Propositional Stabilisation Theory

Interface Types for Causality and Timing Analyses

Michael Mendler
Informatics Theory Group
Information Systems and Applied Computer Sciences
The Otto-Friedrich-University of Bamberg

What is this talk about?

Special purpose type theory (PST) for component interfaces

- to express different forms of causal response behaviour
- resulting in different degrees of constructivity
- specifying various forms of data-dependent schedulability and timing analyses.

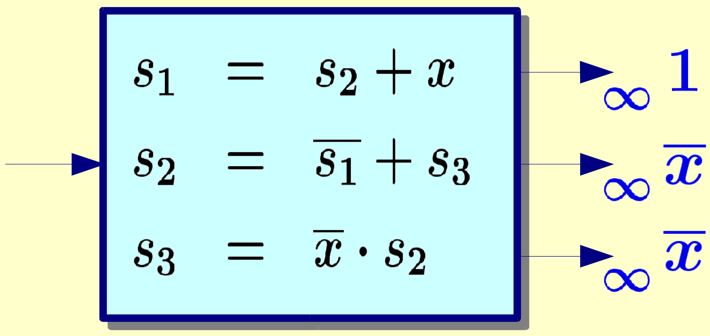
PST is

- purely propositional (enriching Boolean and Ternary Alg.)
- combining Time + Causality + Function
- of intuitionistic, 2nd-order expressiveness.

Constructiveness Analysis --

Pain-in-the-Neck, or Food-for-Thought ?

Motivation



For all inputs there is a unique stationary Boolean solution.
Thus, the system is logically reactive.
However, the system is not constructive.

Motivation

$$s_1 = \bot + x$$
$$s_2 = \overline{\bot} + \bot$$
$$s_3 = \overline{x} \cdot \bot$$

For all inputs there is a unique stationary Boolean solution.
Thus, the system is logically reactive.
However, the system is not constructive.

Motivation

$$\begin{aligned} s_1 &= \bot + x \\ s_2 &= \bot \\ s_3 &= \overline{x} \cdot \bot \end{aligned}$$

For all inputs there is a unique stationary Boolean solution.
Thus, the system is logically reactive.
However, the system is not constructive.

Motivation

$$\begin{aligned} s_1 &= s_2 + x \\ s_2 &= \overline{s_1} + s_3 \\ s_3 &= \overline{x} \cdot s_2 \end{aligned} \quad \approx \quad \begin{aligned} s_1 &= 1 \\ s_2 &= \overline{x} \\ s_3 &= \overline{x} \end{aligned}$$

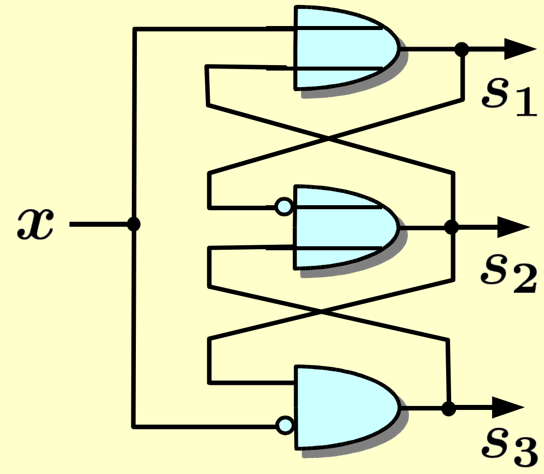
For all inputs there is a unique stationary Boolean solution.
Thus, the system is logically reactive.
However, the system is not constructive.

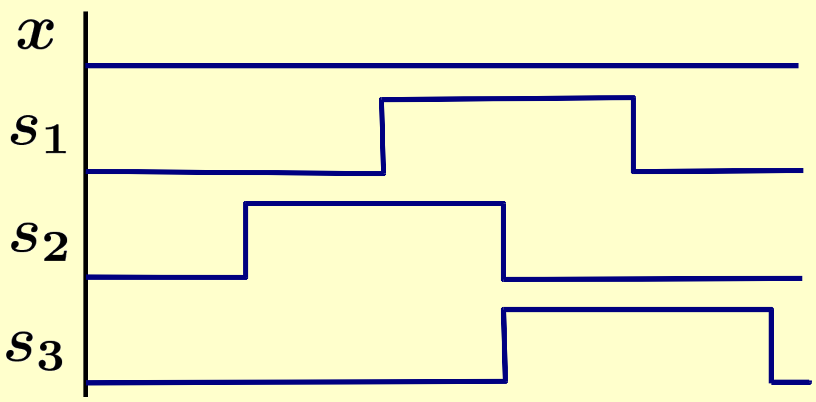
But what if we are compiling for a component-based and distributed architecture ?

