Staff Solutions to Problem Set 7

Reading:
- Sections 14.5. Products, 14.7. Asymptotic Notation (omit 14.6).
- Chapter 15. Counting through Section 15.7. Counting Practice

Problem 1.
Let \( f, g \) be nonnegative real-valued functions such that \( \lim_{x \to \infty} f(x) = \infty \) and \( f \sim g \).
(a) Give an example of \( f, g \) such that \( \not\sim (2^f \sim 2^g) \).

Solution.
\[
f(n) := n + 1 \\
g(n) := n.
\]
Then \( f \sim g \) since \( \lim [(n + 1)/n] = 1 \), but \( 2^f = 2^{n+1} = 2 \cdot 2^n = 2 \cdot 2^g \) so
\[
\lim \frac{2^f}{2^g} = 2 \neq 1.
\]

(b) Prove that \( \log f \sim \log g \).

Solution.
\[
\lim \frac{f}{g} = 1 \\
\log \lim \frac{f}{g} = \log 1 \\
\lim \log \frac{f}{g} = 0 \\
\lim (\log f - \log g) = 0 \\
\lim \frac{\log f - \log g}{\log g} = 0 \\
\lim \frac{\log f}{\log g} - 1 = 0 \\
\lim \frac{\log f}{\log g} = 1
\]
Note that this proof did not need the condition that $\lim_{x \to \infty} f(x) = \infty$.

(c) Use Stirling’s formula to prove that in fact

$$\log(n!) \sim n \log n$$

**Solution.** Taking logs of both sides of Stirling’s formula, we have

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$  \hspace{1cm} \text{(Stirling)}

$$\log(n!) \sim n \log \left(\frac{n}{e}\right) + \log \sqrt{2\pi n}$$  \hspace{1cm} \text{(part (b))}

$$= n \log n - n \log e + \log \sqrt{2\pi n}$$

$$\sim n \log n.$$  

The final step follows from the fact that

$$\lim_{n \to \infty} \frac{n \log n - n \log e + \log \sqrt{2\pi n}}{n \log n}$$

$$= \lim_{n \to \infty} \frac{n \log n}{n \log n} - \frac{n \log e}{n \log n} + \frac{\log \sqrt{2\pi n}}{n \log n} + \frac{(\log n)/2}{n \log n}$$

$$= 1 - \lim_{n \to \infty} \frac{\log e}{\log n} + \lim_{n \to \infty} \frac{\log \sqrt{2\pi n}}{n \log n} + \lim_{n \to \infty} \frac{1}{2n}$$

$$= 1 - 0 - 0 - 0 = 1.$$  

Problem 2.

Arrange the following functions in a sequence $f_1, f_2, \ldots, f_{24}$ so that $f_i = O(f_{i+1})$. Additionally, if $f_i = \Theta(f_{i+1})$, indicate that too:

1. $n \log n$
2. $2^{100}n$
3. $n^{-1}$
4. $n^{-1/2}$
5. $(\log n)/n$
6. $\binom{n}{64}$
7. $n!$
8. $2^{2^{100}}$
9. $2^{2^n}$
10. $2^n$
Staff Solutions to Problem Set 7

11. $3^n$
12. $n2^n$
13. $2^n + 1$
14. $2n$
15. $3n$
16. $\log (n!)$
17. $\log_2 n$
18. $\log_{10} n$
19. $2 \sqrt[n]{n}$
20. $2^{2n}$
21. $4^n$
22. $n^{64}$
23. $n^{65}$
24. $n^n$

Solution. The correct ordering is the following:

1. $n^{-1}$
2. $(\log n)/n$
3. $n^{-1/2}$
4. $2^{100}$
5. $\log_{10} n = \Theta(\log_2 n)$
6. $2^{100} n = \Theta(2n) = \Theta(3n)$
7. $\log (n!) = \Theta(n \log n)$
8. $\left( \frac{n}{64} \right) = \Theta(n^{64})$
9. $n^{65}$
10. $2 \sqrt[n]{n}$
11. $2^n = \Theta(2^{n+1})$
12. $n2^n$
13. $3^n$
14. $4^n = \Theta(2^{2n})$
15. $n!$
16. $n^n$
17. \(2^{2^n}\)

### Problem 3.

Fermat’s Little Theorem 9.10.8\(^1\) asserts that

\[ a^p \equiv a \pmod{p} \]  

(1)

for all primes \(p\) and nonnegative integers \(a\). This is immediate for \(a = 0, 1\) so we assume that \(a \geq 2\).

This problem offers a proof of (1) by counting strings over a fixed alphabet with \(a\) characters.

(a) How many length-\(k\) strings are there over an \(a\)-character alphabet?

**Solution.** \(a^k\).

How many of these are strings use more than one character?

**Solution.** \(a^k - a\).

For each of the \(a\) characters, there is exactly one length-\(k\) string using only that character.

