15-251

Great Theoretical Ideas in Computer Science

This is The Big Oh!

Lecture 21, November 4, 2008

Counting

The Power of One

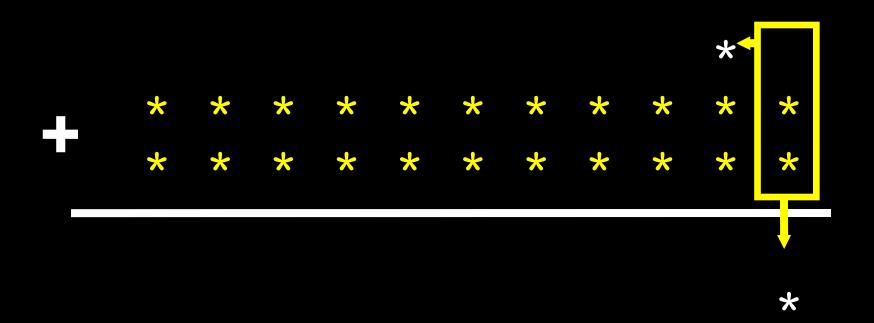
Algebra

The Power of X

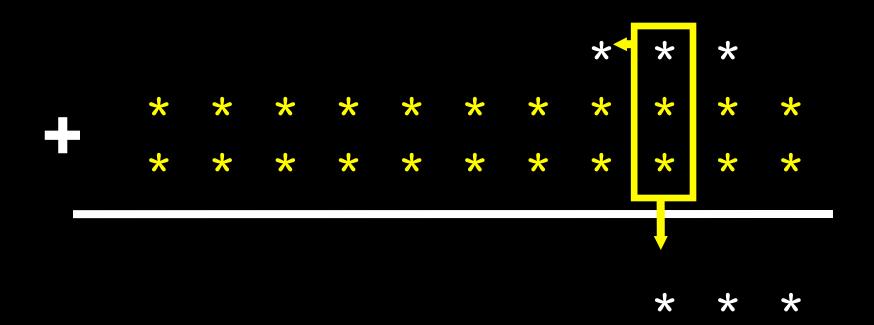
Asymptotics

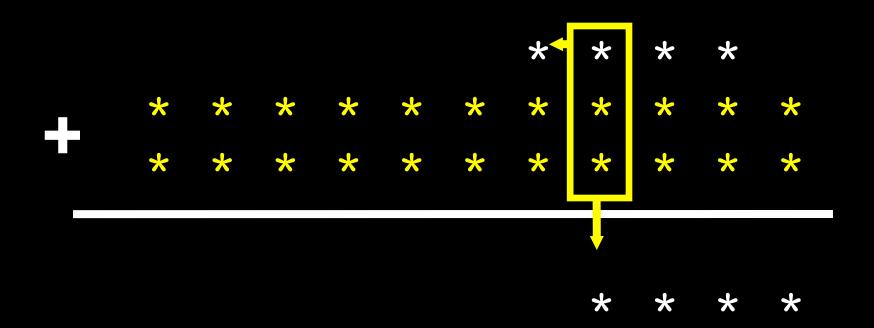
The Power of O













"Grade school addition"

Time complexity of grade school addition



T(n) = amount of time grade school addition uses to add two n-bit numbers

Time complexity of grade school addition



T(n) = amount of time grade school addition uses to add two n-bit numbers

What do we mean by "time"?

Our Goal

We want to define "time" in a way that transcends implementation details and allows us to make assertions about grade school addition in a very general yet useful way.

Roadblock ???

A given algorithm will take different amounts of time on the same inputs depending on such factors as:

- Processor speed
- Instruction set
- Disk speed
- Brand of compiler

Pick any particular computer M and define c to be the time it takes to perform on that computer.

Pick any particular computer M and define c to be the time it takes to perform on that computer.

Total time to add two n-bit numbers using grade school addition:

Pick any particular computer M and define c to be the time it takes to perform on that computer.

Total time to add two n-bit numbers using grade school addition:

cn [i.e., c time for each of n columns]

On another computer M', the time to perform may be c'.

