CSC3001 Discrete Mathematics

Midterm Examination

November 9, 2024: 9:30am - 12:00pm

Name: ______________________________ Student ID: ______________________________

Answer ALL questions in the Answer Book.

Question	Points	Score
1	20	
2	20	
3	16	
4	16	
5	12	
6	16	
Total:	100	

1. (20 points) Let n be a positive integer. We want to compute how many valid ways to add n pairs of parentheses. E.g. There are 5 valid ways to add 3 pairs of parentheses, namely, $((())), (()()), (())(), ()(()), ()()()$. Let r_n denote the number of ways to add n pairs of parentheses. Denote $r_0 = 1$.

   (a) (10 points) Find a recursion of r_n using $r_0, r_1, \ldots, r_{n-1}$. Briefly justify your solution.

   (b) (10 points) Find r_4 and r_5 .

> **Solution:**
>
> (a) We have $r_n = \sum_{i=1}^{n} r_{i-1} r_{n-i}$. In fact, consider the valid parentheses always start with a "(". All possible combinations of $n-1$ pairs can be split into two sub-problems: $i-1$ pairs on the left in a pair of parentheses, and $n-i$ pairs on the right.
>
> (b) $r_4 = 14$, $r_5 = 42$.

2. (20 points) Let D be the domain of all people. Let predicate $\text{nice}(x), x \in D$ denote that x is a nice person, predicate $\text{busy}(x), x \in D$ denote that x is a busy person, and $\text{friend}(x, y), x, y \in D$ denote that x, y are friends. Using D, nice, busy, and friend to represent the following statements in first-order logic.

   - Every busy person has at least one friend;
   - Nice people never have a busy person as a friend.

> **Solution:** $\forall x \in D,\ (\text{busy}(x) \to \exists y \in D,\ \text{friend}(x, y))$; $\forall x \in D,\ (\text{nice}(x) \to \neg \exists y \in D,\ \text{busy}(y) \land \text{friend}(x, y))$.

3. (16 points) Let k, n be positive integers. Alice recently learned a "telescoping" trick to derive the sum of integer power formulas. Namely, by $k^4 - (k-1)^4 = k^4 - \left(k^4 - 4k^3 + 6k^2 - 4k + 1\right) = 4k^3 - 6k^2 + 4k - 1$, Alice knows

$$\sum_{k=1}^{n} \left[k^4 - (k-1)^4\right] = 4\sum_{k=1}^{n} k^3 - 6\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 .$$

   (a) (8 points) Show that

$$\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6 .$$

   (b) (8 points) Find a polynomial formula for $\sum_{k=1}^{n} k^3$.

Solution:

(a) We use induction to prove the statement. For the base case $n = 1$, both sides of the equation are 1. For the induction step, assume that the equation holds for k, then we have $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$. Then, for $n = k+1$,

$$\begin{aligned}\sum_{k=1}^{n+1} k^2 &= n(n+1)(2n+1)/6 + (n+1)^2 \\ &= (n+1)(n+2)(2n+3)/6\,.\end{aligned}$$

By induction the statement holds for all $n \in \mathbb{Z}^+$.

(b) Because

$$\begin{aligned} n^4 &= \sum_{k=1}^{n} \left[k^4 - (k-1)^4\right] \\ &= 4\sum_{k=1}^{n} k^3 - 6\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 \\ &= 4\sum_{k=1}^{n} k^3 - 6n(n+1)(2n+1)/6 + 4n(n+1)/2 - n \\ &= 4\sum_{k=1}^{n} k^3 - n(n+1)(2n+1) + 2n(n+1) - n\,, \end{aligned}$$

we have

$$\begin{aligned} 4\sum_{k=1}^{n} k^3 &= n^4 + n(n+1)(2n+1) - 2n(n+1) + n \\ &= n^2(n+1)^2\,. \end{aligned}$$

Therefore, $\sum_{k=1}^{n} k^3 = n^2(n+1)^2/4$.

4. (16 points) Prove that there are infinitely many prime numbers of the form $4k+3$ for some nonnegative integer k.

Solution: Suppose that there are only finitely many primes of the form $4k+3$, namely $q_1, q_2, \ldots, q_n$. Let $Q = 4q_1q_2\cdots q_n - 1$. Note that Q is of the form $4k+3$. If Q is prime, then we have found a prime of the desired form different from all those listed. If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k+1$ or of the form $4k+3$, and the product of primes of the form $4k+1$ is also of this form, there must be a factor of Q of the form $4k+3$ different from the primes we listed.

