CS5800 Algorithms

Solutions for Recitations from Sep 16, 2019 to Sep 20, 2019

Ravi Sundaram

Problem 1 (Asymptotics)

1. Return a list of the following functions separated by the symbol $\equiv$ or $\ll$, where $f \equiv g$ means $f = \Theta(g)$ and $f \ll g$ means $f = O(g)$. For example, if the functions are $\log n, n, 5n, 2^n$ a correct answer is $\log n \ll n \equiv 5n \ll 2^n$. All logarithms are in base 2. Prove each relation formally (the adjacent ones in the ordering you come up with).

   (a) $1/n$
   (b) $n \log n$
   (c) $\log n!$
   (d) $n^{1/\log n}$
   (e) $\log^2 n$
   (f) $\log^2(n \log n)$

   Solution:

   $1/n \ll n^{1/\log n} \ll \log^2 n \equiv \log^2(n \log n) \ll n \log n \equiv \log n!$
   Some brief explanations for the trickier ones:
   $n^{1/\log n} = 2^{\log n/\log n} = 2$
   $\log n! \approx \log n^n = n \log n$ (Stirling's Approximation).
   $\log^2(n \log n) = \log^2(n) + \log^2(\log n)$, and we can ignore right hand term for asymptotic complexity.
   ...

   ■

2. For some given functions, f, g, h, decide which of the following statements is correct and give a formal proof.

   (a) If $f(n) = O(g(n))$, then $f(n) = O(\log g(n))$
   (b) If $f(n) = \Theta(g(n))$, then $(f(n)^2) = \Theta(g(n)^3)$
   (c) If $f(n) = \Omega(n * g(n))$, $g(n) = \Omega(n * h(n))$, then $f(n) = \Omega(n^2 * h(n))$

Solution:

1. Take $f(n) = g(n) = n$
2. Take $f(n) = g(n) = n$

1. If $f(n) = \Omega(n * g(n))$, $g(n) = \Omega(n * h(n))$, then $f(n) = \Omega(n^2 * h(n))$

Solution:

By definition of $f(n) = \Omega(n * g(n))$, we get that

$$\exists c_1, \exists n_1 \text{ such that } f(n) \geq c_1 n g(n) \quad \forall n \geq n_1$$

By definition of $g(n) = \Omega(n * h(n))$, we get that

$$\exists c_2, \exists n_2 \text{ such that } g(n) \geq c_2 n h(n) \quad \forall n \geq n_2$$

We want to show that

$$\exists c_3, \exists n_3 \text{ such that } f(n) \geq c_3 n^2 h(n) \quad \forall n \geq n_3$$

In other words we are trying to find some c_3, n_3 so that the above holds. We want to apply what's given to us (the definitions). So the c_3, n_3 will depend on the c_1, c_2 and n_1, n_2 in some manner. In this problem, we can plug in the inequality of $g(n)$ to get

$$f(n) \geq c_1 n g(n) \geq c_1 n c_2 n h(n) = c_1 c_2 n^2 h(n)$$

Now this is looking good. But be careful, we need to choose some n_3 so that both the definitions hold. How can we do this? Easy, just set $n = max(n_1, n_2)$. And note that we can think of c_3 as $c_1 c_2$. So in the end, we found the existence of some c_3, n_3 such that

$$\exists c_3, \exists n_3 \text{ such that } f(n) \geq c_3 n^2 h(n) \quad \forall n \geq n_3$$

Since

$$f(n) \geq c_1 c_2 n^2 h(n) \quad \forall n \geq max(n_1, n_2)$$

...

■

Problem 2 (Diffie-Hellman)

1. As a refresher on how Diffie-Hellman works, there are two players, Alice and Bob trying to create a secure key, that some eavesdropper Eve can't figure out without brute force. There is some public information that Alice Bob, and Eve can see, namely some prime p, and some g s.t $1 < g < p$ such that $g^1, g^2, ..., g^{p-1}$ are all different. Now, Alice has a secret key a that only she can see, and Bob has a secret key b. Alice sends $g^a \ mod \ p$ to Bob over an unsecured channel. Bob then calculates $(g^a)^b$ mod p. Bob sends g^a mod p to Alice also over an unsecured channel. Alice then calculates $(g^b)^a$ mod p. Now note that Alice and Bob have the same private key since $(g^b)^a$ mod $p = (g^a)^b$ mod $p = g^{ab}$ mod p. And Eve can't figure it out without checking all the powers of g, which could take a very long time if p is large.

