Flex Ray:
Serial Interface -
a Formal Model for Coding and Decoding

Seminar: The FlexRay Communication Protocol

Chair of Prof. Dr. W. J. Paul

Talk by Michael Gerke

14-10-2005

Overview

- General remarks
- Encoding
- Low level bit transfer
- Decoding:
  - Voting
  - Strobing

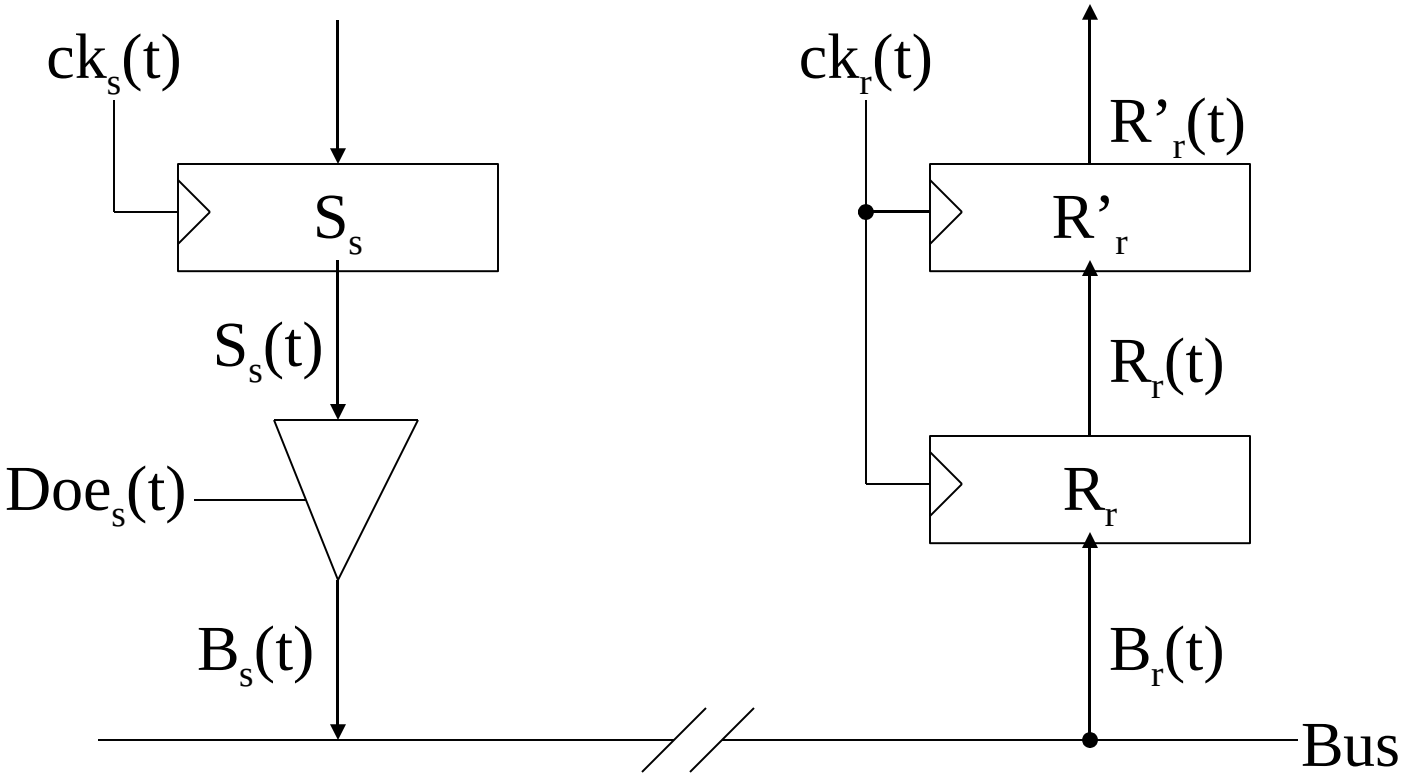
General remarks

- TSS = 0^1
- We ignore glitches
- Reception controlled by different state machine

