Ch 13 – Proofs: Self-Stabilizing Lynch-Welch

The objective is to make the Lynch-Welch algorithm of Ch10 withstand any number of transient faults and and at the same time up to f Byzantine faults.

Dwelling into the proofs

if v generates a beat at time t **then**

  if $i \neq 0$ **then**

    ▹ beats should align with every M^{th} pulse, hence reset

    reset(R^{+}) delay the next pulse

  else if Algorithm 16 requires generating a pulse before $H_v(t) + R^{-}$ **then**

    ▹ reset at pulse time t' to avoid early pulse or message

    reset($R^{+} - (H_v(t') - H_v(t))$), where t' is the current time delay the next pulse

  else if next pulse is not generated by local time $H_v(t) + R^{+}$ **then**

    ▹ reset to avoid late pulse and

    ▹ start listening for other nodes' pulses on time

    reset(0) force a pulse

  end if

end if i=0 and well aligned (green window)

Function(**reset**(τ))

stop local instance of Algorithm 16

wait for τ local time

$i := 0$

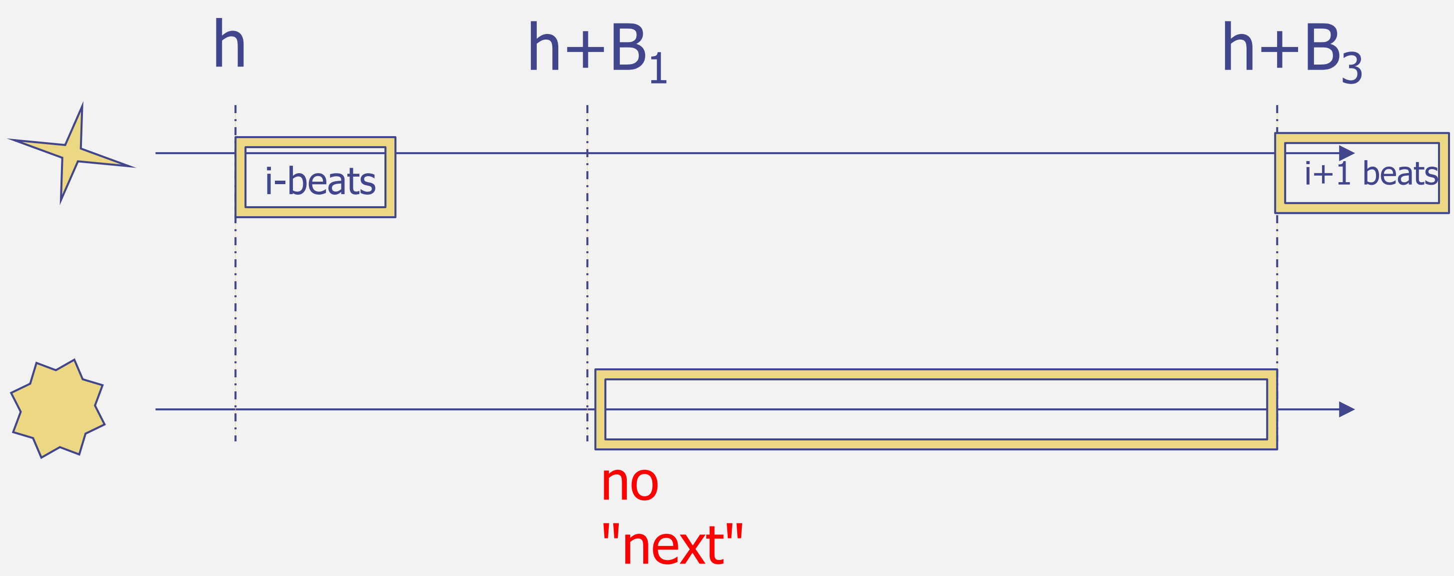
initialize a new local instance of Algorithm 16

From the pseudocode given in Algorithm 17, it is straightforward to verify that $v \in V_g$ generates a pulse at a local time from $[H_v(h_{v,1}) + R^{-}, H_v(h_{v,1}) + R^{+}]$, and does not generate a pulse at a local time from $[H_v(h_{v,1}), H_v(h_{v,1}) + R^{-})$.

