A Sampling Approach to Analysis of Continuous Time Metric Temporal Logic

Paritosh Pandya

Tata Institute of Fundamental Research, Mumbai

Joint Work with

Gaurav Chakravorty, S.N. Krishna, Kuntal Loya, Babita Sharma, Supratik Chakraborty

IIT Bombay and IIT Kanpur

* Partially supported by the TIFR Project 11P202 titled *Construction, Analysis and Verification of Embedded Systems*

Timed Systems

- Evolution of system state with time
- Specified used temporal logics [Puneli 77]
- Modelled using Automata
- Decision Problems: Validity Checking, Model Checking.

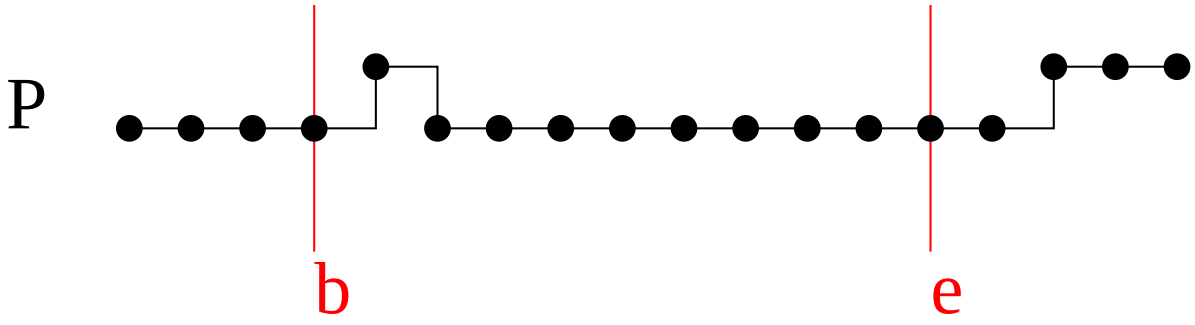
Metric Time

- Logics: Metric Temporal Logic MTL [Koy90], Duration Calculus [ZHR91]
- Automata: Timed Automata [Alur-Dill 1990]

Issue: Different notions of times,
Decidability varies based on nature of time.

Timed Behaviours

$Pvar$ observable propositions.
Behaviour $\theta(p) : Time \rightarrow \{0, 1\}$



Continuous Time $T = \Re^0$.

- Finitely Variable Behaviours: Finitely many state changes in finite interval.
- Right Continuous Behaviours: No Glitches.
  $\forall t \exists \delta > 0$ s.t. $\theta(P)$ is constant in interval $[t : t + \delta)$.

Other Time Structures

Sampled Time

- Countable set of real-valued time points where the state is recorded.

  $$(s_0, 0), (s_1, 2.3), (s_3, \pi), (s_4, 5.7), \ldots$$

- Timed words model [Alur-Dill].
- Close connection to Timed/Hybrid Automata.

Discrete Time Natural numbered sampling points.

- Useful describing for clocked circuits, synchronous systems, qualitative behaviour.
- Digital (finite precision) clocks.

On Discretely Being Dense

Morphisms between behaviours with different time structures.
Translations between logics with different time structures.

- Continuous Time $\longrightarrow$ Sampled Time $\longrightarrow$ Discrete Time
- Preserve either models or counter-models or both.
- Provide a partial technique for the Verification of Continuous Time Logic Formulae by reduction to Discrete Time Formulae.

Frames and Behaviours

A behaviour is $(\mathbb{F}, \theta)$.

- Frame $\mathbb{F}$ – sequence of convex intervals "covering" $\Re^0$.
  $\mathbb{F} = (F_1, F_2, \ldots)$ such that $\nearrow F_i = \nwarrow F_{i+1}$ and $(\cup_i F_i) = \Re^0$.
- $dom(\mathbb{F})$ the indices of sequence $\mathbb{F}$.
  Valuation $\theta \in dom(\mathbb{F}) \rightarrow 2^{Pvar}$

Example A behaviour $(\mathbb{F}, \theta)$ is given below.

$\mathbb{F}$	=	[0,1.5)	[1.5,2.4)	[2.4]	[2.4]	[2.4,3)	[3,4.3)	[4.3,∞)
θ	=	$\neg P$,	P,	$\neg P$,	P,	$\neg P$,	P,	$\neg P$

Here, $dom(\mathbb{F}) = \{1, 2, \ldots, 7\}$ and $\theta(1) = \neg P$.

