A note on countability

Philipp Festerling

November 2012

Preliminaries

This note contains solutions to all exercises from the Exercise Book dealing with countability (Exercise Book: Problems 9 to 12). You are welcome to report any error.

Before beginning solving the exercises, two introductory remarks are necessary. Firstly, in Problem 9 we will use the fact that any subset of a finite set is finite. You will probably be surprised that proving this apparently quite intuitive result requires some amount of work. According to agreement with Niels Jørgen, we do not need to go through this formal proof. If you are interested, however, you find a sketch of the proof in the appendix to this note. Secondly, Definition 0.8 of the lecture notes requires the existence of a bijection $f : \mathbb{N} \to A$ for a set A to be countable. In some cases, however, you may end up with showing the existence of a bijection $g : A \to \mathbb{N}$. Since g is a bijection, the inverse $g^{-1} : \mathbb{N} \to A$ exists, and this inverse g^{-1} is a bijection of $\mathbb{N}$ with A, showing that A is countable. You find a proof of this result in the appendix to this note. Similarly, you may end up with showing the existence of a bijection $h : A \to B$ where A is countable. Hence, there exists a bijection $g : \mathbb{N} \to A$. The composition $h \circ g : \mathbb{N} \to B$ such that $h \circ g(n) = h(g(n))$ for $n \in \mathbb{N}$ is then a bijection of $\mathbb{N}$ with B, showing that B is countable. The straightforward proof of this result is left as a voluntary exercise. Now we are ready to have a look on the first of the exercises about countability.

Exercise Book Problem 9

1.

Let A be an infinite subset of $\mathbb{N}$ and assume for the moment

$$A_n = \{m \in A : m > n\} = \emptyset.$$

for some $n \in \mathbb{N}$. Then $m \leq n$ for all $m \in A$ implying that A is a subset of the finite set $\{1, ..., n\}$. By the first introductory remark, A was finite contradicting the assumption that A is infinite. Hence $A_n \neq \emptyset$ for all $n \in \mathbb{N}$.

2.

Let $f : \mathbb{N} \to A$ be defined as in the exercise. If $k \in \mathbb{N}$ then $f(k)$ is the first element of $A_{f(k-1)} = \{m \in A : m > f(k-1)\}$ implying that $f(k) > f(k-1)$. Repeating this argument shows that $f(k) > f(k-1) > ... > f(1)$. Assume then $m > n$. It follows that $f(m) > f(n)$ showing that f is *one-to-one*. To show that f is *onto*, let a be an arbitrary element of A. The image set $f(\mathbb{N})$ cannot be included in the set $\{1, ..., a\}$ since we just have shown that f is *one-to-one* implying that $f(\mathbb{N})$ is infinite. There exists thus an $n \in \mathbb{N}$ such that $f(n) > a$. Let m be the smallest element of $\mathbb{N}$ such that $f(m) \geq a$. It follows that $f(k) < a$ for all $k < m$ and $a \in A \setminus f(\{1, ..., m-1\})$. On the contrary, $f(m)$ is defined to be the first element of $A_{f(m-1)}$ implying that $f(m)$ is the smallest element of the set $A \setminus f(\{1, ..., m-1\})$ which in turn implies that $f(m) \leq a$. Putting both inequalities together results in $f(m) = a$. Hence, $f : \mathbb{N} \to A$ is a bijection of $\mathbb{N}$ with A and by Definition 0.8 follows that A is countable.

3.

If B is a nonempty subset of $\mathbb{N}$, then B is either finite or infinite. If it is infinite, the previous result shows that B is countable. Thus B is at most countable.

4.

Let X be an arbitrary countable set and let Y be an nonempty subset of X. By Definition 0.8, there is an injection g of X into $\mathbb{N}$ and the restriction of $g|_Y$ on Y is an injection of Y into $\mathbb{N}$. If one changes the range of $g|_Y$, one can obtain a bijection of Y with a subset of $\mathbb{N}$. The previous result shows then that Y is at most countable.

Exercise Book Problem 10

Consider following function $g : \mathbb{Z} \to \mathbb{N}$ such that

$$g : k \in \mathbb{Z} \mapsto \begin{cases} 2k & \text{if } k > 0 \\ 2|k| + 1 & \text{if } k \leq 0 \end{cases}$$

Let n be an arbitrary element of $\mathbb{N}$. If n is even, then there exists $k \in \mathbb{Z}$ where $k = \frac{n}{2}$ such that $g(k) = n$. If n is odd, then there exixts $l \in \mathbb{Z}$ where $l = -\frac{n-1}{2}$ such that $g(l) = n$. This shows that g is *onto*. To show that g is *one-to-one*, assume that $g(k) = g(l)$ where $k, l \in \mathbb{Z}$. Then either $2k = 2l$ or $2|k| + 1 = 2|l| + 1$. In either case, $k = l$. Hence, g is a bijection of $\mathbb{Z}$ with $\mathbb{N}$ showing that $\mathbb{Z}$ is countable.

