INTRODUCTION TO PROOFS
formerly called Foundation and Proofs
Notes by Dr. Lynne H. Walling

8. Cardinality

Definitions. We say that two nonempty sets A and B have the same cardinality if there is a bijective map $f : A \to B$, and we write $|A| = |B|$. Note that (1) $h : A \to A$ defined by $h(x) = x$ is bijective; (2) when $f : A \to B$ is bijective, $f^{-1} : B \to A$ exists and is also bijective; and (3) if $f : A \to B$ and $g : B \to C$ are bijective, then so is $g \circ f : A \to C$. Thus $|A| = |A|$; $|A| = |B| \implies |B| = |A|$; and $[(|A| = |B|) \wedge (|B| = |C|)] \implies (|A| = |C|)$. (We are tempted to say that having the same cardinality is an equivalence relation on "the set of all sets"; however, it is known that there is no injection from $\mathcal{P}(X) = \{A : A \subseteq X\}$ into X. So if X were "the set of all sets", we would have $\mathcal{P}(X) \subseteq X$, and the inclusion map $\iota : \mathcal{P}(X) \to X$ defined by $\iota(A) = A$ would contradict that there is no injection from $\mathcal{P}(X)$ into X. Thus "the set of all sets" does not exist.)

We say a set Y has at least as many elements as a set X if there is an injective map $f : X \to Y$, and in this case we write $|X| \le |Y|$. If there is an injection from X into Y but no bijection between X and Y, we write $|X| < |Y|$. (Note that when $X \subseteq Y$ and $X \ne \emptyset$, the map $\iota : X \to Y$ defined by $\iota(x) = x$ is injective.)

Let A be a set. When $A = \emptyset$, we set $|A| = 0$. Now suppose $n \in \mathbb{Z}_+$ and $f : \{1, 2, \ldots, n\} \to A$ is bijective, we write $|A| = n$ and we say A has n elements. Further, we can enumerate the elements of A as $a_1, a_2, \ldots, a_n$ where $a_i = f(i)$, and since f is injective, $a_i = a_j$ if and only if $i = j$.

When $|A| \in \mathbb{Z}_{\ge 0}$, we say A is a finite set. When A is not a finite set we say A is an infinite set.

Suppose A is a finite set with $|A| = n$ ($n \in \mathbb{Z}_{\ge 0}$) and B is a subset of A; we accept without proof that $|B| = m$ where $m \le n$ ($m \in \mathbb{Z}_{\ge 0}$), and that $A = B$ if and only if $m = n$. We also accept without proof that $\mathbb{Z}_+$ is infinite. Note that we have assumed the following: Suppose $B \subseteq A$; if A is finite then B is finite. The contrapositive of this statement is: Suppose $B \subseteq A$; if B is infinite then A is infinite.

We will eventually see that $|\mathbb{Z}_+| = |\mathbb{Z}| = |\mathbb{Q}_+| = |\mathbb{Q}|$, but $|\mathbb{Z}_+| < |\mathbb{R}|$.

Proposition 8.1. *Suppose $A, B \subseteq X$ where X is some set, where A, B are nonempty finite sets with $A \cap B = \emptyset$. Then $|A \cup B| = |A| + |B|$.*

Proof. Let $s, t \in \mathbb{Z}_+$ so that $|A| = s$ and $|B| = t$. Thus we can enumerate the elements of A as $a_1, a_2, \ldots, a_s$ where $a_i = a_j$ only if $i = j$ (here i, j are integers between 1 and s). Similarly, we can enumerate the elements of B as $b_1, b_2, \ldots, b_t$ where $b_i = b_j$ only if $i = j$ (here i, j are integers between 1 and t). We also know that for any integers i, j with $1 \le i \le s$ and $1 \le j \le t$, we have $a_i \ne b_j$ since $A \cap B = \emptyset$.

Define $f : \{1, 2, \ldots, s + t\} \to A \cup B$ by

$$f(n) = \begin{cases} a_n & \text{if } 1 \le n \le s, \\ b_{n-s} & \text{if } s < n \le s + t. \end{cases}$$

As an exercise, one shows that f is bijective. $\square$

Definition. We say a set X is countable if there is a bijective function $f : \mathbb{Z}_+ \to X$, or equivalently, if there is a bijective map $g : X \to \mathbb{Z}_+$. (Note: Some texts say a set if countable if it is finite or if there is a bijective function $f : \mathbb{Z}_+ \to X$, and when there is a bijective function $f : \mathbb{Z}_+ \to X$, these texts say X is countably infinite.)

