CS207 - Discrete Structures
End-semester examination

13 Nov 2014
Maximum Marks: 70
Max time: 3 hrs

Instructions:

- Attempt *all* questions. Even if you are unable to solve some sub-parts of a question, you may *assume and use* them to solve the remaining sub-parts.
- Write all answers and proofs carefully. Considerable weightage will be given to clarity and completeness of proofs.
- If you are making any assumptions or using results proved in class/tutorials, you *must* state them clearly.
- Do *NOT* copy or use any other unfair means. The penalty will be an FR grade and offenders will be reported to the Disciplinary Action Committee.

---

1. For each of the below state true or false with a justification in 2-3 sentences. [12]

   (a) The set G of all 2×2 matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where a, b are not both simultaneously zero real numbers, is an abelian sub-group of $GL_2(\mathbb{R})$ (the group of invertible 2×2 matrices with real entries).

   (b) The Diffie-Hellman key-exchange and the RSA cryptosystem discussed in class both use the same cyclic group $(\mathbb{Z}_p, \times_p)$, for some prime p.

   (c) For positive integers a, b, m we have $a \equiv b \mod m$ iff $a^n \equiv b^n \mod m$ for all $n \in \mathbb{Z}^+$.

   (d) The remainder when 3^{50} is divided by 7 is 4

2. Recall that, for a simple graph $G = (V, E)$, its complement is the graph $\bar{G} = (V', E')$ such that $V = V'$ and $(i, j) \in E'$ iff $(i, j) \notin E$. A simple graph $G = (V, E)$ is called self-complementary, if it is isomorphic to its complement. Let $|V| = n$. [4+4+6]

(a) Recall that P_k is the path graph on k vertices. Other than P_1, find another $\ell \in \mathbb{N}$ such that P_ℓ is a self-complementary graph. Are there any other self-complementary paths? Justify.

(b) Determine the values of k for which C_k, the cycle with k vertices, is self-complementary.

(c) For any simple graph G, show that if G is self-complementary, then $n \equiv 0 \mod 4$ or $n \equiv 1 \mod 4$.

3. In a village there are three schools with n students in each of them. Every student from any of the schools is on speaking terms with at least $n+1$ students from the other two schools. Show that we can find three students, no two from the same school, who are on speaking terms with each other. [6]

4. (a) Take a standard deck of cards, and deal them out into 13 piles of 4 cards each. Show, using Hall's theorem, that it is always possible to select exactly 1 card from each pile, such that the 13 selected cards contain exactly one card of each rank (ace, 2, 3, . . . , queen, king). [6]

(b) Let H be a finite group and let K be a subgroup of H. Let $n = |G|/|H|$. Show, using part (a) or otherwise, that there exist elements $h_1, h_2, \ldots, h_n \in H$ such that $h_1K, h_2K, \ldots, h_nK$ are the left cosets of K and $Kh_1, Kh_2, \ldots, Kh_n$ are the right cosets of K. [6]

5. Let $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ be a function s.t., $f(f(i)) = 1$ for all $i \in \{1, \ldots, n\}$. [2+6]

(a) Prove that $f(1) = 1$.

(b) Show that the number of such functions is

$$\sum_{k=1}^{n-1} \binom{n-1}{k} k^{n-1-k}$$

6. Let S be a set of size n. Consider the poset $(2^S, \subseteq)$. Our goal in this problem is to bound the size of any antichain in this poset. Recall that an antichain is a subset of pairwise incomparable elements in a poset while a chain is a totally ordered subset of the poset. [3+3+6+4]

(a) Consider the set of *maximal chains* in $(2^S, \subseteq)$, where a maximal chain is a chain to which no other element can be added. Show that there are at most $n!$ maximal chains.

(b) Let $\mathcal{M}$ be any anti-chain. Consider $\mathcal{P} = \{(\mathcal{C}, M) \mid M \in \mathcal{M}$ is a set and $\mathcal{C}$ is a maximal chain containing $M\}$. We will count such ordered pairs in two ways. First, using (a) show that $|\mathcal{P}| \leq n!$

(c) Prove that

$$|\mathcal{P}| = \sum_{M \in \mathcal{M}} |M|!(n - |M|)!$$

(d) Using the above, conclude that the length of any anti-chain in $(2^S, \subseteq)$ is $\leq \binom{n}{\lfloor n/2 \rfloor}$.

7. Which topic and which theorem/result did you like best in this course? Why? Explain in a few sentences. [2]