

## MACHINE

*BIT\_DEFINITION*

## CONSTANTS

*BIT*,  
*bit\_not*,  
*bit\_and*,  
*bit\_or*,  
*bit\_xor*,  
*bool\_bit*

## PROPERTIES

$BIT = 0 \dots 1$

$\wedge \text{bit\_not} \in BIT \rightarrow BIT$   
 $\wedge \text{bit\_not} = \lambda (bb). (bb \in BIT \mid 1-bb)$

$\wedge \text{bit\_and} \in BIT \times BIT \rightarrow BIT$   
 $\wedge \forall (b1, b2). (b1 \in BIT \wedge b2 \in BIT \Rightarrow ((\text{bit\_and}(b1, b2) = 1) \Leftrightarrow (b1 = 1) \wedge (b2 = 1)))$

$\wedge \text{bit\_or} \in BIT \times BIT \rightarrow BIT$   
 $\wedge \forall (b1, b2). (b1 \in BIT \wedge b2 \in BIT \Rightarrow ((\text{bit\_or}(b1, b2) = 1) \Leftrightarrow (b1 = 1) \vee (b2 = 1)))$

$\wedge \text{bit\_xor} \in BIT \times BIT \rightarrow BIT$   
 $\wedge \forall (b1, b2). (b1 \in BIT \wedge b2 \in BIT \Rightarrow ((\text{bit\_xor}(b1, b2) = 1) \Leftrightarrow (b1 \neq b2)))$

$\wedge \text{bool\_bit} \in \mathbf{BOOL} \rightarrow BIT$   
 $\wedge \text{bool\_bit} = \{ \mathbf{TRUE} \mapsto 1, \mathbf{FALSE} \mapsto 0 \}$

## ASSERTIONS

$\forall (bb). (bb \in BIT \Rightarrow \text{bit\_not}(bb) = 1-bb)$   
 $\wedge \text{bit\_not}(0) = 1$   
 $\wedge \text{bit\_not}(1) = 0$   
 $\wedge \forall (bb). (bb \in BIT \Rightarrow \text{bit\_not}(\text{bit\_not}(bb)) = bb)$   
 $\wedge \text{bit\_and}(0,0) = 0$   
 $\wedge \text{bit\_and}(0,1) = 0$   
 $\wedge \text{bit\_and}(1,0) = 0$   
 $\wedge \text{bit\_and}(1,1) = 1$

$$\begin{aligned}
& \wedge \forall (b1,b2).(b1 \in BIT \wedge b2 \in BIT \Rightarrow (bit\_and(b1, b2) = bit\_and(b2,b1)) \ ) \\
& \wedge \forall (b1,b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_and(b1, b2)=1 \Rightarrow bit\_and(b2,b1)=1 \ ) \\
& \wedge \forall (b1,b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_and(b1, b2)=0 \Rightarrow bit\_and(b2,b1)=0 \ )
\end{aligned}$$

$$\begin{aligned}
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \Rightarrow (bit\_and(b1, bit\_and(b2,b3)) = \\
& bit\_and(bit\_and(b1,b2),b3))) \\
& \wedge \forall (b1).(b1 \in BIT \Rightarrow (bit\_and(b1, 1) = b1)) \\
& \wedge \forall (b1).(b1 \in BIT \Rightarrow (bit\_and(b1, 0) = 0))
\end{aligned}$$

$$\begin{aligned}
& \wedge bit\_or(0,0) = 0 \\
& \wedge bit\_or(0,1) = 1 \\
& \wedge bit\_or(1,0) = 1 \\
& \wedge bit\_or(1,1) = 1 \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \Rightarrow (bit\_or(b1, b2) = bit\_or(b2,b1))) \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_or(b1, b2)=1 \Rightarrow bit\_or(b2,b1)=1) \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_or(b1, b2)=0 \Rightarrow bit\_or(b2,b1)=0) \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_or(b1,0)=1 \Rightarrow b1=1) \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_or(b1,0)=0 \Rightarrow b1=0)
\end{aligned}$$

$$\begin{aligned}
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \Rightarrow (bit\_or(b1, bit\_or(b2,b3)) = \\
& bit\_or(bit\_or(b1,b2),b3))) \\
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \wedge bit\_or(b1,b2)=1 \Rightarrow \\
& bit\_or(b1,bit\_or(b2,b3))=1) \\
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \wedge bit\_or(b1,b2)=1 \Rightarrow bit\_or(b1, \\
& bit\_or(b2,b3)) = bit\_or(1,b3)) \\
& \wedge \forall (b1).(b1 \in BIT \Rightarrow (bit\_or(b1, 1) = 1)) \\
& \wedge \forall (b1).(b1 \in BIT \Rightarrow (bit\_or(b1, 0) = b1)) \\
& \wedge \forall (b1).(b1 \in BIT \Rightarrow (bit\_or(1,b1) = 1)) \\
& \wedge \forall (b1).(b1 \in BIT \Rightarrow (bit\_or(0,b1) = b1))
\end{aligned}$$

$$\begin{aligned}
& \wedge bit\_xor(0,0) = 0 \\
& \wedge bit\_xor(0,1) = 1 \\
& \wedge bit\_xor(1,0) = 1 \\
& \wedge bit\_xor(1,1) = 0 \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \Rightarrow (bit\_xor(b1, b2) = bit\_xor(b2,b1))) \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_xor(b1, b2)=1 \Rightarrow bit\_xor(b2,b1)=1) \\
& \wedge \forall (b1, b2).(b1 \in BIT \wedge b2 \in BIT \wedge bit\_xor(b1, b2)=0 \Rightarrow bit\_xor(b2,b1)=0)
\end{aligned}$$

$$\begin{aligned}
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \Rightarrow (bit\_xor(b1, bit\_xor(b2,b3)) = \\
& bit\_xor(bit\_xor(b1,b2),b3))) \\
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \wedge bit\_xor(b1,b2)=1 \Rightarrow \\
& bit\_xor(b1,bit\_xor(b2,b3))=1) \\
& \wedge \forall (b1,b2,b3).(b1 \in BIT \wedge b2 \in BIT \wedge b3 \in BIT \wedge bit\_xor(b1,b2)=1 \Rightarrow bit\_xor(b1, \\
& bit\_xor(b2,b3)) = bit\_xor(1,b3))
\end{aligned}$$

$$\wedge \forall (bb).(bb \in BIT \Rightarrow bit\_xor(bb,bb) = 0)$$

$$\begin{aligned}
& \wedge bool\_bit(\mathbf{TRUE}) = 1 \\
& \wedge bool\_bit(\mathbf{FALSE}) = 0
\end{aligned}$$

$$\begin{aligned}
& \wedge \forall (bb).(bb \in BIT \Rightarrow bb = 0 \vee bb = 1) \\
& \wedge \forall (bb).(bb \in BIT \wedge \neg (bb = 0) \Rightarrow bb = 1)
\end{aligned}$$

$$\wedge \forall (bb).(bb \in BIT \wedge \neg (bb = 1) \Rightarrow bb = 0)$$

**END**