Points

Given frame $\mathbb{F} = (F_1, F_2, \ldots)$, a time point is (t, i) with $t \in F_i$. Here t is the time stamp and i is the phase number.

- $Points(\mathbb{F}) \stackrel{\text{def}}{=} \{(t, i) \mid t \in F_i\}$
- Time points are linearly ordered:
  $(t_1, i_1) \leq (t_2, i_2) \iff (t_1 \leq t_2) \wedge (i_1 \leq i_2)$.
- distance $d(b, e)$ between time points:
  $d((t, i), (t', i')) = |t - t'|$.
- We use b, e, z for points. Initial point is $\overline{0} = (0, 1)$.

Example Points $(0.5, 1) < (2.4, 3) < (2.4, 4) < (2.4, 5) < (3, 6)$

$\mathbb{F}$	=	[0,1.5)	[1.5,2.4)	[2.4]	[2.4]	[2.4,3)	[3,4.3)	[4.3,∞)
θ	=	$\neg P$,	P,		$\neg P$,	P,	$\neg P$,	P,	$\neg P$

State $\hat{\theta}(2.4, 3) = \neg P$ and $\hat{\theta}(2.4, 4) = P$ and $\hat{\theta}(2.4, 5) = \neg P$.

Observable Points

Only a subset S of points $points(\mathbb{F})$ can be observable.
Initial point $\overline{0} \in S$.

- S must be *time divergent*, i.e for $t \in \Re^0$ there exists $(t', i') \in S$ with $t' > t$.
- $(S, \mathbb{F}, \theta)$ is called o-behaviour.
- M denotes given collection of o-behaviours.

Example

- Strictly monotonic time: $M_{st} \stackrel{\text{def}}{=} \{(S, \mathbb{F}, \theta) \in M_{ct} \mid \text{for all } (i+1) \in dom(\mathbb{F}).\ F_i \cap F_{i+1} = \emptyset\}$.

We can generically define MTL over class of behaviours M

Metric Temporal Logic

- Let $I = \langle i, j \rangle$ denote interval with integral end points $i, j \in \aleph$. $j = \infty$ is also allowed for right open interval.
- Interval is non-empty but can be closed, open or half-open and also singular.
  E.g. $[2, 3],\ (2, 3],\ (2, 3),\ [2, 2],\ [2, \infty)$.
- Let $k + \langle i, j \rangle$ denote $\langle k + i, k + j \rangle$.

Syntax of MTL

$$\top \mid p \mid \phi \wedge \psi \mid \neg\phi \mid \phi \mathcal{S}_I \psi \mid \phi \mathcal{U}_I \Psi$$

$\phi \mathcal{U}_I \psi$ holds at point b provided ψ holds at some $e \geq b$ s.t. $d(b, e) \in I$ and ϕ holds for all $z : b \leq z < e$.

Semantics

Given o-behaviour $(S, \mathbb{F}, \theta)$ and $b \in S$, define $S, \mathbb{F}, \theta, b \models \phi$

$S, \mathbb{F}, \theta, b \models p$ iff $p \in \theta(i)$ where $b = (t, i)$

$S, \mathbb{F}, \theta, b \models \phi \mathcal{U}_I \psi$ iff for some $e \in S : b \leq e$.
$d(b, e) \in I$ and $S, \mathbb{F}, \theta, e \models \psi$ and
for all $z \in S : b \leq z < e$. $S, \mathbb{F}, \theta, z \models \phi$

$S, \mathbb{F}, \theta, b \models \phi \mathcal{S}_I \psi$ iff for some $e \in S : e \leq b$.
$d(e, b) \in I$ and $S, \mathbb{F}, \theta, e \models \psi$ and
for all $z \in S : e < z \leq b$. $S, \mathbb{F}, \theta, z \models \phi$

Note that $\mathcal{U}_I$ and $\mathcal{S}_I$ are relativized to the set of observable points.

Satisfiability

$MTL[M]$ denotes that formulae are interpreted over o-behaviours from M.

- Model is $(S, \mathbb{F}, \theta, b)$
- Anchored validity: $S, \mathbb{F}, \theta \models \phi$ iff $S, \mathbb{F}, \theta, \overline{0} \models \phi$
- $M \models \phi$ iff $S, \mathbb{F}, \theta \models \phi$ for all $(S, \mathbb{F}, \theta) \in M$
- $\phi \in MTL[M]$ is satisfiable if for some $(S, \mathbb{F}, \theta) \in M$ we have $S, \mathbb{F}, \theta \models \phi$.

