ASYNCHRONOUS SELF-TIMED RINGS FOR RANDOMNESS GENERATION

Abdelkarim CHERKAOUI (LaHC)
Viktor FISCHER (LaHC)
Alain AUBERT (LaHC)
Laurent FESQUET (TIMA)

Jean Monnet University ï St-Etienne FRANCE

Introduction

- Performances of True Random Number Generators depend essentially on the quality of the entropy source
- Many TRNG principles rely on extracting jitter from ring oscillators
- Classic inverter based ring oscillators are easy to implement, but suffer from a low robustness to process and voltage variability

Improving RO robustness => Improving TRNG robustness

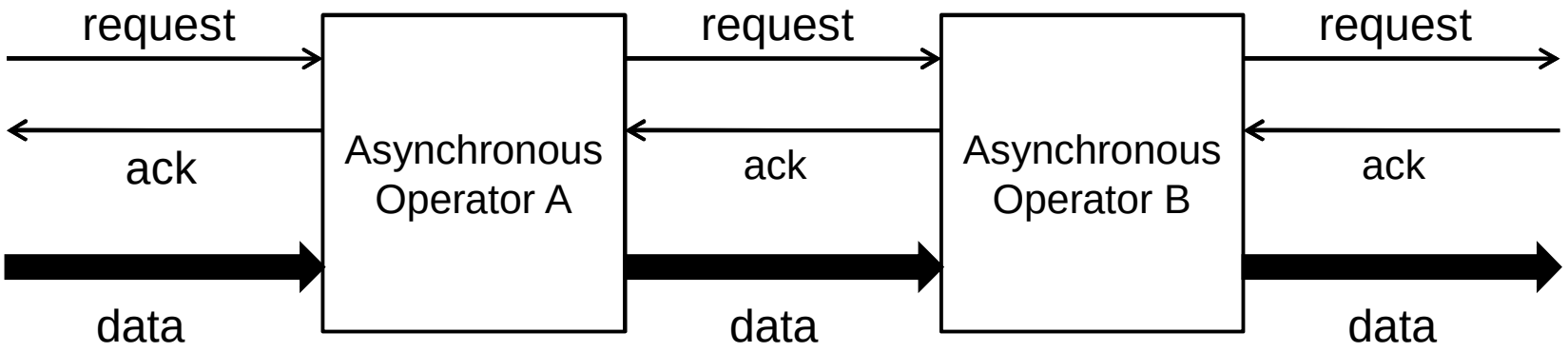
- Asynchronous self-timed rings have been studied on ASIC targets and show some interesting properties

Outline

- **Asynchronous Self-timed Rings**
  - Behavioral model
  - Time Accurate model
- **Our work on Asynchronous Self-timed Rings**
  - ASTR on Altera Cyclone III target
  - Robustness to process and voltage variability
  - Jitter measurements
  - Influence of surrounding logic
- **Analysis**
- **Conclusion**

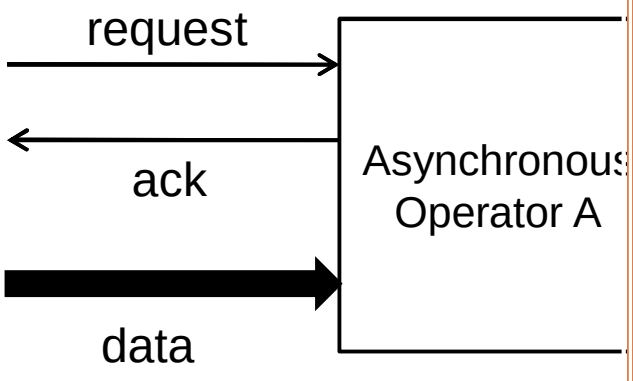
Asynchronous Design

- **Principle** — local synchronization between elements exchanging data
- **Execution** — bi-directionnal communication channels and adapted communication protocol



Asynchronous Design

- **Principle** — local synchronization between elements exchanging data
- **Execution** — bi-directionnal communication channels and adapted communication protocol

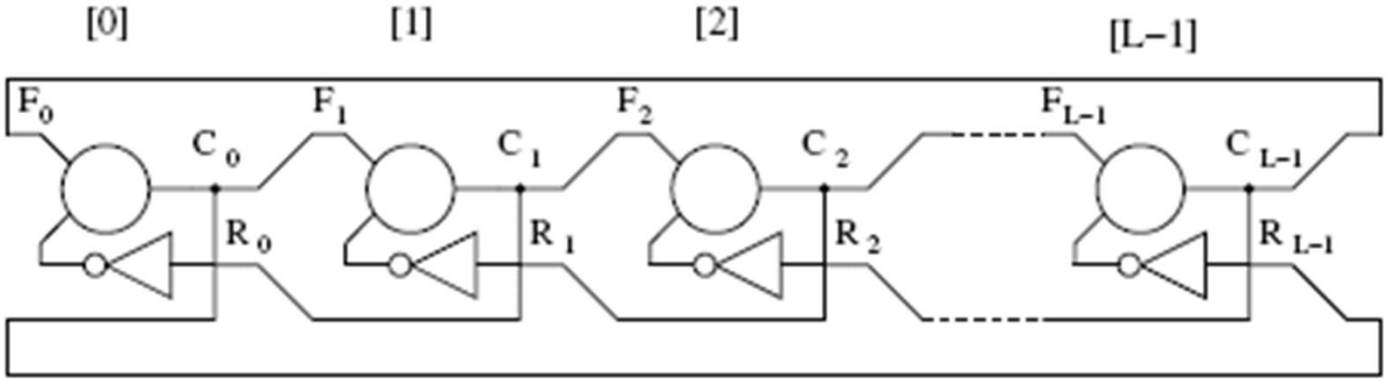


Why Consider Asynchronous circuits ?

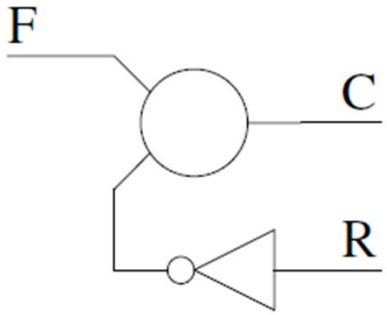
- Low power consumption
- High operating speed
- Less emissions of electro-magnetic noise
- Robustness toward PVT variations
- Improved modularity
- No clock distribution and clock skew problems

Asynchronous Self-timed Rings (ASTR)

- Ring structure : closed loop of an asynchronous micropipeline



- Basic stage cell : Muller gate + inverter



(a) Stage structure

F	R	C
0	0	C^{-1}
0	1	0
1	0	1
1	1	C^{-1}

(b) Stage truth table

ASTR History

[1] J. C. Ebergen, S. Fairbanks, and I. E. Sutherland, **"Predicting performance of micropipelines using charlie diagrams"**, in *Proceedings of the Fourth International Symposium on Advanced Research in Asynchronous Circuits and Systems, ASYNC'98, San Diego, CA, USA, Mar./Apr. 1998, pp. 238–246.*

[2] A. Winstanley and M. R. Greenstreet, **"Temporal properties of self-timed rings"**, in *Proceedings of the 11th Advanced Research Working Conference on Correct Hardware Design and Verification Methods, CHARM'01. London, UK: Springer-Verlag, 2001, pp. 140–154.*

[3] S. Fairbanks and S. Moore, **"Analog micropipeline rings for high precision timing**", in *Proceedings on the 10th International Symposium on Asynchronous Circuits and Systems, ASYNC'04, Apr. 2004, pp. 41–50.*

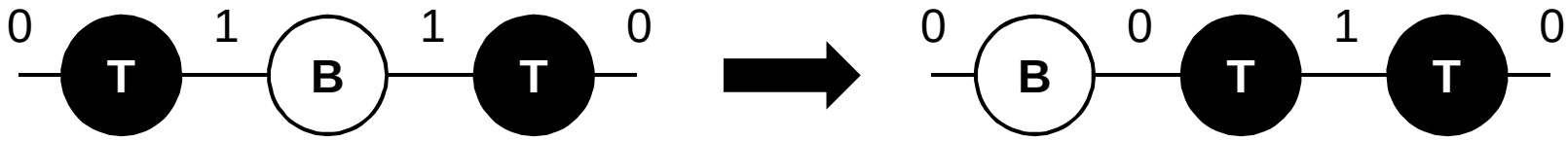
[4] J. Hamon, L. Fesquet, B. Miscopein, and M. Renaudin, **«High-level time-accurate model for the design of self-timed ring oscillators»,** in *Proceedings on the 14th International Symposium on Asynchronous Circuits and Systems, ASYNC'08,* Newcastle, United Kingdom, April 2008.

Behavioral Model : a Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Propagation Rule
  - A token propagates from left to right to the next stage if it contains a bubble
  - A bubble propagates from right to left to the previous stage if it contains a token



- Asynchronous handshake protocol

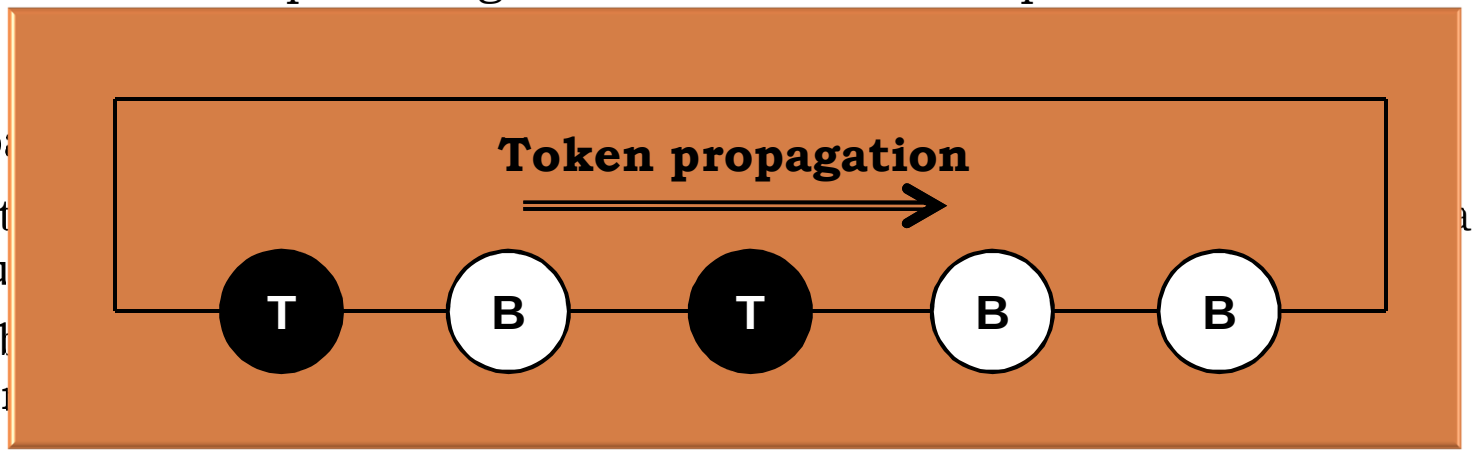
Behavioral Model : a Bubbles and Tokens Story

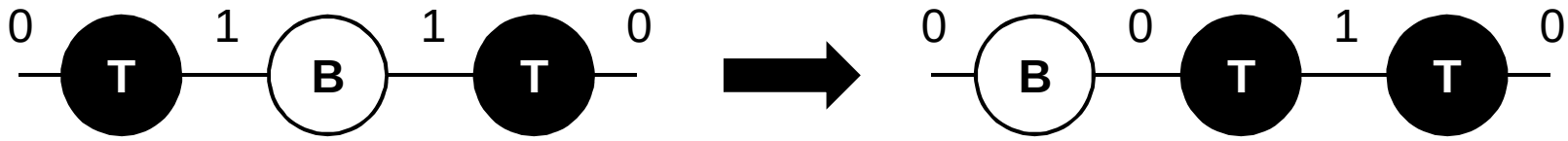
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

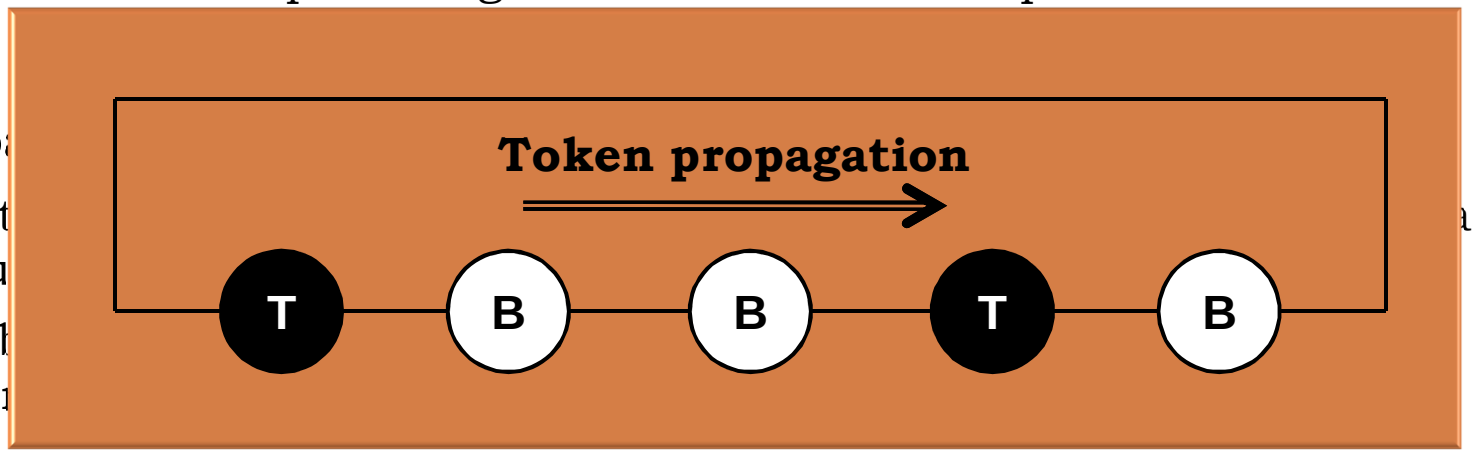
Behavioral Model : a Bubbles and Tokens Story

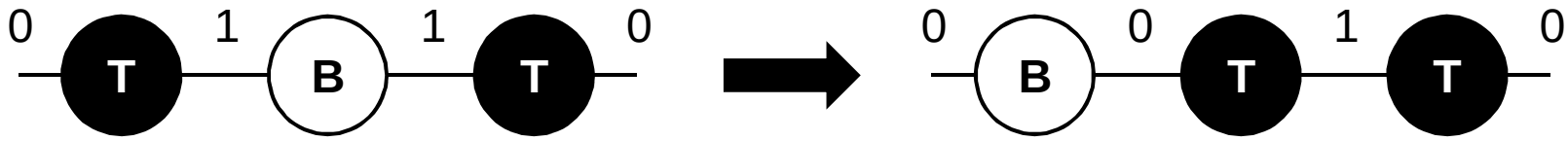
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

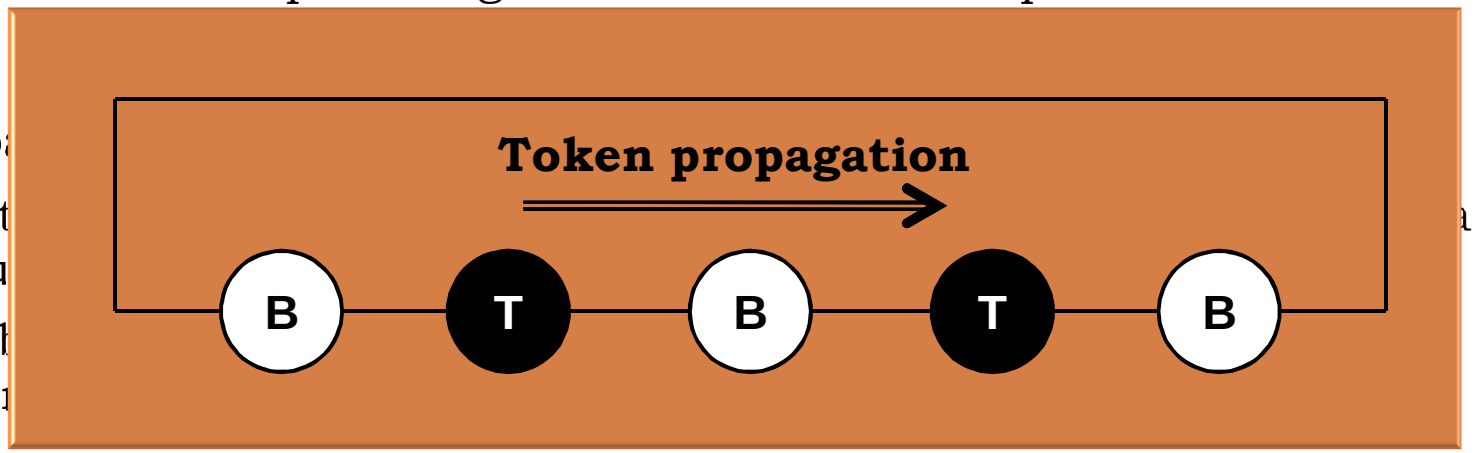
Behavioral Model : a Bubbles and Tokens Story

