CSC240 Winter 2024 Homework Assignment 3

My name and student number: Haoyun (Bill) Xi, 1009992019
The list of people with whom I discussed this homework assignment: NONE

1. Let $\mathcal{F}$ be the set of all functions from D to D, where D is a nonempty set. Consider the following two predicates with domain $\mathcal{F} \times \mathcal{F}$:

$$\begin{aligned} P(f,g) &= \exists y \in D.\forall x \in D.[f(g(x)) \neq y] \text{ and} \\ Q(f,g) &= \exists v \in D.[\forall u \in D.(f(u) \neq v) \text{ OR } \forall u \in D.(g(u) \neq v)]. \end{aligned}$$

Formally prove that $\forall f \in \mathcal{F}.\forall g \in \mathcal{F}.(P(f,g) \text{ IMPLIES } Q(f,g))$.
Remember to number all lines, indent properly, and justify all your steps, including references to the appropriate line numbers, as described in Proof Outlines. Only do one step of the proof per line.

Proof

1 Let $f \in \mathcal{F}$ be arbitrary
2 Let $g \in \mathcal{F}$ be arbitrary
3 Assume $P(f,g)$
4 $\exists y \in D.\forall x \in D.[f(g(x)) \neq y]$; definition of $P(f,g)$, L3
5 Let $i \in D$ be such that $\forall x \in D.[f(g(x)) \neq i]$; instantiation, L4
6 R OR NOT(R); tautology
7 Let $S = \exists a \in D.(f(a) = i)$
8 $\exists a \in D.(f(a) = i)$ OR NOT($\exists a \in D.(f(a) = i)$); substitution of all R by S, L6
9 Assume $\exists a \in D.(f(a) = i)$
10 Let $r \in D$ be such that $f(r) = i$; instantiation, L9
11 Let $v = r$
12 $v \in D$
13 To obtain a contradiction, assume NOT($\forall u \in D.(g(u) \neq v)$)
14 $\exists u \in D.(g(u) = v)$; negation of quantifiers, L13
15 Let $k \in D$ be such that $g(k) = v$; instantiation, L14
16 $f(g(k)) = f(v)$; property of function, L15
17 $f(g(k)) = f(r)$; substitute $v = r$ from L11 to L16
18 $f(g(k)) = i$; substitute $f(r) = i$ from L10 to L17
19 $f(g(k)) \neq i$; specialization, L5, L15
20 This is a contradiction: L18, L19
21 $\forall u \in D.(g(u) \neq v)$; proof by contradiction, L13, L20
22 $\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)$; proof of disjunction, L21
23 $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$; construction, L11, L12, L22
24 $\exists a \in D.(f(a) = i)$ IMPLIES $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$; direct proof, L9, L23
25 Assume NOT($\exists a \in D.(f(a) = i)$)
26 $\forall a \in D.(f(a) \neq i)$; negation of quantifiers, L25

27 $\forall u \in D.(f(u) \neq i)$; substitute u for quantified a L26
28 Let $v = i$
29 $v \in D$
30 $\forall u \in D.(f(u) \neq v)$; substitute $v = i$ from L28 to L27
31 $\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)$; proof of disjunction, L30
32 $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$; construction, L28, L29, L31
33 NOT$(\exists a \in D.(f(a) = i))$ IMPLIES $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$; direct proof, L25, L32
34 $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$; proof by cases, L8, L24, L33
35 $Q(f, g)$; definition of Q, L34
36 $P(f, g)$ IMPLIES $Q(f, g)$; direct proof L3, L35
37 $\forall g \in \mathcal{F}.(P(f, g)$ IMPLIES $Q(f, g))$; generalization, L2, L36
38 $\forall f \in \mathcal{F}.\forall g \in \mathcal{F}.(P(f, g)$ IMPLIES $Q(f, g))$; generalization, L1, L37

2. Recall that, if p is a polynomial of degree $m \geq 1$, then there exist coefficients a_i for $0 \leq i \leq m$ such that $a_m \neq 0$ and, for all numbers n,

$$p(n) = \sum_{i=0}^{m} a_i n^i.$$

Give a well-structured informal proof that, for any polynomial p of degree at least 1 whose coefficients are natural numbers, there is a natural number n such that $p(n)$ is not prime.

Proof:
We will prove by contradiction.

- Assume there is a polynomial p of degree $m \geq 1$ whose coefficients are natural numbers, where for all natural number n, $p(n)$ is a prime.

  Let $p(n) = a_0 + \sum_{i=1}^{m} a_i n^i$, where $a_m \neq 0$, $m \geq 1$, and $a_i \geq 0$ for $0 \leq i \leq m$.

  By our assumption, $p(0) = a_0$ is a prime (every term containing n goes to 0).

  Since $a_0 \in \mathbb{N}, p(a_0) = a_0 + \sum_{i=1}^{m} a_i \cdot (a_0)^i = a_0 \cdot \left(1 + \sum_{i=1}^{m} a_i \cdot (a_0)^{i-1}\right)$ is also a prime.

  By the definition of a prime, $p(a_i)$ only has 1 and itself as factors, therefore:

  - case 1: $a_0 = 1$
    Since we have shown a_0 is a prime under the assumption, we have $a_0 \neq 0$ and $a_0 \neq 1$ since 0 and 1 are not prime. There is a contradiction.
  - case 2: $(1 + \sum_{i=1}^{m} a_i \cdot (a_0)^{i-1}) = 1$. Immediately, we have: $\sum_{i=1}^{m} a_i \cdot (a_0)^{i-1} = 0$
    Since for $0 \leq i \leq m$, $a_i \geq 0$, we have each term $a_i \cdot (a_0)^{i-1} \geq 0$. Since $a_0 \geq 2$ and $i - 1 \geq 0$, the latter term $(a_0)^{i-1} \geq 1$. To keep the summation 0, we must have $a_i = 0$ for $1 \leq i \leq m$ $(a_1 = ... = a_m = 0)$, which contradicts with $a_m \neq 0$

  Therefore, $p(a_i)$ cannot be prime. This contradicts to $p(a_i)$ is a prime.

Because of the contradiction, we conclude there is NO polynomial p of degree $m \geq 1$ whose coefficients are natural numbers, where for all natural number n, $p(n)$ is a prime. This is equivalent to say for any polynomial p of degree at least 1 whose coefficients are natural numbers, there is a natural number n such that $p(n)$ is not prime.