Entwurfsmethodik
Institut für Informatik

JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

www.uni-frankfurt.de

A Symbolic Approach for Mixed-Signal Model Checking

Alexander Jesser, *Lars Hedrich*

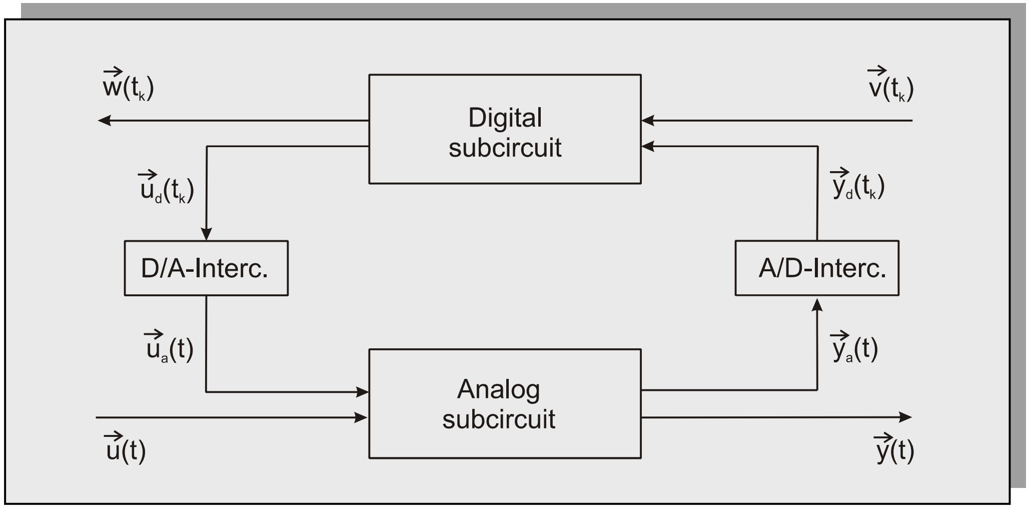
21.01.2008

13th Asia and South Pacific Design Automation Conference ASP-DAC 2008,Seoul, Korea January 21-24, 2008

Outline

- Mixed-Signal System Decomposition
- Real-Time Transition Structure (RTTS)
- Computational Data structure (MTBDDs)
- CTL-AT as the Specification language
- MS Verification Flow
- CTL-AT Evaluation Algorithms
- Verification Results (PLL)
- Summary

Mixed-Signal Decomposition (Interfaces)



D/A-Interconnection: ramp function:

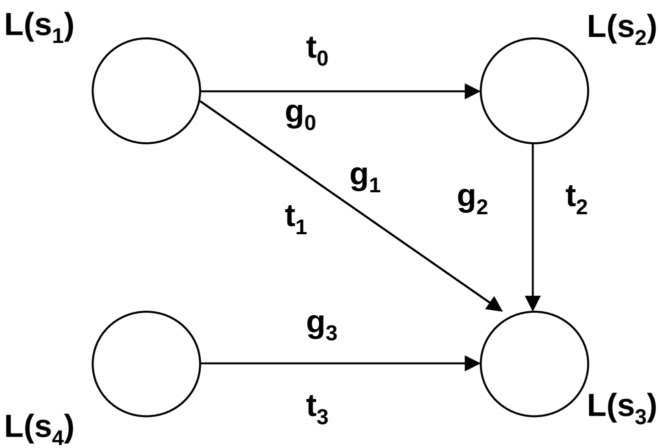
$$\vec{u}_a(t) = inj(\vec{u}_d(t_k)) = \begin{cases} u_{\max}^{(i)} : u_d^{(i)}(t) = 1, \forall 1 \le i \le n, t_k \le t < t_{k+1} \\ u_{\min}^{(i)} : u_d^{(i)}(t) = 0, \forall 1 \le i \le n, t_k \le t < t_{k+1} \end{cases}$$

A/D-Interface: 1-bit quantizer:

$$\vec{y}_d(t_k) = quant(\vec{y}_a(t)) = \begin{cases} y_d^{(i)} = 1 : y_a^{(i)}(t_k) \ge y_{thresh}^{(i)}, \forall 1 \le i \le m \\ y_d^{(i)} = 0 : y_a^{(i)}(t_k) < y_{thresh}^{(i)}, \forall 1 \le i \le m \end{cases}$$

Real Timed Transition Structure

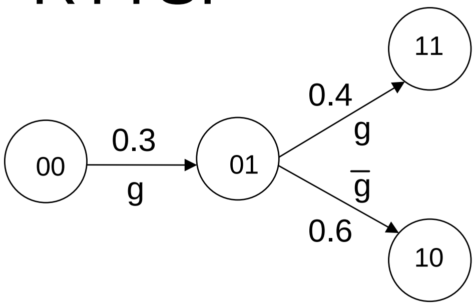
- **Real Timed Transition Structures (RTTS)**
  - Time extension of Kripke structures
    - Time delay represents the dynamic behavior of the system
  - Inputs are necessary because of the intercommunication of both subsystems
  - Basic structure for the analog specification language CTL-AT



- L … labeling function
- t_i … delay time
- g_i …inputs

Characteristic Transition Function (CTF)

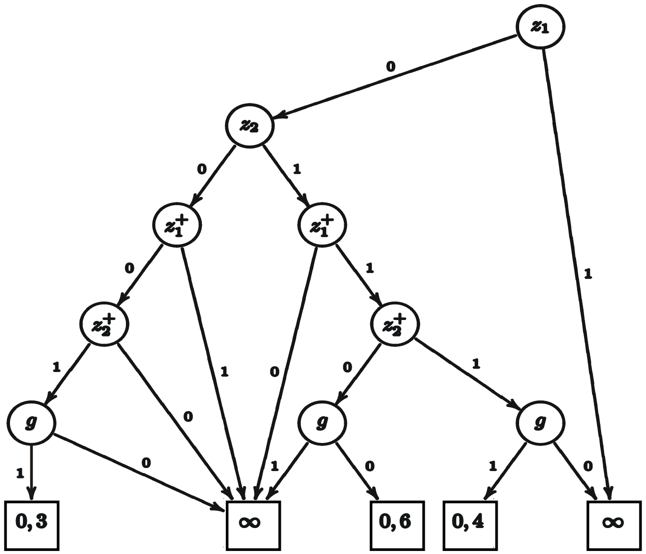
RTTS:



