Mathematical and Logical Foundations of Computer Science

Solutions

Main Summer Examinations 2022

Mathematical and Logical Foundations of Computer Science

Question 1

(a) **Numbers and sets**

(i) Compute 4^2 and 4^3 modulo 3. From these results, conjecture a property $P(n)$ of 4^n modulo 3. Prove by induction that $P(n)$ is satisfied for all $n \in \mathbb{N}$. **[3 marks]**

(ii) Let $sqrt : \{x \in \mathbb{N} \mid x \geq 0\} \to \{y \in \mathbb{R} \mid y \geq 0\}$ be the square root function from non-negative integers to non-negative reals, i.e. $sqrt(x) = y$ if and only if $x = y^2$.

Is $sqrt$ injective? surjective? bijective? Justify your answers. **[3 marks]**

(iii) Let `float javaSqrt(int x)` be a Java implementation of this square root function (assume it throws an exception if `x` is negative). Discuss the differences between $sqrt$ and `javaSqrt` when considered as mathematical functions between sets. **[4 marks]**

(b) **Linear algebra**

Consider the three points

$$P_1 = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} \qquad P_2 = \begin{pmatrix} -1 \\ 0 \\ 4 \end{pmatrix} \qquad P_3 = \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix}$$

(i) Show that these form the corners of an equilateral triangle (i.e. a triangle where all sides have the same length). **[2 marks]**

(ii) The triangle defines a plane M in $\mathbb{R}^3$. Give its parametric representation and its normal form. **[4 marks]**

(iii) Another plane N is given by

$$\begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} + q \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + r \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$$

Find the line of intersection of M and N. **[4 marks]**

Show your working for each part.

Model answer / LOs / Creativity:

(a) (i) $4^2 = 16 = 3 \cdot 5 + 1 \equiv 1 \bmod 3$ and $4^3 = 64 = 3 \cdot 21 + 1 \equiv 1 \bmod 3$.

We conjecture that $4^n \equiv 1 \bmod 3$ for all $n \in \mathbb{N}$. We will prove it by induction on n.

Base case: $4^0 = 1 \equiv 1 \bmod 3$.

Inductive step: Suppose for a given $n \in \mathbb{N}$ that $4^n \equiv 1 \bmod 3$. Then, $4^{n+1} = 4 \cdot 4^n \equiv 4 \cdot 1 \bmod 3 \equiv 4 \bmod 3$. Hence, $4^{n+1} \equiv 1 \bmod 3$.

Thus, we have by induction on n that, for all $n \in \mathbb{N}$, $4^n \equiv 1 \bmod 3$.

(ii) **Injective?** Take $x, x' \in \mathbb{N}$, $x, x' \geq 0$ and $y, y' \in \mathbb{R}$, $y, y' \geq 0$ such that $y = sqrt(x)$ and $y' = sqrt(x')$, meaning that $x = y^2$ and $x' = y'^2$.

Suppose that $y = y'$, this implies that $y^2 = y'^2$, and hence $x = x'$. Therefore, yes, $sqrt$ is injective.

Surjective? Take $y \in \mathbb{R}$,$y \geq 0$. Is there necessarily an $x \in \mathbb{N}$, $x \geq 0$ such that $y = sqrt(x)$, i.e., $y^2 = x$? No, take for example $y = \frac{1}{2}$, then $y^2 = \frac{1}{4} \notin \mathbb{N}$. Therefore, no, $sqrt$ is not surjective.

Bijective? No, $sqrt$ is not bijective since it is not surjective.

(iii) The two functions have different domains and co-domains: `javaSqrt` is defined only for numbers less than or equal to `Integer.MAX_VALUE` and its output is a floating point number. The set of all floating point numbers is a finite subset of $\mathbb{Q}$. Thus, while the range of $sqrt$ includes irrational numbers such as $\sqrt{2}$, the range of `javaSqrt` is limited to rationals.

Because of rounding, the property $(\texttt{javaSqrt(x)})^2 = x$ does not generally hold exactly (though it is true approximately).

(b) (i) distance $P_1P_2 = \sqrt{(-1-1)^2 + (0-2)^2 + (4-4)^2} = 2\sqrt{2}$

distance $P_1P_3 = \sqrt{(-1-1)^2 + (2-2)^2 + (2-4)^2} = 2\sqrt{2}$

distance $P_2P_3 = \sqrt{(-1+1)^2 + (2-0)^2 + (2-4)^2} = 2\sqrt{2}$

Hence, $P_1P_2 = P_1P_3 = P_2P_3$ meaning that the triangle $P_1P_2P_3$ is equilateral.

(ii) $\overrightarrow{P_1P_2} = \begin{pmatrix} -1-1 \\ 0-2 \\ 4-4 \end{pmatrix} = \begin{pmatrix} -2 \\ -2 \\ 0 \end{pmatrix}$ and $\overrightarrow{P_1P_3} = \begin{pmatrix} -1-1 \\ 2-2 \\ 2-4 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ -2 \end{pmatrix}$.