Let \(z\) be a length-\(k\) string. The *length-\(n\) rotation* of \(z\) is the string \(yx\), where \(z = xy\) and the length, \(|x|\), of \(x\) is remainder\((n, k)\).

(b) Verify that if \(u\) is a length-\(n\) rotation of \(z\), and \(v\) is a length-\(m\) rotation of \(u\), then \(v\) is a length-\((n + m)\) rotation of \(z\).

**Solution.** Suppose \(z = wxy\) where \(|w| = n, |x| = m\). Then \(u = xyw\), and so \(v = ywx\). But \(|wx| = n + m\), so \(v\) is the length-\(n + m\) rotation of \(z\). This argument applies to \(n, m, n + m > |z|\) by taking remainders on division by \(|z|\).

**STAFF NOTE:** TBA - Explain about remainders more clearly?

(c) Let \(\approx\) be the “is a rotation of” relation on strings. That is,

\[ v \approx z \iff v \text{ is a length-}n\text{ rotation of } z \]

for some \(n \in \mathbb{N}\). Prove that \(\approx\) is an equivalence relation.

**Solution.** *Proof.* Reflexivity follows since everything is a length 0 rotation of itself. Symmetry follows because \(v\) is a length \(m\) rotation of \(z\) iff \(z\) is a length \(|z| - \text{remainder}(m, |z|)\) rotation of \(v\). Transitivity follows from part (b).

(d) Prove that if \(xy = yx\) then \(x\) and \(y\) each consist of repetitions of some string \(u\). That is, if \(xy = yx\), then \(x, y \in u^*\) for some string \(u\).

*Hint:* By induction on the length \(|xy|\) of \(xy\).

(Old hint leading to more cumbersome proof: Let \(u\) be the shortest positive length string such that \(uy = yu\).)

---

\(^1\)This Theorem is usually stated as

\[ a^{p-1} = 1 \pmod{p}, \]

for all primes \(p\) and integers \(a\) not divisible by \(p\). This follows immediately from (1) by canceling \(a\).
Solution. Proof. By strong induction with the induction hypothesis

\[ P(n) := \forall \text{ strings } x, y. |xy| = n \text{ IMPLIES } \exists u. x, y \in u^*. \]

**Base case** \((n = 0)\). Immediate.

**Induction step.** Suppose \( |xy| = n + 1 \) and \( xy = yx \). We must now show that \( x, y \in u^* \) for some string \( u \).

Since \( x \) and \( y \) are interchangeable in the hypotheses, we may assume that \( |x| \leq |y| \). If \( |x| = 0 \), then letting \( u := y \) yields \( x, y \in u^* \), so we may assume \( |x| > 0 \).

Now \( xy = yx \) implies that \( y = xy' \) for some string \( y' \). So we have

\[ x(xy') = xy = yx = (xy')x = x(y'x), \]

and therefore

\[ xy' = y'x. \]

Also \( |xy'| < |xy| \). By induction hypothesis, we have

\[ x, y' \in u^* \]

for some string \( u \). Since \( y = xy' \) is a concatenation of strings in \( u^* \), we conclude that \( y \in u^* \).

\(\blacksquare\)

(e) Conclude that if \( p \) is prime and \( z \) is a length-\( p \) string containing at least two different characters, then \( z \) is equivalent under \( \approx \) to exactly \( p \) strings (counting itself).

**Solution.** By part (d), \( z \in u^* \) for some string \( u \). Letting \( m \) be the length of the shortest such \( u \), it follows that \( z \) is \( \approx \)-equivalent to exactly \( m \) strings. In particular, \( |z| \) is a multiple of \( m \).

But \( |z| = p \), so \( m \) must be 1 or \( p \), and since \( z \) has at least two different characters, \( m \neq 1 \). So \( z \) is equivalent to exactly \( p \) strings.

\(\blacksquare\)

(f) Conclude from parts (a) and (e) that \( p \mid (a^p - a) \), which proves Fermat’s Little Theorem (1).

**Solution.** From part (a), there are \( a^p - a \) length-\( p \) strings made from an alphabet with \( a \) characters that contain at least 2 different characters. From (e), a length-\( p \) string of at least two different characters is equivalent under \( \approx \) to exactly \( p \) other strings. Partitioning the strings with two or more characters into equivalence classes under \( \approx \), it follows that each block of the partition has \( p \) elements, and therefore the total number of strings is a multiple of \( p \). That is, \( p \mid a^p - a \), and therefore \( a^p \equiv a \pmod p \), as desired.

\(\blacksquare\)

**Problem 4.**

Answer the following questions with a number or a simple formula involving factorials and binomial coefficients. Briefly explain your answers.

(a) How many ways are there to order the 26 letters of the alphabet so that no two of the vowels \( a, e, i, o, u \) appear consecutively and the last letter in the ordering is not a vowel?

