

To determine the cost of an algorithm let $T(n)$ be the number of operations that the algorithm does for an input of size n .

If $T(n) = 3n^2 + 2n + 5$ we say the algorithm is quadratic in n .

For large n the term $3n^2$ dominates the cost of the alg.

Definition: Let $n \in \mathbb{N}$ and $f: \mathbb{N} \rightarrow \mathbb{R}$ and $g: \mathbb{N} \rightarrow \mathbb{R}$.

We say g dominates f if $\exists c > 0$ and $\exists k \in \mathbb{N}$

such that $|f(n)| \leq c |g(n)|$ for $n \geq k$.

Define $O(g(n)) = \{ f(n) : g(n) \text{ dominates } f(n) \}$.

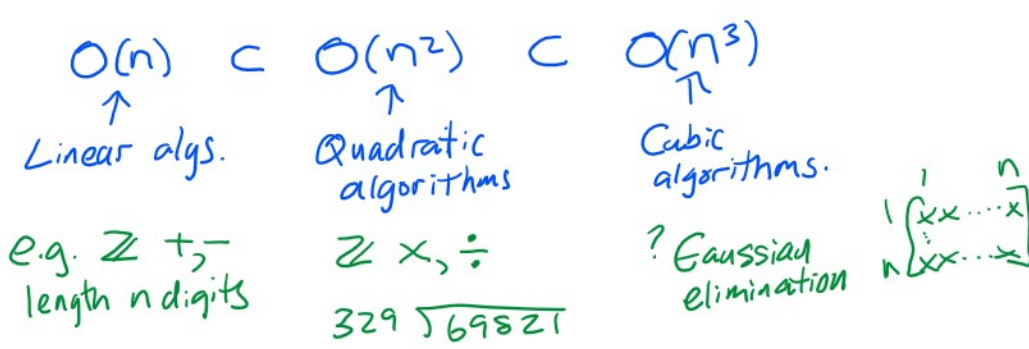
Examples.

$$2n^2 + 5 \in O(n^2) \text{ because } 2n^2 + 5 \leq 7n^2 \text{ for } n \geq 1$$

$$3n + 1 \in O(n^2) \text{ because } 3n + 1 \leq 4n^2 \text{ for } n \geq 1$$

$$n^3 \notin O(n^2) \text{ because } n^3 \not\leq cn^2 \text{ for } n > c$$

So $O(n^2) = \{ an^2 + bn + c, an + b, a \cdot n^{1.5} + bn + c, n \log_2 n, \dots \}$



How do we show $O(f(n)) = O(g(n))$? $O(3n^2 + 1) = O(n^2 + 2n)$?

We show $O(f(n)) \subset O(g(n))$ and $O(g(n)) \subset O(f(n))$.

I claim if $f(n) \in O(g(n))$ then $O(f(n)) \subset O(g(n))$.

Proof: Suppose $f(n) \in O(g(n)) \Rightarrow |f(n)| \leq c_1 |g(n)| \text{ for } n \geq k_1$.

Let $h(n) \in O(f(n)) \Rightarrow |h(n)| \leq c_2 |f(n)| \text{ for } n \geq k_2$

$\Rightarrow |h(n)| \leq c_2 \cdot [c_1 |g(n)|] \text{ for } n \geq \max(k_1, k_2)$.

$= c_1 \cdot c_2 |g(n)| \text{ for } n \geq \dots$

$$\Rightarrow h(n) \in O(g(n)).$$

Exercise: For $a > 1$ and $b > 1$ show $O(\log_a n) = O(\log_b n)$.
 Hint: $\log_a n = \frac{\ln n}{\ln a}$. $= O(\log n)$

Properties of $O(g(n))$.

