

- Measure the goodness of <u>algorithms</u>
 - efficiency
 - asymptotic notations: e.g. O(n²)
 - worst case
 - average case
 - amortized
- Measure the difficulty of problems
 - NP-complete
 - undecidable
 - lower bound
- Is the algorithm optimal?

0/1 Knapsack problem

| | P_1 | P ₂ | P ₃ | P ₄ | P ₅ | P ₆ | P ₇ | P ₈ |
|--------|-------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| Value | 10 | 5 | 1 | 9 | 3 | 4 | 11 | 17 |
| Weight | 7 | 3 | 3 | 10 | 1 | 9 | 22 | 15 |

M(weight limit)=14 best solution: P_1 , P_2 , P_3 , P_5 (optimal) This problem is <u>NP-complete</u>.

1 -5

1 -7

Traveling salesperson problem

• Given: A set of n planar points

Find: A <u>closed tour</u> which includes all points <u>exactly once</u> such that its total length is <u>minimized</u>.

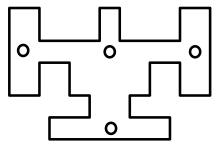
• This problem is <u>NP-complete</u>.

Partition problem

- Given: A set of positive integers S Find: S₁ and S₂ such that S₁ \cap S₂=Ø, S₁ \cup S₂=S, $\sum_{i \in S_1} i = \sum_{i \in S_2} i$
- (partition into S_1 and S_2 such that the sum of S_1 is equal to that of S_2)
- e.g. S={1, 7, 10, 4, 6, 8, 3, 13}
 - S₁={1, 10, 4, 8, 3}

• This problem is <u>NP-complete</u>.

Art gallery problem



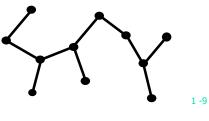
Given: an art gallery

Determine: min # of guards and their placements such that the entire art gallery can be monitored.

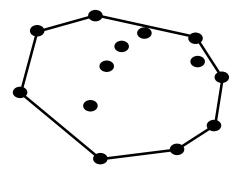
NP-complete

Minimum spanning tree

- graph: greedy method
- geometry(on a plane): <u>divide-and-</u> <u>conquer</u>
- # of possible spanning trees for n points: nⁿ⁻²
- $n=10 \rightarrow 10^8$, $n=100 \rightarrow 10^{196}$



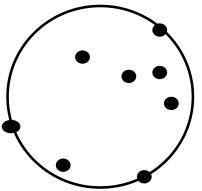
Convex hull



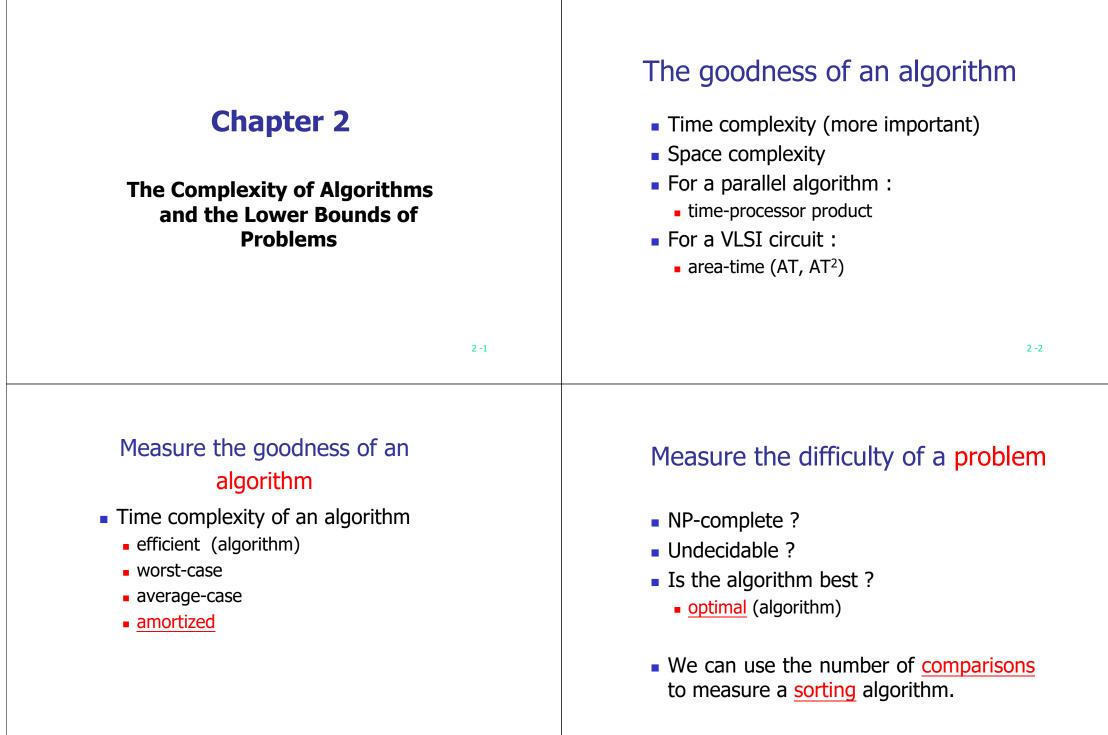
- Given a set of planar points, find a <u>smallest</u> <u>convex polygon</u> which contains all points.
- It is not obvious to find a convex hull by examining all possible solutions
- divide-and-conquer

1 -10

One-center problem



- Given a set of planar points, find a <u>smallest</u> <u>circle</u> which contains all points.
- Prune-and-search



Asymptotic notations

■ <u>Def</u>: f(n) = O(g(n)) "at most" $\exists c, n_0 \ni |f(n)| \le c|g(n)| \forall n \ge n_0$ ■ e.g. $f(n) = 3n^2 + 2$ $g(n) = n^2$ $\Rightarrow n_0=2, c=4$ $\therefore f(n) = O(n^2)$

2 -5

2 -7

- $\underline{\text{Def}}$: $f(n) = \Omega(g(n))$ "at least", "lower bound" $\exists c, \text{ and } n_0, \exists |f(n)| \ge c|g(n)| \forall n \ge n_0$ e. g. $f(n) = 3n^2 + 2 = \Omega(n^2) \text{ or } \Omega(n)$
- $\underline{\text{Def}}$: $f(n) = \Theta(g(n))$ $\exists c_1, c_2, \text{ and } n_0, \exists c_1 | g(n) | \le |f(n)| \le c_2 |g(n)| \forall n \ge n_0$ e. g. $f(n) = 3n^2 + 2 = \Theta(n^2)$
- <u>Def</u> : $f(n) \sim o(g(n))$ $\lim_{n \to \infty} \frac{f(n)}{g(n)} \to 1$ e.g. $f(n) = 3n^2 + n = o(3n^2)$

2 -6

Problem size

| | 10 | 10 ² | 10 ³ | 104 |
|---------------------|----------------------|----------------------|--------------------|---------------------|
| log ₂ n | 3.3 | 6.6 | 10 | 13.3 |
| n | 10 | 10 ² | 10 ³ | 104 |
| nlog ₂ n | 0.33x10 ² | 0.7x10 ³ | 104 | 1.3x10 ⁵ |
| n² | 10 ² | 104 | 10 ⁶ | 10 ⁸ |
| 2 ⁿ | 1024 | 1.3x10 ³⁰ | >10 ¹⁰⁰ | >10 ¹⁰⁰ |
| n! | 3x10 ⁶ | >10 ¹⁰⁰ | >10 ¹⁰⁰ | >10 ¹⁰⁰ |

Common computing time functions

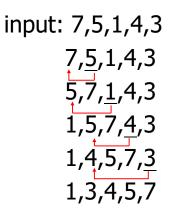
- $O(1) < O(\log n) < O(n) < O(n \log n) < O(n^2) < O(n^3) < O(2^n) < O(n!) < O(n^n)$
 - Exponential algorithm: O(2ⁿ)
 - <u>Polynomial algorithm:</u> e.g. O(n²), O(nlogn)
- Algorithm A : O(n³), Algorithm B : O(n)
 - Should Algorithm B run faster than A?
 NO !
 - It is true only when n is large enough!

Time Complexity Functions

Analysis of algorithms

- Best case: easiest
- Worst case
- Average case: hardest

Straight insertion sort



 $\begin{array}{l} \mbox{Algorithm 2.1 Straight Insertion Sort} \\ \hline \mbox{Input: } x_1, x_2, \dots, x_n \\ \hline \mbox{Output: The sorted sequence of } x_1, x_2, \dots, x_n \\ \hline \mbox{For } j := 2 \ to n \ do \\ \hline \mbox{Begin} \\ i := j - 1 \\ x := x_j \\ \hline \mbox{While } x < x_i \ and \ i > 0 \ do \\ \hline \mbox{Begin} \\ x_{i+1} := x_i \\ i := i - 1 \\ \hline \mbox{End} \\ x_{i+1} := x \\ \hline \mbox{End} \end{array}$

Inversion table

- $(a_1, a_2, ..., a_n)$: a permutation of $\{1, 2, ..., n\}$
- $(d_1, d_2, ..., d_n)$: the <u>inversion table</u> of $(a_1, a_2, ..., a_n)$
- d_j: the number of elements to the left of j that are greater than j
- e.g. permutation (7 5 1 4 3 2 6) inversion table 2 4 3 2 1 1 0
- e.g. permutation (7 6 5 4 3 2 1) inversion table 6 5 4 3 2 1 0

2 -9

Analysis of # of movements

M: # of data movements in straight insertion sort

temporary

e.g. d₃=2

$$M = \sum_{i=1}^{n-1} (2 + d_i)$$

2 -13

Analysis by inversion table

best case: already sorted
 d_i = 0 for 1 ≤ i ≤ n
 ⇒M = 2(n - 1) = O(n)

 worst case: reversely sorted
 d₁ = n - 1

2 -14

• average case:

x_i is being inserted into the sorted sequence

x₁ x₂ ... x _{j-1}

- the probability that x_i is the largest: 1/j
 - takes 2 data movements
- the probability that x_j is the second largest : 1/j
 - takes 3 data movements



• *#* of movements for inserting x_i:

$$\frac{2}{j} + \frac{3}{j} + \dots + \frac{j+1}{j} = \frac{j+3}{2}$$
$$M = \sum_{j=2}^{n} \frac{j+3}{2} = \frac{(n+8)(n-1)}{4} = O(n^2)$$

Analysis of *#* of exchanges

- <u>Method 1 (straightforward)</u>
- x_j is being inserted into the sorted sequence
 x₁ x₂ x_{i-1}

 $M = \sum_{i=1}^{n-1} (2+d_i) = 2(n-1) + \frac{n(n-1)}{2} = O(n^2)$

- If x_j is the kth $(1 \le k \le j)$ largest, it takes (k-1) exchanges.
- ∎ e.g. 1 5 7↔4

 $d_2 = n - 2$

 $d_{i} = n - i$

 $d_{n} = 0$

- 1 4 5 7
- # of exchanges required for x_i to be inserted:

$$\frac{0}{j} + \frac{1}{j} + \dots + \frac{j-1}{j} = \frac{j-1}{2}$$

• *#* of exchanges for sorting:

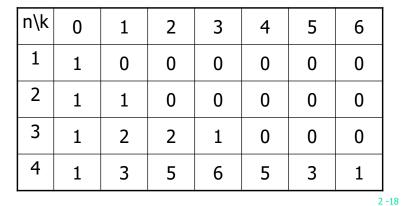
$$\sum_{j=2}^{n} \frac{j-1}{2}$$

= $\sum_{j=2}^{n} \frac{j}{2} - \sum_{j=2}^{n} \frac{1}{2}$
= $\frac{1}{2} \cdot \frac{(n-1)(n+2)}{2} - \frac{n-1}{2}$
= $\frac{n(n-1)}{4}$

2 -17

Method 2: with inversion table and generating function

 $I_n(k)$: # of permutations in *n* nmbers which have exactly *k* inversions



| • Assume we have $I_3(k)$, $0 \le k$ | \leq 3. We wi | |
|---------------------------------------|-----------------|--|
| calculate $I_4(k)$. | | |

| (1) a ₁ | $a_2 a_3 a_4 $ (2 | 2) a ₁ a ₂ a ₃ a ₄ ↑ |
|--------------------|--|---|
| | largest | second largest |
| | G ₃ (Z) | $ZG_3(Z)$ |
| (3) a ₁ | a ₂ a ₃ a ₄ (| 4) a ₁ a ₂ a ₃ a ₄ |
| | \uparrow | \uparrow |
| | third larges | |
| | $Z^2G_3(Z)$ | $Z^3G_3(Z)$ |

| case | I ₄ (0) | I ₄ (1) | I ₄ (2) | I ₄ (3) | I ₄ (4) | I ₄ (5) | I ₄ (6) |
|------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| 1 | I ₃ (0) | I ₃ (1) | I ₃ (2) | I ₃ (3) | | | |
| 2 | | I ₃ (0) | I ₃ (1) | I ₃ (2) | I ₃ (3) | | |
| 3 | | | I ₃ (0) | I ₃ (1) | I ₃ (2) | I ₃ (3) | |
| 4 | | | | I ₃ (0) | I ₃ (1) | I ₃ (2) | I ₃ (3) |

| case | I ₄ (0) | I ₄ (1) | I ₄ (2) | I ₄ (3) | I ₄ (4) | I ₄ (5) | I ₄ (6) |
|-------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| 1 | 1 | 2 | 2 | 1 | | | |
| 2 | | 1 | 2 | 2 | 1 | | |
| 3 | | | 1 | 2 | 2 | 1 | |
| 4 | | | | 1 | 2 | 2 | 1 |
| total | 1 | 3 | 5 | 6 | 5 | 3 | 1 |

• generating function for
$$I_n(k)$$

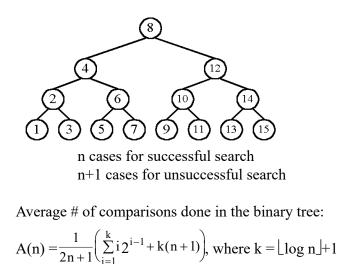
 $G_n(Z) = \sum_{k=0}^{m} I_n(k)Z^k$
• for n = 4
 $G_4(Z) = (1 + 3Z + 5Z^2 + 6Z^3 + 5Z^4 + 3Z^5 + Z^6)$
 $= (1 + Z + Z^2 + Z^3)G_3(Z)$
• in general,
 $G_n(Z) = (1 + Z + Z^2 + \dots + Z^{n-1})G_{n-1}(Z)$

2 -21

$$P_{n}(k): \text{ probability that a given permutation} \\ \text{of } n \text{ numbers has } k \text{ inversions} \\ \text{e. generating function for } P_{n}(k): \\ g_{n}(Z) = \sum_{k=0}^{m} P_{n}(k) Z^{k} = \sum_{k=0}^{m} \frac{ln(k)}{n!} Z^{k} \\ = \frac{1}{n!} G_{n}(Z) \\ = \frac{1+Z+Z^{2}+\dots+Z^{n-1}}{n} \cdot \frac{1+Z+Z^{2}+Z^{n-2}}{n-1} \cdots \frac{1+Z}{2} \cdot 1 \\ \sum_{k=0}^{m} k P_{n}(k) = g_{n}'(1) \\ = \frac{1+2+\dots+(n-1)}{n} + \frac{1+2+\dots+(n-2)}{n-1} + \dots + \frac{1}{2} + 0 \\ = \frac{n-1}{2} + \frac{n-2}{2} + \dots + \frac{1}{2} + 0 \\ = \frac{1}{4}n(n-1) \end{aligned}$$

Binary search

sorted sequence : (search 9) 4 5 7 9 10 12 1 15 step 1 step 2 ↑ step 3 <u>best case</u>: 1 step = O(1) • worst case: $(\lfloor \log_2 n \rfloor + 1)$ steps = O(log n) average case: O(log n) steps



Worst case of quicksort

- Worst case: O(n²)
- In each round, the number used to split is either the smallest or the largest.

•
$$n + (n-1) + \dots + 1 = \frac{n(n+1)}{2} = O(n^2)$$

Average case of quicksort

<u>Average case</u>: O(n log n)

| s n-s |
|--|
| include the splitter |
| T(n) = Avg(T(s) + T(n-s)) + cn, c is a constant |
| l≤s≤n |
| $= \frac{1}{n} \sum_{s=1}^{n} (T(s) + T(n-s)) + cn$ |
| $= \frac{1}{n} (T(1)+T(n-1)+T(2)+T(n-2)+\dots+T(n)+T(0))+cn, T(0)=0$ |
| $= \frac{1}{n}(2T(1)+2T(2)+\dots+2T(n-1)+T(n))+cn$ |

2 -29

 $(n-1)T(n) = 2T(1)+2T(2)+\dots+2T(n-1) + cn^2\dots(1)$ (n-2)T(n-1)=2T(1)+2T(2)+\dots+2T(n-2)+c(n-1)^2\dots(2)

(1) - (2)

(n-1)T(n) - (n-2)T(n-1) = 2T(n-1)+c(2n-1)(n-1)T(n) - nT(n-1) = c(2n-1)

 $\frac{T(n)}{n} = \frac{T(n-1)}{n-1} + c(\frac{1}{n} + \frac{1}{n-1})$ = $c(\frac{1}{n} + \frac{1}{n-1}) + c(\frac{1}{n-1} + \frac{1}{n-2}) + \dots + c(\frac{1}{2} + 1) + T(1), T(1) = 0$ = $c(\frac{1}{n} + \frac{1}{n-1} + \dots + \frac{1}{2}) + c(\frac{1}{n-1} + \frac{1}{n-2} + \dots + 1)$ Harmonic number[Knuth 1986] $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ $= \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \varepsilon$, where $0 < \varepsilon < \frac{1}{252n^6}$ $\gamma = 0.5772156649 \cdots$. $H_n = O(\log n)$

$$\frac{T(n)}{n} = c(H_n-1) + cH_{n-1}$$
$$= c(2H_n-\frac{1}{n}-1)$$
$$\Rightarrow T(n) = 2 c n H_n - c(n+1)$$
$$= O(n \log n)$$

2-D ranking finding

- **Def**: Let $A = (x_1, y_1)$, $B = (x_2, y_2)$. B dominates A iff $x_2 > x_1$ and $y_2 > y_1$
- <u>Def</u>: Given a set S of n points, the <u>rank</u> of a point x is the number of points dominated by x.

 $\begin{array}{c|c} B & \bullet D \\ A \bullet & \bullet C \\ \bullet E \end{array}$

$$rank(A) = 0 rank(B) = 1 rank(C) = 1$$

rank(D) = 3 rank(E) = 0

2 -33

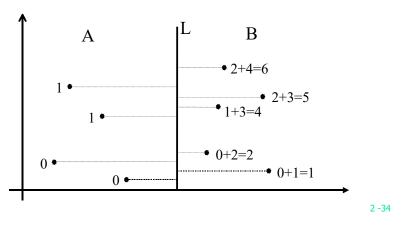
Divide-and-conquer 2-D ranking finding

- Step 1: Split the points along the median line L into A and B.
- Step 2: Find ranks of points in A and ranks of points in B, recursively.
- Step 3: Sort points in A and B according to their y-values. Update the ranks of points in B.

Straightforward algorithm:

compare all pairs of points : $O(n^2)$

More efficient algorithm (<u>divide-and-conquer</u>)



 time complexity : step 1 : O(n) (finding median) step 3 : O(n log n) (sorting)

• total time complexity :

$$T(n) \le 2T(\frac{n}{2}) + c_1 n \log n + c_2 n, \qquad c_1, c_2 \text{ are constants}$$

$$\le 2T(\frac{n}{2}) + c n \log n , \qquad \text{let } c = c_1 + c_2$$

$$\le 4T(\frac{n}{4}) + c n \log \frac{n}{2} + c n \log n$$

$$\le nT(1) + c(n \log n + n \log \frac{n}{2} + n \log \frac{n}{4} + \dots + n \log 2)$$

$$= nT(1) + \frac{cn \log n(\log n + \log 2)}{2}$$

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

Lower bound

- <u>Def</u>: A <u>lower bound</u> of a <u>problem</u> is the least time complexity required for any algorithm which can be used to solve this problem.
- ☆ worst case lower bound
 ☆ average case lower bound
- The lower bound for a problem is <u>not unique</u>.
 - e.g. Ω(1), Ω(n), Ω(n log n) are all lower bounds for sorting.
 - $(\Omega(1), \Omega(n) \text{ are trivial})$

- At present, if the <u>highest</u> lower bound of a problem is Ω(n log n) and the time complexity of the <u>best</u> algorithm is O(n²).
 - We may try to find a higher lower bound.
 - We may try to find a better algorithm.
 - Both of the lower bound and the algorithm may be improved.
- If the present lower bound is Ω(n log n) and there is an algorithm with time complexity O(n log n), then the algorithm is <u>optimal</u>.

The worst case lower bound of sorting

6 permutations for 3 data elements

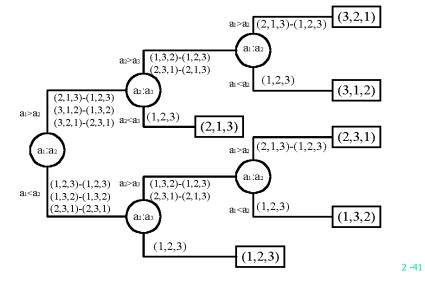
| a_1 | a ₂ | a ₃ |
|-------|----------------|----------------|
| 1 | 2 | 3 |
| 1 | 3 | 2 |
| 2 | 1 | 3 |
| 2 | 3 | 1 |
| 3 | 1 | 2 |
| 3 | 2 | 1 |

Straight insertion sort:

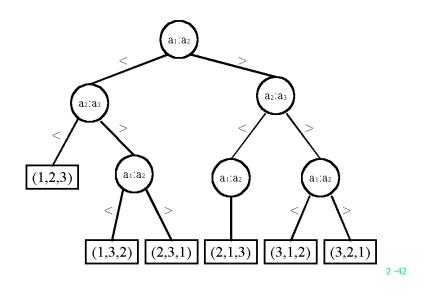
input data: (2, 3, 1)
(1) a₁:a₂
(2) a₂:a₃, a₂↔a₃
(3) a₁:a₂, a₁↔a₂
input data: (2, 1, 3)
(1)a₁:a₂, a₁↔a₂
(2)a₂:a₃

2 - 37

Decision tree for straight insertion sort



Decision tree for bubble sort



Lower bound of sorting

- Every sorting algorithm (based on comparisons) corresponds to a <u>decision tree</u>.
- To find the lower bound, we have to find the <u>depth</u> of a binary tree with the smallest depth.
- n! distinct permutations
 <u>n! leaf nodes</u> in the binary decision tree.
- balanced tree has the smallest depth:

$\lceil \log(n!) \rceil = \Omega(n \log n)$

lower bound for sorting: $\Omega(n \log n)$

(See the next page.)

Method 1:

$$log(n!) = log(n(n-1)\cdots 1)$$

= log2 + log3 +...+ log n
> $\int_{1}^{n} log x dx$
= log $e \int_{1}^{n} ln x dx$
= log $e[x ln x - x]_{1}^{n}$
= log $e(n ln n - n + 1)$
= n log n - n log $e + 1.44$
 \geq n log n - 1.44n
= $\Omega(n \log n)$

Method 2:

• Stirling approximation:

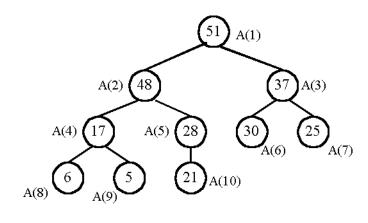
$$n! \approx S_n = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$
$$\log n! \approx \log \sqrt{2\pi} + \frac{1}{2}\log n + n\log \frac{n}{e} \approx n\log n = \Omega(n\log n)$$

| n | n! | S _n |
|-----|-------------------------|-------------------------|
| 1 | 1 | 0.922 |
| 2 | 2 | 1.919 |
| 3 | 6 | 5.825 |
| 4 | 24 | 23.447 |
| 5 | 120 | 118.02 |
| 6 | 720 | 707.39 |
| 10 | 3,628,800 | 3,598,600 |
| 20 | 2.433x10 ¹⁸ | 2.423x10 ¹⁸ |
| 100 | 9.333x10 ¹⁵⁷ | 9.328x10 ¹⁵⁷ |
| | | |

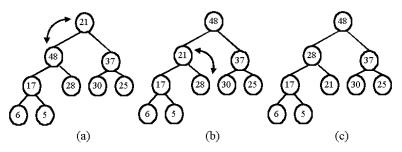
2 -45

Heapsort—An optimal sorting algorithm

• A heap : parent \geq son



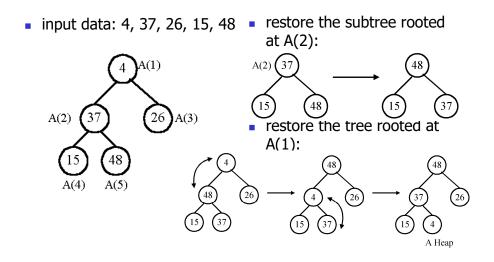
• output the maximum and restore:

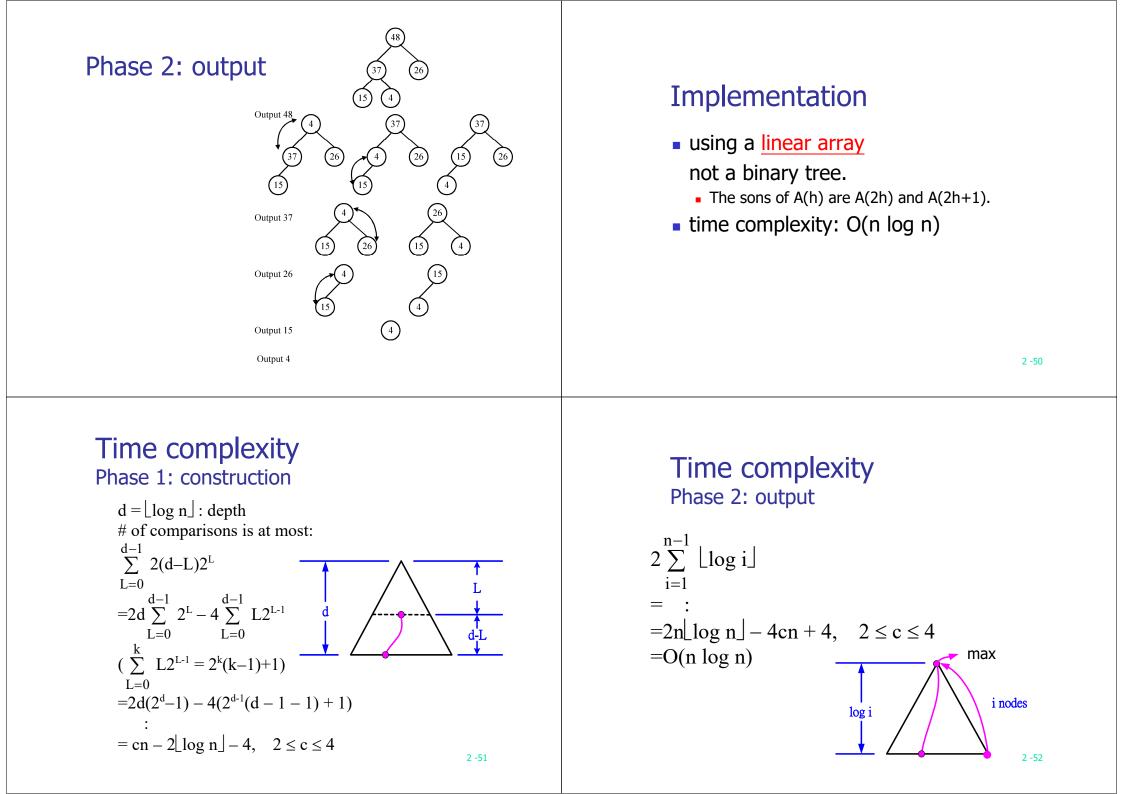


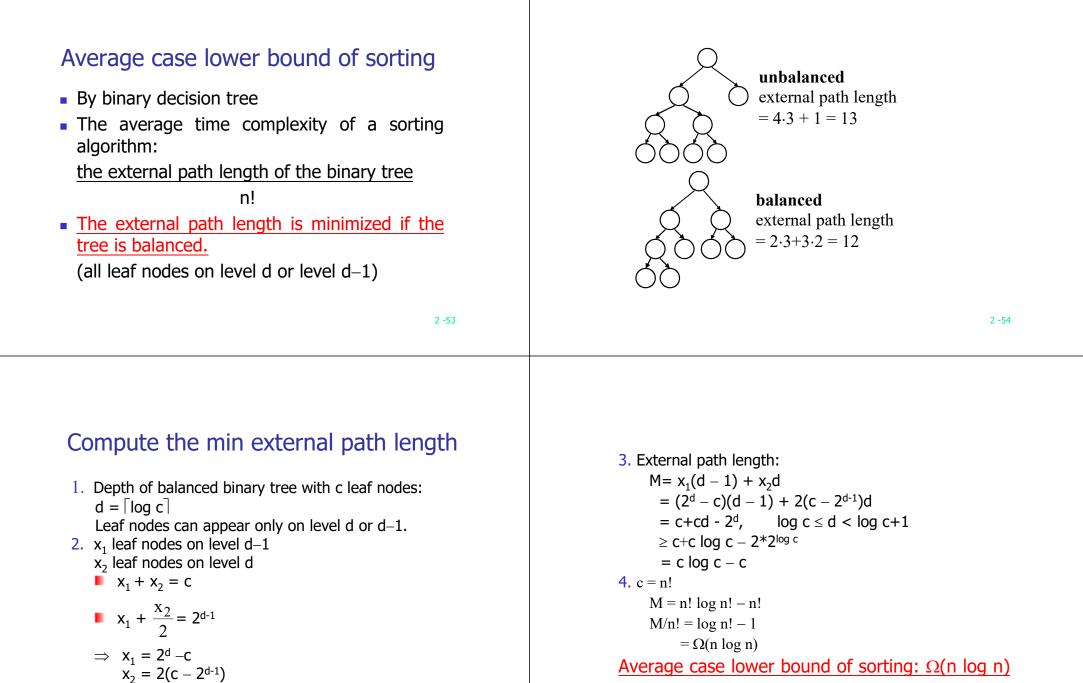
Heapsort:

- Phase 1: Construction
- Phase 2: Output

Phase 1: construction







Average case lower bound of sorting: $\Omega(n \log n)$

Improving a lower bound through oracles Quicksort & Heapsort Problem P: merge two sorted sequences A Quicksort is optimal in the average case. and B with lengths m and n. (O(n log n) in average) Conventional 2-way merging: (i)worst case time complexity of heapsort is 3 5 6 $O(n \log n)$ 1 4 (ii)average case lower bound: $\Omega(n \log n)$ Complexity: at most m+n-1 comparisons average case time complexity of heapsort is $O(n \log n)$ Heapsort is optimal in the average case. 2 -57 2 -58 When m = n $\log\binom{m+n}{n} = \log\frac{(2m)!}{(m!)^2} = \log((2m)!) - 2\log m!$ (1) Binary decision tree: There are $\binom{m+n}{n}$ ways ! Using Stirling approximation $n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$ $\binom{m+n}{n}$ leaf nodes in the decision tree. $\log\binom{m+n}{n} \approx (\log\sqrt{2\pi} + \log\sqrt{2m} + 2m\log\frac{2m}{e}) \Rightarrow$ The lower bound for merging: $\lceil \log \binom{m+n}{n} \rceil \leq m + n - 1$ (conventional merging) $-2\left(\log\sqrt{2\pi} + \log\sqrt{m} + m\log\frac{m}{2}\right)$ $\approx 2m - \frac{1}{2}\log m + O(1) < 2m - 1$ Optimal algorithm: conventional merging needs 2m-1 comparisons

(2) Oracle:

- The oracle tries its best to cause the algorithm to work as <u>hard</u> as it might. (to give a very hard data set)
- Two sorted sequences:
 - A: a₁ < a₂ < ... < a_m

- The very hard case:
 - $a_1 < b_1 < a_2 < b_2 < \dots < a_m < b_m$

We must compare:

 a₁: b₁
 b₁: a₂
 a₂: b₂
 :
 b_{m-1}: a_{m-1}
 a_m: b_m

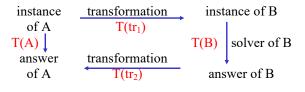
 Otherwise, we may get a wrother set a wrother se

- Otherwise, we may get a wrong result for some input data.
 e.g. If b₁ and a₂ are not compared, we can not distinguish a₁ < b₁ < a₂ < b₂ < ... < a_m < b_m and a₁ < a₂ < b₁ < b₂ < ... < a_m < b_m
 Thus, at least 2m-1 comparisons are required.
- The conventional merging algorithm is optimal for m = n.

