

Theory of Computation
CS 378, Colby College
Prof. Eric Aaron
An Example Proof: $\forall S. S \subseteq S$

These notes include a fully detailed proof of the proposition $\forall S. S \subseteq S$. In particular, it illustrates the principle that every inference step has a reason, and for formal proofs in Computer Science—a discipline in which formal reasoning needs to at a level of detail so precise that even computers can follow it (sort of)!—those reasons should be explicitly given as part of a proof.

Claim: Every set S is a subset of itself. Stated formally, $\forall S. S \subseteq S$.

Proof: Before starting the proof, it's good to write down the needed definitions—this saves the cognitive demand of needing to remember them or look them up elsewhere.

Definition: S is a subset of T , written $S \subseteq T$, exactly when $\forall x. x \in S \rightarrow x \in T$.

Then, as the first step in showing $\forall S. S \subseteq S$, because it's a universal quantification, we consider an arbitrarily chosen set—for convenience, we'll call it S —and for that particular S , we **need to prove** $S \subseteq S$. This is the standard, general technique for proving a proposition of the form $\forall x. P(x)$: Consider an arbitrarily chosen entity of the proper type, and prove that proposition P holds for that entity. (Please talk with your Prof. if this inference step is unfamiliar to you!)

Now, it remains to show $S \subseteq S$. By the definition of subset (given above) applied to $S \subseteq S$, we **need to prove** $\forall x. x \in S \rightarrow x \in S$. For that universally quantified proposition, we consider arbitrarily chosen x and **need to prove** $x \in S \rightarrow x \in S$.

Because we need to prove an implication, we use the standard technique of assuming the *antecedent* (the proposition on the left side of the implication arrow, the “if” part) and under that assumption, proving the *consequent* (the proposition on the right side of the implication arrow, the “then” part). So, we assume $x \in S$, and under that assumption, we **need to prove** $x \in S$. Because $x \in S$ has been assumed, it must be true, which completes the proof.

Notes from your Prof.

- When writing a proof and reducing the original Claim to sub-claims that need to be proved, it's not necessary to underline / boldface / whatever the **need to prove** parts that indicate those sub-claims. For my own style, I think that doing so makes it easier to follow the proof structure, so I choose to do so; there's no problem with you using different style for your proofs, as long as every step is clear and all relevant details are present in your proofs.
- Many times, proofs are written using *implicit universal quantification*—that is, if a variable isn't given a particular meaning, it's assumed to be universally quantified. With this convention, the original claim would be written as $S \subseteq S$ (with S universally

quantified, but not explicitly written as such—it’s implicit universal quantification!), and the claim after applying the definition of subset would be written as $x \in S \rightarrow x \in S$ (with x universally quantified, implicitly). Using this convention, proofs also often do not make the “consider arbitrarily chosen ...” step explicit.

In the proof above, to illustrate all of the steps in the proof, I explicitly included these details. Whatever style you choose to use for writing proofs, it is important for you as a computer scientist to know what all the steps are when dealing with variables in your proofs! (As always, please feel free to talk with your Prof. if you have any questions!)