A parametric representation of M is given as $P_1 + s \cdot \overrightarrow{P_1P_2} + t \cdot \overrightarrow{P_1P_3}$. Therefore,

$$M = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} + s \cdot \begin{pmatrix} -2 \\ -2 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} -2 \\ 0 \\ -2 \end{pmatrix}$$

An equational representation of M is given by $ax + by + cz = d$ with the values of a, b, c computed from $\overrightarrow{P_1P_2}$ and $\overrightarrow{P_1P_3}$, and d from a, b, c and P_1:

$$\begin{aligned} a &= (-2) \cdot (-2) - 0 \cdot (-2) = 4 \\ b &= 0 \cdot (-2) - (-2) \cdot (-2) = -4 \\ c &= (-2) \cdot 0 - (-2) \cdot (-2) = -4 \\ d &= 4 \cdot 1 + (-4) \cdot 2 + (-4) \cdot 4 = -20 \end{aligned}$$

That is, M is described as $x - y - z = -5$.

(iii) The intersection between M and N is given by the system:

$$\begin{cases} 1 + q + 2r = 1 - 2s - 2t \\ q = 2 - 2s \\ 3 + q + r = 4 - 2t \end{cases}$$

Which we can rewrite as:

$$\begin{cases} q + 2r + 2s + 2t = 0 \\ q + 2s = 2 \\ q + r + 2t = 1 \end{cases}$$

To which we apply the Gaussian elimination algortihm:

$$\left(\begin{array}{cccc|c} 1 & 2 & 2 & 2 & 0 \\ 1 & 0 & 2 & 0 & 2 \\ 1 & 1 & 0 & 2 & 1 \end{array}\right) \xrightarrow{(3)-(1),\ (2)-(1)} \left(\begin{array}{cccc|c} 1 & 2 & 2 & 2 & 0 \\ 0 & -2 & 0 & -2 & 2 \\ 0 & -1 & -2 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{2(3)-(2)} \left(\begin{array}{cccc|c} 1 & 2 & 2 & 2 & 0 \\ 0 & -2 & 0 & -2 & 2 \\ 0 & 0 & -4 & 2 & 0 \end{array}\right)$$

The final equation is equivalent to $t = 2s$, which can be plugged into the parametric representation of M. The parametric representation of the intersection line between M and N is therefore given by:

$$L = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} + s \cdot \begin{pmatrix} -2 \\ -2 \\ 0 \end{pmatrix} + (2s) \cdot \begin{pmatrix} -2 \\ 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} + s \cdot \begin{pmatrix} -6 \\ -2 \\ -4 \end{pmatrix}$$

or, simplified:

$$L = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} + s \cdot \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$$

The same result can alternatively be found by plugging the parametric representation of N into the normal form equation of M.

Learning outcomes:

- " Solve mathematical problems in algebra and set theory" (a&b);
- "Apply mathematical techniques to solve a problem within a computer science setting" (a(iii)).

Creativity will be required in a(i) and a(iii).

Question 2

(a) **Propositional Logic**

Let F be the formula $(A \vee B) \rightarrow (B \vee A)$, and
let G be the formula $A \rightarrow (B \rightarrow (\neg B \vee \neg A)) \rightarrow \neg B$.

(i) Provide a constructive Sequent Calculus proof of F. **[4 marks]**

(ii) Provide a constructive Natural Deduction proof of G. **[6 marks]**

(iii) Is G satisfiable? Justify your answer. **[2 marks]**

(b) **Predicate Logic**

Consider the following signature:

- Function symbols: `zero` (arity 0); `succ` (arity 1)
- Predicate symbols: $<$ (arity 2); $\leq$ (arity 2)

We will use infix notation for the binary symbols $<$ and $\leq$. Consider the following formula that captures a property of the above symbols:

- let S_1 be $\forall x.\neg(x < 0)$

For simplicity we write 0 for `zero`, 1 for `succ(zero)`, 2 for `succ(succ(zero))`, etc.

(i) Provide a constructive Natural Deduction proof of:

$$S_1 \rightarrow \neg \exists x.\forall y.x < y$$

[4 marks]

(ii) Provide a model M_1 such that $\vDash_{M_1} \neg(\forall x.\forall y.x < y \rightarrow x \leq y)$, and a model M_2 such that $\vDash_{M_2} \forall x.\forall y.x \leq y \rightarrow x < y$ **[4 marks]**

Model answer / LOs / Creativity:

(a) (i) Here is a constructive Sequent Calculus proof of F:

$$\begin{prooftree}
\AxiomC{}
\RightLabel{$[Id]$}
\UnaryInfC{$A \vdash A$}
\RightLabel{$[\vee R_2]$}
\UnaryInfC{$A \vdash B \vee A$}
\AxiomC{}
\RightLabel{$[Id]$}
\UnaryInfC{$B \vdash B$}
\RightLabel{$[\vee R_1]$}
\UnaryInfC{$B \vdash B \vee A$}
\RightLabel{$[\vee L]$}
\BinaryInfC{$A \vee B \vdash B \vee A$}
\RightLabel{$[\rightarrow R]$}
\UnaryInfC{$\vdash (A \vee B) \rightarrow (B \vee A)$}
\end{prooftree}$$

(ii) Here is a constructive Natural Deduction proof of G:

$$\begin{prooftree}
\AxiomC{$\overline{B \rightarrow (\neg B \vee \neg A)}^{\,2}$}
\AxiomC{$\overline{B}^{\,3}$}
\RightLabel{$[\rightarrow E]$}
\BinaryInfC{$\neg B \vee \neg A$}
\AxiomC{$\overline{B}^{\,3}$}
\AxiomC{$\overline{\neg B}^{\,4}$}
\RightLabel{$[\rightarrow E]$}
\BinaryInfC{$\bot$}
\RightLabel{$4\ [\rightarrow I]$}
\UnaryInfC{$\neg B \rightarrow \bot$}
\AxiomC{$\overline{A}^{\,1}$}
\AxiomC{$\overline{\neg A}^{\,5}$}
\RightLabel{$[\rightarrow E]$}
\BinaryInfC{$\bot$}
\RightLabel{$5\ [\rightarrow I]$}
\UnaryInfC{$\neg A \rightarrow \bot$}
\RightLabel{$[\vee E]$}
\TrinaryInfC{$\bot$}
\RightLabel{$3\ [\neg I]$}
\UnaryInfC{$\neg B$}
\RightLabel{$2\ [\rightarrow I]$}
\UnaryInfC{$(B \rightarrow (\neg B \vee \neg A)) \rightarrow \neg B$}
\RightLabel{$1\ [\rightarrow I]$}
\UnaryInfC{$A \rightarrow (B \rightarrow (\neg B \vee \neg A)) \rightarrow \neg B$}
\end{prooftree}$$

(iii) One possible answer is: G is valid by soundness, and therefore satisfiable too. Another possible answer would be to provide any valuation (as all valuations satisfy the formulas) and show using a truth table just for that valuation, that it indeed satisfies the formula.

(b) (i) Here is a proof of $S_1 \rightarrow \neg\exists x.\forall y.x < y$:

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{\scriptsize 2}
\UnaryInfC{$\exists x.\forall y.x < y$}
\AxiomC{}
\RightLabel{\scriptsize 3}
\UnaryInfC{$\forall y.z < y$}
\RightLabel{\scriptsize $[\forall E]$}
\UnaryInfC{$z < 0$}
\AxiomC{}
\RightLabel{\scriptsize 1}
\UnaryInfC{$\forall x.\neg(x < 0)$}
\RightLabel{\scriptsize $[\forall E]$}
\UnaryInfC{$\neg(z < 0)$}
\RightLabel{\scriptsize $[\neg E]$}
\BinaryInfC{$\bot$}
\RightLabel{\scriptsize 3 $[\exists E]$}
\BinaryInfC{$\bot$}
\RightLabel{\scriptsize 2 $[\neg I]$}
\UnaryInfC{$\neg\exists x.\forall y.x < y$}
\RightLabel{\scriptsize 1 $[\rightarrow I]$}
\UnaryInfC{$S_1 \rightarrow \neg\exists x.\forall y.x < y$}
\end{prooftree}
$$

(ii) For example, the models $M_1 = \langle \mathbb{N}, \langle 0, \langle n \rangle \mapsto n+1 \rangle, \langle \{\langle n, m \rangle \mid n \leq m\}, \{\langle n, m \rangle \mid n < m\} \rangle \rangle$ and $M_1' = \langle \{0\}, \langle 0, \langle n \rangle \mapsto n \rangle, \langle \{\langle n, m \rangle \mid \text{True}\}, \emptyset \rangle \rangle$ are models of $\neg(\forall x.\forall y.x < y \rightarrow x \leq y)$; and the models $M_2 = \langle \mathbb{N}, \langle 0, \langle n \rangle \mapsto n+1 \rangle, \langle \{\langle n, m \rangle \mid n \leq m\}, \{\langle n, m \rangle \mid n < m\} \rangle \rangle$ and $M_2' = \langle \{0\}, \langle 0, \langle n \rangle \mapsto n \rangle, \langle \{\langle n, m \rangle \mid \text{True}\}, \emptyset \rangle \rangle$ are models of $\forall x.\forall y.x \leq y \rightarrow x < y$.

Learning outcomes:

- "Understand and apply algorithms for key problems in logic such as satisfiability." (a);
- "Write formal proofs for propositional and predicate logic" (a & b);
- "Apply logical techniques to solve a problem within a computer science setting" (a & b).

Creativity will be required in a & b to come up with proofs and models.