

$$\log_b(M \cdot N) = \log_b M + \log_b N \quad \log_b(1) = 0$$

$$\log_b\left(\frac{M}{N}\right) = \log_b M - \log_b N \quad \log_b b = 1$$

$$\log_b(M^k) = k \cdot \log_b M \quad \log_b b^k = k$$

$$b > 1, M, N > 0 \quad b^{\log_b(k)} = k$$

### Master Theorem

$$T(n) = aT\left(\lceil n/b \rceil\right) + O(n^d)$$

$$a > 1, b > 1, d \geq 0$$

$$T(n) = \begin{cases} O(n^d) & d > \log_b a, a < b \\ O(n^d \log n) & d = \log_b a, a = b \\ O(n^{\log_b a}) & d < \log_b a, a > b \end{cases}$$

$O(|V|+|E|)$

DFS  $\begin{bmatrix} u & \downarrow & v & \downarrow & u \end{bmatrix}$  Tree/Forward

uses a stack  $\begin{bmatrix} \downarrow & u & \downarrow & v & \downarrow \end{bmatrix}$  Back

edge  $(u, v)$   $\begin{bmatrix} u & \downarrow & v & \downarrow & u \end{bmatrix}$  Cross

reverse postorder == top sort

### Summations

$$1+2+3+\dots+(N-1)+N = \sum_{i=1}^N i \in \Theta(N^2)$$

$$1+2+4+\dots+(N/2)+N = \sum_{i=0}^{N/2} 2^i \in \Theta(N)$$

$$1+2+4+\dots+2^{N-1}+2^N = \sum_{i=0}^N 2^i \in \Theta(2^N)$$

$$\log(n!) \in \Theta(n \log n)$$

$$S_n = \frac{a_1(1-r^n)}{1-r} \text{ geo}$$

$$\text{DAG } H_k = \sum_{i=1}^k \frac{1}{i} = \Theta(\log k)$$

- has a sink and a source

- a directed graph has a cycle iff its DFS has a back edge

- Every edge leads to vertex w/ lower post #

- Every directed graph is a DAG of its SCCs

- explore(u) will stop when all nodes reachable from u have been visited

- node w/ highest post # in a DFS must lie in a source SCC

- If C and C' address same edge from C to C', the highest post # in C > highest post # in C'

SCCs Two nodes u and v of a directed graph are strongly connected if path u to v and v to u

SCC is a set of vertices such that any pair u, v are strongly connected

$$a = e^{2\pi i \theta_1} \quad b = e^{2\pi i \theta_2} \quad ab = e^{2\pi i (\theta_1 + \theta_2)} \quad Mn(w) = \frac{1}{n} \cdot Mn(w^{-1})$$

$$\begin{array}{c} \text{FFT} \\ \left[ \begin{array}{ccccc} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{n-1} \\ 1 & w^2 & w^4 & \cdots & w^{2(n-1)} \\ 1 & w^{(n-1)} & w^{2(n-1)} & \cdots & w^{(n-1)(n-1)} \end{array} \right] \quad w = e^{\frac{2\pi i}{n}} \\ \left[ \begin{array}{c} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{array} \right] \quad w^{ij} \quad O(n \log n) \end{array}$$

Group even & odd powers to reduce calc

- SSC Finding
1. run DFS on  $G^R$  to get post order #s if directed Graph linear time
  2. Init cnum = 0
  3. DFS on G processing vertices in decreasing post numbers. In pre-visit, set  $cc(v) = cnum$ . Increment cnum when stack empties.

