CS054: Countability

The goal of this worksheet is to give you practice with cardinality, countability, and uncountability. It's not for a grade—no need to turn it in! I'll post solutions, but you'll get the most out of it if you don't peek.

1. Write an injective function from `bool` to RPS.

   Solution: $f(\top) = \mathsf{rock}$ and $f(\bot) = \mathsf{scissors}$ is one.

2. How many different injective functions from `bool` to RPS are there?

   Solution: There are $P(3, 2) = 6$ possibilities.

3. Write a surjective function from RPS to `bool`.

   Solution: $f(\mathsf{rock}) = \top$, and $f(\mathsf{scissors}) = f(\mathsf{paper}) = \bot$ is one.

4. How many surjective functions from RPS to `bool` are there?

   Solution: Because $|\mathsf{RPS}| = 3$ and $|\texttt{bool}| = 2$, one element of `bool` will need to be hit twice.

   If we hit $\top$ twice, then there are $C(3, 2) = 3$ possible functions. If we hit $\bot$ twice, then there are 3 possible functions. So there are 6 in total.

5. (a) Give an example of finite sets A and B where $|A \cup B| = |A| + |B|$.

Solution: Take, say, $A = \texttt{bool}$ and $B = \mathsf{RPS}$, where $A \cup B = \{\top, \bot, \mathsf{rock}, \mathsf{paper}, \mathsf{scissors}\}$ and $|A \cup B| = 5 = 2 + 3 = |A| + |B|$.

(b) Give an example of finite sets A and B where $|A \cup B| \neq |A| + |B|$.

Solution: Take, say, $A = \texttt{bool}$ and $B = \{\top\}$, where $A \cup B = A$, so $|A \cup B| = 2 \neq 2 + 1 = |A| + |B|$.

(c) Give a condition on finite sets A and B that characterizes when $|A \cup B| = |A| + |B|$. No need to prove it (but good to think about how you might!).

Solution: $A \cap B = \emptyset$, i.e., A and B are disjoint.

6. Prove that if A is countable, then so is $\texttt{option}(A) = \{\texttt{some}(a) \mid a \in A\} \uplus \{\texttt{none}\}$.

Solution:

Using injection: If A is countable, there exists $f : A \to \mathbb{N}$, injective. To show $\texttt{option}(A)$ is countable, we can define a 'lifted' $f' : \texttt{option}(A) \to \mathbb{N}$ as follows:

$$f'(\texttt{none}) = 0 \qquad f'(\texttt{some}(a)) = 1 + f(a)$$

We must show that f' is injective. Let x and y be given such that $f'(x) = f'(y)$; we must show $x = y$.

If $x = \texttt{none}$, then $f'(x) = 0$, and so $f'(y) = 0$. It must then be the case that y is also $\texttt{none}$, since adding one to a natural can't yield 0.

On the other hand, if $x = \texttt{some}(a)$, then $f'(x) = 1 + f(a)$, i.e., $f'(x) \neq 0$. So it can't be the case that $y = \texttt{none}$, so $y = \texttt{some}(b)$. Therefore $f(y) = 1 + f(b)$. If $1 + f(a) = 1 + f(b)$, then $f(a) = f(b)$—and if f is injective, $a = b$, so $x = \texttt{some}(a) = \texttt{some}(b) = y$.

Using surjection: If A is countable, there exists $g : \mathbb{N} \to A$, surjective. To show $\texttt{option}(A)$ is countable, we can define a 'lifted' $g' : \mathbb{N} \to \texttt{option}(A)$.

$$g'(0) = \texttt{none} \qquad g'(S(n)) = \texttt{some}(g(n))$$

We must show that g' is surjective. Let $x \in \texttt{option}(A)$ be given; we find a number n such that $g'(n) = x$.

If $x = \texttt{none}$, choose $n = 0$.

If $x = \texttt{some}(a)$, then there must be some n' such that $g(n') = a$ (because g is surjective). So let $n = S(n')$, where:

$$g'(n) = g'(S(n')) = \texttt{some}(g(n')) = \texttt{some}(a) = x.$$

Pro tip: for practice, try to prove this using both injection and surjection!

7. The English alphabet has 26 letters, A through Z. Prove that the set of possible words—i.e., one or more letters—is countable.

   (This is a hard question. Hint: can you use primes in a creative way? Feel free to assume useful facts about prime factoring.)

Solution: Let each letter correspond to a prime number with a function p: $p(A) = 2$, $p(B) = 3$, and so on through $p(Y) = 97$ and $p(Z) = 101$.

Each nonempty word is of the form $c_1 \dots c_n$, for $n \geq 1$ and letters c_i. We define $f : \mathsf{Word} \to \mathbb{N}$ as follows:

$$f(c) = p(c) \qquad f(c_1 \cdots c_n) = p(c_1)^{f(c_2 \cdots c_n)}$$

We claim that f is injective. We prove that each word is mapped to a distinct number by induction on n, the length of the word, leaving the word itself general. (Alternatively, we could consider words to be lists and go by induction on the word itself. Either works.)

If $n = 0$, then it's not a valid word.

If $n = 1$, then $f(c) = p(c)$, i.e., a single-letter word just maps to the prime for its one letter. Each of these are distinct.

If $n = n' + 1$, then let $c_1 \cdot c_n$ be given of length n; we know $f(c_1 \cdots c_n) = p(c_1)^{f(c_2 \cdot c_n)}$. We must show that this word is mapped to a distinct number; our IH shows that every word of length n' is mapped to a distinct number.

First, no word starting with a letter other than c_1 can be equal to $p(c_1)^{f(c_2 \cdot c_n)}$, because each prime has distinct powers with just one prime factor.

