End Semester Exam

CS 207 :: Autumn 2021

November 17, 2021

1. Please carefully read the statements below and check the boxes next to them to indicate that you agree.

☐ I pledge on my honour that I will not give or receive any unauthorized help on this quiz and all the answers I provide will be my own. I understand that this is a closed-book quiz and I shall not consult any online or offline resources during the exam.

☐ I shall cooperate with the invigilators so that they can monitor my actions during the quiz through video. I understand that this video can be recorded by the invigilators.

Notation:

- $[n]$ denotes the set $\{1, \ldots, n\}$
- $\mathbb{N}$ denotes the set of all non-negative integers
- $\mathbb{Z}^+$ denotes the set of all positive integers.

2. **Logical Equivalence** [3 marks]

P and Q are predicates over some non-empty domain of discourse $\mathcal{S}$, and R is a predicate over $\mathcal{S} \times \mathcal{S}$.

Indicate whether the following statement is true or not. All the quantifiers ($\forall$ and $\exists$) refer to the domain $\mathcal{S}$.

(a)

$$\forall x\, \forall y\, \forall z\ P(x) \vee Q(x)\ \vee\ R(y,z)$$
$$\equiv$$
$$\big(\exists x\ \neg P(x) \wedge \neg Q(x)\big) \rightarrow \forall y\, \forall z\ R(y,z)$$

☐ A. True

☐ B. False

(b)

$$\forall x\, \forall y\, \forall z\ P(x) \vee Q(x)\ \vee\ R(y,z)$$
$$\equiv$$
$$\exists x\ \big(\neg P(x) \wedge \neg Q(x) \rightarrow \forall y\, \forall z\ R(y,z)\big)$$

☐ A. True

☐ B. False

(c)

$$\forall x\, \forall y\, \forall z\ P(x)\ \vee\ Q(x) \vee R(y,z)$$
$$\equiv$$
$$\forall y\, \forall z\ \big(\neg R(y,z)\ \rightarrow \forall x\ P(x) \vee Q(x)\big)$$

☐ A. True

☐ B. False

3. **Order-Preserving/Inverting Functions**

[2 marks]

Let $(S, \leq)$ be a poset.

Suppose $f : S \to S$ is an *order-preserving* function and $g : S \to S$ is an *order-inverting* function. That is,

$$\forall x, y \in S,\ x \leq y \to (f(x) \leq f(y)) \wedge (g(y) \leq g(x)).$$

Then, for each of the following functions, choose the right option:

(a)
$g \circ f$ is:

- [ ] A. Order preserving
- [ ] B. Order inverting
- [ ] C. Possibly neither

(b)
In the following, suppose $S = \mathbb{R}$, the set of real numbers, with the standard $\leq$ order.

h defined by $h(x) = f(x) - f(f(x))$ is:

- [ ] A. Order preserving
- [ ] B. Order inverting
- [ ] C. Possibly neither

(c)
In the following, suppose $S = \mathbb{R}$, the set of real numbers, with the standard $\leq$ order.

h defined by $h(x) = g(x) - g(g(x))$ is:

- ☐ A. Order preserving
- ☐ B. Order inverting
- ☐ C. Possibly neither

(d)
In the following, suppose $S = \mathbb{R}$, the set of real numbers, with the standard $\leq$ order.

h defined by $h(x) = (f(x))^3 - (g(x))^3$ is:

- ☐ A. Order preserving
- ☐ B. Order inverting
- ☐ C. Possibly neither

4. **Counting Walks**

[2 marks]

Consider two adjacent nodes u, v in the cycle C_n. How many *walks* of length exactly k are there that start at u and end at v? State your answer for all $n \geq 3$ and all $k \geq 1$.

Solution: W.l.o.g. suppose v is clockwise from u. Then a walk from u to v should consist of one more clockwise step than all the anti-clockwise steps, in any order. If k is even, there are no such walks. When k is odd, the number of such walks is $\binom{k}{\lfloor k/2 \rfloor}$.

5. **Closed Form from Generating Function**

[2 marks]

Suppose for a function f over $\mathbb{N}$, the generating function is given by

$$G_f(X) = \frac{3X}{(1-X)^5} + \frac{1}{(1-X)^3}.$$

Give a closed form expression for $f(n)$, in the form $3a + b$, where a, b are suitable binomial coefficients.

