Combining Interval Arithmetic and Three-Valued Temporal Logics for the Verification of Analog Systems

DASMOD

Dependable Adaptive Systems and Mathematical Modeling

R. Gentilini, K. Schneider, **A. Dreyer**

TU Kaiserslautern
Reaktive Systeme
Fachbereich Informatik

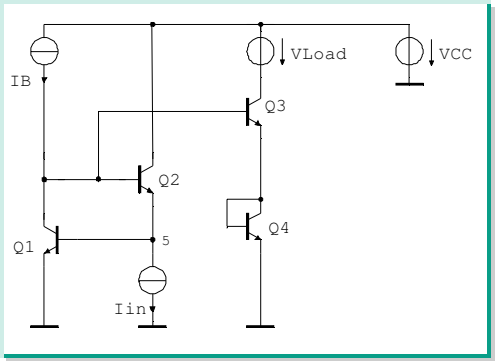
Fraunhofer-Institut für Techno- und Wirtschaftsmathematik

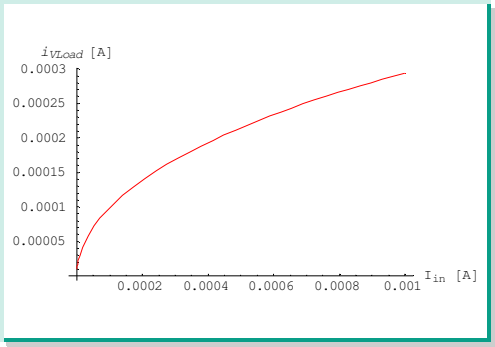
10. Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen"