Characteristic transition function (CTF)

$$\chi_\delta(s,s^+,g) = \begin{cases} \tau & :(s,s^+,g)\in\delta \\ \infty & :(s,s^+,g)\notin\delta \end{cases}$$

Transition MTBDD:



$$\chi_\delta = \bigvee_{s_i,s_j} \tau_{i,j}\cdot(\vec{z} \equiv \vec{z}(s_i))(\vec{z}^+ \equiv \vec{z}(s_j))(\vec{g} \equiv \vec{g}(s_i,s_j))$$

$$\begin{aligned}\chi_\delta = \; & 0.3\cdot(\overline{z}_1\overline{z}_2\overline{z}_1^+ z_2^+ g)\vee \\ & 0.4\cdot(\overline{z}_1 z_2 z_1^+ z_2^+ g)\vee \\ & 0.6\cdot(\overline{z}_1 z_2 z_1^+\overline{z}_2^+\overline{g})\vee \\ & \infty\cdot(z_1 \vee \overline{z}_2\overline{z}_2^+ \vee z_2^+\overline{g} \vee z_2 z_1^+ \vee z_2\overline{z}_1^+)\end{aligned}$$

CTL-AT syntax

- Syntax:

$$\Phi = a \mid z * v \mid \Phi \circ \Phi \mid \neg\Phi \mid \rhd \Diamond\Box\, \Phi \mid \rhd\, \Phi U \Box\, \Phi \mid \rhd\, \Phi R \Box\, \Phi$$

$a \in AP$… atomic proposition

z … analog state variable

$v \in \mathbb{R}$ … state boundaries

$* \in \{\leq, \geq, <, >\}$

$\circ \in \{\vee, \wedge\}$

$\rhd \in \{A, E\}$

$\Box = [t_l, t_h] \qquad t_l, t_h \in \mathbb{R}, t_l \leq t_h$

$\Diamond \in \{X, F, G, U, R\}$

- CTL-AT is CTL extended by:
  - Analog (state) variables (e.g. voltages, currents)
    - e.g.: $(V_2 > 1.456)$
  - Inequalities for describing analog state regions
  - Time Intervals $[t_l \ldots t_h]$ for describing real-time behavior
  - Inverse time path operators
    - $Y=X^{-1}$, $P=F^{-1}$, $H=G^{1}$, $S=U^{-1}$

CTL-AT semantics

- Formal semantic

$\mathcal{T}_\ltimes \models_\ltimes p_i \iff p_i \in L(s)$

$\mathcal{T}_\ltimes \models_\ltimes \neg\phi_\ltimes \iff \mathcal{T}_\ltimes \not\models \phi_\ltimes$

$\mathcal{T}_\ltimes \models_\ltimes \phi_\ltimes \wedge \psi_\ltimes \iff \mathcal{T}_\ltimes \models_\ltimes \phi_\ltimes$ *and*

$\mathcal{T}_\ltimes \models_\ltimes \phi_\ltimes \vee \psi_\ltimes \iff \mathcal{T}_\ltimes \models_\ltimes \phi_\ltimes$ *or*

$\mathcal{T}_\ltimes \models_\ltimes EX(\phi_\ltimes) \iff$ *There exists a*
$(s, s') \in \delta : (\mathcal{T}$

$\mathcal{T}_\ltimes \models_\ltimes AX(\phi_\ltimes) \iff$ *For all succes*
$(s, s') \in \delta : (\mathcal{T}$

$\mathcal{T}_\ltimes \models_\ltimes EF[t_l, t_h](\phi_\ltimes) \iff \exists\pi \text{ in } \mathcal{T}_\ltimes \exists i : t$

$\mathcal{T}_\ltimes \models_\ltimes EG[t_l, t_h](\phi_\ltimes) \iff \exists\pi \text{ in } \mathcal{T}_\ltimes \forall i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}_\ltimes \restriction \pi[i]) \models_\ltimes \phi_\ltimes]$

$\mathcal{T}_\ltimes \models_\ltimes AF[t_l, t_h](\phi_\ltimes) \iff \forall\pi \text{ in } \mathcal{T}_\ltimes \exists i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}_\ltimes \restriction \pi[i]) \models_\ltimes \phi_\ltimes]$

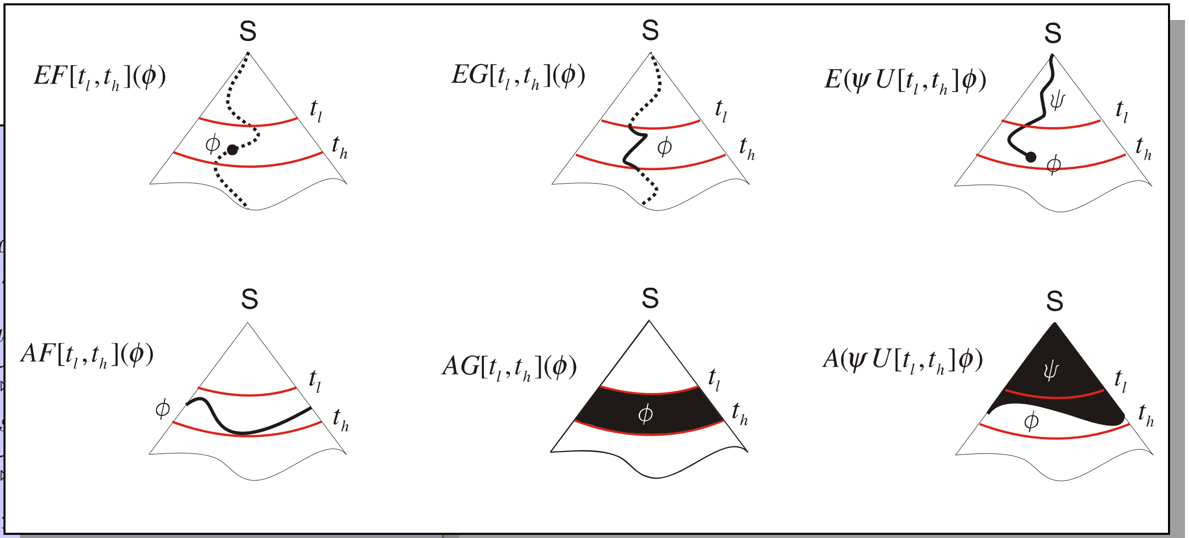
$\mathcal{T}_\ltimes \models_\ltimes AG[t_l, t_h](\phi_\ltimes) \iff \forall\pi \text{ in } \mathcal{T}_\ltimes \forall i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}_\ltimes \restriction \pi[i]) \models_\ltimes \phi_\ltimes]$