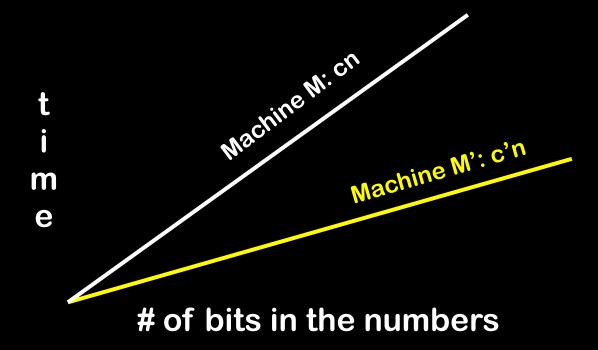
On another computer M', the time to perform may be c'.

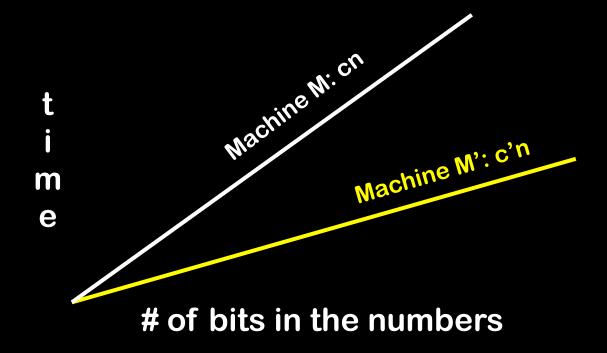
Total time to add two n-bit numbers using grade school addition:

On another computer M', the time to perform may be c'.

Total time to add two n-bit numbers using grade school addition:

c'n [c' time for each of n columns]





The fact that we get a line is invariant under changes of implementations. Different machines result in different slopes, but the time taken grows linearly as input size increases.

Thus we arrive at an implementation-independent insight:

Grade School Addition is a linear time algorithm

Thus we arrive at an implementation-independent insight:

Grade School Addition is a linear time algorithm

This process of abstracting away details and determining the rate of resource usage in terms of the problem size n is one of the fundamental ideas in computer science.

Time vs Input Size

For any algorithm, define Input Size = # of bits to specify its inputs.

Time vs Input Size

For any algorithm, define Input Size = # of bits to specify its inputs.

Define

TIME_n = the worst-case amount of time used by the algorithm on inputs of size n

Time vs Input Size

For any algorithm, define Input Size = # of bits to specify its inputs.

Define

TIME_n = the worst-case amount of time used by the algorithm on inputs of size n

We often ask: What is the growth rate of Time,?

How to multiply 2 n-bit numbers.



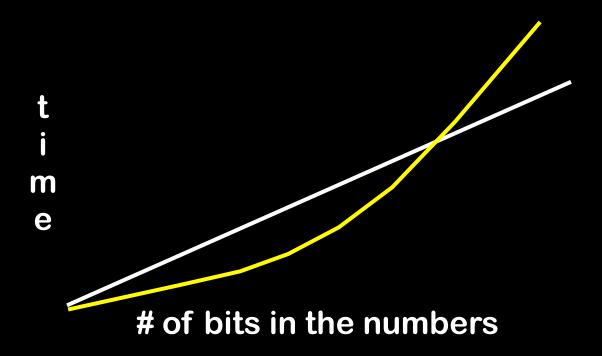
How to multiply 2 n-bit numbers.



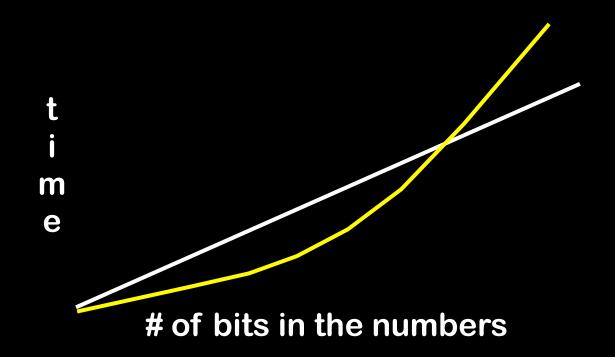
How to multiply 2 n-bit numbers.



