Assignment 1, Due on September 3rd, Wednesday

1. (2 **points**) Page 8 of DPV, 0.1(c), 0.1(e), 0.1(f) 0.1(g), 0.1(j), 0.1(k), 0.1(m), 0.1(o), 0.1(p), 0.1(q),
2. (3 **points**) Page 9 of DPV, 0.2

In each of the following situations, indicate whether $f = O(g)$, or $f = \Omega(g)$, or both (in which case $f = \Theta(g)$).

c. $f(n) = 100 \cdot n + \log n$ and $g(n) = n + (\log n)^2$.

$$\lim_{n \to +\infty} \frac{100 \cdot n + \log n}{n + (\log n)^2} = \lim_{n \to +\infty} \frac{100 + 1/n}{1 + 2 \cdot \log n / n} \approx 100 \Rightarrow f(n) = \Theta(g(n)).$$

e. $f(n) = \log(2 \cdot n)$ and $g(n) = \log(3 \cdot n)$.

$$f(n) = \log 2 + \log n, \text{ and } g(n) = \log 3 + \log n \Rightarrow f(n) = \Theta(g(n)).$$

f. $f(n) = 10 \cdot \log n$ and $g(n) = \log(n^2)$.

$$g(n) = 2 \cdot \log n \Rightarrow f(n) = \Theta(g(n)).$$

g. $f(n) = n^{1.01}$ and $g(n) = n \log^2 n$.

$$\begin{aligned} \lim_{n \to +\infty} \frac{f(n)}{g(n)} &= \frac{n^{0.01}}{(\log n)^2} = \frac{0.01 \cdot n^{-0.99}}{2 \cdot \log n \cdot n^{-1}} \\ &= \frac{0.005 \cdot n^{0.01}}{\log n} = 0.005 \cdot 0.01 \cdot n^{0.01} \Rightarrow f(n) = \Omega(g(n)). \end{aligned}$$

j. $f(n) = (\log n)^{\log n}$ and $g(n) = n/\log n$.
Let $n = 2^k$. $f(n) = k^k$ and $g(n) = 2^k/k$. Thus, $f(n) = \Omega(g(n))$.

k. $f(n) = \sqrt{n}$ and $g(n) = (\log n)^3$.
Let $n = 2^k$. $f(n) = 2^{k-1}$ and $g(n) = k^3$. Thus, $f(n) = \Omega(g(n))$.

In each of the following situations, indicate whether $f = O(g)$, or $f = \Omega(g)$, or both (in which case $f = \Theta(g)$).

m. $f(n) = n \cdot 2^n$ and $g(n) = 3^n$.

$$\lim_{n \to +\infty} \frac{n \cdot 2^n}{3^n} = \frac{n}{1.5^n} \Rightarrow f(n) = O(g(n)).$$

o. $f(n) = n!$ and $g(n) = 2^n$.
From Stirling formula, $f(n) \approx \sqrt{2 \cdot \pi \cdot n} \cdot (\frac{n}{e})^n$. Thus, $f(n) = \Omega(g(n))$.

p. $f(n) = (\log n)^{\log n}$ and $g(n) = 2^{\log n^2}$.
Let $\log n = k$. $f(n) = k^k$ and $g(n) = 2^{k^2} = 2^{k \cdot k} = (2^k)^k$. Thus, $f(n) = O(g(n))$.

q. $f(n) = \sum_{i=1}^{n} i^k$ and $g(n) = n^{k+1}$. k is a constant.

$$f(n) = 1^k + 2^k + \ldots + n^k \leq n^k + n^k + \ldots n^k = n \cdot n^k = n^{k+1} = g(n) \Rightarrow f(n) = O(g(n)).$$

Also,

$$\begin{aligned} f(n) &= 1^k + 2^k + \ldots + (\frac{n}{2})^k + (\frac{n}{2} + 1)^k + \ldots + n^k \geq \frac{n^k}{2^k} + \frac{n^k}{2^k} + \ldots + \frac{n^k}{2^k} \\ &= \frac{n}{2} \cdot \frac{1}{2^k} \cdot n^k = n^{k+1} \cdot \frac{1}{2^{k+1}} \Rightarrow f(n) = \Omega(g(n)). \end{aligned}$$

Thus, $f(n) = \Theta(g(n))$.

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

1. $\Theta(1)$ if $c < 1$.
2. $\Theta(n)$ if $c = 1$.
3. $\Theta(c^n)$ if $c > 1$.

Proof.

