

Automated Verification and Control Synthesis of Complex Models

Alessandro Abate

Department of Computer Science, University of Oxford

www.oxcav.org

Simons Institute - April 2021

Formal verification: successes and frontiers



• industrial impact in checking correctness of

protocols, hardware circuits, and software

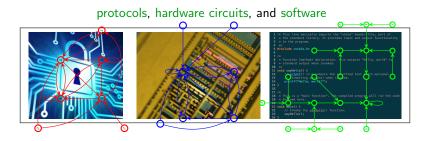


• model-based, automated, and sound guarantees (formal certificates)

Formal verification: successes and frontiers



• industrial impact in checking correctness of

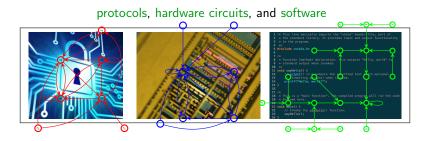


• model-based, automated, and sound guarantees (formal certificates)

Formal verification: successes and frontiers

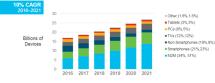


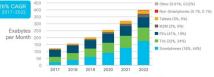
• industrial impact in checking correctness of



• model-based, automated, and sound guarantees (formal certificates)



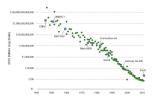




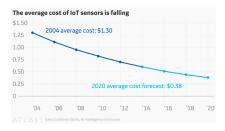
* Figures (n) refer to 2015, 2021 device share Source: Cisco VNI Global IP Traffic Forecast, 2016–2021

* Figures (n) refer to 2017, 2022 traffic share Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

[courtesy M. Zamani]



Nate: The Paid2 has computing power equal to 1500 villion individualities per second (MPR). Each data point represents the cost of 1500 MPR of computing power lased on the power and police of a specific computing device released that peor. Secure: Measure of the



• tech trends: advances in sensing, networking and embedded computation

Cost of Computing Power Equal to an iPad 2







- integration of learning from data within model-based verification & control ("learning for verification and control")
- certified reinforcement learning for policy synthesis ("certified learning")





- verification and control of complex models
 - dynamical models with uncertainty, noise
 - via formal abstractions



Building automation systems - a CPS exemplar







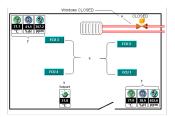
Building automation system setup in rooms 478/9 at Oxford CS

- advanced modelling for smart buildings
- applications: certifiable energy management
 - control of temperature, humidity, CO₂
 - Image: Market Market
 - I fault-tolerant certified control
 - demand-response over smart grids

Building automation systems - a CPS exemplar







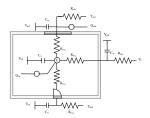
Building automation system setup in rooms 478/9 at Oxford CS

- advanced modelling for smart buildings
- applications: certifiable energy management
 - O control of temperature, humidity, CO₂
 - 2 model-based predictive maintenance of devices
 - I fault-tolerant certified control
 - demand-response over smart grids

Building automation systems - a CPS exemplar







Building automation system setup in rooms 478/9 at Oxford CS

- advanced modelling for smart buildings
- applications: certifiable energy management
 - control of temperature, humidity, CO₂
 - Image: Market Market
 - I fault-tolerant certified control
 - demand-response over smart grids

Building automation systems - a complex model

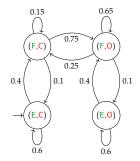


• model CO₂ dynamics, coupled with temperature evolution

$$\begin{aligned} x_{k+1} &= x_k + \frac{\Delta}{V} \left(-\mathbbm{1}_{ON} m x_k + \mu_{\{O,C\}} (C_{out} - x_k) \right) + \mathbbm{1}_F C_{occ} + \sigma_x w_k \\ y_{k+1} &= y_k + \frac{\Delta}{C} \left(\mathbbm{1}_{ON} m (T_{set} - y_k) + \mu_{\{O,C\}} \frac{1}{R} (T_{out} - y_k) \right) + \mathbbm{1}_F T_{occ,k} + \sigma_y w_k \end{aligned}$$

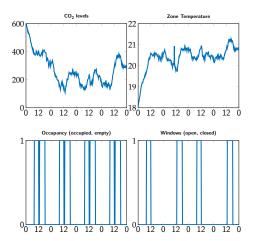
where
$$T_{occ,k} = \nu x_k + \zeta$$

- x zone CO₂ level
- y zone temperature
- *T_{set}* set temperature (air circulation)
- *T_{out}* outside temperature (window)
- T_{occ} generated heat (occupants)
- $\sigma_{(\cdot)}$ variance of noise $w_k \sim \mathcal{N}(0, 1)$



Building automation systems - a complex model



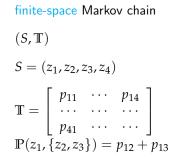


Parameter	Value
С	94.41 J/°C
T_{set}	20 °C
T _{out}	24 °C
ν	$2.4 \cdot 10^{-4}$
ζ	0.0107

• air circulation: ON

Complex models: from finite to uncountable

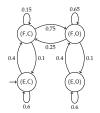


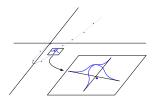


uncountable-space Markov process

$$\mathbb{S} = \mathbb{R}^2$$

$$\begin{split} \mathfrak{T}(dx|s) &= \frac{e^{-\frac{1}{2}(x-m(s))^T \Sigma^{-1}(s)(x-m(s))}}{\sqrt{2\pi}|\Sigma(s)|^{1/2}} dx\\ \mathbb{P}(s,A) &= \int_A \mathfrak{T}(dx|s), \quad A \subseteq \mathfrak{S} \end{split}$$





