CSE 421: Introduction to Algorithms

Divide and Conquer

Winter 2005
Paul Beame

1

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)

2

Fast exponentiation

- Power($\mathbf{a}$,$\mathbf{n}$)
  - **Input:** integer $\mathbf{n}$ and number $\mathbf{a}$
  - **Output:** $\mathbf{a^n}$
- Obvious algorithm
  - $\mathbf{n-1}$ multiplications
- Observation:
  - if $\mathbf{n}$ is even, $\mathbf{n=2m}$, then $\mathbf{a^n=a^m \bullet a^m}$

3

Divide & Conquer Algorithm

- Power($\mathbf{a}$,$\mathbf{n}$)
  - if $\mathbf{n=0}$ then return($\mathbf{1}$)
  - else if $\mathbf{n=1}$ then return($\mathbf{a}$)
  - else
    - $\mathbf{x} \leftarrow$ Power($\mathbf{a}$,$\lfloor \mathbf{n/2} \rfloor$)
    - if $\mathbf{n}$ is even then
      - return($\mathbf{x \bullet x}$)
    - else
      - return($\mathbf{a \bullet x \bullet x}$)

4

Analysis

- Worst-case recurrence
  - $\mathbf{T(n)=T(\lfloor n/2 \rfloor)+2}$ for $\mathbf{n \geq 1}$
  - $\mathbf{T(1)=0}$
- Time
  - $\mathbf{T(n)=T(\lfloor n/2 \rfloor)+2 \leq T(\lfloor n/4 \rfloor)+2+2} \leq \ldots$
    $\leq \mathbf{T(1)}+\underbrace{\mathbf{2}+\ldots+\mathbf{2}}_{\log_2 n \text{ copies}} = \mathbf{2} \log_2 \mathbf{n}$
- More precise analysis:
  - $\mathbf{T(n)} = \lceil \log_2 \mathbf{n} \rceil$ + # of $\mathbf{1}$'s in $\mathbf{n}$'s binary representation

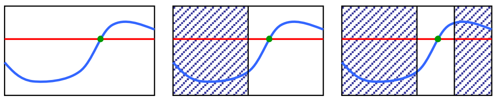
5

A Practical Application- RSA

- Instead of $\mathbf{a^n}$ want $\mathbf{a^n}$ **mod N**
  - $\mathbf{a^{i+j}}$ mod $\mathbf{N}$ = (($\mathbf{a^i}$ mod $\mathbf{N}$)$\bullet$($\mathbf{a^j}$ mod $\mathbf{N}$)) mod $\mathbf{N}$
  - same algorithm applies with each $\mathbf{x \bullet y}$ replaced by
    - (($\mathbf{x}$ mod $\mathbf{N}$)$\bullet$($\mathbf{y}$ mod $\mathbf{N}$)) mod $\mathbf{N}$
- In RSA cryptosystem (widely used for security)
  - need $\mathbf{a^n}$ **mod N** where $\mathbf{a}$, $\mathbf{n}$, $\mathbf{N}$ each typically have **1024** bits
  - Power: at most **2048** multiplies of 1024 bit numbers
    - relatively easy for modern machines
  - Naive algorithm: $\mathbf{2^{1024}}$ multiplies

6

Binary search for roots (bisection method)



- Given:
  - continuous function **f** and two points **a**<**b** with **f(a)** ≤ **0** and **f(b) > 0**
- Find:
  - approximation to **c** s.t. **f(c)=0** and **a**<**c**<**b**

7

Bisection method

Bisection(**a**,**b**, **ε**)
    if (**a**-**b**) < **ε** then
        return(**a**)
    else
        c ←(**a**+**b**)/**2**
        if **f**(**c**) ≤ **0** then
            return(Bisection(**c**,**b**,**ε**))
        else
            return(Bisection(**a**,**c**,**ε**))

8

Time Analysis

- At each step we halved the size of the interval
- It started at size **b**-**a**
- It ended at size **ε**
- # of calls to f is $\log_2((b-a)/\varepsilon)$

