# CSC3001 Discrete Mathematics

## Mid-term Examination

November 5, 2022: 9:00am - 11:30am

Name: ________________________ Student ID: ________________________

Answer ALL questions in the Answer Book.

| Question | Points | Score |
|---|---|---|
| 1 | 20 | |
| 2 | 20 | |
| 3 | 20 | |
| 4 | 16 | |
| 5 | 16 | |
| 6 | 8 | |
| Total: | 100 | |

1. (20 points) For $n \in \mathbb{Z}^+$, let $A(n) = \{b \in \mathbb{Z}^+ \mid n|b\}$ and $B(n) = \{b \in \mathbb{Z}^+ \mid b|n\}$.
   (a) (10 points) Find $B(6)$ and $|B(6)|$.
   (b) (10 points) Show that there is a unique element in $A(n) \cap B(n)$.

**Solution:**

**Part (a)** $B(6) = \{1, 2, 3, 6\}$. $|B(6)| = 4$.

**Part (b)** As $n|n$, we have $n \in A(n)$ and $n \in B(n)$, and subsequently $n \in A(n) \cap B(n)$. Meanwhile, any element in $B(n)$ is at most $n$ and any element in $A(n)$ is at least $n$. As such $n$ is the unique element in $A(n) \cap B(n)$.

2. (20 points) Let $p, q, r$ be statements.
   (a) (10 points) Determine whether $p \to (q \to r)$ is logically equivalent to $(p \to q) \to r$. Please justify your answer.
   (b) (10 points) Find a logical formula that only contains the logical operators $\wedge, \vee, \neg$ and the statements $p, q$ for **the negation of** $p \leftrightarrow q$.

**Solution:**

**Part (a)** The two formulas are not equivalent. If $p, q, r$ are all false, then $p \to (q \to r)$ is true while $(p \to q) \to r$ is false.

**Part (b)** Recall that $p \to q \equiv \neg p \vee q$. Then

$$\begin{aligned}
\neg(p \leftrightarrow q) &\equiv \neg((p \to q) \wedge (q \to p)) \\
&\equiv \neg((\neg p \vee q) \wedge (\neg q \vee p)) \\
&\equiv (\neg(\neg p \vee q) \vee \neg(\neg q \vee p)) \\
&\equiv (p \wedge \neg q) \vee (q \wedge \neg p) .
\end{aligned}$$

3. (20 points) Let $n, a, b$ be positive integers. We say an integer $n$ is $(a, b)$-makeable if $n$ can be written as a nonnegative integer linear combination of $a$ and $b$, i.e., $n = xa + yb$ where $x, y$ are nonnegative integers.
   (a) (10 points) Show that every integer $n \geq 4$ is $(2, 5)$-makeable.
   (b) (10 points) Show that every integer $n \geq 12$ that is divisible by 3 is $(6, 15)$-makeable.

**Solution:**

**Part (a)** Let us prove by induction on $n$. It is clear that 4 and 5 are $(2,5)$-makeable as $4 = 2 \cdot 2 + 0 \cdot 5$ and $5 = 0 \cdot 2 + 1 \cdot 5$. Assume every integer $m$ that satisfies $4 \leq m < n$ for some $n \geq 6$ is $(2,5)$-makeable. Then we have $4 \leq n - 2 < n$. Since $(n-2)$ is $(2,5)$-makeable by the induction hypothesis, we can write $n - 2 = 2x + 5y$ for some nonnegative integers $x, y$. It follows that $n = 2(x+1) + 5y$ and thus $n$ is $(2,5)$-makeable. In conclusion, every integer $n \geq 4$ is $(2,5)$-makeable.

**Part (b)** Observe that $\gcd(6,15) = 3$. From Part (a), every integer $n \geq 4$ can be written as $n = 2x + 5y$ for some nonnegative integers $x, y$. Therefore, for every $n \geq 4$ we have $3n = 6x + 15y$ for some nonnegative integers $x, y$. In other words, every integer no smaller than 12 and divisible by 3 is $(6,15)$-makeable.

4. (16 points) For $n \in \mathbb{Z}^+$, a degree-$n$ polynomial $c(x)$ is an expression $c_n x^n + \cdots + c_1 x + c_0$ with real variable $x \in \mathbb{R}$ and real coefficients $c_n, \ldots, c_1, c_0$, where $c_n \neq 0$. A nonzero constant is regarded as a degree-0 polynomial and the zero constant is regarded as the degree-$(-1)$ polynomial.

For polynomials $a(x), r(x), b(x)$, where the degree of $b(x)$ is positive, define the following congruence relation

$$a(x) \equiv r(x) \pmod{b(x)}$$

to mean that there exists a polynomial $q(x)$ such that $a(x) = q(x)b(x) + r(x)$ holds for every $x$. In the lectures, we defined a congruence relation between integers. In this question, the congruence relation is defined on polynomials.