2 -61

Finding lower bound by problem transformation

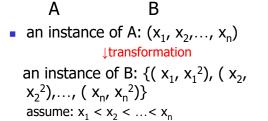
- Problem A <u>reduces to</u> problem B (A∝B)
 - iff A can be solved by using any algorithm which solves B.
 - If $A \propto B$, B is more difficult.

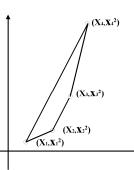


• Note: $T(tr_1) + T(tr_2) < T(B)$ $T(A) \le T(tr_1) + T(tr_2) + T(B) \sim O(T(B))$

The lower bound of the convex hull problem

sorting ∞ convex hull





- If the convex hull problem can be solved, we can also solve the sorting problem.
 - The lower bound of sorting: $\Omega(n \log n)$
- The lower bound of the convex hull problem: $\Omega(n \log n)$

The lower bound of the Euclidean minimal spanning tree (MST) problem

- sorting ∝ Euclidean MST В
 - Α
- an instance of A: (x_1, x_2, \dots, x_n) I transformation
 - an instance of B: {(x_1 , 0), (x_2 , 0),..., (x_n , 0)}

2 -66

- Assume $x_1 < x_2 < x_3 < ... < x_n$
- \Leftrightarrow there is an edge between (x_i, 0) and (x_{i+1}, 0) in the MST, where $1 \le i \le n-1$

- If the Euclidean MST problem can be solved, we can also solve the sorting problem.
 - The lower bound of sorting: $\Omega(n \log n)$
- The lower bound of the Euclidean MST problem: $\Omega(n \log n)$

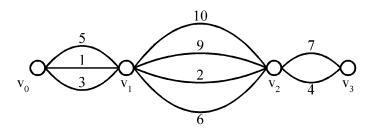
Chapter 3 The Greedy Method A simple example Problem: Pick k numbers out of n numbers such that the <u>sum</u> of these k numbers is the <u>largest</u>. Algorithm: FOR i = 1 to k pick out the <u>largest</u> number and delete this number from the input. ENDFOR

The greedy method

- Suppose that a problem can be solved by a sequence of decisions. The greedy method has that <u>each decision is locally optimal</u>. <u>These locally optimal solutions will finally add</u> <u>up to a globally optimal solution</u>.
- <戰國策.秦策>范睢對秦昭襄王說:「王不如 遠交而近攻,<u>得寸</u>,王之寸;<u>得尺</u>,亦王之尺 也。」
- Only a few optimization problems can be solved by the greedy method.

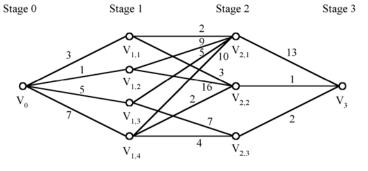
Shortest paths on a special graph

- <u>Problem</u>: Find a <u>shortest path</u> from v_0 to v_3 .
- The greedy method can solve this problem.
- The shortest path: 1 + 2 + 4 = 7.



Shortest paths on a multi-stage graph

• <u>Problem</u>: Find a shortest path from v_0 to v_3 in the <u>multi-stage graph</u>.



- Greedy method: $v_0v_{1,2}v_{2,1}v_3 = 23$
- Optimal: $v_0 v_{1,1} v_{2,2} v_3 = 7$
- The greedy method does not work.

3 -5

Solution of the above problem

 d_{min}(i,j): minimum distance between i and j.

$$d_{\min}(v_0, v_3) = \min \begin{cases} 3 + d_{\min}(v_{1,1}, v_3) \\ 1 + d_{\min}(v_{1,2}, v_3) \\ 5 + d_{\min}(v_{1,3}, v_3) \\ 7 + d_{\min}(v_{1,4}, v_3) \end{cases}$$

 This problem can be solved by the dynamic programming method.

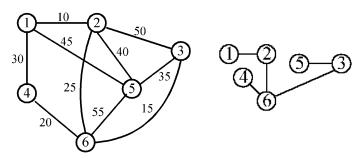
3 -6

Minimum spanning trees (MST)

- It may be defined on <u>Euclidean space</u> points or on a <u>graph</u>.
- G = (V, E): weighted connected undirected graph
- Spanning tree : $S = (V, T), T \subseteq E,$ undirected tree
- Minimum spanning tree(MST) : a spanning tree with the smallest total weight.

An example of MST

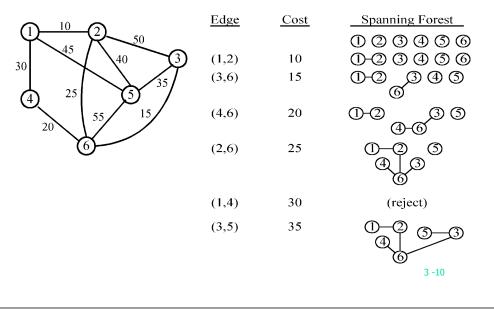
 A graph and one of its minimum costs spanning tree



Kruskal's algorithm for finding MST

Step 1: Sort all edges into nondecreasing order.
Step 2: Add the next smallest weight edge to the forest if it will not cause a cycle.
Step 3: Stop if n-1 edges. Otherwise, go to Step2.

An example of Kruskal's algorithm



The details for constructing MST

- How do we check if a cycle is formed when a new edge is added?
 - By the <u>SET and UNION</u> method.
- Each tree in the spanning forest is represented by a <u>SET</u>.
 - If (u, v) ∈ E and u, v are in the same set, then the addition of (u, v) will form a cycle.
 - If $(u, v) \in E$ and $u \in S_1$, $v \in S_2$, then perform <u>UNION</u> of S_1 and S_2 .

Time complexity

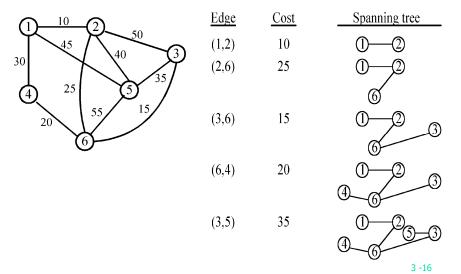
- Time complexity: O(|E| log|E|)
 - Step 1: O(|E| log|E|)
 - Step 2 & Step 3: O(| *E* | α (| *E* |, |*V* |))
 Where α is the inverse of Ackermann's function.

Ackermann's function Inverse of Ackermann's function • $\alpha(m, n) = \min\{i \ge 1 | A(i, \lfloor m/n \rfloor) > \log_2 n\}$ for $j \ge 1$ $A(1, j) = 2^{j}$ Practically, $A(3,4) > \log_2 n$ A(i,1) = A(i-1,2)for $i \ge 2$ $\Rightarrow \alpha(m, n) \leq 3$ A(i, j) = A(i-1, A(i, j-1)) for $i, j \ge 2$ $\Rightarrow \alpha(m, n)$ is almost a constant. $\Rightarrow A(p, q+1) > A(p, q), A(p+1, q) > A(p, q)$ 3 -13 3 -14

Prim's algorithm for finding MST

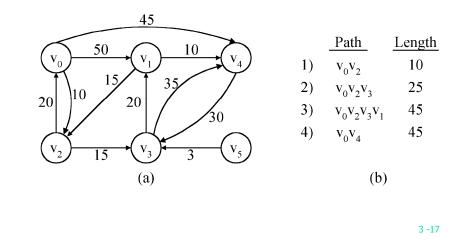
Step 1: x ∈ V, Let A = {x}, B = V - {x}.Step 2: Select (u, v) ∈ E, u ∈ A, v ∈ Bsuch that (u, v) has the smallest weightbetween A and B.Step 3: Put (u, v) in the tree. A = A ∪ {v},B = B - {v}Step 4: If B = Ø, stop; otherwise, go to
Step 2.

An example for Prim's algorithm

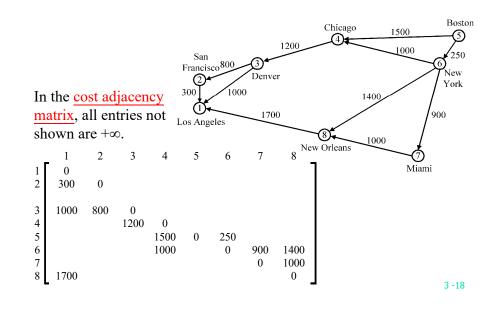


The single-source shortest path problem

shortest paths from v₀ to <u>all destinations</u>



Dijkstra's algorithm



Bostor Chicago 1500 (5) 250 Sar Francisco⁸⁰⁰ Neu York 300 Los Angeles New Orleans Vertex Miam Iteration S Selected (1) (2) (3) (4) (5) (6) (7) (8) Initial 5 1 6 1500 0 250 +00 +00 +00 +00 +00 2 5,6 7 250 1150 1650 1250 0 $+\infty$ +00 +00 3 5,6,7 4 +00 $+\infty$ 1250 250 1150 1650 +00 - 0 5,6,7,4 4 8 2450 1250 0 250 1150 1650 +00 $+\infty$ 5 5,6,7,4,8 3 3350 +∞ 2450 1250 0 250 1150 1650 6 5,6,7,4,8,3 2 3350 3250 2450 1250 0 250 1150 1650 5,6,7,4,8,3,2 3350 3250 2450 1250 0 250 1150 1650

• <u>Time complexity : $O(n^2)$ </u>, n = |V|.

3 -19

The longest path problem

- Can we use Dijkstra's algorithm to find the <u>longest path</u> from a starting vertex to an ending vertex in an <u>acyclic directed graph</u>?
- There are 3 possible ways to apply Dijkstra's algorithm:
 - Directly use "<u>max</u>" operations instead of "<u>min</u>" operations.
 - Convert all <u>positive</u> weights to be <u>negative</u>. Then find the shortest path.
 - Give a very large positive number M. If the weight of an edge is w, now <u>M-w</u> is used to replace w. Then find the shortest path.
- All these 3 possible ways would <u>not work</u>!

CPM for the longest path problem

 The longest path(critical path) problem can be solved by the critical path method(CPM) :

<u>Step 1</u>:Find a topological ordering.

Step 2: Find the critical path.

(see [Horiwitz 1995].)

 [[Horowitz 1995] E. Howowitz, S. Sahni and D. Metha, *Fundamentals of Data Structures in C++*, Computer Science Press, New York, 1995

3 -21

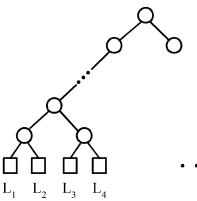
The 2-way merging problem

- # of comparisons required for the linear 2way merge algorithm is m₁+ m₂ -1 where m₁ and m₂ are the lengths of the two sorted lists respectively.
 - 2-way merging example
 - 2 3 5 6
 - 1 4 7 8
- The problem: There are n sorted lists, each of length m_i. What is the <u>optimal sequence of</u> <u>merging process</u> to merge these n lists into one sorted list ?

3 -22

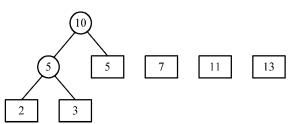
Extended binary trees

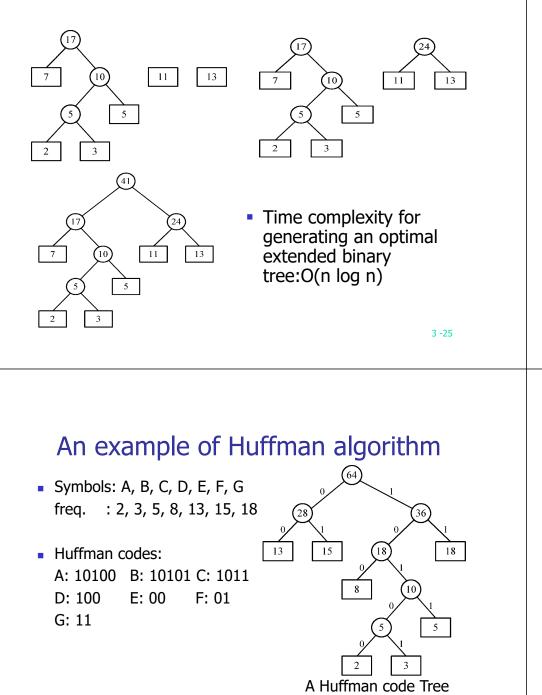
An extended binary tree representing a 2-way merge



An example of 2-way merging

Example: 6 sorted lists with lengths 2, 3, 5, 7, 11 and 13.

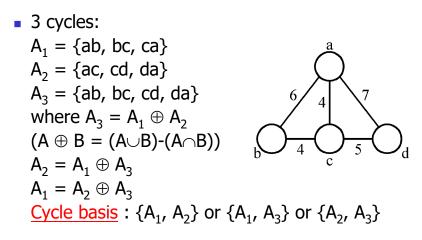




- In telecommunication, how do we represent a set of messages, each with an access frequency, by a sequence of 0's and 1's?
- To minimize the transmission and decoding costs, we may use short strings to represent more frequently used messages.
- This problem can by solved by using an extended binary tree which is used in the <u>2-</u> way merging problem.

3 -26

The minimal cycle basis problem



Huffman codes

- Def : A cycle basis of a graph is a set of cycles such that every cycle in the graph can be generated by applying ⊕ on some cycles of this basis.
- <u>Minimal cycle basis</u> : smallest total weight of all edges in this cycle.
- e.g. {A₁, A₂}

3 -29

Detailed steps for the minimal cycle basis problem

• Step 1 :

A cycle basis corresponds to the <u>fundamental set of</u> <u>cycles</u> with respect to a spanning tree.

a graph a spanning tree a fundamental set of cycles # of cycles in a cycle basis : e_{2} e_{3} e_{4} e_{5} e_{5} e_{7} e_{6} e_{7} e_{6} e_{7} e_{7}

- Algorithm for finding a minimal cycle basis:
 - <u>Step 1</u>: Determine the size of the minimal cycle basis, demoted as k.
 - <u>Step 2</u>: Find all of the cycles. Sort all cycles(by weight).
 - <u>Step 3</u>: Add cycles to the cycle basis one by one. Check if the added cycle is a <u>linear combination</u> of some cycles already existing in the basis. If it is, delete this cycle.

<u>Step 4</u>: Stop if the cycle basis has k cycles.

3 -30

Step 2:

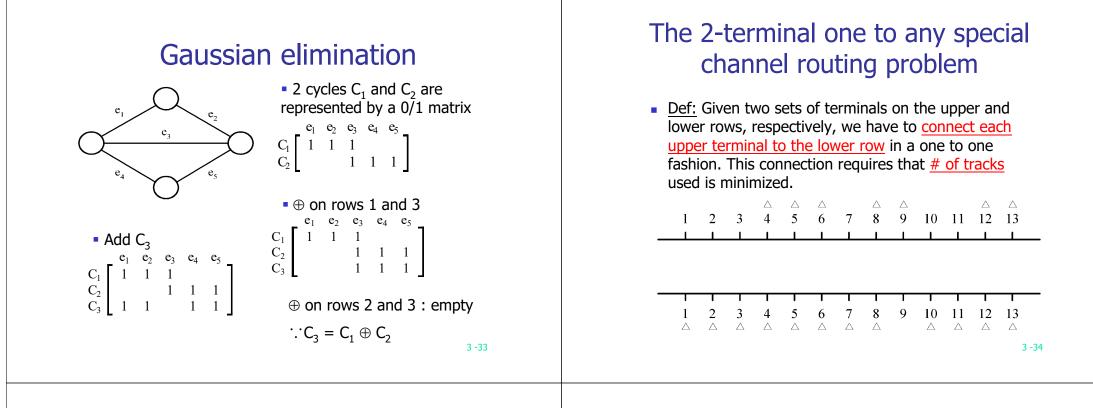
How to find all cycles in a graph? [Reingold, Nievergelt and Deo 1977] How many cycles in a graph in the worst case?

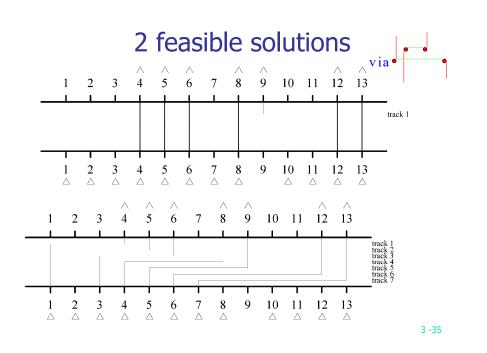
In a complete digraph of n vertices and n(n-1) edges:

$$\sum_{i=2}^{n} C_{i}^{n} (i-1)! > (n-1)!$$

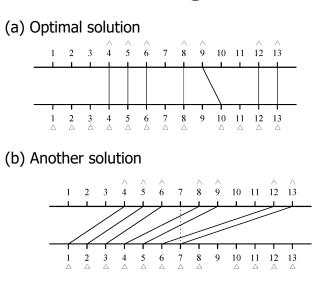
• Step 3:

How to check if a cycle is a linear combination of some cycles? Using Gaussian elimination.

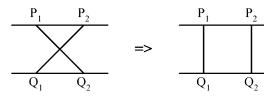




Redrawing solutions



- At each point, the <u>local density</u> of the solution is # of lines the vertical line intersects.
- The problem: to minimize the <u>density</u>. The density is a lower bound of # of <u>tracks</u>.
- Upper row terminals: P₁, P₂,..., P_n from left to right
- Lower row terminals: Q₁,Q₂,..., Q_m from left to right m > n.
- It would never have a crossing connection:



- Suppose that we have a method to determine the minimum density, d, of a problem instance.
- The greedy algorithm:
- <u>Step 1</u> : P_1 is connected Q_1 .
- <u>Step 2</u> : After P_i is connected to Q_j, we check whether P_{i+1} can be connected to Q_{j+1}. If the density is increased to d+1, try to connect P_{i+1} to Q_{j+2}.

<u>Step 3</u> : Repeat Step2 until all P_i 's are connected.

3 -38

The knapsack problem

n objects, each with a weight w_i > 0

 a profit p_i > 0
 capacity of knapsack: M

 $\begin{array}{ll} & \sum\limits_{1\leq i\leq n} p_i x_i \\ \text{Maximize} & \sum\limits_{1\leq i\leq n} w_i x_i \leq M \\ \text{Subject to} & \sum\limits_{1\leq i\leq n} w_i x_i \leq M \\ & 0\leq x_i\leq 1,\ 1\leq i\leq n \end{array}$

The knapsack algorithm

The greedy algorithm:

Step 1: Sort p_i/w_i into <u>nonincreasing</u> order. Step 2: Put the objects into the knapsack according to the sorted sequence as possible as we can.

e. g.

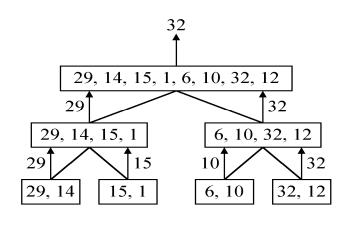
n = 3, M = 20, $(p_1, p_2, p_3) = (25, 24, 15)$ $(w_1, w_2, w_3) = (18, 15, 10)$ Sol: $p_1/w_1 = 25/18 = 1.39$ $p_2/w_2 = 24/15 = 1.6$ $p_3/w_3 = 15/10 = 1.5$ Optimal solution: $x_1 = 0, x_2 = 1, x_3 = 1/2$

Chapter 4

The Divide-and-Conquer Strategy

A simple example

finding the maximum of a set S of n numbers



Time complexity

 Time complexity: $T(n) = \begin{cases} 2T(n/2)+1, n>2\\ 1, n\leq 2 \end{cases}$
 Calculation of T(n): Assume n = 2^k, T(n) = 2T(n/2)+1 = 2(2T(n/4)+1)+1 = 4T(n/4)+2+1 : = 2^{k-1}T(2)+2^{k-2}+...+4+2+1 = 2^{k-1}+2^{k-2}+...+4+2+1 = 2^{k-1}+2^{k-2}+...+4+2+1 = 2^k-1 = n-1

諫逐客書—李斯

 文選自 < 史記. 李斯列傳>, 是李斯上呈 秦王政的一篇奏疏。

 「惠王用張儀之計,拔三川之地,西并 巴、蜀,北收上郡,南取漢中,包九夷, 制鄢(一弓)、郢(一厶[×]),東據成皋之險, 割膏腴之壤,遂散六國之從(縱),使之 西面事秦,功施(一[×])到今。」
 註:秦滅六國順序:韓、趙、魏、楚、

```
燕、齊
```

4 -1

A general divide-and-conquer algorithm

- Step 1: If the problem size is small, solve this problem directly; otherwise, split the original problem into 2 sub-problems with equal sizes.
- Step 2: Recursively solve these 2 sub-problems by applying this algorithm.

Step 3: Merge the solutions of the 2 subproblems into a solution of the original problem.

4 -5

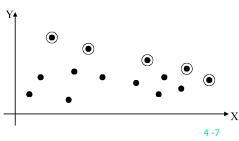
Time complexity of the general algorithm

Time complexity: T(n)={ 2T(n/2)+S(n)+M(n), n≥c b, n < c
where S(n) : time for splitting M(n) : time for merging b : a constant c : a constant
e.g. Binary search
e.g. quick sort
e.g. merge sort e.g. 2 6 5 3 7 4 8 1

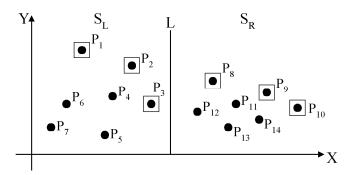
2-D maxima finding problem

- **Def**: A point (x₁, y₁) dominates (x₂, y₂) if x₁
 x₂ and y₁ > y₂. A point is called a maximum if no other point dominates it
- Straightforward method : <u>Compare every pair</u> of points.

Time complexity: O(n²)



Divide-and-conquer for maxima finding



The maximal points of $\rm S_L$ and $\rm S_R$

The algorithm:

- Input: A set S of n planar points.
- Output: The maximal points of S.
- Step 1: If S contains only one point, return it as the maximum. Otherwise, find a line L perpendicular to the X-axis which separates S into S_I and S_R , with equal sizes.
- <u>Step 2:</u> <u>Recursively</u> find the maximal points of S_L and S_R .
- <u>Step 3:</u> Find the largest y-value of S_R , denoted as y_R . Discard each of the maximal points of S_L if its y-value is less than or equal to y_R .

Time complexity: T(n)
 Step 1: O(n)
 Step 2: 2T(n/2)
 Step 3: O(n)

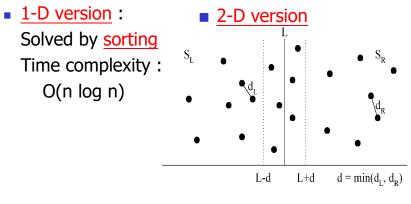
 $T(n) = \begin{cases} 2T(n/2) + O(n) + O(n) & , n > 1 \\ 1 & , n = 1 \end{cases}$

Assume $n = 2^k$ T(n) = O(n log n)

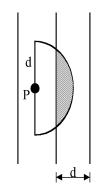
4 -10

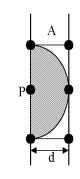
The closest pair problem

 Given a set S of n points, find a pair of points which are <u>closest</u> together.



• at most 6 points in area A:



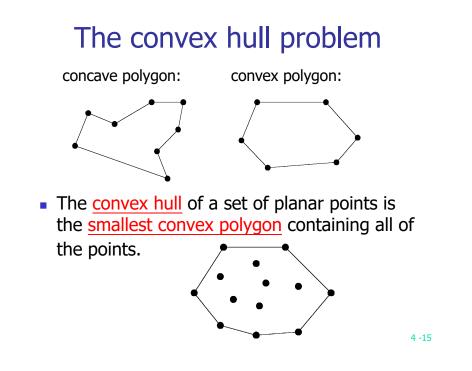


The algorithm:

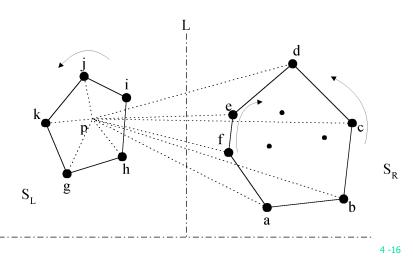
- Input: A set S of n planar points.
- <u>Output:</u> The distance between two closest points.
- <u>Step 1:</u> Sort points in S according to their y-values.
- <u>Step 2:</u> If S contains only one point, return infinity as its distance.
- Step 3: Find a median line L perpendicular to the X-axis to divide S into S_L and S_R , with equal sizes.
- <u>Step 4: Recursively</u> apply Steps 2 and 3 to solve the closest pair problems of S_L and S_R . Let $d_L(d_R)$ denote the distance between the closest pair in $S_L(S_R)$. Let $d = min(d_L, d_R)$.

- <u>Step 5:</u> For a point P in the half-slab bounded by L-d and L, let its y-value be denoted as y_P . For each such P, find all points in the halfslab bounded by L and L+d whose y-value fall within y_P +d and y_P -d. If the distance d' between P and a point in the other half-slab is less than d, let d=d'. The final value of d is the answer.
- Time complexity: O(n log n) Step 1: O(n log n) Steps 2~5: $T(n) = \begin{cases} 2T(n/2) + O(n) + O(n) & , n > 1 \\ 1 & , n = 1 \end{cases}$ $\Rightarrow T(n) = O(n log n)$

4 -14



The divide-and-conquer strategy to solve the problem:



- <u>The merging procedure:</u>
- 1. Select an <u>interior point</u> p.
- 2. There are 3 sequences of points which have increasing polar angles with respect to p.
 - (1) g, h, i, j, k
 - (2) a, b, c, d
 - (3) f, e
- 3. <u>Merge</u> these 3 sequences into 1 sequence: g, h, a, b, f, c, e, d, i, j, k.
- 4. Apply Graham scan to examine the points one by one and eliminate the points which cause reflexive angles.

(See the example on the next page.)

4 -17

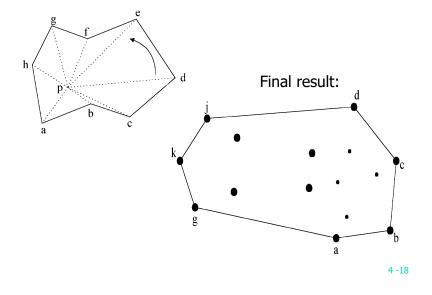
Divide-and-conquer for convex hull

- Input : A set S of planar points
- <u>Output</u>: A convex hull for S
- Step 1: If S contains no more than five points, use exhaustive searching to find the convex hull and return.
- <u>Step 2:</u> Find a median line perpendicular to the X-axis which <u>divides</u> S into S_L and S_R , with equal sizes.
- Step 3: Recursively construct convex hulls for S_L and S_R , denoted as Hull(S_L) and Hull(S_R), respectively.