Probabilistic model checking of complex models



- general specifications expressed as PCTL formulae, e.g.
- simplest instance: probabilistic safety is the probability that the execution, started at s, stays in safe set A during the time horizon [0, N]

$$\mathcal{P}_s(A) = \mathbb{P}_s(s_k \in A, \forall k \in [0, N])$$

• select $p \in [0, 1]$; probabilistic safe set with safety level p is

$$S(\mathbf{p}) = \{s \in \mathcal{S} : \mathcal{P}_s(\mathbf{A}) \ge \mathbf{p}\}$$

• PCTL formula: $\mathbb{P}_{\leq 1-p}$ (true $\mathbb{U}^{\leq N} \neg A$)

Probabilistic model checking of complex models



- general specifications expressed as PCTL formulae, e.g.
- simplest instance: probabilistic safety is the probability that the execution, started at s, stays in safe set A during the time horizon [0, N]

$$\mathcal{P}_s(A) = \mathbb{P}_s(s_k \in A, \forall k \in [0, N])$$

• select $p \in [0, 1]$; probabilistic safe set with safety level p is

$$S(p) = \{s \in S : \mathcal{P}_s(A) \ge p\}$$

- PCTL formula: $\mathbb{P}_{\leq 1-p}$ (true $\mathbb{U}^{\leq N} \neg A$)
- $\mathcal{P}_s(A)$ can be fully characterised (and optimised)
- issues with computation of $\mathcal{P}_s(A)$ and of S(p)



complex specification

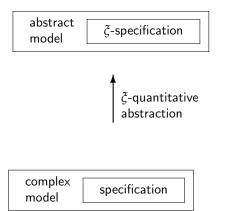
Alessandro Abate, CS, Oxford



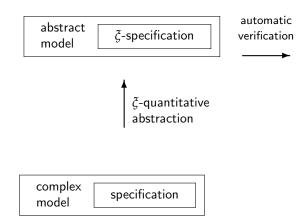
 ξ -quantitative abstraction

complex specification

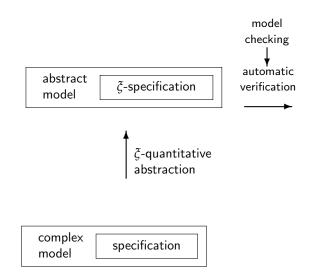




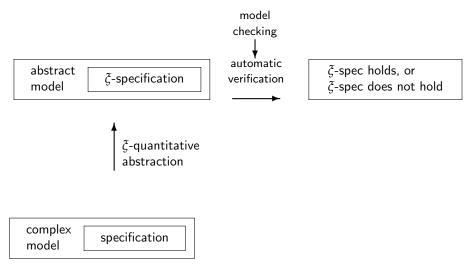




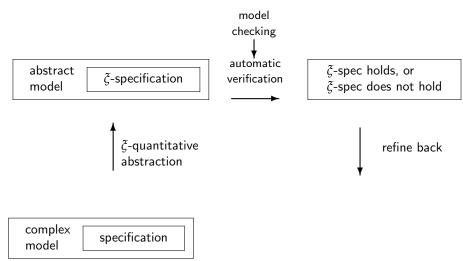




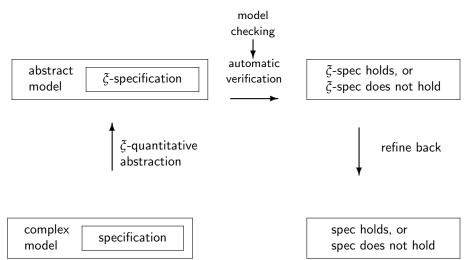




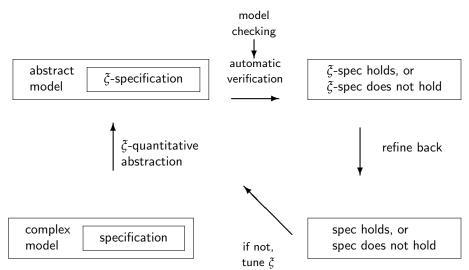














- \bullet approximate stochastic process (\mathbb{S},\mathbb{T}) as MC $(S,\mathbb{T}),$ where
 - $S = \{z_1, z_2, \dots, z_p\}$ finite set of abstract states
 - $\mathbb{T}: \mathbb{S} \times \mathbb{S} \rightarrow [0,1]$ transition probability matrix

• approximate stochastic process $(\mathcal{S}, \mathcal{T})$ as MC (S, \mathbb{T}) , where

•
$$S = \{z_1, z_2, \dots, z_p\}$$
 – finite set of abstract states

• $\mathbb{T}: \mathbb{S} \times \mathbb{S} \rightarrow [0,1]$ – transition probability matrix

• algorithm:

```
input: stochastic process (S, T)
```

output: MC (S, \mathbb{T})





• approximate stochastic process $(\mathcal{S}, \mathcal{T})$ as MC (S, \mathbb{T}) , where

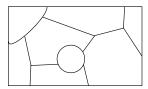
•
$$S = \{z_1, z_2, \dots, z_p\}$$
 – finite set of abstract states

- $\mathbb{T}: \mathbb{S} \times \mathbb{S} \rightarrow [0,1]$ transition probability matrix
- algorithm:

input: stochastic process $(\mathcal{S}, \mathcal{T})$

1 select finite partition
$$\mathcal{S} = \cup_{i=1}^p S_i$$

output: MC (S, \mathbb{T})





• approximate stochastic process $(\mathcal{S}, \mathcal{T})$ as MC (S, \mathbb{T}) , where

