Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60005: Foundations of Computing Science **Autumn 2023**

Class Test 1 **4th of September 2023, 6:15 PM – 7:15 PM** **Marks = 20**

Answer all questions. State all assumptions you make. Keep your answers concise.

---

1. (a) For each of the following arguments, if the argument is valid, then prove it; otherwise, give a counter-example to show that the argument is invalid.

i.

$$\begin{array}{l} \neg(\neg p \lor q) \\ \neg t \rightarrow \neg s \\ (p \land \neg q) \rightarrow \neg s \\ \neg t \lor r \\ \hline \therefore r \end{array}$$

Solution: The argument is invalid. Consider the assignment $p = \top$, $q = \bot$, $s = \bot$, $t = \bot$, $r = \bot$ (here $\bot$ denotes false). Then $\neg(\neg p \lor q) = p \land \neg q = \top$, $(p \land \neg q) \rightarrow \neg s$ holds and as a consequence $\neg t \rightarrow \neg s$ is true. But this implies the last statement is true irrespective of the value r ttakes. The assignment satisfies the four given premises but not the conclusion.

ii.

$$\begin{array}{l} \neg r \rightarrow p \\ q \rightarrow \neg p \\ \neg(r \lor t) \\ \hline \therefore q \lor t \end{array}$$

Solution: The argument is invalid. Consider the assignment $r = \bot, t = \bot, p = \top$, $q = \bot$. This assignment satisfies the three given premises but not the conclusion.

(b) Assume that the following predicates/formulas are defined (over the set of natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$):

- $\mathsf{Div}(x, y)$: true if x divides y and false otherwise
- $x < y$: true iff x is strictly less than y
- $\mathsf{Prime}(p)$: true iff p is a prime number

Write down formulas in predicate logic for the following.

i. $\mathsf{Pow}_p(x)$: true iff x is a power of the prime p.
Solution:

$$\forall y\, ((\mathsf{Div}(y, x) \land \mathsf{Prime}(y)) \rightarrow (y = p))$$

ii. $\mathsf{Digit}(v, y, b)$: true iff p-ary digit of v at position y is b.
Here, position is specified by y which is a power of p. For example, the binary digit of 1000110010111 at position 2^2, 2^4 and 2^5 are respectively 1 (third bit from right), 1 (fifth bit from right) and 0 (sixth bit from right).
Solution:

$$\exists a \exists r\, ((v = apy + by + r) \land (r < y) \land (b < p))$$

(1+1)+(1+2)= 5

2. Let S be any countable subset of $\mathbb{R}$. Show that $\mathbb{R} \sim \mathbb{R} \setminus S$. 5

Solution: Since S is countable, the elements of S can be numbered $s_0, s_1, s_2, \ldots$. Let $r_0, r_1, r_2, \ldots$ be distinct elements of $\mathbb{R}$. Such elements exist for otherwise $\mathbb{R}$ would be countable. Now define a map $f : \mathbb{R} \to \mathbb{R} \setminus S$ as follows: for all $i \in \mathbb{N}$, $f(s_i) = r_{2i}$ and $f(r_i) = r_{2i+1}$; for all $x \in \mathbb{R} \setminus \{r_0, r_1, r_2, \ldots\}$, $f(x) = x$. Clearly f is a bijection. For all $i \in \mathbb{N}$, $f^{-1}(r_i) = r_{(i-1)/2}$ if i is odd and $f^{-1}(r_i) = s_{i/2}$ if i is even; for all $x \in \mathbb{R} \setminus \{r_0, r_1, r_2, \ldots\}$, $f^{-1}(x) = x$. Therefore $\mathbb{R} \sim \mathbb{R} \setminus S$.

3. Let $(G, \circ)$ be a group. Define a relation $\mathcal{R}$ on G as follows: For all $(x, y) \in G \times G$, $(x, y) \in \mathcal{R}$ if and only if $\exists a \in G$ such that $a \circ x = y \circ a$. Prove that $\mathcal{R}$ is an equivalence relation. 5

Solution: We show that $\mathcal{R}$ is reflexive, symmetric and transitive.