$\mathcal{T}_\ltimes \models_\ltimes E(\psi_\ltimes U[t_l, t_h]\phi_\ltimes) \iff \exists\pi \text{ in } \mathcal{T}_\ltimes \exists i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}_\ltimes \restriction \pi[i]) \models_\ltimes \phi_\ltimes$ *and*
$\forall j < i((\mathcal{T}_\ltimes \restriction \pi[j]) \models_\ltimes \psi_\ltimes)]$

$\mathcal{T}_\ltimes \models_\ltimes A(\psi_\ltimes U[t_l, t_h]\phi_\ltimes) \iff \forall\pi \text{ in } \mathcal{T}_\ltimes \exists i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}$
$\forall j < i((\mathcal{T}_\ltimes \restriction \pi[j]) \models_\ltimes \psi_\ltimes)]$

$\mathcal{T}_\ltimes \models_\ltimes E(\psi_\ltimes R[t_l, t_h]\phi_\ltimes) \iff \exists\pi \text{ in } \mathcal{T}_\ltimes \forall i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}$
$\exists j : t_{\leq j} \in [t_l, t_h], j < i((\mathcal{T}_\ltimes \restriction$

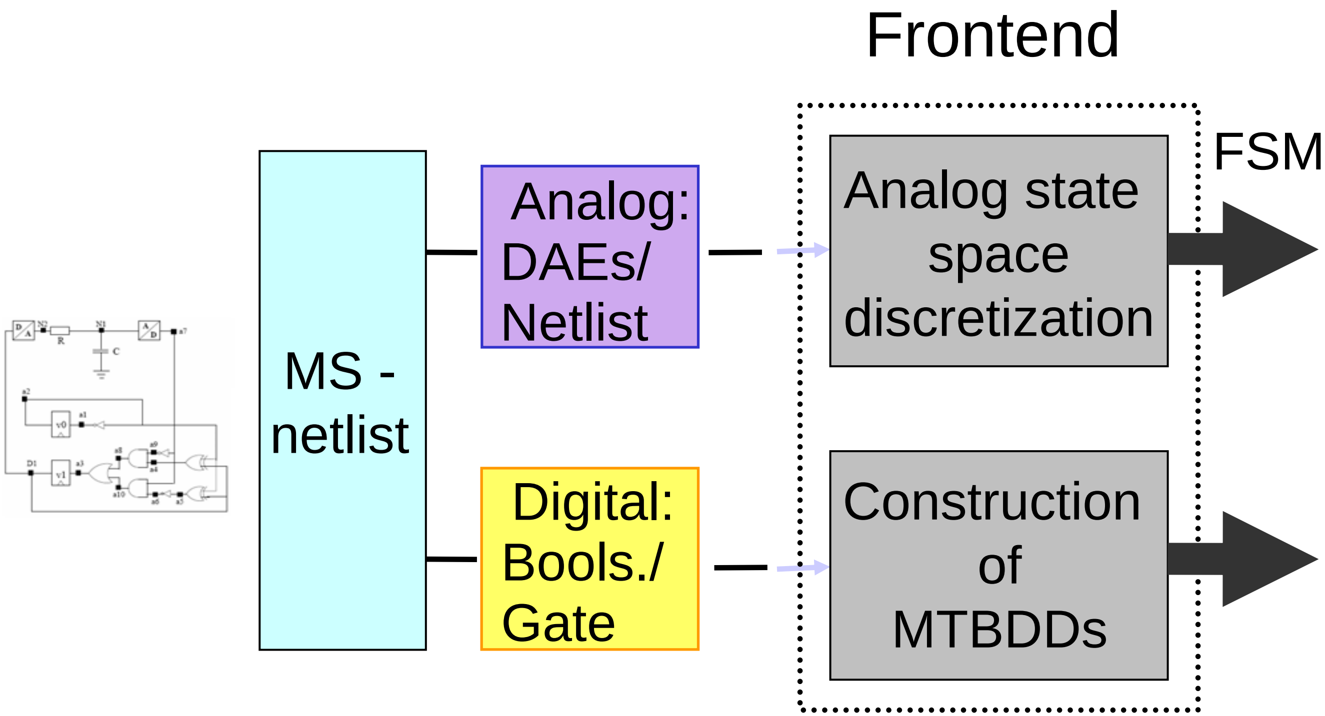
$\mathcal{T}_\ltimes \models_\ltimes A(\psi_\ltimes R[t_l, t_h]\phi_\ltimes) \iff \forall\pi \text{ in } \mathcal{T}_\ltimes \forall i : t_{\leq i} \in [t_l, t_h][(\mathcal{T}$
$\exists j : t_{\leq j} \in [t_l, t_h], j < i((\mathcal{T}_\ltimes \restriction$



