Contents

1 SM0 Theory **3**

1.1 Datatypes 3

1.2 Definitions 3

1.3 Theorems 3

1 SM0 Theory

Built: 09 April 2019
Parent Theories: ssm1

1.1 Datatypes

```
command = NP npriv | PR privcmd

npriv = status

output = on | off

privcmd = launch | reset

staff = Alice | Bob | Carol

state = STBY | ACTIVE
```

1.2 Definitions

[certs2_def]

```
⊢ ∀cmd npriv privcmd.
     certs2 cmd npriv privcmd =
     [Name Carol controls prop (SOME (NP npriv));
      Name Carol says prop (SOME (PR privcmd)) impf prop NONE]
```

[certs_def]

```
⊢ ∀cmd npriv privcmd.
     certs cmd npriv privcmd =
     [Name Alice controls prop (SOME (NP npriv));
      Name Alice controls prop (SOME (PR privcmd));
      Name Bob controls prop (SOME (NP npriv));
      Name Bob says prop (SOME (PR privcmd)) impf prop NONE]
```

[SM0StateInterp_def]

```
⊢ ∀state. SM0StateInterp state = TT
```

1.3 Theorems

[Alice_exec_privcmd_justified_thm]

```
⊢ ∀NS Out M Oi Os.
     TR (M,Oi,Os) (exec (PR privcmd))
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
          (Name Alice says prop (SOME (PR privcmd))::ins) s
          outs)
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
          (NS s (exec (PR privcmd)))
          (Out s (exec (PR privcmd))::outs)) ⇔
     inputOK (Name Alice says prop (SOME (PR privcmd))) ∧
     CFGInterpret (M,Oi,Os)
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
          (Name Alice says prop (SOME (PR privcmd))::ins) s
          outs) ∧ (M,Oi,Os) sat prop (SOME (PR privcmd))
```

[Alice_justified_privcmd_exec_thm]

```
 ⊢ ∀NS Out M Oi Os cmd npriv privcmd ins s outs.
     inputOK (Name Alice says prop (SOME (PR privcmd))) ∧
     CFGInterpret (M,Oi,Os)
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
          (Name Alice says prop (SOME (PR privcmd))::ins) s
          outs) ⇒
     TR (M,Oi,Os) (exec (PR privcmd))
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
          (Name Alice says prop (SOME (PR privcmd))::ins) s
          outs)
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
          (NS s (exec (PR privcmd)))
          (Out s (exec (PR privcmd))::outs))
```

[Alice_privcmd_lemma]

```
 ⊢ CFGInterpret (M,Oi,Os)
     (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
        (Name Alice says prop (SOME (PR privcmd))::ins) s
        outs) ⇒
   (M,Oi,Os) sat prop (SOME (PR privcmd))
```

[Alice_privcmd_verified_thm]

```
 ⊢ ∀NS Out M Oi Os.
     TR (M,Oi,Os) (exec (PR privcmd))
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
          (Name Alice says prop (SOME (PR privcmd))::ins) s
          outs)
       (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
          (NS s (exec (PR privcmd)))
          (Out s (exec (PR privcmd))::outs)) ⇒
     (M,Oi,Os) sat prop (SOME (PR privcmd))
```

[Carol_discard_lemma]

```
 ⊢ TR (M,Oi,Os) discard
     (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
        (Name Carol says prop (SOME cmd)::ins) s outs)
     (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
        (SM0ns s discard) (SM0out s discard::outs))
```

[Carol_rejected_lemma]

```
⊢ ¬inputOK (Name Carol says prop (SOME $cmd$))
```

[command_distinct_clauses]

```
⊢ ∀$a'$ $a$. NP $a$ ≠ PR $a'$
```

[command_one_one]

```
⊢ (∀$a$ $a'$. (NP $a$ = NP $a'$) ⟺ ($a$ = $a'$)) ∧
  ∀$a$ $a'$. (PR $a$ = PR $a'$) ⟺ ($a$ = $a'$)
```