BFS  $(G, s)$   $O(|V|+|E|)$

for all  $u \in V$ :  $\text{dist}(u) = \infty$

$\text{dist}(s) = 0$

$Q = [s]$  (queue with only s)

while Q is not empty:

$u = \text{eject}(Q)$

for all edges  $(u, v) \in E$ :

if  $\text{dist}(v) = \infty$ :

inject(Q, v)

$\text{dist}(v) = \text{dist}(u) + 1$

Dijkstra  $(G, l, s)$  priority queue

for all  $u \in V$ :  $\text{dist}(u) = \infty$   $\text{prev}(u) = \text{nil}$

$\text{dist}(s) = 0$

H = makequeue(V) (using dist-values as key)

while H is not empty:

$u = \text{deletemin}(H)$

$O(|V| \log |V|)$   
binary heap

for all edges  $(u, v) \in E$ :

if  $\text{dist}(v) > \text{dist}(u) + l(u, v)$ :

$\text{dist}(v) = \text{dist}(u) + l(u, v)$

$\text{prev}(v) = u$

$\text{decreasekey}(H, v)$

Bellman-Ford  $(G, l, s)$ :  $O(|V| \cdot |E|)$

for all  $u \in V$ :  $\text{dist}(u) = \infty$   $\text{prev}(u) = \text{nil}$

$\text{dist}(s) = 0$

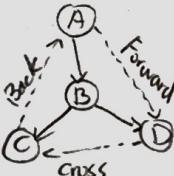
repeat  $|V|-1$  times:

run 1 more time to detect reg cycle

for all  $e \in E$ :

$\text{update}(e)$

Least updates if run in topo order for DAGs



$f(n) \in \Omega(g(n))$   $f$  is lower bounded by  $g$   
 $f(n) \in O(g(n))$   $f$  is upper bounded by  $g$

$$\begin{bmatrix} 4 \\ 3 \\ 2 \\ 1 \end{bmatrix}$$

$$x^3 + 2x^2 + 3x + 4$$

No edge weights: Try DFS / SCC decomposition

DAG: try topo sort

Has edge weight: Modify Dijkstra / Bellman-Ford (if neg weight)

$$T(n) = 2T(\sqrt{n}) + 3 \text{ and } T(2) = 3 \quad n^{1/2} = 2$$

$$t = \Theta(\log \log n) \quad T(n) = \Theta(\log n) \quad 2^{h+1} - 1$$

More FFT

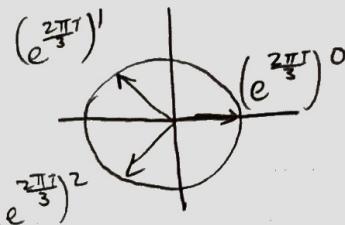
$$P(x) = A(x^4) + xB(x^2)$$

$$P(x^2) = A(x^4) + x^2B(x^4)$$

$$P(x^3) = A(x^6) + x^2B(x^6)$$

$$P(x^4) = A(x^8) + x^2B(x^8)$$

Need  $d+1$  pts for deg  $d$  polynomial



for  $j=0$  to  $n/2$ :

$$\begin{aligned} r_j &= s_j + \omega^j (s'_j) & n=2 & -1 \\ r_{j+n/2} &= s_j - \omega^j (s'_j) & n=4 & -i \\ && n=8 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \end{aligned}$$

LP row max  $z$ ,  $\sum x_i = 1$   $\geq$  expected val for each pure  
 $(z \in X_2 - X_3)$

for  $n$ , we have  $n$  roots of unity  
 $e^{2\pi i 0}, e^{2\pi i \frac{1}{n}}, e^{2\pi i \frac{2}{n}}, \dots, e^{2\pi i \frac{(n-1)}{n}}$

$$P(x) = P_1(x^3) + xP_2(x^3) + x^2P_3(x^3)$$

$$P_1(x^3) = a_0 + a_3x^3 + a_6x^6$$

$$P_2(x^3) = a_1 + a_4x^3 + a_7x^6$$

$$P_3(x^3) = a_2 + a_5x^3 + a_8x^6$$

Complex # inverse 1. write reciprocal

2. multiply top and bottom by conjugate

3. simplify

for  $j=0$  to  $n/2$ :

$$r_j = s_j + \omega^j (s'_j)$$

$$r_{j+n/2} = s_j - \omega^j (s'_j)$$

if  $w=1$ : return  $A(1)$

express  $A(x)$  in form  $Ae(x^2) + xAo(x^2)$

call IFFT( $A_e, w^2$ ) for  $A_e$  at even powers

call FFT( $A_o, w^2$ ) for  $A_o$  at even powers

for  $j=0$  to  $n-1$ :

$$\text{compute } A(w^j) = A_e(w^{2j}) + w^j A_o(w^{2j})$$

return  $A(w^0), \dots, A(w^{n-1})$

$$\begin{array}{c} \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \\ \text{row} \\ \text{normal} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & 1 & i \end{pmatrix} \end{array}$$