Definitions: Clocks

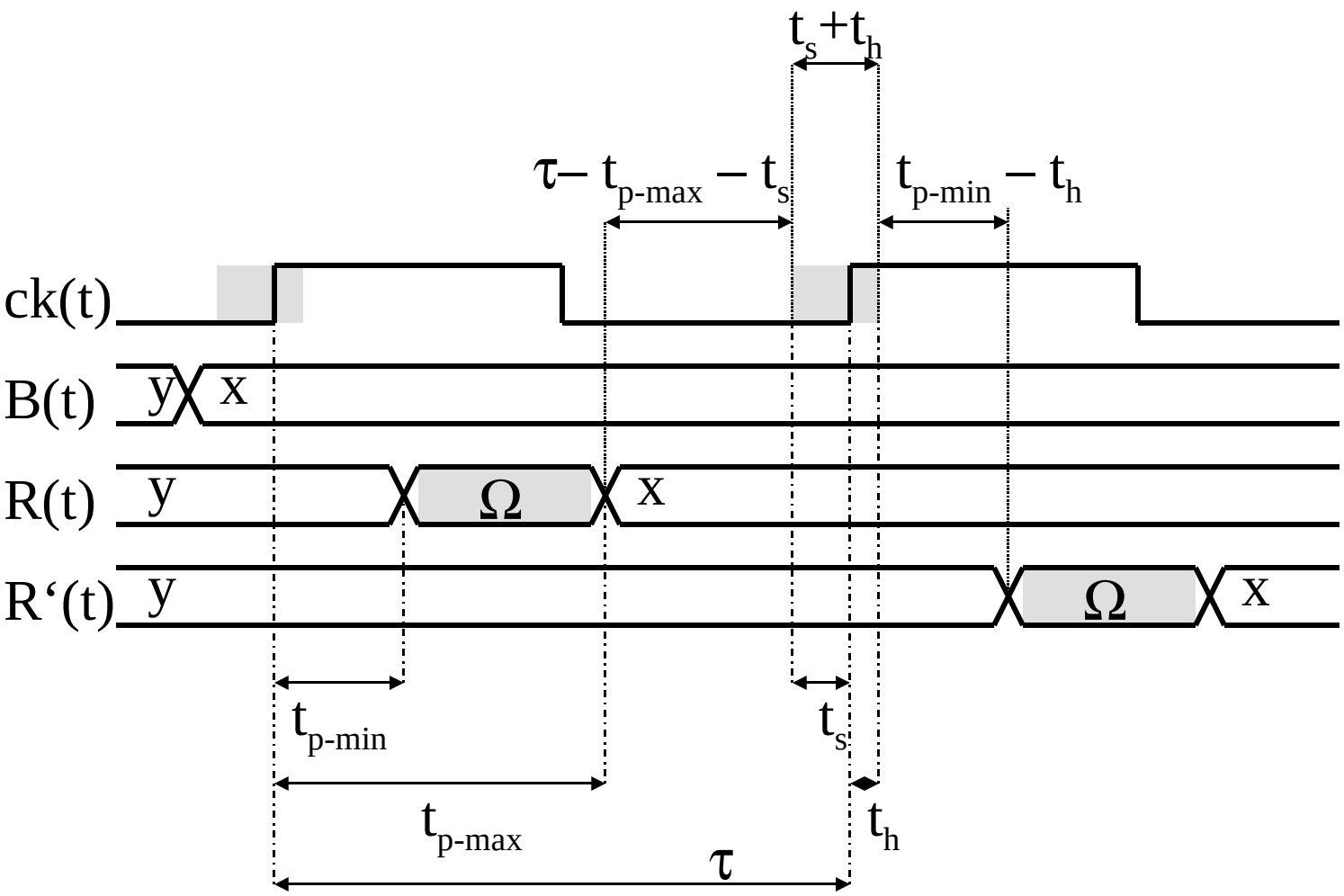
- Node number u: ECU_u has clock signal $ck_u(t)$ with cycle time $_u$
- We assume drift is at most 0.15%
- $e_u(i)$: i^{th} rising edge of ck_u
- i^{th} cycle of ECU_u: $[e_u(i),e_u(i+1)[$

Serial bus interface:



Lower indices: X_s *=sender's* X *and* X_r *=receiver's* X

Definition: Register semantics

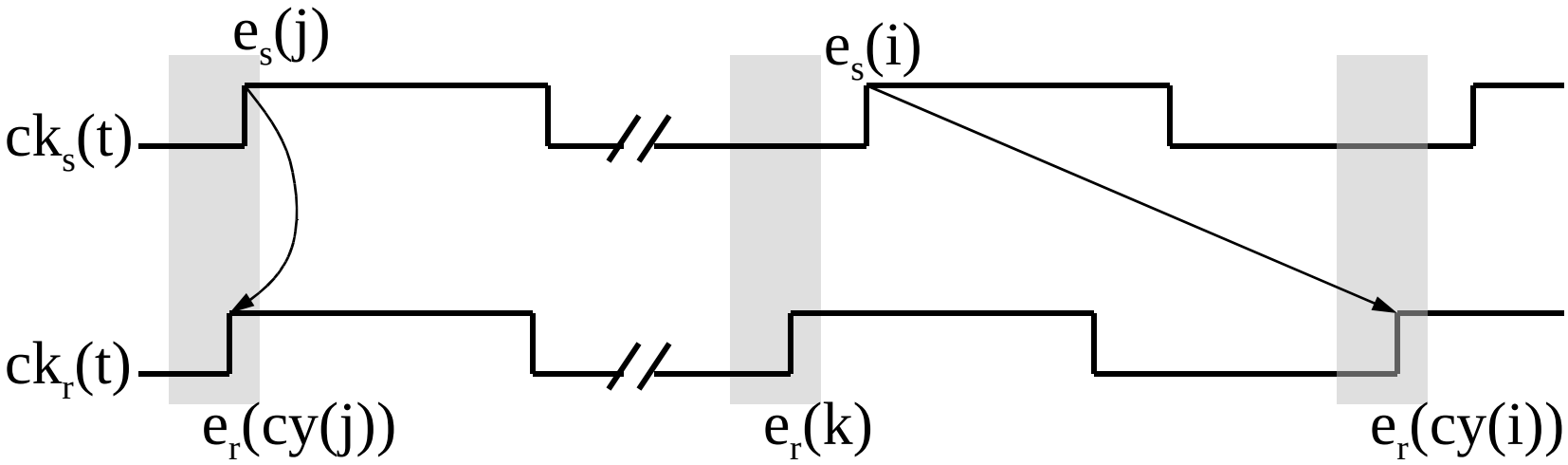


Definition: Formal register semantics

- Old value of R=y.
- B(t)=x: $t \in [e(i)-t_s, e(i)+t_h]$: sampling interval
- $$R(t) = \begin{cases} y & : t \le e(i) + t_{p-min} \\ & : e(i) + t_{p-min} < t < e(i) + t_{p-max} \\ x & : t \ge e(i) + t_{p-max} \end{cases}$$
- $R'(t) \in \{0,1\}$
- normal: $R'(e(i)+t_{p\text{-}max}) = R(e(i)-t_s)$

Note that we get a delay of 1 caused by the second register R'.

Definition: Bus connection



First affected receiver cycle:

$$cy(i)=\max\{k|e_r(k)+t_h<e_s(i)\}+1$$

Definition:
Formal Bus connection

If the sender s puts new value B_s^i on the bus in cycle i at clock edge $e_s(i)$:

$$B_s^i \neq B_s^{i-1}$$

The first affected receiver cycle is denoted by:

$$cy(i)=\max\{k|e_r(k)+t_h<e_s(i)\}+1$$

Upper indices: $X^i = X$ *directly before the end of cycle* i *(when all hardware has stabilized)*

Lemma 1

IF $x = B_s^i = \ldots = B_s^{i+7}$

THEN $R'_r{}^{cy(i)+k+1} = R_r^{cy(i)+k} = x;\ k \in [\beta:\beta+6];\ \beta \in \{0,1\}$

If the sender holds the bus stable for eight consecutive cycles, then the receiver samples during at least 7 consecutive cycles the correct value x. The value of β depends on the difference between sender and receiver clock and is either 0 or 1.

Proof: Lemma 1

Let clock drift be bounded by 0.15% and only one node be sending.