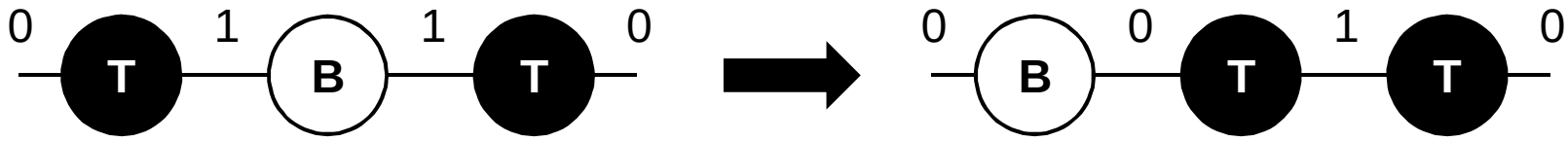
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

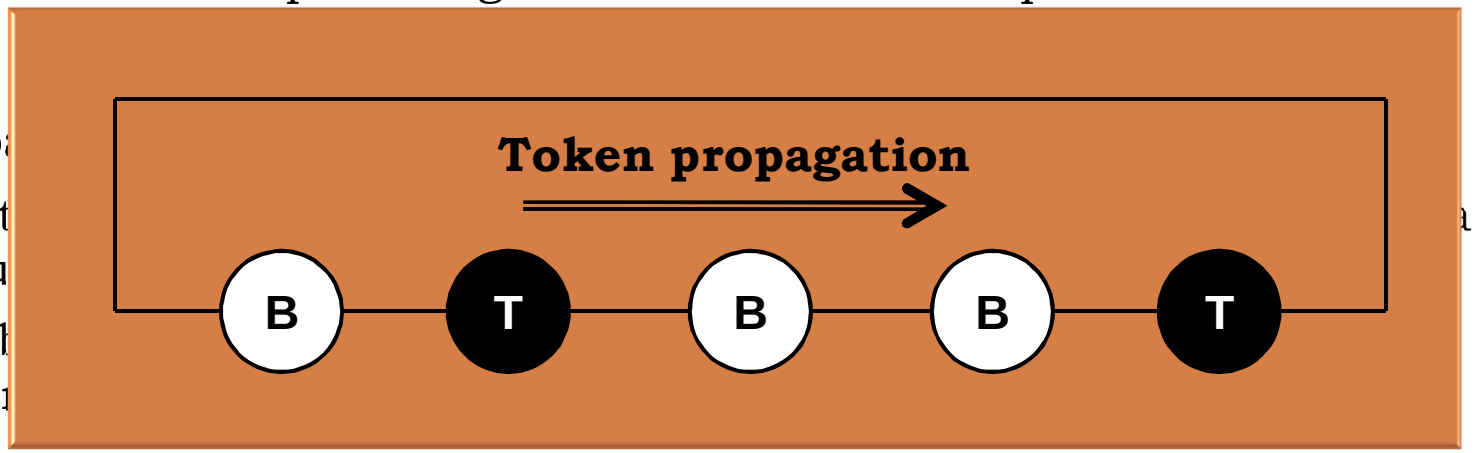
Behavioral Model : a Bubbles and Tokens Story

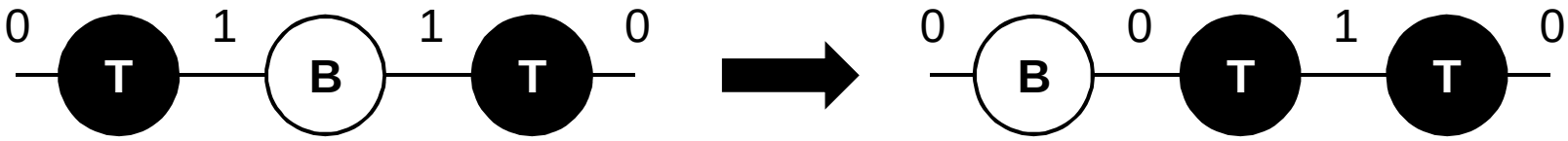
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Propa
  - A t
    bu
  - A h
    co





- Asynchronous handshake protocol

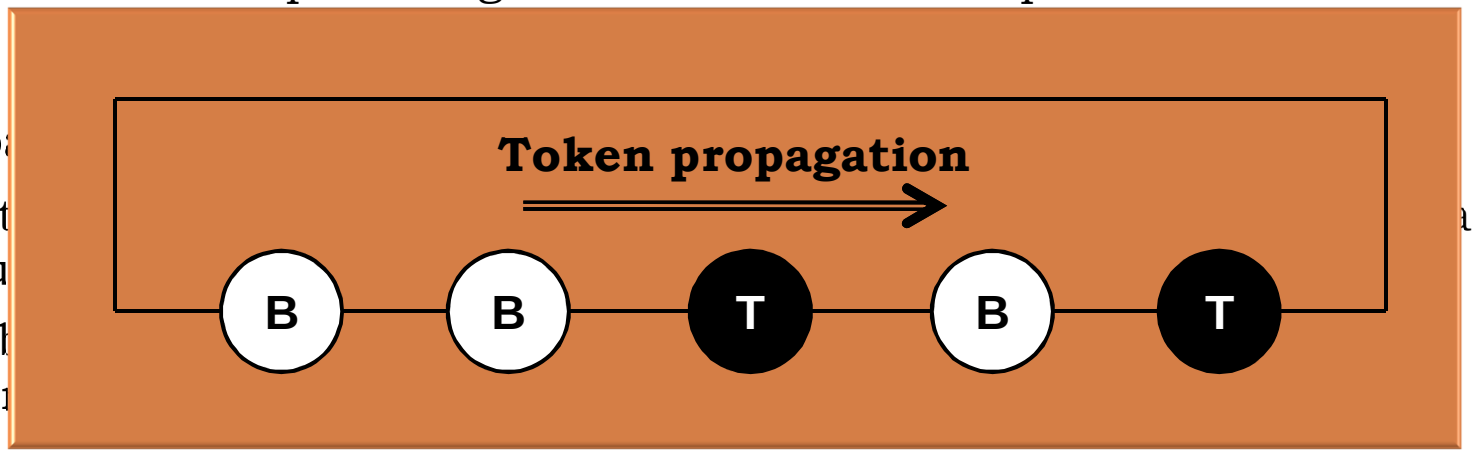
Behavioral Model : a Bubbles and Tokens Story

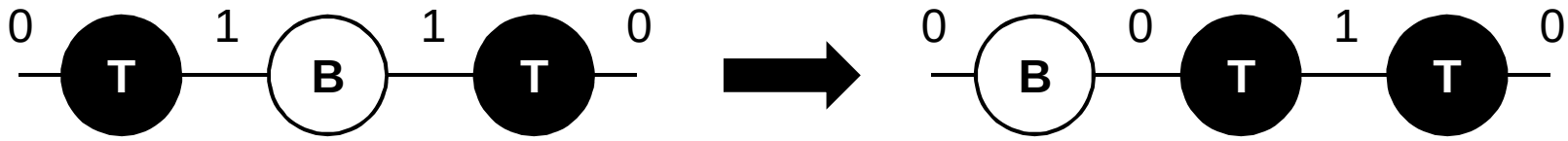
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

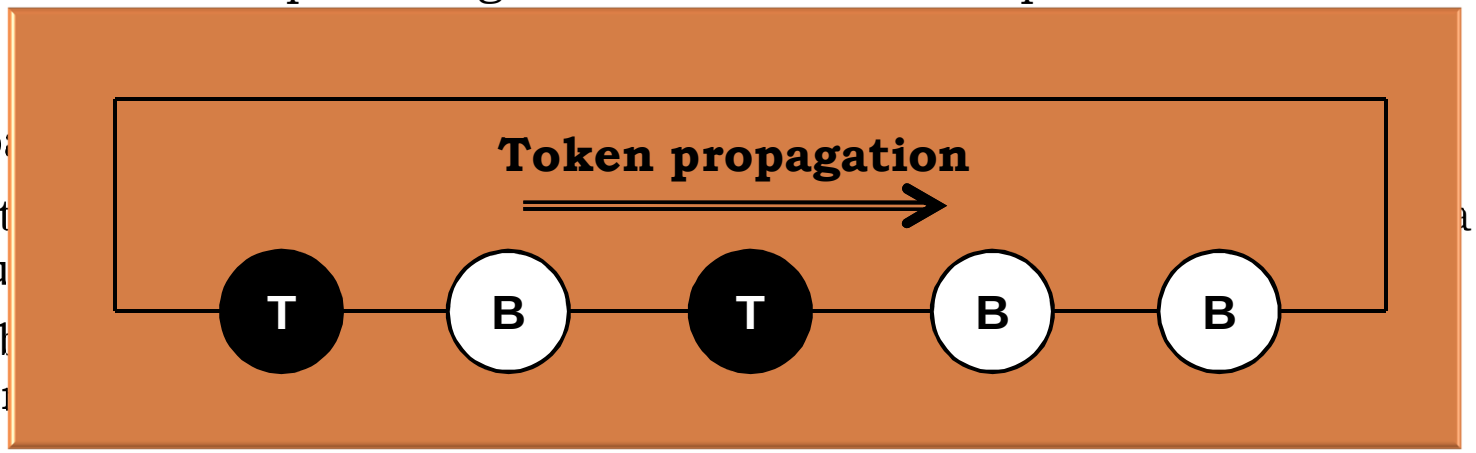
Behavioral Model : a Bubbles and Tokens Story

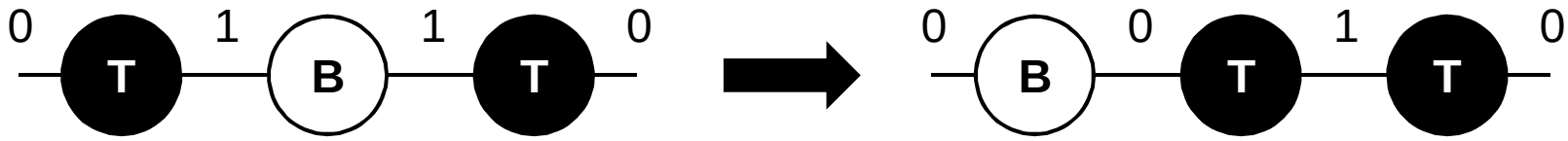
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

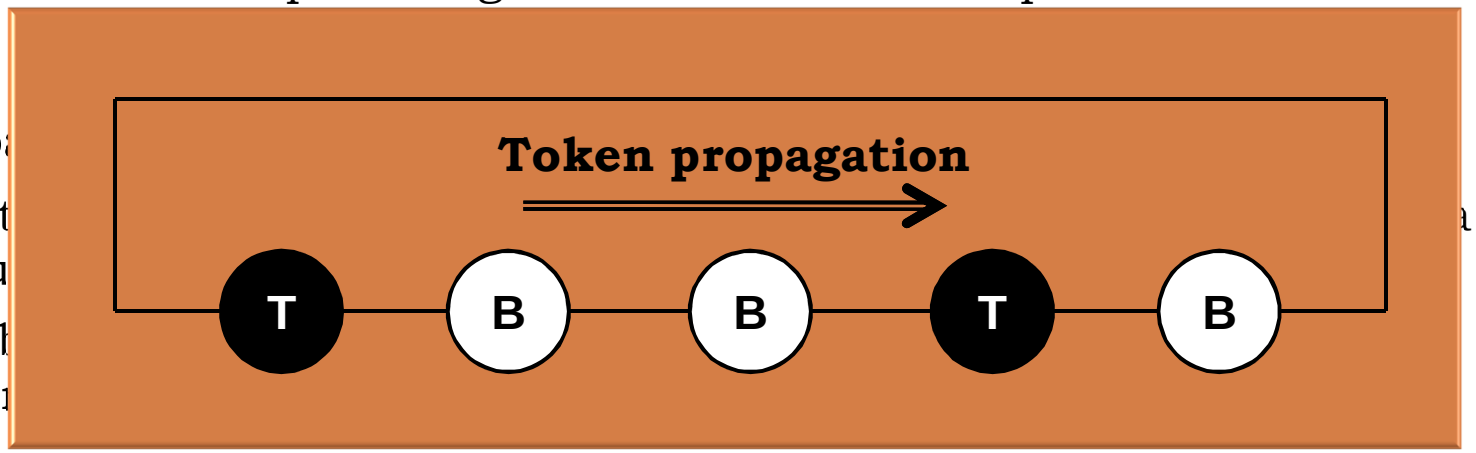
Behavioral Model : a Bubbles and Tokens Story

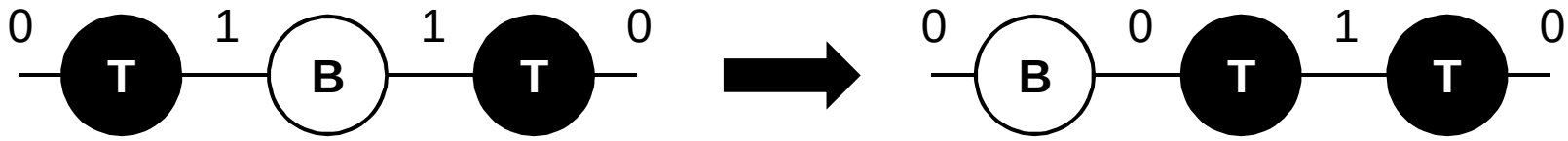
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

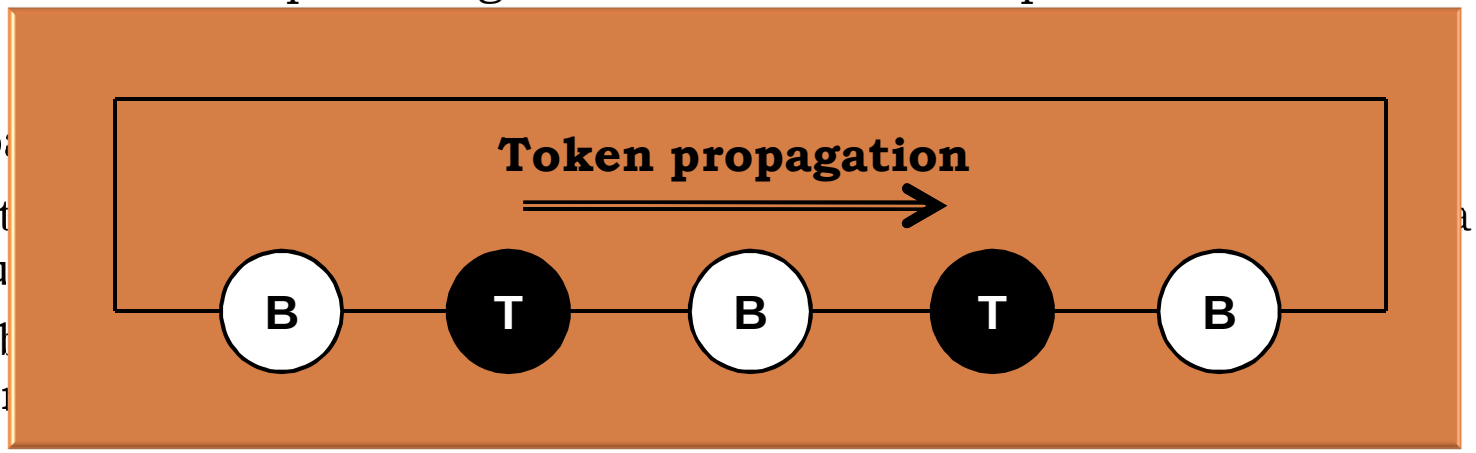
Behavioral Model : a Bubbles and Tokens Story

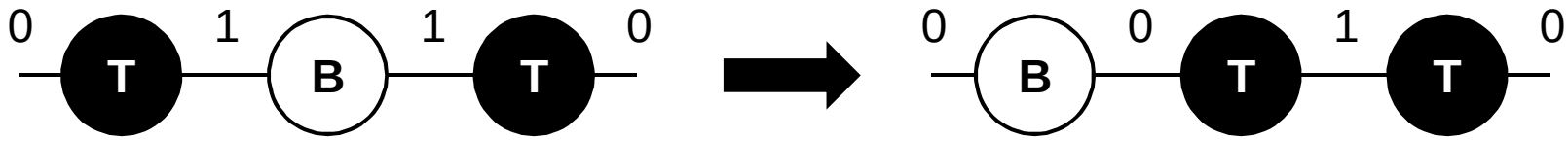
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

