

I worked alone without getting any help, except asking questions on Piazza and reading the Notes of this course.

## 1 Bijective or not?

(a)

(i) **Yes**

Proof (one-to-one): Suppose  $f(x) = f(y)$ , then  $10^{-5}x = 10^{-5}y$ . Since  $10^{-5} \neq 0$ , so we can divide both sides by  $10^{-5} \neq 0$ , which gives us that  $x = y$ . So,  $f(x) = f(y) \implies x = y$ , so  $f : \mathbb{R} \rightarrow \mathbb{R}$  is injective.

Proof (onto): If  $y \in \mathbb{R}$ , then  $f(10^5 y) = 10^{-5} 10^5 y = y$ . With  $y \in \mathbb{R}$ , so  $10^5 y \in \mathbb{R}$ , which means that  $y$  has a pre-image. Thus every  $y \in \mathbb{R}$  has a pre-image, so  $f : \mathbb{R} \rightarrow \mathbb{R}$  is onto.

Thus,  $f : \mathbb{R} \rightarrow \mathbb{R}$  is both one-to-one and onto, so it is a bijection.

(ii) **No**

We proceed by providing a counterexample to show that  $f : \mathbb{Z} \cup \{\pi\} \rightarrow \mathbb{R}$  is not onto, which implies that it is not a bijection.

Consider  $y = 0.123456$ , where  $y \in \mathbb{R}$ , so  $y$  is in the range. Suppose, for a contradiction, that some  $x_y \in \mathbb{Z} \cup \{\pi\}$  such that  $f(x_y) = y$ . Let  $A$  be the assertion that  $x_y \in \mathbb{Z} \cup \{\pi\}$ . So,  $10^{-5}x_y = y = 0.123456$ . So, multiply both sides  $10^5$ ,  $10^5 10^{-5}x_y = 10^5 \cdot 0.123456$ , which gives us that  $x_y = 12345.6$ . However, we know that  $x_y \notin \mathbb{Z}$  and that  $x_y \notin \pi$ , so we have  $x_y \notin \mathbb{Z} \cup \{\pi\}$ , which implies that  $\neg A$ . So,  $A \wedge \neg A$  holds, which gives the contradiction.

Thus,  $f : \mathbb{Z} \cup \{\pi\} \rightarrow \mathbb{R}$  is not onto, which implies that it is not a bijection.

(b)

(i) **No**

Consider  $p = 7$ , and then consider  $x_1 = 2, x_2 = 3$ , which are both in the domain of  $f : \mathbb{N} \setminus \{0\} \rightarrow \{0, \dots, p\}$  with  $2, 3 \in \mathbb{N} \setminus \{0\}$ . However, with  $x_1 = 2, x_2 = 3$ , so  $f(x_1) = p = 7 = 2 \cdot 3 + 1 \equiv 1 \pmod{2}$  and  $f(x_2) = p = 7 = 2 \cdot 3 + 1 \equiv 1 \pmod{3}$ , which means that  $f(x_1) = f(x_2)$  while  $x_1 \neq x_2$ .

Thus,  $f : \mathbb{N} \setminus \{0\} \rightarrow \{0, \dots, p\}$  is not one-to-one by definition, so it's not a bijection.

(ii) **Yes**

First, since  $p > 2$  is prime, so  $p$  is an odd number, and so  $(p+1)/2, (p-1)/2 \in \mathbb{Z}$ . Then, for any arbitrary  $x$  in the domain of  $f : \{(p+1)/2, \dots, p\} \rightarrow \{0, \dots, (p-1)/2\}$ , we have  $(p+1)/2 \leq x \leq p$ . So,  $0 \leq (p-x) \leq \frac{p-1}{2} < x$ , and so  $p-x \in \{0, \dots, (p-1)/2\}$ , which means that  $p-x$  is the only solution. Thus,  $f(x) = p \bmod x = p-x$ .