•
$$S = \{z_1, z_2, \dots, z_p\}$$
 – finite set of abstract states

• $\mathbb{T}: \mathbb{S} \times \mathbb{S} \rightarrow [0,1]$ – transition probability matrix

• algorithm:

input: stochastic process $(\mathcal{S}, \mathcal{T})$

- 1 select finite partition $\mathcal{S} = \cup_{i=1}^p S_i$
- 2 select representative points $z_i \in S_i$
- 3 define finite state space $S := \{z_i, i = 1, ..., p\}$

output: MC (S, \mathbb{T})





• approximate stochastic process $(\mathcal{S}, \mathcal{T})$ as MC (S, \mathbb{T}) , where

•
$$S = \{z_1, z_2, \dots, z_p\}$$
 – finite set of abstract states

• $\mathbb{T}: \mathbb{S} \times \mathbb{S} \rightarrow [0,1]$ – transition probability matrix

• algorithm:

input: stochastic process $(\mathfrak{S}, \mathfrak{T})$

- 1 select finite partition $\mathbb{S} = \cup_{i=1}^p S_i$
- 2 select representative points $z_i \in S_i$
- 3 define finite state space $S := \{z_i, i = 1, ..., p\}$

4 compute transition probability matrix: $\mathbb{T}(z_i, z_j) = \mathbb{T}(S_j \mid z_i)$ output: MC (S, \mathbb{T})





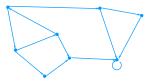
- approximate stochastic process $(\mathcal{S}, \mathcal{T})$ as MC $(\mathcal{S}, \mathbb{T})$, where
 - $S = \{z_1, z_2, \dots, z_p\}$ finite set of abstract states
 - $\mathbb{T}: \mathbb{S} \times \mathbb{S} \rightarrow [0,1]$ transition probability matrix

• algorithm:

input: stochastic process $(\mathfrak{S},\mathfrak{T})$

- 1 select finite partition $\mathbb{S} = \cup_{i=1}^p S_i$
- 2 select representative points $z_i \in S_i$
- 3 define finite state space $S := \{z_i, i = 1, ..., p\}$

4 compute transition probability matrix: $\mathbb{T}(z_i, z_j) = \mathbb{T}(S_j \mid z_i)$ output: MC (S, \mathbb{T})





Model checking probabilistic safety via formal abstractions



• safety set $A \subset S$, time horizon N, safety level p

Model checking probabilistic safety via formal abstractions



- safety set $A \subset S$, time horizon N, safety level p
- δ -abstract $(\mathcal{S}, \mathfrak{T})$ as MC $(\mathcal{S}, \mathbb{T})$, so that $A \to A_{\delta}$, quantify error $\xi(\delta, \mathbb{N})$
- \Rightarrow probabilistic safe set

$$S(p) = \{s \in \mathcal{S} : \mathcal{P}_s(A) \ge p\}$$

= $\{s \in \mathcal{S} : (1 - \mathcal{P}_s(A)) \le 1 - p\}$

Model checking probabilistic safety via formal abstractions



- safety set $A \subset S$, time horizon N, safety level p
- δ -abstract $(\mathcal{S}, \mathfrak{T})$ as MC $(\mathcal{S}, \mathbb{T})$, so that $A \to A_{\delta}$, quantify error $\xi(\delta, \mathbb{N})$
- \Rightarrow probabilistic safe set

$$S(p) = \{s \in \mathcal{S} : \mathcal{P}_s(A) \ge p\}$$

= $\{s \in \mathcal{S} : (1 - \mathcal{P}_s(A)) \le 1 - p\}$

can be computed via

$$\begin{split} Z_{\delta}(p + \xi) &\doteq \mathsf{Sat}\left(\mathbb{P}_{\leq 1-p-\xi}\left(\mathsf{true}\ \mathsf{U}^{\leq N} \neg A_{\delta}\right)\right) \\ &= \left\{z \in S : z \models \mathbb{P}_{\leq 1-p-\xi}\left(\mathsf{true}\ \mathsf{U}^{\leq N} \neg A_{\delta}\right)\right\} \end{split}$$

Formal abstractions: error $\boldsymbol{\xi}$



• consider $\Im(d\bar{s}|s) = \mathfrak{t}(\bar{s}|s)d\bar{s}$; assume \mathfrak{t} is Lipschitz continuous, namely

$$\exists 0 \leq h_{s} < \infty : \quad \left| \mathfrak{t}(\bar{s}|s) - \mathfrak{t}(\bar{s}|s') \right| \leq h_{s} \left\| s - s' \right\|, \quad \forall s, s', \bar{s} \in \mathbb{S}$$

Formal abstractions: error $\boldsymbol{\xi}$



• consider $\Upsilon(d\bar{s}|s) = \mathfrak{t}(\bar{s}|s)d\bar{s}$; assume \mathfrak{t} is Lipschitz continuous, namely

$$\exists 0 \leq \underline{h}_{s} < \infty : \quad \left| \mathfrak{t}(\bar{s}|s) - \mathfrak{t}(\bar{s}|s') \right| \leq \underline{h}_{s} \left\| s - s' \right\|, \quad \forall s, s', \bar{s} \in \mathbb{S}$$

- one-step error (related to approximate probabilistic bisimulation) $\epsilon = \frac{h_s}{\delta} \mathscr{L}(A)$
 - δ max diameter of partition sets
 - $\mathscr{L}(A)$ volume of set of interest
- N-step error (tuneable via δ) $\xi(\delta, N) = \epsilon N$

