CECS 528, Learning Outcome Assessment 5, Spring 2024, Dr. Ebert

NO NOTES, BOOKS, ELECTRONIC DEVICES, OR INTERPERSONAL COMMUNICATION ALLOWED. Submit each solution on a separate sheet of paper.

Problems

LO1. Solve the following problems.

(a) Show each of the subproblem instances that must be solved when using the recursive division algorithm for finding the quotient and remainder of x/y. Do this for $x = 111$ and $y = 19$. Make sure to provide the solution to each subproblem instance. Hint: there are eight subproblem instances, including the original problem instance.
Solution.

(b) Consider the RSA key set ($N = 221 = 13 \cdot 17, e = 7$). Determine the decryption key d.
Solution.

LO2. Solve the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 4T(n/8) + n^{\log_4 8}$. Defend your answer.
Solution. $n^{\log_8 4} = n^{\delta}$ for some $\delta < 1$, while $n^{\log_4 8} = n^{1+\varepsilon}$ for some $\varepsilon > 0$. Hence $f(n) = n^{1+\varepsilon} = \Omega(n^{\delta+\varepsilon'})$ for any $\varepsilon' < 1 + \varepsilon - \delta$. $\therefore$ By Case 3 of M.T. $T(n) = \Theta(n^{\log_4 8})$

(b) Use the substitution method to prove that, if $T(n)$ satisfies

$$T(n) = 4T(n/2) + 2n$$

then $T(n) = \mathrm{O}(n^2)$.

Solution.

Inductive assumption: $T(k) \le ck^2 + dk$ for all $k < n$, and for some constants $c > 0$ and d.

Show $T(n) \le cn^2 + dn$.

$$T(n) = 4T(n/2) + 2n \le 4c\left(\frac{n}{2}\right)^2 + d\left(\frac{n}{2}\right) + 2n$$

$$= cn^2 + \frac{d}{2}n + 2n \le cn^2 \iff d \le -4$$ ✓

LO3. Solve each of the following problems.

(a) Recall that the `find_statistic` algorithm makes use of Quicksort's partitioning algorithm and uses a pivot that is guaranteed to have at least

$$3(\lfloor \frac{1}{2} \lceil \frac{n}{5} \rceil \rfloor - 2) \ge 3(\frac{1}{2} \cdot \frac{n}{5} - 3) = \frac{3n}{10} - 9 \ge n/4$$

members of a on both its left and right sides, assuming $n \ge 200$. Rewrite all three inequalities/equalities with updated constants, assuming that the algorithm now uses groups of 11 instead of groups of 5. Give the rationale for how you decided to replace the 3 on the left side of the very first inequality.

Solution.

$$6\left(\left\lfloor \frac{1}{2} \left\lceil \frac{n}{11} \right\rceil \right\rfloor - 2\right) \ge 6\left(\frac{n}{22} - 3\right) = \frac{3n}{11} - 18 \ge \left(\frac{3n}{11} - \frac{n}{4}\right) \ge 18 \iff \frac{12n}{44} - \frac{11n}{44} \ge 18 \iff n \ge (44)(18)$$

(b) Use Strassen's products $P_1 = a(f-h) = af - ah$, $P_2 = (a+b)h = ah + bh$, $P_3 = (c+d)e = ce + de$, $P_4 = d(g-e) = dg - de$, $P_5 = (a+d)(e+h) = ae + ah + de + dh$, $P_6 = (b-d)(g+h) = bg + bh - dg - dh$, $P_7 = (a-c)(e+f) = ae - ce - cf + af$. to compute the matrix product

$$\begin{matrix} a & b \\ \end{matrix}\quad \begin{matrix} e & f \\ \end{matrix}$$

$$\begin{pmatrix} 4 & 2 \\ 1 & -3 \\ c & d \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -2 & 5 \\ g & h \end{pmatrix}$$

Show all work.

Solution.

$P_1 = 4(-6) = -24$
$P_2 = (6)(5) = 30$
$P_3 = (-2)(3) = -6$
$P_4 = (-3)(-5) = 15$
$P_5 = (1)(8) = 8$
$P_6 = (5)(3) = 15$
$P_7 = (3)(2) = 6$

$r = P_5 + P_6 - P_2 + P_4 = 8 + 15 - 30 + 15 = 8$
$s = af + bh = P_1 + P_2 = 6$
$t = ce + dg = P_3 + P_4 = -6 + 15 = 9$
$u = P_5 - P_7 - P_3 + P_1 = 8 - 6 + 6 - 24 = -16$

LO4. Solve each of the following problems.