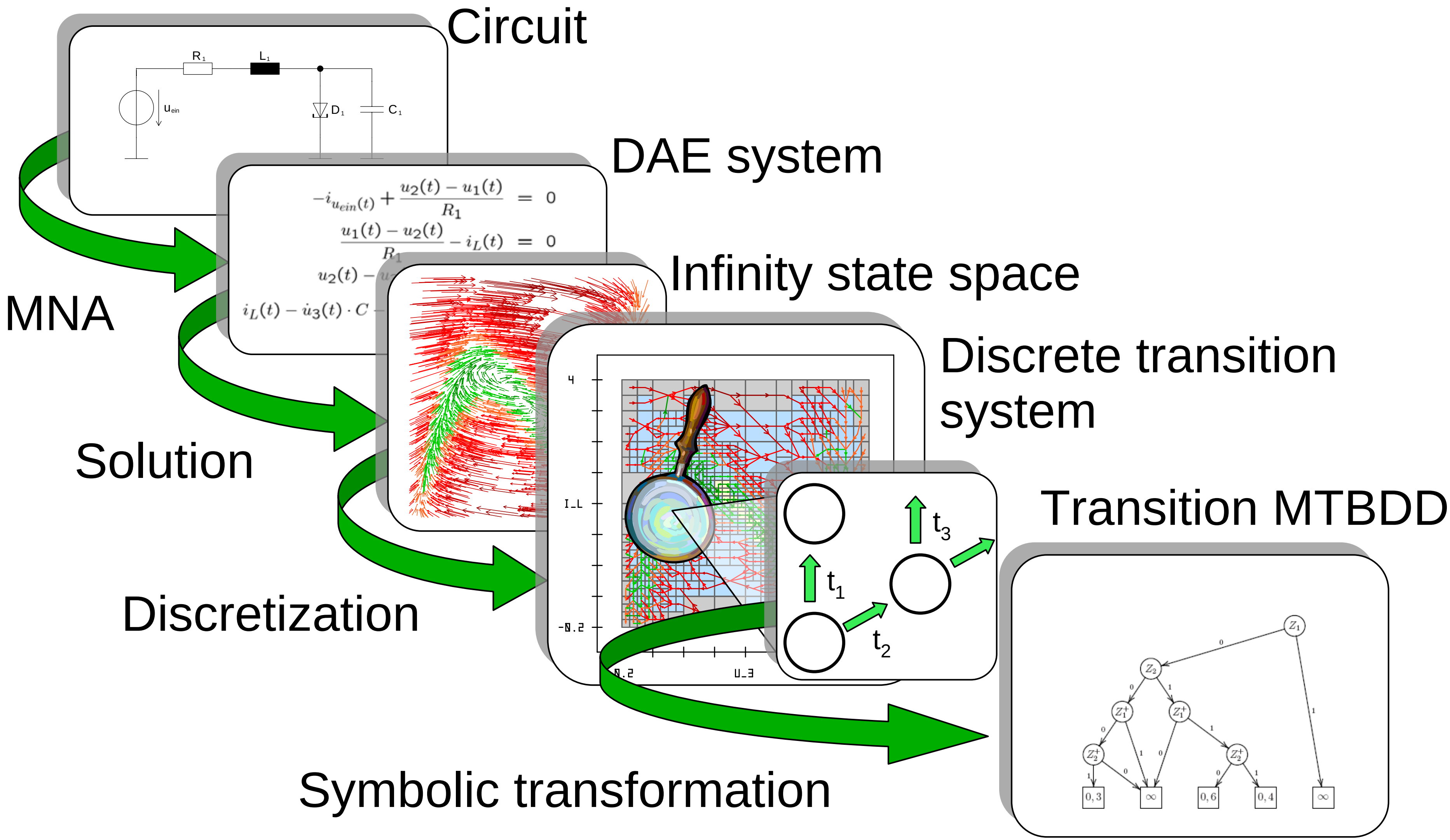
- Equivalences similar to CTL

$$AX(\phi_\ltimes) \equiv \neg EX(\neg\phi_\ltimes)$$
$$EF[t_l, t_h](\phi_\ltimes) \equiv E(1U[t_l, t_h]\phi_\ltimes)$$
$$AF[t_l, t_h](\phi_\ltimes) \equiv \neg EG[t_l, t_h](\neg\phi_\ltimes)$$
$$AG[t_l, t_h](\phi_\ltimes) \equiv \neg EF[t_l, t_h](\neg\phi_\ltimes)$$
$$A(\psi_\ltimes U[t_l, t_h]\phi_\ltimes) \equiv \neg E(\neg\phi_\ltimes U[t_l, t_h](\neg\psi_\ltimes \wedge \neg\phi_\ltimes)) \wedge \neg EG[t_l, t_h](\neg\phi_\ltimes)$$
$$EG[t_l, t_h](\phi_\ltimes) \equiv E(\perp R[t_l, t_h]\phi_\ltimes)$$
$$E(\psi_\ltimes R[t_l, t_h]\phi_\ltimes) \equiv \neg A(\neg\psi_\ltimes U[t_l, t_h]\neg\phi_\ltimes)$$
$$A(\psi_\ltimes R[t_l, t_h]\phi_\ltimes) \equiv \neg E(\neg\psi_\ltimes U[t_l, t_h]\neg\phi_\ltimes)$$