Solution: Using the extended binomial theorem, the coefficient of X^n is

$$\begin{aligned}(-1)^{n-1} 3 \binom{-5}{n-1} + (-1)^n \binom{-3}{n} &= 3 \cdot \frac{5 \cdot \dots \cdot (3+n)}{(n-1)!} + \frac{3 \cdot \dots \cdot (2+n)}{n!} \\ &= 3\binom{n+3}{4} + \binom{n+2}{2}\end{aligned}$$

6. **Regular Graphs**

[3 marks]

Recall that in a regular graph, all the vertices have the same degree. Prove that in any non-empty regular graph with n vertices, any independent set is of size at most $n/2$.

7. **Chains in Divisibility Poset** [3 marks]

Consider the divisibility poset $(\mathbb{Z}^+, |)$ over the set of positive integers. Suppose $a = p_1^{d_1} \cdot \cdots \cdot p_t^{d_t}$ is the prime factorization of an integer $a > 1$. How many maximal chains are there in which a is the maximum element?

Solution: A maximal chain with a is specified by a sequence of integers $1 = a_0, a_1, \ldots, a_d = a$, where $b_j := a_j / a_{j-1} \in \{p_1, \ldots, p_t\}$, (with each p_i occuring as b_j for d_i indices j). The sequence is fully specified by an ordering of a multi-set consisting of d_i instances of p_i. This equals $\frac{d!}{\prod_{i=1}^t d_i!}$ where $d = \sum_{i=1}^t d_i$.

8. **Partition Number**

[3 marks]

Recall that the partition number $p_n(k)$ denotes the number of integer solutions for $x_1 + \ldots + x_n = k$ satisfying

$$1 \leq x_1 \leq \cdots \leq x_n.$$

Give an expression for the number of solutions that must instead satisfy the stricter condition

$$1 < x_1 \leq \cdots \leq x_{n-1} < x_n,$$

where, the first and last inequalities are strict (the others remain unchanged). You may assume $n > 2$. Justify your answer.

Solution: Consider a solution for $x_1 + \ldots + x_n = k$ satisfying $1 < x_1 \leq \cdots \leq x_{n-1} < x_n$. Let $y_i = x_i - 1$ for $i < n$ and $y_n = x_n - 2$. Observe that $y_1 > 0$, $y_i = x_i - 1 \geq x_{i-1} - 1 = y_{i-1}$ for $i < n$, and $y_n = x_n - 2 > x_{n-1} - 2 = y_{n-1} - 1$. That is, $y_1 \geq 1$ and $y_i \geq y_{i-1}$ for all $i \leq n$. Hence, $1 \leq y_1 \leq \cdots \leq y_n$, and $y_1 + \ldots + y_n = k - (n+1)$. Conversely, if $y_1, \cdots, y_n$ satisfy the above conditions, then $x_i = y_i + 1$ for $i < n$ and $x_n = y_n + 2$ satisfy the original conditions in the problem. Thus there is a bijection between solutions of the two problems. The number of solutions for the new problem is $p_n(k - (n+1))$.

9. **Integer Solution**

[3 marks]

Give a necessary and sufficient condition for 3 positive integers a, b, c to admit an integer solution (x, y, z) to the equation $ax + by + cz = 1$. Prove your claim (based on results from class).

Also, find such a solution when $a = 18$, $b = 26, c = 35$.

Solution: The condition is that $\gcd(a, b, c) = 1$, where $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

Firstly, suppose this condition holds. Let $d = \gcd(a, b)$ so that $d = \alpha a + \beta b$ for some integers α, β. Further, since $\gcd(d, c) = 1$, there exist integers γ, δ such that $\gamma d + \delta c = 1$. Hence, $ax + by + cz = 1$ where $x = \alpha\gamma$, $y = \beta\gamma$ and $z = \delta$.

Conversely, $\gcd(a, b, c)|(ax + by + cz)$ for any x, y, z, and hence if there is an integer solution to the given equation, then $\gcd(a, b, c)|1$. That is, $\gcd(a, b, c) = 1$.

Since $\gcd(18, 26, 39) = 1$ we can find a solution. By EEA to compute $\gcd(26, 18) = 2$ we have $(26, 18) \to (18, 8 = 26-18) \to (8, 2 = 18-2\cdot 8)$ and hence $2 = 18-2(26-18) = 3\cdot 18-2\cdot 26$. Further, $39-19\cdot 2 = 1$. Hence, $39 - 19(3 \cdot 18 - 2 \cdot 26) = 1$. That is, $(-57)18 + 38 \cdot 26 + 1 \cdot 39 = 1$.

