Undergrad Complexity: Problem Set 1

Ben Chaplin

Problem 1. A variadic function $f : \mathbb{N}^* \to \mathbb{N}$ is called a **coding function** if there are "inverse" functions $g : \mathbb{N} \to \mathbb{N}$ and $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that:

$$\begin{aligned} g(f(a_1, \ldots, a_n)) &= n \\ h(f(a_1, \ldots, a_n), i) &= a_i \qquad\qquad\qquad 1 \leq i \leq n \end{aligned}$$

for all sequences $a_1, \ldots, a_n$. Thus g determines the length of a sequence and h decodes it back to its elements. Moreover, h and g are supposed to be easily computable but let's ignore that for the time being. Now consider the pairing function π defined by:

$$\pi(x, y) = \binom{x + y + 1}{2} + x + 1$$

and define f as follows:

$$\begin{aligned} f(nil) &= 0 \\ f(a) &= \pi(0, a) \\ f(a_1, \ldots, a_n) &= \pi(f(a_2, \ldots, a_n), a_1) \end{aligned}$$

1. Show that π is injective.
2. Show that f is a coding function (make sure to explain what the appropriate decoding functions g and h are).
3. What whould happen if we replaced $\pi(x, y)$ by $\pi(x, y) - 1$? How could you fix the issue?

Answer (1.1)**.** First, note that:

$$\begin{aligned} \binom{x + y + 1}{2} &= \frac{(x + y)(x + y + 1)}{2} \qquad (1) \\ &= 1 + 2 + \ldots + (x + y) \qquad (2) \end{aligned}$$

Take $(x_1, y_1), (x_2, y_2) \in \mathbb{N} \times \mathbb{N}$ such that $\pi(x_1, y_1) = \pi(x_2, y_2)$. Assume to the contrary that $x_1 + y_1 \neq x_2 + y_2$, and without loss of generality, suppose that $x_1 + y_1 < x_2 + y_2$.

$$\binom{x_1 + y_1 + 1}{2} + x_1 + 1 = \binom{x_2 + y_2 + 1}{2} + x_2 + 1$$

By (1) and (2):

$$\begin{aligned} 1+2+\ldots+(x_1+y_1)+x_1+1 &= 1+2+\ldots+(x_2+y_2)+x_2+1 \qquad (3)\\ x_1-x_2 &= (1+2+\ldots(x_2+y_2))-(1+2+\ldots+(x_1+y_1))\\ &\geq x_2+y_2\\ x_1 &\geq 2x_2+y_2\\ x_1+y_1 &\geq 2x_2+y_2+y_1\\ &\geq x_2+y_2, \end{aligned}$$

a contradiction. Thus $x_1+y_1 = x_2+y_2$. Then, by (3), $x_1 = x_2$. So $y_1 = y_2$ and π is injective.

Answer (1.2)**.**

Lemma 1. *f is injective over inputs of the same size.*

Proof. We proceed by induction over the size of the input. If $n = 1$, then $f(x) = \pi(0, x)$, so f is injective by the fact that π is injective. Suppose f is injective for inputs of size $n-1$ and consider inputs of size n: $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{N}^n$ where $f(a_1, \ldots, a_n) = f(b_1, \ldots, b_n)$.

$$\begin{aligned} f(a_1,\ldots,a_n) &= f(b_1,\ldots,b_n)\\ \pi(f(a_2,\ldots,a_n),a_1) &= \pi(f(b_2,\ldots,b_n),b_1) \end{aligned}$$

So by the fact that π is injective, $a_1 = b_1$ and $f(a_2, \ldots, a_n) = f(b_2, \ldots, b_n)$. Thus, $a_i = b_i$ for $1 \leq i \leq n$. □

Lemma 2. *$f(\mathbb{N}^n)$ and $f(\mathbb{N}^m)$ are disjoint for any $n \neq m \in \mathbb{N}$.*

Proof. Suppose $m < n$ and $f(a_1, \ldots, a_m) = f(b_1, \ldots, b_n)$. Then:

$$\pi(f(a_2,\ldots,a_m),a_1) = \pi(f(b_2,\ldots,b_n),b_1)$$

Then $a_1 = b_1$. Furthermore, because π is injective:

$$\pi(f(a_3,\ldots,a_m),a_2) = \pi(f(b_3,\ldots,b_n),b_2)$$

So $a_2 = b_2$. By the same logic, $a_i = b_i$ for $1 \leq i \leq m$. But then we have:

$$\begin{aligned} \pi(f(nil),a_m) &= \pi(f(b_{m+1},\ldots,b_n),b_m)\\ f(nil) &= f(b_{m+1},\ldots,b_n)\\ 0 &= f(b_{m+1},\ldots,b_n) \end{aligned}$$

But this cannot be the case because $f(x) > 0$ for all $x \in \mathbb{N}^* - \{nil\}$. □

Lemma 1 and **Lemma 2** show that f is injective over $\mathbb{N}^*$. Thus, f has a partial inverse. We can now define g and h over all $x \in f(\mathbb{N}^*)$.

$$\begin{aligned} g(x) &= |(f^{-1}(x)|\\ h(x,i) &= P_i^{|f^{-1}(x)|}(f^{-1}(x)) \qquad \text{where } P \text{ is the projection function} \end{aligned}$$

Answer (1.3)**.** Defining π as:

$$\pi(x, y) = \binom{x + y + 1}{2} + x$$

does not change the fact that π is injective. However, it throws a wrench in our proof of **Lemma 2** from **Answer 1.2**. We can no longer assume that $f(x) > 0$ for all $x \in \mathbb{N}^* - \{nil\}$, as now:

$$f(0) = f(0, 0) = \ldots = 0$$

Actually, now **Lemma 2** is false. A counterexample: $f(x) = f(x, 0)$. But trailing 0's are the only case—we can see this via the proof of **Lemma 2**. We can define f^{-1} more carefully:

$$f^{-1}(a_1, \ldots, a_n) = f^{-1}(a_1, \ldots, a_i)$$

where $a_i \neq 0$ for the largest $i \leq n$. Now h is saved. But g is a goner.