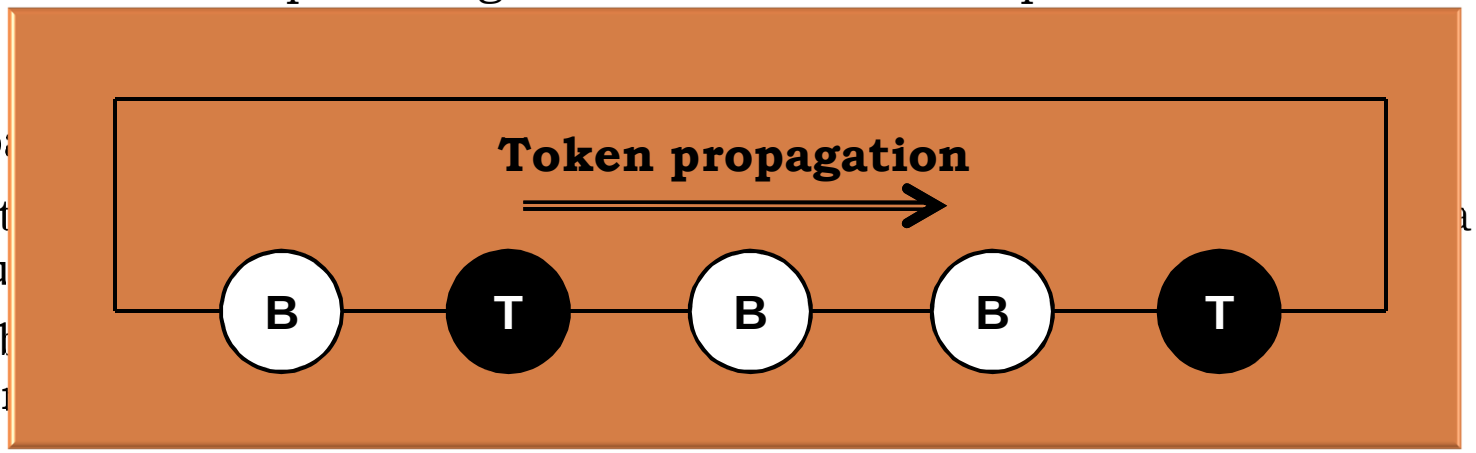
Behavioral Model : a Bubbles and Tokens Story

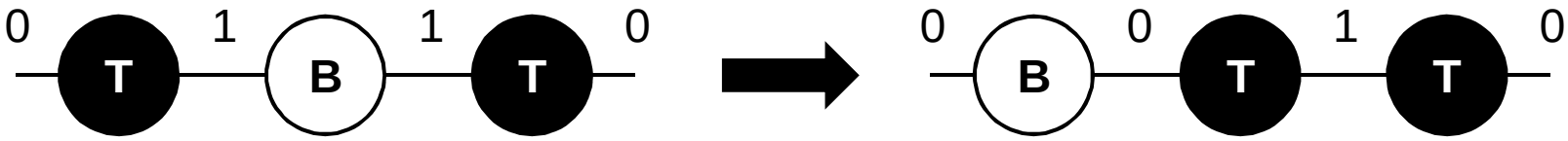
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Propa
  - A t
    bu
  - A h
    co





- Asynchronous handshake protocol

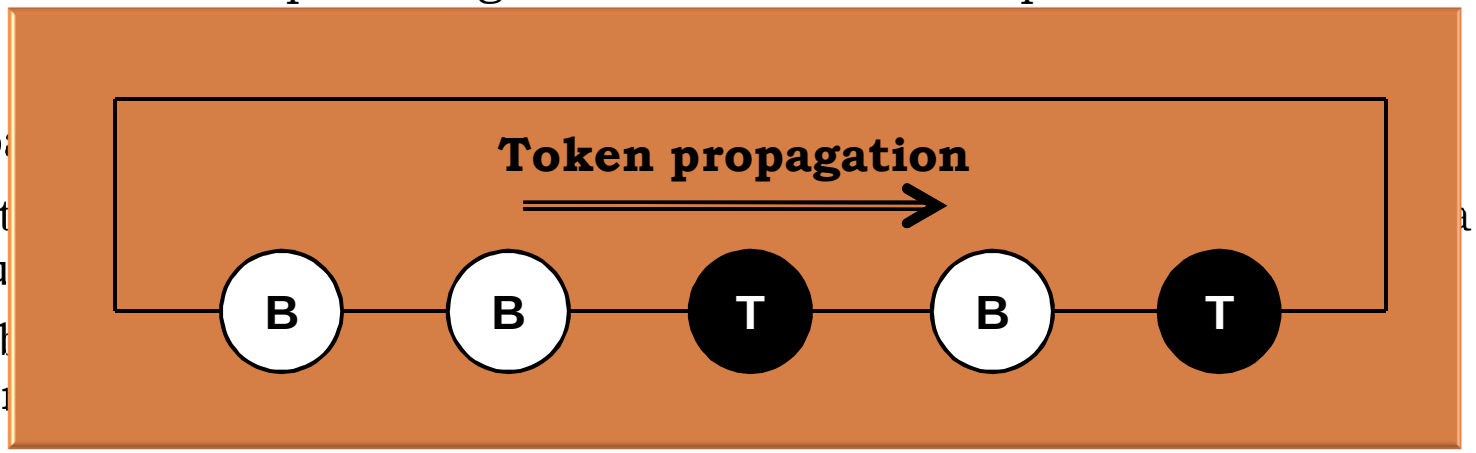
Behavioral Model : a Bubbles and Tokens Story

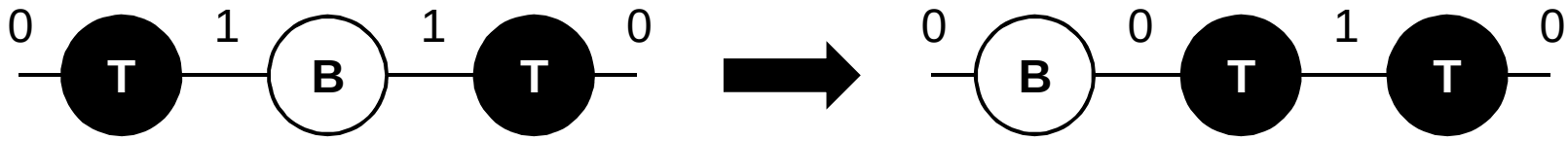
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





- Asynchronous handshake protocol

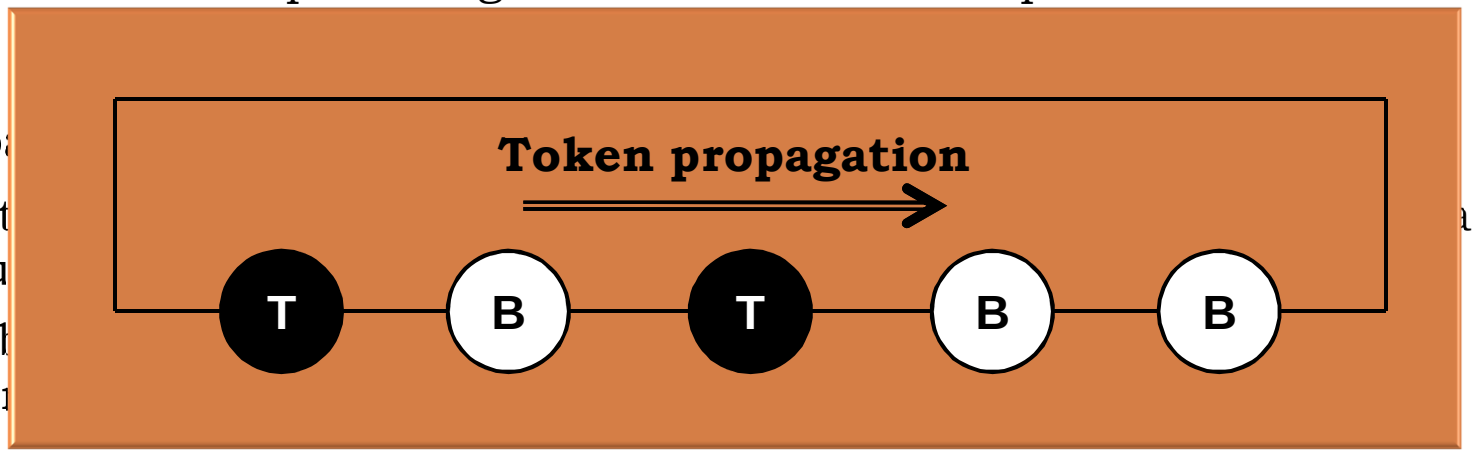
Behavioral Model : a Bubbles and Tokens Story

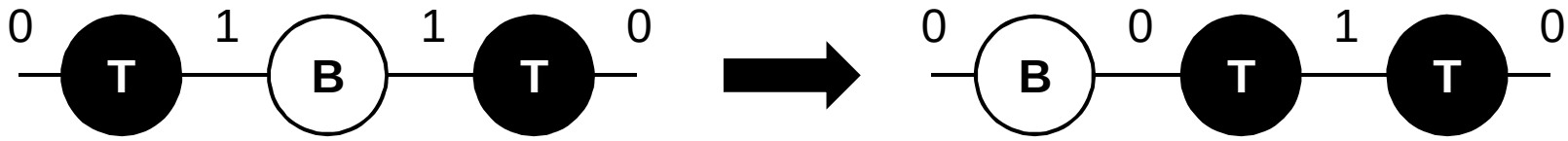
- Data representation

  Bubble Output's stage is equal to its input

  Token Output's stage is different from its input

- Prop
  - A t
    bu
  - A
    co





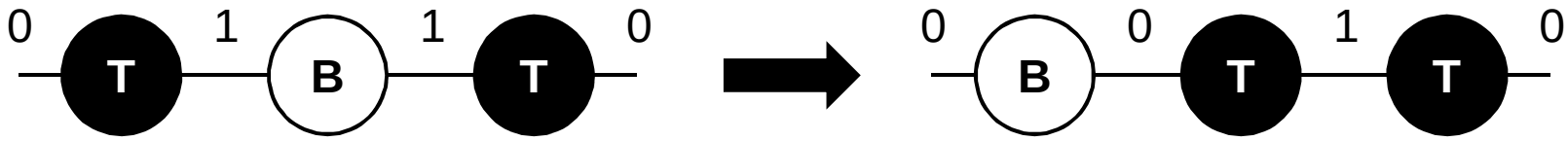
- Asynchronous handshake protocol

Behavioral Model : a Bubbles and Tokens Story

- Data representation

Bubble	Output's stage is equal to its input
Token	Output's stage is different from its input

- Propagation Rule
  - A token propagates from left to right to the next stage if it contains a bubble
  - A bubble propagates from right to left to the previous stage if it contains a token



- Asynchronous handshake protocol

Steady Regime

- Steady Regime shows 2 oscillation modes

Evenly-spaced	Tokens evenly spread all around the ring and propagate with a constant spacing
Burst	Tokens get together to form a cluster that propagates around the ring

- Example : 32-stage ring

- Is it possible to predict the oscillation mode ? How ?

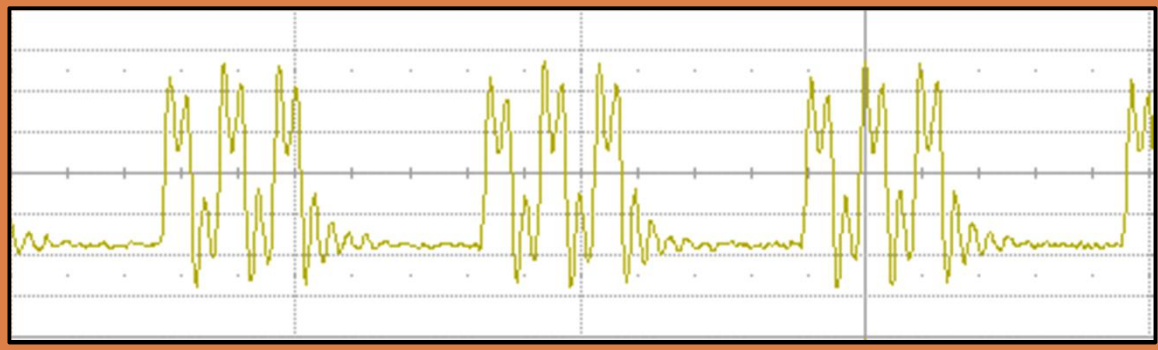
Steady Regime

- Steady Reg
  Evenly-spa

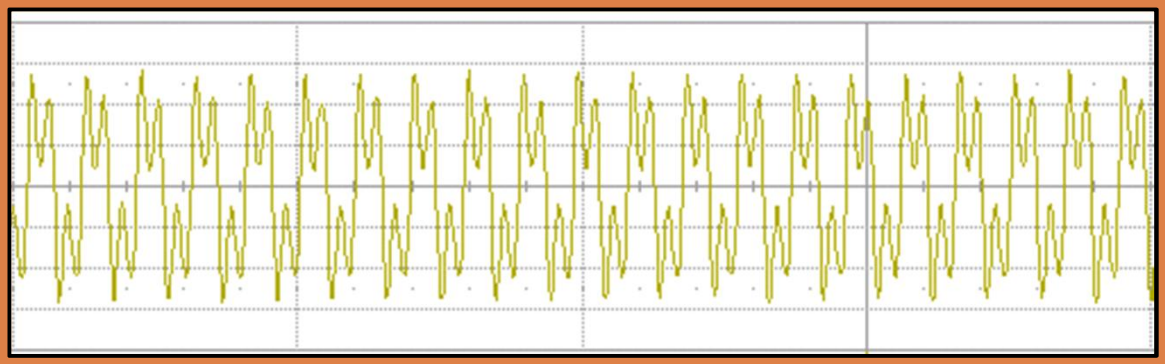
  Burst

- Example :

- Is it possib



(a) 6 tokens in burst Mode



(b) 14 tokens in evenly-spaced Mode

Steady Regime

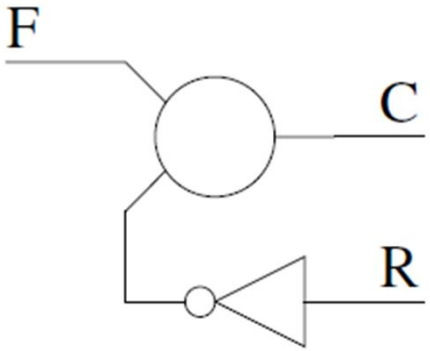
- Steady Regime shows 2 oscillation modes

Evenly-spaced	Tokens evenly spread all around the ring and propagate with a constant spacing
Burst	Tokens get together to form a cluster that propagates around the ring

- Example : 32-stage ring

- Is it possible to predict the oscillation mode ? How ?

