CSC240 Winter 2024 Homework Assignment 3

My name and student number: Joseph Siu, 1010085701
The list of people with whom I discussed this homework assignment:

Hrithik Parag Shah

Serif Wu

Joseph Siu

Sanchit Manchanda

Abhi Prajapati

Sepehr Jafari

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 $\forall f \in \mathcal{F}.\forall g \in \mathcal{F}.(P(f,g)$ 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 be an arbitrary element of $\mathcal{F}$;
2 Let g be an arbitrary element of $\mathcal{F}$;
3 Assume $P(f,g)$;
4 $\exists y \in D.\forall x \in D.(f(g(x)) \neq y)$; by definition of $P(f,g)$: 3
5 Let $w \in D$ be such that $\forall x \in D.(f(g(x)) \neq w)$; instantiation 4
6 $(\forall u \in D.f(u) \neq w)$ OR NOT$(\forall u \in D.f(u) \neq w)$; tautology
7 Case 1: Assume $\forall u \in D.f(u) \neq w$;
8 $\forall u \in D.(f(u) \neq w)$ OR $\forall u \in D.(g(u) \neq w)$; proof of disjunction: 7
9 $\exists w \in D.[\forall u \in D.(f(u) \neq w)$ OR $\forall u \in D.(g(u) \neq w)]$; construction: 5, 8
10 $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$;
substitution of bound variable w for v: 9
11 $(\forall u \in D.f(u) \neq w)$ IMPLIES $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$;
direct proof: 7, 10
12 Case 2: Assume NOT$(\forall u \in D.f(u) \neq w)$;
13 NOT$(\forall u \in D.f(u) \neq w)$ IFF $(\exists u \in D.\text{NOT}(f(u) \neq w))$;
tautology, negation of quantifier
14 $\exists u \in D.\text{NOT}(f(u) \neq w)$; modus ponens: 12, 13
15 $[\exists u \in D.\text{NOT}(f(u) \neq w)]$ IFF $[\exists u \in D.\text{NOT}(\text{NOT}(f(u) = w))]$;
tautology, definition of $\neq$

16 $\exists u \in D.\text{NOT}(\text{NOT}(f(u) = w))$; modus ponens: 14, 15

17 $[\exists u \in D.\text{NOT}(\text{NOT}(f(u) = w))]$ IFF $[\exists u \in D.f(u) = w]$;
tautology, definition of negation

18 $\exists u \in D.f(u) = w$; modus ponens: 16, 17

19 Let $z \in D$ be such that $f(z) = w$; instantiation: 18

20 To obtain a contradiction, assume $\text{NOT}(\forall p \in D.z \neq g(p))$;

21 $\text{NOT}(\forall p \in D.z \neq g(p))$ IFF $(\exists p \in D.\text{NOT}(z \neq g(p)))$;
tautology, negation of quantifier

22 $\exists p \in D.\text{NOT}(z \neq g(p))$; modus ponens: 20, 21

23 $(\exists p \in D.\text{NOT}(z \neq g(p)))$ IFF $(\exists p \in D.\text{NOT}(\text{NOT}(z = g(p))))$;
tautology, definition of $\neq$

24 $\exists p \in D.\text{NOT}(\text{NOT}(z = g(p)))$; modus ponens: 22, 23

25 $(\exists p \in D.\text{NOT}(\text{NOT}(z = g(p))))$ IFF $(\exists p \in D.z = g(p))$;
tautology, definition of negation

26 $\exists p \in D.z = g(p)$; modus ponens: 24, 25

27 Let $e \in D$ be such that $z = g(e)$; instantiation: 26

28 $f(g(e)) \neq w$; specialization: 27, 5

29 $f(z) \neq w$; substitution of an occurence of $g(e)$ by z: 28, 27

30 This is a contradiction: 19, 29

31 $\forall p \in D.z \neq g(p)$; proof by contradiction: 20, 30

32 $\forall u \in D.z \neq g(u)$; substitution of bound variable p for u: 31

33 $\forall u \in D.f(u) \neq z$ OR $\forall u \in D.g(u) \neq z$; proof of disjunction: 32

