171 (termination) Each of the following formulas attempts to say that specification S requires termination from prestate σ :

(i) $\forall \sigma' \cdot\ S \wedge t<\infty \Rightarrow t'<\infty$

(ii) $\forall \sigma' \cdot\ S \Rightarrow \exists n\colon nat \cdot\ t' \le t+n$

According to each formula, for what prestates does the following specification require termination? Comment on whether it is reasonable. That's $2\times3 = 6$ questions.

(a) $x\ge0 \Rightarrow x'=0 \wedge t' = t+x$ where x is an integer variable

(b) $t<\infty \Rightarrow t'<\infty$

(c) $\exists n\colon nat \cdot\ t' \le t+n$

After trying the question, scroll down to the solution.

§ The formulas are supposed to say whether specification S requires termination. According to the textbook Subsection 4.2.2, "specifying termination without a practical time bound is worthless" because we cannot observe nontermination. The Oxford University philosopher Karl Popper goes further: he says that it's scientifically meaningless to talk about termination without a time bound. In Information Theory, the statement "Execution of S terminates." conveys no information (0 bits of information). According to Bayesian probability, we cannot confirm something (increase its probability) without a test that can potentially disconfirm it (decrease its probability), and there is no test that can disconfirm termination without a time bound. That's a lot of agreement that termination without a time bound is worthless. So it doesn't really matter what formulas (i) and (ii) say about the termination of (a), (b), and (c). (For more on this, see Observations on the Halting Problem.)

Formula (i) says that execution of S , started at a finite time, ends at a finite time. Formula (ii) appears to say more: it says that execution of S ends within a time bound. But formula (ii) doesn't say what the time bound is; it just says the time bound "exists". The following calculation simplifies our task.

$\exists n{:}\ nat\cdot\ t' \le t+n$ — case idempotent
$=$ $\exists n\cdot$ **if** $t{=}\infty$ **then** $t' \le t+n$ **then** $t' \le t+n$ **fi** — context
$=$ $\exists n\cdot$ **if** $t{=}\infty$ **then** $t' \le \infty+n$ **then** $t' \le t+n$ **fi** — absorption
$=$ $\exists n\cdot$ **if** $t{=}\infty$ **then** $t' \le \infty$ **then** $t' \le t+n$ **fi** — extreme
$=$ $\exists n\cdot$ **if** $t{=}\infty$ **then** $\top$ **then** $t' \le t+n$ **fi** — one case, inclusion
$=$ $\exists n\cdot\ t{<}\infty \Rightarrow t' \le t+n$ — in $t+n$, t and n are finite
$=$ $t{<}\infty \Rightarrow t'{<}\infty$

So (b) and (c) are equal specifications. And

$\forall \sigma'\cdot\ S \Rightarrow \exists n{:}\ nat\cdot\ t' \le t+n$ — just proven
$=$ $\forall \sigma'\cdot\ S \Rightarrow (t{<}\infty \Rightarrow t'{<}\infty)$ — portation
$=$ $\forall \sigma'\cdot\ S \wedge t{<}\infty \Rightarrow t'{<}\infty$

So (i) and (ii) are equal formulas. Saying there is a time bound without saying what the bound is just says the time is finite. That reduces the 6 questions to 2 questions.

(a i) $\forall x', t'\cdot\ (x{\ge}0 \Rightarrow x'{=}0 \wedge t' = t{+}x) \wedge t{<}\infty \Rightarrow t'{<}\infty$ — case idempotent
$=$ $\forall x', t'\cdot$ **if** $t'{=}\infty$ **then** $(x{\ge}0 \Rightarrow x'{=}0 \wedge t' = t{+}x) \wedge t{<}\infty \Rightarrow t'{<}\infty$
else $(x{\ge}0 \Rightarrow x'{=}0 \wedge t' = t{+}x) \wedge t{<}\infty \Rightarrow t'{<}\infty$ **fi** — context
$=$ $\forall x', t'\cdot$ **if** $t'{=}\infty$ **then** $(x{\ge}0 \Rightarrow x'{=}0 \wedge \infty = t{+}x) \wedge t{<}\infty \Rightarrow \bot$
else $(x{\ge}0 \Rightarrow x'{=}0 \wedge t' = t{+}x) \wedge t{<}\infty \Rightarrow \top$ **fi**
in $\infty = t+x$, x is finite, so t must be infinite
in **then**-part, indirect, inclusion
in **else**-part, base
$=$ $\forall x', t'\cdot$ **if** $t'{=}\infty$ **then** $\neg(x{\ge}0 \Rightarrow x'{=}0 \wedge t{=}\infty) \vee t{=}\infty$ **else** $\top$ **fi** — one case
$=$ $\forall x', t'\cdot\ t'{=}\infty \Rightarrow \neg(x{\ge}0 \Rightarrow x'{=}0 \wedge t{=}\infty) \vee t{=}\infty$ — one-point for t'
$=$ $\forall x'\cdot\ \neg(x{\ge}0 \Rightarrow x'{=}0 \wedge t{=}\infty) \vee t{=}\infty$ — context
$=$ $\neg(x{\ge}0 \Rightarrow x'{=}0 \wedge \bot) \vee t{=}\infty$ — base
$=$ $\neg(x{\ge}0 \Rightarrow \bot) \vee t{=}\infty$ — indirect
$=$ $\neg(x{<}0) \vee t{=}\infty$
$=$ $x{\ge}0 \vee t{=}\infty$

This says that (a) requires termination if $x{\ge}0$, which is reasonable. It also says (a) requires termination if $t{=}\infty$. If (a) sequentially follows an infinite loop, then the loop ends at time ∞ (it never ends), so (a) starts at time ∞ (it never starts), and its execution must terminate. That makes no sense.

(a ii) same as (a i).

(b i)
$$\begin{array}{lll} & \forall t' \cdot\ (t<\infty \Rightarrow t'<\infty) \wedge t<\infty\ \Rightarrow\ t'<\infty & \text{portation} \\ = & \forall t' \cdot\ (t<\infty \Rightarrow t'<\infty) \Rightarrow (t<\infty\ \Rightarrow\ t'<\infty) & \text{reflexive} \\ = & \forall t' \cdot\ \top & \text{identity} \\ = & \top & \end{array}$$

This says that (b) always requires termination, which is what (b) says. But

$$t<\infty \Rightarrow t'<\infty \quad \Leftarrow \quad t := t+1.\ t<\infty \Rightarrow t'<\infty$$

so (b) can be implemented as an infinite loop, contrary to what (b) says. That's because an observer cannot say whether execution will terminate.

(b ii) same as (b i).

(c i) same as (b i).

(c ii) same as (b i).