Lecture 1 Asymptotic Notations, Euclid's algorithm

Tuesday, January 7, 2020 11:23 AM

- Asymptotic notations

  measure roughly how fast a function grows

  function: $f(n)$: running time of an algorithm on an input of size n

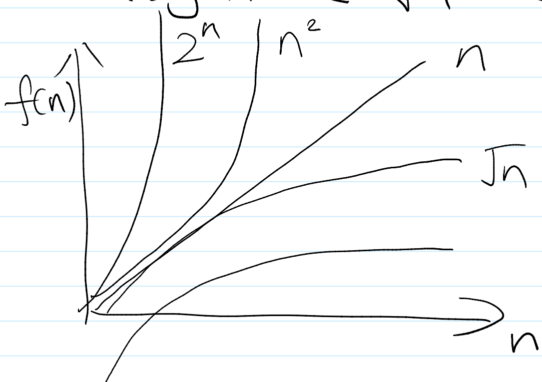
- Definitions
  - $f(n) = O(g(n))$, if there exists constants $\boxed{C > 0,\ n_0 > 0}$ s.t. for every $n \geq n_0$, $f(n) \leq C \cdot g(n)$

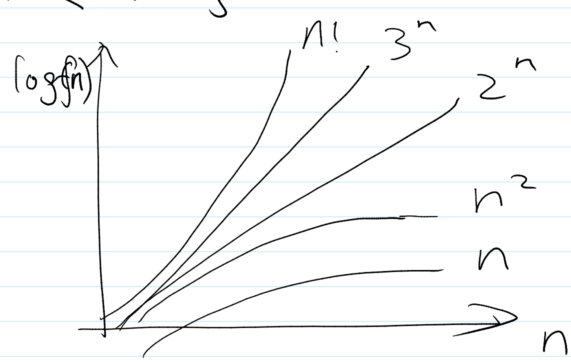
    $(\leq)$ (upperbound on $f(n)$)
  - $f(n) = \Omega(g(n))$, if there exists constants $C > 0$, $n_0 > 0$ s.t. for every $n \geq n_0$, $f(n) \geq C \cdot g(n)$

    $(\geq)$ (lowerbound on $f(n)$)
  - $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$, and $f(n) = \Omega(g(n))$

    $(\approx)$

$$\log n < \sqrt{n} < n < n \log n < n^2 < n^3 < 2^n < n!$$





- Examples

① $f(n) = 3n^2 + 6n$, $f(n) = O(n^2)$

Proof: Choose $C = 9$, $n_0 = 1$

for every $n \geq n_0 = 1$, $n^2 \geq n$

$f(n) = 3n^2 + 6n \leq 9n^2 = 9\ g(n)$ $\square$

② $f(n) = n\log_2 n$, then $f(n) \neq O(n)$ c n^2

Proof Idea:: need to prove

for every $C>0$, $n_0>0$, can find

some n s.t. $\boxed{n \geq n_0}$, but $\boxed{n\log_2 n > C\cdot n}$

$\Downarrow$

$\log_2 n > c$

$n > 2^c$

Proof: for every $C>0$, $n_0>0$

can choose n s.t. $n \geq n_0$, $n > 2^c$

for this n, $n\log_2 n > C\cdot n$, this contradicts with the definition of $f(n) = O(g(n))$ $\square$

- reason to use asymptotic notation

for $i = 1$ to $n-1$

for $j = i+1$ to n

do something 1

$f(n) = (n-1) + (n-2) + \cdots + 1$

$f(n) = \frac{n(n-1)}{2}$

$f(n) \leq \underbrace{n + n + \cdots + n}_{n-1} = n(n-1) = O(n^2)$

- Euclids algorithm
  - greatest common divisor (gcd)

gcd(a,b) : largest number c that divides both a and b

gcd(12, 20) = 4 12/4 = 3 20/4 = 5

gcd(a, b)

if b == 0 then return(a)

else return $\underline{\gcd(b, \overline{a \bmod b})}$

$\gcd(12, 20) = \gcd(20, 12) = \gcd(12, 8) = \gcd(8, 4)$
$= \gcd(4, 0)$
$= 4$

Proof idea: recursion $\Longrightarrow$ induction

do induction on b

(IH) induction hypothesis: whenever $b \le n$, $\gcd(a, b)$ returns the correct greatest common divisor of a, b.

base case: $n = 0$, $\gcd(a, 0)$ returns the correct number.

greatest common divisor of $a, 0$ is a

induction step: Suppose IH is true for n

want to prove IH is also true for $n+1$

if $b = n+1$ $\gcd(a, b)$ returns $\gcd(b, a \bmod b)$

by IH, $\gcd(b, a \bmod b)$ is the greatest common divisor of b and $(a \bmod b)$

need: $\underline{\gcd(a, b) = \gcd(b, a \bmod b)}$

going to prove: any k that divides a, b also divides b, $a \bmod b$, and vice versa

k divides $a, \underline{b} \Longrightarrow k$ divides $\underline{b}, a \bmod b$

$\frac{a}{k}$ $\frac{b}{k}$ are integers

$a \bmod b = a - h \cdot b$ for some integer h

$$\frac{a \bmod b}{k} = \frac{a - hb}{k} = \frac{a}{k} - h \cdot \frac{b}{k} = \text{integer}$$

integers

$\square$

complete proof:

complete proof:

Prove using induction.

Induction Hypothesis: for any $b \le n$, $\gcd(a,b)$ computes the greatest common divisor correctly.

base case: if $b=0$, then $\gcd(a,0)$ outputs a, which is correct.

induction: suppose IH is true for $b \le n$, when $b = n+1$

algorithm outputs $\gcd(b, a \bmod b)$

since $0 \le a \bmod b \le n$, by IH we know Euclid's algorithm computes $\gcd(b, a \bmod b)$ correctly.

Therefore we only need to show $\gcd(b, a \bmod b) = \gcd(a,b)$

we do that by showing the set of common divisors for (a,b) and $(b, a \bmod b)$ are the same, which is to say

① if k is a common divisor of (a,b), then k is also a common divisor of $(b, a \bmod b)$

② if k is a common divisor of $(b, a \bmod b)$, then k is also a common divisor of (a, b)

Proof of ①: by definition we know $a \bmod b = a - zb$ for some integer z.

now: $\frac{a \bmod b}{k} = \frac{a - zb}{k} = \frac{a}{k} - z \cdot \frac{b}{k}$

since k is a common divisor of (a,b), $\frac{a}{k}$, $\frac{b}{k}$ are integers

hence $\frac{a \bmod b}{k} = \frac{a}{k} - z \cdot \frac{b}{k}$ is also an integer

k divides both b and $a \bmod b$.

Proof of ② by definition we know $a \bmod b = a - zb$ for some integer z.

now: $\frac{a}{k} = \frac{(a \bmod b) + zb}{k} = \frac{a \bmod b}{k} + z\frac{b}{k}$

since k is a common divisor of $(b, a \bmod b)$ $\frac{b}{k}$, $\frac{a \bmod b}{k}$ are integers

hence $\frac{a}{k} = \frac{a \bmod b}{k} + z\frac{b}{k}$ is also an integer

k divides both a and b. $\square$