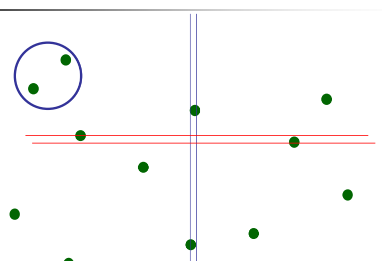
9

Euclidean Closest Pair

- Given a set **P** of n points $p_1,\ldots,p_n$ with real-valued coordinates
- Find the pair of points $p_i,p_j \in P$ such that the Euclidean distance $d(p_i,p_j)$ is minimized
- $\Theta(n^2)$ possible pairs
- In one dimension there is an easy **O**(**n** log **n**) algorithm
  - Sort the points
  - Compare consecutive elements in the sorted list
- What about points in the plane?

10

Closest Pair in the Plane



No single direction along which one can sort points to guarantee success!

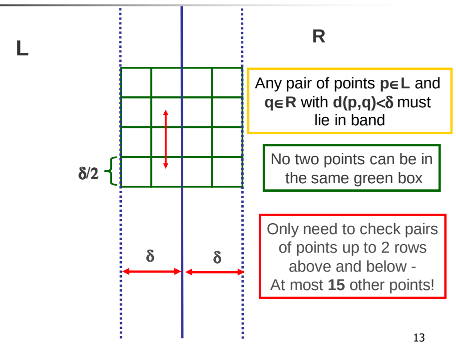
11

Closest Pair In the Plane: Divide and Conquer

- Sort the points by their **x** coordinates
- Split the points into two sets of **n**/2 points **L** and **R** by **x** coordinate
- Recursively compute
  - closest pair of points in **L**, (p_L,q_L)
  - closest pair of points in **R**, (p_R,q_R)
- Let $\delta=\min\{d(p_L,q_L),d(p_R,q_R)\}$ and let (**p**,**q**) be the pair of points that has distance δ
- This may not be enough!
  - Closest pair of points may involve one point from **L** and the other from **R**!

12

A clever geometric idea



Closest Pair Recombining

- Sort points by **y** coordinate ahead of time
- On recombination only compare each point in **L∪R** to the **12** points above it in the **y** sorted order
- If any of those distances is better than **δ** replace **(p,q)** by the best of those pairs
- **O(n log n)** for **x** and **y** sorting at start
- Two recursive calls on problems on half size
- **O(n)** recombination
- Total **O(n log n)**

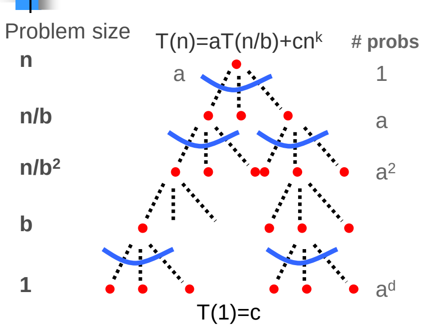
Sometimes two sub-problems aren't enough

- More general divide and conquer
  - You've broken the problem into a different sub-problems
  - Each has size at most **n/b**
  - The cost of the break-up and recombining the sub-problem solutions is $O(n^k)$
- Recurrence
  - $T(n) \le a \cdot T(n/b) + c \cdot n^k$

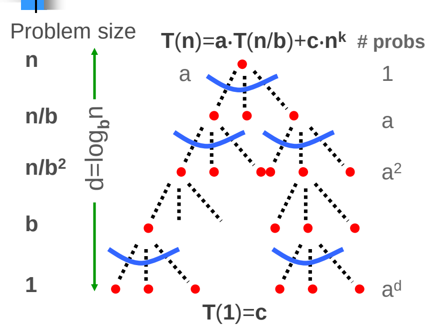
Master Divide and Conquer Recurrence

- If $T(n) \le a \cdot T(n/b) + c \cdot n^k$ for $n>b$ then
  - if $a>b^k$ then $T(n)$ is $\Theta(n^{\log_b a})$
  - if $a<b^k$ then $T(n)$ is $\Theta(n^k)$
  - if $a=b^k$ then $T(n)$ is $\Theta(n^k \log n)$
- Works even if it is $\lceil n/b \rceil$ instead of **n/b**.

