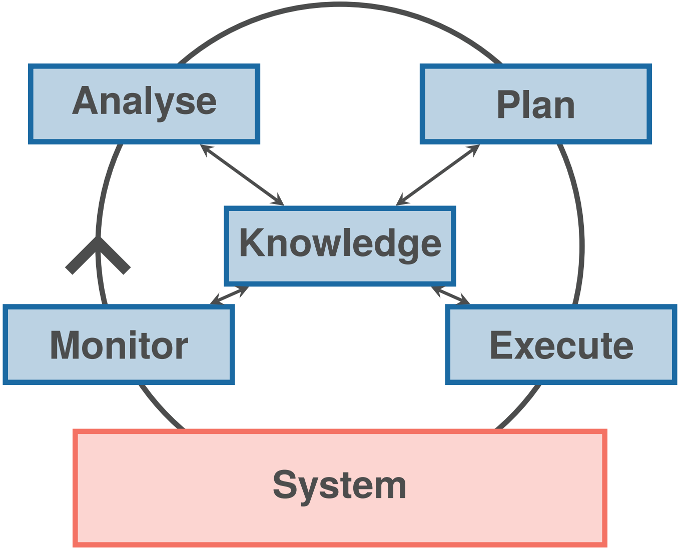
Formal-methods support for runtime adaptation in role-based systems

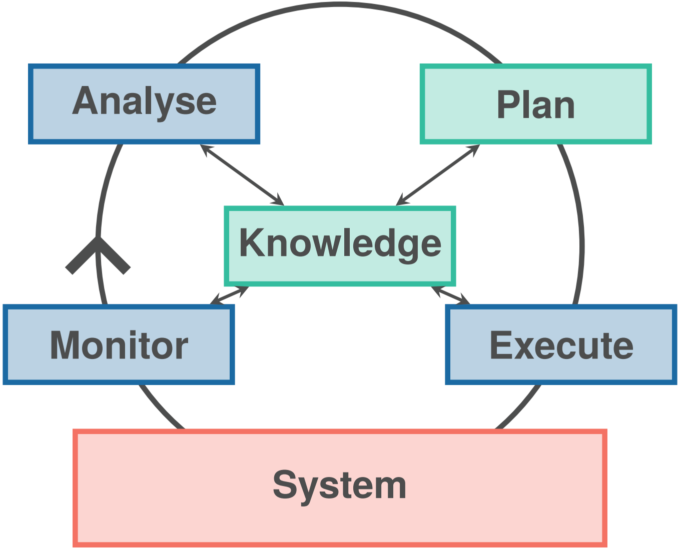
Max Korn

Chair

Institute of Theoretical Computer Science – TU Dresden

16-11-2020


Analyse
Plan
Knowledge
Monitor
Execute
System


Analyse
Plan
Knowledge
Monitor
Execute
System

Outline

State of the Art

Contributions

- PMC-based Decision Making
- Statistical Analysis of Decider Performance

Experiments

Conclusion

State of the Art

System-verification

Verify system properties at the design stage, like:

- Resilience (Cámara and de Lemos (2012))
- Safety (Güdemann, Ortmeier, and Reif (2006))
- Performance (M. Becker, Luckey, and S. Becker (2013))

State of the Art

System-verification

Verify system properties at the design stage, like:

- Resilience (Cámara and de Lemos (2012))
- Safety (Güdemann, Ortmeier, and Reif (2006))
- Performance (M. Becker, Luckey, and S. Becker (2013))

Decision making

Effective decision making by computing expected consequences of decisions

State of the Art

System-verification

Verify system properties at the design stage, like:

- Resilience (Cámara and de Lemos (2012))
- Safety (Güdemann, Ortmeier, and Reif (2006))
- Performance (M. Becker, Luckey, and S. Becker (2013))

Decision making

Effective decision making by computing expected consequences of decisions

Main Challenge
Complexity of system representation

Decision making with Formal Methods

Decision making with Formal Methods

- simulation reduction (Calinescu et al. (2011))
- statistical methods (Iftikhar and Weyns (2014))