- ① $O(cf(n)) = O(f(n))$ for any constant $c > 0$.
 E.g. $O(3n^2) = O(n^2)$. Proof: Exercise.
- ② If $f(n) \in O(g(n))$ then $O(|f(n)| + |g(n)|) = O(|g(n)|)$.
 E.g. $O(\underbrace{3n^2}_{g(n)} + \underbrace{2n+11}_{f(n)}) \stackrel{②}{=} O(3n^2) \stackrel{①}{=} O(n^2)$.
- ③ $f(n) \cdot O(g(n)) = O(f(n) \cdot g(n))$ e.g. $2n \cdot O(n) = O(2n^2)$.

Often we want to add $O(f(n)) + O(g(n))$. For example

Algorithm foo

$$\begin{array}{l} \text{Step 1} \dots\dots \leq \underline{2n \log_2 n + n} \in \underline{O(n \log n)} \\ \text{Step 2} \dots\dots = 3n^2 + 2n - 1 \in O(n^2) \\ \text{Step 3} \dots\dots = 2n + 5 \in O(n) \end{array}$$

$$O(n \log n) + O(n^2) + O(n) = O(\underline{n \log n} + n^2 + n) = O(n^2)$$

Define $O(f(n)) + O(g(n)) = O(|f(n)| + |g(n)|)$
 E.g. $O(1+n^2) + O(n^2) = O(1+2n^2) = O(n^2)$.

Suppose $f(x), g(x) \in \mathbb{Z}[x]$ of degree n .

Suppose we want to compute $h(x) = f(x) \cdot g(x) \pmod{x^{n+1}}$

$$\text{E.g. } \underbrace{(1+2x)}_{n=1} \cdot \underbrace{(2+3x)}_{n=1} \pmod{x^2} = 1 \cdot 2 + (1 \cdot 3 + 2 \cdot 2) \cdot x^1 = 2 + 7x$$

$$\text{Let } f(x) = a_0 + a_1 x + \dots + a_n x^n$$

$$\text{and } g(x) = b_0 + b_1 x + \dots + b_n x^n$$

$$\text{Let } h(x) = c_0 + c_1 x + \dots + c_n x^n$$

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + b_0 a_1$$

$$\vdots$$

$$\begin{aligned}
C_0 &= a_0 b_0 \\
C_1 &= a_0 b_1 + b_0 a_1 \\
C_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\
&\vdots \\
C_n &= a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0.
\end{aligned}$$

Algorithm SeriesMult.

```

for k = 0, 1, ..., n do # compute C_k
  C_k = 0
  for i = 0, 1, ..., k do
    C_k = C_k + a_i * b_{k-i}
  
```

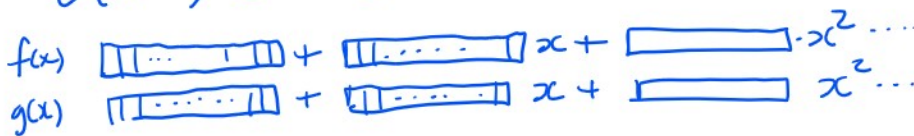
} $\leftarrow z^{(k+1)} \in O(k)$.

Let $T(n)$ be the # of arithmetic operations in \mathbb{Z} that alg. SeriesMult does.

$$\begin{aligned}
T(n) &= \sum_{k=0}^n z_{k+z} = \sum_{k=0}^n z_k + \left(\sum_{k=0}^n z \right) \\
&= z \sum_{k=0}^n k + z(n+1) \\
&= z \frac{n(n+1)}{2} + z(n+1) = (n+1)(n+2) \in O(n^2)
\end{aligned}$$

$$\begin{aligned}
T(n) &= \sum_{k=0}^n O(k) = O(0) + O(1) + O(2) + \dots + O(n) \\
&= O(0 + 1 + 2 + \dots + n) \\
&= O\left(\frac{n(n+1)}{2} = \frac{n^2}{2} + \frac{n}{2}\right) = O(n^2) \text{ arithmetic operations in } \mathbb{Z}.
\end{aligned}$$

Question: Is the time complexity of Algorithm SeriesMult $O(n^2)$? No.



The time will also depend on the cost of the coefficient arithmetic.