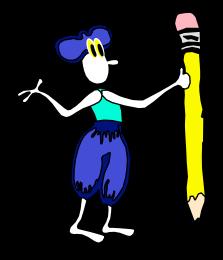
Grade School Addition: Linear time Grade School Multiplication: Quadratic time



Grade School Addition: Linear time Grade School Multiplication: Quadratic time

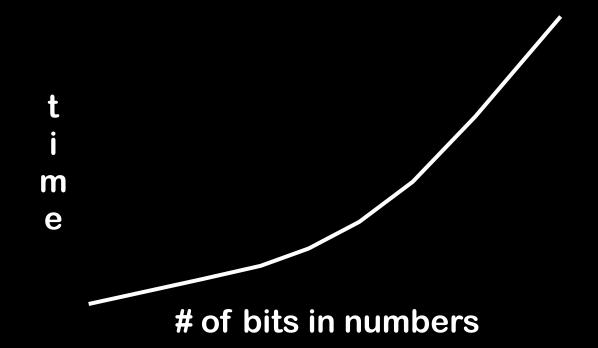


No matter how dramatic the difference in the constants, the quadratic curve will eventually dominate the linear curve



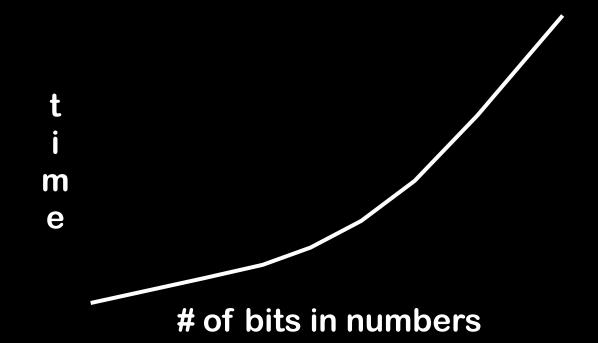
How much time does it take to square the number n using grade school multiplication?

Grade School Multiplication: Quadratic time



c(log n)² time to square the number n

Grade School Multiplication: Quadratic time



c(log n)² time to square the number n Input size is measured in bits, unless we say otherwise.

Nursery School Addition

Input: Two n-bit numbers, a and b

Output: a + b

Nursery School Addition

Input: Two n-bit numbers, a and b

Output: a + b

Start at a and increment (by 1) b times

Nursery School Addition

Input: Two n-bit numbers, a and b

Output: a + b

Start at a and increment (by 1) b times

$$T(n) = ?$$

Nursery School Addition

Input: Two n-bit numbers, a and b

Output: a + b

Start at a and increment (by 1) b times

$$T(n) = ?$$

If b = 000...0000, then NSA takes almost no time

Nursery School Addition

Input: Two n-bit numbers, a and b

Output: a + b

Start at a and increment (by 1) b times

$$T(n) = ?$$

If b = 000...0000, then NSA takes almost no time

If b = 1111...11111, then NSA takes cn2ⁿ time

Worst Case Time

Worst Case Time T(n) for algorithm A:

T(n) = Max_[all permissible inputs X of size n]
(Running time of algorithm A on input X).

What is T(n)?

Kindergarten Multiplication Input: Two n-bit numbers, a and b

Output: a * b

What is T(n)?

Kindergarten Multiplication Input: Two n-bit numbers, a and b

Output: a * b

Start with a and add a, b-1 times

What is T(n)?

Kindergarten Multiplication

Input: Two n-bit numbers, a and b

Output: a * b

Start with a and add a, b-1 times

Remember, we always pick the WORST CASE input for the input size n.

Thus, $T(n) = cn2^n$

Thus, Nursery School adding and Kindergarten multiplication are exponential time.

They scale HORRIBLY as input size grows.

Grade school methods scale polynomially: just linear and quadratic. Thus, we can add and multiply fairly large numbers.

If T(n) is not polynomial, the algorithm is not efficient: the run time scales too poorly with the input size.

If T(n) is not polynomial, the algorithm is not efficient: the run time scales too poorly with the input size.

This will be the yardstick with which we will measure "efficiency".

Multiplication is efficient, what about "reverse multiplication"?

Multiplication is efficient, what about "reverse multiplication"?

Let's define FACTORING(N) to be any method to produce a non-trivial factor of N, or to assert that N is prime.

Trial division up to √N

Trial division up to √N

```
for k = 2 to √ N do

if k | N then

return "N has a non-trivial factor k"

return "N is prime"
```

Trial division up to √N

```
for k = 2 to √ N do
    if k | N then
    return "N has a non-trivial factor k"
return "N is prime"
```

 $c \sqrt{N (log N)^2}$ time if division is c $(log N)^2$ time

Trial division up to √N

```
for k = 2 to √ N do
    if k | N then
    return "N has a non-trivial factor k"
return "N is prime"
```

 $c \sqrt{N} (log N)^2$ time if division is $c (log N)^2$ time

Is this efficient?