Time Accurate Model (1)



(a) Stage structure

F	R	C
0	0	C^{-1}
0	1	0
1	0	1
1	1	C^{-1}

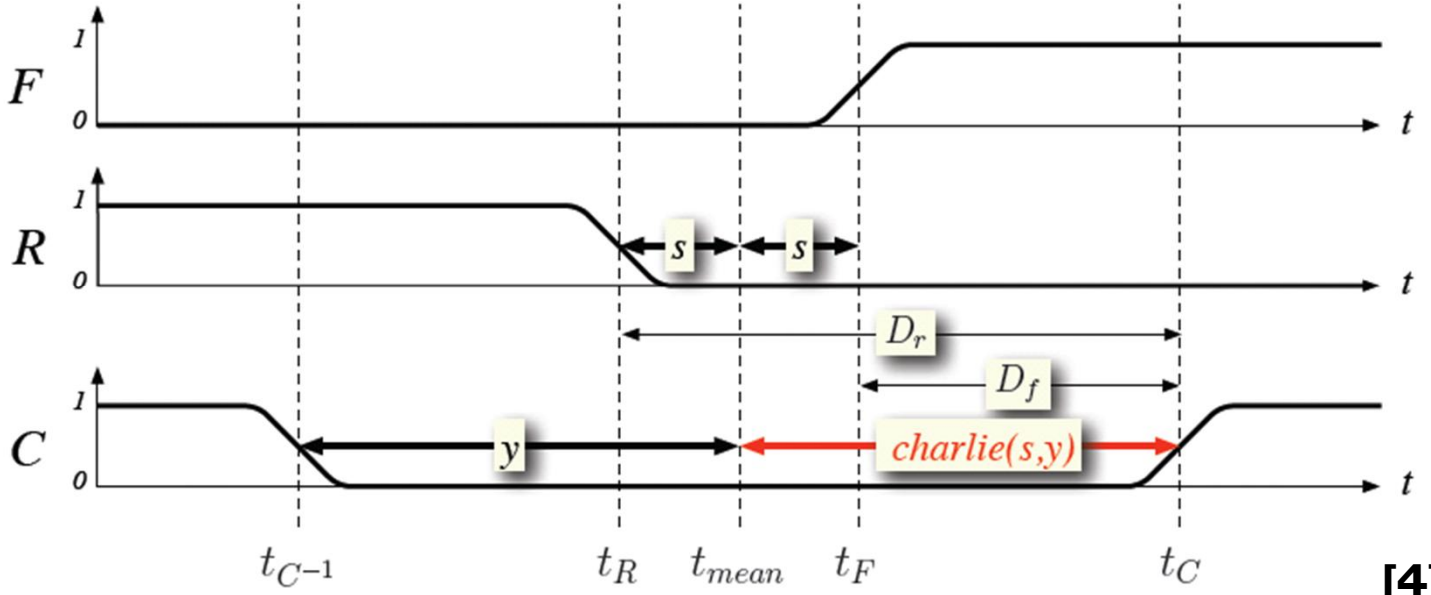
(b) Stage truth table

- Stage delay is influenced by two analog phenomena [2]

Charlie Effect	The closer are the input's events, the longer is the stage propagation delay
Drafting Effect	The shorter is the elapsed time between two successive outputs commutation the shorter will be the stage propagation delay

Time Accurate Model (2)

- Ring stage chronogram



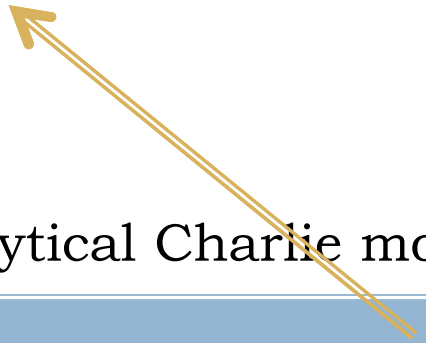
[4]

- Analytical Charlie model

$$charlie(s,y) = D_{mean} + \sqrt{D_{charlie}{}^2 + (s - s_{\min})^2} - B^{-\frac{y}{A}}$$

Time Accurate Model (2)

Static delays
- Mean forward
and reverse delay



- Analytical Charlie model

$$charlie(s,y) = D_{mean} + \sqrt{D_{charlie}{}^2 + (s - s_{\min})^2} - B^{-\frac{y}{A}}$$

Time Accurate Model (2)

Charlie effect
- Charlie magnitude
- Half separation time

Static delays
- Mean forward and reverse delay

- Analytical Charlie model

$$charlie(s,y) = D_{mean} + \sqrt{D_{charlie}{}^2 + (s - s_{\min})^2} - B^{-\frac{y}{A}}$$

Time Accurate Model (2)

Charlie effect
- Charlie magnitude
- Half separation time

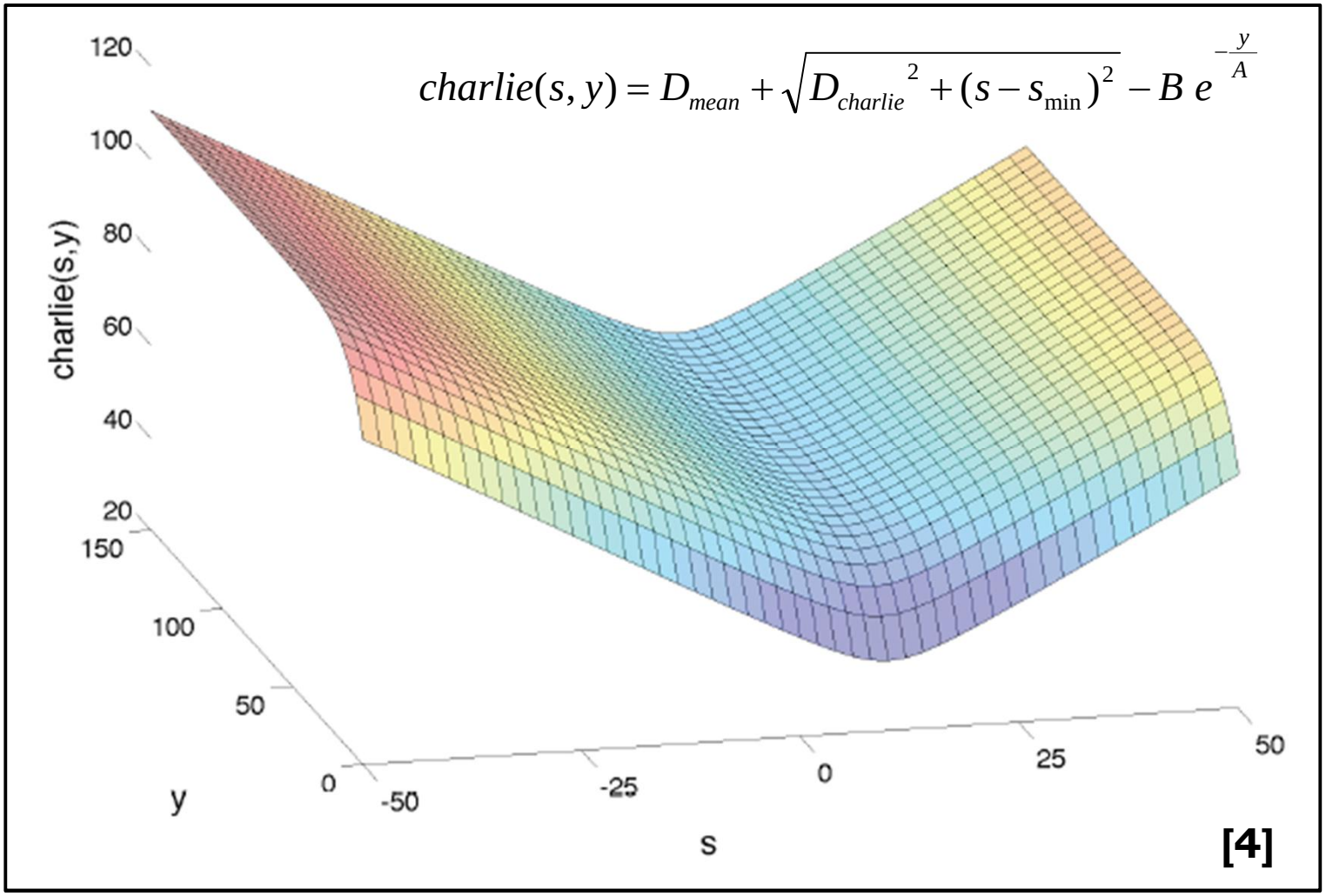
Drafting effect
- Drafting magnitude
- Drafting duration
- Elapsed time from last commutation

Static delays
- Mean forward and reverse delay

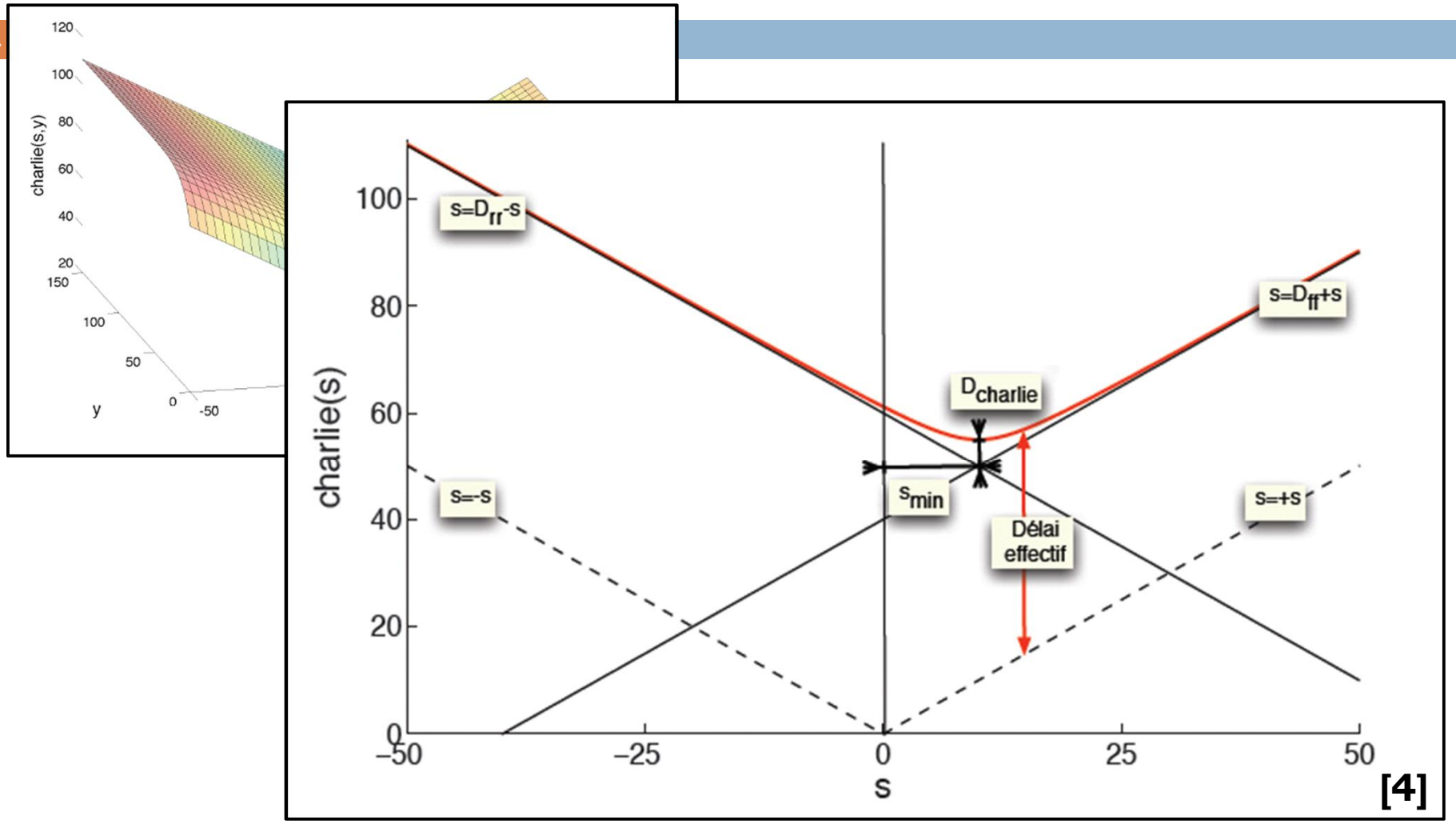
- Analytical Charlie model

$$charlie(s,y) = D_{mean} + \sqrt{D_{charlie}{}^2 + (s - s_{\min})^2} - B^{-\frac{y}{A}}$$

The Charlie 3D Diagram

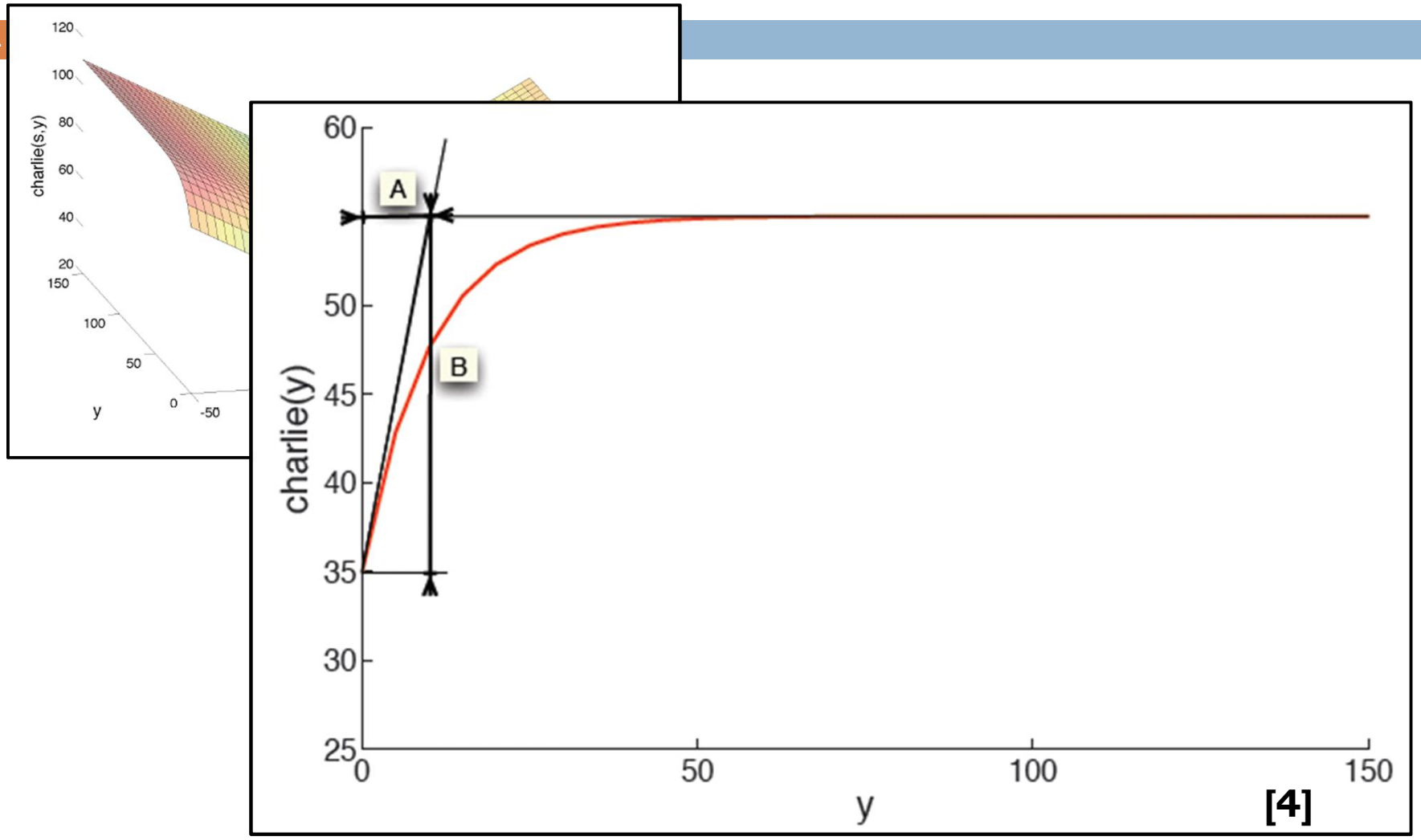


The Charlie 3D Diagram



(a) charlie(s) for constant *y*

The Charlie 3D Diagram

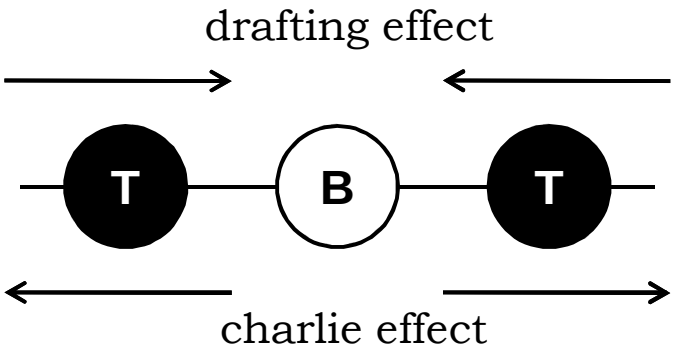


(b) charlie(y) for constant *s*

Time Accurate Model : Analysis

- Considering the token/bubble abstraction

Charlie Effect	two tokens evolving closely will push away from each other
Drafting Effect	a token crossing a stage will accelerate next token crossing the stage



- Considering propagation modes

Charlie Effect	favorises evenly-spaced oscillating mode
Drafting Effect	favorises burst oscillating mode

Avoiding the Burst

- Oscillation mode and frequency depend mainly on
  - Number of tokens and bubbles in the ring
  - Charlie and drafting parameters
  - Classic timing parameters (static forward and reverse delays)

- Evenly-spaced volume and Burst volume are evaluated in a 4 dimensionnal space formed by the stage parameters

