Introduction to Algorithms

Divide and Conquer
Multiplication

Integer Multiplication

Integer Arithmetic

Add: Given two n-bit integers a and b, compute a + b.

Add

1	1	1	1	1	1	0	1	
	1	1	0	1	0	1	0	1
+	0	1	1	1	1	1	0	1
1	0	1	0	1	0	0	1	0

O(n) bit operations.

Multiply: Given two n-bit integers a and b, compute a × b. The “grade school” method:

Multiply

								1	1	0	1	0	1	0	1
							*	0	1	1	1	1	1	0	1
								1	1	0	1	0	1	0	1
							0	0	0	0	0	0	0	0	
						1	1	0	1	0	1	0	1		
					1	1	0	1	0	1	0	1			
				1	1	0	1	0	1	0	1				
			1	1	0	1	0	1	0	1					
		1	1	0	1	0	1	0	1						
	0	0	0	0	0	0	0	0							
0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1

$O(n^2)$ bit operations.

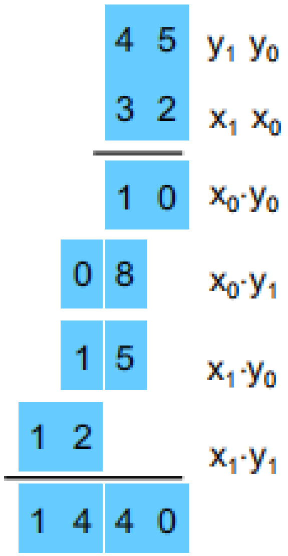
How to use Divide and Conquer?

Suppose we want to multiply two 2-digit integers (32,45).

We can do this by multiplying four 1-digit integers

Then, use add/shift to obtain the result:

$$
\begin{aligned}
x &= 10x_1 + x_0 \\
y &= 10y_1 + y_0 \\
xy &= (10x_1 + x_0)(10y_1 + y_0) \\
&= 100\, x_1y_1 + 10(x_1y_0 + x_0y_1) + x_0y_0
\end{aligned}
$$



Same idea works when multiplying n-digit integers:

- Divide into 4 n/2-digit integers.
- Recursively multiply
- Then merge solutions

A Divide and Conquer for Integer Multiplication

Let x, y be two n-bit integers

Write $x = 2^{n/2}x_1 + x_0$ and $y = 2^{n/2}y_1 + y_0$

where x_0, x_1, y_0, y_1 are all n/2-bit integers.

$$
\begin{aligned}
x &= 2^{n/2} \cdot x_1 + x_0 \\
y &= 2^{n/2} \cdot y_1 + y_0 \\
xy &= \left(2^{n/2} \cdot x_1 + x_0\right)\left(2^{n/2} \cdot y_1 + y_0\right) \\
&= 2^{n} \cdot x_1 y_1 + 2^{n/2} \cdot (x_1 y_0 + x_0 y_1) + x_0 y_0
\end{aligned}
$$

Therefore,

$$T(n) = 4T\left(\frac{n}{2}\right) + \Theta(n)$$

We only need 3 values

$x_1y_1, x_0y_0, x_1y_0 + x_0y_1$

Can we find all 3 by only 3 multiplication?

So,

$$T(n) = \Theta(n^2).$$

$$T(n) = a\,T\left(\frac{n}{b}\right) + cn^k$$ If $a > b^k$ then $T(n) = \Theta\left(n^{\log_b a}\right)$

Key Trick: 4 multiplies at the price of 3

$$x = 2^{n/2} \cdot x_1 + x_0$$
$$y = 2^{n/2} \cdot y_1 + y_0$$
$$xy = \left(2^{n/2} \cdot x_1 + x_0\right)\left(2^{n/2} \cdot y_1 + y_0\right)$$
$$= 2^n \cdot x_1 y_1 + 2^{n/2}\left(x_1 y_0 + x_0 y_1\right) + x_0 y_0$$

$$\alpha = x_1 + x_0$$
$$\beta = y_1 + y_0$$
$$\alpha\beta = (x_1 + x_0)(y_1 + y_0)$$
$$= x_1 y_1 + (x_1 y_0 + x_0 y_1) + x_0 y_0$$
$$(x_1 y_0 + x_0 y_1) = \alpha\beta - x_1 y_1 - x_0 y_0$$