Erlangen, 5. – 7. Mrz 2007

Fraunhofer Institut Techno- und Wirtschaftsmathematik

Symbolic Approximation using Simulations





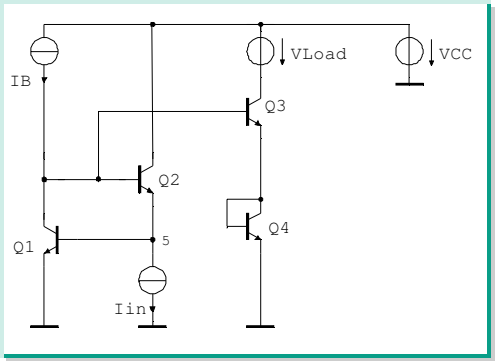
Symbolic equations

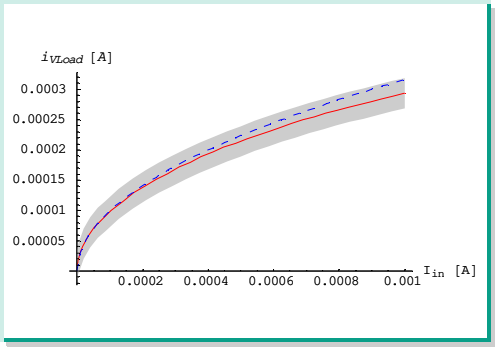
- 27 equations
- 17 parameters

$$i_{C_{Q2}} + i_{VCC} + i_{VLoad} = -I_B$$
$$i_{E_{Q2}} + i_{E_{Q3}} + i_{C_{Q1}} = I_B$$
$$i_{E_{Q4}} + i_{C_{Q3}} + i_{E_{Q3}} = 0$$
$$i_{E_{Q1}} + i_{E_{Q2}} = -I_{in}$$
$$i_{C_{Q3}} - i_{VLoad} = 0$$
$$-i_{E_{Q3}} - i_{C_{Q1}} - i_{E_{Q2}} = 0$$
$$i_{E_{Q1}} = i_{B_{Q1}}$$
$$-i_{E_{Q3}} - i_{E_{Q1}} = i_{C_{Q1}}$$
$$i_{C_{Q1}} = V_3\, G_{min} + \left(-1 + e^{\frac{V_3}{V_t}}\right) Is_{Q1} - \left(1 + \frac{1}{Br_{Q1}}\right)\left(\left(-V_3 + V_5\right) G_{min} + \left(-1 + e^{\frac{-V_5+V_3}{V_t}}\right) Is_{Q1}\right)$$
$$i_{B_{Q1}} = \frac{V_3 G_{min}\left(-1+e^{\frac{V_3}{V_t}}\right) Is_{Q1}}{Br_{Q1}} + \frac{\left(-V_3+V_5\right) G_{min}\left(-1+e^{\frac{-V_5+V_3}{V_t}}\right) Is_{Q1}}{Br_{Q1}}$$
$$-i_{E_{Q2}} - i_{C_{Q2}} - i_{E_{Q2}} = 0$$
$$i_{E_{Q2}} = i_{B_{Q2}}$$
$$-i_{E_{Q3}} - i_{E_{Q2}} = i_{C_{Q2}}$$
$$i_{C_{Q2}} = \left(V_3 - V_5\right) G_{min} + \left(-1 + e^{\frac{V_3-V_5}{V_t}}\right) Is_{Q2} - \left(1 + \frac{1}{Br_{Q2}}\right)\left(\left(-V_1 + V_3\right) G_{min} + \left(-1 + e^{\frac{-V_1+V_3}{V_t}}\right) Is_{Q2}\right)$$
$$i_{B_{Q2}} = \frac{\left(-V_1+V_3\right) G_{min}\left(-1+e^{\frac{-V_1+V_3}{V_t}}\right) Is_{Q2}}{Br_{Q2}} + \frac{\left(V_3-V_5\right) G_{min}\left(-1+e^{\frac{V_3-V_5}{V_t}}\right) Is_{Q2}}{Br_{Q2}}$$
$$-i_{E_{Q3}} - i_{C_{Q3}} - i_{E_{Q3}} = 0$$
$$i_{E_{Q3}} = i_{B_{Q3}}$$
$$-i_{E_{Q3}} - i_{E_{Q3}} = i_{C_{Q3}}$$
$$i_{C_{Q3}} = \left(V_3 - V_4\right) G_{min} + \left(-1 + e^{\frac{V_3-V_4}{V_t}}\right) Is_{Q3} - \left(1 + \frac{1}{Br_{Q3}}\right)\left(\left(V_3 - V_{out}\right) G_{min} + \left(-1 + e^{\frac{V_3-V_{out}}{V_t}}\right) Is_{Q3}\right)$$
$$i_{B_{Q3}} = \frac{\left(V_3-V_4\right) G_{min}\left(-1+e^{\frac{V_3-V_4}{V_t}}\right) Is_{Q3}}{Br_{Q3}} + \frac{\left(V_3-V_{out}\right) G_{min}\left(-1+e^{\frac{V_3-V_{out}}{V_t}}\right) Is_{Q3}}{Br_{Q3}}$$
$$-i_{E_{Q4}} - i_{C_{Q4}} - i_{E_{Q4}} = 0$$
$$i_{E_{Q4}} = i_{B_{Q4}}$$
$$-i_{E_{Q4}} - i_{E_{Q4}} = i_{C_{Q4}}$$
$$i_{C_{Q4}} = V_4\, G_{min} + \left(-1 + e^{\frac{V_4}{V_t}}\right) Is_{Q4}$$
$$i_{B_{Q4}} = \frac{V_4 G_{min}\left(-1+e^{\frac{V_4}{V_t}}\right) Is_{Q4}}{Br_{Q4}}$$
$$V_1 - V_{out} = V_{Load}$$
$$V_1 = V_{CC}$$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Symbolic Approximation using Simulations





Symbolic equations

- 27 equations
- 17 parameters

Reduced equations

- 4 equations
- 7 parameters

$$-I_{in} + e^{\frac{v_3 - v_5}{Vt}}\, Is_{Q2} = 0$$

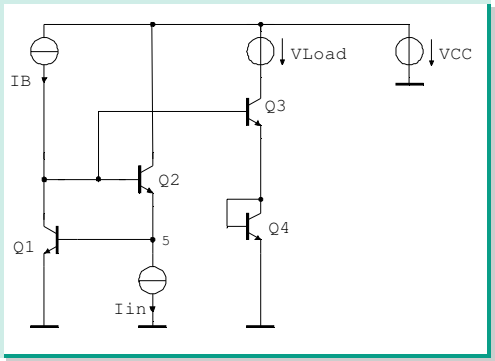
$$I_B - e^{\frac{v_5}{Vt}}\, Is_{Q1} = 0$$