Exercise Book Problem 11

Let $\mathbb{N} \times \mathbb{N} = \{(m, n) : m \in \mathbb{N}, n \in \mathbb{N}\}$ and let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined such that

$$f((m,n)) = 2^m 3^n.$$

1.

Assume $f((m,n)) = f((l,k))$ where $(m,n),(l,k) \in \mathbb{N}\times\mathbb{N}$. If $m < l$ then

$$3^n = 2^{l-m}3^k$$

contradicting the fact that 3^n is an odd number for all $n = 1,2,3,...$. Hence $m = l$ and $3^n = 3^k$. If $n < k$ then $1 = 3^{k-n}$ leading again to a contradiction. Hence $n = k$ and $(m,n) = (k,l)$. This shows that f is an injection of $\mathbb{N}\times\mathbb{N}$ into $\mathbb{N}$.

2.

If one changes the range of f, one can obtain a bijection of $\mathbb{N}\times\mathbb{N}$ with a subset of $\mathbb{N}$. Call this subset of $\mathbb{N}$ for B. By part 3 of Problem 9 follows that $\mathbb{N}\times\mathbb{N}$ is at most countable. The set B, however, must necessarily be infinite since f is an injection showing that $\mathbb{N}\times\mathbb{N}$ is countable.

3.

Let A and B be two arbitrary countable sets and consider the set $A \times B = \{(a,b) : a \in A, b \in B\}$. There exist two bijections $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$. Define the function $h : A\times B \to \mathbb{N}\times\mathbb{N}$ such that $h((a,b)) = (f(a), g(b))$. Assume $h((a,b)) = h((c,d))$ where (a,b) and (c,d) are arbitrary elements of $A\times B$. Then $(f(a), g(b)) = (f(c), g(d))$ implying that $f(a) = f(c)$ and $g(b) = g(d)$. Since both f and g are *one-to-one*, it follows that $a = c$ and $b = d$ and thus $(a,b) = (c,d)$. This shows that h is *one-to-one*. To show that h is *onto* assume $(n,m) \in \mathbb{N}\times\mathbb{N}$. Since f is *onto*, there exists an $a \in A$ such that $f(a) = n$. Similarly, there exists $b \in B$ such that $g(b) = m$. Hence, there exists an $(a,b) \in A \times B$ such that $h((a,b)) = (n,m)$ showing that h is a bijection of $A \times B$ with $\mathbb{N}\times\mathbb{N}$. Since $\mathbb{N}\times\mathbb{N}$ is countable, $A \times B$ is countable.

Exercise Book Problem 12

1.

Let $\mathbb{Q}$ be the set of rational numbers. Let A be the set defined as

$$A = \{(m,n) \in \mathbb{Z}\times\mathbb{N} : \gcd(m,n) = 1\}.$$

Since both $\mathbb{Z}$ and $\mathbb{N}$ are countable sets, the product $\mathbb{Z}\times\mathbb{N}$ is countable by part 3 of problem 11. Let $m = 21$ and $n = 10$. Then $\gcd(21,10) = 1$ showing that A is a nonempty subset of $\mathbb{Z}\times\mathbb{N}$. By part 4 of problem 9, A is at most countable. One can of course find infinitely many integers $m \in \mathbb{Z}$ such that $\gcd(m,1) = 1$ showing that A is countable.

2.

For the second part, you need one addtional result which is just presented without proof.