Motivation

$$
\begin{aligned}
s_1 &= s_2 + x \\
s_2 &= \overline{s_1} + s_3 \\
s_3 &= \overline{x} \cdot s_2
\end{aligned}
$$

$\not\approx$





Oscillation under up-bounded inertial delay scheduling *[Brzozowski & Seger]*

Constructiveness Analysis

The distributed, multi-threaded execution of a logically reactive P may produce anomalous behaviour:

- -- deadlocks, oscillation,
- -- non-determinism, metastability.

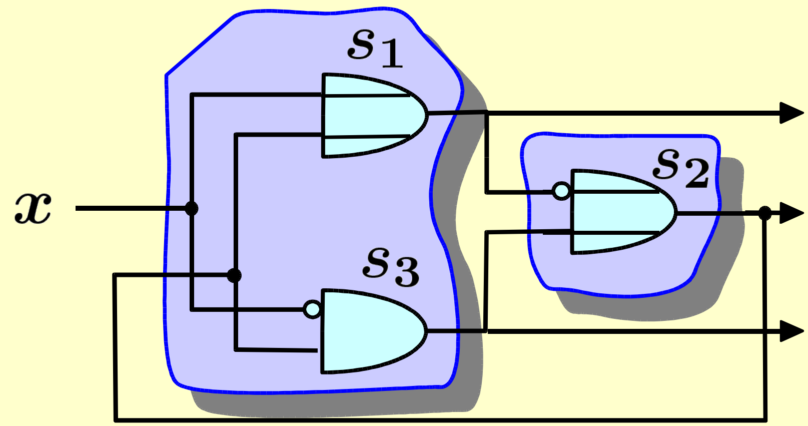
The problem may (often) be fixed at two levels:

Constrain Run-time System: Find a restricted schedule which avoids anomalies and guarantees stabilisation.

Constrain Code Generator: Harden P's code so it becomes constructive under arbitrary run-time schedules.

Example

$$\begin{aligned} s_1 &= s_2 + x \\ s_2 &= \overline{s_1} + s_3 \\ s_3 &= \overline{x} \cdot s_2 \end{aligned}$$



Oscillation can be avoided if we

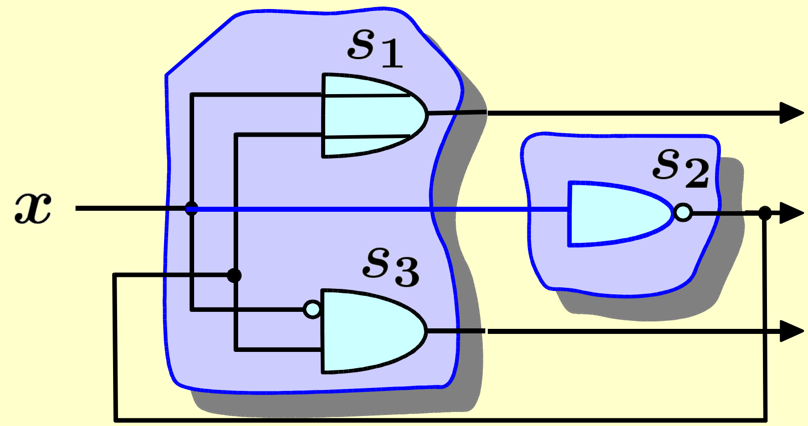
- schedule s_1, s_3 with higher priority than s_2 or
- implement s_1, s_3 atomically, as 2in/2out complex-gate.

Then, whenever s_2 is executed, we maintain the invariant

$$s_2 = \overline{s_1} + s_3 = \overline{x}$$

Example

$$s_1 = s_2 + x$$
$$s_2 = \overline{s_1} + s_3$$
$$s_3 = \overline{x} \cdot s_2$$



Oscillation can be avoided if we

- schedule s_1, s_3 with higher priority than s_2 or
- implement s_1, s_3 atomically, as 2in/2out complex-gate.

Then, whenever s_2 is executed, we maintain the invariant

$$s_2 = \overline{s_1} + s_3 = \overline{x}$$

- Alternatively, we may harden the code.