	Dijkstra	Heap Runtime	
deletion in	$O( V )$	$O(1)$	$ V  \cdot \text{deleterain}$ $( V  +  E ) \cdot \text{insert}$
insert/decrease key	$O( V )$	$O( V )$	$O( V  +  E ) \log  V $
	$O(\log  V )$	$O(\log  V )$	$O(( V  +  E ) \log  V )$
bi-heap	$O(d \log  V )$	$O(\frac{\log  V }{\log d})$	$O(( V  \cdot d +  E ) \frac{\log  V }{\log d})$
day heap	$O(\log  V )$	$O(1)$ amortized	$O( V  \log  V  +  E )$
Fib-heap	$O(\log  V )$	$O(1)$ amortized	$O( V  \log  V  +  E )$

Misc. If  $\text{post}(u) < \text{pre}(v)$  in DFS,  
edge  $(u, v)$  cannot exist

Kruskal O(E log V)

Add lightest edge w/o cycles

### Properties of tree

Tree w/ n nodes has n-1 edges  
connected graph  $G(V, E)$  w/

$|E| = |V| - 1$  is a tree

Undirected graph is a tree iff there is a unique path between any pair of nodes.

### Cut property

Edges  $X$  are part of a MST of  $G = (V, E)$ . Pick any subset of nodes  $S$  for which  $X$  does not cross between  $S$  and  $V-S$ , and let  $e$  be the lightest edge across the partition. Then  $X \cup e$  is part of some MST.

### Prims

Each iter, subtree  $X$  grows by one lightest edge between a vertex in  $S$  and one outside  $S$ .

### Huffman

Opt encoding based on distribution

- keep combining two lowest frequencies nodes

- if more than 0.4, then code word of length 1 guaranteed

### Horn Formulas

- Implications - LHS is an AND of any # of pos literals and RHS is a single pos literal.

$$(Z \wedge W) \Rightarrow U$$

If left holds, right must be true

- pure negative clauses, consisting of an OR of any # of negative literals.

$$(T_1 \vee \bar{V} \vee T_2)$$

- To solve, set all to false while there is an implication not satisfied:

set RHS of implication to True

If all pure neg clauses are satisfied return assignment

return "impossible"

### Set cover Algorithm

while (S isn't covered):

Pick the set  $S_i$  w/

largest # of uncovered elems.

### Dynamic Programming

Longest increasing subsequence

$$L = \{ \}$$

for  $j = 1, 2, \dots, n$

$$L[j] = 1 + \max\{L[i] : (i, j) \text{ in } E\}$$

return  $\max(L)$   $O(n^2)$

### Edit distance

- choose from min of adding a gap between letters or matching the two letters and move un.

for  $i = 0, 1, \dots, m$

$$E(i, 0) = i$$

for  $j = 1, 2, \dots, n$

$$E(0, j) = j$$

for  $i = 1, 2, \dots, m$

for  $j = 1, 2, \dots, n$

$$E(i, j) = \min\{E(i-1, j) + 1,$$

$$E(i, j-1) + 1, E(i-1, j-1) + \text{diff}(i, j)\}$$

return  $E(m, n)$

### Knapsack $O(nW)$

w/ repetition:

$$K(w) = \max_{\text{items}} \{K(w-w_i) + v_i\}$$

w/o repetition:

$$k(w, j) = \max_{\text{items}} \{k(w-w_j, j-1) + v_j, k(w, j-1)\}$$

### Chain Matrix Multiplication

$$C(i, j) = \min \{C(i, k) + C(k+1, j) + m_{i-1} \cdot m_k \cdot m_j\}$$

### Traveling Salesman Problem

$$C((1, \dots, n), 1) = 0 \quad O(n^2 n)$$

for  $s = 2 \dots n$ :