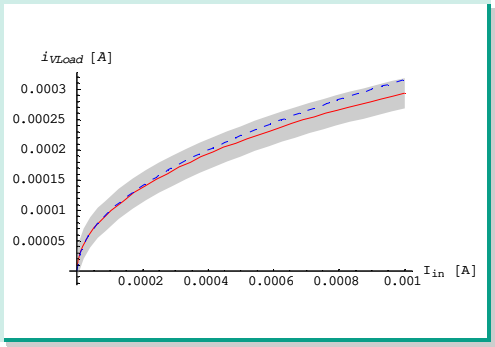
$$i_{VLoad} - e^{\frac{v_3 - v_4}{Vt}}\, Is_{Q3} = 0$$

$$i_{VLoad} - e^{\frac{v_4}{Vt}}\, Is_{Q4} = 0$$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Symbolic Approximation using Simulations





Symbolic equations

- 27 equations
- 17 parameters

Reduced equations

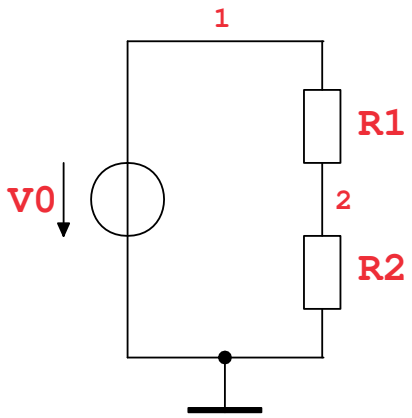
- 4 equations
- 7 parameters

Explicit formula

$$i_{vload}^{simple} = \sqrt{\frac{Is_{Q3}\, Is_{Q4}}{Is_{Q1}\, Is_{Q2}}}\, \sqrt{I_B}\, \sqrt{I_{in}}$$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Parameter Tolerances using Interval Arithmetic



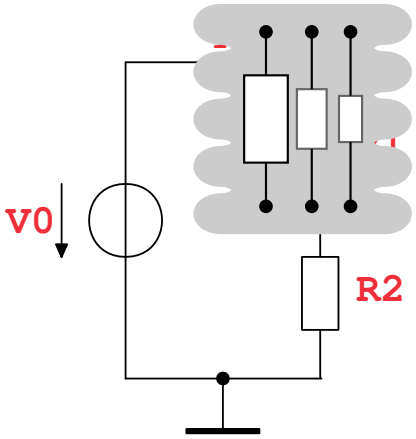
– Simulations ensure validity for discrete settings only

$\texttt{V0} = 1\,\mathrm{V} \qquad \texttt{R1} = 10\Omega \qquad \texttt{R2} = 100\Omega$

$V_2 = \frac{V_0}{R_1/R_2+1} \approx 0.909\,\mathrm{V}$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Parameter Tolerances using Interval Arithmetic



- Simulations ensure validity for discrete settings only
- Interval-valued computations can verify properties for domains

$$\texttt{V0} = 1\,\mathrm{V} \pm 10\%,\ \texttt{R1} = 10\Omega \pm 10\%,\ \texttt{R2} = 100\Omega \pm 10\%,$$
$$V_2 = \frac{V_0}{R_1/R_2+1} \approx 0.909\,\mathrm{V}$$
$$V_2 \in \frac{[0.9,1.1]}{[9,11]/[90,110]+1} = [0.80, 1.02]$$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Validation of Symbolic Approximations

Compare different accuracy levels

$$i_{vload} \approx i_{vload}^{simple} \; ?$$

$$i_{vload} = \frac{\sqrt{Is_{Q3} Is_{Q4} \left((0.025 Is_{Q3} Is_{Q4} - Is_{Q2} Is_{Q1}) 10^{-2} {I_{in}}^2 + Is_{Q1} Is_{Q2} I_B I_{in}\right)} - 5{\cdot}10^{-3} I_{in} Is_{Q3} Is_{Q4}}{Is_{Q1} Is_{Q2}}$$

$$i_{vload}^{simple} = \sqrt{\frac{Is_{Q3}\, Is_{Q4}}{Is_{Q1}\, Is_{Q2}}}\, \sqrt{I_B}\, \sqrt{I_{in}}$$

