THREE VALUED AUTOMATED REASONING ON ANALOG PROPERTIES

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

R. Gentilini[1)] , K. Schneider [1)], and A. Dreyer [2)]

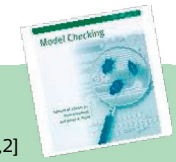
1) Reactive Syestems Group, Computer Science Depertment, University of Kaiserslautern, Germany
gentilin@informatik.uni-kl.de, Klaus.Schneider@informatik.uni-kl.de

2) Fraunhofer Research Institute for Applied Mathematics, Kaiserslautern, Germany
Alexander.Dreyer@itwm.fraunhofer.de

Fraunhofer Institut Techno- und Wirtschaftsmathematik

Motivations

Digital Circ. model Checking



Model Checking:

A well established **verification** tech. [1,2] for **finite systems** (e.g digital circ.). Properties formally stated in a temporal logic language**:**

- ! Are verified along **all system's paths**
- ! **Entirely automatically**

Analog Model Checking

A natural way to apply model checking in the context of verification of analog circuit is the extraction of a finite digital abstraction from the corresponding (infinte states) systems. However, **two main problems** have to be considered in order to derive an effective verification technique for analog circuits [3]:

- ? Need of disposing of formal tools to relate abstractions and systems (e.g. **can we trust properties established on the digital abstraction?)**
- ? Need of disposing of **adequate languages to state analog prop.**

CTLf : A Language for the Specification of Analog Properties

What is the CTLf language?

A suitable **enrichment** of the **classical CTL temporal logic** originally designed for the temporal analisys of digital finite systems. In particular, we allow **'basic formulae' to state the membership in boxes of arbitrary elementary functional relations**.

Which analog properties allow to model?

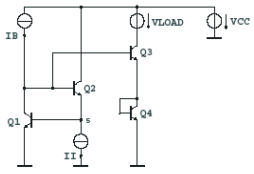
> general properties on the **relative value of input/system variables of an analog model, while the latter evolves**.

> general **properties relating the rate at which system variables decrease/increase** along their evolution, since corresponding derivative functions can be explicitly stated in basic formulae.

Definition 1 (CTL_f **Syntax**) *Let $X = \{x_1, \ldots, x_n\}$ be a finite set of real valued variables. The set of* CTL_f *formulæ is defined according the following grammar:*

$$\begin{array}{lll} \phi ::= & f(x_{i_1}, \ldots, x_{i_m}) \rhd I & \text{(basic formulæ testing membership in box } I\text{)} \\ & \neg\phi | \phi \vee \phi & \text{(boolean combinators)} \\ & \mathsf{E}\phi\mathsf{U}\phi | \mathsf{A}\phi\mathsf{U}\phi & \text{(temporal combinators \& path quantifiers)} \end{array}$$

where $1 \le i_1 \le \cdots \le i_m \le n$, $f : \mathbb{R}^m \mapsto \mathbb{R}^p$ is an arbitrary composition of elementary functions, I is a box in $\mathbb{IR}^p$.



Example 1 *In the square root function block above, the output current I_0 (measured through the voltage source* VLOAD*) is roughly given by the square root of the product of input currents I_I, I_B, and a constant factor β is a constant related to parameters of the transistors $Q_1, \ldots, Q_4$.:*

$$I_0 = \beta \sqrt{I_I}\sqrt{I_B}\ , \qquad (1)$$

Property 1 can be naturally modeled by means of the CTL_f *l formula 2 below stating that "Globally along the evolution of all trajectories, the relation $(I_0 - \beta\sqrt{I_I}\sqrt{I_B}\,) \in [-\delta, +\delta]$" holds:*

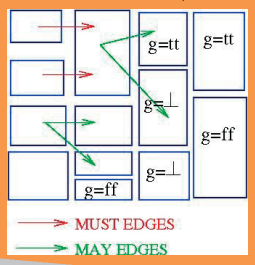
$$\mathsf{AG}((I_0 - \beta\sqrt{I_I}\sqrt{I_B}\,) \rhd [-\delta, +\delta]) \qquad (2)$$

CTLf Three Valued Model Checking for Analog Circuits

We use **Interval Arithmetic** to provide a **Three Valued Semantics to our CTLf language** on suitable grid-like abstractions (box modal abstraction) of the infinite states-space for the analog circuit.

Why a three-valued semantics?

1) A natural choice since **it could be not possible to state a definite value for CTLf formulae on any abstract state**
2) Most important, it **allows to apply three valued model checking** techniques (rather than classical two valued ones) and to state a **fundamental preservation result** for verified CTLf formulae (i.e. **any formula stated true/false on the digital abstraction can be trusted on the original sys**).



Definition 1 (Box Modal Abstraction (BMA)) *Let $X = \{x_1, \ldots, x_n\}$ be a set of n real valued variables. A Box Modal Abstraction on X is a tuple $(\mathcal{B}, \xrightarrow{must}, \xrightarrow{may})$, where:*

- *$\mathcal{B}$ is a finite collection of boxes over $\mathbb{R}^n$.*
- *$\xrightarrow{must}$ and $\xrightarrow{may}$ are binary relations on $\mathcal{B}$. We assume that $\xrightarrow{must} \subseteq \xrightarrow{may} \subseteq \mathcal{B} \times \mathcal{B}$ and that $\xrightarrow{may}$ is total (i.e. each box has at least one may transition departing from it).*