Trial division up to √N

```
for k = 2 to √ N do

if k | N then

return "N has a non-trivial factor k"

return "N is prime"
```

c √N (logN)² time if division is c (logN)² time

Is this efficient?

No! The input length n = log N. Hence we're using $c 2^{n/2} n^2$ time.

Can we do better?

Can we do better?

We know of methods for FACTORING that are sub-exponential (about 2^{n1/3} time) but nothing efficient.

For any monotonic function f from the positive integers to the positive integers, we say

```
"f = O(n)" or "f is O(n)"
```

For any monotonic function f from the positive integers to the positive integers, we say

"
$$f = O(n)$$
" or " $f is O(n)$ "

If some constant times n eventually dominates f

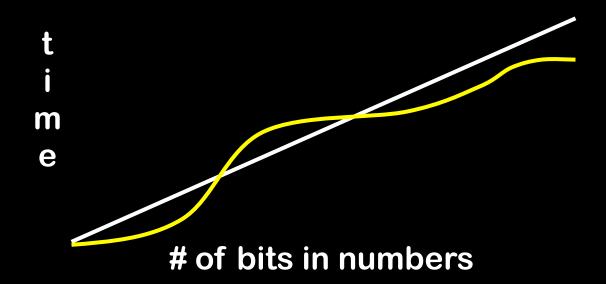
For any monotonic function f from the positive integers to the positive integers, we say

"
$$f = O(n)$$
" or " $f is O(n)$ "

If some constant times n eventually dominates f

[Formally: there exists a constant c such that for all sufficiently large n: $f(n) \le cn$]

f = O(n) means that there is a line that can be drawn that stays above f from some point on



Other Useful Notation: Ω

For any monotonic function f from the positive integers to the positive integers, we say

```
"f = \Omega(n)" or "f is \Omega(n)"
```

Other Useful Notation: Ω

For any monotonic function f from the positive integers to the positive integers, we say

"f =
$$\Omega(n)$$
" or "f is $\Omega(n)$ "

If f eventually dominates some constant times n

Other Useful Notation: Ω

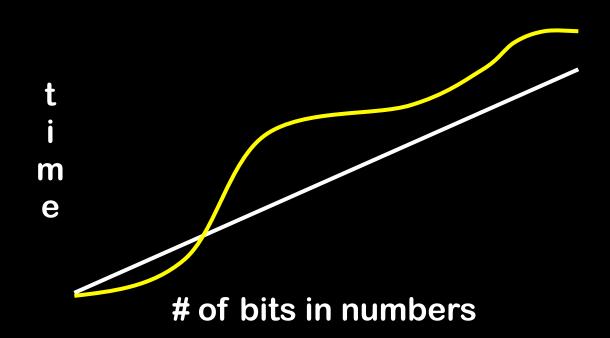
For any monotonic function f from the positive integers to the positive integers, we say

"f =
$$\Omega(n)$$
" or "f is $\Omega(n)$ "

If f eventually dominates some constant times n

[Formally: there exists a constant c such that for all sufficiently large n: f(n) ≥ cn]

f = Ω(n) means that there is a line that can be drawn that stays below f from some point on



Yet More Useful Notation: Θ

For any monotonic function f from the positive integers to the positive integers, we say

```
"f = \Theta(n)" or "f is \Theta(n)"
```

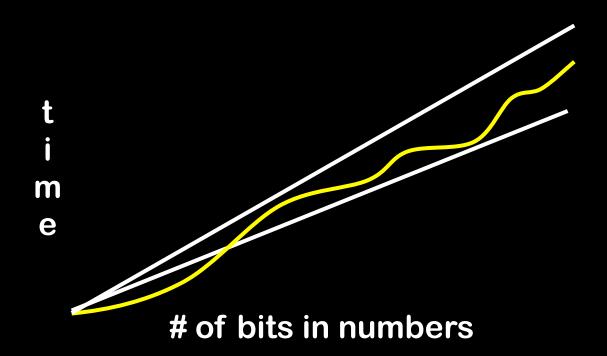
Yet More Useful Notation: Θ

For any monotonic function f from the positive integers to the positive integers, we say

```
"f = \Theta(n)" or "f is \Theta(n)"
```

```
if: f = O(n) and f = \Omega(n)
```

$f = \Theta(n)$ means that f can be sandwiched between two lines from some point on.