Key Trick: 4 multiplies at the price of 3

Theorem [Karatsuba-Ofman, 1962] Can multiply two n-digit integers in $O(n^{1.585\ldots})$ bit operations.

$$x = 2^{n/2} \cdot x_1 + x_0 \Rightarrow \alpha = x_1 + x_0$$
$$y = 2^{n/2} \cdot y_1 + y_0 \Rightarrow \beta = y_1 + y_0$$
$$xy = \left(2^{n/2} \cdot x_1 + x_0\right)\left(2^{n/2} \cdot y_1 + y_0\right)$$
$$= 2^n \cdot \underbrace{x_1 y_1}_{A} + 2^{n/2} \cdot \underbrace{(x_1 y_0 + x_0 y_1)}_{\alpha\beta - A - B} + \underbrace{x_0 y_0}_{B}$$

To multiply two n-bit integers:

- Add two n/2 bit integers.
- Multiply three n/2-bit integers.
- Add, subtract, and shift n/2-bit integers to obtain result.

$$T(n) = 3T\left(\frac{n}{2}\right) + O(n) \Rightarrow T(n) = O\left(n^{\log_2 3}\right) = O(n^{1.585\ldots})$$

Integer Multiplication (Summary)

- Naïve: $\Theta(n^2)$
- Karatsuba: $\Theta(n^{1.585\ldots})$
- Amusing exercise: generalize Karatsuba to do 5 size n/3 subproblems

  This gives $\Theta(n^{1.46\ldots})$ time algorithm

- Best known algorithm runs in $\Theta(n \log n)$ using fast Fourier transform

  but mostly unused in practice (unless you need really big numbers - a billion digits of π, say)

- Best lower bound $O(n)$: A fundamental open problem

Median

Selecting k-th smallest

Problem: Given numbers $x_1, \dots, x_n$ and an integer $1 \leq k \leq n$ output the k-th smallest number

$$\mathrm{Sel}(\{x_1, \dots, x_n\}, k)$$

A simple algorithm: Sort the numbers in time O(n log n) then return the k-th smallest in the array.

Can we do better?

Yes, in time $O(n)$ if $k = 1$ or $k = 2$.

Can we do $O(n)$ for all possible values of k?

Assume all numbers are distinct for simplicity.

An Idea

Choose a number w from $x_1, \ldots, x_n$

Define

- $S_<(w) = \{x_i : x_i < w\}$
- $S_=(w) = \{x_i : x_i = w\}$
- $S_>(w) = \{x_i : x_i > w\}$

Can be computed in linear time

Solve the problem recursively as follows:

- If $k \leq |S_<(w)|$, output $Sel(S_<(w), k)$
- Else if $k \leq |S_<(w)| + |S_=(w)|$, output w
- Else output $Sel(S_>(w), k - |S_<(w)| - |S_=(w)|)$

Ideally want $|S_<(w)|, |S_>(w)| \leq n/2$. In this case ALG runs in $O(n) + O\left(\frac{n}{2}\right) + O\left(\frac{n}{4}\right) + \cdots + O(1) = O(n)$.