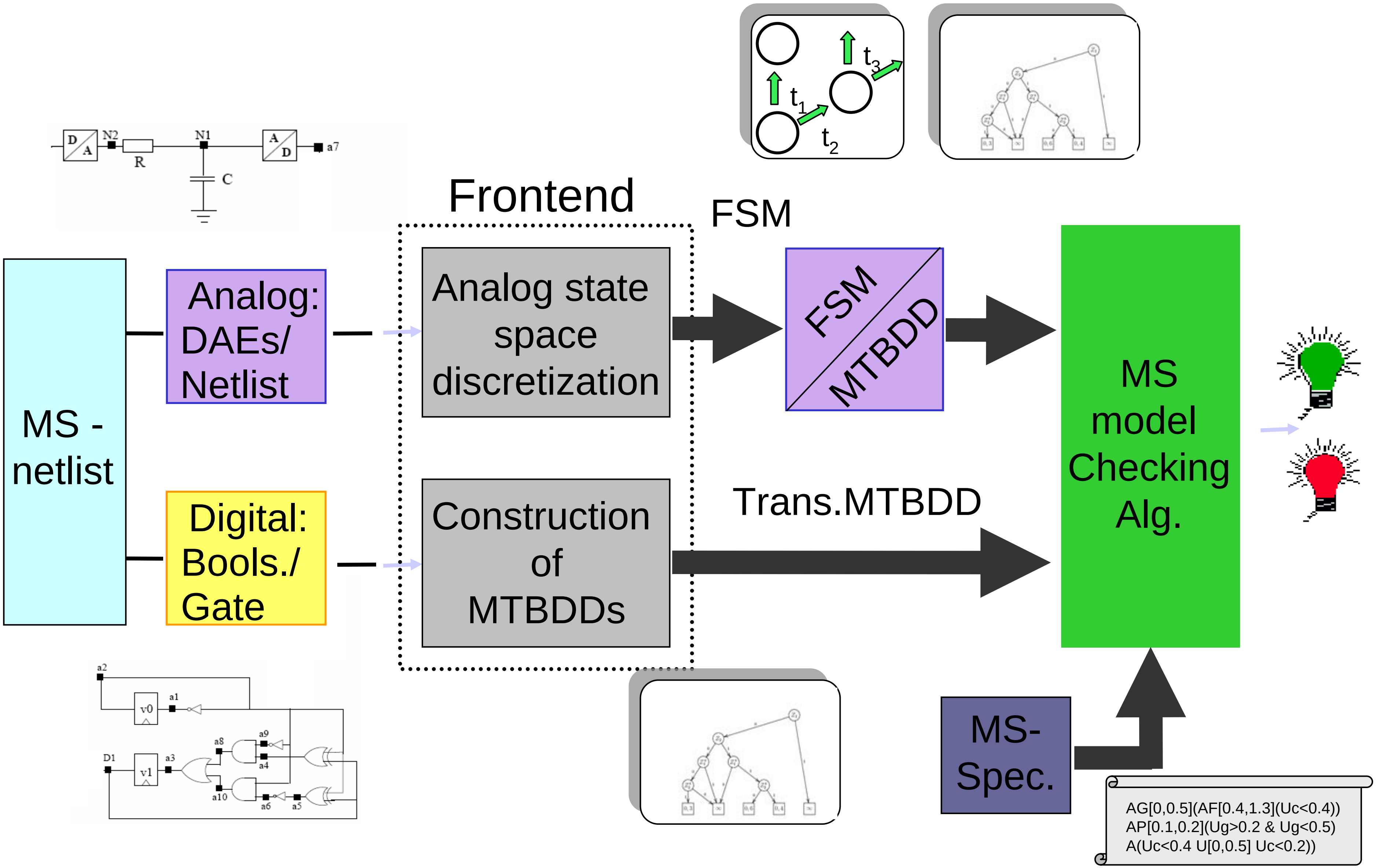
MS - model checking flow



Discrete modelling of analog circuits



MS - model checking flow (cont.)



Mixed CTL-AT properties

- Mixed CTL-AT formula consists of analog and digital initial states

$$\varphi = \varphi^D \wedge \varphi^A$$

- Evaluation of MS CTL-AT formulas can not be done independent to the appropriate other subsystem

$$EF^{MS}[t_l, t_h](\varphi) = \left\langle EF^{D_A}[t_l, t_h](\varphi^D) \right\rangle \wedge \left\langle EF^{A_D}[t_l, t_h](\varphi^A) \right\rangle$$

- Pre-image computation by variable quantification

$$\mathrm{EX}(\varphi) = \exists \vec{z}^{+} \exists \vec{e} \exists \vec{w} : \chi_\delta(\vec{z}, \vec{e}, \vec{w}) \wedge \chi_\varphi(\vec{z}^{+})$$

$$\mathrm{AX}(\varphi) = \exists \vec{z}^{+} \exists \vec{e} \forall \vec{w} : \chi_\delta(\vec{z}, \vec{e}, \vec{w}) \wedge \chi_\varphi(\vec{z}^{+})$$

$$\vec{w} \in \{\vec{u}, \vec{v}, \vec{u}, \vec{y}\}$$

$$\vec{e} \in \{\vec{u}_d, \vec{u}_a, \vec{y}_d, \vec{y}_a\}$$

MS CTL-AT Algorithms

Algorithm 1 CTLschedul($\phi_A, \phi_D, \varphi_A, \varphi_D, \chi_{\delta_A}, \chi_{\delta_D}, [t_l, t_h]$)

$A_{Min} =$ getMinTransition(ϕ_A, χ_{δ_A})
$D_{Min} =$ getMinTransition(ϕ_D, χ_{δ_D})
if $A_{Min} \leq t_h \vee D_{Min} \leq t_h$ **then**
  if $A_{Min} < D_{Min}$ **then**
    $(\Theta_A, \phi_{AI}) =$ CheckCTL($\phi_A, \varphi_A, \chi_{\delta_A}, [t_{tl}, D_{Min}]$)
    $\varphi_D =$ CheckImpact(ϕ_{AI}, ϕ_D)
    $(\Theta_D, \phi_{DI}) =$ CheckCTL($\phi_D, \varphi_D, \chi_{\delta_D}, [t_{tl}, D_{Min}]$)
    $\varphi_A =$ CheckImpact(ϕ_{DI}, ϕ_{AI})
    $t_l = t_l - D_{Min}$
    $t_h = t_h - D_{Min}$
  else
    $(\Theta_D, \phi_{DI}) =$ CheckCTL($\phi_D, \varphi_D, \chi_{\delta_D}, [t_l, A_{Min}]$)
    $\varphi_A =$ CheckImpact(ϕ_{DI}, ϕ_A)
    $(\Theta_A, \phi_{AI}) =$ CheckCTL($\phi_A, \varphi_A, \chi_{\delta_A}, [t_l, A_{Min}]$)
    $\varphi_D =$ CheckImpact(ϕ_{AI}, ϕ_{DI})
    $t_l = t_l - A_{Min}$
    $t_h = t_h - A_{Min}$
  end if