The sampling intervals of all receiver edges cy(i)+k are in a region of time where the bus is stable.

If the sampling interval for k=0 is not in this region, then the sampling interval for k=7 is and vice versa, so I can select $\beta \in \{0,1\}$ such that the Lemma holds.

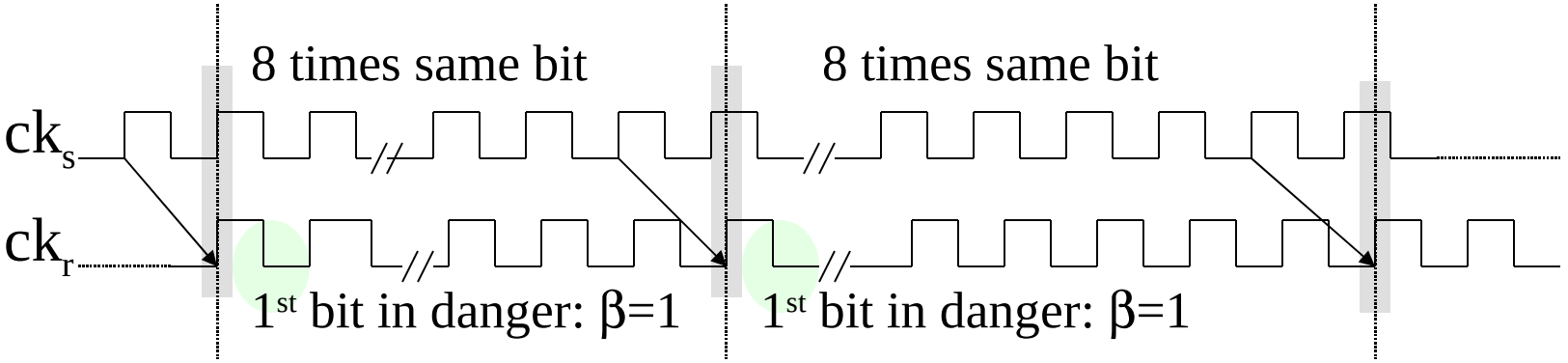
Lemma 2

IF $x = B_s^{i-8} = \ldots = B_s^{i-1}$ and $\neg x = B_s^{i} = \ldots = B_s^{i+7}$

THEN for i': $\neg x = R'^{i'}_{r} \neq R'^{i'-1}_{r}$: $i' \in cy(i)+[0:1]+1$

If the sender transmits x in cycles i–8 to i–1 and ¬x in cycles i to i+7, then the cycle i' in which ¬x occurs for the first time in is bounded by an interval of two cycles: $i' \in cy(i)+[0:1]+1$

Proof: Lemma 2



As clock drift is bounded by 0.15%, we know that for two succeeding intervals of 8 consecutively sent bits the value of β is the same.

Lemma 3

$\forall i: \forall k < 600:\ cy(i+k) \in cy(i) + k + [-1:1]$

During 600 cycles, a clock can get at most one cycle difference to the idealized clock due to drift.

Proof: Lemma 3

Usually: $cy(i+1)=cy(i)+1$, clock drift can cause:

$cy(i+1)=cy(i)$ or $cy(i+1)=cy(i+2)$

As drift is bounded by 0.15%, this can happen at most once in $1/0.0015>600$ cycles.

Definition: Frame assembly

m : message to be transferred

f(m) : frame to be sent (and to be reassembled)

F(m) : bit vector to be transmitted

Definition: Frame assembly

f(m)=

TSS FSS BSS m[0] ... BSS m[l–1] FES

As each bit is transmitted for 8 cycles:

$F(m)=f(m)[0]^8 \ldots f(m)[l'-1]^8$

Sender cycles are numbered such that:

$B_s^i=F(m)[i]$

Lemma 4

$\forall f(m)[i]: \exists \beta \in \{0,1\}: \forall k \in [\beta:\beta+6]:$

$R'_r{}^{cy(8\cdot i)+k+1} = R_r{}^{cy(8\cdot i)+k} = f(m)[i]$

This means the bit f(m)[i] is correctly sampled at receiver edge cy(8·i)+k

Proof: Lemma 4

Bus stable for 8 consecutive cycles:

$B_s^{8 \cdot i+k} = f(m)[i]$ for $k \in [0:7]$

Apply Lemma 1

Voting: Definition

v^j=majority vote over last five R' values: R'^j, …, R'^{j-4}

Note that we get a delay of 2 cycles caused by the voting process.