Beats and Feedbacks

Definition 13.2 (Feedback Mechanism). *Nodes $v \in V_g$ generate* beats *at times $h_{v,i} \in \mathbb{R}$, $i \in \mathbb{N}$, such that for parameters $0 < B_1 < B_2 < B_3 \in \mathbb{R}$ and σ_h (a skew bound) the following properties hold, for all $i \in \mathbb{N}$.*

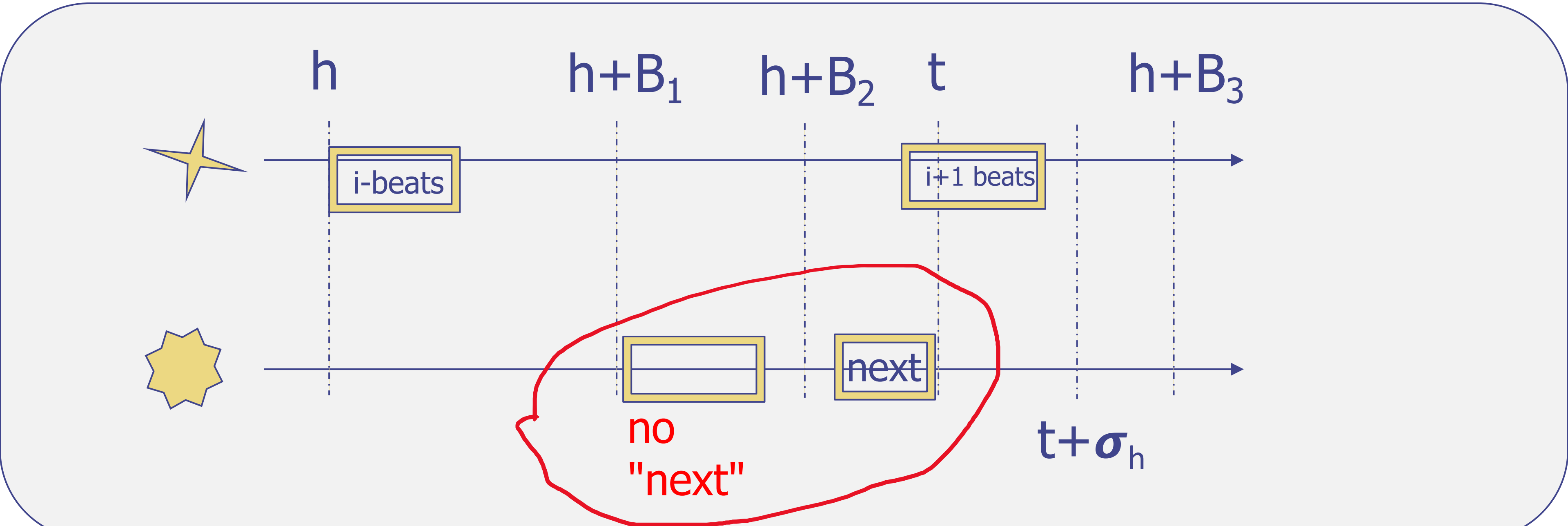
1. *For all $v, w \in V_g$, we have that $|h_{v,i} - h_{w,i}| \leq \sigma_h$.*
2. *If no $v \in V_g$ triggers its NEXT signal during $[\min_{w \in V_g}\{h_{w,i}\} + B_1, t]$ for some $t < \min_{w \in V_g}\{h_{w,i}\} + B_3$, then $\min_{w \in V_g}\{h_{w,i+1}\} > t$.*



Recall: Beats and Feedbacks

Definition 13.2 (Feedback Mechanism). *Nodes $v \in V_g$ generate* beats *at times $h_{v,i} \in \mathbb{R}$, $i \in \mathbb{N}$, such that for parameters $0 < B_1 < B_2 < B_3 \in \mathbb{R}$ and σ_h (a skew bound) the following properties hold, for all $i \in \mathbb{N}$.*

1. *For all $v, w \in V_g$, we have that $|h_{v,i} - h_{w,i}| \le \sigma_h$.*
2. *If no $v \in V_g$ triggers its NEXT signal during $[\min_{w \in V_g}\{h_{w,i}\} + B_1, t]$ for some $t < \min_{w \in V_g}\{h_{w,i}\} + B_3$, then $\min_{w \in V_g}\{h_{w,i+1}\} > t$.*
3. *If all $v \in V_g$ trigger their NEXT signals during $[\min_{w \in V_g}\{h_{w,i}\} + B_2, t]$ for some $t \le \min_{w \in V_g}\{h_{w,i}\} + B_3$, then $\max_{w \in V_g}\{h_{w,i+1}\} \le t + \sigma_h$.*



Breakout room:

Discussing how one should tackle the proof.