Example

For $Is_{Qi} = 10^{-16}$A, $I_{in}/1\text{mA} \in [0.2, 0.3]$, and $I_B/1\text{mA} \in [0.1, 0.2]$ interval techniques **prove** $\left|(i_{vload} - i_{vload}^{simple})/i_{vload}\right| < 2.5\%$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Formal Verification of Analog Circuits

Motivation:
Simulation vs.
Formal Verification

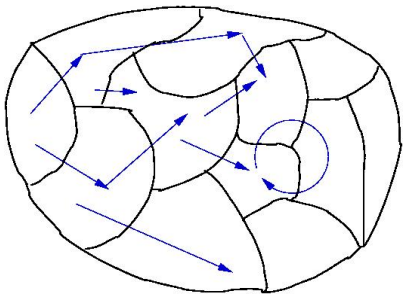
Formal verification techniques aim at:

- Verifying system properties **before manufacturing**
- **Automated** verification process
- Coping with the **variability** of parameters and input signals

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Model Checking Verification Technique

Established technique for



Verification of **discrete finite systems**.

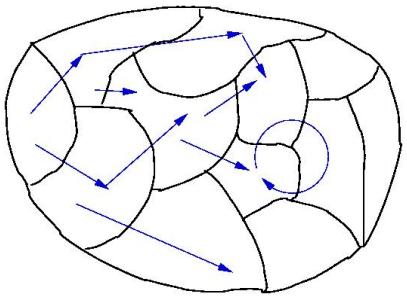
Properties stated via a temporal logic language are verified:

- completely **automated**,
- on **any computational path** of the graph-modeled system

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Model Checking Verification Technique

Established technique for



Verification of **discrete finite systems**.

Properties stated via a temporal logic language are verified:

- completely **automated**,
- on **any computational path** of the graph-modeled system

Natural extension

Extending the model checking technique to analog circuits involves the **extraction of some discrete approximation** of the infinite graph underlying the evolution of an analog circuit.

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Model Checking of Analog Properties

Two major issues

To be considered for obtaining an effective verification technique:

- need of **adequate languages** to formulate analog properties,
- need of formal tools to **ensure preservation** results from the abstraction to the analog model.

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

CTL_f: Language for Modeling of Analog Properties

Enrichment of classical CTL

Allows *basic formulæ* to state the membership in boxes of values given by arbitrary elementary functional relations.

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

CTL$_f$: Language for Modeling of Analog Properties

Enrichment of classical CTL

Allows *basic formulæ* to state the membership in boxes of values given by arbitrary elementary functional relations.

CTL$_f$ **Syntax**

Let $X = \{x_1, \ldots, x_n\}$ be a finite set of real-valued variables.

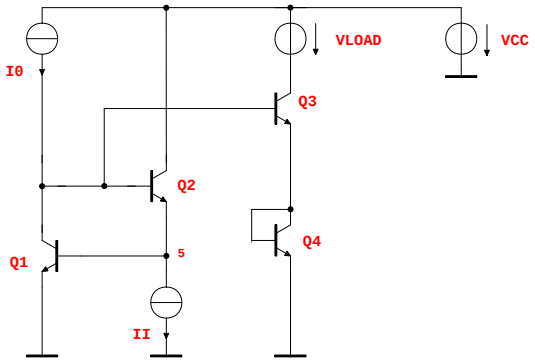
The set of CTL$_f$ formulæ is defined according to

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

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

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Back to the Example



– In the **square root function block** property (1) holds:

$$I_0 = \beta \sqrt{I_I}\,\sqrt{I_B}\ , \tag{1}$$

– CTL_f formula encoding property (1):