Proof (one-to-one): Suppose  $f(x_1) = f(x_2)$ , then using our deduction above, so  $p-x_1 = p-x_2$ . Add  $(-p+x_1+x_2)$  to both sides and we have that  $x_2 = x_1$ . So  $f(x_1) = f(x_2) \implies x_1 = x_2$ , so  $f : \{(p+1)/2, \dots, p\} \rightarrow \{0, \dots, (p-1)/2\}$  is injective.

Proof (onto): Now, if  $y \in \{0, \dots, (p-1)/2\}$ , then by our deductions above again, so  $f(p-y) = p-(p-y) = y$ . With  $0 \leq y \leq \frac{p-1}{2}$ , so  $\frac{p+1}{2} \leq (p-y) \leq p$ , which means that  $(p-y) \in \{(p+1)/2, \dots, p\}$ ; in other words,  $(p-y)$  is in the domain of  $f : \{(p+1)/2, \dots, p\} \rightarrow \{0, \dots, (p-1)/2\}$ , which means that  $y$  has a pre-image. Thus, every  $y \in \{0, \dots, (p-1)/2\}$  has a pre-image, so  $f : \{(p+1)/2, \dots, p\} \rightarrow \{0, \dots, (p-1)/2\}$  is onto.

Thus,  $f : \{(p+1)/2, \dots, p\} \rightarrow \{0, \dots, (p-1)/2\}$  is both one-to-one and onto, so it is a bijection.

(c) **No**

Since the domain  $D$  is defined as  $D = \{0, \dots, n\}$ , so its cardinality is  $|D| = n + 1$ , which is finite. Then, since the range is  $\mathcal{P}(D)$ , using Note 10, so its cardinality is  $|\mathcal{P}(D)| = 2^{|D|} = 2^{n+1} > n + 1 = |D|$  for all  $n \in \mathbb{N}$ . We will do a short proof by induction for the claim that  $2^{n+1} > n + 1 \forall n \in \mathbb{N}$ .

Base case ( $n = 0$ ):  $2^1 = 2 > 1$ , so the base case is correct.

Induction Hypothesis: For  $n = k \geq 0$ ,  $2^{k+1} > k + 1$

Inductive Step: Consider  $n = k + 1 \geq 1$ , so  $2^{n+1} = 2^{k+2} = 2 \cdot 2^{k+1}$ . Then, using our induction hypothesis, so  $2^{k+2} = 2 \cdot 2^{k+1} > 2 \cdot (k + 1) = 2k + 2 \geq k + 2 = (k + 1) + 1$ , as desired.

Thus, by the principal of mathematical induction, we have  $2^{n+1} > n + 1 \forall n \in \mathbb{N}$ .

Thus, the cardinality of the domain of  $f : D \rightarrow \mathcal{P}(D)$  is strictly smaller than its range, which means that  $f : D \rightarrow \mathcal{P}(D)$  cannot be surjective. We'll insert a small proof by contradiction to for this claim.

Let  $R$  be the assertion that  $|\mathcal{P}(D)| > |D|$ . Assume that  $f : D \rightarrow \mathcal{P}(D)$  is surjective, then there must exist a function  $g : \mathcal{P}(D) \rightarrow D$  that's injective, which indicates that  $|\mathcal{P}(D)| \leq |D|$ , which implies  $\neg R$ , so  $R \wedge \neg R$  holds, which raises the contradiction.

Therefore,  $f : D \rightarrow \mathcal{P}(D)$  is not surjective, and thus, it cannot be bijective.

(d) **Yes**

Since  $X = 1234567890$ , so  $X$  does not have any repeating digits. Then, since  $X'$  is obtained by randomly shuffling  $X$ , so  $X'$  have the same set of digits as  $X$ , and  $X'$  does not have any repeating digits.