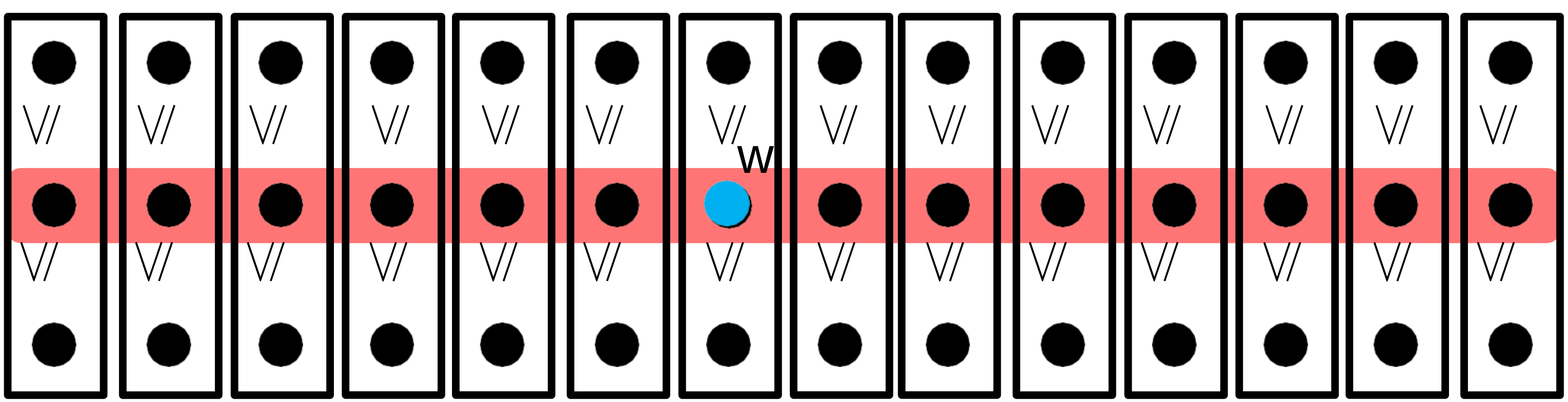
How to choose w?

Suppose we choose w uniformly at random
similar to the pivot in quicksort.

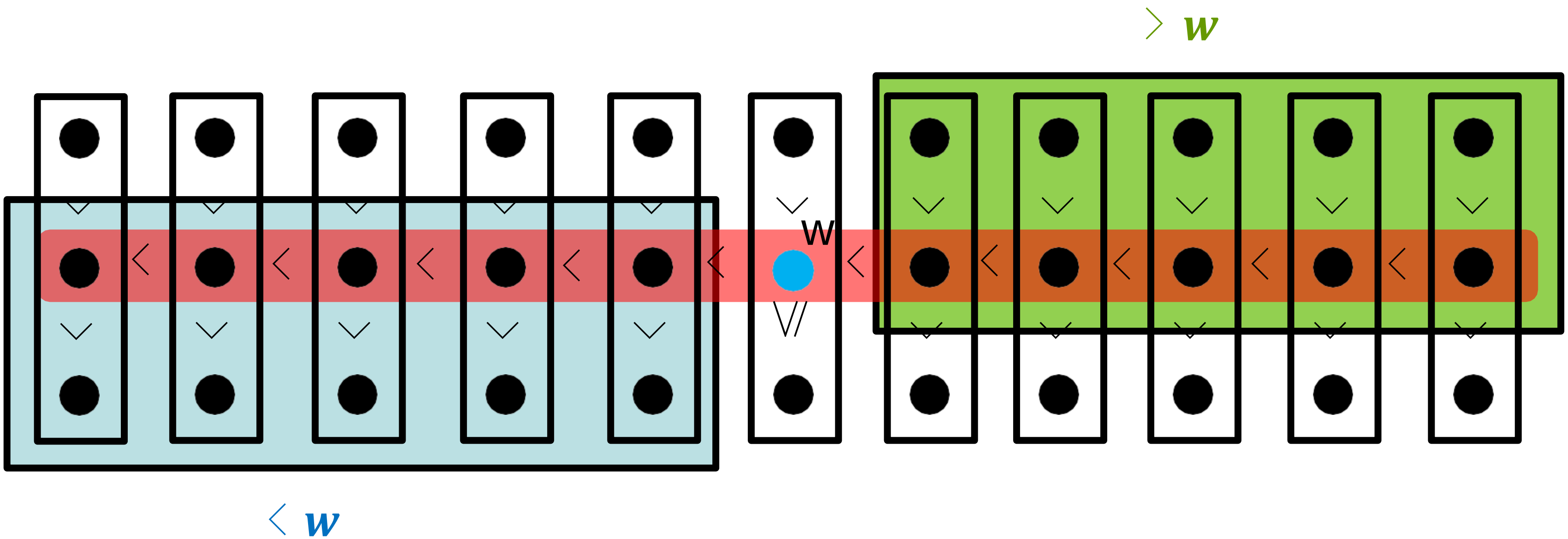
Then, $\mathbb{E}[|S_{<}(w)|] = \mathbb{E}[|S_{>}(w)|] = n/2$. Algorithm runs in $O(n)$ in expectation.

