

Soundness of the Quasi-Synchronous Abstraction

Guillaume Baudart

Timothy Bourke

Marc Pouzet

École normale supérieure, INRIA Paris

The Cooking Book



VERIMAG

UNITE MIXTE DE RECHERCHE

Centre Equation
2 avenue de Vignate
38610 GIERES
Tel. +33 4 76 63 48 48
Fax +33 4 76 63 48 50

The Quasi-Synchronous Approach to Distributed Control Systems

Crisys draft

October 2000

The Cooking Book

Chapter 2

The Architectural Evolution

Aircraft control systems illustrate this evolution which can also be found in many other fields of industrial control

2.1 Analog/Digital Communication

Starting from networks of analog boards, progressively some boards were replaced by discrete digital boards, and then by computers. Communication between the digital parts and the parts which remained analog was mainly based on periodic sampling (analog to digital conversion) and holding (digital to analog conversion), sampling periods being adapted to the frequency properties of the signals that traveled through the network. This allowed several technologies to smoothly cooperate. Figure 2.1 illustrates this evolution.

2.2 Serial Links

This technique was suitable up to the time when two connected analog boards were replaced by digital ones. Then these two also had to communicate and serial port communication appeared as the simplest way of replacing analog to digital and digital to analog communication as both can be seen as latches or memories. Figure 2.2 shows a typical situation borrowed from an automatic subway application. Each computer monitors a rail track section and runs a periodic program. Computers are linked together by serial lines

2.4 Supervision

In most cases, this architecture is being added a supervisor, for monitoring purposes. The communication between the supervisor and field computers is however very different from the communication between field computers. It is an event-based communication which is assumed not to be time nor safety critical and which takes place either on special time slots of the field bus, or on a dedicated communication medium. The important fact, here, is that it should not perturbate neither the periodic behavior of field computers, nor their communication.

2.5 Provision against Byzantine Problems

In these very critical systems, Byzantine faults cannot be neglected and this is why some architectural precautions have to be taken in order to alleviate their consequences. For instance, these busses provide some protection against Byzantine problems [22], in the sense that they are based on broadcast: communication with several partners only involve one emission. Thus a failed unit cannot diversely lie to its partners. Then messages are protected by either error correcting and/or detecting codes which can be assumed to be powerful enough so that their failing be negligible with respect to the probabilistic fault tolerance requirements of the system under consideration.

2.6 Communication Abstraction

According to what precedes, we can quite precisely state an abstract property of this kind of communication medium, which is a bounded delay communication property:

Property 1. *First, we assume that every process P is periodic with a period varying between small margins:*

$$T_{Pm} \leq T_P \leq T_{PM}$$

Then,

Property 2. *Let T_{sM} and T_{rM} be the respective maximal periods of the sender and of the receiver, and n the maximum number of non negligible consecutive failed receives (in the case of error correction, $n = 1$).*

The Cooking Book

Chapter 2

The Architectural Evolution

Aircraft control systems illustrate this evolution which can also be found in many other fields of industrial control

8

Crisys Esprit Project

2.4 Supervision

In most cases, this architecture is being added a supervisor, for monitoring purposes. The communication between the supervisor and field computers is however very different from the communication between field computers. It is an event-based communication which is assumed not to be time nor safety critical and which takes place either on special time slots of the field bus, or on a dedicated communication medium. The important fact, here, is that it should not perturbate neither the periodic behavior of field computers, nor their communication.

2.5 Provision against Byzantine Problems

In these very critical systems, Byzantine faults cannot be neglected and this is why some architectural precautions have to be taken in order to allevi-

Property 1. *First, we assume that every process P is periodic with a period varying between small margins:*

$$T_{Pm} \leq T_P \leq T_{PM}$$

This technique was suitable up to the time when two connected analog boards were replaced by digital ones. Then these two also had to communicate and serial port communication appeared as the simplest way of replacing analog to digital and digital to analog communication as both can be seen as latches or memories. Figure 2.2 shows a typical situation borrowed from an automatic subway application. Each computer monitors a rail track section and runs a periodic program. Computers are linked together by serial lines

varying between small margins:

$$T_{Pm} \leq T_P \leq T_{PM}$$

Then,

Property 2. *Let T_{sM} and T_{rM} be the respective maximal periods of the sender and of the receiver, and n the maximum number of non negligible consecutive failed receives (in the case of error correction, $n = 1$).*

The Cooking Book

Chapter 2

The Architectural Evolution

Aircraft control systems illustrate this evolution which can also be found in many other fields of industrial control

8

Crisys Esprit Project

2.4 Supervision

In most cases, this architecture is being added a supervisor, for monitoring purposes. The communication between the supervisor and field computers is however very different from the communication between field computers. It is an event-based communication which is assumed not to be time nor safety critical and which takes place either on special time slots of the field bus, or on a dedicated communication medium. The important fact, here, is that it should not perturbate neither the periodic behavior of field computers, nor their communication.

2.5 Provision against Byzantine Problems

In these very critical systems, Byzantine faults cannot be neglected and this is why some architectural precautions have to be taken in order to allevi-

Property 1. *First, we assume that every process P is periodic with a period varying between small margins:*

$$T_{Pm} \leq T_P \leq T_{PM}$$

Quasi-Periodic Architecture

This technique was suitable up to the time when two connected analog boards were replaced by digital ones. Then these two also had to communicate and serial port communication appeared as the simplest way of replacing analog to digital and digital to analog communication as both can be seen as latches or memories. Figure 2.2 shows a typical situation borrowed from an automatic subway application. Each computer monitors a rail track section and runs a periodic program. Computers are linked together by serial lines

varying between small margins:

$$T_{Pm} \leq T_P \leq T_{PM}$$

Then,

Property 2. *Let T_{sM} and T_{rM} be the respective maximal periods of the sender and of the receiver, and n the maximum number of non negligible consecutive failed receives (in the case of error correction, $n = 1$).*

The Cooking Book

Chapter 3

A Synchronous Tool set for Quasi-Synchronous Systems

In this chapter we show how synchronous design tools allow a global system description, simulation and validation. We first describe our notation. Then we show how to describe systems implemented on a quasi-synchronous architecture and how to simulate them.

3.1 Synchronous Data-Flow Notations

In the sequel, algorithms are expressed using a functional notation, that is to say by abstracting over time indices, in order to stay consistent with design tools. Thus, a signal definition:

$$x_1 = x_2 \text{ means } \forall n \in N : x_1(nT) = x_2(nT).$$

3.1.1 Usual Operators

An operation:

$$(x_1 - x_2)(nT) \text{ means } x_1(nT) - x_2(nT)$$

and similarly,

3.2.1 Shared Memory

Given a sequence u written in the shared memory at clock cw and an initial content v , the current content of the memory can be expressed as:

$$mem(v, cw, u) = v \text{ fby } (\text{current}(v, cw) \ u)$$

where the delay accounts for short² undetermined transmission delays.

Then, the sequence read at clock cr is :

$$u' = mem(v, cw, u) \text{ when } cr$$

3.2.2 Formalizing Periodic Clocks

This could be done in some real-time framework, such as timed automata [2], but, for the sake of simplicity, we prefer here to characterize the fact that two independent clocks have approximately the same period by saying that:

Any of the two clocks cannot take the value "t" more than twice between two successive "t" values of the other one.

This can be formalized by saying that the boolean vector stream composed of the two clocks should never contain the subsequence:

$$\begin{bmatrix} t \\ - \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$

nor the one obtained by exchanging coordinates. (Here, $-$ is a wild card representing any of the two values $\{t, f\}$.)

Now, such regular expressions yield finite state recognizability and can be associated a finite-state recognizing dynamic system *Same_Period*³.

Furthermore, replacing in what precedes 2 by n allows defining similar *Same_Period_n* systems.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

³This can be automatically generated in Lustre, thanks to the REGLO tool [23].

The Cooking Book

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Chapter 3

A Synchronous Tool set for Quasi-Synchronous Systems

In this chapter we show how synchronous design tools allow a global system description, simulation and validation. We first describe our notation. Then we show how to describe systems implemented on a quasi-synchronous architecture and how to simulate them.

3.1 Synchronous Data-Flow Notations

In the sequel, algorithms are expressed using a functional notation, that is to say by abstracting over time indices, in order to stay consistent with design tools. Thus, a signal definition:

$$x_1 = x_2 \text{ means } \forall n \in N : x_1(nT) = x_2(nT).$$

3.1.1 Usual Operators

An operation:

$$(x_1 - x_2)(nT) \text{ means } x_1(nT) - x_2(nT)$$

and similarly,

$$mem(v, cw, u) = v \text{ by } (current(v, cw) \ u)$$

where the delay accounts for short² undetermined transmission delays.

Then, the sequence read at clock cr is :

$$u' = mem(v, cw, u) \text{ when } cr$$

3.2.2 Formalizing Periodic Clocks

This could be done in some real-time framework, such as timed automata [2], but, for the sake of simplicity, we prefer here to characterize the fact that two independent clocks have approximately the same period by saying that:

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

This can be formalized by saying that the boolean vector stream composed of the two clocks should never contain the subsequence:

$$\begin{bmatrix} t \\ - \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$

nor the one obtained by exchanging coordinates. (Here, $-$ is a wild card representing any of the two values $\{t, f\}$.)

Now, such regular expressions yield finite state recognizability and can be associated a finite-state recognizing dynamic system *Same_Period*³.

Furthermore, replacing in what precedes 2 by n allows defining similar *Same_Period_n* systems.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

³This can be automatically generated in Lustre, thanks to the REGLO tool [23].

The Cooking Book

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Chapter 3

$mem(v, cw, u) = v \text{ by } (current(v, cw) \ u)$

This can be formalized by saying that the boolean vector stream composed of the two clocks should never contain the subsequence:

$$\begin{bmatrix} t \\ - \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$

3.1.1 Usual Operators

An operation:

$(x_1 - x_2)(nT)$ means $x_1(nT) - x_2(nT)$

and similarly,

nor the one obtained by exchanging coordinates. (Here, $-$ is a wild card representing any of the two values $\{t, f\}$.)

Now, such regular expressions yield finite state recognizability and can be associated a finite-state recognizing dynamic system *Same_Period*³.

Furthermore, replacing in what precedes 2 by n allows defining similar *Same_Period_n* systems.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

³This can be automatically generated in Lustre, thanks to the REGLO tool [23].

The Cooking Book

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Chapter 3

$mem(v, cw, u) = v \text{ by } (current(v, cw) \ u)$

This can be formalized by saying that the boolean vector stream composed of the two clocks should never contain the subsequence:

$$\begin{bmatrix} t \\ - \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$

Quasi-Synchrony

3.1.1 Usual Operators

An operation:

$(x_1 - x_2)(nT)$ means $x_1(nT) - x_2(nT)$

and similarly,

nor the one obtained by exchanging coordinates. (Here, $-$ is a wild card representing any of the two values $\{t, f\}$.)

Now, such regular expressions yield finite state recognizability and can be associated a finite-state recognizing dynamic system *Same_Period*³.

Furthermore, replacing in what precedes 2 by n allows defining similar *Same_Period* _{n} systems.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

³This can be automatically generated in Lustre, thanks to the REGLO tool [23].

The Cooking Book

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Chapter 3

$mem(v, cw, u) = v \text{ by } (current(v, cw) \ u)$

This can be formalized by saying that the boolean vector stream composed of the two clocks should never contain the subsequence:

$$\begin{bmatrix} t \\ - \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$

Quasi-Synchrony

3.1.1 Usual Operators

nor the one obtained by exchanging coordinates. (Here, $-$ is a wild card representing any of the two values $\{t, f\}$.)

Now, such regular expressions yield finite state recognizability and can be associated a finite state recognizing dynamic system. *Same. Defined 3.*

the delay accounts for short² undetermined transmission delays.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

The Cooking Book



VERIMAG

UNITE MIXTE DE RECHERCHE

Centre Equation
2 avenue de Vignate
38610 GIERES
Tel. +33 4 76 63 48 48
Fax +33 4 76 63 48 50

The Quasi-Synchronous Approach to Distributed Control Systems

Crisys draft

October 2000

The Cooking Book

2006

©IEEE Computer Society Press, ACSD'06

Simulation and Verification of Asynchronous Systems by means of a Synchronous Model*

Nicolas Halbwachs and Louis Mandel[†]
Vérimag[‡] Grenoble – France

Abstract

Synchrony and asynchrony are commonly opposed to each other. Now, in embedded applications, actual solutions are often situated in between, with synchronous processes composed in a partially asynchronous way. Examples of such intermediate solutions are GALS, quasi-synchronous periodic processes, deadline-driven task scheduling. . . In this paper, we illustrate the use of the synchronous paradigm to model and validate such partially asynchronous applications. We show that, through the use of sporadic activation of processes and simulation of non-determinism by the way of auxiliary inputs, the synchronous paradigm allows a precise control of asynchrony. The approach is illustrated on a real case study, proposed in the framework of the European Integrated project "Assert".

1 Introduction

It is well admitted, now, that the synchronous paradigm [4, 20] can significantly ease the modeling, programming, and validation of embedded systems and software. The synchronous parallel composition helps in structuring the model, without introducing non-determinism. The determinism of the model is also an invaluable advantage for its validation: tests are reproducible, and model-checking is not faced with the proliferation of states due to non-deterministic interleaving of processes.

It is also recognized that the synchronous paradigm is not the panacea, since it does not directly apply to intrinsically asynchronous situations, such as distributed systems, or applications mixing long tasks and urgent sporadic requests. This is why numerous works (see, e.g., [7] for a synthesis) are devoted to combining synchrony with asynchrony, or to extending the synchronous model towards less

synchronous applications. For instance, "Communicating reactive processes" [11] or "Multiclock Esterel" [10] are extensions of the synchronous language Esterel [8] to cope with non perfectly synchronous concurrency. On the other hand, the paradigm of "Globally asynchronous, locally synchronous systems" (GALS) has been proposed [16, 1, 9] to describe general asynchronous systems, while keeping as much as possible the advantages of synchronous components. "Tag machines" [6, 5] are an even more general and abstract attempt in the same direction. [17] mixes synchronous (Signal) and asynchronous (Promela) models for verifying GALS.

Another track of research addresses the compilation of synchronous programs towards distributed or non strictly synchronous code. While some distribution methods aim at strictly preserving the synchronous semantics [13, 12], other proposals only preserve the functional semantics [14, 15, 27, 26].

Finally, other works concern the modeling of asynchronous systems within the synchronous paradigm. It is well-known since [24, 25] that a synchronous formalism can be used to express asynchrony. The only need is to express sporadic activation (or stuttering) of processes — which is allowed in all existing synchronous languages — and explicit non-determinism. The modeling tool Model-Build [2, 3] — developed within the European projects SafeAir and SafeAir2 — and the Polychrony workbench [23, 19, 18] are based on this idea. In this paper, we report on our use of this kind of approach in the framework of the Assert project.

Assert is a European Integrated Project devoted to the design of embedded systems from the system architecture level down to the code, with special emphasis on high-level modeling, proof-based design, and component reuse. Aerospace industry (avionics, launchers, and satellites) constitutes the main application domain of Assert. In this framework, we propose a methodology based on a high-level behavioral modeling and verification of an application, using a synchronous formalism. Since the automatic generation of distributed code is not an objective of the project, the automatic code generation is only applied separately to

VERIMAG

UNITE DE RECHERCHE

The Quasi-Synchronous Approach to Distributed Control Systems

Crisys draft

October 2000

*This work was partially supported by the European Commission under the Integrated Project Assert, IST 004033

[†]email: {Nicolas.Halbwachs, Louis.Mandel}@imag.fr

[‡]Vérimag is a joint laboratory of Université Joseph Fourier, CNRS and INPG associated with IMAG.

The Cooking Book

2006

©IEEE Computer Society Press, ACSD'06

Simulation and Verification of Asynchronous Systems by means of a Synchronous Model*

Nicolas Halbwachs and Louis Mandel†
Vérimag‡ Grenoble – France

Abstract

Synchrony and asynchrony are commonly to each other. Now, in embedded applica- tual solutions are often situated in between, chronous processes composed in a partially asy way. Examples of such intermediate solutions: quasi-synchronous periodic processes, deadline- scheduling... In this paper, we illustrate the use chronous paradigm to model and validate suc asynchronous applications. We show that, throu of sporadic activation of processes and simulati determinism by the way of auxiliary inputs, the sy paradigm allows a precise control of asynchron proach is illustrated on a real case study, propo framework of the European Integrated project “.

1 Introduction

It is well admitted, now, that the sy paradigm [4, 20] can significantly ease the mod gramming, and validation of embedded system ware. The synchronous parallel composition help turing the model, without introducing non-de The determinism of the model is also an invalua tage for its validation: tests are reproducible, a checking is not faced with the proliferation of st non-deterministic interleaving of processes.

It is also recognized that the synchronous p not the panacea, since it does not directly apply cally asynchronous situations, such as distribute or applications mixing long tasks and urgent sq quests. This is why numerous works (see, e.g. synthesis) are devoted to combining synchrony chrony, or to extending the synchronous model to

*This work was partially supported by the European Comu the Integrated Project Assert, IST 004033
†email: {Nicolas.Halbwachs, Louis.Mandel}
‡Verimag is a joint laboratory of Université Joseph Fourie INPG associated with IMAG.

IRIMAG
XTE DE RECHERCHE

2008

Synchronous modeling and validation of schedulers dealing with shared resources²

Erwan Jahier, Nicolas Halbwachs, Pascal Raymond

Jul 17 2008

Abstract

Architecture Description Languages (ADLs) allow embedded systems to be described as assemblies of hardware and software components. It is attractive to use such a global modelling as a basis for early system analysis. However, in such descriptions, the applicative software is often abstracted away, and is supposed to be developed in some host programming language. This forbids to take the applicative software into account in such early validation. To overcome this limitation, a solution consists in translating the ADL description into an executable model, which can be simulated and validated together with the software. In a previous paper [8], we proposed such a translation of AADL (Architecture Analysis & Design Language) specifications into an executable synchronous model. The present paper is a continuation of this work, and deals with expressing the behavior of complex scheduling policies managing shared resources. We provide a synchronous specification for two shared resource scheduling protocols: the well-known basic priority inheritance protocol (BIP), and the priority ceiling protocol (PCP). This results in an automated translation of AADL models into a purely Boolean synchronous (Lustre) scheduler, that can be directly model-checked, possibly with the actual software.

Keywords: Embedded systems, Simulation, Scheduling, Formal Verification, Architecture Description Languages, Synchronous Languages

Reviewers: Florence Maraninchi

Notes:

How to cite this report:

```
@techreport { ,
  title = { Synchronous modeling and validation of schedulers dealing with shared resources3 },
  authors = { Erwan Jahier, Nicolas Halbwachs, Pascal Raymond },
  institution = { Verimag Research Report },
  number = { TR-2008-10 },
  year = { },
  note = { }
}
```

ach to
ns

The Cooking Book

2006

©IEEE Computer Society Press, ACSD'06

Simulation and Verification of Asynchronous Systems by means of a Synchronous Model*

Nicolas Halbwachs and Louis Mandel[†]
Vérimag[‡] Grenoble – France

Abstract

*Synchrony and asynchrony are commonly to each other. Now, in embedded applica- tual solutions are often situated in between, chronous processes composed in a partially asy way. Examples of such intermediate solutions quasi-synchronous periodic processes, deadline- scheduling... In this paper, we illustrate the use chronous paradigm to model and validate suc asynchronous applications. We show that, throu of sporadic activation of processes and simulati determinism by the way of auxiliary inputs, the sy paradigm allows a precise control of asynchron proach is illustrated on a real case study, propo framework of the European Integrated project *.*

1 Introduction

It is well admitted, now, that the sy paradigm [4, 20] can significantly ease the mod gramming, and validation of embedded system ware. The synchronous parallel composition help turing the model, without introducing non-de The determinism of the model is also an invalua tage for its validation: tests are reproducible, a checking is not faced with the proliferation of st non-deterministic interleaving of processes.

It is also recognized that the synchronous p not the panacea, since it does not directly apply cally asynchronous situations, such as distribute or applications mixing long tasks and urgent s requests. This is why numerous works (see, e.g. synthesis) are devoted to combining synchrony chrony, or to extending the synchronous model to

*This work was partially supported by the European Comu the Integrated Project Asserit, IST 004033

[†]email: {Nicolas.Halbwachs, Louis.Mandel}

[‡]Vérimag is a joint laboratory of Université Joseph Fourie INPG associated with IMAG.

VERIMAG
XTE DE RECHERCHE

2008

Synchronous modeling and validation of schedulers dealing with shared resources²

Erwan Jahier, Nicolas Halbwachs, Pascal Raymond

Jul 17 2008

Abstract

Architecture Description Languages (ADLs) allow embedded systems to be described as assemblies of hardware and software components. It is attractive to use such a global modelling as a basis for early system analysis. However, in such descriptions, the applicative software is often abstracted away, and is supposed to be developed in some host programming language. This forbids to take the applicative software into account in such early validation. To overcome this limitation, a solution consists in translating the ADL description into an executable model, which can be simulated and validated together with the software. In a previous paper [8], we proposed such a translation of AADL (Architecture Analysis & Design Language) specifications into an executable synchronous model. The present paper is a continuation of this work, and deals with expressing the behavior of complex scheduling policies managing shared resources. We provide a synchronous specification for two shared resource scheduling protocols: the well-known basic priority inheritance protocol (BIP), and the priority ceiling protocol (PCP). This results in an automated translation of AADL models into a purely Boolean synchronous (Lustre) scheduler, that can be directly model-checked, possibly with the actual software.

Keywords: Embedded systems, Simulation, Scheduling, Formal Verification, Architecture Description Languages, Synchronous Languages

Reviewers: Florence Maraninchi

Notes:

How to cite this report:

```
@techreport { ,
  title = { Synchronous modeling and validation of schedulers dealing with shared resources3 },
  authors = { Erwan Jahier, Nicolas Halbwachs, Pascal Raymond },
  institution = { Vérimag Research Report },
  number = { TR-2008-10 },
  year = { },
  note = { }
}
```

2014

VERIFICATION OF QUASI-SYNCHRONOUS SYSTEMS WITH UPPAAL

S. Bhattacharyya⁺, S. Miller⁺, J. Yang⁺⁺, S. Smolka⁺⁺, B. Meng⁺⁺⁺, C. Stickse^{l+++}, C. Tinelli⁺⁺⁺

⁺Rockwell Collins, Advanced Technology Center, Cedar Rapids, IA

⁺⁺SUNY, Stony Brook, NY

⁺⁺⁺University of Iowa, Iowa City, IA

Abstract

Modern defense systems are complex distributed software systems implemented over heterogeneous and constantly evolving hardware and software platforms. Distributed agreement protocols are often developed exploiting the fact that their systems are *quasi-synchronous*, where even though the clocks of the different nodes are not synchronized, they all run at the same rate, or multiples of the same rate, modulo their drift and jitter.

This paper describes an effort to provide systems designers and engineers with an intuitive modeling environment that allows them to specify the high-level architecture and synchronization logic of quasi-synchronous systems using widely available systems-engineering notations and tools. To this end, a translator was developed that translates system architectural models specified in a subset of SysML into the Architectural Analysis and Description Language (AADL). Translators were also developed that translate the AADL models into the input language of the Uppaal and Kind model checkers.

The Uppaal model checker. supports the modeling, verification, and validation of real-time systems modeled as a network of timed automata. This paper focuses on the challenges encountered in translating from AADL to Uppaal, and illustrates the overall approach with a common avionics example: the Pilot Flying System.

Keywords: AADL, quasi-synchronous, model checking, verification, Uppaal, Pilot Flying system.

Introduction

Modern defense systems are complex software systems implemented over heterogeneous and constantly evolving hardware and software platforms. Due to the failure rates of individual hardware components, critical functions must be implemented as redundant, fault-tolerant systems in order to meet

their reliability requirements. This is achieved by distributing these functions over multiple processing components connected by fault-tolerant networks. When a system is replicated to achieve a high level of reliability, the individual components still need to agree on some part of the global system state, such as which node is the current leader. While the amount of state that needs to be consistent is often small, the required consistency is essential for the correct behavior of the system.

In developing distributed agreement protocols, engineers often exploit the fact that their systems are *quasi-synchronous*, where even though the clocks of the different nodes are not synchronized, they all run at the same rate, or multiples of the same rate, modulo their drift and jitter. While such designs often appear to work correctly at first, their intrinsic asynchrony makes them prone to race and deadlock conditions. These latent design errors often do not appear until late in system integration or even after the system is deployed.

This paper describes an effort to provide systems designers and engineers with an intuitive modeling environment that allows them to specify the high-level architecture and synchronization logic of quasi-synchronous systems using widely available system-engineering notations and tools. A translator was developed that translates system architectural models specified in a subset of the SysML systems engineering modeling language into the Architectural Analysis and Description Language (AADL). Translators were also developed that translate the AADL models into the input language of the Uppaal [1] and Kind [2] model checkers. Example quasi-synchronous systems were created in SysML and automatically translated into AADL, Kind, and Uppaal. The Kind and Uppaal model checkers were then used to verify these systems' distributed agreement protocols.

978-1-4799-5001-0/14/\$31.00 ©2014 IEEE

8A4-1

Institut National Polytechnique de Grenoble

The Cooking Book

2006

©IEEE Computer Society Press, ACSD'06

Simulation and Verification of Asynchronous Systems by means of a Synchronous Model*

Nicolas Halbwachs and Louis Mandel†
Vérimag‡ Grenoble – France

Abstract

*Synchrony and asynchrony are commonly to each other. Now, in embedded applica- tual solutions are often situated in between, chronous processes composed in a partially asy way. Examples of such intermediate solutions: quasi-synchronous periodic processes, deadline- scheduling... In this paper, we illustrate the use chronous paradigm to model and validate suc asynchronous applications. We show that, throu of sporadic activation of processes and simulati determinism by the way of auxiliary inputs, the sy paradigm allows a precise control of asynchron proach is illustrated on a real case study, propo framework of the European Integrated project *.*

1 Introduction

It is well admitted, now, that the sy paradigm [4, 20] can significantly ease the mod gramming, and validation of embedded system ware. The synchronous parallel composition help turing the model, without introducing non-de The determinism of the model is also an invalua tage for its validation: tests are reproducible, a checking is not faced with the proliferation of st non-deterministic interleaving of processes.

It is also recognized that the synchronous p not the panacea, since it does not directly apply cally asynchronous situations, such as distribute or applications mixing long tasks and urgent s requests. This is why numerous works (see, e.g. synthesis) are devoted to combining synchrony chrony, or to extending the synchronous model to

*This work was partially supported by the European Comu the Integrated Project Assent, IST 004033

†email: {Nicolas.Halbwachs, Louis.Mandel}

‡Verimag is a joint laboratory of Université Joseph Fourie INPG associated with IMAG.

IRIMAG
XTE DE RECHERCHE

2008

Synchronous modeling and validation of schedulers dealing with shared resources²

Erwan Jahier, Nicolas Halbwachs, Pascal Raymond

Jul 17 2008

Abstract

Architecture Description Languages (ADLs) allow embedded systems to be described as assemblies of hardware and software components. It is attractive to use such a global modelling as a basis for early system analysis. However, in such descriptions, the applicative software is often abstracted away, and is supposed to be developed in some host programming language. This forbids to take the applicative software into account in such early validation. To overcome this limitation, a solution consists in translating the ADL description into an executable model, which can be simulated and validated together with the software. In a previous paper [8], we proposed such a translation of AADL (Architecture Analysis & Design Language) specifications into an executable synchronous model. The present paper is a continuation of this work, and deals with expressing the behavior of complex scheduling policies managing shared resources. We provide a synchronous specification for two shared resource scheduling protocols: the well-known basic priority inheritance protocol (BIP), and the priority ceiling protocol (PCP). This results in an automated translation of AADL models into a purely Boolean synchronous (Lustre) scheduler, that can be directly model-checked, possibly with the actual software.

Keywords: Embedded systems, Simulation, Scheduling, Formal Verification, Architecture Descript Languages, Synchronous Languages

Reviewers: Florence Maraninchi

Notes:

How to cite this report:

```
@techreport { ,
  title = { Synchronous modeling and validation of schedulers dealing with shared resources3 },
  authors = { Erwan Jahier, Nicolas Halbwachs, Pascal Raymond },
  institution = { Verimag Research Report },
  number = { TR-2008-10 },
  year = { },
  note = { }
}
```

2014

VERIFICATION OF QUASI-SYNCHRONOUS SYSTEMS WITH UPPAAL

S. Bhattacharyya⁺, S. Miller⁺, J. Yang⁺⁺, S. Smolka⁺⁺, B. Meng⁺⁺⁺, C. Stickse⁺⁺⁺, C. Tinelli⁺⁺⁺

⁺Rockwell Collins, Advanced Technology Center, Cedar Rapids, IA

⁺⁺SUNY, Stony Brook, NY

⁺⁺⁺University of Iowa, Iowa City, IA

Abstract

Modern defense systems are com software systems implemented over and constantly evolving hardware platforms. Distributed agreement prot developed exploiting the fact that th quasi-synchronous, where even thoug the different nodes are not synchroniz at the same rate, or multiples of modulo their drift and jitter.

This paper describes an effort to p designers and engineers with an intu environment that allows them to sp level architecture and synchronization synchronous systems using widely ava engineering notations and tools. T translator was developed that tra architectural models specified in a su into the Architectural Analysis an Language (AADL). Translators were that translate the AADL models language of the Uppaal and Kind mod

The Uppaal model checker, modeling, verification, and validatio systems modeled as a network of ti This paper focuses on the challenges translating from AADL to Uppaal, an overall approach with a common avi the Pilot Flying System.

Keywords: AADL, quasi-synch checking, verification, Uppaal, Pilot F

Introduction

Modern defense systems are cor systems implemented over heter constantly evolving hardware and soft Due to the failure rates of indivi components, critical functions must b as redundant, fault-tolerant systems in

978-1-4799-5001-0/14/\$31.00 ©2014

Institut National Pol

2015



AFRL-RI-RS-TR-2015-171

FORMAL VERIFICATION OF QUASI-SYNCHRONOUS SYSTEMS

ROCKWELL COLLINS

JULY 2015

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ AIR FORCE MATERIEL COMMAND

■ UNITED STATES AIR FORCE

■ ROME, NY 13441

The Cooking Book

For the quasi-synchronous abstraction alone...

2006

©IEEE Computer Society Press, ACSD'06

Simulation and Verification of Asynchronous Systems by means of a Synchronous Model*

Nicolas Halbwachs and Louis Mandel†
Vérimag‡ Grenoble – France

Abstract

Synchrony and asynchrony are commonly to each other. Now, in embedded applica- tual solutions are often situated in between, chronous processes composed in a partially asy way. Examples of such intermediate solutions quasi-synchronous periodic processes, deadline- scheduling... In this paper, we illustrate the use chronous paradigm to model and validate suc asynchronous applications. We show that, throu of sporadic activation of processes and simulati determinism by the way of auxiliary inputs, the sy paradigm allows a precise control of asynchron proach is illustrated on a real case study, propo framework of the European Integrated project *.

1 Introduction

It is well admitted, now, that the sy paradigm [4, 20] can significantly ease the mod gramming, and validation of embedded system ware. The synchronous parallel composition help turing the model, without introducing non-de The determinism of the model is also an invalua tage for its validation: tests are reproducible, a checking is not faced with the proliferation of st non-deterministic interleaving of processes.

It is also recognized that the synchronous p not the panacea, since it does not directly apply cally asynchronous situations, such as distribute or applications mixing long tasks and urgent s requests. This is why numerous works (see, e.g. synthesis) are devoted to combining synchrony chrony, or to extending the synchronous model to

*This work was partially supported by the European Comu the Integrated Project Assent, IST 004033

†email: {Nicolas.Halbwachs, Louis.Mandel}

‡Verimag is a joint laboratory of Université Joseph Fourie INPG associated with IMAG.

VERIMAG
CENTRE DE RECHERCHE

2008

Synchronous modeling and validation of schedulers dealing with shared resources²

Erwan Jahier, Nicolas Halbwachs, Pascal Raymond

Jul 17 2008

Abstract

Architecture Description Languages (ADLs) allow embedded systems to be described as assemblies of hardware and software components. It is attractive to use such a global modelling as a basis for early system analysis. However, in such descriptions, the applicative software is often abstracted away, and is supposed to be developed in some host programming language. This forbids to take the applicative software into account in such early validation. To overcome this limitation, a solution consists in translating the ADL description into an executable model, which can be simulated and validated together with the software. In a previous paper [8], we proposed such a translation of AADL (Architecture Analysis & Design Language) specifications into an executable synchronous model. The present paper is a continuation of this work, and deals with expressing the behavior of complex scheduling policies managing shared resources. We provide a synchronous specification for two shared resource scheduling protocols: the well-known basic priority inheritance protocol (BIP), and the priority ceiling protocol (PCP). This results in an automated translation of AADL models into a purely Boolean synchronous (Lustre) scheduler, that can be directly model-checked, possibly with the actual software.