Proof (one-to-one): Suppose  $f(x) = f(y)$  with  $x, y \in \{0, \dots, 9\}$ , then the  $(x + 1)^{th}$  digit of  $X'$  is the same as the  $(y + 1)^{th}$  digit of  $X'$ . Since we have shown earlier that  $X'$  does not have any repeating digits, so this means that  $x + 1 = y + 1$ , and so we have  $x = y$ . So,  $f(x) = f(y) \implies x = y$ , so  $f : \{0, \dots, 9\} \rightarrow \{0, \dots, 9\}$  is injective.

Proof (onto): If  $y \in \{0, \dots, 9\}$  is in the range of  $f$ , then  $y$  is a digit of the original  $X$ , and thus,  $y$  is a digit of  $X'$  by assumption of  $X'$ . Suppose  $y$  is the  $k^{th}$  digit of  $X'$ , so we have that  $k \in \mathbb{Z}, 1 \leq k \leq 10$ . Consider  $f(k - 1)$ , with  $0 \leq (k - 1) \leq 9$ , which means that  $k - 1 \in \{0, \dots, 9\}$  is in the domain. Then, we also have that  $f(k - 1) =$  the  $(k - 1 + 1)^{th} = k^{th}$  digit of  $X'$ , which by our assumption, is equal to  $y$ . So,  $f(k - 1) = y$ , which means that  $y$  has a pre-image. Thus every  $y \in \{0, \dots, 9\}$  has a pre-image, so  $f : \{0, \dots, 9\} \rightarrow \{0, \dots, 9\}$  is onto.

Thus,  $f : \{0, \dots, 9\} \rightarrow \{0, \dots, 9\}$  is both one-to-one and onto, so it is a bijection.

## 2 Counting Tools

(a) Countable

We divide the problem into two cases, where exactly one must be true: (1)  $A, B$  are both finite; or (2)  $A, B$  are not both finite.

Case (1): Given that  $A, B$  are both finite, so we can enumerate the elements of  $A$  as  $a_0, a_1, a_2, \dots, a_m$  and the elements of  $B$  as  $b_0, b_1, \dots, b_n$ . Thus, there is a total of  $(m+1)(n+1)$  different elements of  $A \times B$ , which means that  $A \times B$  is finite, and thus it's countable by definition.

Case (2): Given that  $A, B$  are not both finite (we include the cases where exactly one of them is finite, as it will still be a bijection between  $A \times B$  and  $\mathbb{N}$  when we do the spiral/diagonal enumeration).

Since  $A$  is countable, so we can enumerate the elements of  $A$  like this:  $a_0, a_1, a_2, \dots$ . Similarly, the elements of the countable set  $B$  can be enumerated as  $b_0, b_1, b_2, \dots$ , so we can write  $A \times B$  as:

$$\begin{array}{cccc} (a_0, b_0) & (a_1, b_0) & (a_2, b_0) & \dots \\ (a_0, b_1) & (a_1, b_1) & (a_2, b_1) & \dots \\ (a_0, b_2) & (a_1, b_2) & (a_2, b_2) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Thus, we can enumerate the elements of  $A \times B$ , i.e. create an injection from  $A \times B$  to  $\mathbb{N}$ , by counting the elements of  $A \times B$  in a spiral/diagonal way like this (following the lines and arrows):

Diagram illustrating a sequence of points in a 2D grid:

- Row 0:  $(a_0, b_0) \rightarrow (a_1, b_0) \rightarrow (a_2, b_0) \rightarrow \dots$
- Row 1:  $(a_0, b_1) \leftarrow (a_1, b_1) \leftarrow (a_2, b_1) \leftarrow \dots$
- Row 2:  $(a_0, b_2) \leftarrow (a_1, b_2) \leftarrow (a_2, b_2) \leftarrow \dots$

Arrows indicate the sequence of points, showing a path from  $(a_0, b_0)$  to  $(a_1, b_1)$  to  $(a_2, b_2)$ .

