Solutions to Quiz 2

Problem 1 (10 points). True/False. Circle the appropriate answer.

(a) (2 points) A state machine with a strictly decreasing derived variable must terminate.

True **False**

Solution. F ■

(b) (2 points) In a set of stable marriages with more than one couple, it is possible for everyone to be married to the person at the bottom of their preference list.

True **False**

Solution. F: every couple would be a rogue couple. ■

(c) (2 points) An infinite geometric sum whose ratio between successive terms is r converges if $|r| \leq 1$.

True **False**

Solution. F when $r = 1$. ■

(d) (2 points) Four books can be stacked at the edge of a table so that the top book lies completely over the edge of the table.

True **False**

Solution. T, as observed in the Notes. ■

(e) (2 points) The security of RSA relies on the assumption that the ability to decipher RSA-encrypted messages efficiently would imply the ability to factor key-sized numbers efficiently.

True **False**

Solution. The correct answer is F. The security of RSA is shakier than the presumed difficultly of factoring, as noted in a pset. Very few students got this right, and since we did not adequately define what security formally means, we awarded 2 points to everyone.■

Problem 2 (20 points). (a) (10 points) Using the Pulverizer, find an x in the range $[0 \ldots 99]$ such that x is an inverse of 19 modulo 100.

Solution. There are two valid approaches. **Solution 1:** Use the Pulverizer to find integers s, t such that $s19 + t100 = 1$. Then $s \bmod 100$ will be 19^{-1}. In this case the Pulverizer yields $-21 \cdot 19 + 4 \cdot 100 = 1$, so $19^{-1} \equiv -21 \equiv 79 \pmod{100}$. **Solution 2:** Find $k = \phi(100)$, so by Euler's Theorem, $19^{-1} \equiv 19^{k-1} \pmod{100}$. Then $19^{k-1} \bmod 100$ will be 19^{-1}. This can be computed by at most $\lfloor \log 100 \rfloor = 6$ squarings modulo 100. ■

(b) (5 points) What is the value of $\phi(360)$, where ϕ is Euler's function? _____

Solution. Note that $360 = 2^3 \cdot 3^2 \cdot 5$. It follows that $\phi(360) = 4 \cdot 6 \cdot 4 = 96$. ■

(c) (5 points) What is the value of $7^{98} \bmod 360$? _____

Solution. Since 7 and 360 are relatively prime, we have by Euler's Theorem that $7^{96} \equiv 1 \pmod{360}$, and so

$$7^{98} = 7^{96} \cdot 7^2 \equiv 1 \cdot 49 \equiv 49 \pmod{360}.$$

■

Problem 3 (15 points). Consider the following functions:

$f_1(n) = \log(n!)$ $f_2(n) = 10^{100}$ $f_3(n) = \sum_{i=1}^{n}(1/i)$ $f_4(n) = \log(4^n)$
$f_5(n) = \log(n^n)$ $f_6(n) = 2 + \sin n$ $f_7(n) = \log(6^n)$

(a) (10 points) List the digits $1, \ldots, 7$ in an order such that if digit i comes before j in your list, then $f_i = O(f_j)$.

Solution. 2, 6, 3, 4, 7, 1, 5. ■

(b) (5 points) List a sequence of sets of the digits so that i and j are in the same set iff $f_i = \Theta(f_j)$. Write your list in a form such as "$\{543\}, \{76\}, \{21\}$".

Solution. $\{2, 6\}\{3\}\{4, 7\}\{1, 5\}$. ■

Problem 4 (20 points). Write simple formulas for the following quantities. You do not have to calculate numerical values for the formulas.

(a) (6 points) The number of rearrangements of the word $BAZOOKA$ in which the two O's do not appear next to each other.