Keywords: Embedded systems, Simulation, Scheduling, Formal Verification, Architecture Descript Languages, Synchronous Languages

Reviewers: Florence Maraninchi

Notes:

How to cite this report:

```
@techreport { ,
  title = { Synchronous modeling and validation of schedulers dealing with shared resources3 },
  authors = { Erwan Jahier, Nicolas Halbwachs, Pascal Raymond },
  institution = { Verimag Research Report },
  number = { TR-2008-10 },
  year = { },
  note = { }
}
```

2014

VERIFICATION OF QUASI-SYNCHRONOUS SYSTEMS WITH UPPAAL

S. Bhattacharyya⁺, S. Miller⁺, J. Yang⁺⁺, S. Smolka⁺⁺, B. Meng⁺⁺⁺, C. Stickse⁺⁺⁺, C. Tinelli⁺⁺⁺

⁺Rockwell Collins, Advanced Technology Center, Cedar Rapids, IA

⁺⁺SUNY, Stony Brook, NY

⁺⁺⁺University of Iowa, Iowa City, IA

Abstract

Modern defense systems are com software systems implemented over and constantly evolving hardware platforms. Distributed agreement prot developed exploiting the fact that th quasi-synchronous, where even thoug the different nodes are not synchroniz at the same rate, or multiples of modulo their drift and jitter.

This paper describes an effort to p designers and engineers with an intu environment that allows them to sp level architecture and synchronization synchronous systems using widely av engineering notations and tools. T translator was developed that tra architectural models specified in a su into the Architectural Analysis an Language (AADL). Translators were that translate the AADL models language of the Uppaal and Kind mod

The Uppaal model checker, modeling, verification, and validatio systems modeled as a network of ti This paper focuses on the challenges translating from AADL to Uppaal, an overall approach with a common avi the Pilot Flying System.

Keywords: AADL, quasi-synch checking, verification, Uppaal, Pilot F

Introduction

Modern defense systems are co systems implemented over heter constantly evolving hardware and soft Due to the failure rates of indivi components, critical functions must b as redundant, fault-tolerant systems in

978-1-4799-5001-0/14/\$31.00 ©2014

Institut National Pol

2015



AFRL-RI-RS-TR-2015-171

FORMAL VERIFICATION OF QUASI-SYNCHRONOUS SYSTEMS

ROCKWELL COLLINS

JULY 2015

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

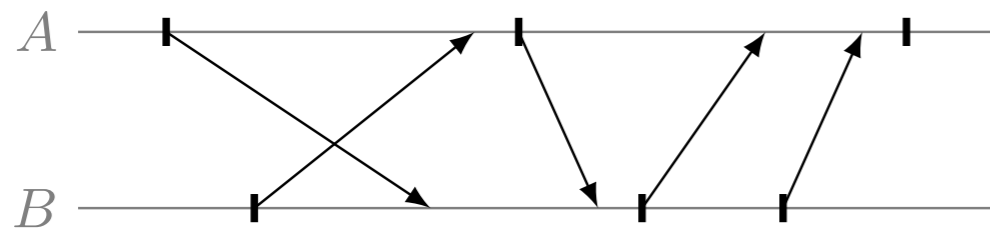
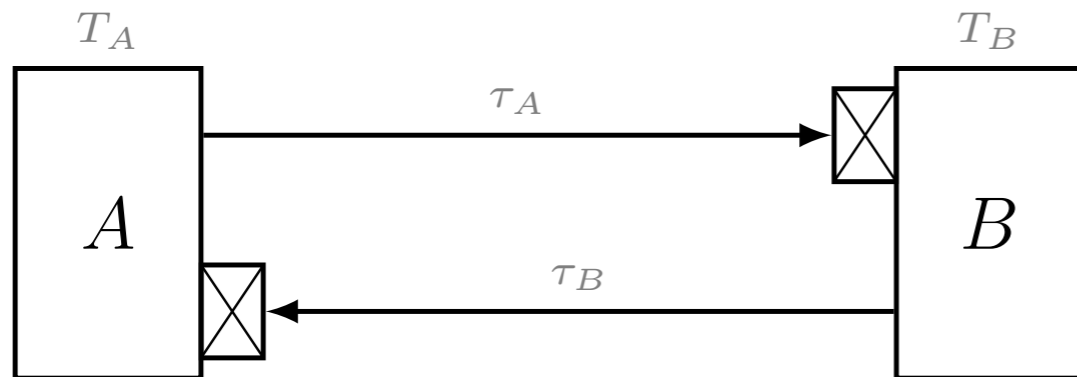
AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ AIR FORCE MATERIEL COMMAND ■ UNITED STATES AIR FORCE ■ ROME, NY 13441

The Big Picture

$$0 < T_{\min} \leq T_A, T_B \leq T_{\max}$$

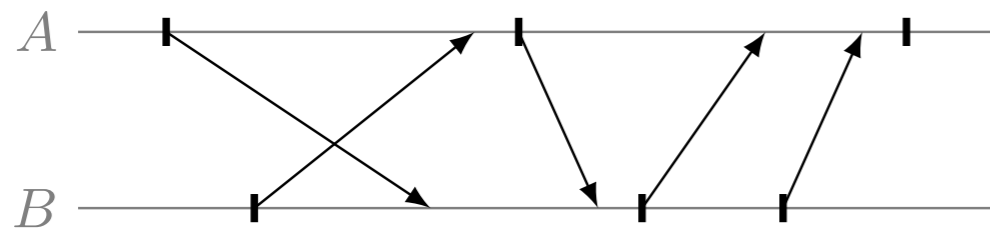
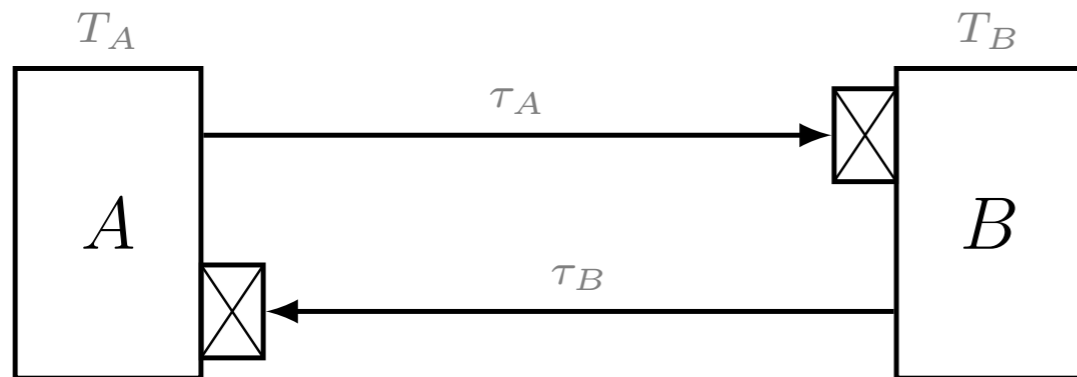
$$0 < \tau_{\min} \leq \tau_A, \tau_B \leq \tau_{\max}$$



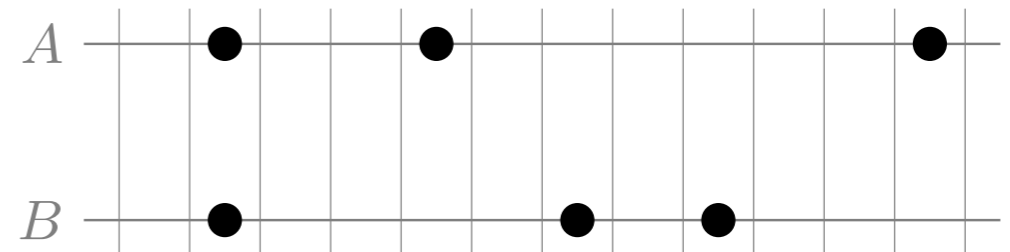
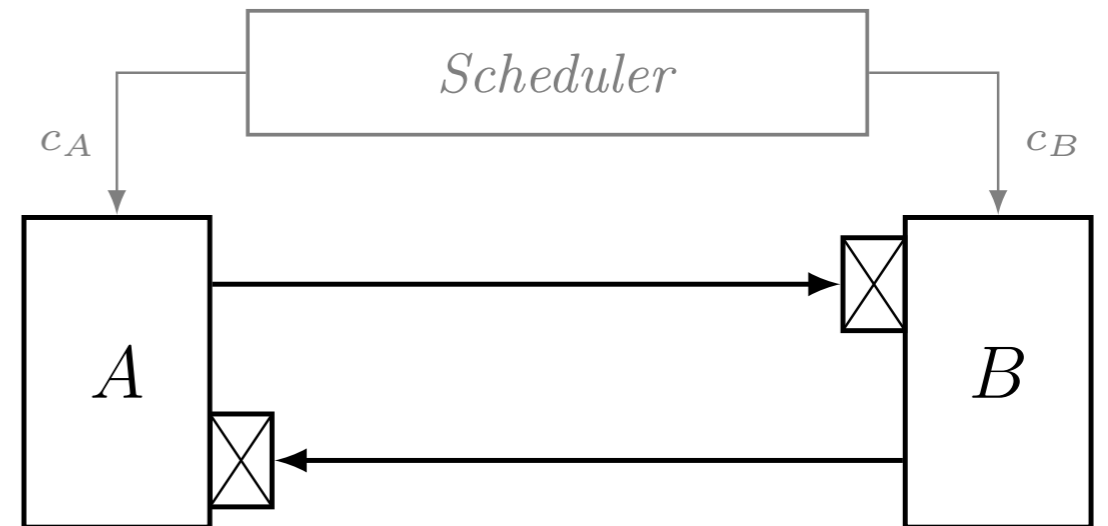
Real-time Model (RT)

The Big Picture

$$0 < T_{\min} \leq T_A, T_B \leq T_{\max}$$
$$0 < \tau_{\min} \leq \tau_A, \tau_B \leq \tau_{\max}$$



Real-time Model (RT)

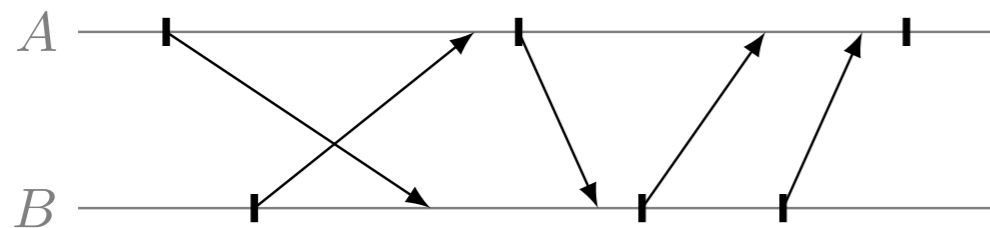
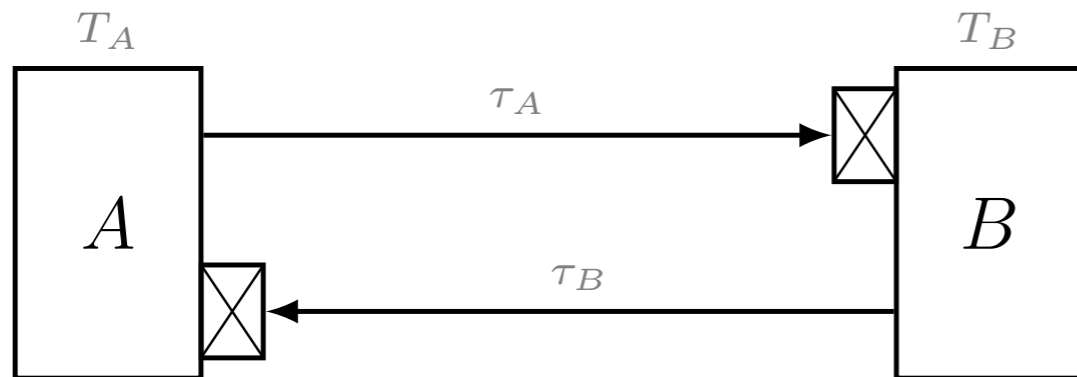


Discrete-time Model (DT)

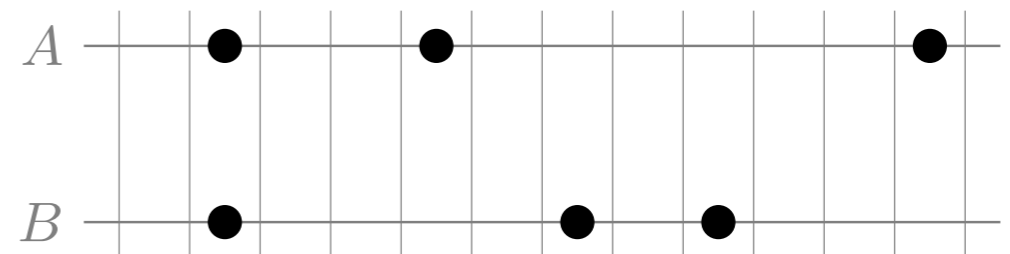
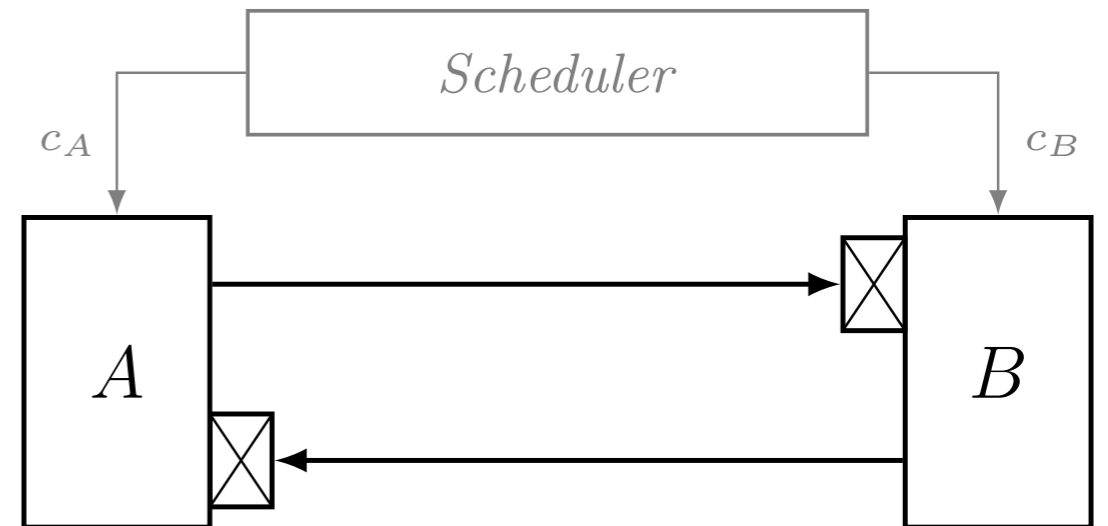
The Big Picture

$$0 < T_{\min} \leq T_A, T_B \leq T_{\max}$$

$$0 < \tau_{\min} \leq \tau_A, \tau_B \leq \tau_{\max}$$



Real-time Model (RT)



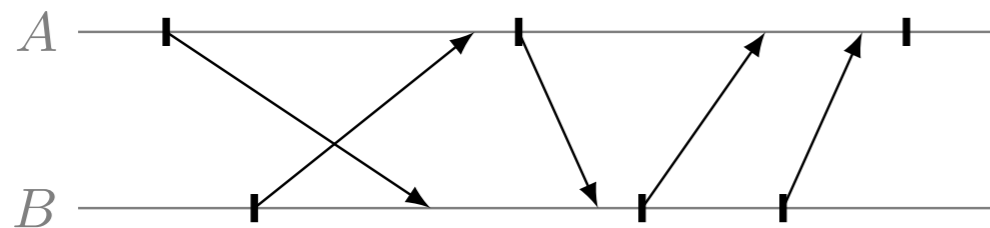
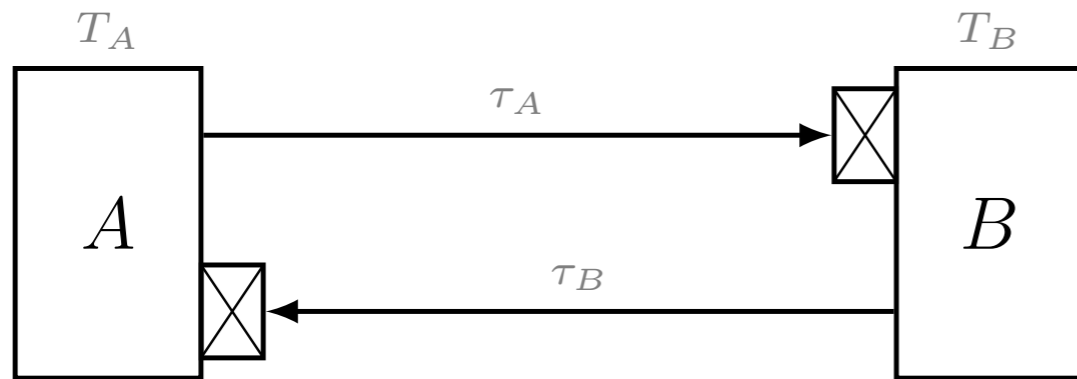
Discrete-time Model (DT)

$$DT \models \varphi$$

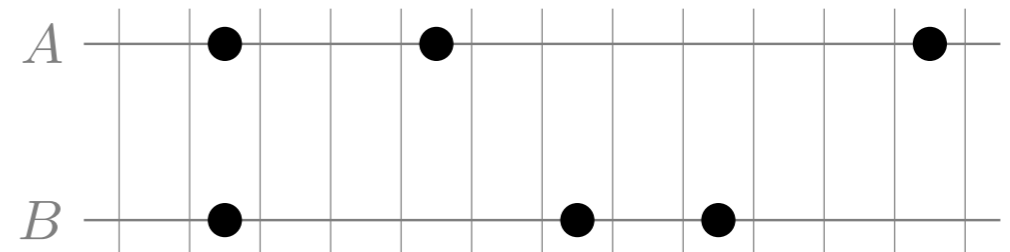
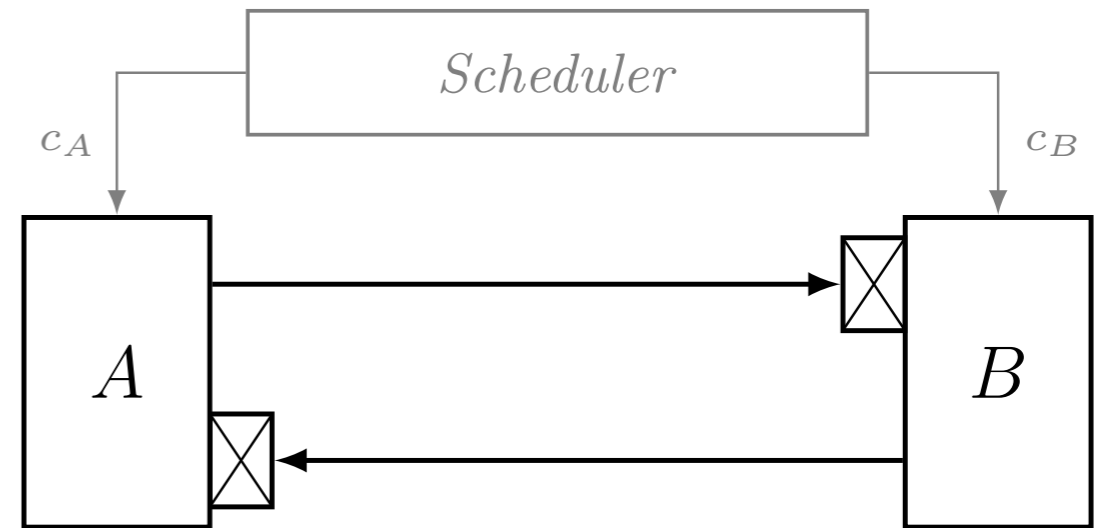
The Big Picture

$$0 < T_{\min} \leq T_A, T_B \leq T_{\max}$$

$$0 < \tau_{\min} \leq \tau_A, \tau_B \leq \tau_{\max}$$



Real-time Model (RT)



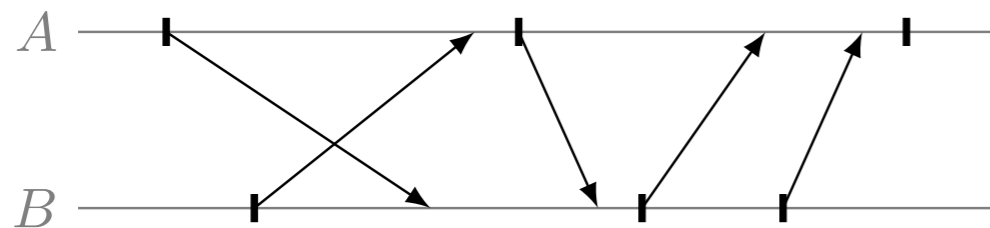
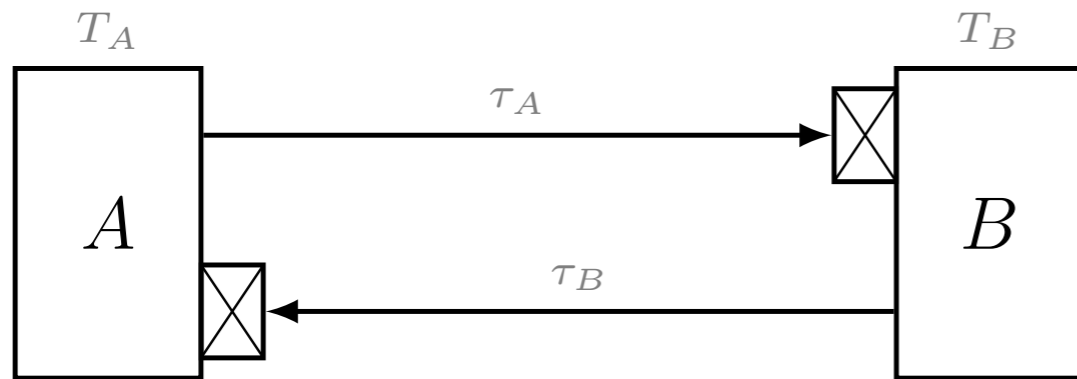
Discrete-time Model (DT)

$$RT \models \varphi \quad \longleftrightarrow \quad DT \models \varphi$$

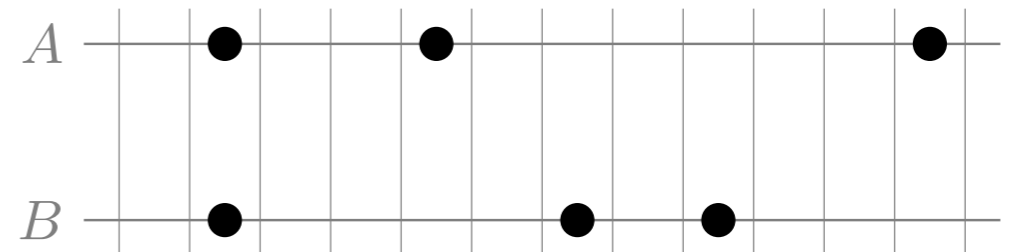
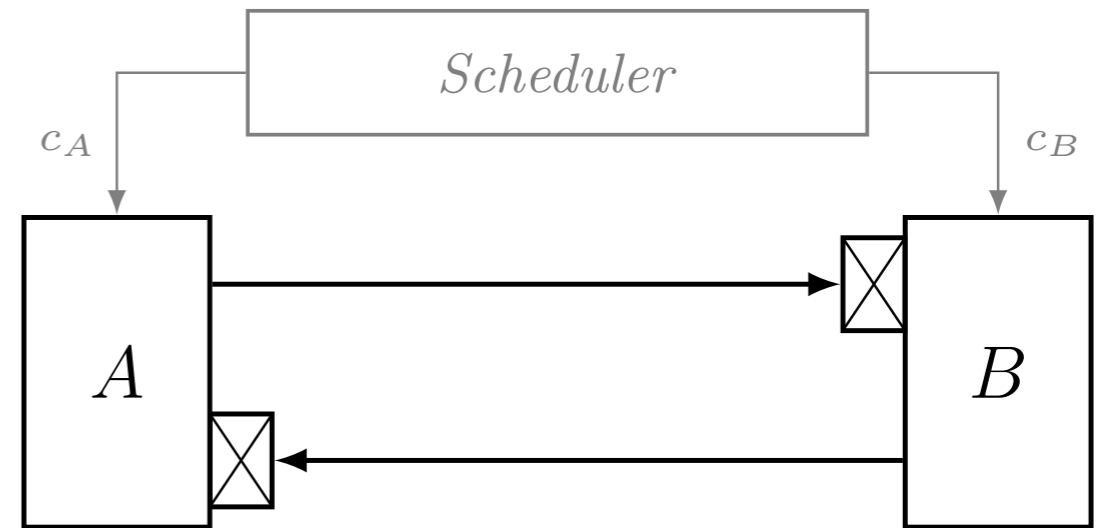
The Big Picture

$$0 < T_{\min} \leq T_A, T_B \leq T_{\max}$$

$$0 < \tau_{\min} \leq \tau_A, \tau_B \leq \tau_{\max}$$



Real-time Model (RT)



Discrete-time Model (DT)

$$RT \models \varphi$$

Soundness

$$DT \models \varphi$$

Quasi-Periodic Architectures

Property 1. *First, we assume that every process P is periodic with a period varying between small margins:*

$$T_{Pm} \leq T_P \leq T_{PM}$$

Definition (Quasi-Periodic Architecture):

- A set of “quasi-periodic” processes with local clocks and nominal period T^n (jitter ε)

$$0 < T_{\min} \leq T^n \leq T_{\max} \quad \text{or} \\ T^n - \varepsilon \leq \kappa_i - \kappa_{i-1} \leq T^n + \varepsilon$$

$(\kappa_i)_{i \in \mathbb{N}}$ clock activations

- Buffered communication without message inversion or loss
- Bounded communication delay

$$\tau_{\min} \leq \tau \leq \tau_{\max}$$

Quasi-Periodic Architectures

Property 1. *First, we assume that every process P is periodic with a period varying between small margins:*

$$T_{Pm} \leq T_P \leq T_{PM}$$

Definition (Trace): A (quasi-periodic) trace \mathcal{E} is a set of activation events $\{A_i \mid A \in \mathcal{N} \wedge i \in \mathbb{N}\}$ and two functions

- $t(A_i)$ the date of event
- $\tau(A_i, B)$ the transmission delay of message sent at A_i to B

For a quasi-periodic trace we have

$$\begin{aligned} 0 < T_{min} &\leq t(A_{i+1}) - t(A_i) \leq T_{max}, \\ 0 < \tau_{min} &\leq \tau(A_i, B) \leq \tau_{max}. \end{aligned}$$

Quasi-Periodic Architectures

Property 1. *First, we assume that every process P is periodic with a period varying between small margins:*

$$T_{Pm} \leq T_P \leq T_{PM}$$

Definition (Happened Before): For a trace \mathcal{E} , let \rightarrow be the smallest relation on activation events that satisfies

(local) If $i \leq 0$, $A_i \rightarrow A_{i+1}$.

(recv) If $t(A_i) + \tau(A_i, B) \leq t(B_j)$ then $A_i \rightarrow B_j$

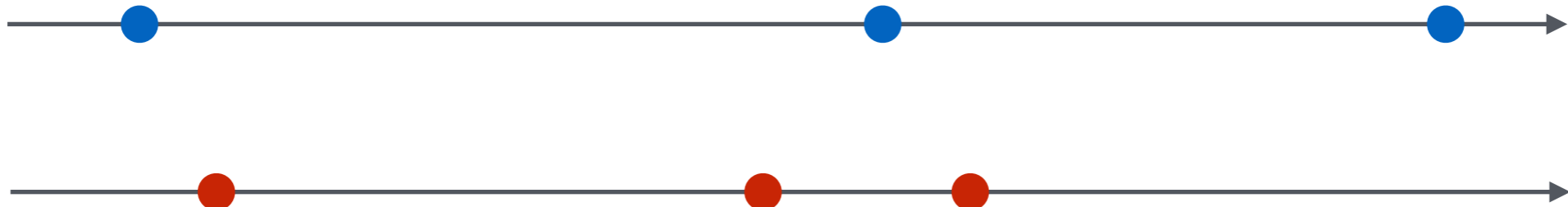
Node are only triggered by their local clock

Message receptions are not explicitly modelled.

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

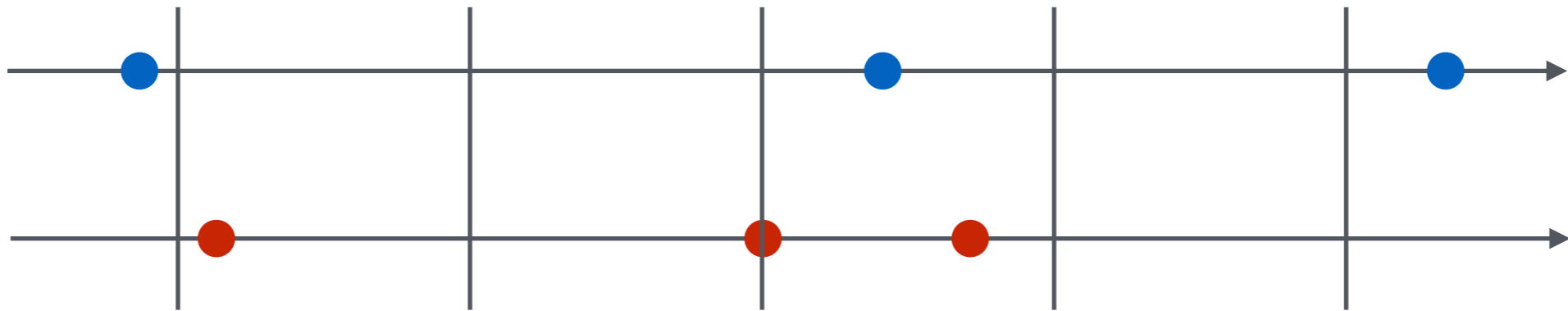
Periodic sampling?



Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

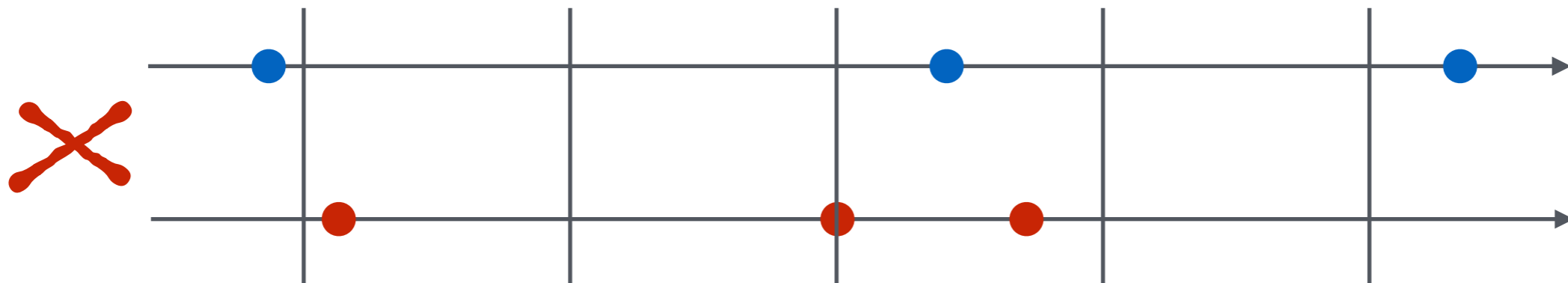
Periodic sampling?



Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

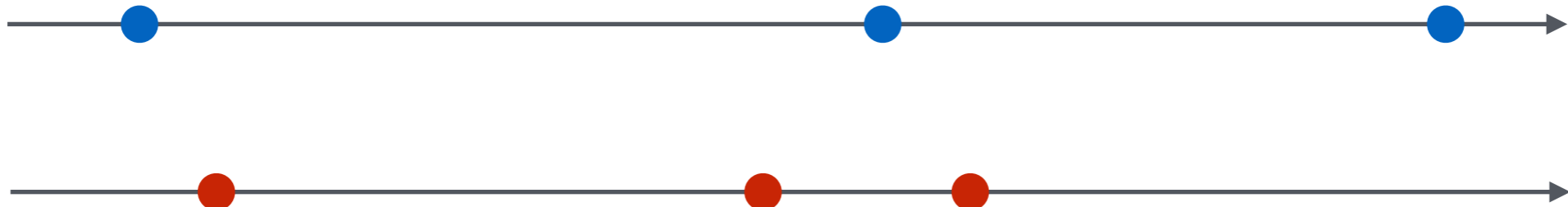
Periodic sampling?



Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

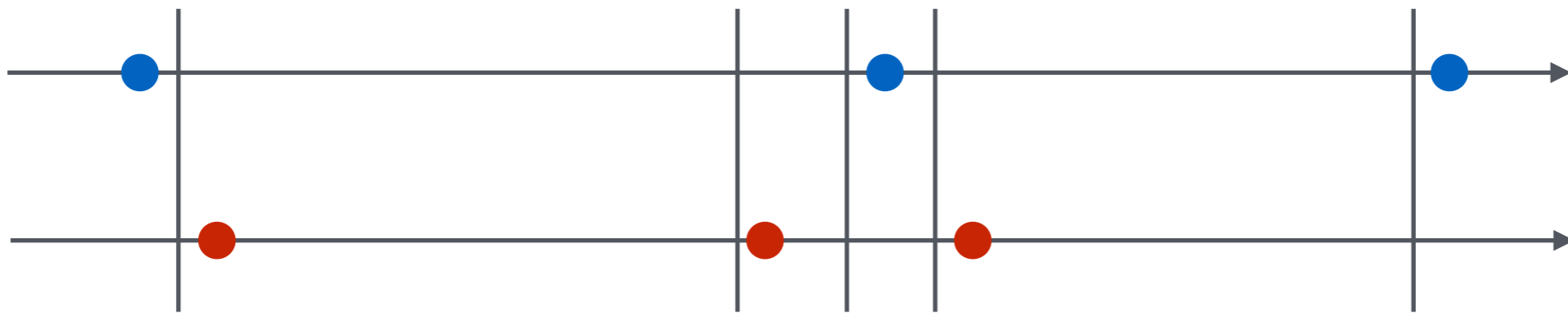
Event-driven sampling?



Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?

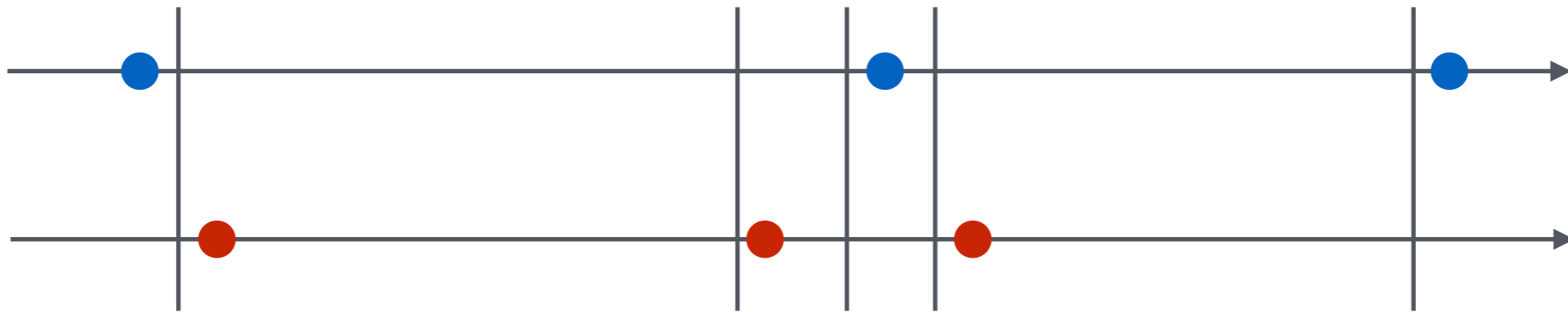


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?

Something is missing...

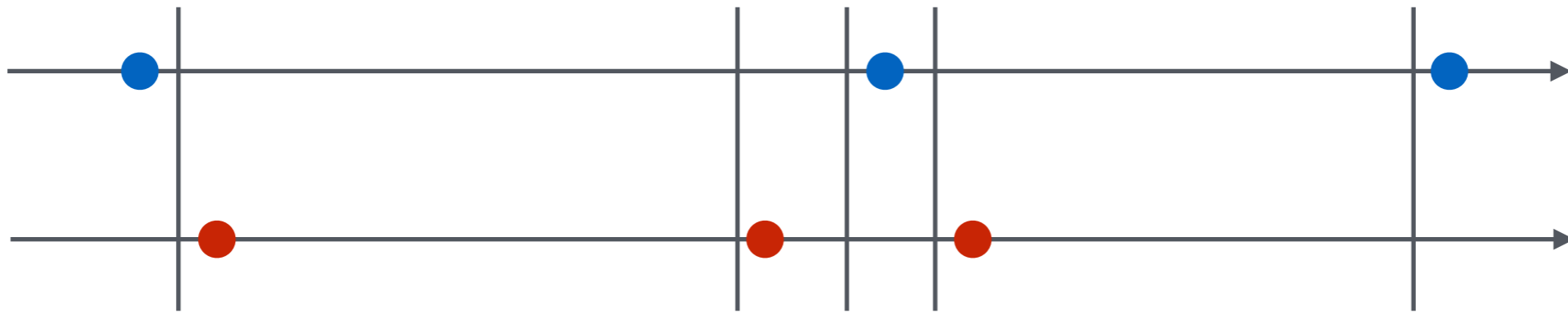


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?

Something is missing...



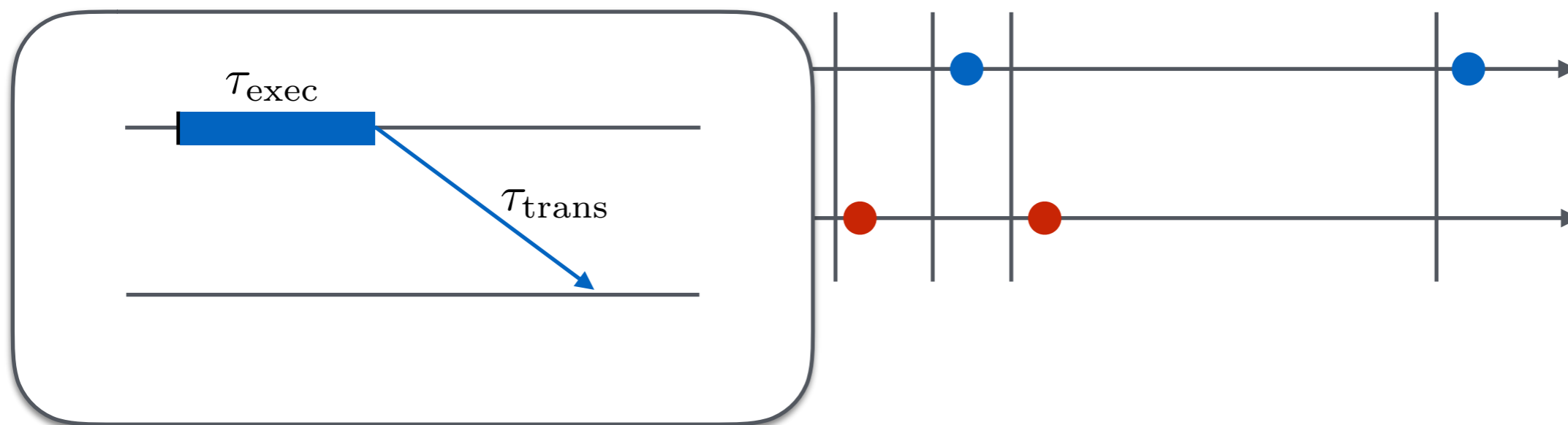
What about execution and transmission time?

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?

Something is missing...



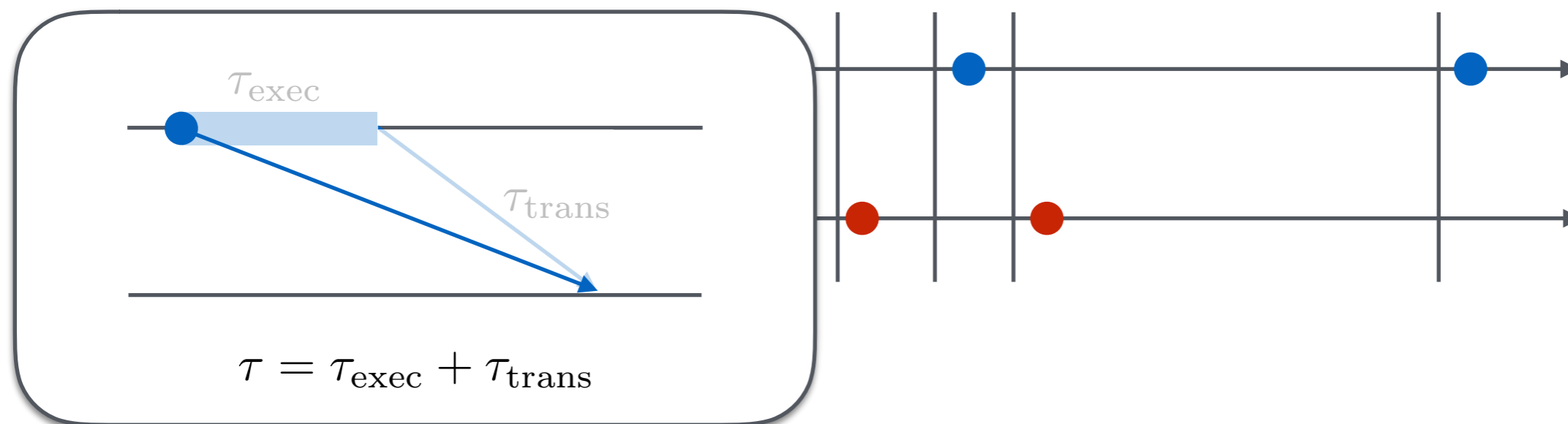
What about execution and transmission time?

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?

Something is missing...

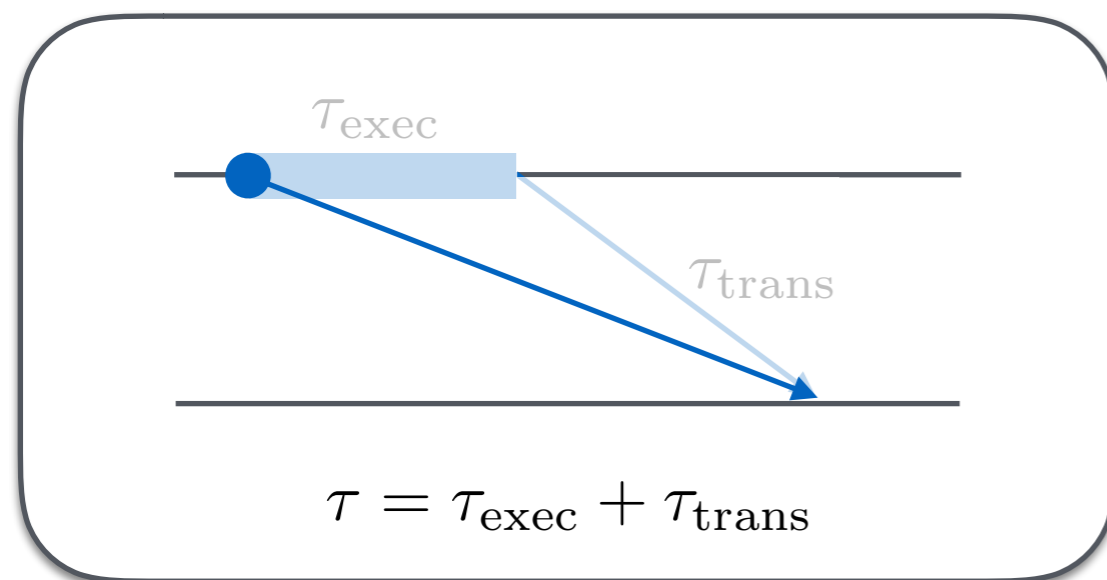


What about execution and transmission time?

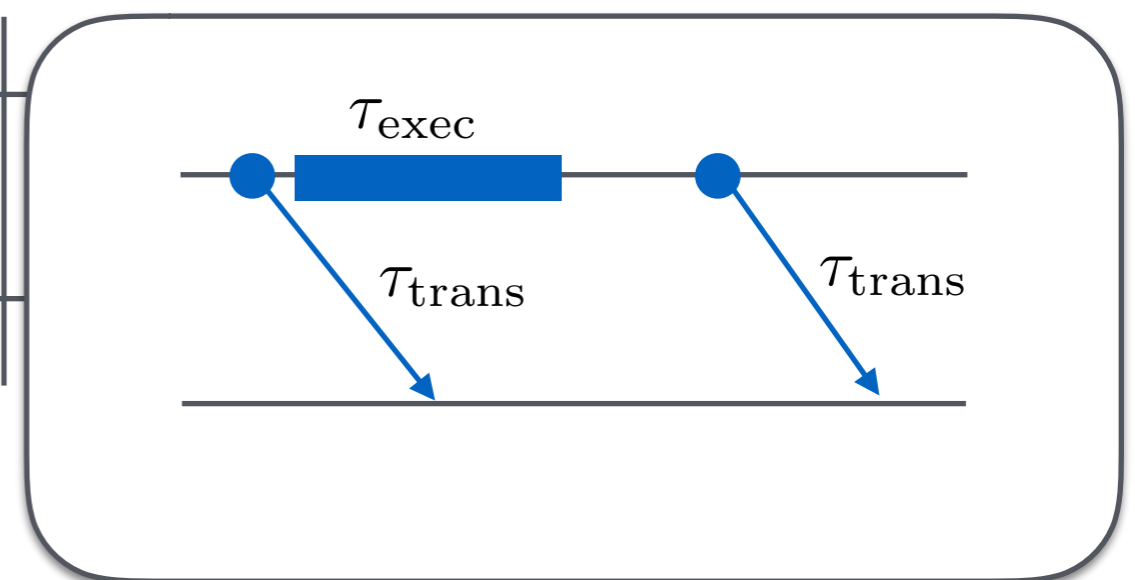
Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?



Something is missing...

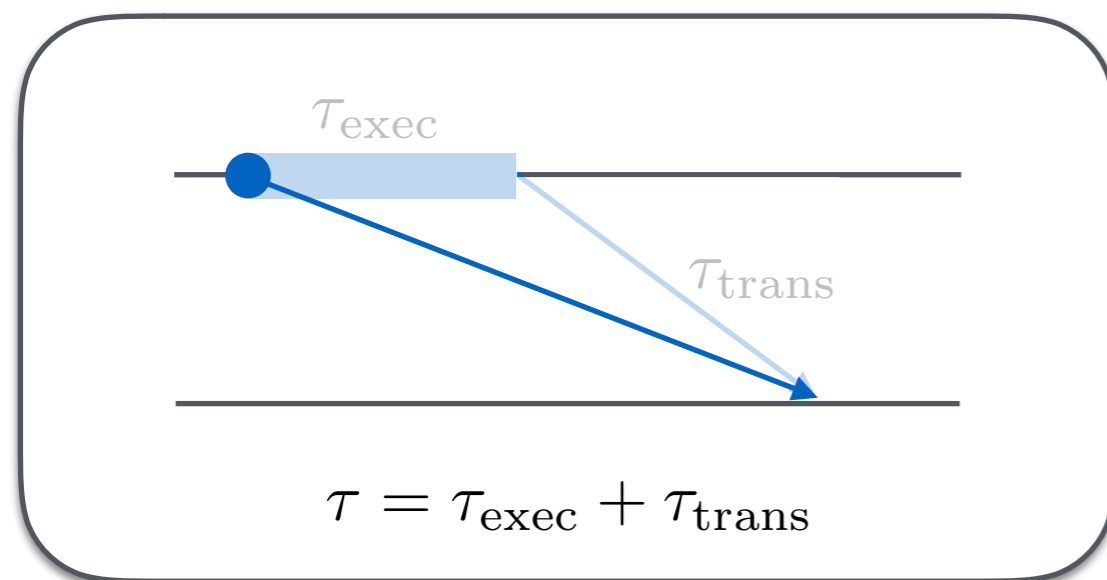


What about execution and transmission time?

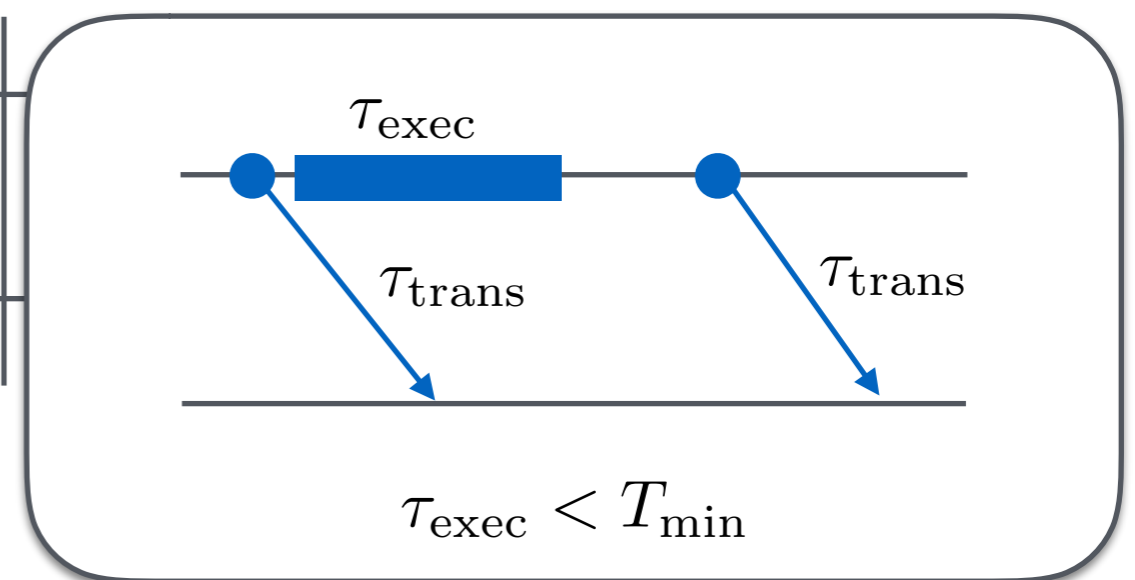
Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?



Something is missing...

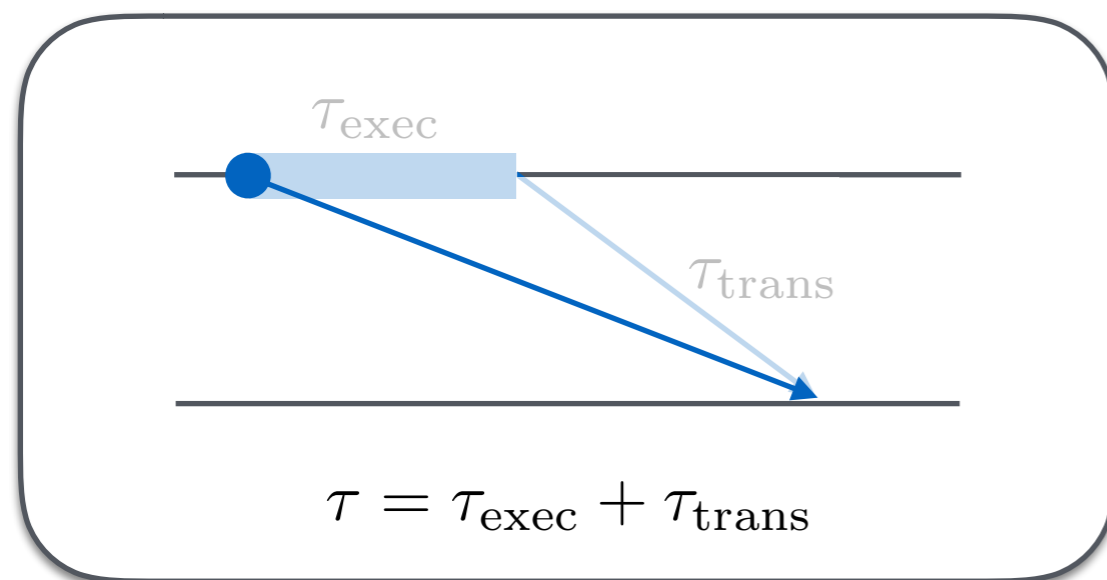


What about execution and transmission time?

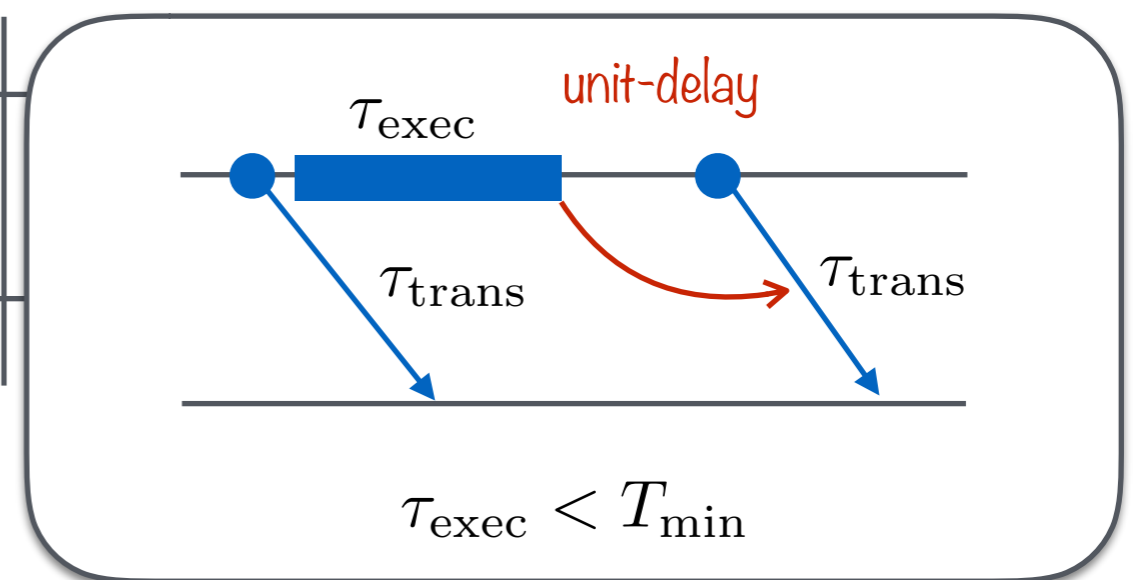
Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?



Something is missing...

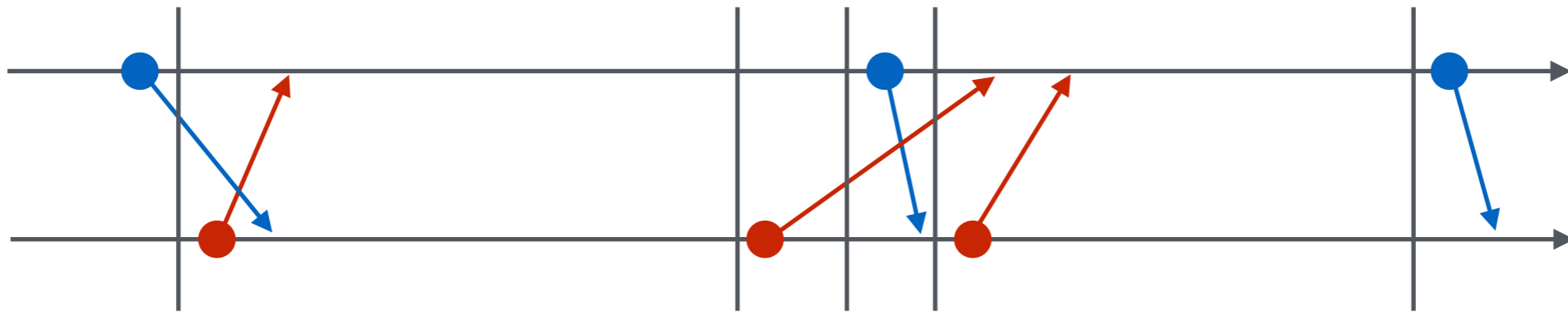


What about execution and transmission time?

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

Event-driven sampling?

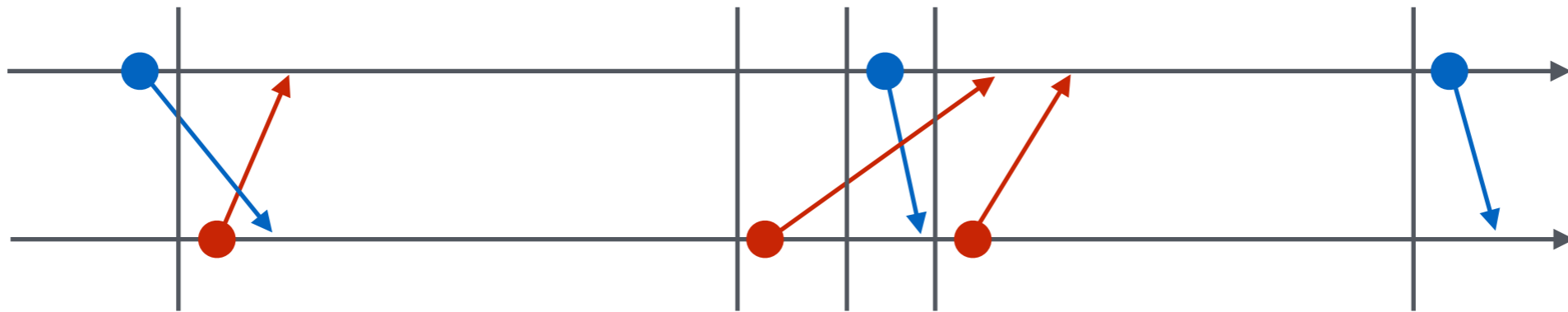


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Event-driven sampling?

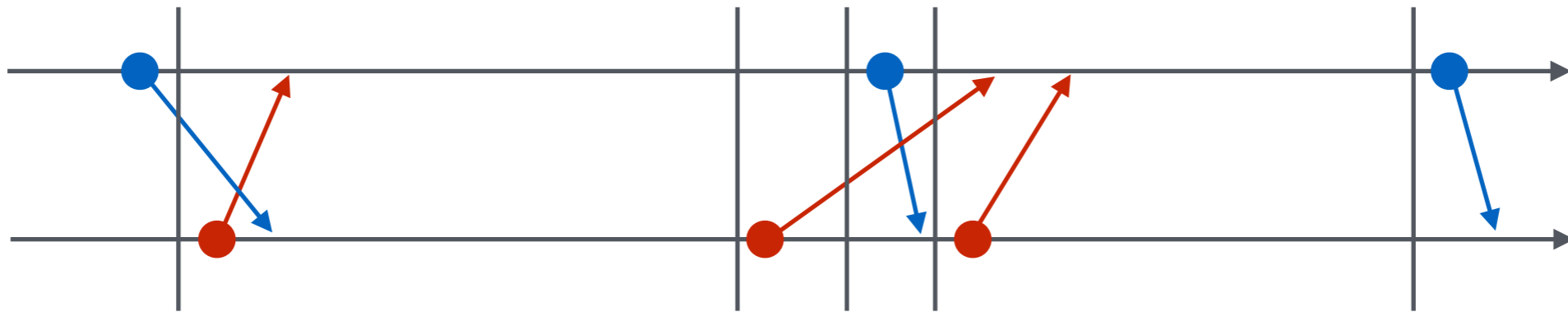


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Event-driven sampling?



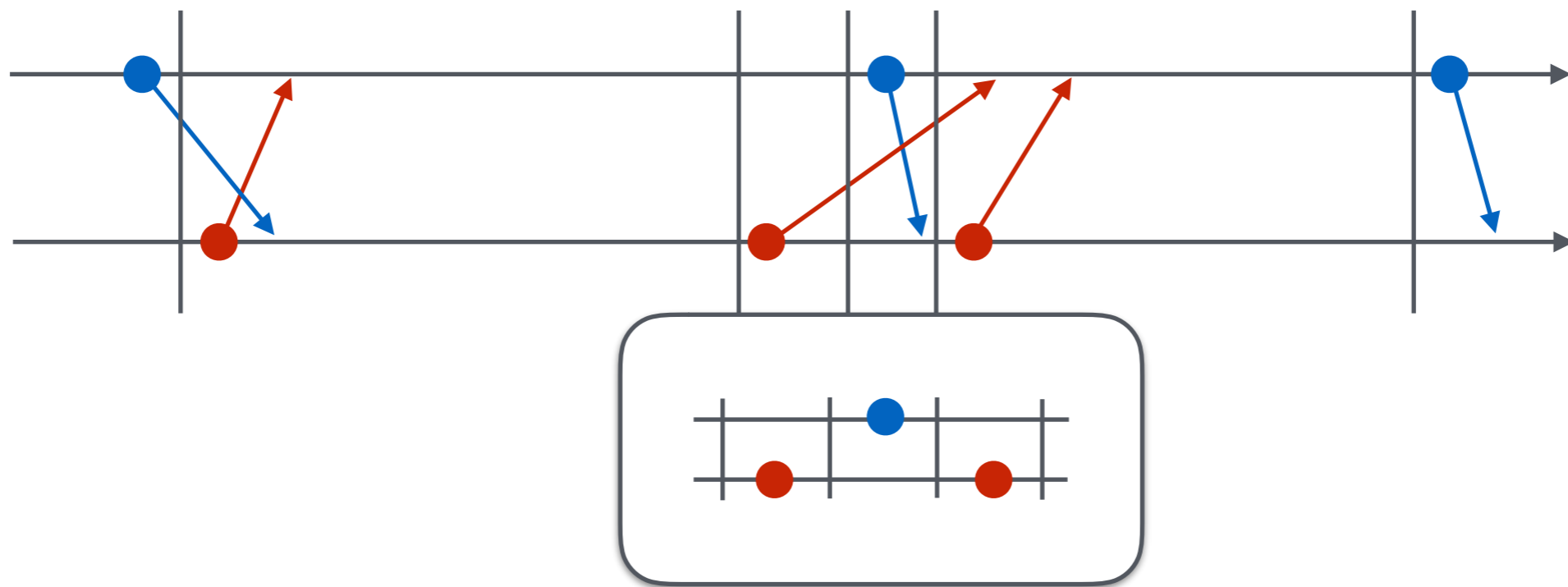
Half the events: much less possible interleavings

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Event-driven sampling?



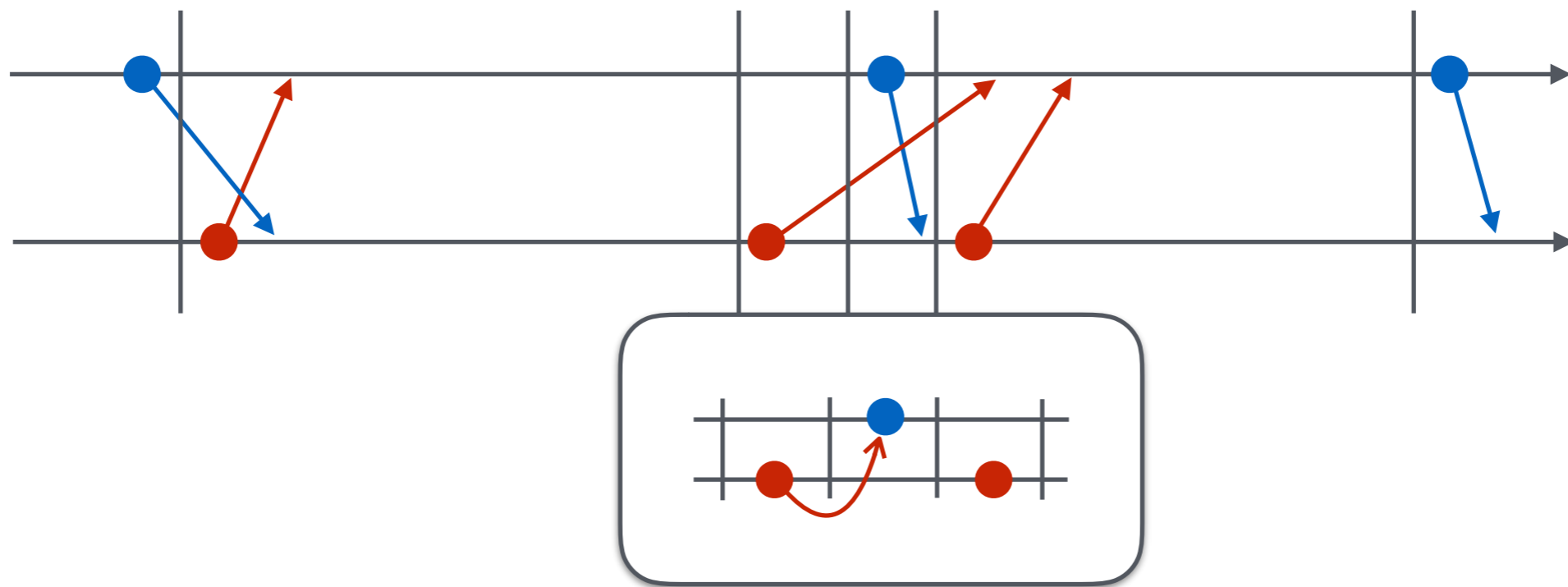
Half the events: much less possible interleavings

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Event-driven sampling?