  $(\tilde{\Theta}_A, \tilde{\Theta}_D) =$ CTLschedul($\phi_{AI}, \phi_{DI}, \varphi_A, \varphi_D, \chi_{\delta_A}, \chi_{\delta_D}, [t_l, t_h]$)
  $\Theta_A = \Theta_A \cup \tilde{\Theta}_A$
  $\Theta_D = \Theta_D \cup \tilde{\Theta}_D$
  return Θ_A, Θ_D
end if

Problems:

- Different time characteristics
  - Digital: synchronous
  - Analog: continuous
- Interaction between both sub-circuits

MS CTL-AT Algorithms (ex.: EF operation)

- **Assumption: Global digital clock τ_{clk}**

Algorithm 2 CheckDigitalTimeEF($\phi_D, \chi_{\delta_D}, [t_l, t_h]$)

```
Ω_i = false, Ω_{i+1} = φ_D, Υ = φ_D, Θ = false
if t_l < τ_clk then
    Θ = φ_D
end if
while t_h ≥ τ_clk do
    if Ω_i ≠ Ω_{i+1} then
        t_h = t_h − τ_clk, t_l = t_l − τ_clk
        Ω_i = Ω_{i+1}
        Υ = CheckEX(Υ, χ_{δ_D})
        if t_l < τ_clk then
            Θ = Θ ∪ Υ
        end if
        Ω_{i+1} = Υ ∪ Ω_i
    else
        Θ = Θ ∪ Ω_{i+1}
        t_h = 0
    end if
end while
return Θ, Υ
```

- Taking care about time constraints
- Simple EX operation (Quantification)
- Returns results and front state for further processing

MS CTL-AT Algorithms (ex.: EF operation)

- Different transition delay times

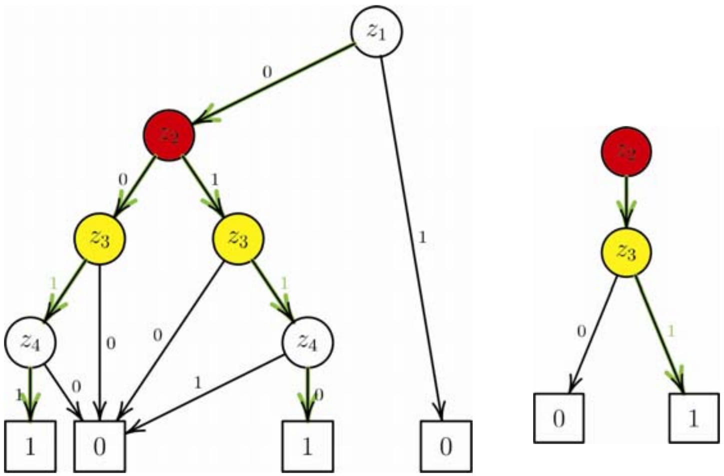
Algorithm 3 CheckAnalogTimeEF($\phi_A, \chi_{\delta_A}, [t_l, t_h]$)

$\Theta = false, \Upsilon = false$
for all transitions $\lambda(\phi_A, \chi_{\delta_A}) \in \delta$ **do**
  τ_{tr} = getTransitionTime($\lambda(\phi_A, \chi_{\delta_A})$)
  if $t_l < \tau_{tr}$ **then**
    $\Theta = \phi_A$
  end if
  if $\tau_{tr} \leq t_h$ **then**
    ϕ_A = CheckEX($\phi_A, \chi_{\delta_A}, \tau_{tr}$)
    $(\tilde{\Theta}, \tilde{\Upsilon})$ = CheckAnalogTimeEF($\phi_A, \chi_{\delta_A}, [t_l\text{-}\tau_{tr}, t_h\text{-}\tau_{tr}]$)
    $\Theta = \Theta \cup \tilde{\Theta}, \Upsilon = \Upsilon \cup \tilde{\Upsilon}$
  else
    $\Upsilon = \phi_A$
  end if
end for
return Θ, Υ

- Taking care about time constraints
- Simple EX operation (Quantification)
- Recursive traversaling through the analog state space
- Returns results and front state for further processing

MS CTL-AT Algorithms (CheckImpact)

- Analysis of dependent intercommunication signals
- Modifies the according transition MTBDD



Algorithm	CheckImpact(ϕ, χ_δ)

$\Omega = \emptyset$

for $\forall$ *states* $\phi_i \in \phi$ **do**

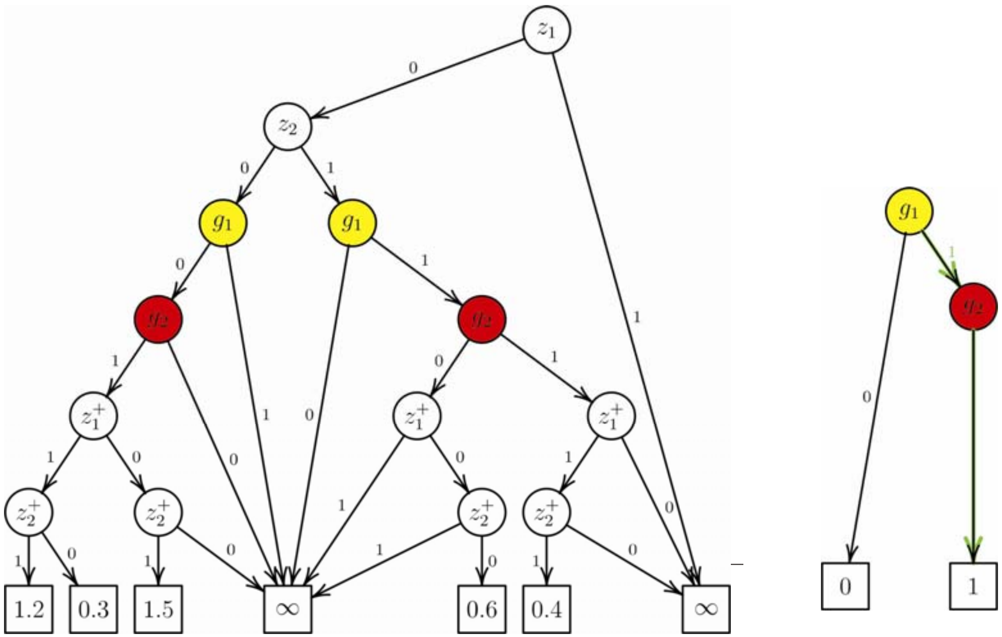
  $\varphi_{out} = \text{getOutputCube}(\phi_i)$

