Extracting exact time bounds from logical proofs

Mauro Ferrari Camillo Fiorentini Mario Ornaghi

Dipartimento di Scienze dell'Informazione
Università degli Studi di Milano
{ferram,fiorenti,ornaghi}@dsi.unimi.it

Abstract Accurate evaluation of delays of combinatorial circuits is crucial in circuit verification and design. In this paper we present a logical approach to timing analysis which allows us to compute exact stabilization bounds while proving the correctness of the boolean behavior.

1 Introduction

Accurate evaluation of delay times of combination logic components is crucial in circuit verification and design [4,7]. For example, it is fundamental in determining the clock rate. Thus, various *timing analysis* methods have been developed in the literature for detecting different kinds of delays, as worst case or minimum delays, as well as for evaluating exact data-depended delays (see [4,7] for a discussion). In traditional approaches, timing analysis does not take into account data dependencies. In this way *false paths*, i.e., paths that cannot be activated by any input, may be detected and false path elimination is necessary to ensure accurate timing analysis. Moreover, many approaches model worst case and minimum gate delays as constants, while such delays may depend on the rising and falling times of the input signals and more accurate *gate models* are needed [4].

Among the timing analysis methods that have been developed in the literature, here we consider the logically based ones, see, e.g., [2,12,6,1,7]. Their logical nature automatically excludes false paths, since they are based on sound logical semantics. A semantics represents an abstraction from the physical details, and takes into account only the aspects that are relevant for a given kind of analysis. For example, if we are only interested in the functional analysis of a combination logic network, models based on classical logic are sufficient, while three valued logic allows us to take into account unstable or unknown signals [2]. Models based on Intuitionistic Logic and on Lax Logic have been proposed in [6,7]; they support in a uniform way both functionality analysis and input-dependent timing analysis with accurate gate models.

In this paper we consider a modification of the approaches based on Intuitionistic and Lax logic. The main differences are in the adopted propositional language and in the formalization of time bounds. We consider optimal (exact) time bound evaluation for any kind of formulas, while the aforementioned approaches consider optimal bounds for restricted classes of formulas. Moreover, for suitable restrictions on waveforms, we have a completeness result for the logic $\mathbf{F}_{\mathrm{Cl}}$, which is a maximal axiomatizable and decidable intermediate logic [9].

In Section 2 we introduce and briefly discuss waveforms, and we define our propositional language and its waveform interpretation. In Section 3 we introduce time bounds and a constructive semantics based on them, and we show a calculus that is valid with respect to this semantics and allows us to prove functional correctness while evaluating, at the same time, exact delays. Finally, in Section 4 we briefly discuss the logical aspects of the proposed semantics.

2 Waveforms and Circuits

As in [7,8], a *signal* is a discrete timed boolean function $\sigma \in \mathbf{N} \to \mathbf{B}$. A *circuit* is characterized by a set $\mathbf{S}$ of *observables* and a *waveform* is a map $V \in \mathbf{S} \to \mathbf{N} \to \mathbf{B}$ associating with every observable a signal. A waveform represents an observable property of a circuit C, and an (observable) *behavior* of C is a set of waveforms.

For a waveform V, V^t denotes the waveform obtained by shifting V of t, i.e., $V^t(a)(k) = V(a)(t+k)$ for all $a \in \mathbf{S}, k \in \mathbf{N}$. We are interested in stabilization delays, hence in waveforms that stabilize at some time. In particular, we say that:

1. V is *stable* iff, for every $a \in \mathbf{S}$ and for every $t \in \mathbf{N}$, $V(a)(t) = V(a)(0)$;
2. V is *stable at* t, with $t \in \mathbf{N}$, iff V^t is stable;
3. V is *eventually stable* iff, for every $a \in \mathbf{S}$, there exists $t \in \mathbf{N}$ such that, for every $k \geq t$, $V(a)(k) = V(a)(t)$.

To express *stabilization properties* of waveforms and behaviors, we use a propositional language $\mathcal{L}_{\mathbf{S}}$ based on a denumerable set of *observables* $\mathbf{S} = \{a, b, c_1, c_2, \dots\}$. Formulas of $\mathcal{L}_{\mathbf{S}}$ are inductively defined as follows: for every $a \in \mathbf{S}$, a is an *atomic* formula of $\mathcal{L}_{\mathbf{S}}$; if $A, B \in \mathcal{L}_{\mathbf{S}}$, then $A \wedge B$, $A \vee B$, $A \to B$, $\neg A$, $\Box A$ belong to $\mathcal{L}_{\mathbf{S}}$.