Solution. Total number of arrangements is:

$$\binom{7}{2, 2, 1, 1, 1} = \frac{7!}{2!\,2!} = 1260. \tag{1}$$

The number of arrangements in which the two O's *do* appear next to each other is the number of rearrangements of $BAZOKA$ since we can treat the double-O as though it was a single O:

$$\binom{6}{2, 1, 1, 1, 1} = \frac{6!}{2!} = 360.$$

Therefore, the number of arrangements in which the O's do *not* appear together is:

$$\binom{7}{2, 2, 1, 1, 1} - \binom{6}{2, 1, 1, 1, 1} = 1260 - 360 = 900.$$

■

(b) (6 points) The number of rearrangements of the word $BAZOOKA$ in which the two O's do not appear next to each other *and* that do not start with B.

Solution. Total number of arrangements that *do* start with B is the number of rearrangements of $AZOOKA$:

$$\binom{6}{2,2,1,1} = \frac{6!}{2!\,2!} = 180.$$

Number of arrangements starting with B *and* with two O's next to each other is the number of arrangements of $AZOKA$:

$$\binom{5}{2,1,1,1} = \frac{5!}{2!} = 60.$$

By inclusion-exclusion it follows that the number of arrangements in which the two O's appear together *or* that start with B is the number that have two O's together plus the number that start with B, minus the number that do both:

$$360 + 180 - 60 = 480. \tag{2}$$

So the number that neither have two O's next to each other nor start with B is the total (1) minus those that do one or the other (2), namely

$$1260 - 480 = 780.$$

■

(c) (2 points) The number of *nonnegative integer* solutions to the equality:

$$x_1 + x_2 + \ldots + x_{10} = 100.$$

Solution. There is a bijection from the set of nonnegative solutions to the above equation to the set of 109 bit binary strings with exactly 9 1's. The number of such binary strings is:

$$\binom{100+9}{9}.$$

■

(d) (6 points) The number of *positive integer* solutions to the inequality:

$$x_1 + x_2 + \ldots + x_{10} \leq 100.$$

Solution. There is an immediate bijection between the number of *positive* solutions to the above inequality:

$$x_1 + x_2 + \ldots + x_{10} \leq 100, \tag{3}$$

and the number of solutions to the equality

$$x_1 + x_2 + \ldots + x_{10} + x_{11} = 100, \tag{4}$$

in which the first ten variables are positive. Then, the mapping which subtracts 1 from the positive values of $x_1, x_2, \ldots, x_{10}$ is a bijection between these solutions of (4) and the nonnegative solutions of

$$x_1 + x_2 + \ldots + x_{10} + x_{11} = 100 - 10 = 90,$$

which we know the same as the number of $90 + 10$ bit strings with 10 one's, namely:

$$\binom{100}{10}.$$

■

Problem 5 (10 points). To prove that $n^4 = O(\sum_{i=1}^{n} i^3)$ we can use the integral method to bound the sum. In particular, we should obtain a(n)

upper lower (CIRCLE THE RIGHT CHOICE)

bound on the sum that is equal to the value of $\int_a^b (x+c)^d dx$ where

a is _____, b is _____, c is _____, and d is _____.

Solution. The sum must be greater than ϵn^4 for some positive ϵ in order for n^4 to be O(the sum). That is, we need such a **lower** bound on the sum. To do this, we choose the constants so that integral is $\leq$ the sum, and is also $> \epsilon n^4$. Choosing $d = 3$, and $a = 0, b = n, c = 0$, for example, will do the job. It would also be OK to increase this value for a by a constant (say $a = 1$), and decrease c by the same constant (say $c = -1$), and decrease the value of b by a constant (say $b = n - 2$). ■

Problem 6 (25 points). We will describe a process that operates on sequences of numbers. The process will start with a sequence that is some *permutation* of the length $4n$ sequence

$$(1, 2, \ldots, n, 1, 2, \ldots, n, 1, 2, \ldots, 2n).$$

(a) (7 points) Write a simple formula for the number of possible starting sequences.