Next, by the IH we know that $f(c_2 \cdot c_n)$ is distinct from every other number produced by f—so $c_1 \cdots c_n$ is unique in being the$f(c_2 \cdot c_n)$-th power of $p(c_1)$, the prime for c_1. QED

8. Prove that $\texttt{bt}(\mathbb{N})$ is countable.

   (Hint: first do question (7); then try to use primes.)

Solution: Let $f : \texttt{bt}(\mathbb{N}) \to \mathbb{N}$ be defined as follows:

$$f(\texttt{empty}) = 2 \qquad f(\texttt{node}(l, n, r)) = 3^{f(l)}5^n7^{f(r)}$$

We must show that f is injective. Let $t_1, t_2 \in \texttt{bt}(\mathbb{N})$ be given such that $f(t_1) = f(t_2)$; we must show that $t_1 = t_2$. We go by induction on t_1, leaving t_2 general.

($t_1 = \texttt{empty}$) Here $f(t_1) = 2$. To have $f(t_2) = 0$, we must have $t_2 = \texttt{empty}$, since f's `node` case is never even.

($t_1 = \texttt{node}(l_1, n_1, r_1)$) Here $f(t_1) = 3^{f(l_1)}5^{n_1}7^{f(r_1)}$. We must show that quantity equal to $f(t_2)$; our IH gives us injectivity for f on l_1 and r_1.

First, it can't be the case that $t_2 = \texttt{empty}$, since $f(t_1)$ is odd. So $t_2 = \texttt{node}(l_2, n_2, r_2)$ and $f(t_2) = 3^{f(l_2)}5^{n_2}7^{f(r_2)}$.

Since 3, 5, and 7 are distinct primes, the only way we could have $3^{f(l_1)}5^{n_1}7^{f(r_1)} = 3^{f(l_2)}5^{n_2}7^{f(r_2)}$ is to have each prime factor be the same, i.e., $3^{f(l_1)} = 3^{f(l_2)}$ and $5^{n_1} = 5^{n_2}$ and $7^{f(l_1)} = 7^{f(l_2)}$.

Since exponentiation is injective, we have $f(l_1) = f(l_2)$ and $n_1 = n_2$ and $f(r_1) = f(r_2)$. The IH on l_1 then yields $l_1 = l_2$; similarly, the IH on l_2 yields $r_1 = r_2$. So $t_1 = \texttt{node}(l_1, n_1, r_1) = \texttt{node}(l_2, n_2, r_2) = t_2$, as desired. QED

9. In light of questions (6), (7), and (8), give a general argument (but not a proof) that every inductive data type over countable components is countable.

Solution: You can map each constructor to a product of distinct primes, as we did for $\texttt{bt}(\mathbb{N})$. Empty constructors are just their own prime (e.g., $f(\texttt{empty}) = 2$) while constructors with arguments assign primes for each argument and raise them to some recursive power (e.g., $f(\texttt{node}(l, n, r)) = 3^{f(l)}5^n7^{f(r)}$).

In the case for $\texttt{bt}(\mathbb{N})$, we didn't have to convert the n in a `node`, but we of course could do a similar encoding for trees (or whatever) holding anything else.

The core idea of these proofs is due to Kurt Gödel, one of the most important people in 20^{th} Century math and logic; the technique of using primes to characterize alternatives. is called *Gödel numbering*.

10. (a) Give an example of a set A where $A \to \mathbb{N}$ is countable. No need to prove it (but it's good practice, of course!).

Solution: $A = \emptyset$ is an easy one—there are no such functions. $A = \mathsf{unit}$ is good, too: there's one function for each $n \in \mathbb{N}$, the constant-n function. `bool` works, as does RPS...

(b) Give an example of a set A where $A \to \mathbb{N}$ is countable. No need to prove it (but it's good practice, of course!).

Solution: We've already seen $\mathbb{N} \to \mathbb{N}$ is uncountable, so $A = \mathbb{N}$ is a good one. So is $A = \mathbb{Z}$ or $A = \texttt{option}(\mathbb{N})$, say.

(c) Characterize when $A \to \mathbb{N}$ is countable. No need to prove it (but how would you?).

Solution: $A \to \mathbb{N}$ is countable when A is finite. Even the smallest infinite set—$A = \mathbb{N}$ itself—yields an uncountable set of functions.
If A is a finite set, I would prove that $A \to \mathbb{N}$ is countable by induction on $|A|$. The base case, $|A| = 0$ is easy, since $A = \emptyset$. In the inductive case, we can distinguish a new, $n + 1$st element. Use the IH to find that we're countable without that element, and then copy the argument in question (6) to add our distinguished element.

11. Prove that the complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ are uncountable.

Solution: We can prove it most easily via containment: $a + 0 \cdot i$ is a complex number, i.e., $a \in \mathbb{R}$ implies $a \in \mathbb{C}$, so $|\mathbb{R}| \leq |\mathbb{C}|$. Since $\mathbb{R}$ is uncountable, so is $\mathbb{C}$.

12. Prove that $\mathbb{N} \to \texttt{base}$ is uncountable.

Solution: By diagonalization.

Suppose for a contradiction that $\mathbb{N} \to \texttt{base}$ was countable—in which case there must exist a surjection $f : \mathbb{N} \to (\mathbb{N} \to \texttt{base})$.

Define the diagonalization gadget $d(n) = \texttt{complement}(f(n)(n))$, i.e., d looks up the nth function in f, calls it on n, and then complements the result.

Since f is surjective, there must exist some m such that $f(m) = d$. What, then, is $d(m)$? We have:

$$\begin{aligned} d(m) &= \texttt{complement}(f(m)(m)) \\ &= \texttt{complement}(d(m)) \end{aligned}$$

But there is no $b \in \texttt{base}$ such that $b = \texttt{complement}(b)$—a contradiction. QED