### Divide And Conquer

#### Imran Rashid

University of Washington

February 14, 2008

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ



#### 1 Basic Idea

2 Mergesort ReviewWhy does it work?

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

#### 1 Basic Idea

- 2 Mergesort ReviewWhy does it work?
- 3 More Real Applications
   Closest Pair of Points
   Integer Multiplication
  - integer multiplication

▲ロト ▲帰 ト ▲ヨト ▲ヨト - ヨ - の々ぐ

#### 1 Basic Idea

- 2 Mergesort ReviewWhy does it work?
- 3 More Real Applications
  Closest Pair of Points
  Integer Multiplication

◆□▶ ◆□▶ ◆□▶ ◆□▶ → □ ◇ ◇ ◇



### Outline

#### 1 Basic Idea

- 2 Mergesort ReviewWhy does it work?
- 3 More Real Applications
   Closest Pair of Points
   Integer Multiplication

◆□▶ ◆□▶ ◆三▶ ◆三▶ →三 ● ● ●

4 Solving Recurrences

### Algorithm Design Techniques

#### Divide & Conquer

- Reduce problem to one or more sub-problems of the same type
- Typically, each sub-problem is at most a constant fraction of the size of the original problem
  - e.g. Mergesort, Binary Search, Strassen's Algorithm, Quicksort (kind of)

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

### Outline

#### 1 Basic Idea

# 2 Mergesort ReviewWhy does it work?

3 More Real Applications
 Closest Pair of Points
 Integer Multiplication

◆□▶ ◆□▶ ◆三▶ ◆三▶ →三 ● ● ●

4 Solving Recurrences

### Mergesort — The Recurrence

 Mergesort: (recursively) sort 2 half-lists, then merge results.

• 
$$T(n) = 2T(n/2) + cn, n > 2$$

$$T(1) = 0$$

# Solution: T(n) = O(n log n) (details later)



◆□▶ ◆□▶ ◆□▶ ◆□▶ → □ ◇ ◇ ◇

### Merge Sort — Algorithm

#### **Algorithm 1** MergeSort(*A*[1...*n*])

if 
$$n = 1$$
 return A  
 $L = MergeSort(A[1...n/2])$   
 $U = MergeSort(A[n/2 + 1...n])$   
return  $Merge(U, L)$ 

**Algorithm 2** Merge(*L*[1...*n*], *U*[1...*n*])

C, new array 
$$[1...2n]$$
  
 $a = 1, b = 1$   
for  $i = 1$  to  $2n$  do  
 $C[i] =$  smaller of  $L[a], U[b]$ , and correspondingly  $a++$  or  
 $b++$   
end for  
return C

### Going From Code to Recurrence

- Carefully define what you're counting, and write it down!
  - "Let C(n) be the number of comparisons between sort keys used by MergeSort when sorting a list of length n 1"

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

- In code, clearly separate <u>base case</u> from <u>recursive case</u>, highlight <u>recursive calls</u>, and <u>operations being counted</u>.
- Write Recurrence(s)

### The Recurrence

$$T(n) = \begin{cases} 0 & \text{if } n = 1 \\ 2T(n/2) + (n-1) & \text{if } n > 1 \end{cases}$$

 Total time: proportional to T(n) (loops, copying data, parameter passing, etc.)

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

### Why Balanced Subdivision?

- Alternative "divide & conquer" algorithm:
  - 1 Sort n-1
  - 2 Sort last 1
  - 3 Merge them

• 
$$T(n) = T(n-1) + T(1) + 2n$$
 for  $n \ge 2$ 

- **T**(1) = 0
- Solution:  $T(n) = 2n + 2(n-1) + 2(n-2) \dots = \Theta(n^2)$

◆□▶ ◆□▶ ◆□▶ ◆□▶ → □ ◇ ◇ ◇

### Another D&C Approach

Suppose we've already invented DumbSort, taking time n<sup>2</sup>

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

- Try Just One Level of divide & conquer:
  - DumbSort(first n/2 elements)
  - DumbSort(last n/2 elements)
  - Merge results
- Time: $2(n/2)^2 + n = n^2/2 + n < n^2$ 
  - Almost twice as fast!