  $\Omega = \Omega \vee \varphi_{out}$

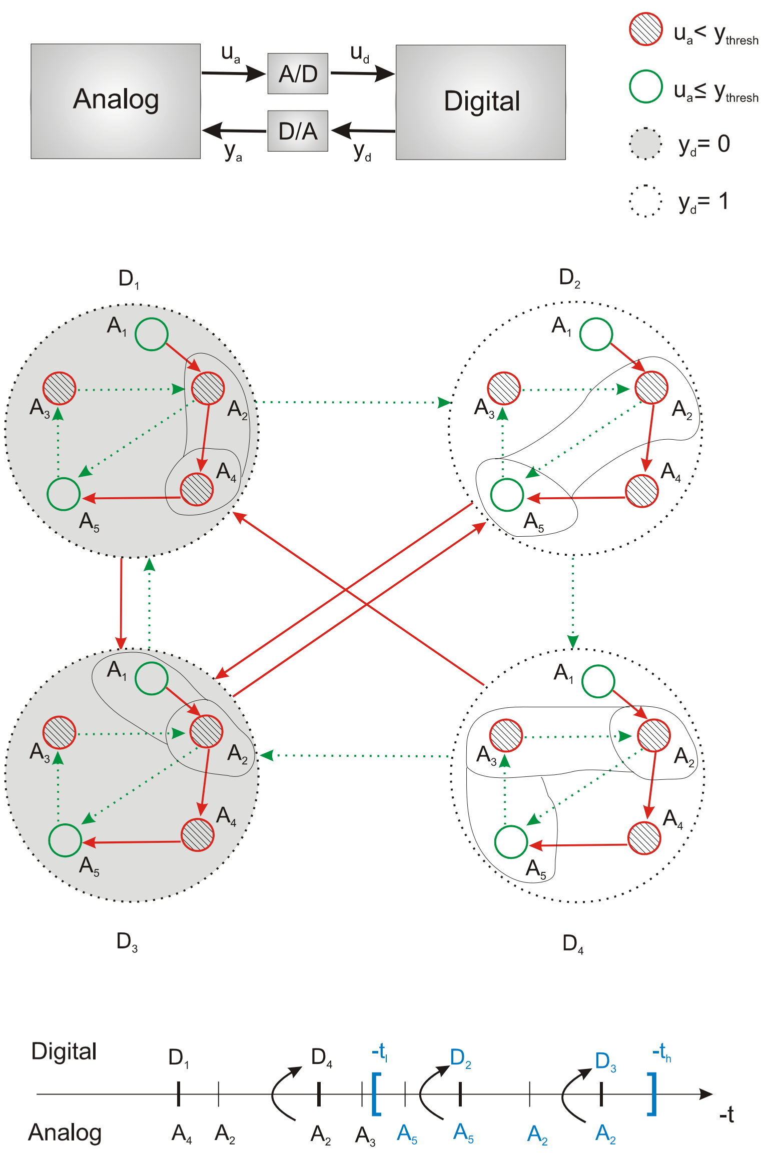
end for

$\varphi_{inp} = \text{getInputCube}(\Omega, \chi_\delta)$

return φ_{inp}



MScheck Demonstration



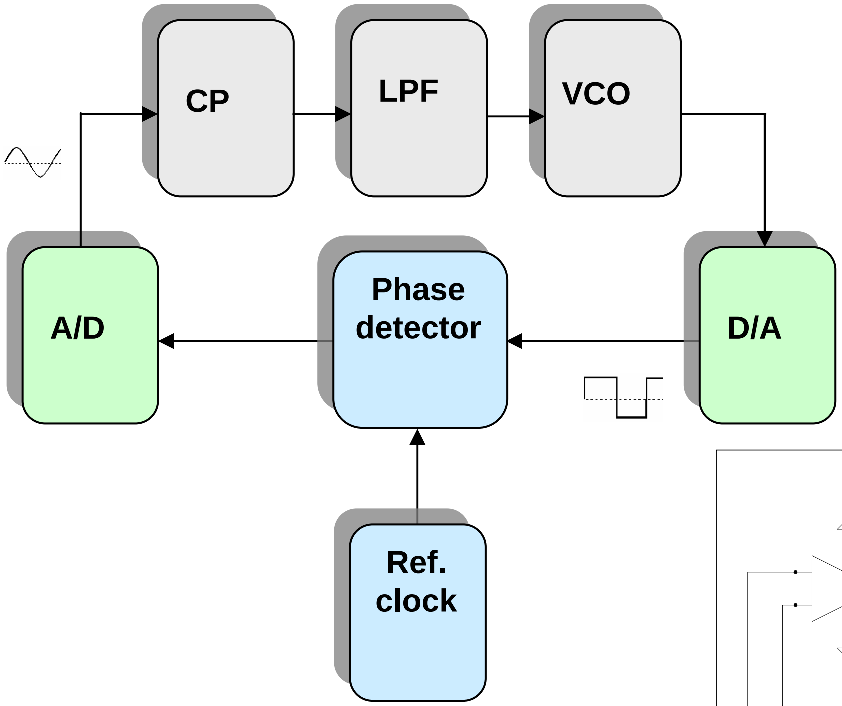
Assumption (w.l.o.g.):

$$\forall i : t_i^A \leq t_{clk}^D$$

CTL-AT formula:

$$EF[t_l, t_h](D_1 \wedge A_4)$$

Example: Phase Locked Loop (PLL)