Formal abstractions: error $\boldsymbol{\xi}$



• consider $\Upsilon(d\bar{s}|s) = \mathfrak{t}(\bar{s}|s)d\bar{s}$; assume \mathfrak{t} is Lipschitz continuous, namely

$$\exists 0 \leq h_{s} < \infty : \quad \left| \mathfrak{t}(\bar{s}|s) - \mathfrak{t}(\bar{s}|s') \right| \leq h_{s} \left\| s - s' \right\|, \quad \forall s, s', \bar{s} \in \mathbb{S}$$

- one-step error (related to approximate probabilistic bisimulation) $\epsilon = \frac{h_s}{\delta} \mathscr{L}(A)$ • δ – max diameter of partition sets
 - $\mathscr{L}(A)$ volume of set of interest
- N-step error (tuneable via δ) $\xi(\delta, N) = \epsilon N$

 \rightarrow improved and generalised error



Cridding procedure	Bounds of the hermal		
Uniform Gridden	aughtr a	The results a maximum error I	14
	Loschitz (incl. formel MC error)	4.077e-82	
Adaptive Oredang: occe-spoker	10-100 ·	COLUMN 2	•2 • • • • • • • • • • • • • • • • • •
		Laberted Tarta	N NA2227
Kame Databution	The same of the tarried function	Take Set	42 4
User Defined	KemePunctor/Diampie m		
Hormal Oab Burlion			45
	Search for the file	Add Remove Edt	05 020 0204
Problem selection		1	
	Tarb set Target set		Pot the grid Color the grid
Presidente Tarley a	10583-8608-0	Expert to PDEM	
Personal Annual Annua	Salari Solari		
	Select Select		
			Initial condition The probability give
Desired abstraction error Sumber of ter	and and the local states of the		
	R 9925 H	Seve Ter counts	
			Extend Calculate
			1
Distance processory	Burds of National		
Uniform Greeken	Loochtz -	Se multip raision over (1
Adultive Grocing	Lauchtz + Lauchtz (nd. formi WC error)	The reading reasons over (
Uniform Greeken	Loochtz -		1
Adultive Grocing	Lauchtz (nd. formi WC error)	8.996+00	1
Adaptive Creating Booswatcas	Londer (not form (it's artsr) +	8.996e-02	
Uniform Greating Adaptive Greating Book-House Adaptive Greating Book-House Remel Detribution	Likechtz (no. form MC artar) *	8.999e-00 Labeled Sels	1 8.8 8.9
Union Groop Rosevecul Adaptive Groop Rosevecul Adaptive Groop Rosevecul Kame/Datibutos User Defined	Londer (not form (it's artsr) +	8.996e-02	
Uniform Greating Adaptive Greating Book-House Adaptive Greating Book-House Remel Detribution	Render on town of even at a second of the se	8.996e-00 Lebeled Sels Serler Sel * Target Sel *	1 8.8 8.9
Union Groop Rosevecul Adaptive Groop Rosevecul Adaptive Groop Rosevecul Kame/Datibutos User Defined	Likechtz (no. form MC artar) *	8.999e-00 Labeled Sels	
Index Conseq Adaptive Oracing Excel-yibidi Adaptive Oracing Excel-yibidi , Kame Dathbulon Marma Dathbulon ,	Lange21 * Lange21 (m) filmed 500 article Min-Max *	8.996e-00 Lebeled Sels Serler Sel * Target Sel *	
Institute Geology Book-Hoart Abspilve Groups Book-Hoart Abspilve Groups Book-Hoart Abspilve Groups Book-Hoart Assessible Research Assessible As	Ander (no development)	8.996e-00 Lebeled Sels Serler Sel * Target Sel *	
Valence George Massen of Society Book-receive Assessed Society Book-replane FrameDatabasis NameDatabasis Amerikana Society Amerikana Society Amerikana Amerikana Society Amerikana Society Amerikana Amerikana Society Amerikana Society Amerikana Amerikana Society Amerikana Society Ame	Lange21 * Lange21 (m) filmed 500 article Min-Max *	89994-00 Label (Prin Safe Set Appl Set Appl Set	
Index Codep)	Annual control of service * Annual Control of Service * Service Control One Service *	8.996e-00 Lebeled Sels Serler Sel * Target Sel *	
Valence George Massen of Society Book-receive Assessed Society Book-replane FrameDatabasis NameDatabasis Amerikana Society Amerikana Society Amerikana Amerikana Society Amerikana Society Amerikana Amerikana Society Amerikana Society Amerikana Amerikana Society Amerikana Society Ame	Ander in the second secon	89994-00 Label (Prin Safe Set Appl Set Appl Set	
Index Codep)	Annual control of service * Annual Control of Service * Service Control One Service *	89994-00 Label (Prin Safe Set Appl Set Appl Set	
Johon Coope Anapies Coope Anapies Coope Anapies Coope Anapies Coope Anapies Coope Anapies Anap	And the formation of a second	89994-00 Label (Prin Safe Set Appl Set Appl Set	
Index Codep)	And the formation of a second	89994-00 Label (Prin Safe Set Appl Set Appl Set	

