Computer Science Tripos Part IA and IB

2019-2020
Exam Question
Cover sheet

Student BGN2023A**…..……**

Paper2**……**

Question number8**……**

How did you answer this question?

Timed	☐	Open Book	☑
Untimed	☑	Closed Book	☐

Questions

List all the questions you have answered for this paper here. 1,4,6,7,8

Computer Science Tripos Honour Code

1. We take it as a principle that maintaining the integrity and fairness of examinations should be regarded as a collaboration between students and the Department.
2. The students undertake that they will not help others in examinations and will not receive any help from others (students or non-students).
3. Students will actively contribute to ensuring that all students adhere to the code.
4. Students will keep to the conditions of the assessment and will accurately report those conditions when asked.
5. The Department will not make any attempt at remote invigilation of online examinations.

I **undertake to respect the Computer Science Tripos honour code**

Tick the box to confirm ☑

8a) (i)

Let d be an integer. We will prove that if $d \mid a \wedge d \mid b \iff d \mid (a-b) \wedge d \mid b$.

($\implies$) Assume that d divides both a and b. Then, there exist some integers m and n such that $a = dm$ and $b = dn$. We then have $(a-b) = (dm - dn) = d(m-n)$, so $d \mid (a-b)$.

($\impliedby$) Assume that d divides both $a-b$ and b. Then there exist some integers s and t sich that $a - b = ds$ and $b = dt$. We then have $a = a - b + b = ds + dt = d(s+t)$, so $d \mid a$.

Since the integers that divide a and b are the same as those that divide $(a-b)$ and b, this means that $\gcd(a,b) = \gcd(a-b,b)$ as required.

(ii)

For $q = 0$ the statement is trivially true.

Assume that the statement is true for $q = k$, i.e. for all $n, k \in \mathbb{N}$,
$\gcd(2^{kn+r} - 1, 2^n - 1) = \gcd(2^r - 1, 2^n - 1)$

For $q = k+1$, using the proof from part (i):

$$\begin{aligned}\gcd(2^{(k+1)n+r} - 1, 2^n - 1) &= \gcd(2^{(k+1)n+r} - 2^n, 2^n - 1) \\ &= \gcd(2^n(2^{kn+r} - 1), 2^n - 1)\end{aligned}$$

Since $\gcd(2^n, 2^n - 1) = 1$, we can say

$$\begin{aligned}\gcd(2^{(k+1)n+r} - 1, 2^n - 1) &= \gcd(2^{kn+r} - 1, 2^n - 1) \\ &= \gcd(2^r - 1, 2^n - 1)\end{aligned}$$

And so the statement is true by induction.

(iii)

Starting from the statement in part (ii) - but replacing the q with k so that it is not confused with the q in this question - let $r = n$, so that $\gcd(2^{kn+n} - 1, 2^n - 1) = \gcd(2^n - 1, 2^n - 1)$.

The right hand side is trivially equal to $2^n - 1$. Let $q = k+1$, and the left hand side becomes $\gcd(2^{qn} - 1, 2^n - 1)$. We then have $\gcd(2^{qn} - 1, 2^n - 1) = 2^n - 1$ as required.

(iv)

Using the proof from part (ii), let q and r be such that $m = qn + r$ and $0 \leq r < n$. We then have a process that mimics Euclid's algorithm in the exponent, so that
$\gcd(2^m - 1, 2^n - 1) = \gcd(2^n - 1, 2^r - 1)$. Following the algorithms to its conclusion, this would give us $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)} - 1$.

b) Suppose that $f : \mathbb{N} \Rightarrow (\mathbb{N} \Rightarrow \{0,1\})$ is a function. We define the function
$M = \{(n, 1 - f(n)(n)) \mid n \in \mathbb{N}\}$

M is clearly an element of $(\mathbb{N} \Rightarrow \{0,1\})$. We will show that for all $n \in \mathbb{N}$, $f(n) \neq M$.

1. If $(n, 1) \in M$ then $(n, 0) \in f(n)$, so $f(n) \neq M$ since they both map n to a different value.
2. If $(n, 0) \in M$ then $(n, 1) \in f(n)$, so $f(n) \neq M$ by the same argument as above.

Therefore there is no $a \in \mathbb{N}$ such that $M = f(a)$. So f cannot be surjective.