

Algorithm Design and Analysis
CS 376, Colby College
Prof. Eric Aaron
An Example Proof: $|\mathcal{P}(S)| = 2^{|S|}$

These notes include a detailed proof of the claim that for any finite set S , $|\mathcal{P}(S)| = 2^{|S|}$. In particular, it illustrates a subtle point about the induction, and how it can be remedied by being very clear about the inductive proof structure and the proof goal (i.e., the claim to be proved) at every step. This level of detail is integral to formal reasoning in Computer Science, a level of detail so precise that even computers can follow it (sort of)!

Although this level of full detail and clarity of inductive structure may not be required for full credit on CS376 exercises, it's still worth understanding, to help you improve as constructors of rigorous, formal proofs.

In general, in an inductive proof, please be sure to clearly state what the induction is over, and construct the proof accordingly. This may seem straightforward, but it can be very subtle and hard to do in some cases—and this was one of them!

Claim: $\forall S: \{\text{finite sets}\}. |\mathcal{P}(S)| = 2^{|S|}$.

Note that because this is not directly a universally quantified statement about integers or natural numbers—or, more generally, about all elements of a recursively defined set—this is not *as stated* a candidate for proof by induction. Fortunately, it can be readily rewritten ... that phrase “finite set” does a lot of heavy lifting! It means that the sets we’re considering are those that have a natural number as their size. So, the set of all finite sets is the set of all sets with some natural number size, and really, the claim to be proved here is:

Claim: $\forall n: \mathbb{N}. \forall S. (|S| = n) \rightarrow (|\mathcal{P}(S)| = 2^{|S|})$.

This is something we can prove by induction! We proceed by induction on n over the natural numbers.

Base Case: The base case is $n = 0$. It remains to prove that $\forall S. (|S| = 0) \rightarrow (|\mathcal{P}(S)| = 2^{|S|})$. So, consider arbitrarily chosen set S ; for that S , we need to show $(|S| = 0) \rightarrow (|\mathcal{P}(S)| = 2^{|S|})$. So, assume $|S| = 0$, and show $|\mathcal{P}(S)| = 2^{|S|}$.

Because $|S| = 0$, $\mathcal{P}(S) = \{\emptyset\}$, so $|\mathcal{P}(S)| = 1 = 2^0 = 2^{|S|}$, completing the base case.

This next part is where people often loosen their grip on precision and detail in this proof! Note the clarity of the inductive hypothesis in this formulation, and how neatly it supports the inductive case:

IH: Assume that for arbitrarily chosen k , $\forall S. (|S| = k) \rightarrow (|\mathcal{P}(S)| = 2^{|S|})$.

Inductive Case: Using the IH, show that $\forall S. (|S| = k + 1) \rightarrow (|\mathcal{P}(S)| = 2^{|S|})$. To do this,

consider arbitrarily chosen set S ; for that S , we'll show $(|S| = k + 1) \rightarrow (|\mathcal{P}(S)| = 2^{|S|})$. So, assume $|S| = k + 1$, and show $|\mathcal{P}(S)| = 2^{|S|}$.

Because $|S| = k + 1 \geq 1$, there must be at least one element of S . Consider an arbitrarily chosen element $x \in S$, and let $S' = S - \{x\}$. By definition of set difference, $|S'| = |S| - 1 = (k + 1) - 1 = k$; by the IH, $|\mathcal{P}(S')| = 2^{|S'|} = 2^k$. **And we know the IH applies, because it is explicitly for every set of size k** —there is no concern about whether or not it applies to the particular subset of S formed by subtracting x , a detail that many arguments do not acknowledge.

From here, the proof is completed by the ideas with which you are familiar: Any $T \in \mathcal{P}(S)$ is either such that $T \in \mathcal{P}(S')$ or $T = T' \cup \{x\}$ for some $T' \in \mathcal{P}(S')$; that is, $\mathcal{P}(S) = \mathcal{P}(S') \cup \{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}$.

Note that because $x \notin S'$, exactly one of those—either $T \in \mathcal{P}(S')$, or $T = T' \cup \{x\}$ for some $T' \in \mathcal{P}(S')$ —is true for any $T \in \mathcal{P}(S)$.

Moreover, any set of form $T' \cup \{x\}$ can be formed in only one unique way, from that particular $T' \in \mathcal{P}(S')$, so $|\{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}| = |\{T' \mid T' \in \mathcal{P}(S')\}| = |\mathcal{P}(S')|$.

Therefore, by properties of set union and disjoint sets, $|\mathcal{P}(S)| = |\mathcal{P}(S') \cup \{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}| = |\mathcal{P}(S')| + |\{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}| = |\mathcal{P}(S')| + |\mathcal{P}(S')| = 2|\mathcal{P}(S')|$. By the IH, that equals $2(2^k) = 2^{k+1}$, which shows that $|\mathcal{P}(S)| = 2^{k+1}$, which is $2^{|S|}$ because of the assumption $|S| = k + 1$.

Notes from your Prof.

- This inductive proof explicitly states the IH and states where / how it is applied. Please be sure to do that in all mathematical induction proofs for CS376.
- A subtle point: Without noting that $\mathcal{P}(S')$ and $\{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}$ are disjoint sets (i.e., they have no element in common, because $x \notin S'$), we can't make the claim that $|\mathcal{P}(S') \cup \{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}| = |\mathcal{P}(S')| + |\{T' \cup \{x\} \mid T' \in \mathcal{P}(S')\}|$, on which the proof relies. (Please see me if there are questions about this!)
- The differences in details between this write-up and a different inductive proof write-up can be very subtle—often, students don't see it at first. Please feel free to have a one-on-one conversation with me, so I can help clear things up for you, if you'd like!
- As mentioned above, in most, if not all cases, this full level of detail and clarity in inductive structure above isn't required for full credit on exercises in CS376. Still, understanding it will help you develop abstract reasoning skills that are helpful for showing algorithm correctness. As always, please feel free to talk with your Prof. if you have any questions!