Final Examination

Your name:_____

Circle the name of your TA/LA:

Chiyoun Jay Jeffrey Jessica Tina

- This final is **closed book**, though you are allowed one two-sided, handwritten crib sheet. There is an Appendix that repeats some information. Total time is 3 hours.
- There are twelve (12) problems totaling 100 points.
- Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Please keep your entire answer to a problem on that problem's page.
- You may assume any of the results presented in class or in the lecture notes, unless the problem states otherwise.
- GOOD LUCK!

DO NOT WRITE BELOW THIS LINE

Problem	Points	Grade	Grader
1	20		
2	5		
3	4		
4	5		
5	7		
6	10		
7	8		
8	6		
9	7		
10	5		
11	3		
12	20		
Total	100		

Problem 1 (20 points)**.**

(a) (5 points) Circle all the properties below that are preserved under graph isomorphism.

- Two edges are of equal length.
- There is a simple cycle that traverses all the vertices.
- The graph is connected when we remove any two edges.
- There exists an edge that is an edge of every spanning tree.
- The negation of a property that is preserved under isomorphism.

(b) (4 points) For each of the relations below, indicate whether it is *transitive* but not a partial order (**Tr**), a *total order* (**Tot**), a *strict partial order* that is not total (**S**), a *weak partial order* that is not total (**W**), or *none* of the above (**N**).

- the "is a subgraph of" relation on graphs. (Note that every graph is a considered a subgraph of itself.) _____

Let f, g be nonnegative functions on the real numbers.

- the "Big Oh" relation, $f = O(g)$, _____
- the "Little Oh" relation, $f = o(g)$, _____
- the "asymptotically equal" relation, $f \sim g$. _____

(c) (11 points) Circle **true** for the statements below that are true, and provide counterexamples for those that are not.

The following statements about trees:

- Any connected subgraph is a tree.
  true
  false:

- Adding an edge between two vertices creates a cycle.
  true
  false:

- The number of vertices is one less than twice the number of leaves.
  true
  false:

The following statements about the greatest common divisor:

- If $\gcd(a, b) \neq 1$ and $\gcd(b, c) \neq 1$, then $\gcd(a, c) \neq 1$.
  true
  false:

- $\gcd(k + a, k + b) = k + \gcd(a, b)$ for all $k > 0$.
  true
  false:

- If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
  true
  false:

- $\gcd(a^n, b^n) = (\gcd(a, b))^n$
  true
  false:

The following statements about equivalence mod n, where $n > 1$.

- If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.
  true
  false:

- If $a \equiv b \pmod{\phi(n)}$ for $a, b > 0$, then $c^a \equiv c^b \pmod{n}$.
  true
  false:

- If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$ for any polynomial $P(x)$ with integer coefficients.
  true
  false:

- If $a \equiv b \pmod{nm}$, then $a \equiv b \pmod{n}$, for $m \geq 1$.
  true
  false:

Problem 2 (5 points)**.** Define the set, M, of strings of matched right parentheses, `)`, and left parentheses, `(`, recursively as follows:

- **Base case:** $\lambda \in M$, where λ is the *empty* string,
- **Constructor case:** if $s, t \in M$, then $(s)\,t \in M$.

A string p is a *prefix* of a string q iff there exists some string p' such that $pp' = q$. (Strings p and p' need not be in M.)

Prove using induction that any prefix of a string in M has at most as many `)`'s as `(`'s.

Problem 3 (4 points)**.** Four unfortunate children want to be adopted by four loving foster families. A child can only be adopted by one family, and a family can only adopt one child. Here are their preference rankings (most-favoured to least-favoured):

Child	Families
Lucy:	Hatfields, McCoys, Grinches, Scrooges
Bottlecap:	Grinches, Scrooges, McCoys, Hatfields
Spud:	Hatfields, Scrooges, Grinches, McCoys
Dingdong:	McCoys, Grinches, Scrooges, Hatfields

Family	Children
Grinches:	Dingdong, Spud, Lucy, Bottlecap
Hatfields:	Dingdong, Lucy, Spud, Bottlecap
Scrooges:	Lucy, Bottlecap, Spud, Dingdong
McCoys:	Bottlecap, Dingdong, Lucy, Spud

Suppose each family adopts one of these children. Explain why Lucy must be adopted by the Hatfields, or else there will be a *rogue pair*, that is, there will be a child who prefers another family to its adopted family, and that other family prefers that child to their own.

Problem 4 (5 points)**.**

(a) (3 points) Show that

$$(an)^{b/n} \sim 1.$$

where a, b are positive constants and $\sim$ denotes asymptotic equality. *Hint:* $an = a2^{\log_2 n}$.

