A New Exposition of the Formal Semantics of IEEE 1800 SVA

Doron Bustan and John Havlicek

Freescale Semiconductor, Inc.

23 January 2006

Abstract The point of this note is to propose a way to rewrite the formal semantics for SVA that is closer to the presentation of the intuitive syntax and semantics, that captures the notion of clock flow, and that is cleaner than the current IEEE 1800 standard exposition. In particular, the new exposition of the formal semantics should allow the semantics of multiply-clocked derived forms to be defined more easily and precisely than with the current IEEE 1800 standard exposition.

1 Abstract grammars

The new exposition does not distinguish unclocked from clocked sequences and properties. The abstract grammar for sequences is

$R ::= b$	[boolean expression]
$\mid$ `(1,` v `=` e`)`	[local variable assignment]
$\mid$ `@(`c`)` R	[clocking event]
$\mid$ `(`R`)`	[parenthesis]
$\mid$ R `##1` R	[concatenation]
$\mid$ R `##0` R	[fusion]
$\mid$ R `or` R	[union]
$\mid$ R `intersect` R	[intersection]
$\mid$ `first_match(`R`)`	[firstmatch]
$\mid$ R`[*0]`	[empty]
$\mid$ R`[*1:$]`	[positive repetition]

Here b denotes a boolean expression, e denotes an expression, v denotes a local variable, and c denotes a clocking event. The abstract grammar for properties is

$P ::= R$	[sequence]
$\mid$ `@(`c`)` P	[clocking event]
$\mid$ `(`P`)`	[parenthesis]
$\mid$ `not` P	[negation]
$\mid$ P `or` P	[or]
$\mid$ P `and` P	[and]
$\mid$ R `|->` P	[implication]
$\mid$ `disable iff (`b`)` P	[abort]

2 Semantics

2.1 Clock ticks

Definition 2.1. *The finite word v is a clock tick of c iff $|v| > 0$ and $v^{|v|-1} \Vdash c$ and for all $0 \leq i < |v| - 1$, $v^i \Vdash \texttt{!}c$.* □

Lemma 2.2. *Let u, v be clock ticks of c. If $u \leq v$ and $u^{|u|-1}$ is not $\top$, then $u = v$.*

Proof: Suppose $u < v$. Then $u^{|u|-1} \Vdash c$ because u is a clock tick of c. Also, $u^{|u|-1} \Vdash \texttt{!}c$ because v is a clock tick of c. Since $u^{|u|-1}$ is not $\top$, this is a contradiction. □

2.2 Tight satisfaction of sequences without local variables

Without local variables, tight satisfaction is a four-way relation. $w, c, c' \models\!\models R$ means that with incoming clocking event c, w tightly satisfies R in such a way that the outgoing clocking event is c'.

Let w be a finite word. Let b denote a boolean expression, c, c', d denote clocking events, R, R' denote sequences.

- $w, c, c' \models\!\models b$ iff $c' = c$ and w is a clock tick of c and $w^{|w|-1} \Vdash b$.
- $w, c, c' \models\!\models \texttt{@(}d\texttt{)}\ R$ iff $w, d, c' \models\!\models R$.
- $w, c, c' \models\!\models \texttt{(}R\texttt{)}$ iff $c' = c$ and there exists d such that $w, c, d \models\!\models R$.
- $w, c, c' \models\!\models R\ \texttt{\#\#1}\ R'$ iff there exist x, y, d such that $w = xy$ and $x, c, d \models\!\models R$ and $y, d, c' \models\!\models R'$.
- $w, c, c' \models\!\models R\ \texttt{\#\#0}\ R'$ iff there exist x, y, z, d such that $w = xyz$ and $|y| = 1$ and $xy, c, d \models\!\models R$ and $yz, d, c' \models\!\models R'$.
- $w, c, c' \models\!\models R\ \texttt{or}\ R'$ iff either $w, c, c' \models\!\models R$ or $w, c, c' \models\!\models R'$.
- $w, c, c' \models\!\models R\ \texttt{intersect}\ R'$ iff both $w, c, c' \models\!\models R$ and $w, c, c' \models\!\models R'$.
- $w, c, c' \models\!\models \texttt{first\_match(}R\texttt{)}$ iff $c' = c$ and there exists d such that $w, c, d \models\!\models R$ and for all x, y, d' such that $w = xy$ and $\bar{x}, c, d' \models\!\models R$, $|y| = 0$.
- $w, c, c' \models\!\models R\texttt{[*0]}$ iff $c' = c$ and $|w| = 0$.
- $w, c, c' \models\!\models R\texttt{[*1:\$]}$ iff there exist $c_0, w_1, c_1, w_2, c_2, ..., w_j, c_j$ $(j > 0)$ such that $c_0 = c$ and $c_j = c'$ and $w = w_1 w_2 \cdots w_j$ and for all $1 \leq i \leq j$, $w_i, c_{i-1}, c_i \models\!\models R$.