We say that a waveform V *validates a stabilization property* A *at time* t, written $t, V \Vdash A$, if one of the following conditions holds:

$t, V \Vdash a$, where $a \in \mathbf{S}$, iff $V(a)(k) = 1$ for all $k \geq t$;
$t, V \Vdash \Box B$ iff $k, V \Vdash B$ for some $k \geq t$;
$t, V \Vdash B \wedge C$ iff $t, V \Vdash B$ and $t, V \Vdash C$;
$t, V \Vdash B \vee C$ iff either $t, V \Vdash B$ or $t, V \Vdash C$;
$t, V \Vdash B \to C$ iff, for every $k \geq t$, if $k, V \Vdash B$, then $l, V \Vdash C$ for some $l \geq k$;
$t, V \Vdash \neg a$, where $a \in \mathbf{S}$, iff $V(a)(k) = 0$ for all $k \geq t$;
$t, V \Vdash \neg\Box B$ iff $k, V \Vdash \neg B$ for some $k \geq t$;
$t, V \Vdash \neg(B \wedge C)$ iff either $t, V \Vdash \neg B$ or $t, V \Vdash \neg C$;
$t, V \Vdash \neg(B \vee C)$ iff $t, V \Vdash \neg B$ and $t, V \Vdash \neg C$;
$t, V \Vdash \neg(B \to C)$ iff $t, V \Vdash B$ and $t, V \Vdash \neg C$;
$t, V \Vdash \neg\neg B$ iff $t, V \Vdash B$.

It is easy to check that $t, V \Vdash A$ implies $h, V \Vdash A$, for all $h \geq t$ and that $t, V^k \Vdash A$ iff $t + k, V \Vdash A$.

For a atomic, a and $\neg a$ denote the stability of the observable signal $V(a)$ (at time t, with value 1 and 0 respectively). Implication underlies a propagation delay, i.e., $t, V \Vdash A \to B$ means that, whenever, at some $t' \geq t$, A "stabilizes" ($t', V \Vdash A$), after a certain amount of time s, B will "stabilize" ($t' + s, V \Vdash B$). The unary modal operator $\Box$ means future stabilization. Validation of $\wedge, \vee$ is defined as expected. As for the negation, the above semantics defines it as a constructive negation and the validity of $\neg A$ is defined recursively on the structure of A (see [10]). We remark that $t, V \Vdash \neg\Box B$ is stronger than $t, V \nVdash \Box B$. See Section 3 for a comparison between our semantics and the one of [7,8].

A logical characterization of stable and eventually stable waveforms is the following: V is *stable* iff $0, V \Vdash A \vee \neg A$ for every formula A, and V is *eventually stable* iff $0, V \Vdash \Box A \vee \neg\Box A$ for every formula A.

If V is an eventually stable waveform, we can associate with it the classical interpretation V^{CL} such that, for every $a \in \mathbf{S}$, $V^{\mathrm{CL}}(a) = 0$ if $0, V \Vdash \neg\Box a$ and $V^{\mathrm{CL}}(a) = 1$ if $0, V \Vdash \Box a$.

Given a boolean function $f : \mathbf{B}^n \to \mathbf{B}$, we say that a formula $F(a_1, \ldots, a_n, b)$ of $\mathcal{L}_\mathbf{S}$ *represents* f iff, for every eventually stable waveform V, $0, V \Vdash \Box F(a_1, \ldots, a_n, b)$ iff $f(V^{\mathrm{CL}}(a_1), \ldots, V^{\mathrm{CL}}(a_n)) = V^{\mathrm{CL}}(b)$.

To give an example, we provide the specification of the XOR circuit of Figure 1 and of its components. The behavior of the gates INV and NAND is specified by:

$$\mathrm{INV}(x, y) \equiv (x \to \neg y) \wedge (\neg x \to y)$$
$$\mathrm{NAND}(x, y, z) \equiv (x \wedge y \to \neg z) \wedge (\neg x \vee \neg y \to z)$$

and it is easy to check that such formulas represent the corresponding boolean functions $inv : \mathbf{B} \to \mathbf{B}$ and $nand : \mathbf{B}^2 \to \mathbf{B}$. Similarly, the behavior of the XOR circuit is specified by the formula

$$\mathrm{XOR}(x, y, z) \equiv ((x \wedge \neg y) \vee (\neg x \wedge y) \to z) \wedge ((x \wedge y) \vee (\neg x \wedge \neg y) \to \neg z)$$

representing the boolean function $xor : \mathbf{B}^2 \to \mathbf{B}$.

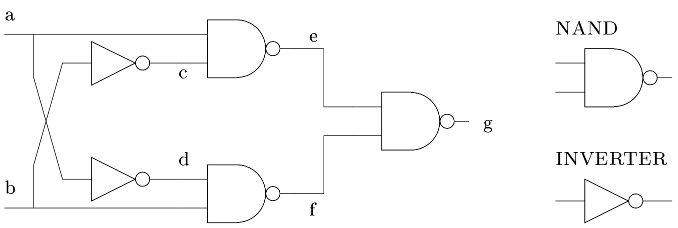

Figure 1.