[inputOK2_def]

```
⊢ (inputOK2 (Name Carol says prop (SOME $cmd$)) ⟺ T) ∧
  (inputOK2 TT ⟺ F) ∧ (inputOK2 FF ⟺ F) ∧
  (inputOK2 (prop $v$) ⟺ F) ∧ (inputOK2 (notf $v_1$) ⟺ F) ∧
  (inputOK2 ($v_2$ andf $v_3$) ⟺ F) ∧ (inputOK2 ($v_4$ orf $v_5$) ⟺ F) ∧
  (inputOK2 ($v_6$ impf $v_7$) ⟺ F) ∧ (inputOK2 ($v_8$ eqf $v_9$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says TT) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says FF) ⟺ F) ∧
  (inputOK2 (Name Alice says prop (SOME $v142$)) ⟺ F) ∧
  (inputOK2 (Name Bob says prop (SOME $v142$)) ⟺ F) ∧
  (inputOK2 (Name $v132$ says prop NONE) ⟺ F) ∧
  (inputOK2 ($v133$ meet $v134$ says prop $v_{66}$) ⟺ F) ∧
  (inputOK2 ($v135$ quoting $v136$ says prop $v_{66}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says notf $v_{67}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says ($v_{68}$ andf $v_{69}$)) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says ($v_{70}$ orf $v_{71}$)) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says ($v_{72}$ impf $v_{73}$)) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says ($v_{74}$ eqf $v_{75}$)) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{76}$ says $v_{77}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{78}$ speaks_for $v_{79}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{80}$ controls $v_{81}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says reps $v_{82}$ $v_{83}$ $v_{84}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{85}$ domi $v_{86}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{87}$ eqi $v_{88}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{89}$ doms $v_{90}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{91}$ eqs $v_{92}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{93}$ eqn $v_{94}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{95}$ lte $v_{96}$) ⟺ F) ∧
  (inputOK2 ($v_{10}$ says $v_{97}$ lt $v_{98}$) ⟺ F) ∧
  (inputOK2 ($v_{12}$ speaks_for $v_{13}$) ⟺ F) ∧
  (inputOK2 ($v_{14}$ controls $v_{15}$) ⟺ F) ∧
  (inputOK2 (reps $v_{16}$ $v_{17}$ $v_{18}$) ⟺ F) ∧
  (inputOK2 ($v_{19}$ domi $v_{20}$) ⟺ F) ∧
  (inputOK2 ($v_{21}$ eqi $v_{22}$) ⟺ F) ∧
  (inputOK2 ($v_{23}$ doms $v_{24}$) ⟺ F) ∧
  (inputOK2 ($v_{25}$ eqs $v_{26}$) ⟺ F) ∧
  (inputOK2 ($v_{27}$ eqn $v_{28}$) ⟺ F) ∧
  (inputOK2 ($v_{29}$ lte $v_{30}$) ⟺ F) ∧ (inputOK2 ($v_{31}$ lt $v_{32}$) ⟺ F)
```

[inputOK2_ind]

