CSC3001: Discrete Mathematics

Assignment 1

Instructions:

1. Print out this question paper (**two-sided**) and write down your full working on the blank area.
2. You can have discussions with your classmates. However, make sure all the solutions you submit are your own work. Any plagirism will be given **ZERO** mark.
3. Submission of this assignment should **NOT** be later than **5pm on 11th of October**.
4. Before your submission, please **make a softcopy** of your work for further discussion in a tutorial.
5. After making your softcopy, submit your assignment to the dropbox located on the 4th floor in Chengdao Building.

Student Number: ____________________ **Name:** _______________

1. (*20 points*) Given statements p, q, r, s, which of the following arguments are valid? (**Note:** you need to give the reason in order to obtain full mark.)

$$\text{(i)}\quad \begin{array}{ll} & (p \vee q) \to \neg r \\ & p \to \neg q \\ & \neg q \to p \\ \hline \therefore & \neg r \end{array} \qquad \text{(ii)}\quad \begin{array}{ll} & p \to q \\ & q \to \neg p \\ \hline \therefore & p \leftrightarrow q \end{array} \qquad \text{(iii)}\quad \begin{array}{ll} & (q \wedge r) \to p \\ & (p \vee q) \to r \\ \hline \therefore & s \leftrightarrow s \end{array}$$

Solution.

(i) Let the conclusion be false and all assumptions be true. From the first assumption we have

$$p \vee q = F \qquad \Rightarrow \qquad p = q = F.$$

This shows that for the third assumption we have

$$T \to F$$

which is false.
Therefore, it is impossible that the conclusion is false when all assumptions are true. Hence, the argument is valid.

(ii) Consider the following truth table:

p	q	$p \to q$	$q \to \neg p$	$p \leftrightarrow q$
T	T	T	F	T
T	F	F	T	F
F	T	T	T	F
F	F	T	T	T

So the argument is invalid.
(**Warning:** the argument $((p \to q) \wedge (q \to \neg p)) \to (p \to \neg p)$ is NOT valid, as "$\neg p$" is DEPENDENT of "p"!!! Compared with Transitivity Argument.)

(iii) Note that the conclusion is a tautology, so the argument is valid.

2. (*20 points*) Let $a \in \mathbb{Z}, b \in \mathbb{Z}^+$. Use Well Ordering Principle to prove that there exist $q, r \in \mathbb{Z}$ such that

$$a = qb + r \qquad \text{and} \qquad 0 \le r < b$$

Solution. Let

$$S = \{a - xb \in \mathbb{N} | x \in \mathbb{Z}\}$$

Then $S \subseteq \mathbb{N}$.
In particular, if $x = -|a|$, we have

$$a - xb = a + |a|b = |a|(b \pm 1) \ge 0 \qquad \Rightarrow \qquad a + |a|b \in S$$

So $S \neq \emptyset$.
By Well Ordering Principle, S contains a least element $r \geq 0$ and $r = a - qb$ for some $q \in \mathbb{Z}$. To see $r < b$, we assume the opposite, i.e., $r \geq b$. Then

$$r - b = a - qb - b = a - (q+1)b \geq 0 \qquad \Rightarrow \qquad r - b \text{ is a smaller element in } S$$

This is a contradiction. So $r < b$.

3. (*20 points*)

(a) Translate the following statement into logical formula without predicates.

> For each $a, b \in \mathbb{Z}^+$ with $a \leq b$, we have
> $$\frac{a}{b} = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_m}$$
> for some mutually distinct $d_1, \ldots, d_m \in \mathbb{Z}^+$.

(b) Use mathematical induction to prove the statement in (a).
(Full mark will be given **ONLY** if you use mathematical induction.)

Solution.

(a) $\forall a, b \in \mathbb{Z}^+, \exists m, d_1, \ldots, d_m \in \mathbb{Z}^+, \forall i, j \in \{1, \ldots, m\}$,
$(a > b) \vee \left(((d_i \neq d_j) \vee (i = j)) \wedge \left(\frac{a}{b} = \sum_{k=1}^{m} \frac{1}{d_k} \right) \right)$

(b) For $n \in \mathbb{Z}^+$, set

$$P(n) := \text{“The statement holds whenever } a \text{ or } b \leq n.\text{”}$$

When $n = 1$, we have $a = 1$ or $b = 1$. If $a = 1$, then $\frac{a}{b} = \frac{1}{b}$; if $b = 1$, then $a = 1$. Hence, $P(1)$ holds.
Assume $P(k)$ holds for some $k \geq 1$. For $n = k + 1$, it suffices to consider the case that $a = k + 1$, and so

$$\frac{a}{b} = \frac{k+1}{b} = \frac{k}{b} + \frac{1}{b}$$

By $P(k)$ we know that $k/b = \sum_{i=1}^{m} \frac{1}{d_i}$ for some mutually distinct d_i. If $d_i \neq b$ for all i, then we are done. Otherwise we note that the formula

$$\frac{1}{d} = \frac{1}{d+1} + \frac{1}{d(d+1)} \tag{1}$$

will replace the given denominator d by some greater denominators. W.l.o.g, assume $d_m = \max\{d_i | i = 1, \ldots, m\}$. Then we may repeatedly apply formula (1) on $1/b$ until all the replacing denominators become greater than d_m, and thus $a/b = \sum \frac{1}{d_j}$ for some mutually distinct d_j. This procedure will stop in finitely many steps as d_m is finite. Hence, $P(k+1)$ also holds.
Therefore, $P(n)$ holds for all $n \in \mathbb{Z}^+$.

