$A == [ns : \mathbb{F}\,\mathbb{N}_1]$
$AInit == [A' \mid ns' = \varnothing]$
$New == [\Delta A;\ n? : \mathbb{N}_1 \mid ns' = ns \cup \{n?\}]$
$MSF == [\Xi A;\ m! : \mathbb{N}_1 \mid ns \neq \varnothing;\ m! = max\ ns]$

$$
\begin{array}{|l}
\text{— } AM2SF \text{ —}\\
\Xi A \\
m1!, m2! : \mathbb{N}_1 \\
\hline
\#\, ns > 1 \\
m1! = max\ ns \\
m2! = max\ (ns \setminus \{m1!\}) \\
\hline
\end{array}
$$

Injective seq ensures the 2 msf are unique.

$$
\begin{array}{|l}
\text{— } C3 \text{ —}\\
cs : \mathrm{iseq}\,\mathbb{N}_1 \\
\hline
(\_ < \_) \fatsemi cs \subseteq cs \fatsemi (\_ < \_) \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\text{— } C3Init \text{ —}\\
C3' \\
\hline
cs' = \langle\rangle \\
\hline
\end{array}
$$

$LI3 == [A;\ C3 \mid ns = ran\ cs]$

Note $cs \setminus \langle ma! \rangle$ is not equivalent,
because a sequence is a function, and the domain mapping of $\langle ma! \rangle$ is different to cs
(You did it wrong this way before)

$$
\begin{array}{|l}
\text{— } C3MSF2 \text{ —}\\
\Xi C3;\ ma!, mb! : \mathbb{N}_1 \\
\hline
\#(ran\ cs) \geq 2 \\
ma! = last\ cs \\
mb! = cs\,(\#\, cs - 1) \\
\hline
\end{array}
$$

Prove that C3 refines the Abstract specification of the widget nodule machine:

$$\forall\, C3' \bullet C3Init \Rightarrow \exists\, A' \bullet LI' \wedge AInit$$

$$[De - sugar]$$

$$\forall\, cs' : \mathrm{iseq}\, \mathbb{N}_1 \mid (\_ < \_) \mathbin{;} cs' \subseteq cs' \mathbin{;} (\_ < \_) \bullet cs' = \langle\rangle \Rightarrow \\ \quad \exists\, ns' : \mathbb{F}\, \mathbb{N}_1 \bullet ns' = ran\ cs' \wedge ns' = \varnothing$$

$$[One\ point\ rule:\ ns']$$

$$\forall\, cs' : \mathrm{iseq}\, \mathbb{N}_1 \mid (\_ < \_) \mathbin{;} cs' \subseteq cs' \mathbin{;} (\_ < \_) \bullet cs' = \langle\rangle \Rightarrow \\ \quad \varnothing = ran\ cs'$$

$$[One\ point\ rule:\ cs']$$

$$\varnothing = ran\ \langle\rangle$$

$$[Definition\ ran]$$

$$True$$