CSI2101 Discrete Structures Winter 2009: Extra material: recurrence relations and number theory

Lucia Moura

Winter 2009

Master Theorem for Divide-and-Conquer Recurrence Relations

Theorem (Master Theorem)

Let f be an increasing function that satisfies the recurrence relation:

$$f(n) = af(n/b) + cn^d,$$

whenever $n = b^k$, where k is a positive integer, $a \geq 1$, b is an integer greater than 1, and c and d are real numbers with c positive and d non-negative. Then,

$$f(n) \text{ is } \begin{cases} O(n^d) & \text{if } a < b^d \\ O(n^d \log n) & \text{if } a = b^d \\ O(n^{\log_b a}) & \text{if } a > b^d. \end{cases}$$

Proof of the master theorem

We can prove the theorem by showing the following steps:

1. Show that if $a = b^d$ and n is a power of b, then $f(n) = f(1)n^d + cn^d \log_b n$.
   Once this is shown, it is clear that if $a = b^d$ then $f(n) \in O(n^d \log n)$.
2. Show that if $a \neq b^d$ and n is a power of b, then $f(n) = c_1 n^d + c_2 n^{log_b a}$, where $c_1 = b^d c/(b^d - a)$ and $c_2 = f(1) + b^d c/(a - b^d)$.
3. Once the previous is shown, we get:
   if $a < b^d$, then $\log_b a < d$, so
   $f(n) = c_1 n^d + c_2 n^{\log_b a} \leq (c_1 + c_2) n^d \in O(n^d)$.
   if $a > b^d$, then $\log_b a > d$, so
   $f(n) = c_1 n^d + c_2 n^{\log_b a} \leq (c_1 + c_2) n^{\log_b a} \in O(n^{\log_b a})$.

Proving item 1:

Lemma

If $a = b^d$ and n is a power of b, then $f(n) = f(1)n^d + cn^d \log_b n$.

Proof:

Let $k = \log_b n$, that is $n^k = b$. Iterating $f(n) = af(n/b) + cn^d$, we get:

$$
\begin{aligned}
f(n) &= a(af(n/b^2) + c(n/b)^d) + cn^d = a^2 f(n/b^2) + ac(n/b)^d + cn^d \\
&= a^2(af(n/b^3) + c(n/b^2)) + ac(n/b)^d + cn^d \\
&= a^3 f(n/b^3) + a^2 c(n/b^2)^d + ac(n/b)^d + cn^d \\
&= \ldots = a^k f(1) + \sum_{j=0}^{k-1} a^j c(n/b^j)^d = a^k f(1) + \sum_{j=0}^{k-1} cn^d \\
&= a^k f(1) + kcn^d = a^{\log_b n} f(1) + (\log_b n)cn^d \\
&= n^{\log_b a} f(1) + cn^d \log_b n = n^d f(1) + cn^d \log_b n.
\end{aligned}
$$

Proving item 2:

Lemma

If $a \neq b^d$ and n is a power of b, then $f(n) = c_1 n^d + c_2 n^{log_b a}$, where $c_1 = b^d c/(b^d - a)$ and $c_2 = f(1) + b^d c/(a - b^d)$.

Proof:

Let $k = \log_b n$; i. e. $n = b^k$. We will prove the lemma by induction on k.
Basis: If $n = 1$ and $k = 0$, then
$c_1 n^d + c_2 n^{\log_b a} = c_1 + c_2 = b^d c/(b^d - a) + f(1) + b^d c/(a - b^d) = f(1)$.
Inductive step: Assume lemma is true for k, where $n = b^k$. Then, for
$n = b^{k+1}$, $f(n) = af(n/b) + cn^d =$
$a((b^d c/(b^d - a))(n/b)^d + (f(1) + b^d c/(a - b^d))(n/b)^{\log_b a})) + cn^d =$
$(b^d c/(b^d - a))n^d a/b^d + (f(1) + b^d c/(a - b^d))n^{\log_b a} + cn^d =$
$n^d[ac/(b^d - a) + c(b^d - a)/(b^d - a)] + [f(1) + b^d c/(a - b^d c)]n^{\log_b a} =$
$(b^d c/(b^d - a))n^d + (f(1) + b^d c/(a - b^d))n^{\log_b a}$. $\square$

Chinese Remainder Theorem: solving systems of congruences

A Chinese Mathematician asked in the first century:

> *There are certain things whose number is unknown. When divided by* 3*, the remainder is* 2*; when divided by* 5 *the remainder is* 3*; and when divided by* 7*, the remainder is* 2*. What will be the number of things?*

This puzzle is asking for the solution of the following system of congruences:

$$
\begin{aligned}
x &\equiv 2 \pmod{3}, \\
x &\equiv 3 \pmod{5}, \\
x &\equiv 2 \pmod{7}.
\end{aligned}
$$

Theorem

Chinese Reminder Theorem Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then, the system:

$$\begin{array}{rcl} x & \equiv & a_1 \pmod{m_1}, \\ x & \equiv & a_2 \pmod{m_2}, \\ \ldots & & \ldots \\ x & \equiv & a_n \pmod{m_n}, \end{array}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution).

Proof of the Chinese Reminder Theorem (existence part)

In order to construct a simultaneous solution, let $M_k = m/m_k$. Note that $gcd(m_k, M_k) = 1$. So there exists y_k inverse of M_k modulo m_k.
Then $x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n$ is a simulatneous solution.
Indeed, for any $1 \leq k \leq n$, since for $j \neq k$, all terms except kth term are 0 modulo m_k, which gives $x \equiv a_2M_ky_k \equiv a_k \pmod{m_k}$. $\square$

Showing that this is a unique solution is exercise 3.7-24, which is recommended.

Exercise: Solve the system of congruences given at the begining of this section.