(a) (8 points) Let $a(x), b(x)$ be polynomials, where the degree of $b(x)$ is positive. Show that there is a unique polynomial $r(x)$ with degree smaller than $b(x)$ such that $a(x) \equiv r(x) \pmod{b(x)}$.

(b) (8 points) A fundamental lemma in algebra states that when $f(x)$ is a polynomial and $x^*, y^* \in \mathbb{R}$, $f(x) \equiv y^* \pmod{x - x^*}$ if and only if $f(x^*) = y^*$. You could use this lemma without proof.

Let $k \in \mathbb{Z}^+, k \geq 2$. Let $x_1, \ldots, x_k$ be distinct real numbers, and $y_1, \ldots, y_k$ be real numbers. Show that there exists a unique polynomial $f(x)$ of degree at most $k-1$, such that $f(x_i) = y_i$ holds for every $i = 1, \ldots, k$.

**Solution:**

**Part (a)** Let $S = \{r(x) \text{ is a polynomial} \mid a(x) \equiv r(x) \bmod b(x)\}$. Let $D = \{\text{degree of } r(x) \mid r(x) \in S\}$. Because $a(x) \in S$, $D$ is nonempty. Let the minimum element of $D$ be $n'$ and let the degree of $b(x)$ be $n$.

Existence: We prove this by contradiction. If $n' \geq n$, then specify one polynomial $r(x) = r_{n'} x^{n'} + \cdots + r_1 x_1 + r_0$ in $S$ with degree $n'$. Write $b(x) = b_n x^n + \cdots + b_1 x_1 + b_0$.

Then $r(x) - \frac{r_{n'}}{b_n} x^{n'-n} b(x)$ does not have the $x^{n'}$ term and hence has a degree at most $n' - 1$. Meanwhile, as $r(x) \in S$, then there is a $q(x)$ such that $a(x) = q(x)b(x) + r(x)$. Then $a(x) = (q(x) + \frac{r_{n'}}{b_n} x^{n'-n})b(x) + r(x) - \frac{r_{n'}}{b_n} x^{n'-n} b(x)$, which implies $r(x) - \frac{r_{n'}}{b_n} x^{n'-n} b(x) \in S$. This contradicts the minimality of $n'$ in $D$. We conclude that $n' < n$.

Uniqueness: If there are two polynomials $r_1(x)$ and $r_2(x)$ then we could write $a(x) = q_1(x)b(x) + r_1(x)$ and $a(x) = q_2(x)b(x) + r_2(x)$. Then $(q_1(x) - q_2(x))b(x) = r_2(x) - r_1(x)$. Because the RHS polynomial has a degree smaller than $b(x)$, for this equation to hold the LHS polynomial must have a degree smaller than $b(x)$ as well. Otherwise for some sufficiently large $x$ the LHS will be strictly larger. The only way this happens is when $q_1(x) - q_2(x) = 0$, and otherwise LHS has a degree at least that of $b(x)$. Then we conclude $r_1(x) = r_2(x)$.

**Part (b)**

Existence: Let

$$f(x) = \frac{y_1(x - x_2)(x - x_3) \cdots (x - x_k)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_k)} + \cdots + \frac{(x - x_1)(x - x_2) \cdots (x - x_{k-1})y_k}{(x_k - x_1)(x_k - x_2) \cdots (x_k - x_{k-1})}.$$

The degree of $f(x)$ is at most $k - 1$ by its explicit formula. Plugging $x_i$ into $f(x)$, there is only one term that is nonzero, which is $y_i$.

Uniqueness: Suppose that both $f_1(x)$ and $f_2(x)$ satisfy $f(x_i) = y_i$ for all $i$. As $f(x_i) = y_i$ is satisfied for both $f_1(x)$ and $f_2(x)$, by the lemma we have $f_1(x) - f_2(x) \equiv 0 \bmod (x - x_i)$ for every $i$. We thus write $f_1(x) - f_2(x) = q(x)(x - x_1)$. Because $q(x_2)(x_2 - x_1) = 0$ we have $q(x_2) = 0$. Then by the lemma again $q(x) \equiv 0 \bmod (x - x_2)$, and therefore $f_1(x) - f_2(x) = q'(x)(x - x_2)(x - x_1)$ for some $q'(x)$. Repeat this process and use the lemma for $k - 2$ more times. We have $f_1(x) - f_2(x) \equiv 0 \bmod (x - x_1) \cdots (x - x_k)$, which by part (a) guarantees that at most one of $f_1(x)$ and $f_2(x)$ could be of degree at most $k - 1$.