   Form groups of three. Pick one person to be Alice, one person to be Bob, and one person to be Eve. (can you guess why Eve is used). We are going to walk through a concrete instance of the Diffie-Hellman protocol. In our case, let $p = 19$ and let $g = 13$. Now Alice pick a number a so that $1 < a < 19$ and Bob pick a number b so that $1 < b < 19$ (and maybe don't pick too high of a number for your own sake). Keep these numbers secret.

   Now Alice, calculate 13^a mod 19 and Bob calculate 13^b mod 19. Eve, when the time comes, you're going to try to guess the secret key. So Eve, you are going to listen to Alice and Bob send g^a mod

p and g^b mod p to each other, and you are going to try to figure out their private key g^{ab} mod p. You need to figure out either a or b, and then since you know both g^a and g^b you can plug in the secret value and calculate g^{ab} mod p. Alice and Bob, once you are ready, announce your g^a mod p and g^b mod p values to your group. Eve you have 30 seconds to guess g^{ab} mod p. During this time, Alice and Bob calculate the secret key and verify with each other that it's the same. Go!

Eve if you guessed it, you win a prize. Otherwise, Alice and Bob, if you guys got the same private key, then you win prizes.

Problem 3 (Induction and Functions)

1. Let q be a real number other than 1. Use induction on n to prove that $\sum_{i=0}^{n-1} q^i = (q^n - 1)/(q - 1)$
2. Let $f : \mathbb{R} \to \mathbb{R}$ be a function such that $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$. Show that
   1) $f(0) = 0$
   2) $f(n) = nf(1)$ for $n \in \mathbb{N}$.
3. Prove that $|\sum_{i=1}^{n} a_i| \leq \sum_{i=1}^{n} |a_i|$ for $a_i \in \mathbb{R}$. (Hint: Triangle Inequality)
4. Show that any value of 12 cents or more can be attained using some arbitrary amount of 4 and 5 cent denomination coins (this problem is an example of strong induction).

Solution:

1. Base case, $q^0 = (q - 1)/(q - 1)$. Now assume true for k, so $\sum_{i=0}^{k} q^i = (q^{k+1} - 1)/(q - 1)$. Now we want to show that $\sum_{i=0}^{k+1} q^i = (q^{k+2} - 1)/(q - 1)$. We know that $\sum_{i=0}^{k+1} q^i = \sum_{i=0}^{k} q^i + q^{k+1} = (q^{k+1}-1)/(q-1)+q^{k+1}$ by inductive hypothesis. Finishing the algebra gives you the right solution.
2. (a) Proof by contradiction. Suppose $f(0) \neq 0$. Then for any a, $f(a) = f(a + 0) = f(a) + f(0)$. If $f(0) \neq 0$, this is impossible.
   (b) By induction. Base case is previous part. Suppose $f(k) = kf(1)$. Then $f(k + 1) = f(k) + f(1) = kf(1) + f(1) = (k + 1)f(k)$. Then we are done.
3. Base case is $i = 1$, this is obviously true. Suppose true for k, in other words $|\sum_{i=1}^{k} a_i| \leq \sum_{i=1}^{k} |a_i|$. Now we want to show true for $k + 1$, or that $|\sum_{i=1}^{k+1} a_i| \leq \sum_{i=1}^{k+1} |a_i|$. By triangle inequality, $|\sum_{i=1}^{k+1} a_i| \leq |\sum_{i=1}^{k} a_i| + |a_{k+1}|$. Now by inductive hypothesis, $|\sum_{i=1}^{k} a_i| + |a_{k+1}| \leq \sum_{i=1}^{k+1} |a_i| + |a_{k+1}| = \sum_{i=1}^{k+1} |a_i|$
4. To get 12 cents, we can do 3 4 cent coins. To get 13 cents, we can do 2 4 cents coins and 1 5 cent coin. To get 14 cents, we can do 2 5 cent coins and 1 4 cent coin. To get 15 cents, we can do 3 5 cent coins. Now, to get 16/17/18/19 coins, we can add a 4 cent coin to one of the previous arrangements, and the (strong) induction goes through (here our base case is 12,13,14,15).