(b) (2 points) Show that

$$\sqrt[n]{n!} = \Theta(n).$$

Problem 5 (7 points)**.**

(a) (2 points) Define a bijection between the nonnegative integers and all the even integers.

(b) (1 point) Let A_i be the set of length n binary strings in which `011` occurs starting at the ith position. (So A_i is empty for $i > n - 2$.) For $i < j$, the intersections $A_i \cap A_j$ that are nonempty are all the same size. What is $|A_i \cap A_j|$ in this case?

(c) (1 point) Let t be the number of intersections $A_i \cap A_j$ that are nonempty, where $i < j$. Express t as a binomial coefficient:

(d) (3 points) How many length 9 binary strings that contain the substring `011` are there? You should express your answer as an integer or as a simple expression which may include the constant, t, of part (c).

Hint: Inclusion-exclusion for $\left|\bigcup_1^7 A_i\right|$.

Problem 6 (10 points)**.** A *triangle* in a graph is a set of three mutually adjacent vertices. A graph is *triangle-free* if it has no triangles. In the following problem, we consider only finite graphs.

(a) (7 points) Prove that if a planar graph is triangle-free, then it has a vertex of degree at most 3.

(b) (3 points) Use part (a) to give an elementary proof that every triangle-free planar graph is 4-colorable. (You may not, of course, assume the 4-color Theorem for planar graphs in your proof.)

Problem 7 (8 points)**.** The following state machine describes an algorithm to calculate $a^n \pmod m$ efficiently.

Its states are triples of nonnegative integers (x, y, z). The initial state is $(a, n, 1)$. When $y > 0$, the state machine follows the following rule

$$(x, y, z) \to \begin{cases} (\text{rem}(x^2, m), y/2, z) & \text{if } 2 \mid y \\ (\text{rem}(x^2, m), (y-1)/2, \text{rem}(xz, m)) & \text{otherwise.} \end{cases}$$

When $y = 0$, the state machine terminates and outputs z.

(a) (2 points) Circle the statement below that is an invariant of this state machine.

- $x^y z = a^n$
- $a^y z \equiv x^n \pmod m$
- $x^y z \equiv a^n \pmod m$
- $\text{rem}(x^{yz}, m) = \text{rem}(a^n, m)$

(b) (3 points) Prove that the answer to part (a) is invariant.

(c) (1 point) Conclude that if and when this algorithm terminates, $z \equiv a^n \pmod m$.

(d) (2 points) Explain why this algorithm terminates in $O(\log_2 n)$ steps.

Problem 8 (6 points)**.**

(a) (2 points) Give a combinatorial proof of the following identity.

$$\sum_{i=0}^{k} \binom{n}{i}\binom{n}{k-i} = \binom{2n}{k}. \tag{1}$$

Hint: Consider the number of size-k subsets of $\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$.

(b) (2 points) Explain why the number of size-k subsets of $\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$ is the coefficient of x^k in $(1+x)^{2n}$. *Hint:* Convolution Rule.

(c) (2 points) Use part (b) and the fact that $(1+x)^{2n} = (1+x)^n(1+x)^n$ to give an alternative proof of equation (1).

Problem 9 (7 points)**.** A $2k$*-cycle* communication network is illustrated below.