Let e be the identity of $(G, \circ)$. For every $x \in G$, $e \circ x = x \circ e$ and hence $(x, x) \in \mathcal{R}$. $\mathcal{R}$ is reflexive.

Let $x, y \in G$ such that $(x, y)\mathcal{R}$. There exists $a \in G$ such that $a \circ x = y \circ a$. Let a^{-1} be the inverse of a. We have

$$a \circ x = y \circ a$$
$$a \circ x \circ a^{-1} = y \qquad \text{‘multiplying’ both sides on the right by } a^{-1}$$
$$x \circ a^{-1} = a^{-1} \circ y \qquad \text{‘multiplying’ both sides on the left by } a^{-1}$$

that is, $a^{-1} \circ y = x \circ a^{-1}$ and hence $(y, x) \in \mathcal{R}$. Hence $\mathcal{R}$ is symmetric.

Now, suppose that $(x, y), (y, z) \in \mathcal{R}$. There exist a, b such that

$$a \circ x = y \circ a \tag{1}$$

and

$$b \circ y = z \circ b. \tag{2}$$

‘multiplying’ both sides of Equation 1 on the left by b, we have

$$b \circ a \circ x = b \circ y \circ a.$$

Using Equation 2, substitute for $b \circ y$ with $z \circ b$. We get

$$b \circ a \circ x = z \circ b \circ a,$$

and therefore $(x, z) \in \mathcal{R}$ implying that $\mathcal{R}$ is transitive.

4. Let $S = \mathbb{R} \setminus \{0\} \times \mathbb{R}$. Define the operation $\circ$ as follows: $(u, v) \circ (x, y) = (ux, vx + y)$.

   (a) Is $(S, \circ)$ a group? If so, is it Abelian?

   Solution: Let $(u, v), (x, y), (w, z) \in S$. Then u, x are non-zero reals and so is their product. Also, $vx + y \in \mathbb{R}$ and so S is closed under $\circ$. We have

$$\begin{aligned}((u, v) \circ (x, y)) \circ (w, z) &= (ux, vx + y) \circ (w, z)\\ &= (uxw, wvx + wy + z)\\ &= (u(xy), v(xw) + (yw + z))\\ &= (u, v) \circ (xw, yw + z)\\ &= (u, v) \circ ((x, y) \circ (w, z))\end{aligned}$$

   and hence $(S, \circ)$ is associative. For any $(x, y) \in S$, $(x, y) \circ (1, 0) = (x, y) = (1, 0) \circ (x, y)$ and so $(1, 0)$ is the identity. For any $(x, y) \in S$, $(\frac{1}{x}, -\frac{y}{x}) \in S$ since $x \neq 0$. Also, $(x, y) \circ (\frac{1}{x}, -\frac{y}{x}) = (1, 0)$ and $(\frac{1}{x}, -\frac{y}{x}) \circ (x, y) = (1, 0)$ and therefore $(\frac{1}{x}, -\frac{y}{x})$ is the inverse of (x, y). We have shown that $(S, \circ)$ is a group.

   Consider $(1, 2), (2, -3) \in S$. We have $(1, 2) \circ (2, -3) = (2, 1)$ and $(2, -3) \circ (1, 2) = (2, -1)$ and $(2, 1) \neq (2, -1)$. $(S, \circ)$ is not Abelian.

   (b) Define $\hat{S} = \mathbb{Q} \setminus \{0\} \times \mathbb{Q}$. Is $(\hat{S}, \circ)$ a group?

Solution: $\mathbb{Q}$ is closed under addition and multiplication. Multiplication is associative. Also, every non-zero element has a multiplicative inverse. From these it follows that, all group properties hold for $(\hat{S}, \circ)$ as well. Identity and inverse are identical to the those for $(S, \circ)$.

$\boxed{4+1 = 5}$