Generation of Signals under Temporal Constraints for CPS Testing

Benoît Barbot[1], Nicolas Basset[2] and Thao Dang[2]

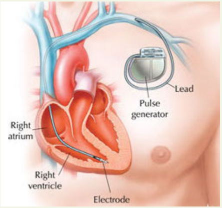
[1]LACL, Université Paris Est Créteil, France

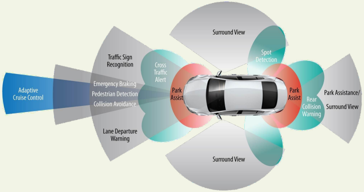
[2]VERIMAG/CNRS, Université Grenoble Alpes, France

Vendredi 24 Mai 2019, Mefosyloma

Cyber Physical System (CPS)

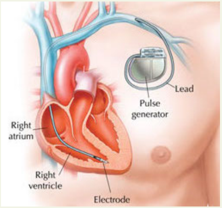
Examples

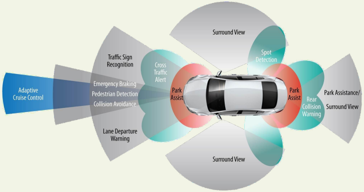




Cyber Physical System (CPS)

Examples





System with three different interacting aspects

- ▷ A continuous deterministic part following differential equations
- ▷ A discrete part with deterministicaly guarded transitions
- ▷ Interactions with the environment

Cyber Physical System Analysis

State-space

- Continuous part difficult to analyse
- Discrete part state space can be large
- Interaction difficult to model

Cyber Physical System Analysis

State-space

- Continuous part difficult to analyse
- Discrete part state space can be large
- Interaction difficult to model

$\Rightarrow$ Testing

Testing is the only tractable validation technique
Require the generation of real-valued signal as input of the CPS.

Cyber Physical System Analysis

State-space

- Continuous part difficult to analyse
- Discrete part state space can be large
- Interaction difficult to model

⇒ Testing

Testing is the only tractable validation technique
Require the generation of real-valued signal as input of the CPS.

CPS testing problem

Input signal	$\longrightarrow \boxed{\text{CPS}} \longrightarrow$	Output signal
w	f	$f(w)$
$\forall w, w \models \phi$	$\Rightarrow$	$f(w) \models \psi$

Specifying input signals

Domain of signals

- ▷ In full generality: $\mathbb{R} \to \mathbb{R}^n$

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \to \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \to D$

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \to \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \to D$
  No finite representation

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \rightarrow \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \rightarrow D$
  No finite representation
- Piece-wise regular i.e. constant/linear/polynomial between discrete events

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \to \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \to D$
  No finite representation
- Piece-wise regular i.e. constant/linear/polynomial between discrete events
  How to define events

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \to \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \to D$
  No finite representation
- Piece-wise regular i.e. constant/linear/polynomial between discrete events
  How to define events
- A time automaton defines a language from which a signal is mapped over.

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \to \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \to D$
  No finite representation
- Piece-wise regular i.e. constant/linear/polynomial between discrete events
  How to define events
- A time automaton defines a language from which a signal is mapped over.

Using time automaton to model signal [Alur & Dill, 1994]

- Well suited for modelling time constraints between events.
- Compact representation.

Specifying input signals

Domain of signals

- In full generality: $\mathbb{R} \to \mathbb{R}^n$
- Bounding the signal to a compact domain $D \subset \mathbb{R}^n$: $[0; T] \to D$
  No finite representation
- Piece-wise regular i.e. constant/linear/polynomial between discrete events
  How to define events
- A time automaton defines a language from which a signal is mapped over.

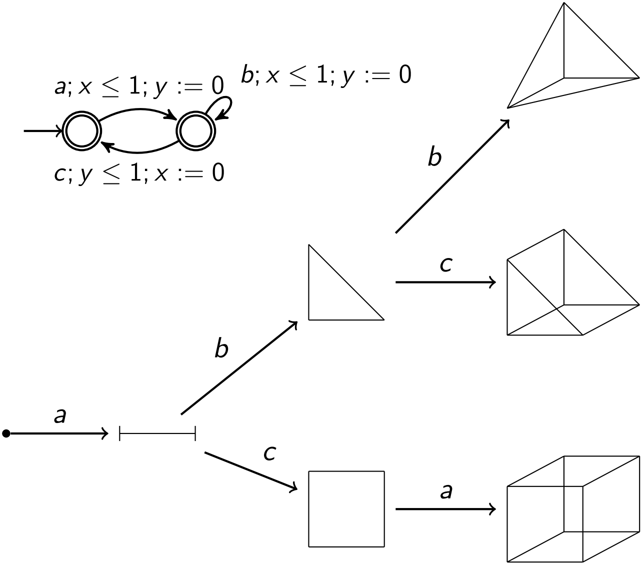
Using time automaton to model signal [Alur & Dill, 1994]

- Well suited for modelling time constraints between events.
- Compact representation.