Continuous Time MTL_{ct}

- Time is continuous but finitely variable
- Time is weakly monotonic
- For any $\mathbb{F}$ all points are observable: $S = points(\mathbb{F})$

$$M_{ct} \stackrel{\text{def}}{=} \{(Points(\mathbb{F}), \mathbb{F}, \theta) \mid \mathbb{F} \in FRAM,\ \theta \in BEH(\mathbb{F})\}.$$

$$MTL_{ct} = MTL[M_{ct}].$$

Theorem[Alur-Henzinger93] Satisfiability of MTL_{ct} formulae is undecidable.

Sampled Timed Behaviours

- Let $Ch(\mathbb{F})$ set of beginning point of each phase
- Set of observable points $S_{\mathbb{F}}$ is adequate for $\mathbb{F}$ if
  - $Ch(\mathbb{F}) \subseteq S_{\mathbb{F}}$,
  - $S_{\mathbb{F}}$ is countably infinite and time divergent.
- Logic MTL_{pt} is given by $MTL[M_{pt}]$.
  $M_{pt} = \{(S_{\mathbb{F}}, \mathbb{F}, \theta) \mid S_{\mathbb{F}}$ is adequate$\}$.

Example

F	[0,		3.2) [3.2,		*)		
Ch(F)	0		3.2				
S(F)	0	2.7	3.2	4.1	6.1	8.1	...

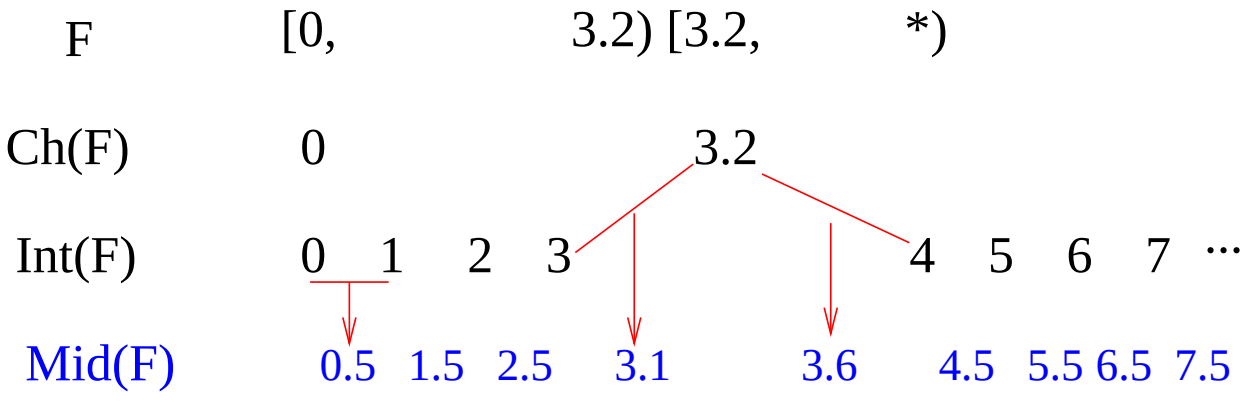
Approach

- Continuous time logic is more natural for specification.
  $\Diamond_{[2,3]}\phi \quad \Rightarrow \quad \Diamond_{[1,1]}(\Diamond_{[1,2]}\phi)$.
- Sampled Time Logic is easier to analyse algorithmically.

Approach Specify in Continuous time and verify in Sampled time.

Well Sampled IDL

Given $\mathbb{F}$ define $WS(\mathbb{F})$ the set of well sampling points with 1-oversampling.



.

- $WS(\mathbb{F}) = Ch(\mathbb{F}) \cup Int(\mathbb{F}) \cup Mid(\mathbb{F})$
- $M_{ws} = \{(WS(\mathbb{F}), \mathbb{F}, \theta)\}$
- $MTL_{ws} \stackrel{\text{def}}{=} MTL[M_{ws}]$

Sampling Approximation

$f : \Re^0 \rightarrow WS(\mathbb{F})$.

$f(b) = b$ if $b \in WS(\mathbb{F})$

$f(b)$ maps to midpoint otherwise.

