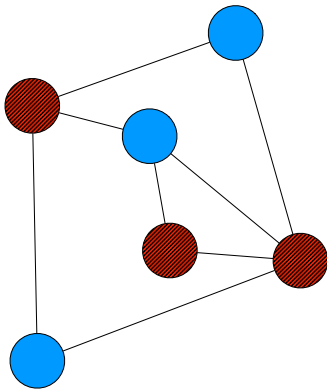# Asymptotic Analysis

Slides by Carl Kingsford

Jan. 27, 2014

AD Chapter 2

Independent Set

Definition (Independent Set). Given a graph $G = (V, E)$ an independent set is a set $S \subseteq V$ if no two nodes in S are joined by an edge.

Independent Set

Definition (Independent Set). Given a graph $G = (V, E)$ an independent set is a set $S \subseteq V$ if no two nodes in S are joined by an edge.

Maximum Independent Set. Given a graph G, find the largest independent set.

Apparently a difficult problem. (No efficient algorithm known, and good reason to suspect that none exists.)

Combinatorial Problems

Problems like Independent Set, Minimum Spanning Tree, etc. can be thought of as families of instances:

- ▶ An instance of Independent Set is specified by a particular graph G.
- ▶ An instance of Minimum Spanning Tree is given by the graph G and weights d.

Instances often have a natural way of encoding them in the computer:

- ▶ A graph with n nodes might be specified by an $n \times n$ matrix or a list of edges.

Instance Sizes

Size of the instance is the space used to represent it.

Usually use n to represent this size.

Generally, "larger" instances are more difficult than smaller ones.

Can often break the problem down into:

- ▶ Search space: the set of feasible solutions (every independent set or spanning tree)
- ▶ Objective function: a way of measuring how good the solution is (size of independent set, stability of perfect matching)

Difficulty is not necessarily proportional to size of the search space.

Efficient Algorithms

Definition (Efficiency). An algorithm is efficient if its <u>worst-case</u> runtime is bounded by a polynomial function of the input size.

▶ There is a polynomial $p(n)$ such that for <u>every instance</u> of size n, the algorithm solves the instance in <u>fewer than $p(n)$</u> steps.

Generally, the problems we consider will have huge search spaces.

How many subsets of nodes are there in a graph of n nodes?

Any polynomial is **much** smaller than the search space.

Efficient Algorithms

Definition (Efficiency). An algorithm is efficient if its <u>worst-case</u> runtime is bounded by a polynomial function of the input size.

▶ There is a polynomial $p(n)$ such that for <u>every instance</u> of size n, the algorithm solves the instance in <u>fewer than $p(n)$</u> steps.

Generally, the problems we consider will have huge search spaces.

How many subsets of nodes are there in a graph of n nodes? $\quad$ 2^n

Any polynomial is **much** smaller than the search space.

Efficient Algorithms, II

This definition of efficiently is not perfect:

1. There are non-polynomal algorithms that are usually the best choice in practice (e.g. simplex method for linear programming).

2. There are polynomial time algorithms that are almost never used in practice (e.g. ellipsoid algorithm for linear programming).

3. An algorithm that takes n^{100} steps would be "efficient" by this definition, but horrible in practice.

4. An algorithm that takes $n^{1+0.002 \log n}$ is probably useful in practice, but it is not "efficient".

Benefits of the definition

But it has a lot of benefits:

1. It's concrete and falsifiable — avoids "vague" arguments about which algorithm is better.

2. Average performance is hard to define.

3. The exceptions are apparently fewer than the cases where polynomial time corresponds to useful algorithms in practice.

4. There is normally a **huge** difference between polynomial time and other natural runtimes

   (If you can do 1 million steps per second and $n = 1,000,000$, then a n^2 algorithm would take 12 days, but a 1.5^n algorithm would take far more than 10^{25} years)

Asymptotic Upper Bounds

A running time of $n^2 + 4n + 2$ is usually too detailed. Rather, we're interested in how the runtime grows as the problem size grows.

Definition (O). A runtime $T(n)$ is $O(f(n))$ if there exist constants $n_0 \geq 0$ and $c > 0$ such that:

$$T(n) \leq cf(n) \qquad \text{for all } n \geq n_0$$

What does this mean?