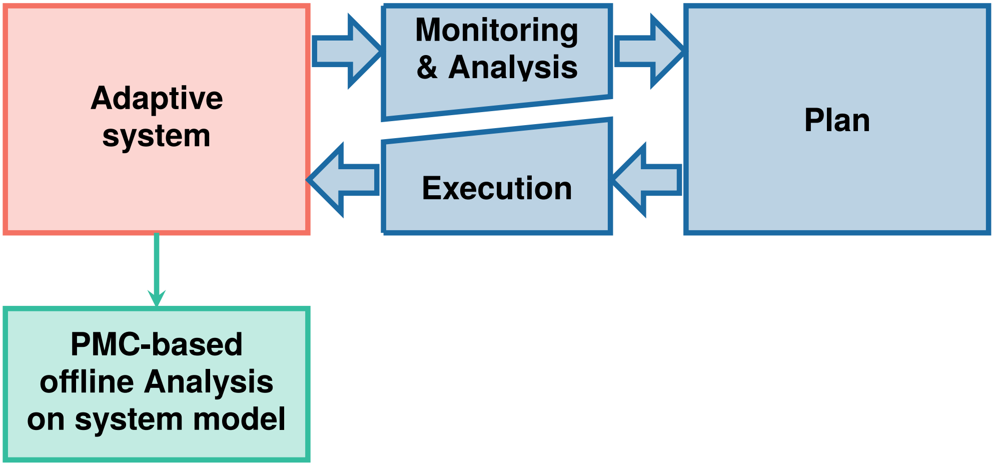
Decision making with Formal Methods

- simulation reduction (Calinescu et al. (2011))
- statistical methods (Iftikhar and Weyns (2014))
- Parametric Model Checking(Filieri, Ghezzi, and Tamburrelli (2011))
- Pre-computation of Scenarios (Saller, Lochau, and Reimund (2013))