$\Rightarrow$ require to sample time words from time automaton language.

Geometrical shape of time language

Constraints of timings along a path w = polytope P^L_w



$\texttt{Vol}(P^L_{abb}) = \frac{1}{6}$

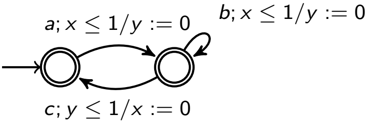
$\texttt{Vol}(P^L_{abc}) = \frac{1}{2}$

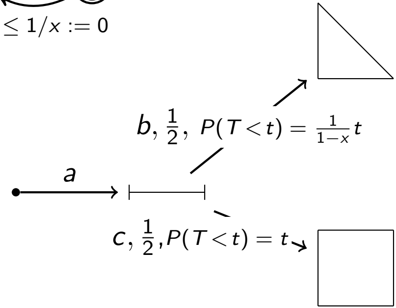
$\texttt{Vol}(P^L_{aca}) = 1$

Isotropic sampling (a "by-default" sampling)

At each step...

- ▷ assign same weight to every edge e and pick one randomly;
- ▷ assign same weight to every time t such that (t, e) can be taken.

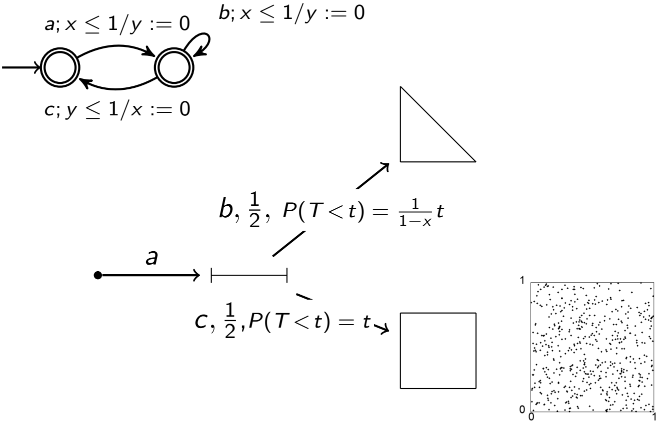




Isotropic sampling (a "by-default" sampling)

At each step...

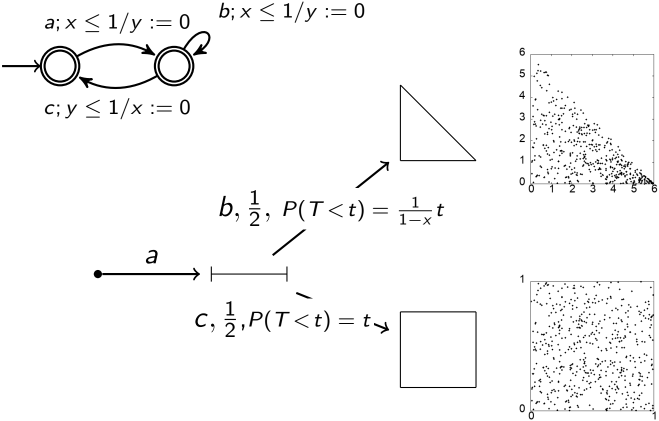
- ▷ assign same weight to every edge e and pick one randomly;
- ▷ assign same weight to every time t such that (t, e) can be taken.



Isotropic sampling (a "by-default" sampling)

At each step...

- ▷ assign same weight to every edge e and pick one randomly;
- ▷ assign same weight to every time t such that (t, e) can be taken.



Polytopes and CDF

Uniform distribution for a fixed word

Given a word α in the language of the automaton; and $\mathcal{P}$ the associated polytope. The uniform distribution over timed vector $\mathbf{t} \in \mathcal{P}$ assigns the density probability $\omega(\mathbf{t}) = \frac{1}{\mathsf{Vol}(\mathcal{P})}$.

Polytopes and CDF

Uniform distribution for a fixed word

Given a word α in the language of the automaton; and $\mathcal{P}$ the associated polytope. The uniform distribution over timed vector $\mathbf{t} \in \mathcal{P}$ assigns the density probability $\omega(\mathbf{t}) = \frac{1}{\mathsf{Vol}(\mathcal{P})}$.

