CENG 223

Discrete Computational Structures

Fall 2018-2019

Homework 2 - Solutions

Question 1

Let $f : A \to B$ and $g : B \to C$. Prove the following:

a)

$$\begin{aligned}(g \circ f)^{-1}(C_0) &= \{a \in A \mid (g \circ f)(a) \in C_0\} \\ &= \{a \in A \mid g(f(a)) \in C_0\} \\ &= \{a \in A \mid g(b) \in C_0 \wedge f(a) = b\} \\ &= f^{-1}(\{b \in B \mid g(b) \in C_0\}) \\ &= f^{-1}(g^{-1}(C_0))\end{aligned}$$

b) Since f and g are injective: $(f(a_1) = f(a_2)) \to (a_1 = a_2)$ and $(g(b_1) = g(b_2)) \to (b_1 = b_2)$. Take a_1 and a_2 such that $g \circ f(a_1) = g \circ f(a_2)$. This implies $f(a_1) = f(a_2)$ due to the injectivity of g. This in turn implies $a_1 = a_2$. Then $g \circ f$ is injective.

c) Assume f is not injective. Then there exists a_1, a_2 such that, $a_1 \neq a_2, f(a_1) = f(a_2) = b$. Since g is a function $g(b) = g \circ f(a_1) = g \circ f(a_2)$. Contradicting the injectivity of $g \circ f$. Hence f must be injective.
We already know that g may be injective by part b). However this is not a necessity: assume $b_1, b_2 \in B,\ b_1 \neq b_2,\ f(a_1) = b_1$ for some $a_1 \in A$, and $f(a) \neq b_2$ for all $a \in A$. Assume further that $g(b_1) = g(b_2) = c$ for some $c \in C$, and g satisfies injectivity for all $b \in B$ such that $b \neq b_1 \wedge b \neq b_2$. Then we have g as not injective, and $g \circ f$ as injective. So g may also not be injective.

d) (sketch of proof) Since g and f are surjective, g hits every element of C and f hits every element of B. Hence $g \circ f$ hits every element of C.

e) Assume g is not surjective. Then there is an element $c_1 \in C$ such that $g(b) \neq c_1, \forall b \in B$. Contradicting the surjectivity of $g \circ f$. So g must be surjective.
Similar to part c), we cannot deduce the surjectivity of f: assume $g(B_0) = C$ for some $B_0 \subsetneq B$, and $f(A) = B_0$. Such an f does not cover all of B, however, $g \circ f(A) = C$.

Question 2

a) If f has a left inverse we have $g \circ f(A) = A$. This function is a bijection from A to itself. Hence g is surjective and f is injective by Question 1. If f has a right inverse we have $f \circ h(B) = B$. Then f is surjective and h is injective.

b) Define $f : \{1\} \to \{1, 2\}$ such that $f(1) = 2$. This function has the left inverse g where $g(2) = 1$, yet no right inverses.

c) Define $h : \{1, 2\} \to \{1\}$ such that $h(1) = h(2) = 1$. This function attains a right inverse but no left inverses.

d) Take g_1, g_2 such that $g_1(1) = g_1(2) = 1$ and $g_2(1) = 2, g_2(2) = 1$ in part b). Both are left inverses.
Take k_1, k_2 such that $k_1(1) = 1$ and $k_2(1) = 2$. Both are right inverses for h defined in part c).

e) If f has a left inverse and a right inverse, it is both surjective and injective by part a). Then f is a bijection.
$g = h = f^{-1}$: take $b \in B$. Since f is surjective $f^{-1}(b) = a$ for some $a \in A$. $g \circ f(a) = a$ implies $g(b) = a$. Whence we see that g agrees with f^{-1} everywhere on B implying $g = f^{-1}$. Similarly, $f \circ h(b) = b = f(a)$. Then $h(b) = a$ by using the injectivity of f. This implies $h = f^{-1}$. Hence, $g = h = f^{-1}$.