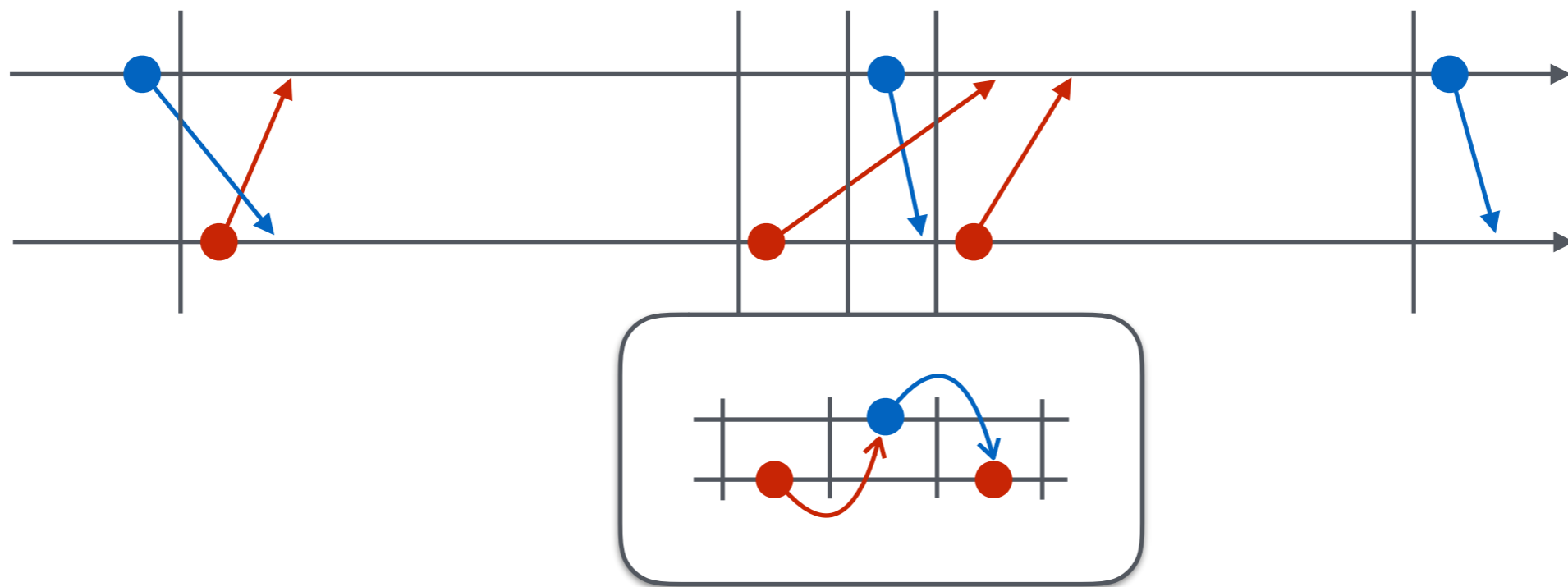
Half the events: much less possible interleavings

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Event-driven sampling?



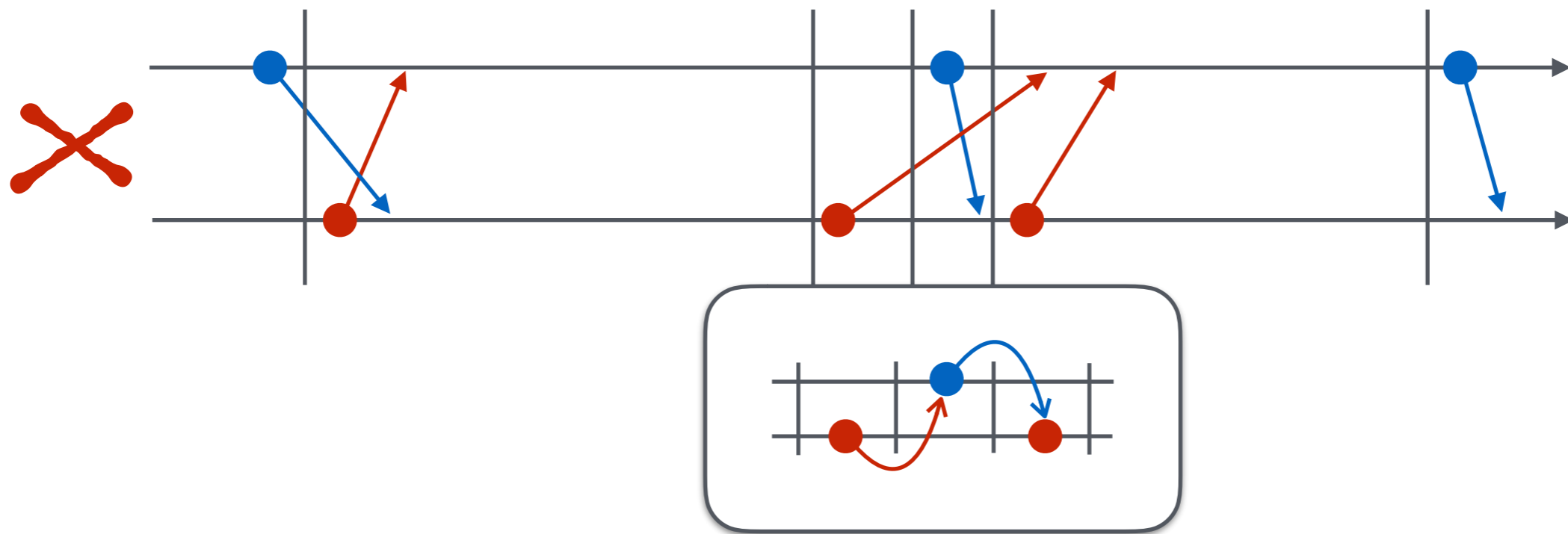
Half the events: much less possible interleavings

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Event-driven sampling?



Half the events: much less possible interleavings

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Definition (Unitary Discretization): A function $f : \mathcal{E} \rightarrow \mathbb{N}$ that assigns each event in a (real-time) trace to a logical instant of a corresponding discrete trace, is a *unitary discretization* if:

$$\forall A_i, B_j \in \mathcal{E}, A_i \rightarrow B_j \iff f(A_i) < f(B_j) \text{ and } A \rightrightarrows B$$

$A \rightrightarrows B$ Node A communicate with node B

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Definition (Unitary Discretization): A function $f : \mathcal{E} \rightarrow \mathbb{N}$ that assigns each event in a (real-time) trace to a logical instant of a corresponding discrete trace, is a *unitary discretization* if:

$$\forall A_i, B_j \in \mathcal{E}, A_i \rightarrow B_j \iff f(A_i) < f(B_j) \text{ and } A \rightrightarrows B$$

$A \rightrightarrows B$ Node A communicate with node B

Map real-time and synchronous causality

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Definition (Unitary Discretization): A function $f : \mathcal{E} \rightarrow \mathbb{N}$ that assigns each event in a (real-time) trace to a logical instant of a corresponding discrete trace, is a *unitary discretization* if:

$$\forall A_i, B_j \in \mathcal{E}, A_i \rightarrow B_j \iff f(A_i) < f(B_j) \text{ and } A \Rightarrow B$$

$A \Rightarrow B$ Node A communicate with node B

Map **real-time** and synchronous causality

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Definition (Unitary Discretization): A function $f : \mathcal{E} \rightarrow \mathbb{N}$ that assigns each event in a (real-time) trace to a logical instant of a corresponding discrete trace, is a *unitary discretization* if:

$$\forall A_i, B_j \in \mathcal{E}, A_i \rightarrow B_j \iff f(A_i) < f(B_j) \text{ and } A \Rightarrow B$$

$A \Rightarrow B$ Node A communicate with node B

Map **real-time** and **synchronous** causality

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Definition (Unitary Discretization): A function $f : \mathcal{E} \rightarrow \mathbb{N}$ that assigns each event in a (real-time) trace to a logical instant of a corresponding discrete trace, is a *unitary discretization* if:

$$\forall A_i, B_j \in \mathcal{E}, A_i \rightarrow B_j \iff f(A_i) < f(B_j) \text{ and } A \Rightarrow B$$

$A \Rightarrow B$ Node A communicate with node B

Map real-time and synchronous causality

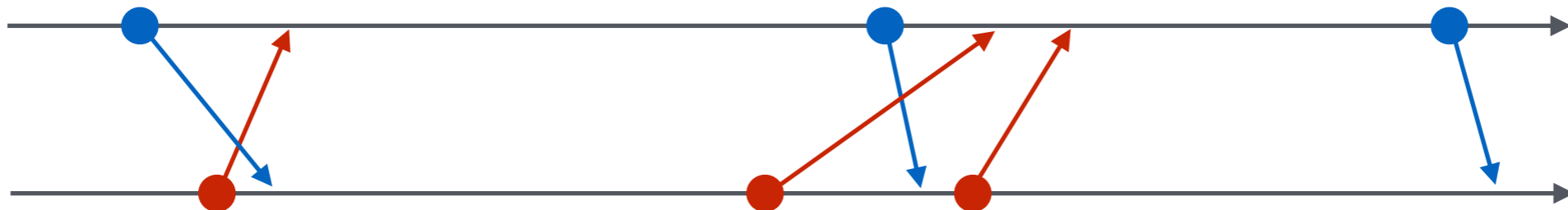
Problem: Are quasi-periodic architectures unitary discretizable?

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

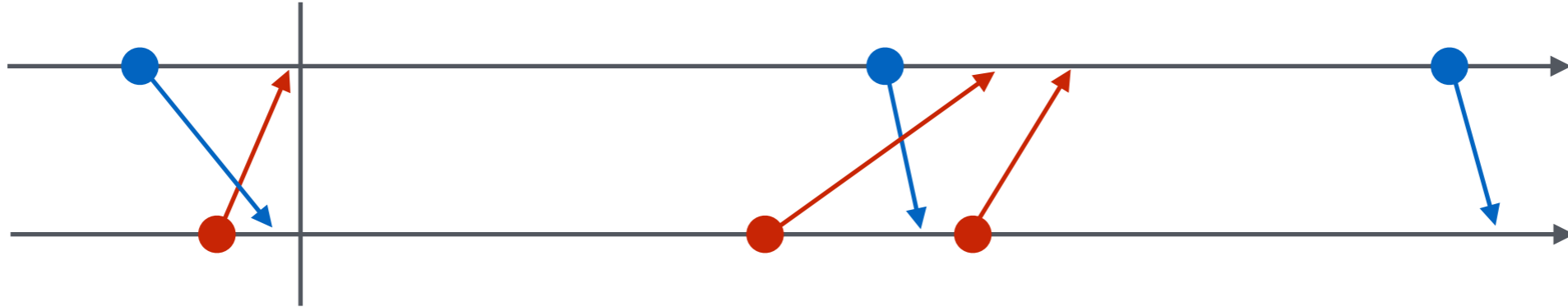


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

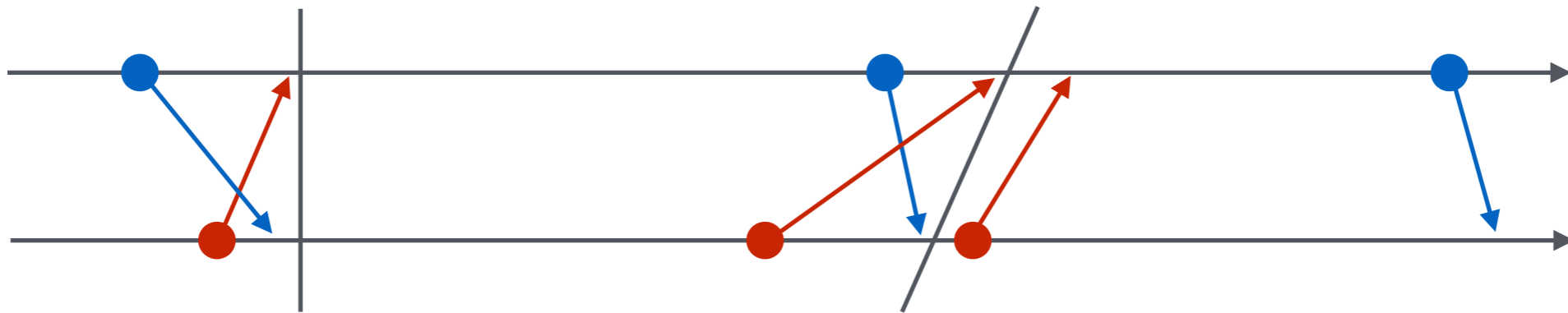


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

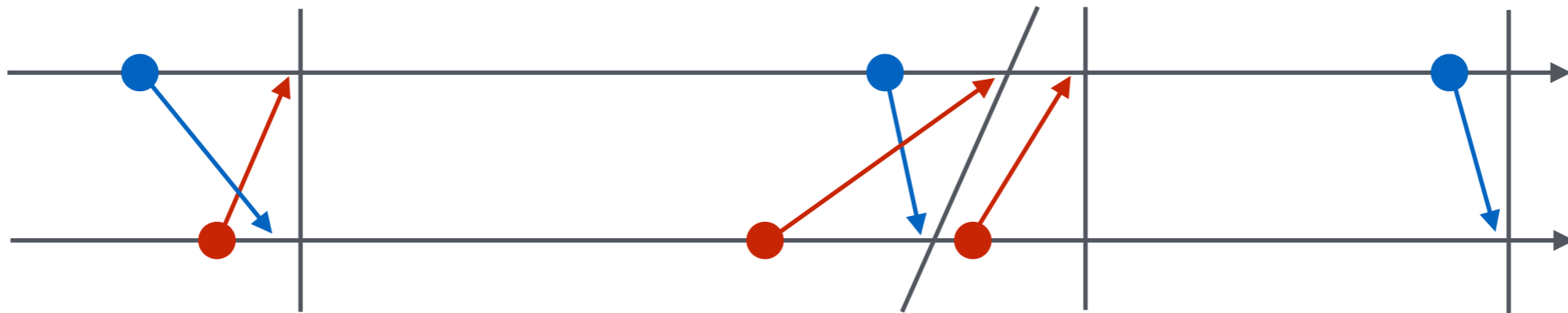


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

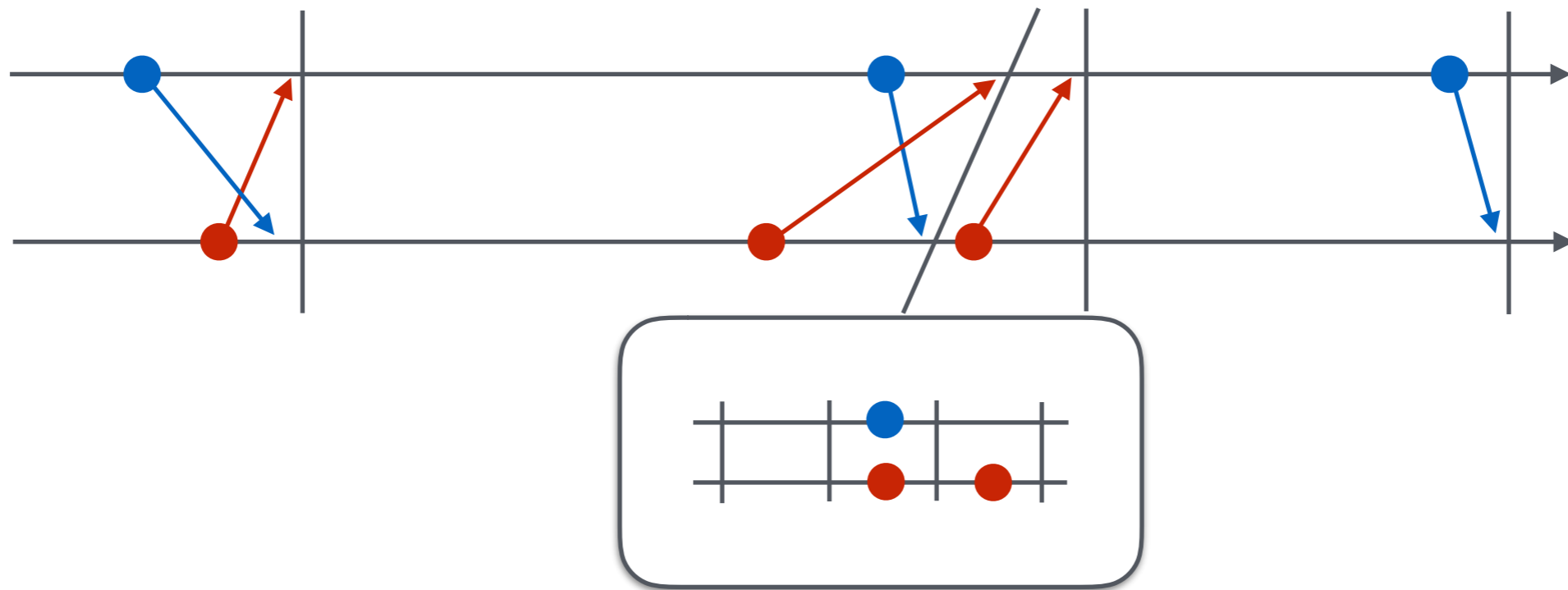


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

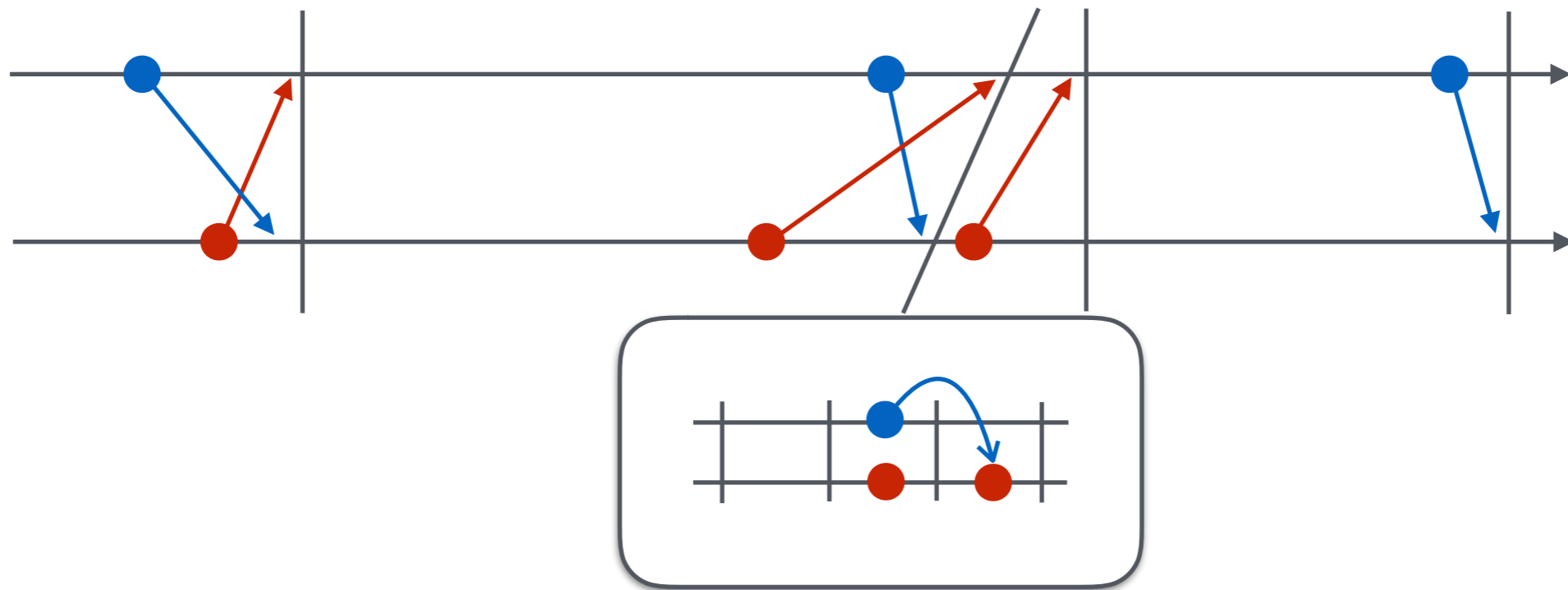


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

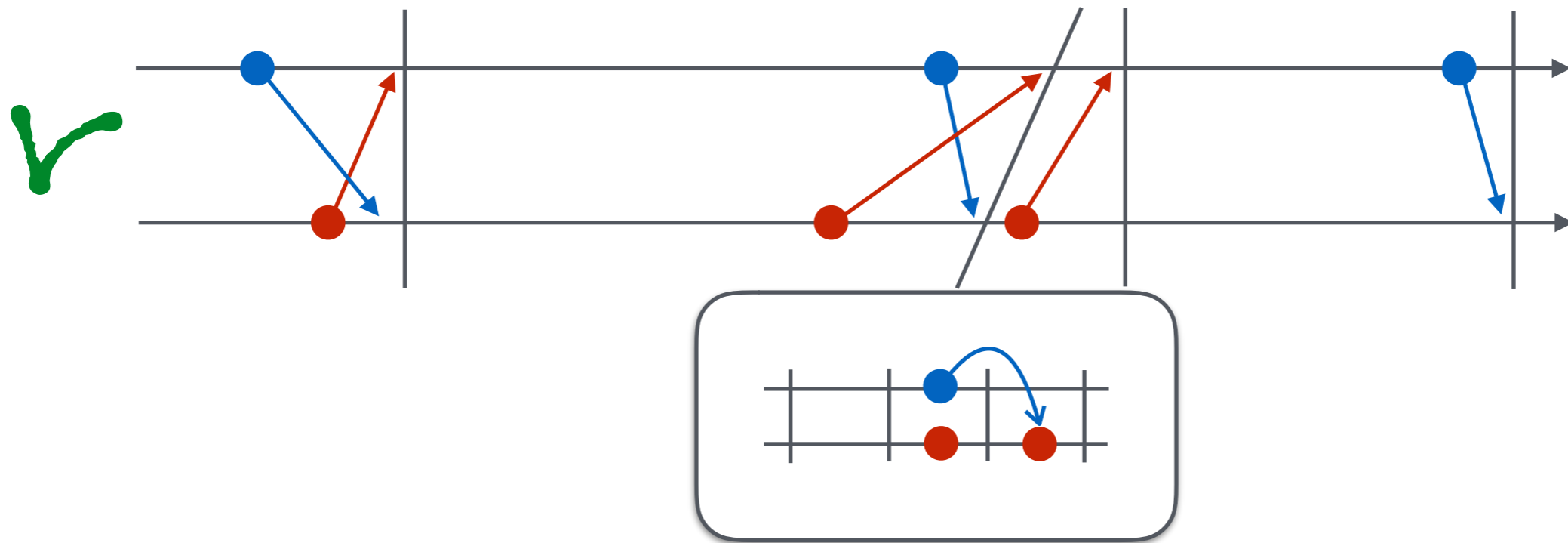


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

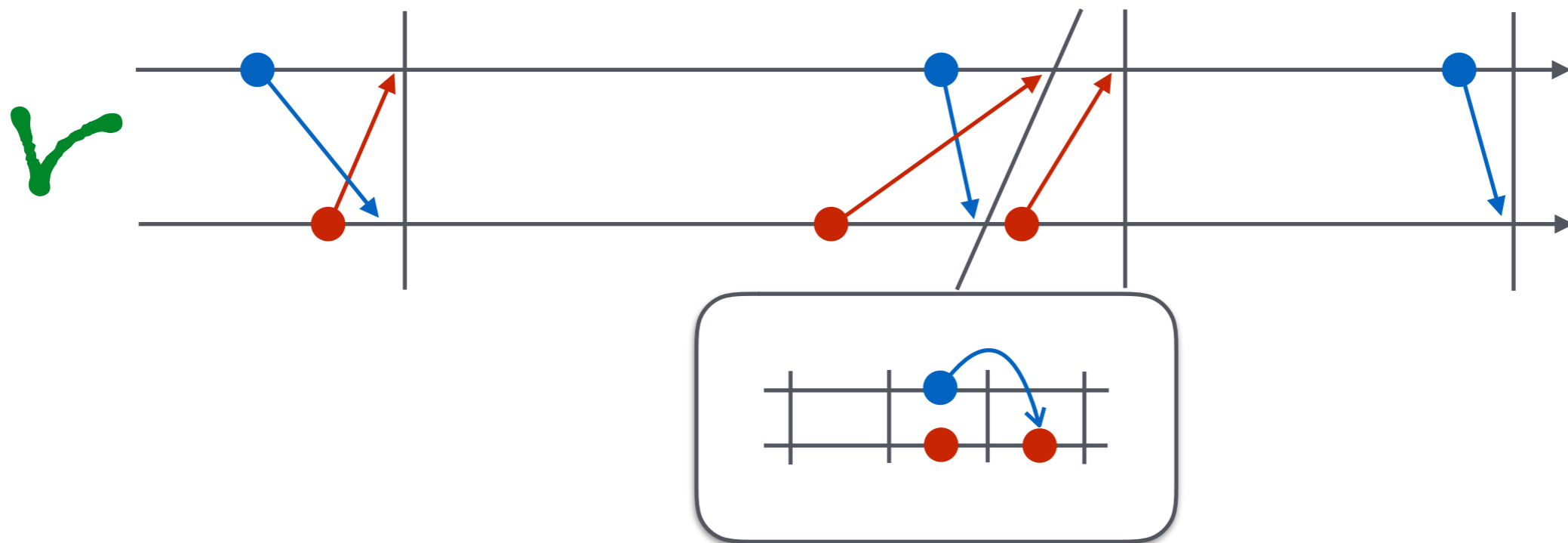


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?



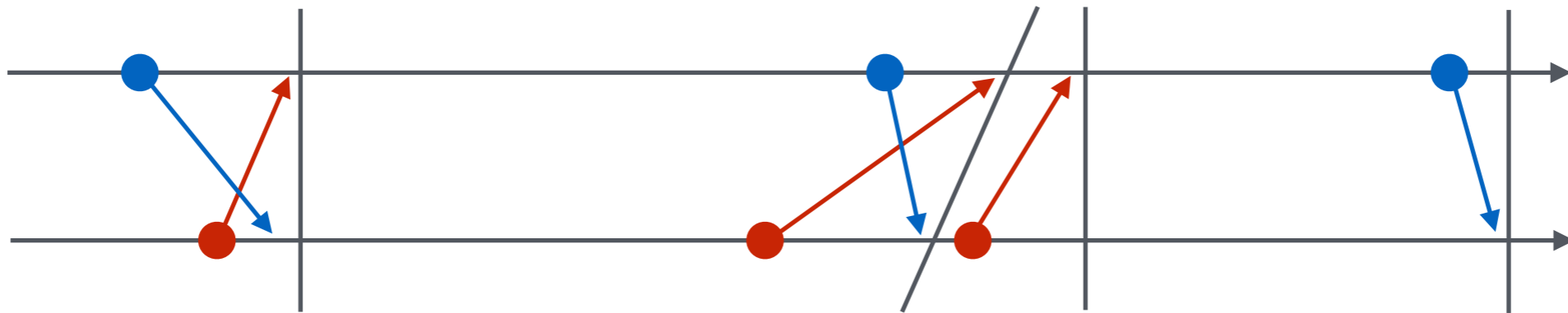
We loose the link between discrete- and real-time

Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

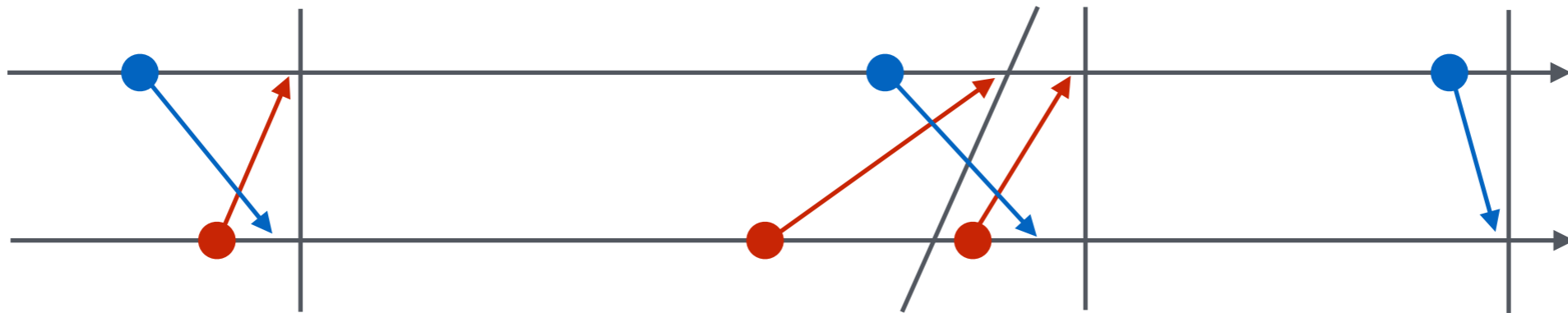


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

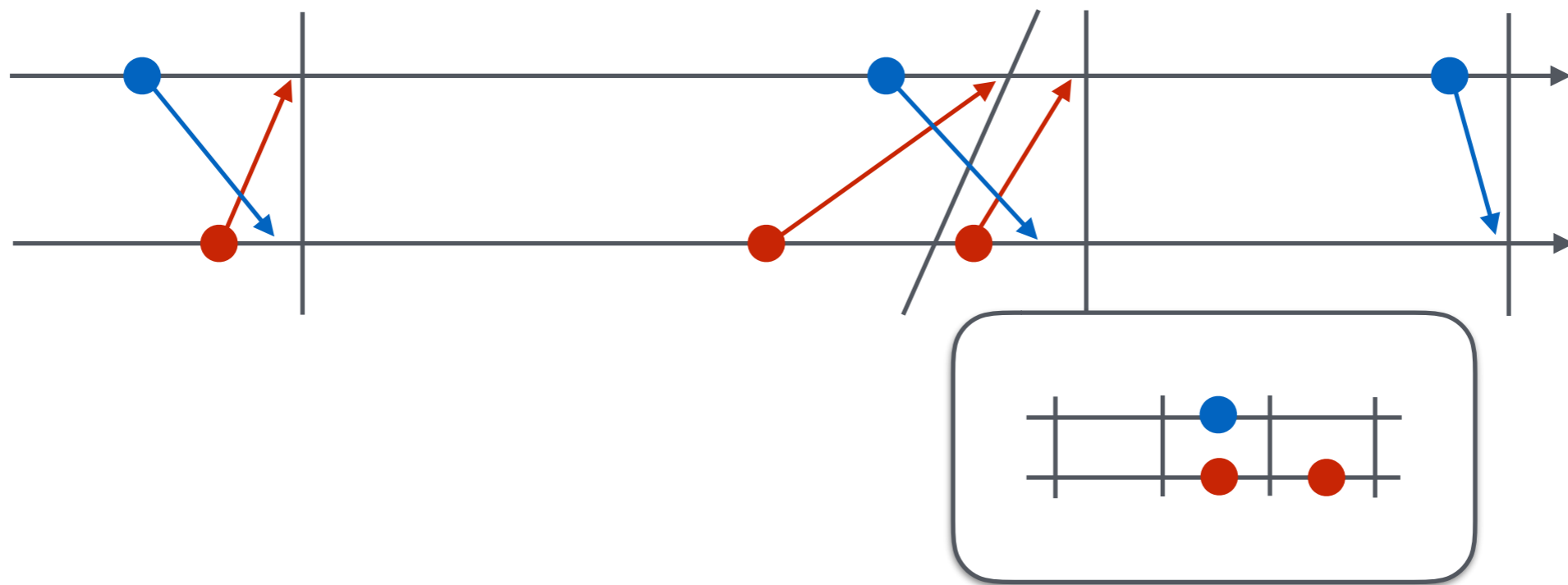


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

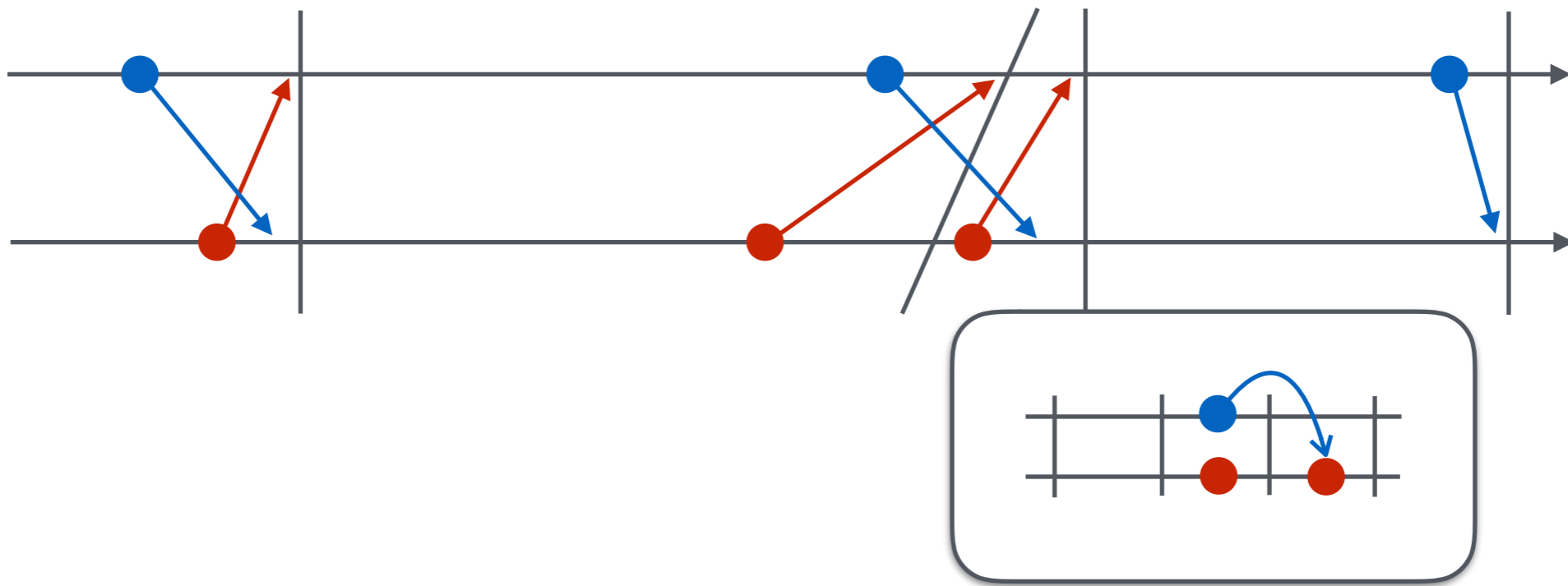


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

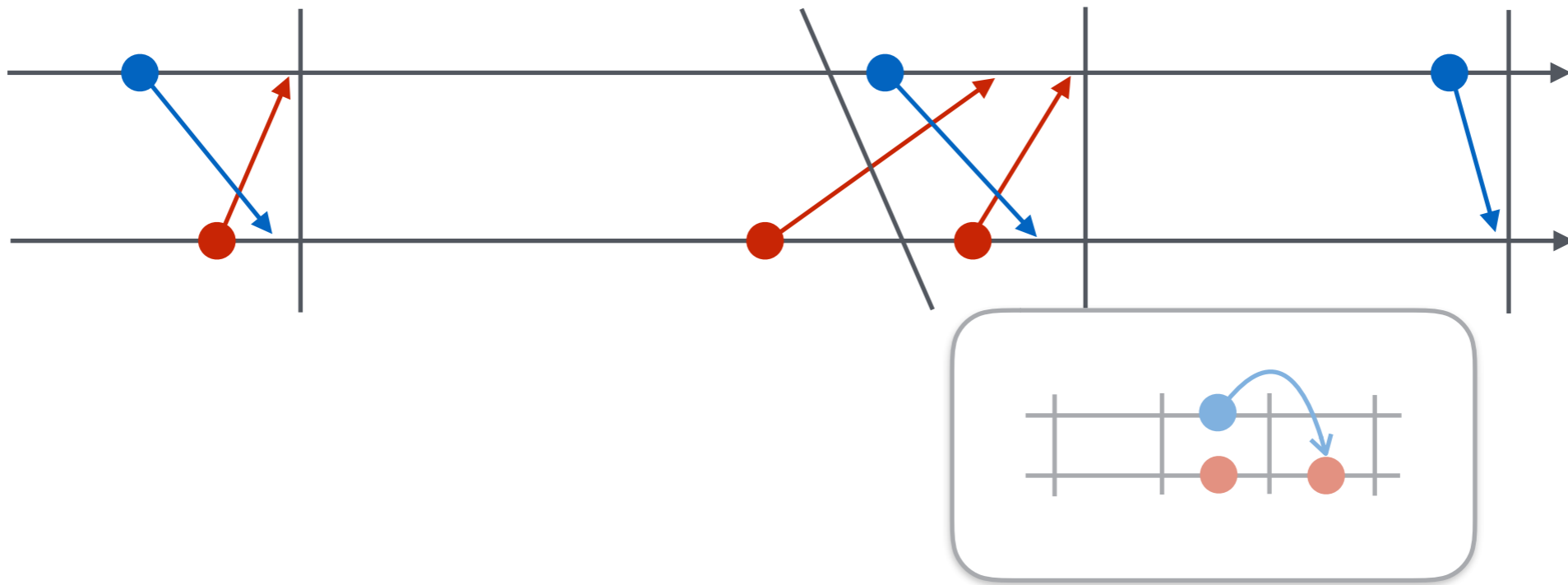


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

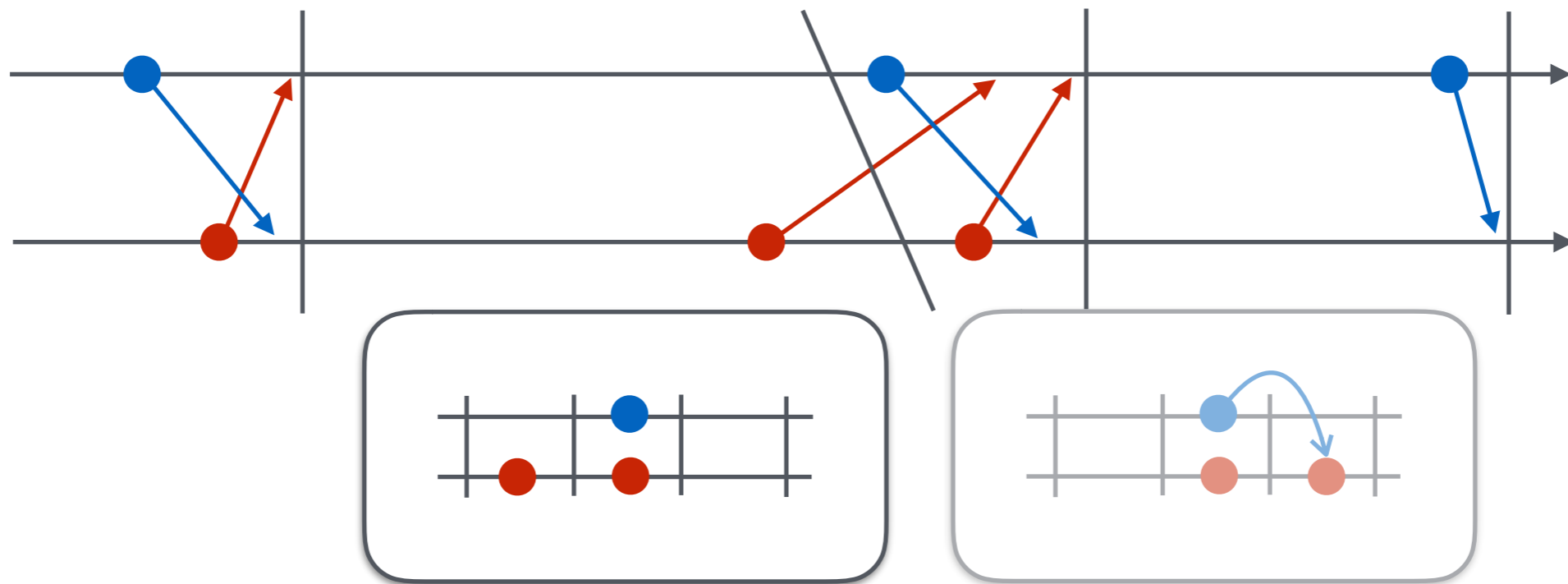


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

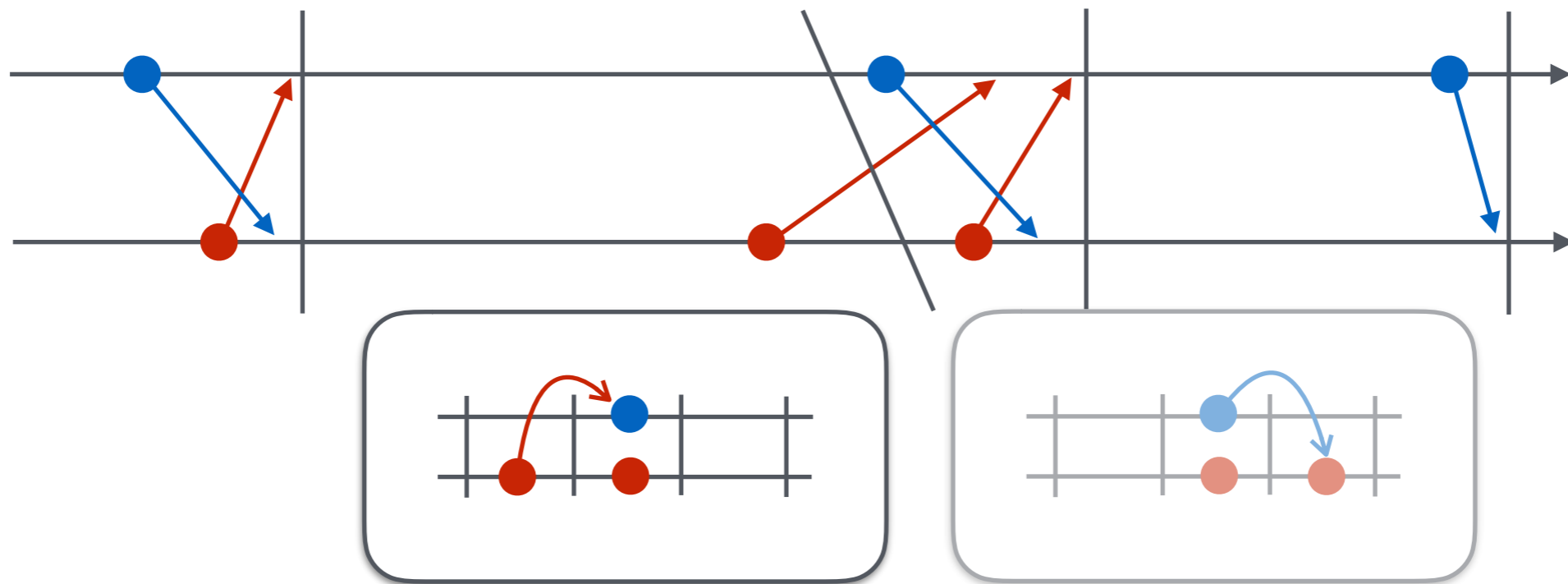


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

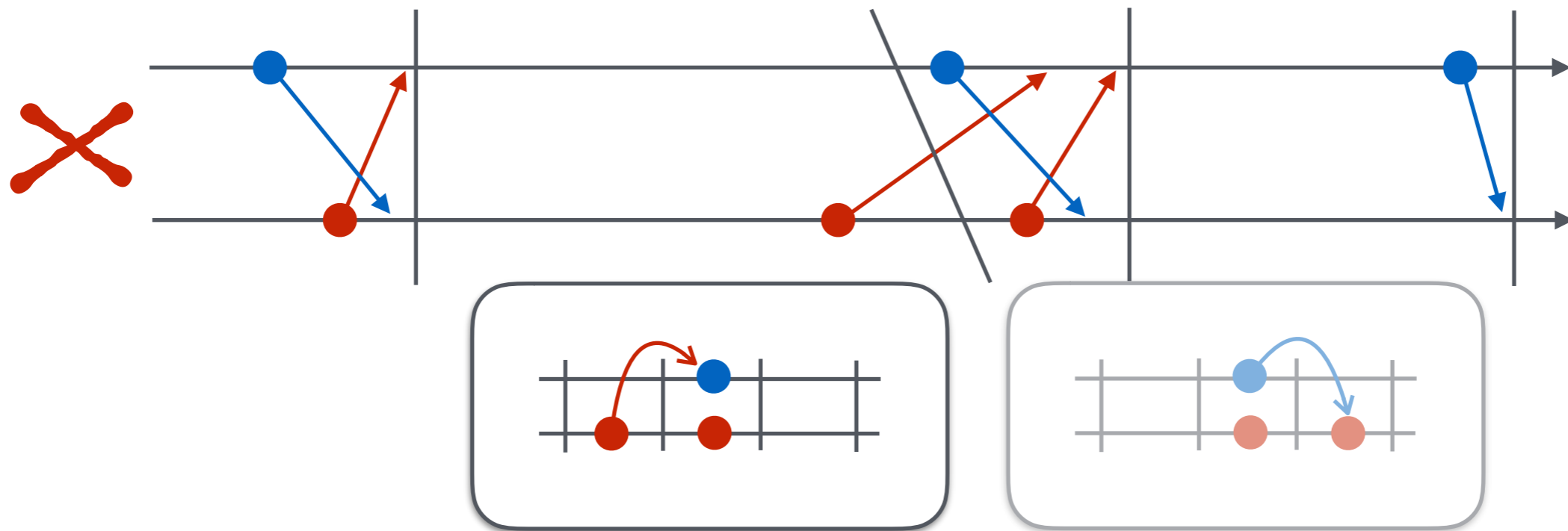


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

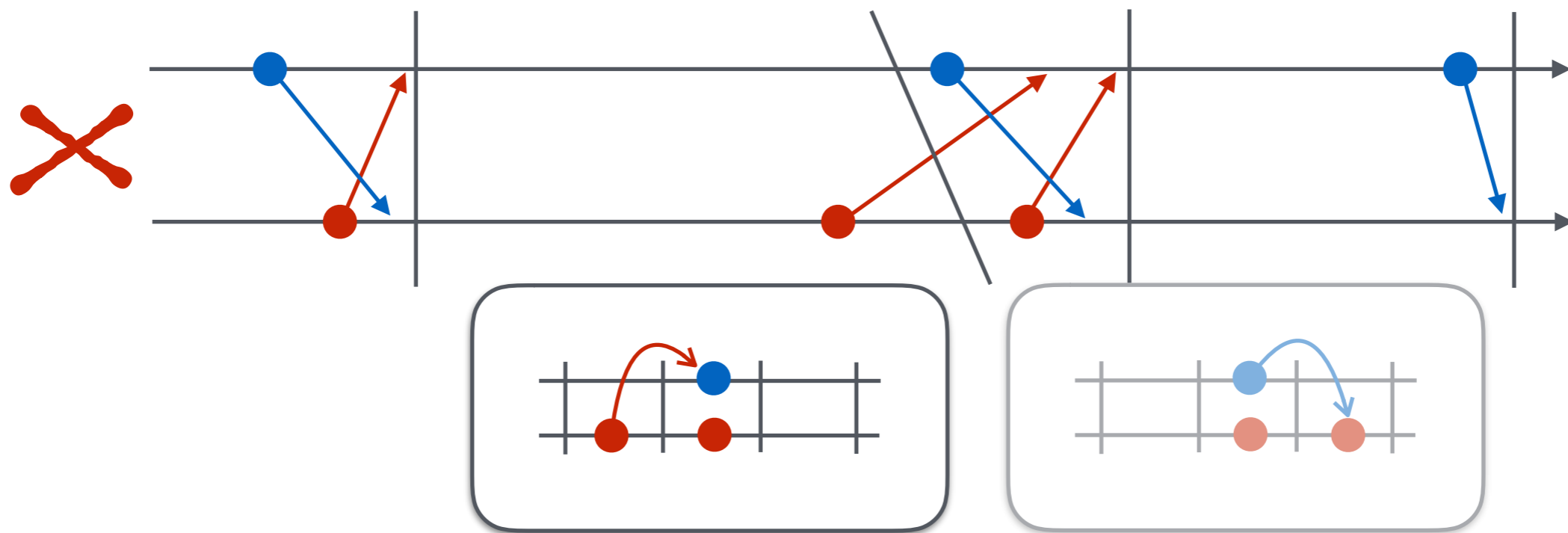


Unitary Discretization

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

the delay accounts for short² undetermined transmission delays.

Twisting the tick?

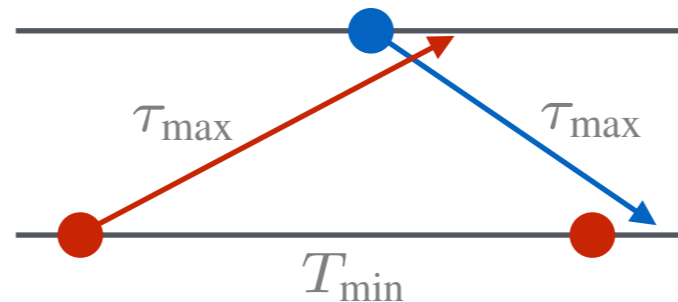


Some traces cannot be unitary discretized

Unitary Discretization

Theorem (2-nodes systems): A quasi-periodic architectures with two nodes is unitary discretizable if and only if

$$T_{\min} \geq 2\tau_{\max}.$$

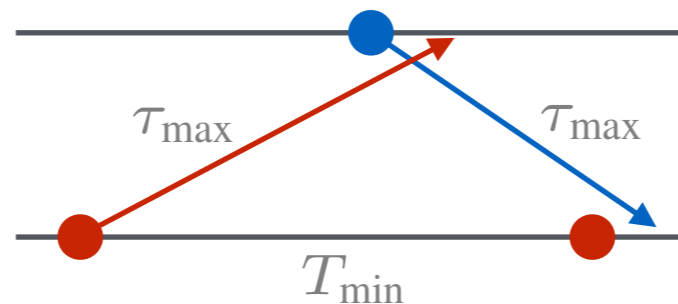


Worst-case scenario

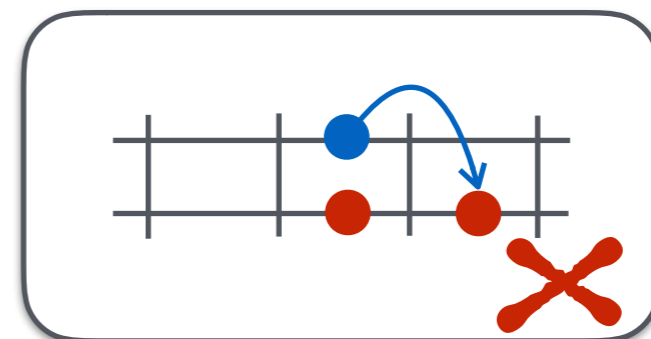
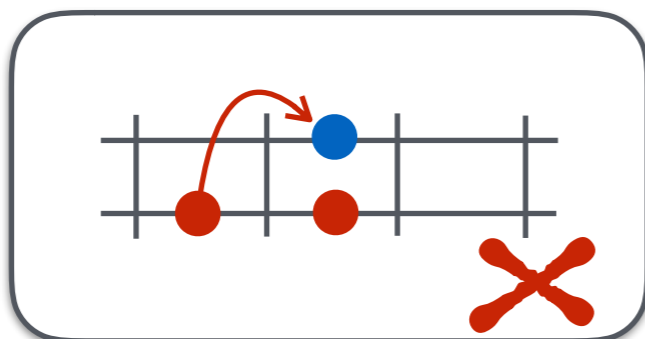
Unitary Discretization

Theorem (2-nodes systems): A quasi-periodic architectures with two nodes is unitary discretizable if and only if

$$T_{\min} \geq 2\tau_{\max}.$$



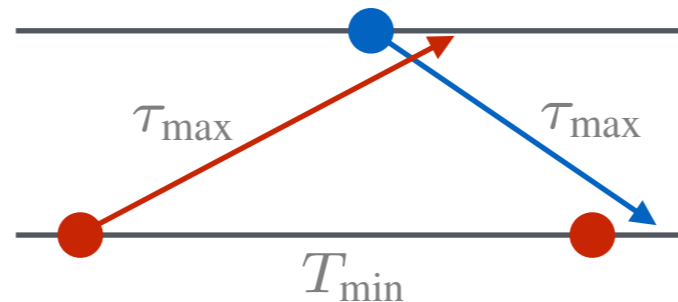
Worst-case scenario



Unitary Discretization

Theorem (2-nodes systems): A quasi-periodic architectures with two nodes is unitary discretizable if and only if

$$T_{\min} \geq 2\tau_{\max}.$$



Worst-case scenario

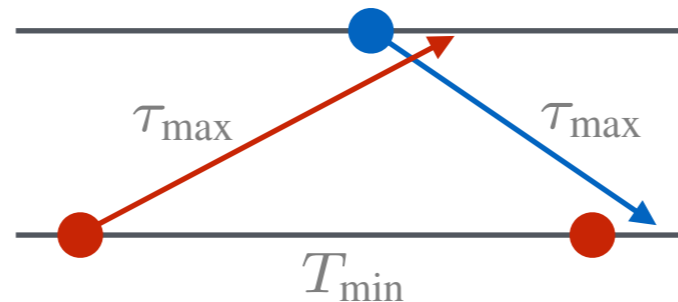
the delay accounts for short² undetermined transmission delays.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

Unitary Discretization

Theorem (2-nodes systems): A quasi-periodic architectures with two nodes is unitary discretizable if and only if

$$T_{\min} \geq 2\tau_{\max}.$$



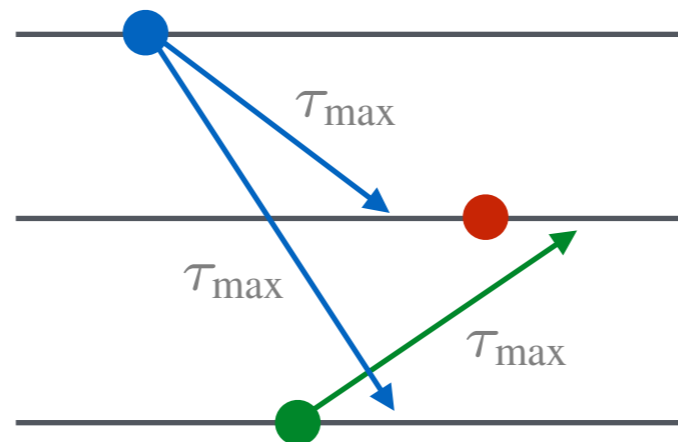
Worst-case scenario

the delay accounts for short² undetermined transmission delays.

²Significantly shorter than the periods of read and write clocks. If longer transmission delays are needed, modeling should be more complex.

Unitary Discretization

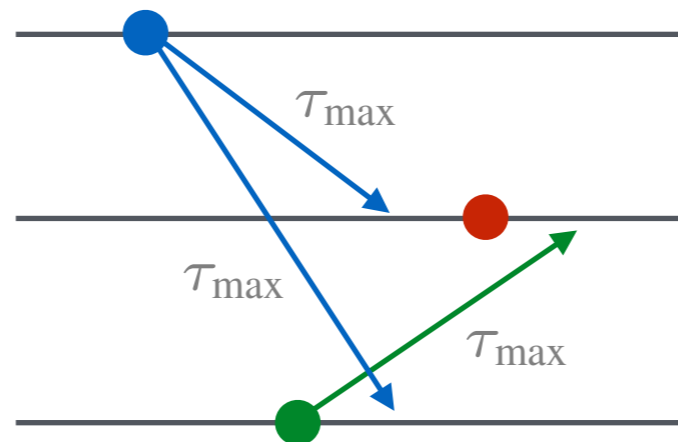
Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.



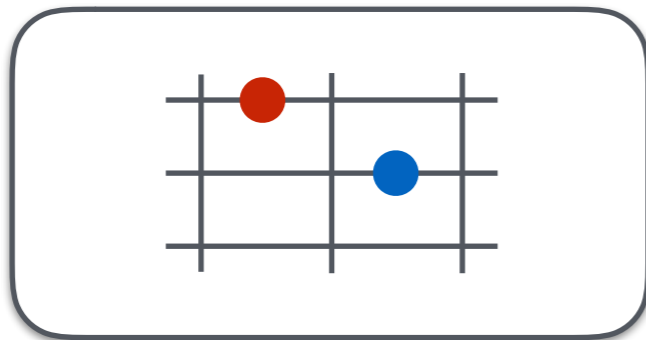
Always possible

Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

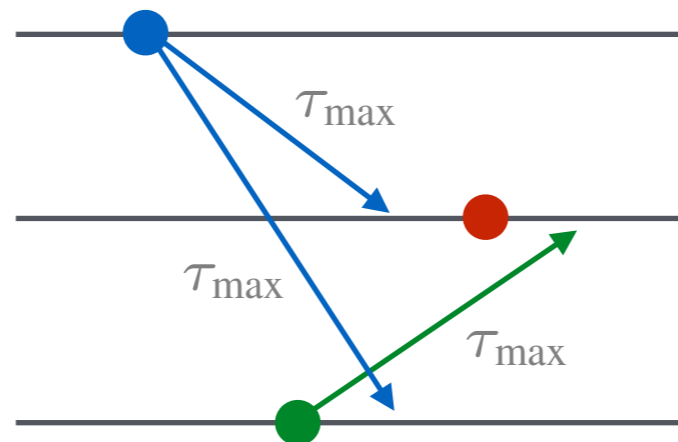


Always possible

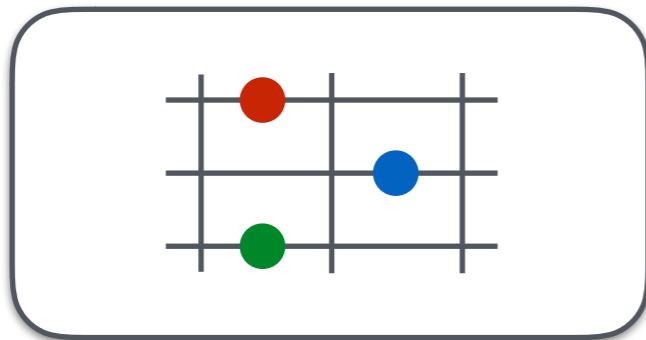


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

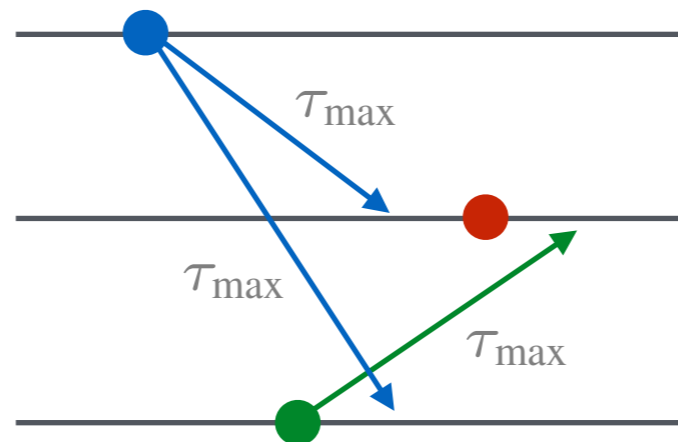


Always possible

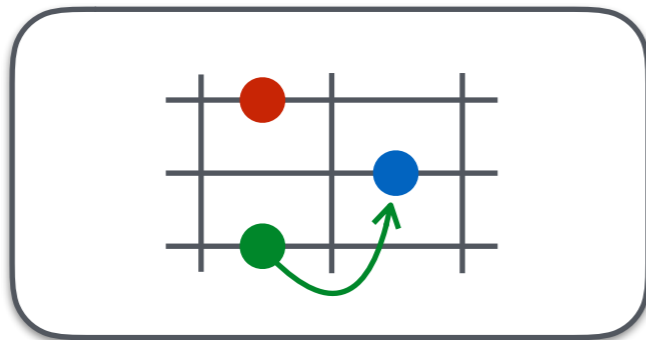


Unitary Discretization

Theorem (general systems): A quasi-periodic architecture with more than two nodes is, in general, not unitary discretizable.