for all subsets  $S$  in  $\{1, 2, \dots, n\}$  of size  $s$  and has 1:

$$C(S, 1) = \infty$$

for all  $j$  in  $S, j \neq 1$ :

$$C(S, j) = \min(C(S - \{j\}, i) + d_{ij})$$

$i \in S, i \neq j, j \neq 1$

### LP

1. max  $\Rightarrow$  min, just mul obj func by -1

2. Turn inequality constraint like  $\sum_{i=1}^n a_{ix_i} \leq b$

into an equation, use a new var  $s$  and

$$\text{use } \sum_{i=1}^n a_{ix_i} + s = b, s \geq 0$$

3. To change  $ax = b$ , write as  $ax \leq b$  and  $ax \geq b$

4. If LP unbounded, dual must be infeasible.

### Max-Flow Min Cut

size of max flow in a network equals the capacity of the smallest  $(S, t)$  cut where an  $(S, t)$  partitions the vertices into 2 disjoint groups  $L$  and  $R$  such that  $S$  in  $L$  and  $t$  in  $R$ .

### Ford-Fulkerson $O(|E| * f)$

1. While there exists an augmenting path from  $S \rightarrow t$
2. push as much flow along the path possible
3. when no path exists, max-flow found

### Zero sum games

maximizer:

$$\max z$$

$$z \leq 5x_1 - 3x_2 + 3x_3$$

$$z \leq -x_2 + x_3$$

$$z \leq -2x_1 - 10x_2 - 4x_3$$

$$x_1 + x_2 + x_3 = 1$$

$$x_1, x_2, x_3 \geq 0$$

minimizer:

$$\min w$$

$$w \geq 5y_1 - 2y_3$$

$$w \geq -3y_1 - y_2 - 10y_3$$

$$w \geq 3y_1 + y_2 - 4y_3$$

$$y_1 + y_2 + y_3 = 1$$

$$y_1, y_2, y_3 \geq 0$$

$$\log^*(65536) = 4$$

set cover  $O(\ln n)$

### Dual

$$\max c_1 x_1 + \dots + c_n x_n \quad \min b_1 y_1 + \dots + b_m y_m$$

$$a_{11} x_1 + \dots + a_{1n} x_n \leq b_1 \quad a_{1j} y_1 + \dots + a_{mj} y_m \geq c_j$$

for  $i \in I$

for  $j \in N$

$$a_{ii} x_1 + \dots + a_{in} x_n = b_i$$

for  $i \in E$

$$a_{ij} y_1 + \dots + a_{mj} y_m = c_j$$

for  $j \notin N$

$$y_i \geq 0 \text{ for } i \in I$$

$$\min 5y_1 + 2y_2$$

$$y_1 + 3y_2 \geq 2$$

$$3y_1 + 4y_2 \geq 2$$

$$x_1, x_2 \geq 0$$

$$y_1, y_2 \geq 0$$

We constrain  $y_1, y_2$  so that they yield well  $x_1, x_2$  that are  $\geq$  those in primal obj. LP will give  $(y_1 + 3y_2)x_1 + (2y_1 + 4y_2)x_2 \leq 5y_1 + 2y_2$ . The constraints in dual force  $4y_1 + 3y_2 \geq 2$  and  $2y_1 + 4y_2 \geq 1$ .  $x_1 + x_2 \leq 5y_1 + 2y_2$  for all feasible

### Simplex

typically poly time, exp worst case

let  $v$  be any vertex of feasible region while there's a neighbor w/ better value

$$\text{set } v = v'$$

return  $v$

Two player coin game

Array  $[a_1 \dots a_n]$

Let  $S(i, j)$  be the maximum score the curr player can obtain if player is left w/ arry  $A[i \dots j]$