- <u>Step 4</u>: Apply the merging procedure to <u>merge</u> Hull(S_L) and Hull(S_R) together to form a convex hull.
- Time complexity:

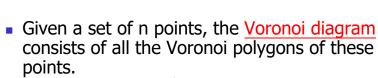
T(n) = 2T(n/2) + O(n)= O(n log n)

• e.g. points b and f need to be deleted.



The Voronoi diagram problem • e.g. The <u>Voronoi diagram</u> for three points $\frac{L_{12}}{L_{12}}$ **Definition of Voronoi diagrams Definition of Voronoi diagrams Definiti**

 $\bullet P_2 \quad R_2$



 $\mathbf{R}_1 = \mathbf{P}_1$

Each L_{ij} is the <u>perpendicular bisector</u> of line segment $\overline{P_iP_i}$. The intersection of three L_{ii} 's is

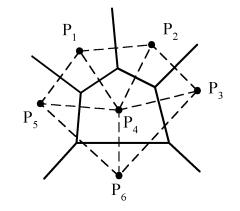
the circumcenter ($\not P_1 P_2 P_3$.

P_1 P_2 P_5 P_4 P_3 P_6

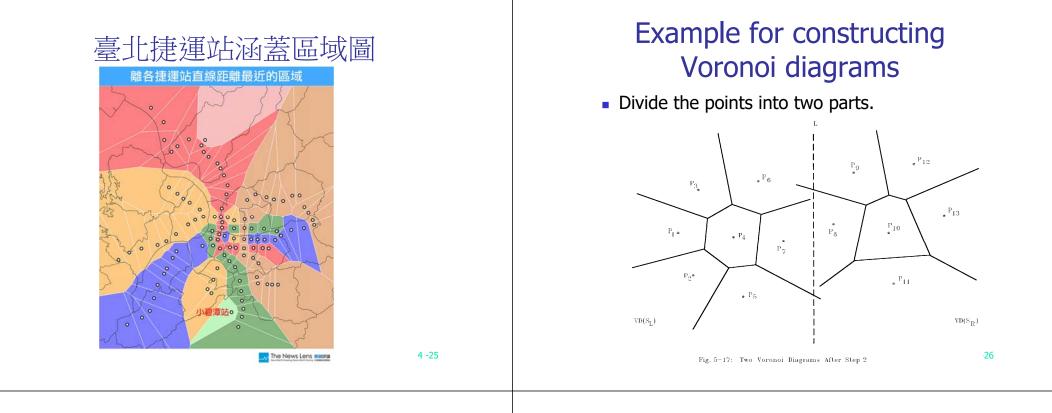
 The vertices of the Voronoi diagram are called <u>Voronoi points</u> and its segments are called <u>Voronoi edges</u>.

Delaunay triangulation

 $V(i) = \bigcap H(P_i, P_j)$

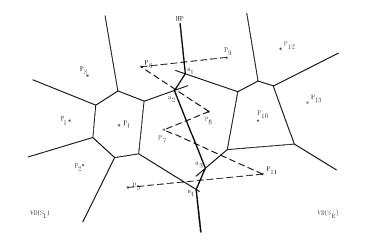


4 -21



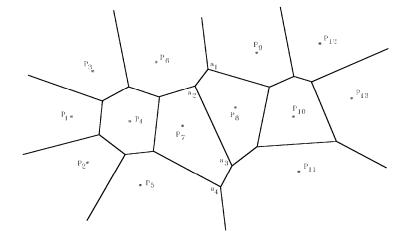
Merging two Voronoi diagrams

Merging along the <u>piecewise linear hyperplane</u>



The final Voronoi diagram

After merging



Divide-and-conquer for Voronoi diagram

<u>Input</u>: A set S of n planar points.
 <u>Output</u>: The Voronoi diagram of S.
 <u>Step 1</u>: If S contains only one point, return.
 <u>Step 2</u>: Find a median line L perpendicular to the X-axis which <u>divides</u> S into S_L and S_R, with equal sizes.

Step 3: Construct Voronoi diagrams of S_L and S_R recursively. Denote these Voronoi diagrams by VD(S_L) and VD(S_R). **Step 4:** Construct a dividing piece-wise linear hyperplane HP which is the locus of points simultaneously closest to a point in S_L and a point in S_R . Discard all segments of VD(S_L) which lie to the right of HP and all segments of VD(S_R) that lie to the left of HP. The resulting graph is the Voronoi diagram of S.

(See details on the next page.)

4 -29

Mergeing Two Voronoi Diagrams into One Voronoi Diagram

 Input: (a) S_L and S_R where S_L and S_R are divided by a perpendicular line L. (b) VD(S_L) and VD(S_R).
 Output: VD(S) where S = S_L ∩S_R
 Step 1: Find the convex hulls of S_L and S_R, denoted as Hull(S_L) and Hull(S_R), respectively. (A special algorithm for finding a convex hull in this case will by given later.) **Step 2:** Find segments $\overline{P_a P_b}$ and $\overline{P_c P_d}$ which join HULL(S_L) and HULL(S_R) into a convex hull (P_a and P_c belong to S_L and P_b and P_d belong to S_R) Assume that $\overline{P_a P_b}$ lies above $\overline{P_c P_d}$. Let x = a, y = b, SG= $\overline{P_x P_y}$ and HP = \emptyset . **Step 3:** Find the perpendicular bisector of SG.

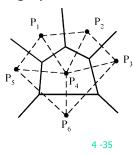
Denote it by BS. Let HP = HP \cup {BS}. If SG = $\overline{PP_{+}}$, go to Step 5; otherwise, go to Step 4.

Properties of Voronoi Diagrams Step 4: The ray from $VD(S_1)$ and $VD(S_R)$ which BS first intersects with must be a Def: Given a point P and a set S of points, perpendicular bisector of either $\overline{P_{P_{r}}}$ or $\overline{P_{P_{r}}}$ for the distance between P and S is the distance some z. If this ray is the perpendicular between P and P_i which is the nearest bisector of $\overline{P_{y}P_{z}}$, then let SG = $\overline{P_{z}P_{z}}$; otherwise, neighbor of P in S. let SG = \overline{PP} . Go to Step 3. • The HP obtained from the above algorithm is Step 5: Discard the edges of VD(S₁) which the locus of points which keep equal extend to the right of HP and discard the distances to S_{I} and S_{R} . edges of $VD(S_{P})$ which extend to the left of • The HP is monotonic in y. HP. The resulting graph is the Voronoi diagram of $S = S_1 \cup S_p$.

4 -33

of Voronoi edges

- $\frac{\text{\# of edges of a Voronoi diagram } \leq 3n 6,}{\text{where n is \# of points.}}$
- Reasoning:
 - i. # of edges of a <u>planar graph</u> with n vertices \leq 3n 6.
 - ii. A Delaunay triangulation is a planar graph.
 - iii. Edges in Delaunay triangulation
 - $\xleftarrow{}^{1-1}$ edges in Voronoi diagram.

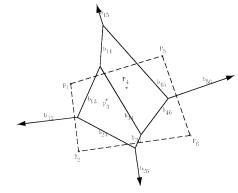


of Voronoi vertices

- <u># of Voronoi vertices ≤ 2n 4.</u>
- Reasoning:
 - Let F, E and V denote # of <u>face</u>, <u>edges</u> and <u>vertices</u> in a planar graph.
 Euler's relation: F = E V + 2.
 - ii. In a Delaunay triangulation, triangle $\xleftarrow{}^{1-1}$ Voronoi vertex $V = n, E \le 3n - 6$ $\Rightarrow F = E - V + 2 \le 3n - 6 - n + 2 = 2n - 4.$

Construct a convex hull from a Voronoi diagram

 After a <u>Voronoi diagram</u> is constructed, a <u>convex hull</u> can by found in O(n) time.



4 -37

Construct a convex hull from a Voronoi diagram

- <u>Step 1</u>: Find an infinite ray by examining all Voronoi edges.
- <u>Step 2</u>: Let P_i be the point to the left of the infinite ray. P_i is a <u>convex hull</u> vertex. Examine the Voronoi polygon of P_i to find the next infinite ray.
- Step 3: Repeat Step 2 until we return to the starting ray.

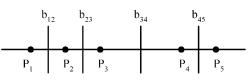
4 -38

Time complexity

- Time complexity for merging 2 Voronoi diagrams:
 - Total: O(n)
 - Step 1: O(n)
 - Step 2: O(n)
 - Step 3 ~ Step 5: O(n) (at most 3n - 6 edges in VD(S_L) and VD(S_R) and at most n segments in HP)
- <u>Time complexity for constructing a Voronoi</u> <u>diagram</u>: O(n log n) because T(n) = 2T(n/2) + O(n)=O(n log n)

Lower bound

 The <u>lower bound</u> of the Voronoi diagram problem is Ω(n log n). sorting ∞ Voronoi diagram problem



The Voronoi diagram for a set of points on a straight line

Applications of Voronoi diagrams

- The Euclidean nearest neighbor searching problem.
- The Euclidean all nearest neighbor problem.

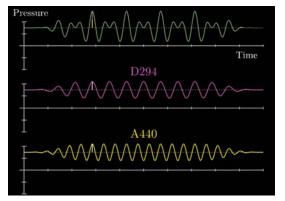
Fast Fourier transform (FFT)

• Fourier transform $b(f) = \int_{-\infty}^{\infty} a(t)e^{i2\pi ft} dt, \text{ where } i = \sqrt{-1}$ • Inverse Fourier transform $a(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} b(f)e^{-i2\pi ft} dt$ • Discrete Fourier transform(DFT) Given $a_0, a_1, \dots, a_{n-1}, \text{ compute}$ $b_j = \sum_{k=0}^{n-1} a_k e^{i2\pi jk/n}, 0 \le j \le n-1$ $= \sum_{k=0}^{n-1} a_k \omega^{kj}, \text{ where } \omega = e^{i2\pi/n}$

4 -41

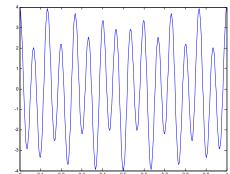
DFT and waveform(1)

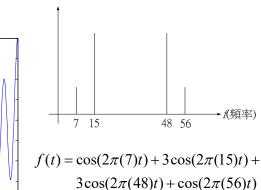
 Any <u>periodic</u> waveform can be decomposed into the <u>linear sum of sinusoid</u> functions (sine or cosine).



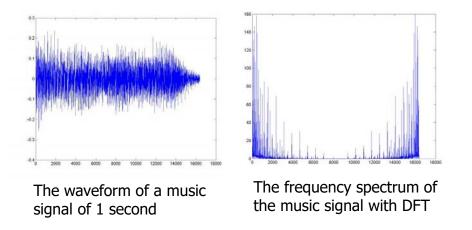
DFT and waveform(2)

 Any <u>periodic</u> waveform can be decomposed into the <u>linear sum of sinusoid</u> functions (sine or cosine).





DFT and waveform (3)



4 -45

An application of the FFT — polynomial multiplication

Polynomial multiplication:

$$f(x) = \sum_{j=0}^{n-1} a_j x^j, \quad g(x) = \sum_{k=0}^{n-1} c_k x^k \qquad h(x) = f(x) \bullet g(x)$$

- The <u>straightforward</u> product requires O(n²) time.
- DFT notations:
 - $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$ Let $b_j = f(w^j)$, $0 \le j \le n-1$, $w^n = 1$ $\{b_0, b_1, \dots, b_{n-1}\}$ is the DFT of $\{a_0, a_1, \dots, a_{n-1}\}$. $h(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_{n-1} x^{n-1}$ $a_k = \frac{1}{n} h(w^{-k})$, $0 \le j \le n-1$ $\{a_0, a_1, \dots, a_{n-1}\}$ is the inverse DFT of $\{b_0, b_1, \dots, b_{n-1}\}$.

Fast polynomial multiplication

Step 1: Let N be the smallest integer that N=2q and N≥2n-1. Step 2: Compute FFT of $\{a_0, a_1, \dots, a_{n-1}, 0, 0, \dots, 0\}$. Step 3: Compute FFT of $\{c_0, c_1, \dots, c_{n-1}, 0, 0, \dots, 0\}$. Step 4: Compute $f(w^j) \bullet g(w^j)$, $0 \le j \le N-1$, $w = e^{2\pi i/N}$ Step 5: Let $h(w^j) = f(w^j) \bullet g(w^j)$ Compute inverse DFT of $\{h(w^0), h(w^1), \dots, h(w^{N-1})\}$. The resulting sequence of numbers are the coefficients of h(x).

Time complexity: O(NlogN)=O(nlogn), N<4n.

FFT algorithm

Inverse DFT

$$a_k = \frac{1}{n} \sum_{j=0}^{n-1} b_j \omega^{-jk}, \ 0 \le k \le n-1$$

- $e^{i\theta} = \cos\theta + i\sin\theta$ $\omega^n = (e^{i2\pi/n})^n = e^{i2\pi} = \cos 2\pi + i\sin 2\pi = 1$ $\omega^{n/2} = (e^{i2\pi/n})^{n/2} = e^{i\pi} = \cos\pi + i\sin\pi = -1$
- DFT can be computed in O(n²) time by a straightforward method.
- DFT can be solved by the divide-and-conquer strategy (FFT) in <u>O(nlog n) time</u>.

FFT algorithm when n=4FFT algorithm when n=8• $n=4, w=e^{2\pi/4}, w^4=1, w^2=-1$ $b_j = \sum_{k=0}^{n-1} a_k e^{i2\pi jk/n}$ • $n=8, w=e^{2\pi/8}, w^8=1, w^4=-1$ $b_j = \sum_{k=0}^{n-1} a_k e^{i2\pi j k/n} = \sum_{k=0}^{n-1} a_k \omega^{kj}$ $b_0 = a_0 + a_1 + a_2 + a_3$ $b_1 = a_0 + a_1 w + a_2 w^2 + a_3 w^3$ $=\sum_{k=1}^{n-1}a_{k}\omega^{kj}$ $b_0 = a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7$ $b_2 = a_0 + a_1 w^2 + a_2 w^4 + a_3 w^6$ $b_1 = a_0 + a_1 W + a_2 W^2 + a_3 W^3 + a_4 W^4 + a_5 W^5 + a_6 W^6 + a_7 W^7$ $b_3 = a_0 + a_1 w^3 + a_2 w^6 + a_3 w^9$ $b_2 = a_0 + a_1 W^2 + a_2 W^4 + a_3 W^6 + a_4 W^8 + a_5 W^{10} + a_6 W^{12} + a_7 W^{14}$ another form: $b_3 = a_0 + a_1 w^3 + a_2 w^6 + a_3 w^9 + a_4 w^{12} + a_5 w^{15} + a_6 w^{18} + a_7 w^{21}$ $b_0 = (a_0 + a_2) + (a_1 + a_3)$ $b_4 = a_0 + a_1 w^4 + a_2 w^8 + a_3 w^{12} + a_4 w^{16} + a_5 w^{20} + a_6 w^{24} + a_7 w^{28}$ $b_2 = (a_0 + a_2 w^4) + (a_1 w^2 + a_3 w^6) = (a_0 + a_2) - (a_1 + a_3)$ • When we calculate b_0 , we shall calculate $(a_0 + a_2)$ $b_5 = a_0 + a_1 w^5 + a_2 w^{10} + a_3 w^{15} + a_4 w^{20} + a_5 w^{25} + a_6 w^{30} + a_7 w^{35}$ and $(a_1 + a_3)$. Later, b_2 van be easily calculated. $b_6 = a_0 + a_1 w^6 + a_2 w^{12} + a_3 w^{18} + a_4 w^{24} + a_5 w^{30} + a_6 w^{36} + a_7 w^{42}$ Similarly, $b_7 = a_0 + a_1 W^7 + a_2 W^{14} + a_3 W^{21} + a_4 W^{28} + a_5 W^{35} + a_6 W^{42} + a_7 W^{49}$ $b_1 = (a_0 + a_2 w^2) + (a_1 w + a_3 w^3) = (a_0 - a_2) + w(a_1 - a_3)$ $b_3 = (a_0 + a_2 W^6) + (a_1 W^3 + a_3 W^9) = (a_0 - a_2) - W(a_1 - a_3).$ 4 - 49 4 -50 After reordering, we have • $C_0 = a_0 + a_2 + a_4 + a_6$ $C_1 = a_0 + a_2 w^2 + a_4 w^4 + a_6 w^6$ $b_0 = (a_0 + a_2 + a_4 + a_6) + (a_1 + a_3 + a_5 + a_7)$ $C_2 = a_0 + a_2 W^4 + a_4 W^8 + a_6 W^{12}$ $b_1 = (a_0 + a_2 W^2 + a_4 W^4 + a_6 W^6) + W(a_1 + a_3 W^2 + a_5 W^4 + a_7 W^6)$ $C_3 = a_0 + a_2 W^6 + a_4 W^{12} + a_6 W^{18}$ $b_2 = (a_0 + a_2 W^4 + a_4 W^8 + a_6 W^{12}) + W^2 (a_1 + a_3 W^4 + a_5 W^8 + a_7 W^{12})$ $b_3 = (a_0 + a_2 w^6 + a_4 w^{12} + a_6 w^{18}) + w^3 (a_1 + a_3 w^6 + a_5 w^{12} + a_7 w^{18})$ • Let $x = w^2 = e^{2\pi/4}$ $b_4 = (a_0 + a_2 + a_4 + a_6) - (a_1 + a_3 + a_5 + a_7)$ $C_0 = a_0 + a_2 + a_4 + a_6$ $b_5 = (a_0 + a_2 w^2 + a_4 w^4 + a_6 w^6) - w(a_1 + a_3 w^2 + a_5 w^4 + a_7 w^6)$ $C_1 = a_0 + a_2 x + a_4 x^2 + a_6 x^3$ $b_6 = (a_0 + a_2 W^4 + a_4 W^8 + a_6 W^{12}) - W^2 (a_1 + a_3 W^4 + a_5 W^8 + a_7 W^{12})$ $c_2 = a_0 + a_2 x^2 + a_4 x^4 + a_6 x^6$ $b_7 = (a_0 + a_2 W^6 + a_4 W^{12} + a_6 W^{18}) - W^3 (a_1 + a_3 W^6 + a_5 W^{12} + a_7 W^{18})$ $C_3 = a_0 + a_2 x^3 + a_4 x^6 + a_6 x^9$ Rewrite as • Thus, $\{c_0, c_1, c_2, c_3\}$ is FFT of $\{a_0, a_2, a_4, a_6\}$. $b_4 = c_0 - d_0 = c_0 + w^4 d_0$ $b_0 = c_0 + d_0$ $b_5 = c_1 - w d_1 = c_1 + w^5 d_1$ $b_1 = c_1 + wd_1$ Similarly, $\{d_0, d_1, d_2, d_3\}$ is FFT of $\{a_1, a_3, a_5, a_7\}$. $b_2 = c_2 + w^2 d_2$ $b_6 = c_2 - w^2 d_2 = c_2 + w^6 d_2$ $b_7 = c_3 - w^2 d_3 = c_3 + w^7 d_3$ $b_3 = c_3 + w^2 d_3$

General FFT

• In general, let $w = e^{2\pi/n}$ (assume *n* is even.) $w^{n}=1, w^{n/2}=-1$ $b_{j}=a_{0}+a_{1}w^{j}+a_{2}w^{2j}+\ldots+a_{n-1}w^{(n-1)j},$ $=\{a_{0}+a_{2}w^{2j}+a_{4}w^{4j}+\ldots+a_{n-2}w^{(n-2)j}\}+$ $w^{j}\{a_{1}+a_{3}w^{2j}+a_{5}w^{4j}+\ldots+a_{n-1}w^{(n-2)j}\}$ $=c_{j}+w^{j}d_{j}$ $b_{j+n/2}=a_{0}+a_{1}w^{j+n/2}+a_{2}w^{2j+n}+a_{3}w^{3j+3n/2}+\ldots$ $+a_{n-1}w^{(n-1)j+n(n-1)/2}$ $=a_{0}-a_{1}w^{j}+a_{2}w^{2j}-a_{3}w^{3j}+\ldots+a_{n-2}w^{(n-2)j}-a_{n-1}w^{(n-1)j}$ $=c_{j}-w^{j}d_{j}$ $=c_{j}+w^{j+n/2}d_{j}$

4 -53

$$\label{eq:step 3: compute b_j:} \begin{split} \underline{Step 3:} & \text{Compute b}_j: \\ & b_j = c_j + w^j d_j \ \text{ for } 0 \leq j \leq n/2 \text{ - } 1 \\ & b_{j+n/2} = c_j - w^j d_j \ \text{ for } 0 \leq j \leq n/2 \text{ - } 1. \end{split}$$

• Time complexity:

T(n) = 2T(n/2) + O(n)= O(n log n)

Divide-and-conquer (FFT)

4 -54

Matrix multiplication

- Let A, B and C be $n \times n$ matrices C = AB $C(i, j) = \sum_{1 \le k \le n} A(i, k)B(k, j)$
- The <u>straightforward</u> method to perform a matrix multiplication requires O(n³) time.

Divide-and-conquer approach
•
$$C = AB$$

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

$$C_{11} = A_{11} B_{11} + A_{12} B_{21}$$

$$C_{12} = A_{11} B_{12} + A_{12} B_{22}$$

$$C_{21} = A_{21} B_{11} + A_{22} B_{21}$$

$$C_{22} = A_{21} B_{12} + A_{22} B_{22}$$
• Time complexity:

$$T(n) = \begin{cases} b \\ 8T(n/2) + cn^{2}, n \geq 2 \end{cases}$$
(# of additions : n²)
We get $T(n) = O(n^{3})$

Strassen's matrix multiplicaiton

•
$$P = (A_{11} + A_{22})(B_{11} + B_{22})$$

 $Q = (A_{21} + A_{22})B_{11}$
 $R = A_{11}(B_{12} - B_{22})$
 $S = A_{22}(B_{21} - B_{11})$
 $T = (A_{11} + A_{12})B_{22}$
 $U = (A_{21} - A_{11})(B_{11} + B_{12})$
 $V = (A_{12} - A_{22})(B_{21} + B_{22}).$
• $C_{11} = P + S - T + V$
 $C_{12} = R + T$
 $C_{21} = Q + S$
 $C_{22} = P + R - Q + U$
4-58

Time complexity

- 7 multiplications and 18 additions or subtractions
- Time complexity:

$$T(n) = \begin{cases} b, & n \le 2\\ 7T(n/2) + an^2, & n \le 2 \end{cases}$$

$$T(n) = an^2 + 7T(n/2)$$

$$= an^2 + 7(a(\frac{n}{2})^2 + 7T(n/4))$$

$$= an^2 + \frac{7}{4}an^2 + 7^2T(n/4)$$

$$= \cdots$$

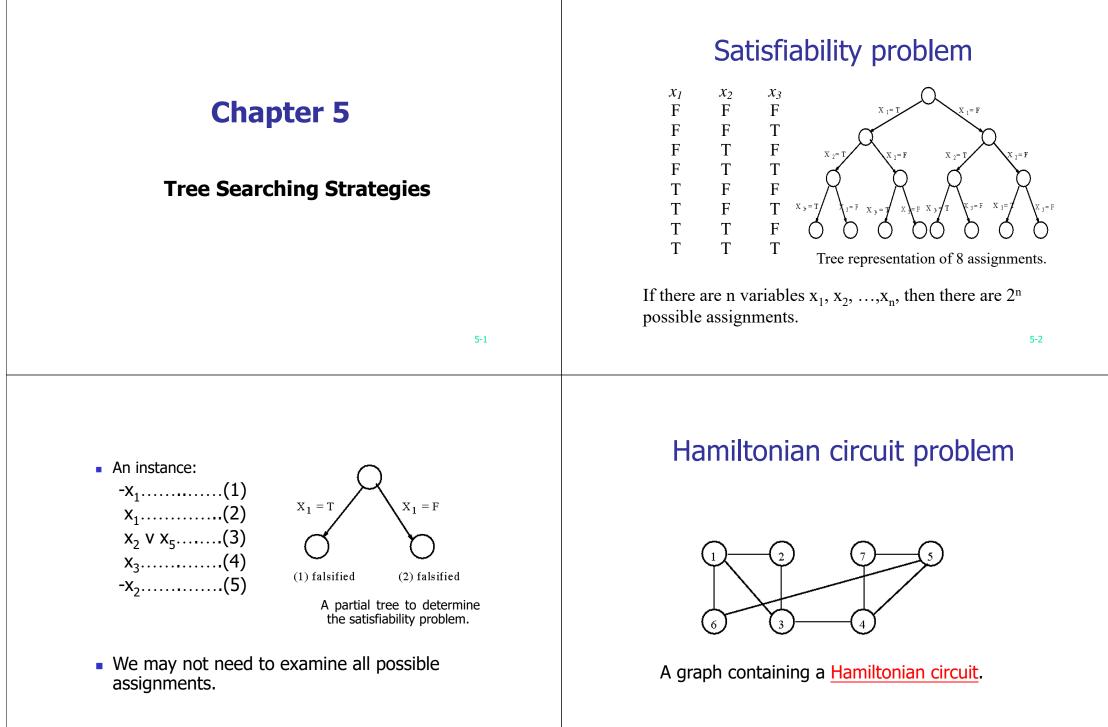
$$\vdots$$

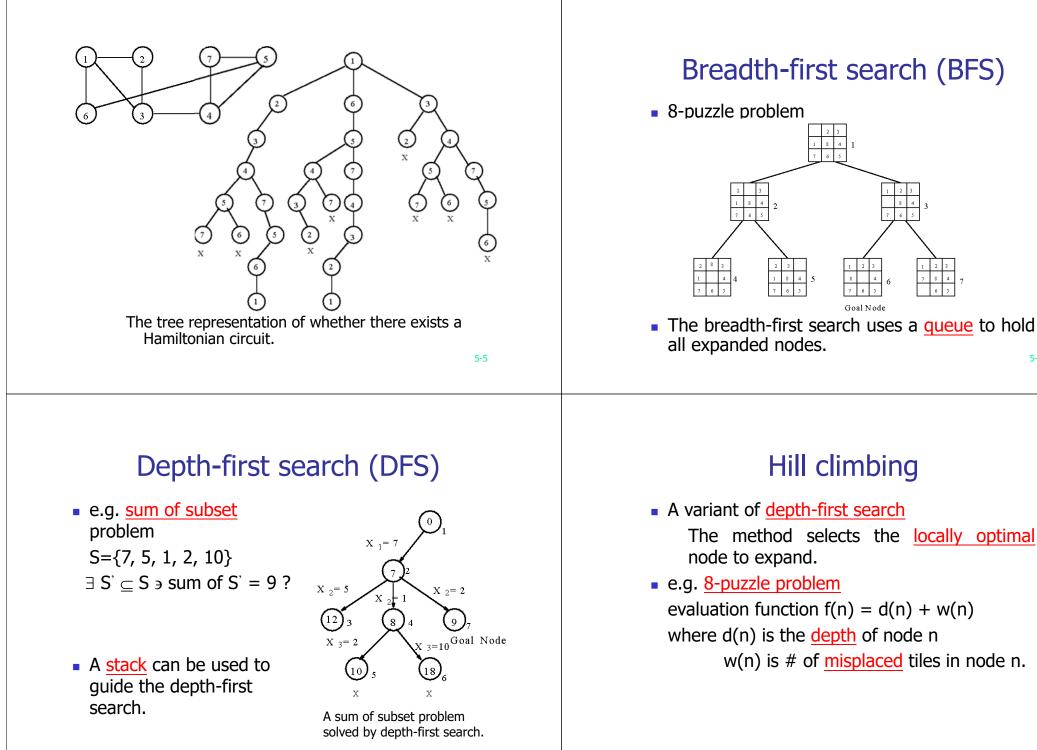
$$= an^2(1 + \frac{7}{4} + (\frac{7}{4})^2 + \cdots + (\frac{7}{4})^{k-1}) + 7^kT(1)$$

$$\leq cn^2(\frac{7}{4})^{\log_2 n} + 7^{\log_2 n}, c \text{ is a constant}$$

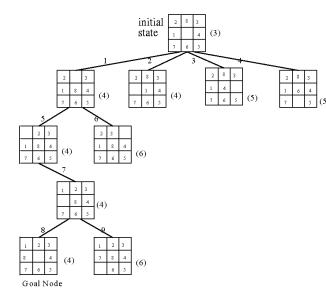
$$= cn^2(\frac{7}{4})^{\log_2 n} + n^{\log_2 7} = cn^{\log_2 4 - \log_2 7 + \log_2 4} + n^{\log_2 7}$$

$$= O(n^{\log_2 7}) \cong O(n^{2.81})$$



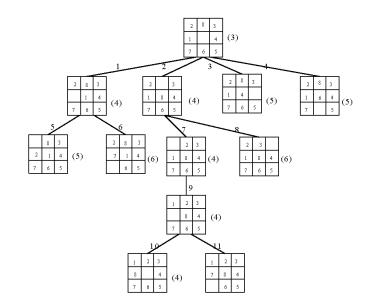


5-8



An 8-puzzle problem solved by a hill climbing method.

5-9



An 8-puzzle problem solved by a <u>best-first</u> search scheme.

