CECS 528, Learning Outcome Assessment 5, Pink With Solutions in Back, Fall 2023, 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) Find the multiplicative inverse of 21 mod 58.

(b) For the Strassen-Solovay primality test, is $a = 3$ an accomplice or witness to the fact that $n = 5$ is not prime? Show all work.

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.

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

$$T(n) = 2T(n/2) + 7n \log n$$

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

LO3. Solve each of the following problems.

(a) Recall the combine step of the `Minimum Distance Pair (MDP)` algorithm where, for each point P in the δ-strip, there is a $2\delta \times \delta$ rectangle whose bottom side contains P and is bisected by the vertical line that divides the points into left and right subsets. Explain why there can be at most 7 other points (from the problem instance) in this rectangle.

(b) Consider the following algorithm called `multiply` for multiplying two n-bit binary numbers x and y, where we assume n is even. Let x_L and x_R be the leftmost $n/2$ and rightmost $n/2$ bits of x respectively. Define y_L and y_R similarly. Let P_1 be the result of calling `multiply` on inputs x_L and y_L, P_2 be the result of calling `multiply` on inputs x_R and y_R, and P_3 the result of calling `multiply` on inputs $x_L + x_R$ and $y_L + y_R$. Then return the value $P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2$. For the two binary integers $x = 11010101$ and $y = 01101100$, determine the values of P_1, P_2, and P_3 at the root level of recursion, and verify that $xy = P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2$. Hint: you may evaluate P_1, P_2, and P_3 non-recursively using base-10.

LO4. Solve each of the following problems.

(a) When using the FFT algorithm to compute $\mathrm{DFT}_8^{-1}(6, -5, -3, 4, -8, 2, -1, 10)$, provide a list of all the subproblem instances that must be computed. Hint: there are 15 of them (including the original problem instance) and $\mathrm{DFT}_4^{-1}(-5, 4, 2, 10)$ is one of them.

(b) Compute $\text{DFT}_4(5, 2, 3, -4)$ using the FFT algorithm. Show the solution to each of the seven subproblem instances and, for each one, clearly represent it using DFT notation and apply the formula for computing it. Show all work.

LO5. Answer the following with regards to a correctness-proof outline for the Task Selection algorithm (TSA).

(a) Let $T = t_1, \ldots, t_m$ be the set of non-overlapping tasks selected by TSA and sorted by finish time, i.e. $f(t_i) < f(t_{i+1})$ for all $i = 1, \ldots, m-1$. Let T_{opt} be an optimal set of tasks and assume that, for some $k \geq 1$, $t_1, \ldots, t_{k-1} \in T_{\text{opt}}$, but $t_k \notin T_{\text{opt}}$. Explain why there must be at least one task $t' \in T_{\text{opt}}$ that overlaps with t_k. Hint: "Because if there was no such task ...".

(b) Explain why there is *at most* one task $t' \in T_{\text{opt}}$ that overlaps with t_k. Hint: assume there are two overlapping tasks, t' and t'', and explain why this creates a contradiction.

(c) Thus, we can define a new optimal set of tasks $\hat{T}_{\text{opt}} = T_{\text{opt}} - \{t'\} + \{t_k\}$ that contains $t_1, \ldots, t_k$. Continuing in this manner, we may obtain an optimal set of tasks T_{opt} for which $T \subseteq T_{\text{opt}}$. Moreover, we also have $T_{\text{opt}} \subseteq T$, since there is no way of add another task to T that does not overlap with one of T's tasks. For example, explain why it would not be possible to place a task t in between tasks t_i and t_{i+1} for some $i = 1, \ldots, m-1$. Therefore, we have established that $T = T_{\text{opt}}$ and TSA is correct.

Solutions

LO1. Solve the following problems.

