The Size of the Set of Subsets, together with Alternative Proofs
by Henry M. Walker, Grinnell College

Theorem: Let S be a set with n elements.
Then S has 2^n subsets.

Proof 1:

Let $P(S)$ be the set of all subsets of S, and let H be the set of n-character strings of 0's and 1's.
Order the elements of S as $s_1, s_2, \ldots s_n$.

Define function $f : P(S) \to H$ as follows:
For $Q \in P(S)$, let $f(Q) = r_1 r_2 \ldots r_n$ where r_i is 1 if $s_i \in Q$ and 0 otherwise.

f is clearly 1-1 and onto (i.e., f is a bijection), and the theorem follows.

Proof 2: Order the elements of S as $s_1, s_2, \ldots s_n$, and let $P(S)$ be the set of all subsets of S.
Let H represent the binary numbers between 0 and $2^n - 1$. Since all numbers in this range may be represented by n binary digits, H includes n-digit sequences

$000\ldots00$ (n 0's),
$000\ldots01$ ($n-1$ 0's followed by a 1),
$\ldots$,
$111\ldots11$ (n 1's).

Each element Q in $P(S)$ is a subset of S contains zero or more elements of S, and one can determine whether each s_i is in Q for $i = 1, 2, \ldots n$.

Define function $f : P(S) \to H$ as follows:
For $Q \in P(S)$, let $f(Q) = r_1 r_2 \ldots r_n$, where r_i is the digit 1 if $s_i \in S$ and 0 otherwise, for $i = 1, 2, \ldots n$.

Claim: f is 1-1 and onto (i.e., f is a bijection)
Proof of Claim:
1-1: For subsets X_1 and X_2 of S, $f(X_1)$ and $f(X_2)$ will differ in each digit for which an element in one subset is not also in the other. Thus, $X_1 \neq X_2 \Longrightarrow f(X_1) \neq f(X_2)$
onto: Given an n-digit binary number b (i.e., a number in H, let X be the subset of S which contains element s_i if and only if the i^{th} digit of b is 1. Then $f(S) = b$.

Since f is 1-1 and onto, each subset of S is paired with a number in H. Since elements of H provide a count (in binary) of numbers from 0 to $2^n - 1$, H has size s^n, and $P(S)$ also must have size s^n.

Proof 3: Let $P(S)$ be the set of all subsets of S.
We construct a mechanism (called a function) to count the elements of $P(S)$.

Step 1: We examine the binary numbers from 0 through $2^n - 1$.
Discussion of Step 1: In binary notation, the digits represent powers of 2. For $k+1$ digits, the bits represent the powers $2^k, 2^{k-1}, 2^{k-2}, \ldots 2^1, 2^0$. Thus, the number 1, followed by k 0's (i.e., $1000\ldots000$) represents the number 2^k. Subtracting 1 from this number in binary yields $111\ldots111$ (k 1's) or $2^k - 1$. Turning to the theorem at hand, the number 2^n is represented in binary by n 1s.

If we count in binary, therefore, the numbers 0 through $2^n - 1$ may be represented as 0, 1, 10, 11, ..., n 1s. If we add leading 0s to these numbers as needed, so that each number from 0 through $2^n - 1$ is written using n bits, the resulting sequence becomes:

$000\ldots00$ (n 0's),
$000\ldots01$ ($n-1$ 0's followed by a 1),
$000\ldots10$ ($n-2$ 0's followed by a 10),
$000\ldots11$ ($n-2$ 0's followed by a 11),
$\ldots$,
$111\ldots11$ (n 1's).

For future reference, define the set H to be this collection of binary numbers between 0 and 2^n.

Step 2: We consider a representation of the elements of S.
Discussion of Step 2: Since S is a given set of n elements, we may fix an order for these elements, and then label the elements as the sequence $s_1, s_2, \ldots s_n$

Step 3: We develop a mechanism to count all subsets of $P(S)$.
Discussion of Step 3: We define a function $g : H \rightarrow P(S)$ as a mechanism to count all elements in $P(S)$.