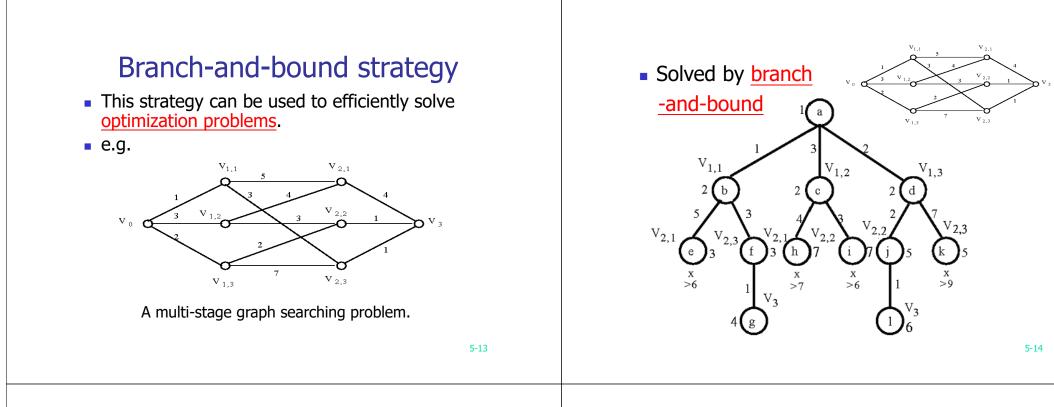
Best-first search strategy

- Combine <u>depth-first search</u> and <u>breadth-first</u> <u>search</u>.
- Selecting the node with the <u>best estimated</u> cost among all nodes.
- This method has a global view.
- The priority queue (heap) can be used as the data structure of best-first search.

5-10

Best-First Search Scheme

- Step1: Form a one-element list consisting of the root node.
- Step2: Remove the first element from the list. Expand the first element. If one of the descendants of the first element is a goal node, then stop; otherwise, add the descendants into the list.
- Step3: Sort the entire list by the values of some estimation function.
- Step4: If the list is empty, then failure. Otherwise, go to Step 2.



Personnel assignment problem

- A linearly ordered set of persons $P=\{P_1, P_2, ..., P_n\}$ where $P_1 < P_2 < ... < P_n$
- A partially ordered set of jobs J={J₁, J₂, ..., J_n}
- Suppose that P_i and P_j are assigned to jobs $f(P_i)$ and $f(P_j)$ respectively. If $f(P_i) \le f(P_j)$, then $P_i \le P_j$. Cost C_{jj} is the cost of assigning P_i to J_j . We want to find a <u>feasible assignment</u> with the minimum cost. i.e.

 $\begin{array}{l} X_{ij} = 1 \mbox{ if } P_i \mbox{ is assigned to } J_j \\ X_{ij} = 0 \mbox{ otherwise.} \end{array}$ $\begin{array}{l} \mbox{ Minimize } \sum_{i,j} C_{ij} X_{ij} \end{array}$ e.g. A partial ordering of jobs

$$\begin{array}{ccc} \mathbf{J}_1 & \mathbf{J}_2 \\ \downarrow & \searrow & \downarrow \\ \mathbf{J}_3 & \mathbf{J}_4 \end{array}$$

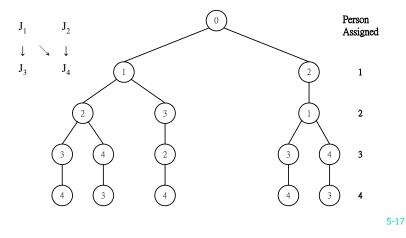
 After topological sorting, one of the following topologically sorted sequences will be

generated: J_1 , J_2 , J_3 , J_4

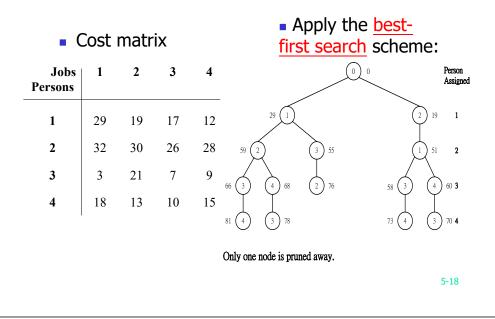
• One of feasible assignments: $P_1 \rightarrow J_1, P_2 \rightarrow J_2, P_3 \rightarrow J_3, P_4 \rightarrow J_4$

A solution tree

 All possible solutions can be represented by a <u>solution tree</u>.



Cost matrix



Reduced cost matrix

4

| Cost matrix | | | | | | |
|---------------------------------|----|----|----------|----|---|--|
| Jobs Persons | 1 | 2 | 3 | 4 | D | |
| 1 | 29 | 19 | 17 | 12 | 1 | |
| 2 | 32 | 30 | 17 26 | 28 | | |
| 3 | 3 | 21 | 7 | 9 | | |
| 4 | 18 | 13 | 10 | 15 | | |

| • <u>Re</u> | duce | d cos | st m | atrix | <u>_</u> |
|-----------------|------|-------|------|-------|----------|
| Jobs Persons | 1 | 2 | 3 | 4 | |
| 1 | 17 | 4 | 5 | 0 | (-12) |
| 2 | 6 | 1 | 0 | 2 | (-26) |
| 3 | 0 | 15 | 4 | 6 | (-3) |

0

(-3)

0

8

• A <u>reduced cost matrix</u> can be obtained:

subtract a constant from each row and each column respectively such that each row and each column contains at least one zero.

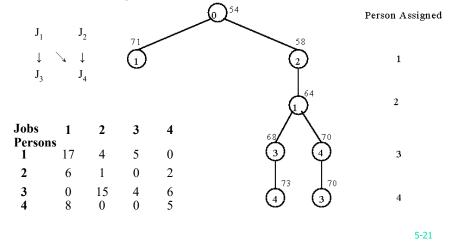
- Total cost subtracted: 12+26+3+10+3 = 54
- This is a <u>lower bound</u> of our solution.

(-10)

5

Branch-and-bound for the personnel assignment problem

Bounding of subsolutions:



The traveling salesperson optimization problem

• It is <u>NP-complete</u>.

A cost matrix

| j i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--------|----|----------|----------|----------|---------------------------------------|----------|----------|--|
| 1 | x | 3 | 93 | 13 | 33 | 9 | 57 | |
| 2 | 4 | ∞ | 77 | 42 | 21 | 16 | 34 | |
| 3 | 45 | 17 | ∞ | 36 | 16 | 28 | 25 | |
| 4 | 39 | 90 | 80 | ∞ | 56 | 7 | 91 | |
| 5 | 28 | 46 | 88 | 33 | ∞ | 25 | 57 | |
| 6 | 3 | 88 | 18 | 46 | 92 | ∞ | 7 | |
| 7 | 44 | 26 | 33 | 27 | 33 21 16 56 ∞ 92 84 | 39 | ∞ | |
| | | | | | | | | |

5-22

• A reduced cost matrix

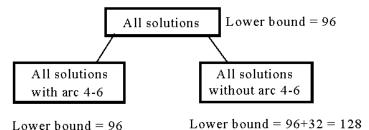
| j i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--------|----|----------|----------|----------|----------|----------|------|-------|
| 1 | x | 0 | 90 | 10 | 30 | 6 | 54 | (-3) |
| 2 | 0 | ∞ | 73 | 38 | 17 | 12 | 30 | (-4) |
| 3 | 29 | 1 | ∞ | 20 | 0 | 12 | 9 | (-16) |
| 4 | 32 | 83 | 73 | ∞ | 49 | 0 | 84 | (-7) |
| 5 | 3 | 21 | 63 | 8 | ∞ | 0 | 32 | (-25) |
| 6 | 0 | 85 | 15 | 43 | 89 | ∞ | 4 | (-3) |
| 7 | 18 | 0 | 7 | 1 | 58 | 13 | x | (-26) |
| | | | | | | Re | duce | d: 84 |

Another reduced matrix

| j i | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|--------|----|----------|------|----------|----------|----|------|
| 1 | 00 | 0 | 83 | 9 | 30 | 6 | 50 |
| 2 | 0 | ∞ | 66 | 37 | 17 | 12 | 26 |
| 3 | 29 | 1 | œ | 19 | 0 | 12 | 5 |
| 4 | 32 | 83 | 66 | ∞ | 49 | 0 | 80 |
| 5 | 3 | 21 | 56 | 7 | ∞ | 0 | 28 |
| 6 | 0 | 85 | 8 | 42 | 89 | œ | 0 |
| 7 | 18 | 0 | 0 | 0 | 58 | 13 | 00 |
| | | | (-7) | (-1) | | | (-4) |

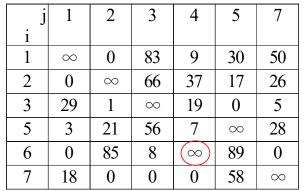
Total cost reduced: 84+7+1+4 = 96 (lower bound)

The highest level of a decision tree:



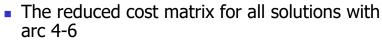
- If we use arc 3-5 to split, the difference on the lower bounds is 17+1 = 18.
- 5-25

 A reduced cost matrix if arc (4,6) is included in the solution.



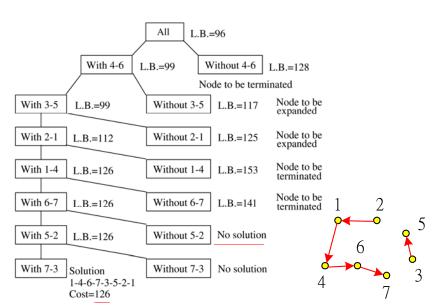
Arc (6,4) is changed to be infinity since it can not be included in the solution.

5-26



| j i | 1 | 2 | 3 | 4 | 5 | 7 | |
|--------|----|----------|----------|----------|--------------------------------|----------|------|
| 1 | x | 0 | 83 | 9 | 30 17 0 ∞ 89 58 | 50 | |
| 2 | 0 | ∞ | 66 | 37 | 17 | 26 | |
| 3 | 29 | 1 | ∞ | 19 | 0 | 5 | |
| 5 | 0 | 18 | 53 | 4 | x | 25 | (-3) |
| 6 | 0 | 85 | 8 | ∞ | 89 | 0 | |
| 7 | 18 | 0 | 0 | 0 | 58 | ∞ | |
| | | | | | | | |

 Total cost reduced: 96+3 = 99 (new lower bound)



A branch-and-bound solution of a traveling salesperson problem.

The 0/1 knapsack problem

| Positive integer P ₁ , P ₂ ,, P _n (profit) | | | | | | | |
|---|--|--|--|--|--|--|--|
| | W ₁ , W ₂ ,, W _n (weight) | | | | | | |
| M (capacity) | | | | | | | |
| | n | | | | | | |
| maximize | | | | | | | |
| | i=1 | | | | | | |
| subject to | $\sum_{i=1}^{n} W_i X_i \le M$ $X_i = 0 \text{ or } 1, i = 1,, n.$ | | | | | | |
| <u>j</u> | i=1 | | | | | | |

The problem is modified:

minimize $-\sum_{i=1}^{n} P_i X_i$

5-29

Relax the restriction

- Relax our restriction from X_i = 0 or 1 to 0 \leq X_i \leq 1 (knapsack problem)
- Let $-\sum_{i=1}^{n} P_i X_i$ be an optimal solution for 0/1

knapsack problem and $-\sum_{i=1}^{n} P_i X'_i$ be an optimal

solution for knapsack problem. Let $Y = -\sum_{i=1}^{n} P_i X_i$,

$$\begin{split} \boldsymbol{Y}^{'} &= -\sum_{i=1}^{n} \boldsymbol{P}_{i} \boldsymbol{X}_{i}^{\prime} \, . \\ \Rightarrow \boldsymbol{Y}^{'} \leq \boldsymbol{Y} \end{split}$$

| • | e.g. r | n = 6, | , M = | 34 | | | | | |
|---|---|--------|-------|----|----|----|---|--|--|
| | i | 1 | 2 | 3 | 4 | 5 | 6 | | |
| | P _i | 6 | 10 | 4 | 5 | 6 | 4 | | |
| | W _i | 10 | 19 | 8 | 10 | 12 | 8 | | |
| | $(\mathbf{P}_i/\mathbf{W}_i \ge \mathbf{P}_{i+1}/\mathbf{W}_{i+1})$ | | | | | | | | |
| • A feasible solution: $X_1 = 1, X_2 = 1, X_3 = 0, X_4 = 0, X_5 = 0, X_6 = 0$ | | | | | | | | | |

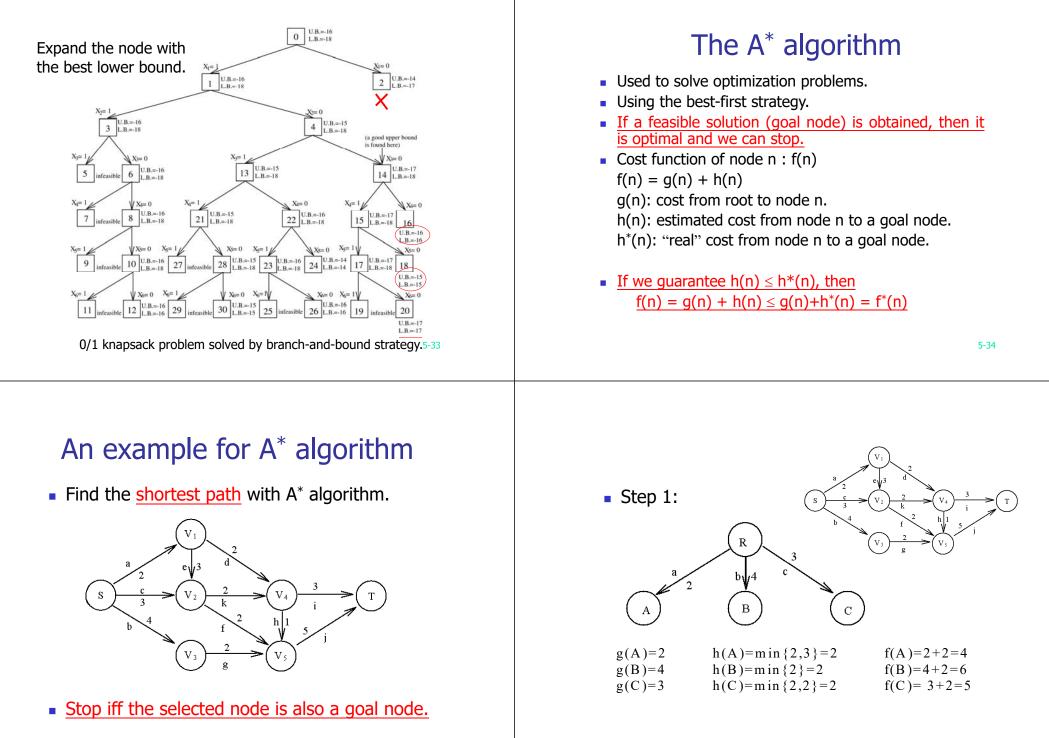
 $(P_1+P_2) = -16$ (upper bound) Any solution higher than -16 can not be an optimal solution.

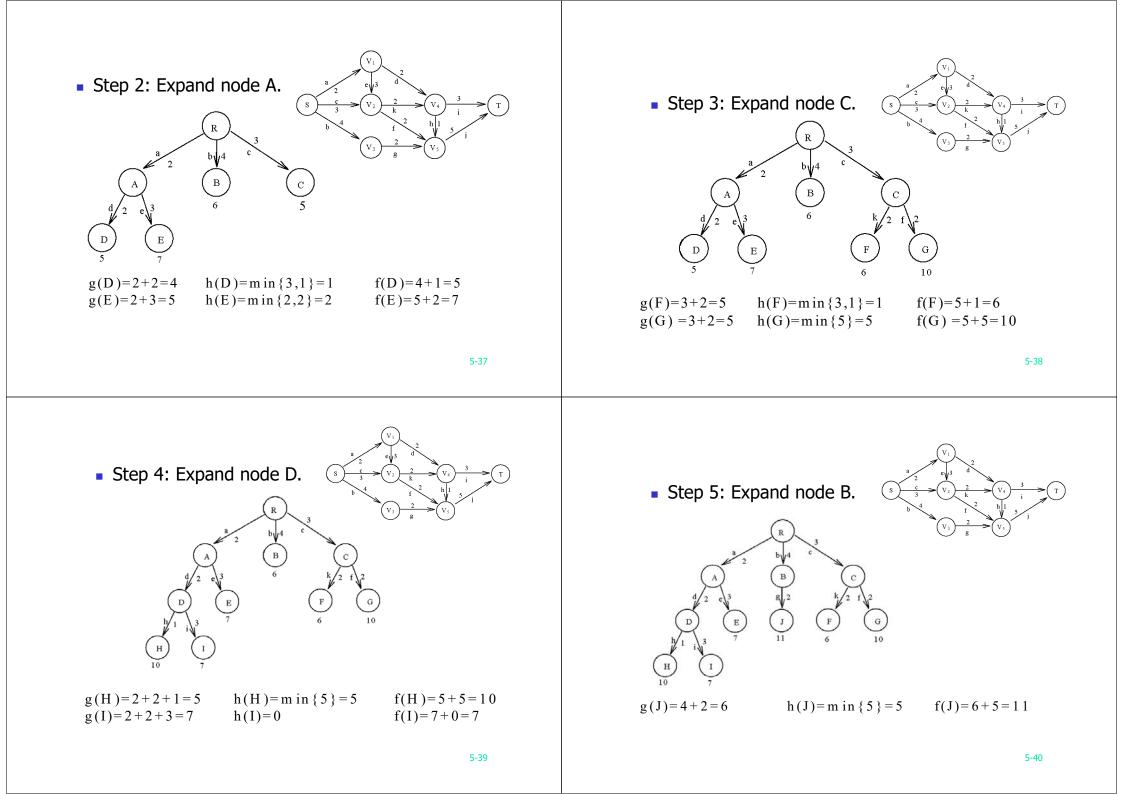
Upper bound and lower bound

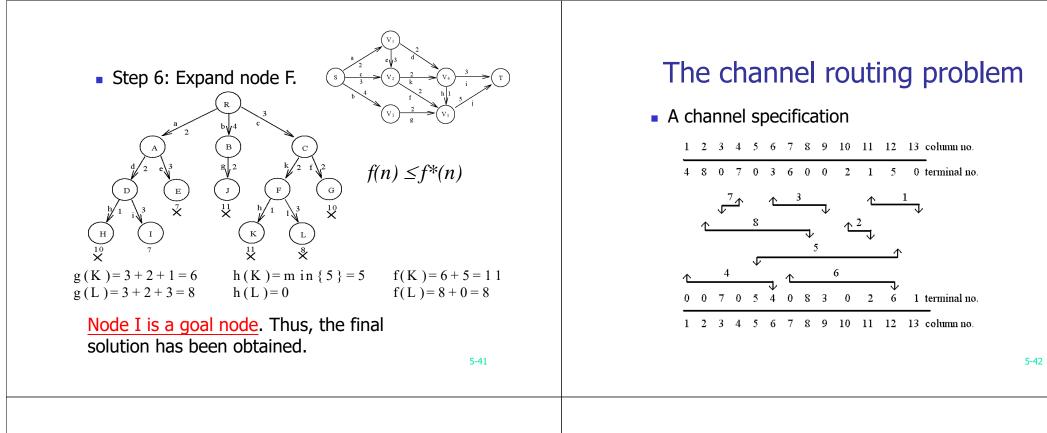
We can use <u>the greedy method</u> to find an optimal solution for knapsack problem:

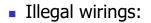
 $X_1 = 1, X_2 = 1, X_3 = 5/8, X_4 = 0, X_5 = 0, X_6 = 0$ -(P₁+P₂+5/8P₃) = -18.5 (lower bound) -18 is our lower bound. (only consider integers)

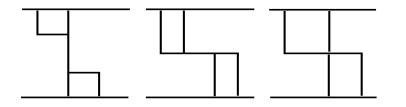
$$\Rightarrow -18 \le \text{optimal solution} \le -16 \\ \text{optimal solution: } X_1 = 1, X_2 = 0, X_3 = 0, X_4 = 1, X_5 = 1, X_6 = 0 \\ -(P_1+P_4+P_5) = -17$$





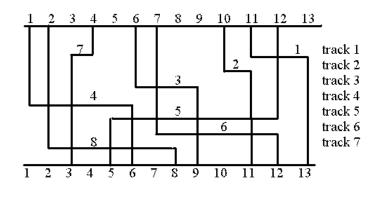




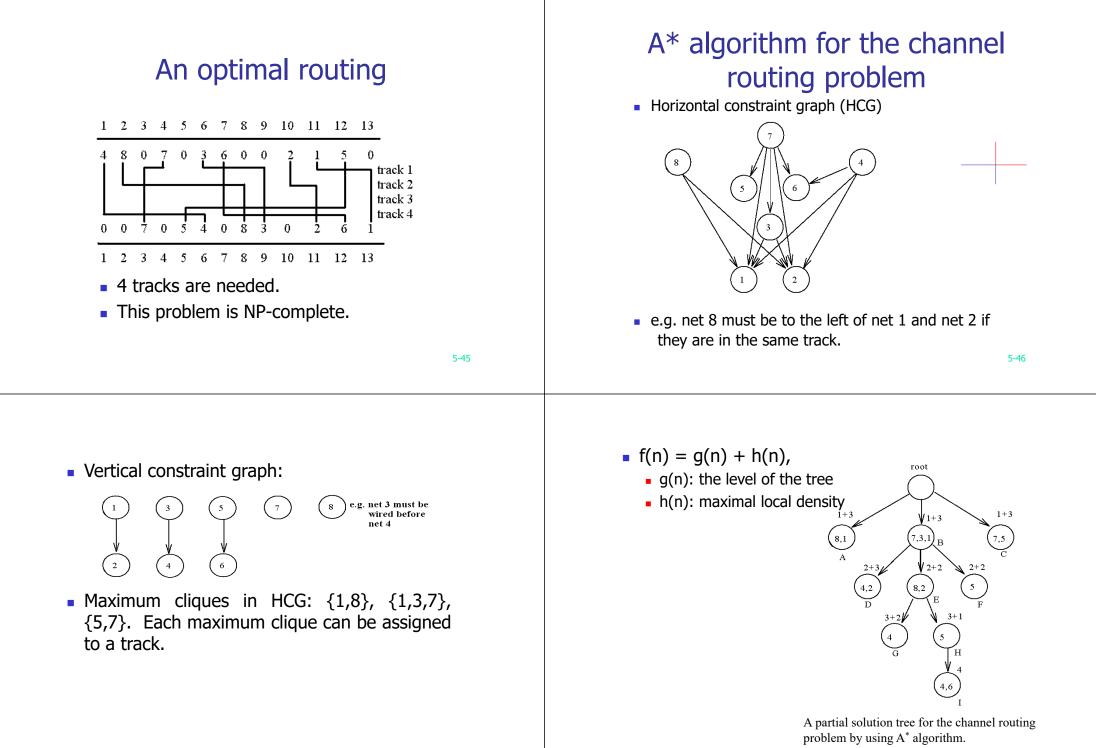


• We want to find a routing which minimizes the number of tracks.

A feasible routing



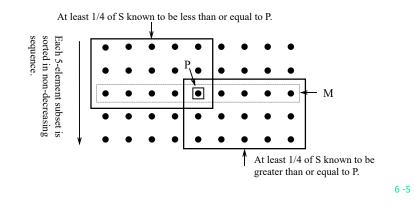
• 7 tracks are needed.



| | A simple example: Binary search | | | | | |
|---|---|--|--|--|--|--|
| Chapter 6 | sorted sequence : (search 9) 1 4 5 7 9 10 12 15 | | | | | |
| Prune-and-Search 6-1 | step 2 step 2 step 3 After each comparison, a half of the data set are pruned away. Binary search can be viewed as a special divide-and-conquer method, since there exists no solution in another half and then no merging is done. | | | | | |
| <section-header><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></section-header> | $\begin{array}{l} \textbf{Prune-and-search concept for}\\ \textbf{the selection problem}\\ \textbf{a}_1, \textbf{a}_2,, \textbf{a}_n \\ \textbf{b}_2 \\ \textbf{b}_3 \\ \textbf{c}_3;\\ \textbf{c}_3$ | | | | | |

How to select P?

• The n elements are divided into $\left\lceil \frac{n}{5} \right\rceil$ subsets. (Each subset has 5 elements.)



Prune-and-search approach

- Input: A set S of n elements.
- <u>Output:</u> The kth smallest element of S.
- Step 1: Divide S into $\lceil n/5 \rceil$ subsets. Each subset contains five elements. Add some dummy ∞ elements to the last subset if n is not a net multiple of S.
- Step 2: Sort each subset of elements.
- Step 3: <u>Recursively</u>, find the element p which is the median of the medians of the n/5 subsets..

6 -6

- <u>Step 4: Partition</u> S into S_1 , S_2 and S_3 , which contain the elements less than, equal to, and greater than p, respectively.
- <u>Step 5</u>: If $|S_1| \ge k$, then discard S_2 and S_3 and solve the problem that selects the kth smallest element from S_1 during the next iteration;
- else if $|S_1| + |S_2| \ge k$ then p is the kth smallest element of S;
- otherwise, let $k' = k |S_1| |S_2|$, solve the problem that selects the k'th smallest element from S₃ during the next iteration.

Time complexity

- At least n/4 elements are pruned away during each iteration.
- The problem remaining in step 5 contains at most 3n/4 elements.
- Time complexity: T(n) = O(n)
 - step 1: O(n)
 - step 2: O(n)
 - step 3: T(n/5)
 - step 4: O(n)
 - step 5: T(3n/4)
 - T(n) = T(3n/4) + T(n/5) + O(n)

Let
$$T(n) = a_0 + a_1n + a_2n^2 + ..., a_1 \neq 0$$

 $T(3n/4) = a_0 + (3/4)a_1n + (9/16)a_2n^2 + ...$
 $T(n/5) = a_0 + (1/5)a_1n + (1/25)a_2n^2 + ...$
 $T(3n/4 + n/5) = T(19n/20) = a_0 + (19/20)a_1n + (361/400)a_2n^2 + ...$
 $T(3n/4) + T(n/5) \le a_0 + T(19n/20)$
 $\Rightarrow T(n) \le cn + T(19n/20)$
 $\le cn + (19/20)cn + T((19/20)^2n)$
 \vdots
 $\le cn + (19/20)cn + (19/20)^2cn + ... + (19/20)^pcn + T((19/20)^{p-1}n \le 1 \le (19/20)^{p-1}n \le 1 \le (19/20)^{p-1}}$
 $= \frac{1+\frac{19}{20}e^{-n+b}}{\frac{1}{20}e^{-n+b}}$
 $\le 20 cn + b$
 $= O(n)$ 6-9

Time complexity analysis

Assume that the time needed to execute the prune-and-search in each iteration is O(n^k) for some constant k and the worst case run time of the prune-and-search algorithm is T(n). Then

$$T(n) = T((1-f)n) + O(n^k)$$

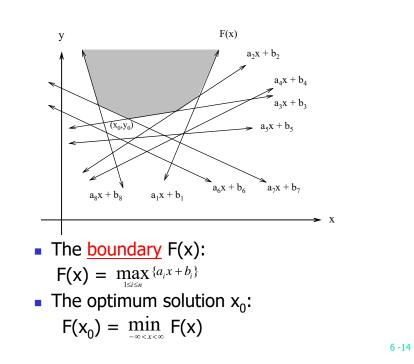
We have T(n) ≤ T((1-f) n) + cn^k for sufficiently large n. ≤ T((1-f)²n) + cn^k + c(1-f)^kn^k : ≤ c^{*} + cn^k + c(1-f)^kn^k + c(1-f)^{2k}n^k + ... + c(1-f)^{pk}n^k = c^{*} + cn^k(1 + (1-f)^k + (1-f)^{2k} + ... + (1-f)^{pk}). Since 1 - f < 1, as n → ∞, ∴ T(n) = O(n^k)
Thus, the time-complexity of the whole pruneand-search process is of the same order as the time-complexity in each iteration.

Linear programming with two variables

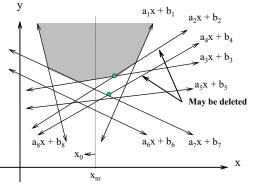
- Minimize ax + by
- subject to $a_ix + b_iy \ge c_i$, i = 1, 2, ..., n
- Simplified two-variable linear programming problem:

Minimize y

subject to $y \ge a_i x + b_i$, i = 1, 2, ..., n



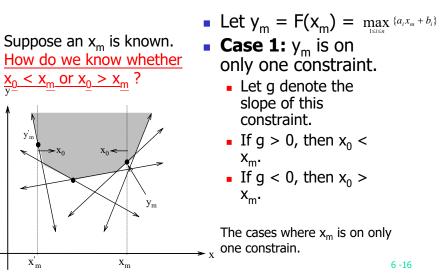
Constraints deletion

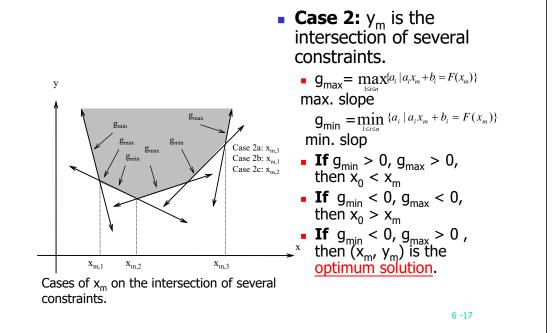


• If $x_0 < x_m$ and the intersection of $a_3x +$ b_3 and $a_2x + b_2$ is greater than x_m, then one of these two constraints is always smaller than the other for $x < x_m$. Thus, this constraint can be deleted.

• It is similar for $x_0 > 0$ X_m.

Determining the direction of the optimum solution





How to choose x_m?

 We arbitrarily group the n constraints into n/2 pairs. For each pair, find their intersection. Among these n/2 intersections, choose the median of their x-coordinates as x_m.