Degrees of Causality

There are many "causality improving" transformations:

- e.g., Boussinot, Schneider:

$$s \cdot f(s) \sqsubseteq s \cdot f(1)$$

$$s \cdot f + \overline{s} \cdot g \sqsubseteq s \cdot f + \overline{s} \cdot g + f \cdot g$$

- ... and there should be more.

Now,

- A Theory of Causal Interface Types
- Semantical characterisation of degrees of causality
- compositional analyses

Introducing PST Type Theory

PST — Type Theory

Types

- intuitionistic modal logic (modal operator "❍")
- ❍M "true" = M "valid in bounded time"

PST — Type Theory

Types

$$M ::= a{=}v \mid M \wedge N \mid M \vee N \mid M \supset N \mid \neg M \mid \circ M$$

$$a \in \mathsf{Sig} \quad v \in \mathbb{B}$$

PST — Type Theory

Specifying Reactions

$$\text{KSystem} \subseteq \text{Sig} \longrightarrow \mathbb{N} \longrightarrow \mathbb{B}$$

$$\text{KSystem} \models \boldsymbol{M} \text{ iff } \exists \boldsymbol{\delta} \in [\boldsymbol{M}]. \forall \boldsymbol{V} \in \text{KSystem}. \boldsymbol{V} \models \boldsymbol{\delta} : \boldsymbol{M}$$

Semantics

- M — stabilisation type (causality + function)
- $\boldsymbol{\delta} \in [\boldsymbol{M}]$ — timing constraint (λ-terms)
- $\boldsymbol{V} \models \boldsymbol{\delta} : \boldsymbol{M}$ — waveform $\boldsymbol{V} \in \text{Sig} \longrightarrow \mathbb{N} \longrightarrow \mathbb{B}$
  satisfies $\boldsymbol{M}$
  with timing constraint $\boldsymbol{\delta} \in [\boldsymbol{M}]$

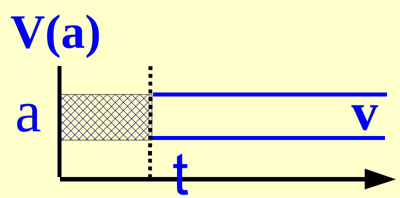
PST Timing Information

Type M		Timinig Information $[M]$
$M \wedge N$	conjunction	$[M \wedge N] = [M] \times [N]$ cartesian product
$M \vee N$	disjunction	$[M \vee N] = [M] + [N]$ disjoint union
$M \supset N$	implication	$[M \supset N] = [M] \rightarrow [N]$ function space
$\circ M$	modality	$[\circ M] = \mathbb{N} \times [M]$ propagation delay
$a{=}v$	atomic	$[a{=}v] = 1$ no information

Propositions-as-Types Principle

PST Waveform Specification

$V(a) \downarrow_t v$



“ Signal a stabilises to value v in waveform V as from time t”

V^δ is the time-shifted waveform $V^\delta(a)(t) = V(a)(t+\delta)$

$V \models 0 : a{=}v$ iff $V(a) \downarrow_0 v$

$V \models (c,d) : M \wedge N$ iff $V \models c : M$ and $V \models d : N$

$V \models ($ …

$V \models ($ …

$V \models f$ … $M].$

… $\Rightarrow$

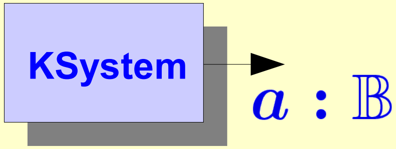
$V^\delta \models f(c) : N$

$V \models (\delta, c) : \circ M$ iff $V^\delta \models c : M$

Variation of the standard Realisability Interpretation for Intuitionistic Logic

Stabilisation Types for a Single Signal

In how many ways can we say an output responds with a Boolean ?



predicate logic	PST stabilisation type
$\forall V.\ \exists v.\ \exists t.\ V(a)\downarrow_t v$	$\neg\neg(a{=}1 \oplus a{=}0)$
$\exists v.\ \forall V.\ \exists t.\ V(a)\downarrow_t v$	$\neg\neg a{=}1 \vee \neg\neg a{=}0$
$\exists t.\ \forall V.\ \exists v.\ V(a)\downarrow_t v$	$\circ(a{=}1 \oplus a{=}0)$
$\exists v.\ \exists t.\ \forall V.\ V(a)\downarrow_t v$	$\circ a{=}1 \vee \circ a{=}0$
$\forall V.\ \exists v.\ \forall t.\ V(a)\downarrow_t v$	$a{=}1 \oplus a{=}0$
$\exists v.\ \forall V.\ \forall t.\ V(a)\downarrow_t v$	$a{=}1 \vee a{=}0$

$$\phi \oplus \psi =_{\mathrm{df}} ((\phi \supset \psi) \supset \psi) \wedge ((\psi \supset \phi) \supset \phi)$$