10. **Modular Arithmetic**

[4 marks]

Compute the two least significant digits in the decimal representation of $103^{\left(104^{112}\right)}$. Justify your answer.

Solution:

$103^x \equiv 3^x \pmod{100}$.

$3 \in \mathbb{Z}_{100}^*$, so by Euler's totient theorem, $3^x \equiv 3^y \pmod{100}$ if $x \equiv y \pmod{\phi(100)}$. $\phi(100) = 40$.

$104^{112} \equiv 24^{112} \pmod{40}$.

$24 \notin \mathbb{Z}_{40}^*$, so the totient theorem cannot be applied. Writing $40 = 8 \times 5$, the CRT representation of 24 is $(0, 4)$. Raising it to an even power makes it equal to $(0, 1)$. This CRT representation corresponds to (by solving using EEA or by checking all multiples of 8 less than 40) 16.

Hence $24^{112} \equiv 16 \pmod{40}$.

Hence $103^{\left(104^{112}\right)} \equiv 3^{16} \pmod{100}$.

By repeated squaring modulo 100, starting from $3^4 = 81$, we have $3^8 \equiv 81^2 \equiv 61 \pmod{100}$, and $3^{16} \equiv 61^2 \equiv 21 \pmod{100}$.

Hence the last two digits are 21.

11. **Cut Vertex**

In a connected graph, a vertex is said to be a *cut-vertex* if removing it (and all the edges incident on it) from the graph results in a graph with two or more connected components.

(a)

[1 mark]

Give an example of a connected graph with n vertices of which $n-2$ are cut-vertices.

Solution: The path graph P_n with n nodes.

(b)

[3 marks]

Prove using strong induction that any connected graph G with at least two vertices has at least two vertices that are not cut vertices.

Solution: We induct on the number of vertices of the graph.
The base case corresponds to a connected graph with two vertices, and indeed neither of these vertices is a cut-vertex: removing either vertex results in a graph with a single vertex, which is a connected graph.
Suppose the claim holds for all graphs with k or fewer vertices. Consider an arbitrary connected graph G with $k+1$ vertices. We shall prove that G has two vertices which are not cut-vertices.
If G has no cut-vertex, then we are already done. So, suppose G has a cut-vertex v. Let $G_1, \ldots, G_t$, $t > 1$, denote the connected components after removing v from G. Now, define H_i as the graph obtained from G_i by adding the vertex v back, and inserting all the edges in G of the form $\{u, v\}$ where u is in G_i. Since G_i has at least one vertex, H_i has at least two vertices. Further, H_i is connected, because G_i is connected, and v must be connected to at least one vertex of G_i (since originally G was connected). Hence by the induction hypothesis, H_i has two vertices say x_i, y_i which are not cut-vertices. At most one of these two vertices is v; then the other one is not a cut-vertex in G, because removing it from G (without removing v) results in a connected graph. Since this holds for each $i = 1, \ldots, t$ and $t > 1$, we have at least two such vertices.

12. **Poset of Equivalences**

We shall denote a relation over $[n]$ as a subset of $[n] \times [n]$.

Let $\mathcal{Q}$ denote the set of all *equivalence relations* over the set $[n]$. Below we consider the poset $(\mathcal{Q}, \subseteq)$.

(a)

[1 mark]

Give a chain of size n in this poset. Briefly argue that your answer is indeed a chain.

Solution: Let $R_i = \{(x, y) \mid x = y$ or, both $x, y \leq i\}$. Firstly, R_i is an equivalence relation. Further, $R_i \subseteq R_{i+1}$ since $(x, y) \in R_i \implies x, y \leq i \implies x, y \leq i+1 \implies (x, y) \in R_{i+1}$. Further R_i and R_{i+1} are distinct (as $(i, i+1) \in R_{i+1} - R_i$).
Hence $R_1 \subseteq R_2 \subseteq \cdots \subseteq R_n$ is a chain.

(b)

[2 marks]

Show that any $R_1, R_2 \in \mathcal{Q}$ has a greatest lower bound $R \in \mathcal{Q}$. Explicitly describe R, and argue that it is an equivalence relation over $[n]$, and that it is the greatest lower bound.

