MACHINE

BIT_VECTOR_DEFINITION

SEES

BIT_DEFINITION

CONSTANTS

BIT_VECTOR,
bv_catenate,
bv_sub,
bv_zero,
bv_one,
bv_size,
bv_not,
bv_and,
bv_or,
bv_xor,
bv_get,
bv_set,
bv_clear,
bv_put,
bv_index

PROPERTIES

$BIT\_VECTOR = \mathbf{seq1}(BIT)$

$\land\ bv\_size \in BIT\_VECTOR \rightarrow \mathcal{N}_1$
$\land\ bv\_size = \lambda\ (bv).(bv \in BIT\_VECTOR \mid \mathbf{size}(bv))$

$\land\ bv\_size \in BIT\_VECTOR \rightarrow \mathcal{N}_1$
$\land\ bv\_size = \lambda\ (bv).(bv \in BIT\_VECTOR \mid \mathbf{size}(bv))$

$\land\ bv\_catenate \in BIT\_VECTOR \times BIT\_VECTOR \rightarrow BIT\_VECTOR$
$\land\ bv\_catenate = \lambda\ (v1,v2)\ .\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \mid v1 \frown v2)$

$\land\ bv\_index \in BIT\_VECTOR \rightarrow \mathcal{P}\ (\ \mathcal{N}\ )$
$\land\ bv\_index = \lambda\ (v1)\ .\ (v1 \in BIT\_VECTOR \mid 0\ ..\ (bv\_size(v1)\text{-}1))$

$\land\ bv\_sub \in BIT\_VECTOR \times \mathcal{N} \times \mathcal{N} \rightarrow BIT\_VECTOR$
$\land\ bv\_sub = \lambda\ (bv,low,high)\ .\ (bv \in BIT\_VECTOR \land low \in 0\ ..\ (bv\_size(bv)\text{-}1) \land high \in low\ ..\ (bv\_size(bv)\text{-}1)$
$\mid \lambda\ (i0).(i0 \in 1\ ..\ (high\text{-}low+1) \mid bv(i0+low)\ ))$

$\land\ bv\_zero \in \mathcal{N}_1 \rightarrow BIT\_VECTOR$
$\land\ bv\_zero = \lambda\ (sz)\ .\ (sz \in \mathcal{N}_1 \mid (1\ ..\ sz) \times \{0\})$

$\land\ bv\_one \in \mathcal{N}_1 \rightarrow BIT\_VECTOR$

$\wedge\ \mathit{bv\_one} = \lambda\ (\mathit{sz})\ .\ (\mathit{sz} \in \mathcal{N}_1 \mid (1 \mathrel{..} \mathit{sz}) \times \{1\})$

$\wedge\ \mathit{bv\_not} \in \mathit{BIT\_VECTOR} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_not} = \lambda\ (\mathit{v1}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \mid \lambda\ (\mathit{idx}).(\mathit{idx} \in 1 \mathrel{..} \mathit{bv\_size}(\mathit{v1}) \mid \mathit{bit\_not}(\mathit{v1}(\mathit{idx})\ )\ )\ )$

$\wedge\ \mathit{bv\_and} \in \mathit{BIT\_VECTOR} \times \mathit{BIT\_VECTOR} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_and} = \lambda\ (\mathit{v1},\mathit{v2}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{v2} \in \mathit{BIT\_VECTOR} \wedge \mathit{bv\_size}(\mathit{v1}) = \mathit{bv\_size}(\mathit{v2}) \mid$
$\lambda\ (\mathit{idx}).(\mathit{idx} \in 1 \mathrel{..} \mathit{bv\_size}(\mathit{v1}) \mid \mathit{bit\_and}(\mathit{v1}(\mathit{idx}),\mathit{v2}(\mathit{idx}))))$

$\wedge\ \mathit{bv\_or} \in \mathit{BIT\_VECTOR} \times \mathit{BIT\_VECTOR} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_or} = \lambda\ (\mathit{v1},\mathit{v2}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{v2} \in \mathit{BIT\_VECTOR} \wedge \mathit{bv\_size}(\mathit{v1}) = \mathit{bv\_size}(\mathit{v2}) \mid$
$\lambda\ (\mathit{idx}).(\mathit{idx} \in 1 \mathrel{..} \mathit{bv\_size}(\mathit{v1}) \mid \mathit{bit\_or}(\mathit{v1}(\mathit{idx}),\mathit{v2}(\mathit{idx}))))$

