Today:
- more fun w/ big-Oh
- Complexity of algs
- mod, div, gcd...

"f is $O(g)$" $\Rightarrow$ $f \leq g$ with 2 caveats:
- for big inputs
- up to a constant factor

def'n: $\exists c > 0.\ \exists N_0 > 0.\ \forall n > N_0.\ f(n) \leq c \cdot g(n)$

Example: Show $4n^2 + 17n \in \underbrace{O(n^3)}_{\text{a set}}$

Scratch work:

$4n^2 + 17n \leq \underbrace{?}\, n^3$

$4n^2 + 17n \leq 4n^3 + 17n^3 = 21 n^3$

Take $c = 21$
good when $n \geq 1$.
Take $N_0 = 1$.

My soln: Yes, $4n^2 + 17n \in O(n^3)$:
Take $c = 21$, $N_0 = 1$ in def'n of big-oh:

$\forall n \geq 1$, $4n^2 + 17n \leq 4n^3 + 17n^3 = 21n^3 = c \cdot n^3$.

Q.E.D.

Is $4n^2 + 17n \leq c \cdot n^2$ for some c whenever $n > \_\_$?

$4n^2 + 17n \leq 4n^2 + 17n^2 = \underbrace{21}_{c} n^2$

Yes, $4n^2 + 17n \in O(n^2)$

Is $4n^2 + 17n \leq c \cdot n$, for some c, whenever $n > \_\_$?

Try $c = 1000$: Not good enough,
since $4 \cdot (1000^2) + 17 \cdot 1000 \overset{?}{\leq} \underbrace{1000}_{c} \cdot 1000$

$$\underline{\neg \exists x. (H(x) \land R(x))}$$

$$\overset{?}{\neq} \quad \forall x. (\neg H(x) \land \neg R(x))$$

$$\equiv \quad \forall x. \neg (H(x) \land R(x))$$

$$\equiv \quad \forall x. (\neg H(x) \lor \neg R(x))$$

$C(x) \equiv x$ has a Cat

$F(x) \equiv$ Ferret

$D(x) \equiv$ Dog

Give formula: for each animal, somebody owns that type of animal.

$$\cancel{\exists x. (C(x) \land F(x) \land D(x))}$$

$$(\exists x. C(x)) \land \boxed{(\exists v. D(v))} \land (\exists w. F(w))$$

$$\equiv \exists x. \exists v. \exists w. (C(x) \land D(v) \land F(w))$$

How to prove

$g(n)=n$

$f(n) = 4n^2 + 17n$ is not $O(n)$?

I need to show

$\neg\left(\exists c \geq 0, N_0 \geq 0.\ \forall n > N_0,\ f(n) \leq c \cdot g(n)\right)$

That is, show:

$\forall c \geq 0\ \forall N_0 \geq 0.\ \neg\left(\forall n > N_0,\ f(n) \leq c \cdot g(n)\right)$

We show by direct proof:
For arbitrary c, N_0 we'll show
$\neg(\forall n > N_0,\ f(n) \leq c\,g(n))$.

That is:

$\exists n > N_0.\ \neg\left(f(n) \leq c \cdot g(n)\right)$

$\equiv \quad \exists n > N_0.\ f(n) > c \cdot g(n)$.

Take $n^* = \max(c+1, N_0) \geq c$.
Then:

$$
\begin{aligned}
f(n^*) &= 4(n^*)^2 + 17(n^*) \\
&\geq 4(n^*)(n^*) + \boxed{17(n^*)} \\
&\geq 4(n^*)(n^*) \\
&\geq 4(c)(n^*) \\
&\geq c \cdot n^* = c \cdot g(n^*)
\end{aligned}
$$

$433x \geq 400x$

Thus $4n^2 + 17n$ is not in $O(n)$.
Q.E.D.

define $\sum_{i=1}^{n} i^3$ means

```
sum=0
for (i=1, i≤n, ++i){
    sum += i^3
}
```

Ex: $\sum_{i=7}^{10} i^2 = 7^2+8^2+9^2+10^2 = 300\text{ish}$

Problem: Show $\sum_{i=1}^{n} i^3 \in O(n^4)$

Sol'n:

$$\sum_{i=1}^{n} i^3 = \underbrace{1^3+2^3+3^3+\cdots+n^3}_{n \text{ terms}}$$

want $\le c \cdot n^4$

for some c, whenever n > some N_0.

$$\le n^3+n^3+n^3+\cdots+n^3+n^3$$

$$= n \cdot n^3 = n^4$$

$\le 1 \cdot n^4$

→ $f \in o(g)$ means "$f < g$"

→ $f \in O(g)$ means "$f \leq g$" w/ 2 caveats

→ $f \in \Theta(g)$ means $f = g$

→ $f \in \Omega(g)$ means "$f \geq g$"

→ $f \in \omega(g)$ means "$f > g$"

$4n^2 + 17n \leq n^2$ so $4n^2+17n$ is $\Theta(n^2)$

def'n: f is $\Theta(g)$ iff $f \in O(g) \wedge g \in O(f)$.