- for all large enough instances
- the running time is bounded by a constant multiple of $f(n)$

Asymptotic Lower Bounds

$O(\cdot)$ talks about the *longest* possible time an algorithm could take.
$\Omega(\cdot)$ talks about the *shortest* possible time.

Definition (Ω). $T(n)$ is $\Omega(f(n))$ if there are constants $\epsilon > 0$ and $n_0 \geq 0$ so that:

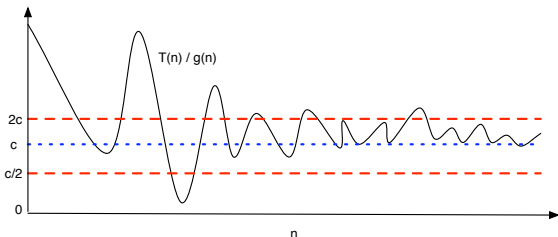$$T(n) \geq \epsilon f(n) \qquad \text{for all } n \geq n_0$$

Tight bounds

Definition (Θ). $T(n)$ is $\Theta(f(n))$ if $T(n)$ is $O(f(n))$ and $\Omega(f(n))$.

If we know that $T(n)$ is $\Theta(f(n))$ then $f(n)$ is the "right" asymptotic running time: it will run faster than $O(f(n))$ on all instances and some instances might take that long.

Asymptotic Limit

Theorem (Theta). *If $\lim_{n\to\infty} \frac{T(n)}{g(n)}$ equals some $c > 0$, then $T(n) = \Theta(g(n))$.*

There is an n_0 such that $c/2 \leq T(n)/g(n) \leq 2c$ for all $n \geq n_0$.

Therefore, $T(n) \leq 2cg(n)$ for $n \geq n_0 \Rightarrow T(n) = O(g(n))$.

Also, $T(n) \geq \frac{c}{2}g(n)$ for $n \geq n_0 \Rightarrow T(n) = \Omega(g(n))$.

Linear Time

Linear time usually means you look at each element a constant number of times.

- Finding the maximum element in a list:

```
max = a[1]
for i = 2 to n:
    if a[i] > max then
        set max = a[i]
Endfor
```

This does a constant amount of work per element in array a.
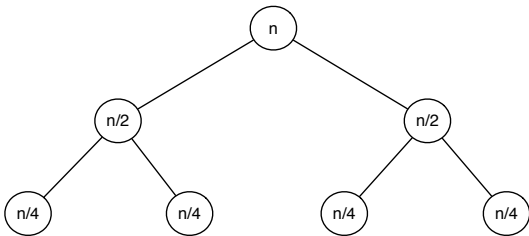
- Merging sorted lists.

$O(n \log n)$

$O(n \log n)$ time is common because of sorting (often the slowest step in an algorithm).

Where does the $O(n \log n)$ come from?

$O(n \log n)$

$O(n \log n)$ time is common because of sorting (often the slowest step in an algorithm).
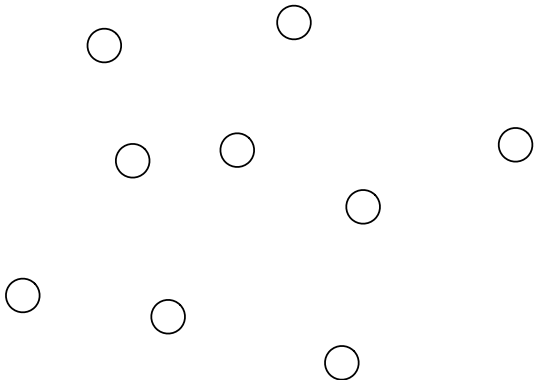
Where does the $O(n \log n)$ come from?

$$T(n) = 2T(n/2) + n$$

Quadratic Time — $O(n^2)$

A brute force algorithm for: Given a set of points, what is the smallest distance between them.
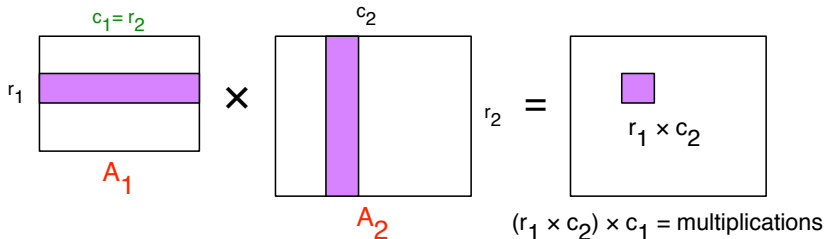

$\binom{n}{2}$ pairs

$O(n^3)$

Ex. 1. Given n sets $S_1, S_2, \ldots, S_n$ that are subsets of $\{1, \ldots, n\}$, is there some pair of sets that is disjoint?

