CS170–Fall 2013 — Solutions to Homework 1

Zackery Field, section Di 109, cs170-fe

September 6, 2013

1. Getting Started

I understand the course policies.

2. Compare Growth Rates

"Commonsense rules"

(a) Multiplicative constants can be omitted: $14 \log n = O(\log n)$

(b) n^a dominates n^b if $a > b$: $O(n^2) > O(n)$

(c) Any exponential dominates any polynomial: 3^ndominates n^{100}(it also dominates $a^n$where $a < n$)

(d) Any polynomial dominates any logarithm: n dominated $(\log n)^3$. Another: n^2 dominates $nlogn$

Begin problems:

(a) $f(n) = n^{3.75}$, $g(n) = n^{2.72}$
$f(n) = \Omega(g(n))$, by rule (b) where $f(n) = n^a$ and $g(n) = n^b$.

(b) $f(n) = 10n - (\log n)^2$, $g(n) = n + \log n$
$f(n) = 10n - (\log n)^2 = O(n)$, by rules (a) and (d)
$g(n) = n + \log n = O(n)$, by rule (d)
$\therefore f(n) = \Theta(g(n))$

(c) $f(n) = n^3 + 1000$, $g(n) = n^3 - 1000$
$f(n) = O(n^3)$, by rule (b)
$g(n) = O(n^3)$, by rule (b)
$\therefore f(n) = \Theta(g(n))$

(d) $f(n) = \log 500n$, $g(n) = \log 8n$

$$\begin{aligned} f(n) &= \log 500n \\ &= \log 500 + \log n \\ &= O(\log n) \text{ , } \log n \text{dominates } \log 500 \\ g(n) &= \log 8n \\ &= \log 8 + \log n \\ &= O(\log n) \end{aligned}$$

$\therefore f(n) = \Theta(g(n))$

(e) $f(n) = 5\log n$, $g(n) = \log(n^7)$

$$\begin{aligned} f(n) &= 5\log n \\ &= O(\log n) \\ g(n) &= \log(n^7) \\ &= 7\log n \\ &= O(\log n) \end{aligned}$$

$\therefore f(n) = \Theta(g(n))$

(f) $f(n) = 5n\log 5n$, $g(n) = n\log n$

$$\begin{aligned} f(n) &= 5n\log 5n \\ &= 5n\log 5 + 5n\log n \\ &= O(n\log n) \\ g(n) &= O(n\log n) \end{aligned}$$

$\therefore f(n) = \Theta(g(n))$

(g) $f(n) = \frac{n^3}{\log n}$, $g(n) = n^4(\log n)^3$

$$\begin{aligned} \frac{f(n)}{g(n)} &= \frac{\frac{n^3}{\log n}}{n^4(\log n)^3} \\ &= \frac{n^3}{n^4(\log n)^4} \\ &= \frac{1}{n(\log n)^4} \text{ which is not bounded} \end{aligned}$$

$\therefore f(n) = O(g(n))$

(h) $f(n) = n(\log n)^5$, $g(n) = n^{1.01}$

$$\begin{aligned} \frac{f(n)}{g(n)} &= \frac{n(\log n)^5}{n^{1.01}} \\ &= \frac{(\log n)^5}{n^{0.01}} \text{ which is not bounded} \end{aligned}$$

$\therefore f(n) = O(g(n))$, by rule (d).

(i) $f(n) = (logn)^{100}$, $g(n) = n^{0.01}$
$f(n) = O(g(n))$, by rule (d)

(j) $f(n) = \sqrt[3]{n}$, $g(n) = (\log n)^2$
$f(n) = \Omega(g(n))$, by rule (d)

(k) $f(n) = n \log n$, $g(n) = (\log n)^{\log n}$

$$\begin{aligned} \frac{f(n)}{g(n)} &= \frac{n \log n}{(\log n)^{\log n}} \\ &= \frac{n}{(\log n)^{(\log n - 1)}} \text{ which is not bounded} \end{aligned}$$

$\therefore f(n) = \Omega(g(n))$, by rule (d)

(l) $f(n) = n^{\frac{1}{3}}$, $g(n) = 3^{\log_2 n}$
$f(n) = O(g(n))$, by rule (c)

(m) $f(n) = 5^n$, $g(n) = n4^n$

(n) $f(n) = 2^n$, $g(n) = 2^{3n}$
Lemma I : If $f(n) \neq O(g(n))$ then $f(n) = \Omega(g(n))$, follows from the definition of big O notation.
if $f(n) = O(g(n))$, then$\exists c$ s.t. $f(n) = c * g(n)$, where c is constant.

$$\begin{aligned} f(n) &= c * g(n) \\ 2^n &= c * 2^{3n} \\ \log_2(2^n) &= \log_2(c * 2^{3n}) \\ n &= \log_2 c + 3n \\ n &= c + 3n \\ c &= -2n \end{aligned}$$

$\forall n$, $\nexists$c, $c = -2n$. $\therefore f(n) = \Omega(g(n))$, by lemma I.