5. (16 points) Let $n$ be a nonnegative integer and $s(n)$ be the number of sequences $(x_1, x_2, \ldots, x_k)$ of integers satisfying $1 \leq x_i \leq n$ for $i = 1, 2, \ldots, k$ and $x_{i+1} \geq 2x_i$ for $i = 1, 2, \ldots, k - 1$. The length of the sequence is not specified; in particular, the empty sequence is included. For example, $s(0) = 1$ since only the empty sequence occurs and $s(4) = 10$ since the set of all possible sequences in this case is $\{\text{the empty sequence}, (1), (2), (3), (4), (1, 2), (1, 3), (1, 4), (2, 4), (1, 2, 4)\}$.

   (a) (8 points) Fine a recurrence relation for $s(n), n \geq 1$.

   (b) (8 points) Show that the generating function $S(t) = s(0) + s(1)t + s(2)t^2 + \ldots$ of the sequence $s(n)$ satisfies

   $$(1 - t)S(t) = (1 + t)S(t^2).$$

**Solution:**

**Part (a)** Let us divide the sequences counted by $s(n)$ into two classes: those not containing $n$ and those containing $n$. There are $s(n-1)$ sequences in the first class. For every sequence in the second class, all terms other than $n$ are at most $n/2$ so every sequence in the second class is obtained from a sequence of integers with $1 \le x_i \le \lfloor n/2 \rfloor$ and $x_{i+1} \ge 2x_i$ by adjoining $n$. It follows that there are $s(\lfloor n/2 \rfloor)$ sequences in the second class. Thus, we obtain the recurrence:

$$s(n) = s(n-1) + s(\lfloor n/2 \rfloor)\,, \quad n \ge 1\,.$$

**Part (b)** We have the following one-to-one correspondences between sequences and their respective generating functions:

$$\begin{array}{ccccccccc}
( & s(0), & s(1), & s(2), & s(3), & \dots & ) & \leftrightarrow & S(t)\,, \\
( & 0, & s(0), & s(1), & s(2), & \dots & ) & \leftrightarrow & tS(t)\,, \\
( & s(0), & 0, & s(1), & 0, & \dots & ) & \leftrightarrow & S(t^2)\,, \\
( & 0, & s(0), & 0, & s(1), & \dots & ) & \leftrightarrow & tS(t^2)\,.
\end{array}$$

Therefore, the coefficient of $t^n, n \ge 1$ in $tS(t)$ is $s(n-1)$ and that in $(1+t)S(t^2)$ is $s(\lfloor n/2 \rfloor)$. Moreover, the constant term of $tS(t) + (1+t)S(t^2)$ is $s(0)$. Thus, by Part (a), we have $S(t) = tS(t) + (1+t)S(t^2)$, i.e., $(1-t)S(t) = (1+t)S(t^2)$.

6. (8 points) For $x \in \mathbb{R}$, denote $\lfloor x \rceil$ as the nearest integer rounding of $x$. That is, if $x - \lfloor x \rfloor \ge 0.5$, then $\lfloor x \rceil = \lfloor x \rfloor + 1$, and if $x - \lfloor x \rfloor < 0.5$ then $\lfloor x \rceil = \lfloor x \rfloor$.

   Show that for $n \in \mathbb{Z}^+$, $\lfloor \sqrt{2n+1} \rceil$ is the largest positive integer $p$ such that

$$1 + 2 + \cdots + (p-1) \le n\,.$$

**Solution:**

As $1+2+\cdots+(p-1) = (p-1)p/2$, we obtain that if and only if $p \le \frac{1}{2} + \sqrt{\frac{1}{4} + 2n}$, $1 + 2 + \cdots + (p-1) \le n$. The largest such $p$ will therefore be $\lfloor \frac{1}{2} + \sqrt{\frac{1}{4} + 2n} \rfloor$, which is by definition equivalent to $\lfloor \sqrt{2n + \frac{1}{4}} \rceil$.

It amounts to showing $\lfloor \sqrt{2n + \frac{1}{4}} \rceil = \lfloor \sqrt{2n+1} \rceil$. Because $\sqrt{2n+1} - \sqrt{2n + \frac{1}{4}} < \frac{1}{2}$, the only way $\lfloor \sqrt{2n + \frac{1}{4}} \rceil$ is smaller than $\lfloor \sqrt{2n+1} \rceil$ is when the latter ends with a (proper) fraction at least 0.5 while the former ends with a fraction smaller than 0.5, with the same integer part. When $8n+1$ is a perfect square, $\sqrt{2n + \frac{1}{4}}$ ends with 0.5, and this must not be the case. When $8n+1$ is not a perfect square, then for some $k$, $8(n+k)+1$ must be the next odd perfect square, because all odd perfect squares are in the form of $8m+1$. As $2n+1$ is smaller than $2(n+k)+\frac{1}{4}$ for any $k$, its fractional part must not exceed 0.5, as we desired.