Thus, there is an injection  $f : A \times B \rightarrow \mathbb{N}$  as no two elements lie in the same position and by the fact that this mapping certainly maps every element of  $A \times B$  to a natural number, because every such element appears somewhere (exactly once) in the grid, and the spiral hits every point in the grid.

On the other hand, due to our counting strategy (no double-counting) as well as the fact that each element of  $A \times B$  is unique, so there's also an injection  $g : \mathbb{N} \rightarrow A \times B$  just by following our counting strategy. Thus, using the Cantor-Bernstein theorem and our Note, so there's a **bijection**  $h : A \times B \rightarrow \mathbb{N}$ , which by definition, shows that  $A \times B$  is countable.



(b) Countable

We divide the problem into two cases, where exactly one must be true: (1)  $A, B_i$  are all finite; or (2)  $A, B_i$  are not all finite.

Case (1): Given that  $A, B_i$  are all finite, so we can enumerate the elements of  $A$  as  $a_0, a_1, a_2, \dots, a_m$ . Thus,  $\cup_{i \in A} B_i = B_{a_0} \cup B_{a_1} \cup B_{a_2} \cup \dots \cup B_{a_m}$ . Then, we can enumerate of each  $B_{a_j}$  that has  $n_j \in \mathbb{N}$  elements as  $b_{j,0}, b_{j,1}, \dots, b_{j,n_j-1}$ . Thus, there's a total of  $\sum_{i=0}^m n_i$  elements in  $\cup_{i \in A} B_i$ , and this is a finite number. Thus,  $\cup_{i \in A} B_i$  is finite, and thus it's countable by definition.

Case (2): Given that  $A, B$  are not both finite (again, we include the case where exactly one of them are finite, as it will still be a bijection between  $\cup_{i \in A} B_i$  and  $\mathbb{N}$  when we do the spiral/diagonal enumeration).

Since  $A$  is countable, so we can enumerate the elements of  $A$  like this:  $a_0, a_1, a_2, \dots$ . Similarly, the elements of any of the countable set  $B_{a_j}$  can be enumerated as  $b_{j,0}, b_{j,1}, b_{j,2}, \dots$ . So we can write  $\cup_{i \in A} B_i = (B_{a_0} \cup B_{a_1} \cup B_{a_2} \cup \dots)$  as:

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$	...
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	...
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$	...
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Thus, we can enumerate the elements of  $\cup_{i \in A} B_i$ , i.e. create an injection from  $\cup_{i \in A} B_i$  to  $\mathbb{N}$ , by counting the elements of  $\cup_{i \in A} B_i$  in a spiral/diagonal way like this (following the lines and arrows):

	0	1	5	6	
	$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$	...
2	$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	...
3	$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$	...
4	$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$	...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Thus, there is an injection  $f : \cup_{i \in A} B_i \rightarrow \mathbb{N}$  as no two elements lie in the same position and by the fact that this mapping certainly maps every element of  $\cup_{i \in A} B_i$  to a natural number, because every such element appears somewhere (exactly once) in the grid, and the spiral hits every point in the grid.

On the other hand, due to our counting strategy (no double-counting) as well as the fact that each element of  $\cup_{i \in A} B_i$  is unique, so there's also an injection  $g : \mathbb{N} \rightarrow \cup_{i \in A} B_i$  just by following our counting strategy. Thus, using the Cantor-Bernstein theorem and our Note, so there's a bijection  $h : \cup_{i \in A} B_i \rightarrow \mathbb{N}$ , which by definition, shows that  $\cup_{i \in A} B_i$  is countable.

