CS170 cribsheet midterm1

Order of Growth

Formal

UpperBound O : LowerBound Ω : Constant Θ
$\frac{a(n)}{b(n)} > 0, a(n) \in \Omega(b(n))$ $\frac{a(n)}{b(n)} < c, a(n) \in O(b(n))$
$\frac{a(n)}{b(n)} = c, a(n) \in \Theta(b(n))$

Tricks

$7^{\log(n)^2} = (2^{\log(7)})^{(\log(n))^2} = (2^{\log(n)})^{\log(7)\log(n)} \approx n^{\log(n)}$

$n! = 2^{n\log(n)}$ ::$36^5 = 6^{10}$

Solve the comparison by integration.

$(a+bi)*(c+di) \to r = ab, s = bd, t = (a+b)(c+d) = r - s + (t - r - s)i$

add/multiply

Karatsuba's $= \Theta(n^{\log_2 3})$

Prove

Geom sum series: $g(n) = \frac{1-c^{n+1}}{1-c} = \frac{c^{n+1}-1}{c-1}$

Induction: $\gcd(F_{k+1}, F_{k+1}) = \gcd(F_{k+1}, F_{k+2} - F_{K+1}) = \gcd(F_{k+1}, F_k) = 1$

Numbers before prime $1/n$: in $O(n)$ time. Geom dist.$E[X] = \sum_{i=1}^{\infty} i * P[X = i] = \sum_{i=1}^{\infty} i * (1-p)^{(i-1)}p$
$p = probheads, i - 1 = tailsthrows$
$= p * dp/dt(\sum_{i=1}^{\infty} -(1-p)^i) \to_{sums} = -1/p$ Integrate:
$E[X] = p * (1/p^2) = 1/p$

Binary Search: if N is a square. Why only $\log n$ for power max? $N = q^k \to \log N = k\log \to k = \log N/\log q \leq \log N$

For any power: poweringoperation$\{\sum_{i=1}^{k} in * n = O(k^2n^2)\}$
Repeat $\log n$ times to get $O(n^6)$

Modular Arithmetic

Quadratic residue busniess. Fermat's theorem:
$\forall 1 \leq a < p : a^{p-1} \equiv 1 mod p$ if p is prime.

Euler's Theorem: $m^{(p-1)(q-1)} \equiv 1(modpq)$ Multitudes:
$2013^{2014} = 3^{2012+2} = (3^{503})^4 * 3^2 = 1 * 3^2 = 4 allmod5$
$2012^{2013} = 2^{2012+1} = (2^{503})^2 * 2^1 = 1 * 2 = 2 allmod5$

$5^{170^{70}} mod5$: take $170^{70} = 4s + t$ form
$170^{70} = (2*85)^{(2*35)} = (4*85^2)^{35} = 0 mod4$

Worst RSA: We know N,e,d: $k = (ed-1)/(p-1)(q-1)$, limit k$\in 1,2$ by $e = 3, d < (p-1)(q-1)$ Solve two eq system for p and q modulating k, use $N = pq$.

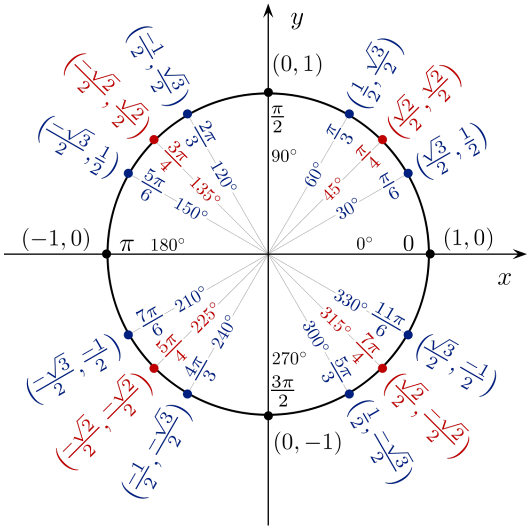
Randomize recoverable RSA w/ $(M^e * k^e)^d modN = MkmodN$ then multiply by k^{-1}

Primality testing: Doesn't catch Carmichaels. you did this for euler project already