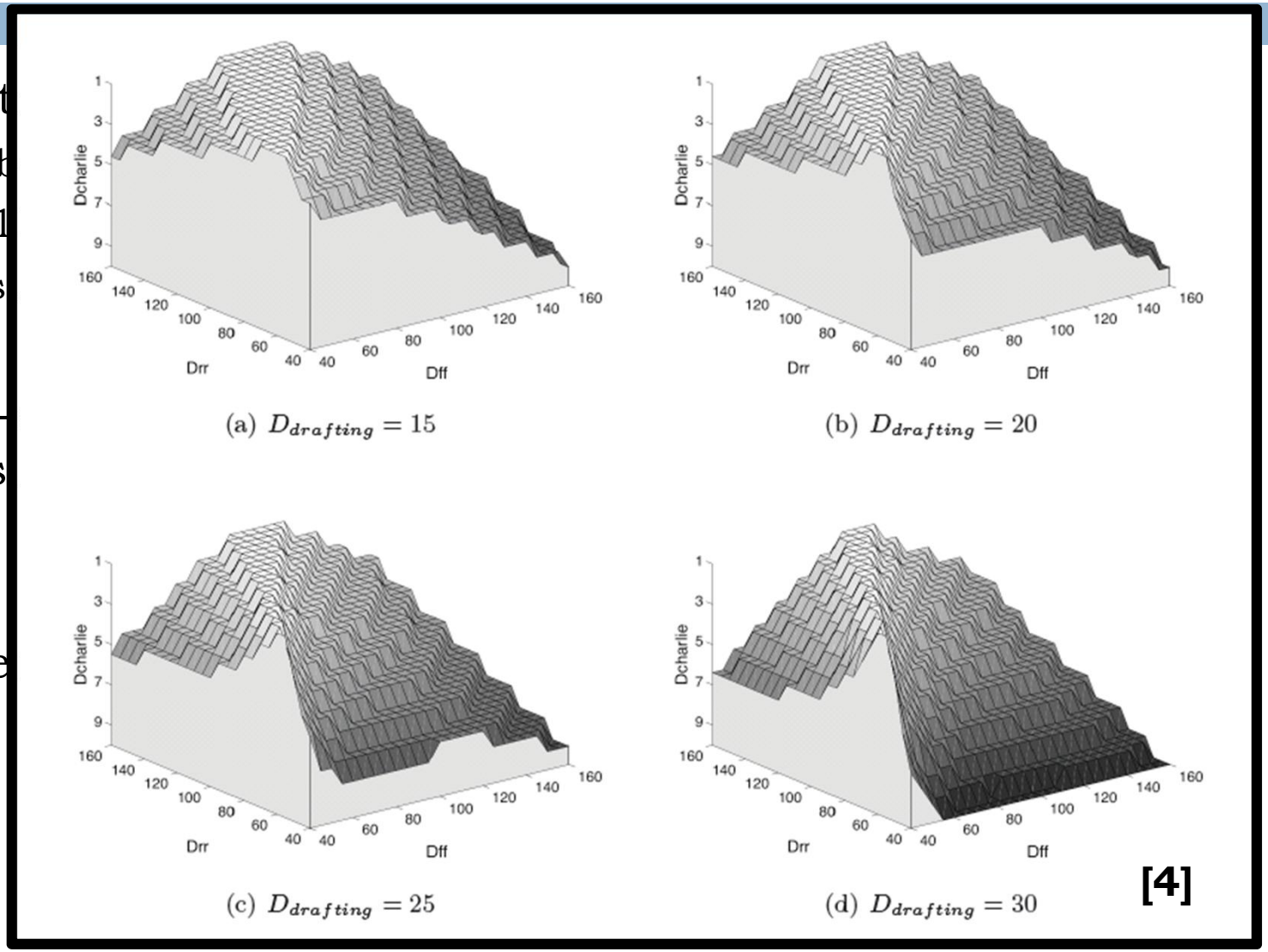
- Sufficient condition to guarantee the evenly-spaced mode

$$\frac{D_{ff}}{D_{rr}} = \frac{N_T}{N_B}$$

[4]

Avoiding the Burst

- Oscillat
  - Numb
  - Charl
  - Class
- Evenly-
  dimens
- Sufficie



[4]

Avoiding the Burst

- Oscillation mode and frequency depend mainly on
  - Number of tokens and bubbles in the ring
  - Charlie and drafting parameters
  - Classic timing parameters (static forward and reverse delays)

- Evenly-spaced volume and Burst volume are evaluated in a 4 dimensionnal space formed by the stage parameters

- Sufficient condition to guarantee the evenly-spaced mode

$$\frac{D_{ff}}{D_{rr}} = \frac{N_T}{N_B}$$

[4]

Functionnal Comparison : IRO/ASTR

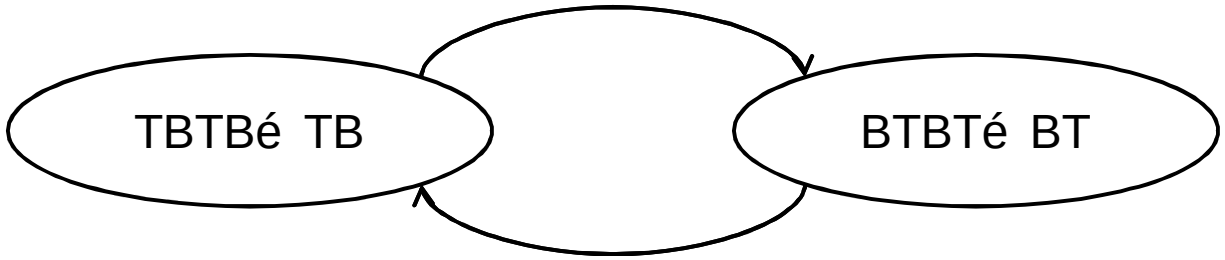
	IRO	ASTR
Stage structure	Inverter	Muller gate + Inverter
Behavior	One event propagating throughout the ring	Several events propagating simultaneously
Oscillation modes	Evenly-spaced	Evenly-spaced + Burst
Frequency	Depends on number of stages and stage delays	More complex dependency
Analog Effects	Drafting effect	Drafting effect + Charlie effect

ASTR on Altera Cyclone III target (1)

- An important evenly-spaced volume
  - ⇒ high Charlie effect
- Short commutation time compared to propagation delay
  - ⇒ low Drafting effect
- Ring stage implemented inside one LUT
  - ⇒ $D_{rr} = D_{ff}$
- A simple design rule to insure the evenly-spaced mode
  - ⇒ $N_T = N_B$

ASTR on Altera Cyclone III target (2)

- In the steady evenly-spaced regime the ring oscillates between two states

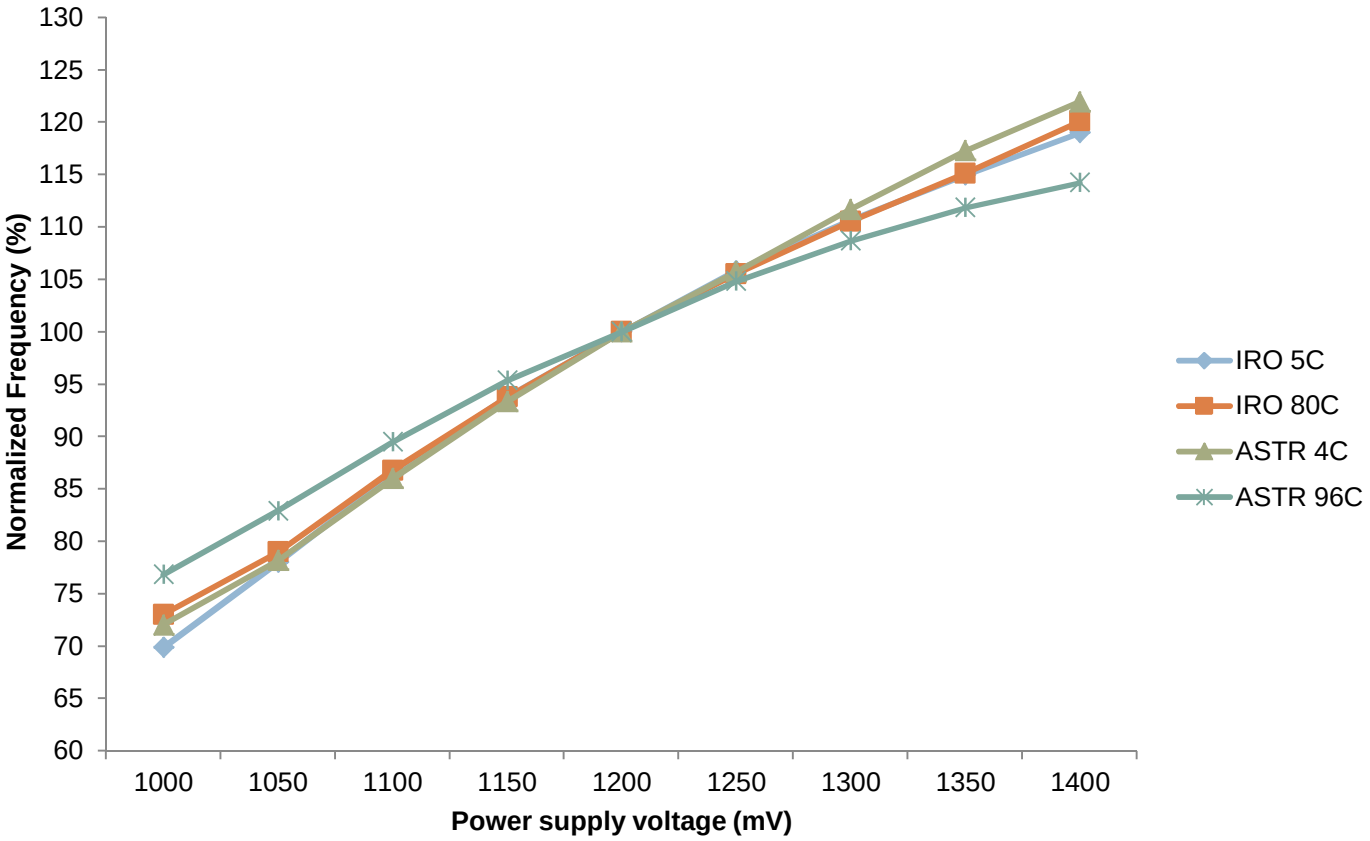


- Events happen with null separation times

$$T_{osc} = 4 * (D_{LUT} + D_{charlie})$$

Robustness to Voltage Variations (1)

- Normalized frequency Vs power supply voltage



$$F_n = \frac{F}{F_{nom}}$$

Robustness to Voltage Variations (2)

- Normalized frequency range Vs power supply voltage

$$\Delta F = \frac{F_{\max} - F_{\min}}{F_{nom}}$$

	Nominal frequency (Mhz)	Normalized frequency range
IRO 5C	375.82	49.15 %
IRO 25C	73.49	47.72 %
IRO 80C	22.84	47.07 %
ASTR 4C	653.47	49.95 %
ASTR 24C	432.54	44.20 %
ASTR 48C	407.90	**38.72 %**
ASTR 64C	368.58	**38.87 %**
ASTR 96C	320.48	**37.38 %**

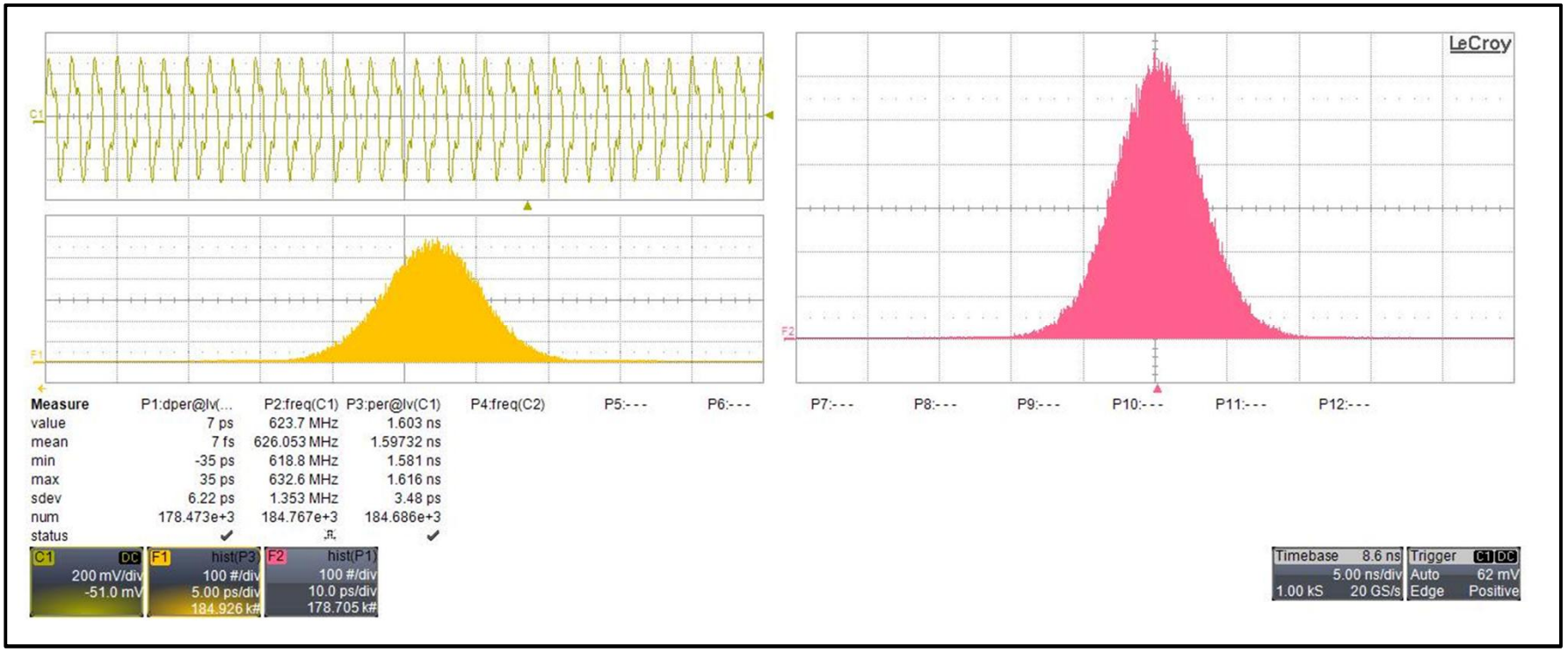
Robustness to Process Variability

- Preliminary tests using 5 Altera Cyclone III boards : frequency dispersion

	Board 1	Board 2	Board 3	Board 4	Board 5	Relative standard deviation
IRO 3C	654.42	646.84	641.56	645.60	642.12	**0.79 %**
IRO 5C	305.72	306.44	302.54	304.87	302.20	**0.62 %**
ASTR 4C	669.05	660.06	658.60	659.90	655.62	**0.76 %**
ASTR 96C	328.16	328.54	327.55	328.47	327.46	**0.15 %**

Jitter Shapes

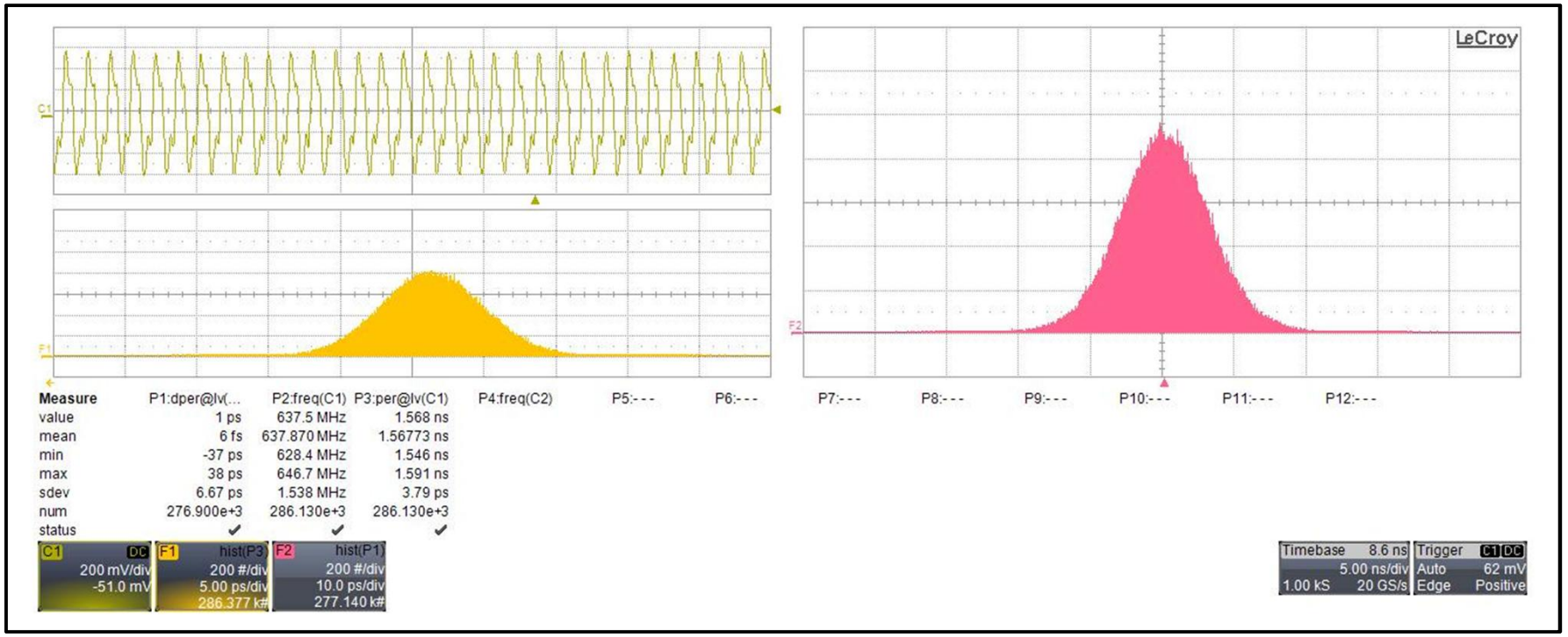
- Without deterministic noise and surrounding logic, both oscillators exhibit gaussian jitter