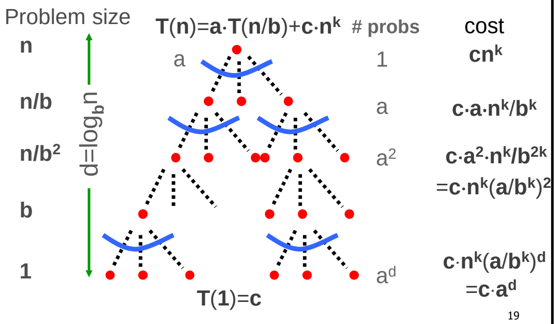
Proving Master recurrence



Proving Master recurrence



Proving Master recurrence



Geometric Series

- $S \quad = t + tr + tr^2 + \ldots + tr^{n-1}$
- $r \cdot S \quad = \quad tr + tr^2 + \ldots + tr^{n-1} + tr^n$
- $(r-1)S = tr^n - t$
- so $S = t(r^n - 1)/(r-1)$ if $r \neq 1$.

- Simple rule
  - If $r \neq 1$ then S is a constant times largest term in series

Total Cost

- Geometric series
  - ratio a/b^k
  - $d+1 = \log_b n + 1$ terms
  - first term cn^k, last term ca^d
- If $a/b^k = 1$
  - all terms are equal $T(n)$ is $\Theta(n^k \log n)$
- If $a/b^k < 1$
  - first term is largest $T(n)$ is $\Theta(n^k)$
- If $a/b^k > 1$
  - last term is largest $T(n)$ is $\Theta(a^d) = \Theta(a^{\log_b n}) = \Theta(n^{\log_b a})$
  (To see this take $\log_b$ of both sides)

Multiplying Matrices

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \bullet \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31}+a_{14}b_{41} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32}+a_{14}b_{42} & \circ & a_{11}b_{14}+a_{12}b_{24}+a_{13}b_{34}+a_{14}b_{44} \\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31}+a_{24}b_{41} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32}+a_{24}b_{42} & \circ & a_{21}b_{14}+a_{22}b_{24}+a_{23}b_{34}+a_{24}b_{44} \\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31}+a_{34}b_{41} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32}+a_{34}b_{42} & \circ & a_{31}b_{14}+a_{32}b_{24}+a_{33}b_{34}+a_{34}b_{44} \\ a_{41}b_{11}+a_{42}b_{21}+a_{43}b_{31}+a_{44}b_{41} & a_{41}b_{12}+a_{42}b_{22}+a_{43}b_{32}+a_{44}b_{42} & \circ & a_{41}b_{14}+a_{42}b_{24}+a_{43}b_{34}+a_{44}b_{44} \end{bmatrix}$$

- n^3 multiplications, n^3-n^2 additions

Multiplying Matrices

```
for i=1 to n
    for j=1 to n
        C[i,j]←0
        for k=1 to n
            C[i,j]=C[i,j]+A[i,k]·B[k,j]
        endfor
    endfor
endfor
```


Multiplying Matrices

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \bullet \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31}+a_{14}b_{41} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32}+a_{14}b_{42} & \circ & a_{11}b_{14}+a_{12}b_{24}+a_{13}b_{34}+a_{14}b_{44} \\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31}+a_{24}b_{41} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32}+a_{24}b_{42} & \circ & a_{21}b_{14}+a_{22}b_{24}+a_{23}b_{34}+a_{24}b_{44} \\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31}+a_{34}b_{41} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32}+a_{34}b_{42} & \circ & a_{31}b_{14}+a_{32}b_{24}+a_{33}b_{34}+a_{34}b_{44} \\ a_{41}b_{11}+a_{42}b_{21}+a_{43}b_{31}+a_{44}b_{41} & a_{41}b_{12}+a_{42}b_{22}+a_{43}b_{32}+a_{44}b_{42} & \circ & a_{41}b_{14}+a_{42}b_{24}+a_{43}b_{34}+a_{44}b_{44} \end{bmatrix}$$