Let b be a binary integer between 0 and 2^n., and let $b_1 b_2 \ldots b_n$ be its binary expansion in the set H.

Define function $g : h \rightarrow P(S)$ by $g(b) = \{s_i \mid b_i = 1\}$ for $i = 1, \ldots n$.

With this definition, g is well defined, since each bit in a binary integer b corresponds unambiguously to an element of S, and reading along the bits of b indicates exactly what subset will correspond to $g(b)$.

To show g is 1-1, consider two binary numbers h_1 and h_2 in H, and suppose $g(h_1) = g(h_2)$. Let $T = g(h_1) = g(h_2)$, For each i between 1 and n,

if $s_i \in T$, then the i^{th} bit of both h_1 and h_2 must be 1, by the definition of g.
if $s_i \notin T$, then the i^{th} bit of both h_1 and h_2 must be 0, by the definition of g.

Putting these bits together, $g(h_1) = g(h_2)$ requires that every bit of h_1 is the same as the corresponding bit of h_2, and it follows that $h_1 = h_2$.

To show g is onto, consider a subset R of S. From R, construct a binary integer b with bits $b_1 b_2 \ldots b_n$ as follows:

For $i = 1$ to n, let $b_i = 1$ if $s_i \in R$ and let $b_i = 0$ otherwise.

By the construction and definition of g, $g(b) = R$, so g is 1-1.

Step 4: The Theorem follows by counting.
Discussion of Step 4: Altogether, function g provides a 1-1 correspondence between the numbers 0 and $2^n - 1$, effectively providing a mechanism that uses these integers to count each subset of S exactly once.

Proof 4: Suppose set S has n elements.
If $n = 0$, then S is the empty set, and its only subset is itself.

If $n > 0$, pick an element $s \in S$, and let U be the set S with the element s removed. Since U has $n - 1$ elements, the power set $P(U)$ of U contains 2^{n-1} subsets. Also, let $P^*(U)$ consist of all subsets in $P(U)$ with the element S added.

Since $P(S) = P(U) \bigcup P^*(U)$, $P(U)$ and $P^*(U)$ are disjoint, and $P(U)$ and $P^*(U)$ each have 2^{n-1} elements, it follows that $P(S)$ has 2^n elements.

Proof 5: Suppose set S has n elements.
The proof proceeds by mathematical induction on n with the following induction hypothesis:

> $IH(n)$: If S is any set with n elements, then it has exactly 2^n subsets.

Base case $(n = 0)$*:* If $n = 0$, then S is the empty set. The only subset of the empty set is the empty set itself, so there are exactly $1 = 2^0$ subsets, as required by $IH(0)$.

Induction case $(n > 0)$*:* Assume the Induction Hypothesis $IH(k)$ for integers $k < n$; the following argument shows that $IH(n)$ is true as well.

Since $n > 0$, the set S has at least one element. Pick s as one such element, and consider the set U obtained by removing the element s from S, sometimes written $U = S - \{s\}$.

Since one element has been removed from S, U has $n - 1$ elements, the Induction Hypothesis $IH(n - 1)$ applies to U, and U has 2^{n-1} subsets. Label this collection of 2^{n-1} subsets as W.

Next, form a new collection N of sets by adding the element s to each subset in W. Since each element of W is a subset of S and since s is an element of S, each element of N is also a subset of S.

Now, suppose A and B are two distinct elements of W; that is, A and B are distinct subsets of $U = S - \{s\}$. Since A and B are distinct, there is at least one element in A that is not in B or one element in B that is not in A. That is, A and B differ by some element $q \in U$. Since neither A or B contain s, $q \neq s$, so q remains a difference between $A \bigcup \{s\}$ and $B \bigcup \{s\}$. Altogether, this shows that the number of elements in N is the same as the number of elements in W, namely 2^{n-1}.