2.3 Neutral satisfaction of properties without local variables

Without local variables, neutral satisfaction is a three-way relation. $w, c \models P$ means that with incoming clocking event c, w neutrally satisfies P.

Let w be a finite or infinite word. Let b denote a boolean expression, c, c', d denote clocking events, P, P' denote properties.

- $w, c \models R$ iff there exist x, c' such that $x \leq w$ and $x, c, c' \models\!\models R$.

- $w, c \models$ `@(`d`)` P iff $w, d \models P$.
- $w, c \models$ `(`P`)` iff $w, c \models P$.
- $w, c \models$ `not` P iff $\bar{w}, c \not\models P$.
- $w, c \models P$ `or` P' iff either $w, c \models P$ or $w, c \models P'$.
- $w, c \models P$ `and` P' iff both $w, c \models P$ and $w, c \models P'$.
- $w, c \models R$ `|->` P iff for all x, y, z, d such that $w = xyz$ and $|y| = 1$ and $xy, c, d \models\!\models R$, $yz, d \models P$.
- $w, c \models$ `disable iff (`b`)` P iff either $w, c \models P$ or there exists $0 \leq k < |w|$ such that $w^k \models\!\!\!\models b$ and $w^{0..k-1}\top^\omega, c \models P$. Here, $w^{0..-1}$ denotes the empty word.

2.4 Tight satisfaction of sequences with local variables

With local variables, tight satisfaction is a six-way relation. $w, c, L, c', L' \models\!\models R$ means that with incoming clocking event c and incoming local variable context L, w tightly satisfies R in such a way that the outgoing clocking event is c' and the outgoing local variable context is L'.

Let w be a finite word. Let b denote a boolean expression, v, v' denote local variables, c_0, c_1, c, c', d denote clocking events, R, R' denote sequences, L_0, L_1, L, L', L'' denotes local variable contexts.