Question 3

f is injective.
Let $f(a_1, b_1) = f(a_2, b_2)$. Then we have $(a_1 + b_1 - 1, b_1) = (a_2 + b_2 - 1, b_2)$ from which $b_1 = b_2$ immediately follows. Using this we get $a_1 = a_2$.
f is surjective.
Let $(a, b) \in A$. Then we have $f(a-b+1, b) = (a-b+1+b-1, b) = (a, b)$. Note that $a-b+1 \in \mathbb{Z}^+$ since $b \leq a$ (membership condition of A).
g is injective.
Let $g(a_1, b_1) = g(a_2, b_2)$. Then we have:

$$\frac{1}{2}a_1(a_1 - 1) + b_1 = \frac{1}{2}a_2(a_2 - 1) + b_2$$

Assume $a_1 \neq a_2$. Without loss of generality assume $a_1 > a_2$ which implies $b_1 < b_2$.

$$\begin{aligned}
\frac{1}{2}(a_1^2 - a_1) - \frac{1}{2}(a_2^2 - a_2) &= b_2 - b_1 \\
a_1^2 - a_2^2 - a_1 + a_2 &= 2(b_2 - b_1) \\
a_1^2 - a_2^2 &= a_1 - a_2 + 2(b_2 - b_1) \\
a_1 + a_2 = 1 + 2\frac{b_2 - b_1}{a_1 - a_2} &< 1 + 2b_2
\end{aligned}$$

But since $a_2 \geq b_2$ and $a_1 > a_2$, $a_1 \geq b_2 + 1$. Adding a_2 to both sides and using $a_2 \geq b_2$ gives $a_1 + a_2 \geq 2b_2 + 1$. Contradiction.
Note that $A \subset \mathbb{Z}^+ \times \mathbb{Z}^+$, so that $b_1 = 0$ or $b_2 = 0$ can safely be disregarded. Otherwise, the function g would not be injective, for example $g(4, 4) = g(5, 0) = 10$.
g is surjective.
Let $a \in \mathbb{Z}^+$, and x be the maximal integer such that $1/2\ x(x-1) < a$. Define $y = a - 1/2\ x(x-1)$. We have to show that $y \leq x$. Assume $y > x$. Then $y = x + c$ for some $c \in \mathbb{Z}^+$ which makes

$$a = \frac{1}{2}(x^2 - x) + x + c = \frac{1}{2}(x^2 + x) + c = \frac{1}{2}(x + 1)x + c$$

which contradicts the maximality of x. Hence g is surjective.

Question 4

a) `Sketch of Proof`
Each polynomial in the given form can be characterized by n-tuples $(a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$. Since $\mathbb{Q}$ is countable, so is its finite product $\mathbb{Q}^n$. Now, we are assigning each of this tuples some finite number of roots (assumption given by the question), and unions of this sets will also be countable. The acquired set is the roots of polynomials of a fixed degree n.
The set of algebraic numbers is the union of roots to all degrees of polynomials. Since the arbitrary union of countable sets is again countable, the set of algebraic number is countable.

b) Since $\mathbb{R}$ is the union of algebraic numbers and transcendental numbers, and algebraic numbers are countable, transcendental number must be uncountable. For otherwise, real numbers would be countable as a union of two countable sets, which is a contradiction.

Question 5

$n \ln n = \Theta(k)$ implies

$$c_1 k \leq n \ln n \leq c_2 k \;\rightarrow\; c_1 \frac{k}{lnk} \leq n \frac{\ln n}{\ln k} \leq c_2 \frac{k}{\ln k}, \qquad k \geq k_0 \tag{1}$$

Taking the ln of all sides we also have $\ln c_1 + \ln k \leq \ln n + \ln \ln n \leq \ln c_2 + \ln k$. For large n we have $\ln n + \ln \ln n < 2 \ln n$, so that the left inequality of 1 becomes:

$$\ln c_1 + \ln k \leq \ln n + \ln \ln n < 2 \ln n \;\rightarrow\; 1 < 2 \frac{\ln n}{\ln k}$$

