

Proofs with quantifiers.A) $\exists x \in X: Q(x)$.One way of proving such a statement is by construction: produce an explicit $x \in X$ satisfying $Q(x)$.

Proof template:

Proposition. $\exists x \in X: Q(x)$.Proof.Let $x =$ [write down an $x \in X$ that works.
Then demonstrate that it works]. So $Q(x)$.

□

Example:

Proposition 1. $\exists n \in \mathbb{N}, 2^{2^n} + 1$ is composite (not prime).Proof.Let $n = 5$. Then $2^{2^n} + 1 = 2^{2^5} + 1 = 4294967297$
 $= 641 \cdot 6700417$, so $2^{2^n} + 1$ is composite.

Not all existence proofs are constructive:

Proposition 2. $\exists p \in \{\text{prime numbers}\}, p > 10^{10}$.ProofWe know (to be proved later) that $\exists$ infinitely many primes. List them in increasing order: $p_1, p_2, p_3, \dots$ Each prime p_n is at least one larger than the

(2)

previous one (since primes are integers), so eventually,

$$p_n > 10^{10^{10}}.$$

(For example, choosing $n = 10^{10} + 1$ will work.)

(B) $\forall x \in X, Q(x)$.

This statement is the same as
 $x \in X \Rightarrow Q(x)$.

Proof template:

Proposition. $\forall x \in X, Q(x)$.

Proof.

Assume $x \in X$. [Then do what's necessary to show:] Therefore, $Q(x)$.

So $\forall x \in X, Q(x)$.
 (optional)

□

Example (see HW5, S-POP Exercise B(iii)-1):

Proposition 3.

$$\forall m \in \mathbb{Z}, 6 \mid m(m+1)(m+2).$$

Proof.

Assume $m \in \mathbb{Z}$. By S-POP Exercise B(i)-9, an integer n is divisible by 6 iff n is even and divisible by 3. So it will suffice to show that $m(m+1)(m+2)$ is even and is divisible by 3.

1) To show $m(m+1)(m+2)$ is even, write

$m = 2k + r$, where $k, r \in \mathbb{Z}$ and either $k=0$ or $k=1$. We consider two cases:

a) $r=0$. [DIY: meaning "do it yourself."]

b) $r=1$. Then $m=2k+1$, so

$$\begin{aligned} m(m+1)(m+2) &= (2k+1)(2k+2)(2k+3) \\ &= 2 \cdot ((2k+1)(k+1)(2k+3)), \end{aligned}$$

so m is even.

In either case ($r=0$ or $r=1$), $m(m+1)(m+2)$ is even.

2) To show that $3 \mid m(m+1)(m+2)$, use the division algorithm to write

$$m = 3l + r$$

where $l, r \in \mathbb{Z}$ and $l=0, 1$, or 2 . We consider three cases:

a) $r=0$. Then $m=3l$, so

$$m(m+1)(m+2) = \dots \text{ [DIY]}$$

b) $r=1$. [DIY]

c) $r=2$. [DIY]

In each case ($r=0, 1$, or 2), ... [DIY].

So $m(m+1)(m+2)$ is both even and divisible by 3. Therefore, [DIY].

□