(c) Uncountable

We use the Cantor's Diagonalization Proof:

Let  $\mathcal{F}$  be the set of all functions  $f$  from  $\mathbb{N}$  to  $\mathbb{N}$  such that  $f$  is non-decreasing. We can represent a function  $f \in \mathcal{F}$  as an infinite sequence  $(f(0), f(1), \dots)$ , where the  $i^{th}$  element is  $f(i)$ . Suppose towards a contradiction that there is a bijection from  $\mathbb{N}$  to  $\mathcal{F}$  where we list the functions  $f$  of  $\mathcal{F}$  in increasing order (i.e., Let  $x < y, x, y \in \mathbb{N}$ , then for the  $x^{th}$  and  $y^{th}$  enumerated function,  $f_x$  and  $f_y$ , we have that  $f_x(i) \leq f_y(i) \forall i \in \mathbb{N}$ ):

$$\begin{aligned} 0 &\iff (f_0(0), f_0(1), f_0(2), f_0(3), \dots) \\ 1 &\iff (f_1(0), f_1(1), f_1(2), f_1(3), \dots) \\ 2 &\iff (f_2(0), f_2(1), f_2(2), f_2(3), \dots) \\ 3 &\iff (f_3(0), f_3(1), f_3(2), f_3(3), \dots) \\ &\vdots \end{aligned}$$

Consider the function  $g : \mathbb{N} \rightarrow \mathbb{N}$  where  $g(i) = f_i(i) + 1 \forall i \in \mathbb{N}$ . We claim that  $g$  is a valid non-decreasing function from  $\mathbb{N}$  to  $\mathbb{N}$  that is not in our list of functions  $f$ . We provide a short proof by contradiction for this claim.

Suppose, for a contradiction, that  $g$  is in our list of functions, then let  $g$  be the  $n^{th}$  function, i.e.  $g = f_n$ . So,  $g(\cdot) = f_n(\cdot)$ . However,  $g(\cdot)$  and  $f_n(\cdot)$  differ in the  $n^{th}$  number, since  $g(n) = f_n(n) + 1 \neq f_n(n)$ , which implies that  $g \neq f_n$ , which gives the contradiction.

Thus, by the Cantor's Diagonalization Proof, we have that the set of all functions  $f$  from  $\mathbb{N}$  to  $\mathbb{N}$ , such that  $f$  is non-decreasing, is uncountable.

Q.E.D.

(d) Countable

Let  $\mathcal{F}$  be the set of all functions  $f$  from  $\mathbb{N}$  to  $\mathbb{N}$  such that  $f$  is non-increasing. We can represent a function  $f \in \mathcal{F}$  as an infinite sequence  $(f(0), f(1), \dots)$ , where the  $i^{th}$  element is  $f(i)$ . Consider the following representation of all elements (functions) of  $\mathcal{F}$ :

$$\mathcal{F} = \cup_{i_1 \in \mathbb{N}} (i_1, \dots) = (0, \dots) \cup (1, \dots) \cup (2, \dots)$$

i.e. (one) infinite sequence that starts with 0  $\cup$  infinite sequences that starts with 1  $\cup$  infinite sequences that starts with 2  $\cup \dots$

Then, any infinite sequence that starts with  $k$  could be enumerated/represented as:

$$\cup_{i_2} (k, i_2, \dots) = (k, 0, \dots), (k, 1, \dots), (k, 2, \dots), \dots$$

i.e. infinite sequence that starts with  $k, 0 \cup$  infinite sequence that starts with  $k, 1 \cup$  infinite sequence that starts with  $k, 2 \cup \dots$

Continuing the argument, we could enumerate each possibility of the current element by representing them as a union of infinite sequences that “identifies” the next unidentified (yet) element.

Since each step of enumeration where we “identify” one more element in the infinite sequence is a union of  $\mathbb{N}$ , which is countable, sets of countable elements by recursion, so each “subset” of the enumeration is countable by the results obtained in 2(b). Therefore,  $\mathcal{F}$ , the set of all functions  $f$  from  $\mathbb{N}$  to  $\mathbb{N}$  such that  $f$  is non-increasing, is also countable as it's also the union of countable sets ( $\mathbb{N}$ ) of countable elements...

Q.E.D.