Divide and Conquer

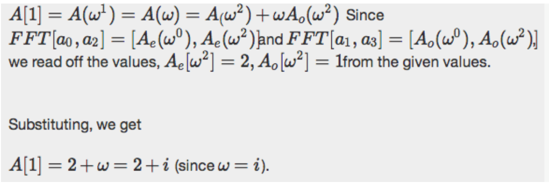
Master's Theorem:
$T(n) = aT(n/b) + O(n^d), a > 0, b > 1, d \geq 0$
$O(n^d) \to d > \log_b a$ :: $O(n^d \log n) \to d = \log_b a$ ::
$O(n^{\log_b a}) \to d < \log_b a$
Majority Element: If there is a majority element then it will be a majority element of A_1 or $A_2, , O(n\log n)$. Or you could use the pairing-discard approach $T(n) = T(n/2) + O(n) = O(n)$
For finding kth smallest element in array,
$O(n)average, O(n^2)worst$

$$\text{selection}(S,k) = \begin{cases} \text{selection}(S_L, k) & \text{if } k \leq |S_L| \\ v & \text{if } |S_L| < k \leq |S_L| + |S_v| \\ \text{selection}(S_R, k - |S_L| - |S_v|) & \text{if } k > |S_L| + |S_v|. \end{cases}$$



y
x
$(0,1)$
$(-1,0)$
$(1,0)$
$(0,-1)$
$\frac{\pi}{2}$
90°
$\frac{\pi}{3}$
60°
$\frac{\pi}{4}$
45°
$\frac{\pi}{6}$
30°
0°
0
$\frac{2\pi}{3}$
120°
$\frac{3\pi}{4}$
135°
$\frac{5\pi}{6}$
150°
π
180°
$\frac{7\pi}{6}$
210°
$\frac{5\pi}{4}$
225°
$\frac{4\pi}{3}$
240°
270°
$\frac{3\pi}{2}$
$\frac{5\pi}{3}$
300°
$\frac{7\pi}{4}$
315°
$\frac{11\pi}{6}$
330°
$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$
$\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$
$\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)$
$\left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$
$\left(\frac{-\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$
$\left(\frac{-\sqrt{3}}{2}, \frac{1}{2}\right)$
$\left(\frac{-\sqrt{3}}{2}, \frac{-1}{2}\right)$
$\left(\frac{-\sqrt{2}}{2}, \frac{-\sqrt{2}}{2}\right)$
$\left(\frac{-1}{2}, \frac{-\sqrt{3}}{2}\right)$
$\left(\frac{1}{2}, \frac{-\sqrt{3}}{2}\right)$
$\left(\frac{\sqrt{2}}{2}, \frac{-\sqrt{2}}{2}\right)$
$\left(\frac{\sqrt{3}}{2}, \frac{-1}{2}\right)$

Complex number practice: $\omega = e^{2\pi i/8}, n = 8, = \sqrt{2}/2 + i\sqrt{2}/2$
$\omega^7 = e^{2\pi i(7/8)} = \sqrt{2}/2 - i\sqrt{2}/2 = \omega^-1, \omega^7 + \omega = \sqrt{2}$
$p(x) = x^2 + 1, p(\omega) = 1 + i, p(\omega^2) = 0, p(\omega^3) = 1 - i$
Missing integer: Array A of numbers [0,N]. Split into N/2 and count the bits in least significant position. You know how may 1-bits to expect. If that number is spot on, missing=0, otherwise missing=1. For each of these splits and counts we downsize by N/2 $\to T(n) = T(n/2) + O(n) = O(n)$, all without bit complexity
Pareto points: Sort $O(n\log n)$ and then do linear scan in reverse order $O(n)$
FFT: $A(x) = 1 + 2x - x^2 + 3x^3$
$(x_1, x_2, x_3, x_4) = (\omega^0, \omega^1, \omega^2, \omega^3) = (1, i, -1, -i)$ :: $\omega = e^{2\pi i/n}$
In general find the nearest power of two as n
Split into
$A(x) = A_e(x) + xA_o(x)$ :: $A_e(x) = 1 - x, A_o(x) = 2 + 3x$
$A_e(\omega^{2j}) + \omega^i A_o(\omega^{2j})$
DFT Matrix entry: $(m,n) = \omega^{m*n} = e^{(2\pi i/n)*mn}$ Inverse
DFT AMmtrix entry: $(m,n) = (1/n) * \omega^{-m*n} = e^{-(2\pi i/n)*mn}$



$A[1] = A(\omega^1) = A(\omega) = A_(\omega^2) + \omega A_o(\omega^2)$ Since
$FFT[a_0, a_2] = [A_e(\omega^0), A_e(\omega^2)]$and $FFT[a_1, a_3] = [A_o(\omega^0), A_o(\omega^2)]$
we read off the values, $A_e[\omega^2] = 2, A_o[\omega^2] = 1$from the given values.