Multiplying Matrices

$$\begin{bmatrix} a_{11} & a_{12} & \boxed{a_{13} & a_{14}} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \bullet \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31}+a_{14}b_{41} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32}+a_{14}b_{42} & \circ & a_{11}b_{14}+a_{12}b_{24}+a_{13}b_{34}+a_{14}b_{44} \\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31}+a_{24}b_{41} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32}+a_{24}b_{42} & \circ & a_{21}b_{14}+a_{22}b_{24}+a_{23}b_{34}+a_{24}b_{44} \\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31}+a_{34}b_{41} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32}+a_{34}b_{42} & \circ & a_{31}b_{14}+a_{32}b_{24}+a_{33}b_{34}+a_{34}b_{44} \\ a_{41}b_{11}+a_{42}b_{21}+a_{43}b_{31}+a_{44}b_{41} & a_{41}b_{12}+a_{42}b_{22}+a_{43}b_{32}+a_{44}b_{42} & \circ & a_{41}b_{14}+a_{42}b_{24}+a_{43}b_{34}+a_{44}b_{44} \end{bmatrix}$$

Multiplying Matrices

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \bullet \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} A_{11}B_{11}+A_{12}B_{21} & A_{11}B_{12}+A_{12}B_{22} \\ A_{21}B_{11}+A_{22}B_{21} & A_{21}B_{12}+A_{22}B_{22} \end{bmatrix}$$

Simple Divide and Conquer

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} A_{11}B_{11}+A_{12}B_{21} & A_{11}B_{12}+A_{12}B_{22} \\ A_{21}B_{11}+A_{22}B_{21} & A_{21}B_{12}+A_{22}B_{22} \end{bmatrix}$$

- $T(n)=8T(n/2)+4(n/2)^2=8T(n/2)+n^2$
  - $8>2^2$ so $T(n)$ is $\Theta(n^{\log_b a}) = \Theta(n^{\log_2 8}) = \Theta(n^3)$

Strassen's Divide and Conquer Algorithm

- Strassen's algorithm
  - Multiply 2x2 matrices using 7 instead of 8 multiplications (and lots more than 4 additions)
  - $T(n)=7\,T(n/2)+cn^2$
    - $7>2^2$ so $T(n)$ is $\Theta(n^{\log_2 7})$ which is $O(n^{2.81\ldots})$
  - Fastest algorithms theoretically use $O(n^{2.376})$ time
    - not practical but Strassen's is practical **provided calculations are exact** and we stop recursion when matrix has size about 100 (maybe 10)

The algorithm

$P_1 \leftarrow A_{12}(B_{11}+B_{21})$; $P_2 \leftarrow A_{21}(B_{12}+B_{22})$

$P_3 \leftarrow (A_{11} - A_{12})B_{11}$; $P_4 \leftarrow (A_{22} - A_{21})B_{22}$

$P_5 \leftarrow (A_{22} - A_{12})(B_{21} - B_{22})$

$P_6 \leftarrow (A_{11} - A_{21})(B_{12} - B_{11})$

$P_7 \leftarrow (A_{21} - A_{12})(B_{11}+B_{22})$

$C_{11} \leftarrow P_1+P_3$; $C_{12} \leftarrow P_2+P_3+P_6 - P_7$

$C_{21} \leftarrow P_1+P_4+P_5+P_7$; $C_{22} \leftarrow P_2+P_4$

Another Divide &Conquer Example: Multiplying Faster

- If you analyze our usual grade school algorithm for multiplying numbers
  - $\Theta(n^2)$ time
  - On real machines each "digit" is, e.g., **32** bits long but still get $\Theta(n^2)$ running time with this algorithm when run on **n**-bit multiplication
- We can do better!
  - We'll describe the basic ideas by multiplying polynomials rather than integers
  - Advantage is we don't get confused by worrying about carries at first