(e) Countable

Let  $\mathcal{F}$  be the set of all bijective functions  $f$  from  $\mathbb{N}$  to  $\mathbb{N}$ . Again, We can represent a function  $f \in \mathcal{F}$  as an infinite sequence  $(f(0), f(1), \dots)$ , where the  $i^{th}$  element is  $f(i)$ . Consider the following listing of all elements (functions) of  $\mathcal{F}$ :

$$\begin{aligned}
0 &\iff (0, 1, 2, 3, 4, \dots) \\
1 &\iff (1, 0, 2, 3, 4, \dots) \\
2 &\iff (0, 2, 1, 3, 4, \dots) \\
3 &\iff (1, 2, 0, 3, 4, \dots) \\
4 &\iff (2, 0, 1, 3, 4, \dots) \\
5 &\iff (2, 1, 0, 3, 4, \dots) \\
6 &\iff (0, 1, 3, 2, 4, \dots) \\
7 &\iff (0, 2, 3, 1, 4, \dots) \\
8 &\iff (0, 3, 1, 2, 4, \dots) \\
9 &\iff (0, 3, 2, 1, 4, \dots) \\
10 &\iff (1, 0, 3, 2, 4, \dots) \\
11 &\iff (1, 2, 3, 0, 4, \dots) \\
12 &\iff (1, 3, 0, 2, 4, \dots) \\
13 &\iff (1, 3, 2, 0, 4, \dots) \\
14 &\iff (2, 0, 3, 1, 4, \dots) \\
15 &\iff (2, 1, 3, 0, 4, \dots) \\
16 &\iff (2, 3, 0, 1, 4, \dots) \\
17 &\iff (2, 3, 1, 0, 4, \dots) \\
18 &\iff (3, 0, 1, 2, 4, \dots) \\
19 &\iff (3, 0, 2, 1, 4, \dots) \\
20 &\iff (3, 1, 0, 2, 4, \dots) \\
21 &\iff (3, 1, 2, 0, 4, \dots) \\
22 &\iff (3, 2, 0, 1, 4, \dots) \\
23 &\iff (3, 2, 1, 0, 4, \dots) \\
&\vdots
\end{aligned}$$

Thus, we are listing out the elements of  $\mathcal{F}$  in an “increasing” order, as we would list out all possible permutations of the first  $k$  numbers (while leaving  $f(n) = n$  for all  $n > k, n \in \mathbb{N}$ ) before having the  $(k + 1)^{th}$  number being “switched out of its place”, as demonstrated by the enumerating technique above.

Thus, we can conclude that this mapping certainly maps every element of  $\mathcal{F}$  to a natural number, which implies that there is an injection  $f : \mathcal{F} \rightarrow \mathbb{N}$  as no two elements lie in the same position. Therefore, there is a bijection between  $\mathcal{F}$  and some subset  $C \subseteq \mathbb{N}$  of  $\mathbb{N}$ , which by definition, means that  $\mathcal{F}$ , the set of all bijective functions  $f$  from  $\mathbb{N}$  to  $\mathbb{N}$ , is countable.

Q.E.D.

### 3 Impossible Programs

(a) Cannot exist

We proceed with a proof by contradiction and use the reduction technique. Suppose, for a contradiction, that such a program  $P$  exists. Using the given information, so the program looks like this:

```
P(F, x, y)
  if F(x) = y, then return True
  else, return False
```

Thus, this function could be used as a subroutine to solve the Halting Problem where we construct an algorithm like this:

```
Halt(Program, x)
  Construct a program Program' that, on any input, returns Program(x)
  return P(Program', x, Program(x))
```

where  $Program'$  can be constructed rather easily (following Note 11):

```
Program'(y)
  return Program(x)
```

So, we can see that  $Program'(x)$  returns  $Program(x)$  if and only if  $Program(x)$  halts. Thus, by assumption of the program  $P$  in the problem, so  $P(Program', x, Program(x))$  is True if and only if  $Program(x)$  halts.