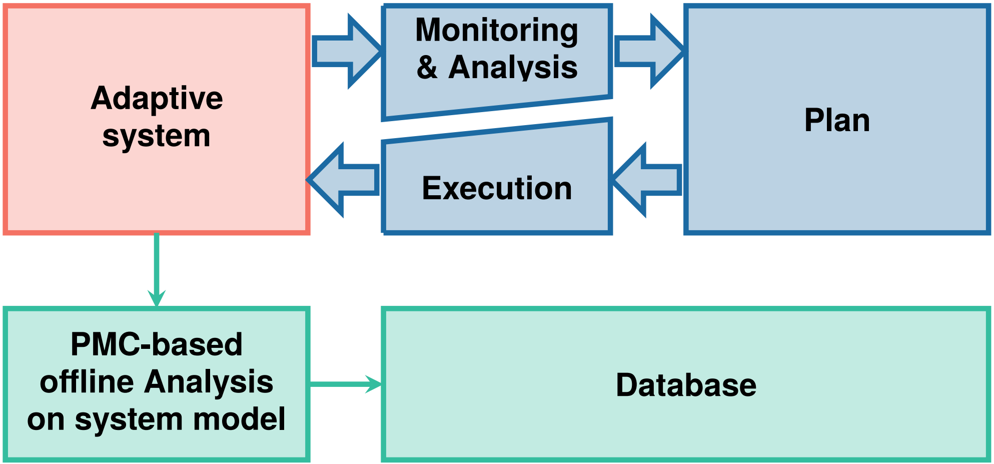
Contributions

Fundamental Concept

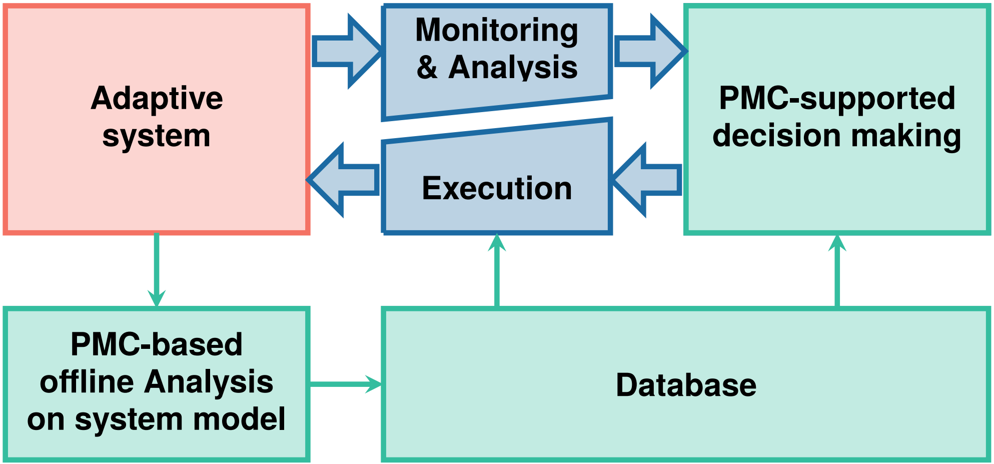
Fundamental Concept



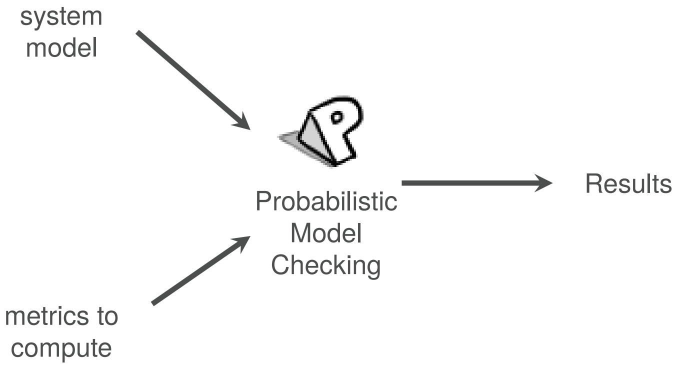
Fundamental Concept



Fundamental Concept



PMC-based Decision Making



Objective of the Decider

Objective of the Decider

Split the **global objective** into multiple **local metrics**

Objective of the Decider

Split the **global objective** into multiple **local metrics**

Local Metrics

- $Pr(\texttt{P1})$
- $Exp(\texttt{E1})$

⋮

Objective of the Decider

Split the **global objective** into multiple **local metrics**

Global Objective

keep P1 $\geq$ 0.9

minimise E1

⋮

Local Metrics

- $Pr(\texttt{P1})$
- $Exp(\texttt{E1})$

⋮

Objective of the Decider

Split the **global objective** into multiple **local metrics**

Global Objective

Strategy

keep P1 $\geq$ 0.9

minimise E1

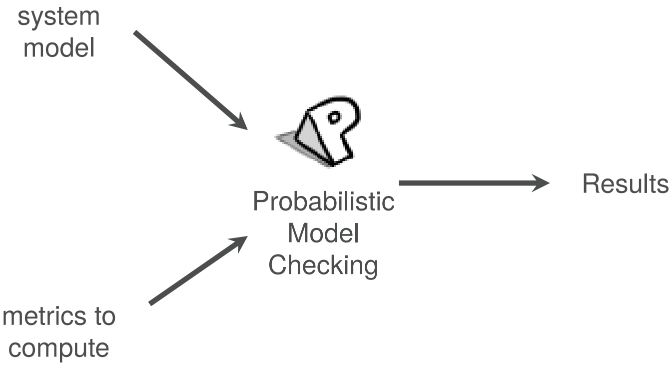
⋮

Local Metrics

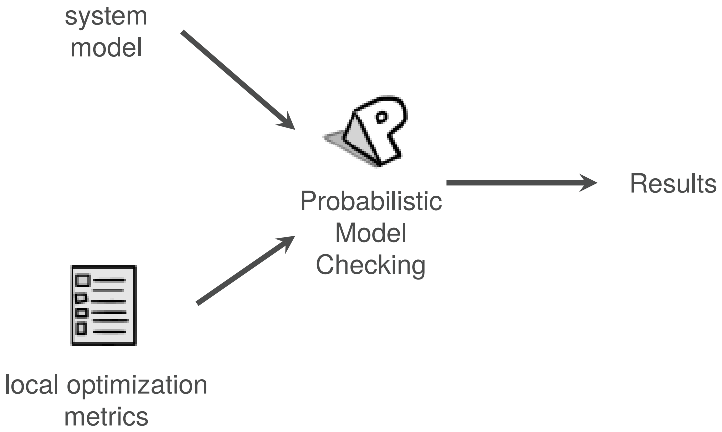
- $Pr(\texttt{P1})$
- $Exp(\texttt{E1})$