Assume the sets are represented as bit vectors. Natural algorithm: for every pair of sets i and j, test whether they overlap by going through all the elements in i and j.

Ex. 2. "Standard" rule for matrix multiplication:

$(r_1 \times c_2) \times c_1 =$ multiplications

$O(n^k)$

Larger polynomials arise from exploring smaller search spaces exhaustively:

Independent Set of Size k. Given a graph with n nodes, find an independent set of size k or report none exists.

```
For every subset S of k nodes
    If S is an independent set then        (*)
        return S
Endfor
return Failure
```

How many subsets of k nodes are there?

Exponential Time

What if we didn't limit ourselves to independent sets of size k, and instead want to find the largest independent set?

Brute force algorithms search through all possibilities.

How many subsets of nodes are there in an n-node graph?

What's the runtime of the brute force search search for a largest independent set?

Exponential Time

What if we didn't limit ourselves to independent sets of size k, and instead want to find the largest independent set?

Brute force algorithms search through all possibilities.

How many subsets of nodes are there in an n-node graph? 2^n

What's the runtime of the brute force search search for a largest independent set?

Exponential Time

What if we didn't limit ourselves to independent sets of size k, and instead want to find the largest independent set?

Brute force algorithms search through all possibilities.

How many subsets of nodes are there in an n-node graph? 2^n

What's the runtime of the brute force search search for a largest independent set? $O(n^2 2^n)$

Sublinear Time

Sublinear time means we don't even look at every input.

Since it takes n time just to read the input, we have to work in a model where we count how many queries to the data we make.

Sublinear usually means we don't have too look at every element.

Example?

Sublinear Time

Sublinear time means we don't even look at every input.

Since it takes n time just to read the input, we have to work in a model where we count how many queries to the data we make.

Sublinear usually means we don't have too look at every element.

Example? Binary search — $O(\log n)$

Properties of O, Ω, Θ

Example (Transitivity of O).

Show that if $f(n) = O(g(n))$ and $g = O(h(n))$
then $f(n) = O(h(n))$.

Solution:

By the assumptions, there are constants c_f, n_f, c_g, n_g such that
$f(n) \leq c_f g(n)$ and $g(n) \leq c_g h(n)$ for all $n \geq \max\{n_f, n_g\}$.

Therefore
$$f(n) \leq c_f g(n) \leq c_f c_g h(n)$$
and setting $c = c_f c_g$ and $n_0 = \max\{n_f, n_g\}$. ☐

Example (Transitivity of Ω).

Show that if $f = \Omega(g)$ and $g = \Omega(h)$ then $f = \Omega(h)$.

Solution:

A very similar argument to the previous example:

- there are c_f, n_f such that $f(n) \geq c_f g(n)$ for all $n \geq n_f$, and
- there are c_g, n_g such that $g(n) \geq c_g h(n)$ for all $n \geq n_g$.

Substituting in for $g(n)$ we get $f(n) \geq c_f c_g h(n)$ for all $n \geq \max\{n_f, n_g\}$. $\qquad\square$

Example (Multiplication).

For positive functions $f(n)$, $f'(n)$, $g(n)$, $g'(n)$, if $f(n) = O(f'(n))$ and $g(n) = O(g'(n))$ then $f(n)g(n) = O(f'(n)g'(n))$.

Solution:

There are constants c_f, n_f, c_g, n_g as specified in the definition of O-notation:

$$f(n) \leq c_f f'(n) \qquad \text{for all } n > n_f$$
$$g(n) \leq c_g g'(n) \qquad \text{for all } n > n_g$$

So for $n > \max\{n_f, n_g\}$ both statements above hold, and we have:

$$f(n)g(n) \leq c_f f'(n) c_g g'(n) = c_f c_g f'(n) g'(n).$$

Taking $c = c_f c_g$ and $n_0 = \max\{n_f, n_g\}$ yields the desired statement. $\qquad\square$

Example (Max).