- $w, c_0, L_0, c_1, L_1 \models\!\models b$ iff $c_1 = c_0$ and $L_1 = L_0$ and w is a clock tick of c_0 and $w^{|w|-1} \models\!\!\!\models b[L_0]$.
- $w, c_0, L_0, c_1, L_1 \models\!\models$ `(1, `v `=` e`)` iff $c_1 = c_0$ and w is a clock tick of c_0 and $\mathrm{dom}(L_1) = \mathrm{dom}(L_0) \cup \{v\}$ and $L_1(v) = e[L_0, w^{|w|-1}]$ and $L_1(v') = L_0(v')$ for $v' \in \mathrm{dom}(L_0) - \{v\}$.
- $w, c_0, L_0, c_1, L_1 \models\!\models$ `@(`c`)` R iff $w, c, L_0, c_1, L_1 \models\!\models R$.
- $w, c_0, L_0, c_1, L_1 \models\!\models$ `(`R`)` iff $c_1 = c_0$ and there exists c such that $w, c_0, L_0, c, L_1 \models\!\models R$.
- $w, c_0, L_0, c_1, L_1 \models\!\models R$ `##1` R' iff there exist x, y, c, L such that $w = xy$ and $x, c_0, L_0, c, L \models\!\models R$ and $y, c, L, c_1, L_1 \models\!\models R'$.
- $w, c_0, L_0, c_1, L_1 \models\!\models R$ `##0` R' iff there exist x, y, z, c, L such that $w = xyz$ and $|y| = 1$ and $xy, c_0, L_0, c, L \models\!\models R$ and $yz, c, L, c_1, L_1 \models\!\models R'$.
- $w, c_0, L_0, c_1, L_1 \models\!\models R$ `or` R' iff there exists L such that either $w, c_0, L_0, c_1, L \models\!\models R$ or $w, c_0, L_0, c_1, L_1 \models\!\models R'$ and L_1 is obtained from L by restricting its domain to $\mathit{flow}(\mathrm{dom}(L_0), R$ `or` $R')$.
- $w, c_0, L_0, c_1, L_1 \models\!\models R$ `intersect` R' iff there exist L, L' such that both $w, c_0, L_0, c_1, L \models\!\models R$ and $w, c_0, L_0, c_1, L' \models\!\models R'$ and such that $L_1 = L|_D \cup L'|_{D'}$, where
  - $D = \mathit{flow}(\mathrm{dom}(L_0), R) - (\mathit{block}(R$ `intersect` $R') \cup \mathit{sample}(R'))$
  - $D' = \mathit{flow}(\mathrm{dom}(L_0), R') - (\mathit{block}(R$ `intersect` $R') \cup \mathit{sample}(R))$

- $w, c_0, L_0, c_1, L_1 \models$ `first_match(`R`)` iff $c_1 = c_0$ and there exists c such that $w, c_0, L_0, c, L_1 \models R$ and for all x, y, c', L' such that $w = xy$ and $\bar{x}, c_0, L_0, c', L' \models R$, $|y| = 0$.
- $w, c_0, L_0, c_1, L_1 \models R$`[*0]` iff $c_1 = c_0$ and $L_1 = L_0$ and $|w| = 0$.
- $w, c_0, L_0, c_1, L_1 \models R$`[*1:$]` iff there exist $c_{(0)} = c_0$, $L_{(0)} = L_0$, w_1, $c_{(1)}$, $L_{(1)}$, w_2, $c_{(2)}$, $L_{(2)}$, $\ldots, w_j$, $c_{(j)} = c_1$, $L_{(j)} = L_1$ $(j > 0)$ such that $w = w_1 w_2 \cdots w_j$ and for all $1 \leq i \leq j$, $w_i, c_{(i-1)}, L_{(i-1)}, c_{(i)}, L_{(i)} \models R$.

2.5 Neutral satisfaction of properties with local variables

With local variables, neutral satisfaction is a four-way relation. $w, c, L \models P$ means that with incoming clocking event c and incoming local variable context L, w neutrally satisfies P.

Let w be a finite or infinite word. Let b denote a boolean expression, c, c', d denote clocking events, P, P' denote properties, L, L' denotes local variable contexts.

- $w, c, L \models R$ iff there exist x, c', L' such that $x \leq w$ and $x, c, L, c', L' \models R$.
- $w, c, L \models$ `@(`d`)` P iff $w, d, L \models P$.
- $w, c, L \models$ `(`P`)` iff $w, c, L \models P$.
- $w, c, L \models$ `not` P iff $\bar{w}, c, L \not\models P$.
- $w, c, L \models P$ `or` P' iff either $w, c, L \models P$ or $w, c, L \models P'$.
- $w, c, L \models P$ `and` P' iff both $w, c, L \models P$ and $w, c, L \models P'$.
- $w, c, L \models R$ `|->` P iff for all x, y, z, c', L' such that $w = xyz$ and $|y| = 1$ and $xy, c, L, c', L' \models R$, $yz, c', L' \models P$.
- $w, c, L \models$ `disable iff (`b`)` P iff either $w, c, L \models P$ or there exists $0 \leq k < |w|$ such that $w^k \not\models b$ and $w^{0..k-1}\top^\omega, c, L \models P$. Here, $w^{0..-1}$ denotes the empty word.