We wish to prove that $|P(A)| = 2^{|A|}$. For example, if $A = \{0, 1\}$, then $P(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$, and we have $|A| = 2$ and $|P(A)| = 4$, which could be a number of formulas (ie $n+2, n*2, n^2, 2^n$ where $n = |A|$).

As discussed in class, the correct formula is $2^n$. The key insight is to see that adding one element to a set doubles the size of the powerset.

Why is this? Again consider $A = \{0, 1\}$ with $P(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. Now let $B = A \cup \{2\}$ and consider $P(B)$. We can divide the elements of $P(B)$ into two groups: those that do not contain the element 2 and those that do contain 2. Those that do not contain the element 2 are the subsets that do not contain the element 2, and those that do contain the element 2 are all of the members of $P(A)$. Also, each of those that do contain 2 can be formed from exactly one member of $P(A)$, and each member of $P(A)$ can be used to form exactly one element that does contain 2. Thus we have $|P(B)| = |P(A)| + |P(A)| = 2|P(A)|$.

Now we will use induction to prove that $|P(A)| = 2^{|A|}$ for any set $A$.

First, let $p(n)$ be the proposition that for any set $A$, if $|A| = n$, then $|P(A)| = 2^n$. We will prove by induction that $p(n)$ is true for all $n \geq 0$.

**Base case:** $n = 0$. For $A = \{\}$, we have $|A| = 0$ and $P(A) = P(\{\}) = \{\emptyset\}$ and so $|P(A)| = |\{\emptyset\}| = 1 = 2^0 = 2^n$ where $|A| = n$. This proves that $p(0)$ is true.

**Inductive case:** $n > 0$. Assume the following Inductive Hypothesis (IH): for any $k \geq 0$, assume that $p(k)$ is true, that is, for any set $A$, if $|A| = k$ then $|P(A)| = 2^k$.

Now we must prove that the IH implies that $p(k+1)$ is true, that is, for any set $B$, if $|B| = k+1$ then $|P(B)| = 2^{k+1}$. Now let $B$ be a set with $|B| = k+1 > 0$. Now for any $x \in B$ we can find the set $A = B - \{x\}$ which gives $B = A \cup \{x\}$ and $x \notin A$. Now consider the set $P(B)$. The elements of $P(B)$ can be divided into 2 groups: those that contain $x$ and those that do not. Those that do not contain $x$ are all of the members of $P(A)$. Also, each of those that do contain $x$ can be formed from exactly one member of $P(A)$, and each member of $P(A)$ can be used to form exactly one element that does contain $x$. Thus we have $|P(B)| = |P(A)| + |P(A)| = 2|P(A)|$. But by construction, $|A| = k$, and so by the IH, $|P(A)| = 2^k$ and so we have $2 \cdot |P(A)| = 2 \cdot 2^k = 2^{k+1}$. Thus we have $|P(B)| = 2^{k+1}$, and since $|B| = k+1$, we have proved that for any $k \geq 0$, the IH implies that $p(k+1)$ is true. That is, we have proved that for any $k \geq 0$, if $p(k)$ is true, then $p(k+1)$ is also true.

Therefore, from the base case and the inductive case, we conclude by induction that $p(n)$ is true for all $n \geq 0$, which is what was to be proved.

As an interesting final exercise, try to put one of the other formula (eg $2n$) into the proof and see that it fails. Finally, note the ligature in the previous sentence.