Recurrence

$$S(i, j) = \max\{L_i, R_j\}$$

$$L_i = A[i] + \min\{S(i+2, j), S(i+1, j-1)\}$$

$$R_j = A[j] + \min\{S(i+1, j-1), S(i, j-2)\}$$

Base cases

$$S(i, j) = \begin{cases} 0 & \text{if } i > j \\ A[i] & \text{if } i = j \end{cases}$$

Breaking chocolate

$B[i_1, j_1, i_2, j_2]$  to be the minimum # of

breaks needed to separate sub-matrix

$A[i_1 \dots i_2, j_1 \dots j_2]$  into pure pieces

Recurrence

$$B[i_1, j_1, i_2, j_2] =$$

$\min \{ 0, \text{ if all } A[i_1 \dots i_2, j_1 \dots j_2] \text{ are equal} \}$

$$1 + B[i_1, j_1, i_1+k, j_2] + B[i_1+k+1, j_1, i_2, j_2]$$

$$1 + B[i_1, j_1, i_2, j_1+k] + B[i_1, j_1+k+1, i_2, j_2]$$

for any  $k \in \{1, \dots, i_2 - i_1\}$

$$j_2 - j_1$$

Balloon popping

$C(i, j)$  = the maximum amount of money by popping all balloons in the sequence  $i, i+1, \dots, j$ . Smallest case is 1 balloon. size of sub problem is # of sub

size of sub problem is # of sub

Base case

one balloon  $\rightarrow$  popped

Recurrence

$$C(i, j) = \max_{i \leq k \leq j} \{ C(i, k-1) + C(k+1, j) + S_{i-1} \cdot S_k \cdot S_{j+1} \}$$

Zero sum games

max w

$$w \leq 200x_1$$

$$w \leq -100x_1 + 200x_2$$

$$x_1 + x_2 = 1$$

$$x_1, x_2 \geq 0$$

min z

$$z \geq 200y_1 - 100y_2$$

$$z \geq 200y_2$$

$$200y_1 - 100y_2 = 200y_2$$

$$200x_1 = -100x_1 + 200x_2$$

$$300x_1 = 200x_2$$

$$3x_1 = 2x_2$$

$$200y_1 = 300y_2$$

$$2y_1 = 3y_2$$

$$y_1 = 0.6 \quad y_2 = 0.4$$

Since  $x_1 + x_2 = 1$ ,  $x_1 = 0.4 \quad x_2 = 0.6$

find max by setting equal

expected payoff

$$200x_1y_1 - 100x_1y_2 + 0x_2y_1 + 200x_2y_2 = 80$$

moving on a grid

Let  $T(i, j)$  be the min # of tokens

needed to start at cell  $(i, j)$  and reach  $(n, n)$

Base cases

$$T(n, n) = 0$$

Recurrence

$$\text{Let } T(i, j) = \max \{ \min(T(i+1, j), T(i, j+1)) - G(i, j), 0 \}$$

minimum gold strikes

Let  $S(i)$  be the minimum # of strikes

needed to reach checkpoint n from i

$$S(n) = 0$$

$$S(i) = 1 + \min_{i+1 \leq j \leq i+d(i)} S(j) \quad \text{for } i < n$$

n entries

each takes  $O(1)$

$\Rightarrow O(n)$

## H-hard Problems (NP-Comp) Easy Problems (in P)

3SAT

TSP

Longest path

3D Matching

Knapsack

Independent set

Integer LP

Rudrata Path

Balanced Cut

2SAT, HORN SAT

MST

shortest path

bipartite matching

unary knapsack

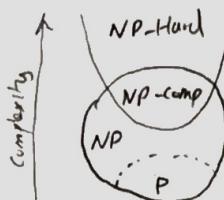
Independent sets on trees

LP

Euler Path

Minimum cut

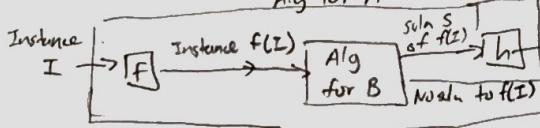
## P ≠ NP



If  $A \rightarrow B$ , B is at least as hard as A.