http://sourceforge.net/projects/faust2



Crieding procedure			
Uniform Gridden	Daurbitt .	The resulting maximum error E	11 500
	Lipschitz (nd. formal MC error)	4.077e-82	
Adaptive Oredang: eccei+poten .	m-max	COLORGE COLORGE	•2 *
		Laberted Tarts	N N N N N N N N N N N N N N N N N N N
Kamel Oabibution	The same of the twitel function	Calified Deta	42 4
User Defined	Kenself-preferef sample m	Cale Cal a	
Home Oah buton	Search for the Ste		
	AND A DO IN THE	Add Parmive Edit	
Problem selection	Tarte set Target set		Pot the grid Color the grid
Presby Acres 4	10582-8808-0	Expert to PECAL	
Pormale Free	Select Select		
			initial condition The probability pi
Desired ababaction error Sumber of In			
	No De propert	Seve To courts	Trind Catulate
0.05 2			
0.05			
0.05 2	Burds, of the Serve		,
Debleg procedure Instrum Garanne	Losoftz -	De mysleg mainer over f	
Dridbig procedure Uniter Groceg Magne & Dridbig Dar-Scart	Applied (incl. formal MC error)	De reading mainur our E	
Debleg procedure Instrum Garanne	Losoftz -		1
Diddeg procedure Didden Groups processor Alagine Drafting Socie-palar	Lander *	8.996+00	1
Discolog procedure Instant Gooding Society and Society and Society Society Society Society (Society Society So	Applied (incl. formal MC error)		1
Disbog prosiders proton footby Anapter Dool too - sold Anapter Dool too - sold Three Datase The Tabase	Lander *	8.996e-02	1
Discolog procedure Instant Gooding Society and Society and Society Society Society Society (Society Society So	Annotation formers and service and Annotation The same of the tarmet function KernelFunction/Cample m	8.996e-00 Lebeled Sele Sele Sel Target Sel v	1
Disbog prosiders proton footby Anapter Dool too - sold Anapter Dool too - sold Three Datase The Tabase	Bachter * * * * * * * * * * * * * * * * * * *	8.996e-00 Lessent Sets	
Dribble postelane United Georgenetisten Andere Georgenetisten Andere Georgenetisten Dier Erbert Neise Georgenetisten Dier Erbert Neise Georgenetisten Dier Erbert	The name affine served functions Resolution Resoluti	8.996e-00 Lebeled Sele Sele Sel Target Sel v	
Ording products Instructional sectors Name of Control Sectors Name o	Benefit	89994-00 Lobeled Enh Safe Set 4 Add Rancer Edit	
Overg posebre Uniter Overg Apple Overg App	Sector * Mathematic sector * The sector of the sector *	8.996e-00 Lebeled Sele Sele Sel Target Sel v	
Dobro procedure Unitern Control	Benefit	89994-00 Lobeled Enh Safe Set 4 Add Rancer Edit	
Overg posebre Uniter Overg Apple Overg App	Sector * Mathematic sector * The sector of the sector *	89994-00 Lobeled Enh Safe Set 4 Add Rancer Edit	
Overg posebre Uniter Overg Apple Overg App	And the formation of th	89994-00 Lobeled Enh Safe Set 4 Add Rancer Edit	1 8 8 8 8 8 8 8 8 8 8 8 8 8

http://sourceforge.net/projects/faust2





Cristing procedure			
Uniform Gridden	author a	The resulting maximum error 8	14
Adaptive Gridding: bcal-vecal	Lpechitz (incl. formal MC error)	4.0774-02	
Adaptive threaking: bicar-spoker	17-150 ·		
		Labeled Deta	
Kernel Clebibution	The same of the same function	Safe Sel A	
New Selfred .	KemellundenDxample.m		
	Search for the file	Add Semine Edd	
		AN HARDY ER	05 020 02-04
Problem selection	Tarb ed. Target ed.	1	Pot the grid
Probability Tarbola	14532-4698-0	Faced in PERM	
Person-Juneid Pormula Pres		000000000	
romus ree	Select Select		initial condition The probability pl
			the processing pr
Desired abebaction error Sumber of 5	me alapa N		
2.03	Run The program	Dave the results	Extend California
Drobins procedury	Buck stations		
Drebby procedure		Do malto maine ere f	
Adultive Grocky	Landrid and forms MC errors	De reading senimus nor E	
Juniform Griedero	100032	The resulting maximum more it 15550-02	1
Adultive Grocky	Landrid and forms MC errors	8.996e-02	1
Adultive Grocky	Landrid and forms MC errors	8.996e-02 Labeled Dels	1 8.8 8.4
Inform Gradeg Respire Decorg Scar-Scar Adapter Gradeg Scar-Splan Remeil/Detroion	Equilibrium (and format line strate) (and format line strate of the tested function	8.999e-00 Labored Dets	
Adaptive Grotting Book-Hoad Adaptive Grotting Book-Hoad Adaptive Grotting Book-spolar Kame/Datribution	Execute a finance set array Rev Maas The scales of the tament function ServerFunctionComplete	8.996e-02 Labeled Dels	
Inform Gradeg Respire Decorg Scar-Scar Adapter Gradeg Scar-Splan Remeil/Detroion	Equilibrium (and format line strate) (and format line strate of the tested function	8.999e-00 Labored Dets	
Unitere George Door-ecut Asspire George Door-ecut Asspire George Door-pose Kamel Dartbulon Uper Defect Norme Dartbulon 	Leading and former Mill arrays and a first strategy of the Mark	8.999e-00 Latered Set Serie Set Target Set	
Instein Gooden Soor-House Assets Gooden Soor-House Assets Gooden Soor-House , Name Databuton Der Definet Anne Detabuton , Protein Selecton	Execute a finance set array Rev Maas The scales of the tament function ServerFunctionComplete	8.999e-00 Latered Set Serie Set Target Set	
Instrum Concept, Analysis Conceptual and Analysis Conceptual Analysis Conceptu	Leading and former Mill arrays and a first strategy of the Mark	8.999e-00 Latered Set Serie Set Target Set	
Internet Geology Beak-Head Asspire Groups and Asspire Groups Beak-Head Asspire Groups Beak-Head Asspire Groups Beak Beak Beak Beak Beak Beak Beak Beak	Annual Processor * Annual	1999-00 Latent Teh Topp Set v Alt Rance Edit	
Instant Groups poor-sourd Anapter Oroding Sour-spour Anapter Oroding Sour-spour Remail/Sourbuildin Terror Source Anapter Source Protein Sourc	Anno Constant Co	1999-00 Latent Teh Topp Set v Alt Rance Edit	
Instant George Bool-Hoad Anapier Group Bool-Hoad Anapier Group Bool-Hoad Anapier Group Bool Ammeliate Sustant Protein Selection Protein Selection Protein Selection Protein Selection Protein Selection	And the second s	1999-00 Latent Teh Topp Set v Alt Rance Edit	
Instant Groups poor-sourd Anapter Oroding Sour-spour Anapter Oroding Sour-spour Remail/Sourbuildin Terror Source Anapter Source Protein Sourc	And the second s	1999-00 Latent Teh Topp Set v Alt Rance Edit	