Solution: Consider the relation $R = R_1 \cap R_2$. This is an equivalence relation; in particular it is transitive because $(x, y), (y, z) \in R \implies (x, y), (y, z) \in R_i$ for $i = 1, 2 \implies (x, z) \in R_i$ for $i = 1, 2$ $\implies (x, z) \in R$.
R is clearly a lower bound for R_1, R_2. Further, in any lower bound R' it must be the case that if $(x, y) \in R$ then $(x, y) \in R'$. That is $R' \subseteq R$, so that R is the greatest lower bound.

(c)

[3 marks]

Show that any $R_1, R_2 \in \mathcal{Q}$ has a least upper bound $R \in \mathcal{Q}$. Explicitly describe R, and argue that it is an equivalence relation over $[n]$, and that it is the least upper bound.

Solution: Consider the relation $R' = R_1 \cup R_2$. Define R to be the transitive closure of R'.
First, we argue that R is an equivalence relation. R is reflexive because R' is (since, say R_1 is) and $R' \subseteq R'$. R is symmetric, because if $(x, y) \in R$, then there is a sequence $x = z_1, \ldots, z_t = y$ such that $(z_i, z_{i+1}) \in R'$; but R' is symmetric and hence there is also a sequence $y = z'_1, \ldots, z'_t = x$ where $(z'_i, z'_{i+1}) = (z_{t+1-i}, z_{t-i}) \in R'$; thus $(y, x) \in R$. Finally, R is transitive as it is a transitive closure.
Next, R is an upper bound of R_1, R_2 since $R_i \subseteq R' \subseteq R$ for $i = 1, 2$.
Finally, if $R'' \in \mathcal{Q}$ is an upper bound of R_1, R_2, then $R' \subseteq R''$. Further, R'' being an equivalence relation, is transitive, and hence it must contain the transitive closure of any of its subsets. In particular, $R \subseteq R''$. Hence R is the least upper bound.

13. **Counting Derangements**

A *derangement* over a finite set X is a bijection $f : X \to X$ such that there is no x for which $f(x) = x$. Let $D(n)$ denote the number of derangements over $[n]$.

(a)

[3 marks]

Prove that for $n > 2$, there exist some two numbers a, b such that

$$D(n) = (n-1)(D(a) + D(b)).$$

Explicitly describe what a, b are as a function of n.

Solution: $\{a, b\} = \{n-1, n-2\}$.
In a bijection $f : [n] \to [n]$ without fixed points, $f(1)$ can take $n-1$ values. For each such choice $f(1) = z$, there are two possibilities: $f(z) = 1$ or $f(z) \neq 1$.
There are $D(n-2)$ derangements over $[n]$ satisfying the first case (i.e., $f(1) = z$ and $f(z) = 1$), because restricted to the domain $[n] - \{1, z\}$, f needs to be a derangement.
Functions of the second kind – i.e., derangements such that $f(1) = z$ and $f(z) \neq 1$ – are exactly those such that $\sigma_z(f(1)) = 1$, and $\sigma_z \circ f$ is a derangement over $[n] - \{1\}$, where σ_z is a bijection over $[n]$ which swaps 1 and z, but leaves all other elements fixed. To see this, note that

- $f(1) = z$ iff $\sigma_z(f(1) = 1$,
- $f(z) \neq 1$ iff $\sigma_z(f(z)) \neq z$,
- for all x other than $1, z$, $f(x) \neq x$ iff $\sigma_z(f(x)) \neq \sigma_z(x) = x$.

There are $D(n-1)$ choices for $\sigma_z \circ f$, and hence for f satisfying the second case.

(b)

[3 marks]

Prove that for all $n \geq 1$,

$$D(n) = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$$

Solution: We can use inclusion-exclusion to compute the size of the set $S_1 \cup \cdots \cup S_n$, where S_j is the set of bijections which fix j. Intersection of i such sets has size $(n-i)!$, and there are $\binom{n}{i}$ such sets. Then by the inclusion-exclusion principle,

$$|S_1 \cup \cdots \cup S_n| = \sum_{i=1}^{n} (-1)^{i-1} \binom{n}{i} (n-i)! = \sum_{i=1}^{n} (-1)^{i-1} \frac{n!}{i!}$$

Subtracting this from the total number of bijections $n!$ gives the desired formula.
Alternate solution: This can also be shown by induction and the previous part.
$D(1) = 0 = 1(1-1)$, and $D(2) = 1 = 2(1 - 1 + \frac{1}{2})$ satisfy the given formula.