$\wedge\ \mathit{bv\_xor} \in \mathit{BIT\_VECTOR} \times \mathit{BIT\_VECTOR} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_xor} = \lambda\ (\mathit{v1},\mathit{v2}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{v2} \in \mathit{BIT\_VECTOR} \wedge \mathit{bv\_size}(\mathit{v1}) = \mathit{bv\_size}(\mathit{v2}) \mid$
$\lambda\ (\mathit{idx}).(\mathit{idx} \in 1 \mathrel{..} \mathit{bv\_size}(\mathit{v1}) \mid \mathit{bit\_xor}(\mathit{v1}(\mathit{idx}),\mathit{v2}(\mathit{idx}))))$

$\wedge\ \mathit{bv\_get} \in \mathit{BIT\_VECTOR} \times \mathcal{N} \rightarrow \mathit{BIT}$
$\wedge\ \mathit{bv\_get} = \lambda\ (\mathit{v1},\mathit{idx}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{idx} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{v1})\text{-}1) \mid \mathit{v1}(\mathit{idx}{+}1))$

$\wedge\ \mathit{bv\_set} \in \mathit{BIT\_VECTOR} \times \mathcal{N} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_set} = \lambda\ (\mathit{v1},\mathit{idx}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{idx} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{v1})\text{-}1) \mid \mathit{v1} \mathbin{<\!\!+} \{\ (\mathit{idx}{+}1) \mapsto 1\ \})$

$\wedge\ \mathit{bv\_clear} \in \mathit{BIT\_VECTOR} \times \mathcal{N} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_clear} = \lambda\ (\mathit{v1},\mathit{idx}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{idx} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{v1})\text{-}1) \mid \mathit{v1} \mathbin{<\!\!+} \{\ (\mathit{idx}{+}1) \mapsto 0\ \})$

$\wedge\ \mathit{bv\_put} \in \mathit{BIT\_VECTOR} \times \mathcal{N} \times \mathit{BIT} \rightarrow \mathit{BIT\_VECTOR}$
$\wedge\ \mathit{bv\_put} = \lambda\ (\mathit{v1},\mathit{idx},\mathit{bit}).(\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{idx} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{v1})\text{-}1) \wedge \mathit{bit} \in \mathit{BIT} \mid \mathit{v1} \mathbin{<\!\!+} \{\ (\mathit{idx}{+}1) \mapsto \mathit{bit}\ \})$

ASSERTIONS

$\forall\ \mathit{bv}.(\mathit{bv} \in \mathit{BIT\_VECTOR} \Rightarrow \mathit{bv\_size}(\mathit{bv\_not}(\mathit{bv})) = \mathit{bv\_size}(\mathit{bv}));$

$\forall\ (\mathit{bv},\mathit{indx}).(\mathit{bv} \in \mathit{BIT\_VECTOR} \wedge \mathit{indx} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{bv})\text{-}1) \Rightarrow (\mathit{bv\_get}(\mathit{bv\_not}(\mathit{bv\_not}(\mathit{bv})),\mathit{indx}) = \mathit{bv\_get}(\mathit{bv},\mathit{indx})\ ));$

$\forall\ (\mathit{v1},\mathit{v2}).\ (\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{v2} \in \mathit{BIT\_VECTOR} \Rightarrow$
$\mathit{bv\_size}(\mathit{bv\_catenate}(\mathit{v1},\ \mathit{v2})) = \mathit{bv\_size}(\mathit{v1}) + \mathit{bv\_size}(\mathit{v2}));$

$\forall\ (\mathit{bv},\mathit{low},\mathit{high}).\ (\mathit{bv} \in \mathit{BIT\_VECTOR} \wedge \mathit{low} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{bv})\text{-}1) \wedge \mathit{high} \in 0 \mathrel{..} (\mathit{bv\_size}(\mathit{bv})\text{-}1) \wedge \mathit{low} \leq \mathit{high} \Rightarrow$
$\mathit{bv\_size}(\mathit{bv\_sub}(\mathit{bv},\ \mathit{low},\ \mathit{high})) = \mathit{high}\text{-}\mathit{low});$