Note: Suppose X is a countable set; so by definition there is a bijective map $f : \mathbb{Z}_+ \to X$. Thus we can enumerate the elements of X as $x_1, x_2, x_3, \ldots$ where $x_i = f(i)$ for $i \in \mathbb{Z}_+$.

Example: The set of positive even integers is countable: Let $A = \{2x : x \in \mathbb{Z}_+ \}$. Define $f : \mathbb{Z}_+ \to A$ by $f(x) = 2x$. To see f is injective, suppose $x, y \in \mathbb{Z}_+$ so that $f(x) = f(y)$. Thus $2x = 2y$, so $x = y$, showing that f is injective. To see f is surjective, take $a \in A$. Thus $a = 2x$ for some $x \in \mathbb{Z}_+$, and hence $a = 2x = f(x)$; so f is surjective. This shows that f is bijective, and hence A is countable. Similarly, the set of odd positive integers, $\{2x - 1 : x \in \mathbb{Z}_+ \}$, can be shown to be countable.

Theorem 8.2. *Suppose $f : X \to Y$ is injective and $A \subseteq X$. Then $|A| = |f(A)|$.*

Proof. Let $B = f(A)$. Define $g : A \to B$ by $g(a) = f(a)$. By the definition of B, $B = f(A) = g(A)$, so g is surjective. Suppose $a, a' \in A$ so that $g(a) = g(a')$. Then $f(a) = f(a')$, and since f is injective, this means $a = a'$. Hence g is injective. Thus g is bijective, so $|A| = |g(A)|$. We also know that $g(A) = B = f(A)$, so $|A| = |g(A)| = |f(A)|$. $\square$

The next theorem may seem intuitively obvious, but a proper proof is beyond the scope of this course.

Theorem 8.3. (a) *Every infinite set contains a countable subset.*

(b) *(Cantor-Schröder-Bernstein Theorem) If X, Y are sets with $|X| \le |Y|$ and $|Y| \le |X|$ then $|X| = |Y|$. That is, if X, Y are sets so that there exist injective functions $g : X \to Y$ and $h : Y \to X$ then there is a bijective function $f : X \to Y$.*

(In some texts, this theorem is called the Cantor-Bernstein Theorem or the Schöder-Bernstein Theorem; an interesting proof of this theorem due to Halmos can be found in the book by Pierre Grillet, which is available as an electronic book from the University of Bristol library.)

Corollary 8.4. *Suppose $X \subseteq \mathbb{Z}_+$. Then X is finite or countable.*

Proof. If X is finite then we are done. So suppose X is infinite. We have an injective map $g : X \to \mathbb{Z}_+$ given by $g(x) = x$, so $|X| \le |\mathbb{Z}_+|$. On the other hand, we know X contains a countable subset A. Hence there is a bijective map $h : \mathbb{Z}_+ \to A$. Define $f : \mathbb{Z}_+ \to X$ by $f(n) = h(n)$. So f

gives us an injective map from $\mathbb{Z}_+$ into X. Thus $|\mathbb{Z}_+| \leq |X|$, and so by the Cantor-Bernstein Theorem, there is a bijective map $f : \mathbb{Z}_+ \to X$. Hence X is countable. □

The next result is very useful when proving a set is countable.

Corollary 8.5. *Suppose X is an infinite set. Then X is countable if and only if there is an injective map $f : X \to \mathbb{Z}_+$.*

Proof. First suppose there is an injective map $f : X \to \mathbb{Z}_+$. Thus $|X| = |f(X)|$, and $f(X)$ is a subset of $\mathbb{Z}_+$. Since X is not finite and $|X| = |f(X)|$, $f(X)$ is not finite. Hence (by the previous corollary), $f(x)$ is countable, and hence X is countable.

Now suppose that X is countable. Thus there is a bijective $g : \mathbb{Z}_+ \to X$. Since g is bijective, g^{-1} exists. With $f = g^{-1}$, we have that $f : X \to \mathbb{Z}_+$ is bijective and hence injective. □

As exercises, one proves the following.