⋮

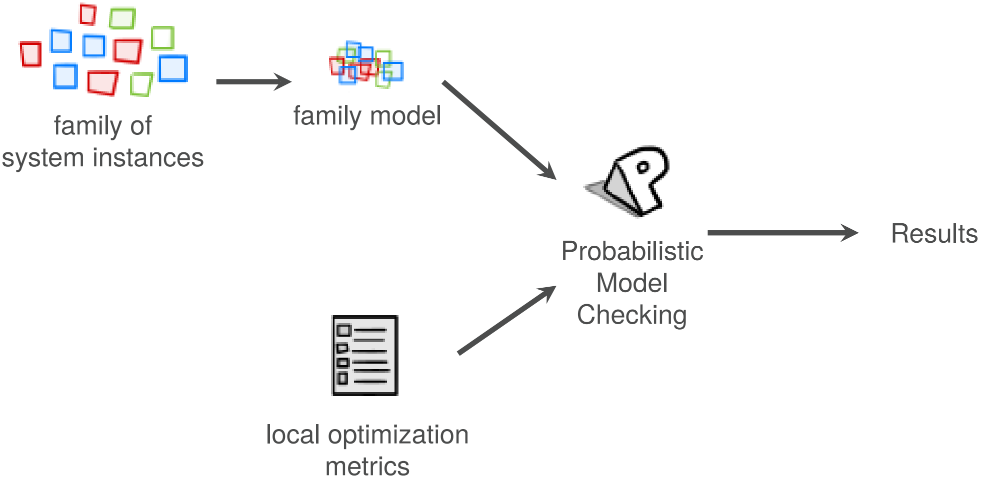
PMC-based Decision Making



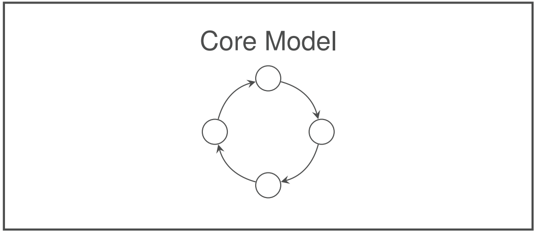
PMC-based Decision Making



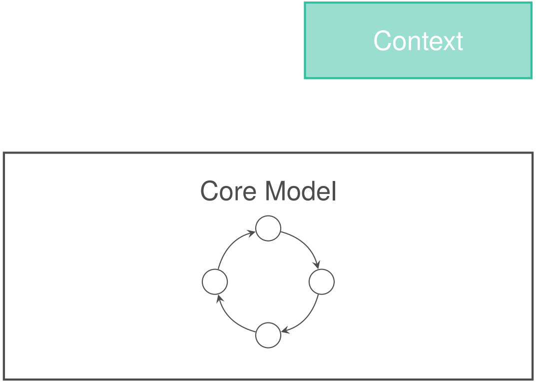
PMC-based Decision Making



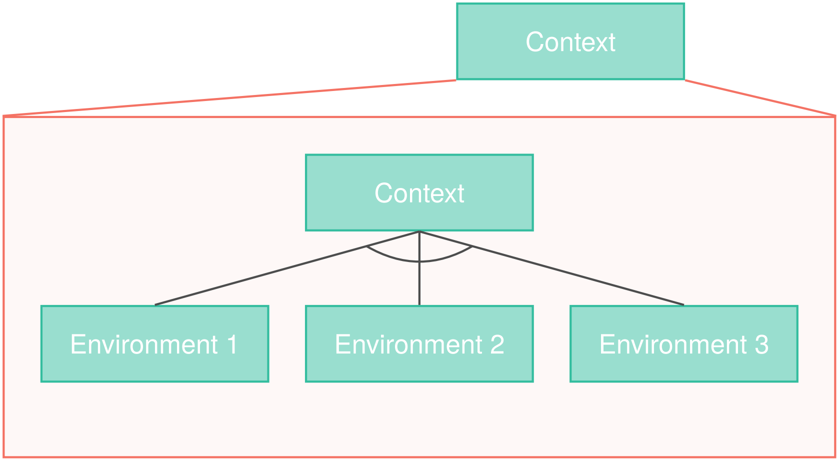
Family Model



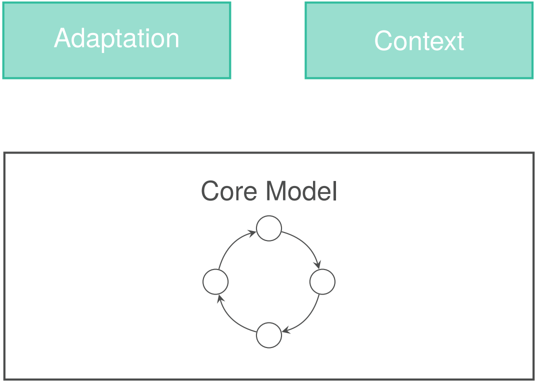
Family Model



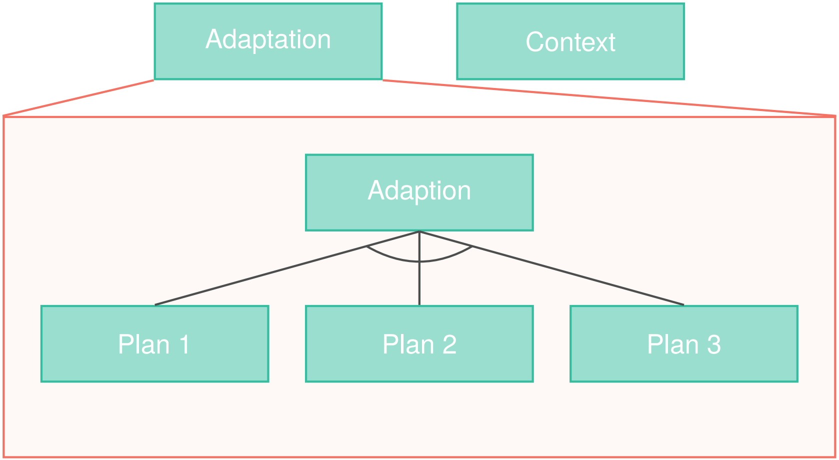
