Proofs

What is a proof?
A deductive argument showing a statement is true based on previous knowledge (axioms)

Why are they important/useful?
Allows us to be sure that something is true
In algs: allow us to prove properties of algorithms

An example
Prove the sum of two odd integers is even
Proof techniques?
- example/counterexample
- enumeration
- by cases
- by inference (aka direct proof)
- trivially
- contrapositive
- contradiction
- induction (strong and weak)

Proof by induction (weak)
Proving something about a sequence of events by:
1. first: proving that some starting case is true and
2. then: proving that if a given event in the sequence were true then the next event would be true

Proof by induction (weak)
1. **Base case**: prove some starting case is true
2. **Inductive case**: Assume some event is true and prove the next event is true
   a. **Inductive hypothesis**: Assume the event is true (usually k or k-1)
   b. **Inductive step to prove**: What you’re trying to prove assuming the inductive hypothesis is true
   c. **Proof of inductive step**

Proof by induction example
Prove: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
1. **Base case**: prove some starting case is true
2. **Inductive case**: Assume some event is true and prove the next event is true
   a. **Inductive hypothesis**: Assume the event is true (usually k or k-1)
   b. **Inductive step to prove**: What you’re trying to prove assuming the inductive hypothesis is true
   c. **Proof of inductive step**
Base case

Prove: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Show it is true for $n = 1$

$$\sum_{i=1}^{1} i = 1 = \frac{1 \times 2}{2}$$

Inductive case

Prove: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Inductive hypothesis: assume $n = k - 1$ is true

$$\sum_{i=1}^{k-1} i = \frac{(k-1) \times k}{2}$$

Prove:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$
Inductive case: proof

Prove: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$  
IH: $\sum_{i=1}^{k-1} i = \frac{(k-1)k}{2}$

$$
\sum_{i=1}^{k} i = k + \sum_{i=1}^{k-1} i \quad \text{by definition of sum}
$$
$$
= k + \frac{(k-1)k}{2} \quad \text{by IH}
$$
$$
= \frac{2k + (k-1)k}{2}
$$
$$
= \frac{2k^2 + (k-1)k}{2}
$$
$$
= \frac{k^2 + k}{2}
$$
$$
= \frac{k(k+1)}{2}
$$

Why does this work?

Layout of a proof by induction

1. State what you’re trying to prove
   We show that XXX using proof by induction
2. Prove base case
3. State the inductive hypothesis
4. Inductive proof
   a. State what you want to show (may include a variable change, e.g., $k$ in instead of $n$)
   b. Show a step by step derivation from the left hand side resulting in the right hand side. Give justifications for steps that are non-trivial

Inductive proofs

Weak vs. strong?
Inductive proofs

Weak: inductive hypothesis only assumes it holds for some step (e.g., $k$th step)

Strong: inductive hypothesis assumes it holds for all steps from the base case up to $k$

---

Sorting

Input: An array of numbers $A$
Output: The number in sorted order, i.e., $A[i] \leq A[j] \forall i < j$

---

Sorting

What sorting algorithm?

1. for $j \leftarrow 2$ to $\text{length}[A]$
2. $\text{current} \leftarrow A[j]$
3. $i \leftarrow j - 1$
4. while $i > 0$ and $A[i] > \text{current}$
5. $A[i + 1] \leftarrow A[i]$
6. $i \leftarrow i - 1$
7. $A[i + 1] \leftarrow \text{current}$

---

Sorting

Insertion Sort($A$)
1. for $j \leftarrow 2$ to $\text{length}[A]$
2. $\text{current} \leftarrow A[j]$
3. $i \leftarrow j - 1$
4. while $i > 0$ and $A[i] > \text{current}$
5. $A[i + 1] \leftarrow A[i]$
6. $i \leftarrow i - 1$
7. $A[i + 1] \leftarrow \text{current}$
Does it terminate?

Is it correct?

How long does it take to run?

Memory usage?

**Insertion-sort**

```
INSERTION-SORT(A)
1 for j ← 2 to length[A]
2 current ← A[j]
3 i ← j - 1
4 while i > 0 and A[i] > current
5 \[ A[i + 1] ← A[i] \]
6 i ← i - 1
7 A[i + 1] ← current
```

Does it terminate?

**Loop invariant**

A statement about a loop that is true before the loop begins and after each iteration of the loop.

Upon termination of the loop, the invariant should help you show something useful about the algorithm.

```
INSERTION-SORT(A)
1 for j ← 2 to length[A]
2 current ← A[j]
3 i ← j - 1
4 while i > 0 and A[i] > current
5 \[ A[i + 1] ← A[i] \]
6 i ← i - 1
7 A[i + 1] ← current
```

Is it correct? Can you prove it?
Loop invariant

Loop invariant: A statement about a loop that is true before the loop begins and after each iteration of the loop.