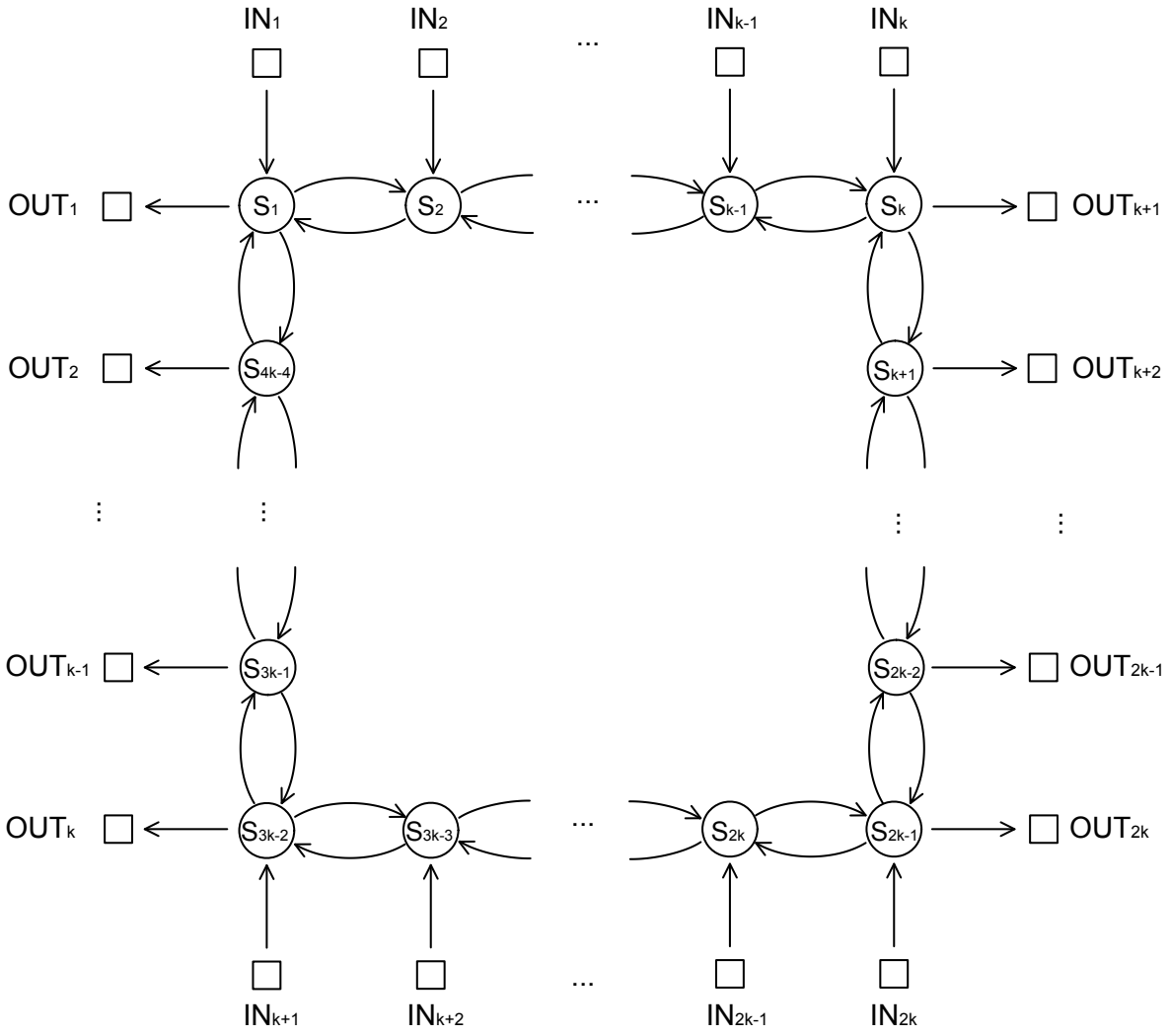

Figure 1: $2k$-cycle network.

For the permutation routing problems given below, it can be shown (though you may take it as given) that congestion is minimized by shortest-path routing with the added stipulation that ties are settled by routing packets clockwise.[1]

(a) (3 points) What is the congestion of the set of paths in the solution to the routing problem described by the permutation

$$\pi(i) = i \text{ for } 1 \leq i \leq 2k$$

and where does this congestion occur (which switches are most overloaded)?

(b) (4 points) What is the congestion of the set of paths in the solution to the routing problem described by the permutation

$$\begin{aligned} \pi(1) &= 2k \\ \pi(i) &= i \text{ for } 1 < i < 2k \\ \pi(2k) &= 1 \end{aligned}$$

and where does this congestion occur (which switches are most overloaded)?

[1] A tie occurs at an input when there are two or more minimum length paths from the input to its specified output.

Problem 10 (5 points)**.** Suppose that *Let's Make a Deal* is played according to different rules. There are three doors, with a prize hidden behind one of them. The contestant is allowed to pick a door. The host then reveals one of the remaining doors randomly, which may or may not have a prize behind it. If the host reveals the door with a prize, the contestant loses. Otherwise, the contestant is allowed to stay with his original door or to switch to the remaining door.

(a) (2 points) What is the probability that the host reveals an empty door?

(b) (3 points) Given that the host revealed an empty door, what is the probability that the contestant will win the game by switching?

Problem 11 (3 points)**.** Independently toss a fair coin and roll a fair die with three faces, numbered 1 through 3. Let H be the indicator variable for getting Heads, and D be the random variable for the number on the die. Define random variable $C ::= \mathrm{rem}(H + D, 2)$.

Which pairs of H, D, C are independent? (Short answer; no proof called for.)

Problem 12 (20 points)**.** The parts of the following problem are designed so that later parts can be answered correctly even if some earlier answers are incorrect.

Jeff wanted to see what would happen if he put a quarter on a railroad track. The result of his experiment was a biased coin that, when flipped, came up heads with probability 2/3 and tails with probability 1/3.

(a) (4 points) If Jeff repeatedly and independently flips his coin, what is the expected number of flips until the sequence HH comes up?