Initial requirements on round execution

We fall back on the original LW protocol and proofs.

To use it we need to make sure that following holds:

1) No more resets (disturbing LW loop)
2) All correct start with an assumed skew (S)
3) Messages sent by correct nodes in a given round should be received by all correct nodes after they start the current round and before they compute Δ
4) T is large enough to accommodate the adjustments for the next iteration

To use the LW proofs we assume:

$\delta = u + (1-\vartheta)d + (\vartheta^2 + \vartheta - 2)S$

$7 - 6\vartheta^2 > 0$

$T := (\vartheta^2 + \vartheta + 1)S + \vartheta d + R^{--}$

Assumed Inequalities

We assume the following holds, we later show that we can obtain that.

$$R^+ \geq R^- + (3\vartheta + 4)S(M) + \sigma_h \tag{13.1}$$

$$\mathcal{S} = R^+ + \sigma_h - R^-/\vartheta \tag{13.2}$$

$$\mathcal{S} \geq \frac{2(2\vartheta - 1)\delta + 2(\vartheta - 1)T}{2 - \vartheta} \tag{13.3}$$

$$\frac{R^-}{\vartheta} \geq \sigma_h + \vartheta\mathcal{S} + d \tag{13.4}$$

Assumed Inequalities

We assume the following holds, we later show that we can get that.

$$R^+ \geq R^- + (3\vartheta + 4)S(M) + \sigma_h \tag{13.1}$$

$$\mathcal{S} = R^+ + \sigma_h - R^-/\vartheta \tag{13.2}$$

$$\mathcal{S} \geq \frac{2(2\vartheta - 1)\delta + 2(\vartheta - 1)T}{2 - \vartheta} \tag{13.3}$$

$$\frac{R^-}{\vartheta} \geq \sigma_h + \vartheta\mathcal{S} + d \tag{13.4}$$

$$\frac{B_2}{\vartheta} > \sigma_h + R^+ + T + 3\mathcal{S} \tag{13.5}$$

$$B_1 > \sigma_h + R^+ \tag{13.6}$$

$$B_3 > R^+ + (M - 1)(T + 3\mathcal{S}) + (\vartheta + 1)\mathcal{S}(M) + \sigma_h \tag{13.7}$$

Assumed Inequalities

We assume the following holds, we later show that we can get that.

$$R^+ \geq R^- + (3\vartheta + 4)S(M) + \sigma_h \tag{13.1}$$

$$\mathcal{S} = R^+ + \sigma_h - R^-/\vartheta \tag{13.2}$$

$$\mathcal{S} \geq \frac{2(2\vartheta - 1)\delta + 2(\vartheta - 1)T}{2 - \vartheta} \tag{13.3}$$

$$\frac{R^-}{\vartheta} \geq \sigma_h + \vartheta\mathcal{S} + d \tag{13.4}$$

$$\frac{B_2}{\vartheta} > \sigma_h + R^+ + T + 3\mathcal{S} \tag{13.5}$$

$$B_1 > \sigma_h + R^+ \tag{13.6}$$

$$B_3 > R^+ + (M - 1)(T + 3\mathcal{S}) + (\vartheta + 1)\mathcal{S}(M) + \sigma_h \tag{13.7}$$

$$B_2 \leq \frac{R^-}{\vartheta} + (M - 1)\left(\frac{T - (\vartheta + 1)\mathcal{S}}{\vartheta}\right) + \mathcal{S}(M) \tag{13.8}$$

$$\cancel{\frac{R^+}{\vartheta} \geq (\vartheta + 1)\mathcal{S}(M) + \sigma_h} \tag{13.9}$$

$$\mathcal{S}(M) < \frac{\vartheta\mathcal{S} - \sigma_h}{\vartheta + 1} \tag{13.10}$$

if v generates a beat at time t **then**

  if $i \neq 0$ **then**

    ▹ beats should align with every M^{th} pulse, hence reset

    reset(R^{+}) delay the next pulse

  else if Algorithm 16 requires generating a pulse before $H_v(t) + R^{-}$ **then**

