Given a specification \( P \) and a prestate \( \sigma \) with \( t \) as time variable, we might define “the exact precondition for termination” as follows:

\[
\exists n: \text{nat} \cdot \forall \sigma' \cdot t' \leq t+n \iff P
\]

Letting \( x \) be an integer variable, find the exact precondition for termination of the following, and comment on whether it is reasonable.

(a) \( x \geq 0 \Rightarrow t' \leq t+x \)

§

\[\exists n: \text{nat} \cdot \forall x', t' \cdot t' \leq t+n \iff (x \geq 0 \Rightarrow t' \leq t+x) \quad \text{idempotence for } x' \; ; \; \text{material imp} \]

\[= \exists n: \text{nat} \cdot \forall t' \cdot t' \leq t+n \iff (x < 0 \lor t' \leq t+x) \quad \text{antidistribution; distribution} \]

\[= \exists n: \text{nat} \cdot (\forall t' \cdot t' \leq t+n \iff x < 0) \land (\forall t' \cdot t' \leq t+n \iff t' \leq t+x) \quad \text{distrib; connection} \]

\[= \exists n: \text{nat} \cdot (t=\infty \iff x < 0) \land t+n \geq t+x) \]

\[= x \geq 0 \lor t=\infty \]

If \( x \) starts with a nonnegative value, it seems reasonable that \( x \geq 0 \Rightarrow t' \leq t+x \) requires termination. If the computation starts at time \( \infty \) (which means it never starts, because it comes after an infinite loop), it seems unreasonable to require termination. On the other hand, you cannot observe a computation starting at time \( \infty \) and then failing to terminate, so this disjunct is vacuous.

(b) \( \exists n: \text{nat} \cdot t' \leq t+n \)

§

\[\exists m: \text{nat} \cdot \forall x', t' \cdot t' \leq t+m \iff \exists n: \text{nat} \cdot t' \leq t+n \]

\[= \exists m: \text{nat} \cdot \forall x', n \cdot t' \leq t+m \iff t' \leq t+n \]

\[= \exists m: \text{nat} \cdot \forall n \cdot n < m \lor t=\infty \]

\[= t=\infty \]

If the computation starts at a finite time, this specification does not require termination. Although the specification says that there is a constant upper bound on the execution time, it leaves that constant totally unspecified. An observer would never be able to complain that a computation has taken too long — even if the computation is infinite. But if the computation starts at time \( \infty \), the comment of part (a) applies.

(c) \( \exists f: \text{int} \rightarrow \text{nat} \cdot t' \leq t + fx \)

§ This is just like part (b).

\[\exists m: \text{nat} \cdot \forall x', t' \cdot t' \leq t+m \iff \exists f: \text{int} \rightarrow \text{nat} \cdot t' \leq t + fx \]

\[= \exists m: \text{nat} \cdot \forall x', f \cdot t' \leq t+m \iff t' \leq t+fx \]

\[= \exists m: \forall f \cdot fx \leq m \lor t=\infty \]

\[= t=\infty \]