Three Levels of Signal Evaluation

$$V^{\infty}(a) \quad =_{\mathrm{df}} \quad \begin{cases} \mathbf{1} & \exists t.\ V(a) \downarrow_t \mathbf{1} \\ \mathbf{0} & \exists t.\ V(a) \downarrow_t \mathbf{0} \\ \bot & \text{otherwise} \end{cases}$$

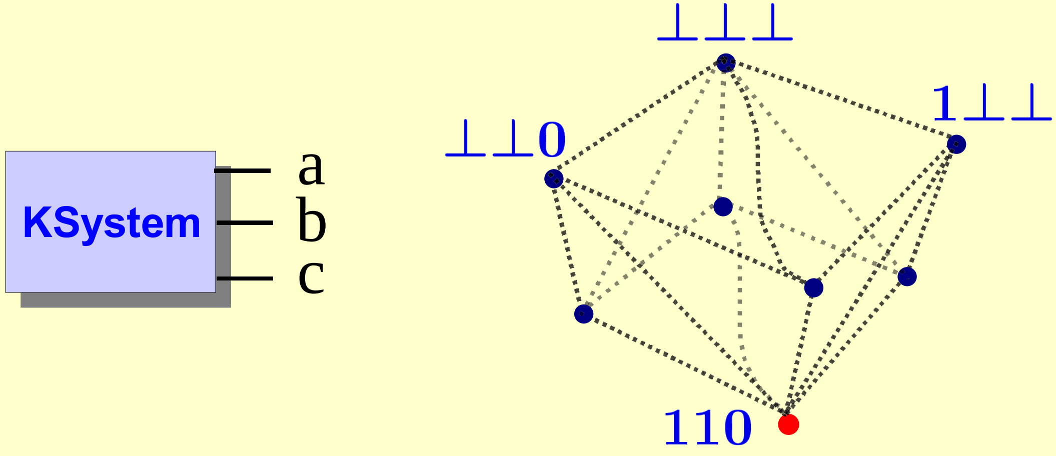
$f : \mathbb{B}^2 \longrightarrow \mathbb{B}$ Boolean function

$f^{\infty} : \mathbb{K}^2 \longrightarrow \mathbb{K}$ ternary extension of f

predicate logic	PST stabilisation type
$\forall V. \exists t.\ V(c) \downarrow_t f^{\infty}(V^{\infty}(a), V^{\infty}(b))$	$\neg\neg(c = f(a, b))$
$\exists t. \forall V.\ V(c) \downarrow_t f^{\infty}(V^{\infty}(a), V^{\infty}(b))$	$\circ(c = f(a, b))$
$\forall t. \forall V.\ V(c) \downarrow_t f^{\infty}(V^{\infty}(a), V^{\infty}(b))$	$c = f(a, b)$

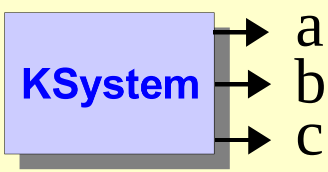
Causality Types for Signal Vectors

In how many "causal ways" can we produce a unique stationary response (logical correctness) ?