### Another D&C Approach, cont.

- Moral 1: "two halves are better than a whole"
  - Two problems of half size are <u>better</u> than one full-size problem, even given the O(n) overhead of recombining, since the base algorithm has super-linear complexity.
- Moral 2: "If a little's good, then more's better"
  - two levels of D&C would be almost 4 times faster, 3 levels almost 8, etc., even though overhead is growing. Best is usually full recursion down to some small constant size (balancing "work" vs "overhead").

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

### Another D&C Approach, cont.

#### Moral 3: unbalanced division not as good:

$$(.1n)^2 + (.9n)^2 + n = .82n^2 + n$$

- The 18% savings compounds significantly if you carry recursion to more levels, actually giving O(nlogn), but with a bigger constant. So worth doing if you can't get 50-50 split, but balanced is better if you can.
- This is intuitively why Quicksort with random splitter is good – badly unbalanced splits are rare, and not instantly fatal.

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

• 
$$(1)^2 + (n-1)^2 + n = n^2 - 2n + 2 + n$$

Little improvement here.

### Outline

#### 1 Basic Idea

- 2 Mergesort ReviewWhy does it work?
- 3 More Real Applications
  Closest Pair of Points
  Integer Multiplication

▲ロト ▲帰 ト ▲ヨト ▲ヨト - ヨ - の々ぐ



### **Closest Pair of Points**

- Closest pair. Given n points in the plane, find a pair with smallest Euclidean distance between them.
- Fundamental geometric primitive.
  - Graphics, computer vision, geographic information systems, molecular modeling, air traffic control.
  - Special case of nearest neighbor, Euclidean MST, Voronoi.
- Brute force. Check all pairs of points p and q with Θ(n<sup>2</sup>) comparisons.
- 1-D version.  $O(n \log n)$  easy if points are on a line.
- (Assumption: No two points have same x coordinate.)

### Closest Pair of Points: First Attempt

Divide. Sub-divide region into 4 quadrants.



◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへの

### Closest Pair of Points: First Attempt

- Divide. Sub-divide region into 4 quadrants.
- Obstacle. Impossible to ensure n/4 points in each piece.



- Algorithm.
  - **1** Divide: draw vertical line L so that roughly n/2 points on each side.

3

- ▲ @ ▶ - ▲ 글 ▶



- Algorithm.
  - **1** Divide: draw vertical line L so that roughly n/2 points on each side.

3

- - E - b

**2** Conquer: find closest pair in each side recursively.



- Algorithm.
  - **1** Divide: draw vertical line L so that roughly n/2 points on each side.
  - 2 Conquer: find closest pair in each side recursively.
  - **3** Combine: find closest pair with one point in each side.

3



#### Algorithm.

- **1** Divide: draw vertical line L so that roughly n/2 points on each side.
- 2 Conquer: find closest pair in each side recursively.
- 3 Combine: find closest pair with one point in each side.

(E) < E)</p>

э

- 4 Return best of 3 solutions.
- But isn't the Combine step  $\Theta(n^2)$ !!



Find closest pair with one point in each side, assuming that distance  $< \delta = min$ (left half, right half).



- Find closest pair with one point in each side, assuming that distance  $< \delta = min$ (left half, right half).
  - Observation: only need to consider points within  $\delta$  of line L.

・ロト ・ 一下・ ・ ヨト ・ ヨト

-



- Find closest pair with one point in each side, assuming that distance  $< \delta = min(\text{left half, right half}).$ 
  - Observation: only need to consider points within  $\delta$  of line L.

- 4 周 ト 4 ヨ ト 4 ヨ ト

Sort points in  $2\delta$ -strip by their y coordinate.



- Find closest pair with one point in each side, assuming that distance  $< \delta = min$ (left half, right half).
  - Observation: only need to consider points within  $\delta$  of line L.
  - Sort points in  $2\delta$ -strip by their y coordinate.
  - Only check distances of those within 8 positions in sorted list!