Proposition 8.6. *Suppose X is a countable set.*

(a) *Suppose A is a subset of X; then A is finite or countable.*
(b) *Suppose A is a subset of X. If A is finite then $X \setminus A$ is countable.*
(c) *X contains a subset B so that B and $X \setminus B$ are countable.*
(d) *Suppose $f : C \to X$ is injective; then C is finite or countable.*

Theorem 8.7. *Suppose $A, B \subseteq X$ where X is some set; suppose A is a countable set and B is a nonempty, finite set with $A \cap B = \emptyset$. Then $A \cup B$ is countable.*

Proof. [The idea of this proof is that of the "Hilbert hotel", where there is always room for another guest: The Hilbert hotel has countably many rooms, labeled $1, 2, 3, \ldots$ (so for each number in $\mathbb{Z}_+$, there is a room with that number). One night, all the rooms are occupied, and another potential guest arrives at the hotel looking for a room. The manager says, no problem! Then the manager announces to the guests that every guest is to move to the next room (so the guests in room n move to room $n + 1$). Thus all the guests still have rooms, and room 1 has been made available to the new arrival.]

Since A is countable, there is an injective map $f : A \to \mathbb{Z}_+$. B is finite, so we can list the distinct elements of B as $b_1, \ldots, b_m$ where $m = |B| \in \mathbb{Z}_+$. Define $g : A \cup B \to \mathbb{Z}_+$ by

$$g(x) = \begin{cases} i & \text{if } x = b_i, \\ f(x) + m & \text{if } x \in A. \end{cases}$$

We claim that g is injective. To see this, take $x, y \in A \cup B$ so that $x \neq y$. If $x, y \in B$ then $x = b_i$ and $y = b_j$ for some $i, j \in \mathbb{Z}_+$ so that $i \leq m$, $j \leq m$ with $i \neq j$, and hence $g(x) = i \neq j = g(y)$. If $x \in B$ and $y \in A$ then $x = b_i$ for some $i \in \mathbb{Z}_+$ with $i \leq m$, and hence $g(x) = i < m + 1 \leq g(y) + m + 1$. If $x, y \in A$, then since $x \neq y$ and f is injective, we have $f(x) \neq f(y)$ and so $g(x) = f(x) + m + 1 \neq f(y) + m + 1 = g(y)$. Therefore g is injective. Since $A \subseteq A \cup B$ and A is infinite, $A \cup B$ is infinite. Since $g : A \cup B \to \mathbb{Z}_+$ is injective and $A \cup B$ is infinite, $A \cup B$ is countable. □

Theorem 8.8. $\mathbb{Z}_+ \times \mathbb{Z}_+$ *is countable.*

Proof. We have that $\mathbb{Z}_+ \times \mathbb{Z}_+$ is infinite, as $\{(x, 1) : x \in \mathbb{Z}_+\}$ is an infinite subset of $\mathbb{Z}_+ \times \mathbb{Z}_+$.

We arrange the elements of $\mathbb{Z}_+ \times \mathbb{Z}_+$ in a grid:

$$\begin{array}{ccccc} (1,1) & (1,2) & (1,3) & (1,4) & \cdots \\ (2,1) & (2,2) & (2,3) & (2,4) & \cdots \\ (3,1) & (3,2) & (3,3) & (3,4) & \cdots \\ (4,1) & (4,2) & (4,3) & (4,4) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$

We order the elements of this grid along the cross-diagonals:

$$(1,1);\ (1,2),\ (2,1);\ (1,3),\ (2,2),\ (3,1);\ldots$$

We will define $f : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ so that $f((1,1)) = 1$, $f((1,2)) = 2$, $f((2,1)) = 3$, $f((1,3)) = 4$, $f(2,2) = 5$, $f(3,1) = 6$, etc. We now find a formula to define f.

The kth cross-diagonal contains the pairs $(1, k), (2, k-1), (3, k-2), \ldots, (k, 1)$. So this cross-diagonal has k pairs. Thus the number of pairs in the first $k-1$ cross-diagonals is

$$1 + 2 + 3 + \cdots + (k-1) = \frac{(k-1)k}{2}.$$

Thus we define $f : \mathbb{Z}_+ \times \mathbb{Z}_+$ by

$$f((i, k+1-i)) = \frac{(k-1)k}{2} + i.$$

To show f is injective, suppose $x, y \in \mathbb{Z}_+ \times \mathbb{Z}_+$ so that $f(x) = f(y)$. Thus $\exists i, k \in \mathbb{Z}_+$ so that $i \le k$ and $x = (i, k+1-i)$ (so x is on the kth cross-diagonal). Suppose first that y is also on the kth cross-diagonal; thus $\exists j \in \mathbb{Z}_+$ so that $j \le k$ and $y = (j, k+1-j)$. Then