IRO 3C

Jitter Shapes

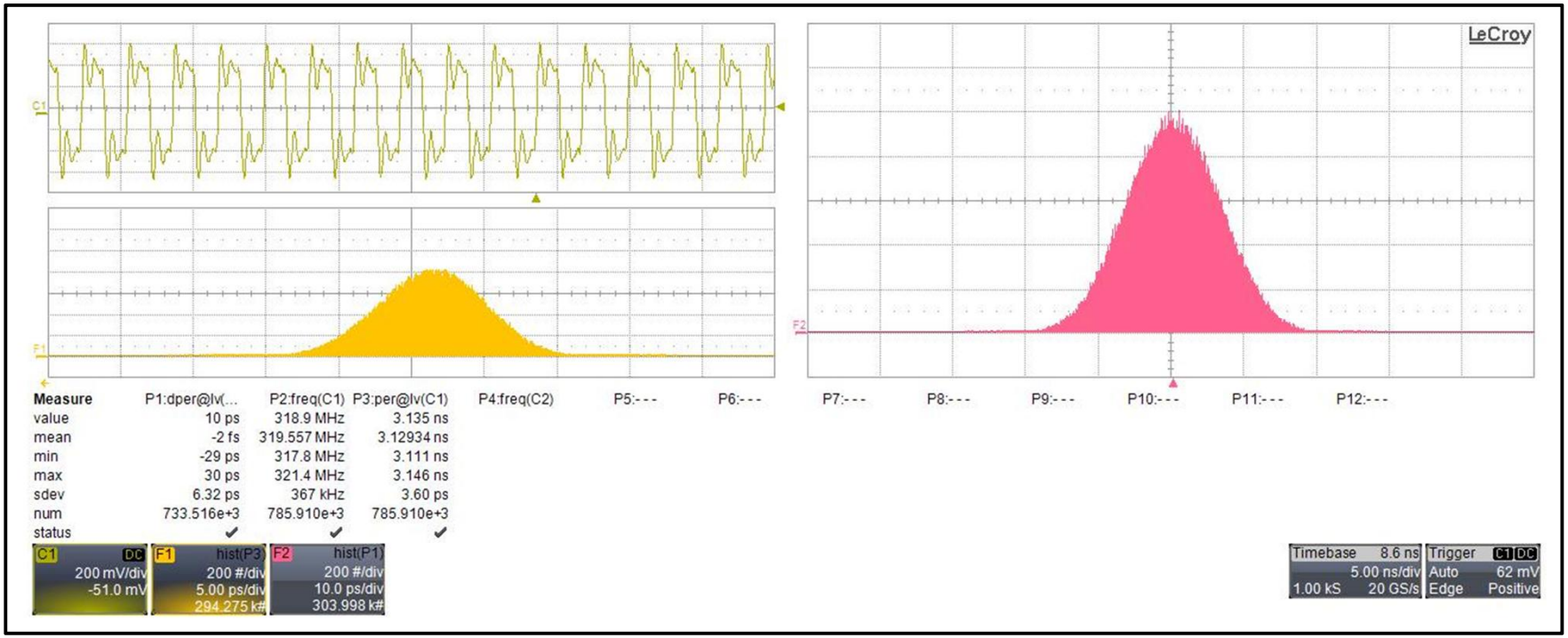
- Without deterministic noise and surrounding logic, both oscillators exhibit gaussian jitter



ASTR 4C

Jitter Shapes

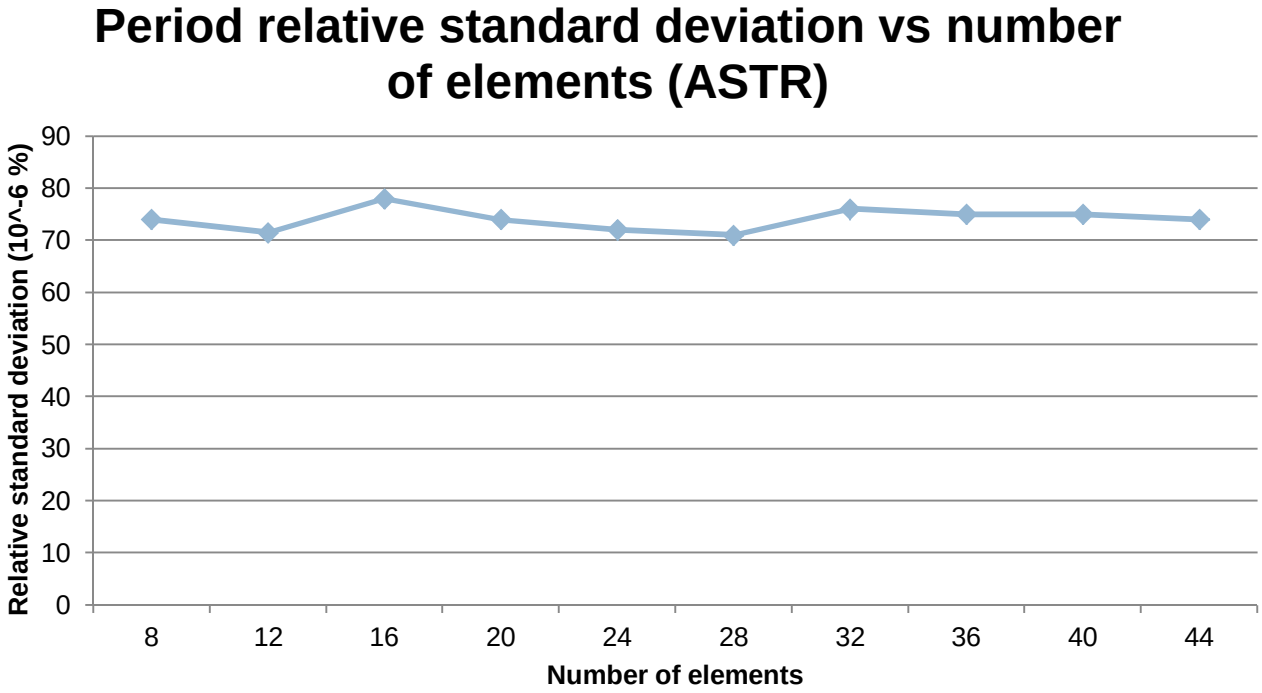
- Without deterministic noise and surrounding logic, both oscillators exhibit gaussian jitter



ASTR 96C

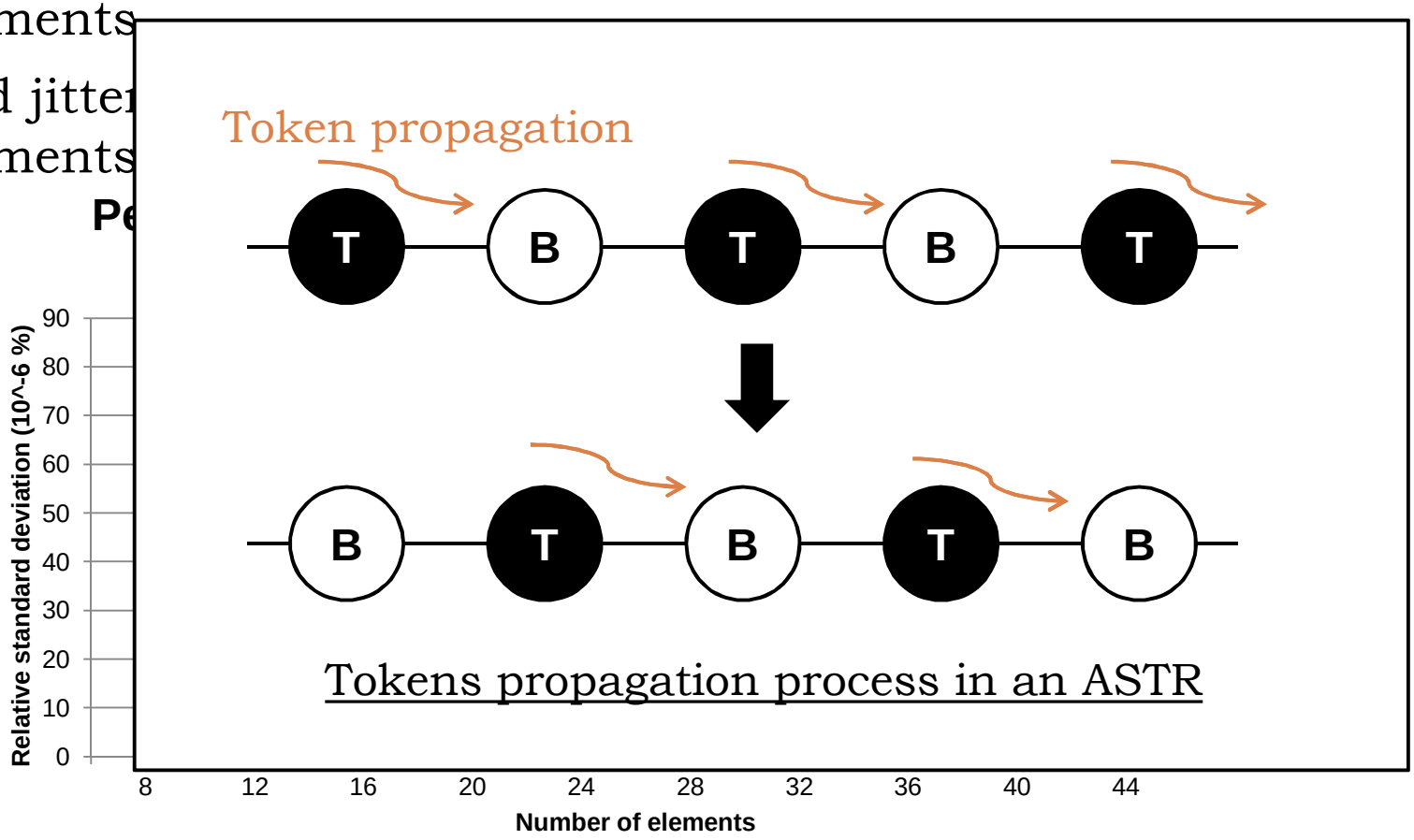
Jitter Measurements

- Jitter accumulation in IRO has been well studied : period standard deviation follows a square root law with the number of elements
- Period jitter seems to be constant with respect to the number of elements for ASTR



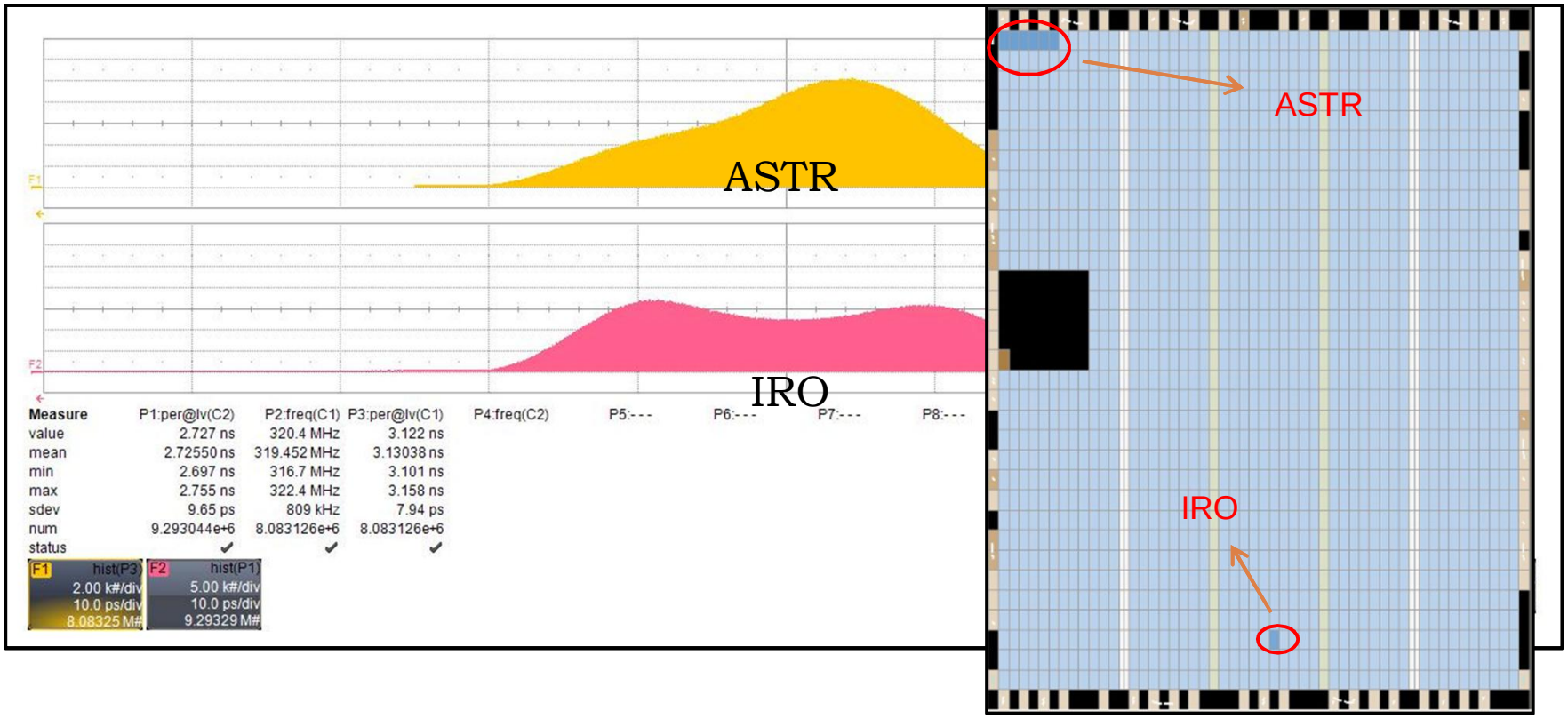
Jitter Measurements

- Jitter accumulation in IRO has been well studied : period standard deviation follows a square root law with the number of elements
- Period jitter