Lemma 5

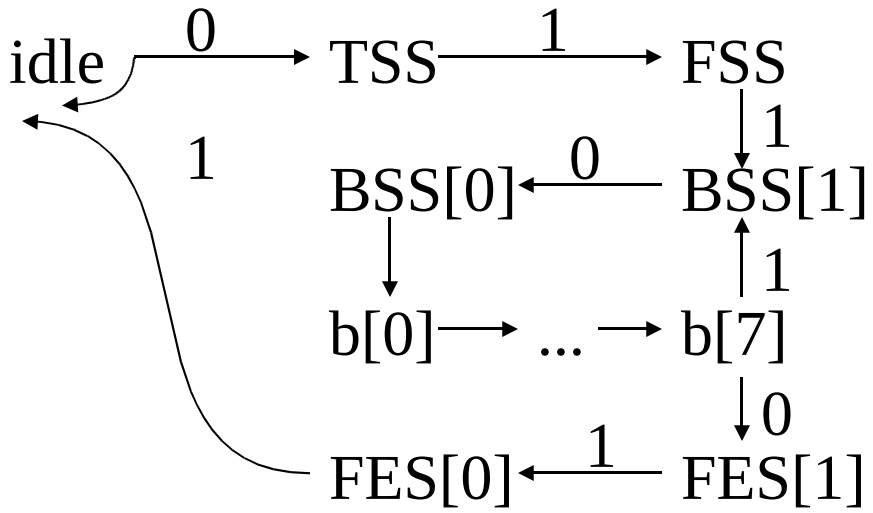
$\forall f(m)[i]: \exists \beta \in \{0,1\}: \forall k \in [\beta+2:\beta+8]: v^{cy(8\cdot i)+k+1} = f(m)[i]$

This means the bit f(m)[i] is correctly voted at receiver edge cy(8·i)+k+1

Proof: Lemma 5

Lemma 4 entails that in cycles $cy(8 \cdot i)+k+1$ for $k \in [\beta+2:\beta+8]$ we have received at least three copies of bit $f(m)[i]$.

Bit strobing: Automaton



Transition function: $\Delta(s,i)$

Automaton clocked at: $strobe^t$

Bit strobing: Definitions

strobe point: $strobe^j=(cnt^j=4)$

$$state^{t+1}=\begin{cases}(state^t, v^t) & : strobe^t \\ state^t & : otherwise\end{cases}$$

$$sync^j= ((state^j=idle)\wedge v^{j-1})\vee((state^j=BSS[1])\wedge v^{j-1}\wedge\neg v^j)$$

$$cnt^{j+1}=\begin{cases}1 & : sync^j \\ (cnt^j+1) \bmod 8 & : otherwise\end{cases}$$

Bit strobing: Definitions

str(h) denotes the index of the cycle of the $(h+1)^{th}$ activation of the strobe signal

sy(h) denotes the index of the (last) cycle of the $(h+1)^{th}$ activation of the sync signal

nb(h) is the number of bits of f(m) sent in synchronization interval [sy(h):sy(h+1)]

$NB(h)=\sum_{h'<h} nb(h')$

The Theorem: Motivation

We want to show that the message is correctly reassembled by the receiver.

In order to do so, we will show that the automaton and the syncing work as expected and thus the right bits are strobed.

These criteria will be formulated as an invariant.