Can we get $O(n)$ running time deterministically?

- Partition numbers into sets of size 3.
- Sort each set (takes O(n))
- $w = Sel(midpoints, n/6)$



How to lower bound $|S_<(w)|, |S_>(w)|$?

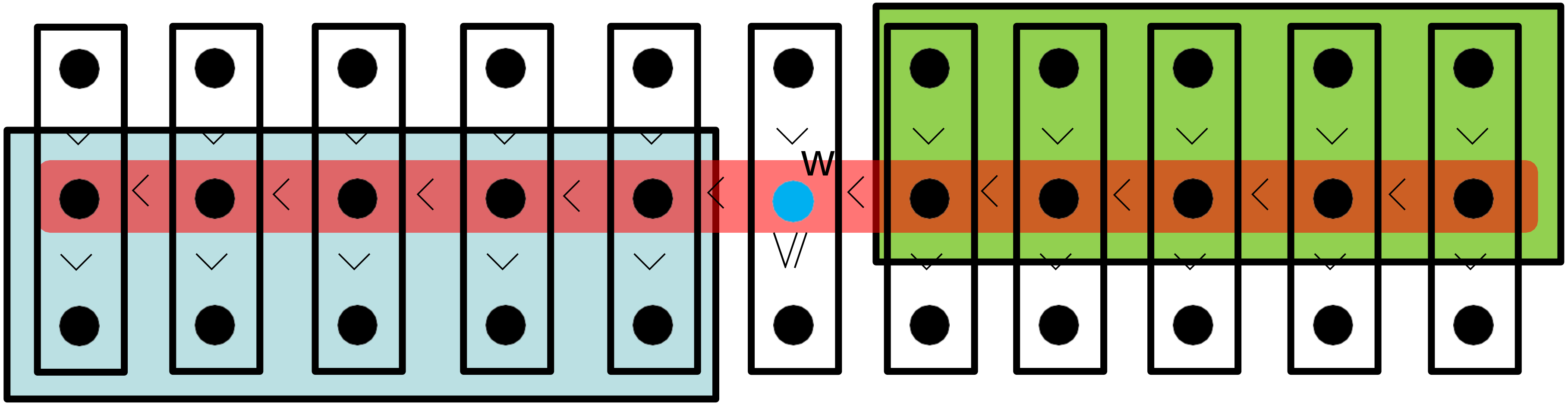


- $|S_<(w)| \geqslant 2\left(\frac{n}{6}\right) = \frac{n}{3}$
- $|S_>(w)| \geqslant 2\left(\frac{n}{6}\right) = \frac{n}{3}$.

$$\frac{n}{3} \leq |S_<(w)|, |S_>(w)| \leq \frac{2n}{3}$$

So, what is the running time?

Asymptotic Running Time?



- If $k \leqslant |S_<(w)|$, output $Sel(S_<(w), k)$
- Else if $k \leqslant |S_<(w)| + |S_=(w)|$, output w
- Else output $Sel(S_>(w), k - S_<(w) - S_=(w))$

O(nlog n) again?
So, what is the point?

Where $\frac{n}{3} \leqslant |S_<(w)|, |S_>(w)| \leqslant \frac{2n}{3}$

$$T(n) = T\left(\frac{n}{3}\right) + T\left(\frac{2n}{3}\right) + O(n) \Rightarrow T(n) = O(n \log n)$$

D&C Summary

Idea:

"Two halves are better than a whole"

- if the base algorithm has super-linear complexity.

"If a little's good, then more's better"

  - repeat above, recursively

- Applications: Many.
  - Binary Search, Merge Sort, (Quicksort),
  - Root of a Function
  - Closest points,
  - Integer multiplication
  - Median
  - Matrix Multiplication