The *formal verification task* of the circuit of Figure 1 consists in exhibiting a formal proof (in the adequate logic) of the formula

$$\mathrm{INV}(b, c) \wedge \mathrm{NAND}(a, c, e) \wedge \mathrm{INV}(a, d) \wedge \mathrm{NAND}(b, d, f) \wedge \mathrm{NAND}(e, f, g) \to \mathrm{XOR}(a, b, g)$$

If our aim is only to prove the correctness of the above circuit classical logic is sufficient. But if we aim to extract information about the stabilization delays of the circuit from the correctness proof, we need to introduce an intensional semantics of formulas that takes into account temporal information.

3 Stabilization Bounds

The validation $\Vdash$ provides an interpretation of formulas as stabilization properties, but the information about stabilization delays is not explicit. To extract stabilization delays we need an analysis of all the waveforms of a behavior. To deal with delays in our logic, we use *stabilization bounds.* They have been introduced in [6] and are inspired by evaluation forms introduced in [10]. Evaluation forms correspond to structural truth evaluations of formulas, and stabilization bounds combine both truth and timing analysis.

Different kinds of stabilization bounds correspond to different timing analyses. In [7] the information about delays is linked to the operator $\Box$ (indicated by $\bigcirc$ in [7]). In contrast, we interpret $\Box$ as a “don't care” operator and we do not associate any time information with it (the only possible delay is 0), but we associate a stabilization information with atomic formulas and with every logical connective not in the scope of the $\Box$ operator. In particular, a stabilization bound for a and $\neg a$, with $a \in \mathbf{S}$, fixes an upper bound for the stabilization of the signal $V(a)$. The stabilization bounds for $\wedge, \rightarrow, \vee$ are defined as in [7], while the interpretation of $\neg$ and $\Box$ is peculiar of our approach.

Formally, we assign to every formula A of $\mathcal{L}_{\mathbf{S}}$ a set of *stabilization bounds* $\lceil A \rceil$ and an equivalence relation $\sim_A$ between elements of $\lceil A \rceil$, inductively on the structure of A:

– If $A = a$ or $A = \neg a$, with $a \in \mathbf{S}$, then $\lceil A \rceil = \mathbf{N}$, and $t \sim_A t'$ for every $t, t' \in \lceil A \rceil$.
– If $A = \Box B$ or $A = \neg\Box B$ then $\lceil A \rceil = 0$, and $0 \sim_A 0$.
– $\lceil B \wedge C \rceil = \lceil B \rceil \times \lceil C \rceil$ and $(\beta, \gamma) \sim_{B \wedge C} (\beta', \gamma')$ iff $\beta \sim_B \beta'$ and $\gamma \sim_C \gamma'$.
– $\lceil A_1 \vee A_2 \rceil = \lceil A_1 \rceil \oplus \lceil A_2 \rceil$ (where $\oplus$ denotes the disjoint sum, that is the set of pairs $(1, \alpha)$ or $(2, \alpha')$ with $\alpha \in \lceil A_1 \rceil$ and $\alpha' \in \lceil A_2 \rceil$) and $(i, \alpha) \sim_{A_1 \vee A_2} (j, \alpha')$ iff $i = j$ and $\alpha \sim_{A_i} \alpha'$.
– $\lceil B \rightarrow C \rceil = \{f \mid f : \lceil B \rceil \rightarrow \lceil C \rceil \text{ s.t. } \beta \sim_B \beta' \text{ implies } f(\beta) \sim_C f(\beta')\}$, and $f \sim_{B \rightarrow C} f'$ iff $f(\beta) \sim_C f'(\beta)$ for every $\beta \in \lceil B \rceil$.
– $\lceil \neg(A_1 \wedge A_2) \rceil = \lceil \neg A_1 \rceil \oplus \lceil \neg A_2 \rceil$ and $(i, \alpha) \sim_{\neg(A_1 \wedge A_2)} (j, \alpha')$ iff $i = j$ and $\alpha \sim_{\neg A_i} \alpha'$.
– $\lceil \neg(B \vee C) \rceil = \lceil \neg B \rceil \times \lceil \neg C \rceil$ and $(\beta, \gamma) \sim_{\neg(B \vee C)} (\beta', \gamma')$ iff $\beta \sim_{\neg B} \beta'$ and $\gamma \sim_{\neg C} \gamma'$.
– $\lceil \neg(B \rightarrow C) \rceil = \lceil B \rceil \times \lceil \neg C \rceil$ and $(\beta, \gamma) \sim_{\neg(B \rightarrow C)} (\beta', \gamma')$ iff $\beta \sim_B \beta'$ and $\gamma \sim_{\neg C} \gamma'$.
– $\lceil \neg\neg B \rceil = \lceil B \rceil$ and $\beta \sim_{\neg\neg B} \beta'$ iff $\beta \sim_B \beta'$.