Substituting, we get

$A[1] = 2 + \omega = 2 + i$ (since $\omega = i$).

$$FFT([u,v,x,y])_k = FFT([u,x])_k + \omega^k FFT([v,y])_k$$
$$FFT([u,v,x,y])_{k+2} = FFT([u,x])_k - \omega^k FFT([v,y])_k,$$

Graphs

Facts

Undirec graph w/ n verts and n edges has cycle by induction.
Stongly connected: path between any two points :: TREE EDGES <=> CROSS EDGES depending on DFS
Dijkstra's: Put all edges on a list and mark distance ∞, $O(|V|)$ time.

Kruskal's - greeedy - returns smallest edge not in cycle to be in MST

DP

Find a substructure in the subproblems. Begin with the smallest subproblem and show how the solution to that problem will give you the "most", "least", "largest", "smallest", etc. and then give a recurrence for the possible steps before it. MORE SIMPLE THAN YOU THINK!

LP

LPs must maximize only one objective function.

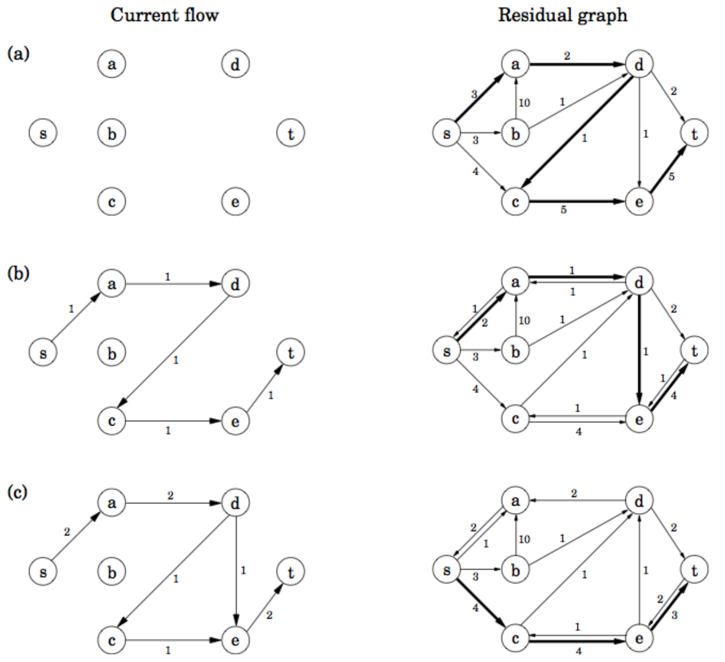
Dual and primal are equal then that is the optimum. Transpose everything to get dual. Simply add dummy variables to all of the original equations and summ the dummy variables in the objective. Simplex solves vertex linear programs, but it does not gurantee integer solutions.

$$|\alpha_{\text{new}}\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|01\rangle .$$

Reduce NP, NP-complete

If you reduce A to B then you show how to solve A using B algorithm. Showing NP-complete: first show B is in NP. Then show that applying B algorithm to some other NP-complete problem will yield a solution. Make sure that the input and output processing functions run in **polynomial time**.
A→B is A in outer box of B.
NP completes SAT, 3SAT, Hamiltonian Path,

e shown in bold.



Primal LP:

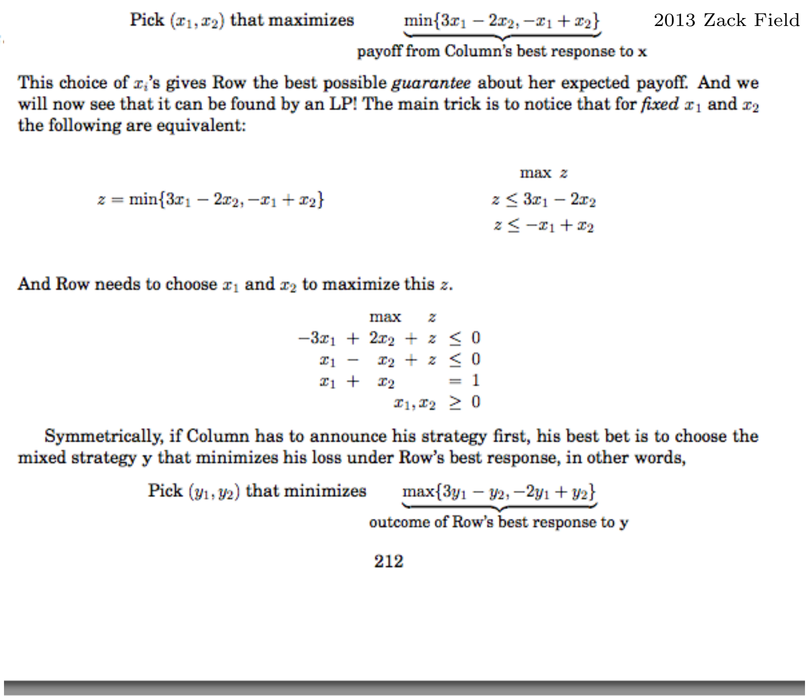
$$\begin{aligned} &\max\ c_1x_1 + \cdots + c_nx_n \\ &a_{i1}x_1 + \cdots + a_{in}x_n \le b_i \quad \text{for } i \in I \\ &a_{i1}x_1 + \cdots + a_{in}x_n = b_i \quad \text{for } i \in E \\ &x_j \ge 0 \quad \text{for } j \in N \end{aligned}$$

Dual LP:

$$\begin{aligned} &\min\ b_1y_1 + \cdots + b_my_m \\ &a_{1j}y_1 + \cdots + a_{mj}y_m \ge c_j \quad \text{for } j \in N \\ &a_{1j}y_1 + \cdots + a_{mj}y_m = c_j \quad \text{for } j \notin N \\ &y_i \ge 0 \quad \text{for } i \in I \end{aligned}$$

$$\sum_{i,j} G_{ij} \cdot \text{Prob[Row plays } i\text{, Column plays } j] = \sum_{i,j} G_{ij} x_i y_j$$

2013 Zack Field



$$\text{Pick } (x_1, x_2) \text{ that maximizes } \underbrace{\min\{3x_1 - 2x_2, -x_1 + x_2\}}_{\text{payoff from Column's best response to x}}$$

This choice of x_i's gives Row the best possible *guarantee* about her expected payoff. And we will now see that it can be found by an LP! The main trick is to notice that for *fixed* x_1 and x_2 the following are equivalent:

$$z = \min\{3x_1 - 2x_2, -x_1 + x_2\} \qquad \begin{array}{c} \max z \\ z \le 3x_1 - 2x_2 \\ z \le -x_1 + x_2 \end{array}$$

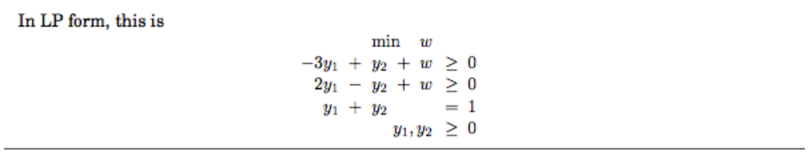
And Row needs to choose x_1 and x_2 to maximize this z.

$$\begin{array}{rcrcrl} & & \max & & z & \\ -3x_1 & + & 2x_2 & + & z & \le 0 \\ x_1 & - & x_2 & + & z & \le 0 \\ x_1 & + & x_2 & & & = 1 \\ & & & & x_1, x_2 & \ge 0 \end{array}$$

Symmetrically, if Column has to announce his strategy first, his best bet is to choose the mixed strategy y that minimizes his loss under Row's best response, in other words,

$$\text{Pick } (y_1, y_2) \text{ that minimizes } \underbrace{\max\{3y_1 - y_2, -2y_1 + y_2\}}_{\text{outcome of Row's best response to y}}$$

$$G = \begin{array}{|c|cc|} \hline & m & t \\ \hline e & 3 & -1 \\ s & -2 & 1 \\ \hline \end{array}$$



In LP form, this is

$$\begin{array}{rcrcrl} & & \min & & w & \\ -3y_1 & + & y_2 & + & w & \ge 0 \\ 2y_1 & - & y_2 & + & w & \ge 0 \\ y_1 & + & y_2 & & & = 1 \\ & & & & y_1, y_2 & \ge 0 \end{array}$$