

THEORY EvtBTheoryProofRule

IMPORT THEORY EvtBPO

TYPE PARAMETERS STATE, EVENT

THEOREMS

thm1 :
 $\forall m, e \cdot m \in \text{Machine}(\text{STATE}, \text{EVENT}) \wedge e \in \text{Convergent}(m) \wedge e \in \text{Event}(m) \wedge \text{Event_WellCons}(m) \wedge \text{Tag_Event_WellCons}(m) \Rightarrow e \in \text{Progress}(m)$

PROOF RULES

extension_def :

Metavariables

m : *Machine*(STATE, EVENT)

Rewrite Rules

rewConsistency : *check_Machine_Consistency*(*m*)

rhs1 : $\top \Rightarrow \text{Mch_THM}(m) \wedge \text{Mch_INV}(m) \wedge \text{Mch_FIS}(m) \wedge \text{Mch_NAT}(m) \wedge \text{Mch_VARIANT}(m)$

rewMCH : *m* \in *Machine*(STATE, EVENT)

rhs1 : $\top \Rightarrow$

$\exists p_E, p_S, p_Ie, p_P, p_V, p_C, p_O, p_AP, p_B, p_G, p_In, p_T \cdot m = \text{Cons_machine}(p_E, p_S, p_Ie, p_P, p_AP, p_G, p_B, p_In, p_T, p_V, p_O, p_C)$

rewWCons : *Machine_WellCons*(*m*)

rhs1 : $\top \Rightarrow \text{BAP_WellCons}(m) \wedge \text{Grd_WellCons}(m) \wedge \text{Event_WellCons}(m) \wedge \text{Tag_Event_WellCons}(m) \wedge \text{Variant_WellCons}(m)$

rewBAPWC : *BAP_WellCons*(*m*)

rhs1 : $\top \Rightarrow \forall b, p \cdot \text{Progress}(m) = p \wedge \text{BAP}(m) = b \Rightarrow \text{dom}(b) = p$

rewGRDWC : *Grd_WellCons*(*m*)

rhs1 : $\top \Rightarrow \forall g, p \cdot \text{Progress}(m) = p \wedge \text{Grd}(m) = g \Rightarrow \text{dom}(g) = p$

rewEvtWC : *Event_WellCons*(*m*)

rhs1 : $\top \Rightarrow \forall Ev, In, Pro \cdot \text{Init}(m) = In \wedge \text{Event}(m) = Ev \wedge \text{Progress}(m) = Pro \Rightarrow \text{partition}(Ev, \{In\}, Pro)$

rewVarWC : *Variant_WellCons*(*m*)

rhs1 : $\top \Rightarrow \forall \text{variant}, \text{inv} \cdot \text{Inv}(m) = \text{inv} \wedge \text{Variant}(m) = \text{variant} \Rightarrow \text{inv} \triangleleft \text{variant} \in \text{inv} \rightarrow \mathbb{Z}$

rewTagWC : *Tag_Event_WellCons*(*m*)

rhs1 : $\top \Rightarrow \forall \text{ordinary}, \text{init}, \text{ev}, \text{convergent} \cdot \text{Init}(m) = \text{init} \wedge \text{Ordinary}(m) = \text{ordinary} \wedge \text{Convergent}(m) = \text{convergent} \wedge \text{Event}(m) = \text{ev} \Rightarrow \text{partition}(\text{ev}, \text{ordinary}, \text{convergent}) \wedge \text{init} \in \text{ordinary}$

rewThm : *Mch_THM*(*m*)

rhs1 : $\top \Rightarrow \forall \text{inv}, \text{thm} \cdot \text{Inv}(m) = \text{inv} \wedge \text{Thm}(m) = \text{thm} \Rightarrow \text{inv} \subseteq \text{thm}$

rewInvInit : *Mch_INV_Init*(*m*)

rhs1 : $\top \Rightarrow \forall \text{inv}, \text{ap} \cdot \text{Inv}(m) = \text{inv} \wedge \text{AP}(m) = \text{ap} \Rightarrow \text{ap} \subseteq \text{inv}$

rewFISInit : *Mch_FIS_Init*(*m*)

rhs1 : $\top \Rightarrow \forall \text{inv}, \text{ap} \cdot \text{Inv}(m) = \text{inv} \wedge \text{AP}(m) = \text{ap} \Rightarrow \text{ap} \cap \text{inv} \neq \emptyset$

rewFIS : *Mch_FIS*(*m*)

rhs1 : $\top \Rightarrow \text{Mch_FIS_Init}(m) \wedge (\forall e, \text{pro}, \text{inv}, \text{grd}, \text{bap} \cdot \text{Progress}(m) = \text{pro} \wedge e \in \text{pro} \wedge \text{Inv}(m) = \text{inv} \wedge \text{Grd}(m) = \text{grd} \wedge \text{BAP}(m) = \text{bap} \Rightarrow \text{inv} \cap \text{grd}[\{e\}] \subseteq \text{dom}(\text{bap}[\{e\}]))$

rewInv : *Mch_INV*(*m*)

rhs1 : $\top \Rightarrow \text{Mch_INV_Init}(m) \wedge (\forall e, \text{pro}, \text{inv}, \text{grd}, \text{bap} \cdot \text{Progress}(m) = \text{pro} \wedge e \in \text{pro} \wedge \text{Inv}(m) = \text{inv} \wedge \text{Grd}(m) = \text{grd} \wedge \text{BAP}(m) = \text{bap} \Rightarrow \text{bap}[\{e\}][\text{inv} \cap \text{grd}[\{e\}]] \subseteq \text{inv})$

rewNat : *Mch_NAT*(*m*)

rhs1 : $\top \Rightarrow \forall \text{variant}, \text{inv}, \text{grd}, \text{convergent} \cdot \text{Variant}(m) = \text{variant} \wedge \text{Inv}(m) = \text{inv} \wedge \text{Convergent}(m) = \text{convergent} \wedge \text{Grd}(m) = \text{grd} \Rightarrow \text{variant}[\text{inv} \cap \text{grd}[\text{convergent}]] \subseteq \mathbb{N}$

rewVar : *Mch_VARIANT*(*m*)

rhs1 : $\top \Rightarrow \forall e, s, \text{ev}, \text{conv}, \text{st}, \text{inv}, \text{grd}, \text{sp}, \text{bap}, \text{var} \cdot \text{Event}(m) = \text{ev} \wedge \text{Convergent}(m) = \text{conv} \wedge \text{Inv}(m) = \text{inv} \wedge \text{State}(m) = \text{st} \wedge \text{Grd}(m) = \text{grd} \wedge e \in \text{ev} \wedge e \in \text{conv} \wedge s \in \text{st} \wedge s \in \text{inv} \wedge \text{BAP}(m) = \text{bap} \wedge \text{Variant}(m) = \text{var} \wedge s \in \text{grd}[\{e\}] \wedge \text{sp} \in \text{bap}[\{e\}][\{s\}] \Rightarrow (\text{inv} \triangleleft \text{var})(s) > (\text{inv} \triangleleft \text{var})(\text{sp})$

END