$$\frac{(k-1)k}{2} + i = f(x) = f(y) = \frac{(k-1)k}{2} + j.$$

Hence $i = j$ and so $x = y$. Now suppose y is not on the kth cross-diagonal. So there exist $j, m \in \mathbb{Z}_+$ so that $j \le m$ and $y = (j, m+1-j)$. So y is on the mth cross-diagonal where $m \ne k$; hence $m > k$ or $k > m$. Without loss of generality, assume $m > k$. [If it is the case that $k > m$ then we rename x as y and y as x.] Thus $m = k + r$ for some $r \in \mathbb{Z}_+$. So

$$f(x) = \frac{k-1)k}{2} + i \le \frac{(k-1)k}{2} + k,$$

and

$$\begin{aligned} f(y) &= \frac{(k+r-1)(k+r)}{2} + j \\ &= \frac{(k-1)k}{2} + kr + \frac{(r-1)r}{2} + j \\ &\ge \frac{(k-1)k}{2} + k + 1 \end{aligned}$$

(since $kr \ge k$, $r(r-1) \ge 0$, and $j \ge 1$). Therefore $f(x) \ne f(y)$, contradicting the assumption that $f(x) = f(y)$.

Hence, if $f(x) = f(y)$ then x and y are on the same cross-diagonal and $x = y$. This shows f is injective. □

Suppose X, Y are countable. Then certainly $X \times Y$ is infinite: Choose $y_0 \in Y$. Define $f : X \times \{y_0\} \to X$ by $f(x, y_0) = x$. One easily shows f is bijective, so $|X \times \{y_0\}| = |X|$, and hence $X \times \{y_0\}$ is countable. As $X \times \{y_0\} \subseteq X \times Y$, $X \times Y$ is infinite (as it contains an infinite subset).

As an exercise, one proves the following somewhat anti-intuitive result.

Corollary 8.9. *$\mathbb{Q}_+$ and $\mathbb{Q}$ are countable.*

Also as an exercise, one proves the following.

Proposition 8.10. *Suppose X, Y are countable. Then:*

(a) *$X \times Y$ is countable.*
(b) *Suppose also $X \cap Y = \emptyset$. Then $X \cup Y$ is countable.*

Note: Since $\mathbb{Z}$ is an infinite subset of $\mathbb{Q}$ and $\mathbb{Q}$ is countable, $\mathbb{Z}$ must be countable.

Corollary 8.11. *Let $\{A_n : n \in \mathbb{Z}_+\}$ be a (countable) collection of countable sets that are pairwise disjoint. Then $\cup_{n \in \mathbb{Z}_+} A_n$ is countable.*

Proof. First note that since A_1 is infinite and $A_1 \subseteq \cup_{n \in \mathbb{Z}_+} A_n$, we know that $\cup_{n \in \mathbb{Z}_+} A_n$ is also infinite. We have seen that if X is a countable set, Y is an infinite set, and $\exists$ an injective map $g : Y \to X$, then Y is countable. Thus to prove that $\cup_{n \in \mathbb{Z}_+} A_n$ is countable, we will prove there is an injective function $g : \cup_{n \in \mathbb{Z}_+} A_n \to \mathbb{Z}_+ \times \mathbb{Z}_+$.

For each $n \in \mathbb{Z}_+$, enumerate the elements of A_n as $a_{n1}, a_{n2}, a_{n3}, \ldots$. [Recall that since A_n is countable, there is a bijective function $f_n : \mathbb{Z}_+ \to A_n$; for $k \in \mathbb{Z}_+$, set $a_{nk} = f_n(k)$.] Now define $g : \cup_{n=1}^{\infty} A_n \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by $g(a_{mk}) = (m, k)$. [Since the A_n are pairwise disjoint, g is actually a function.] To see g is injective, suppose $g(a_{mk}) = g(a_{st})$ for some $m, k, s, t \in \mathbb{Z}_+$. Thus $(m, k) = (s, t)$, so $m = s$, $k = t$, and hence $a_{mk} = a_{st}$. Thus g is injective. So we have an injective function from $\cup_{n=1}^{\infty}$ into a countable set; since $\cup_{n=1}^{\infty} A_n$ contains the infinite set A_1 and hence is infinite, $\cup_{n=1}^{\infty} A_n$ is countable.

□