Notes on Polynomials

- These are just formal sequences of coefficients
  - when we show something multiplied by x^k it just means shifted **k** places to the left – basically no work

Usual polynomial multiplication

$$
\begin{array}{r}
4x^2 + 2x + 2 \\
x^2 - \ 3x + 1 \\
\hline
4x^2 + 2x + 2 \\
-12x^3 - 6x^2 - 6x \quad \\
4x^4 + 2x^3 + 2x^2 \qquad\qquad \\
\hline
4x^4 - 10x^3 + 0x^2 - 4x + 2
\end{array}
$$

Polynomial Multiplication

- **Given:**
  - Degree **n-1** polynomials **P** and **Q**
    - $P = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}$
    - $Q = b_0 + b_1 x + b_2 x^2 + \dots + b_{n-2}x^{n-2} + b_{n-1}x^{n-1}$
- **Compute:**
  - Degree **2n-2** Polynomial **P Q**
  - $P Q = a_0b_0 + (a_0b_1+a_1b_0)\,x + (a_0b_2+a_1b_1+a_2b_0)\,x^2 + \dots + (a_{n-2}b_{n-1}+a_{n-1}b_{n-2})\,x^{2n-3} + a_{n-1}b_{n-1}\,x^{2n-2}$
- **Obvious Algorithm:**
  - Compute all a_ib_j and collect terms
  - $\Theta(n^2)$ time

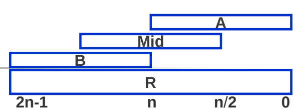
Naive Divide and Conquer

- Assume **n=2k**
  - $P = (a_0 + a_1\ x + a_2 x^2 + \dots + a_{k-2} x^{k-2} + a_{k-1} x^{k-1}) + (a_k + a_{k+1} x + \dots + a_{n-2}x^{k-2} + a_{n-1}x^{k-1})\, x^k$
    $= P_0 + P_1 x^k$ where P_0 and P_1 are degree **k-1** polynomials
  - Similarly $Q = Q_0 + Q_1 x^k$
- $P Q = (P_0+P_1x^k)(Q_0+Q_1x^k)$
  $= P_0Q_0 + (P_1Q_0+P_0Q_1)x^k + P_1Q_1x^{2k}$
- **4** sub-problems of size **k=n/2** plus linear combining
  - $T(n)=4\cdot T(n/2)+cn$ Solution $T(n) = \Theta(n^2)$

Karatsuba's Algorithm

- A better way to compute the terms
  - Compute
    - $A \leftarrow P_0Q_0$
    - $B \leftarrow P_1Q_1$
    - $C \leftarrow (P_0+P_1)(Q_0+Q_1) = P_0Q_0+P_1Q_0+P_0Q_1+P_1Q_1$
  - Then
    - $P_0Q_1+P_1Q_0 = C-A-B$
    - So $PQ=A+(C-A-B)x^k+Bx^{2k}$
  - **3** sub-problems of size **n/2** plus **O**(**n**) work
    - $T(n) = 3\ T(n/2) + cn$
    - $T(n) = O(n^\alpha)$ where $\alpha = \log_2 3 = 1.59\dots$

Karatsuba: Details



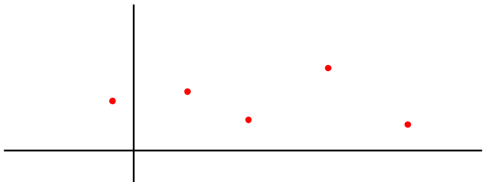
PolyMul(**P**, **Q**):

```
// P, Q are length n =2k vectors, with P[i], Q[i] being
// the coefficient of x^i in polynomials P, Q respectively.
// Let Pzero be elements 0..k-1 of P; Pone be elements k..n-1
// Qzero, Qone : similar
If n=1 then Return(P[0]*Q[0]) else
  A ← PolyMul(Pzero, Qzero);     // result is a (2k-1)-vector
  B ← PolyMul(Pone, Qone);       // ditto
  Psum ← Pzero + Pone;           // add corresponding elements
  Qsum ← Qzero + Qone;           // ditto
  C ← polyMul(Psum, Qsum);       // another (2k-1)-vector
  Mid ← C – A – B;               // subtract correspond elements
  R ← A + Shift(Mid, n/2) +Shift(B,n)   // a (2n-1)-vector
  Return( R);
```