Family Model



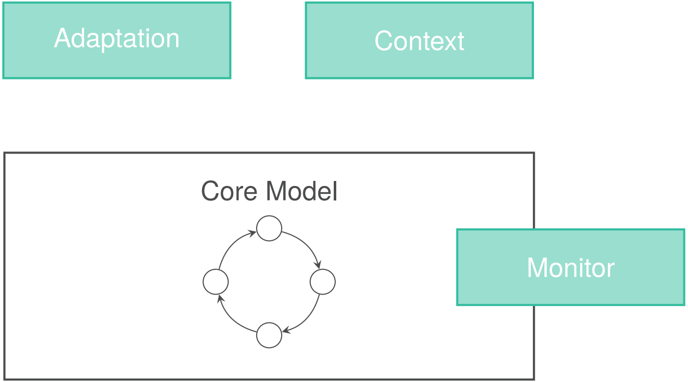
Family Model



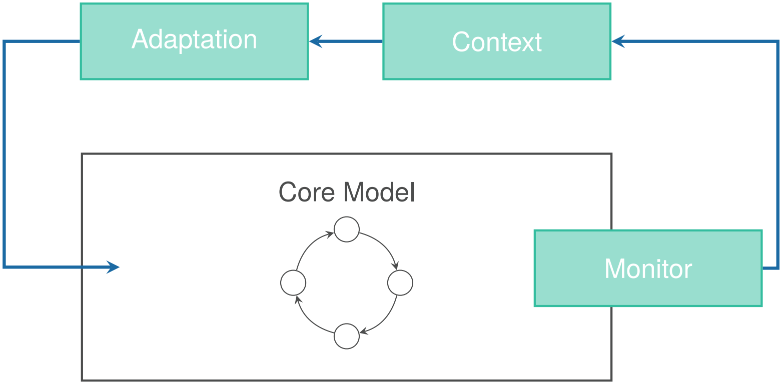
Family Model



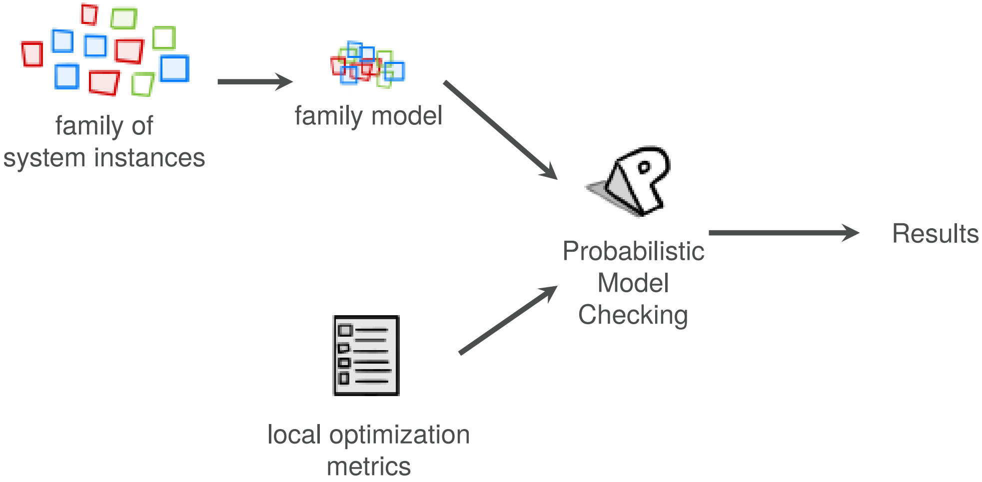
Family Model



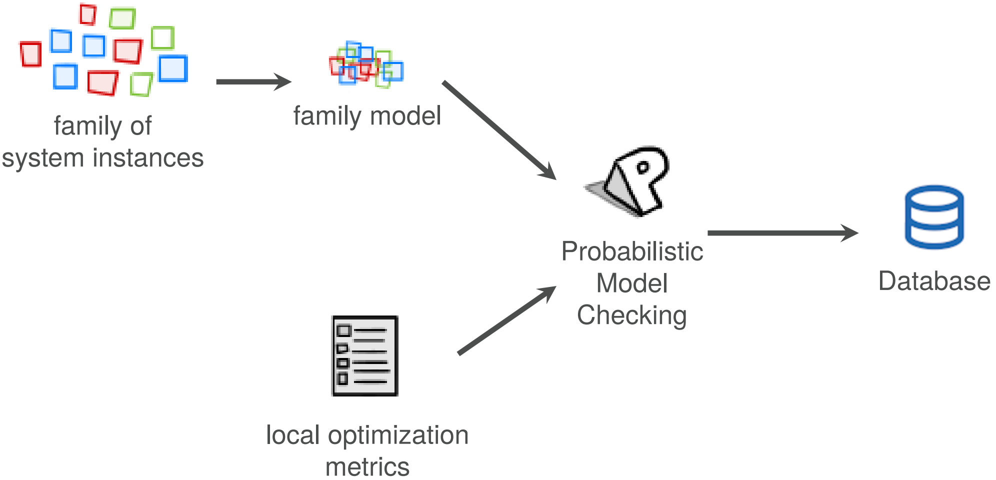
Family Model



PMC-based Decision Making



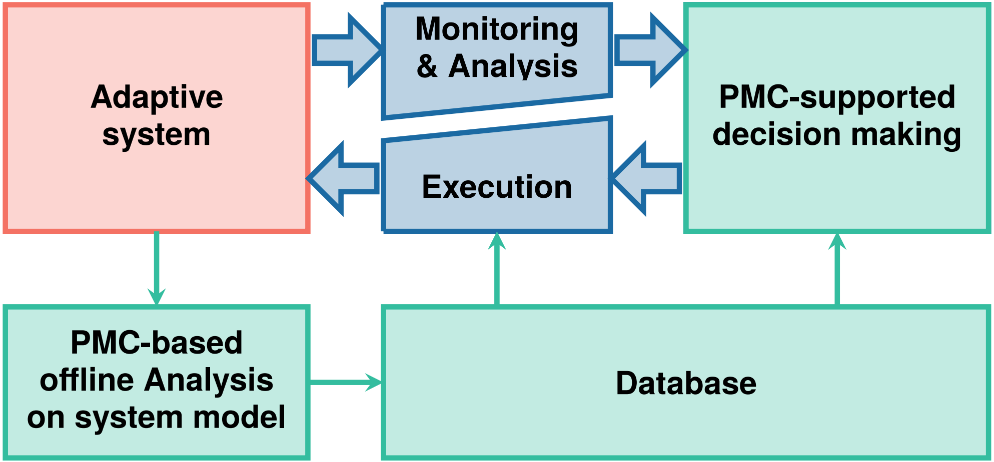
PMC-based Decision Making



Database

Environment	Plan	Observable Variable 1	Observable Variable 2	P1	E1	...
1	1	0	0	0.7	34.5	...
1	1	0	1	0.64	29.0	...
1	1	1	0	0.61	28.7	...
1	1	1	1	0.57	25.1	...
1	2	0	0	0.9	50.1	...
1	2	0	1	0.95	45.6	...
1	2	1	0	0.81	33.6	...
1	2	1	1	0.89	34.8	...
2	1	0	0	0.3	87.3	...
2	1	0	1	0.4	90.1	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Fundamental Concept