At the start of each iteration of the for loop of lines 1-7 the subarray $A[1..j-1]$ is the sorted version of the original elements of $A[1..j-1]$.

\[\text{INSERTION-SORT}(A)\]
\begin{align*}
\text{1} & \text{ for } j \leftarrow 2 \text{ to } \text{length}[A] \\
\text{2} & \quad \text{current} \leftarrow A[j] \\
\text{3} & \quad i \leftarrow j - 1 \\
\text{4} & \quad \text{while } i > 0 \text{ and } A[i] > \text{current} \\
\text{5} & \quad A[i+1] \leftarrow A[i] \\
\text{6} & \quad i \leftarrow i - 1 \\
\text{7} & \quad A[i+1] \leftarrow \text{current}
\end{align*}

Proof by induction
- Base case: invariant is true before loop
- Inductive case: it is true after each iteration

Insertion-sort

Asymptotic notation

How long will it take to run?

How do you answer the question: “what is the running time of algorithm x?”

Talk about the computational cost of an algorithm that focuses on the essential parts and ignores irrelevant details.

You’ve seen some of this already:
- linear
- $n \log n$
- $n^2$
Asymptotic notation

Precisely calculating the actual steps is tedious and not generally useful.

Different operations take different amounts of time. Even from run to run, things such as caching, etc. cause variations.

We want to identify categories of algorithmic runtimes.

For example...

$f_1(n)$ takes $n^2$ steps
$f_2(n)$ takes $2n + 100$ steps
$f_3(n)$ takes $3n + 1$ steps

Which algorithm is better?
Is the difference between $f_2$ and $f_3$ important/significant?

Runtime examples

<table>
<thead>
<tr>
<th>$n$</th>
<th>$n$</th>
<th>$n \log n$</th>
<th>$n^3$</th>
<th>$2^n$</th>
<th>$n!$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>4 sec</td>
</tr>
<tr>
<td>20</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>18 min</td>
</tr>
<tr>
<td>100</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>1 sec</td>
<td>10^{17} years</td>
</tr>
<tr>
<td>1000</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>1 sec</td>
<td>18 min</td>
<td>very long</td>
</tr>
<tr>
<td>10,000</td>
<td>&lt; 1 sec</td>
<td>&lt; 1 sec</td>
<td>2 min</td>
<td>12 days</td>
<td>very long</td>
</tr>
<tr>
<td>100,000</td>
<td>&lt; 1 sec</td>
<td>2 sec</td>
<td>3 hours</td>
<td>32 years</td>
<td>very long</td>
</tr>
</tbody>
</table>

(adapted from [2], Table 2.1, pg. 34)

Big O: Upper bound

$O(g(n))$ is the set of functions:

$$O(g(n)) = \left\{ f(n) : \exists c, n_0 \text{ such that } 0 \leq f(n) \leq cg(n) \text{ for all } n \geq n_0 \right\}$$
**Big O: Upper bound**

\[ O(g(n)) \] is the set of functions:

\[
O(g(n)) = \left\{ f(n) : \text{there exists positive constants } c \text{ and } n_0 \text{ such that } 0 \leq f(n) \leq cg(n) \text{ for all } n \geq n_0 \right\}
\]

We can bound the function \( f(n) \) above by some constant factor of \( g(n) \).

**Example:**

\[
\begin{align*}
f_1(x) &= 3n^2 \\
O(n^2) &= f_2(x) = 1/2n^2 + 100 \\
f_3(x) &= n^2 + 5n + 40 \\
f_4(x) &= 6n
\end{align*}
\]

**Big O: Upper bound**

Generally, we’re most interested in big O notation since it is an upper bound on the running time.
Omega: Lower bound

\( \Omega(g(n)) \) is the set of functions:

\[ \Omega(g(n)) = \left\{ f(n) : \text{there exists positive constants } c \text{ and } n_0 \text{ such that} \right. \]
\[ 0 \leq cg(n) \leq f(n) \text{ for all } n \geq n_0 \]

We can bound the function \( f(n) \) below by some constant factor of \( g(n) \)

Theta: Upper and lower bound

\( \Theta(g(n)) \) is the set of functions:

\[ \Theta(g(n)) = \left\{ f(n) : \text{there exists positive constants } c, c_0 \text{ and } n_0 \text{ such that} \right. \]
\[ 0 \leq c_0 g(n) \leq f(n) \leq c g(n) \text{ for all } n \geq n_0 \]
Theta: Upper and lower bound

$\Theta(g(n))$ is the set of functions:

$$\Theta(g(n)) = \left\{ f(n) : \text{there exists positive constants } c, c', n, \text{ such that } 0 \leq c g(n) \leq f(n) \leq c' g(n) \text{ for all } n \geq n_0 \right\}$$

We can bound the function $f(n)$ above and below by some constant factor of $g(n)$ (though different constants).