・ロト ・ 一 ・ ・ ヨ ・ ・ ヨ ・



### Closest Pair of Points: $\delta$ -strip

- Def. Let s<sub>i</sub> be the point in the 2δ-strip, with the ith smallest y-coordinate.
- Claim. If |i j| > 8, then the distance between  $s_i$  and  $s_j$  is at least  $\delta$ .
- Pf.
  - No two points lie in same  $1/2\delta$ -by- $1/2\delta$  box.
  - only 8 boxes



### Closest Pair Algorithm

if  $n \leq 1$  return  $\infty$ 

Sort points by x coordinate

Choose line *L* to divide points in half by *x* coordinate.  $\delta = min(ClosestPair(left), ClosestPair(right))$ 

Delete all points further than  $\delta$  from L.

Sort remaining points by y coordinate, say p[1] to p[m]for i = 1 to m do

$$\begin{array}{l} k \leftarrow 1 \\ \text{while } (i + k \leq m) \&\& (p[i + k].y < p[i].y + \delta) \text{ do} \\ \delta \leftarrow \min(\delta, dist(p[i], p[i + k])) \\ k \leftarrow k + 1 \\ \text{end while} \\ \text{end for} \end{array}$$

### Going From Code to Recurrence

- Carefully define what you're counting, and write it down!
  - "Let C(n) be the number of distance calculations made while finding the closest pair of n points"

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

- In code, clearly separate base case from recursive case, highlight recursive calls, and operations being counted.
- Write Recurrence(s)

### Closest Pair of Points: Analysis, distance calcs

Running time:

$$T(n) = \begin{cases} 0 & \text{if } n = 1\\ 2T(n/2) + 7n & \text{if } n > 1 \end{cases}$$
$$\Rightarrow T(n) = O(n \log n)$$

BUT - that's only the number of distance calculations

### Closest Pair of Points: Analysis, comparisons

- $\blacksquare$  More comparisons needed, b/c of sort ...
- Running time.

$$T(n) = \begin{cases} 0 & \text{if } n = 1\\ 2T(n/2) + n \log n & \text{if } n > 1 \end{cases}$$

$$\Rightarrow T(n) = O(n \log^2 n)$$

- **Q**. Can we achieve  $O(n \log n)$ ?
- A. Yes. Don't sort points from scratch each time.
  - Sort by x at top level only.
  - $\blacksquare$  Each recursive call returns  $\delta$  and list of all points sorted by y
  - Sort by merging two pre-sorted lists.

### Integer Arithmetic

- Add. Given two n-digit integers a and b, compute a + b.
   O(n) bit operations.
- Multiply. Given two n-digit integers a and b, compute a × b.

< □ > < 同 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

• Brute force solution:  $\Theta(n^2)$  bit operations.

### Divide-and-Conquer Multiplication: Warmup

■ To multiply two *n*-digit integers:

- Multiply four  $\frac{n}{2}$ -digit integers.
- Add  $\frac{n}{2}$ -digit integers, and shift to obtain result.

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

$$T(n) = 4T(n/2) + cn \Rightarrow T(n) = \Theta(n^2)$$

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

### Key trick: 2 multiplies for the price of 1:

$$\begin{aligned} \alpha &= x_1 + x_0 \\ \beta &= y_1 + y_0 \\ \alpha \beta &= (x_1 + x_0)(y_1 + y_0) \\ &= x_1 y_1 + (x_1 y_0 + x_0 y_1) + x_0 y_0 \\ (x_1 y_0 + x_0 y_1) &= \alpha \beta - x_1 y_1 - x_0 y_0 \end{aligned}$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

### Key trick: 2 multiplies for the price of 1:

$$\alpha = x_1 + x_0$$
  

$$\beta = y_1 + y_0$$
  

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

$$= x_1y_1 + (x_1y_0 + x_0y_1) + x_0y_0$$
  

$$(x_1y_0 + x_0y_1) = \alpha\beta - x_1y_1 - x_0y_0$$

$$\begin{aligned} x \times y &= (2^{n/2} x_1 + x_0)(2^{n/2} y_1 + y_0) \\ &= 2^n x_1 y_1 + 2^{n/2} (x_1 y_0 + x_0 y_1) + x_0 y_0 \\ &= 2^n x_1 y_1 + 2^{n/2} (\alpha \beta - x_1 y_1 - x_0 y_0) + x_0 y_0 \end{aligned}$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