Properties of f

- f is Onto and Weakly order preserving:
  $b \leq e \;\; \Rightarrow f(b) \leq f(e)$
- f is not strictly order preserving: $b < e \;\; \not\Rightarrow f(b) < f(e)$
- State does not change in closed interval $[f(b), b]$.
- $d(f(b), b) < 0.5$

Bounded Sampling Error $-1 \; < \; d(b, e) - d(f(b), f(e)) \; < \; 1.$

Sampling of Models and Errors

Approximate continuous time model $(Points(\mathbb{F}), \mathbb{F}, \theta, b)$ to a canonical sampled-time model $(WS(\mathbb{F}), \mathbb{F}, \theta, f(b))$.

Error bounds $-1 \ < \ d(b,e) - d(f(b), f(e)) \ < \ 1$

Idea: Relax the constants (intervals) in the formulae to account for sampling errors.

Given a (open, closed or half-open) interval $I = \langle i, j \rangle$ let

- I^+ be $(i-1, j+1)$ if $i - 1 \geq 0$ and be $[0, j+1)$ otherwise.
- I^- be $[i+1, j-1]$ if $i + 1 \geq j - 1$, and be undefined otherwise.

Sampling Abstraction

Translations Let α^+ and α^- : $MTL_{ct} \rightarrow MTL_{ws}$.

Example: $\alpha^+(p\mathcal{U}_{[2,4]}q) = p\mathcal{U}_{(1,5)}q$ and
$\alpha^-(p\mathcal{U}_{[2,4]}q) = p\mathcal{U}_{[3,3]}q$.

Theorem [Sampling Abstraction]

1. $\mathbb{F}, \theta, b \models_{ct} \phi \Rightarrow \mathbb{F}, \theta, f(b) \models_{ws} \alpha^+(\phi)$.
2. $\mathbb{F}, \theta, b \models_{ct} \phi \Leftarrow \mathbb{F}, \theta, f(b) \models_{ws} \alpha^-(\phi)$

Corollary

1. $\models_{ws} \alpha^-(\phi) \Rightarrow \models_{ct} \phi$,
2. $\mathbb{F}, \theta, f(b) \not\models_{ws} \alpha^+(\phi) \Rightarrow \mathbb{F}, \theta, b \not\models_{ct} \phi$.

Sampling Abstraction Definition

- $\alpha^+(p) = \alpha^-(p) = p$.
- $\alpha^+(\phi \wedge \psi) = \alpha^+(\phi) \wedge \alpha^+(\psi)$ and $\alpha^-(\phi \wedge \psi) = \alpha^-(\phi) \wedge \alpha^-(\psi)$.
- $\alpha^+(\neg\phi) = \neg\alpha^-(\phi)$ and $\alpha^-(\neg\phi) = \neg\alpha^+(\phi)$.
- $\alpha^+(\phi \mathcal{U}_I \psi) = \alpha^+(\phi)\, \mathcal{U}_{I^+}\, \alpha^+(\psi)$.
- $\alpha^-(\phi \mathcal{U}_I \psi) = \alpha^-(\phi)\, \mathcal{U}_{I^-}\, \alpha^-(\psi)$.
- $\alpha^+(\phi \mathcal{S}_I \psi) = \alpha^+(\phi)\, \mathcal{S}_{I^+}\, \alpha^+(\psi)$.
- $\alpha^-(\phi \mathcal{S}_I \psi) = \alpha^-(\phi)\, \mathcal{S}_{I^-}\, \alpha^-(\psi)$.
- $\alpha^-(\phi \mathcal{U}_I \psi)$ and $\alpha^-(\phi \mathcal{S}_I \psi)$ are $false$ when I^- is undefined.

Decidability and Model checking

Theorem The Satisfiability of MTL_{pt} is undecidable [AH93]. The satisfiability of MTL_{ws} is also undecidable.

- Special cases are known to be decidable. E.g. MTL_{pt} without $\mathcal{S}_I$ over finite timed words [Ouaknine-Worrell].
- Standard automata theory of timed and hybrid systems is based on sampled time models.
- Several partial techniques such as bounded model checking can be used.

Integer Time

A frame $\mathbb{F}$ is called discrete if $Ch(\mathbb{F}) \subseteq Int(\mathbb{F})$. In discrete frames state changes only at integer times.