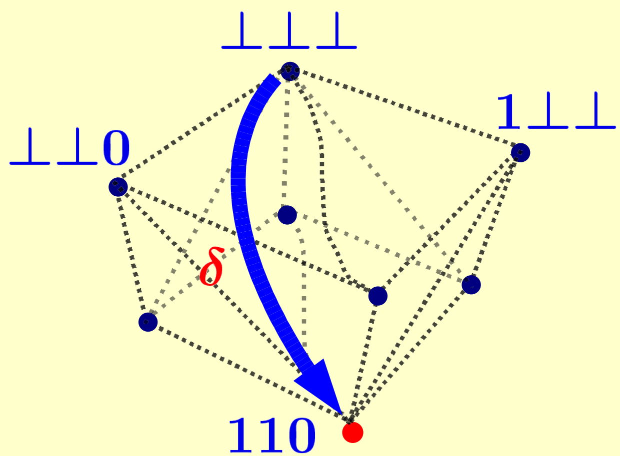


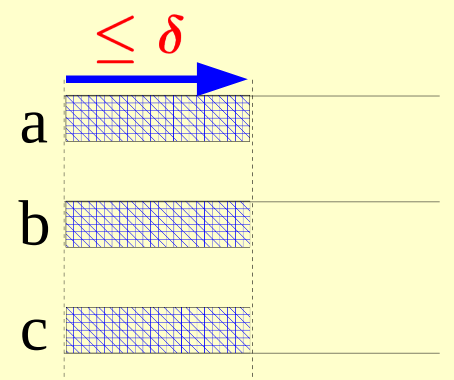
Causality Types for Signal Vectors

In how many "causal ways" can we produce a unique stationary response (logical correctness) ?



$\delta : M_1$



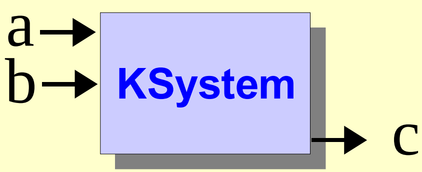


$t_a = t_b = t_c \leq \delta$

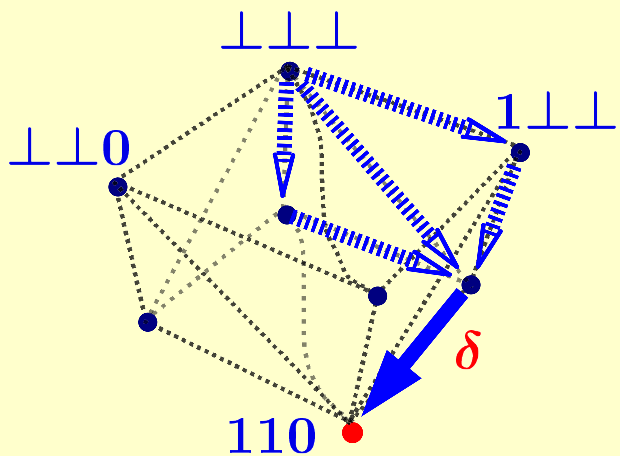
$$M_1 \;=\; \circ(a{=}1 \wedge b{=}1 \wedge c{=}0) \wedge (a{=}1 \supset b{=}1) \wedge (b{=}1 \supset c{=}0) \wedge (c{=}0 \supset a{=}1)$$

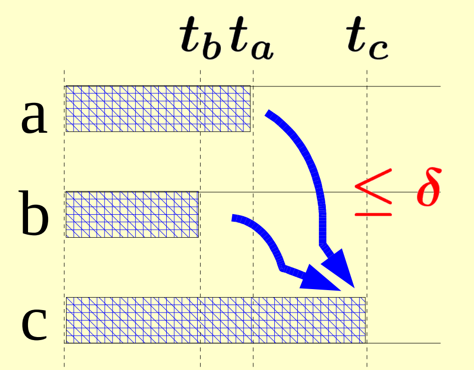
Causality Types for Signal Vectors

In how many “causal ways” can we produce a unique stationary response (logical correctness) ?



$\delta : M_2$





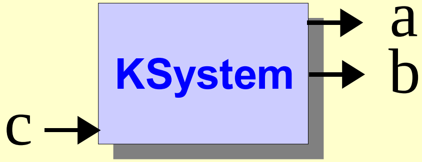
$$t_c < \infty$$

$$max(t_a, t_b) \leq t_c \leq \max(t_a, t_b) + \delta$$

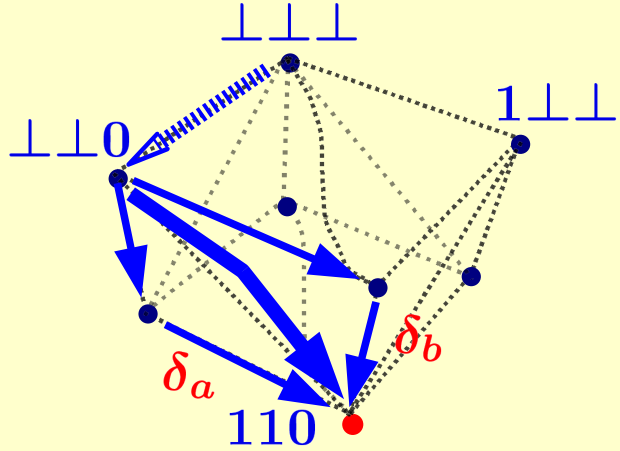
$$M_2 \;=\; ((a{=}1 \wedge b{=}1) \supset \circ c{=}0) \wedge (c{=}0 \supset (a{=}1 \wedge b{=}1)) \wedge \neg\neg c{=}0$$