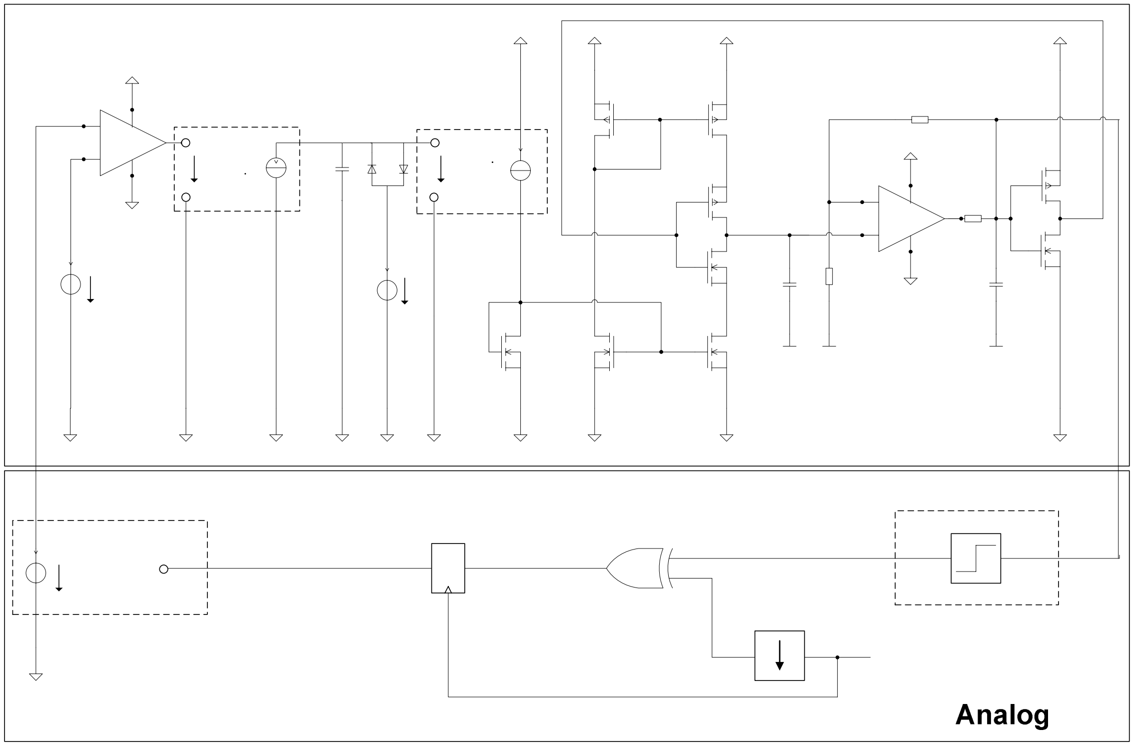
Legend:

CP: charge pump

LPF: Low Pass Filter

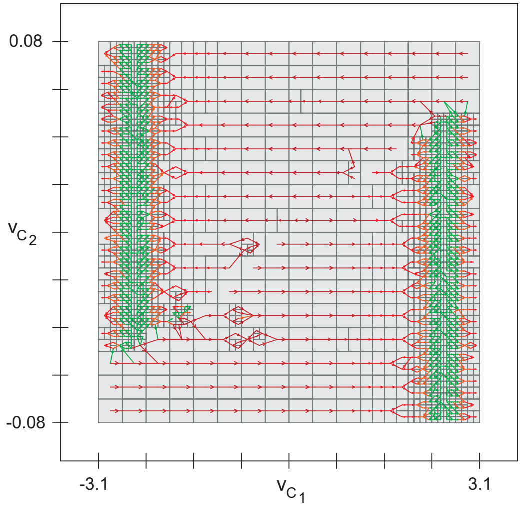
VCO: Voltage Control Oscillator

Schematic

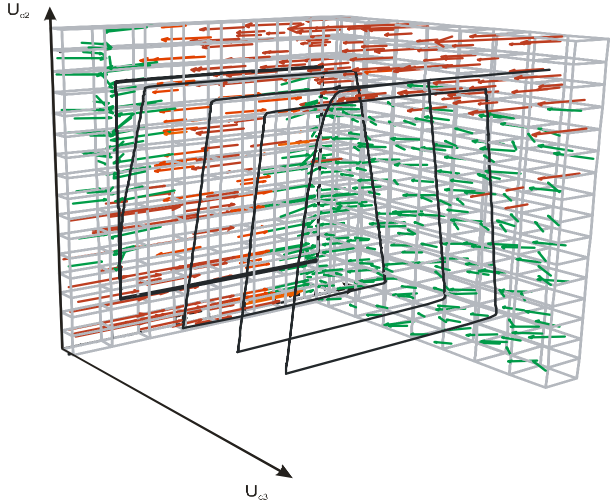


Verification Results

VCO state space



Analog sub-state space



Verification Results:

Reachability

$$\phi_{lock} \models EP[0.0ms, 20.0ms](\phi_D \wedge \phi_A)$$

Locking behavior

$$true \models AF[0.0ms, 30.0ms](\phi_{lock})$$

Conclusion

- A symbolic approach for Mixed-Signal model checking is given based on
  - Real-Time transition structures (RTTS)
  - MTBDDs representing transition relations
  - CTL-AT as the specification language
  - based on modified fixpoint algorithms for evaluating CTL-AT formulas
- The approach is demonstrated on a PLL
  - analyzing reachability and
  - locking behavior