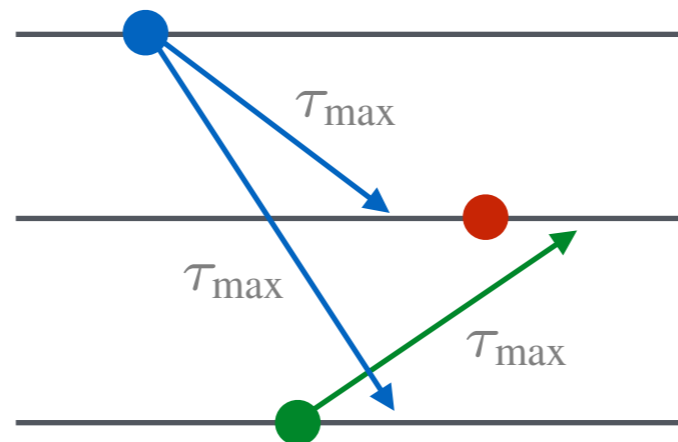


Always possible

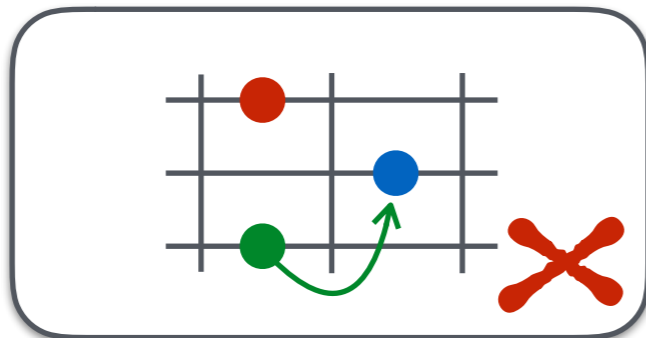


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

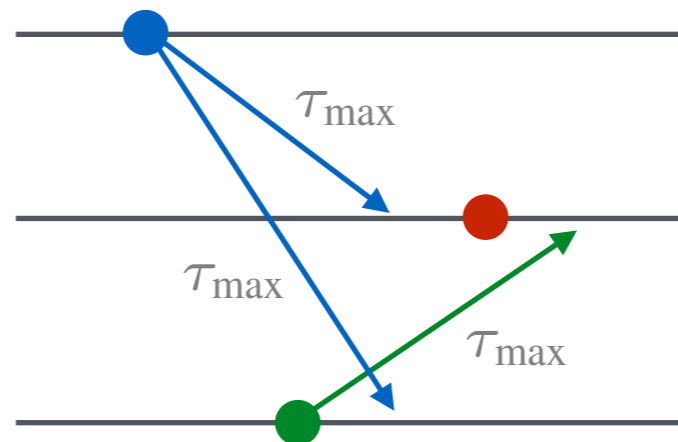


Always possible

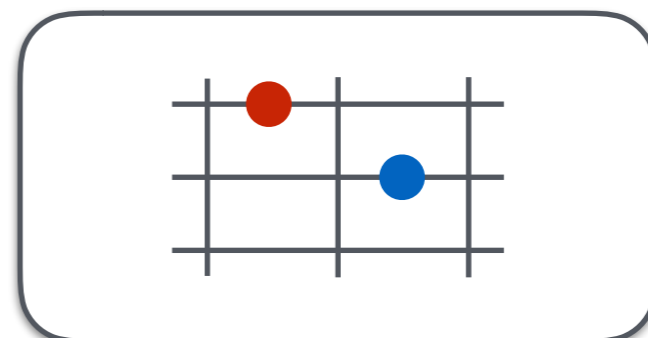
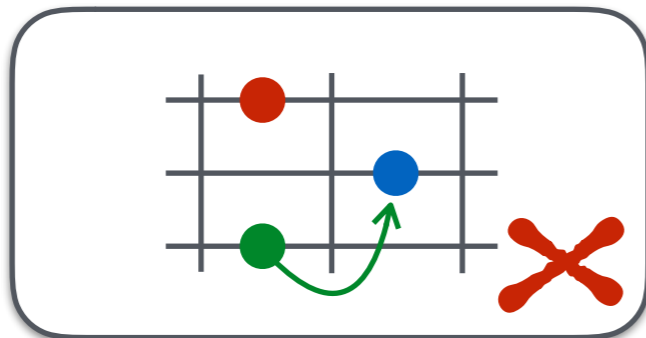


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

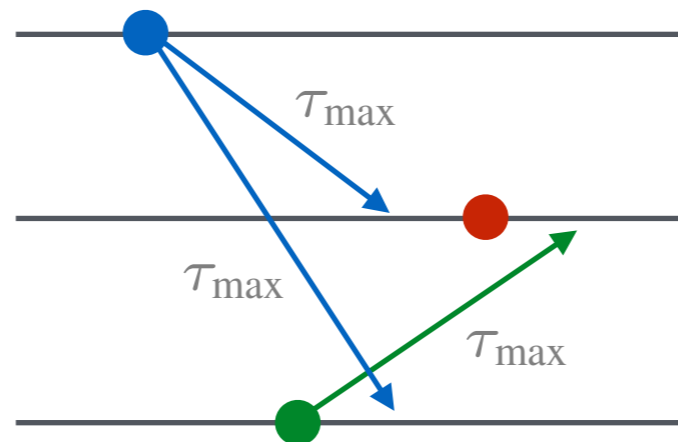


Always possible

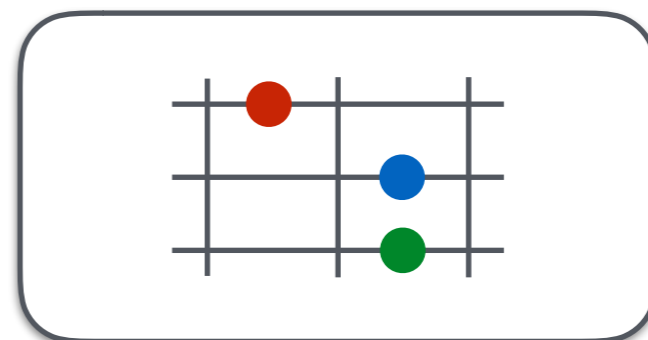
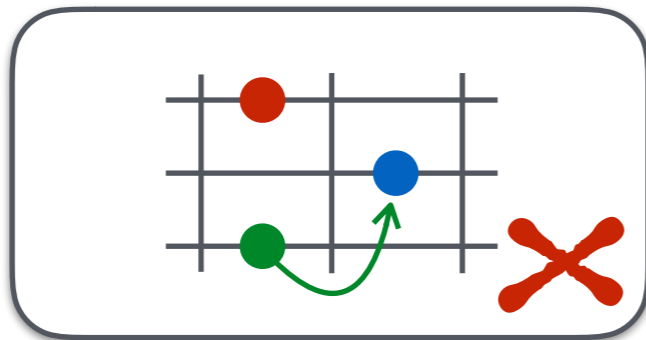


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

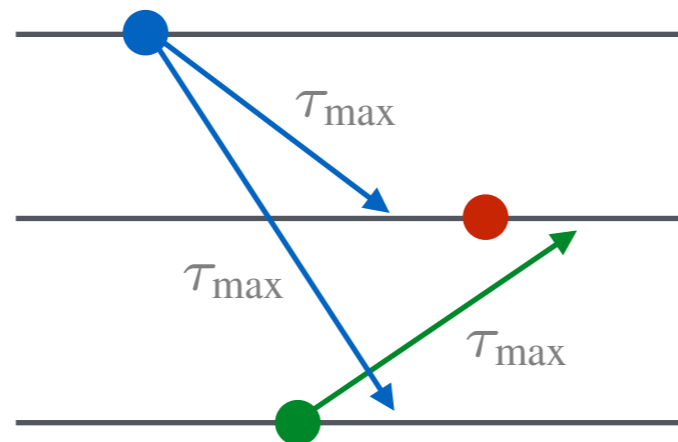


Always possible

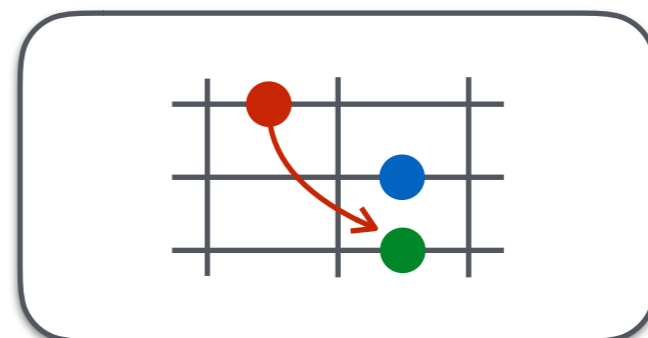
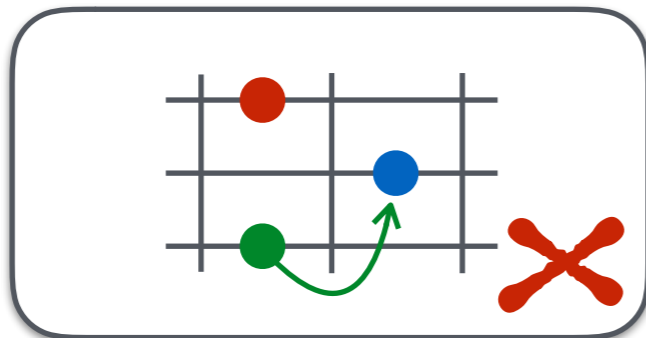


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

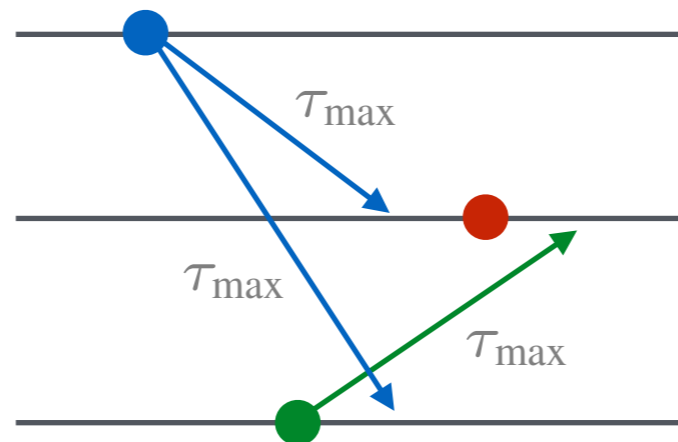


Always possible

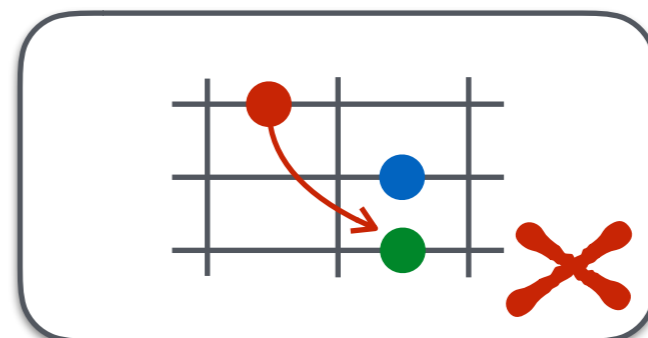
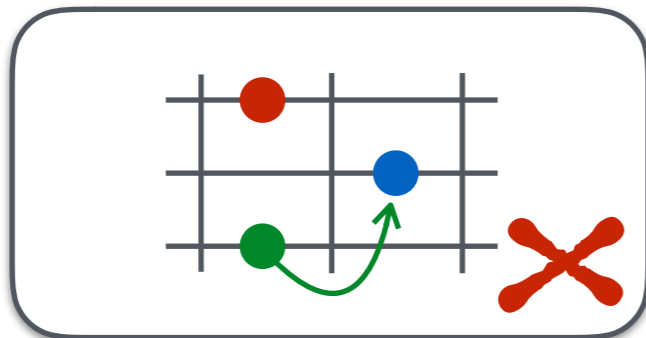


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.

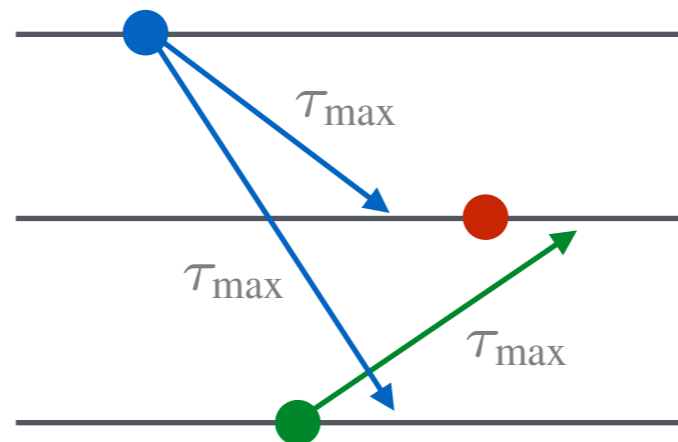


Always possible

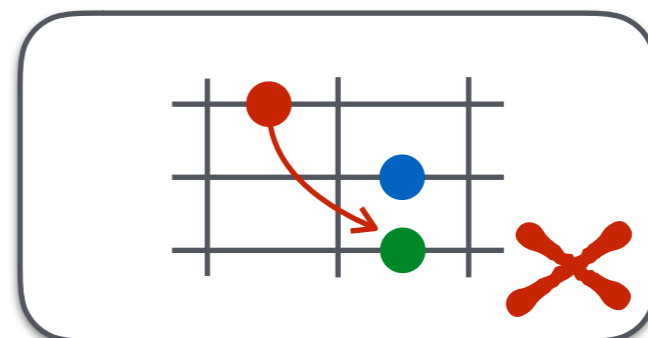
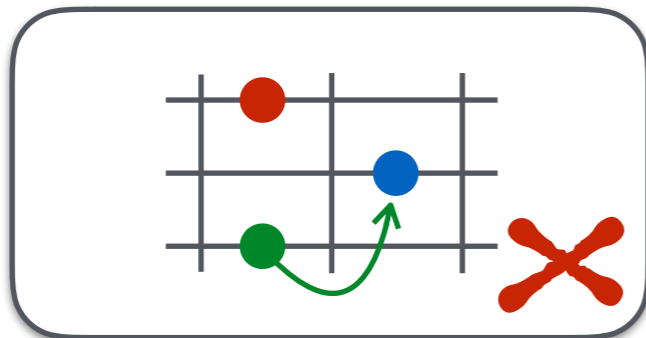


Unitary Discretization

Theorem (general systems): A quasi-periodic architectures with more than two nodes is, in general, not unitary discretizable.



Always possible



Constraining Communications

Proposition: If f is a unitary discretization for a trace, for a pair of nodes where $A \Rightarrow B$ we have that

$$\begin{aligned} A_i \rightarrow B_j &\implies f(A_i) < f(B_j), \\ A_i \not\rightarrow B_j &\implies f(A_i) \geq f(B_j). \end{aligned}$$

We gather all these constraints in a weighted graph

Vertices: Activations of the nodes

Edges:

- If $A_i \rightarrow B_j$ then $A_i \xrightarrow{1} B_j$
- If $A \Rightarrow B$ and $A_i \not\rightarrow B_j$ then $B_j \xrightarrow{0} A_i$

Constraining Communications

Proposition: If f is a unitary discretization for a trace, for a pair of nodes where $A \Rightarrow B$ we have that

$$\begin{aligned} A_i \xrightarrow{1} B_j &\implies f(A_i) < f(B_j), \\ B_j \xrightarrow{0} A_i &\implies f(B_j) \leq f(A_i). \end{aligned}$$

We gather all these constraints in a weighted graph

Vertices: Activations of the nodes

Edges:

- If $A_i \rightarrow B_j$ then $A_i \xrightarrow{1} B_j$
- If $A \Rightarrow B$ and $A_i \not\rightarrow B_j$ then $B_j \xrightarrow{0} A_i$

Constraining Communications

$$\begin{aligned} A_i \xrightarrow{1} B_j &\implies f(A_i) < f(B_j), \\ B_j \xrightarrow{0} A_i &\implies f(B_j) \leq f(A_i). \end{aligned}$$

Lemma: For a trace, there exists a unitary discretization if and only if the corresponding graph has no cycle of positive weight

Proof:

- If there is a cycle of positive weight, there is an event A_i such that $f(A_i) < f(A_i)$
- Otherwise, the function that maps each event A_i to the longest path that lead to A_i is a unitary discretization

Constraining Communications

$$\begin{aligned} A_i \xrightarrow{1} B_j &\implies f(A_i) < f(B_j), \\ B_j \xrightarrow{0} A_i &\implies f(B_j) \leq f(A_i). \end{aligned}$$

Lemma: For a trace, there exists a unitary discretization if and only if the corresponding graph has no cycle of positive weight

Proof:

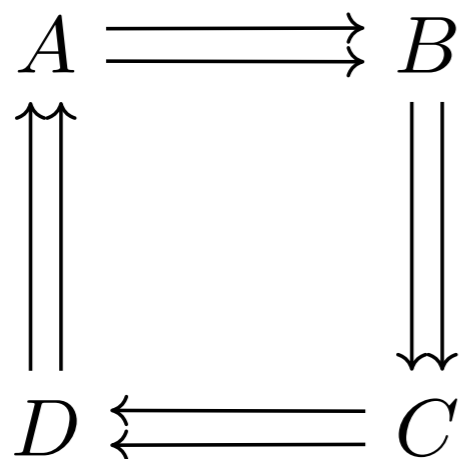
- If there is a cycle of positive weight, there is an event A_i such that $f(A_i) < f(A_i)$
- Otherwise, the function that maps each event A_i to the longest path that lead to A_i is a unitary discretization

Leave room for all the predecessors...

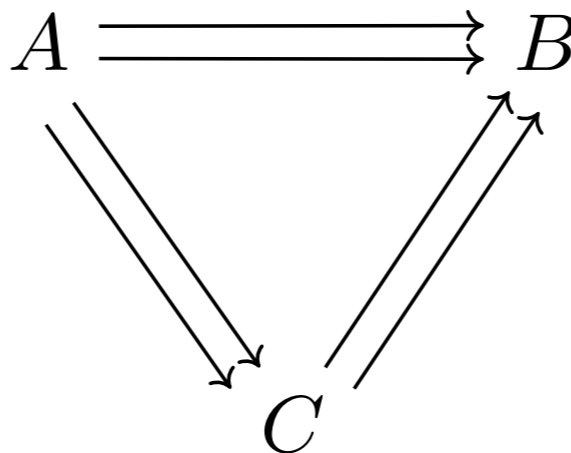
Constraining Communications

Proposition: A cycle of positive weight can be reduced to a cycle of positive weight based on a u -cycle of the communication graph.

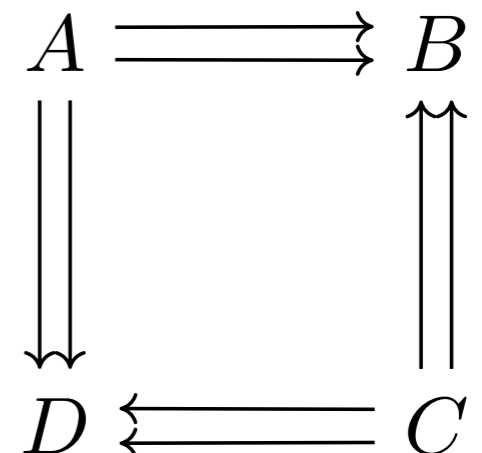
u -cycle: cycle of the undirected communication graph



Cycle



Unbalanced



Balanced

Constraining Communications

L_c : size of the longest elementary communication cycle

Theorem: A quasi-periodic architecture is unitary discretizable if and only if

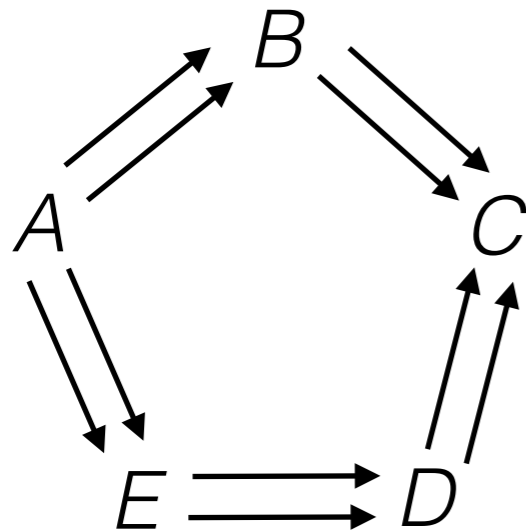
1. all u -cycle of the communication graph are either cycles or balanced u -cycle, and,
2. there is no balanced u -cycle in the communication graph or $\tau_{min} = \tau_{max}$, and,
3. there is no cycle in the communication graph, or

$$T_{min} \geq L_c \tau_{max}$$

Constraining Communications

Proof: If there is a u -cycle, construction of a counter-example

Communications

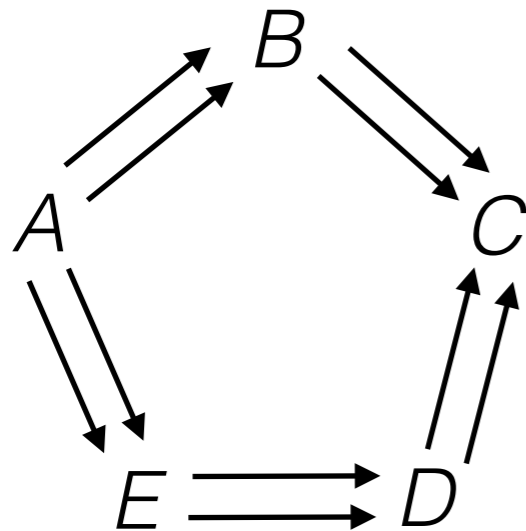


A _____
B _____
C _____
D _____
E _____

Constraining Communications

Proof: If there is a u -cycle, construction of a counter-example

Communications



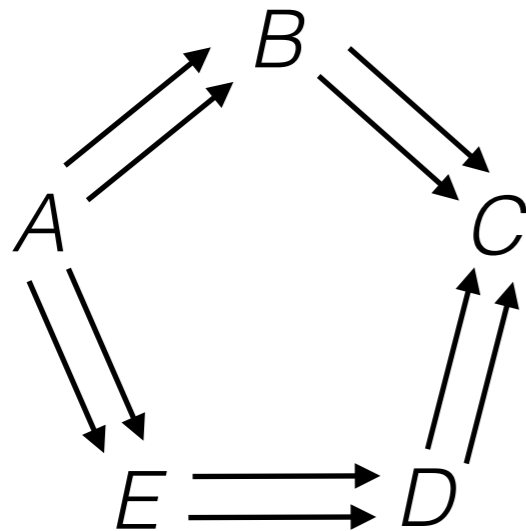
$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \longrightarrow \longrightarrow$

A _____
B _____
C _____
D _____
E _____

Constraining Communications

Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \longrightarrow \longrightarrow$

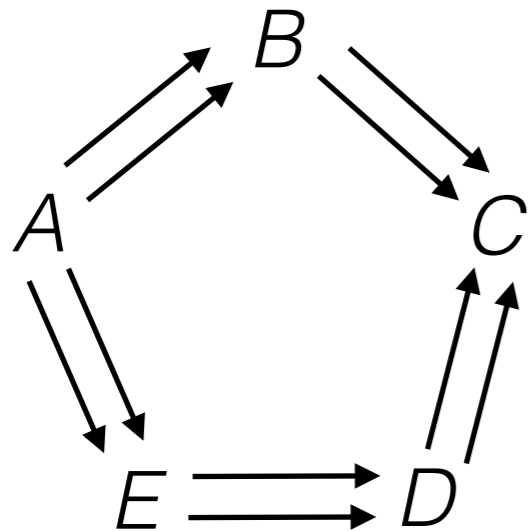
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$

A _____
 B _____
 C _____
 D _____
 E _____

Constraining Communications

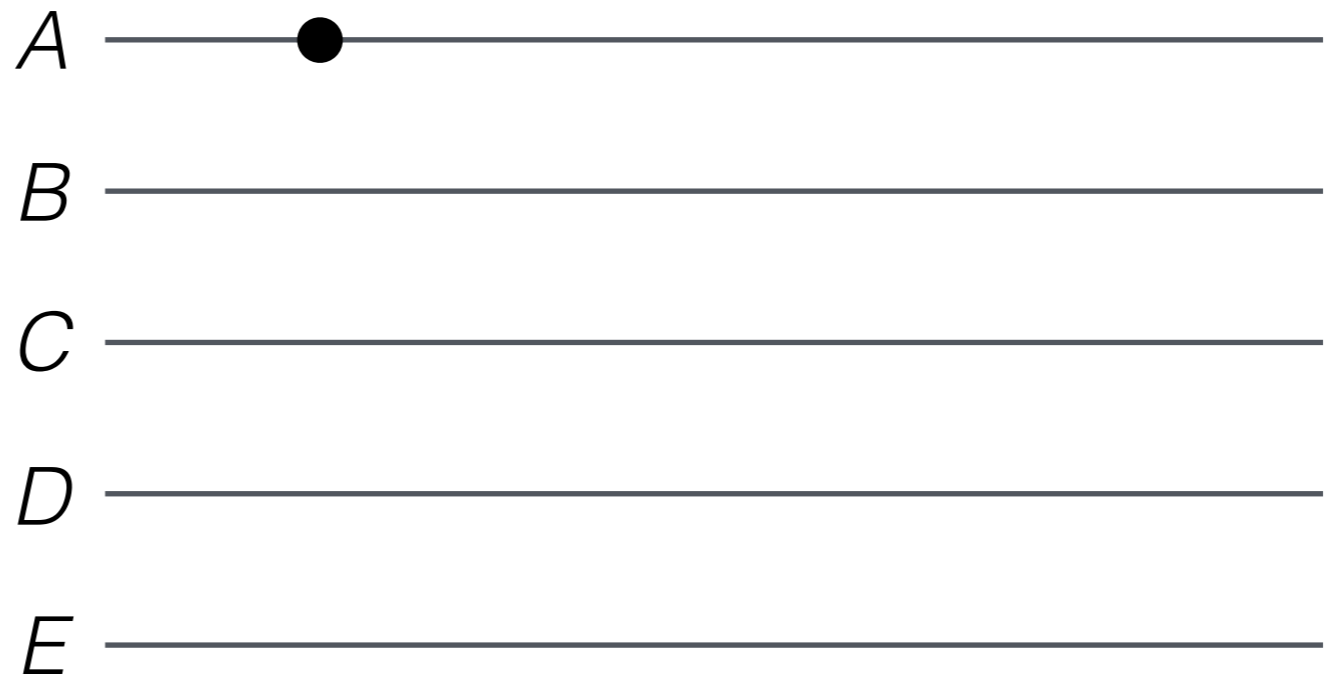
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3$: # ←←←
 $p = 2$: # →→→

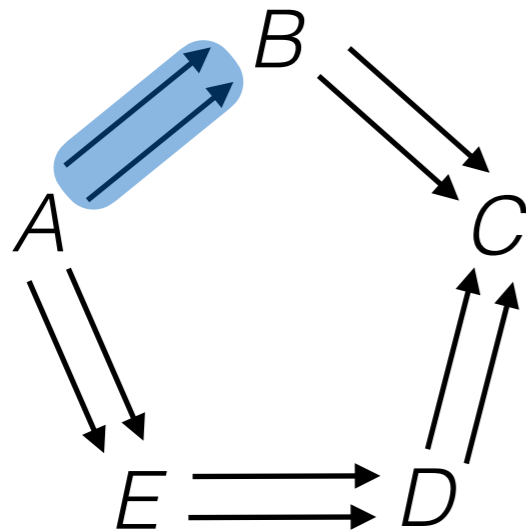
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

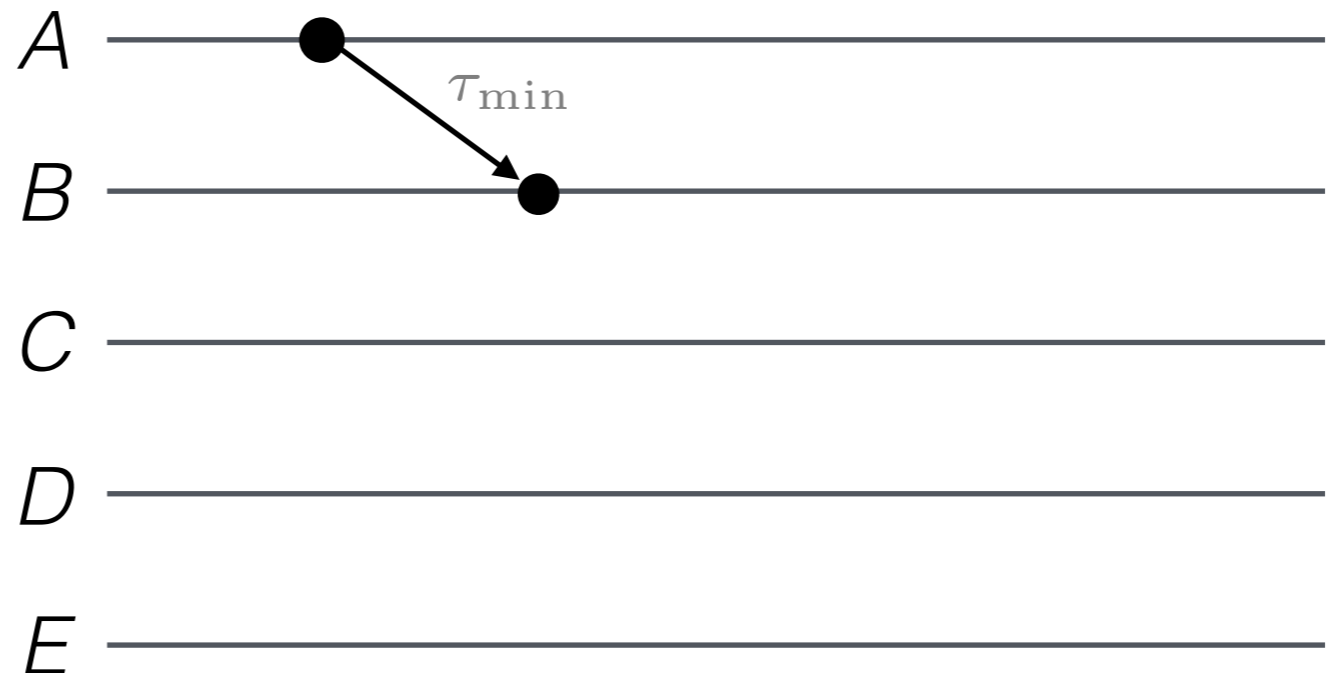
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \longrightarrow \longrightarrow$

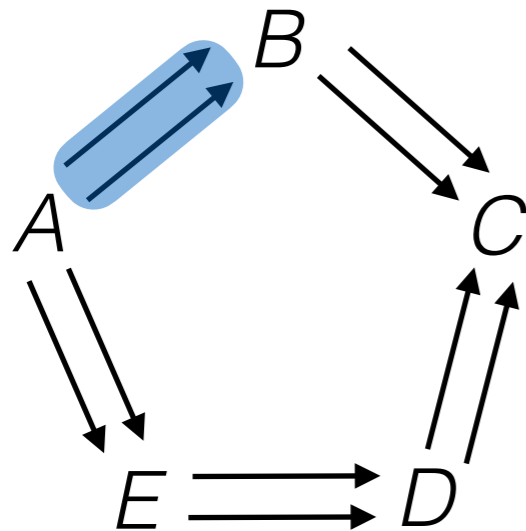
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

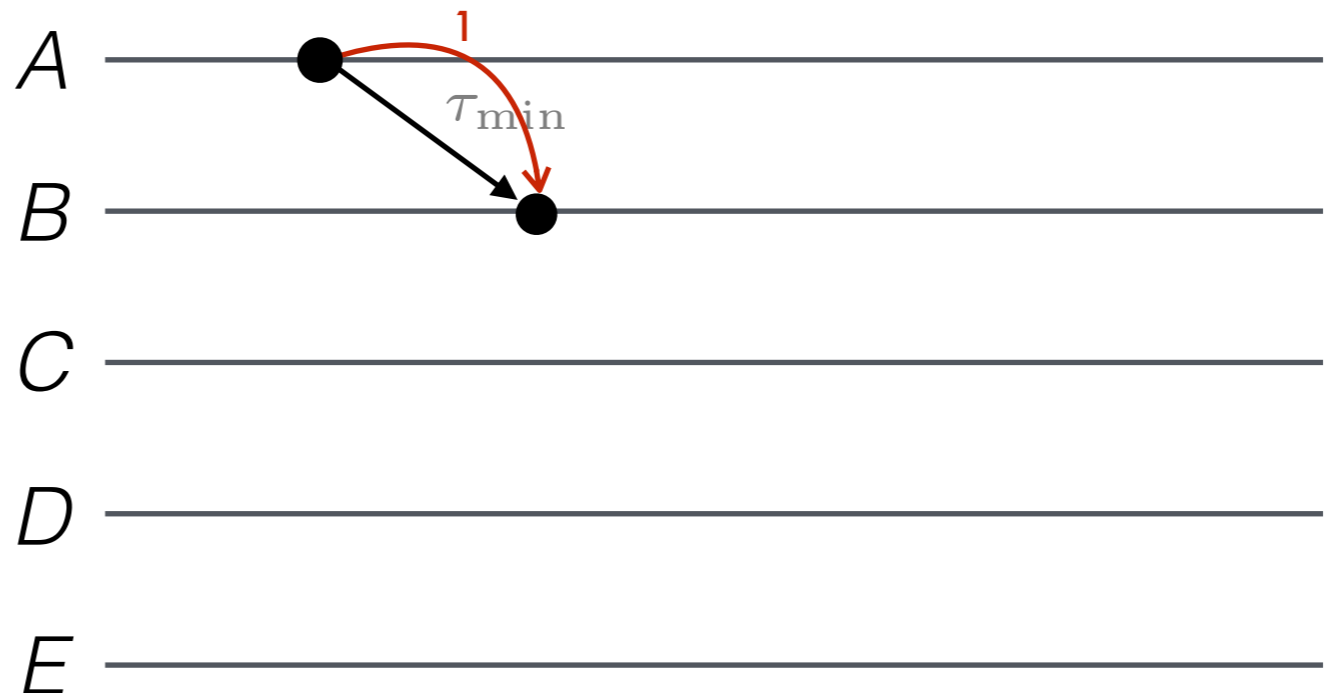
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3$: # ←←←
 $p = 2$: # →→→

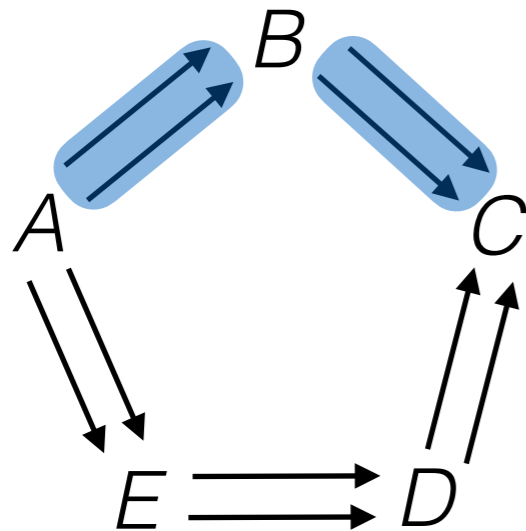
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

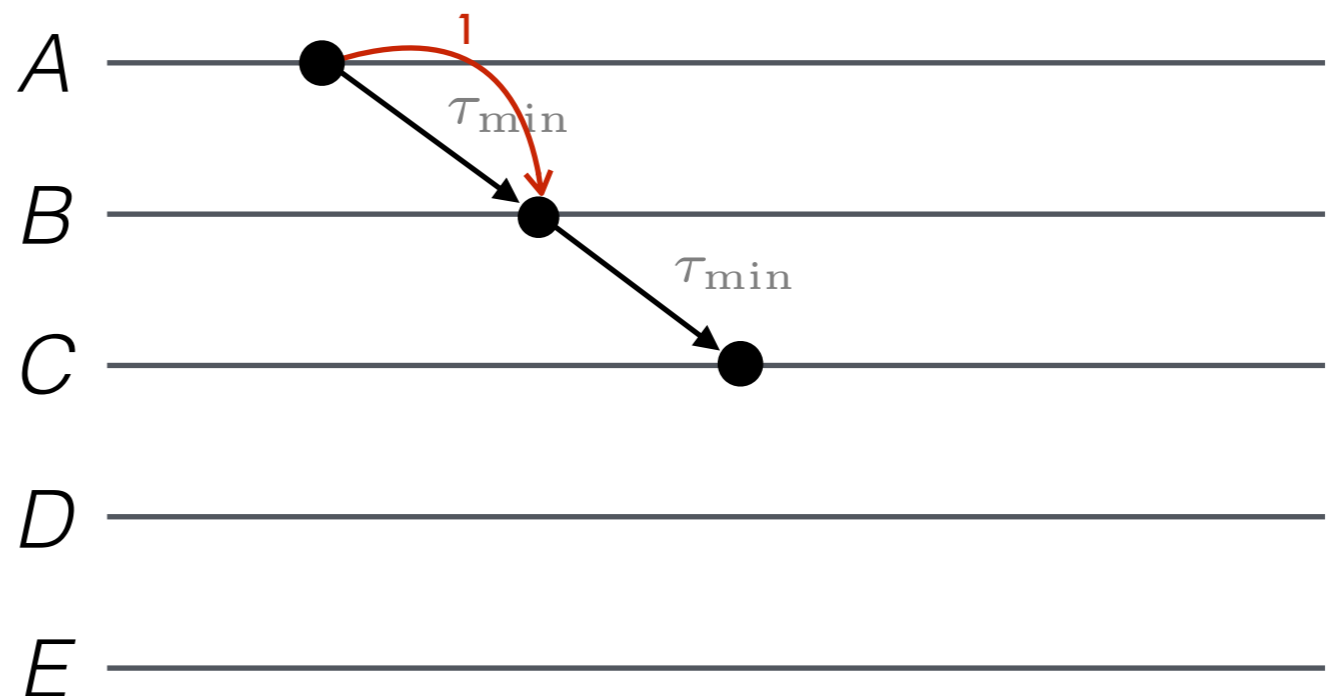
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \Rightarrow \Rightarrow$