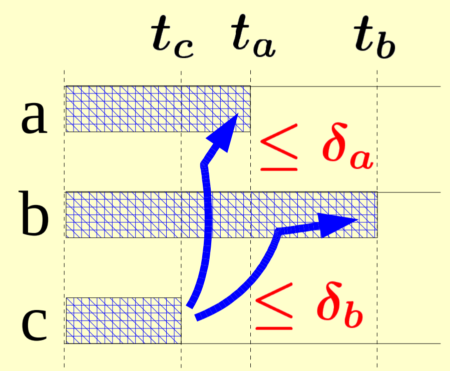
Causality Types for Signal Vectors

In how many "causal ways" can we produce a unique stationary response (logical correctness) ?



$(\delta_a, \delta_b) : M_3$





$t_c < \infty$

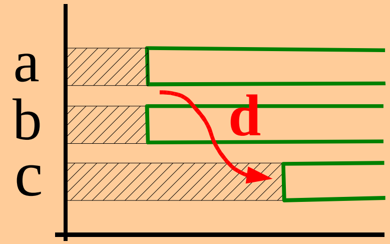
$t_c \leq t_a, t_b \leq t_c + \delta_a$

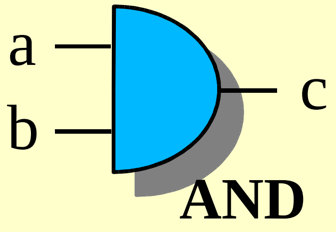
$$M_3 \;=\; (c{=}0 \supset (\circ a{=}1 \wedge \circ b{=}1)) \wedge ((a{=}1 \vee b{=}1) \supset c{=}0) \wedge \neg\neg c{=}0$$

Interfaces for Causality and Timing

Example — Stabilisation Models

d:AND data-independent "topological" model





d timing information

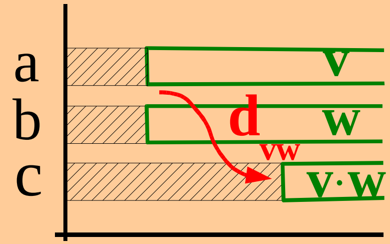
$\mathbf{d} \in \mathbf{Nat} \approx [\ \mathbf{AND}\ ]$

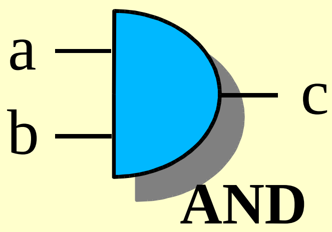
AND type specification

$$((a{=}1 \oplus a{=}0) \wedge (b{=}1 \oplus b{=}0)) \supset \circ(c{=}1 \oplus c{=}0)$$

Example — Stabilisation Models

d:AND data-dependent "topolocial" model





d timing information

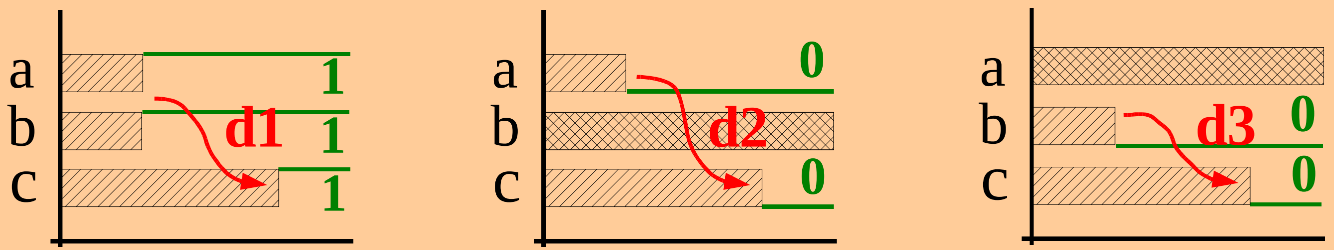
$$d = (d_{00}, d_{01}, d_{10}, d_{11}) \in \text{Nat}^4 \approx [\ \text{AND}\ ]$$