$$
\begin{array}{l}
\vdash \forall P.\\
\quad (\forall \mathit{cmd}.\ P\ (\mathtt{Name\ Carol\ says\ prop\ (SOME}\ \mathit{cmd}\mathtt{)))}\ \land\ P\ \mathtt{TT}\ \land\ P\ \mathtt{FF}\ \land\\
\quad (\forall v.\ P\ (\mathtt{prop}\ v))\ \land\ (\forall v_1.\ P\ (\mathtt{notf}\ v_1))\ \land\\
\quad (\forall v_2\ v_3.\ P\ (v_2\ \mathtt{andf}\ v_3))\ \land\ (\forall v_4\ v_5.\ P\ (v_4\ \mathtt{orf}\ v_5))\ \land\\
\quad (\forall v_6\ v_7.\ P\ (v_6\ \mathtt{impf}\ v_7))\ \land\ (\forall v_8\ v_9.\ P\ (v_8\ \mathtt{eqf}\ v_9))\ \land\\
\quad (\forall v_{10}.\ P\ (v_{10}\ \mathtt{says\ TT}))\ \land\ (\forall v_{10}.\ P\ (v_{10}\ \mathtt{says\ FF}))\ \land\\
\quad (\forall \mathit{v142}.\ P\ (\mathtt{Name\ Alice\ says\ prop\ (SOME}\ \mathit{v142}\mathtt{)))}\ \land\\
\quad (\forall \mathit{v142}.\ P\ (\mathtt{Name\ Bob\ says\ prop\ (SOME}\ \mathit{v142}\mathtt{)))}\ \land\\
\quad (\forall \mathit{v132}.\ P\ (\mathtt{Name}\ \mathit{v132}\ \mathtt{says\ prop\ NONE))}\ \land\\
\quad (\forall \mathit{v133}\ \mathit{v134}\ v_{66}.\ P\ (\mathit{v133}\ \mathtt{meet}\ \mathit{v134}\ \mathtt{says\ prop}\ v_{66}))\ \land\\
\quad (\forall \mathit{v135}\ \mathit{v136}\ v_{66}.\ P\ (\mathit{v135}\ \mathtt{quoting}\ \mathit{v136}\ \mathtt{says\ prop}\ v_{66}))\ \land\\
\quad (\forall v_{10}\ v_{67}.\ P\ (v_{10}\ \mathtt{says\ notf}\ v_{67}))\ \land\\
\quad (\forall v_{10}\ v_{68}\ v_{69}.\ P\ (v_{10}\ \mathtt{says}\ (v_{68}\ \mathtt{andf}\ v_{69})))\ \land\\
\quad (\forall v_{10}\ v_{70}\ v_{71}.\ P\ (v_{10}\ \mathtt{says}\ (v_{70}\ \mathtt{orf}\ v_{71})))\ \land\\
\quad (\forall v_{10}\ v_{72}\ v_{73}.\ P\ (v_{10}\ \mathtt{says}\ (v_{72}\ \mathtt{impf}\ v_{73})))\ \land\\
\quad (\forall v_{10}\ v_{74}\ v_{75}.\ P\ (v_{10}\ \mathtt{says}\ (v_{74}\ \mathtt{eqf}\ v_{75})))\ \land\\
\quad (\forall v_{10}\ v_{76}\ v_{77}.\ P\ (v_{10}\ \mathtt{says}\ v_{76}\ \mathtt{says}\ v_{77}))\ \land\\
\quad (\forall v_{10}\ v_{78}\ v_{79}.\ P\ (v_{10}\ \mathtt{says}\ v_{78}\ \mathtt{speaks\_for}\ v_{79}))\ \land\\
\quad (\forall v_{10}\ v_{80}\ v_{81}.\ P\ (v_{10}\ \mathtt{says}\ v_{80}\ \mathtt{controls}\ v_{81}))\ \land\\
\quad (\forall v_{10}\ v_{82}\ v_{83}\ v_{84}.\ P\ (v_{10}\ \mathtt{says\ reps}\ v_{82}\ v_{83}\ v_{84}))\ \land\\
\quad (\forall v_{10}\ v_{85}\ v_{86}.\ P\ (v_{10}\ \mathtt{says}\ v_{85}\ \mathtt{domi}\ v_{86}))\ \land\\
\quad (\forall v_{10}\ v_{87}\ v_{88}.\ P\ (v_{10}\ \mathtt{says}\ v_{87}\ \mathtt{eqi}\ v_{88}))\ \land\\
\quad (\forall v_{10}\ v_{89}\ v_{90}.\ P\ (v_{10}\ \mathtt{says}\ v_{89}\ \mathtt{doms}\ v_{90}))\ \land\\
\quad (\forall v_{10}\ v_{91}\ v_{92}.\ P\ (v_{10}\ \mathtt{says}\ v_{91}\ \mathtt{eqs}\ v_{92}))\ \land\\
\quad (\forall v_{10}\ v_{93}\ v_{94}.\ P\ (v_{10}\ \mathtt{says}\ v_{93}\ \mathtt{eqn}\ v_{94}))\ \land\\
\quad (\forall v_{10}\ v_{95}\ v_{96}.\ P\ (v_{10}\ \mathtt{says}\ v_{95}\ \mathtt{lte}\ v_{96}))\ \land\\
\quad (\forall v_{10}\ v_{97}\ v_{98}.\ P\ (v_{10}\ \mathtt{says}\ v_{97}\ \mathtt{lt}\ v_{98}))\ \land\\
\quad (\forall v_{12}\ v_{13}.\ P\ (v_{12}\ \mathtt{speaks\_for}\ v_{13}))\ \land\\
\quad (\forall v_{14}\ v_{15}.\ P\ (v_{14}\ \mathtt{controls}\ v_{15}))\ \land\\
\quad (\forall v_{16}\ v_{17}\ v_{18}.\ P\ (\mathtt{reps}\ v_{16}\ v_{17}\ v_{18}))\ \land\\
\quad (\forall v_{19}\ v_{20}.\ P\ (v_{19}\ \mathtt{domi}\ v_{20}))\ \land\\
\quad (\forall v_{21}\ v_{22}.\ P\ (v_{21}\ \mathtt{eqi}\ v_{22}))\ \land\\
\quad (\forall v_{23}\ v_{24}.\ P\ (v_{23}\ \mathtt{doms}\ v_{24}))\ \land\\
\quad (\forall v_{25}\ v_{26}.\ P\ (v_{25}\ \mathtt{eqs}\ v_{26}))\ \land\ (\forall v_{27}\ v_{28}.\ P\ (v_{27}\ \mathtt{eqn}\ v_{28}))\ \land\\
\quad (\forall v_{29}\ v_{30}.\ P\ (v_{29}\ \mathtt{lte}\ v_{30}))\ \land\ (\forall v_{31}\ v_{32}.\ P\ (v_{31}\ \mathtt{lt}\ v_{32}))\ \Rightarrow\\
\quad \forall v.\ P\ v
\end{array}
$$