If any search problem can be reduced to B, then B is NP-Complete

Alg for A



To prove reduction:

1. Prove pre-process and post-process polynomial
2. Given B soln SB, h(SB) is valid soln to A
3. No soln to B  $\rightarrow$  no soln to A

or soln to A, then there exists solution to B

Copied w/ NP-Completeness

Backtracking: Try an assignment, test if it meets our constraint. If not, reject.

Branch and Bound: To reject a subproblem in a minimization prob, we must be certain that its cost exceeds some other soln

Approximation Alg: For a min. prob, find a soln w/ factor

$$\alpha = \max_I \frac{A(I)}{\text{OPT}(I)}$$

local search: If we have a set of soln, we def a neighborhood to relate them, then we seek local optima

Matching: subset of edges that have no vertices in common, any matching is a lower bound on the optimal soln for vertex cover.

TSP - Is there a tour, which visits each node exactly once, within budget b.

Rudrata path = path passing thru each vertex exactly once

Balanced cut: with Budget b for cut, partition into 2 sets such that each has  $\geq 1/3$  elements

3D matching: Given M valid tuples, match n boys, girls, pets. Find n disjoint triples that get along

Independent set: Graph, integer g: find g vertices that are independent (no 2 share edge)

Vertex cover: b vertices that touch every edge

Dominating set: b vertices s.t. every edge is in the set, or has a neighbor in the set

Set cover: given subsets, select b subsets such that the union is the entire set

Clique: g vertices, each is connected w/ every other

Longest path: is there a simple path, length g or more, from s to t?

## All of NP

SAT

3SAT

3D Matching

$O-1$  Equations

Independent set

clique

subset sum

ILP

Rudrata cycle

TSP

## Quantum

$$|d\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

$$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Partial Measure: look at one bit

Result: 0 (w/ prob  $|\alpha_{00}|^2 + |\alpha_{01}|^2$ )

New internal state:  $\frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

Scale to make probs add to 1  $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$

$$|\alpha_0|0\rangle + \alpha_1|1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

$$\text{Joint state: } \alpha_0 \beta_0 |00\rangle + \alpha_0 \beta_1 |01\rangle + \alpha_1 \beta_0 |10\rangle + \alpha_1 \beta_1 |11\rangle$$

Not all can be decomposed, e.g.  $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Hadamard Gate

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$\text{Two bits } H(|\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0 + \alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0 - \alpha_1}{\sqrt{2}}|1\rangle$$

CNOT

takes two qubits and flips the target bit if the control bit is set to 1

Modular If  $x \equiv x' \pmod{N}$  and  $y \equiv y' \pmod{N}$

$$xy \equiv x'y' \pmod{N} \text{ and } xy \equiv x'y' \pmod{N}$$

If  $x, y$  are pos int and  $x \gg y$ ,  $\gcd(x, y) = \gcd(x \bmod y, y)$

Fermat Little Theorem  $a^{p-1} \equiv 1 \pmod{p}$  if p is prime  $1 \leq a < p$

Carmichael #'s - passes Fermat but not prime

MWU probability of choosing i is  $\frac{w_i}{W}$  where W = total weight

# of mistakes M made by MWU w/ factor of  $(1-\varepsilon)$  is

$$M \leq (1+\varepsilon)m + \frac{\ln n}{\varepsilon} \quad \text{take deriv and set to 0 to find } \varepsilon$$

m is the # of mistakes of the best expert

$$\text{Regret } R = \frac{1}{T} \left( \sum_{t=1}^T c(x_t) - \min_k \sum_{t=1}^T c(x_t, k) \right)$$

larger  $\varepsilon$  = more penalty for mistakes

To prove A is NP-Comp: problem must be in NP

2. Find B in NP-Hard s.t.  $B \rightarrow A$

$$NP \rightarrow B \quad B \rightarrow A \quad NP \rightarrow A$$

## Hashing

$n = 257$

$$\text{IP addresses} - \text{hash}(x_1, \dots, x_4) = \sum_{i=1}^4 a_i \cdot x_i \bmod n$$

pick  $a_i$  at random

If two IP differs at  $x_4 \neq y_4$  then:

$$\sum_{i=1}^3 a_i (x_i - y_i) \equiv a_4 \cdot (y_4 - x_4) \bmod n$$

$n$  is prime so  $(y_4 - x_4)$  must have unique inverse

Set LHS to  $c$ , then  $a_4$  needs to be  $c(y_4 - x_4)^{-1} \bmod n$  which has probability  $1/n$ .