Multiplication

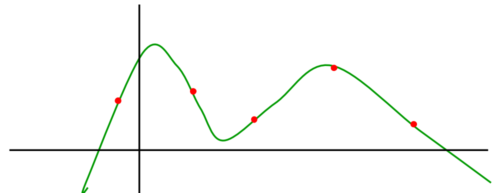
- Polynomials
  - Naïve: $\Theta(n^2)$
  - Karatsuba: $\Theta(n^{1.59\dots})$
  - Best known: $\Theta(n \log n)$
    - "Fast Fourier Transform"
    - FFT widely used for signal processing
- Integers
  - Similar, but some ugly details re: carries, etc. gives $\Theta(n \log n \log\log n)$,
    - mostly unused in practice except for symbolic manipulation systems like Maple

Hints towards FFT: Interpolation



Given set of values at 5 points

Hints towards FFT: Interpolation



Given set of values at **5** points
Can find unique degree **4** polynomial going through these points

Interpolation

- Given values of degree **n-1** polynomial **R** at **n** distinct points $y_1,\dots,y_n$
  - $R(y_1),\dots,R(y_n)$
- Compute coefficients $c_0,\dots,c_{n-1}$ such that
  - $R(x)=c_0+c_1x+c_2x^2+\dots+c_{n-1}x^{n-1}$
- System of linear equations in $c_0,\dots,c_{n-1}$

$$c_0+c_1y_1+c_2y_1^2+\dots+c_{n-1}y_1^{n-1}=R(y_1)$$
$$c_0+c_1y_2+c_2y_2^2+\dots+c_{n-1}y_2^{n-1}=R(y_2)$$
$$\dots$$
$$c_0+c_1y_n+c_2y_n^2+\dots+c_{n-1}y_n^{n-1}=R(y_n)$$

known

unknown

Interpolation: n equations in n unknowns

- Matrix form of the linear system

$$\begin{pmatrix} 1 & y_1 & y_1^2 & \dots & y_1^{n-1} \\ 1 & y_2 & y_2^2 & \dots & y_2^{n-1} \\ & \dots & & & \\ & \dots & & & \\ 1 & y_n & y_n^2 & \dots & y_n^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ . \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} R(y_1) \\ R(y_2) \\ . \\ . \\ R(y_n) \end{pmatrix}$$

- Fact: Determinant of the matrix is $\prod_{i<j}(y_i-y_j)$ which is not **0** since points are distinct
  - System has a unique solution $c_0,\dots,c_{n-1}$

Hints towards FFT: Evaluation & Interpolation

$$\begin{tikzcd}
\boxed{\begin{array}{l} P: a_0,a_1,\dots,a_{n-1} \\ Q: b_0,b_1,\dots,b_{n-1} \end{array}} \arrow[rr, "\substack{\text{ordinary polynomial} \\ \text{multiplication } \boldsymbol{\Theta(n^2)}}", "c_k \leftarrow \sum_{i+j=k} a_ib_j"'] \arrow[d, "\substack{\text{evaluation} \\ \text{at } \mathbf{y_0,\dots,y_{2n-1}} \\ O(?)}"] & & \boxed{R: c_0,c_1,\dots,c_{2n-1}} \\
\boxed{\begin{array}{c} P(y_0),Q(y_0) \\ P(y_1),Q(y_1) \\ \dots \\ P(y_{2n-1}),Q(y_{2n-1}) \end{array}} \arrow[rr, "\substack{\text{point-wise} \\ \text{multiplication} \\ \text{of numbers } \mathbf{O(n)}}"] & & \boxed{\begin{array}{c} R(y_0)\leftarrow P(y_0)\cdot Q(y_0) \\ R(y_1)\leftarrow P(y_1)\cdot Q(y_1) \\ \dots \\ R(y_{2n-1})\leftarrow P(y_{2n-1})\cdot Q(y_{2n-1}) \end{array}} \arrow[u, "\substack{\text{interpolation} \\ \text{from } \mathbf{y_0,\dots,y_{2n-1}} \\ O(?)}"']
\end{tikzcd}$$