Cumulative Density Function (CDF)

The CDF of the uniform distribution over α is $F : \mathcal{P} \to [0; 1]$ defines as $F(\mathbf{t}) = \int_{\mathbf{T}<\mathbf{t}} \omega(\mathbf{T}) d\mathbf{T}$. Moreover, the CDF F can be written as:

$$F(t_1, \ldots, t_n) = F_1(t_1) F_2(t_2 | t_1) \ldots F_n(t_n | t_1, \ldots, t_{n-1})$$

Polytopes and CDF

Uniform distribution for a fixed word

Given a word α in the language of the automaton; and $\mathcal{P}$ the associated polytope. The uniform distribution over timed vector $\mathbf{t} \in \mathcal{P}$ assigns the density probability $\omega(\mathbf{t}) = \frac{1}{\mathsf{Vol}(\mathcal{P})}$.

Cumulative Density Function (CDF)

The CDF of the uniform distribution over α is $F : \mathcal{P} \to [0;1]$ defines as $F(\mathbf{t}) = \int_{\mathbf{T}<\mathbf{t}} \omega(\mathbf{T}) d\mathbf{T}$. Moreover, the CDF F can be written as:

$$F(t_1, \ldots, t_n) = F_1(t_1) F_2(t_2|t_1) \ldots F_n(t_n|t_1, \ldots, t_{n-1})$$

In QEST16

Given a path in a TA; one can effectively compute the CDF of the uniform distribution in the form $F_i(t_i|t_1, \ldots, t_{i-1}) = \frac{\pi_i(t_1,\ldots,t_i)}{\gamma_i(t_1,\ldots,t_{i-1})}$ with π_i and γ_i polynomials of degree i.

QEST16 in a nutshell

Method

- Compute the forward reachable zone-graph of the automaton.
- Compute recusively the volume of language for each state of the zone-graph.
- The PDF $\omega(t)$ is the normallized volume.

Recursive definition over state of the zone-graph

$$\begin{aligned}
v_0(s) &= 1 \\
v_{n+1}(s) &= \sum_{\delta \in \Delta(s)} \int_{\mathrm{lb}_\delta(s)}^{\mathrm{ub}_\delta(s)} v_n(s_{(t,\delta)}) \mathrm{d}t.
\end{aligned}$$

QEST16 in a nutshell

Method

- Compute the forward reachable zone-graph of the automaton.
- Compute recusively the volume of language for each state of the zone-graph.
- The PDF $\omega(t)$ is the normallized volume.

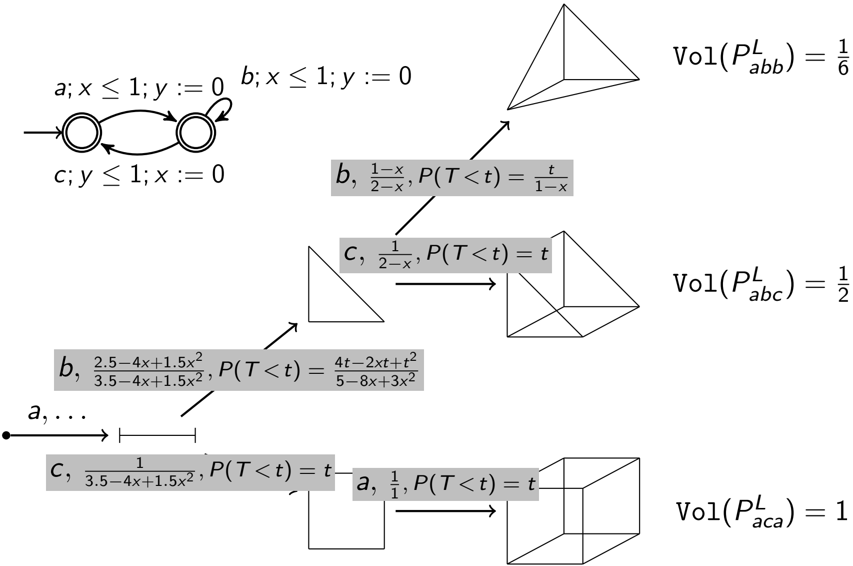
Recursive definition over state of the zone-graph

$$
\begin{aligned}
v_0(s) &= 1 \\
v_{n+1}(s) &= \sum_{\delta \in \Delta(s)} \int_{\mathrm{lb}_\delta(s)}^{\mathrm{ub}_\delta(s)} v_n(s_{(t,\delta)}) \mathrm{d}t.
\end{aligned}
$$

Shape of zone matter !

Zone-graph require additionnal splitting to ensure that the integral is simple.

Example



$a; x \leq 1; y := 0$
$b; x \leq 1; y := 0$
$c; y \leq 1; x := 0$
$b,\ \frac{1-x}{2-x}, P(T<t) = \frac{t}{1-x}$
$c,\ \frac{1}{2-x}, P(T<t) = t$
$b,\ \frac{2.5-4x+1.5x^2}{3.5-4x+1.5x^2}, P(T<t) = \frac{4t-2xt+t^2}{5-8x+3x^2}$
$a, \ldots$
$c,\ \frac{1}{3.5-4x+1.5x^2}, P(T<t) = t$
$a,\ \frac{1}{1}, P(T<t) = t$
$\mathtt{Vol}(P^L_{abb}) = \frac{1}{6}$
$\mathtt{Vol}(P^L_{abc}) = \frac{1}{2}$
$\mathtt{Vol}(P^L_{aca}) = 1$

Sampling polytopes

Unit cube

In practice sampling methods produce floating point number in $[0;1]$.
How to sample the uniform distribution ?