*Hint: Every vowel appears to the left of a consonant.*

**Solution.** The constraint on where vowels can appear is equivalent to the requirement that every vowel appears to the left of a consonant. So given a sequence of the 21 consonants, there are \( \binom{21}{5} \) positions where the 5 vowels can be placed. After determining such a placement, we can reorder the consonants and vowels in any order. Thus, the number is:

\[ \binom{21}{5} \cdot 21! \cdot 5! \]

\(\blacksquare\)
(b) How many ways are there to order the 26 letters of the alphabet so that there are at least two consonants immediately following each vowel?

Solution. The pattern of consonants and vowels in any permutation of the 26 letters of the alphabet can be indicated by a binary string with 5 ones indicating where the vowels occur and 21 zeros where the consonants occur. Patterns where every vowel has at least two consonants to its right can be constructed by taking a sequence of 16 zeros and inserting “10” to the left of 5 of the 16 zeros. There are \( \binom{16}{5} \) ways to do this. For any such pattern, there are 5! ways to place the vowels in the positions where ones occur and 21! ways to place the consonants where the zeroes occur. Thus, the final answer is:

\[
\binom{16}{5} 
\cdot 5! 
\cdot 21!.
\]

(c) In how many different ways can \( 2n \) students be paired up?

Solution.

\[
\frac{(2n)!}{n!2^n}.
\]

(2)

There are \( (2n)! \) permutations of the \( 2n \) people. A permutation can be mapped to a pairing up of the \( 2n \) people by pairing consecutive people in the permutation. That is, one pair consists of the first and second people, another pair of the third and fourth people, through an \( n \)th pair of the \( (2n - 1) \)st and \( 2n \)th people in the permutation.

Two permutations will map to the same set of pairs iff one permutation can be changed into the other permuting the order of the consecutive pairs or by switching the elements of a pair. Since there are \( n \) consecutive pairs, there are \( n! \) ways to permute the pairs and \( 2^n \) ways to switch the order within pairs. So the mapping from permutations to sets of pairs is \( n!2^n \). Now the Division Rule 15.4 implies that the number of ways to divide \( 2n \) people into \( n \) pairs is given by (2).

(d) Two \( n \)-digit sequences of digits 0,1,\ldots,9 are said to be of the same type if the digits of one are a permutation of the digits of the other. For \( n = 8 \), for example, the sequences 03089929 and 00238899 are the same type. How many types of \( n \)-digit sequences are there?

Solution. The type of a string is determined simply by the numbers of occurrences of the digits 0–9 in the string. So there is a bijection between types of strings and strings with \( n \) 0’s and nine 1’s: the length of the block of 0’s before the \( i \)th 1 (starting with \( i = 0 \)) equals the number of occurrences of the digit \( i \), and the length of the block of 0’s following the last 1 equals the number of occurrences of the digit 9. Therefore, the number of different types is

\[
\binom{n + 9}{9}.
\]

Problem 5.

A pizza house is having a promotional sale. Their commercial reads:

We offer 9 different toppings for your pizza! Buy 3 large pizzas at the regular price, and you can get each one with as many different toppings as you wish, absolutely free. That’s 22, 369, 621 different ways to choose your pizzas!
The ad writer was a former Harvard student who had evaluated the formula \((2^9)^3/3!\) on his calculator and gotten close to 22,369,621. Unfortunately, \((2^9)^3/3!\) can’t be an integer, so clearly something is wrong. What mistaken reasoning might have led the ad writer to this formula? Explain how to fix the mistake and get a correct formula.

**Solution.** The number of ways to choose toppings for one pizza is the number of the possible subsets of the set of 9 toppings, namely, \(2^9\). The ad writer presumably then used the Product Rule to conclude that there were \((2^9)^3\) sequences of three topping choices. Then he probably reasoned that each way of making three topping choices arises from \(3!\) sequences, so the Division Rule would imply that the number of ways to choose three pizzas is \((2^9)^3/3!\).

It’s true that every set of three different topping choices arises from \(3!\) different length-3 sequences of choices. The mistake is that if some of the three choices are the same, then the set of three choices arises from fewer than \(3!\) sequences. For example, if all three pizzas have the same toppings, there is only one sequence of topping choices.

One fix is to consider ways to choose toppings with 1, 2 and 3 different topping choices. There are \(2^9(2^9 - 1)(2^9 - 2)/3!\) ways to choose a set of 3 different choices, \(2^9(2^9 - 1)\) ways to choose one topping choice to be used on two pizzas and a second choice for the third pizza, and \(2^9\) ways to choose one topping for all three pizzas, giving

\[
\frac{2^9(2^9 - 1)(2^9 - 2)}{3!} + 2^9(2^9 - 1) + 2^9 = 22,500,864.
\]

ways to choose three pizzas.

Alternatively, we can observe that this is exactly the problem of selecting a dozen donuts of five possible different kinds—except now there are 3 donuts and \(2^9\) kinds. Hence, there is a bijection to the number of \((2^9 + 2)\)-bit strings with exactly \(2^9 - 1\) ones and 3 zeros:

\[
\binom{2^9 + 2}{3} = 22,500,864.
\]