[inputOK_def]

$$
\begin{array}{l}
\vdash (\mathtt{inputOK\ (Name\ Alice\ says\ prop\ (SOME}\ \mathit{cmd}\mathtt{))}\ \iff\ \mathtt{T)}\ \land\\
\quad (\mathtt{inputOK\ (Name\ Bob\ says\ prop\ (SOME}\ \mathit{cmd}\mathtt{))}\ \iff\ \mathtt{T)}\ \land\\
\quad (\mathtt{inputOK\ TT}\ \iff\ \mathtt{F)}\ \land\ (\mathtt{inputOK\ FF}\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK\ (prop}\ v)\ \iff\ \mathtt{F)}\ \land\ (\mathtt{inputOK\ (notf}\ v_1)\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK}\ (v_2\ \mathtt{andf}\ v_3)\ \iff\ \mathtt{F)}\ \land\ (\mathtt{inputOK}\ (v_4\ \mathtt{orf}\ v_5)\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK}\ (v_6\ \mathtt{impf}\ v_7)\ \iff\ \mathtt{F)}\ \land\ (\mathtt{inputOK}\ (v_8\ \mathtt{eqf}\ v_9)\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK}\ (v_{10}\ \mathtt{says\ TT)}\ \iff\ \mathtt{F)}\ \land\ (\mathtt{inputOK}\ (v_{10}\ \mathtt{says\ FF)}\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK\ (Name\ Carol\ says\ prop\ (SOME}\ \mathit{v142}\mathtt{))}\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK\ (Name}\ \mathit{v132}\ \mathtt{says\ prop\ NONE)}\ \iff\ \mathtt{F)}\ \land\\
\quad (\mathtt{inputOK}\ (\mathit{v133}\ \mathtt{meet}\ \mathit{v134}\ \mathtt{says\ prop}\ v_{66})\ \iff\ \mathtt{F)}\ \land
\end{array}
$$