Sampling polytopes

Unit cube

In practice sampling methods produce floating point number in $[0;1]$.
How to sample the uniform distribution ?

Inverse Sampling

Recalls $F_i(t_i|t_1,\ldots,t_{i-1})$ is a polynomial in $t_i \to [0;1]$.

- Sample a real u in $[0;1]$
- Compute t_i as the root of $F_i(t_i|t_1,\ldots,t_{i-1}) - u$

Note that F_i is a strictly increasing polynomial $\Rightarrow$ Newton method applies.

Sampling polytopes

Unit cube

In practice sampling methods produce floating point number in $[0;1]$.
How to sample the uniform distribution ?

Inverse Sampling

Recalls $F_i(t_i|t_1,\ldots,t_{i-1})$ is a polynomial in $t_i \to [0;1]$.

- Sample a real u in $[0;1]$
- Compute t_i as the root of $F_i(t_i|t_1,\ldots,t_{i-1}) - u$

Note that F_i is a strictly increasing polynomial $\Rightarrow$ Newton method applies.

$F^{-1} : [0;1]^n \to \mathcal{P}$

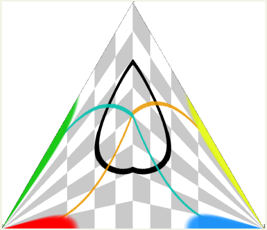
- ▷ Given $\mathbf{u}$ in $[0;1]^n$
- ▷ Apply inverse sampling iteratively to obtain $\mathbf{t} \in \mathcal{P}$

Sampling polytopes II

Example in dimension 2

$[0;1]^2$

$$\xrightarrow{F^{-1}}$$
$$\xleftarrow{F}$$



$$\left\{ (x,y) \middle| \begin{array}{l} 0 \leq x \\ 0 \leq y \\ y \leq 2x \\ y \leq 2-2x \end{array} \right\}$$

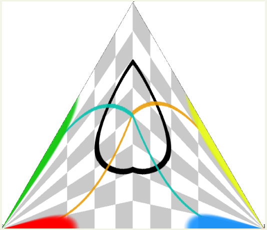
Sampling polytopes II

Example in dimension 2

$[0;1]^2$

$\xrightarrow{F^{-1}}$

$\xleftarrow{F}$

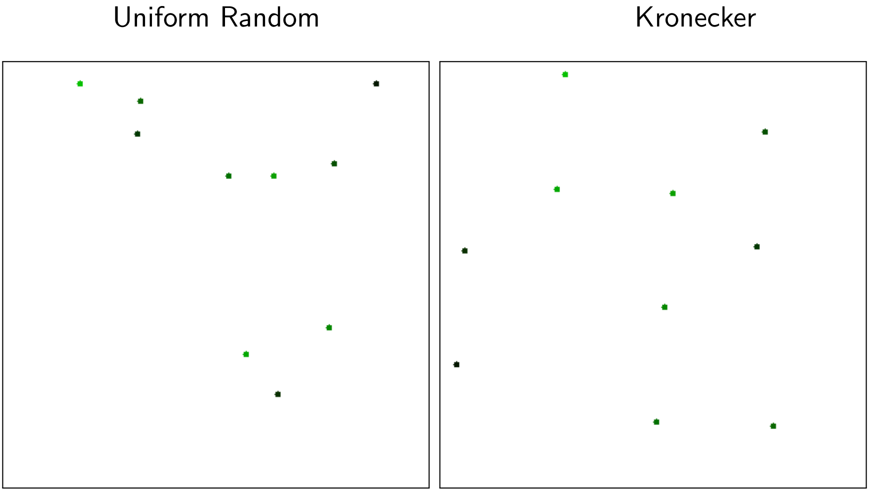


$$\left\{ (x,y) \middle| \begin{array}{l} 0 \leq x \\ 0 \leq y \\ y \leq 2x \\ y \leq 2-2x \end{array} \right\}$$