Objective of the Decider

Split the **global objective** into multiple **local metrics**

Global Objective

Strategy

keep P1 $\geq$ 0.9

minimise E1

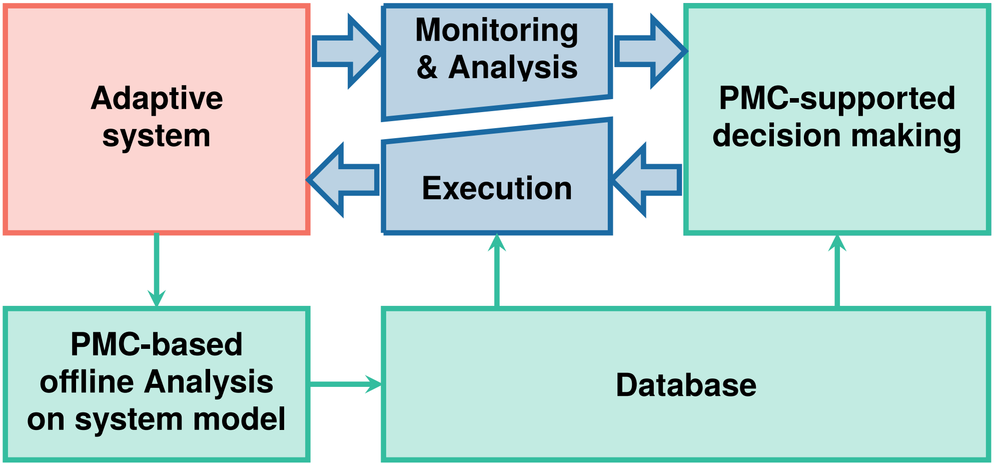
⋮

Local Metrics

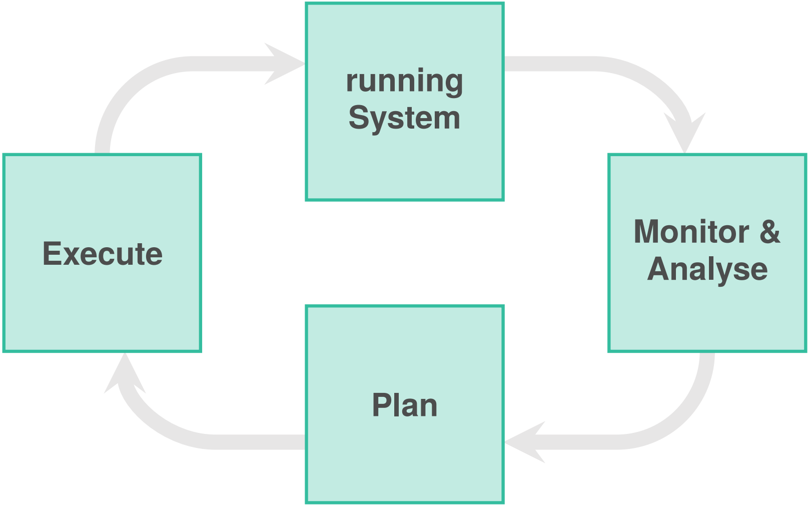
- $Pr(\texttt{P1})$
- $Exp(\texttt{E1})$