(a) Find the multiplicative inverse of 21 mod 58.
Solution. We have

$$58 = 21(2) + 16,$$

$$21 = 16(1) + 5,$$

and

$$16 = 5(3) + 1.$$

Therefore, we have

$$16 + 5(-3) = 1 \Longleftrightarrow$$

$$16 + (21 - 16)(-3) = 21(-3) + 16(4) = 1 \Longleftrightarrow$$

$$21(-3) + (58 - 21(2))(4) = 58(4) + 21(-11) = 1 \Rightarrow (21)(-11) \equiv 1 \bmod 58.$$

(b) For the Strassen-Solovay primality test, is $a = 3$ an accomplice or witness to the fact that $n = 5$ is prime? Show all work.
Solution. We have $3^{\frac{5-1}{2}} = 3^2 = 9$. Also,

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Finally, $9 \equiv -1 \bmod 5$ and so $n = 3$ bears witness to the fact that 5 is a prime number.

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. By Case 3 of the Master Theorem, $T(n) = \Theta(n^{\log_4 8})$. This is because $n^{\log_8 4} = o(n^{\log_4 8})$.

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

$$T(n) = 2T(n/2) + 7n \log n$$

then $T(n) = \mathrm{O}(n \log^2 n)$.
Solution. Inductive Assumption: $T(k) \leq Ck \log^2 k$ for all $k < n$. Show $T(n) \leq Cn \log^2 n$. We have

$$T(n) = 2T(n/2) + 7n \log n \leq 2C(\frac{n}{2}) \log^2(\frac{n}{2}) + 7n \log n = Cn(\log n - 1)^2 + 7n \log n =$$

$$Cn\log^2 n - 2Cn\log n + 7n\log n + Cn \leq Cn\log^2 n \iff C(2\log n - 1) \geq 7\log n \iff$$
$$C \geq \frac{7}{2 - \frac{1}{\log n}},$$

which is true so long as $C \geq 4$ and n is sufficiently large. This is because, as n increases, the right side converges to 3.5.

LO3. Solve each of the following problems.

(a) Recall the combine step of the `Minimum Distance Pair (MDP)` algorithm where, for each point P in the δ-strip, there is a $2\delta \times \delta$ rectangle whose bottom side contains P and is bisected by the vertical line that divides the points into left and right subsets. Explain why there can be at most 7 other points (from the problem instance) in this rectangle.

Solution. The $2\delta \times \delta$ rectangle consists of two $\delta \times \delta$ squares, one on each side of the problem-instance dividing line. Moreover, we know that any two points in the data set that are both on one side of the dividing line are at least δ away from each other. Therefore, in a $\delta \times \delta$ square there can be at most 4 points in the data set within that square. And so the $2\delta \times \delta$ rectangle can contain at most 4+4 = 8 data points, one of which is point P. That leaves at most 7 other points in the rectangle.

(b) Consider the following algorithm called `multiply` for multiplying two n-bit binary numbers x and y, where we assume n is even. Let x_L and x_R be the leftmost $n/2$ and rightmost $n/2$ bits of x respectively. Define y_L and y_R similarly. Let P_1 be the result of calling `multiply` on inputs x_L and y_L, P_2 be the result of calling `multiply` on inputs x_R and y_R, and P_3 the result of calling `multiply` on inputs $x_L + x_R$ and $y_L + y_R$. Then return the value $P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2$. For the two binary integers $x = 11010101$ and $y = 01101100$, determine the values of P_1, P_2, and P_3 at the root level of recursion, and verify that $xy = P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2$. Hint: you may evaluate P_1, P_2, and P_3 non-recursively using base-10.

Solution. We have $x = 213$, $y = 108$, $x_L = 13$, $x_R = 5$, $y_L = 6$, and $y_R = 12$. Thus, $P_1 = 78$, $P_2 = 60$, and $P_3 = (18)(18) = 324$. Then

$$P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2 = (78)(256) + (324 - 78 - 60)(16) + 60 = 23004 = xy = (213)(108).$$

LO4. Solve each of the following problems.

(a) When using the FFT algorithm to compute $\mathrm{DFT}_8^{-1}(6, -5, -3, 4, -8, 2, -1, 10)$, provide a list of all the subproblem instances that must be computed. Hint: there are 15 of them (including the original problem instance) and $\mathrm{DFT}_4^{-1}(-5, 4, 2, 10)$ is one of them.