Sampling methods

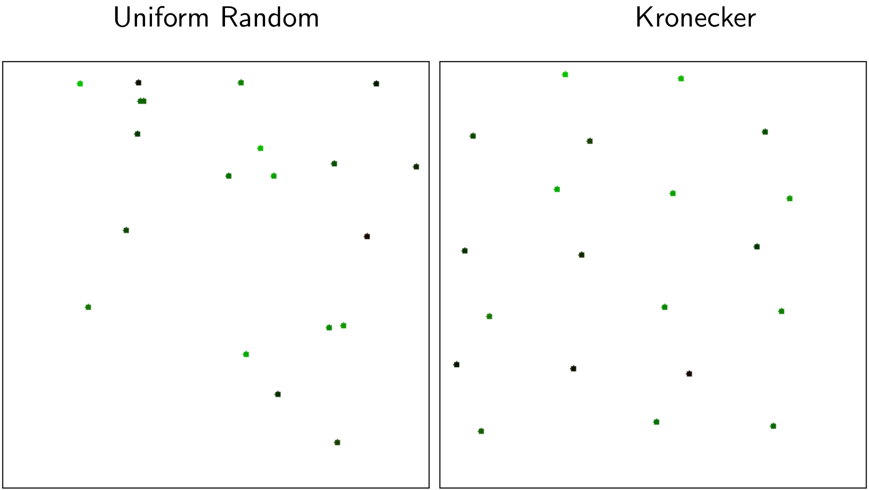
- ▷ Uniform (Pseudo) Random number
- ▷ Low discrepancy sequence

Random vs low discrepancy sequence (Empirical)



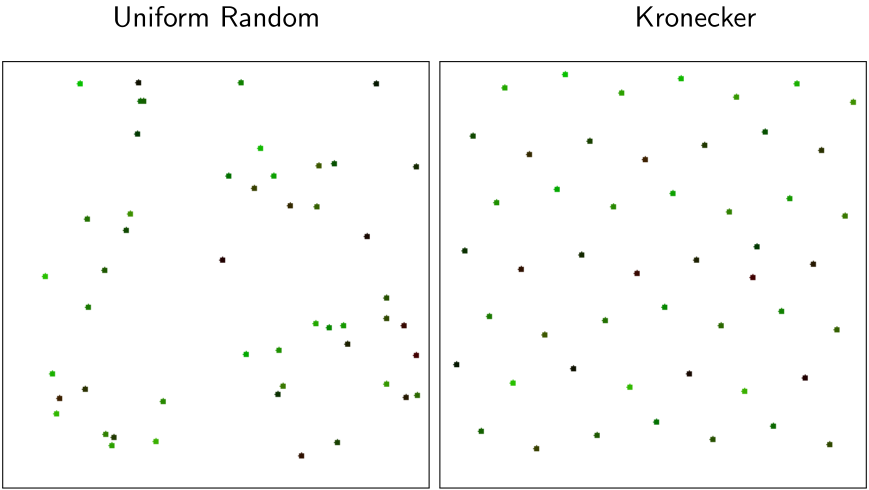
$n = 10$

Random vs low discrepancy sequence (Empirical)



$n = 20$

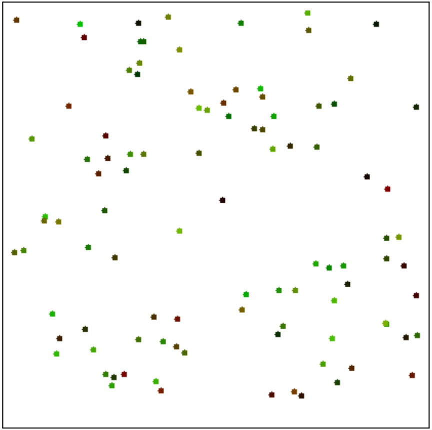
Random vs low discrepancy sequence (Empirical)



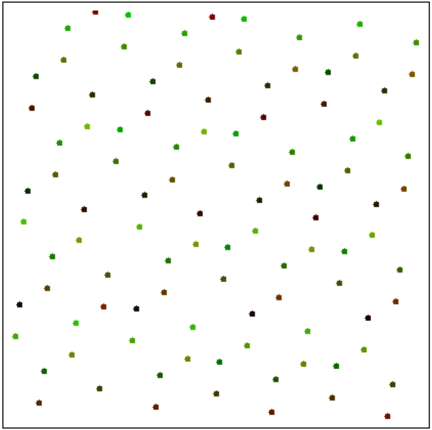
$n = 50$

Random vs low discrepancy sequence (Empirical)