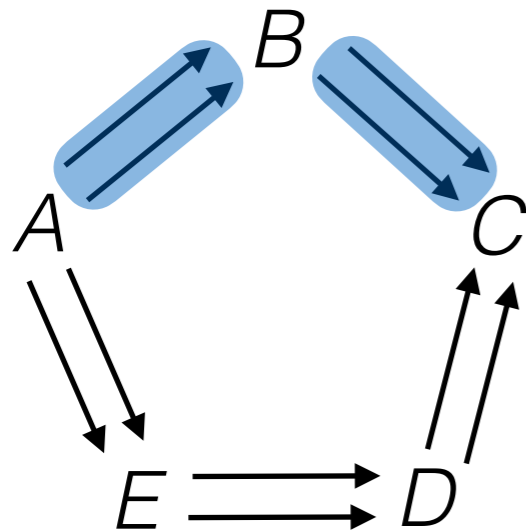
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

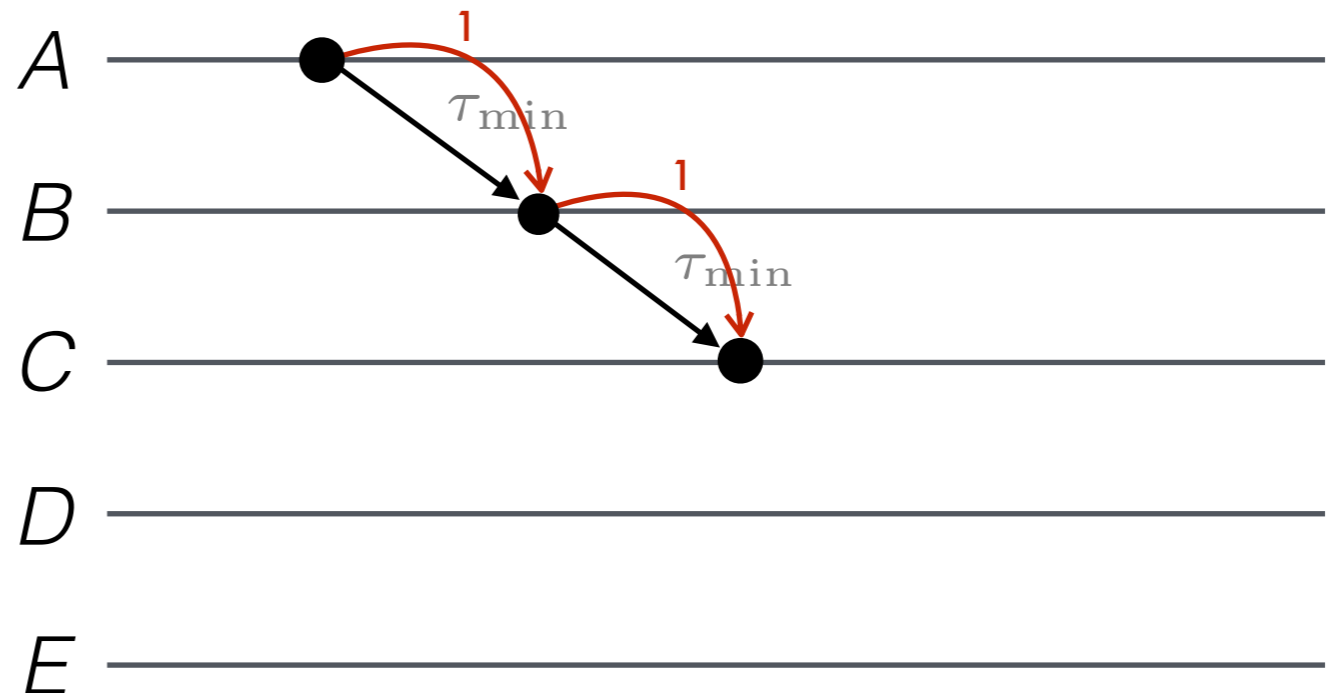
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3$: # ←←←
 $p = 2$: # →→→

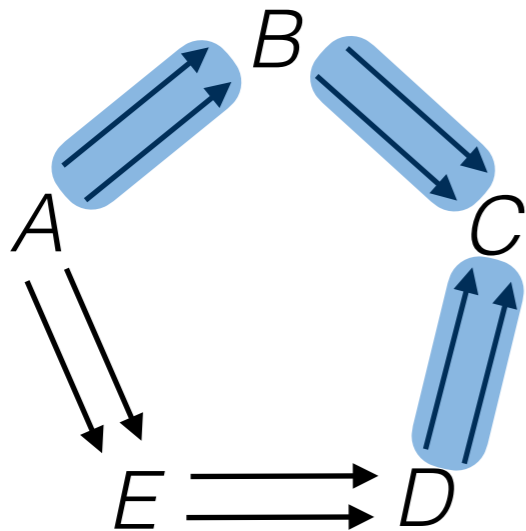
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

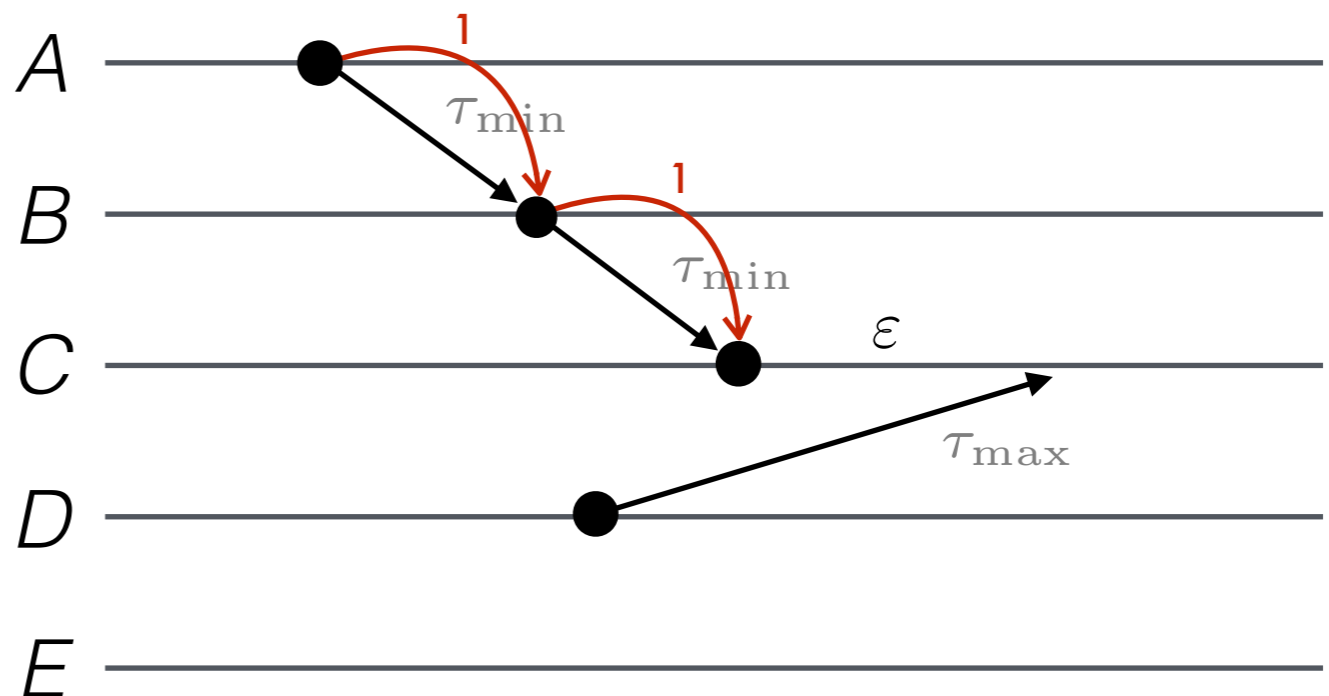
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \Rightarrow \Rightarrow$

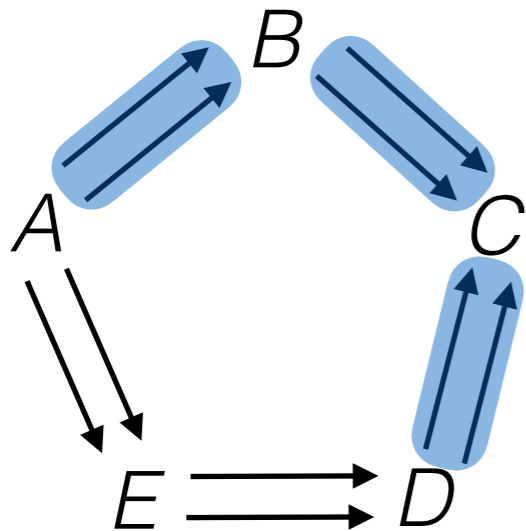
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

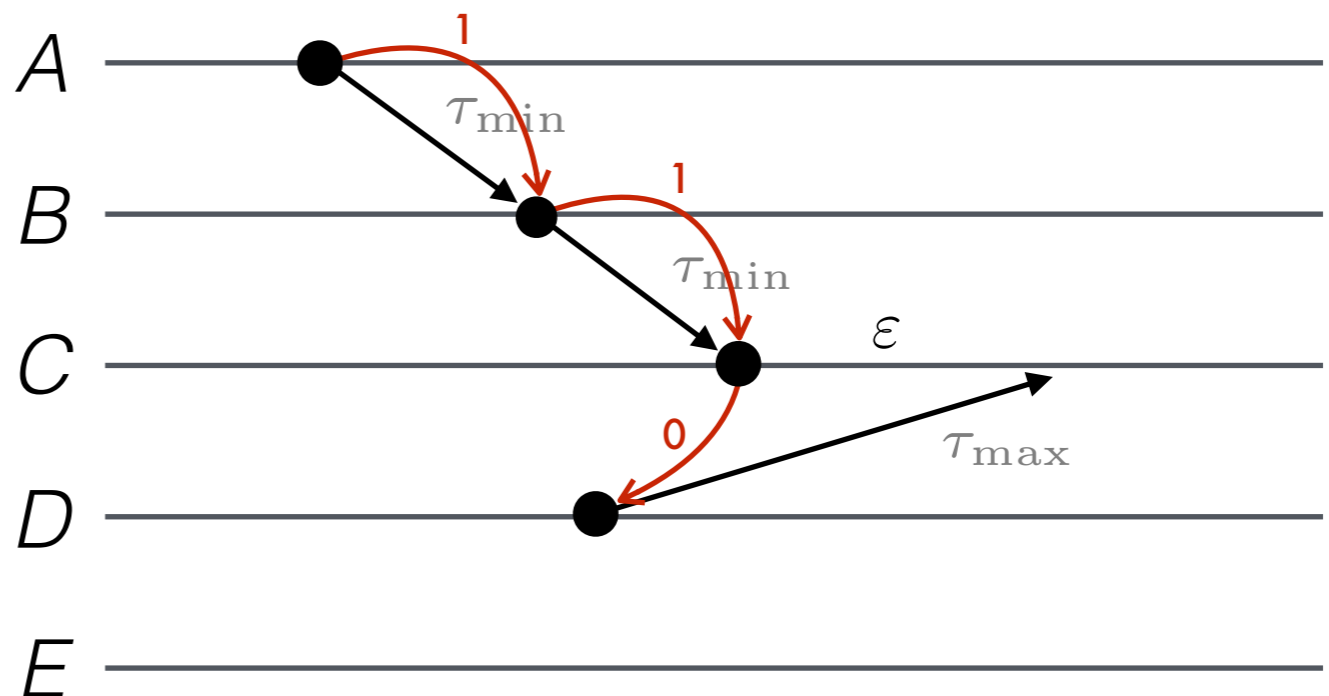
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \Rightarrow \Rightarrow$

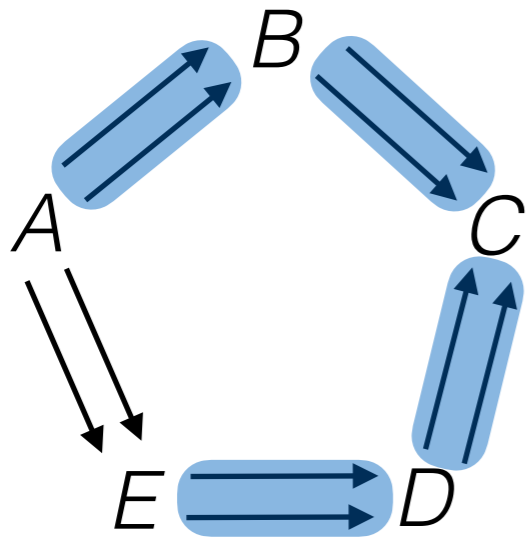
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

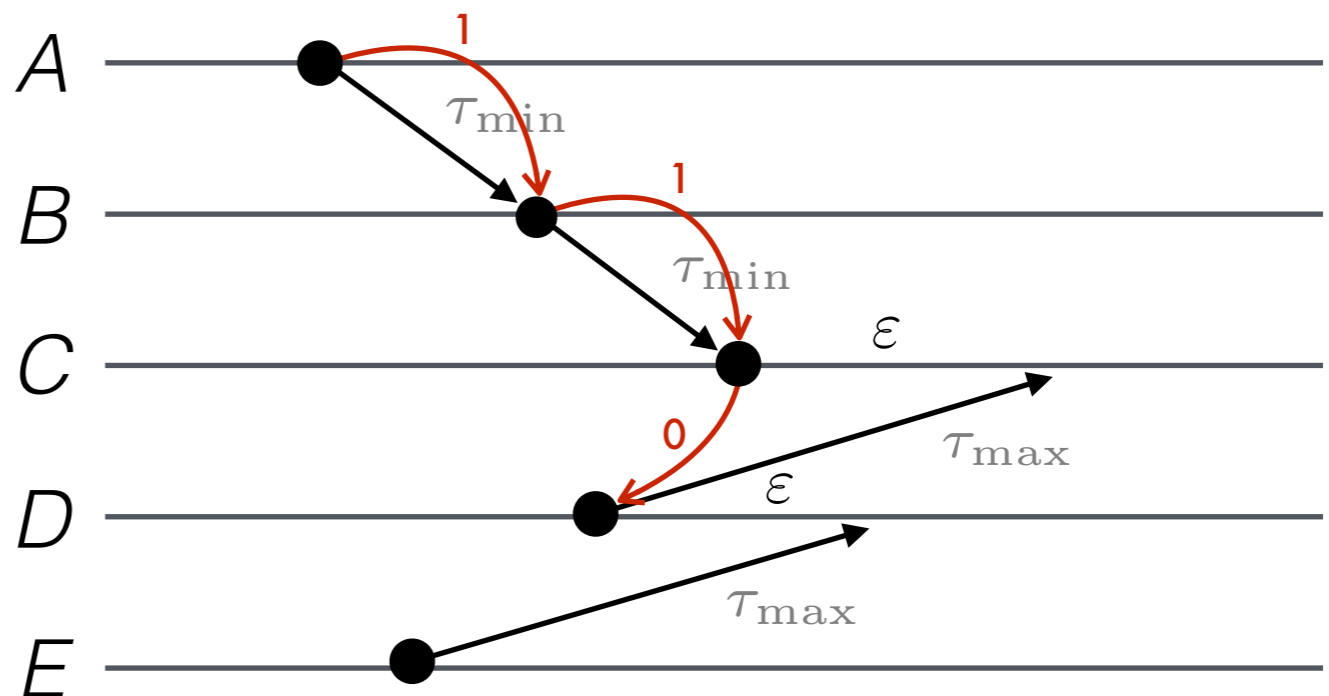
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \longrightarrow \longrightarrow$

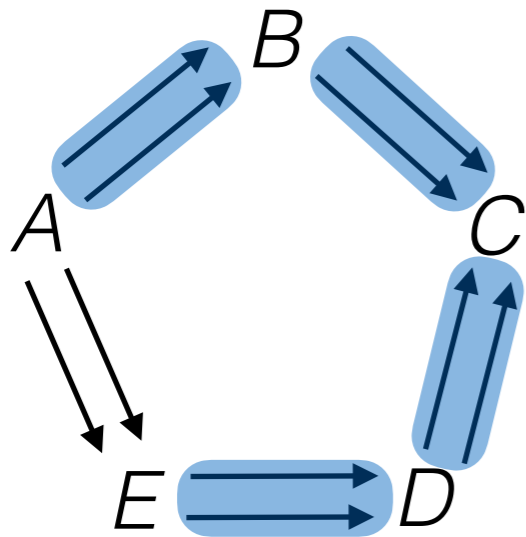
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

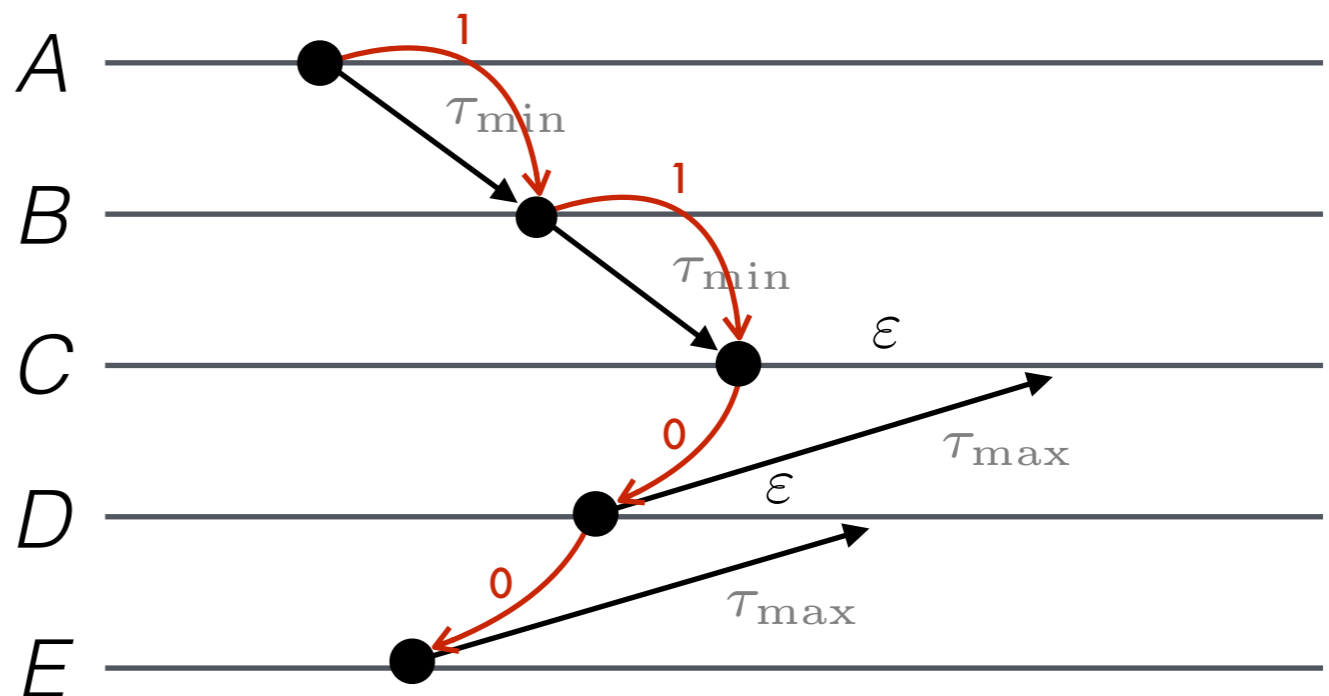
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \longrightarrow \longrightarrow$

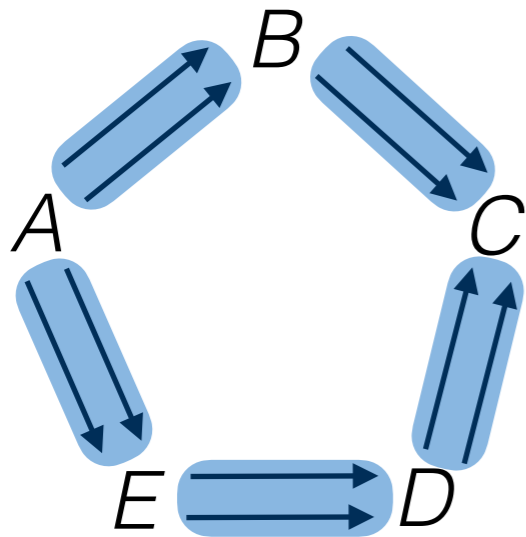
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

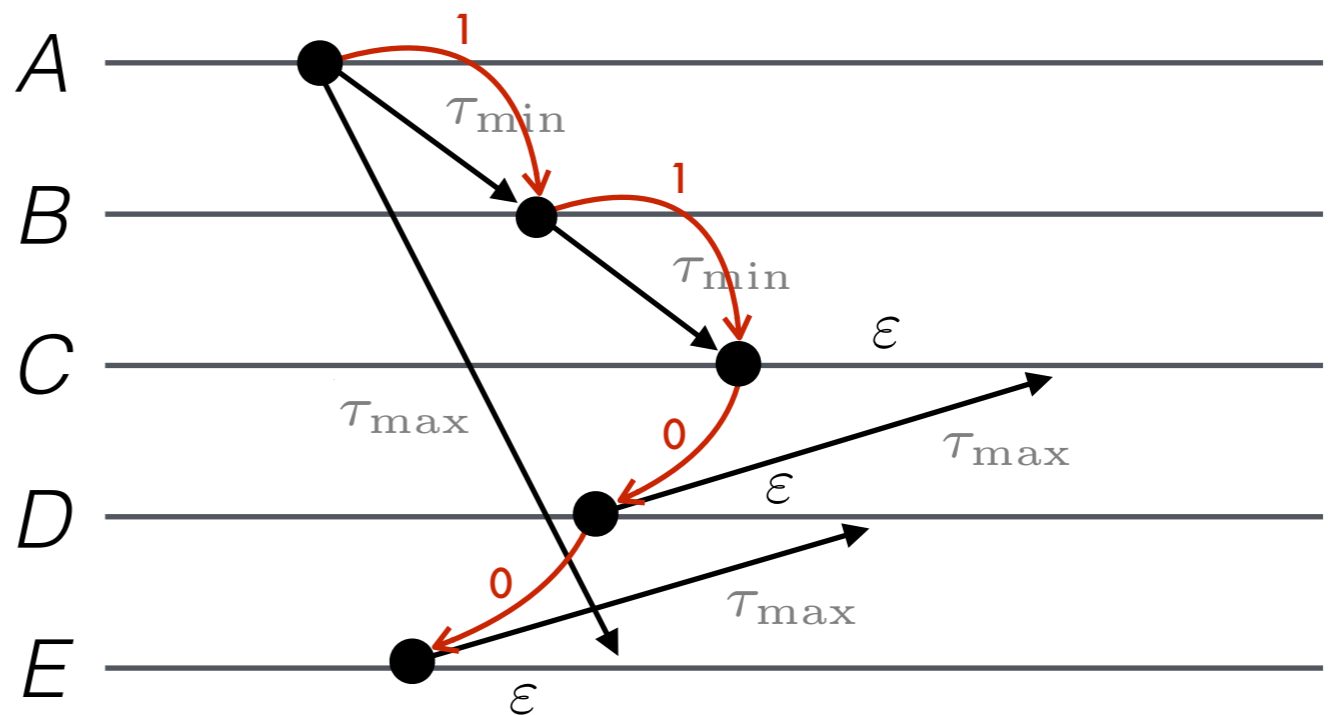
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3: \# \leftarrow \leftarrow \leftarrow$
 $p = 2: \# \longrightarrow \longrightarrow$

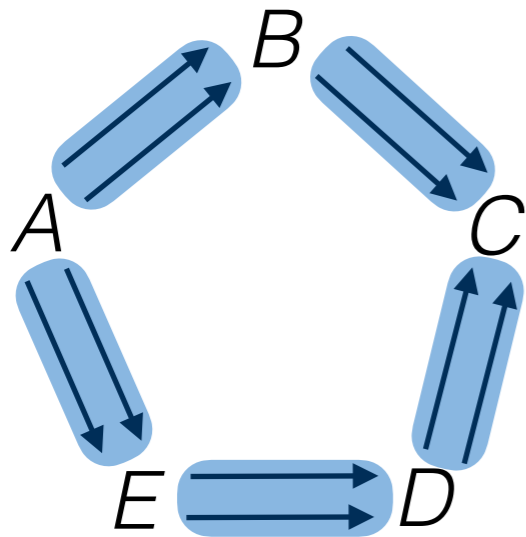
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$





Constraining Communications

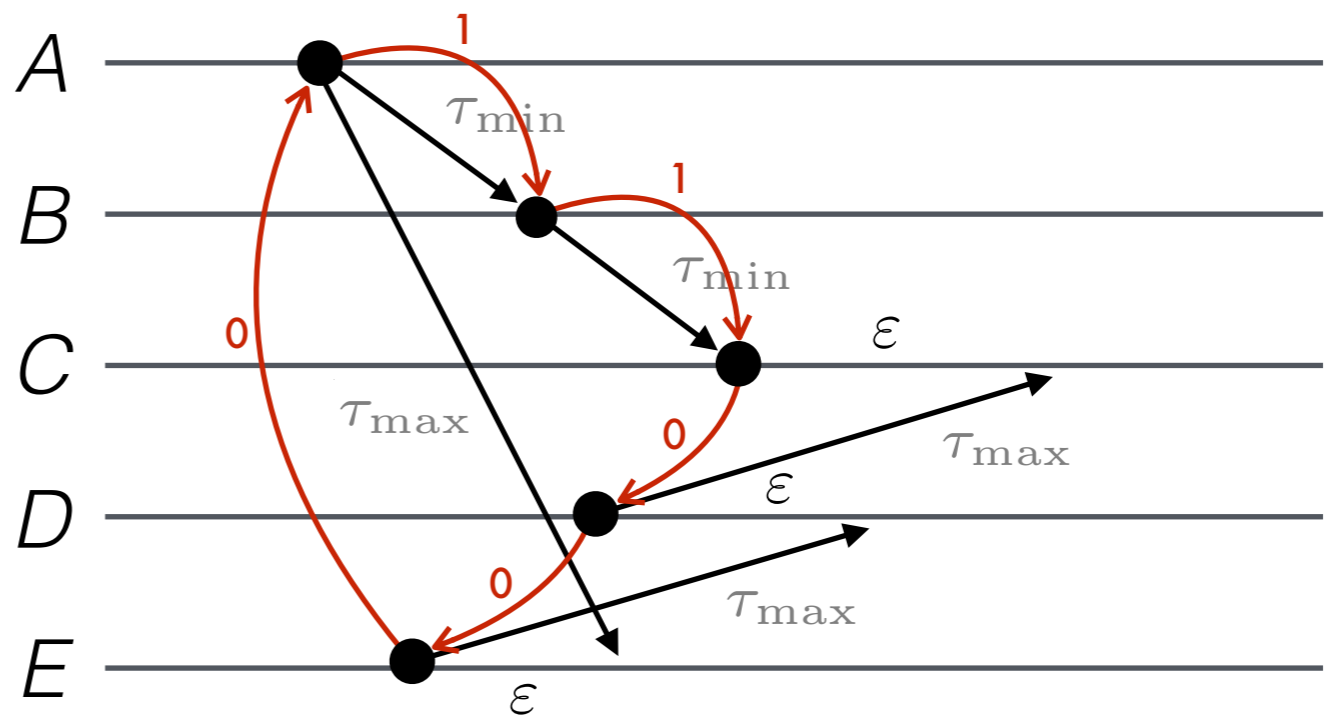
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3$: # 
 $p = 2$: # 

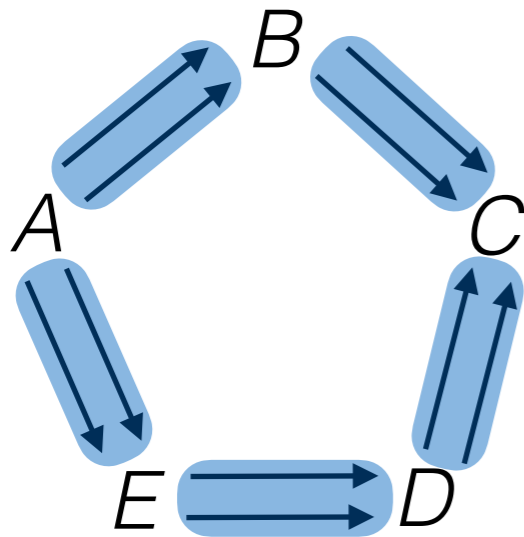
$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



Constraining Communications

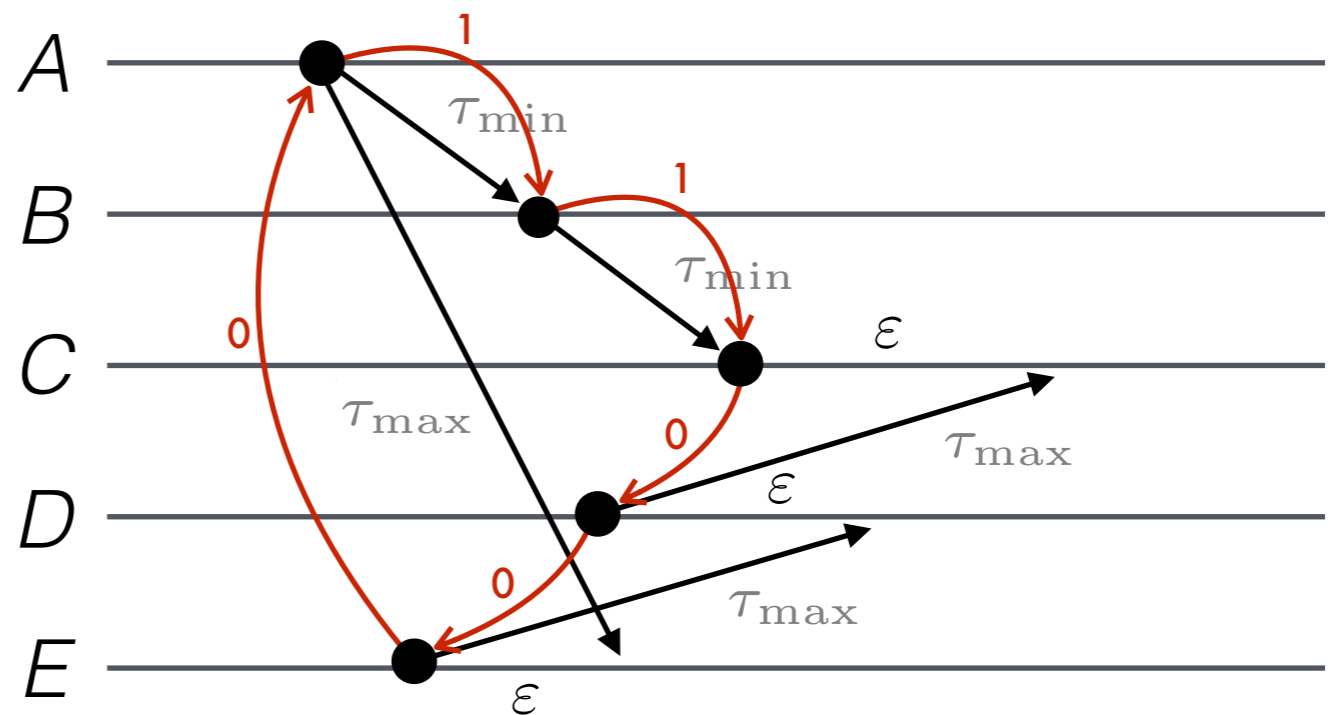
Proof: If there is a u -cycle, construction of a counter-example

Communications



$q = 3$: # $\leftarrow \leftarrow \leftarrow$
 $p = 2$: # $\Rightarrow \Rightarrow$

$$q > p \implies \varepsilon = (q\tau_{\max} - p\tau_{\min})/q > 0$$



We built a cycle of positive weight!

