

**CSC165
DIRECT PROOFS**

GARY BAUMGARTNER

SOME EXAMPLES

Consider

$$(S1) \exists i \in N, \forall j \in N, j > i \rightarrow a_j < a_i$$

and the two sequences

$$(A) 1, 2, 3, 2, 1, 2, 3, 2, 1, 2, 3, 2, 1, 2, \dots$$

$$(B) 4, 3, 2, 1, 4, 3, 2, 4, 3, 3, 3, 3, 3, \dots$$

S1 can be summarized informally: there's an element larger than all the elements after it.

S1 is true for B: $i = 7$ is an example.

S1 is false for A: every value occurs again. Alternatively: every element is at most 3, and there's always another 3.

A and B were given informally: they rely on us to look at the sequence and see what's going on (especially: fill in the ...). For a formal proof, we want a formal definition of A and B, to use with our formal definition of S1.

$$B: \forall i \in N, a_i = \begin{cases} 4, & i = 0 \vee i = 4 \vee i = 7 \\ 3, & i = 1 \vee i = 5 \vee i \geq 8 \\ 2, & i = 2 \vee i = 6 \\ 1, & i = 3 \end{cases}.$$

Here's our proof of S1 for B:

Let $i = 7$.

Then $i \in N$.

Let $j \in N$.

Suppose $j > i$.

Then $j > 7$, so $j \geq 8$.

Thus $a_j = 3 < 4 = a_7 = a_i$.

So $a_j < a_i$.

Hence $j > i \rightarrow a_j < a_i$.

Since j is an arbitrary element of N : $\forall j \in N, j > i \rightarrow a_j < a_i$.

Since $i \in N$: $\exists i \in N, \forall j \in N, j > i \rightarrow a_j < a_i$.

$$A: \forall i \in N, a_i = \begin{cases} 1. & i \text{ is a multiple of } 4 \\ 2. & i \text{ is odd} \\ 3. & i \text{ is 2 more than a multiple of } 4 \end{cases}.$$

To prove S1 is false for A, we prove its negation: $\forall i \in N, \exists j \in N, j > i \wedge a_j \geq a_i$.

Let $i \in N$.

Let $j = 4i + 2$.

Then $j \in N$, since $i \in N$.

Also, $j = 4i + 2 = 3i + i + 2 \geq i + 2$, since $i \geq 0$.

Thus $j \geq i + 2 > i$.

Also, $a_j = a_{4i+2} = 3 \geq a_i$, since all the elements of A are ≤ 3 .

Hence $j > i \wedge a_j \geq a_i$.

Since $j \in N: \forall j \in N, j > i \wedge a_j \geq a_i$.

Since i is an arbitrary element of $N: \forall i \in N, \exists j \in N, j > i \wedge a_j \geq a_i$.

USING A UNIVERSAL

Once we've proven a statement, we can call it a "theorem", "lemma", "proposition", or "corollary". These all mean that the statement is known to be true. How to choose among the four labels we don't go into here.

Recall that we proved the following.

Theorem. $\forall x \in R, x > 0 \rightarrow \frac{1}{x+2} < 3$.

Let's try to prove

$$(S2) \forall x \in R, x \neq 0 \rightarrow \frac{1}{x^2+2} < 3.$$

First, let's think of the theorem like a Java method. It takes an argument of a certain type: a real number x . If we've established the precondition $x > 0$ then we get back $\frac{1}{x+2} < 3$.

We could try to prove S2 by mimicing the proof of the theorem. But this would be like using a method by copying its code, rather than just calling it. So we'll try to use the theorem (not its proof) to prove S2:

Let $x \in R$.

Suppose $x \neq 0$.

Then $x^2 \in R$.

Also, $x^2 \geq 0$.

Since $x \neq 0$, $x^2 \neq 0$.

So $x^2 > 0$.

Since $x^2 \in R$ and $x^2 > 0$, the theorem tells us that $\frac{1}{x^2+2} < 3$.

Hence $x \neq 0 \rightarrow \frac{1}{x^2+2} < 3$.

Since x is an arbitrary element of $R: \forall x \in R, x \neq 0 \rightarrow \frac{1}{x^2+2} < 3$.

Using the Java analogy: we made sure that x^2 satisfied the preconditions, then we passed it to the theorem, then we got the result back for x^2 . Notice that, just like in Java, the name of the parameter is irrelevant when we use the result.

USING AN EXISTENTIAL

Recall from your calculus course:

Theorem. *If a function from R to R is continuous, then it is bounded above on $[0, 1]$.*

Let F = the set of functions from R to R .

For $f \in F$, let $c(f) = f$ is continuous.

We can phrase the theorem more formally.

Theorem. $1 \forall f \in F, c(f) \rightarrow \exists m \in R, \forall x \in R, 0 \leq x \leq 1 \rightarrow f(x) \leq m.$

This kind of result is difficult to prove from scratch (see your calculus course for details). But once we have this theorem, we can prove some similar theorems from it. We'll use it to prove that every continuous function from R to R is bounded below on $[0, 1]$, i.e.

$$(S3) \forall f \in F, c(f) \rightarrow \exists m \in R, \forall x \in R, 0 \leq x \leq 1 \rightarrow f(x) \geq m.$$

To do this we'll also need a second result from calculus.

Theorem. $2 \forall f \in F, c(f) \rightarrow c(-f).$

Here's the proof of of S3:

Let $f \in F$.

Suppose $c(f)$.

By Theorem 2, $c(-f)$.

Also, $-f \in F$, so by Theorem 1: $\exists m \in R, \forall x \in R, 0 \leq x \leq 1 \rightarrow -f(x) \leq m.$

Let $m_0 \in R$ be such that $\forall x \in R, 0 \leq x \leq 1 \rightarrow -f(x) \leq m_0$ (*).

[This is how we use an existential: introduce a variable with the property].

Let $m = -m_0$. Then $m \in R$.

Let $x \in R$.

Suppose $0 \leq x \leq 1$.

Then by (*), $-f(x) \leq m_0$.

So $f(x) \geq -m_0 = m$.

Thus $0 \leq x \leq 1 \rightarrow f(x) \geq m$.

Since x is an arbitrary element of R : $\forall x \in R, 0 \leq x \leq 1 \rightarrow -f(x) \geq m$.

Since $m \in R$: $\exists m \in R, \forall x \in R, 0 \leq x \leq 1 \rightarrow -f(x) \geq m$.

Thus $c(f) \rightarrow \exists m \in R, \forall x \in R, 0 \leq x \leq 1 \rightarrow -f(x) \geq m$.

Since x is an arbitrary element of R :

$\forall f \in F, c(f) \rightarrow \exists m \in R, \forall x \in R, 0 \leq x \leq 1 \rightarrow f(x) \geq m$.