Math 240: Homework 5

Daniel Ko

Spring 2020

§1 1

Fix positive integers a and b. Here's an inductive definition of a set S:
Foundation rule: $a, b \in S$
Constructor rule: If $m, n \in S$, then $m - n \in S$.

a. Suppose h is a common factor of a and b. Use the exclusion rule to prove that for every $n \in S$, h divides n.

Proof.
There must be integers c_a and c_b such that $a = hc_a$ and $b = hc_b$. By the contructor rule, $a - b \in S$ where $a - b = hc_a - hc_b = h(c_a - c_b)$. Thus, all other generated elements will have h as a common factor because of the exclusion rule. Therefore, by the exclusion rule we have proven that for every $n \in S$, h divides n. □

b. Suppose $k \in S$ is a positive integer which is not a factor of a. Prove that there is some $l \in S$ such that $0 < l < k$.

Proof.
Consider the sequence: $\{a, a-k, a-2k, \cdots\}$. Let this sequence be a subset of $\mathbb{N}$. It is clear that all elements in this sequence are elements of S by the constructor rule. By the well ordering principle, there exists a smallest element in this sequence. An l that always fits the criteria of $0 < l < k$ is the smallest element in this sequence. l must be less than k because if l wasn't less than k then l would not be the smallest element in the sequence. Let $a - nk$ be the first negative term that is generated. Then, our sequence must stop at $a - (n+1)k$ and this would be the smallest element in this set by the well ordering principle. Since, a is not a factor of k, l cannot be 0. Therefore, there exists an l such that $0 < l < k$. □

c. Use (b) and the above fact to prove that there is some positive integer in S which is a common factor of a and b.

Proof.
Consider this strictly decreasing sequence: $\{(a+b), (a+b)-k, (a+b)-2k, \cdots\}$ which is a subset of $\mathbb{N}$. By the well ordering principle, this sequence must be finite, such that it ends at $(a+b) - nk > 0$ and $(a+b) - (n+1)k < 0$, where $n \in \mathbb{N}$. Suppose there is no positive integer, l, in S that is a common factor of a and b. By construction of our sequence $a + b - (n+1)k < l$. By (b) l such that, $0 < l < k_{!a}$ and $0 < l < k_{!b}$, where $k_{!a}$ and $k_{!b}$ are integers that are not factors of a and b respectively. However, this leads to a contradiction because if this were true, then l would be a common factor of a and b. Thus, there exists a positive interger in S which is a common factor of a and b. □

d. Use (a) and (c) to conclude that S contains gcd(a,b)

Proof. From part c, we know there is a positive integer in S that is a common divisor of a and b. From part a, we know that this will divide all $n \in S$. Assume that there is a gcd(a,b) that is greater than the common divisor in S. This must mean gcd(a,b) $\neq m - n$, where $m, n \in S$. However, this is a contradiction because all common divisors must be generated using the constructor rule because it is a multiple of all $n \in S$. Thus, S must contain gcd(a,b). □

§2 2

a. Prove by structural induction that for all $x \in \{0,1\}^*, \lambda x = x$.

Proof.
We proceed by induction on x. Let $P(x)$ be the predicate "$x \in \{0,1\}^*, \lambda x = x$".

Base case: Show $P(\lambda)$ holds.
$P(\lambda) = \lambda\lambda = \lambda$ by foundation rule in concatenation.

Inductive step: If $P(x)$ holds, then $P(xi)$ holds, where $i \in \{0,1\}$
Fix $x \in \{0,1\}^*$ and $i \in \{0,1\}$ and assume that $P(x)$ holds. We show that $P(xi)$ holds.

$$\begin{aligned} P(xi) &= \lambda xi \\ &= xi \text{ by inductive hypothesis} \end{aligned}$$

□

b. Consider the function reverse: $\{0,1\}^* \to \{0,1\}^*$ which reverses a binary string e.g. reverse(01001) = 10010. Give an inductive definition of reverse.

Proof.
Foundation rule: reverse(i) = i, where $i \in \{\lambda, 0, 1\}$.
Constructor rule: reverse(xi) = ireverse(x), where $x \in \{0,1\}^*$ □

c. Using your inductive definition, prove that for all $x, y \in \{0,1\}^*$, reverse(xy) = reverse(y)reverse(x).

Proof.
Let $y \in \{0,1\}^*$. y_n repesents the nth digit and y_0^{n-4} represents the substring from 0 to $n-4$.
Let the length of y be n.

$$\begin{aligned} \text{reverse}(xy) &= y_n \text{reverse}(xy_0^{n-1}) \\ &= y_{n_1} y_{n-1} \text{reverse}(xy_0^{n-2}) \\ &\cdots \\ &= y_n y_{n-1} y_{n-2} \cdots y_1 y_0 \text{reverse}(x) \\ &= \text{reverse}(y_n) y_{n-1} y_{n-2} \cdots y_1 y_0 \text{reverse}(x) \\ &= \text{reverse}(y_{n-1} y_n) y_{n-2} \cdots y_1 y_0 \text{reverse}(x) \\ &\cdots \\ &= \text{reverse}(y) \text{reverse}(x) \end{aligned}$$

□