4. (*20 points*) Prove that

$$A = \{5a \mid a \in \mathbb{Z}\}, \qquad B = \left\{5\left\lfloor \frac{4b}{3} \right\rfloor - 2 \,\middle|\, b \in \mathbb{Z}\right\}, \qquad C = \{20c - 7 \mid c \in \mathbb{Z}\}$$

form a partition for the set $X = \left\{\left\lfloor \frac{5x+1}{2} \right\rfloor \,\middle|\, x \in \mathbb{Z}\right\}$.

Proof. From

$$5a = 5\left\lfloor \frac{4b}{3} \right\rfloor - 2 \quad \Rightarrow \quad 5\left(\left\lfloor \frac{4b}{3} \right\rfloor - a\right) = 2$$

we see that there do not exist $a, b \in \mathbb{Z}$ such that the above equation holds, so $A \cap B = \emptyset$.
From

$$5a = 20c - 7 \quad \Rightarrow \quad 5(4c - a) = 7$$

we also see that $A \cap C = \emptyset$.
For set B, we have

- If $b = 3k$, then $5\left\lfloor \frac{4b}{3} \right\rfloor - 2 = 20k - 2 \neq 20c - 7$;
- If $b = 3k+1$, then $5\left\lfloor \frac{4b}{3} \right\rfloor - 2 = 5(4k+1) - 2 = 20k + 3 \neq 20c - 7$;
- If $b = 3k+2$, then $5\left\lfloor \frac{4b}{3} \right\rfloor - 2 = 5(4k+2) - 2 = 20k + 8 \neq 20c - 7$.

So $B \cap C = \emptyset$.
For set X, we have

- If $x = 2t$, then $\left\lfloor \frac{5x+1}{2} \right\rfloor = 5t \in A$;
- If $x = 2t+1$, then $\left\lfloor \frac{5x+1}{2} \right\rfloor = 5t + 3$. And we have
  - If $t = 4u$, then $5t + 3 = 20t + 3 \in B$;
  - If $t = 4u+1$, then $5t + 3 = 20t + 8 \in B$;
  - If $t = 4u+2$, then $5t + 3 = 20t + 13 = 20(t+1) - 7 \in C$;
  - If $t = 4u+3$, then $5t + 3 = 20t + 18 = 20(t+1) - 2 \in B$.

Hence, $X \subseteq A \cup B \cup C$.
On the other hand, for each $5a \in A$ we have $x = 2a$ such that

$$5a = \left\lfloor \frac{5x+1}{2} \right\rfloor \in X$$

For each $5\left\lfloor \frac{4b}{3} \right\rfloor - 2 \in B$ we have $x = 2\left\lfloor \frac{4b}{3} \right\rfloor - 1$ such that

$$5\left\lfloor \frac{4b}{3} \right\rfloor - 2 = \left\lfloor \frac{5x+1}{2} \right\rfloor \in X$$

For each $20c - 7 \in C$ we have $x = 2c - 3$ such that

$$20c - 7 = \left\lfloor \frac{5x+1}{2} \right\rfloor \in X$$

Therefore, $A \cup B \cup C \subseteq X$ and $\{A, B, C\}$ is a partition of X. $\square$

5. (*20 points*) Let $\alpha, \beta \in \mathbb{R}$ be such that none of them is a root of a nonzero polynomial with integer coefficients (that is, $c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$, where $c_i \in \mathbb{Z}$). Show that there are at least two irrational numbers contained in the following set

$$S = \{\alpha + \beta, \alpha - \beta, \alpha\beta\}$$

Solution. First note that both α, β are irrational, otherwise $\alpha = \dfrac{n}{m}$ for some $m, n \in \mathbb{Z}$, and it is the root of

$$x - \frac{n}{m} = 0 \qquad \Rightarrow \qquad mx - n = 0$$

which is a contradiction.
Consider that

$$(\alpha + \beta) + (\alpha - \beta) = 2\alpha$$

is irrational, so either $\alpha + \beta$ or $\alpha - \beta$ is irrational.
Suppose that $\alpha + \beta = \dfrac{n}{m}, \alpha\beta = \dfrac{p}{q}$ for some $m, n, p, q \in \mathbb{Z}$. Consider that α, β are roots of the polynomial

$$x^2 - (\alpha + \beta)x + \alpha\beta$$

so α, β are also roots of

$$x^2 - \frac{n}{m}x + \frac{p}{q} = 0 \qquad \Rightarrow \qquad mqx^2 - nqx + pm = 0$$

which is a contradiction. So either $\alpha + \beta$ or $\alpha\beta$ is irrtational.
Similarly, either $\alpha - \beta$ or $\alpha\beta$ is irrational, as $\alpha, -\beta$ are roots of the polynomial

$$x^2 - (\alpha - \beta)x - \alpha\beta$$

There are two cases for the set S:

① If $\alpha + \beta$ is irrational. Since either $\alpha - \beta$ or $\alpha\beta$ is irrational, so there are at least two irrational numbers in S.

② If $\alpha + \beta$ is rational. Then $\alpha - \beta$ must be irrational as one of them must be. Similarly, $\alpha\beta$ must be irrational. So there are at least two irrational numbers in S.

6. (*10 points*) [**bonus question**] A kid is playing a game on a 4×4 table whose entries are filled with mutually distinct numbers. He needs to make a reshuffle on these numbers so that the numbers on the same line (only consider horizontal, vertical, and two diagonal directions) also appear on the same line after the reshuffle. After trying a few times he conjectures that the ordering of the numbers are always preserved, that is, if b is a number between a, c on a line, then b is also a number between a, c on the new line after the reshuffle. Is this conjecture true? And is this conjecture true for any $n \times n$ table?

Initial configuration

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

A fesible reshuffle

4	3	2	1
8	7	6	5
12	11	10	9
16	15	14	13

Proof. Given an $n \times n$ table, label the entries as the figure below (here we require that the lines EH, GJ, IL, FK contain equal number of entries, and the lines FG, HI, JK, EL contain equal number of entries). Obviously, the corner entries and the diagonal entries are the only entries lying in at least 3 lines with n entries.

A	$\cdots$	E	$\cdots$	F	$\cdots$	B
$\vdots$	$\ddots$		$\ddots$		$\ddots$	$\vdots$
L		$\ddots$		$\ddots$		G
$\vdots$	$\ddots$		$\ddots$		$\ddots$	$\vdots$
K		$\ddots$		$\ddots$		H
$\vdots$	$\ddots$		$\ddots$		$\ddots$	$\vdots$
D	$\cdots$	J	$\cdots$	I	$\cdots$	C

Fact. Rewinding any reshuffle is also a reshuffle. Note that each reshuffle is a bijection of entries sending the straight lines to straight lines. Thus, each reshuffle is also a bijection of straight lines from one configuration to the other. It follows that the rewind of each reshuffle also sends straight lines to stragiht lines, and so it is a reshuffle.

Claim 1. A reshuffle must send a diagonal to a digaonal, and send four sides to four sides. We first see that none of the four sides (AB, BC, CD, AD) can be reshuffled to a diagonal line (AC or BD). Otherwise, say assume AB is reshuffled to AC. Then the entries between A and B would have to be reshuffled to the diagonal entries, which is impossible. Hence, the four sides can only be reshuffled to a horizontal or a vertical. Moreover, since rewinding a reshuffle is also a reshuffle, a diagonal line must be reshuffled to a diagonal line.

Now suppose that AB is reshuffled to a line ℓ which is none of the four sides. Pick consecutive entries X, Y, Z from ℓ. Then there exist entries $P, Q \notin \ell$ such that

$$XP \cap ZP = P, \quad XQ \cap ZQ = Q$$

Again, since rewinding a reshuffle is also a reshuffle, when AB is rewinded to a side, the lines XP, ZP, XQ, ZQ should be rewinded to four distinct lines, which is impossible. This shows that each reshuffle must send four sides to four sides.

Claim 2. The corner entries must be sent to the corner entries. Since the diagonals only meet the four sides at the corner entries.

Claim 3. The lines parallel to a diagonal should be reshuffled to the lines parallel to the reshuffled diagonal. Note that any horizontal or vertical would intersect the diagonals, so the lines parallel to a diagonal cannot be reshuffled to a horizontal or a vertical.

Suppose it happens that these parallel lines are reshuffled to the lines not parallel to the reshuffled diagonal. W.l.o.g, let us say A, C are fixed under the reshuffle. Further, we may also assume B, D are fixed under the reshuffle. Suppose EH is one of such a parallel line. Then E, H are reshuffled to F, K respectively. Consequently, L is reshuffled to G. However, note that L is an entry on AD while G is not, this is impossible.

Conclusion. If a reshuffle fixes all corner entries, then it fixes all entries. Based on the above discussion, when we fix A, B, C, D, the entries on four sides must be all fixed, and so all horizontals and verticals are fixed. Since each entry can be viewed as the intersection of a horizontal and a vertical, it follows that all entries are fixed in this case, and hence the ordering is preserved in any line. $\square$