For any two monotonic functions f and g from the positive integers to the positive integers, we say

```
"f = O(g)" or "f is O(g)"
```

For any two monotonic functions f and g from the positive integers to the positive integers, we say

"
$$f = O(g)$$
" or " $f is O(g)$ "

If some constant times g eventually dominates f

Notation to Discuss Growth Rates

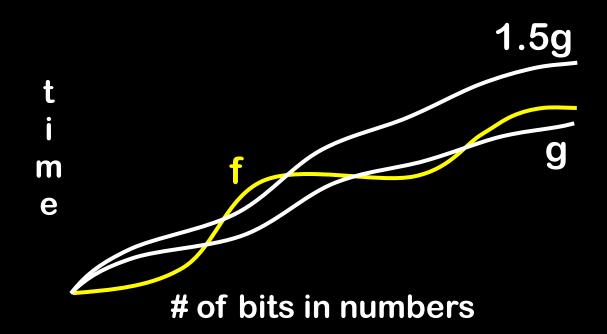
For any two monotonic functions f and g from the positive integers to the positive integers, we say

"
$$f = O(g)$$
" or " $f is O(g)$ "

If some constant times g eventually dominates f

[Formally: there exists a constant c such that for all sufficiently large n: $f(n) \le c g(n)$]

f = O(g) means that there is some constant c such that c g(n) stays above f(n) from some point on.



Other Useful Notation: Ω

For any two monotonic functions f and g from the positive integers to the positive integers, we say

```
"f = \Omega(g)" or "f is \Omega(g)"
```

Other Useful Notation: Ω

For any two monotonic functions f and g from the positive integers to the positive integers, we say

"f =
$$\Omega(g)$$
" or "f is $\Omega(g)$ "

If f eventually dominates some constant times g

Other Useful Notation: Ω

For any two monotonic functions f and g from the positive integers to the positive integers, we say

"f =
$$\Omega(g)$$
" or "f is $\Omega(g)$ "

If f eventually dominates some constant times g

[Formally: there exists a constant c such that for all sufficiently large n: $f(n) \ge c g(n)$]

Yet More Useful Notation: Θ

For any two monotonic functions f and g from the positive integers to the positive integers, we say

```
"f = \Theta(g)" or "f is \Theta(g)"
```

Yet More Useful Notation: Θ

For any two monotonic functions f and g from the positive integers to the positive integers, we say

```
"f = \Theta(g)" or "f is \Theta(g)"
```

```
If: f = O(g) and f = \Omega(g)
```

• $n = O(n^2)$?

Take c = 1For all $n \ge 1$, it holds that $n \le cn^2$

• $n = O(\sqrt{n})$?

• $n = O(\sqrt{n})$? No

•
$$n = O(\sqrt{n})$$
 ? No

Suppose it were true that n ≤ c √n for some constant c and large enough n

- $n = O(n^2)$? Yes!
- $n = O(\sqrt{n})$? No

Suppose it were true that $n \le c \sqrt{n}$ for some constant c and large enough n Cancelling, we would get $\sqrt{n} \le c$. Which is false for $n > c^2$

•
$$n = O(n^2)$$
 ? Yes!

•
$$n = O(\sqrt{n})$$
? No

•
$$3n^2 + 4n + 4 = O(n^2)$$
?

•
$$3n^2 + 4n + 4 = \Omega(n^2)$$
?

•
$$n^2 = \Omega(n \log n)$$
?

•
$$n^2 \log n = \Theta(n^2)$$
?

•
$$n = O(n^2)$$
 ? Yes!

•
$$n = O(\sqrt{n})$$
? No

•
$$3n^2 + 4n + 4 = O(n^2)$$
? Yes!

•
$$3n^2 + 4n + 4 = \Omega(n^2)$$
?

•
$$n^2 = \Omega(n \log n)$$
?

•
$$n^2 \log n = \Theta(n^2)$$
?

•
$$n = O(n^2)$$
 ? Yes!

•
$$n = O(\sqrt{n})$$
 ? No

•
$$3n^2 + 4n + 4 = O(n^2)$$
? Yes!

•
$$3n^2 + 4n + 4 = \Omega(n^2)$$
? Yes!

•
$$n^2 = \Omega(n \log n)$$
?

•
$$n^2 \log n = \Theta(n^2)$$
?

•
$$n = O(n^2)$$
 ? Yes!

•
$$n = O(\sqrt{n})$$
? No

•
$$3n^2 + 4n + 4 = O(n^2)$$
? Yes!