Definition 2 (Must & May Paths) *Let $\mathcal{A} = (\mathcal{B}, \xrightarrow{must}, \xrightarrow{may})$ be a BMA on $X = \{x_1, \ldots, x_n\}$. A may-path (must-path) in $\mathcal{A}$ is an infinite sequence of boxes $\{b_i\}_{i\in\mathbb{N}}$ such that for all $i \ge 0$ it holds that $b_i \xrightarrow{may} b_{i+1}$ ($b_i \xrightarrow{must} b_{i+1}$). We use the notation $\{b_i\}_{i\in\mathbb{N}}^{may}$ ($\{b_i\}_{i\in\mathbb{N}}^{must}$) to denote may-paths (must-paths). A may-subpath (must-subpath) is a finite prefix of a may-path (must-path).*

Definition 1 (Preserving BMA) *Consider an analog model $\mathcal{C} = \langle X^D, X^I, \mathcal{D}, \mathcal{I}\rangle$ and let $n = |X^D \cup X^I|$. A box modal abstraction $\mathcal{A} = \langle \mathcal{B}, \xrightarrow{must}, \xrightarrow{may}\rangle$ on $X = X^D \cup X^I$ is said preserving for $\mathcal{C}$ iff there exists a relation $\lessdot \subseteq \mathcal{B} \times \mathbb{R}^n$ such that, whenever $b \lessdot v$, the following rules hold:*

1. *For each basic CTL_f formula ϕ, $[b \models_3 \gamma] \prec [v \models \gamma]$.*
2. *If $\{b_i\}_{1\le i\le k}^{must}$ is a must-subpath departing from b in $\mathcal{A}$, then $\mathcal{C}$ admits a trajectory ρ departing from v such that there exists an increasing sequence of real values $\{t_i\}_{0\le i\le k}$ such that:*

$$\forall t \in \mathbb{R}(t_{i-1} \le t \le t_i \rightarrow b_i \lessdot \rho(t))$$

3. *If $\mathcal{C}$ admits a trajectory $\rho(t)$ departing from v, then $\mathcal{A}$ admits a may-path $\{b_i\}_{i\in\mathbb{N}}^{may}$ such that there exists an increasing sequence of real values $\{t_i\}_{i\in\mathbb{N}}$ such that:*

$$\forall t \in \mathbb{R}(t_i \le t \le t_{i+1} \rightarrow b_i \lessdot \rho(t))$$

Definition 1 (CTL_f Abstract Semantics) *Let $\mathcal{A} = \langle \mathcal{B}, \xrightarrow{must}, \xrightarrow{may}\rangle$ be a BMA on $X = \{x_1, \ldots, x_n\}$. Given $b \in \mathcal{B}$ and a CTL_f formula ϕ, we define $[b \models_3 \phi]$ to be one of the three values in $\{\mathsf{tt}, \mathsf{ff}, \perp\}$, according to:*

- *If $\phi = f(x_{i_1}, \ldots, x_{i_m}) \rhd I$, then $[b \models_3 \phi] = \mathsf{tt}$. If $[f](b) \cap I = \emptyset$, then $[b \models_3 \phi] = \mathsf{ff}$. Otherwise, $[b \models_3 \phi] = \perp$*
- *If ϕ is a boolean combination, then its three-way value is defined according to strong three valued Kleene rules.*
- *If $\phi = \mathsf{E}\phi_1\mathsf{U}\phi_2$, then $[b \models_3 \phi]$ is defined as:*

$$\begin{cases} \mathsf{tt} & \text{if } \exists \text{ a must-subpath } \{b_i\}_{i=0..k}^{must} \text{ departing from } b \text{ such that:} \\ & ([b_k \models_3 \phi_2] = \mathsf{tt}) \wedge \forall i (0 \le i \le k (([b_i \models_3 \phi_1] = \mathsf{tt}); \\ \mathsf{ff} & \text{if } \forall \text{ may-path } \{b_i\}_{i\in\mathbb{N}}^{may} \text{ departing from } b \wedge \forall\ i \ge 0, \text{ it holds:} \\ & ([b_i \models_3 \phi_2] \ne \mathsf{ff}) \rightarrow \exists j < i([b_j \models_3 \phi_2] \approx \mathsf{ff}) \\ \perp & \text{otherwise.} \end{cases}$$

The three-way value for the case $\phi = \mathsf{A}\phi_1\mathsf{U}\phi_2$ is similarly defined.

Theorem 1 *Let $\mathcal{C} = \langle X^D, X^I, \mathcal{D}, \mathcal{I}\rangle$ to be an analog model and let $n = |X^D \cup X^I|$. If $\mathcal{A} = \langle \mathcal{B}, \xrightarrow{must}, \xrightarrow{may}\rangle$ is a preserving box modal abstraction for $\mathcal{C}$, then:*

$$\forall b \in \mathcal{B}, \forall v \in \mathbb{R}^n, \forall \phi \in \mathsf{CTL}_f((b \lessdot v) \rightarrow ([b \models_3 \phi] \prec [v \models \phi]))$$

where $\lessdot \subseteq \mathcal{B} \times \mathbb{R}^n$ denotes the preserving concretization relation for $\mathcal{A}$ and $\mathcal{C}$.

[1] E. Clarke, O. Grumberg, D. Peled. *"Model Checking"* MIT Press, 2000.

[2] K. Schneider. *"Verification of Reactive Systems"* Springer-Verlag, 2004.

[3] W. Hartong, L. Hedrich, E. Barke *"Model Checking Algorithms for Analog Verification"* In Proocedings of 39° Conference On Design Automation, pages 542-547, 2002.