1,2

Practice Exam Solutions

see posted typeset notes later! Canvas files, solutions

T 1.1 $a^{n+1} = O(a^n)$? True. $a^{n+1} = a a^n = O(a^n)$.
~~If a increases,~~

F 1.2 $a^{2n} = O(a^n)$? $a^{2n}/a^n = a^n$ which diverges.
Also $a^{2n} = (a^2)^n$. $(c+\varepsilon)^n >> c^n$.

F 1.3 $f = \Omega(p)$ and $f = O(q) \Rightarrow \forall n \in \mathbb{R}$ that $p(n) \leq q(n)$?
false! Big O only says about asymptotics. may exist small values of n, with $p(n) \geq q(n)$

F 1.4 $a > b$, $n^a - n^b$ is $O(n^{a-b})$. False. $n^3 - n^2 = \Omega(n^3)$ and not $O(n^{3-2}) = O(n)$. $n^3 - n^2$ is not $O(n)$.

T 1.5 $n^b - n^a = O(n^a)$ when $a > b$? for large enough n, This is infact, negative, so is $O(1)$ and is then $O(n^a)$ certainly

F 1.6 $O(n^a) - O(n^a) = 0$. underspecified but still false.
$2n^3 - n^3 = n^3 \neq 0$.

2.1 $f(n) = n^3 + 2n$, $g(n) = 12n^2 + 21\sqrt{n}$, $g(n) = O(f(n))$

2.2 $f(n) = (\log n)^2$, $g(n) = \log n + \sqrt{n}$ ($n^{0.5}$) You can prove $(\log n)^k = O(n^c)$ for any $k, c > 0$. So even $(\log n)^{100} << n^{0.01}$ eventually.
To prove, use Lopitals.

2.3 $f(n) = 2\log_5(3^n)$, $g = n + 4n^{0.2}$ $f = O(g)$, $g = O(f)$

2.4 $f(n) = 8^{\log_2 n}$, $g = n\log n$. $g(n) = O(f(n))$ $8^{\log_2 n} =$

1.06 $n^{\log_2 8}$. Since $\log_2 8 > 1$, $f(n) = n^{1+\varepsilon}$ for some $\varepsilon > 0$. $\frac{f(n)}{g(n)} = \frac{n^{1+\varepsilon}}{n\log n} =$

$\frac{n^\varepsilon}{\log n}$ diverges. recall $\forall c > 0$ that $\log n << n^c$.

3

First we prove the closed form of the geometric series in the infinite case.

$x = 1 + c + c^2 + c^3 + \dots$ so $x = 1 + cx$

$= 1 + c(\cancel{1} + c + c^2 + \dots)$ $x - cx = 1$

$= 1 + cx$ $x = \frac{1}{1-c}$.

only technically true when ~~...~~ $c < 1$.

Now consider the bounded summation

$1 + c + c^2 + c^3 + \dots + c^n =$ and notice

$(1 + c + c^2 + \dots) - c^{n+1} - c^{n+2} - c^{n+3} - \dots =$

$(1 + c + c^2 + \dots) - c^{n+1}(1 + c + c^2 + \dots) =$

$x - c^{n+1}x = x(1 - c^{n+1}) = \boxed{\frac{1 - c^{n+1}}{1-c}} = g(n)$

If $c < 1$ then $c^{n+1} < c$ so $\lim_{n\to\infty} g(n) \cancel{=} 0$ so $g(n) = O(1)$

if $c = 1$ then $1 + c + c^2 + \dots c^n = \overbrace{1 + 1 + 1 + 1 + \dots + 1}^{n} = O(n)$.

if $c > 1$ then $c^{n+1} > c$ so $\frac{1 - c^{n+1}}{1-c} = \frac{1}{1-c} - \frac{c^{n+1}}{1-c} =$

$\frac{1}{1-c} \frac{-c}{1-c} c^n = \frac{1}{1-c} + \frac{c}{c-1} c^n = O(c^n)$.