Karatsuba's algorithm and evaluation and interpolation

- Strassen gave a way of doing **2**x**2** matrix multiplies with fewer multiplications
- Karatsuba's algorithm can be thought of as a way of multiplying degree **1** polynomials (which have **2** coefficients) using fewer multiplications
  - $PQ=(P_0+P_1z)(Q_0+Q_1z)$
    $= P_0Q_0 + (P_1Q_0+P_0Q_1)z + P_1Q_1z^2$
  - Evaluate at **0,1,-1** (Could also use other points)
    - $A = P(0)Q(0)= P_0Q_0$
    - $C = P(1)Q(1)=(P_0+P_1)(Q_0+Q_1)$
    - $D = P(-1)Q(-1)=(P_0-P_1)(Q_0-Q_1)$
  - Interpolating, Karatsuba's **Mid**=(**C-D**)/**2** and **B=**(**C+D**)/**2-A**

Hints towards FFT: Evaluation at Special Points

- Evaluation of polynomial at **1** point takes **O**(**n**)
  - So **2n** points (naively) takes **O**(n^2)—no savings
- Key trick:
  - use carefully chosen points where there's some sharing of work for several points, namely various powers of $\omega = e^{2\pi i/n}$, $i = \sqrt{-1}$
- Plus more Divide & Conquer.
- Result:
  - both evaluation and interpolation in **O**(**n** log **n**) time

43

Fun facts about $\omega=e^{2\pi i/n}$ for even n

- $\omega^n = 1$
- $\omega^{n/2} = -1$
- $\omega^{n/2+k} = -\omega^k$ for all values of **k**
- $\omega^2 = e^{2\pi i/m}$ where **m=n/2**
- $\omega^k = \cos(2k\pi/n)+i\sin(2k\pi/n)$ so can compute with powers of ω

44

The key idea for n even

- $P(\omega) = a_0+a_1\omega+a_2\omega^2+a_3\omega^3+a_4\omega^4+\ldots+a_{n-1}\omega^{n-1}$
  $= a_0 + a_2\omega^2 + a_4\omega^4 + \ldots + a_{n-2}\omega^{n-2}$
  $+ a_1\omega + a_3\omega^3 + a_5\omega^5 + \ldots + a_{n-1}\omega^{n-1}$
  $= P_{even}(\omega^2) + \omega P_{odd}(\omega^2)$
- $P(-\omega) = a_0 - a_1\omega + a_2\omega^2 - a_3\omega^3 + a_4\omega^4 - \ldots - a_{n-1}\omega^{n-1}$
  $= a_0 + a_2\omega^2 + a_4\omega^4 + \ldots + a_{n-2}\omega^{n-2}$
  $- (a_1\omega + a_3\omega^3 + a_5\omega^5 + \ldots + a_{n-1}\omega^{n-1})$
  $= P_{even}(\omega^2) - \omega P_{odd}(\omega^2)$