Lemma 1 *If a divides bc and $\gcd(a, b) = 1$, then a divides c.*

Define $f : A \to \mathbb{Q}$ such that

$$f((m, n)) = \frac{m}{n}$$

for all $(m, n) \in A$. Given $r \in Q$ $(r \neq 0)$, it can be represented as a fraction $\frac{p}{q}$ for some $p, q \in \mathbb{Z}$. Without loss of generality, we may assume $q > 0$. If $q < 0$, we can use the representation $\frac{-p}{-q}$. Let $d = \gcd(p, q)$. By definition, we can write $p = md$ and $q = nd$ for some $m, n \in Z$ with $\gcd(m, n) = 1$ where $n > 0$ since $q > 0$. Hence, $r = \frac{p}{q} = \frac{md}{nd} = \frac{m}{n}$ and $(m, n) \in A$. This shows that f is *onto*. To show that f is *one-to-one*, assume $f((m_1, n_1)) = f((m_2, n_2))$ where $(m_i, n_i) \in A$ and where $\gcd(m_i, n_i) = 1$ for $i = 1, 2$. Then $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ and both fractions represent the same rational number. Cross-multiplying results in $m_1 n_2 = n_1 m_2$ showing that n_2 divides $n_1 m_2$ as well as n_1 divides $m_1 n_2$. Since $\gcd(m_i, n_i) = 1$ for $i = 1, 2$ it follows by Lemma 7 that n_2 divides n_1 and n_1 divides n_2. Since both n_1 and n_2 are positive, it follows that $n_2 \leq n_1$ and $n_1 \leq n_2$. Putting both inequalities together results in $n_1 = n_2$. Using this last result in $m_1 n_2 = n_1 m_2 \Rightarrow (m_1 - m_2) n_2 = 0$ implies that $m_1 = m_2$ and thus $(m_1, n_1) = (m_2, n_2)$ which shows that f is *one-to-one*. Hence, there exists a bijection f of A with $\mathbb{Q}$. Since A is countable, $\mathbb{Q}$ is countable.

As a byproduct, this exercise shows that every rational number $r \in Q$ has a unique representation in lowest terms. Surjectivity of f proves the existence, while injectivity of f proves uniqueness.

Appendix

Let us first define the concept of a finite set.

Definition 2 *A set A is said to be finite if it is empty or if there exists a bijection*

$$f : A \to \{1, ..., n\}$$

for some positive integer n.

The next step involves showing that any subset B of a finite set A is finite. Before doing so, we need a lemma and a theorem and the desired result follows then as a corollary.

Lemma 3 *Let n be a positive integer. If a is an element of the set A, then there exists a bijection f of the set A with the set $\{1, ..., n + 1\}$ if and only if there exists a bijection g of the set $A \setminus a$ with the set $\{1, ..., n\}$.*

Instead of proving this lemma, I would rather explain the meaning of it. It basically states that if you have a set A, and the set, resulting by removing one element from A, is finite, then A is also finite. Conversely, if you have a set B, and the set, resulting by adding one element to B, is finite, then B is also finite.

Theorem 4 *Let A be a set and suppose there exists a bijection $f : A \to \{1, ..., n\}$ for some positive integer n. If B is a nonempty proper subset of A, then there exists a bijection $g : B \to \{1, ..., m\}$ for some $m < n$.*

Proof. The theorem is obviously true for $n = 1$ since then there does not exist any nonempty proper subset B of A. Assume then the theorem is true for n. We have to show that the theorem is true for $n + 1$. Suppose $f : A \to \{1, ..., n + 1\}$ is a bijection and B is a proper subset of A. Let $b \in B$. Lemma 3 shows there exists a bijection $g : A \setminus b \to \{1, ..., n\}$. Since $B \setminus b$ is a proper subset of $A \setminus b$ and since the theorem is true for n, two cases may occur. Either $B \setminus b = \emptyset$ or there exists a bijection $h : B \setminus b \to \{1, ..., t\}$ for some $t < n$. If $B \setminus b = \emptyset$ then there exists obviously a bijection from B with $\{1\}$. If $B \setminus b \neq \emptyset$ then there exists a bijection from B with $\{1, ..., t + 1\}$ by Lemma 3. In both cases, there exists a bijection from B with $\{1, ..., m\}$ for some $m < n + 1$, as required. ■

Corollary 5 *Any subset B of a finite set A is finite.*

Proof. Use Theorem 4 for all proper subsets B of A and use additionally Lemma 3 to cover the case where $B = A$. ■

Lemma 6 *Let $f : X \to Y$ be a bijection of X with Y. Then the inverse function $f^{-1} : Y \to X$ is a bijection, too.*

Proof. Since f^{-1} is the inverse function to f it follows that for all $y \in Y$, $f^{-1}(y) = x$ implies $x \in X$ and $f(x) = y$. Assume then $f^{-1}(y) = f^{-1}(y')$ for some $y, y' \in Y$. If $f^{-1}(y) = x$ and $f^{-1}(y') = x'$, it follows that $x = x'$ and $f(x) = y = y' = f(x')$ showing that f^{-1} is *one-to-one*. In order to show that f^{-1} is *onto*, consider an arbitrary $x \in X$. Then $f(x) = y$ for some $y \in Y$. Since f^{-1} is the inverse function to f, $f^{-1}(y) = x$, showing that f^{-1} is *onto*. ■

Lemma 7 *Let $f : X \to Y$ be a bijection of X with Y and let $g : Y \to Z$ be a bijection of Y with Z. Then the composition $g \circ f : X \to Z$ such that $g \circ f(x) = g(f(x))$ for $x \in X$ is a bijection, too.*

Proof. Left as a voluntary exercise. ■