5. (12 points) Let a, b, n be nonnegative integers and $a \geq b$. Consider Euclid's greatest common divisor algorithm.

   gcd(a,b)
   if $b = 0$ **then**
       Output a
   else
       Write $a = qb + r$, where $q = \lfloor a/b \rfloor$, $r = a - qb$ (1)
       Output gcd(b,r)
   end if

   Let $f_1 = f_2 = 1$, $f_k = f_{k-1} + f_{k-2}$, $\forall k \geq 2$. Show that if $b < f_n$, $n \geq 1$, then gcd(a,b) executes line (1) for at most $n - 1$ times.

Solution: We instead prove that for Euclid's algorithm to execute (1) at least n times, a, b need to be at least f_{n+1}, f_n, respectively. We prove this by induction. The base case is $n = 1$, where a, b are indeed at least 1. For the induction step, with the induction hypothesis, the new a for $n + 1$ steps is at least the new $b + r$, which is at least $f_{n+1} + f_n = f_{n+2}$ as we desired.

Remark: This proof was published by Gabriel Lamé in 1844 and represents the beginning of computational complexity theory.

6. (16 points) Let k, r be positive integers.

   (a) (8 points) Let $\mathcal{F} = \{\{1, 2, 3\}, \{1, 3, 4\}, \{1, 3, 5\}, \{2, 6, 7\}, \{5, 8, 9\}, \{4, 7, 9\}\}$. Find a set $W \subseteq \mathcal{F}$ and a set S, such that $|W|$ is at least 3, while every pair of distinct sets $X, Y \in W$, $X \neq Y$, satisfy $X \cap Y = S$.

   (b) (8 points) Let $\mathcal{F}$ be a collection of more than $k!(r-1)^k$ distinct non-empty sets each of size at most k. Prove that there is a collection W of at least r distinct sets in $\mathcal{F}$, such that there exists a set S where for every pair of distinct sets X, Y in W, $X \neq Y$, we have $X \cap Y = S$.

Solution:

A sunflower is a collection of sets $W = \{A_1, \cdots, A_r\}$ if there exists a set S (which is called the *core*), such that for any $i \neq j$, we have $A_i \cap A_j = S$. The sets A_i are called the *petals* of the sunflower.

(a) The sunflower $W = \{\{1, 2, 3\}, \{1, 3, 4\}, \{1, 3, 5\}\}$; The core $S = \{1, 3\}$.

(b) We proceed by induction on k. For $k = 1$, we have more than $r - 1$ disjoint 1-element sets, so any r of them form a sunflower with r petals (and an empty set core). Now let $k \geq 2$, and take a maximal family $\mathcal{A} = \{A_1, \cdots, A_t\}$ of pairwise disjoint members of $\mathcal{F}$. Here maximal means that it is impossible to add another set to the family while maintaining the property that all sets are pairwise disjoint. If $t \geq r$, then these sets form a sunflower with $t \geq r$ petals (and an empty set core) and the statement follows.

Assume that $t \leq r-1$ and let $B = A_1 \cup \cdots \cup A_t$. Then $|B| \leq k(r-1)$. By the maximality of $\mathcal{A}$, the set B intersects every member of $\mathcal{F}$. Then some set $x \in B$ must be contained in at least

$$\frac{|\mathcal{F}|}{|B|} > \frac{k!(r-1)^k}{k(r-1)} = (k-1)!(r-1)^{k-1}$$

many members of $\mathcal{F}$. Delete x from these sets and consider the family

$$\mathcal{F}_x = \{A \backslash \{x\} : A \in \mathcal{F}, x \in S\}.$$

Then all sets in $\mathcal{F}_x$ have at most $k-1$ elements. By the inductive hypothesis, there is a sunflower with r petals in $\mathcal{F}_x$. If we add x back to all of the sets in this sunflower, then we still have a sunflower with r petals, but now all sets are in $\mathcal{F}$, as we desired.

Remark: This statement is known as the sunflower lemma, which was proved by Erdös and Rado in 1960. It asserts that a large enough collection of sets, i.e. of size more than $k!(r-1)^k$, must contain a sunflower of r petals. This bound has been recently improved to $O(r\log(kr))^k$ by a series of works. See the blogpost written by Terence Tao.