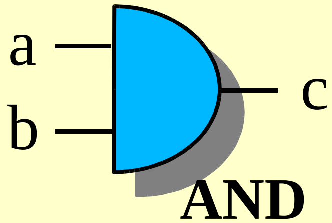
AND type specification

$$((a{=}1 \vee a{=}0) \wedge (b{=}1 \vee b{=}0)) \supset \circ(c = a \cdot b)$$

Example — Stabilisation Models

d:AND data-dependent "floating mode" model





d timing information

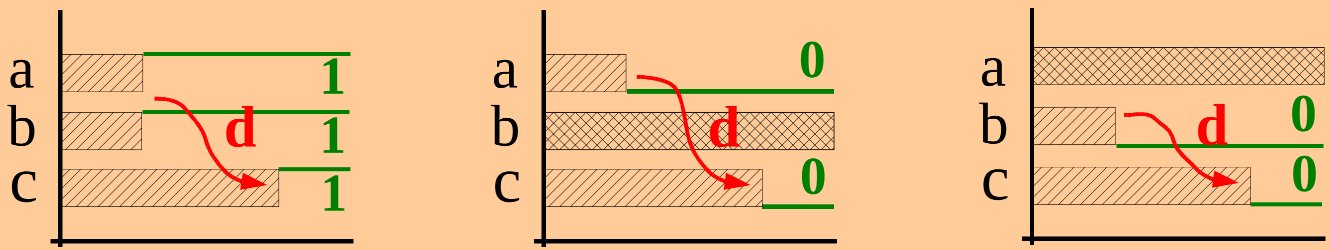
d = (d1, d2, d3) $\in$ Nat^3 $\approx$ [AND]

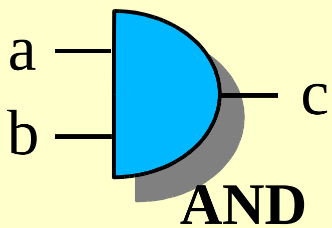
AND type specification

$$((a{=}1 \wedge b{=}1) \vee a{=}0 \vee b{=}0) \supset \circ(c = a \cdot b)$$

Example — Stabilisation Models

d:AND **data-independent "floating mode" model**





d **timing information**

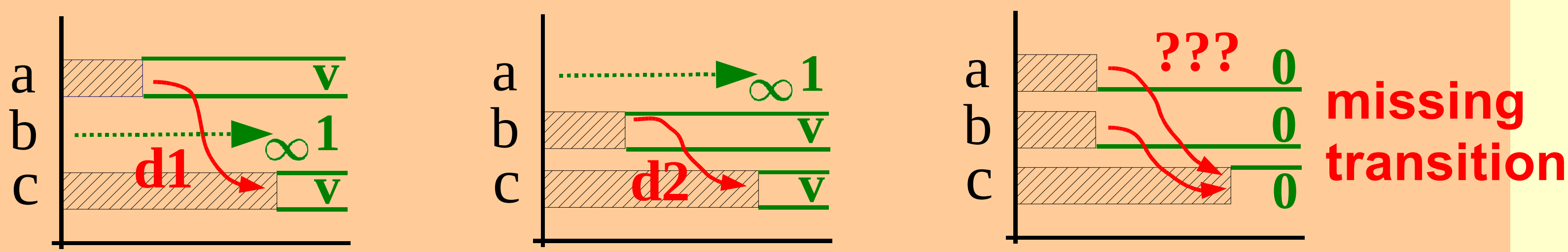
d $\in$ **Nat ≈ [AND]**

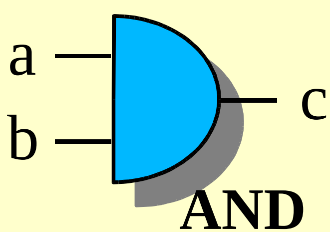
AND type specification

$$((a{=}1 \wedge b{=}1) \oplus a{=}0 \oplus b{=}0) \supset \circ(c = a \cdot b)$$

Example — Stabilisation Models

d:AND   data-dependent "static sensitization" model





d timing information

$$d = (d1, d2) \in Nat^2 \approx [\ AND\ ]$$

AND type specification

$$((\neg\neg a{=}1 \wedge b = v) \vee (a = v \wedge \neg\neg b{=}1)) \supset \circ(c = v)$$

