Counting

Joseph R. Mileti

February 23, 2015

1 The Cardinality of Sets

We will spend a significant amount of time trying to count the number of elements in certain sets. For now, we will study some simple properties that will become extremely useful later when employed in clever ways.

Definition 1.1. *Given a set A, we let $|A|$ be the number of elements of A, and we call $|A|$ the cardinality of A. If A is infinite, then we write $|A| = \infty$.*

Of course, if we list the elements of a set A, then it's usually quite easy to determine $|A|$. For example, we trivially have $|\{1, \sqrt{2}, \frac{5}{2}, 18\}| = 4$. However, it can be very hard to determine the cardinality of a set. For example, consider the set

$$A = \{(x, y) \in \mathbb{Z}^2 : x^3 = y^2 + 1\}$$

Determining the elements of A is nontrivial. It's easy to see that $(1, 0) \in A$, but it's not clear whether there are any other elements. Using some nontrivial number theory, it is possible to show that $A = \{(1, 0)\}$, and hence $|A| = 1$.

We start with one of the most basic, yet important, rules about the cardinality of sets.

Definition 1.2. *We say that two sets A and B are disjoint if $A \cap B = \emptyset$.*

Fact 1.3 (Sum Rule)**.** *If A and B are finite disjoint sets, then $|A \cup B| = |A| + |B|$.*

We won't give a formal proof of this fact, because it is so basic that it's hard to know what to assume (although if one goes through the trouble of axiomatizing math with something like set theory, then it's possible to give a formal proof by induction on $|B|$). At any rate, the key fact is that since A and B are disjoint, they have no elements in common. Therefore, each element of $A \cup B$ is in exactly one of A or B. Notice that the assumption that A and B are disjoint is essential. If $A = \{1, 2\}$ and $B = \{2, 3\}$, then $|A| = 2 = |B|$, but $|A \cup B| = 3$ because $A \cup B = \{1, 2, 3\}$.

Although the next result is again very intuitive, we show how to prove it using the Sum Rule.

Proposition 1.4 (Complement Rule)**.** *If A and B are finite sets and $B \subseteq A$, then $|A \backslash B| = |A| - |B|$.*

Proof. Notice that $A \backslash B$ and B are disjoint sets and that $(A \backslash B) \cup B = A$. Using the Sum Rule, we conclude that $|A \backslash B| + |B| = |A|$. The result follows. □

We can now easily generalize this to the case where B may not be a subset of A.

Proposition 1.5 (General Complement Rule)**.** *If A and B are finite sets, then $|A \backslash B| = |A| - |A \cap B|$.*

Proof. We have $A \backslash B = A \backslash (A \cap B)$. Since $A \cap B \subseteq A$, we can now apply the Complement Rule. □

We can generalize the Sum Rule to the following.

Definition 1.6. *A collection of sets $A_1, A_2, \dots, A_n$ is* pairwise disjoint *if $A_i \cap A_j = \emptyset$ whenever $i \neq j$.*

Fact 1.7 (General Sum Rule)**.** *If $A_1, A_2, \dots, A_n$ are finite sets that are pairwise disjoint sets, then $|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$.*

Again, we won't give a formal proof of this fact (although it it possible to do so from the Sum Rule by induction on n). Notice that as above the pairwise disjoint assumption is key, and it's not even enough to assume that $A_1 \cap A_2 \cap \dots \cap A_n = \emptyset$ (see the homework).

Proposition 1.8. *If A and B are finite sets, we have $|A \cup B| = |A| + |B| - |A \cap B|$.*

Proof. Consider the three sets $A \backslash B$, $B \backslash A$, and $A \cap B$. These three sets are pairwise disjoint, and their union is $A \cup B$. Using the General Sum Rule, we conclude that

$$|A \cup B| = |A \backslash B| + |B \backslash A| + |A \cap B|$$

Now $|A \backslash B| = |A| - |A \cap B|$ and $|B \backslash A| = |B| - |A \cap B|$ by the General Complement Rule. Plugging these in, we conclude that

$$|A \cup B| = |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B|$$

and hence

$$|A \cup B| = |A| + |B| - |A \cap B|$$

□

Proposition 1.9 (Product Rule)**.** *If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.*