Uniform Random

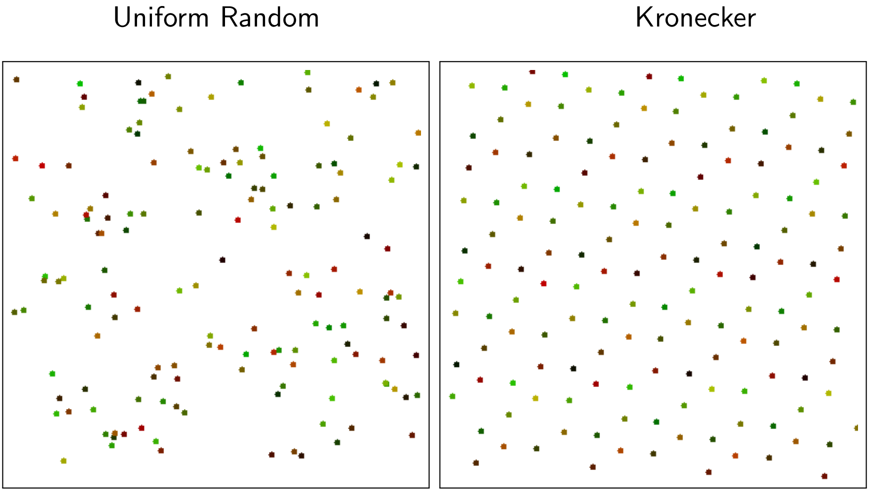


Kronecker



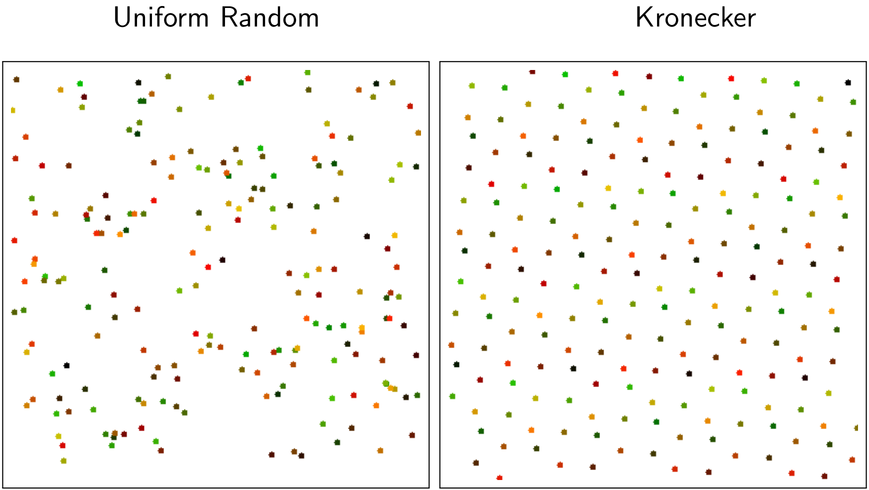
$n = 100$

Random vs low discrepancy sequence (Empirical)



$n = 150$

Random vs low discrepancy sequence (Empirical)



$n = 200$

Discrepancy

Star Discrepancy Definition

For $\mathbf{b} = (b_1, \ldots, b_n) \in [0,1]^n$, we define the box $[\mathbf{0}, \mathbf{b}] = [0, b_1] \times \cdots \times [0, b_n]$. The star discrepancy of a finite set S is defined as:

$$D_\star(S) = \sup_{\mathbf{b} \in [0,1]^n} \left| \mathtt{Vol}([\mathbf{0}, \mathbf{b}]) - \frac{|S \cap [\mathbf{0}, \mathbf{b}]|}{|S|} \right| .$$

Random vs low discrepancy sequence (theory)

For $g : [0,1]^n \to [a,b])$:

(Pseudo) Random sequence

Guarantee given as probabilistic framing i.e. confidence interval.
ex Chernoff-Hoeffding bounds: Let $z > 0$, let $1 - 2e^{-2z^2}$ be the confidence level:

$$\mathbb{P}\left(\left|\frac{1}{N}\sum_{n=1}^{N} g(\mathbf{p}^{(n)}) - \int_{[0,1]^n} g(\mathbf{r})d\mathbf{r}\right| < 2z\frac{b-a}{\sqrt{N}}\right) \geq 1 - 2e^{-2z^2}$$

Random vs low discrepancy sequence (theory)

For $g : [0,1]^n \to [a,b])$:

(Pseudo) Random sequence

Guarantee given as probabilistic framing i.e. confidence interval.
ex Chernoff-Hoeffding bounds: Let $z > 0$, let $1 - 2e^{-2z^2}$ be the confidence level:

$$\mathbb{P}\left(\left|\frac{1}{N}\sum_{n=1}^{N} g(\mathbf{p}^{(n)}) - \int_{[0,1]^n} g(\mathbf{r})d\mathbf{r}\right| < 2z\frac{b-a}{\sqrt{N}}\right) \geq 1 - 2e^{-2z^2}$$