Integer Timed MTL

- The set of sampling points is exactly the set of points with integer time stamps. Behaviours are discrete
- $M_{ZF} \stackrel{\text{def}}{=} \{(Int(\mathbb{F}), \mathbb{F}, \theta, b) \mid \mathbb{F} \text{ is discrete}\}$
- $MTL_{ZF} \stackrel{\text{def}}{=} MTL[M_{ZF}]$

Theorem [AH93,Hen98] Satisfiability of MTL_{ZF} is decidable and EXPSPACE-complete (assuming binary encoding of integer constants).

Digitization

Transforms Sampled time model into discrete time model [HMP93].

Example: $\mathbb{F} = [0, 1.5)[1.5, 4.35)[4.35, \infty)$.
Then, $[\mathbb{F}] \downarrow 0.4 = [0, 2)[2, 4)[4, \infty)$,
and $[\mathbb{F}] \downarrow 0.6 = [0, 1)[1, 4)[4, \infty)$.

The set of digitizations
$Z((S, \mathbb{F}, \theta, b)) = \{(S, \mathbb{F}, \theta, b) \downarrow \epsilon \mid 0 \leq \epsilon < 1\}$.

- In digitization, the number and ordering of phases remains same.
- The end points of the phases and sampling points are shifted to nearby integer points.
- Digitizationn causes quantization error in distance measurement.

Digitization Abstraction

Given an interval I

- $I\uparrow$ be the smallest closed interval containing I
- $I\downarrow$ be the largest open interval contained in I.
- If I is singleton closed interval $[i,i]$ then $I\downarrow$ is undefined.

Example: $[2,4)\uparrow \;=\; [2,4]$ and $[2,4)\downarrow \;=\; (2,4)$.

Translations β^+ and β^- : $MTL_{ws} \rightarrow MTL_{ZF}$.

Example $\beta^+(p\mathcal{U}_{[2,4)}q) \;=\; p\mathcal{U}_{[2,4]}q$ and
$\beta^-(p\mathcal{U}_{[2,4)}q) \;=\; p\mathcal{U}_{(2,4)}q$.

Digitization Abstraction

Translations β^+ and β^- : $MTL_{ws} \rightarrow MTL_{ZF}$.

Theorem[Digitization abstraction]

1. $S, \mathbb{F}, \theta, b \models_{ws} \phi \quad \Rightarrow \quad Z(S, \mathbb{F}, \theta, b) \models_Z \beta^+(\phi)$,
2. $S, \mathbb{F}, \theta, b \models_{ws} \phi \quad \Leftarrow \quad Z(S, \mathbb{F}, \theta, b)) \models_Z \beta^-(\phi)$.

Corollary

1. $\models_Z \beta^-(\phi) \quad \Rightarrow \quad \models_{ws} \phi$,
2. $S, \mathbb{F}, \theta, b \not\models_Z \beta^+(\phi) \quad \Rightarrow \quad S, \mathbb{F}, \theta, b \not\models_{ws} \phi$.

Digitization Reduction

- $\beta^+(p) = \beta^-(p) = p$.
- $\beta^+(\phi \wedge \psi) = \beta^+(\phi) \wedge \beta^+(\psi)$ and $\beta^-(\phi \wedge \psi) = \beta^-(\phi) \wedge \beta^-(\psi)$.
- $\beta^+(\neg\phi) = \neg\beta^-(\phi)$ and $\beta^-(\neg\phi) = \neg\beta^+(\phi)$.
- $\beta^+(\phi \mathcal{U}_I \psi) = \beta^+(\phi)\, \mathcal{U}_{I\uparrow}\, \beta^+(\psi)$.
- $\beta^-(\phi \mathcal{U}_I \psi) = \beta^-(\phi)\, \mathcal{U}_{I\downarrow}\, \beta^-(\psi)$.
- $\beta^+(\phi \mathcal{S}_I \psi) = \beta^+(\phi)\, \mathcal{S}_{I\uparrow}\, \beta^+(\psi)$.
- $\beta^-(\phi \mathcal{S}_I \psi) = \beta^-(\phi)\, \mathcal{S}_{I\downarrow}\, \beta^-(\psi)$.
- $\beta^-(\phi \mathcal{U}_I \psi)$ and $\beta^-(\phi \mathcal{S}_I \psi)$ are $false$ when $I\downarrow$ is undefined.