$\sim_A$ has been introduced to cut undesired functions in the definition of $\lceil B \rightarrow C \rceil$. Intuitively, a stabilization bound $\alpha \in \lceil A \rceil$ intensionally represents a set of waveforms V that validate A for the "same reasons" and with the "same delay bounds". Formally, we say that V *validates* A *with stabilization bound* α, and we write $\alpha, V \models A$, if one of the following conditions holds.

- $t, V \models a$, with $a \in \mathbf{S}$, iff $t, V \Vdash a$;
- $t, V \models \neg a$, with $a \in \mathbf{S}$, iff $t, V \Vdash \neg a$;
- $0, V \models \Box B$ iff $t, V \Vdash B$ for some $t \in \mathbf{N}$;
- $(\beta, \gamma), V \models B \wedge C$ iff $\beta, V \models B$ and $\gamma, V \models C$;
- $(i, \alpha), V \models A_1 \vee A_2$ iff $\alpha, V \models A_i$, where $i \in \{1, 2\}$;
- $f, V \models B \rightarrow C$ iff, for every $t \in \mathbf{N}$ and $\beta \in \lceil B \rceil$, $\beta, V^t \models B$ implies $f(\beta), V^t \models C$;
- $0, V \models \neg\Box B$ iff $t, V \Vdash \neg B$ for some $t \in \mathbf{N}$;
- $(i, \alpha), V \models \neg(A_1 \wedge A_2)$ iff $\alpha, V \models \neg A_i$, where $i \in \{1, 2\}$;
- $(\beta, \gamma), V \models \neg(B \vee C)$ iff $\beta, V \models \neg B$ and $\gamma, V \models \neg C$;
- $(\beta, \gamma), V \models \neg(B \rightarrow C)$ iff $\beta, V \models B$ and $\gamma, V \models \neg C$;
- $\beta, V \models \neg\neg B$ iff $\beta, V \models B$.

To give an example, the INV and NAND gates of the previous section have the following sets of stabilization bounds: $\lceil \mathrm{INV}(x, y) \rceil = (\mathbf{N} \rightarrow \mathbf{N}) \times (\mathbf{N} \rightarrow \mathbf{N})$ and $\lceil \mathrm{NAND}(x, y, z) \rceil = (\mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}) \times (\mathbf{N} \oplus \mathbf{N} \rightarrow \mathbf{N})$. $(\mathcal{I}_1, \mathcal{I}_2) \in \lceil \mathrm{INV}(x, y) \rceil$, with $\mathcal{I}_1(t) = \mathcal{I}_2(t) = t + \delta_I$, provides an example of a data-independent stabilization bound for the INV gate: *it represents* the set of valuations V such that $V(y)$ stabilizes at time $t + \delta_I$ if $V(x)$ stabilizes at time t with constant delay δ_I. Similarly for $(\mathcal{N}_1, \mathcal{N}_2) \in \lceil \mathrm{NAND}(x, y, z) \rceil$, with $\mathcal{N}_1((t_1, t_2)) = \max\{t_1, t_2\} + \delta_N$ and $\mathcal{N}_2((i, t)) = t + \delta_N$. In the general case stabilization bounds represent data-dependent information; e.g., a stabilization bound for $\mathrm{NAND}(x, y, z)$ may consist of a pair of functions $(\mathcal{N}'_1, \mathcal{N}'_2)$, where $\mathcal{N}'_1$ calculates the stabilization bound for output stable to 0 and $\mathcal{N}'_2$ for output stable to 1; in the former case the bound depends on both inputs values while in the latter it depends on exactly one input value. We remark that the *nand* function can be represented by different formulas, e.g., $\mathrm{NAND}'(x,y,z) \equiv (x \wedge y \rightarrow \neg z) \wedge (\neg x \rightarrow z) \wedge (\neg y \rightarrow z)$. Actually, $\lceil \mathrm{NAND}(x,y,z) \rceil \neq \lceil \mathrm{NAND}'(x,y,z) \rceil$ but, how we will discuss later, the stabilization information is essentially the same.

It is easy to prove that validity is preserved by time shifting, i.e., $\alpha, V \models A$ implies $\alpha, V^t \models A$ for every $t \in \mathbf{N}$. Moreover, we can prove:

Proposition 1. *Let T be the following time evaluation function:*

- $T(t) = t$, *for* $t \in \mathbf{N}$;
- $T((\alpha,\beta)) = \max\{T(\alpha), T(\beta)\}$;
- $T((i,\alpha)) = T(\alpha)$, *for* $i = 1, 2$;
- $T(f) = 0$, *with f any function.*

Let V be a waveform and let A be a formula. For every $t \in \mathbf{N}$, $t, V \Vdash A$ if and only if there is $\alpha \in \lceil A \rceil$ such that $T(\alpha) \leq t$ and $\alpha, V \models A$.

