HONORS ALGORITHMS | 2025-02-10

p 1

$h(n)$ grows exponentially
if $\exists c>0$

$$h(n) = \Omega(\exp(n^c))$$

Example: $e^{\sqrt{n}}$

lower bound

$$n! > \left(\frac{n}{e}\right)^n > 2^n \leftarrow \text{if } n>7$$

Simply exponential growth

$$< \begin{array}{l} \exp(O(n)) \\ \exp(\Omega(n)) \\ \exp(\Theta(n)) \end{array}$$

$\frac{\ln x}{x} \to 0 \overset{\forall \varepsilon > 0}{\Longrightarrow} \frac{\ln x}{x^{\varepsilon}} \to 0$ BOOTSTRAPPING

$\boxed{p2}$

EX. Exponential decay beats polynomial growth

If f grows polynomially
and g " exponentially
then $f(n) = o(g(n))$
i.e. $\frac{f(n)}{g(n)} \to 0$

---

example: $\frac{n^{100}}{e^{\sqrt{n}}} \to 0$

Do NOT USE L'Hôpital
just substitution of var's

$\frac{\ln x}{x} \to 0$

BARON MUNCHHAUSEN

predicate $P : \Omega \to \{0,1\}$

on a set Ω

domain codomain

N/Y

F/T

$a \in \Omega$

$P(a)$ means $P(a)=1$

$P(a) \iff Q(a)$

$P(a)$ & $Q(a)$

Configuration:
assignment to each variable

$\mathcal{C}$ = configuration space

feasible [illegible] : can occur
in actual run
of algorithm

$x_i \in D_i$ $\quad$ D_i domain of x_i

e.g. $\quad$ x_i is Boolean: $D_i = \{0,1\}$
x_i is real: $D_i = \mathbb{R}$

$$\mathcal{C} = D_1 \times \cdots \times D_N$$

$X \in \mathcal{C}$

$(*)$ **while** P **do** T

predicate on $\mathcal{C}$ — $P : \mathcal{C} \to \{0,1\}$

"set of instructions" — $T : \mathcal{C} \to \mathcal{C}$

DEF predicate $R : \mathcal{C} \to \{0,1\}$ is a loop-invariant for the loop $(*)$ if

$$(\forall X \in \mathcal{C})\big(P(X) \wedge R(X) \Rightarrow \boxed{R(T(X))}\big)$$

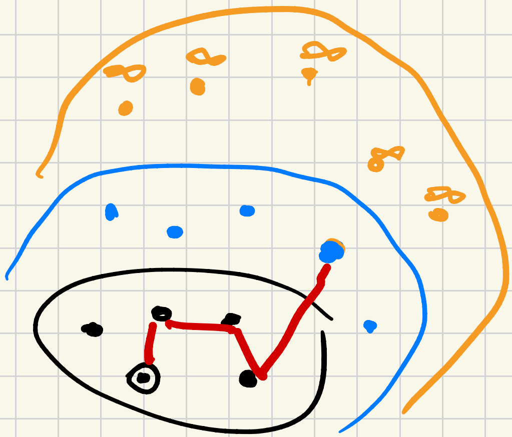
X enters while loop

AND

$\therefore$ If $P(X) \wedge R(X)$ true at the beginning of executing the while loop in iteration $\Rightarrow$ $R(X)$ true at the end (on exit)

EXAMPLE DIJKSTRA

R_4 $\left\{ \begin{array}{l} (\forall x \in V) \\ \quad q(x) \text{ is the min} \\ \text{cost of reach } x \\ \text{entirely through} \\ \text{black vertices} \end{array} \right.$



R_1 : $(\forall u)(u \in Q \iff status(u) = GRAY)$ **L.I.**

R_2 : $(\forall u)(\, status(u) = WHITE \implies q(u) = \infty)$ **L.I.**

$\not\Longleftarrow$

R_3 : $(\forall u,v)(\text{if } status(u) = BLACK \wedge status(v) \neq BLACK$ then $q(u) \leq q(v))$

not a L.I.

BUT $R_1 \wedge R_2 \wedge R_3$ is a L.I.

$R_1 \wedge \cdots \wedge R_4$ is a L.I.

Computing 2^N is exp. time
and exp space:
output has exp many digits

namely if $b(N) = n$ $\Longrightarrow N \geq 2^{n-1}$
then $b(2^N) = N+1 > \underbrace{2^{n-1}}_{\text{exponential}}$

$\underbrace{\exp((\ln 2)\cdot(n-1))}_{\Omega(n)}$

MODULAR EXPONENTIATION

INPUT: a, b, m

OUTPUT: $(a^b \bmod m)$