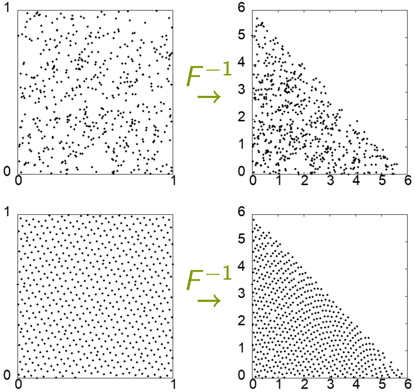
Low Discrepancy Sequence

Guarantee given as deterministic framing i.e. interval using Koksma-Hlawka inequality.

$$\left|\frac{1}{N}\sum_{n=1}^{N} g(\mathbf{p}^{(n)}) - \int_{[0,1]^n} g(\mathbf{r})d\mathbf{r}\right| \leq V^*(g)(D_*(S))^{1/n}$$

Application to the Evaluation of Uniformity Degree

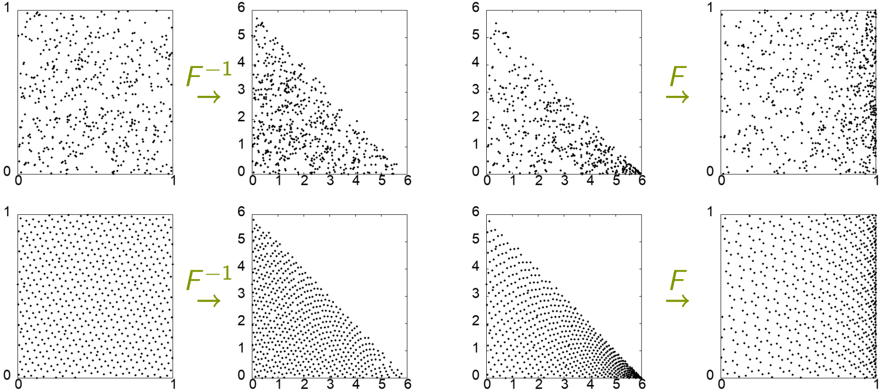
Sampling



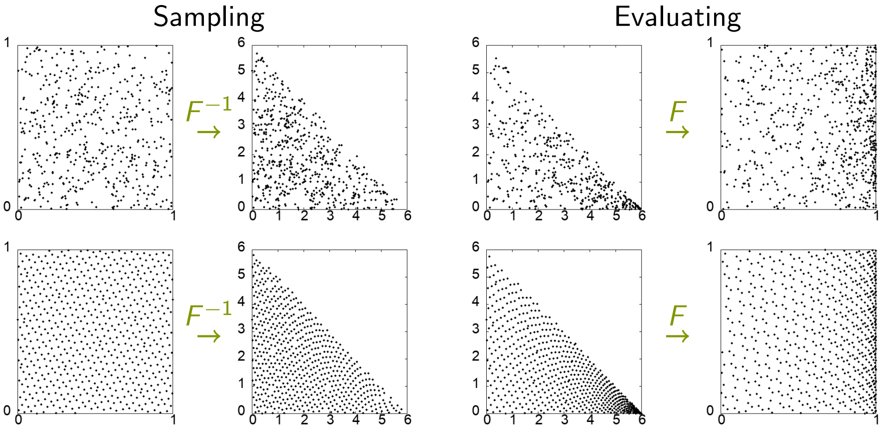
Application to the Evaluation of Uniformity Degree

Sampling

Evaluating



Application to the Evaluation of Uniformity Degree



Kolmogorov-Smirnov test

- ▷ Quantify the distance between two distributions.
- ▷ When apply between an empirical distribution S and the uniform one, equivalent to $D_\star(S)$.

Application To CPS Testing

CPS Testing Abstract

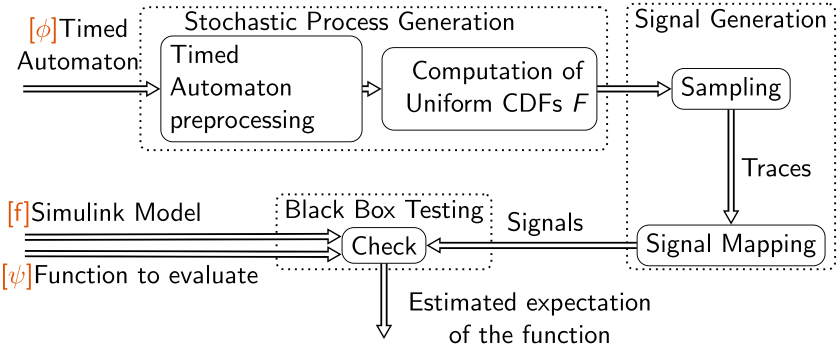
Input signal $\longrightarrow$ $\boxed{\text{CPS}}$ $\longrightarrow$ Output signal

w	f	$f(w)$
$w \models \phi$	$\Rightarrow$	$f(w) \models \psi$

Application To CPS Testing

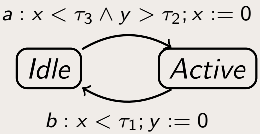
CPS Testing Abstract

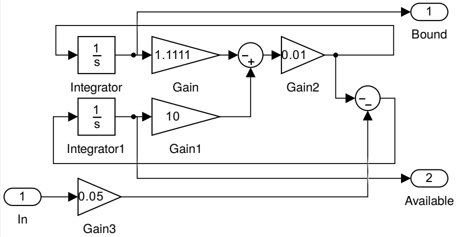
Input signal	$\longrightarrow$ CPS $\longrightarrow$	Output signal
w	f	$f(w)$
$w \models \phi$	$\Rightarrow$	$f(w) \models \psi$