Prune-and-Search approach

- Input: Constraints S: a_ix + b_i, i=1, 2, ..., n.
- <u>Output</u>: The value x₀ such that y is minimized at x₀ subject to the above constraints.
- Step 1: If S contains no more than two constraints, solve this problem by a brute force method.
- <u>Step 2</u>: Divide S into n/2 <u>pairs</u> of constraints randomly. For each pair of constraints $a_ix + b_j$ and $a_jx + b_j$, find the <u>intersection</u> p_{ij} of them and denote its x-value as x_{ij} .
- <u>Step 3:</u> Among the x_{ij} 's, find the <u>median</u> x_m .

Step 6:

<u>Case 6a:</u> If $x_0 < x_m$, for each pair of constraints whose x-coordinate intersection is larger than x_m , prune away the constraint which is always <u>smaller</u> than the other for $x \le x_m$.

<u>Case 6b:</u> If $x_0 > x_m$, do similarly.

Let S denote the set of remaining constraints. Go to Step 2.

- There are totally ln/2 intersections. <u>Thus, ln/4</u> <u>constraints are pruned away for each iteration</u>.
- Time complexity:

$$T(n) = T(3n/4) + O(n)$$

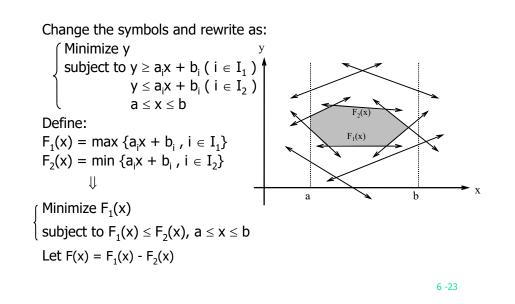
= O(n)

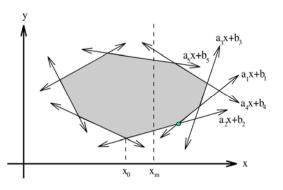
6 -21

The general two-variable linear programming problem

$$\begin{array}{l} \mbox{Minimize ax + by} \\ \mbox{subject to } a_ix + b_iy \geq c_i \ , \ i = 1, \ 2, \ ..., \ n \\ \mbox{Let } x' = x \\ y' = ax + by \\ \downarrow \\ \mbox{Minimize } y' \\ \mbox{subject to } a_i'x' + b_i'y' \geq c_i' \ , \ i = 1, \ 2, \ ..., \ n \\ \mbox{where } a_i' = a_i - b_ia/b, \ b_i' = b_i/b, \ c_i' = c_i \end{array}$$

6 -22





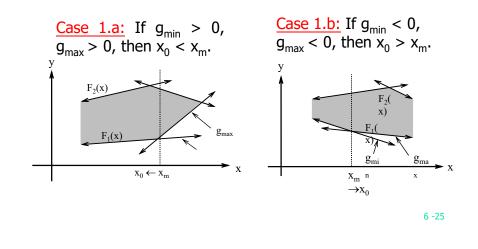
• If we know $x_0 < x_m$, then $a_1x + b_1$ can be deleted because $a_1x + b_1 < a_2x + b_2$ for $x < x_m$.

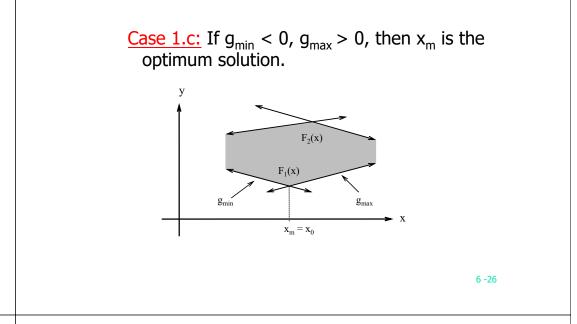
Define:

- $g_{min} = min \{a_i \mid i \in I_1, a_i x_m + b_i = F_1(x_m)\}$, min. slope
- $g_{max} = max\{a_i \mid i \in I_1, a_ix_m + b_i = F_1(x_m)\}$, max. slope
- $h_{min} = min \{a_i \mid i \in I_2, a_i x_m + b_i = F_2(x_m)\}$, min. slope
- $h_{max} = max\{a_i \mid i \in I_2, a_ix_m + b_i = F_2(x_m)\}$, max. slope

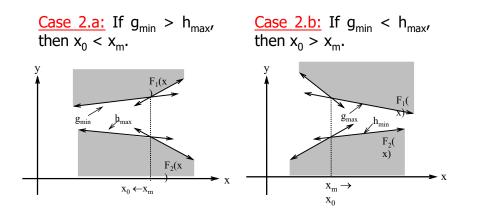
Determining the solution

• Case 1: If $F(x_m) \le 0$, then x_m is feasible.

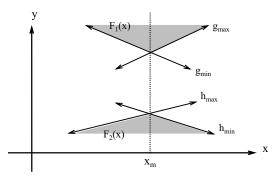




• Case 2: If $F(x_m) > 0$, x_m is infeasible.



<u>Case 2.c:</u> If $g_{min} \le h_{max}$, and $g_{max} \ge h_{min}$, then no feasible solution exists.



Prune-and-search approach

Input: Constraints: I₁: y ≥ a_ix + b_i, i = 1, 2, ..., n₁ I₂: y ≤ a_ix + b_i, i = n₁+1, n₁+2, ..., n. a ≤ x ≤ b
Output: The value x₀ such that y is minimized at x₀ subject to the above constraints.
Step 1: Arrange the constraints in I₁ and I₂ into arbitrary disjoint pairs respectively. For each pair, if a_ix + b_i is parallel to a_ix + b_j, delete a_ix + b_i if b_i < b_i for i, j∈I₁ or b_i > b_i for i, j∈I₂. Otherwise, find the intersection p_{ij} of y = a_ix + b_i and y = a_jx + b_j. Let the xcoordinate of p_{ij} be x_{ij}. <u>Step 2:</u> Find the median x_m of x_{ij} 's (at most $\left\lfloor \frac{n}{2} \right\rfloor$ points).

Step 3:

- a. If x_m is optimal, report this and exit.
- b. If no feasible solution exists, report this and exit.
- c. Otherwise, determine whether the optimum solution lies to the left, or right, of x_m .
- Step 4: Discard at least 1/4 of the constraints. Go to Step 1.
- Time complexity:

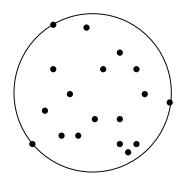
$$T(n) = T(3n/4)+O(n)$$

= O(n)

6 -30

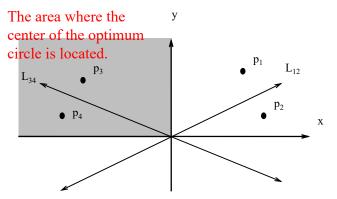
The 1-center problem

 Given n planar points, find a <u>smallest</u> <u>circle</u> to cover these n points.



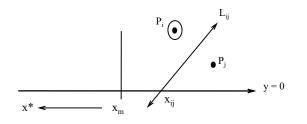
The pruning rule

- $\rm L_{1\,2}$: bisector of segment connecting $\rho_{\rm 1}$ and $\rho_{\rm 2}$,
- L_{34} : bisector of segments connecting p_3 and p_4
- ${\rm P}_{\rm 1}\,{\rm can}$ be eliminated without affecting our solution.



The constrained 1-center problem

The center is restricted to lying on a straight line.



6 -33

- Step 4: Find the median of the $\left\lfloor \frac{n}{2} \right\rfloor x_{i,i+1}$'s. Denote it as x_{m} .
- <u>Step 5:</u> Calculate the distance between p_i and x_m for all i. Let p_j be the point which is <u>farthest</u> from x_m . Let x_j denote the projection of p_j onto y = y'. If x_j is to the left (right) of x_m , then the optimal solution, x^* , must be to the left (right) of x_m .
- Step 6: If $x^* < x_m$, for each $x_{i,i+1} > x_m$, prune the point p_i if p_i is <u>closer</u> to x_m than p_{i+1} , otherwise prune the point p_{i+1} ;
 - If $x^* > x_m$, do similarly.
- Step 7: Go to Step 1.
- Time complexity

$$T(n) = T(3n/4)+O(n)$$

= O(n)

Prune-and-search approach

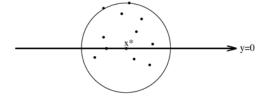
- Input : n points and a straight line y = y'.
- <u>Output:</u> The constrained center on the straight line y = y'.
- Step 1: If n is no more than 2, solve this problem by a brute-force method.
- Step 2: Form disjoint pairs of points (p_1, p_2) , (p_3, p_4) , ..., (p_{n-1}, p_n) . If there are odd number of points, just let the final pair be (p_n, p_1) .
- Step 3: For each pair of points, (p_i, p_{i+1}) , find the point $x_{i,i+1}$ on the line y = y' such that $d(p_i, x_{i,i+1}) = d(p_{i+1}, x_{i,i+1})$.

6 -34

6 - 36

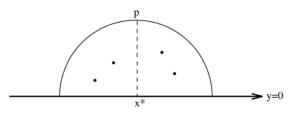
The general 1-center problem

- By the <u>constrained 1-center</u> algorithm, we can determine the center $(x^*, 0)$ on the line y=0.
- We can do more
 - Let (x_s, y_s) be the center of the <u>optimum circle</u>.
 - We can determine whether $y_s > 0$, $y_s < 0$ or $y_s = 0$.
 - Similarly, we can also determine whether x_s > 0, x_s < 0 or x_s = 0



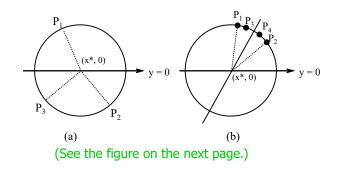
The sign of optimal y

- Let I be the set of points which are <u>farthest</u> from (x*, 0).
- <u>Case 1</u>: I contains one point P = (x_p, y_p) . y_s has the <u>same sign</u> as that of y_p .



6 -37

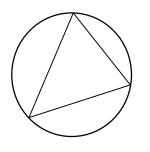
• Case 2 : I contains more than one point. Find the smallest arc spanning all points in I. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be the two end points of the smallest spanning arc. If this arc $\ge 180^\circ$, then $y_s = 0$. else y_s has the same sign as that of $\frac{y_1 + y_2}{2}$.



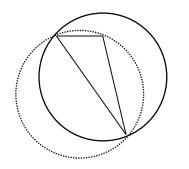
Optimal or not optimal

• an acute triangle:

an obtuse triangle:

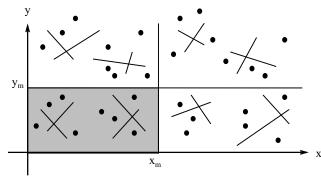


The circle is optimal.



The circle is not optimal.

An example of 1-center problem



- One point for each of n/4 intersections of L_{i+} and L_{i-} is pruned away.
- Thus, <u>n/16 points are pruned away in each iteration</u>.

6 -39

Prune-and-search approach

- Input: A set $S = \{p_1, p_2, ..., p_n\}$ of n points.
- Output: The smallest enclosing circle for S.
- Step 1: If S contains no more than 16 points, solve the problem by a brute-force method.

Step 2: Form disjoint pairs of points, (p_1, p_2) , (p_3, p_4) , ..., (p_{n-1}, p_n) . For each pair of points, (p_i, p_{i+1}) , find the perpendicular bisector of line segment $p_i p_{i+1}$. Denote them as $L_{i/2}$, for i = 2, 4, ..., n, and compute their slopes. Let the slope of L_k be denoted as s_k , for k = 1, 2, 3, ..., n/2.

6 -41

Step 3: Compute the median of s_k 's, and denote it by s_m . Step 4: Rotate the coordinate system so that the x-axis coincide with $y = s_m x$. Let the set of L_k 's with positive (negative) slopes be I⁺ (I⁻). (Both of them are of size n/4.) Step 5: Construct disjoint pairs of lines, (L_{i+}, L_{i-}) for i = 1, 2, ..., n/4, where $L_{i+} \in I^+$ and $L_{i-} \in$ I⁻. Find the intersection of each pair and denote it by (a_i, b_i) , for i = 1, 2, ..., n/4.

6 -42

Step 6: Find the median of b_i 's. Denote it as y*. Apply the constrained 1-center subroutine to S, requiring that the center of circle be located on y=y*. Let the solution of this constrained 1-center problem be (x', y*). Step 7: Determine whether (x', y*) is the optimal solution. If it is, exit; otherwise, record $y_s > y^*$ or $y_s < y^*$.

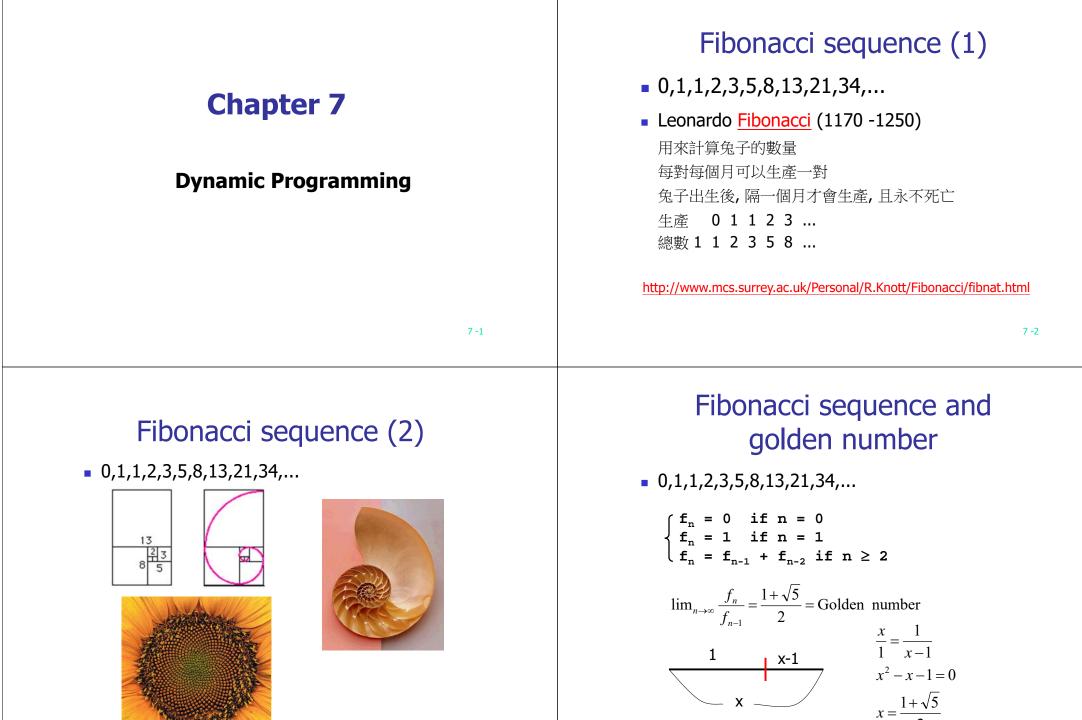
- <u>Step 8:</u> If $y_s > y^*$, find the median of a's for those (a_i, b_i) 's where $b_i < y^*$. If $y_s < y^*$, find the median of a_i 's of those t hose (a_i, b_i) 's where $b_i >$ y^* . Denote the median as x^* . Apply the constrained 1-center algorithm to S, requiring that the center of circle be located on $x = x^*$. Let the solution of this contained 1-center problem be (x^*, y') .
- <u>Step 9</u>: Determine whether (x*, y') is the optimal solution. If it is, exit; otherwise, record x_s > x* and x_s < x*.

Step 10:

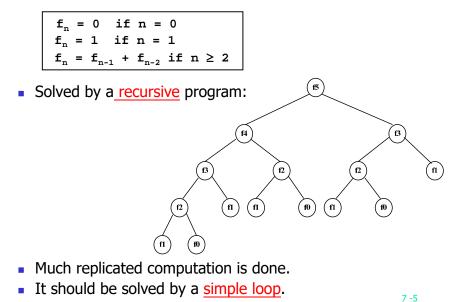
- Case 1: x_s < x* and y_s < y*. Find all (a_i, b_i)'s such that a_i > x* and b_i > y*. Let (a_i, b_i) be the intersection of L_{i+} and L_{i-}. Let L_{i-} be the bisector of p_j and p_k. Prune away p_j(p_k) if p_j(p_k) is closer to (x*, y*) than p_k(p_j).
- <u>Case 2</u>: $x_s > x^*$ and $y_s > y^*$. Do similarly.
- Case 3: $x_s < x^*$ and $y_s > y^*$. Do similarly.
- Case 4: $x_s > x^*$ and $y_s < y^*$. Do similarly.
- Step 11: Let S be the set of the remaining points. Go to Step 1.
- Time complexity :

$$T(n) = T(15n/16)+O(n)$$

= O(n)



Computation of Fibonacci sequence



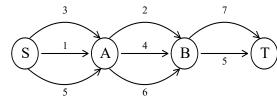
Dynamic Programming

 Dynamic Programming is an algorithm design method that can be used when the solution to a problem may be viewed as the result of a sequence of decisions

7 -6

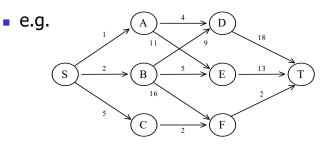
The shortest path

• To find a shortest path in a multi-stage graph

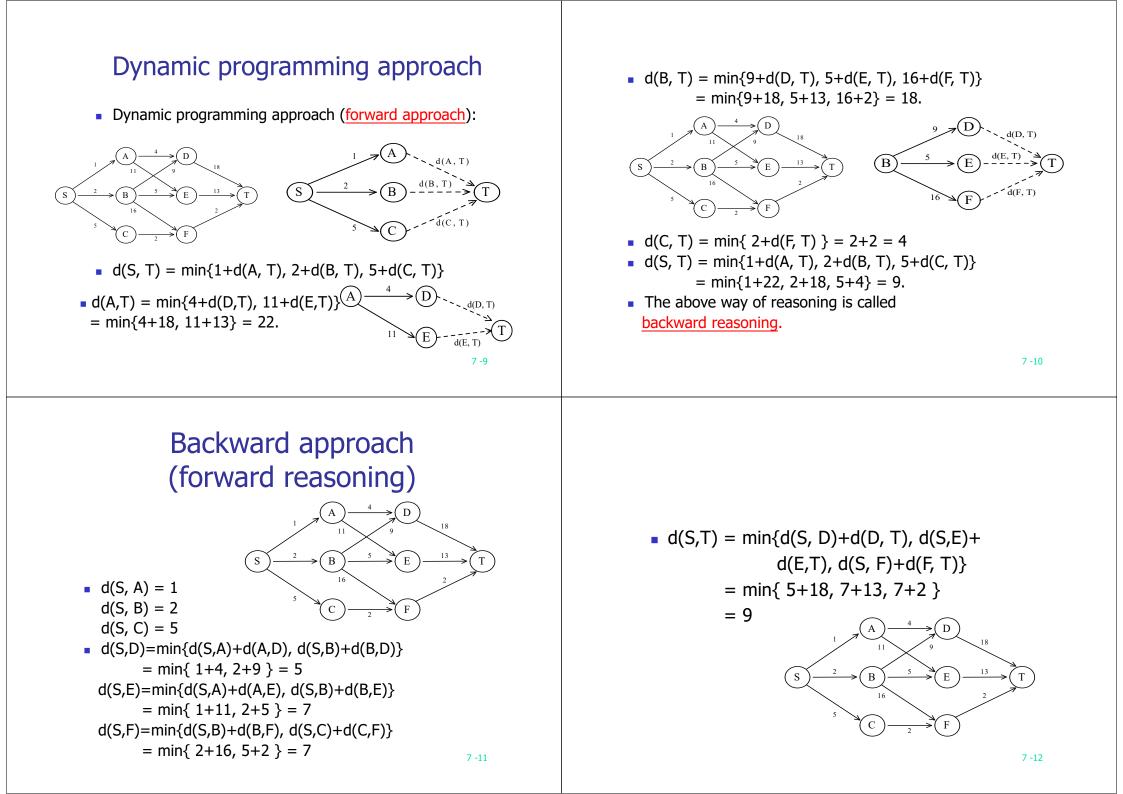


 Apply the greedy method : the shortest path from S to T : 1 + 2 + 5 = 8

The shortest path in multistage graphs



- The <u>greedy method can not</u> be applied to this case: (S, A, D, T) 1+4+18 = 23.
- The real shortest path is:
 (S, C, F, T) 5+2+2 = 9.



Principle of optimality

• Principle of optimality: Suppose that in solving a problem, we have to make a sequence of decisions $D_1, D_2, ..., D_n$. If this sequence is optimal, then the last k decisions, 1 < k < n must be optimal.

 e.g. the shortest path problem
 If i, i₁, i₂, ..., j is a shortest path from i to j, then i₁, i₂, ..., j must be a shortest path from i₁ to j

 In summary, if a problem can be described by a multistage graph, then it can be solved by dynamic programming.

7 -13

Dynamic programming

- Forward approach and backward approach:
 - Note that if the recurrence relations are formulated using the forward approach then the relations are solved backwards . i.e., beginning with the last decision
 - On the other hand if the relations are formulated using the backward approach, they are solved forwards.
- To solve a problem by using dynamic programming:
 - Find out the recurrence relations.
 - Represent the problem by a multistage graph.

7 -14

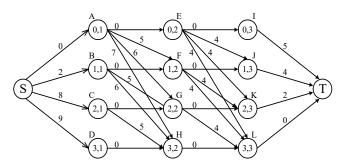
The resource allocation problem

- m resources, n projects
- profit $P_{i, j}$: j resources are allocated to project i.

maximize the total profit.

| Resource | | | |
|----------|---|---|---|
| Project | 1 | 2 | 3 |
| 1 | 2 | 8 | 9 |
| 2 | 5 | 6 | 7 |
| 3 | 4 | 4 | 4 |
| 4 | 2 | 4 | 5 |

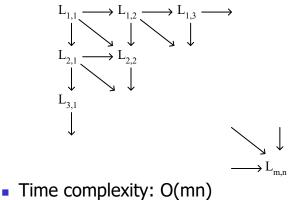
The multistage graph solution

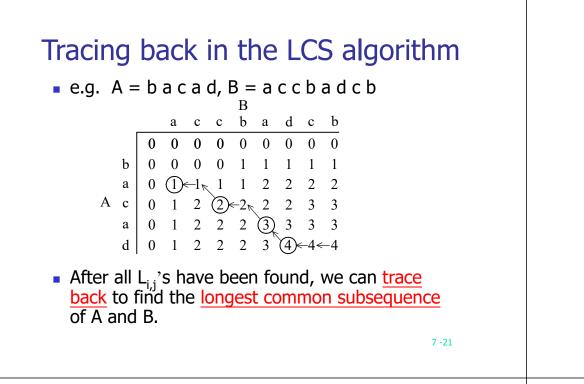


- The resource allocation problem can be described as a multistage graph.
- (i, j) : i resources allocated to projects 1, 2, ..., j

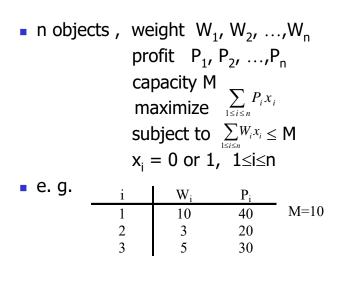
e.g. node H=(3, 2): 3 resources allocated to projects 1, 2.

- The longest common subsequence (LCS) problem Find the longest path from S to T : A string : A = b a c a d (S, C, H, L, T), 8+5+0+0=13 • A subsequence of A: deleting 0 or more 2 resources allocated to project 1. symbols from A (not necessarily consecutive). 1 resource allocated to project 2. e.g. ad, ac, bac, acad, bacad, bcd. 0 resource allocated to projects 3, 4. Common subsequences of A = b a c a d and B = a c c b a d c b : ad, ac, bac, acad.The longest common subsequence (LCS) of A and B: a cad. 7 -17 7 -18 The LCS algorithm The dynamic programming approach for solving the LCS problem: • Let $A = a_1 a_2 \dots a_m$ and $B = b_1 b_2 \dots b_n$ $\hfill \mbox{Let}\ L_{i,j}$ denote the length of the longest
 - Let $L_{i,j}$ denote the length of the longest common subsequence of $a_1 \ a_2 \ \ldots \ a_i$ and $b_1 \ b_2 \ \ldots \ b_{j.}$
 - $L_{i,j} = \begin{cases} L_{i-1,j-1} + 1 & \text{if } a_i = b_j \\ max\{ L_{i-1,j}, L_{i,j-1} \} & \text{if } a_i \neq b_j \\ L_{0,0} = L_{0,j} = L_{i,0} = 0 & \text{for } 1 \le i \le m, \ 1 \le j \le n. \end{cases}$



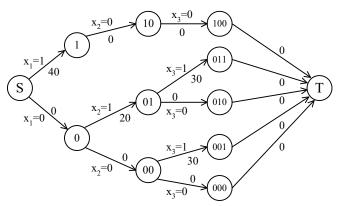


0/1 knapsack problem



The multistage graph solution

 The 0/1 knapsack problem can be described by a multistage graph.



The dynamic programming approach

The longest path represents the optimal solution:

$$x_1 = 0, x_2 = 1, x_3 = 1$$

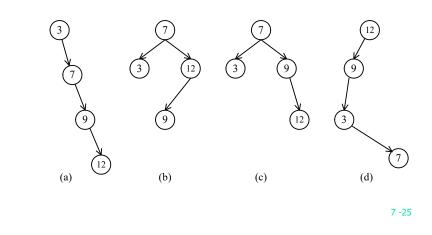
 $\sum_{i=1}^{n} P_i x_i = 20 + 30 = 50$

- Let f_i(Q) be the value of an optimal solution to objects 1,2,3,...,i with capacity Q.
- $f_i(Q) = \max\{ f_{i-1}(Q), f_{i-1}(Q-W_i)+P_i \}$
- The optimal solution is f_n(M).

7 -23

Optimal binary search trees

• e.g. binary search trees for 3, 7, 9, 12;

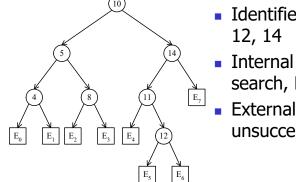


Optimal binary search trees

• n identifiers : $a_1 < a_2 < a_3 < ... < a_n$ P_i, $1 \le i \le n$: the probability that a_i is searched. Q_i, $0 \le i \le n$: the probability that x is searched where $a_i < x < a_{i+1}$ ($a_0 = -\infty$, $a_{n+1} = \infty$).

 $\sum_{i=1}^{n} P_i + \sum_{i=1}^{n} Q_i = 1$

7 -26



- Identifiers : 4, 5, 8, 10, 11, 12, 14
- Internal node : successful search, P_i
- External node : unsuccessful search, Q_i

•The expected cost of a binary tree: $\sum_{n=1}^{n} P_{n} * \text{level}(a_{n}) + \sum_{n=1}^{n} O_{n} * (\text{level}(E_{n}) - 1)$

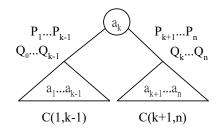
$$\sum_{n=1}^{\infty} P_i * \text{Ievel}(a_i) + \sum_{n=0}^{\infty} Q_i * (\text{Ievel}(E_i) - E_i)$$

The level of the root : 1

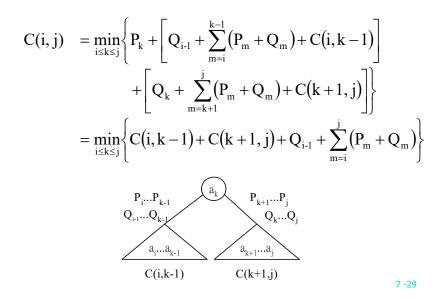
The dynamic programming approach

- Let C(i, j) denote the cost of an optimal binary search tree containing a_i,...,a_i.
- The cost of the optimal binary search tree with a_k as its root :

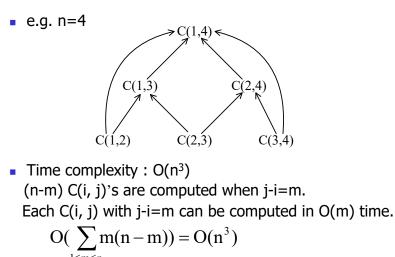
 $C(1,n) = \min_{1 \le k \le n} \left\{ P_k + \left[Q_0 + \sum_{m=1}^{k-1} (P_m + Q_m) + C(1,k-1) \right] + \left[Q_k + \sum_{m=k+1}^n (P_m + Q_m) + C(k+1,n) \right] \right\}$



General formula



Computation relationships of subtrees

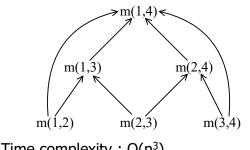


Matrix-chain multiplication

- n matrices A₁, A₂, ..., A_n with size p₀ × p₁, p₁ × p₂, p₂ × p₃, ..., p_{n-1} × p_n To determine the multiplication order such that # of scalar multiplications is minimized.
- To compute $A_i \times A_{i+1},$ we need $p_{i\text{-}1} p_i p_{i+1}$ scalar multiplications.

e.g. n=4, A₁:
$$3 \times 5$$
, A₂: 5×4 , A₃: 4×2 , A₄: 2×5
((A₁ × A₂) × A₃) × A₄, # of scalar multiplications:
 $3 * 5 * 4 + 3 * 4 * 2 + 3 * 2 * 5 = 114$
(A₁ × (A₂ × A₃)) × A₄, # of scalar multiplications:
 $3 * 5 * 2 + 5 * 4 * 2 + 3 * 2 * 5 = 100$
(A₁ × A₂) × (A₃ × A₄), # of scalar multiplications:
 $3 * 5 * 4 + 3 * 4 * 5 + 4 * 2 * 5 = 160$

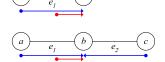
- Let m(i, j) denote the minimum cost for computing $\begin{array}{l} A_i \times A_{i+1} \times \ldots \times A_j \\ m(i,j) = \begin{cases} 0 & \text{if } i = j \\ \min_{i \leq k \leq j \cdot l} \{m(i,k) + m(k+1,j) + p_{i-l}p_kp_j\} & \text{if } i < j \end{cases}$
- Computation sequence :

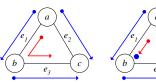


Time complexity : O(n³)

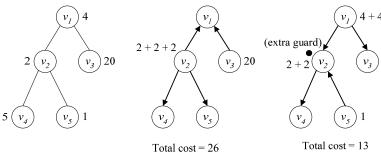
Single step graph edge searching

- <u>fugitive</u>: can move in any speed and is hidden in some edge of an undirected graph G=(V,E)
- edge searcher(guard): search an edge (u, v) from u to v, or stay at vertex u to prevent the fugitive passing through u
- <u>Goal</u>: to capture the fugitive in one step.
- no extra guards needed
- extra guards needed





The weighted single step graph edge searching problem on trees

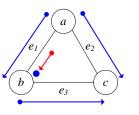


- *T*(*v_i*): the tree includes *v_i*, *v_j* (parent of *v_i*) and all descendant nodes of *v_i*.
- C(T(v_i), v_i, v_j): cost of an optimal searching plan with searching from v_i to v_j.
- $C(T(v_4), v_4, v_2) = 5$ $C(T(v_4), v_2, v_4) = 2$
- $C(T(v_2), v_2, v_1) = 6$ $C(T(v_2), v_1, v_2) = 9$

7 -35

7 -33

- cost of a searcher from u to v: wt(u) a guard staying at u: wt(u)
- Cost of the following: 2wt(a)+wt(b)+wt(b) (one extra guard stays at b)



- <u>Problem definition</u>: To arrange the searchers with the minimal cost to capture the fugitive in one step.
- <u>NP-hard</u> for general graphs; <u>P</u> for trees.