(inputOK ($\mathit{v135}$ quoting $\mathit{v136}$ says prop v_{66}) $\iff$ F) $\wedge$
(inputOK (v_{10} says notf v_{67}) $\iff$ F) $\wedge$
(inputOK (v_{10} says (v_{68} andf v_{69})) $\iff$ F) $\wedge$
(inputOK (v_{10} says (v_{70} orf v_{71})) $\iff$ F) $\wedge$
(inputOK (v_{10} says (v_{72} impf v_{73})) $\iff$ F) $\wedge$
(inputOK (v_{10} says (v_{74} eqf v_{75})) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{76} says v_{77}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{78} speaks_for v_{79}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{80} controls v_{81}) $\iff$ F) $\wedge$
(inputOK (v_{10} says reps v_{82} v_{83} v_{84}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{85} domi v_{86}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{87} eqi v_{88}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{89} doms v_{90}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{91} eqs v_{92}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{93} eqn v_{94}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{95} lte v_{96}) $\iff$ F) $\wedge$
(inputOK (v_{10} says v_{97} lt v_{98}) $\iff$ F) $\wedge$
(inputOK (v_{12} speaks_for v_{13}) $\iff$ F) $\wedge$
(inputOK (v_{14} controls v_{15}) $\iff$ F) $\wedge$
(inputOK (reps v_{16} v_{17} v_{18}) $\iff$ F) $\wedge$
(inputOK (v_{19} domi v_{20}) $\iff$ F) $\wedge$
(inputOK (v_{21} eqi v_{22}) $\iff$ F) $\wedge$
(inputOK (v_{23} doms v_{24}) $\iff$ F) $\wedge$
(inputOK (v_{25} eqs v_{26}) $\iff$ F) $\wedge$ (inputOK (v_{27} eqn v_{28}) $\iff$ F) $\wedge$
(inputOK (v_{29} lte v_{30}) $\iff$ F) $\wedge$ (inputOK (v_{31} lt v_{32}) $\iff$ F)

[inputOK_ind]

$\vdash \forall P$.
($\forall \mathit{cmd}$. P (Name Alice says prop (SOME cmd))) $\wedge$
($\forall \mathit{cmd}$. P (Name Bob says prop (SOME cmd))) $\wedge$ P TT $\wedge$ P FF $\wedge$
($\forall v$. P (prop v)) $\wedge$ ($\forall v_1$. P (notf v_1)) $\wedge$
($\forall v_2$ v_3. P (v_2 andf v_3)) $\wedge$ ($\forall v_4$ v_5. P (v_4 orf v_5)) $\wedge$
($\forall v_6$ v_7. P (v_6 impf v_7)) $\wedge$ ($\forall v_8$ v_9. P (v_8 eqf v_9)) $\wedge$
($\forall v_{10}$. P (v_{10} says TT)) $\wedge$ ($\forall v_{10}$. P (v_{10} says FF)) $\wedge$
($\forall \mathit{v142}$. P (Name Carol says prop (SOME $\mathit{v142}$))) $\wedge$
($\forall \mathit{v132}$. P (Name $\mathit{v132}$ says prop NONE)) $\wedge$
($\forall \mathit{v133}$ $\mathit{v134}$ v_{66}. P ($\mathit{v133}$ meet $\mathit{v134}$ says prop v_{66})) $\wedge$
($\forall \mathit{v135}$ $\mathit{v136}$ v_{66}. P ($\mathit{v135}$ quoting $\mathit{v136}$ says prop v_{66})) $\wedge$
($\forall v_{10}$ v_{67}. P (v_{10} says notf v_{67})) $\wedge$
($\forall v_{10}$ v_{68} v_{69}. P (v_{10} says (v_{68} andf v_{69}))) $\wedge$
($\forall v_{10}$ v_{70} v_{71}. P (v_{10} says (v_{70} orf v_{71}))) $\wedge$
($\forall v_{10}$ v_{72} v_{73}. P (v_{10} says (v_{72} impf v_{73}))) $\wedge$
($\forall v_{10}$ v_{74} v_{75}. P (v_{10} says (v_{74} eqf v_{75}))) $\wedge$
($\forall v_{10}$ v_{76} v_{77}. P (v_{10} says v_{76} says v_{77})) $\wedge$
($\forall v_{10}$ v_{78} v_{79}. P (v_{10} says v_{78} speaks_for v_{79})) $\wedge$
($\forall v_{10}$ v_{80} v_{81}. P (v_{10} says v_{80} controls v_{81})) $\wedge$
($\forall v_{10}$ v_{82} v_{83} v_{84}. P (v_{10} says reps v_{82} v_{83} v_{84})) $\wedge$
($\forall v_{10}$ v_{85} v_{86}. P (v_{10} says v_{85} domi v_{86})) $\wedge$
($\forall v_{10}$ v_{87} v_{88}. P (v_{10} says v_{87} eqi v_{88})) $\wedge$