What is running-time of
insert: number × sorted list-of-numbers → sorted-list-of-nums?

Ans: $\Theta(n)$, worst-case, where n size of list.

What is running time of insert-sort?

I do insert on a list of size 0, then insert into list of size 1, ... size 2, ... size 3, ... size n.

takes time 1, 2, 3, 4, 5, ...

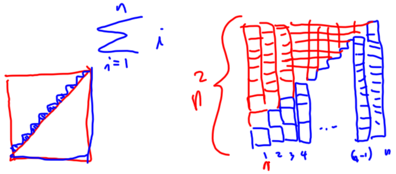
total: $\sum_{i=1}^{n} i = \underbrace{1+2+3+\cdots+n}_{n \text{ times}}$

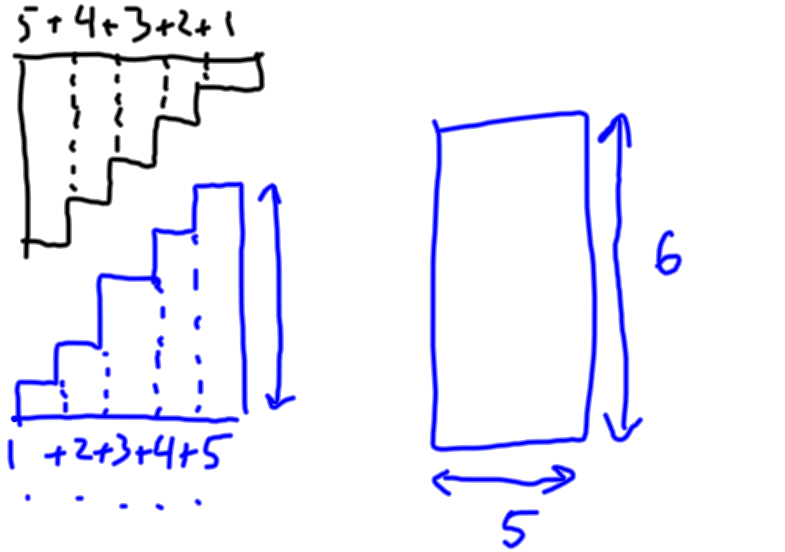
$\leq n+n+n+\cdots+n$

$= n^2$

∴ Insert-sort runs in time $O(n^2)$.

$\sum_{i=1}^{n} i$





Let $S = 1+2+3+4+5$

$+\ S = 5+4+3+2+1$

$2S = 6+6+6+6+6$

Then $2S = 5\cdot 6$, so $S = \frac{30}{2} = 15$

If $S = 1+2+3+\cdots+n$

number of items

the average

Then $2S = n\cdot(n+1)$, so $\boxed{S = \frac{n(n+1)}{2}}$

Arithmetic … integers.

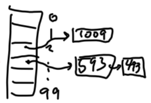
- "n is prime" def'n:
  "$\forall a.\ a|n \rightarrow (a=1 \vee a=n)$"
- "a divides b", "$a|b$"
  means: "$\exists k.\ b=k\cdot a$"
- "a mod b" is the remainder after dividing a by b. ($a \% b$, in C/Java/Algol)

Uses in programming:

- boolean divides(a,b) {
  return((b%a) == 0);
  }

  $|(a,b) = ((b \% a)==0);$
- hashing: put an Object obj into slot obj.hashcode() % k

  size of array



Modular arithmetic:

"$a \equiv b \pmod m$" means:

$m | a-b$.

(a.k.a.: $a\%m = b\%m$.)

Greatest common divisor ("gcd")

of two numbers a,b: is the largest numbers which divides both.

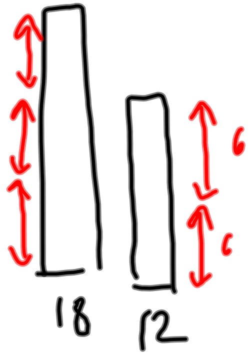
def'n: "$n = \gcd(a,b)$" means:

$\gcd(12,18)=6$ (a = 12, b = 18)
$\gcd(2,20)=2$
$\gcd(17,19)=1$

$$(n|a \wedge n|b) \wedge \forall m.\ (m|a \wedge m|b \rightarrow n \geq m)$$

"n is biggest"

"if m is also a common divisor, then $n \geq m$"



$$\gcd(18,12)=6$$

$$\gcd(17,19)=1$$

$$\gcd(2,20)=2$$

$$\gcd(1726,432)$$

$$=\gcd(432,\ 1726 \% 432)$$

$$=\gcd(432,430)$$

$$=\gcd(430,\ 432 \% 430)$$

$$=\gcd(430,2)$$

$$=2$$