http://sourceforge.net/projects/faust2





Crieding procedure			
Uniform Gridden	Darbit .	The resulting maximum error 8	11 500
	Lipechitz (nol. formal MC error)	4.6774-02	
Adaptive threakly occer-yooker	mottar		02 V
		Laberted Tota	
Kamel Diabibution	The same of the tasket function	Eater East	
Nerr De Ined .	Kernelf-unclos/Example.m		
Torne Genevics	Description for the file		
		Add Remove Edit	05 020 0244
Problem selection	Tarb set Target set	1	Pot the grid Color the grid
Transford Tarrie	14583-1408-0	Faced in PDEAL	
Peach-Looid		Expert to Proces	
Pormula Free .	Select		
			Initial condition The probability pl
Desired abehaction error Sumber of In	ne stops N		
8.05 2	Run The program	Save the results	Extent Cathyler
Dinibility procedure	Burds of Particular		1 1 1 1 1 1 1 1 1 1 1 1 1 1
Onderg procedure Uniform Greece [2]	LoodAt -	De maleg mainer ever (1
Dinibility procedure		The reading mations in use (
Drobby procedure (anthree Grobby back-store)	Loocks	8.996e-00	
Oridoly procedure Sector Googy processor Adaptive Oridoly Socie-plate	Londer / Londer (not found the array) / we have		1
Otoreg procedure Unders processor Massime control post-post Assessed post-post Assessed post-post	Bachtz (no. from KC artic) (Bobba)	8.999e-00 Lettered Dets	
Oridoly procedure Sector Googy processor Adaptive Oridoly Socie-plate	Institution main	8.996e-00 Labeled Sets	
Drebolg blockluw Santon Cooping Analyse Stock and Analyse Stock and a Analyse Stock and Analyse Stock and a Analyse Stock and Analysis and Analysis and Analysis Kame Data Stock and Analysis and Analysis and Analysis Analysis and Analysis and Analysis and Analysis and Analysis Analysis and Analysis and Analysis and Analysis and Analysis Analysis and Analysis and Analysis Analysis and Analysis	Bachtz (no. from KC artic) (Bobba)	8.996+00 Labeled Sels	
Drebolg blockluw Santon Cooping Analyse Stock and Analyse Stock and a Analyse Stock and Analyse Stock and a Analyse Stock and Analysis and Analysis and Analysis Kame Data Stock and Analysis and Analysis and Analysis Analysis and Analysis and Analysis and Analysis and Analysis Analysis and Analysis and Analysis and Analysis and Analysis Analysis and Analysis and Analysis Analysis and Analysis	Institution main	8.996e-00 Letered Sets Safe Set Taget Set v	
Drebolg blockluw Santon Cooping Analyse Stock and Analyse Stock and a Analyse Stock and Analyse Stock and a Analyse Stock and Analysis and Analysis and Analysis Kame Data Stock and Analysis and Analysis and Analysis Analysis and Analysis and Analysis and Analysis and Analysis Analysis and Analysis and Analysis and Analysis and Analysis Analysis and Analysis and Analysis Analysis and Analysis	Institution main	8.996e-00 Letered Sets Safe Set Taget Set v	
Deble protekve Untern George Angelen Debleg kan - yddar (* Samel Debleg kan - yddar (*	Learning the former set array and a former set array set are a former set are a form	8999-00 Local Fach Taget Set v Add Rance Edd	
Diebo pissalare Johnson George Sanakasa Jackes Gibba Salari Sanas Giba Bullon Jackes Giba Salari Patien selectore Patien selectore Patien selectore 1 1	Sector and Sector (Sector (Sect	8.996e-00 Letered Sets Safe Set Taget Set v	
Deble protekve Untern George Angelen Debleg kan - yddar (* Samel Debleg kan - yddar (*	Anote	8999-00 Local Fach Taget Set v Add Rance Edd	
Orders procedure Interno George Analysis of George Laboration Analysis of George Laboration Proceedings and Control Proceedings and Control Proceedings Proceedings of Control Proceedings of Control Proc	Kanada Kana Kanada Kanada Kana	8999-00 Local Fach Taget Set v Add Rance Edd	
Diebo pissalare Johnson George Sanakasa Jackes Gibba Salari Sanas Giba Salari Sanas Giba Salari Partier selectore Problem	Kanada Kana Kanada Kanada Kana	8999-00 Local Fach Taget Set v Add Rance Edd	