$(\forall v_{10}\ v_{89}\ v_{90}.\ P\ (v_{10}\ \texttt{says}\ v_{89}\ \texttt{doms}\ v_{90}))\ \wedge$
$(\forall v_{10}\ v_{91}\ v_{92}.\ P\ (v_{10}\ \texttt{says}\ v_{91}\ \texttt{eqs}\ v_{92}))\ \wedge$
$(\forall v_{10}\ v_{93}\ v_{94}.\ P\ (v_{10}\ \texttt{says}\ v_{93}\ \texttt{eqn}\ v_{94}))\ \wedge$
$(\forall v_{10}\ v_{95}\ v_{96}.\ P\ (v_{10}\ \texttt{says}\ v_{95}\ \texttt{lte}\ v_{96}))\ \wedge$
$(\forall v_{10}\ v_{97}\ v_{98}.\ P\ (v_{10}\ \texttt{says}\ v_{97}\ \texttt{lt}\ v_{98}))\ \wedge$
$(\forall v_{12}\ v_{13}.\ P\ (v_{12}\ \texttt{speaks\_for}\ v_{13}))\ \wedge$
$(\forall v_{14}\ v_{15}.\ P\ (v_{14}\ \texttt{controls}\ v_{15}))\ \wedge$
$(\forall v_{16}\ v_{17}\ v_{18}.\ P\ (\texttt{reps}\ v_{16}\ v_{17}\ v_{18}))\ \wedge$
$(\forall v_{19}\ v_{20}.\ P\ (v_{19}\ \texttt{domi}\ v_{20}))\ \wedge$
$(\forall v_{21}\ v_{22}.\ P\ (v_{21}\ \texttt{eqi}\ v_{22}))\ \wedge$
$(\forall v_{23}\ v_{24}.\ P\ (v_{23}\ \texttt{doms}\ v_{24}))\ \wedge$
$(\forall v_{25}\ v_{26}.\ P\ (v_{25}\ \texttt{eqs}\ v_{26}))\ \wedge\ (\forall v_{27}\ v_{28}.\ P\ (v_{27}\ \texttt{eqn}\ v_{28}))\ \wedge$
$(\forall v_{29}\ v_{30}.\ P\ (v_{29}\ \texttt{lte}\ v_{30}))\ \wedge\ (\forall v_{31}\ v_{32}.\ P\ (v_{31}\ \texttt{lt}\ v_{32}))\ \Rightarrow$
$\forall v.\ P\ v$

[output_distinct_clauses]

$\vdash \texttt{on} \neq \texttt{off}$

[privcmd_distinct_clauses]

$\vdash \texttt{launch} \neq \texttt{reset}$

[SM0ns_def]

```
⊢ (SM0ns STBY (exec (PR reset)) = STBY) ∧
  (SM0ns STBY (exec (PR launch)) = ACTIVE) ∧
  (SM0ns STBY (exec (NP status)) = STBY) ∧
  (SM0ns ACTIVE (exec (PR reset)) = STBY) ∧
  (SM0ns ACTIVE (exec (PR launch)) = ACTIVE) ∧
  (SM0ns ACTIVE (exec (NP status)) = ACTIVE) ∧
  (SM0ns STBY (trap (PR reset)) = STBY) ∧
  (SM0ns STBY (trap (PR launch)) = STBY) ∧
  (SM0ns STBY (trap (NP status)) = STBY) ∧
  (SM0ns ACTIVE (trap (PR reset)) = ACTIVE) ∧
  (SM0ns ACTIVE (trap (PR launch)) = ACTIVE) ∧
  (SM0ns ACTIVE (trap (NP status)) = ACTIVE) ∧
  (SM0ns STBY discard = STBY) ∧ (SM0ns ACTIVE discard = ACTIVE)
```

