Mathematical and Logical Foundations of Computer Science
First Class Test

Solutions

First Class Test 2021/22

Mathematical and Logical Foundations of Computer Science
First Class Test

Question 1 [Numbers and Set Theory]

(a) (i) Suppose A, B, C are subsets of some set X. Draw a Venn diagram for the expression $(A \setminus B) \cup ((B \cap C) \setminus A)$. **[2 marks]**

(ii) Find an expression for $(A \setminus B) \cup ((B \cap C) \setminus A)$ that uses only union, intersection, and complement. **[2 marks]**

(iii) For the sets $D = \{x \in \mathbb{Z} \mid x^2 \leq 40\}$ and $E = \{x \in \mathbb{Z} \mid \text{there exists } y \in \mathbb{Z} \text{ such that } 3y = x\}$ write down D and $D \cap E$ explicitly. **[4 marks]**

(b) (i) Does $\mathbb{Z}_6$ satisfy the law of the multiplicative inverse? In other words, for each $x \in \mathbb{Z}_6$ does there exist $y \in \mathbb{Z}_6$ such that $xy \equiv 1 \bmod 6$? Justify your answer. **[2 marks]**

(ii) Consider the following piece of pseudocode, where n is a natural number:

```
x <- 0
s <- 0
while (x < n) {
   x <- x + 1
   s <- s + 2*x - 1 }
return s
```

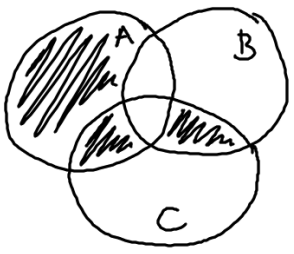
Prove that $s = x^2$ is an invariant of the loop. **[4 marks]**

(c) Java offers functionality for creating arrays of floating point numbers, which have the type `float[]`. The length of such an array is specified as an `int` variable.

Consider the set of all possible arrays of type `float[]`. Is the cardinality of this set finite, countable, or uncountable? Discuss the relationship of this set to the sets of lists and streams of numbers that we defined. **[6 marks]**

Model answer / LOs / Creativity:

(a) (i) The Venn diagram of $(A \setminus B) \cup ((B \cap C) \setminus A)$ should look something like this:



(ii) There are many options. The most straightforward one is to use the equation $Y \setminus Z = Y \cap \overline{Z}$ to get

$$(A \cap \overline{B}) \cup ((B \cap C) \cap \overline{A})$$

but it is also possible to read off other solutions from the Venn diagram.

(iii) $D = \{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$ and $D \cap E = \{-6, -3, 0, 3, 6\}$.

(b) (i) No, $\mathbb{Z}_6$ does not satisfy the law of the multiplicative inverse. This can be seen for example by writing out the times table for either 2, 3, or 4 modulo 6, and noting that 1 does not appear as a product:

$\times$	0	1	2	3	4	5
2	0	2	4	0	2	4

$\times$	0	1	2	3	4	5
3	0	3	0	3	0	3

$\times$	0	1	2	3	4	5
4	0	4	2	0	4	2

Other arguments are fine, as long as they convincingly show that at least one of 2, 3, and 4 does not have a multiplicative inverse.

(ii) At the beginning of the loop, $x = 0$ and $s = 0$, so $s = x^2$ is satisfied.

Now assume $s = x^2$ holds at the beginning of a pass through the loop body. At the end of the loop body we have $s' = s + 2x' - 1$, where $x' = x + 1$. The latter can be rearranged to give $x = x' - 1$. Then, using the assumption:

$$s' = x^2 + 2x' - 1 = (x' - 1)^2 + 2x' - 1 = (x')^2 - 2x' + 1 + 2x' - 1 = (x')^2.$$

Thus the invariant holds at the end of the loop.

(c) The set of all arrays of type `float[]` in Java is finite since the array length is specified by an `int` (therefore finite) and each array element is a `float` (which can only take finitely many different values).

We can think of each array as a finite sequence of numbers (strictly speaking, there is an injective map from arrays to sequences of numbers, though this does not need to be stated). Let F be the set of sequences of numbers that correspond to arrays of type `float[]`.