### Karatsuba Multiplication

To multiply two n-digit integers:

- Add two  $\frac{n}{2}$ -digit integers.
- Multiply three  $\frac{n}{2}$ -digit integers.
- Add, subtract, and shift  $\frac{n}{2}$ -digit integers to obtain result.

$$A = x_1 y_1$$
  

$$B = (x_1 + x_0)(y_1 + y_0)$$
  

$$C = x_0 y_0$$
  

$$xy = 2^n A + 2^{n/2} (B - A - C) + C$$

 Theorem. [Karatsuba-Ofman, 1962] Can multiply two n-digit integers in O(n<sup>1.585</sup>) bit operations.

$$T(n) = 3T(n/2) + cn \Rightarrow T(n) = O(n^{1.585})$$

### Multiplication – The Bottom Line

- Naive:  $\Theta(n^2)$
- Karatsuba: Θ(n<sup>1.59...</sup>)
- Amusing exercise: generalize Karatsuba to do 5 size n/3 subproblems  $\Rightarrow \Theta(n^{1.46...})$
- Best known:  $\Theta(n \log n \log \log n)$ 
  - "Fast Fourier Transform"
  - but mostly unused in practice (unless you need really big numbers - a billion digits of π, say)

(日) (同) (三) (三) (三) (○) (○)

High precision arithmetic <u>IS</u> important for crypto

### Outline

#### 1 Basic Idea

- 2 Mergesort ReviewWhy does it work?
- 3 More Real Applications
   Closest Pair of Points
   Integer Multiplication



うしん 前 ふかく ボット 御 くし く



■ Where they come from, how to find them (above)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ▶ ④ ●

Next: how to solve them

## Mergesort (review)

Mergesort: (recursively) sort 2 half-lists, then merge results.

< □ > < 同 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

- $T(n) = 2T(n/2) + cn, n \ge 2$
- T(1) = 0
- Solution:  $O(n \log n)$

### The Recurrence

- Total time: proportional to C(n)
- (loops, copying data, parameter passing, etc.)

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

# Solve: T(1) = c, T(n) = 2T(n/2) + cn

Count work at each level								
level	num	size	work					
0	$1 = 2^{0}$	п	сп					
1	$2 = 2^{1}$	n/2	2 <i>cn</i> /2					
2	$4 = 2^2$	<i>n</i> /4	4 <i>cn</i> /4					
:	÷	•	:					
i	2 <sup>i</sup>	n/2 <sup>i</sup>	2 <sup>i</sup> cn/2 <sup>i</sup>					
÷	:	:	:					
k-1	$2^{k-1}$	$n/2^{k-1}$	$2^{k-1}cn/2^{k-1}$					
k	2 <sup>k</sup>	$n/2^{k} = 1$	$2^{k}T(1)$					
$\bullet 2^k = n$	$\Rightarrow$	$k = \log k$	ו					
• log <i>n</i> levels, each with $O(n)$ work, $\Rightarrow O(n \log n)$								
			< D > < B > < E	▶ < ≣ ► ≣ • • • • •				

# Solve: T(1) = c, T(n) = 4T(n/2) + cn

Count work at each level								
	level	num	size	work				
	0	$1 = 4^{0}$	п	сп				
	1	$4 = 4^{1}$	n/2	4 <i>cn</i> /2				
	2	$16 = 4^2$	<i>n</i> /4	4 <i>cn</i> /4				
	÷	÷	:	:				
	i	4 <sup><i>i</i></sup>	$n/2^i$	4 <sup>i</sup> cn/2 <sup>i</sup>				
	÷	÷	:	÷				
	k-1	$4^{k-1}$	$n/2^{k-1}$	$4^{k-1}cn/2^{k-1}$				
	k	4 <sup><i>k</i></sup>	$n/2^{k} = 1$	$4^{k}T(1)$				
$ \sum_{i=0}^{k} 4^{i} cn/2^{i} = O(n^{2}) $								