Therefore, if we have such a program  $P$ , then Halt will correctly solve the Halting Problem. Since we know there cannot be such a program Halt (the Halting Problem is uncomputable), so we conclude with contradiction, which means that this program  $P$  does not exist.

Q.E.D.



(b) Cannot exist

We proceed with a proof by contradiction and use the reduction technique. Suppose, for a contradiction, that such a program  $P$  exists. Using the given information, so the program looks like this:

$P(F, G)$

If for all  $x$ , either both  $F(x)$  and  $G(x)$  halts or both  $F(x)$  and  $G(x)$  loops, then return True  
else, return False

Thus, this function could be used as a subroutine to solve the Halting Problem where we construct an algorithm like this:

$\text{Halt}(\text{Program}, x)$

Construct a program,  $\text{TestyHalt}$ , that halts on input  $x$  (i.e. returns 0 directly on input  $x$ ),  
and returns  $\text{Program}(x)$  otherwise  
return  $P(\text{Program}, \text{TestyHalt})$

where  $\text{TestyHalt}$  can be constructed rather easily:

$\text{TestyHalt}(y)$

if  $y == x$ , then return 0 (halts)  
else, return  $\text{Program}(x)$

So, we can see that  $\text{Program}$  and  $\text{TestyHalt}$  are constructed to halt on the same inputs for all inputs except  $x$ , which is the only input we would need to examine. Then, since  $\text{TestyHalt}$  always halts on input  $x$ , so  $P(\text{Program}, \text{TestyHalt})$  is True if and only if  $\text{Program}(x)$  halts just like  $\text{TestyHalt}(x)$  does.

Therefore, if we have such a program  $P$ , then Halt will correctly solve the Halting Problem. Since we know there cannot be such a program Halt (the Halting Problem is uncomputable), so we conclude with contradiction, which means that this program  $P$  does not exist.

Q.E.D.

## 4 Undecided?

### (a) $nk$

Since we're told, for this part specifically, to consider the machine has  $n$  (different) states and the algorithm has  $k$  (different) instructions, so there are  $nk$ -many different state-instruction combinations.

We first observe that each of the  $j$  returned by the algorithm  $\mathcal{A}$  corresponds to a distinct instruction. So, I'll denote a single output of  $\mathcal{A}$ , which is a machine state  $c$  and a number  $j$ , as a state-instruction combination.

Since each different state-instruction combination would lead to a new computation, and also since two identical state-instruction combination would lead to repeated computation, so an algorithm of  $k$  instructions can perform a maximum of  $nk$ -many iterations on an  $n$ -state machine without repeating any computation.

This is possible by having each of these iterations returning a new state-instruction combination (a previously unused pair of instruction number  $j$  and machine state  $c$ ) that hasn't been computed before. In other words, consider the rotational situation where each of the computations  $i_j(s_k)$  would return  $(i_j, s_{k+1})$  for all  $1 \leq k < n$ , and  $i_j(s_n)$  would return  $(i_{j+1}, s_1)$  for all  $0 \leq j < k - 1$ , and finally, let  $i_{k-1}(s_n)$  return  $(i_0, s_1)$ , the first combination. Here, no repeating computation exists for the first  $nk$  iterations of algorithm  $\mathcal{A}$ .

### (b) Direct Proof

We proceed by first showing that if the algorithm is still running after  $nk + 1$  iterations, it will loop forever.

As proved in part (a), the maximum number of iterations that doesn't repeat any computation is  $nk$ , which implies that if the algorithm  $\mathcal{A}$  is still running after  $nk + 1$  iterations, then by the Pidgeon-hole Principal,  $\mathcal{A}$  must have repeated computations somewhere.