•
$$3n^2 + 4n + 4 = \Omega(n^2)$$
? Yes!

•
$$n^2 = \Omega(n \log n)$$
? Yes!

•
$$n^2 \log n = \Theta(n^2)$$
?

•
$$n = O(n^2)$$
 ? Yes!

•
$$n = O(\sqrt{n})$$
? No

•
$$3n^2 + 4n + 4 = O(n^2)$$
? Yes!

•
$$3n^2 + 4n + 4 = \Omega(n^2)$$
? Yes!

•
$$n^2 = \Omega(n \log n)$$
? Yes!

•
$$n^2 \log n = \Theta(n^2)$$
?

•
$$f = O(g)$$

then $g = \Omega(f)$

•
$$f = O(g)$$

then $g = \Omega(f)$

f = O(g) and g = O(h)
 then f = O(h)?

```
\begin{split} &f(n) \leq c \; g(n) \; \text{ for all } n \geq n_0. \\ &\text{ and } g(n) \leq c' \; h(n) \; \text{ for all } n \geq n_0'. \end{split} So f(n) \leq (cc') \; h(n) \; \text{ for all } n \geq \max(n_0, n_0')
```

•
$$f = O(g)$$

then $g = \Omega(f)$

```
\begin{split} &f(n) \leq c \; g(n) \; \; \text{for all } n \geq n_0. \\ &\text{and } g(n) \leq c' \; h(n) \; \; \text{for all } n \geq n_0'. \end{split} So f(n) \leq (cc') \; h(n) \; \text{for all } n \geq \max(n_0, n_0')
```

•
$$f = O(g)$$

then $g = \Omega(f)$ Yes!

Names For Some Growth Rates

Linear Time: T(n) = O(n)

Quadratic Time: $T(n) = O(n^2)$

Cubic Time: $T(n) = O(n^3)$

Names For Some Growth Rates

Linear Time: T(n) = O(n)

Quadratic Time: $T(n) = O(n^2)$

Cubic Time: $T(n) = O(n^3)$

Polynomial Time:

Names For Some Growth Rates

Linear Time: T(n) = O(n)

Quadratic Time: $T(n) = O(n^2)$

Cubic Time: $T(n) = O(n^3)$

Polynomial Time:

for some constant k, $T(n) = O(n^k)$.

Example: $T(n) = 13n^5$

Large Growth Rates

Exponential Time:

Large Growth Rates

Exponential Time:

for some constant k, $T(n) = O(k^n)$

Example: $T(n) = n2^n = O(3^n)$

Logarithmic Time: T(n) = O(logn)

Example: $T(n) = 15log_2(n)$

Logarithmic Time: T(n) = O(logn)

Example: $T(n) = 15\log_2(n)$

Polylogarithmic Time:

for some constant k, T(n) = O(log^k(n))

Logarithmic Time: T(n) = O(logn)

Example: $T(n) = 15\log_2(n)$

Polylogarithmic Time:

for some constant k, $T(n) = O(log^k(n))$

Note: These kind of algorithms can't possibly read all of their inputs.

Logarithmic Time: T(n) = O(logn)

Example: $T(n) = 15log_2(n)$

Polylogarithmic Time:

for some constant k, T(n) = O(log^k(n))

Note: These kind of algorithms can't possibly read all of their inputs.

A very common example of logarithmic time is looking up a word in a sorted dictionary (binary search)

Doubly Exponential Time meansthat for some constant k

Doubly Exponential Time means that for some constant k $T(n) = 2^{2^{kn}}$

Doubly Exponential Time meansthat for some constant k

$$T_{(n)}=2^{2^{kn}}$$

Triply Exponential

Doubly Exponential Time meansthat for some constant k

$$T_{(n)}=2^{2^{kn}}$$

Triply Exponential

$$T_{(n)}=2^{2^{2^{kn}}}$$

```
2STACK(0) = 1
2STACK(n) = 2^{2STACK(n-1)}
```

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(0) = 1$$
$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(5) \ge 10^{80}$$

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(5) \ge 10^{80}$$

= atoms in universe

$$2STACK(0) = 1$$

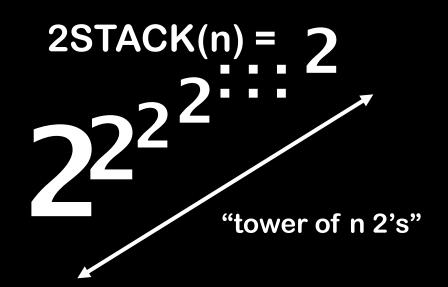
$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$