where $P_{even}(x) = a_0 + a_2x + a_4x^2 + \ldots + a_{n-2}x^{n/2-1}$

and $P_{odd}(x) = a_1 + a_3x + a_5x^2 + \ldots + a_{n-1}x^{n/2-1}$

45

The recursive idea for n a power of 2

- Also
  - P_{even} and P_{odd} have degree **n/2** where
  - $P(\omega^k) = P_{even}(\omega^{2k}) + \omega^k P_{odd}(\omega^{2k})$
  - $P(-\omega^k) = P_{even}(\omega^{2k}) - \omega^k P_{odd}(\omega^{2k})$
- Recursive Algorithm
  - Evaluate P_{even} at $1, \omega^2, \omega^4, \ldots, \omega^{n-2}$
  - Evaluate P_{odd} at $1, \omega^2, \omega^4, \ldots, \omega^{n-2}$
  - Combine to compute **P** at $1, \omega, \omega^2, \ldots, \omega^{n/2-1}$
  - Combine to compute P at $-1, -\omega, -\omega^2, \ldots, -\omega^{n/2-1}$ (i.e. at $\omega^{n/2}, \omega^{n/2+1}, \omega^{n/2+2}, \ldots, \omega^{n-1}$)

ω^2 is $e^{2\pi i/m}$ where **m=n/2** so problems are of same type but smaller size

46

Analysis and more

- Run-time
  - $T(n)=2\cdot T(n/2)+cn$ so $T(n)=O(n \log n)$
- So much for evaluation ... what about interpolation?
  - Given
    - $r_0=R(1)$, $r_1=R(\omega)$, $r_2=R(\omega^2)$,..., $r_{n-1}=R(\omega^{n-1})$
  - Compute
    - $c_0, c_1, \ldots, c_{n-1}$ s.t. $R(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$

47

Interpolation ≈ Evaluation: strange but true

- Weird fact:
  - If we define a new polynomial $S(x) = r_0 + r_1x + r_2x^2 + \ldots + r_{n-1}x^{n-1}$ where $r_0, r_1, \ldots, r_{n-1}$ are the evaluations of **R** at $1, \omega, \ldots, \omega^{n-1}$
  - Then $c_k=S(\omega^{-k})/n$ for $k=0,\ldots,n-1$
- So...
  - evaluate **S** at $1, \omega^{-1}, \omega^{-2}, \ldots, \omega^{-(n-1)}$ then divide each answer by **n** to get the $c_0, \ldots, c_{n-1}$
  - ω^{-1} behaves just like ω did so the same **O**(**n** log **n**) evaluation algorithm applies !

48

Divide and Conquer Summary

- Powerful technique, when applicable
- Divide large problem into a few smaller problems of the same type
- Choosing sub-problems of roughly equal size is usually critical
- Examples:
  - Merge sort, quicksort (sort of), polynomial multiplication, FFT, Strassen's matrix multiplication algorithm, powering, binary search, root finding by bisection, …

Why this is called the discrete Fourier transform

- Real Fourier series
  - Given a real valued function f defined on $[0,2\pi]$ the Fourier series for f is given by $f(x)=a_0+a_1 \cos(x) + a_2 \cos(2x) + \ldots + a_m \cos(mx) + \ldots$ where

$$\boxed{a_m = \frac{1}{2\pi}\int_0^{2\pi} f(x)\cos(mx)\,dx}$$

  - is the component of f of frequency m
  - In signal processing and data compression one ignores all but the components with large a_m and there aren't many since

Why this is called the discrete Fourier transform

- Complex Fourier series
  - Given a function f defined on $[0,2\pi]$ the complex Fourier series for f is given by $f(z)=b_0+b_1 e^{iz} + b_2 e^{2iz} + \ldots + b_m e^{miz} + \ldots$ where

$$\boxed{b_m = \frac{1}{2\pi}\int_0^{2\pi} f(z)\, e^{-miz}\, dz}$$

    is the component of f of frequency m
  - If we **discretize** this integral using values at n **2π/n apart** equally spaced points between 0 and 2π we get

$$\boxed{\bar{b}_m = \frac{1}{n}\sum_{k=0}^{n-1} f_k\, e^{-2km i\pi/n} = \frac{1}{n}\sum_{k=0}^{n-1} f_k\, \omega^{-km} \text{ where } f_k=f(2k\pi/n)}$$

just like interpolation!