34 $\exists z \in D.[\forall u \in D.f(u) \neq z$ OR $\forall u \in D.g(u) \neq z]$; construction: 19, 33

35 $\exists v \in D.[\forall u \in D.f(u) \neq v$ OR $\forall u \in D.g(u) \neq v]$;
substitution of bound variable z for v: 34

36 $\text{NOT}(\forall u \in D.f(u) \neq w)$ IMPLIES $\exists v \in D.[\forall u \in D.f(u) \neq v$ OR $\forall u \in D.g(u) \neq v]$;
direct proof: 12, 35

37 $\exists v \in D.[\forall u \in D.(f(u) \neq v)$ OR $\forall u \in D.(g(u) \neq v)]$; proof by cases: 6, 11, 36

38 $Q(f, g)$; by definition of $Q(f, g)$: 37,

39 $P(f, g)$ IMPLIES $Q(f, g)$; direct proof: 3, 38

40 $\forall g \in \mathcal{F}.[P(f, g)$ IMPLIES $Q(f, g)]$; generalization: 2, 39

41 $\forall f \in \mathcal{F}.\forall g \in \mathcal{F}.[P(f, g)$ IMPLIES $Q(f, g)]$; generalization: 1, 40

□

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.

Assume p is a polynomial of degree $m \geq 1$ whose coefficients are natural numbers;

We consider 3 cases of $a_0 \in \mathbb{N}$: a_0 is 0, 1, or greater than 1;

Case 1: $a_0 = 0$;

Let $n = 0 \in \mathbb{N}$;

$p(n) = \sum_{i=0}^{m} a_i n^i = a_0 \cdot 0^0 + \sum_{i=1}^{m} a_i 0^i = a_0$;

Since 0 is not prime, this implies $p(n) = a_0 = 0$ is also not prime;

For Case 1, we have shown that there exists a natural number n such that $p(n)$ is not prime;

Case 2: $a_0 = 1$;

Let $n = 0 \in \mathbb{N}$;

$p(n) = \sum_{i=0}^{m} a_i n^i = a_0 \cdot 0^0 + \sum_{i=1}^{m} a_i 0^i = a_0$;

Since 1 is not prime, this implies $p(n) = a_0 = 1$ is also not prime;

For Case 2, we have shown that there exists a natural number n such that $p(n)$ is not prime;

Case 3: $a_0 \geq 2$;

Let $n = a_0 \in \mathbb{N}$;

$p(n) = \sum_{i=0}^{m} a_i a_0^i = a_0 \cdot a_0^0 + \sum_{i=1}^{m} a_i a_0^i = a_0 + a_0 \sum_{i=1}^{m} a_i a_0^{i-1} = a_0 \left(1 + \sum_{i=1}^{m} a_i a_0^{i-1}\right)$;

Now, since the addition and multiplication of natural numbers also produce natural numbers, we have $p(n) \in \mathbb{N}$ and $1 + \sum_{i=1}^{m} a_i a_0^{i-1} \in \mathbb{N}$;

Moreover, because $a_0^0 = 1 \geq 1$ and $a_0^{p+1} \geq a_0^p$ for all $p \in \mathbb{N}$, combining with the fact that the product of some nonnegative numbers is also nonnegative, we have $\left(1 + \sum_{i=1}^{m} a_i a_0^{i-1}\right) \geq (1 + a_m a_0^{m-1})$;

Since $a_m \neq 0$ implies $a_m \geq 1$, and $m-1 \geq 0$, we also have that $1+a_m a_0^{m-1} \geq (1+a_m) \geq 2 > 1$;

Hence, because both a_0 and $\left(1 + \sum_{i=1}^{m} a_i a_0^{i-1}\right)$ are natural numbers greater than 1, this means $p(n) = p(a_0)$ can be compose into a product of two natural numbers greater than 1, which implies $p(n)$ is not prime;

For Case 3, we have shown that there exists a natural number n such that $p(n)$ is not prime;

For all cases, we have shown that there is such natural number n which makes $p(n)$ not a prime;

Therefore, we conclude if p is a polynomial of degree $m \geq 1$ whose coefficients are natural numbers, then there is a natural number n such that $p(n)$ is not prime. $\square$