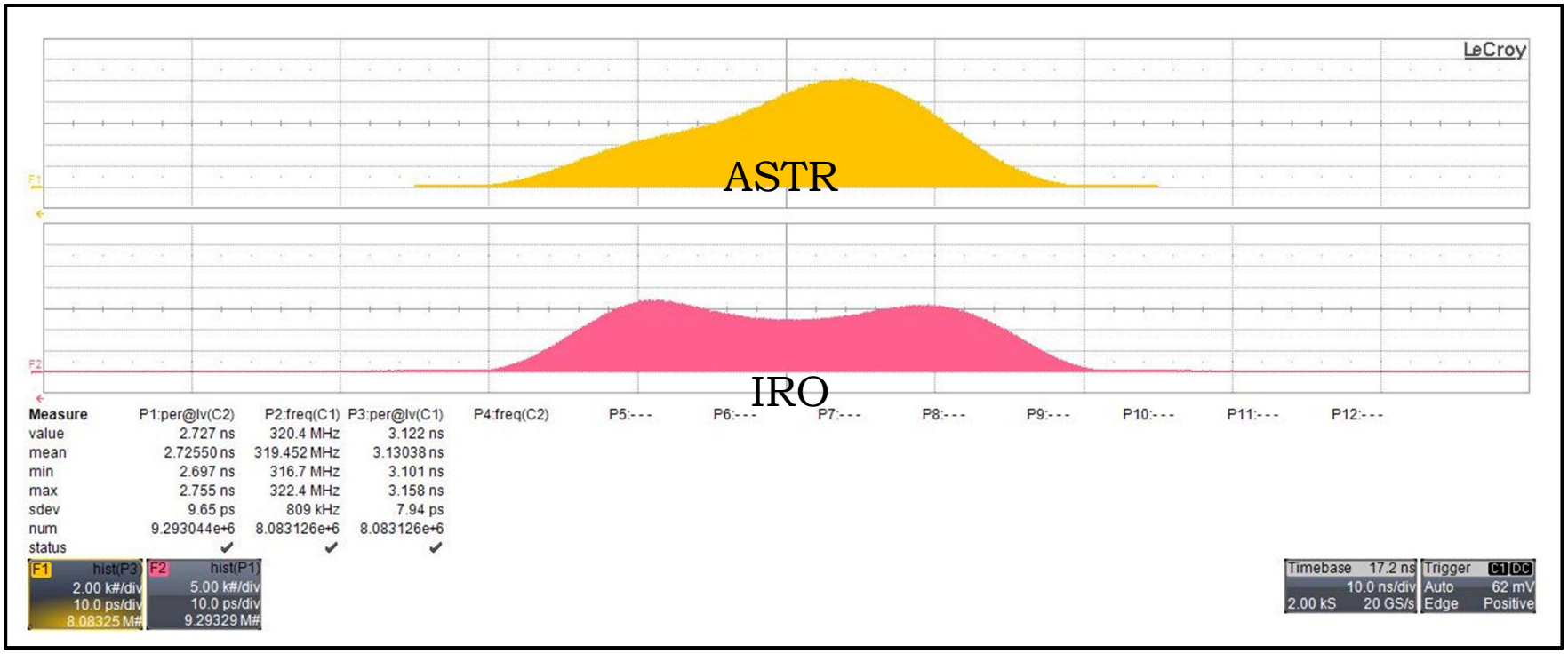
Influence of Surrounding Logic

- A simple experiment : an IRO (5 stages ~ 300 Mhz) and an ASTR (96 stages ~ 320 Mhz) running simultaneously in an Altera Cyclone III board



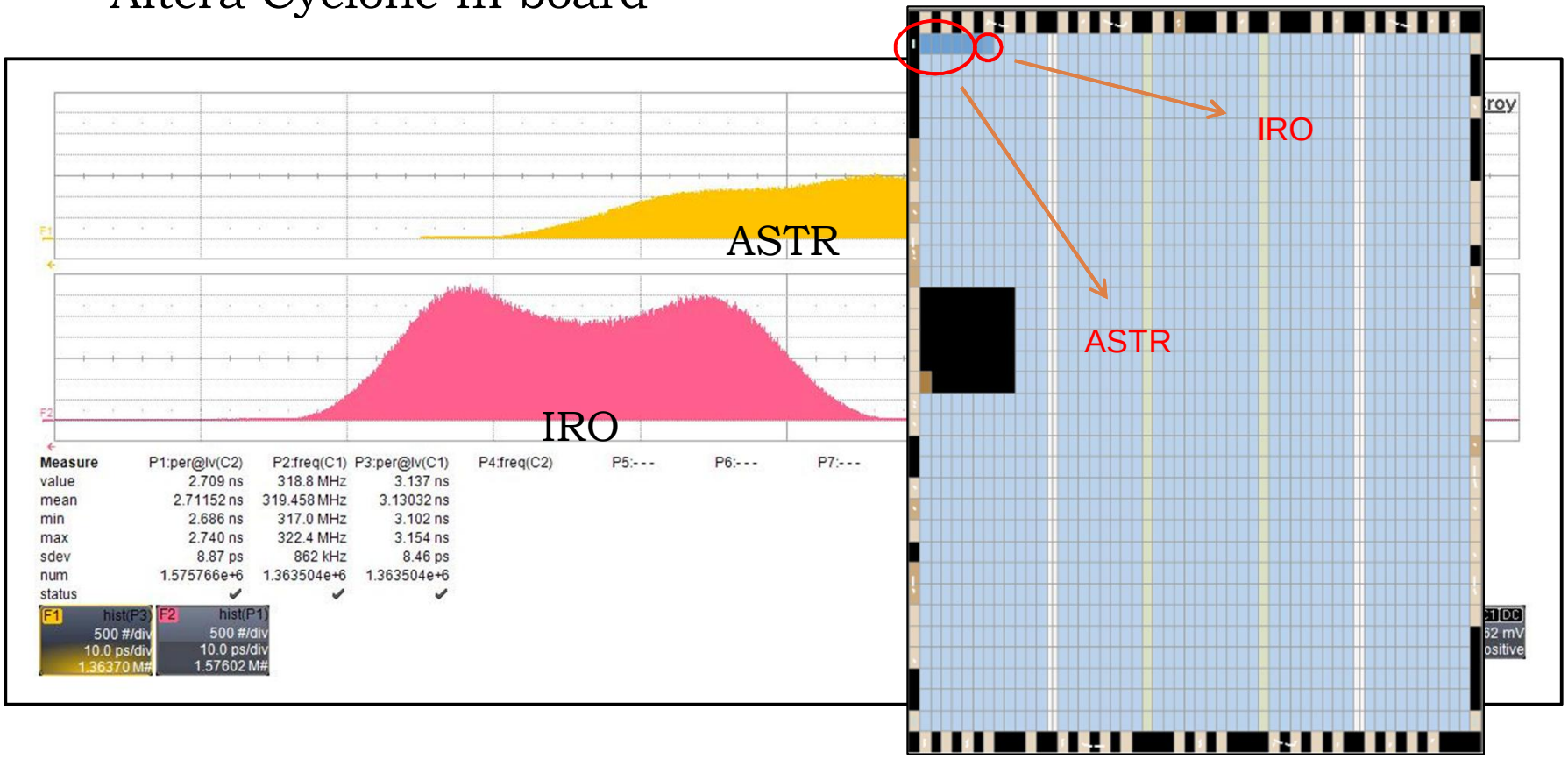
Influence of Surrounding Logic

- A simple experiment : an IRO (5 stages ~ 300 Mhz) and an ASTR (96 stages ~ 320 Mhz) running simultaneously in an Altera Cyclone III board



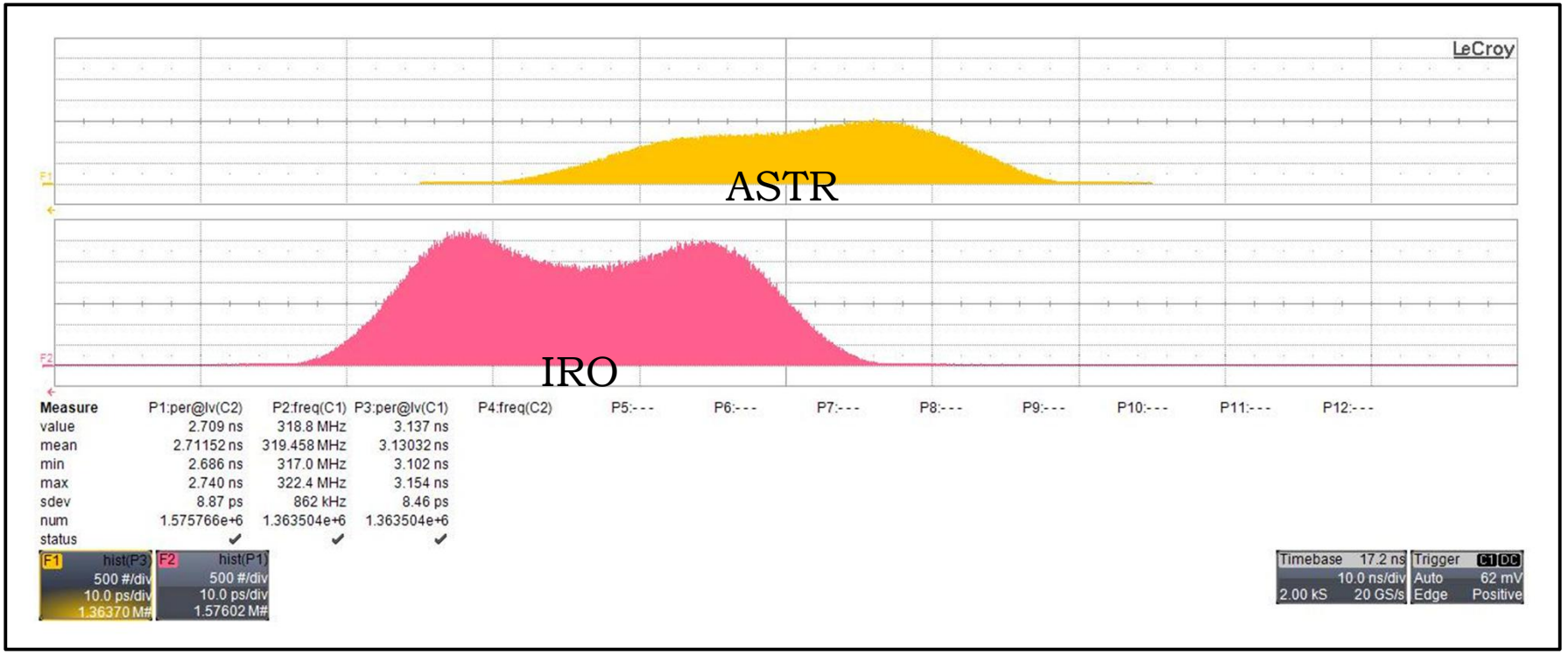
Influence of Surrounding Logic

- A simple experiment : an IRO (5 stages ~ 300 Mhz) and an ASTR (96 stages ~ 320 Mhz) running simultaneously in an Altera Cyclone III board



Influence of Surrounding Logic

- A simple experiment : an IRO (5 stages ~ 300 Mhz) and an ASTR (96 stages ~ 320 Mhz) running simultaneously in an Altera Cyclone III board



Analysis : Routing Counts

- Limitations of constant stage parameters model
  - TBTB … TB configuration : frequency independent from number of stages

$$T_{osc} = 4 * (D_{LUT} + D_{charlie})$$

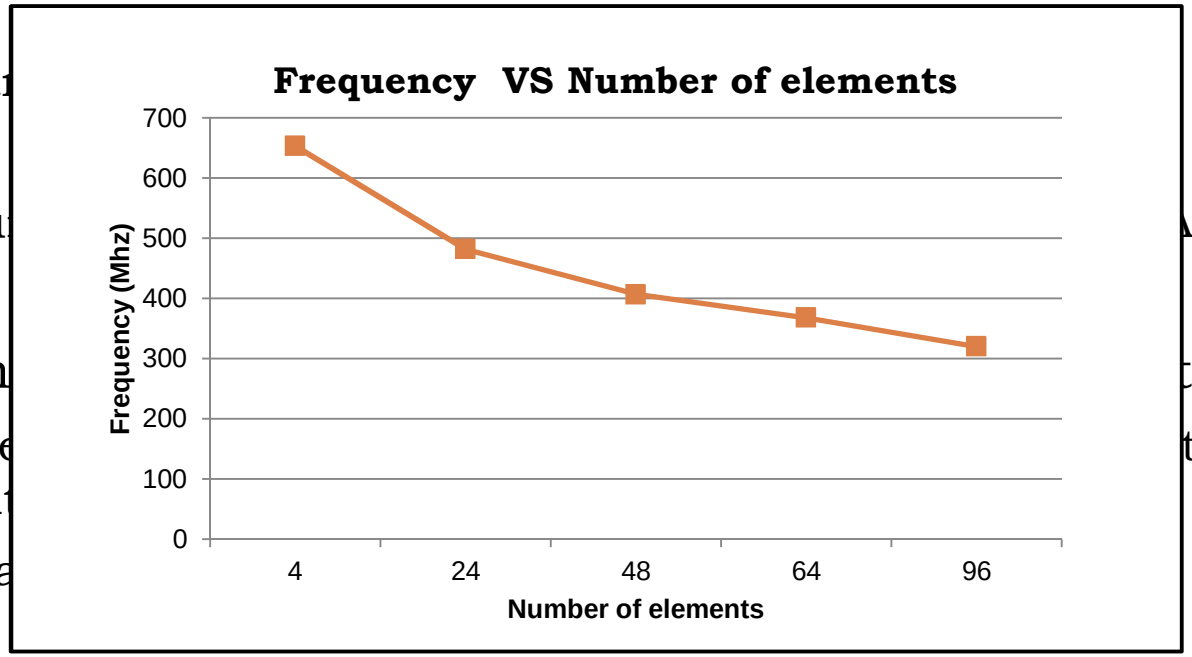
  - Robustness to voltage variations : influence of stage length
  - Well suited for ASIC but placement/routing matters in FPGA
- Extending the existing model to more restrictive targets
  - Consider different timing parameters for each stage : take into account routing
  - Low drafting effect

Analysis : Routing Counts

- Limitations of constant stage parameters model
  - TBTB … TB configuration : frequency independent from number of stages

$$T_{osc} = 4*(D_{LUT} + D_{charlie})$$

  - Robust
  - Well su
- Extendin
  - Conside
    account
  - Low dra



Analysis : Routing Counts

- Limitations of constant stage parameters model
  - TBTB … TB configuration : frequency independent from number of stages

$$T_{osc} = 4 * (D_{LUT} + D_{charlie})$$

  - Robustness to voltage variations : influence of stage length
  - Well suited for ASIC but placement/routing matters in FPGA
- Extending the existing model to more restrictive targets
  - Consider different timing parameters for each stage : take into account routing
  - Low drafting effect

Analysis : Routing Counts

- Limitations of constant stage parameters model
  - TBTB … TB configuration : frequency independent from number of stages

$$T_{osc} = 4*(D_{LUT} + D_{charlie})$$

  - Robustness to voltage variations : influence of stage length
  - Well suited for ASIC but placement/routing matters in FPGA

- Extending the existing model to more restrictive targets
  - Consider different timing parameters for each stage : take into account routing
  - Low drafting effect

➡ $$charlie_i(s) = Ds_i + \sqrt{D_{charlie}{}^2 + s^2}$$

Analysis : Period Expession

- Oscillation period for a 4-stage ring

$$T_{osc} = \sum_{i=1}^{4} Ds_i + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_4 - Ds_2}{2}\right)^2} + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_3 - Ds_1}{2}\right)^2}$$

- General oscillation period expression for an n-stage ring

$$T_{osc} = \frac{4}{n}\sum_{i=1}^{n} Ds_i + f\left(D_{charlie}, Ds_{i, i\in\{1,\ldots,n\}}\right)$$

Analysis : Period Expession

- Oscillation period for a 4-stage ring

$$T_{osc} = \sum_{i=1}^{4} Ds_i + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_4 - Ds_2}{2}\right)^2} + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_3 - Ds_1}{2}\right)^2}$$

- General oscillation period expression for an n-stage ring

$$T_{osc} = \frac{4}{n}\sum_{i=1}^{n} Ds_i + f\left(D_{charlie}, Ds_{i, i\in\{1,\ldots,n\}}\right)$$

static delays contribution

$$\approx 4 * D_{LUT}$$

Charlie effect contribution (non linear)

Analysis : Period Expession

- Oscillation period for a 4-stage ring

$$T_{osc} = \sum_{i=1}^{4} Ds_i + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_4 - Ds_2}{2}\right)^2} + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_3 - Ds_1}{2}\right)^2}$$

- General oscillation period expression for an n-stage ring

$$T_{osc} = \frac{4}{n}\sum_{i=1}^{n} Ds_i + f\left(D_{charlie}, Ds_{i,i\in\{1,\ldots,n\}}\right)$$

static delays contribution

$$\approx 4 * D_{LUT}$$

Robustness to PV

Charlie effect contribution (non linear)

Analysis : Period Expession

- Oscillation period for a 4-stage ring

$$T_{osc} = \sum_{i=1}^{4} Ds_i + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_4 - Ds_2}{2}\right)^2} + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_3 - Ds_1}{2}\right)^2}$$

- General oscillation period expression for an n-stage ring

$$T_{osc} = \frac{4}{n}\sum_{i=1}^{n} Ds_i + f\left(D_{charlie}, Ds_{i,i\in\{1,\ldots,n\}}\right)$$

static delays contribution

$$\approx 4 * D_{LUT}$$

Robustness to PV

Charlie effect contribution (non linear)

Robustness to VV

Analysis : Period Expession

- Oscillation period for a 4-stage ring

$$T_{osc} = \sum_{i=1}^{4} Ds_i + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_4 - Ds_2}{2}\right)^2} + 2\sqrt{D_{charlie}^{\ 2} + \left(\frac{Ds_3 - Ds_1}{2}\right)^2}$$

- General oscillation period expression for an n-stage ring

$$T_{osc} = \frac{4}{n}\sum_{i=1}^{n} Ds_i + f\left(D_{charlie}, Ds_{i, i\in\{1,\ldots,n\}}\right)$$