Invariant

1) Automaton correctly monitors the received bits

2) Message bits are correctly strobed

3)Transitions of automaton occur fast enough,
i.e. before the next bit can be sampled

4) Sync signals are activated at expected times

5) Strobe signals are activated at expected times

Lemma 7 Preconditions

For any receiver cycle j,

for any k=NB(h')+k' with

str(k)≤j and

k'∈[0:nb(h')–1],

and for any h with

sy(h)≤j

it holds:

Lemma 7 Preconditions

For any receiver cycle j;

Induction over j

for any k=NB(h')+k', with

str(k)≤j and

k'∈[0:nb(h')–1],

and for any h with

sy(h)≤j

it holds:

Number of actual bit in this sync interval

Number of bits sent in previous sync intervals 0,…,h'

Number of bits to be sent in this sync interval

Actual sync number: h

NB(h')≤ k≤ NB(h)

Lemma 7 Part 1

1) **If strobe k is the last strobe before cycle j, i.e. $j \in [str(k)+1:str(k+1)]$, then $state^j$ is given as expected (see Automaton):**

In the first sync interval (h'=0) $state^j$ is equal to:

TSS for k'=0; FSS for k'=1 or BSS[1] for k'=2

In the other sync intervals

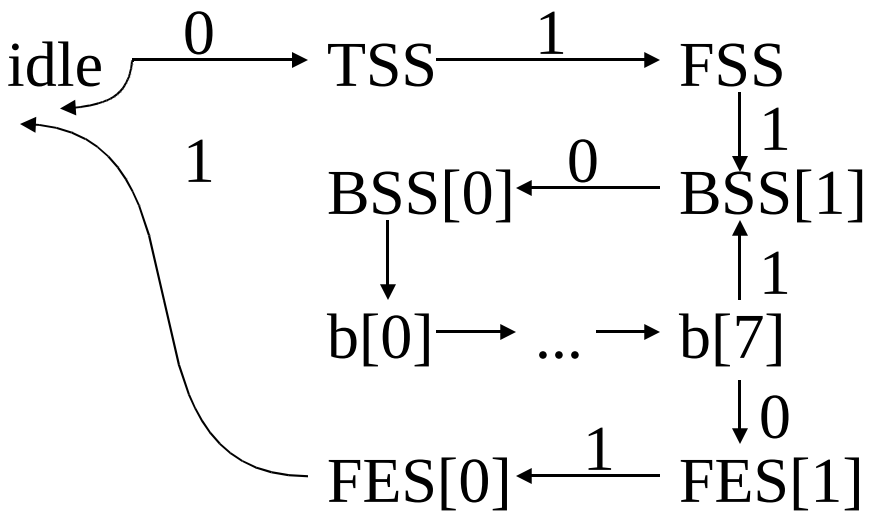
(of length $nb(h') \in [10:11]$), $state^j$ is equal to:

BSS[0] for k'=0 or b[k'–1] for $k' \in [1:8]$

All but the last sync interval ($h' < l$) end with $state^j$=BSS[1] for k'=9

For $h'=l$ we have $state^j$=FES[10–k'] for $k' \in [9:10]$

Reminder: Automaton



Lemma 7 Parts 2-5

2) The sampled signals satisfy $v^{str(k)}=f(m)[k]$

3) $str(k)+1< cy(8\cdot(k+1))+[2:3]+1$

4) $sy(h)\in cy(8\cdot NB(h))+[2:3]+1$

5) $str(k)=sy(h')+8\cdot(k-NB(h')))+4$

Lemma 7 Proof Plan

We do an induction over j.

$I4(j) \wedge I5(j) \Rightarrow I2(j+1) \wedge I3(j+1)$ *(sub-lemma: lemma 6)*

$I2(j+1) \wedge I3(j+1) \Rightarrow I1(j+1)$ *(trivial)*

$I1(j+1) \wedge I3(j+1) \Rightarrow I4(j+1) \wedge I5(j+1)$

I4(j)∧I5(j)⇒I2(j+1)∧I3(j+1)

We want to show:

2)*The message bits are correctly strobed:*

The sampled signals satisfy $v^{str(k)}=f(m)[k]$

3)*Transitions of the automaton occur fast enough, i.e. before the next bit can be sampled:*

$str(k)+1< cy(8\cdot(k+1))+[2:3]+1$

Lemma 6

Assuming that sender cycles NB(h) and corresponding receiver cycles are not to far apart:

IF

(1) *Strobepoint occurs in the expected time bounds* and if

(2) *Syncing occurs in the expected time bounds*

THEN

(i)*The message bits are correctly strobed*

(ii)*Transitions of the automaton occur fast enough, i.e. before the next bit can be sampled*