Solution. Using the Bookkeeper rule: $4n$ digits can be arranged in $4n!$ ways; each digit from 1 to n appears 3 times. Therefore, we have to divide $4n!$ by $3!\ldots3!$, n times. The answer is:

$$\frac{(4n)!}{(3!)^n}$$

■

If $(s_1, \ldots, s_k)$ is a sequence of numbers, then the i and jth elements of the sequence are *out of order* if the number on the left is strictly larger the number on the right, that is, if $i < j$ and $s_i > s_j$. Otherwise, the ith and jth elements are *in order*. Define $p(S)::=$ the number of "out-of-order" pairs of elements in a sequence, S. For example, if S is the sequence

$$(3, 4, 2, 1, 7, 3),$$

then the 1st and 3rd elements of S, (namely, 3 and 2), are out of order, but the 3rd and 6th elements (2 and 3) are in order. The 1st and 6th elements of S are also in order, since they are both 3. In this case, $p(S) = 7$. The *reversal* of $(s_1, \ldots, s_k)$ is $(s_k, \ldots, s_1)$. So the reversal of the sequence S is

$$(3, 7, 1, 2, 4, 3).$$

From the starting sequence, we carry out the following process: (*) Pick two consecutive elements in the current sequence, say the ith and $(i + 1)$st.

I. If the elements are not in order, then **switch them** in the sequence and repeat step (*).

II. If the elements are in order, **remove both**, resulting in a sequence that is shorter by two. If the length of the resulting sequence is zero or one, the process is over. Otherwise, **reverse the sequence** and repeat step (*).

This process can be modelled as a state machine where the states are the sequences that appear at step (*). We then consider the derived variables on the following page:

i. $p(S)$ _____

Solution. None of the Above. **(2 pts)** Reversing a sequence maps an out-of-order pairs of elements into an in order pair of elements with different values. Pairs of elements with the same values stay in order. So the number of out of order pairs can increase *or* decrease depending on whether there were more out-of-order than strictly in order pairs. ■

ii. $\text{length}\,(S)\ \text{rem}\ 2$ _____

Solution. Constant. **(2 pts)** $\text{length}\,(S)$ changes by 0 or 2 at each transition, it parity is unchanged. ■

iii. $\text{length}(S) + p(S)$ _____

Solution. None of the Above. **(3 pts)** While $\text{length}(S)$ decreases by 2 or is unchanged, $p(S)$ may go up or down by more than 2. ■

iv. $\max(p(S), 8n^2)$ _____

Solution. Constant. **(3 pts)** Since there are only $\binom{4n}{2} < 8n^2$ pairs of distinct positions in a length $4n$ sequence, at most this many can be out of order (even fewer because there will be 3 pairs of elements with the same value for each of the values $1, \ldots, n$) and $p(n) \leq$ the total number of such pairs. ■

v. $4n^2 \cdot \text{length}(S) + p(S)$ _____

Solution. Strictly Decreasing. **(4 pts)** In the first transition, $p(S)$ decreases and $\text{length}(S)$ stays the same. The quantity decreases. In the second transition, the $4n^2 \,\text{length}(S)$ decreases by $8n^2$. But $p(S)$ can't change by more than its maximum value, which by the previous part is $\leq \binom{4n}{2} < 8n^2$. So the quantity decreases in this case too. ■

(b) (14 points) Indicate next to each of the derived variables above which one of these properties it has:

constant	C
strictly increasing	SI
strictly decreasing	SD
weakly increasing but not constant	WI
weakly decreasing but not constant	WD
none of the above	N

(c) (2 points) Which of the variable behaviors in i.–v. above immediately implies that the process will definitely terminate? _____

Solution. v. Fact v. implies termination by the Well Ordering Principle. ■

(d) (2 points) Which of the variable behaviors in i.–v. above immediately implies that, starting from any of the possible starting states from part (a), the process will not terminate with a length 1 sequence? _____

Solution. ii. Since every possible start state has length $4n$, Fact ii. implies that every reachable state must be of even length, and so cannot be length 1. ■