If $c = 1$, $g(n) = 1 + 1 + \ldots + 1 = n + 1 = \Theta(n)$. Otherwise,

$$g(n) = \frac{c^{n+1} - 1}{c - 1} = \frac{1 - c^{n+1}}{1 - c}.$$

If $c < 1$, $1 - c < 1 - c^{n+1} < 1$. Thus, $1 < g(n) < \frac{1}{1-c}$. $g(n) = \Theta(1)$.
If $c > 1$, $c^{n+1} > c^{n+1} - 1 > c^n$. Thus, $\frac{c^n}{1-c} < g(n) < \frac{c}{1-c} \cdot c^n$. $g(n) = \Theta(c^n)$. $\square$

Assignment 2, Due on September 10th, Wednesday

1. (1 **point**) Page 39 of DPV, 1.11
2. (2 **points**) Page 40 of DPV, 1.19
3. (2 **points**) Page 40 of DPV, 1.20

Is $4^{1536} - 9^{4824}$ divisible by 35?

Proof.

$$35 = 5 \cdot 7, \quad 5 \text{ and } 7 \text{ are primes.}$$

By Fermat's Little Theorem,

Theorem

For any prime p and $1 \leq a < p$, $a^{p-1} \equiv 1 \mod p$.

Thus, $a^{5-1} \equiv 1 \mod 5$ and $a^{7-1} \equiv 1 \mod 7$. Furthermore, we have $(a^{5-1})^{7-1} = (a^4)^6 = a^{24} \equiv 1 \mod (5 \cdot 7)$. That is $a^{24} \equiv 1 \mod 35$, for all $1 \leq a < 35$. Therefore, $4^{1536} = 4^{24 \cdot 64} \equiv 1 \mod 35$ and $9^{4824} = 9^{24 \cdot 201} \equiv 1 \mod 35$. We conclude that $4^{1536} \equiv 9^{4824} \mod 35$. So the difference is divisible by 35.

□

The *Fibonacci numbers* $F_0, F_1, \ldots$ are given by the recurrence $F_{n+1} = F_n + F_{n-1}$, $F_0 = 0$, $F_1 = 1$. Show that for any $n \geq 1$, $gcd(F_{n+1}, F_n) = 1$.

Proof.

We can show this by induction on n. For $n = 1$, $gcd(F_1, F_2) = gcd(1, 1) = 1$. Now say that the inductive hypothesis is true for all $n \leq k$, this implies that for $n = k + 1$,

$$gcd(F_{k+1}, F_{k+2}) = gcd(F_{k+1}, F_{k+2} - F_{k+1}) = gcd(F_{k+1}, F_k) = 1.$$

Thus, the statement is true for all $n \geq 1$.

□

Find the inverse of: 20 mod 79, 3 mod 62, 21 mod 91, and 5 mod 23.

1. $gcd(20, 79) = gcd(20, 19) = gcd(19, 1) = 1$. Thus, $1 = 20 - 1 \cdot 19 = 20 - 1 \cdot (79 - 3 \cdot 20) = 20 - 79 + 3 \cdot 20 = 4 \cdot 20 - 1 \cdot 79$. So, $20^{-1} = 4 \bmod 79$.
2. $gcd(3, 62) = gcd(3, 2) = gcd(2, 1) = 1$. Thus, $1 = 3 - 2 = 3 - (62 - 20 \cdot 3) = 3 - 62 + 20 \cdot 3 = 21 \cdot 3 - 62 \cdot 1$. So, $3^{-1} = 21 \bmod 62$.
3. $gcd(21, 91) = gcd(21, 7) = gcd(7, 7) \neq 1$. Thus, $21^{-1} \bmod 91$ does not exist.
4. $gcd(5, 23) = gcd(5, 3) = gcd(3, 2) = gcd(2, 1) = 1$. Thus, $1 = 3 - 2 = 3 - (5 - 3) = 3 \cdot 2 - 5 \cdot 1 = (23 - 4 \cdot 5) \cdot 2 - 5 \cdot 1 = 23 \cdot 2 - 9 \cdot 5$. So, $5^{-1} = -9 = 14 \bmod 23$.

Assignment 3, Due on September 24th, Wednesday

1. (1.5 **points.**) Page 40 of DPV, 1.29. You do not need to answer how many bits are needed to choose a function from the family.
2. (1 **point.**) (CLSR page 98, 5.2-4) Use indicator random variable to solve the following problem, which is known as the **hat-check problem**. Each of n customers gives a hat to a hat-checker persona at a restaurant. The hat-checker person gives the hats back to the customer in a random order. What is the expected number of customers that get back their own hat?
3. (1.5 **points.**) (CLSR page 98, 5.2-5) Let $A[1, \ldots, n]$ be an array of n distinct numbers. If $i < j$ and $A[i] < A[j]$, then the pair $(i,\ j)$ is called an **inversion** of A.
    1. (0.5 **point.**) What array with elements from the set $\{1, 2, \ldots, n\}$ has the most inversions? How many does it have?
    2. (1 **point.**) Suppose that the elements of A form a uniform random permutation of $< 1, 2, \ldots, n >$. Use indicator random variables to compute the expected number of inversions.
4. (1 **point**.) (CLSR page 105, 5.3-5) Prove that in the array P in procedure `permute-by-sorting`, the probability that all elements are unique is at least $1 - 1/n$.

Page 40 of DPV, 1.29. You do not need to answer how many bits are needed to choose a function from the family.