The process of repeatedly flipping his coin can be modeled by a state machine with states 0, 1 and 2 representing events and transistions representing conditional probabilities associated with coin flips.

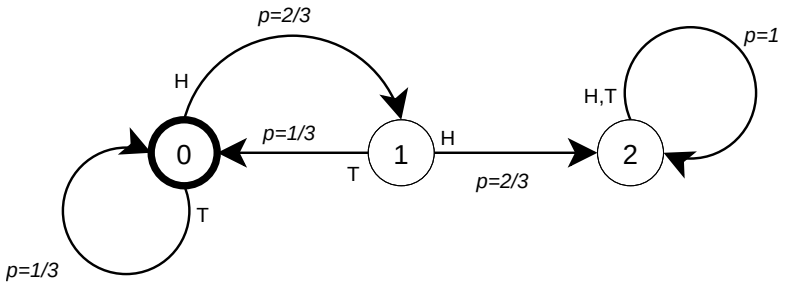

Figure 2: State machine for flipping biased coin.

Let A_n be the probability of being in state 0 after n flips.

The recurrence for A_n is given by:

$$A_0 = 1$$
$$A_1 = \frac{1}{3}$$
$$A_n = \frac{1}{3}A_{n-1} + \frac{2}{9}A_{n-2} \text{ for } n > 1$$

(b) (4 points) Give the generating function $A(x)$ for the sequence $A_0, A_1, A_2, \ldots$.

(c) (4 points) Use your generating function to show that the closed form for the probability of being in state 0 after n flips is

$$A_n = \left(\frac{2}{3}\right)^{n+1} - \left(-\frac{1}{3}\right)^{n+1} \tag{2}$$

Let T be a random variable representing the number of coin flips until the sequence HH comes up for the first time. The distribution of T is given by $\Pr\{T = n\} = \text{PDF}_T(n) = \frac{4}{9}A_{n-2}$.

Simplifying,

$$\text{PDF}_T(n) = \begin{cases} (\frac{2}{3})^{n+1} - 4(-\frac{1}{3})^{n+1} & \text{if } n \geq 1, \\ 0 & \text{if } n < 1. \end{cases}$$

(d) (4 points) Let μ be $\mathrm{E}[T]$. Find a simple formula for $\mathrm{Var}[T]$. Your formula should not have any subscripted summations or products but may include the constant, μ. (The value of μ is the answer to part (a), but by answering in terms of μ, you can get full credit even if your answer to (a) was incorrect.)

Hint: $\sum_{i=1}^{\infty} i^2 x^i = (x(1+x))/(1-x)^3$

(e) (2 points) Let $\sigma^2 = \mathrm{Var}[T]$. What is the Chebyshev bound on the probability that more than n flips occur before HH appears, where $n > \mu$? Your answer should be a simple formula which may involve the unevaluated constants μ and σ. (The value of σ^2 is the answer to part (d), but by answering in terms of μ and σ^2, you can get full credit even if your answers to the previous parts were incorrect.)

(f) (2 points) Show that the actual probability that more than n flips occur before HH appears is asymptotically smaller than the Chebyshev bound of part (e).

Appendix

The Pulverizer: example

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \mathrm{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{array}{rcll} \gcd(259, 70) & = & \gcd(70, 49) & \text{since } \mathrm{rem}(259, 70) = 49 \\ & = & \gcd(49, 21) & \text{since } \mathrm{rem}(70, 49) = 21 \\ & = & \gcd(21, 7) & \text{since } \mathrm{rem}(49, 21) = 7 \\ & = & \gcd(7, 0) & \text{since } \mathrm{rem}(21, 7) = 0 \\ & = & 7. & \end{array}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\mathrm{rem}(x, y)$		$x - q \cdot y$
259	70	49	=	$259 - 3 \cdot 70$
70	49	21	=	$70 - 1 \cdot 49$
			=	$70 - 1 \cdot (259 - 3 \cdot 70)$
			=	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	=	$49 - 2 \cdot 21$
			=	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			=	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

RSA Public Key Encryption

Beforehand The receiver creates a public key and a secret key as follows.

1. Generate two distinct primes, p and q.
2. Let $n = pq$.
3. Select an integer e such that $\gcd(e, (p-1)(q-1)) = 1$.
   The *public key* is the pair (e, n). This should be distributed widely.
4. Compute d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.
   The *secret key* is the pair (d, n). This should be kept hidden!

Encoding The sender encrypts message m to produce m' using the public key:

$$m' = \mathrm{rem}(m^e, n).$$

Decoding The receiver decrypts message m' back to message m using the secret key:

$$m = \mathrm{rem}((m')^d, n).$$