A set is characterised by its elements, so the relationship between two sets is described by whether they have some, all, or none of their elements in common. The following characterise the relationship between F and the sets of lists or streams of numbers:

- F is disjoint from A^ω for any $A \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$, since arrays have finite length and A^ω contains only infinite streams.
- F is a subset of $\mathbb{R}^*$, the set of finite lists of real numbers.
- F is a subset of $\mathbb{Q}^*$ since each floating point number is actually rational.

- F is not a subset of $\mathbb{Z}^*$ or $\mathbb{N}^*$ since many arrays contain non-integral numbers.
- $F \cap \mathbb{Z}^*$ and $F \cap \mathbb{N}^*$ are non-empty because there are arrays of type `float[]` which contain only integers, or only natural numbers.

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

Question 2 [Propositional Logic]

(a) Let F be the following proposition: $(\neg A \vee \neg B) \to (C \to A \wedge B) \to \neg C$. Provide an intuitionistic Natural Deduction proof of F. **[8 marks]**

(b) Let G be the following proposition: $\neg\neg\neg A \to \neg A$.

(i) Provide an intuitionistic Natural Deduction proof of G **[4 marks]**

(ii) Provide a intuitionistic Sequent Calculus proof of G. **[4 marks]**

(c) Let H be $(\neg P \to Q \wedge R) \to P \vee R$. Provide a proof of H using the 2nd classical version of the Sequent Calculus (i.e., the version without additional LEM or DNE rules but with classical sequents instead). **[4 marks]**

Model answer / LOs / Creativity:

(a) Here is an intuitionistic Natural Deduction proof of F:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{C \to A \wedge B}\,2 \quad \dfrac{}{C}\,3}{A \wedge B}\,[\to E]}{A}\,[\wedge E_L] \quad \dfrac{}{\neg A}\,4}{\bot}\,[\neg E]}{\neg A \to \bot}\,4\,[\to I] \quad \dfrac{}{\neg A \vee \neg B}\,1 \quad \dfrac{\dfrac{\dfrac{\dfrac{}{C \to A \wedge B}\,2 \quad \dfrac{}{C}\,3}{A \wedge B}\,[\to E]}{B}\,[\wedge E_R] \quad \dfrac{}{\neg B}\,5}{\bot}\,[\neg E]}{\neg B \to \bot}\,5\,[\to I]}{\bot}\,[\vee E]}{\neg C}\,3\,[\neg I]}{(C \to A \wedge B) \to \neg C}\,2\,[\to I]}{(\neg A \vee \neg B) \to (C \to A \wedge B) \to \neg C}\,1\,[\to I]$$

(b) (i) Here an intuitionistic Natural Deduction proof of G

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg\neg A}\,1 \quad \dfrac{\dfrac{}{\neg A}\,3 \quad \dfrac{}{A}\,2}{\bot}\,[\neg E]}{\neg\neg A}\,3\,[\neg I]}{\bot}\,[\neg E]}{\neg A}\,2\,[\neg I]}{\neg\neg\neg A \to \neg A}\,1\,[\to I]$$

(ii) Here an intuitionistic Sequent Calculus proof of G

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,[Id]}{A, \neg A \vdash \bot}\,[\neg L]}{A \vdash \neg\neg A}\,[\neg R]}{\neg\neg\neg A, A \vdash \bot}\,[\neg L]}{\neg\neg\neg A \vdash \neg A}\,[\neg R]}{\vdash \neg\neg\neg A \to \neg A}\,[\to R]$$

(c) Here a classical Sequent Calculus proof of H

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \vdash P}\,[Id]}{\vdash \neg P, P}\,[\neg R] \quad \dfrac{}{Q, R \vdash R}\,[Id]}{Q \wedge R \vdash R}\,[\wedge L]}{\neg P \to Q \wedge R \vdash P, R}\,[\to L]}{\neg P \to Q \wedge R \vdash P \vee R}\,[\vee R]}{\vdash (\neg P \to Q \wedge R) \to P \vee R}\,[\to R]$$

Learning outcomes: "Write formal proofs for propositional and predicate logic" (a & b); "Apply logical techniques to solve a problem within a computer science setting" (a & b).