- Derivative with respect to voltage for a 4-stage ring

$$\frac{\partial T_{osc}}{\partial V} = \sum_{i=1}^{4}\frac{\partial Ds_i}{\partial V} + \frac{Ds_3 - Ds_1}{2\sqrt{D_{charlie}^2 + \left(\frac{Ds_3 - Ds_1}{2}\right)^2}}\left(\frac{\partial Ds_3}{\partial V} - \frac{\partial Ds_1}{\partial V}\right) + \frac{Ds_4 - Ds_2}{2\sqrt{D_{charlie}^2 + \left(\frac{Ds_4 - Ds_2}{2}\right)^2}}\left(\frac{\partial Ds_4}{\partial V} - \frac{\partial Ds_2}{\partial V}\right)$$

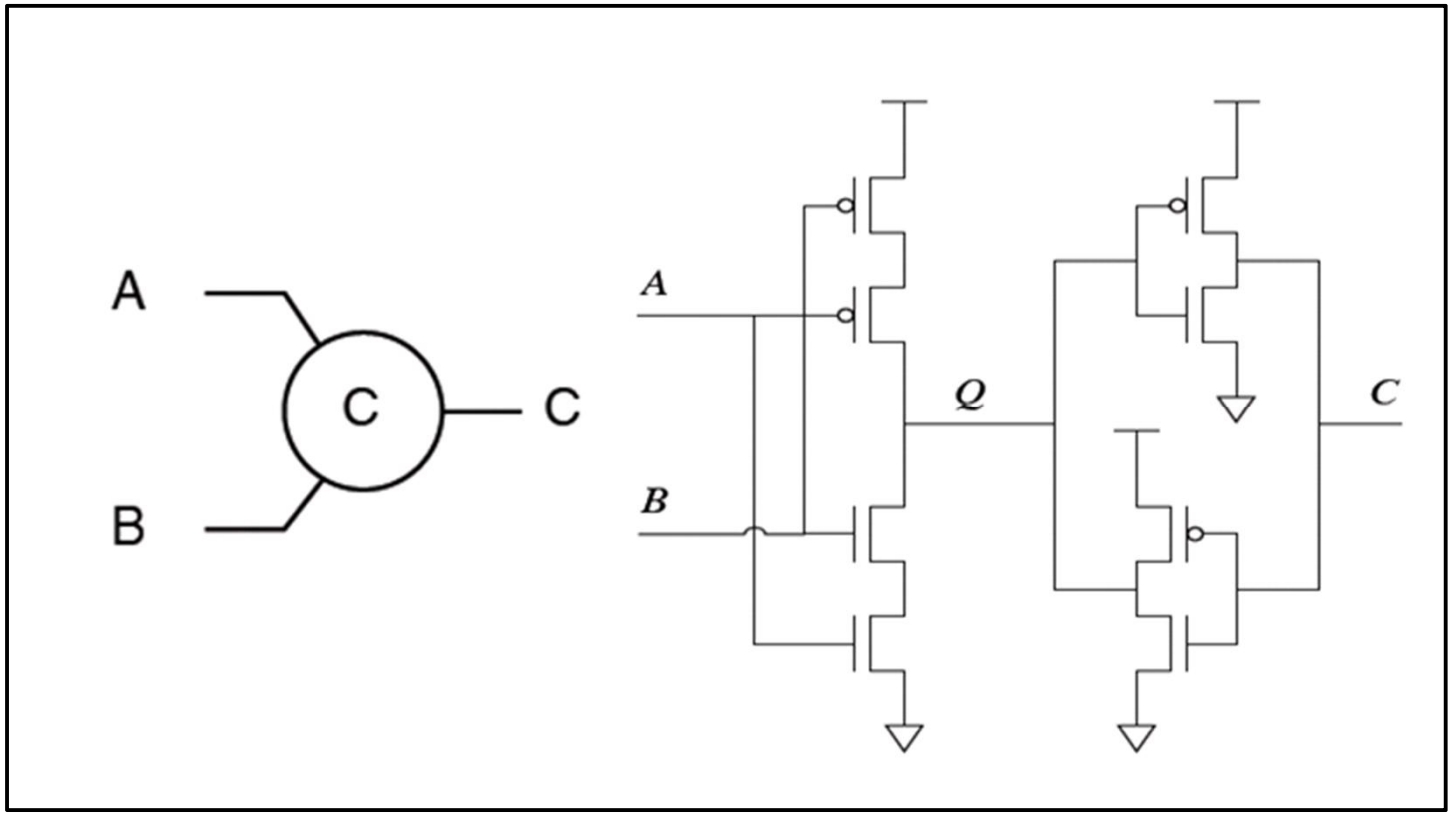
Conclusion

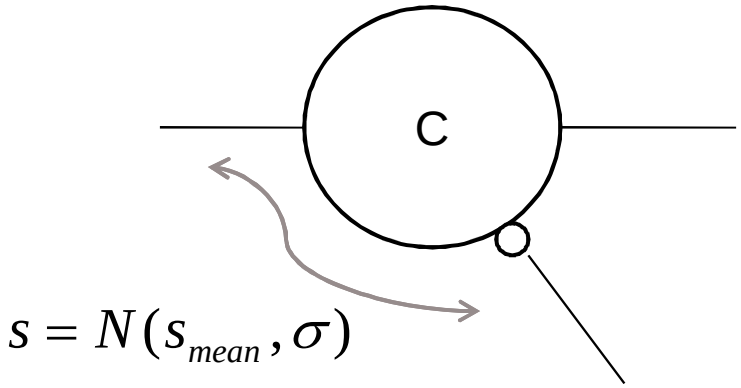
	IRO	ASTR
Behavior	One event evolving in the ring	Several events evolving in the ring simultaneously
Frequency	Linear dependency with number of elements and stage delays	Depends on many parameters
Implementation	Easy	Needs placement
Size	Small (5-stage ~ 300 Mhz)	Medium (96-stage ~ 300 Mhz)
Power Consumption	-	Probably higher than IRO
Robustness to process variability	Increases with number of elements	Increases with number of elements while maintaining high frequency
Robustness to voltage variations	Low	Increases with number of stages
Period jitter	Increases with number of elements (square root accumulation)	Constant with number of elements, in theory a lower deterministic contribution

Future Works

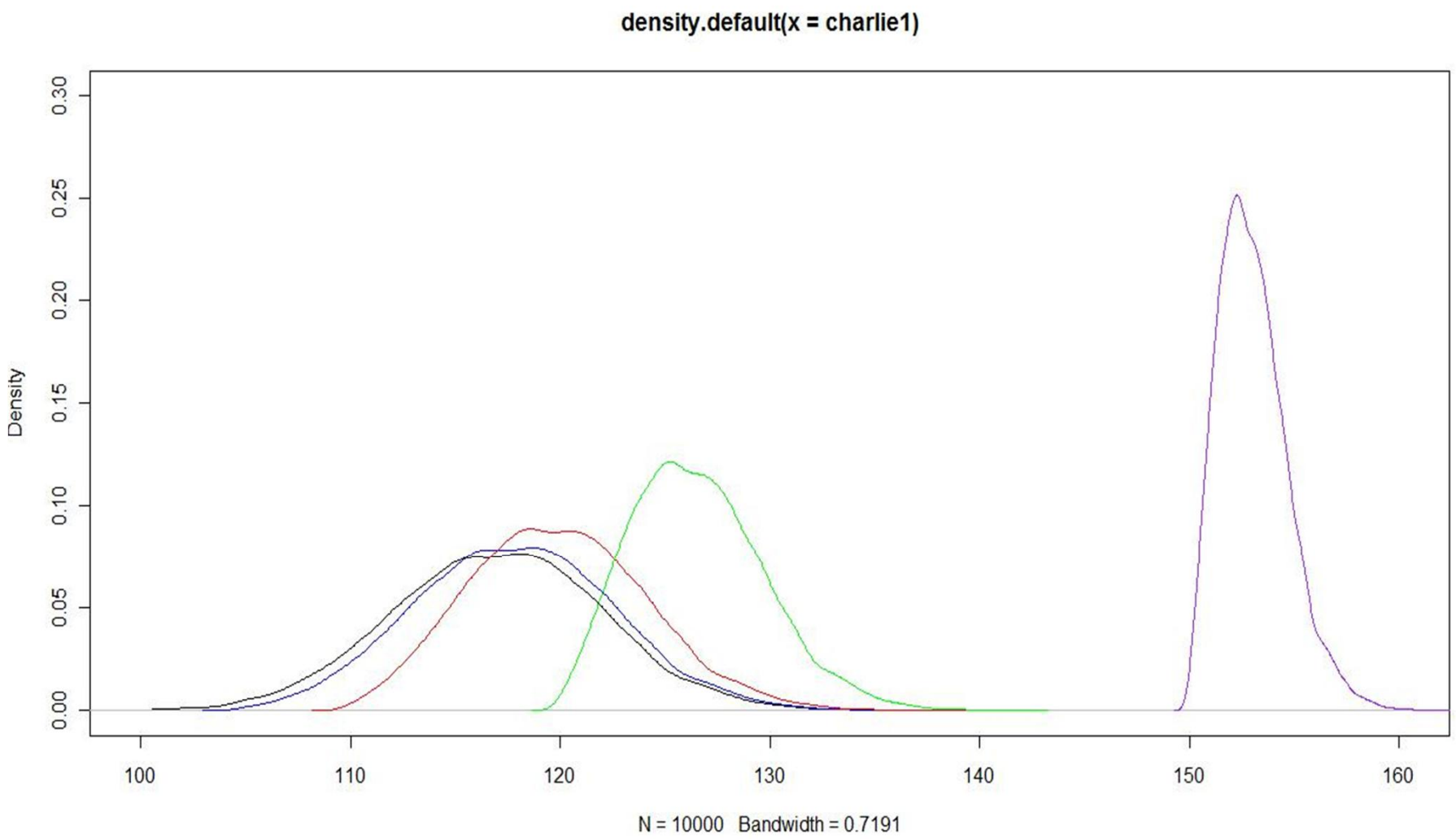
- Regarding robustness : validate the results by doing more measurements, quantify the influence of surrounding logic
- Jitter characterization
- Developping the time accurate model
- Concrete implementation of some TRNG using asynchronous self-timed rings and inverter rings (Sunar generator, Wold & Tan …) to compare robustness at a statistic level

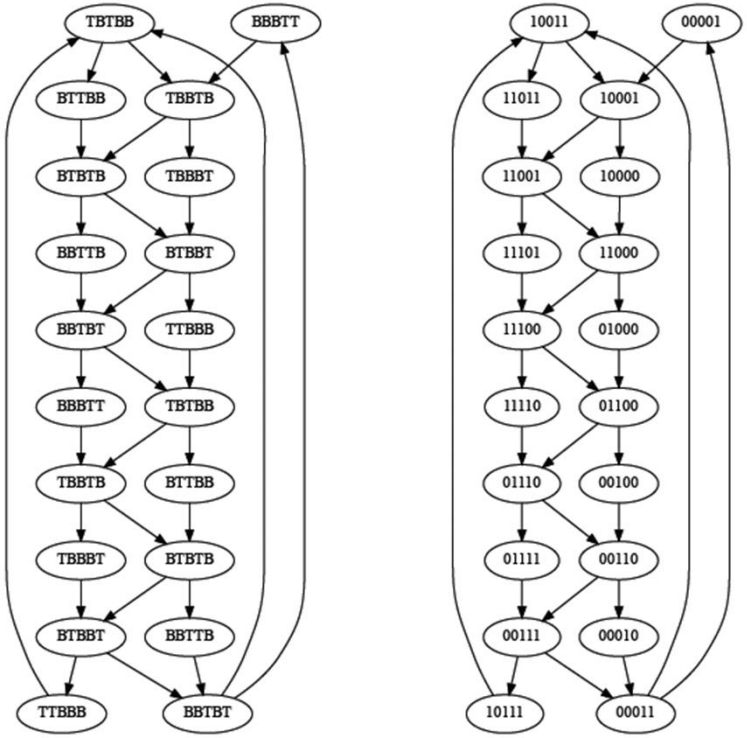
Thank you !

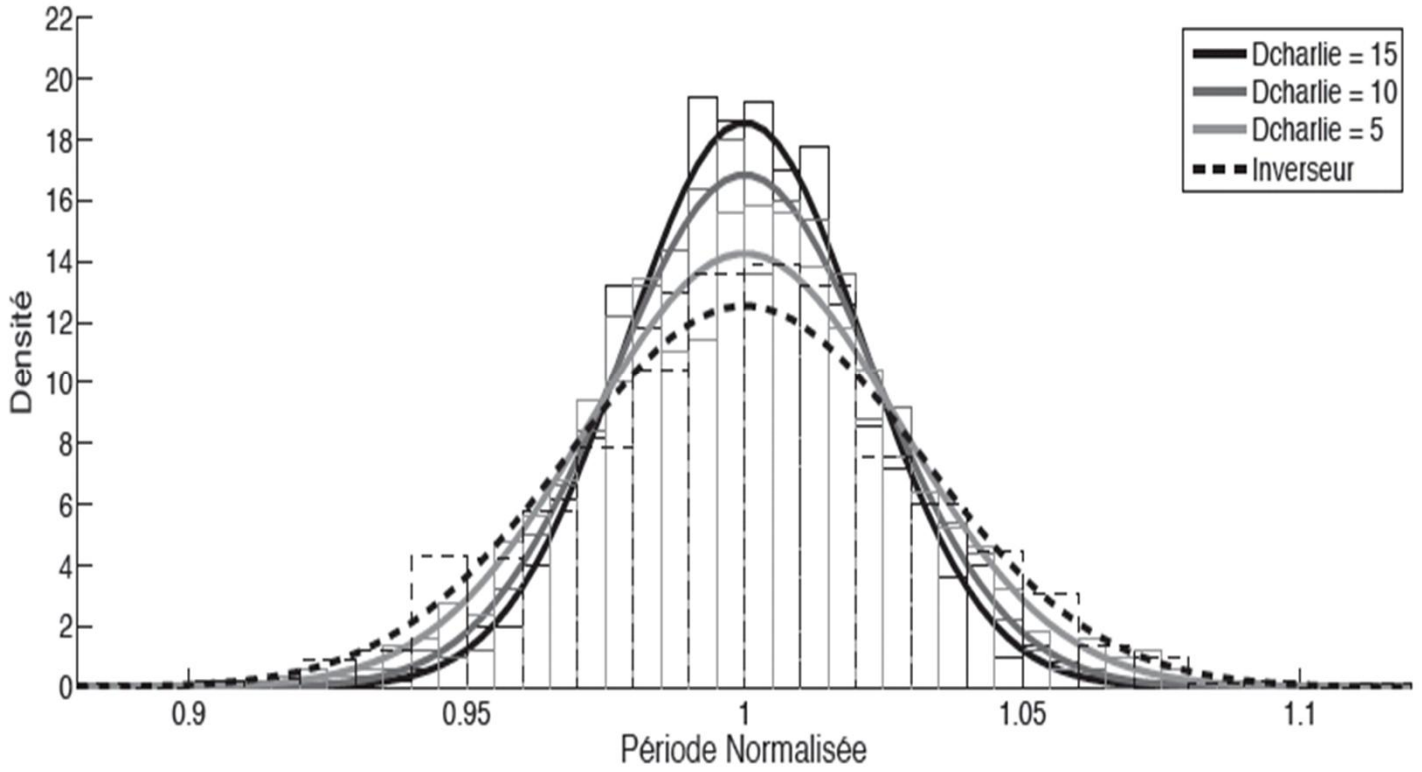

A
B
C
C
A
B
Q
C



$$charlie(s, y) = D_{mean} + \sqrt{D_{charlie}^2 + (s - s_{\min})^2} - B * \exp(-y / A)$$


density.default(x = charlie1)
Density
0.00
0.05
0.10
0.15
0.20
0.25
0.30
100
110
120
130
140
150
160
N = 10000 Bandwidth = 0.7191


TBTBB
BBBTT
BTTBB
TBBTB
BTBTB
TBBBT
BBTTB
BTBBT
BBTBT
TTBBB
BBBTT
TBTBB
TBBTB
BTTBB
TBBBT
BTBTB
BTBBT
BBTTB
TTBBB
BBTBT
10011
00001
11011
10001
11001
10000
11101
11000
11100
01000
11110
01100
01110
00100
01111
00110
00111
00010
10111
00011


Dcharlie = 15
Dcharlie = 10
Dcharlie = 5
Inverseur
Densité
Période Normalisée
0
2
4
6
8
10
12
14
16
18
20
22
0.9
0.95
1
1.05
1.1