- Asymptotic notations
  - notations that measures roughly how much time/space an algorithm requires
  - intuition: \( n^2 \) similar to \( 3n^2 + 5n \), not similar to \( 2^n \)

\[
\begin{align*}
\text{f}(n) &< g(n) \quad \text{if for every } n \geq n_0, \quad f(n) \leq C \cdot g(n) \\
\Omega(g(n)) &\quad \text{if for every } n \geq n_0, \quad f(n) \geq C \cdot g(n) \\
\Theta(g(n)) &\quad \text{if } f(n) = O(g(n)) \text{ and } f(n) = \Omega(g(n))
\end{align*}
\]

- Definitions
- \( f(n) = O(g(n)) \) if there exist constants \( C > 0 \) and \( n_0 \) such that \( f(n) \leq C \cdot g(n) \)
- \( f(n) = \Omega(g(n)) \) if \( f(n) \geq C \cdot g(n) \)
- \( f(n) = \Theta(g(n)) \) if \( f(n) = O(g(n)) \) and \( f(n) = \Omega(g(n)) \)

- Examples:
  1. \( 3n^2 + 5n = O(n^2) \)
     
     Proof: let \( C = 8 \), \( n_0 = 1 \), then for any \( n \geq n_0 \)
     
     \[
     \begin{align*}
     3n^2 + 5n &\leq 2n^2 + 5n^2 = 8n^2 \\
     f(n) &\leq g(n)
     \end{align*}
     \]
  2. \( 2^n \neq O(n^3) \)
     
     Proof: for any constant \( C \) and \( n_0 \), can choose \( n \) s.t. \( n \geq \max \{1024, 2^{\log_2 n_0}\} \)

\[
\begin{align*}
2^n &\geq C \cdot n^2 \\
(\log_2 2^n) &\geq (\log_2 Cn^2) \quad \text{when } n \geq 1024
\end{align*}
\]
\[
\frac{2^n}{n} \geq \frac{\log_2 n^2}{\log_2 C + 2 \log_2 n}
\]

when \( n \geq 1024 \)

\[
n \geq 4 \log_2 n \Rightarrow n - 2 \log_2 n \geq \frac{n}{2} \geq \log_2 C
\]

\[
2^n \geq C n^2
\]

**Proof:** first, we claim that when \( n \geq 1024 \)

\[
n \geq 4 \log_2 n
\]

now, for any constants \( C \) and \( n_0 \), choose

\[
n > \max\{1024, 2 \log_2 C, n_0\}, \text{ we have}
\]

\[
n - 2 \log_2 n \geq n - \frac{n}{2} = \frac{n}{2} > \log_2 C, \text{ so } n > \log_2 C + 2 \log_2 n
\]

\[
n \geq 4 \log_2 n \quad \text{(take } 2^n \text{ on both sides)}
\]

3. \( \log n < \ln n < n < n \log n < n^2 < n^3 < 2^n < 2^n \)

\[\text{any base} \]

4. \( \log_2 n = \Theta (\log_3 n) \)

**Proof:** \( \log_2 n = (\log_3 - 1) \log_2 n \)

- asymptotic vs. exact.

for \( i = n-1 \) to 1

for \( j = 1 \) to \( i \)

if \( a[i] > a[i+1] \) then

Sweep \( (a[i], a[i+1]) \)

- what is \# comparison for array of length \( n \)?

\[
T(n) = 1 + 2 + \ldots + (n-1) = \frac{n(n-1)}{2}
\]

much easier to show \( T(n) = \Theta (n^2) \)

\[
T(n) \leq n + n + \ldots + n = n(n-1) \leq n^2 \Rightarrow T(n) = O(n^2)
\]

\[
T(n) \geq \frac{n}{2} + \left( \frac{n}{2} + 1 \right) + \ldots + (n-1)
\]

\[
\geq \frac{n}{2} + \frac{n}{2} + \ldots + \frac{n}{2}
\]
\[
T(n) \geq \frac{n}{2} + \left( \frac{n}{2} + 1 \right) + \cdots + (n-1) \\
\geq \frac{n}{2} + \frac{n}{2^2} + \cdots + \frac{n}{2} \\
\geq \frac{n^2}{4} \\
\Rightarrow T(n) = \Omega(n^2)
\]

- Euclid's algorithm
  - algorithm for computing greatest common divisor (gcd) of two positive integers.

\[\text{gcd}(15, 9) = 3\]

\[
\text{gcd}(a, b) \\
\quad \text{if } b = 0 \\
\quad \quad \text{return } a \\
\text{else} \\
\quad \quad \text{return } \text{gcd}(b, a \mod b)
\]

\[\text{gcd}(15, 9) \Rightarrow \text{gcd}(9, 6) \Rightarrow \text{gcd}(6, 3) \Rightarrow \frac{\text{gcd}(3, 0)}{3} = 3\]

- Proof of correctness:
  - use induction
  - base case: \(b=0\)
    \[\text{gcd}(a, 0) = a\] trivial
  - induction hypothesis: assume \(\text{gcd}(a, b)\) is correct for all \(b \leq n\) \((IH)\)
  - want to prove \((IH) \Rightarrow \text{gcd}(a, b)\) is correct when \(b=n+1\)
  - algorithm: \(\text{gcd}(a, b) \Rightarrow \text{gcd}(b, a \mod b)\)
    \[\text{if } b = n+1 \quad \text{as } a \mod b \leq n\]
    by \((IH)\) algorithm is correct for \(\text{gcd}(b, a \mod b)\)
  - need to prove: \(\text{gcd}(a, b) = \text{gcd}(b, a \mod b)\)
  - proof: will show that set of common divisors are the same for every \(k\), if \(\frac{a}{k}, \frac{b}{k}\) are integers, \(\frac{a \mod b}{k}\) also integer
    \[\text{if } b \text{ and } a \text{ are integers } a, \text{ also integer}\]
for every $k$, if $\frac{a}{k}, \frac{b}{k}$ are integers, $\frac{a - z b}{k}$ also integer.

(1) $a \mod b = a - z b$ where $z$ is an integer

$\frac{a - z b}{k} = \frac{a}{k} - \frac{z b}{k}$ still an integer.

Complete proof:

Prove using induction.

Induction hypothesis: for any $b \leq n$, $\gcd(a, b)$ 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 $b \leq n$, when $b = n + 1$

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

since $0 \leq a \mod b \leq n$, by IH we know Euclid's

algorithm computes $\gcd(b, a \mod b)$ correctly.

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

we do this by showing the set of common divisors for $(a, b)$ and $(b, a \mod b)$ 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 $(b, a \mod b)$

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

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

now: $\frac{a \mod b}{k} = \frac{a - z b}{k} = \frac{a}{k} - \frac{z b}{k}$

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

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

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

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

now: $\frac{a}{k} = \frac{(a \mod b) + z b}{k} = \frac{a \mod b}{k} + \frac{z b}{k}$
some integer $z$.

Now: \[ \frac{a}{k} = \frac{(a \mod b) + z \cdot b}{k} = \frac{a \mod b}{k} + z \cdot \frac{b}{k} \]

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

Hence: \[ \frac{a}{k} = \frac{a \mod b}{k} + z \cdot \frac{b}{k} \]

is also an integer.

$k$ divides both $a$ and $b$. \[ \square \]