# Solve: T(1) = c, T(n) = 3T(n/2) + cn

Count work at each level							
	level	num	size	work			
	0	$1 = 3^{0}$	n	сп			
	1	$3 = 3^1$	n/2	3 <i>cn</i> /2			
	2	$9 = 3^2$	n/4	9 <i>cn</i> /4			
	÷	:	:	:			
	i	3 <sup>i</sup>	$n/2^i$	3 <sup>i</sup> cn/2 <sup>i</sup>			
	÷	:	:	÷			
	k	3 <sup><i>k</i></sup>	$n/2^{k} = 1$	$3^{k}T(1)$			
• Total Work: $T(n) = \sum_{i=0}^{k} 3^{i} cn/2^{i}$							

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 - のへで

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ



$$T(n) = \sum_{i=0}^{k} 3^{i} cn/2^{i}$$
(1)  
=  $cn \sum_{i=0}^{k} 3^{i}/2^{i}$ (2) for  
=  $cn \sum_{i=0}^{k} \left(\frac{3}{2}\right)^{i}$ (3)  
=  $cn \frac{\left(\frac{3}{2}\right)^{k+1} - 1}{\frac{3}{2} - 1}$ (4) (when  
=  $2cn(\left(\frac{3}{2}\right)^{k+1} - 1)$ (5)

1)  
2) for (3) to (4):  
3) 
$$\sum_{i=0}^{k} x^{i} = \frac{x^{k+1} - 1}{x - 1}$$
  
(when  $x \neq 1$ )  
4)

ロト (四) (三) (三) (三) (三) (三) (三)

$$T(n) < 2cn \left(\frac{3}{2}\right)^{k+1}$$
(1)  
=  $3cn \left(\frac{3}{2}\right)^{k}$ (2)  
=  $3cn \frac{3^{k}}{2^{k}}$ (3)  
=  $3cn \frac{3^{\log_2 n}}{2^{\log_2 n}}$ (4)  
=  $3c (3^{\log_2 n})$ (5)  
=  $3c (n^{\log_2 3})$ (6)  
=  $O(n^{1.58...})$ (7)

$$T(n) < 2cn \left(\frac{3}{2}\right)^{k+1}$$
$$= 3cn \left(\frac{3}{2}\right)^{k}$$
$$= 3cn \frac{3^{k}}{2^{k}}$$
$$= 3cn \frac{3^{\log_2 n}}{2^{\log_2 n}}$$
$$= 3c (3^{\log_2 n})$$
$$= 3c (n^{\log_2 3})$$
$$= O(n^{1.58...})$$

(1)for (5) to (6) (2) $= a^{\log_b n}$ (3) $= \left( b^{\log_b a} \right)^{\log_b n}$  $= \left( b^{\log_b n} \right)^{\log_b a}$ (4) $= n^{\log_b a}$ (5)(6)(7)◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

### Master Divide and Conquer Recurrence

If T(n) = aT(n/b) + cn<sup>k</sup> for n > b then
if a > b<sup>k</sup> then T(n) is Θ(n<sup>log<sub>b</sub> a</sup>). (many subproblems ⇒ leaves dominate)
if a < b<sup>k</sup> then iT(n) is Θ(n<sup>k</sup>) (few subproblems ⇒ top level dominates)
if a = b<sup>k</sup> then T(n) is Θ(n<sup>k</sup>logn) (balanced ⇒ all log n levels contribute)
True even if it is [n/b] instead of n/b.

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

### Divide And Conquer Summary

- If base algorithm is super-linear, dividing into pieces can help. "Two halves better than a whole."
- Very carefully analyze the recurrence. Some constants matter, be careful not to miss anything.
- Solve recurrence with recursion tree or Master Recurrence

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

### More applications

More applications of divide & Conquer in the book:

< □ > < 同 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

- Polynomial Multiplication
- Fast Fourier Transform
  - very useful in signal processing