# CS 170 Fall 2008 - Solutions to Midterm 1

October 14, 2008

1
1. True: $n \log n \leq n^2$.
2. False: $\lim_{n\to\infty} \frac{n^2}{n \log n} = \infty$.
3. True: $2^{c \log_2 n} = \left(2^{\log_2 n}\right)^c = n^c$.
4. False (not always True): For $f(n) = c \log_2 n = O(\log n)$, we have $2^{f(n)} = n^c$ which is not $O(n^3)$ for $c > 3$.
5. True: $\log_{100} 50000 < 2.5$ because $100^{2.5} = 100000 > 50000$; hence by Master's theorem, $T(n) = \Theta(n^{\log_{100} 50000}) = o(n^{2.5})$.
6. False.
7. If we apply Master's theorem, $a = b = 3$ and $c = 1$; since $\log_b a = c$, we have $T(n) = n \log n$.
8. True: $\gcd(3, 8) = 1$ and in fact $3^{-1} = 3$.
9. True: We cannot have $4x = 1 \bmod 8$, since then $4x = 8k + 1$, and 1 would be a multiple of 4, a contradiction.
10. True: There are approximately $N/\ln(N)$ prime numbers $\leq N$. Thus the probability that an $n$-bit number is prime is approximately $\frac{N/\ln(N)}{N} = \frac{1}{\ln(N)}$ for $N = 2^n$. That would be $\approx \frac{\ln 2}{n} = \Theta(\frac{1}{n})$.
11. True.
12. True: Let $u$ be the vertex with lowest post order number that is not a sink. Then there exists some edge $(u, v)$. If vertex $v$ is visited while exploring $u$, then $\text{post}[v] < \text{post}[u]$; hence that cannot happen. This means $v$ is already visited once we begin to explore $u$, but then the edge $(u, v)$ would be a backedge, and the graph would have a cycle, contradicting the fact that the graph is a DAG.
13. False: The graph with vertex set $V = \{1, 2, 3\}$ and edge set $E = \{(1, 2), (2, 1), (1, 3)\}$ is a counterexample. We can have $\text{pre}[1] = 1$, $\text{pre}[2] = 2$, $\text{post}[2] = 3$, $\text{pre}[3] = 4$, $\text{post}[3] = 5$, $\text{post}[1] = 6$, and then vertex 2 has lowest post order but the strongly connected component $\{1, 2\}$ is not a sink strongly connected component, since it has the outgoing edge $(1, 3)$ to the strongly connected component $\{3\}$.

14. $\Theta(n)$: If the graph has a path of length $n-1$, the DFS stack may contain $n$ vertices.
15. $O(\log n)$: The stack space is at most $O(\log n)$, the depth of the tree.

2

1. $N = 77 = pq$ for $p = 7,\ q = 11$. We have $(p-1)(q-1) = 60$ and $d = 7^{-1} \mod 60$. To calculate inverse of 7, we use Extended Euclid algorithm:

$$\begin{aligned} 60 &= 8 \cdot 7 + 4, \\ 7 &= 1 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1. \end{aligned}$$

Thus

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4)) = 2 \cdot 4 + (-1) \cdot 7 \\ &= 2 \cdot (60 - 8 \cdot 7) + (-1) \cdot 7 = 2 \cdot 60 + (-17) \cdot 7. \end{aligned}$$

Hence $(-17) \cdot 7 = 1 \mod 60$ and $d = 7^{-1} = -17 = 43 \mod 60$.

2. Since $\gcd(3, 60) = 3 \neq 1$, we cannot choose $d$ as inverse of $e$.

3

1. $1,\ i,\ -1,\ -i$.
2. $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & 1 & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}.$
3. $\mathrm{FFT}^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & 1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{4} \end{pmatrix}.$

4

1. Let $u_1, \ldots, u_k$ be neighbors of $u$. Vertex $u$ is on a cycle if and only if $[\mathrm{pre}(u_1), \mathrm{post}(u_1)], \ldots, [\mathrm{pre}(u_k), \mathrm{post}(u_k)]$ are disjoint intervals.

   *Proof*: ($\Rightarrow$ part) If $u$ is not on a cycle, then removing $u$ partitions the graph into $k$ subgraphs $G_1, \ldots, G_k$ such that $u_i \in V(G_i)$. DFS on $u$ proceeds by first visiting $u$, then exploring $G_1$ completely, then exploring $G_2$ completely, and so on. Therefore $\mathrm{pre}(u_1) < \mathrm{post}(u_1) < \mathrm{pre}(u_2) < \mathrm{post}(u_2) < \ldots < \mathrm{pre}(u_k) < \mathrm{post}(u_k)$.

   ($\Leftarrow$ part) If $[\mathrm{pre}(u_i), \mathrm{post}(u_i)]$ intersects $[\mathrm{pre}(u_j), \mathrm{post}(u_j)]$, then without loss of generality, we can assume $\mathrm{pre}(u_i) < \mathrm{pre}(u_j) < \mathrm{post}(u_j) < \mathrm{post}(u_j)$. This means that there is a path $P$ from $u_i$ to $u_j$ that does not use vertex $u$. Therefore $u$ is on the cycle $(u, u_i) + P + (u_j, u)$.

2. In fact, we can have a graph where $u$ and $v$ are in the same strongly connected component, and yet pre and post intervals of $u$ and $v$ are disjoint: In directed graph $G = (V, E)$ with vertex set $V = \{a, b, u, v\}$

and edge set $E = \{a, b), (b, u), (u, a), (b, v), (v, a)\}$, we have $\text{pre}(a) = 1$, $\text{pre}(b) = 2$, $\text{pre}(u) = 3$, $\text{post}(u) = 4$, $\text{pre}(v) = 5$, $\text{post}(v) = 6$, $\text{post}(b) = 7$, $\text{post}(a) = 8$, and yet $G$ is strongly connected.

5

1. To find the $k$th smallest number of $n$ numbers:
   1. Divide the $n$ numbers into $n/5$ groups of size 5.
   2. Let $S$ be the set of the medians of these groups. Since finding the median of a set of size 5 takes $O(1)$ time, $S$ can be found in $O(n)$ time.
   3. Find $x = \text{median}(S)$ recursively using $T(n/5)$ time.
   4. Split the $n$ numbers into three sets: $S_L$, $\{x\}$, $S_R$, where $S_L$ is the set of numbers $< x$ and $S_R$ is the set of numbers $> x$. Finding $S_L$ and $S_R$ can be done in $O(n)$ time.
   5. If $k \leq |S_L|$, recursively find the $k$th smallest element in $S_L$; else if $k = |S_L| + 1$, return $x$; else since $k > |S_L| + 1$, recursively find the $(k - |S_L| - 1)$th smallest element in $S_R$. Since we know that $|S_L|, |S_R| \geq 3n/10$, we have $|S_L|, |S_R| \leq 7n/10$, and the recursive call takes $\leq T(7n/10)$ time.

   The total running time amounts to

   $$T(n) = T(n/5) + T(7n/10) + O(n).$$

2. We can prove by induction that $T(n) \leq cn$ for suitable constant $c$:

   $$T(n) = T(n/5) + T(7n/10) + O(n) \leq cn/5 + c \cdot 7n/10 + Cn \leq cn,$$

   as long as $(1/5 + 7/10)c + C \leq c$ or equivalently $c \geq 10C$. Therefore $T(n) = O(n)$.

   (Notice that in the above analysis it is crucial that $1/5 + 7/10 < 1$. Would this recursive algorithm still have $O(n)$ running time if we had divided the numbers into groups of 3 rather than groups of 5?)