Let the repeated computation be at these two iterations  $k_i, k_j$  where  $1 \leq k_i < k_j \leq nk + 1$ . So the computations at  $k_i^{th}$  and  $k_j^{th}$  are repeated, or the same. Then, consider the set of  $(j - i)$  iterations  $S = \{k_i, k_{i+1}, \dots, k_{j-1}\}$ . This would be a cycle as we reach the  $k_j^{th}$  iteration, which means that the set of  $(j - i)$  iterations  $S' = \{k_j, k_{j+1}, \dots, k_{2j-i-1}\}$  is exactly the same as the set  $S$ , thus indicating that a loop must have occurred, which implies that the algorithm  $\mathcal{A}$  would loop forever if the algorithm is still running after  $nk + 1$  iterations.

Then, since  $n, k \in \mathbb{Z}^+$ , so  $2n^2k^2 = n^2k^2 + n^2k^2 \geq nk + 1$ , and thus, the algorithm  $\mathcal{A}$  would loop forever if the algorithm is still running after  $2n^2k^2$  iterations, as desired.

Q.E.D.

### (c) No, it doesn't.

Algorithm designed using our results from part (a) and (b):

$Halts\_Here(\mathcal{A}, x) :$

if algorithm  $\mathcal{A}$  halts on input  $x$  within  $(nk + 1)$  iterations, then return "yes"

if algorithm  $\mathcal{A}$  does not halt on input  $x$  within  $(nk + 1)$  iterations, then return "no"

This does not contradict the undecidability of the Halting problem because it's checking whether algorithm  $\mathcal{A}$  halts within a finite number ( $nk$ ) of iterations, where the Halting problem isn't, which makes the difference. Moreover, we actually proved in Discussion that checking whether a program halts within a finite number of iterations is actually computable.

## 5 Clothing Argument

(a) 10,000

Based on the given information, we can use the First Rule of Counting, so there are  $10 \cdot 10 \cdot 10 \cdot 10 = 10,000$  distinct outfits.

(b) 600

Since we want to wear exactly 2 out of the 4 categories, so we first use the Second Rule of Counting, and we're sampling without replacement, which gives us  $\frac{4!}{(4-2)! \cdot 2!} = \frac{24}{2 \cdot 2} = 6$  ways.

Thus, we can then use the First Rule of Counting, multiplying by the previous number, so there are  $6 \cdot 10 \cdot 10 = 600$  distinct outfits when choosing from exactly two categories.

(c) 5040

Since we want to pick exactly 4 out of the 10 hats, so we first use the Second Rule of Counting, and we're sampling without replacement, which gives us  $\binom{10}{4} = \frac{10!}{(10-4)! \cdot 4!} = 210$  ways.

Thus, we can then use the First Rule of Counting to line them up on a wall, and we're sampling without replacement, multiplying by the previous number, so there are  $210 \cdot 4! = 5040$  of hanging four of the ten hats.

(d) 210

Since we want to pack exactly 4 out of the 10 hats, so we use the Second Rule of Counting, and we're sampling without replacement, which gives us  $\binom{10}{4} = \frac{10!}{(10-4)! \cdot 4!} = 210$  different ways.

We can explain this number in terms of our answer in part (c) since there exists an 24-to-1 function  $f$  from hanging hats (part c) to packing hats (part d) as we discussed in the second paragraph of part (c), which shows that after picking out the 4 out of 10 hats, then there're  $4! = 24$  ways for hanging them up on a wall. Thus,  $f$  will map 24 elements in the domain (the set of hanging ordered 4-hat subsets of the 10 hats) of the function to 1 element in the range (the set of packing 4-hat subsets of the 10 hats) of the function, so this number is  $\frac{1}{24}$  of our answer to part (c), which is correct with  $5040 \cdot \frac{1}{24} = 210$ .

(e) 10

Since we want to pack exactly 3 hats, and for each color, we have three or more of them (that are indistinguishable), so this is a problem of sampling with replacement, but where order does not matter. We are picking 3 hats out of 3 different colors of hats, and using the formula from Note 12, there are  $\binom{3+3-1}{3} = \frac{5!}{(5-3)! \cdot 3!} = \frac{120}{2 \cdot 6} = 10$  distinct sets of 3-hat subsets.