Solution. $\mathrm{DFT}_8^{-1}(6, -5, -3, 4, -8, 2, -1, 10)$, $\mathrm{DFT}_4^{-1}(6, -3, -8, -1)$, $\mathrm{DFT}_4^{-1}(-5, 4, 2, 10)$, $\mathrm{DFT}_2^{-1}(6, -8)$, $\mathrm{DFT}_2^{-1}(-3, -1)$, $\mathrm{DFT}_2^{-1}(-5, 2)$, $\mathrm{DFT}_2^{-1}(4, 10)$, $\mathrm{DFT}_1^{-1}(6)$, $\mathrm{DFT}_1^{-1}(-5)$, $\mathrm{DFT}_1^{-1}(-3)$, $\mathrm{DFT}_1^{-1}(4)$, $\mathrm{DFT}_1^{-1}(-8)$, $\mathrm{DFT}_1^{-1}(2)$, $\mathrm{DFT}_1^{-1}(-1)$, $\mathrm{DFT}_1^{-1}(10)$.

(b) Compute $\mathrm{DFT}_4(5, 2, 3, -4)$ using the FFT algorithm. Show the solution to each of the seven subproblem instances and, for each one, clearly represent it using DFT notation and apply the formula for computing it. Show all work.

Solution. We have

$$\mathrm{DFT}_1(5) = 5 \text{ and } \mathrm{DFT}_1(3) = 3.$$

$$\mathrm{DFT}_2(5,3) = (5,5) + (1,-1) \odot (3,3) = (8,2).$$

$$\mathrm{DFT}_1(2) = 2 \text{ and } \mathrm{DFT}_1(-4) = -4.$$

$$\mathrm{DFT}_2(2,-4) = (2,2) + (1,-1) \odot (-4,-4) = (-2,6).$$

$$\mathrm{DFT}_4(5,2,3,-4) = (8,2,8,2) + (1,i,-1,-i) \odot (-2,6,-2,6) = (6,2+6i,10,2-6i).$$

LO5. Answer the following with regards to a correctness-proof outline for the Task Selection algorithm (TSA).

(a) Let $T = t_1, \ldots, t_m$ be the set of non-overlapping tasks selected by TSA and sorted by finish time, i.e. $f(t_i) < f(t_{i+1})$ for all $i = 1, \ldots, m-1$. Let T_{opt} be an optimal set of tasks and assume that, for some $k \geq 1$, $t_1, \ldots, t_{k-1} \in T_{\text{opt}}$, but $t_k \notin T_{\text{opt}}$. Explain why there must be at least one task $t' \in T_{\text{opt}}$ that overlaps with t_k. Hint: "Because if there was no such task ...".

Solution. Because if there was no such task, then one could add t_k to T_{opt} and obtain a better solution, which contradicts T_{opt} being optimal.

(b) Explain why there is *at most* one task $t' \in T_{\text{opt}}$ that overlaps with t_k. Hint: assume there are two overlapping tasks, t' and t'', and explain why this creates a contradiction.

Solution. If two tasks t' and t'' from T_{opt} overlapped with t_k, then one of the two, say t' would have a finish time that comes before the finish time of t_k (why ?). Moreover, since $t_{k-1} \in T_{\text{opt}}$, t' would start at or after t_{k-1}. Thus, in round k the algorithm would have selected t' instead of t_k.

(c) Thus, we can define a new optimal set of tasks $\hat{T}_{\text{opt}} = T_{\text{opt}} - \{t'\} + \{t_k\}$ that contains $t_1, \ldots, t_k$. Continuing in this manner, we may obtain an optimal set of tasks T_{opt} for which $T \subseteq T_{\text{opt}}$. Moreover, we also have $T_{\text{opt}} \subseteq T$, since there is no way of add another task to T that does not overlap with one of T's tasks. For example, explain why it would not be possible to place a task t in between tasks t_i and t_{i+1} for some $i = 1, \ldots, m-1$. Therefore, we have established that $T = T_{\text{opt}}$ and TSA is correct.

Solution. If there is a task t that occurs between t_i and t_{i+1}, then in round $(i+1)$ TSA would have selected t instead of t_{i+1} since t starts at or after the end of t_i and finishes before t_{i+1}.