    ▹ reset at pulse time t' to avoid early pulse or message

    reset$(R^{+} - (H_v(t') - H_v(t)))$, where t' is the current time delay the next pulse

  else if next pulse is not generated by local time $H_v(t) + R^{+}$ **then**

    ▹ reset to avoid late pulse and

    ▹ start listening for other nodes' pulses on time

    reset(0) force a pulse

  end if

end if i=0 and well aligned (green window)

Function(**reset**(τ))

stop local instance of Algorithm 16

wait for τ local time

$i := 0$

initialize a new local instance of Algorithm 16

From the pseudocode given in Algorithm 17, it is straightforward to verify that $v \in V_g$ generates a pulse at a local time from $[H_v(h_{v,1}) + R^{-}, H_v(h_{v,1}) + R^{+}]$, and does not generate a pulse at a local time from $[H_v(h_{v,1}), H_v(h_{v,1}) + R^{-})$.

Lemma 13.3

Lemma 13.3. *Let* $h := \min_{v \in V_g}\{h_{v,1}\}$. *We have that*

1. *Each* $v \in V_g$ *generates a pulse at a unique time* $p_{v,1} \in [h + R^-/\vartheta, h + \sigma_h + R^+]$.
2. $\|\vec{p}(1)\| \leq \mathcal{S}$.

Assume for now that the next **beat** is far enough not to disrupt the first loop of LW.

By the remarks on the "green window" – each produces a **pulse** in this window – proving 1.

All correct nodes invoke **beat**s within σ_h of each other.
The inequalities imply that they invoke the **pulse**s within S
- proving 2.

Lemma 13.3

Lemma 13.3. *Let* $h := \min_{v \in V_g}\{h_{v,1}\}$. *We have that*

1. *Each* $v \in V_g$ *generates a pulse at a unique time* $p_{v,1} \in [h + R^-/\vartheta, h + \sigma_h + R^+]$.
2. $\|\vec{p}(1)\| \leq \mathcal{S}$.
3. *At time* $p_{v,1}$, $v \in V_g$ *sets* $i := 1$.
4. *At the time* $\min_{v \in V_g}\{p_{v,1}\}$, *no message (of Algorithm 16) sent by node* $v \in V_g$ *before time* $p_{v,1}$ *is in transit any more.*

The 3rd is immediate from the protocol.
The 4th follows from the fact that following a pulse nodes wait for S before sending the single message of Alg 16.
The bound on R- ensures that all previous messages in transit should have arrived before we produce the pulse.

No recent reset

Let $h = \min_{v \in Vg}\{ h_{v,1} \}$ and $h' = \min_{v \in Vg}\{ h_{v,2} \}$
Let H be the infimum of time at which any $v \in V_g$ performs a reset past $p_{v,1}$

Claim: $\max_{v \in Vg}\{ p_{v,2} \} < H$

Proof: By definition, $H > h'$.
Moreover, $H \geq h + B_2$ since no correct send any NEXT signal before that

$$\frac{B_2}{\vartheta} > \sigma_h + R^+ + T + 3S \qquad (13.5)$$

Thus, $H \geq h + \boldsymbol{\sigma}_h + R^+ + T + 3S$
This implies that LW behaves correctly with skew S with period T. The choice of T and δ imply that the current loop is not interrupted.
Thus, $\max_{v \in Vg}\{ p_{v,2} \} \leq \min_{v \in Vg}\{ p_{v,1} \} + P_{max}$
$\leq h + \boldsymbol{\sigma}_h + R^+ + T + 3S < H$

Corollary 13.4

Corollary 13.4. *Suppose for $r \in \mathbb{N}$ that* $\max_{v \in V_g}\{p_{v,r}\} < H$. *Then*

$$\begin{aligned}
\|\vec{p}_r\| &\le \mathcal{S}(r) \\
&:= \frac{\mathcal{S}}{2^{r-1}} + \left(2 - \frac{1}{2^{r-2}}\right)\left(\delta + \left(1 - \frac{1}{\vartheta}\right)(T + \mathcal{S} + \delta)\right) \\
&= \frac{\mathcal{S}}{2^{r-1}} + \mathcal{O}(u + (\vartheta - 1)(\mathcal{S} + d)).
\end{aligned}$$

Moreover, the generated pulses satisfy $P_{\min} \ge (T - (\vartheta + 1)\mathcal{S})/\vartheta$ *and* $P_{\max} \le T + 3\mathcal{S}$.