Proof. Let $n = |A|$ and let $m = |B|$. List the elements of A so that $A = \{a_1, a_2, \dots, a_n\}$. Similarly, list the elements of B so that $B = \{b_1, b_2, \dots, b_m\}$. For each i, let

$$A_i = \{(a_i, b_j) : 1 \leq j \leq m\} = \{(a_i, b_1), (a_i, b_2), \dots, (a_i, b_m)\}$$

Thus, A_i is the subset of $A \times B$ consisting only of those pairs whose first element is a_i. Notice that the sets $A_1, A_2, \dots, A_n$ are pairwise disjoint and that

$$A \times B = A_1 \cup A_2 \cup \dots \cup A_n$$

Furthermore, we have that $|A_i| = m$ for all i. Using the General Sum Rule, we conclude that

$$\begin{aligned}
|A \times B| &= |A_1| + |A_2| + \dots + |A_n| \\
&= m + m + \dots + m \\
&= n \cdot m \\
&= |A| \cdot |B|
\end{aligned}$$

The result follows. □

Using induction (see below), one can prove the following generalization.

Proposition 1.10 (General Product Rule)**.** *If $A_1, A_2, \dots, A_n$ are finite sets, then $|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.*

Corollary 1.11. *If A is a finite set and $n \in \mathbb{N}^+$, then $|A^n| = |A|^n$.*

Corollary 1.12. *For any $n \in \mathbb{N}^+$, we have that $|\{0,1\}^n| = 2^n$, i.e. there are 2^n many sequences of 0's and 1's of length n.*

2 Using Functions to Count

The following fact is intuitively clear. If $f\colon A \to B$ is injective, then every element of B is hit by at most one element of A, so the there must be at least as many elements in B as their are in A. The others can be argued similarly. One can do a formal proof by induction on the cardinalities of A and B, but just as for the Sum Rule we will avoid being so formal.

Fact 2.1. *Let A and B be finite sets and let $f\colon A \to B$ be a function.*

- *If f is injective, then $|A| \leq |B|$.*
- *If f is surjective, then $|B| \leq |A|$.*
- *If f is bijective, then $|A| = |B|$.*

The last of these is often very helpful when to trying to determine the cardinality of a set, and is sometimes called the "Bijection Principle". In general, if we have a set A and want to know $|A|$, then the idea is to build a set B and a bijection $f\colon A \to B$ where $|B|$ is much easier to determine. The most fundamental example of this is the following:

Definition 2.2. *Given a set A, we let $\mathcal{P}(A)$ be the set of all subsets of A, and we call $\mathcal{P}(A)$ the* power set *of A.*

For example, we have

$$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$$

and

$$\mathcal{P}(\{4,5,7\}) = \{\emptyset, \{4\}, \{5\}, \{7\}, \{4,5\}, \{4,7\}, \{5,7\}, \{4,5,7\}\}$$

Proposition 2.3. *Given a set A with $|A| = n$, we have $|\mathcal{P}(A)| = |\{0,1\}^n|$.*

Proof. Let $A = \{a_1, a_2, \dots, a_n\}$ where the a_i are distinct. Define a function $f\colon \{0,1\}^n \to \mathcal{P}(A)$ by letting $f(b_1, b_2, \dots, b_n) = \{a_i : b_i = 1\}$. In other words, given a finite sequence $(b_1, b_2, \dots, b_n)$ of 0's and 1's, we send it to the subset of A obtained by including a_i precisely when the i^{th} element of the sequence is a 1. Notice that if $(b_1, b_2, \dots, b_n) \neq (c_1, c_2, \dots, c_n)$, then we can fix an i with $b_i \neq c_i$, and in this case we have $f(b_1, b_2, \dots, b_n) \neq f(c_1, c_2, \dots, c_n)$ because a_i is one of the sets but not the other. Furthermore, given any $S \subseteq A$, if we let $(b_1, b_2, \dots, b_n) \in \{0,1\}^n$ be defined by letting

$$b_i = \begin{cases} 1 & \text{if } a_i \in S \\ 0 & \text{if } a_i \notin S \end{cases}$$

then $f(b_1, b_2, \dots, b_n) = S$, so f is surjective. Therefore, f is a bijection, and hence $|\{0,1\}^n| = |\mathcal{P}(A)|$. □

Corollary 2.4. *If $|A| = n \in \mathbb{N}^+$, then $|\mathcal{P}(A)| = 2^n$.*

Proof. This is immediate from the bijection principle and Corollary 1.11. □

Since this result is so fundamental, we give another proof that uses both induction and the bijection principle.