Proposition 1 links the intensional semantics based on stabilization bounds and the extensional semantics of Section 2. However, stabilization bounds convey a detailed temporal information allowing us to model exact temporal bounds of the kind considered in [7]. In our setting exact bounds are formalized as follows. Let A be a formula, let $\alpha \in \lceil A \rceil$ and let V be a waveform; α is *exact for V and A* if $\alpha, V \models A$ and one of the following conditions holds:

- $A = \Box B$ or $A = \neg\Box B$;
- $A = a$ or $A = \neg a$, with $a \in \mathbf{S}$, and, for all $t \in \mathbf{N}$, $t, V \models A$ implies $\alpha \leq t$;
- $A = B \wedge C$, $\alpha = (\beta, \gamma)$, β is exact for B and V, and γ is exact for C and V;
- $A = B_1 \vee B_2$, $\alpha = (k, \beta_k)$, with $k \in \{1, 2\}$, and β_k is exact for V and B_k;
- $A = B \rightarrow C$ and, for all $\beta \in \lceil B \rceil$, if β is exact for V and B, then $\alpha(\beta)$ is exact for V and C;
- $A = \neg\neg B$ and α is exact for V and B;
- $A = \neg(B_1 \wedge B_2)$, $\alpha = (k, \beta_k)$, with $k \in \{1, 2\}$, and β_k is exact for V and $\neg B_k$;
- $A = \neg(B \vee C)$, $\alpha = (\beta, \gamma)$, β is exact for V and $\neg B$, γ is exact for V and $\neg C$;
- $A = \neg(B \rightarrow C)$, $\alpha = (\beta, \gamma)$, β is exact for V and B, γ is exact for V and $\neg C$.

For instance, let A be the formula $(a \wedge \neg b) \vee (\neg a \wedge b) \rightarrow g$ and let V be the waveform of Figure 2. We have $\beta, V \models (a \wedge \neg b) \vee (\neg a \wedge b)$ iff $\beta = (1, (t_1, t_2))$, with $t_1 \geq 10$ and $t_2 \geq 20$. The exact stabilization bound for V and $(a \wedge \neg b) \vee (\neg a \wedge b)$ is given by $t_1 = 10$ and $t_2 = 20$, which correspond to the "exact instants" where a stabilizes to 1 and b stabilizes to 0 respectively. Similarly, the exact stabilization bound for V and g is $20 + \delta_I + 2\delta_N$. Therefore, an exact stabilization bound for V and A is any $f \in \mathbf{N}^2 \oplus \mathbf{N}^2 \rightarrow \mathbf{N}$ such that $f, V \models A$ and $f((1, (10, 20))) = 20 + \delta_I + 2\delta_N$. We remark that such a detailed analysis cannot be accomplished using the approach of [7,8].

Now, let us concentrate our attention on eventually stable waveforms $\mathcal{V}^{\mathrm{ES}}$ and let us denote with $\mathbf{L}_{\mathrm{Ef}}$ the set $\{A \;:\; \exists \alpha \in \lceil A \rceil \; \forall V \in \mathcal{V}^{\mathrm{ES}} \; \alpha, V \models A\}$ (we will discuss in Section 4 the properties of $\mathbf{L}_{\mathrm{Ef}}$). Moreover, let $\mathcal{ND}$ be the natural deduction calculus obtained by adding to the natural calculus for Intuitionistic Logic (see [11]) the rules of Table 1. We denote with $\pi : \{A_1, \ldots, A_n\} \vdash B$ the fact that π is a proof with undischarged assumptions $A_1, \ldots, A_n$ and consequence B.

The following result shows a computational interpretation of proofs of $\mathcal{ND}$ allowing us to compute the exact time bounds associated with provable formulas of this calculus. As a corollary one can easily obtain the validity of $\mathcal{ND}$ w.r.t. $\mathbf{L}_{\mathrm{Ef}}$.

$$\dfrac{\neg A_i}{\neg(A_1 \wedge A_2)}\ \scriptstyle{\mathrm{I}\neg\wedge_i\ i\in\{1,2\}} \qquad \dfrac{\neg(A\wedge B) \quad \begin{array}{c}\ldots[\neg A]\\ \vdots\,\pi_1\\ C\end{array} \quad \begin{array}{c}\ldots[\neg B]\\ \vdots\,\pi_2\\ C\end{array}}{C}\ \scriptstyle{\mathrm{E}\neg\wedge}$$

$$\dfrac{A}{\neg\neg A}\ \scriptstyle{\mathrm{I}\neg\neg} \qquad \dfrac{\neg\neg A}{A}\ \scriptstyle{\mathrm{E}\neg\neg} \qquad \dfrac{\neg A \quad \neg B}{\neg(A\vee B)}\ \scriptstyle{\mathrm{I}\neg\vee} \qquad \dfrac{\neg(A_1\vee A_2)}{\neg A_i}\ \scriptstyle{\mathrm{E}\neg\vee\ i\in\{1,2\}}$$