Suppose for all $n \leq k$ the formula holds. Then,

$$
\begin{aligned}
D(k+1) = k(D(k) + D(k-1)) &= k[(\sum_{i=0}^{k-1} \frac{(-1)^i}{i!}(k! + (k-1)!) + k!\frac{(-1)^k}{k!}] \\
&= k[(k-1)!(k+1)\sum_{i=0}^{k-1} \frac{(-1)^i}{i!} + (-1)^k] \\
&= [(k+1)!\sum_{i=0}^{k-1} \frac{(-1)^i}{i!}] + k(-1)^k \\
&= [(k+1)!\sum_{i=0}^{k-1} \frac{(-1)^i}{i!}] + (k+1-1)(-1)^k \\
&= [(k+1)!\sum_{i=0}^{k-1} \frac{(-1)^i}{i!}] + (k+1)!\frac{(-1)^k}{k!} + (k+1)!\frac{(-1)^{k+1}}{(k+1)!} \\
&= (k+1)!\sum_{i=0}^{k+1} \frac{(-1)^i}{i!}
\end{aligned}
$$

14. **Graph and Recursion**

We define a family of graphs X_n as follows.

The vertex set of X_n is $V = \mathbb{P}([n])$ (i.e., the power set of $\{1, \ldots, n\}$).

For any two distinct nodes $u, v \in V$, there is an edge $\{u, v\}$ if and only if $u \subsetneq v$ or $v \subsetneq u$ (i.e., one set is *strictly* contained in the other). For example, in X_3, $\{\{1,2\}, \emptyset\}$ is an edge but $\{\{1,2\}, \{2,3\}\}$ is not.

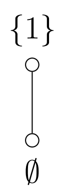
(a)

[1 mark]

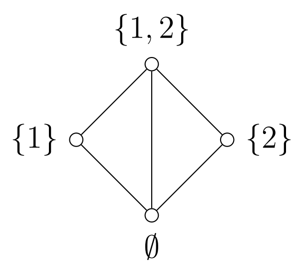
Draw the graphs X_1 and X_2, clearly labeling the nodes.

Solution:

X_1:



X_2:



(b)

[1 mark]

What is the degree of the node u, if $|u| = k$? Justify your answer.

Solution:
A neighbour of u is either a strict subset or a strict superset of u.
There are 2^k subsets of u, of which one is u itself.
A strict superset of u is uniquely specified as $u \cup w$ for $w \subseteq V - u$ and $w \neq \emptyset$. There are 2^{n-k} such sets w, of which one is the empty set.
So degree of u is $(2^k - 1) + (2^{n-k} - 1) = 2^k + 2^{n-k} - 2$.

(c)

[3 marks]

Let $f(n)$ denote the number of edges in X_n. Write a recursive definition for $f(n)$. Justify your formula.

Hint: To check your answer, it may help to know that X_3 has 19 edges.

Solution: Nodes in X_n are of the form u and $u' := u \cup \{n\}$ where u is a node in X_{n-1}. An edge in X_n is of the form $\{u, v\}$, $\{u', v'\}$ or $\{u', v\}$. If of the form $\{u, v\}$ or $\{u', v'\}$, then $\{u, v\}$ is an edge in X_{n-1}; if of the form $\{u', v\}$, either $\{u, v\}$ is an edge in X_{n-1} with $u \supsetneq v$, or $u = v$.
So, an edge $\{u, v\}$ in X_{n-1}, with $u \supsetneq v$ appears as $\{u, v\}$, $\{u', v'\}$ and $\{u', v\}$. Also edges of the form $\{u', u\}$.
$f(1) = 1$ and $f(n) = 3f(n-1) + 2^{n-1}$.

(d)

[3 marks]

Unroll the above recursion as a rooted tree to find a closed form expression for $f(n)$.

Solution: At level i (starting with $i = 0$), there are 3^i nodes, with value 2^{n-1-i}. Up to level $i = n-1$.
So $f(n) = \sum_{i=0}^{n-1} 3^i 2^{n-1-i} = 2^{n-1} \sum_{i=0}^{n-1} (3/2)^i = 2^{n-1}((3/2)^n - 1)/(1/2)) = 3^n - 2^n$.