Constraining Communications

Proof: On the other hand, by contraposition,

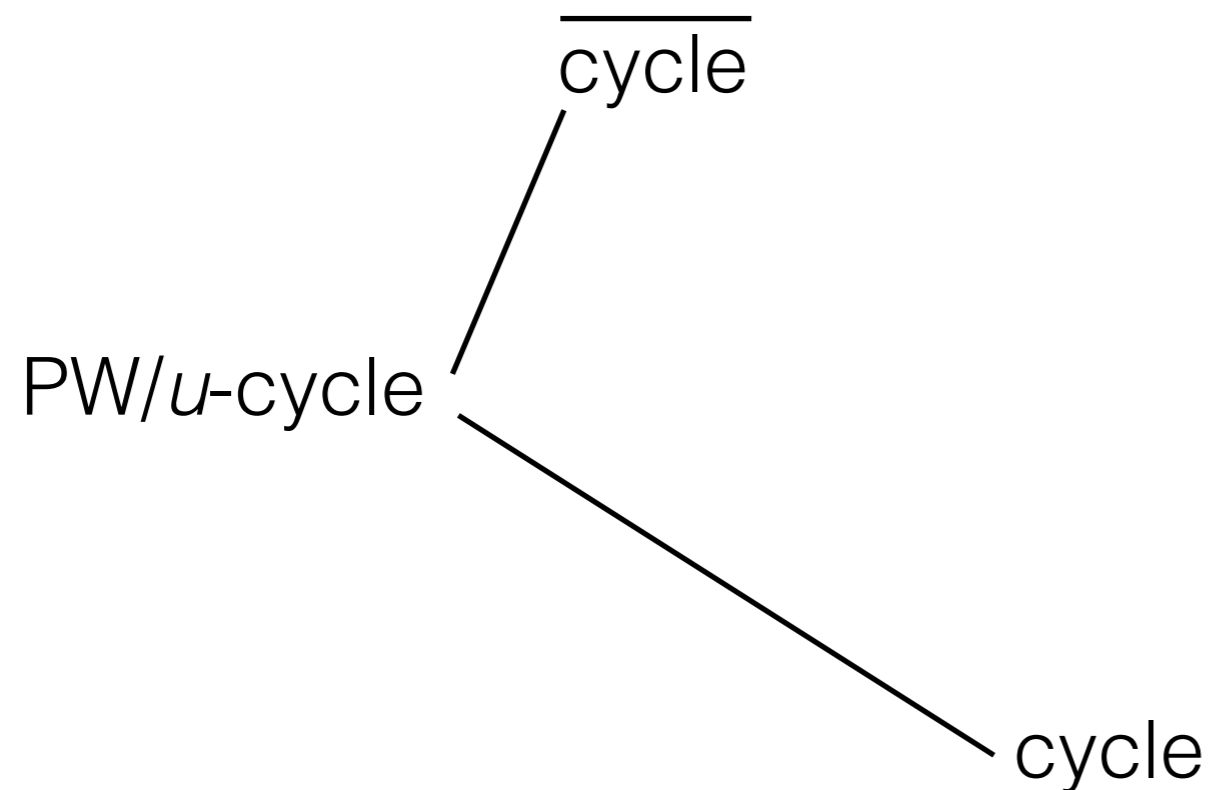
Constraining Communications

Proof: On the other hand, by contraposition,

PW/u -cycle

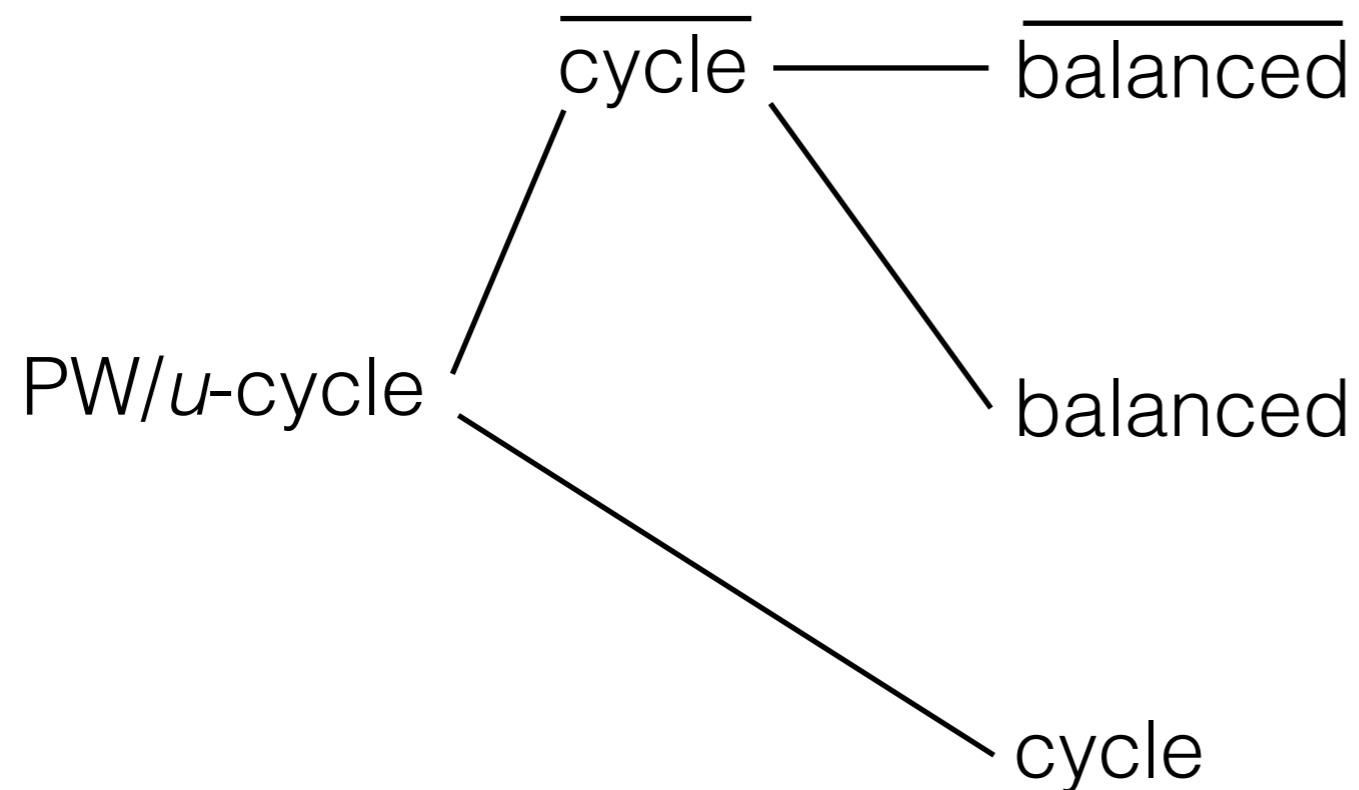
Constraining Communications

Proof: On the other hand, by contraposition,



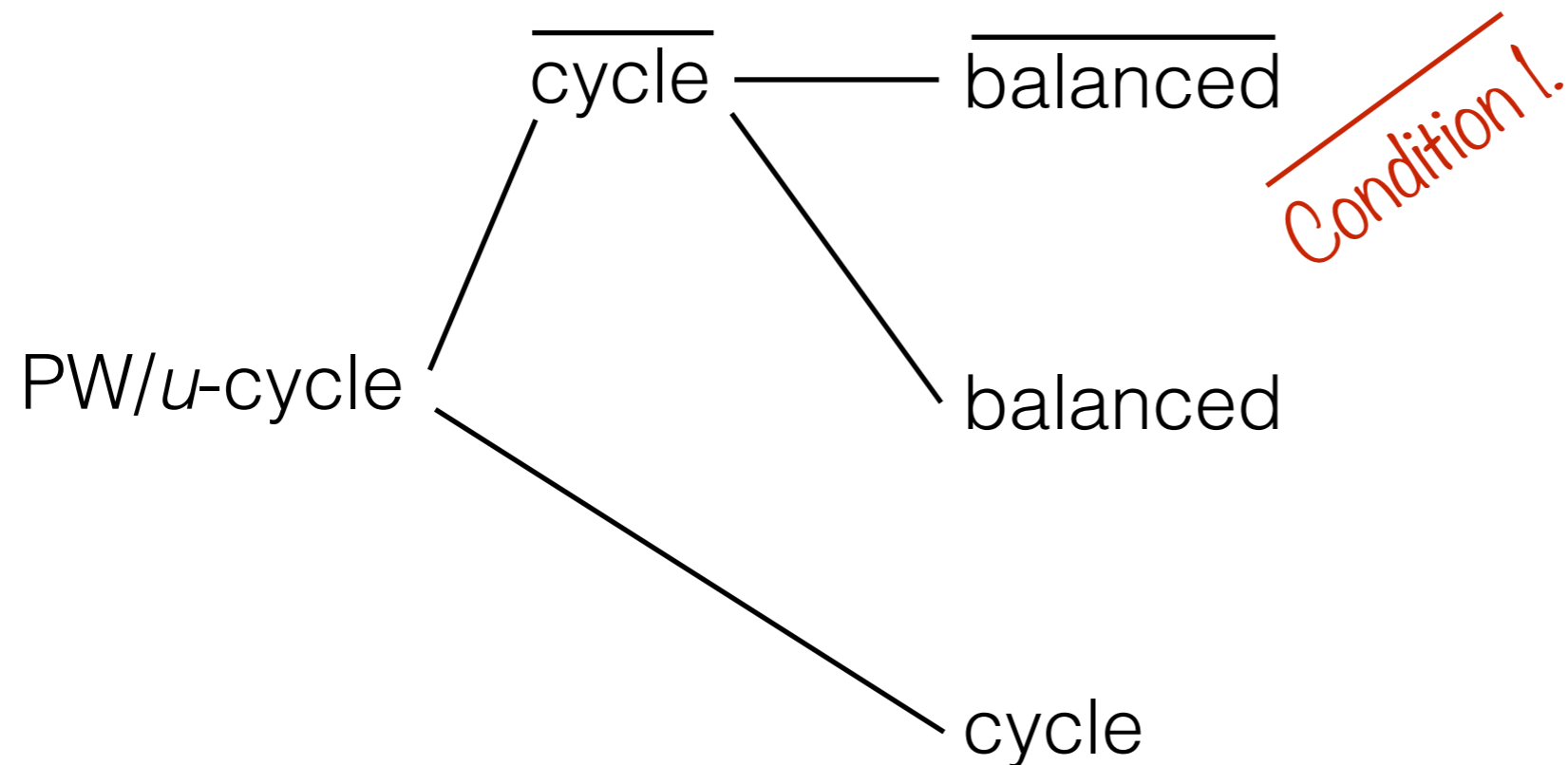
Constraining Communications

Proof: On the other hand, by contraposition,



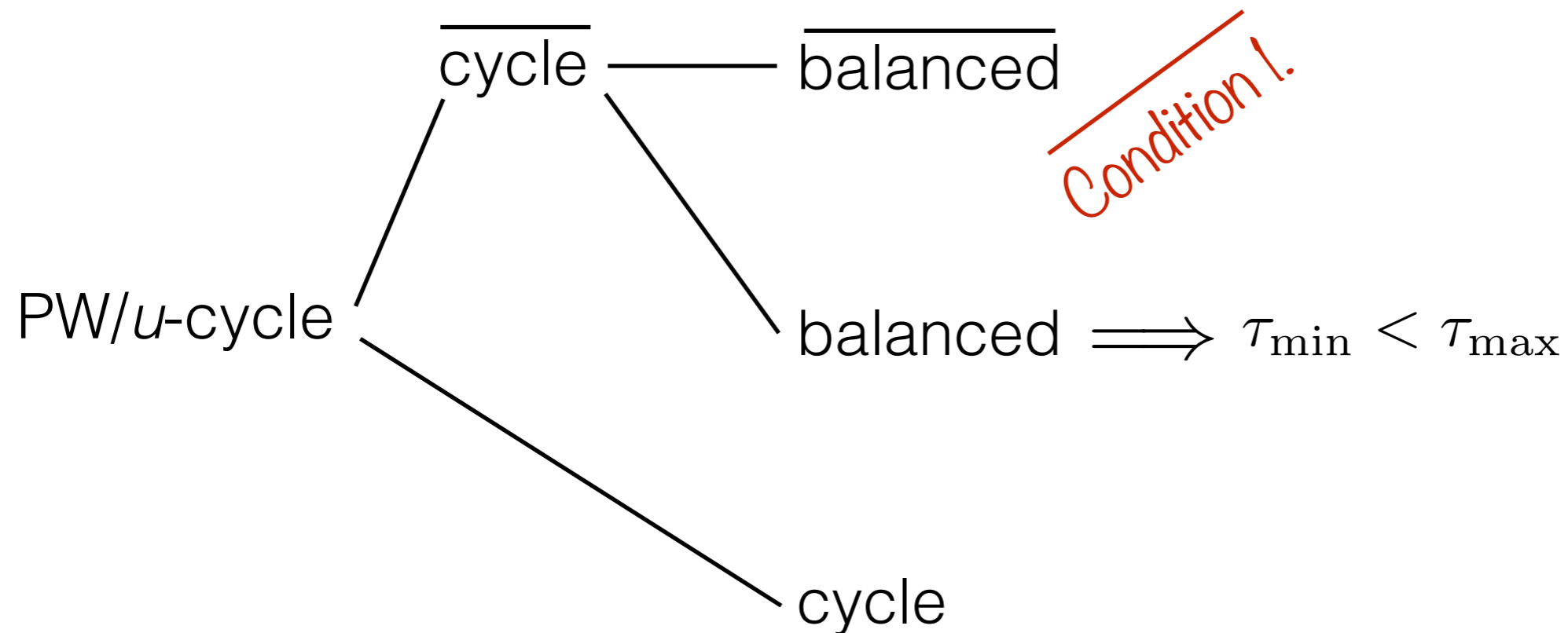
Constraining Communications

Proof: On the other hand, by contraposition,



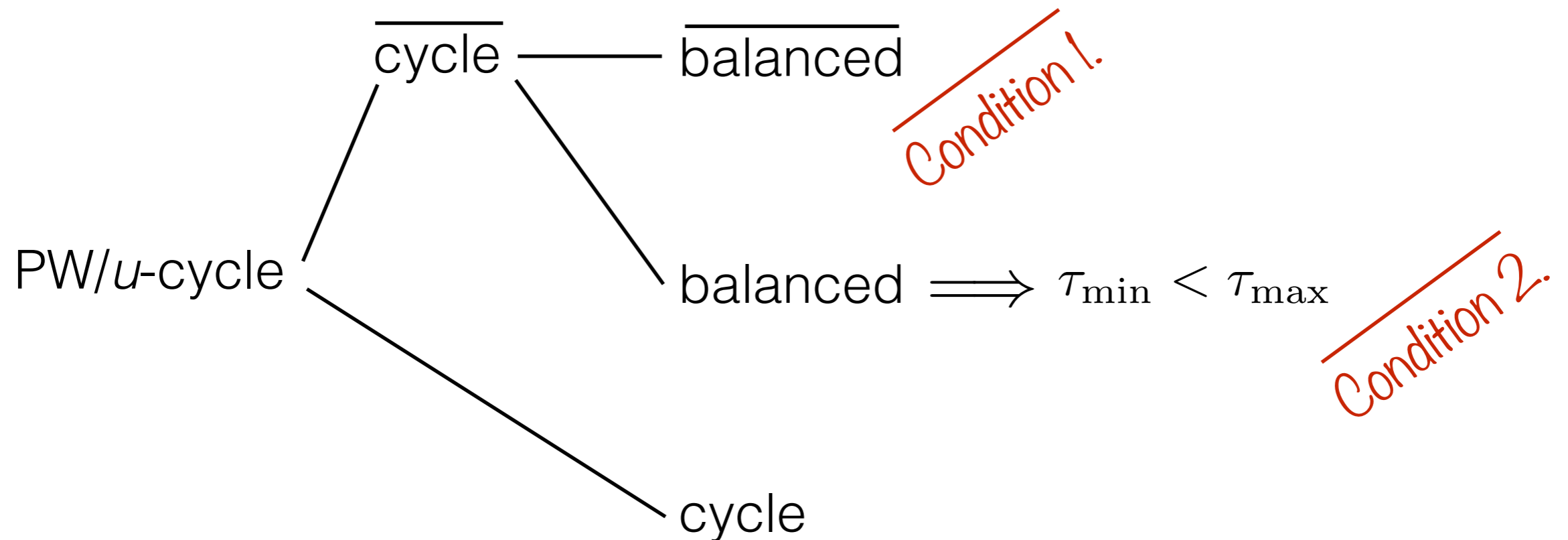
Constraining Communications

Proof: On the other hand, by contraposition,



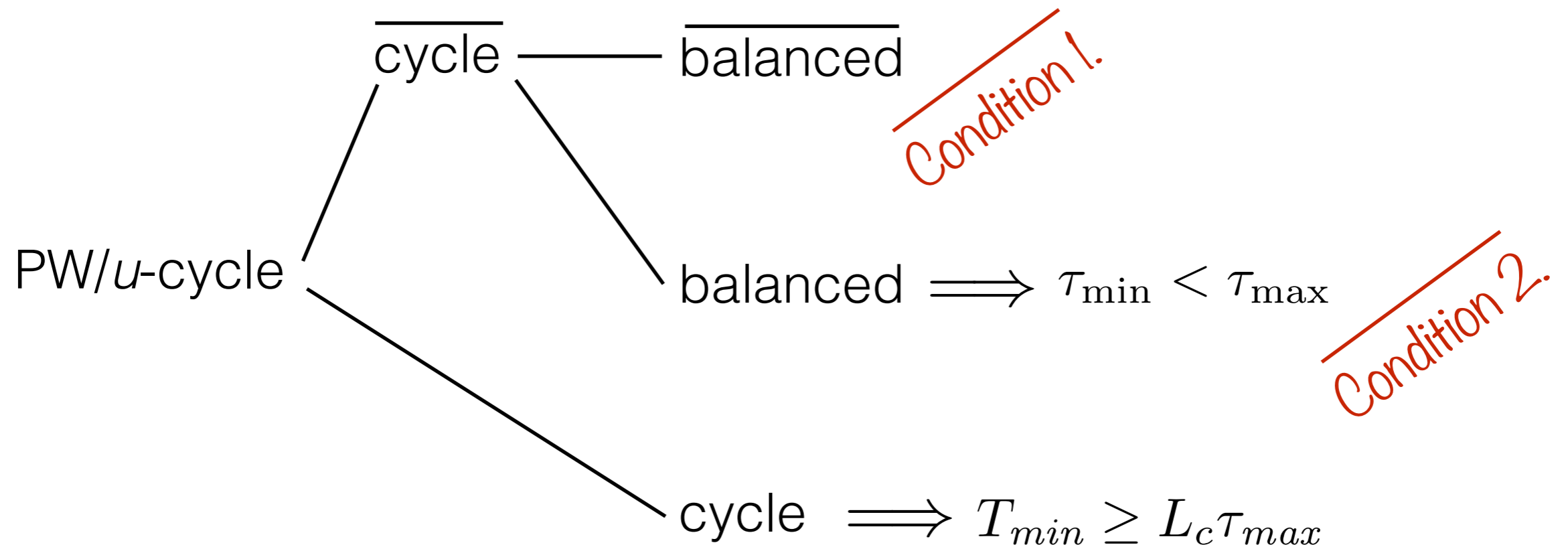
Constraining Communications

Proof: On the other hand, by contraposition,



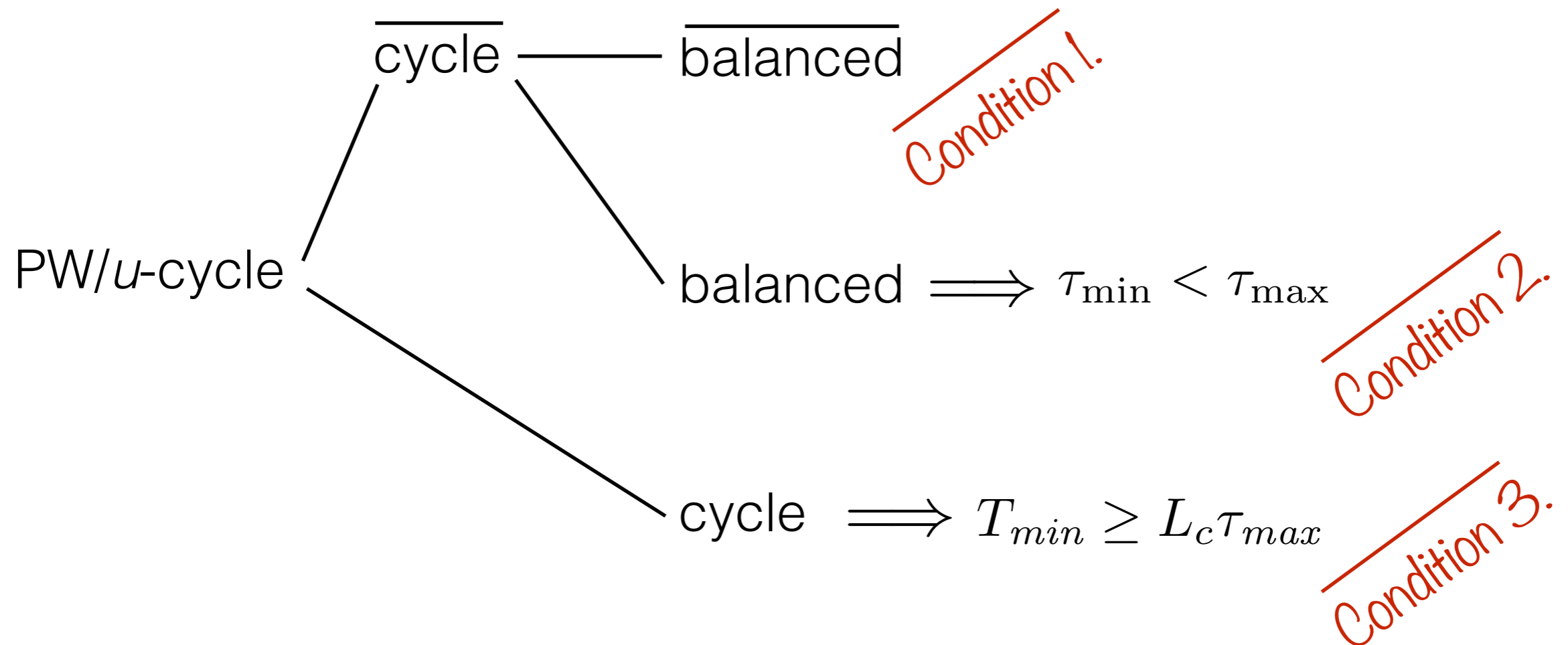
Constraining Communications

Proof: On the other hand, by contraposition,



Constraining Communications

Proof: On the other hand, by contraposition,



The Quasi-Synchronous Abstraction

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

The Quasi-Synchronous Abstraction

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

But there is no direct link between discrete- and real-time

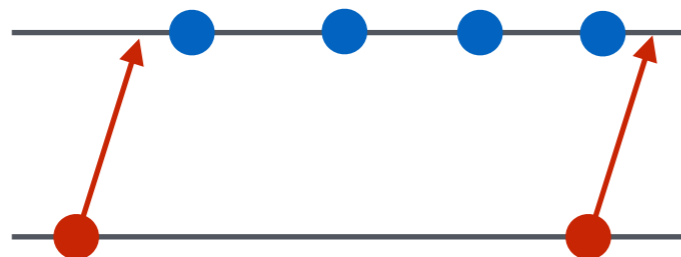
The Quasi-Synchronous Abstraction

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

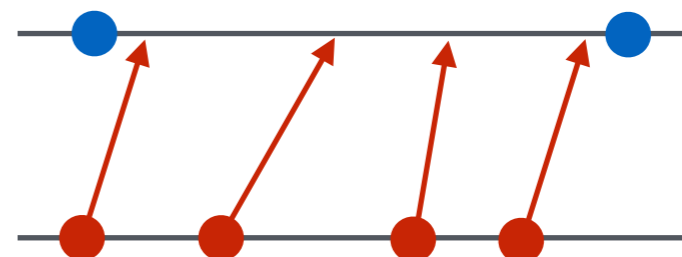
But there is no direct link between discrete- and real-time

For any node:

1. there is no more than n activations between two message receptions
2. there is no more than n message receptions between two activations



Condition 1.



Condition 2.

The Quasi-Synchronous Abstraction

Any of the two clocks cannot take the value “t” more than twice between two successive “t” values of the other one.

But there is no direct link between discrete- and real-time

Definition (n -Quasi-Synchrony): A quasi-periodic architecture is n -quasi-synchronous if for every trace t

1. there exists a unitary discretization f , and
2. for any node $A \Leftarrow B$, there is no chain of activation of length greater than n , that is no i and j such that

$$f(B_j) < f(A_i) < \dots < f(A_{i+n}) \leq f(B_{j+1})$$

$$f(A_j) \leq f(B_i) < \dots < f(B_{i+n}) < f(A_{j+1})$$

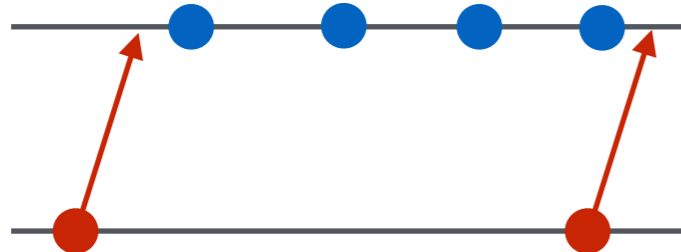
The Quasi-Synchronous Abstraction

This can be formalized by saying that the boolean vector stream composed of the two clocks should never contain the subsequence:

$$\begin{bmatrix} t \\ - \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$

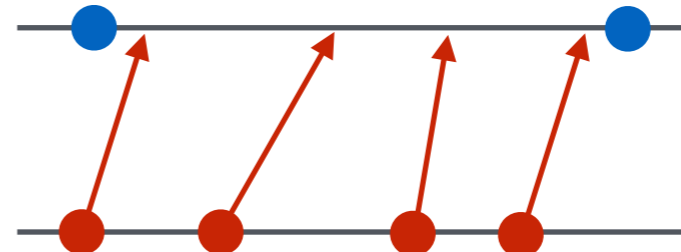
The boolean vector associated to nodes A and B never contains either of the subsequences

$$\left(\begin{bmatrix} t \\ f \end{bmatrix} \cdot \begin{bmatrix} f \\ f \end{bmatrix}^* \right)^n \cdot \begin{bmatrix} t \\ - \end{bmatrix}$$



Condition 1.

$$\begin{bmatrix} - \\ t \end{bmatrix} \cdot \left(\begin{bmatrix} f \\ f \end{bmatrix}^* \cdot \begin{bmatrix} f \\ t \end{bmatrix} \right)^n$$

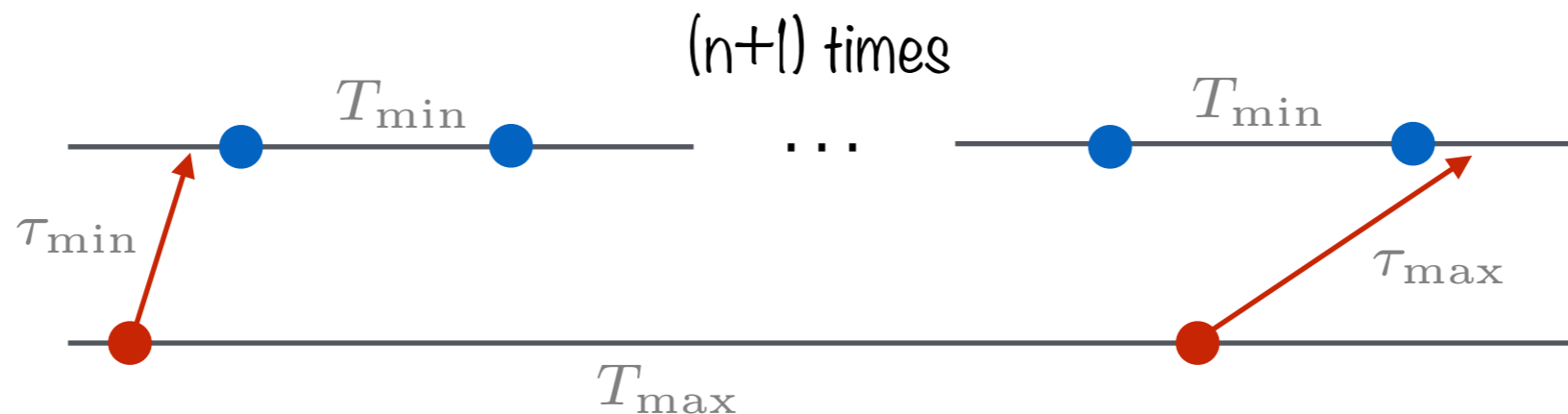


Condition 2.

The Quasi-Synchronous Abstraction

Theorem: A quasi-periodic architecture is n -quasi-synchronous if and only if

1. the conditions for unitary discretizability hold, and,
2. $nT_{\min} + \tau_{\min} \geq T_{\max} + \tau_{\max}$.



Worst-case scenario

Conclusion

The quasi-synchronous abstraction is a nice idea to reduce possible interleavings when using verification tools for discrete models.

Conclusion

The quasi-synchronous abstraction is a nice idea to reduce possible interleavings when using verification tools for discrete models.

Be careful with general systems.

It does not work for bus-based communications with more than two nodes.

Conclusion

The quasi-synchronous abstraction is a nice idea to reduce possible interleavings when using verification tools for discrete models.

Be careful with general systems.

It does not work for bus-based communications with more than two nodes.

It works for two nodes...

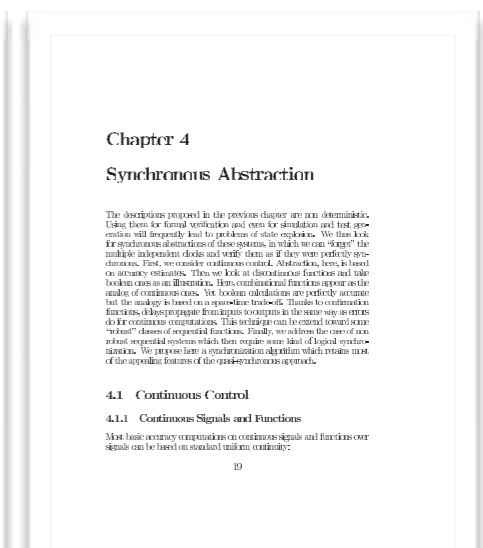
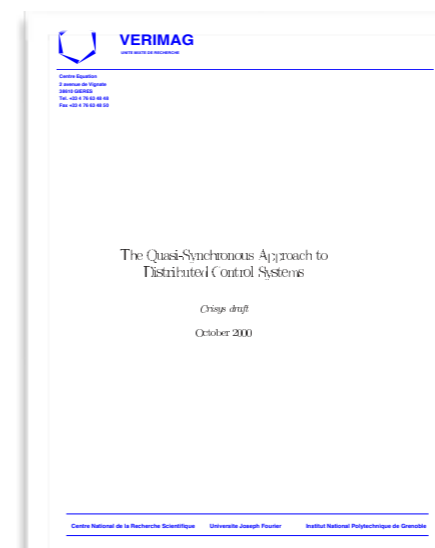
Conclusion

The quasi-synchronous abstraction is a nice idea to reduce possible interleavings when using verification tools for discrete models.

Be careful with general systems.

It does not work for bus-based communications with more than two nodes.

It works for two nodes...



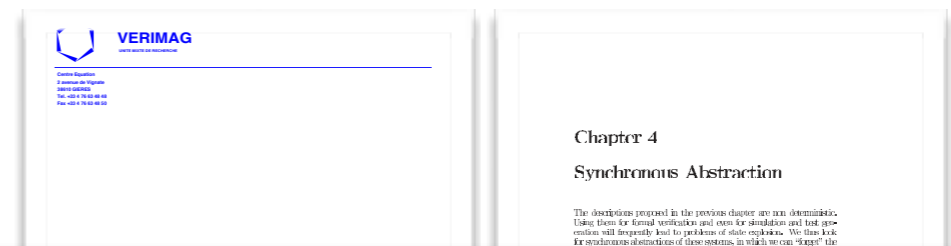
Conclusion

The quasi-synchronous abstraction is a nice idea to reduce possible interleavings when using verification tools for discrete models.

Be careful with general systems.

It does not work for bus-based communications with more than two nodes.

It works for two nodes...



The descriptions proposed in the previous chapter are non deterministic. Using them for formal verification and even for simulation and test generation will frequently lead to problems of state explosion.