Approach to Validity Checking MTL_{ct}

Give Continuous time MTL_{ct} formula ϕ

- Compute $\phi^- \stackrel{\text{def}}{=} \beta^-(\alpha^-(\phi))$. Check the validity of ϕ^-. By theorems, $\models_{ZF} \phi^-$ then $\models_{ct} \phi$. If not valid, proceed below.
- Compute $\phi^+ \stackrel{\text{def}}{=} \beta^+(\alpha^+(\phi))$. Check for counter-example. By theorems, if $\mathbb{F}, \theta, b \not\models_{ZF} \phi^+$ then $r(\mathbb{F}, \theta, b) \not\models_{ct} \phi$.
- If ϕ^- is not valid and ϕ^+ is valid, the method fails to give any result. In this case scaling theorem can be applied.

Scaling Theorem

Theorem $S, \mathbb{F}, \theta, b \models_{ct} \phi$ **iff** $k \cdot S, k \cdot \mathbb{F}, \theta, k \cdot b \models_{dc} \phi_k$
where

- ϕ_k is ϕ with each constant c replaced by $c \cdot k$,
- $k \cdot \mathbb{F}$ obtained by replace each phase $[i, j)$ by $[k \cdot i, k \cdot j)$.
- $k \cdot S$ obtained by replacing each point $(t, i) \in S$ by point $(t \cdot k, i)$

Corollary $\models_{ct} \phi$ **iff** $\models_{ct} \phi_k$

Duration Calculus

- Rich real-time logic for safety and time-bounded liveness property.
- Includes notion of “accumutated duration” of state $\int P$.
- Sampling and digtization approximations have been applied to DC to give strong and weak reduction to Discrete Duration Calculus DDC.
- Provides a partial but pratical technique.

Claim Sampling and digitization of MTL_{ct} can be practically useful.

Gas Burner in DC

- $Concl$ In any interval of a seconds the accumulated duration of Leak is at most b.
  $$\Box(\ell \leq a \ \Rightarrow \ \int Leak \leq b).$$
- $Des1$ Leak lasts at most d seconds at a stretch.
  $$\Box(\lceil\!\lceil Leak \rceil\!\rceil \ \Rightarrow \ \ell \leq d)$$
- $Des2$ Between any two leaks at least c sec.
  $$\Box(\lceil\!\lceil Leak \rceil\!\rceil \frown \lceil\!\lceil \neg Leak \rceil\!\rceil \frown \lceil\!\lceil Leak \rceil\!\rceil \ \Rightarrow \ell > c).$$
- $G(c, d, a, b) \ \stackrel{\text{def}}{=} \ Des1 \wedge Des2 \Rightarrow Concl.$

Correctness: show that $\models G$ for given value of parameters.

Experimental Results

Gas Burner: check $\models G(c, d, a, b)$ for given parameters.

Parameters	DCVALID (hh:mm:ss)	Parameters	DCVALID strong (hh:mm:ss)	DCVALID weak (hh:mm:ss)
Gas Burner: Valid Cases		Gas Burner: Cases with counter examples		
(4,8,30,18)	02.91s	(2,4,99,6)	1.25s	1m 22s
(20,40,120,50)	2m 28.43s	(3,3,150,36)	18m 37s	19m 31.53s
(1,4,20,12)	1.50s	(20,40,200,75)	33m 29.54s	6m 27.55s
(1,4,60,32)	14.95s	(2,4,500,15)	2h 5m 3.75s	2h 4m 8.91s
(2,4,100,53)	1m 1.62s	(5,5,350,25)	2h 13m 53s	2h 14m 12s
(2,4,300,250)	20m 39.22s	(7, 3, 175, 27)	33m 37.47s	32m 57s

In all cases `dc2qddc` translation time is 0.3sec

Experimental Results (continued)

- For $G(2, 6, 15, 7)$ the method failed to give answer. Instance was scaled to $G(4, 12, 30, 14)$ which was proved valid showing also that the original instance is also valid.
- Other Examples: Minepump control, Lift Control, Small Delay Insensitive Circuits.

Conclusions

- Continuous time seems more natural when specifying real-time behaviours.
- There is general lack of tools for continuous time logics/automata.
- Sampling: a technique to approximate continous time logic by sampled time logic.
- Digitization: a technique to approximate sampled time logic by discrete time logic.
- Interesting but partial approach to validity (model) checking of real-time logics.
- Ongoing work: Other sampling schemes.

Main Reference

- A Sampling Approach to the Analysis of Metric Temporal Logic, in *Perspectives in Concurrency*, A Festschrift for P.S. Thiagarajan, Prentice Hall India, 2008.

Thank You

Questions?