Then we have $n < 2n \ln n / \ln k$. Using the right inequality of 1:

$$n < 2n \frac{\ln n}{\ln k} \leq 2c_2 \frac{k}{\ln k} \tag{2}$$

In a similar vein, using $\ln n < \ln n + \ln \ln n$, and $\ln n + \ln \ln n \leq \ln c_2 + \ln k$

$$\begin{aligned} \ln n < \ln c_2 + \ln k \rightarrow \frac{\ln n}{\ln k} &< \frac{\ln c_2}{\ln k} + 1 \\ \rightarrow \frac{\ln n}{\ln k} &< 2 \end{aligned}$$

Using this on the left inequality of 1 we get

$$\begin{aligned} c_1 \frac{k}{\ln k} \leq n \frac{\ln n}{\ln k} &< 2n \\ \frac{c_1}{2} \frac{k}{\ln k} &< n \end{aligned} \tag{3}$$

By 2 and 3 we have $n = \Theta(k / \ln k)$.

Question 6

a) $6 = 1 + 2 + 3$, and $28 = 1 + 2 + 4 + 7 + 14$.

b) Since $2^p - 1$ is a prime it either contributes as it is to a divisor of the number or not. So we can divide the divisors into two sets:

$$A = \{2^0, 2^1, \ldots, 2^{p-1}\}$$

$$B = \{2^0(2^p - 1), 2^1(2^p - 1), \ldots, 2^{p-1}(2^p - 1)\}$$

Since the last element of B as listed above is the number's itself, we are not including in the summation to check the perfectness of the number. Then we have:

$$\begin{aligned}
\sum_{k=0}^{p-1} 2^k + \sum_{k=0}^{p-2} 2^k(2^p - 1) &= \sum_{k=0}^{p-1} 2^k + \sum_{k=p}^{2p-2} 2^k - \sum_{k=0}^{p-2} 2^k \\
&= \sum_{k=0}^{2p-2} 2^k - \sum_{k=0}^{p-2} 2^k \\
&= 2^{2p-1} - 1 - 2^{p-1} - 1 = 2^{2p-1} - 2^{p-1} \\
&= 2^{p-1}(2^p - 1)
\end{aligned}$$

Where $2^n = 1 + \sum_{k=0}^{n-1} 2^k$ is used.

Question 7

a) Assume a solution x exists. Then

$$\begin{aligned}
x \equiv c_1 \pmod{m}, \quad x \equiv c_2 \pmod{n} \\
\rightarrow x = k_1 m + c_1, \quad x = k_2 n + c_2 \\
\rightarrow c_1 - c_2 = -k_1 m + k_2 n
\end{aligned}$$

The right hand side is divisible by $\gcd(m, n)$, so $\gcd(m, n) | c_1 - c_2$.
Assume $\gcd(m, n) | c_1 - c_2$. Then $c_1 - c_2$ can be written as $kt_1 m + kt_2 n$ where $t_1, t_2 \in \mathbb{Z}$ (Bézout's theorem is used). Then a solution $x = c_1 - kt_1 m = c_2 + kt_2 n$ is a solution (as should the reader verify).

b) Assume $x_1 \equiv x_2 \equiv c_1 \pmod{m}$ and $x_1 \equiv x_2 \equiv c_2 \pmod{n}$. Then $x_1 - x_2 \equiv 0 \pmod{m}$ and $x_1 - x_2 \equiv 0 \pmod{n}$. Hence $x_1 - x_2 \equiv 0 \pmod{\operatorname{lcm}(m, n)}$ (reader should verify).
Since every integer $i \in [a \operatorname{lcm}(m, n),\ (a+1) \operatorname{lcm}(m, n))$ where $a \in \mathbb{Z}$ is a member of a different equivalence class, in any such interval $x_1 = x_2$ holds.
This can simply be stated as:

$$x_1, x_2 \in \big[0,\ \operatorname{lcm}(m, n)\big) \quad \wedge \quad x_1 \neq x_2 \qquad \rightarrow x_1 - x_2 \not\equiv 0 \pmod{lcm(m, n)}$$