(o) $f(n) = 7^n$, $g(n) = 7^{n-1}$
if $f(n) = O(g(n))$, then $\exists c$ s.t. $f(n) = c * g(n)$, where c is constant.

$$\begin{aligned}
f(n) &= c * g(n) \\
7^n &= c * 7^{n-1} \\
\log_7(7^n) &= \log_7 c + \log_7(7^{n-1}) \\
n &= c + n - 1 \\
c &= 1
\end{aligned}$$

The reverse can also be shown. Explicitly, $\frac{1}{7}f(n) = g(n)$, and $f(n) = 7 * g(n)$
$\therefore f(n) = \Theta(g(n))$

(p)

(q)

3. Prove Order of Growth

1. Show that, for any constant k,

$$\sum_{i=1}^{n} i^k = \Theta(n^{k+1})$$

Take $f(n) = \sum_{i=1}^{n} i^k$ and $g(n) = n^{k+1}$. Showing that $f(n) = \Theta(g(n))$ is equivalent to showing that $f(n) = O(g(n)) \wedge g(n) = O(f(n))$. Showing that $f(n) = O(g(n))$:

$$\begin{aligned}
\sum_{i=1}^{n} i^k &= 1^k + 2^k + \cdots + n^k \\
&= O(n^k) \text{ , dropping lower order terms} \\
&= O(n^{k+1}) \\
&= O(g(n))
\end{aligned}$$

Showing that $f(n) = \Omega(g(n))$, take $g(n) = (\frac{n}{2})^k$

$$\begin{aligned}
\lim_{n\to\infty} \frac{f(n)}{g(n)} &= \lim_{n\to\infty} \frac{1^k + 2^k + \cdots + n^k}{(\frac{n}{2})^k} \\
&= \lim_{n\to\infty} \frac{1^k}{(\frac{n}{2})^k} + \frac{2^k}{(\frac{n}{2})^k} + \cdots + \frac{(\frac{n}{2})^k}{(\frac{n}{2})^k} + \cdots + \frac{n^k}{(\frac{n}{2})^k} \\
&= 1 + \cdots + 2^k > 0\text{, and finite}
\end{aligned}$$

Now $(\frac{n}{2})^k$ needs to be related to n^{k+1}.

$$\begin{aligned}
\lim_{n\to\infty} \frac{n^{k+1}}{(\frac{n}{2})^k} &= \lim_{n\to\infty} (\frac{n^k}{(\frac{n}{2})^k} + \frac{n}{(\frac{n}{2})^k}) \\
&= \lim_{n\to\infty} (2^k + \frac{n}{(\frac{n}{2})^k}) \\
&= 2^k > 0\text{, and finite.} \\
\therefore \quad (\tfrac{n}{2})^k &= \Theta(n^{k+1})
\end{aligned}$$

$\therefore \sum_{i=1}^{n} i^k = \Omega(n^{k+1}) \wedge \sum_{i=1}^{n} i^k = \Theta(n^{k+1})$ $\square$

2. Show that

$$\log(n!) = \Theta(n \log n)$$

Since this relation is considering asymptotic (large n) behavior I will apply Stirling's approximation. If the equation below can be shown then showing the initial relation is trivial.

$$\ln(n!) = \Theta(n \ln n)$$

Stirling's approximation

$$\begin{aligned}
\ln(n!) &= \ln(n*(n-1)*\cdots*2*1) \\
&= \ln(n)+\ln(n-1)+\cdots+\ln(2) \\
&= \sum_{i=2}^{n}\ln(x) \\
&\approx \int_{2}^{n}\ln(x)dx \\
&= [x\ln x - x]_2^n \\
&= (n\ln n - n) - (2\ln 2 - 2) \\
&\approx n\ln n - n, \text{ for large n } (>100)
\end{aligned}$$

Now to show the asymptotic relation

$$\begin{aligned}
\lim_{n\to\infty}\frac{\ln(n!)}{n\ln n} &\approx \lim_{n\to\infty}\frac{n\ln n - n}{n\ln n} \\
&= \lim_{n\to\infty}\frac{n\ln n}{n\ln n}+\frac{n}{n\ln n} \\
&= 1>0,\text{and finite}
\end{aligned}$$