Lemma 6

IF h’ maximal such that

(1) $str(k)=sy(h')+8\cdot(k-NB(h'))+4$ and if

(2) $sy(h')\in cy(8\cdot NB(h'))+[2:3]+1$

THEN

(i) $v^{str(k)}=f(m)[k]$ and

(ii) $str(k)+1<cy(8\cdot(k+1))+[2:3]+1$

Proof: Lemma 6 (i)

Part(i) using Lemma 3 and Lemma 5:

$$str(k) = sy(h') + 8\cdot(k - NB(h')) + 4$$
$$\in cy(8\cdot NB(h')) + 8\cdot(k - NB(h')) + [6:7] + 1$$
$$\in cy(8\cdot(NB(h') + k - NB(h'))) + [5:8] + 1$$

$$v^{str(k)} = f(m)[k]$$

Proof: Lemma 6 (ii)

Part(ii) using Lemma 3:

$$\begin{aligned} str(k)+1 &\in cy(8\cdot NB(h'))+8\cdot(k-NB(h'))+[6:7]+1+1 \\ &= cy(8\cdot NB(h'))+8\cdot(k-NB(h')+1)+[0:1] \\ &\in cy(8\cdot(NB(h')+k-NB(h')+1))+[-1:2] \\ &< cy(8\cdot(k+1))+[2:3]+1 \end{aligned}$$

I1(j+1)∧I3(j+1)⇒I4(j+1)

We want to show:

4) *sync signals are activated at expected times:*

$sy(h) \in cy(8 \cdot NB(h)) + [2:3] + 1$

Lemma 7 Proof Part 4

We have to show:

(iii)The falling edge that triggers sy(h) is seen by the receiver during the right cycle j

(ii) The automaton is in the state BSS[1] during cycle j

Lemma 7 Proof Part 4(i)

Lemma 2 combined with Lemmas 4 and 5 shows that the falling edge which triggers sy(h) is seen in v^j for $j \in cy(8 \cdot NB(h))+[2:3]+1$

From 2:

First seen in n': $n' \in cy(n)+[0:1]+1$

From 4,5:

$f(m)[i]=v^{cy(8 \cdot i)+[2:3]+1}$

Lemma 7 Proof Part 4(ii)

Part1 implies $state^j$=BSS[1] for cycles $j \in$ [str(k)+1:str(k+1)]