In the following, we assume that in Algorithm 16, estimates are computed according to Lemma 10.8 (yielding $\delta = u + (\vartheta - 1)d + (\vartheta^2 + \vartheta - 2)\mathcal{S}$), $7 - 6\vartheta^2 > 0$, and set $T = (\vartheta^2 + \vartheta + 1)\mathcal{S} + \vartheta d$. + R--

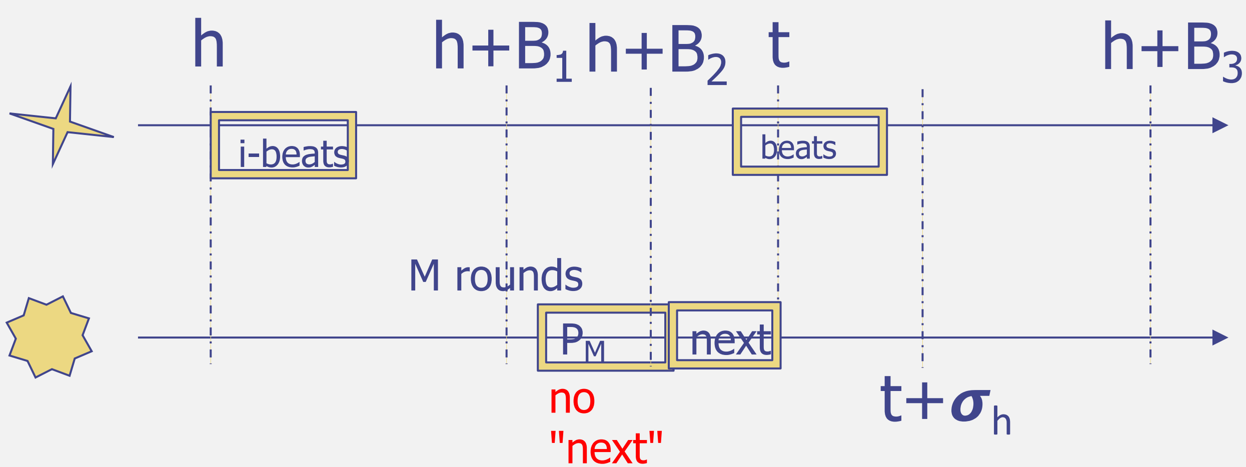
The proof follows the arguments and proofs of Ch10.

Lemma 13.5

Lemma 13.5. *For all $v \in V_g$, it holds that $h_{v,2} \in (p_{v,M} + \mathcal{S}(M), p_{v,M} + (\vartheta + 1)\mathcal{S}(M) + \sigma_h]$. In particular, no node calls the* `reset` *subroutine due to its second beat.*

Let $h = \min_{v \in V_g}\{ h_{v,1} \}$ $h' = \min_{v \in V_g}\{ h_{v,2} \}$ $p = \min_{v \in V_g}\{p_{v,M}\}$.
H be the infimum of time at which any $v \in V_g$ performs a reset

The meta algorithm implies that no $v \in V_g$ triggers NEXT before $\min\{p_{v,M}+S(M), H\}$ (proving the right part).
It also implies that all trigger NEXT past $h+B_2$ (Inequalities)



Lemma 13.5

Lemma 13.5. *For all $v \in V_g$, it holds that $h_{v,2} \in (p_{v,M} + \mathcal{S}(M), p_{v,M} + (\vartheta + 1)\mathcal{S}(M) + \sigma_h]$. In particular, no node calls the* `reset` *subroutine due to its second beat.*

Let $h = \min_{v \in V_g}\{ h_{v,1} \}$ $h' = \min_{v \in V_g}\{ h_{v,2} \}$ $p = \min_{v \in V_g}\{p_{v,M}\}$.
H be the infimum of time at which any $v \in V_g$ performs a reset

LW implies $\max_{v \in V_g}\{p_{v,M}\} \leq p + S(M) < h'$
Since NEXT delayed by $\vartheta S(M)$
$\max_{v \in V_g}\{h_{v,2}\} \leq p + (1 + \vartheta)S(M) + \sigma_h$