Summary PST

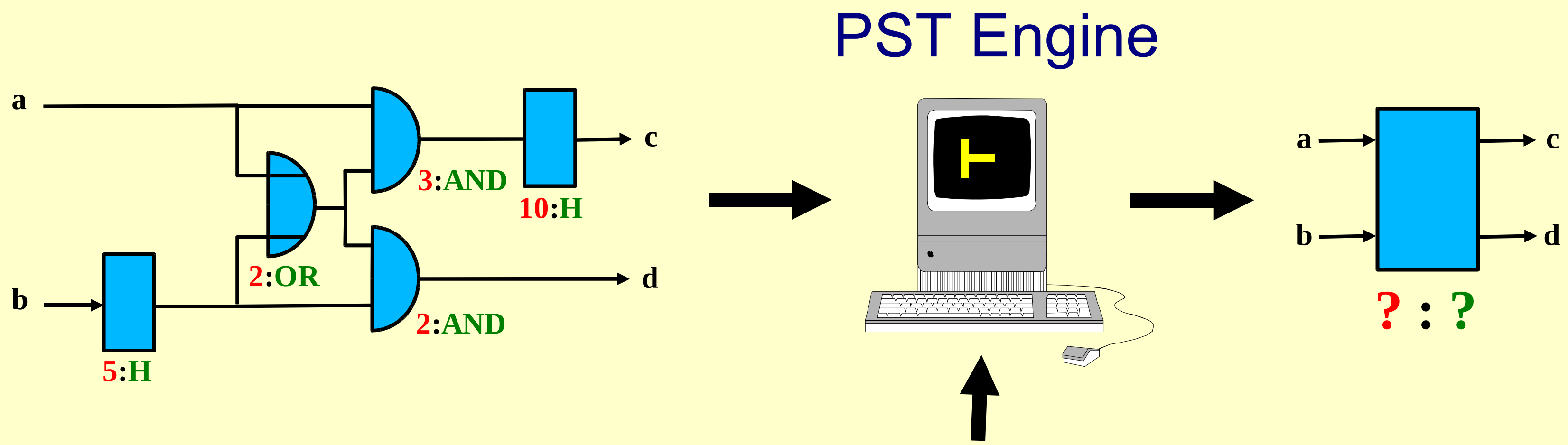
- PST types are intuitionistic, fully compatible with ternary model.
- The difference between reactive and stationary behaviour is the difference between M and $\neg\neg M$.
- A fixed stationary behaviour $\neg\neg M$ can be implemented by various reactive types (causal/timing models) M_1, M_2, M_3 ..., such that

  $$\neg\neg M_1 \equiv \neg\neg M, \quad \neg\neg M_2 \equiv \neg\neg M, \quad \neg\neg M_3 \equiv \neg\neg M, \ldots$$

- PST can characterise different timing analyses...

PST Timing Analyses

PST Timing Analysis



semantical or syntactical deduction in PST

type synthesis and type transformation

Conclusion

PST Reactiveness Analysis — Advantages

- **Adjustable granularity of data abstraction**
- **Compositionality** (= "*divide and conquer*" analyses)
- **Precision**

  - semantical meaning of computed delays is specified uniquely (= data type, type checking)
- **"Lossless" heuristics**

  - free exploration of search space through combination of partial (i.e., incorrect or suboptimal) analyses

PST Reactiveness Analysis — Results

- Deduction in PST captures correct and exact timing analyses for all *elementary* combinational stabilisation models.

- In this fragment a number of well-known analyses can be characterised:

Topological	
Statical	[Benkoski et.al. '90]
Polynomial	[Huang et.al. '91]
Floating	[Chen&Du '90, Devadas et.al. '91]
Viability	[McGeer '89]

Open Problems — Projects, PhD Topics

- **Theory**

  Complete characterisation of PST expressiveness

  Axiomatization

- **Implementation**

  Efficient data structures for fragments of PST

  Toolbox of composable (partial) heuristics

- **Application**

  Explore links: PST analyses – degrees of causality – distributed code generation

Literature

- M. Fairtlough, M. Mendler, Propositional Lax Logic. *Information and Computation, 137(1), Aug. 1997.*
- M. Mendler, Combinational timing analysis in intuitionistic propositional logic. *Formal Methods in System Design, 17(1), Aug. 2000.*
- M. Mendler, Characterising combinational timing analyses in intuitionistic modal logic. *Logic Journal of the IGPL, 8(6), Nov. 2000.*
- M. Fairtlough, M. Mendler, Intensional completeness in an extension of Gödel-Dummet Logic. *Studia Logica, Vol.73, Jan. 2003.*