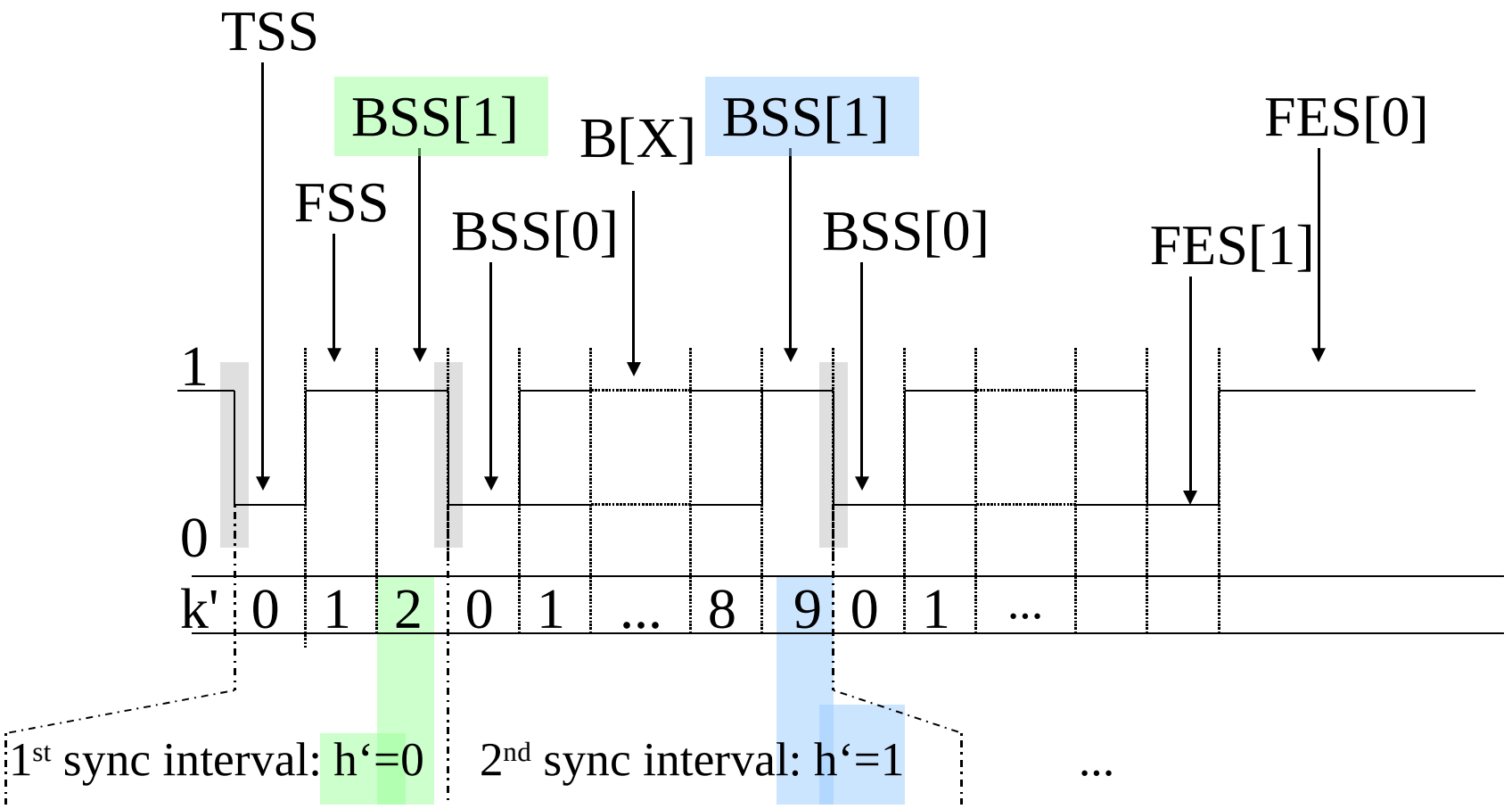
if k is maximal and

$(h'=0 \wedge k'=2) \vee (h' \in [1:l-1] \wedge k'=8)$.

Outside these time intervals the sync signal cannot become active.

Encoding of Frames

remember: k=NB(h')+k'



Lemma 7 Proof Part 4(ii)

Part 3 implies

$$str(k)+1 < cy(8 \cdot (NB(h')+k'+1))+[2:3]+1$$

Thus the automaton is in state BSS[1] one cycle before the first zero of the BSS[0] bit can be possibly sampled.

$I1(j+1) \wedge I3(j+1) \Rightarrow I5(j+1)$

We want to show:

5) strobe signals are activated at expected times:

$str(k)=sy(h')+8\cdot(k-NB(h')))+4$

Lemma 7 Proof Part 5

For the case k’=0:

$$sy(h') \in sy(h'-1)+8\cdot nb(h'-1)+[-1:1]$$
$$=sy(h'-1)+8\cdot(nb(h'-1)-1)+8+[-1:1]$$

From the induction hypothesis:

$$str(k-1)=sy(h'-1)+8\cdot(k-1-NB(h'-1))+4$$
$$=sy(h'-1)+8\cdot(nb(h'-1)-1)+4$$

Thus str(k–1) is before sy(h’) and there is no additional strobe between them.

Lemma 7 Proof Part 5

For the case k'>0 part 5 follows from the induction hypotheses. (k=NB(h')+k')

Definition: Frame reassembly

After reset: empty reconstruction frame f'^{0}

$$f'^{t+1} = \begin{cases} f'^{t} \circ v^{t} & : \text{strobe}^{t} \\ f'^{t} & : \text{otherwise} \end{cases}$$

The theorem

Let clock drift $\delta \leq 0.0015$

Let $L = 8 \cdot l'$ be the length of $F(m)$

$$f'^{\lceil (1+\delta) \cdot L \rceil + 8} = f(m)$$