...

■

Problem 4 (More Counting)

1. Prove that $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$ by counting a set in two different ways.
2. Prove that $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ by counting a set in two different ways.

Solution:

(a) Left side: Pick k committee members, then out of those k pick j to be the leaders.
Right side: Pick j leaders, and from the remaining members pick out $k-j$ to be the rest of the committee members.

(b) Fix some element i. Either element i is included in the k elements chosen on the left or its not. If it is, then $\binom{n-1}{k-1}$ counts ways to pick $k-1$ other elements to include with i. If it is not, then $\binom{n-1}{k}$ counts ways to pick k elements (since i not included).

...

■

Problem 5 (Proof by Contradiction)

We are going to prove the classic result that $\sqrt{2}$ is irrational. To do this, we use proof by contradiction. Let's call the statement we are trying to prove P. If we want to prove that P is true (in this case, we want to prove that $\sqrt{2}$ is irrational), we make the assumption that $\neg P$ is true. Using this assumption, we try to derive find some other statement C, so that $\neg P \implies C \wedge \neg C$, which is logically impossible (a contradiction). And this means that P has to be true.

First we need this result.

1. Explain why if n^2 is even, then n is even.
2. Now prove that $\sqrt{2}$ is irrational.

   Note: This can also be proven through the Fundamental Theorem of Arithmetic, where every rational number has a unique decomposition based on prime numbers...

Solution:

1. If n is odd then n^2 is odd.
2. Suppose $\sqrt{2}$ is irrational. Let p/q be simplified fraction for it (meaning $gcd(p,q) = 1$). Then $2 = p^2/q^2$, or $2q^2 = p^2$. So this means p^2 has to be even, which by above means p is even. But then then if p is even, then p^2 is divisible by 4, meaning q^2 is divisible by 2, which means q is divisible by 2. So therefore, p and q share a common factor, which is a contradiction.

...

■

Problem 6 (Modular Arithmetic)

We are going to prove Fermat's Little Theorem.

1. Let p be a prime. Show that for any integer x not divisible by p, $x^{p-1} \equiv 1 \bmod p$. Hint: Consider the sequence $x, 2x, ..., (p-1)x$.

Solution:

$x, 2x, ..., (p-1)x$ will have all the remainders mod p. To see this, suppose $rx \equiv sx \bmod p$ for some $r \neq s$. Since, x isn't divisible by p, it is invertible. So we get $rx \equiv sx \bmod p$, but this is impossible since $1 \leq r, s \leq p-1$, and $r \neq s$. So then comparing the remainders of both sides, we get $(p-1)!x^{p-1} \equiv (p-1)! \bmod p$, and finally, $x^{p-1} \equiv 1 \bmod p$.

■

Problem 7 (Extras...)

1. Give a bijection between the open interval (0,1) and $\mathbb{R}$. (Hint: Think how to cover all the negative numbers with one half and all the positive numbers with the other half.) Then prove your function is a bijection.

2. (Proof by Contradiction)
   Let n be a composite number. Prove that n has a prime divisor $p \leq \sqrt{n}$.

3. (Counting, similar to part 2 of Problem 2)
   A partition of a set is a grouping of the set's elements into non-empty subsets, in such a way that every element is included in exactly one subset. Let B_n be the number of ways to partition a set of size n. Let C_n be the number of parts used to make all of these partitions. For example, take the set $\{a, b, c\}$.

   B_n is 5 because it has the following 5 partitions:

   $$\begin{aligned} abc \\ a \mid bc \\ b \mid ca \\ c \mid ab \\ a \mid b \mid c \end{aligned}$$

   C_n is 10 because these 10 parts used are to make the partitions $\{a, b, c\}$; $\{a\}, \{b, c\}$; $\{b\}, \{c, a\}$; $\{c\}, \{a, b\}$; and $\{a\}, \{b\}, \{c\}$.

   Prove the identity: $B_n + C_n = B_{n+1}$