http://sourceforge.net/projects/faust2





And Arrison Control of Contr	The reading sequence and the second sequences and the second seco	
Anales design surgeries in the set of the se	Lakent Das Patr for Ant Denne Cor Dept to MCD	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
And Andrewson The state of the sense statement Sense of the sense statement	Lakent Das Patr for Ant Denne Cor Dept to MCD	es o 2 4 o 2 4 es o 2 4 o 2 4 Methode
And Steel Control Control Con	Safe Set	
And Steel Control Control Con	Add Shamve Edit	A Contra yet
New Section Image: Section Sec	Add formore Edit	0.5 0.2 0.2 0.2 0.5 0.2 0.2 0.2 Not respit Contra pt Inde coden The probability Inde coden The probability
Legendre State Legendre	Expert to PECAL	Biller
Analysis Series Analysis Series Formal Press Series debtector error: Survey of time stops I	Expert to PECAL	Pethe prid Cole the prid Initial concilien The probability Initial concilien Cole
Analysis Series Analysis Series Formal Press Series debtector error: Survey of time stops I		Initial candidan The probability probabili
Preside Annual Free		Deel Column
Preside Annual Free		Deel Column
Desired abstraction error . Number of time stops II	Save The counts	Deel Column
226 2 Ku ta popul	Save Der reachts	Deel Column
226 2 Ku ta popul	law bi reals	
38 2	Tare To could	
		1
Ondorg procedure Bounds at the tiernet		,
Leading - Leading -	The resulting maximum error 2	
Adaptive Greating: Bode-VBCall Lov-CH22 (incl. formal MC arror)	8,999+02	0.8
Adaptive Oridolog local - jobal		
	Laboried Sala	16
KamelOld/Bution The same of the Leviel function	Selv Set	
HerrefunderDanple.m	Target Set	8.4
Normal Data button		
· Departer for the file	Add Ranova Edit	
Particular and a second s		
		cau he go
	Export to PRISA	
Formula Free - Select Select		
		Initial condition The probability of
		Mail condition The proceeding g
Protein minutes Target set	Add Renove Edit	82 0.6 -0.4 -0.2 0 0.2 Patter pro Color the pro

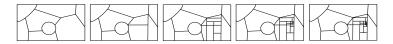
http://sourceforge.net/projects/faust2





Cridding procedure	Bounds of the hernel		
Uniform Gridding -	Leechtz -	The resulting maximum error E	14
Adaptive Gridding: bcall-vecal	Lipechitz (ncl. formal MC error)	4.0776-02	02-0
Adaptive Drading: Dicer-goose	10-014 W		
Kamel Datribution	The name of the Series Surgion	Labeled Sets	
Ine letted		Safe Sat 4	
Norma Date byten	KernelFunctionExample.m		
	Search for the file	Add Remove Edit	
			05 020 0244
Problem selection	Tarte set Target set		Pot the grid Color the grid
Protocology Tarray	4513-4608-0	Expert to PECAL	
Person Louis Pormula Pres	Start Scart		
	Select Select		initial condition The probability (
Desired shaharden erner . Number of ter			
	R 9925 H	Seve Tre courts	
0.05 2			Extend Calculate
Protect including		1	1
Diddeg procedure	Burds of the lemit		
Lindow Graden	Loochtz -	De maleg mainer ovr t	' <u></u>
		The resulting maximum in our t	
Adultive Grocing	Lauchtz (n.d. forme MC error)		
Adaptive Creating Booswatcas	Londer * *		' <u></u>
Uniform Greecey Reserve Greecey Book-Rocal Adaptive Greecey Book-Spikar Kamel Gathbullon	Lauchtz (n.d. forme MC error)	8.996e-00 Labeled Tells	1 8.8 8.6
Union Groop Rosevecul *	Londer * *	8.994e-00 Labeled Dets Serie Serie	
Uniform Greecey Reserve Greecey Book-Rocal Adaptive Greecey Book-Spikar Kamel Gathbullon	Render on town to any a second to any a second to a se	8.996e-00 Letered Tens Serie Seri Target Seri	1 8.8 8.6
Union Groop Rosevecul *	Likechtz (no. form MC artic) *	8.994e-00 Labeled Dets Serie Serie	
Index Conseq Adaptive Oncore End-Victat Adaptive Oncore End-Victat Kame Dathbulon Martina Dathbulon Adaptive Oncore	Landezt * Landezt * Re-Max * The case of the tenet function * Kennel vector/Darget in * Exercit for the file *	8.996e-00 Letered Tens Serie Seri Target Seri	
Institute Geology Book-Hoart Abspilve Groups Book-Hoart Abspilve Groups Book-Hoart Abspilve Groups Book-Hoart Assessible Research Assessible As	Render on town to any a second to any a second to a se	8.996e-00 Letered Tens Serie Seri Target Seri	
Valence George Massen of Society Book-receive Massen of Society Book-receive Massel Society Book-receive Massel Society Massel Society Massel Society Problem Society Problem Society Massel Society Problem Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Masse	Landezt * Landezt * Re-Max * The case of the tenet function * Kennel vector/Darget in * Exercit for the file *	8.996e-00 Letered Tens Serie Seri Target Seri	
Index Codegy Anapter Doce-Lean Anapter Doce Lean Anapter Doce Lean	Annual International State (Section 2014) * The same of PEA former Maximum * Section 2014 The same former Maximum	5964-00 Letend Tels Safe Set 4 Add Rancer Edit	
Valence George Massen of Society Book-receive Massen of Society Book-receive Massel Society Book-receive Massel Society Massel Society Massel Society Problem Society Problem Society Massel Society Problem Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Society Massel Masse	Another Section 10 and 10	5964-00 Letend Tels Safe Set 4 Add Rancer Edit	
Johon Coope Anapies Coope Anapies Coope Anapies Coope Anapies Coope Anapies Coope Anapies Coope Anapies Anapie	And the second s	5964-00 Letend Tels Safe Set 4 Add Rancer Edit	
Index Codegy Anapter Doce-Lean Anapter Doce Lean Anapter Doce Lean	And the second s	5964-00 Letend Tels Safe Set 4 Add Rancer Edit	

