Verificación Formal PCIC 2021-2
Un pequeño ejemplo de distintos estilos de prueba.

Favio Ezequiel Miranda Perea   Lourdes Del Carmen González Huesca

26 de octubre de 2020

El texto está en inglés pues corresponde a un fragmento de un artículo sometido a publicación.

Theorem 1. *There does not exist a natural number n such that* $0 < n < 1$.

Demostración. This is an immediate consequence of the well-ordering principle. □

The above can be considered as a traditional "proof" completely correct and acceptable from an advanced point of view. However, it does not provide enough elements to be mechanized or written as an actual rigorous proof.

Let us next present a textbook traditional proof.

Theorem 2 (A textbook proof)**.** *There does not exist a natural number n such that* $0 < n < 1$.

Demostración. Let $S = \{n \in \mathbb{N} \mid 0 < n < 1\}$ and assume $S \neq \varnothing$. Take $r \in S$ to be the least element in S. Therefore $0 < r < 1$ which implies $0 < r^2 < r < 1$. Thus $r^2 \in S$, which contradicts the minimality of r. Therefore S must be empty. □

This traditional textbook proof, though rigorous, is not suitable to be directly formalized in a Proof Assitant (PA), for apart of the implicit background knowledge required, it does not make explicit a train of thought useful to guide the mechanization. Our experiment consisted of mechanizing the above theorem according to different common strategies of reasoning. First we use forward reasoning, which means going exclusively from the hypotheses towards the conclusion.

Theorem 3 (Forward proof)**.** *There does not exist a natural number n such that* $0 < n < 1$.

Demostración. We assume that $\exists n \in \mathbb{N}$ such that $0 < n < 1$. The well-ordering principle allow us to take a minimal $r \in \mathbb{N}$ such that $0 < r < 1$. Since $0 < r$ we get $0 = 0 \cdot r < r \cdot r$ and as $r < 1$ we obtain $r \cdot r < 1 \cdot r = r$. Thus $0 < r^2 < r$. From this, as $r < 1$, we get $0 < r^2 < 1$. The minimality of r implies now that $r \leq r^2$, which leads us to $r^2 \not< r$, yielding a contradiction. □

Let us observe that in this proof there is no reference to the set S used in the proof of Theorem 2, for its use would complicate the mechanization in a unnecesary way. The proof looks similar to the previous one but it has an explicit forward structure and it provides us with more explanations. The proof script was constructed having Theorem 2 as a guideline using forward reasoning exclusively. This means we avoid the native backward mechanisms of the PA, which resulted in an awkward computer-assisted proof.

Next we explore the opposite approach by constructing a proof using exclusively the backward strategy. The result is Theorem 4 and was obtained discarding the previous proofs as a guideline, using only the same auxiliary results, namely the transitivity of the order relation, its compatibility with respect to the product and the relationship between the order relations . Since the example is quite elementary, this proof was constructed directly in the PA without resorting to pencil and paper.

Theorem 4 (Backward proof)**.** *There does not exist a natural number n such that* $0 < n < 1$*.*

Demostración. We assume that $\exists n \in \mathbb{N}$ such that $0 < n < 1$. Thus, the well-ordering principle allow us to take a minimal $r \in \mathbb{N}$ such that $0 < r < 1$. We will arrive to a contradiction by showing that $r \cdot r \not< r$ and $r \cdot r < r$. To show $r \cdot r \not< r$ it suffices to show $r \leq r \cdot r$. To prove this, we use the minimality of r, and are required to show $0 < r \cdot r < 1$. We separately prove the two inequalities: the first one ($0 < r \cdot r$) is a consequence of $0 \cdot r < r \cdot r$, which is solved by the known fact $0 < r$. For the second inequality it is enough to prove $r \cdot r < r < 1$. Again, it suffices to prove the two inequalities separately. The first one is a consequence of $r \cdot r < 1 \cdot r$, which in turn is entailed by the known fact $0 < r < 1$. The second inequality $r < 1$ is already known. This finishes the proof of $r \cdot r \not< r$. The remaining inequality $r \cdot r < r$ was already proven within the previous case. □

Theorem 4 presents a verbose proof which, in comparison with the usual mathematical proof-writing style, has a cumbersome structure due to the exclusive use of backward reasoning. On the other hand, its mechanization is concise and more readable than the previous one. Let us also observe that the mechanization necessarily contains some mandatory low-level parts, like the need to repeat the proof (that is, the sequence of tactics) corresponding to show $r \cdot r < r$, which is undesirable from a programmer point of view. This and some other low-level issues can be partially prevented [1] but others like the explicit term rewriting of term r with term $1 \cdot r$ are unavoidable.

Consider now the following proof, which was obtained by using Theorem 2 as a guideline but also mantaining a full interaction with the PA.

Theorem 5 (Bidirectional proof)**.** *There does not exist a natural number n such that* $0 < n < 1$*.*

Demostración. We assume that $\exists n \in \mathbb{N}$ such that $0 < n < 1$ and arrive to a contradiction. The well-ordering principle allow us to take a minimal $r \in \mathbb{N}$ such that $0 < r < 1$. We first claim that $r \cdot r < r$. Since $0 < r < 1$, we get $r \cdot r < 1 \cdot r$, that is $r \cdot r < r$. Next, we explicitly contradict the previous claim by showing $r \cdot r \not< r$. To this purpose it suffices to show $r \leq r \cdot r$. From $0 < r$ we get $0 = 0 \cdot r < r \cdot r$. Further, $r \cdot r < r$ and $r < 1$ yield $r \cdot r < 1$. By the minimality of r, to show the required $r \leq r \cdot r$, it suffices to show $0 < r \cdot r < 1$, but this has already been proven. □

As expected this proof has the best of both worlds, namely a well organized text together with a concise proof script. This structure was obtained by a parallel construction of both proofs, one that adequately combines forward and backward reasoning. The full interaction with the PA helped to enhance the argumentation, in particular this proof lacks repeated subproofs, like the one for $r \cdot r < r$ in the proof of Theorem 4.

Finally, let us present a proof gained directly from a proof script whose motivation is to show a simpler mechanization than those already presented. One that does not use library theorems and which is certainly more succint than the previous ones Its simplicity lies on the use of the definitions of $<$ and $\leq$ given in the core library (automatically loaded when starting Coq).

Theorem 6. *There does not exist a natural number n such that* $0 < n < 1$*.*

Demostración. Assuming that there is a natural n such that $0 < n < 1$ we will arrive to a contradiction. We have $0 < n$ and $n < 1$. According to the definition of $n < 1$ we have $S\,n \leq 1$, which by definition yields two cases

- $S\,n = 1$. Then we have $n = 0$ and therefore $0 < 1$ and $0 < 0$, which yields the contradiction.
- $S\,n \leq 0$. This a direct contradiction.

□

[1] For instance by first proving $r \cdot r < r$ as an auxiliary lemma or at the beginning of the proof as in Theorem 5.