$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(5) \ge 10^{80}$$

= atoms in universe

$$2STACK(0) = 1$$
$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$\log^*(2) = 1$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(5) \ge 10^{80}$$

= atoms in universe

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$\log^*(2) = 1$$

$$2STACK(2) = 4$$

$$\log^*(4) = 2$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$2STACK(5) \ge 10^{80}$$

= atoms in universe

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

 $log^*(n) = # of times you have to apply the log function to n to make it <math>\leq 1$

 $\log^*(2) = 1$

 $\log^*(4) = 2$

log*(16) = 3

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

 $\log^*(2) = 1$

 $\log^*(4) = 2$

log*(16) = 3

log*(65536) = 4

$$2STACK(0) = 1$$

$$2STACK(n) = 2^{2STACK(n-1)}$$

$$2STACK(1) = 2$$

$$2STACK(2) = 4$$

$$2STACK(3) = 16$$

$$2STACK(4) = 65536$$

$$log^*(2) = 1$$

$$\log^*(4) = 2$$

$$log*(16) = 3$$

$$log*(65536) = 4$$

$$log*(atoms) = 5$$

So an algorithm that can be shown to run in O(n log*n) Time is Linear Time for all practical purposes!!

$$A(0, n) = n + 1 \text{ for } n \ge 0$$

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$
 $A(m, n) = A(m - 1, A(m, n - 1))$ for $m, n \ge 1$

A(0, n) = n + 1 for $n \ge 0$ A(m, 0) = A(m - 1, 1) for $m \ge 1$ A(m, n) = A(m - 1, A(m, n - 1)) for $m, n \ge 1$

| | n=0 | 1 | 2 | 3 | 4 | 5 | |
|-----|-----|---|---|---|---|---|--|
| m=0 | | | | | | | |
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |

$$A(0, n) = n + 1 \text{ for } n \ge 0$$

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$
 $A(m, n) = A(m - 1, A(m, n - 1))$ for $m, n \ge 1$

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$
 $A(m, n) = A(m - 1, A(m, n - 1))$ for $m, n \ge 1$

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$
 $A(m, n) = A(m - 1, A(m, n - 1))$ for $m, n \ge 1$

A(4,2) > # of particles in universe

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$
 $A(m, n) = A(m - 1, A(m, n - 1))$ for $m, n \ge 1$

A(4,2) > # of particles in universe

A(5,2) can't be written out as decimal in this universe

Define: A'(k) = A(k,k)

Define: A'(k) = A(k,k)

Inverse Ackerman $\alpha(n)$ is the inverse of A'

Define: A'(k) = A(k,k)

Inverse Ackerman $\alpha(n)$ is the inverse of A'

$$A(0, n) = n + 1 \text{ for } n \ge 0$$

Define: A'(k) = A(k,k)

Inverse Ackerman $\alpha(n)$ is the inverse of A'

$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$

Define: A'(k) = A(k,k)

Inverse Ackerman $\alpha(n)$ is the inverse of A'

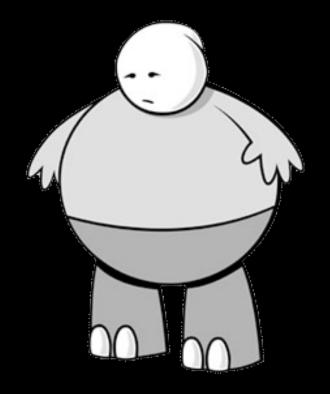
$$A(0, n) = n + 1$$
 for $n \ge 0$
 $A(m, 0) = A(m - 1, 1)$ for $m \ge 1$
 $A(m, n) = A(m - 1, A(m, n - 1))$ for $m, n \ge 1$

Define: A'(k) = A(k,k)

Inverse Ackerman $\alpha(n)$ is the inverse of A'

The inverse Ackermann function – in fact, $\Theta(n \alpha(n))$ arises in the seminal paper of:

D. D. Sleator and R. E. Tarjan. A data structure for dynamic trees. Journal of Computer and System Sciences, 26(3): 362-391, 1983.



Here's What You Need to Know...

- How is "time" measured
- Definitions of:
 - O, Ω, Θ
 - linear, quadratic time, etc
 - log*(n)
 - Ackerman Function