In addition, no element in W is also in N, since all elements in W do not contain s, while all elements of do contain s. As W and N are disjoint, the number of elements in $W \bigcup N$ is $2^{n-1} + 2^{n-1} = 2^n$. Since all elements of $W \bigcup N$ are subsets of S, the number of subsets of S must be at least 2^n.

Finally, every subset V of S either contains s or it does not.

> If V does not contain s, then $V \in W \in W \bigcup N$.
> If V does contain s, then $V - \{s\}$ does not contain s and thus is contained in W. Adding s to $V - \{s\}$ places the result N. Thus, $V \in N \in W \bigcup N$.

Since every subset V of S is contained in $W \bigcup N$, the number of such subsets cannot be bigger than the size of $W \bigcup N$, which is 2^n.

Put together, $W \bigcup N$ contains exactly all subsets of S, proving $IH(n)$, which states that the number of such subsets is 2^n.

Proof 6: This argument proceeds by contradiction:
Let S be a set of n elements, and suppose that the number of subsets of S is not 2^n. Then either the number of subsets is less than 2^n or greater than 2^n. What follows examines each of these possibilities in detail.

Part 1: The number of subsets of S *cannot be less than* 2^n.

Let $P(S)$ be the collection of all subsets of S, and
let St consist of all strings from the alphabet $\{0, 1\}$ of length n.
Also, order the sets of S to yield a sequence $s_1, s_2, \ldots s_n$.

Next, construct a function $f : P(S) \to St$ as follows.

For a subset Q of S, define $f(Q) = t_1t_2 \ldots t_n$, where, for each i, $t_i = 1$ if $s_i \in Q$ and $t_i = 0$ if $s_i \notin Q$. That is, the digits of $f(Q)$ indicate whether or not element s_i is in Q.

Claim: f *is onto:*

Let $t = t_1t_2 \ldots t_n$ be any string of length n over the alphabet $\{0, 1\}$; that is, let t be any element in St. From this string, form a set Q from elements of S, according to the following rules:

For each i between 1 and n,
  if t_i is 1, then place s_i in Q, but
  if t_i is 0, then do not place s_i in Q.

By construction, $f(Q) = t$, so f is onto.

Claim: St contains 2^n elements.

In considering possible strings in St,

  there are 2 choices (0 or 1) for t_1
  there are 2 choices for t_2
  . . .
  there are 2 choices for t_n

Choices for each digit are independent, so overall there are $2 \times 2 \times 2 \ldots \times 2 = 2^n$ possible strings in St.

Since f is an onto function, and the range St has 2^n elements, the domain of f must have at least 2^n, proving the claim for Part 1.

Part 2: The number of subsets of S *cannot be greater than* 2^n.

As in Part 1, Let $P(S)$ be the collection of all subsets of S, and
order the sets of S to yield a sequence $s_1, s_2, \ldots s_n$.

Also, consider all integers between 0 and $2^n - 1$ (inclusive) as represented using binary numbers. Such numbers can be written using no more than n binary digits. However, in the case that the binary representation does not require n, add leading 0's so that all integers from 0 through $2^n - 1$ are represented as n-digit binary numbers. For reference, label this collection of binary numbers as BN.

Now, define a function $g : BN \to P(S)$ as follows.

Let $b_1b_2 \ldots b_n$ be an n-digit binary number in BN.
Then $g(b_1b_2 \ldots b_n)$ is defined as the set Y, where the subset Y is prescribed by the rules:
  if b_i is 1, then place s_i in Y, but
  if b_i is 0, then do not place s_i in Y.

Claim: Function g is onto

Let Q be a subset of S. Consider the n-digit binary number $b_1 b_2 \ldots b_n$ constructed as follows:
if $s_i \in Q$, set $b_i = 1$
if $s_i \notin Q$, set $b_i = 0$

By construction, $g(b_1 b_2 \ldots b_n) = Q$, showing that g is onto.

Finally, since g maps all integers from 0 to $2^n - 1$ onto $P(S)$, the number of elements in $P(S)$ cannot be greater than the number of integers from 0 to $2^n - 1$, namely 2^n, proving Part 2.