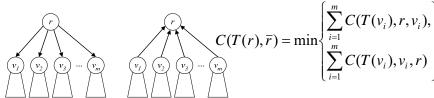
7 -34

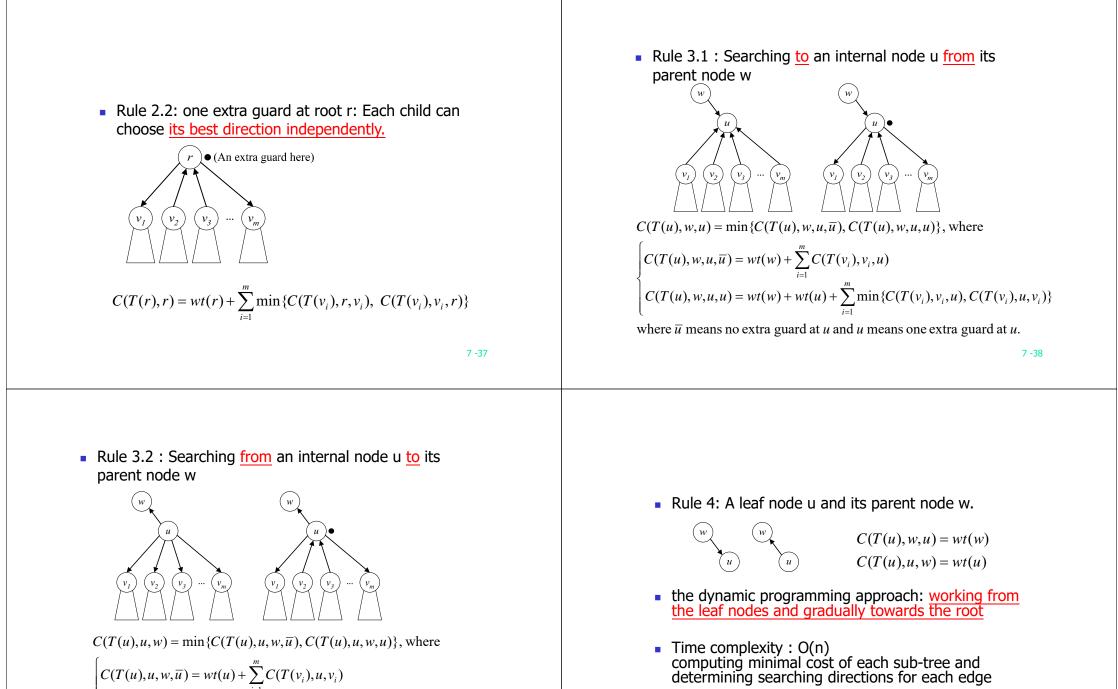
The dynamic programming approach

Rule 1: optimal total cost

 $C(T(r)) = \min\{C(T(r), \bar{r}), C(T(r), r)\},\$ where $C(T(r), \bar{r})$: no extra guard at root rC(T(r), r): one extra guard at root r

 Rule 2.1 : no extra guard at root r: All children must have <u>the same searching direction.</u>





$$C(T(u), u, w, u) = 2wt(u) + \sum_{i=1}^{m} \min\{C(T(v_i), v_i, u), C(T(v_i), u, v_i)\}$$

| <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><text></text></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header> | <text><list-item><list-item><list-item><list-item><list-item><list-item></list-item></list-item></list-item></list-item></list-item></list-item></text> |
|--|--|
| Definition of reduction: Problem A reduces to problem B (A ∝ B) iff A can be solved by a deterministic polynomial time algorithm using a deterministic algorithm that solves B in polynomial time. Up to now, none of the NPC problems can be solved by a deterministic polynomial time algorithm in the worst case. | The theory of NP-completeness always considers the <u>worst case</u>. The lower bound of any NPC problem <u>seems</u> to be in the order of an exponential function. Not all NP problems are difficult. (e.g. the MST problem is an NP problem.) If A, B ∈ NPC, then A ∞ B and B ∞ A. |

Theory of NP-completeness:

If any NPC problem can be solved in polynomialtime, then all NP problems can be solved inpolynomial time.(NP = P)

 It does not <u>seem</u> to have any polynomial time algorithm to solve the NPC problems.

Decision problems

- The solution is simply "Yes" or "No".
- Optimization problems are more difficult.
- e.g. the traveling salesperson problem
 - <u>Optimization</u> version:
 Find the shortest tour
 - Decision version:
 - Is there a tour whose total length is less than or equal to a constant c?

Solving an optimization problem by a decision algorithm :

- - We can easily find the smallest c_i

8- 5

The satisfiability problem

- The <u>satisfiability</u> problem
 - The logical formula :

x₁ v x₂ v x₃

& - x₂

the assignment :

 $\begin{array}{l} x_1 \leftarrow \mathsf{F} \ , \ x_2 \leftarrow \mathsf{F} \ , \ x_3 \leftarrow \mathsf{T} \\ \text{will make the above formula true }. \\ (-x_1, \ -x_2 \ , \ x_3) \ \text{represents} \ \ x_1 \leftarrow \mathsf{F} \ , \ x_2 \leftarrow \mathsf{F} \ , \ x_3 \leftarrow \mathsf{T} \end{array}$

- If there is <u>at least one</u> assignment which satisfies a formula, then we say that this formula is <u>satisfiable</u>; otherwise, it is <u>unsatisfiable</u>.
- An unsatisfiable formula :
 - $x_1 \vee x_2$ & $x_1 \vee -x_2$ & $-x_1 \vee x_2$ & $-x_1 \vee -x_2$

- Definition of the satisfiability problem: Given a <u>Boolean formula</u>, determine whether this formula is <u>satisfiable</u> or not.
- A literal : x_i or $-x_i$
- A <u>clause</u> : $x_1 v x_2 v x_3 \equiv C_i$
- A formula : conjunctive normal form (CNF)

$$C_1 \& C_2 \& \dots \& C_m$$

The resolution principle

Resolution principle

- $C_1 : x_1 v x_2$
- $C_2 : -x_1 \vee x_3$
- $\Rightarrow C_3 : x_2 \vee x_3$ From C. & C.
- From C₁ & C₂, we can obtain C₃, and C₃ can be added into the formula.
- The formula becomes:
 C₁ & C₂ & C₃

| x ₁ | x ₂ | X ₃ | $C_1 \& C_2$ | C ₃ |
|-----------------------|----------------|-----------------------|--------------|----------------|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 |

8-10

- Another example of resolution principle
 - $\mathsf{C}_1: \mathsf{-x}_1 \lor \mathsf{-x}_2 \lor \mathsf{x}_3$
 - $C_2 : x_1 v x_4$
 - $\Rightarrow C_3 : \textbf{-}x_2 \ v \ x_3 \ v \ x_4$
- If no new clauses can be deduced, then it is <u>satisfiable.</u>

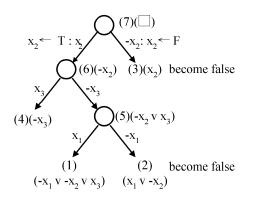
| -x ₁ | v -x ₂ v x ₃ | (1) |
|-----------------------|------------------------------------|-----|
| x ₁ | | (2) |
| X ₂ | | (3) |
| (1) & (2) | -x ₂ v x ₃ | (4) |
| (4) & (3) | X ₃ | (5) |
| (1) & (3) | -x ₁ v x ₃ | (6) |

 If an empty clause is deduced, then it is <u>unsatisfiable</u>.

| (1) |
|----------------------|
| (2) |
| (3) |
| (4) |
| |
| ′ x ₃ (5) |
| (6) |
| (7) |
| |

Semantic tree

- In a <u>semantic tree</u>, each path from the root to a leaf node represents a class of assignments.
- If each leaf node is attached with a clause, then it is <u>unsatisfiable</u>.



8- 13

Decision problems

- Decision version of sorting:
 - Given $a_1, a_2, ..., a_n$ and c, is there a permutation of a_i 's (a_1 ', a_2 ', ..., a_n ') such that $|a_2$ '- a_1 ' | + | a_3 '- a_2 ' | + ... + | a_n '- a_{n-1} ' | < c?
- Not all decision problems are NP problems
 - E.g. halting problem :
 - Given a program with a certain input data, will the program terminate or not?
 - NP-hard
 - Undecidable

Nondeterministic operations and functions

Nondeterministic algorithms

algorithm is of polynomial time-complexity, then

this algorithm is called an NP (nondeterministic

NP problems : (must be decision problems)

traveling salesperson problem (TSP)

satisfiability problem (SAT)

A nondeterminstic algorithm consists of

• If the checking stage of a nondeterministic

phase 1: quessing

phase 2: checking

polynomial) algorithm.

sorting

searching, MST

[Horowitz 1998]

e.a.

- Choice(S) : arbitrarily chooses one of the elements in set S
- Failure : an unsuccessful completion
- Success : a successful completion
- Nonderministic searching algorithm:

 $j \leftarrow choice(1 : n) /* guessing */$

if A(j) = x then success /* checking */ else failure

- A <u>nondeterministic</u> algorithm terminates unsuccessfully iff there does not exist a set of choices leading to a success signal.
- The time required for *choice*(1 : n) is O(1).
- A deterministic interpretation of a nondeterministic algorithm can be made by allowing <u>unbounded parallelism</u> in computation.

Nondeterministic sorting

 $B \leftarrow 0$ /* guessing */ for i = 1 to n do $i \leftarrow choice(1:n)$ if $B[j] \neq 0$ then failure B[i] = A[i]/* checking */ for i = 1 to n-1 do if B[i] > B[i+1] then failure success

8- 17

Nondeterministic SAT

/* guessing */
for i = 1 to n do
 x_i ← choice(true, false)
/* checking */
if E(x₁, x₂, ..., x_n) is true then success
else failure

Cook's theorem

$\frac{NP = P \text{ iff the satisfiability}}{problem \text{ is a P problem.}}$

- SAT is NP-complete.
- It is the first NP-complete problem.
- Every NP problem reduces to SAT.



Stephen Arthur Cook (1939~)

Transforming searching to SAT

Does there exist a number in { x(1), x(2), ..., x(n) }, which is equal to 7?
Assume n = 2.

nondeterministic algorithm:

i = choice(1,2)

if x(i)=7 then SUCCESS

else FAILURE

8- 21

$\begin{array}{l} i=1 \ v \ i=2 \\ \& \ i=1 \rightarrow i \neq 2 \\ \& \ i=2 \rightarrow i \neq 1 \\ \& \ x(1)=7 \ \& \ i=1 \qquad \rightarrow \ SUCCESS \\ \& \ x(2)=7 \ \& \ i=2 \qquad \rightarrow \ SUCCESS \\ \& \ x(1) \neq 7 \ \& \ i=1 \qquad \rightarrow \ FAILURE \\ \& \ x(2) \neq 7 \ \& \ i=2 \qquad \rightarrow \ FAILURE \\ \& \ FAILURE \qquad \rightarrow \ -SUCCESS \\ \& \ SUCCESS \ (Guarantees a successful termination) \\ \& \ x(1)=7 \quad (Input \ Data) \\ \& \ x(2) \neq 7 \end{array}$

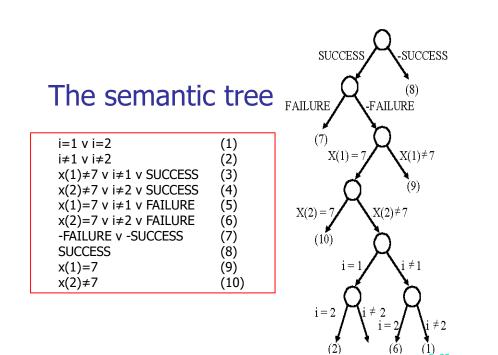
8- 22

| CNF | (con | junctive | normal | form) | : |
|------|------|----------|--------|-------|---|
| :-1: | | | | (1) | |

| 1=1 v = 2 | | (1) |
|------------------------------------|-----|------|
| $i \neq 1 v i \neq 2$ | | (2) |
| $x(1) \neq 7 v i \neq 1 v SUCCESS$ | | (3) |
| $x(2) \neq 7 v i \neq 2 v SUCCESS$ | | (4) |
| $x(1)=7 v i \neq 1 v FAILURE$ | | (5) |
| $x(2)=7 v i \neq 2 v FAILURE$ | | (6) |
| -FAILURE v -SUCCESS | (7) | |
| SUCCESS | | (8) |
| x(1)=7 | | (9) |
| $\mathbf{x}(2) \neq 7$ | | (10) |
| | | |

Satisfiable at the following assignment :

| i=1 | satisfying | (1) |
|---------------|------------|------------------|
| i≠2 | satisfying | (2), (4) and (6) |
| SUCCESS | satisfying | (3), (4) and (8) |
| -FAILURE | satisfying | (7) |
| x(1)=7 | satisfying | (5) and (9) |
| $x(2) \neq 7$ | satisfying | (4) and (10) |



Searching for 7, but $x(1) \neq 7$, $x(2) \neq 7$

• CNF (conjunctive normal form) :

| i=1 v | i=2 | | | (1) |
|------------------------|---------|--------|---------|------|
| i≠1 v | i≠2 | | | (2) |
| x(1)≠7 | v i≠ | =1 v | SUCCESS | (3) |
| x(2)≠7 | v i≠ | =2 v | SUCCESS | (4) |
| x(1)=7 | v i≠ | =1 v | FAILURE | (5) |
| x(2)=7 | v i≠ | =2 v | FAILURE | (6) |
| SUCCES | S | | | (7) |
| -SUCCES | SS v -F | AILURE | | (8) |
| $x(1) \neq 7$ | | | | (9) |
| $\mathbf{x}(2) \neq 7$ | | | | (10) |

8-26

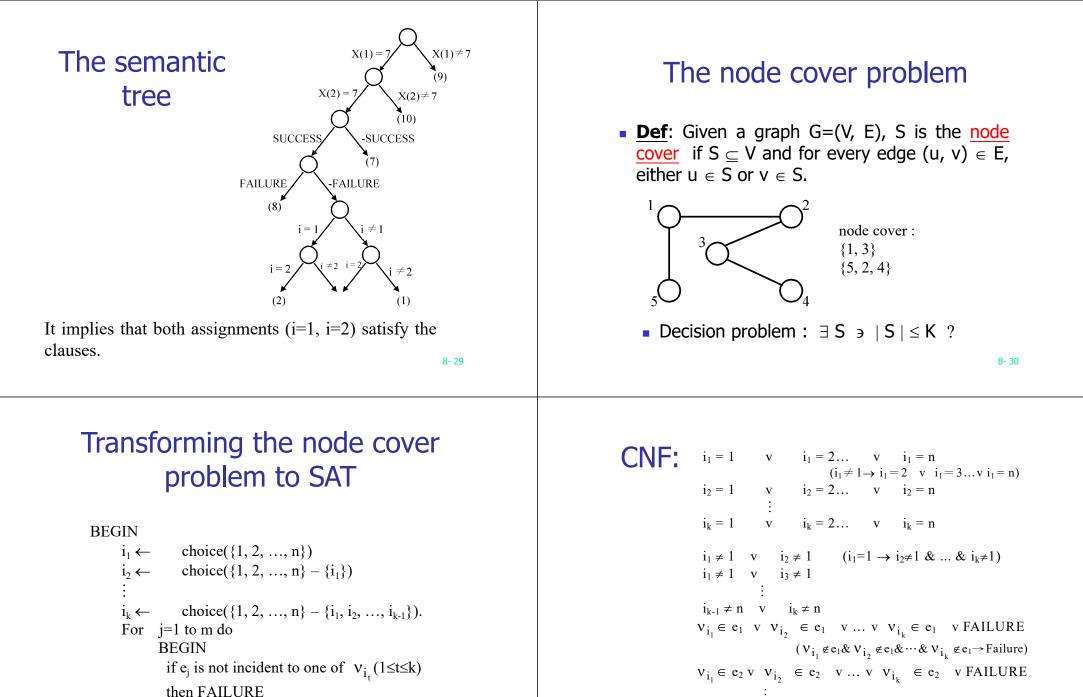
• Apply resolution principle :

| (9) & (5) | i≠1 v FAILURE | (11) | | |
|--|---------------|------|--|--|
| (10) & (6) | i≠2 v FAILURE | (12) | | |
| (7) & (8) | -FAILURE | (13) | | |
| (13) & (11) | i≠1 | (14) | | |
| (13) & (12) | i≠2 | (15) | | |
| (14) & (1) | i=2 | (11) | | |
| (15) & (16) | | (17) | | |
| We get an empty clause \Rightarrow unsatisfiable | | | | |
| \Rightarrow 7 does not exit in x(1) or x(2). | | | | |

Searching for 7, where x(1)=7, x(2)=7

CNF:

| i=1 | v i | =2 | | | (1) |
|----------------|-------|-------|------|---------|------|
| i≠1 | v i | ≠2 | | | (2) |
| x (1)≠7 | v | i≠1 | V | SUCCESS | (3) |
| x(2)≠7 | v | i≠2 | V | SUCCESS | (4) |
| x (1)=7 | v | i≠1 | V | FAILURE | (5) |
| x(2)=7 | v | i≠2 | V | FAILURE | (6) |
| SUCCI | ESS | | | | (7) |
| -SUCC | ESS v | -FAII | LURE | | (8) |
| x(1)=7 | | | | | (9) |
| x(2) = 7 | | | | | (10) |



END

SUCCESS

(To be continued)

 $v_{i_1} \in e_m v v_{i_2} \in e_m v \dots v v_{i_k} \in e_m v \text{ FAILURE}$

SUCCESS

| -SUCCESS v -FAILURE $v_{r_1} \in e_1$ $v_{s_1} \in e_1$ $v_{r_2} \in e_2$ $v_{s_2} \in e_2$ \vdots $v_{r_m} \in e_m$ $v_{s_m} \in e_m$ | | (1) SAT has an NP algorithm. (2) SAT is NP-hard: Every NP algorithm for problem <i>A</i> can be transformed in polynomial time to SAT [Horowitz 1998] such that SAT is satisfiable if and only if the answer for <i>A</i> is "YES". That is, every NP problem ∝ SAT . By (1) and (2), SAT is NP-complete. |
|---|-------|---|
| | 8- 33 | 8- 34 |

Proof of NP-Completeness

- To show that A is NP-complete
 (I) Prove that A is an NP problem.
 (II) Prove that ∃ B ∈ NPC, B ∝ A.
 ⇒ A ∈ NPC
- Why ?

3-satisfiability problem (3-SAT)

SAT is NP-complete

- **Def**: Each clause contains <u>exactly three</u> literals.
- (I) 3-SAT is an NP problem (obviously)
- (II) SAT ∞ 3-SAT
 - Proof:
 - (1) One literal L_1 in a clause in SAT :
 - in 3-SAT : $L_1 v y_1 v y_2$ $L_1 v -y_1 v y_2$ $L_1 v y_1 v -y_2$ $L_1 v -y_1 v -y_2$ $L_1 v -y_1 v -y_2$

(2) Two literals L_1 , L_2 in a clause in SAT : in 3-SAT : $L_1 \vee L_2 \vee Y_1$ $L_1 \vee L_2 \vee -y_1$

(3) Three literals in a clause : remain unchanged.

(4) More than 3 literals $L_1, L_2, ..., L_k$ in a clause : in 3-SAT : $L_1 \vee L_2 \vee Y_1$ $L_{3} v - y_{1} v y_{2}$ $L_{k-2} \vee -y_{k-4} \vee y_{k-3}$ $L_{k-1} \vee L_k \vee -Y_{k-3}$

8-37

Example of transforming SAT to 3-SAT

| • An instance S in SAT : | The insta | ance S' in 3-SAT : |
|---|------------------------|-------------------------------------|
| x ₁ v x ₂ | x_1 | v x ₂ v y ₁ |
| -X ₃ | X_1 | v x ₂ v -y ₁ |
| $x_1 v - x_2 v x_3 v - x_4 v x_5 v x_6$ | -x ₃ | v y ₂ v y ₃ |
| | -x ₃ | v -y ₂ v y ₃ |
| | -x ₃ | v y ₂ v -y ₃ |
| | -x ₃ | v -y ₂ v -y ₃ |
| | x_1 | v -x ₂ v y ₄ |
| | x ₃ | v -y ₄ v y ₅ |
| | -x ₄ | v -y ₅ v y ₆ |
| | x ₅ | v x ₆ v -y ₆ |
| SAT transform | | 3-SAT |
| S | | → S′ |
| | | 8- 38 |

• Proof : S is satisfiable \Leftrightarrow S' is satisfiable "⇒"

```
\leq 3 literals in S (trivial)
consider \geq 4 literals
S: L_1 \vee L_2 \vee ... \vee L_k
S': L_1 \vee L_2 \vee y_1
     L_3 v - y_1 v y_2
     L_4 v - y_2 v y_3
     L_{k-2} v - y_{k-4} v y_{k-3}
     L_{k-1} \vee L_{k} \vee -Y_{k-3}
```

• S is satisfiable \Rightarrow at least L_i = T Assume : $L_i = F \forall j \neq i$ assign : $y_{i-1} = F$ $y_i = T \quad \forall j < i-1$ $y_i = F \quad \forall j > i-1$ $(:: L_i \vee - y_{i-2} \vee y_{i-1})$ \Rightarrow S' is satisfiable. ∎ "⊂" If S' is satisfiable, then assignment satisfying

S' can not contain y_i's only.

 \Rightarrow at least one L_i must be true.

(We can also apply the resolution principle).

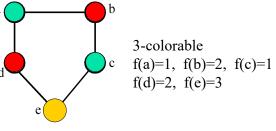
```
Thus, 3-SAT is NP-complete.
```

Comment for 3-SAT

 If a problem is NP-complete, its special cases may or may not be NP-complete.

Chromatic number decision problem (CN)

• **Def**: A <u>coloring</u> of a graph G=(V, E) is a function f: V \rightarrow { 1, 2, 3,..., k } such that if (u, v) \in E, then f(u) \neq f(v). The CN problem is to determine if G has a coloring for k.



<Theorem> Satisfiability with at most 3 literals per clause (SATY) \propto CN.

8- 42

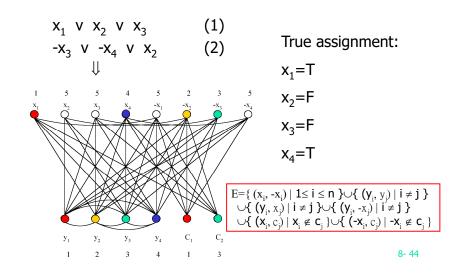
SATY \propto CN

Proof :

instance of SATY : variable : $x_1, x_2, ..., x_n, n \ge 4$ clause : $c_1, c_2, ..., c_r$ instance of CN : G=(V, E) $V=\{x_1, x_2, ..., x_n\} \cup \{-x_1, -x_2, ..., -x_n\}$ $\cup \{y_1, y_2, ..., y_n\} \cup \{c_1, c_2, ..., c_r\}$

 $\begin{array}{c} newly \text{ added} \\ E=\{ \; (x_i, -x_i) \mid 1 \le i \le n \; \} \cup \{ \; (y_i, \, y_j) \mid i \ne j \; \} \\ \cup \{ \; (y_i, \, x_j) \mid i \ne j \; \} \cup \{ \; (y_i, -x_j) \mid i \ne j \; \} \\ \cup \{ \; (x_i, \, c_j) \mid x_i \notin c_j \; \} \cup \{ \; (-x_i, \, c_j) \mid -x_i \notin c_j \; \} \end{array}$

Example of SATY \propto CN



Proof of SATY \propto CN

• Satisfiable \Leftrightarrow n+1 colorable

• "⇒" (1) $f(y_i) = i$ (2) if $x_i = T$, then $f(x_i) = i$, $f(-x_i) = n+1$ else $f(x_i) = n+1$, $f(-x_i) = i$ (3) if x_i in c_j and $x_i = T$, then $f(c_j) = f(x_i)$ if $-x_i$ in c_j and $-x_i = T$, then $f(c_j) = f(-x_i)$ (at least one such x_i)

8- 45

• " \Leftarrow " (1) y_i must be assigned with color i. (2) $f(x_i) \neq f(-x_i)$ either $f(x_i) = i$ and $f(-x_i) = n+1$ or $f(x_i) = n+1$ and $f(-x_i) = i$ (3) at most 3 literals in c_j and $n \ge 4$ \Rightarrow at least one $x_{i'} \ni x_i$ and $-x_i$ are not in c_j $\Rightarrow f(c_j) \neq n+1$ (4) if $f(c_j) = i = f(x_i)$, assign x_i to T if $f(c_j) = i = f(-x_i)$, assign $-x_i$ to T (5) if $f(c_i) = i = f(x_i) \Rightarrow (c_i, x_i) \notin E$

 $\Rightarrow x_i \text{ in } c_j \Rightarrow c_j \text{ is true}$ if f(c_i) = i = f(-x_i) \Rightarrow similarly

8-46

Set cover decision problem

• **<u>Def</u>:** $F = \{S_i\} = \{S_1, S_2, ..., S_k\}$ $\bigcup_{S_i \in F} S_i = \{u_1, u_2, ..., u_n\}$

T is a <u>set cover</u> of F if $T \subseteq F$ and $\bigcup_{S_i \in T} S_i = \bigcup_{S_i \in F} S_i$

- The <u>set cover decision problem</u> is to determine if F has a cover T containing no more than *c* sets.
- Example
 - $F = \{(u_1, u_3), (u_2, u_4), (u_2, u_3), (u_4), (u_1, u_3, u_4)\}$ $S_1 \qquad S_2 \qquad S_3 \qquad S_4 \qquad S_5$ $T = \{ s_1, s_3, s_4 \} \qquad \underline{set \ cover}$ $T = \{ s_1, s_2 \} \qquad set \ cover, \ \underline{exact \ cover}$

Exact cover problem

(Notations same as those in set cover.)

Def: To determine if F has an <u>exact cover</u> T, which is a cover of F and the sets in T are <u>pairwise disjoint</u>.

```
<Theorem> CN \propto exact cover
(No proof here.)
```

Sum of subsets problem

• **<u>Def</u>**: A set of positive numbers $A = \{a_1, b_2\}$ $a_2, ..., a_n$ a constant C Determine if $\exists A' \subseteq A \ni \sum_{i=1}^{n} a_i = C$ • e.g. A = { 7, 5, 19, 1, 12, 8, 14 }

•
$$C = 21$$
, $A' = \{ 7, 14 \}$

• C = 11, no solution

<Theorem > Exact cover \propto sum of subsets.