Proof 2 of Corollary 2.4. We prove the result by induction on $n \in \mathbb{N}^+$.

- *Base Case:* Suppose that $n = 1$. Let A be a set with $|A| = 1$, say $A = \{a\}$. We then have that $\mathcal{P}(A) = \{\emptyset, \{a\}\}$, so $|\mathcal{P}(A)| = 2 = 2^1$.

- *Induction Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. assume that for some fixed $n \in \mathbb{N}^+$, we know that $|\mathcal{P}(A)| = 2^n$ for all sets A with $|A| = n$. Consider an arbitrary set A with $|A| = n + 1$. Fix some (any) element $a_0 \in A$. Let $\mathcal{S} \subseteq \mathcal{P}(A)$ be the collection of subsets of A not having a_0 as an element, and let $\mathcal{T} \subseteq \mathcal{P}(A)$ be the collection of subsets of A having a_0 as an element. Notice then that $\mathcal{S}$ and $\mathcal{T}$ are disjoint sets with $\mathcal{P}(A) = \mathcal{S} \cup \mathcal{T}$, so by the Sum Rule we know that

  $$|\mathcal{P}(A)| = |\mathcal{S}| + |\mathcal{T}|.$$

  Now consider the function $f\colon \mathcal{S} \to \mathcal{T}$ defined by letting $f(B) = B \cup \{a_0\}$, i.e. given $B \in \mathcal{S}$, we have that B is a subset of A not having a_0 as an element, and we send to the subset of A obtained by throwing a_0 in as a new element. Notice that f is a bijection, so $|\mathcal{S}| = |\mathcal{T}|$. Therefore, we have

  $$|\mathcal{P}(A)| = |\mathcal{S}| + |\mathcal{S}|.$$

  Finally, notice that $\mathcal{S} = \mathcal{P}(A \backslash \{a_0\})$, so since $|A \backslash \{a_0\}| = n$, we can use induction to conclude that $|A \backslash \{a_0\}| = 2^n$. Therefore,

  $$|\mathcal{P}(A)| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that if $|A| = n \in \mathbb{N}^+$, then $|\mathcal{P}(A)| = 2^n$. □

By the way, Corollary 2.4 is also true in the case $n = 0$. When $n = 0$, we have $A = \emptyset$ and $\mathcal{P}(\emptyset) = \{\emptyset\}$, so $|\mathcal{P}(\emptyset) = 1 = 2^0$.

Proposition 2.5. *Let A be a set with $|A| = n \in \mathbb{N}^+$ and let $k \in \mathbb{N}$ be such that $0 \leq k \leq n$. The number of subsets of A having cardinality k equals the number of subsets of A having cardinality $n - k$.*

Proof. Let $\mathcal{S}$ be the collection of all subsets of A having cardinality k, and let $\mathcal{T}$ be the collection of all subsets of A having cardinality $n - k$. Define $f\colon \mathcal{S} \to \mathcal{T}$ by letting $f(B) = A \backslash B$, i.e. given $B \subseteq A$ with $|B| = k$, send it to the complement of B in A (notice that if $|B| = k$, then $|A \backslash B| = n - k$ by the complement rule). Notice that f is a bijection (it is surjective because if $C \subseteq A$ is such that $|C| = n - k$, then $|A \backslash C| = k$ and $f(A \backslash C) = C$). Therefore, $|\mathcal{S}| = |\mathcal{T}|$. □

Thus, despite the fact that we do not (yet) have a formula for the number of subsets of a certain size, we know that the number of subsets of size k must equal the number of subsets of size $n - k$ even without this knowledge.