Show that $\max\{f(n), g(n)\} = \Theta(f(n) + g(n))$ for any $f(n), g(n)$ that eventually become and stay positive.

Solution:

We have $\max\{f(n), g(n)\} = O(f(n) + g(n))$ by taking $c = 1$ and n_0 equal to be the point where they become positive.

We have $\max\{f(n), g(n)\} = \Omega(f(n) + g(n))$ taking the same n_0 and $c = 1/2$ since the average of positive functions $f(n)$ and $g(n)$ is always less than the max. $\square$

Example (Polynomials).

Prove that $an^2 + bn + d = O(n^2)$ for all real a, b, d.

Solution:

$$
\begin{aligned}
an^2 + bn + d &\leq |a|n^2 + |b|n + |d| && \text{for all } n \geq 0 \\
&\leq |a|n^2 + |b|n^2 + |d|n^2 && \text{for all } n \geq 1 \\
&= (|a| + |b| + |d|)n^2.
\end{aligned}
$$

Take $c = |a| + |b| + |d|$ and $n_0 = 1$. $\qquad\qquad\square$

Example (Polynomials and Θ).

Show that any degree-d polynomial $p(n) = \sum_{i=0}^{d} \alpha_i n^i$
with $\alpha_d > 0$ is $\Theta(n^d)$.

Solution:

Step 1: A similar argument to the previous example shows that
$p(n)$ is $O(n^d)$. For all $n \geq 1$:

$$p(n) = \sum_{i=0}^{d} \alpha_i n^i \leq \sum_{i=0}^{d} |\alpha_i| n^i \leq \sum_{i=0}^{d} |\alpha_i| n^d = n^d \sum_{i=0}^{d} |\alpha_i|.$$

So take $c = \sum_{i=0}^{d} |\alpha_i|$ and $n_0 = 1$.

Step 2 on next slide.

Step 2: We now show that $p(n)$ is $\Omega(n^d)$. We try to find a c that works in the definition. For $n \geq 1$, we have:

$$cn^d \leq \sum_{i=0}^{d} \alpha_i n_i \iff c \leq \sum_{i=0}^{d} \alpha_i n^i / n^d$$

$$= \alpha_d + \sum_{i=0}^{d-1} \alpha_i n^{i-d} \qquad \text{take out } n^d/n^d \text{ term}$$

$$= \alpha_d + \sum_{i=0}^{d-1} \frac{\alpha_i}{n^{d-i}} \qquad\qquad x^i = 1/x^{-i}.$$

So: need to show that the R.H.S. of the above is > 0 for large enough n. If so, then there will be a c that we can choose.

Step 2, continued: Let $N = \{i : \alpha_i < 0\}$. Then we have:

$$\alpha_d + \sum_{i=0}^{d-1} \frac{\alpha_i}{n^{d-i}} \geq \alpha_d + \sum_{i \in N} \frac{\alpha_i}{n^{d-i}} \qquad \text{b/c we threw out the positive terms}$$

$$= \alpha_d - \sum_{i \in N} \frac{|\alpha_i|}{n^{d-i}}$$

$$\geq \alpha_d - \frac{1}{n} \sum_{i \in N} |\alpha_i| \qquad \text{b/c } 1/n \text{ is the largest dependence on } n$$

Now: $\alpha_d > \frac{1}{n} \sum_{i \in N} |\alpha_i|$ when $n > \frac{\sum_{i \in N} |\alpha_i|}{\alpha_d}$.

At that n and larger, the last line above is strictly greater than 0.

So we choose n_0 equal to $\frac{\sum_{i \in N} |\alpha_i|}{\alpha_d} + 1$ and any c between 0 and $\alpha_d - \frac{1}{n_0} \sum_{i \in N} |\alpha_i|$. $\qquad \square$

Example.

Show that $(n + a)^d = \Theta(n^d)$ when $d > 0$.

Solution:

$(n + a)^d = \sum_{i=0}^{d} \binom{d}{i} a^{d-i} n^i$ by the binomial theorem.

This equals $\sum_{i=0}^{d} \alpha_i n^i$ for $\alpha_i = \binom{d}{i} a^{d-i}$, which is a degree-$d$ polynomial, which is $\Theta(n^d)$ by the previous example. $\qquad\square$