CS 514, Mathematics for Computer Science
Mid-semester Exam, Monsoon 2019
Department of Computer Science and Engineering
IIT Guwahati

Important

1. No questions about the paper will be entertained during the exam.
2. You must answer each question in the space provided for that question in the **answer sheet**. Answers appearing outside the space provided will not be considered.
3. Keep your rough work separate from your answers. A supplementary sheet is being provided for rough work. **Do not attach your rough work to the answer sheet.**
4. This exam has 6 questions over 3 pages, with a total of 60 marks.
5. **Write your roll number at the top of every page in the answer sheet.**

1. Give an example of a function from a set to itself which is
   (a) an injection but not a bijection; (5)
   (b) a surjection but not a bijection. (5)

Solution: The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n + 1$ is injective since $a \neq b \Rightarrow f(a) \neq f(b)$ but is not surjective since 0 is not the image of any element under f. Similarly, the function $f : \mathbb{N} \to \mathbb{N}$ defined by $g(n) = n - 1$ if $n \geq 1$ and $g(0) = 0$ is surjective but not injective, since $g(1) = g(0)$.

2. Let S be the set of all infinite sequences containing only numbers from 1, 2 and 3. Prove or disprove: S is a countable set.

(10)

Solution: We show by diagonalization that the set S is not countable. Suppose S is countable, and $\sigma_0, \sigma_1, \sigma_2 \ldots$ is an enumeration of S, where

$$\sigma_0 = s_{00}s_{01}s_{02}\ldots$$
$$\sigma_1 = s_{10}s_{11}s_{12}\ldots$$
$$\vdots$$

Here each $s_{ij} \in \{1, 2, 3\}$. Then consider the sequence $\tau = t_0 t_1 t_2 \ldots$ where $t_i = f(s_{ii})$ where the function f is defined by $f(1) = 2, f(2) = 3, f(3) = 1$, *i.e.*, t_i is distinct from s_{ii} for all i. Then the sequence τ cannot appear anywhere in the above enumeration, because it differes from σ_i at the i^{th} element for all i. Contradiction.

3. (a) Give a sentence in first-order logic (where the language $\mathcal{L}$ contains $=$, but no other predicate, function or constant symbols) that is satisfied by an interpretation iff its universe contains exactly two elements.

(5)

Solution: $\exists x \exists y[\neg(x = y) \wedge \forall z(z = x \vee z = y)]$

(b) Give a sentence A in first-order logic (over some language $\mathcal{L}$ that you can specify) that is only satisfied by structures whose universes are infinite, *i.e.*, if $\mathcal{M} \models A$ then the universe M of $\mathcal{M}$ is infinite. [Hint: Express that any model of A is a partial order with no minimal element.]

(5)

Solution:
Consider the sentence $A = (A_1 \wedge A_2 \wedge A_3 \wedge A_4)$ in first-order logic, where P is a binary predicate symbol and A_1, A_2, A_3 and A_4 are defined as follows:

$$A_1 = \forall x P(x, x)$$
$$A_2 = \forall x \forall y((P(x, y) \wedge P(y, x)) \rightarrow x = y)$$
$$A_3 = \forall x \forall y \forall z((P(x, y) \wedge P(y, z)) \rightarrow P(x, z))$$
$$A_4 = \neg \exists y \forall x(P(x, y) \rightarrow (x = y))$$

The first three sentences together assert that the interpretation of P must be a partial order. The last sentence says that there is no minimal element, which implies the order must be infinite.

4. Prove that there are no three consecutive odd positive integers, all greater than 3, that are primes, *i.e.*, there are no odd primes of the form p, $p + 2$ and $p + 4$ where $p > 3$.

(10)

Solution: If p is a prime and $p > 3$, p cannot be a multiple of 3. Then there are two cases: $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. In the first case, $p + 2$ is divisible by 3 and in the second, $p + 4$ is divisible by 3.

5. Find the remainder of $26^{1818181}$ divided by 297. [Hint: $1818181 = (180 \cdot 10101) + 1$]. You must justify all your steps.

(10)

Solution:

$$\phi(297) = \phi(3^3 \cdot 11) = (3^3 - 3^2) \cdot 10 = 180$$

since $\phi(p^k) = p^k - p^{k-1}$ if p is prime and $\phi(ab) = \phi(a)\phi(b)$ when a and b are relatively prime. Since $1818181 = (180 \cdot 10101) + 1 = \phi(297) \cdot 10101 + 1$, we have

$$\text{rem}(26^{1818181}, 297) = \text{rem}((26^{\phi(297)})^{10101} \cdot 26, 297) = \mathbf{26}$$

since $26^{\phi(297)} \equiv 1 (\text{mod } 297)$ by Euler's theorem since 26 and 297 are relatively prime.

6. Let $S_k = 1^k + 2^k + \ldots + (p-1)^k$, where p is an odd prime and k is a multiple of $p - 1$. Use Fermat's theorem to prove that $S_k \equiv -1 \pmod p$. You must justify all your steps.

(10)

Solution: We are given that p is an odd prime and k is a multiple of $p - 1$. Now for all i such that $1 \leq i \leq p - 1$, p does not divide i. Hence by Fermat's theorem, $i^{p-1} \equiv 1 \pmod p$ for all i such that $1 \leq i \leq p - 1$. Now since, $k = n(p - 1)$ for some integer n, we have $i^k = i^{n(p-1)} = (i^{p-1})^n \equiv 1^n \equiv 1 \pmod p$ by repeated use of the congruence property of multiplication. Then by using the congruence property of addition, the sum $S_k = \Sigma_{i=1}^{p-1} i^k \equiv 1 + 1 + 1 \ldots + 1 \pmod p \equiv (p - 1) \pmod p \equiv -1 \pmod p$, since $p \equiv 0 \pmod p$.