8-49

Exact cover \propto sum of subsets

• Proof :
instance of exact cover :

$$F = \{ S_1, S_2, ..., S_k \} \qquad \bigcup_{S_i \in F} S_i = \{ u_{1,} u_{2,} ..., u_n \}$$
instance of sum of subsets :

$$A = \{ a_1, a_2, ..., a_k \} \text{ where}$$

$$a_i = \sum_{1 \le j \le n} e_{ij}(k+1)^j \text{ where } e_{ij} = 1 \text{ if } u_j \in S_i$$

$$e_{ij} = 0 \text{ if otherwise.}$$

$$C = \sum_{1 \le j \le n} (k+1)^j = (k+1)((k+1)^n - 1)/k$$
• Why k+1? (See the example on the next page.)
8-50

Example of Exact cover ∞ sum of subsets

Valid transformation: Invalid transformation: $u_1=6, u_2=8, u_3=9, n=3$ EC: $S_1 = \{6, 8\}, S_2 = \{8\}, S_3 = \{8\}, S_3 = \{8\}, S_4 = \{8\}, S_$ EC: $S_1 = \{6,8\}, S_2 = \{9\}, S_3 = \{6,9\}, S_4 = \{8,9\}$ S₄={8,9}. K=4 Suppose k-2=2 is used. $\bigcup S_i = \{u_{1,1}, u_{2,1}, \dots, u_n\} = \{6, 8, 9\}$ SS: $a_1 = 2^1 + 2^2 = 6$ $a_2 = 2^2 = 4$ k=4 $a_3 = 2^2 = 4$ S: $a_1 = 5^1 + 5^2 = 30$ $a_2 = 5^3 = 125$ $a_4 = 2^2 + 2^3 = 12$ $a_3 = 5^1 + 5^3 = 130$ $C=2^{1}+2^{2}+2^{3}=14$ $a_4 = 5^2 + 5^3 = 150$ $C=5^{1}+5^{2}+5^{3}=155$

Partition problem

• **Def**: Given a set of positive numbers A = $\{a_1, a_2, ..., a_n\},\$ determine if \exists a partition P, $\ni \sum_{a_i \in P} a_i = \sum_{a_i \notin P} a_i$ • e. g. A = {3, 6, 1, 9, 4, 11} partition : {3, 1, 9, 4} and {6, 11}

<Theorem > sum of subsets ∞ partition

Sum of subsets \propto partition

proof:

instance of sum of subsets : $A = \{ a_1, a_2, \dots, a_n \}, C$ instance of partition : $B = \{ b_1, b_2, \dots, b_{n+2} \}, \text{ where } b_i = a_i, 1 \le i \le n$ $b_{n+1} = C+1$ $b_{n+2} = (\sum_{1 \le i \le n} a_i)+1-C$ $C = \sum_{a_i \in S} a_i \Leftrightarrow (\sum_{a_i \in S} a_i)+b_{n+2} = (\sum_{a_i \notin S} a_i)+b_{n+1}$ $\Leftrightarrow \text{ partition } : \{ b_i \mid a_i \in S \} \cup \{ b_{n+2} \}$ $and \{ b_i \mid a_i \notin S \} \cup \{ b_{n+1} \}$ Why b_{n+1} = C+1? why not b_{n+1} = C?
 To avoid b_{n+1} and b_{n+2} to be partitioned into the same subset.

8- 54

Bin packing problem

• <u>Def</u>: n items, each of size c_i , $c_i > 0$ Each bin capacity : C Determine if we can assign the items into k bins, $\Im \sum_{i \in \text{bin}_j} \leq C$, $1 \leq j \leq k$.

<Theorem> partition ∞ bin packing.

VLSI discrete layout problem

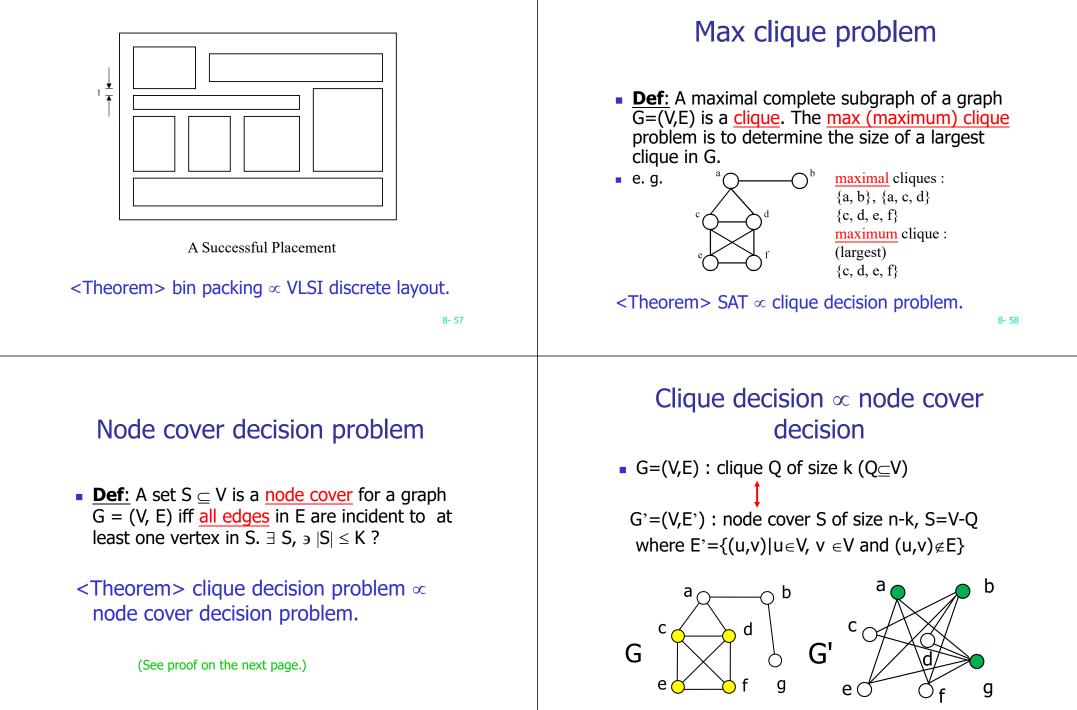
 Given: n rectangles, each with height h_i (integer) width w_i

and an area A

Determine if there is a <u>placement</u> of the n rectangles within the area A according to the rules :

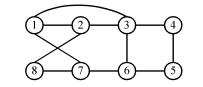
- 1. Boundaries of rectangles parallel to x axis or y axis.
- 2. Corners of rectangles lie on integer points.
- 3. No two rectangles overlap.
- 4. Two rectangles are separated by at least a unit distance.

(See the figure on the next page.)



Hamiltonian cycle problem

 Def: A <u>Hamiltonian cycle</u> is a round trip path along n edges of G which visits <u>every vertex</u> once and returns to its starting vertex.

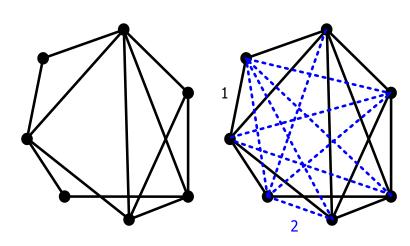


• e.g.

Hamiltonian cycle : 1, 2, 8, 7, 6, 5, 4, 3, 1. <Theorem> SAT ∞ directed Hamiltonian cycle (in a directed graph)

8- 61

Proof of Hamiltonian \propto TSP



Traveling salesperson problem

Def: A tour of a directed graph G=(V, E) is a directed cycle that includes every vertex in V. The problem is to find a tour of minimum cost.

<Theorem> Directed Hamiltonian cycle ∞ traveling salesperson decision problem. (See proof on the next page.)

8- 62

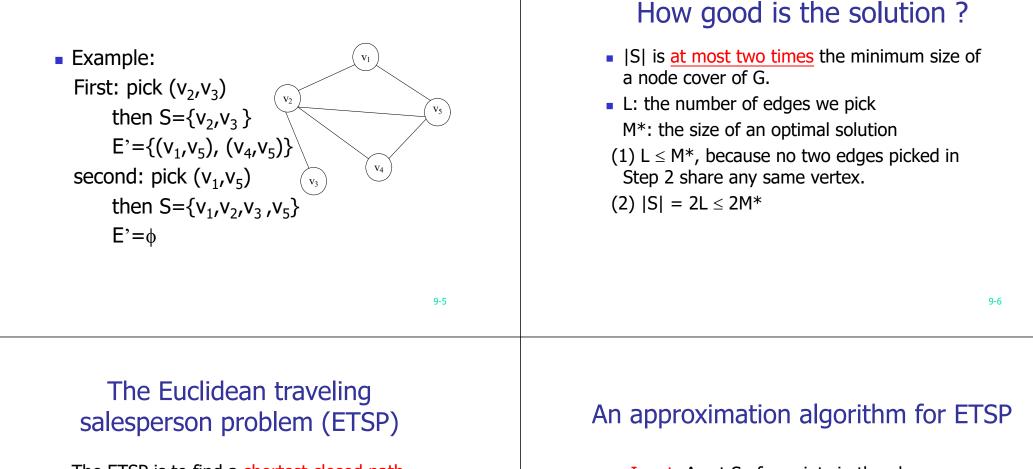
0/1 knapsack problem

- **Def:** n objects, each with a weight $w_i > 0$ a profit $p_i > 0$ capacity of knapsack : M Maximize $\sum_{1 \le i \le n} p_i x_i$ Subject to $\sum_{1 \le i \le n} w_i x_i \le M$ $x_i = 0 \text{ or } 1, 1 \le i \le n$ • Decision version : Given K, $\exists \sum_{1 \le i \le n} p_i x_i \ge K$? • Knapsack problem : $0 \le x_i \le 1, 1 \le i \le n$.
- <Theorem> partition \propto 0/1 knapsack decision problem.

- Refer to Sec. 11.3, Sec. 11.4 and its exercises of [Horowitz 1998] for the proofs of more NPcomplete problems.
 - [[Horowitz 1998] E. Howowitz, S. Sahni and S. Rajasekaran, *Computer Algorithms*, Computer Science Press, New York, 1998,「台北圖書」代理, 02-23625376

Approximation algorithm Up to now, the best algorithm for **Chapter 9** solving an NP-complete problem requires exponential time in the worst case. It is too time-consuming. **Approximation Algorithms** To reduce the time required for solving a problem, we can relax the problem, and obtain a feasible solution "close" to an optimal solution 9-1 An approximation algorithm The node cover problem • **<u>Def</u>**: Given a graph G=(V, E), S is the <u>node</u> Input: A graph G=(V,E). **cover** if $S \subset V$ and for every edge $(u, v) \in E$, Output: A node cover S of G. either $u \in \overline{S}$ or $v \in S$. Step 1: $S=\phi$ and E'=E. V_1 **Step 2:** While E' $\neq \phi$ Pick an arbitrary edge (a,b) in E'. The optimal solution: V_2 V_5 $S=S\cup\{a,b\}.$ $\{V_2, V_5\}$ $E'=E'-\{e | e is incident to a or b\}$ V۵ v_3 Time complexity: O(|E|) The node cover problem is NP-complete. 9-3

9-4



- The ETSP is to find a shortest closed path through a set S of n points in the plane.
- The ETSP is NP-hard.

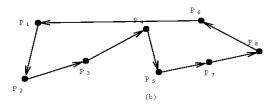
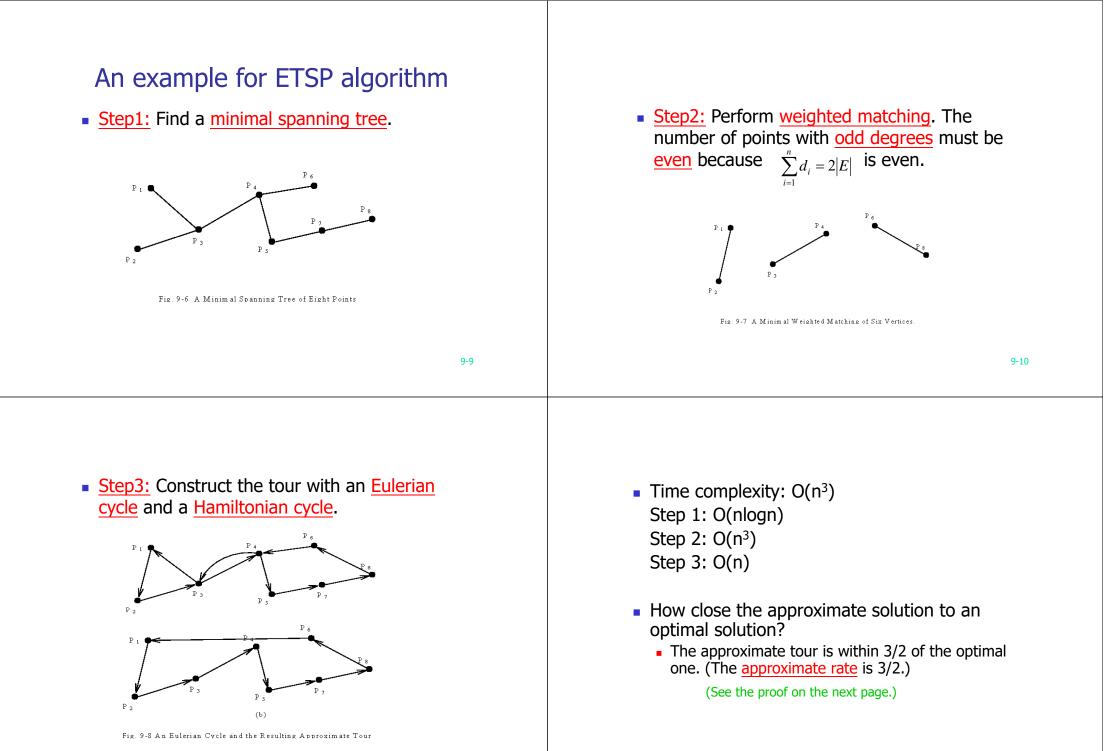
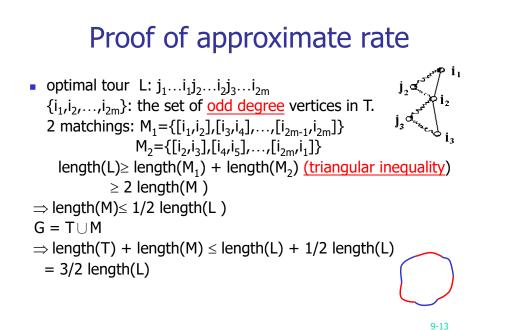


Fig. 9-8 An Eulerian Cycle and the Resulting Approximate Tour

- Input: A set S of n points in the plane.
- <u>Output</u>: An approximate traveling salesperson tour of S.
- Step 1: Find a minimal spanning tree T of S.
- Step 2: Find a minimal Euclidean weighted matching M on the set of vertices of odd degrees in T. Let $G=M \cup T$.
- Step 3: Find an Eulerian cycle of G and then traverse it to find a Hamiltonian cycle as an approximate tour of ETSP by bypassing all previously visited vertices.





An algorithm for finding an optimal solution

<u>Step1</u>: Sort all edges in G = (V,E) into a nondecressing sequence $|e_1| \le |e_2| \le ... \le |e_m|$. Let G(e_i) denote the subgraph obtained from G by deleting all edges longer than e_i .

<u>Step2:</u> i←1

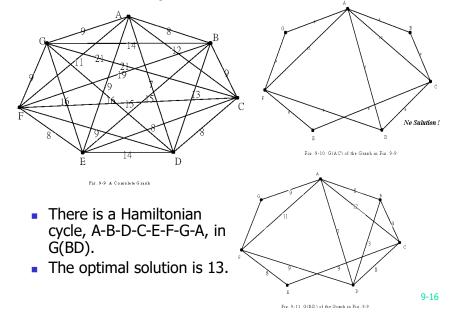
<u>Step3</u>: If there exists a <u>Hamiltonian cycle</u> in $G(e_i)$, then this cycle is the solution and stop. <u>Step4</u>: $i \leftarrow i+1$. Go to Step 3.

The bottleneck traveling salesperson problem (BTSP)

- Minimize the longest edge of a tour.
- This is a <u>mini-max</u> problem.
- This problem is <u>NP-hard</u>.
- The input data for this problem fulfill the following assumptions:
 - The graph is a <u>complete graph</u>.
 - All edges obey the <u>triangular inequality</u> <u>rule</u>.

9-14

An example for BTSP algorithm



Theorem for Hamiltonian cycles

- Def : The t-th power of G=(V,E), denoted as G^t=(V,E^t), is a graph that an edge (u,v)∈E^t if there is a path from u to v with at most t edges in G.
- Theorem: If a graph G is bi-connected, then G^2 has a Hamiltonian cycle. $A \rightarrow C^{C}$ $B \rightarrow C^{C}$ $C \rightarrow C^{C}$ $B \rightarrow C^{C}$ $C \rightarrow C^{C}$ C

not bi-connected

Fig. 9-12 Examples to Illustrate Bi-Connectedness

bi-connected

An example for the theorem

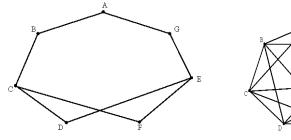
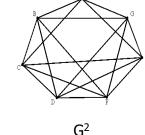


Fig. 9-13 A Bi-Connected Graph



A Hamiltonian cycle: A-B-C-D-E-F-G-A

9-18

An approximation algorithm for BTSP

- <u>Input</u>: A complete graph G=(V,E) where all edges satisfy triangular inequality.
- <u>Output:</u> A tour in G whose longest edges <u>is not</u> <u>greater than twice</u> of the value of an optimal solution to the special bottleneck traveling salesperson problem of G.
- Step 1: Sort the edges into $|e_1| \le |e_2| \le ... \le |e_m|$.

- <u>Step 3:</u> If $G(e_i)$ is <u>bi-connected</u>, construct $G(e_i)^2$, find a Hamiltonian cycle in $G(e_i)^2$ and return this as the output.
- <u>Step 4:</u> i := i + 1. Go to Step 3.



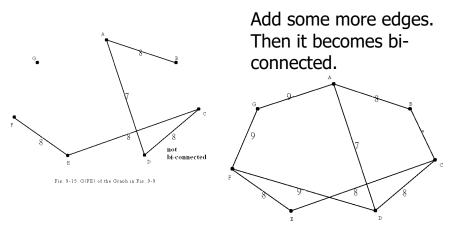
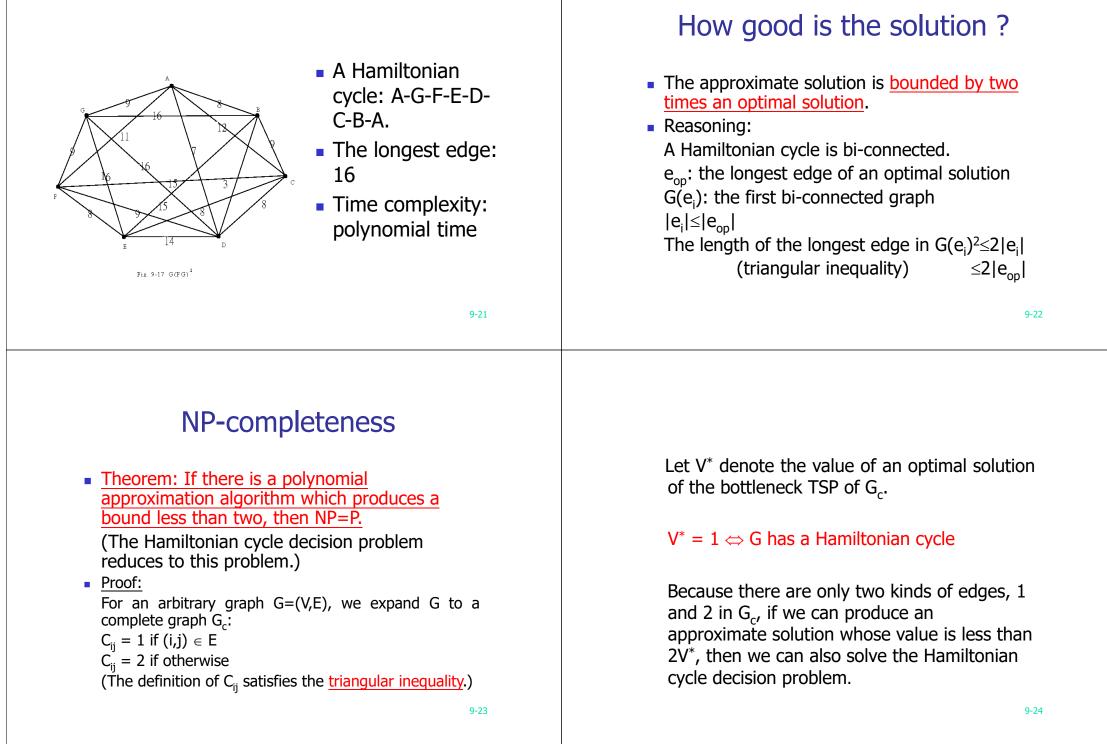
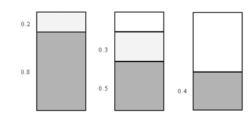


Fig. 9-16 G(FG) of the Graph in Fig. 9-9



The bin packing problem

- n items a₁, a₂, ..., a_n, 0< a_i ≤ 1, 1 ≤ i ≤ n, to determine the minimum number of bins of unit capacity to accommodate all n items.
- E.g. n = 5, {0.8, 0.5, 0.2, 0.3, 0.4}



The bin packing problem is <u>NP-hard</u>.

9-25

An approximation algorithm for the bin packing problem

- An approximation algorithm: (first-fit) place a_i into the lowest-indexed bin which can accommodate a_i.
- <u>Theorem: The number of bins used in the</u> <u>first-fit algorithm is at most twice of the</u> <u>optimal solution</u>.

9-26

Proof of the approximate rate

- Notations:
 - S(a_i): the size of item a_i
 - OPT: # of bins used in an optimal solution
 - m: # of bins used in the first-fit algorithm
 - C(B_i): the sum of the sizes of a_j's packed in bin B_i in the first-fit algorithm

• OPT
$$\geq \sum_{i=1}^{n} S(a_i)$$

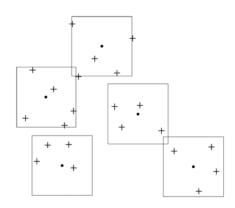
C(B_i) + C(B_{i+1}) > 1
C(B₁)+C(B₂)+...+C(B_m) > m/2

$$\Rightarrow \mathsf{m} < 2 \sum_{i=1}^{m} C(B_i) = 2 \sum_{i=1}^{n} S(a_i) \leq 2 \text{ OPT}$$

The rectilinear m-center problem

- The sides of a <u>rectilinear</u> square are parallel or perpendicular to the x-axis of the Euclidean plane.
- The problem is to find <u>m rectilinear squares</u> covering all of the n given points such that the maximum side length of these squares is minimized.
- This problem is <u>NP-complete</u>.
- This problem for the solution with error ratio
 < 2 is also <u>NP-complete</u>.

(See the example on the next page.)



- Input: P={P₁, P₂, ..., P_n}
- The size of an optimal solution must be equal to one of the L $_{\infty}(P_i,P_j)$'s, $1 \le i < j \le n$, where
 - $L_{\infty}((x_1,y_1),(x_2,y_2)) = \max\{|x_1-x_2|,|y_1-y_2|\}.$

An approximation algorithm

- Input: A set P of n points, number of centers: m
- <u>Output:</u> SQ[1], ..., SQ[m]: A feasible solution of the rectilinear m-center problem with size less than or equal to twice of the size of an optimal solution.
- <u>Step 1:</u> Compute rectilinear distances of all pairs of two points and sort them together with 0 into an ascending sequence D[0]=0, D[1], ..., D[n(n-1)/2].

Step 2: LEFT := 1, RIGHT := n(n-1)/2 //* Binary search Step 3: i := [(LEFT + RIGHT)/2].

Step 4: If Test(m, P, D[i]) is not "failure" then

RIGHT := i-1 else LEFT := i+1

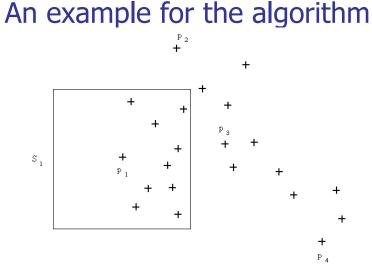
Step 5: If RIGHT = LEFT then

```
return Test(m, P, D[RIGHT])
```

```
else go to Step 3.
```

9-30

Algorithm Test(m, P, r)



The first application of the relaxed test subroutine.

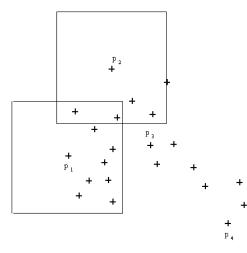
• <u>Input:</u> point set: P, number of centers: m, size: r.

 <u>Output:</u> "failure", or SQ[1], ..., SQ[m] m squares of size 2r covering P.

```
Step 1: PS := P
```

```
Step 2: For i := 1 to m do
```

```
If PS \neq \emptyset then
```



The second application of the test subroutine.

A feasible solution of the rectilinear 5-center problem.

Time complexity

- Time complexity: O(n²logn)
 - Step 1: O(n)
 - Step 2: O(1)
 - Step 3 ~ Step 5:

 $O(\log n)^* O(mn) = O(n^2 \log n)$

How good is the solution ?

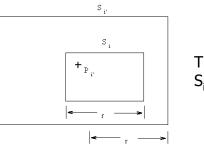
p,

р₂ +

+

+ р₁

- The approximation algorithm is of error ratio 2.
- Reasoning: If r is feasible, then Test(m, P, r) returns a feasible solution of size 2r.



The explanation of $S_i \subset S_i$

| Chapter 10 Amortized Analysis | An example- push and pop • A sequence of operations: OP_1, OP_2, OP_m OP_i : several pops (from the stack) and one push (into the stack) t_i : time spent by OP_i the average time per operation: $t_{ave} = \frac{1}{m} \sum_{i=1}^m t_i$ | |
|---|---|--|
| 10 -1 | 10 -2 | |
| • Example: a sequence of push and pop p: pop, u: push $\frac{i \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8}{OP_i \ 1u \ 1u \ 2p \ 1u \ 1u \ 1u \ 2p \ 1p}$ $\frac{i \ 1 \ 1 \ 3 \ 1 \ 1 \ 3 \ 1 \ 1 \ 1 \ 3 \ 2}{t_i \ 1 \ 1 \ 3 \ 2}$ $t_{ave} = (1+1+3+1+1+1+3+2)/8$ $= 13/8$ $= 1.625$ | • Another example: a sequence of push and pop p: pop, u: push $\frac{i \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8}{OP_i \ 1u \ 1p \ 1u \ 1u \ 1u \ 1u \ 5p \ 1u}$ $\frac{i \ 1 \ 2 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 6 \ 1}{t_i \ 1 \ 2 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 6 \ 1}$ $t_{ave} = (1+2+1+1+1+1+6+1)/8$ $= 14/8$ $= 1.75$ | |

Amortized time and potential function

 $\begin{aligned} \mathbf{a}_{i} &= \mathbf{t}_{i} + \Phi_{i} - \Phi_{i-1} \\ &\mathbf{a}_{i} : \text{ amortized time of OP}_{i} \\ \Phi_{i} : \text{ potential function of the stack after OP}_{i} \\ \Phi_{i} - \Phi_{i-1} : \text{ change of the potential} \end{aligned}$ $\begin{aligned} &\sum_{i=1}^{m} \mathbf{a}_{i} &= \sum_{i=1}^{m} \mathbf{t}_{i} + \sum_{i=1}^{m} (\Phi_{i} - \Phi_{i-1}) \\ &= \sum_{i=1}^{m} \mathbf{t}_{i} + \Phi_{m} - \Phi_{0} \end{aligned}$ If $\Phi_{m} - \Phi_{0} \ge 0$, then $\sum_{i=1}^{m} \mathbf{a}_{i}$ represents an upper <u>bound</u> of $\sum_{i=1}^{m} \mathbf{t}_{i}$

Amortized analysis of the push-and-pop sequence

- Φ_i : # of elements in the stack We have $\Phi_m - \Phi_0 \ge 0$
- Suppose that before we execute Op_i, there are k elements in the stack and Op_i consists of n pops and 1 push.

$$\Phi_{i-1} = k$$

 $t_i = n+1$
Then, $\Phi_i = k - n + 1$
 $a_i = t_i + \Phi_i - \Phi_{i-1}$
 $= (n+1) + (k-n+1)-k$
 $= 2$

specific series of the series

10 -6

• We have
$$(\sum_{i=1}^{m} a_i)/m = 2$$

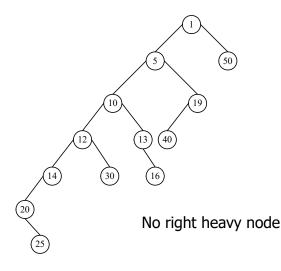
Then, $t_{ave} \le 2$.

 By observation, <u>at most *m* pops and *m*</u> <u>pushes are executed in *m* operations</u>. Thus,

$$t_{ave} \le 2$$

(50)

Step 2: Swap the children along the right path.



10 -9

Amortized analysis of skew heaps

- meld: merge + swapping
- operations on a skew heap:
 - find-min(h): find the min of a skew heap h.
 - insert(x, h): insert x into a skew heap h.
 - delete-min(h): delete the min from a skew heap h.
 - meld(h₁, h₂): meld two skew heaps h₁ and h₂.

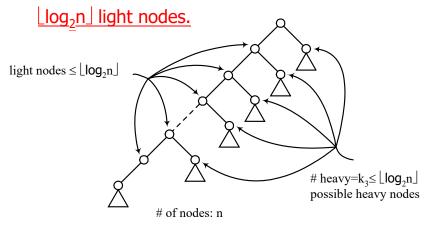
The first three operations can be implemented by <u>melding</u>.

10 -10

Potential function of skew heaps

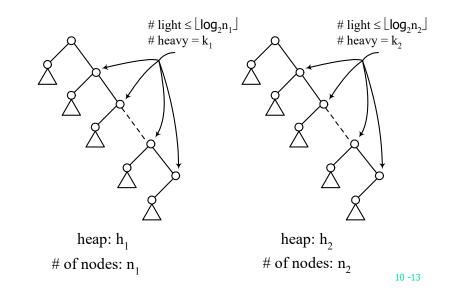
- wt(x): # of descendants of node x, including x.
- heavy node x: wt(x) > wt(p(x))/2, where p(x) is the parent node of x.
- light node : not a heavy node
- potential function Φ_i : # of right heavy nodes of the skew heap.

Any path in an n-node tree contains at most



 The number of <u>right heavy nodes</u> attached to the left path is at most log₂n l.