This proves the claim, provided that there **will not be any reset**

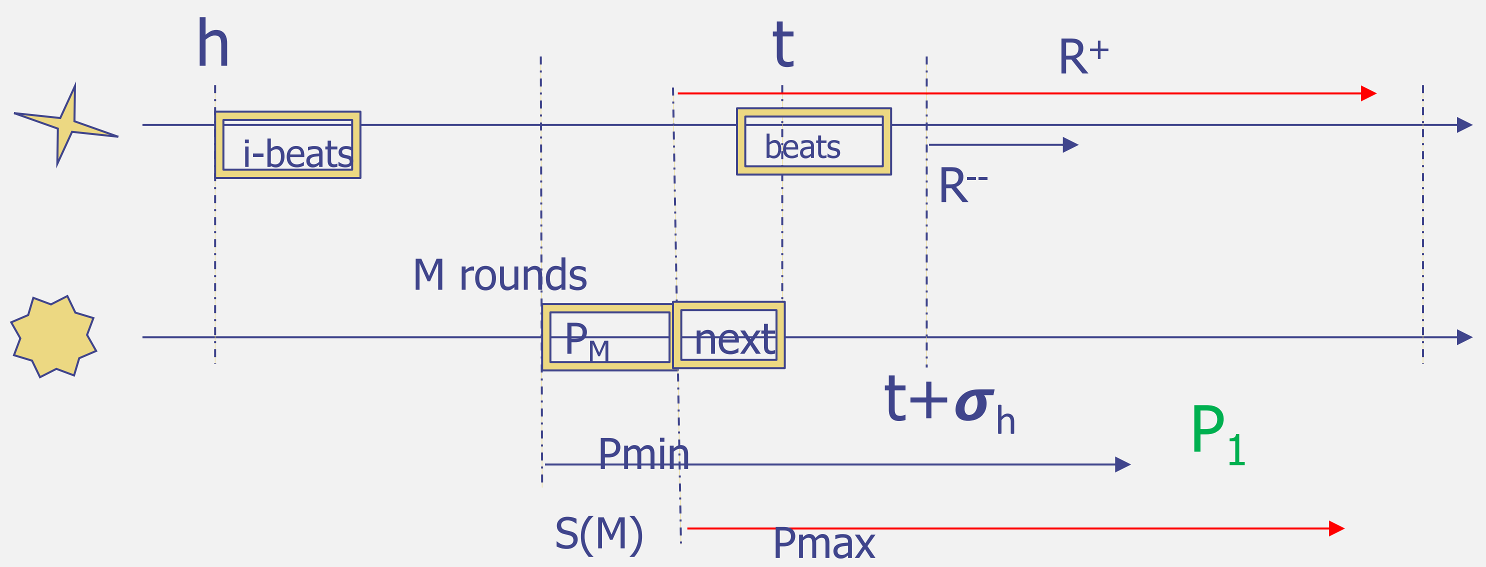
Lemma 13.5

Lemma 13.5. *For all $v \in V_g$, it holds that $h_{v,2} \in (p_{v,M} + \mathcal{S}(M), p_{v,M} + (\vartheta + 1)\mathcal{S}(M) + \sigma_h]$. In particular, no node calls the* `reset` *subroutine due to its second beat.*

By LW: P_{max}-P_{min}=$(\vartheta + 4)S(M)$. We added to R^+ extra $2\vartheta S(M) + \sigma_h$

$P_{\min} \geq (T - (\vartheta + 1)\mathcal{S})/\vartheta$, and $P_{\max} \leq T + 3\mathcal{S}$.

$$R^+ \geq R^- + (3\vartheta + 4)S(M) + \sigma_h \qquad (13.1)$$



Theorem 13.6

Theorem 13.6. *Assume that* $7 - 6\vartheta^2 > 0$ *and* (13.1)-(13.10) *hold. Set* $T := \cancel{\vartheta((\vartheta^2 + \vartheta + 1)\mathcal{S} + \vartheta d)}$. *If the beats behave as required by Definition* 13.2*, Algorithm* 17 *running in conjunction with Algorithm* 16 *(where estimates are computed according to Lemma* 10.8*) is a self-stabilizing solution to the pulse synchronization problem. Its skew is in* $O(u + (\vartheta - 1)(d + \mathcal{S}))$ *and the generated pulses satisfy* $P_{\min} \geq (T - (\vartheta + 1)\mathcal{S})/\vartheta$ *and* $P_{\max} \leq T + 3\mathcal{S}$*. The stabilization time (not accounting for the beats) is* $O(MT) = O(M(\mathcal{S} + d))$.

Proof. We apply Lemma 13.5 to each beat but the first, showing that $H = \infty$. Corollary 13.4 then yields the claims. □