+n]$ ← output merged - " "

do in $m+n-1$ comparisons

$i := 1$, $j := 1$, $k := 1$



while $i \le m$ and $j \le n$

  if $A[i] \le B[j]$

  then $C[k] := A[i]$

    $i{+}{+}$ $i := i+1$

  else $C[k] := B[j]$

    $j{+}{+}$

  endif

  $k{+}{+}$

endwhile

* continued

if $i = m+1$

then

while $j \leq n$

$C[k] := B[j]$

$j{+}{+}$, $k{+}{+}$

endwhile

else

then

while $i \leq m$

$C[k] := B[i]$

$i{+}{+}$, $k{+}{+}$

endif

return $C[1..k]$

$\not{q}$: $j = n+1$

PNT $\Longrightarrow$

2.42 $\quad p_n \sim n \ln n$

$\pi(x)$: prime counting fctn: # primes $\le x$

PNT $\quad \pi(x) \sim \dfrac{x}{\ln x}$

by def $\quad \pi(p_n) = n$

$n = \pi(p_n) \sim \dfrac{p_n}{\ln p_n}$

need: $\ln p_n \sim \ln n$

$p_n \sim n \cdot \ln p_n$

$\ln n \sim \ln \dfrac{p_n}{\ln p_n} = \ln p_n - \ln \ln p_n \sim \ln p_n$ ✓

b/c $\ln \ln p_n = o(\ln p_n)$

CH $P(x) = \prod_{p \le x} p$

$\ln P(x) \sim x$ [$\Longleftrightarrow$ PNT]

$$\sum_{p \le x} \underline{\ln p} \le \pi(x) \cdot \underline{\ln x} \sim \frac{x}{\ln x} \cdot \ln x = x$$

#terms $\pi(x)$

meaning: for most $p \le x$

$\ln p \sim \ln x$

$\nu^*(n) = \max\{\nu(k) \mid k \le n\}$

$\nu(k) = \#$ distinct prime divisors of k

LEMMA $\nu^*(n) = t \iff$

$$P(p_t) \le n < P(p_{t+1})$$

LEMMA $p_t \sim t \cdot \ln t$

$$\underline{p_t} \sim \ln P(p_t) \le \underline{\ln n} < \ln P(p_{t+1}) \sim p_{t+1} \sim \underline{p_t}$$

LEMMA $\frac{p_{t+1}}{p_t} \to 1$

Pf

$p_t \sim t \ln t$

$\frac{p_{t+1}}{p_t} \sim \frac{(t+1)}{t} \cdot \frac{\ln(t+1)}{\ln t}$

$\frac{t+1}{t} \to 1$, $\frac{\ln(t+1)}{\ln t} \to 1$

$t+1 \sim t$

$\ln(t+1) \sim \ln t$

$\therefore \ln n \sim p_t$

THM $\nu^*(n) \sim \frac{\ln n}{\ln \ln n}$

$\nu^*(n) = t$

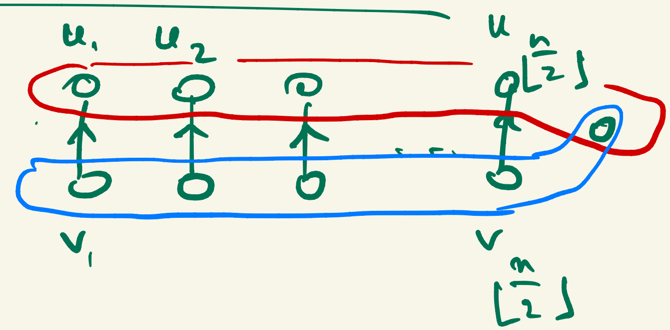
We know

$\underline{\ln n} \sim p_t \sim \underline{t \cdot \ln t}$

$t \sim \frac{\ln n}{\ln t} \sim \frac{\ln n}{\ln \ln n}$

$\underline{\ln \ln n} \sim \ln t + \ln \ln t \sim \underline{\ln t}$

4.45 Find max and min of $x_1 \ldots x_n$ in $\leq \frac{3n}{2}$ comparisons



max

min

$$\left\lfloor \frac{n}{2} \right\rfloor + 2\left(\left\lceil \frac{n}{2} \right\rceil - 1\right) \leq \frac{3n}{2}$$

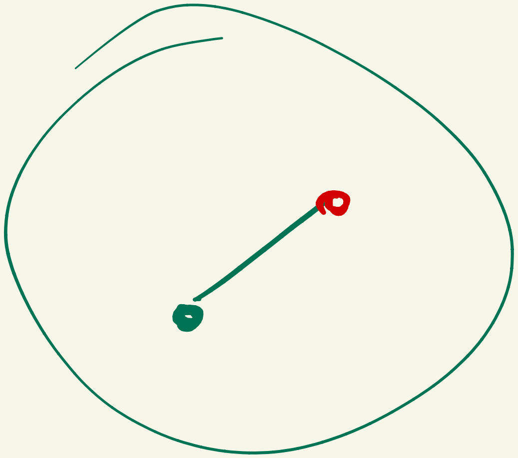
OPTIMAL, see Cormen - Leiserson - Rivest - Stein text

another great text on algorithms: Kleinberg - Tardos

INAPPROXIMABILITY OF CHROMATIC NUMBER

by $\leq n^{\varepsilon}$ colors

requires $\geq n^{1-\varepsilon}$ colors



JOHAN HÅSTAD

P

puzzles solvable in poly time

NP

nondeterministic poly time