(a) When deriving the formula for computing the inverse Fourier Transform DFT_n^{-1}, why is it necessary to divide by n once we have evaluated the polynomial at each of the inverses of the nth roots of unity? Where does the n come from?

Solution. The Fourier Transform Matrix F_n has entry $(F_n)_{ij} = \omega_n^{ij}$. The Inverse of this matrix is the basis for DFT_n^{-1}: $F_n^{-1} = \frac{1}{n}A$, where $A_{ij} = \omega_n^{-ij}$.

(b) Use the IFFT algorithm to compute $\mathrm{DFT}_8^{-1}(6, -5, -3, 4, -8, 2, -1, 10)$. Provide a recursion tree (without drawing its edges) and show the solutions to each subproblem instance. Show all work.

$\mathrm{DFT}_4^{-1}(6, -3, -8, -1) = \frac{1}{2}\left((-1, 7, -1, 7) + (1, -i, -1, i) \odot (-2, -1, -2, -1)\right)$

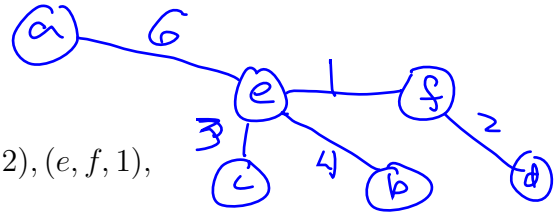
$= \left(-\frac{3}{2}, \frac{7+i}{2}, \frac{1}{2}, \frac{7-i}{2}\right)$

$\mathrm{DFT}_2^{-1}(6, -8) = \frac{1}{2}\left((6, 6) + (1, -1) \odot (-8, -8)\right) = (-1, 7)$

$\mathrm{DFT}_2^{-1}(-3, -1) = \frac{1}{2}\left((-3, -3) + (1, -1) \odot (-1, -1)\right) = (-2, -1)$

$\mathrm{DFT}_1^{-1}(6) = 6$ $\mathrm{DFT}_1^{-1}(-8) = -8$ $\mathrm{DFT}_1^{-1}(-3) = -3$ $\mathrm{DFT}_1^{-1}(-1) = -1$

LO5. For the weighted graph with edges

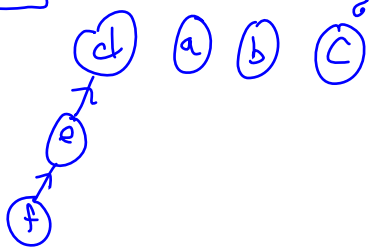


$$(a, e, 6), (b, e, 4), (c, e, 3), (c, f, 5), (d, f, 2), (e, f, 1),$$

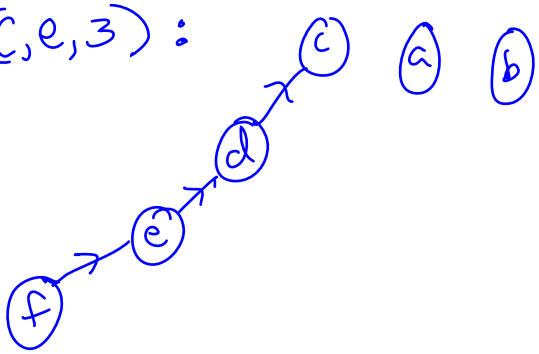
Show how the disjoint-set data structure forest changes when processing each edge in Kruskal's sorted list of edges. When unioning two trees, use the convention that the root of the union is the root which has the *lower* alphabetical order. For example, if two trees, one with root a, the other with root b, are to be unioned, then the unioned tree should have root a.

1. (e, f, 1):

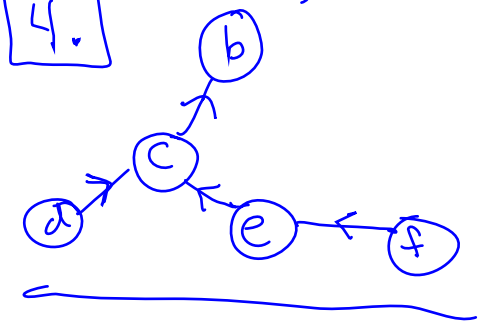
2. (d, f, 2):



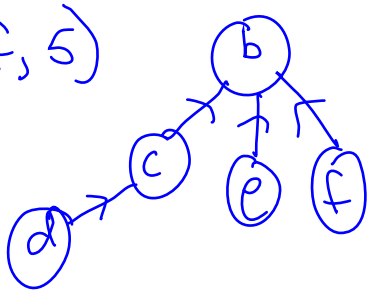
3. (c, e, 3):



4. (b, e, 4)



5. (c, f, 5)



6. (a, e, 6)