Example: KiBaM System

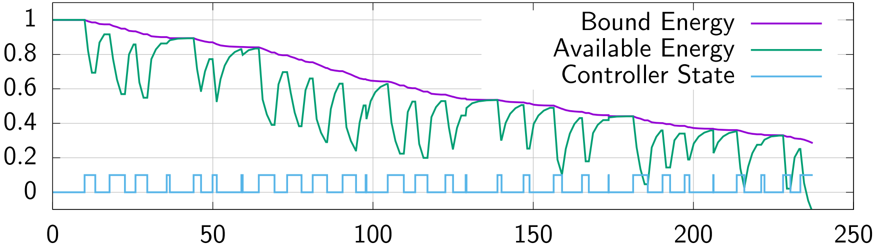
A CPS with a controller and a battery



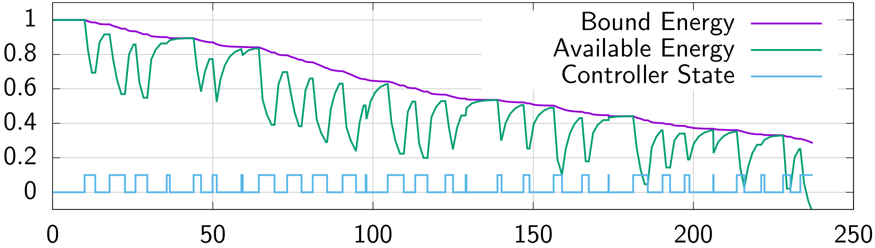


- The controller is switched on at least every τ_3 time unit.
- The controller consume energy when switch on.
- The battery self-recharge on low load.

Example: KiBaM System Results



Example: KiBaM System Results



$(\mathit{Available} > 0)\ \mathrm{U}^{\leq 150}\ \mathrm{T}$

CDF computation: 10s

Number of trajectories: 1,000,000

Uniform Random: Falsifies 53 trajectories, 1400s of simulations

Low discrepancy sequence: Falsifies 56 trajectories, 1600s of simulations

Stability of a $\Sigma\Delta$ Modulator

Characteristics

- Analog to digital converter;
- Mixing discrete-time and continuous-time components;
- Subject to saturation;

$\Rightarrow$ treated as a black box.

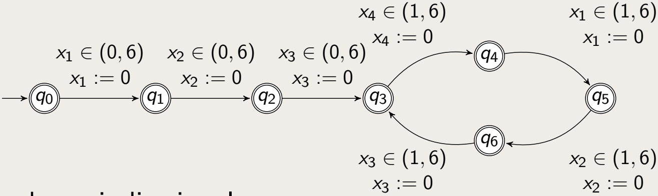
Stability of a $\Sigma\Delta$ Modulator

Characteristics

- Analog to digital converter;
- Mixing discrete-time and continuous-time components;
- Subject to saturation;

$\Rightarrow$ treated as a black box.

Input Signals



- A pseudo-periodic signal.
- Signals are linear interpolation based on location.
- CDF computation: 30s

Stability of a ΣΔ Modulator II

$(\neg \text{saturation}) \mathsf{U}^{\leq \textit{simtime}}\ \mathsf{T}$

- Several batches with a scaling parameter κ for frequencies
- 100 trajectories per batch, simulated in 1 minute
- Several test with scaling parameter for frequencies
  - $\kappa \geq 0.8 \times 10^{-7} \Rightarrow$ saturation detected with both methods
  - $\kappa = 0.6 \times 10^{-7} \Rightarrow$ saturation detected with low discrepancy sequence
  - $\kappa \leq 0.5 \times 10^{-7} \Rightarrow$ no saturation detected

Conclusion and Perspective

Conclusion

- Combining uniform word generation and low-discrepancy sampling;
- Validation of complex CPS system.

Conclusion and Perspective

Conclusion

- ▷ Combining uniform word generation and low-discrepancy sampling;
- ▷ Validation of complex CPS system.

Perspective

- Replacing automaton specification by a specification logic;
- Better sampling of the signal value space;
- An easy to use, self-contained implementation;
- Computing star discrepancy efficiently.