[SM0ns_ind]

```
⊢ ∀P.
    P STBY (exec (PR reset)) ∧ P STBY (exec (PR launch)) ∧
    P STBY (exec (NP status)) ∧ P ACTIVE (exec (PR reset)) ∧
    P ACTIVE (exec (PR launch)) ∧ P ACTIVE (exec (NP status)) ∧
    P STBY (trap (PR reset)) ∧ P STBY (trap (PR launch)) ∧
    P STBY (trap (NP status)) ∧ P ACTIVE (trap (PR reset)) ∧
    P ACTIVE (trap (PR launch)) ∧ P ACTIVE (trap (NP status)) ∧
    P STBY discard ∧ P ACTIVE discard ⇒
    ∀v v1. P v v1
```

[SM0out_def]

```
⊢ (SM0out STBY (exec (PR reset)) = off) ∧
  (SM0out STBY (exec (PR launch)) = on) ∧
  (SM0out STBY (exec (NP status)) = off) ∧
  (SM0out ACTIVE (exec (PR reset)) = off) ∧
  (SM0out ACTIVE (exec (PR launch)) = on) ∧
  (SM0out ACTIVE (exec (NP status)) = on) ∧
  (SM0out STBY (trap (PR reset)) = off) ∧
  (SM0out STBY (trap (PR launch)) = off) ∧
  (SM0out STBY (trap (NP status)) = off) ∧
  (SM0out ACTIVE (trap (PR reset)) = on) ∧
  (SM0out ACTIVE (trap (PR launch)) = on) ∧
  (SM0out ACTIVE (trap (NP status)) = on) ∧
  (SM0out STBY discard = off) ∧ (SM0out ACTIVE discard = on)
```

[SM0out_ind]

```
⊢ ∀P.
    P STBY (exec (PR reset)) ∧ P STBY (exec (PR launch)) ∧
    P STBY (exec (NP status)) ∧ P ACTIVE (exec (PR reset)) ∧
    P ACTIVE (exec (PR launch)) ∧ P ACTIVE (exec (NP status)) ∧
    P STBY (trap (PR reset)) ∧ P STBY (trap (PR launch)) ∧
    P STBY (trap (NP status)) ∧ P ACTIVE (trap (PR reset)) ∧
    P ACTIVE (trap (PR launch)) ∧ P ACTIVE (trap (NP status)) ∧
    P STBY discard ∧ P ACTIVE discard ⇒
```

$\forall v\ v_1.\ P\ v\ v_1$

[staff_distinct_clauses]

```
⊢ Alice ≠ Bob ∧ Alice ≠ Carol ∧ Bob ≠ Carol
```

[state_distinct_clauses]

```
⊢ STBY ≠ ACTIVE
```

Index

SM0 Theory, 3
- Datatypes, 3
- Definitions, 3
  - certs2_def, 3
  - certs_def, 3
  - SM0StateInterp_def, 3
- Theorems, 3
  - Alice_exec_privcmd_justified_thm, 3
  - Alice_justified_privcmd_exec_thm, 4
  - Alice_privcmd_lemma, 4
  - Alice_privcmd_verified_thm, 4
  - Carol_discard_lemma, 4
  - Carol_rejected_lemma, 5
  - command_distinct_clauses, 5
  - command_one_one, 5
  - inputOK2_def, 5
  - inputOK2_ind, 6
  - inputOK_def, 6
  - inputOK_ind, 7
  - output_distinct_clauses, 8
  - privcmd_distinct_clauses, 8
  - SM0ns_def, 8
  - SM0ns_ind, 8
  - SM0out_def, 9
  - SM0out_ind, 9
  - staff_distinct_clauses, 9
  - state_distinct_clauses, 9