$$\dfrac{A \quad \neg B}{\neg(A\rightarrow B)}\ \scriptstyle{\mathrm{I}\neg\rightarrow} \qquad \dfrac{\neg(A\rightarrow B)}{A}\ \scriptstyle{\mathrm{E}\neg\rightarrow_1} \qquad \dfrac{\neg(A\rightarrow B)}{\neg B}\ \scriptstyle{\mathrm{E}\neg\rightarrow_2}$$

$$\dfrac{\begin{array}{c}\ldots[\neg A]\\ \vdots\,\pi_1\\ B\end{array} \quad \begin{array}{c}\ldots[\neg A]\\ \vdots\,\pi_2\\ \neg B\end{array}}{\Box A}\ \scriptstyle{\mathrm{I}\Box} \qquad \dfrac{\begin{array}{c}\ldots[A]\\ \vdots\,\pi_1\\ B\end{array} \quad \begin{array}{c}\ldots[A]\\ \vdots\,\pi_2\\ \neg B\end{array}}{\neg\Box A}\ \scriptstyle{\mathrm{I}\neg\Box} \qquad \dfrac{\begin{array}{c}\ldots[\Box A]\\ \vdots\,\pi_1\\ B\vee C\end{array}}{(\Box A\rightarrow B)\vee(\Box A\rightarrow C)}\ \scriptstyle{\mathrm{KP}\Box}$$

Table 1. Rules for $\mathcal{ND}$

Theorem 1. *Let $\pi : \{A_1,\ldots,A_n\} \vdash B$ be a proof of $\mathcal{ND}$. We can recursively extract from π a function $F_\pi : \lceil A_1\rceil \times \cdots \times \lceil A_n\rceil \rightarrow \lceil B\rceil$ such that, for all $\alpha_1 \in \lceil A_1\rceil$, …, $\alpha_n \in \lceil A_n\rceil$, and for every eventually stable waveform V:*

(i). $\alpha_1, V \models A_1$, …, $\alpha_n, V \models A_n$ *implies* $F_\pi(\alpha_1,\ldots,\alpha_n), V \models B$.
(ii). $\alpha'_1 \sim_{A_1} \alpha_1$,…, $\alpha'_n \sim_{A_n} \alpha_n$ *implies* $F_\pi(\alpha'_1,\ldots,\alpha'_n) \sim_B F_\pi(\alpha_1,\ldots,\alpha_n)$.
(iii). α_1 *exact for* V *and* A_1, …, α_n *exact for* V *and* A_n *implies* $F_\pi(\alpha_1,\ldots,\alpha_n)$ *exact for* V *and* B.

The function F_π of Theorem 1 is defined by induction on the structure of the proof π. As an example we describe the functions associated with the disjunction elimination and the implication introduction rules.
$\vee$-*elimination*:

$$\dfrac{\begin{array}{c}A_1,\ldots,A_k\\ \vdots\,\pi_1\\ B\vee C\end{array} \qquad \begin{array}{c}A_{k+1},\ldots,A_l,[B]\\ \vdots\,\pi_2\\ D\end{array} \qquad \begin{array}{c}A_{l+1},\ldots,A_n,[C]\\ \vdots\,\pi_3\\ D\end{array}}{D}\ \scriptstyle{\vee\mathrm{E}}$$

$$F_\pi(\alpha_1,\ldots,\alpha_n) = \begin{cases} F_{\pi_2}(\alpha_{k+1},\ldots,\alpha_l,\beta) & \text{if } F_{\pi_1}(\alpha_1,\ldots,\alpha_k) = (1,\beta) \\ F_{\pi_3}(\alpha_{l+1},\ldots,\alpha_n,\gamma) & \text{if } F_{\pi_1}(\alpha_1,\ldots,\alpha_k) = (2,\gamma) \end{cases}$$

$\rightarrow$-*introduction*:

$$\dfrac{\begin{array}{c}A_1,\ldots,A_n,[B]\\ \vdots\,\pi_1\\ C\end{array}}{B\rightarrow C}\ \scriptstyle{\rightarrow\mathrm{I}} \qquad F_\pi(\alpha_1,\ldots,\alpha_n) = \lambda\beta.F_{\pi_1}(\alpha_1,\ldots,\alpha_n,\beta)$$

Now, coming back to our example, it is easy to construct a proof Π in $\mathcal{ND}$ of the formula $\mathrm{XOR}(a,b,g)$ depending exactly on the assumptions $\mathrm{INV}(b,c)$, $\mathrm{NAND}(a,c,e)$, $\mathrm{INV}(a,d)$, $\mathrm{NAND}(b,d,f)$, $\mathrm{NAND}(e,f,g)$. The proof Π provides the formal verification of our circuit. Now, let us assume that the gates INV and NAND have the input-independent stabilization bounds $(\mathcal{I}_1, \mathcal{I}_2)$ and $(\mathcal{N}_1, \mathcal{N}_2)$ considered above. Then, F_Π is the function associating with every $(i, (\alpha, \beta)) \in \mathbf{N}^2 \oplus \mathbf{N}^2$ the pair of natural numbers $(F_1(i, (\alpha, \beta)), F_2(i, (\alpha, \beta)))$ where:

$$F_1((i, (\alpha, \beta))) = \begin{cases} \max\{\alpha, \beta + \delta_I\} + 2\delta_N & \text{if } i = 1 \\ \max\{\beta, \alpha + \delta_I\} + 2\delta_N & \text{if } i = 2 \end{cases}$$

$$F_2((i, (\alpha, \beta))) = \begin{cases} \max\{\alpha, \beta\} + \delta_I + 2\delta_N & \text{if } i = 1 \\ \max\{\alpha, \beta\} + 2\delta_N & \text{if } i = 2 \end{cases}$$