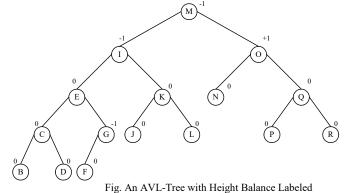
Amortized time

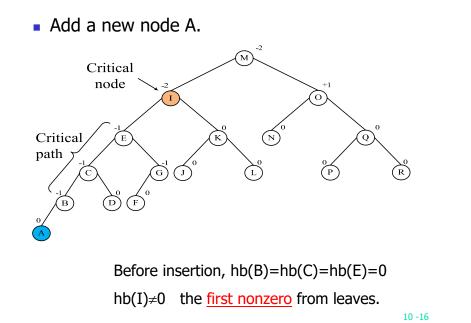


$$\begin{array}{l} a_{i} = t_{i} + \Phi_{i} - \Phi_{i\text{-}1} \\ t_{i} : \text{ time spent by } OP_{i} \\ t_{i} \leq 2 + \lfloor \log_{2}n_{1} \rfloor + k_{1} + \lfloor \log_{2}n_{2} \rfloor + k_{2} \\ (``2`` counts the roots of h_{1} and h_{2}) \\ \leq 2 + 2 \lfloor \log_{2}n \rfloor + k_{1} + k_{2} \\ \text{ where } n = n_{1} + n_{2} \\ \Phi_{i} - \Phi_{i\text{-}1} = k_{3} - (k_{1} + k_{2}) \leq \lfloor \log_{2}n \rfloor - k_{1} - k_{2} \\ a_{i} = t_{i} + \Phi_{i} - \Phi_{i\text{-}1} \\ \leq 2 + 2 \lfloor \log_{2}n \rfloor + k_{1} + k_{2} + \lfloor \log_{2}n \rfloor - k_{1} - k_{2} \\ = 2 + 3 \lfloor \log_{2}n \rfloor \\ \Rightarrow a_{i} = O(\log_{2}n) \end{array}$$

AVL-trees

<u>height balance</u> of node v: hb(v)= (height of right subtree) – (height of left subtree)
The hb(v) of every node <u>never differ by more than 1</u>.





Amortized analysis of AVL-trees

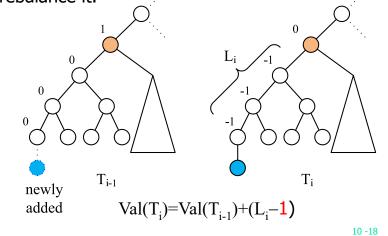
- Consider a sequence of m insertions on an empty AVL-tree.
 - T₀: an empty AVL-tree.
 - T_i: the tree after the ith insertion.
 - L_i: the length of the <u>critical path</u> involved in the ith insertion.
 - X₁: total # of balance factor changing from 0 to +1 or -1 during these m insertions (the total cost for rebalancing)

 $X_1 = \sum_{i=1}^{m} L_i$, we want to find X_1 . Val(T): # of unbalanced node in T (height balance ≠ 0)

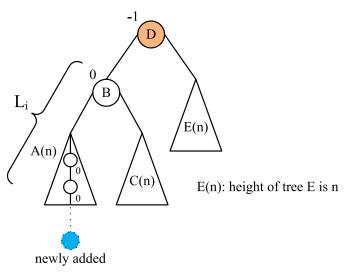
10 -17

Case 1 : Absorption

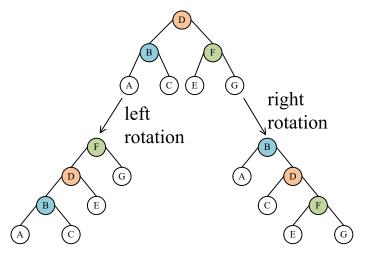
The tree height is <u>not increased</u>, we need not rebalance it.



Case 2.1 Single rotation



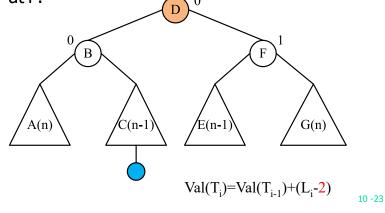
Case 2 : Rebalancing the tree



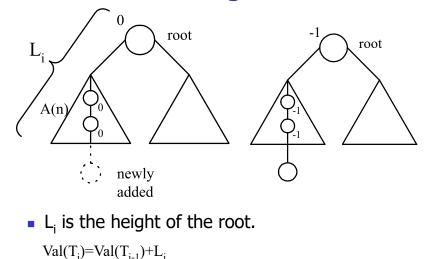
Case 2.1 Single rotation Case 2.2 Double rotation • After a right rotation on the subtree rooted at D: В G(n) D 0 D A(n)A(n)C(n-1 E(n-1) C(n)'E(n) newly added $Val(T_i)=Val(T_{i-1})+(L_i-2)$ 10 -21 10 -22

Case 2.2 Double rotation

 After a left rotation on the subtree rooted at B and a right rotation on the subtree rooted at F:



Case 3 : Height increase



Amortized analysis of X₁

| X ₂ : # of absorptions in case 1 X ₃ : # of single rotations in case 2 X ₄ : # of double rotations in case 2 X ₅ : # of height increases in case 3 | 3 methods for enhancing the sequential search (1) Transpose Heuristics: | ne performance of |
|---|--|-------------------|
| | Query | Sequence |
| $Val(T_m) = Val(T_0) + \sum_{i=1}^{m} L_i - X_2 - 2(X_3 + X_4)$ | В | В |
| $=0+X_1-X_2-2(X_3+X_4)$ | D | D B |
| $Val(T_m) \le 0.618m$ (proved by Knuth) | А | DAB |
| $\Rightarrow X_1 = Val(T_m) + 2(X_2 + X_3 + X_4) - X_2$ | D | DAB |
| $\leq 0.618 \text{m} + 2\text{m}$ | D | DAB |
| = 2.618 m | С | DACB |
| | А | A D C B |
| 10 -25 | | 10 -2 |

(2)<u>Move-to-the-Front Heuristics</u>:

| Query | Sequence |
|-------|----------|
| В | В |
| D | D B |
| А | A D B |
| D | DAB |
| D | DAB |
| С | C D A B |
| А | A C D B |

(3)<u>Count Heuristics</u>: (decreasing order by the count)

A self-organizing sequential

search heuristics

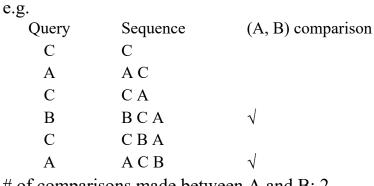
| | 0 | • |
|-------|---|----------|
| Query | | Sequence |
| В | | В |
| D | | B D |
| А | | B D A |
| D | | DBA |
| D | | DBA |
| А | | DAB |
| С | | DABC |
| А | | DABC |
| | | |

Analysis of the move-to-thefront heuristics

- interword comparison: unsuccessful comparison
- intraword comparison: successful comparison
- pairwise independent property:
 - For any sequence S and all pairs P and Q, # of interword comparisons of P and Q is exactly # of interword comparisons made for the subsequence of S consisting of only P's and Q's.

(See the example on the next page.)

Pairwise independent property in move-to-the-front



of comparisons made between A and B: 2

| | | 10 -29 | | | | | | | | 10 -30 |
|-----------------------|------------------------------|--|------------|---|----------------|---------|-------|--------|------|--------|
| | | | Query | Sequence | С | А | С | В | С | А |
| | | | Query | (A, B) | C | л 0 | C | 1 | C | 1 |
| | | | | (A, C) | 0 | 1 | 1 | - | 0 | 1 |
| | | | | (B, C) | 0 | | 0 | 1 | 1 | |
| Consider the Query | e subsequence co Sequence | onsisting of A and B: (A, B) comparison | | | 0 | 1 | 1 | 2 | 1 | 2 |
| A | A | | There | are 3 distin | ct <u>inte</u> | erwore | d com | pariso | ons: | |
| В | BA | \checkmark | | (A, B), (A, C) and (B, C) | | | | | | |
| А | AB | \checkmark | | | | | | | | |
| # of compar | isons made betw | veen A and B: 2 | ado the | e can cons d them up. e total num 1+1+2+1+ | ber o | f intei | | - | | |
| | | 10 -31 | | | | | | | | 10 -32 |

Theorem for the move-to-thefront heuristics

- $C_M(S)$: # of comparisons of the move-to-thefront heuristics
- $C_0(S)$: # of comparisons of the optimal static ordering

$C_M(S) \le 2C_O(S)$

Proof

Proof:

- Inter_M(S): # of interword comparisons of the move to the front heuristics
- Inter_o(S): # of interword comparisons of the optimal static ordering

Let S consist of a A's and b B's, a < b.

The optimal static ordering: BA

 $\left. \begin{array}{l} Inter_{O}(S) = a \\ Inter_{M}(S) \leq 2a \end{array} \right\} \quad \Rightarrow Inter_{M}(S) \leq 2Inter_{O}(S) \end{array}$

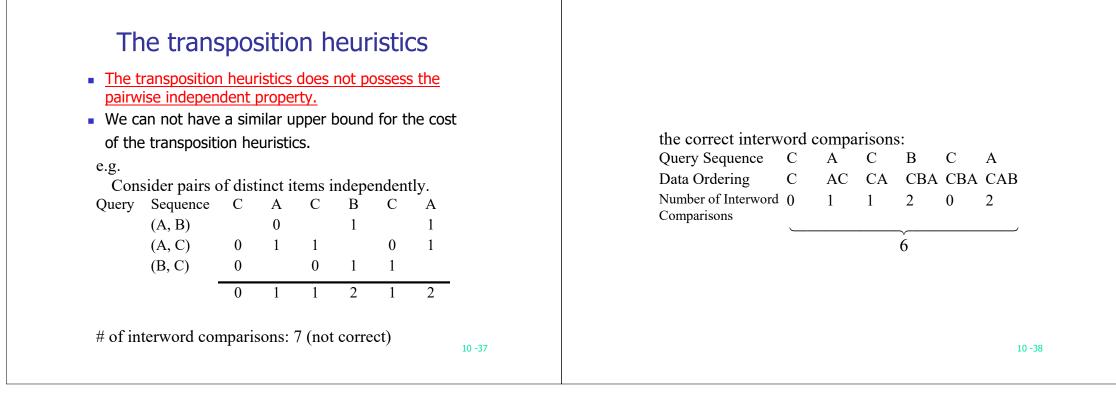
10 -34

Proof (cont.)

- Consider any sequence consisting of more than two items. Because of the pairwise independent property, we have $Inter_{M}(S) \leq 2Inter_{O}(S)$
- Intra_M(S): # of intraword comparisons of the moveto-the-front heuristics
- Intra_o(S): # of intraword comparisons of the optimal static ordering
- $Intra_M(S) = Intra_O(S)$
- Inter_M(S) + Intra_M(S) ≤ 2 Inter_O(S) + Intra_O(S) $\Rightarrow C_M(S) \leq 2C_O(S)$

The count heuristics

• The count heuristics has a similar result: $C_C(S) \le 2C_O(S)$, where $C_C(S)$ is the cost of the count heuristics



Chapter 11

Randomized Algorithms

11 -1

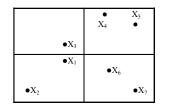
Randomized algorithms

- In a <u>randomized algorithm (probabilistic</u> <u>algorithm</u>), we make some random choices.
- 2 types of randomized algorithms:
 - For an <u>optimization problem</u>, a randomized algorithm gives an optimal solution. The <u>average</u> <u>case time-complexity</u> is more important than the worst case time-complexity.
 - For a decision problem, a randomized algorithm may make mistakes. The probability of producing wrong solutions is very small.

11 -2

The closest pair problem

- This problem can be solved by the divide-andconquer approach in O(nlogn) time.
- The <u>randomized algorithm</u>:
 - Partition the points into several clusters:



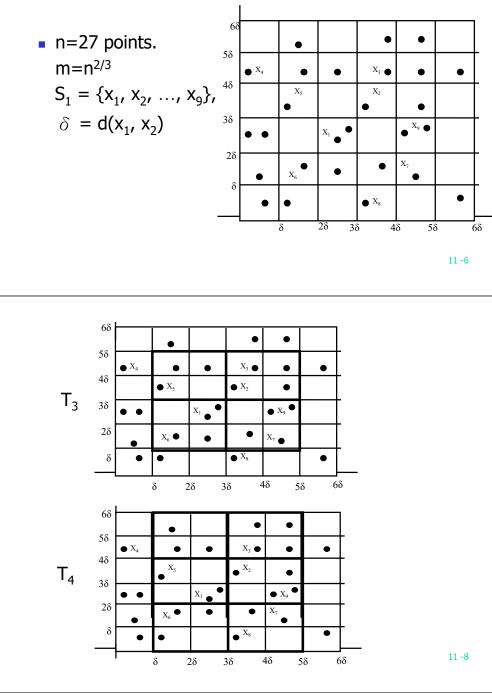
- We only calculate distances among points within the same cluster.
- Similar to the divide-and-conquer strategy. There is a dividing process, but <u>no merging process</u>.

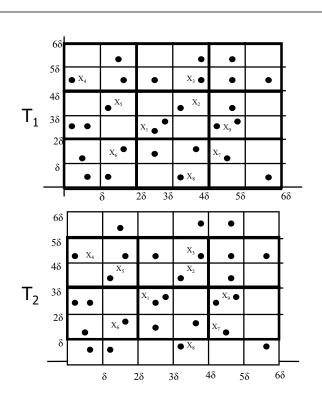
A randomized algorithm for closest pair finding

- Input: A set S consisting of n elements $x_1, x_2, ..., x_n$, where S $\subseteq R^2$.
- Output: The closest pair in S.
- <u>Step 1:</u> Randomly choose a set $S_1 = \{x_{i_1}, x_{i_2}, ..., x_{i_m}\}$ where $\underline{m=n^{2/3}}$. Find the closest pair of S_1 and let the distance between this pair of points be denoted as $\underline{\delta}$.
- Step 2: Construct a set of squares T with meshsize δ .

- Step 3: Construct four sets of squares $T_1,\,T_2,\,T_3$ and T_4 derived from T by doubling the meshsize to $\underline{2\delta}$.
- $\begin{array}{l} \underline{\text{Step 4:}} \text{ For each } T_i, \text{ find the induced} \\ \text{decomposition } S=S_1{}^{(i)} \cup S_2{}^{(i)} \cup \cdots \cup S_j{}^{(i)}, \ 1 \leq i \leq 4, \\ \text{where } S_j{}^{(i)} \text{ is a non-empty intersection of } S \\ \text{with a square of } T_i. \end{array}$
- Step 5: For each x_p , $x_q \in S_j^{(i)}$, compute $d(x_p, x_q)$. Let x_a and x_b be the pair of points with the shortest distance among these pairs. Return x_a and x_b as the closest pair.

An example







Time complexity

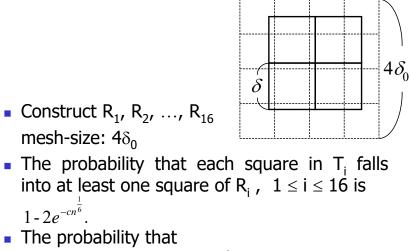
- Time complexity: O(n) in average
- step 1: O(n)

method : Recursively apply the algorithm once,

i.e. randomly choose $(n^{2/3})^{2/3} = n^{4/9}$ points from the $n^{2/3}$ points, then solve it with a straightforward method for the $n^{4/9}$ points: $O(n^{8/9})$

- step 2 ~ Step 4: O(n)
- step 5: O(n)with probability 1-2e^{-cn^{1/6}}

11 -9



$$N(T_i) \le \sum_{i=1}^{16} N(R_i)$$
 is $1 - 2e^{-cn^{\frac{1}{6}}}$.

Analysis of Step 5

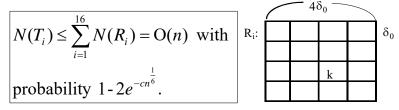
• How many distance computations in step 5? δ : mesh-size in step 1 T_i : partition in step 5 $N(T_i)$: # of distance computations in partition T_i Fact: There exists a particular partition R_0 , whose mesh-size is δ_0 such that (1) $N(R_0) \leq c_0 n$. (2) the probability that $\delta \leq \sqrt{2}\delta_0$ is $1 - 2e^{-cn^{\frac{1}{6}}}$.

11 -10

 Let the square in R₀ with the largest number of elements among the 16 squares have k elements.

 $\frac{k(k-1)}{2} = O(k^{2}), \frac{16k(16k-1)}{2} = O(k^{2})$

•
$$N(R_0) \le c_0 n => N(R_i) \le c_i n$$



A randomized algorithm to test whether a number is prime.

- This problem is very difficult and <u>no</u> <u>polynomial algorithm</u> has been found to solve this problem
- Traditional method: use 2,3,...√N to test whether N is prime. input size of N : B=log₂N (binary representation) √N = 2^{B/2}, exponential function of B

Thus \sqrt{N} can not be viewed as a polynomial function of the input size.

11 -13

Examples for randomized prime number testing

- Example 1: N = 12 Randomly choose 2, 3, 7
 - $2^{12-1} = 2048 \neq 1 \mod 12$
 - \Rightarrow 12 $\,$ is a composite number.

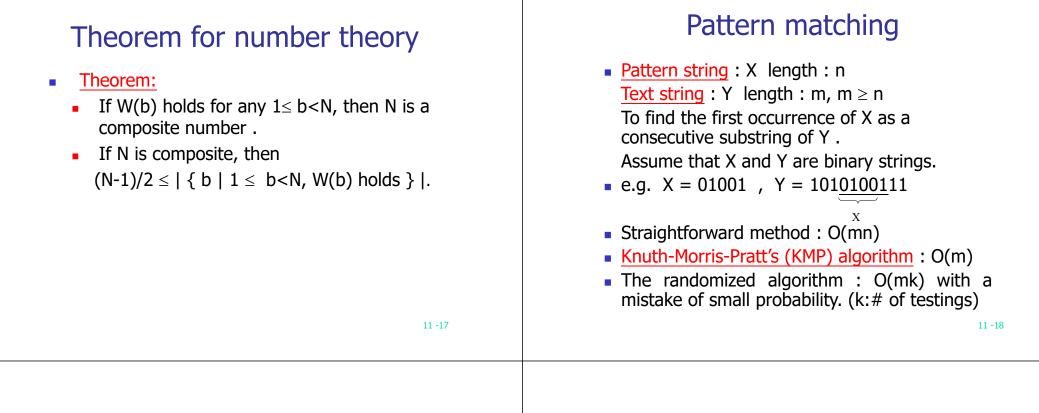
Randomized prime number testing algorithm

Input: A positive number N, and a parameter m.
 Output: Whether N is a prime or not, with probability of being correct at least 1-ε = 1-2^{-m}.
 Step 1: Randomly choose m numbers b₁, b₂, ..., b_m, 1≤ b₁, b₂, ..., b_m <N, where m≥log₂(1/ε).
 Step 2: For each b_i, test whether W(b_i) holds where W(b_i) is defined as follows:

 b₁^{N-1} ≠ 1 mod N or
 j such that N = 1/2⁻¹/2⁻¹ = k is an integer and the greatest common divisor of (b_i)^k-1 and N is not 1 or N.
 If any W(b_i) holds, then return N as a composite number, otherwise, return N as a prime.

11 -14

Example 2: N = 11 Randomly choose 2, 5, 7 (1) 2¹¹⁻¹=1024=1 mod 11 j=1, (N-1)/2^j=5 GCD(2⁵⁻¹, 11) = GCD(31,11) = 1 W(2) does not hold . (2) 5¹¹⁻¹=9765625=1 mod 11 GCD(5⁵-1, 11) = GCD(3124,11) = 11 W(5) does not hold . (3) 7¹¹⁻¹=282475249=1 mod 11 GCD(7⁵-1, 11) = GCD(16806,11) = 1 W(7) does not hold . Thus, 11 is a prime number with the probability of correctness being at least 1-2⁻³= 7/8 .



Binary representation

 $\begin{array}{ll} X = x_1 \, x_2 \ldots x_n \! \in \! \{0,1\} \\ Y = y_1 \, y_2 \ldots y_m \! \in \! \{0,1\} \\ \text{Let } Y(i) \! = \! y_i \, y_{i+1} \ldots y_{i+n-1} \\ \text{A match occurs if } X \! = \! Y(i) \text{ for some } i \ . \end{array} \\ \begin{array}{ll} \text{Binary values of } X \text{ and } Y(i) \text{:} \\ \text{B}(X) = x_1 \! \cdot \! 2^{n-1} + x_2 \! \cdot \! 2^{n-2} + \ldots + x_n \\ \text{B}(Y(i)) = y_i \! \cdot \! 2^{n-1} \! + \! y_{i+1} \! \cdot \! 2^{n-2} \! + \ldots \! + \! y_{i+n-1} \, , \\ 1 \! \leq i \! \leq m \! \cdot \! n \! + \! 1 \end{array}$

Fingerprints of binary strings

- Let p be a randomly chosen prime number in {1,2,...,nt²}, where t = m n + 1.
- Notation: (x_i)_p = x_i mod p
- Fingerprints of X and Y(i): $B_p(x) = (((x_1 \cdot 2)_p + x_2)_p \cdot 2)_p + x_3)_p \cdot 2...$ $B_p(Y(i)) = ((((y_i \cdot 2)_p + y_{i+1})_p \cdot 2 + y_{i+2})_p \cdot 2...$ $\Rightarrow B_p(Y(i+1)) = ((B_p(Y_i) - 2^{n-1} \cdot y_i) \cdot 2 + Y_{i+n})_p$ $= (((B_p(Y_i) - ((2^{n-1})_p \cdot y_i)_p)_p \cdot 2)_p + y_{i+n})_p$

• If X=Y(i), then $B_p(X) = B_p(Y(i))$, but not vice versa.

Examples for using fingerprints

• Example: X = 10110, Y = 110110 n = 5, m = 6, t = m - n + 1 = 2suppose P=3. $B_p(X) = (22)_3 = 1$ $B_p(Y(1)) = (27)_3 = 0$ $\Rightarrow X \neq Y(1)$ $B_p(Y(2)) = ((0-2^4)_3 2+0)_3 = 1$ $\Rightarrow X = Y(2)$

- e.g. X = 10110 , Y = 10011 , P = 3 $B_p(X) = (22)_3 = 1$ $B_p(Y(1)) = (19)_3 = 1$ $\Rightarrow X = Y(1) WRONG!$
- If $B_p(X) \neq B_p(Y(i))$, then $X \neq Y(i)$.
- If B_p(X) = B_p(Y(i)), we may do a bit by bit checking or compute k different fingerprints by using k different prime numbers in {1,2,...nt²}.

11 -21

A randomized algorithm for pattern matching

- <u>Input</u>: A pattern $X = x_1 x_2...x_n$, a text $Y = y_1 y_2...y_m$ and a parameter k.
- Output:
 - (1) No, there is no consecutive substring in Y which matches with X.
 - (2) Yes, $Y(i) = y_i y_{i+1} \dots y_{i+n-1}$ matches with X which is the first occurrence.
- If the answer is "No", there is no mistake.
- If the answer is "Yes", there is some probability that a mistake is made.

Step 1: Randomly choose k prime numbers $p_1, p_2, ..., p_k$ from {1,2,...,nt²}, where t = m - n + 1. Step 2: i = 1. Step 3: j = 1. Step 4: If $B(X)_{Pj} \neq (B(Y_i))_{pj}$, then go to step 5. If j = k, return Y(i) as the answer. j = j + 1. Go to step 4. Step5: If i = t, return "No, there is no consecutive substring in Y which matches with X." i = i + 1. Go to Step 3.

An example for the algorithm

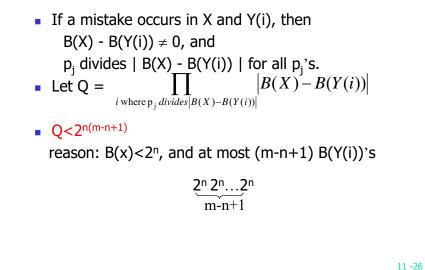
• X = 10110, Y = 100111, $P_1 = 3$, $P_2 = 5$ $B_3(X) = (22)_3 = 1$ $B_5(X) = (22)_5 = 2$ $B_3(Y(2)) = (7)_3 = 1$ $B_5(y(2)) = (7)_5 = 2$ Choose one more prime number, $P_3 = 7$ $B_7(X) = (22)_7 = 1$ $B_7(Y(2)) = (7)_7 = 0$ $\Rightarrow X \neq Y(2)$

11 -25

Theorem for number theory

- Theorem: If $u \ge 29$ and $q < 2^u$, then q has fewer than $\pi(u)$ diffferent prime number divisors where $\pi(u)$ is the number of prime numbers smaller than u.
- Assume $nt \ge 29$.
 - $Q < 2^{n(m-n+1)} = 2^{nt}$
 - \Rightarrow Q has fewer than $\pi(nt)$ different prime number divisors.
- If p_j is a prime number selected from {1, 2, ..., M}, the probability that p_j divides Q is less than $\frac{\pi (nt)}{\pi (M)}$.
- If k different prime numbers are selected from {1, 2, ...,nt²}, the probability that a mistake occurs is less than $\left(\frac{\pi(nt)}{\pi(nt^2)}\right)^k$ provided nt \ge 29.

How often does a mistake occur?



An example for mistake probability

How do we estimate
$$\left(\frac{\pi(nt)}{\pi(nt^2)}\right)^k$$
Theorem: For all $u \ge 17$, $\frac{u}{\ln u} \le \pi(u) \le 1.25506 \frac{u}{\ln u}$
 $\frac{\pi(nt)}{\pi(nt^2)} \le 1.25506 \cdot \frac{nt}{\ln nt} \cdot \frac{\ln(nt^2)}{nt^2}$
 $= \frac{1.25506}{t} (1 + \frac{\ln(t)}{\ln(nt)})$
Example: $n = 10$, $m = 100$, $t = m - n + 1 = 91$
 $\frac{\pi(nt)}{\pi(nt^2)} \le 0.0229$
Let k=4 $(0.0229)^4 \approx 2.75 \times 10^{-7}$ // very small

Interactive proofs: method I

Two persons: A : a spy
 B : the boss of A

When A wants to talk to B , how does B know that <u>A is the real A, not an enemy imitating A</u>?

• Method I : a trivial method

B may ask the name of A's mother (a private secret)

Disadvantage:

The enemy can collect the information, and imitate A the next time.

11 -29

Interactive proofs: method II

Method II:

B may send a Boolean formula to A and ask A to determine its satisfiability (an NP-complete problem). It is assumed that A is a smart person and knows how to solve this NP-complete problem.
B can check the answer and know whether A is the real A or not.
Disadvantage:

The enemy can study methods of <u>mechanical</u> <u>theorem proving</u> and sooner or later he can imitate A.

• In Methods I and II, A and B have revealed too much.

11 -30

A randomized algorithm for interactive proofs

Method III:

B can ask A to solve a <u>quadratic nonresidue</u> <u>problem</u> in which the data can be sent back and forth without revealing much information.

Definition:

GCD(x, y) = 1, y is a <u>quadratic residue mod x</u> if $z^2 \equiv y \mod x$ for some z, 0 < z < x, GCD(x, z) = 1, and y is a <u>quadratic nonresidue mod x</u> if otherwise.

(See the example on the next page.)

An example for quadratic residue/nonresidue

Let

 $QR = \{(x, y) \mid y \text{ is a quadratic residue mod } x\}$

- $QNR = \{(x, y) | y \text{ is a quadratic nonresidue mod } x\}$
- Try to test x = 9, y = 7:
 - $1^2 \equiv 1 \mod 9$ $2^2 \equiv 4 \mod 9$
 - $3^2 \equiv 0 \mod 9 \qquad 4^2 \equiv 7 \mod 9$
 - $5^2 \equiv 7 \mod 9$ $6^2 \equiv 0 \mod 9$
 - $7^2 \equiv 4 \mod 9$ $8^2 \equiv 1 \mod 9$
- We have (9,1), (9,4), (9,7) ∈ QR but (9,5), (9,8) ∈ QNR

Detailed method for interactive proofs

- 1) A and B know x and keep x confidential . B knows y.
- 2) Action of B:

 $\begin{array}{l} \text{Step 1: Randomly choose m bits: } b_1, \ b_2, \ \ldots, \ b_m, \\ \text{where m is the length of the binary} \\ \text{representation of x.} \end{array}$ $\begin{array}{l} \text{Step 2: Find } z_1, \ z_2, \ \ldots, \ z_m \ \text{s.t. GCD}(z_i \ , \ x) = 1 \ \text{for all } i \ . \end{array}$ $\begin{array}{l} \text{Step 3: Compute } w_1, \ w_2, \ \ldots, \ w_m \text{:} \\ w_i \leftarrow z_i^2 \ \text{mod } x \ \text{if } b_i = 0 \ \ //(x, \ w_i) \in \text{QR} \\ w_i \leftarrow (z_i^2 y) \ \text{mod } x \ \text{if } b_i = 1 \ \ //(x, \ w_i) \in \text{QNR} \end{array}$ $\begin{array}{l} \text{Step 4: Send } w_1, \ w_2, \ \ldots, \ w_m \ \text{to A.} \end{array}$

11 -33

3) Action of A: Step 1: Receive w₁, w₂, ..., w_m from B. Step 2: Compute c₁, c₂, ..., c_m: c_i ←0 if (x, w_i) ∈ QR c_i ←1 if (x, w_i) ∈ QNR Send c₁, c₂, ..., c_m to B.
4) Action of B: Step 1: Receive c₁, c₂, ..., c_m from A. Step 2: If (x, y) ∈ QNR and b_i = c_i for all i, then A is the real A (with probability 1-2^{-m}).