$$\text{Universal hash} := \forall x, y \in U, x \neq y = \Pr_{h \in H} [h(x) = h(y)] \leq \frac{1}{m}$$

$$H = \{h : U \rightarrow [m]\}$$

$f : [m] \rightarrow [n]$  then  $n^m$  possible functions

## Set Packing

Find  $k$  mutually disjoint subsets

Proof: Reduce 3D Matching to set packing. Given an instance  $\Phi$  of 3D matching, we can construct instance  $\Psi$  of set packing.

Let the set  $U = \{p_1, \dots, p_n, b_1, \dots, b_n, g_1, \dots, g_n\}$  be the set of all pets, buys, girls in  $\Phi$  and let  $k = n$ . For each tuple  $(p_i, b_j, g_k)$  we create one set  $S_e = \{p_i, b_j, g_k\}$ . The reduction is in polynomial time and a collection of tuples is a valid matching for  $\Phi$  iff their corresponding sets is a valid set packing solution.

Reduce Hamiltonian Path to degree-bounded Spanning Tree. We can make it into a DBST problem w/ graph  $G$  and  $b_i = 2 \forall i$ . If there is a Hamiltonian path, then this is a spanning tree where each deg is at most 2, so it must be the case that DBST has a possible spanning tree where each degree is at most 2.

If there is a ST where deg is at most 2, then this implies there is a Hamiltonian path. Because it is spanning, it includes all vertices, and it's acyclic (tree). If every deg is at most 2, this forces the only possible ST to be a path that visits all the vertices exactly once. This is a Ham Path. So if there is such a ST, there is a Ham Path.

## Streaming

$F_0$  - counts # of distinct items  $F_1$  - length of stream

To estimate item freq  $f_i$  within additive error  $n/k$  using  $O(k(\log n + \log m))$  mem,

1. Maintain set  $S$  of  $k$  counters, for each elem  $i$
2. If  $x_i \in S$ , increment counter for  $x_i$
3. If  $x_i \notin S$ , add  $x_i$  to  $S$  if space avail, else decrement all counters in  $S$ . (Remove when 0)

Exact counts require  $O(n)$  space

Tell if # of distinct items  $N$  is more than  $2k$

1. choose uniformly random hash func  $h : [n] \rightarrow [B]$ , where # of Buckets  $B = O(k)$
2. Output 'yes' if there is some  $x_i \in S$  s.t.  $h(x_i) = 0$  else no

When  $k=2$ , show this is a  $3/4$  approximation

Let OPT denote the total # of elems covered by the optimal soln and let  $x$  denote the # of elems covered by the first subset in the greedy soln. Since OPT elements can be covered by two subsets, the first subset picked by the greedy must cover at least  $OPT/2$  elems.  $x \geq \frac{OPT}{2}$  since at least  $OPT-x$  elems covered by the opt soln is uncovered by the first subset picked by the greedy, the second subset must cover at least  $(OPT-x)/2$  uncovered elems. So greedy covers  $x + (OPT-x)/2 = OPT/2 + x/2 \geq 3OPT/4$

Simplex is exponential time

Doubling the min-cut doesn't double the flow

Two polynomial  $p(x), q(x)$  given in (point, value) can be multiplied in  $O(n)$

Every directed graph can be decomposed into a DAG

Cross edges occur in DFS only if graph directed

Running DFS from a node in a sink SCC yields a SCC of the graph

MST never contains heaviest edge of cycle

MST always contains lightest edge in bridge cut