As an example, let us suppose that $V(a)$ stabilizes to 1 at time 10 and $V(b)$ stabilizes to 0 at time 20 (see Figure 2). The formula $(a \wedge \neg b) \vee (\neg a \wedge b) \to g$ states that $V(g)$ must stabilize to 1, and the stabilization time is given by the exact stabilization bound γ for V and g. By Theorem 1, γ corresponds to the value of F_1 on the exact stabilization bound $(1, (10, 20))$ for V and $(a \wedge \neg b) \vee (\neg a \wedge b)$; therefore $\gamma = F_1((1, (10, 20))) = 20 + \delta_I + 2\delta_N$.

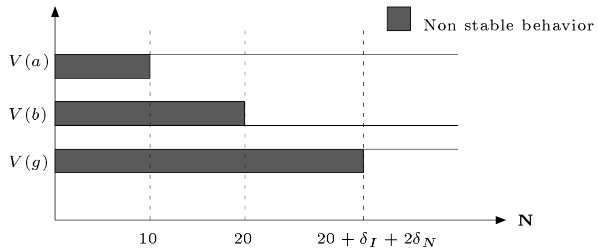

Figure 2.

4 The logics $\mathbf{L}_{\mathrm{Ef}}$ and $\mathbf{F}_{\mathrm{Cl}}$

In the above section we have defined $\mathbf{L}_{\mathrm{Ef}}$ as the set $\{A \,:\, \exists \alpha \in \lceil A \rceil \; \forall V \in \mathcal{V}^{\mathrm{ES}} \; \alpha, V \models A\,\}$, where $\mathcal{V}^{\mathrm{ES}}$ is the set of all the eventually stable waveforms. It can be shown that $\mathbf{L}_{\mathrm{Ef}}$ is a *non-standard intermediate logic*, that is $\mathbf{Int} \subseteq \mathbf{L}_{\mathrm{Ef}} \subseteq \mathbf{Cl}$, where $\mathbf{Int}$ ($\mathbf{Cl}$) denotes the set of the intuitionistically (classically) valid formulas of $\mathcal{L}_{\mathbf{S}}$ and $\mathbf{L}_{\mathrm{Ef}}$ is closed under *modus ponens*. We emphasize that, differently from standard intermediate logics, $\mathbf{L}_{\mathrm{Ef}}$ is not closed under arbitrary substitutions of propositional variables with formulas, but only under substitutions associating a formula of the kind $\Box A$ with every propositional variable. Moreover, $\mathbf{L}_{\mathrm{Ef}}$ has the *disjunction property*, that is $A \vee B \in \mathbf{L}_{\mathrm{Ef}}$ implies $A \in \mathbf{L}_{\mathrm{Ef}}$ or $B \in \mathbf{L}_{\mathrm{Ef}}$. Finally, we remark that, as far as we know, no axiomatization for $\mathbf{L}_{\mathrm{Ef}}$ is known.

Another logic that emerges from our semantical setting is $\mathbf{F}_{\mathrm{Cl}}$, a well-known axiomatizable non-standard intermediate logic which has strong connections with $\mathbf{L}_{\mathrm{Ef}}$. In [9,10] $\mathbf{F}_{\mathrm{Cl}}$ has been characterized as the smallest set of formulas closed under modus ponens containing $\mathbf{Int}$, all the instances of $\mathrm{KP}_\Box$ and all the instances of $\mathrm{At}_\Box$, where:

- $\mathrm{KP}_\Box = (\Box A \to B \vee C) \to (\Box A \to B) \vee (\Box A \to C)$ is the axiom schema obtained by translating the well-known Kreisel and Putnam Principle [3] into the language $\mathcal{L}_{\mathbf{S}}$;
- $\mathrm{At}_\Box = \Box a \to a$ with $a \in \mathbf{S}$.