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

4.1 $T(n) = 2T(n/4) + O(n)$ $\quad a,b,d = 2,4,1$

$\log_4 2 < 1$ so so $O(n)$

4.2 $T(n) = 2T(n/4) + O(1)$ $\quad a,b,d = 2,4,0$

$\log_4 2 = \log_4(\sqrt{4}) = \frac{1}{2}\log_2 \log_4 2 > 0$ so $O(\sqrt{n})$

4.3 $T(n) = 2T(n/4) + O(\sqrt{n})$ $\quad a,b,d = 2,4,\frac{1}{2}$

$d = \log_b a$ so $O(\sqrt{n}\log n)$

4.4 $T(n) = 3T(n/3) + O(1)$ $\quad a,b,d = 3,3,0$ so $O(n)$

$\log_3 3 = 1 > 0$

4.5 $T(n) = 4T(n/3) + O(n^2)$ $\quad a,b,d = 4,3,2$ so

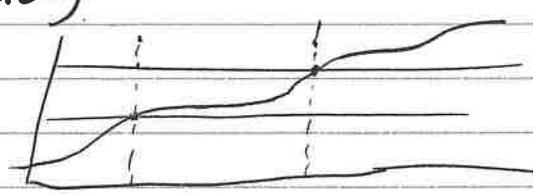
$\log_3 4 < 2$ so $O(n^2)$

$\log_3 9 = 2$

4.6 $T(n) = 5T(2n/3) + O(n^2)$ $\quad a,b,d = 5, 3/2, 2$

$2 < \log_{3/2} 5$ so $O(n^{\log_{3/2} 5})$

5 Just two binary searches



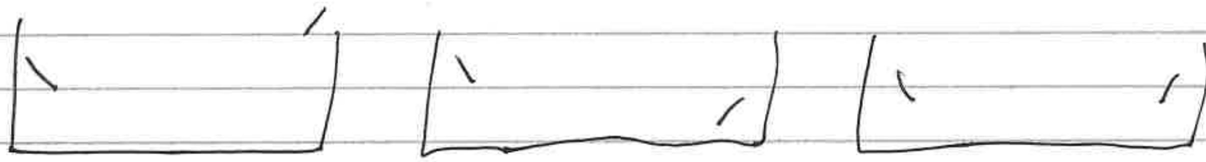
binary search to find the smallest i with $A[i] \geq u$. same for j so $A[j] \geq l$.

note, two top level recursions is not a recursion at each level

$T(n) = T(n/2) + O(1)$ $\quad a \neq 2$.

6 Busy work, but instructive.

7 Given boundary conditions $A[1] \geq A[2]$ and $A[n-1] \leq A[n]$ we know there must exist a local minima.

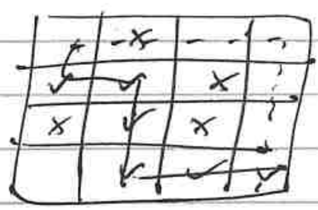


Pick middle point. If $A[i-1] \geq A[i] \leq A[i+1]$ return i. else, compute slope of $A[i-1]$, $A[i+1]$

local min | local min on down sides. | local min on both sides

recurse on downward side. $T(n) = T(n/2) + O(1) = O(\log n)$.

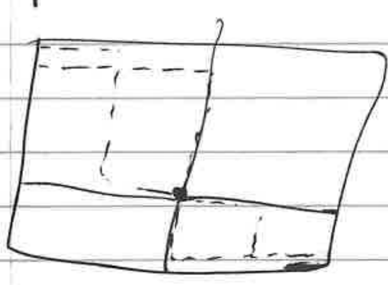
8a Each next cell has 2 possible choices, try each for n^2 long path



each path takes n to write down and there are at most n queries giving us $O(n^2)$.

8b Every path hits every row/column in one spot. Choose middle path and recurse split it into two subproblems each of size $n/2$

so $T(n) = 2T(n/2) + O(n) = O(n \log n)$.



8c a .3 $O(\max(mn, n^2, m^2))$

b .5 $O((m+n) \log(\max(m,n)))$

FLT : $a^{p-1} \equiv 1 \pmod{p}$

9.1 $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7 =$

$2^{18}2^{2} + 3^{6\cdot 5} + 4^{4}4^{36} + 5^{2}5^{48} + 6^{6\cdot 10} \equiv 2^{2} + 3^{0} + 4^{4} + 5^{2} + 6^{0} \equiv$

(256)%7 =4 $4+1+4+4+1 \equiv 1\cancel{6}4 \equiv 0 \bmod 7$

25%7 = 21+4 =4

9.2 what x is $x^{103} \equiv 4 \pmod{11}$ only try $\{0 \ldots 10\}$

$x^{10} \equiv 1 \pmod{11}$ so $x^{103} = x^{100}x^{3} \equiv (x^{10})^{10} x^{3} \equiv 1 \cdot x^{3} \bmod 11$

so compute $0 \ldots 10$ cubed mod 7.

$0^3 \equiv 0$

$1^3 \equiv 1$

$2^3 \equiv 8 \equiv$

$4^3 \equiv 64 \equiv 9$

$5^3 \equiv 125 \equiv 121 + 4 \equiv 4 \bmod 11$, so answer is 5.

10.1 Jerry makes keys

10.2 $p=23, q=29, e=3, d=411$

10.3 $m^e \bmod N = (15)^3 \bmod (23\cdot 29) = 40$

10.4 $m^e \bmod N$ if m is small, and e is small, $m^e \ll 2^{4000}$ so just take cube root instead of discrete log.