$\therefore \log(n!) = \Theta(n\log n)$ $\square$

3. Show that

$$\sum_{i=1}^{n}\frac{1}{i} = \Theta(logn)$$

4. Geometric Series

Show that, if c is a positive real number, then $g(n) = 1 + c + c^2 + \cdots + c^n$ is:

(a) $\Theta(1)$ if $c < 1$
If $c < 1$ $\exists$ a representation of $c = \frac{1}{t}$, where t is a positive integer.

$$g(n) = 1 + \frac{1}{t} + \frac{1}{t^2} + \cdots + \frac{1}{t^n}$$

For the sake of clarity, $g(n) = \Theta(1)$ iff $\lim_{n\to\infty} \frac{g(n)}{1} > 0$ and finite,

$$\begin{aligned}
\lim_{n\to\infty} g(n) &= 1 + \frac{1}{t} + \frac{1}{t^2} + \cdots + \frac{1}{t^n} \\
&= 1
\end{aligned}$$

$\therefore g(n) = \Theta(1)$ if $c < 1$ $\square$

(b) $\Theta(n)$ if $c = 1$
$g(n) = \Theta(n)$ iff $\lim_{n\to\infty} \frac{g(n)}{n} > 0$ and finite

$$\begin{aligned}
\lim_{n\to\infty} \frac{g(n)}{n} &= \lim_{n\to\infty} \frac{1 + 1 + 1^2 + \cdots + 1^n}{n} \\
&= \lim_{n\to\infty} \frac{n+1}{n} \\
&= 1
\end{aligned}$$

$\therefore g(n) = \Theta(n)$ if $c = 1$ $\square$

(c) $\Theta(c^n)$ if $c > 1$
$g(n) = \Theta(c^n)$ iff $\lim_{n\to\infty} \frac{g(n)}{c^n} > 0$ and finite

$$\begin{aligned}
\lim_{n\to\infty} \frac{g(n)}{c^n} &= \lim_{n\to\infty} \frac{1 + c + c^2 + \cdots + c^n}{c^n} \\
&= \lim_{n\to\infty} \frac{1}{c^n} + \frac{c}{c^n} + \frac{c^2}{c^n} + \cdots + \frac{c^{n-1}}{c^n} + \frac{c^n}{c^n} \\
&= \lim_{n\to\infty} 0 + \cdots + \frac{1}{c^2} + \frac{1}{c} + 1 \\
&= 1 + N, \text{ where } 0 < N < 1
\end{aligned}$$

$1 + N > 0$ and finite. $\therefore g(n) = \Theta(c^n)$ if $c > 1$. $\square$

5. Fibonacci Numbers

Show that for any $n > 1$, $\gcd(F_{n+1}, F_n) = 1$

GCD addition Lemma: If $\gcd(a, b) = z$, for $z, a, b \in \mathbb{Z}$, then $\gcd(a + b, b) = z$.

$$
\begin{aligned}
\gcd(a, b) &= z \\
z &= xa + yb \\
\gcd(a + b, b) &= z' \\
z' &= x(a + b) + yb
\end{aligned}
$$

Then since $z'|b$ and $z'|(a + b)$, $z'|a$ also, by $z'|(a + b) - a \Rightarrow z'|z$. By definition $z|a$ and $z|b$ and $z|(a + b) \Rightarrow z|z'$. Since z and z' are both the greatest possible common divisor, $z|z'$, and $z'|z$ then $z = z'$.$\square$

Proof by Induction on n:

Base Cases: $\gcd(F_2, F_1) = \gcd(1, 1) = 1$

Inductive Hypothesis: For arbitrary n, $\gcd(F_{n+1}, F_n) = 1$.

Inductive Step: For $n + 1$,

$$
\begin{aligned}
\gcd(F_{n+2}, F_{n+1}) &= \gcd(F_{n+1} + F_n, F_{n+1}) \\
&= \gcd(F_{n+1}, F_n), \text{ by the GCD addition lemma} \\
&= 1
\end{aligned}
$$

$\therefore \gcd(F_{n+1}, F_n) = 1 \ \forall n \geq 1\square$

6. Modular Arithmetic

Prove or disprove:

If a has an inverse modulo b, then b has an inverse modulo a.

If a has an inverse modulo b then $\exists c, c \in \mathbb{Z}^+$ s.t. $ac \equiv 1 \mod b$. This can also be written as $ac = 1 + kb : (1)$, where k is some positive integer. Since c is an integer $a|(kb+1)$.Converting equation(1) to $b \mod a$ will then take on the form, $kb + 1 \equiv \mod a : (2)$. Then it is the case that $-k$ is multiplicative inverse of $b \mod a$.
$\therefore$if $\exists c$ s.t. $ac \equiv 1 \mod b$,then $\exists d$ s.t. $db \equiv 1 \mod a$. $\square$