$\forall\ (\mathit{v1},\mathit{v2}).\ (\mathit{v1} \in \mathit{BIT\_VECTOR} \wedge \mathit{v2} \in \mathit{BIT\_VECTOR} \wedge \mathit{bv\_size}(\mathit{v1}) = \mathit{bv\_size}(\mathit{v2}) \Rightarrow$
$\mathit{bv\_size}(\mathit{bv\_and}(\mathit{v1},\ \mathit{v2})) = \mathit{bv\_size}(\mathit{v2}));$

$\forall\ (v1,v2,indx).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \land indx \in 0 \mathrel{..} (bv\_size(v1)\text{-}1) \Rightarrow (bv\_get(bv\_and(v1,\ v2),indx) = bv\_get(bv\_and(v2,\ v1),indx)));$

$\forall\ (v1,v2,v3,indx).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land v3 \in BIT\_VECTOR \land bv\_size(v1){=}bv\_size(v2) \land bv\_size(v1){=}bv\_size(v3) \land indx \in 0 \mathrel{..} (bv\_size(v1)\text{-}1) \Rightarrow (bv\_get(bv\_and(v1,\ bv\_and(v2,v3)),indx) = bv\_get(bv\_and(bv\_and(v1,\ v2),\ v3),indx))\ );$

$\forall\ (bv,indx).\ (bv \in BIT\_VECTOR \land indx \in 0 \mathrel{..} (bv\_size(bv)\text{-}1) \Rightarrow (bv\_get(bv\_and(bv,\ bv\_zero(bv\_size(bv))),indx) = bv\_get(bv\_zero(bv\_size(bv)),indx)\ ));$

$\forall\ (bv,indx).\ (bv \in BIT\_VECTOR \land indx \in 0 \mathrel{..} (bv\_size(bv)\text{-}1) \Rightarrow (bv\_get(bv\_and(bv,\ bv\_one(bv\_size(bv))),indx) = bv\_get(bv,indx)));$

$\forall\ (v1,v2).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \Rightarrow bv\_size(bv\_or(v1,\ v2)) = bv\_size(v1));$

$\forall\ (v1,v2,indx).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \land indx \in 0 \mathrel{..} (bv\_size(v1)\text{-}1) \Rightarrow (bv\_get(bv\_or(v1,\ v2),indx) = bv\_get(bv\_or(v2,\ v1),indx)));$

$\forall\ (v1,v2).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \Rightarrow bv\_size(bv\_or(v1,\ v2)) = bv\_size(v2));$

$\forall\ (v1,v2,v3,indx).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land v3 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \land bv\_size(v1) = bv\_size(v3) \land indx \in 0 \mathrel{..} (bv\_size(v1)\text{-}1) \Rightarrow (bv\_get(bv\_or(v1,\ bv\_or(v2,v3)),indx) = bv\_get(bv\_or(bv\_or(v1,\ v2),\ v3),indx)));$

$\forall\ (bv,indx).\ (bv \in BIT\_VECTOR \land indx \in 0 \mathrel{..} (bv\_size(bv)\text{-}1) \Rightarrow (bv\_get(bv\_or(bv,\ bv\_one(bv\_size(bv))),indx) = bv\_get(bv\_one(bv\_size(bv)),indx)));$

$\forall\ (bv,indx).\ (bv \in BIT\_VECTOR \land indx \in 0 \mathrel{..} (bv\_size(bv)\text{-}1) \Rightarrow (bv\_get(bv\_or(bv,\ bv\_zero(bv\_size(bv))),indx) = bv\_get(bv,indx)));$

$\forall\ (v1,v2).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \Rightarrow bv\_size(bv\_xor(v1,\ v2)) = bv\_size(v1));$

$\forall\ (v1,v2).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \Rightarrow bv\_size(bv\_xor(v1,\ v2)) = bv\_size(v2));$

$\forall\ (v1,v2,indx).\ (v1 \in BIT\_VECTOR \land v2 \in BIT\_VECTOR \land bv\_size(v1) = bv\_size(v2) \land indx \in 0 \mathrel{..} (bv\_size(v1)\text{-}1) \Rightarrow (bv\_get(bv\_xor(v1,\ v2),indx) = bv\_get(bv\_xor(v2,\ v1),indx)));$

$\forall\ (bv,indx).\ (bv \in BIT\_VECTOR \land indx \in 0 \mathrel{..} (bv\_size(bv)\text{-}1) \Rightarrow bv\_get(bv\_xor(bv,bv),indx) = bv\_get(bv\_zero(bv\_size(bv)),indx))$

END