http://sourceforge.net/projects/faust2





verification

- abstraction based
- novel algorithm with tighter bounds and more scalability





verification

- abstraction based
- novel algorithm with tighter bounds and more scalability



synthesis

- abstraction based
- optimisation via sparse matrices



verification

- abstraction based
- novel algorithm with tighter bounds and more scalability



synthesis

- abstraction based
- optimisation via sparse matrices

features

• modular

simulation

statistics

 $\bullet \ C++ \ implementation$

automatically generates

visualisation via time

varying histograms

- extendable
- multiple options



verification

- abstraction based
- novel algorithm with tighter bounds and more scalability



synthesis

- abstraction based
- optimisation via sparse matrices

features

simulation

statistics

automatically generates

visualisation via time

varying histograms

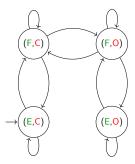
- modular
- C++ implementation
- extendable
- multiple options

Building automation systems - case study



$$\begin{aligned} x_{k+1} &= x_k + \frac{\Delta}{V} \left(-\mathbb{1}_{ON} m x_k + \mu_{\{O,C\}} (C_{out} - x_k) \right) + \mathbb{1}_F C_{occ} + \sigma_x w_k \\ y_{k+1} &= y_k + \frac{\Delta}{C} \left(\mathbb{1}_{ON} m (T_{set} - y_k) + \mu_{\{O,C\}} \frac{1}{R} (T_{out} - y_k) \right) + \mathbb{1}_F T_{occ,k} + \sigma_y w_k \end{aligned}$$

where $T_{occ,k} = \nu x_k + \zeta$



Building automation systems - case study

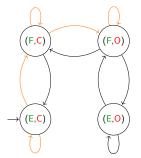
- safe set $A = [300\ 700] ppm \times [19\ 21]^{o}C$
- air circulation: closed-loop control policy at k+1

$$\begin{cases} OFF & \text{if } (x_k, y_k) \leq A \\ ON & \text{if } (x_k, y_k) \geq A \\ \text{stay put} & \text{else} \end{cases}$$

• specification:

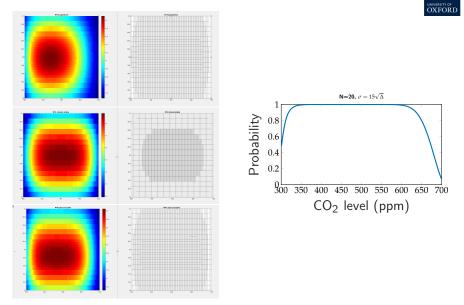
$$\mathbb{P}_{=?}\left[\Box^{\leq 20}(x,y)\in A\right]$$

- 5 hours, 8:00-13:00 ($\Delta = 15$ min, N=20), divided into
 - 8:00-8:30 (N=2) (E,C)
 - 8:30-11:30 (N=12) (F,C)
 - 11:30-13:00 (N=6) (F,O)





Building automation systems – case study





All images used are under Wikimedia CCAS license, or by author

Selected journal references

L. Laurenti, M. Lahijanian, A. Abate, L. Cardelli and M. Kwiatkowska, "Formal and Efficient Control Synthesis for Continuous-Time Stochastic Processes," IEEE Transactions on Automatic Control, vol. 66, no. 1, pp. 17-32, Jan 2021.

S. Haesaert, S.E.Z. Soudjani, and A. Abate, "Verification of general Markov decision processes by approximate similarity relations and policy refinement," SIAM Journal on Control and Optimisation, vol. 55, nr. 4, pp. 2333-2367, 2017.

I. Tkachev, A. Mereacre, J.-P. Katoen, and A. Abate, "Quantitative Model Checking of Controlled Discrete-Time Markov Processes," Information and Computation, vol. 253, nr. 1, pp. 1–35, 2017.

S. Haesaert, N. Cauchi and A. Abate, "Certified policy synthesis for general Markov decision processes: An application in building automation systems," Performance Evaluation, vol. 117, pp. 75-103, 2017.

S.E.Z. Soudjani and A. Abate, "Aggregation and Control of Populations of Thermostatically Controlled Loads by Formal Abstractions," IEEE Transactions on Control Systems Technology. vol. 23, nr. 3, pp. 975–990, 2015.

S.E.Z. Soudjani and A. Abate, "Quantitative Approximation of the Probability Distribution of a Markov Process by Formal Abstractions," Logical Methods in Computer Science, Vol. 11, nr. 3, Oct. 2015.

M. Zamani, P. Mohajerin Esfahani, R. Majumdar, A. Abate, and J. Lygeros, "Symbolic control of stochastic systems via approximately bisimilar finite abstractions," IEEE Transactions on Automatic Control, vol. 59 nr. 12, pp. 3135-3150, Dec. 2014.

I. Tkachev and A. Abate, "Characterization and computation of infinite horizon specifications over Markov processes," Theoretical Computer Science, vol. 515, pp. 1-18, 2014.

S. Soudjani and A. Abate, "Adaptive and Sequential Gridding for Abstraction and Verification of Stochastic Processes," SIAM Journal on Applied Dynamical Systems, vol. 12, nr. 2, pp. 921-956, 2013.

A. Abate, et al., "Approximate Model Checking of Stochastic Hybrid Systems," European Journal of Control, 16(6), 624-641, 2010.

A. Abate, et al., "Probabilistic Reachability and Safety Analysis of Controlled Discrete-Time Stochastic Hybrid Systems," Automatica, 44(11), 2724-2734, Nov. 2008.



Thank you for your attention

For more info: aabate@cs.ox.ac.uk