1. Here H is the same as in the example in the book, only with 2 coefficients instead of 4. With the same reasoning as the proof of the Property in page 46, we assume that $x_2 \neq y_2$ and we want to determine the probability that equation $a_1 \cdot (x_1 - y_1) = a_2 \cdot (y_2 - x_2)$ holds. Assuming we already picked a_1, that probability is equal to $1/m$, since the only way for the equation to hold is to pick a_2 to be $(y_2 - x_2)^{-1} \cdot a_1 \cdot (x_1 - y_1)$ mod m. We can see that, since m is prime, $(y_2 - x_2)^{-1}$ is unique. Thus H is universal. We need $2 \cdot \lceil \log m \rceil$ bits.
2. H is not universal, since according to above analysis, we need a unique inverse of $(y_2 - x_2)$ mod m where $m = 2^k$. For this to hold m has to be prime, which is not true (unless $k = 1$). We need $2 \cdot k$ bits.
3. We calculate $P = \Pr[f(x) = f(y)]$, for $x \neq y$. We have $P = \sum_{i=1}^{m-1} \frac{1}{(m-1)^2} = \frac{1}{m-1}$. Thus H is universal. The total number of functions $f : [m] \rightarrow [m-1]$ is $(m-1)^m$, so we need $m \cdot \log(m-1)$ bits.

(CLSR page 98, 5.2-4) Use indicator random variable to solve the following problem, which is known as the **hat-check problem**. Each of n customers gives a hat to a hat-checker persona at a restaurant. The hat-checker person gives the hats back to the customer in a random order. What is the expected number of customers that get back their own hats?

Proof.

Let $I(X = i)$ be the indictor random variable showing whether the customer i gets his/her hat back.

$$I(X = i) = \begin{cases} 1, & \text{if customer } i \text{ gets his/her hat;} \\ 0, & \text{otherwise.} \end{cases}$$

Let S be the expected number of customers getting back their own hats; S_i be the expectation for customer i gets his/her hat. Then

$$E[S] = E[\sum_{i=1}^{n} S_i] = \sum_{i=1}^{n} E[S_i] = \sum_{i=1}^{n} \Pr\{I(X = i)\} = \sum_{i=1}^{n} \frac{1}{n} = 1.$$

□

Let $A[1,\ldots,n]$ be an array of n distinct numbers. If $i < j$ and $A[i] < A[j]$, then the pair $(i,\ j)$ is called an **inversion** of A.

1. What array with elements from the set $\{1,2,\ldots,n\}$ has the most inversions? How many does it have?
2. Suppose that the elements of A form a uniform random permutation of $< 1,2,\ldots,n >$. Use indicator random variables to compute the expected number of inversions.

Proof.

1. $[1,2,\ldots,n]$ has the most number of inversions: $\sum_{i=1}^{n}(i-1) = \frac{[1+(n-1)]\cdot(n-1)}{2} = \frac{n\cdot(n-1)}{2}$.
2. Let $I(i,j)$ denote the indicator variable that (i,j) is an inversion pair. Let S denote the expected total number of inversions. Let $S_{i,j}$ denote that a pair (i,j) is inverse.

$$
\begin{aligned}
E[S] &= E[\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} S(i,j)] \\
&= \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} E[S(i,j)] = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} \Pr\{I(i,j)=1\} \\
&= \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} \frac{1}{2} = \frac{n\cdot(n-1)}{4}
\end{aligned}
$$

Prove that in the array P in procedure `permute-by-sorting`, the probability that all elements are unique is at least $1 - 1/n$.

Proof.

We choose a range $[1, \ n^3]$ to select an element, $n \geq 2$. The probability that 2 or more elements are NOT selected from the same number is

$$P = \frac{n^3}{n^3} \cdot \frac{n^3-1}{n^3} \cdot \frac{n^3-2}{n^3} \cdot \ldots \cdot \frac{n^3-(n-1)}{n^3}.$$

Since $n \geq 2$, $n^3 - i \geq n^3 - n = n \cdot (n^2-1) \geq n \cdot n = n^2$, for all $0 \leq i < n$.
Thus,

$$\begin{aligned}
P &\geq (1-\frac{1}{n^2}) \cdot (1-\frac{1}{n^2}) \cdot \ldots \cdot (1-\frac{1}{n^2}) = (1-\frac{1}{n^2})^n = \sum_{k=0}^{n} \binom{n}{k} 1^k (-\frac{1}{n^2})^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} (-\frac{1}{n^2})^{n-k} \\
&= 1 - n \cdot \frac{1}{n^2} + \ldots, \quad \text{Note } \binom{n}{k+1} \cdot (\frac{1}{n^2})^{n-(k+1)} \geq \binom{n}{k} \cdot (\frac{1}{n^2})^{n-k} \\
&\quad \text{(That is, the remaining items are positive, if you pick two by two).} \\
&\geq 1 - \frac{1}{n}.
\end{aligned}$$

$\square$