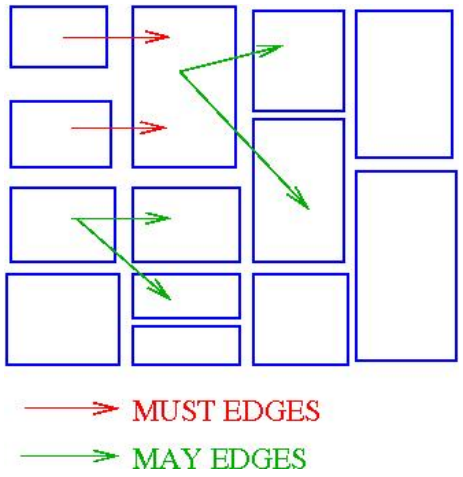
$$\mathsf{AG}((I_0 - \beta \sqrt{I_I}\,\sqrt{I_B}\,) \rhd [-\delta, +\delta]) \tag{2}$$

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Three-valued CTL_f Model Checking on Analog Circuits

Box-modal abstractions

We use *interval arithmetic* to provide a **three-valued semantics** to our CTL_f logic on suitable abstraction of the state space of analog circuits.



Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Three-valued CTL_f Model Checking on Analog Circuits

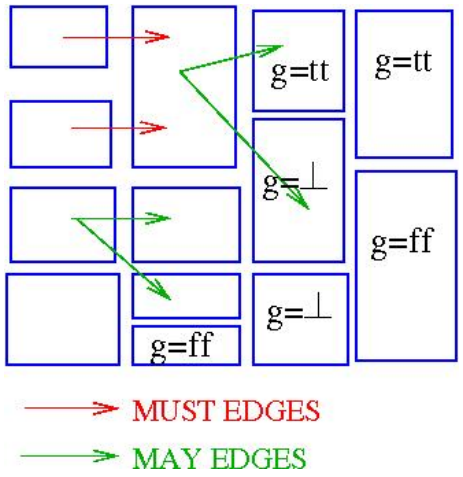
Box-modal abstractions

We use *interval arithmetic* to provide a **three-valued semantics** to our CTL_f logic on suitable abstraction of the state space of analog circuits.

Three-valued semantics

A natural choice since the value of our CTL_f formulae could be indefinite on abstract states (boxes).

Construction of **may**- and **must**-paths in the abstraction.



Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

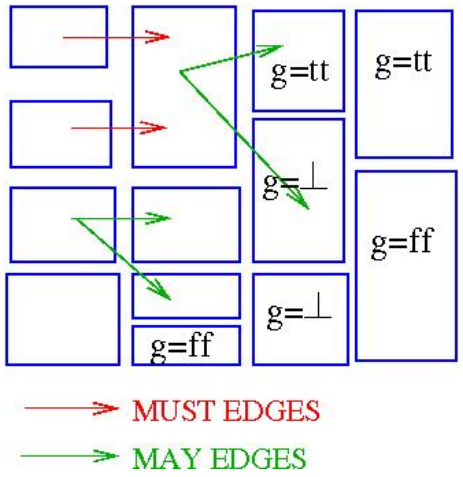
Three-valued CTL_f Model Checking on Analog Circuits

Box-modal abstractions

We use *interval arithmetic* to provide a **three-valued semantics** to our CTL_f logic on suitable abstraction of the state space of analog circuits.

Three-valued semantics

A natural choice since the value of our CTL_f formulae could be indefinite on abstract states (boxes).



Construction of **may**- and **must**-paths in the abstraction.

Fundamental Preservation Result

Any formula stated true/false on the discrete abstraction can be trusted against the original system.

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Summary

Motivation

– Verification of analog approximations

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Summary

Motivation

- Verification of analog approximations

Methods

- Enrichment of classical CTL for analog properties
- Combination of three-valued logic and interval-valued evaluation
- Fundamental preservation result

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik

Summary

Motivation

- Verification of analog approximations

Methods

- Enrichment of classical CTL for analog properties
- Combination of three-valued logic and interval-valued evaluation
- Fundamental preservation result

Outlook

- Application to real-world examples
- Integration in/couping of the symbolic analysis tool **Analog Insydes** for analog circuits and formal verification tool **Averest**

Fraunhofer ITWM Institut Techno- und Wirtschaftsmathematik