Note: A function is theta bounded iff it is big O bounded and Omega bounded.

Visually

$$f(n)$$

Table

<table>
<thead>
<tr>
<th>$f_1(x)$</th>
<th>$3n^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_2(x)$</td>
<td>$1/2n^2 + 100$</td>
</tr>
<tr>
<td>$f_3(x)$</td>
<td>$n^2 + 5n + 40$</td>
</tr>
<tr>
<td>$f_4(x)$</td>
<td>$3n^2 + n \log n$</td>
</tr>
</tbody>
</table>
worst-case vs. best-case vs. average-case

worst-case: what is the worst the running time of the algorithm can be?

best-case: what is the best the running time of the algorithm can be?

average-case: given random data, what is the running time of the algorithm?

Don’t confuse this with O, Ω and Θ. The cases above are situations, asymptotic notation is about bounding particular situations.

Proving bounds: find constants that satisfy inequalities

Show that $5n^2 - 15n + 100$ is $\Theta(n^2)$

Step 1: Prove $O(n^2)$ – Find constants $c$ and $n_0$ such that $5n^2 - 15n + 100 \leq cn^2$ for all $n > n_0$

\[
\begin{align*}
5n^2 &\geq \ 5n^2 - 15n + 100 \\
c &\geq \ 5 - 15/n + 100/n^2
\end{align*}
\]

Let $n_0 = 1$ and $c = 5 + 100 = 105$. $100/n^2$ only get smaller as $n$ increases and we ignore $-15/n$ since it only varies between $-15$ and $0$. 

Visually: upper bound

Visually: lower bound
Proving bounds

Step 2: Prove $\Omega(n^2)$ – Find constants $c$ and $n_0$ such that

$$5n^2 - 15n + 100 \geq cn^2 \text{ for all } n > n_0$$

Let $n_0 = 4$ and $c = 5 - \frac{15}{4} = 1.25$ (or anything less than 1.25). $15n$ is always decreasing and we ignore $100/n^2$ since it is always between 0 and 100.

Bound

Is $5n^2 \in \Omega(n)$? No

How would we prove it?

Assume it’s true.

That means there exists some $c$ and $n_0$ such that

$$5n^2 \leq cn \text{ for } n > n_0$$

$5n \leq c$ contradiction!

Disproving bounds

Assume it’s true.

That means there exists some $c$ and $n_0$ such that

$$5n^2 \leq cn \text{ for } n > n_0$$

$5n \leq c$ contradiction!

Some rules of thumb

Multiplicative constants can be omitted
- $14n$ becomes $n^2$
- $7 \log n$ become $\log n$

Lower order functions can be omitted
- $n + 5$ becomes $n$
- $n^2 + n$ becomes $n^2$
- $n^{1.5}$ dominates $n^{1.4}$

- $n^a$ dominates $n^b$ if $a > b$
- $n^a$ dominates $n$, so $n^a n^b$ becomes $n^a$
- $n^{1.5}$ dominates $n^{1.4}$
Some rules of thumb

- $a^n$ dominates $b^p$ if $a > b$
  - $3^n$ dominates $2^n$

Any exponential dominates any polynomial
- $3^n$ dominates $n^p$
- $2^n$ dominates $n^p$

Any polynomial dominates any logarithm
- $n$ dominates $\log n$ or $\log \log n$
- $n^p$ dominates $n \log n$
- $n^{p/2}$ dominates $\log n$

Do not omit lower order terms of different variables ($n^2 + m$) does not become $n^2$

Big O

- $n^2 + n \log n + 50$
- $2^n - 15n^2 + n^3 \log n$
- $n^{\log n} + n^2 + 15n^3$
- $n^5 + n! + n^n$

Some examples

- $O(1)$ – constant. Fixed amount of work, regardless of the input size
  - add two 32 bit numbers
  - determine if a number is even or odd
  - sum the first 20 elements of an array
  - delete an element from a doubly linked list
- $O(\log n)$ – logarithmic. At each iteration, discards some portion of the input (i.e. half)
  - binary search

Some examples

- $O(n)$ – linear. Do a constant amount of work on each element of the input
  - find an item in a linked list
  - determine the largest element in an array
- $O(n \log n)$ log-linear. Divide and conquer algorithms with a linear amount of work to recombine
  - Sort a list of number with MergeSort
  - FFT
Some examples

- $O(n^2)$ – quadratic. Double nested loops that iterate over the data
  - Insertion sort
- $O(2^n)$ – exponential
  - Enumerate all possible subsets
  - Traveling salesman using dynamic programming
- $O(n!)$
  - Enumerate all permutations
  - Determinant of a matrix with expansion by minors