A valid and complete natural calculus for $\mathbf{F}_{\mathrm{Cl}}$ is the calculus $\mathcal{ND}_{\mathbf{F}_{\mathrm{Cl}}}$ obtained by adding to $\mathcal{ND}$ the rule:

$$\frac{\Box a}{a}\ \mathrm{E\Box AT} \quad \text{with } a \in \mathbf{S}$$

In [9,10] it is proved that $\mathbf{F}_{\mathrm{Cl}}$ is a non-standard intermediate logic with the disjunction property. Moreover, $\mathbf{F}_{\mathrm{Cl}}$ meets some important proof-theoretical properties; indeed it is interpolable and enjoys a Normal Form Theorem that can be used to reduce provability in $\mathbf{F}_{\mathrm{Cl}}$ to provability in **Cl**. In the above quoted papers it is also illustrated the relationship between $\mathbf{F}_{\mathrm{Cl}}$ and *Medvedev Logic of Finite Problems* [5,9].

To characterize $\mathbf{F}_{\mathrm{Cl}}$ in our semantical setting, let $\mathcal{V}_t^{\mathrm{S}}$ denote the set of all the waveforms stable at t for some $t \in \mathbf{N}$; it can be shown that $\mathbf{F}_{\mathrm{Cl}} = \{A \ : \ \exists \alpha \in \lceil A \rceil\ \forall V \in \mathcal{V}_t^{\mathrm{S}}\ \alpha, V \models A\ \}$. From the above semantical characterization it is immediate that $\mathbf{L}_{\mathrm{Ef}} \subseteq \mathbf{F}_{\mathrm{Cl}}$; moreover, $\mathbf{L}_{\mathrm{Ef}}$ contains all the instances of $\mathrm{KP}_\Box$, on the other hand $\mathrm{At}_\Box$ does not hold in $\mathbf{L}_{\mathrm{Ef}}$.

Also from proofs of $\mathcal{ND}_{\mathbf{F}_{\mathrm{Cl}}}$ we can extract exact stabilization bounds. Indeed, an analogous of Theorem 1 holds for $\mathcal{ND}_{\mathbf{F}_{\mathrm{Cl}}}$ where, instead of considering the set of eventually stable waveforms, we consider the set of waveforms stable at t, with $t \in \mathbf{N}$.

5 Conclusion

In this paper we have shown how we can get a timing analysis with data-dependent valuation of exact delays by a specialization of evaluation forms semantics [10]. There are several interesting aspects we aim to investigate in our future work.

As for the semantics here considered, we want to examine thoroughly the kind of delay information related to different formulas representing the same boolean function. This would lead to a deeper understanding of the expressiveness of our language. In this context it is interesting to study extensions of the language by other modal operators as the Lax operator of [7].

Moreover, the semantical setting of evaluation forms supports a variety of specializations that preserve the soundness theorem, that is the fundamental result to compute stabilization bounds with proofs. It is interesting to investigate which of these semantics give rise to useful timing analysis models.

References

1. D.A. Basin and N. Klarlund. Automata based symbolic reasoning in hardware verification. *Formal Methods in Systems Design*, 13(3):255–288, 1998.
2. J. Brzozowski and M. Yoeli. Ternary simulation of binary gate networks. In J. M. Dunn and G. Epstein, editors, *Modern Uses of Multiple-Valued Logic*, pages 41–50. D. Reidel, 1977.
3. A. Chagrov and M. Zakharyaschev. *Modal Logic*. Oxford University Press, 1997.
4. C.T. Gray, W. Liu, R.K. Cavin III, and H.-Y. Hsieh. Circuit delay calculation considering data dependent delays. *INTEGRATION, the VLSI journal*, 17:1–23, 1994.
5. Ju.T. Medvedev. Interpretation of logical formulas by means of finite problems and its relation to the realizability theory. *Soviet Mathematics Doklady*, 4:180–183, 1963.
6. M. Mendler. A timing refinement of intuitionistic proofs and its application to the timing analysis of combinational circuits. In P. Miglioli, U. Moscato, D. Mundici, and M. Ornaghi, editors, *Proceedings of the 5th International Workshop on Theorem Proving with Analytic Tableaux and Related Methods*, pages 261–277. Springer, LNAI 1071, 1996.

7. M. Mendler. Characterising combinational timing analyses in intuitionistic modal logic. *Logic Journal of the IGPL*, 8(6):821–852, 2000.
8. M. Mendler. Timing analysis of combinational circuits in intuitionistic propositional logic. *Formal Methods in System Design*, 17(1):5–37, 2000.
9. P. Miglioli, U. Moscato, M. Ornaghi, S. Quazza, and G. Usberti. Some results on intermediate constructive logics. *Notre Dame Journal of Formal Logic*, 30(4):543–562, 1989.
10. P. Miglioli, U. Moscato, M. Ornaghi, and G. Usberti. A constructivism based on classical truth. *Notre Dame Journal of Formal Logic*, 30(1):67–90, 1989.
11. D. Prawitz. *Natural Deduction*. Almquist and Winksell, 1965.
12. S. Malik. Analysis of Cyclic Combinational Circuits. In *IEEE /ACM International Conference on CAD*, pages 618–627, Santa Clara, California, 1993. ACM/IEEE, IEEE Computer Society Press.