⋮

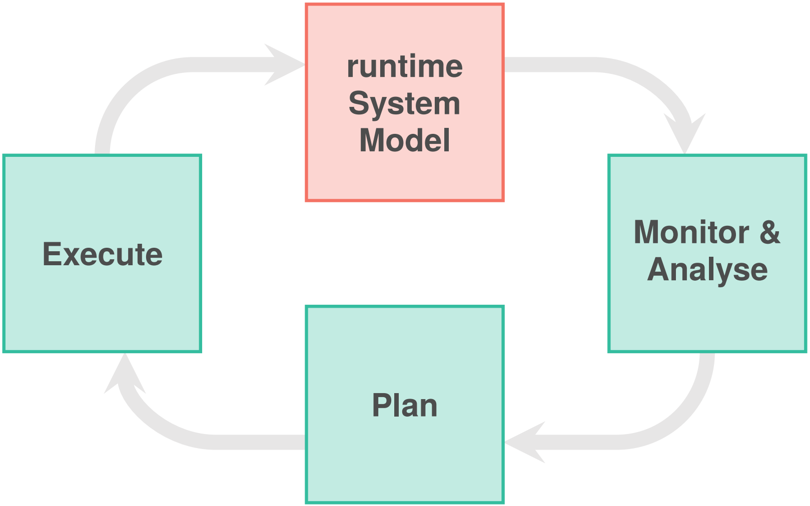
Fundamental Concept



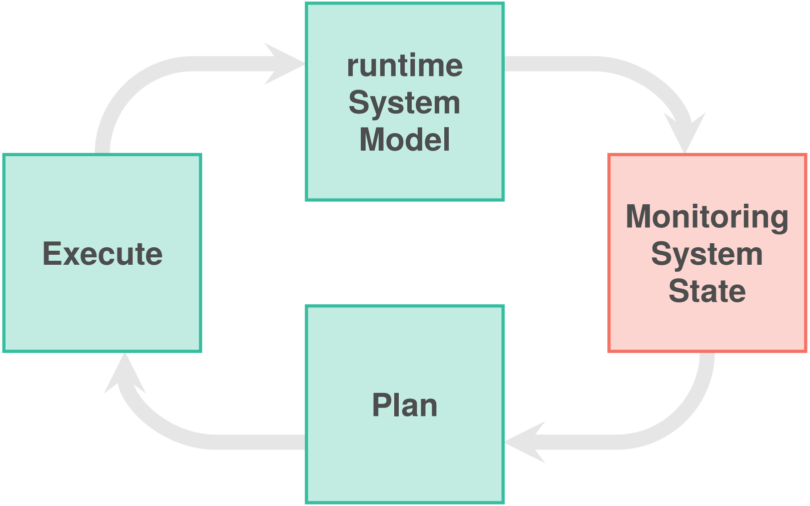
Statistical Analysis of Decider Performance



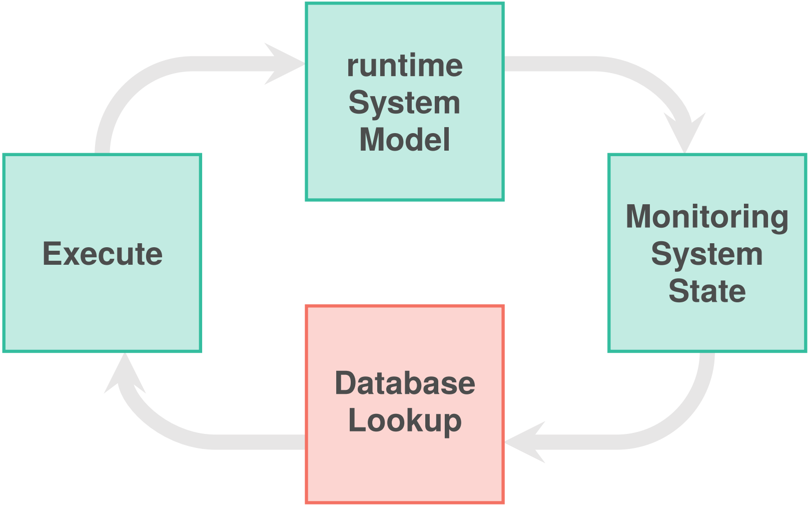
Statistical Analysis of Decider Performance



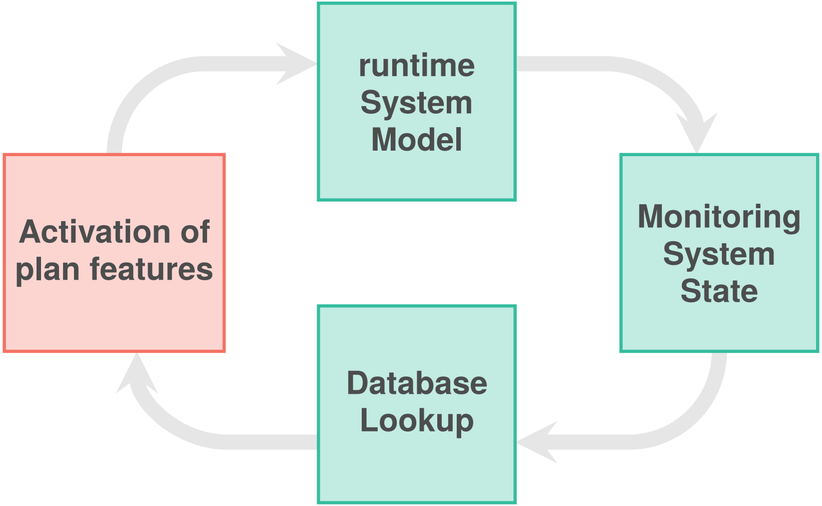
Statistical Analysis of Decider Performance



Statistical Analysis of Decider Performance



Statistical Analysis of Decider Performance



Experiments

Tooling

Implemented using the modelling language ProFeat[1] and the Model Checker Prism[2].

[1] Chrszon et al. (2018)
[2] Kwiatkowska, Norman, and Parker (2011)

Tooling

Implemented using the modelling language ProFeat[1] and the Model Checker Prism[2].

Successful self-adaptation on Prism case-study models:

[1] Chrszon et al. (2018)
[2] Kwiatkowska, Norman, and Parker (2011)

Tooling

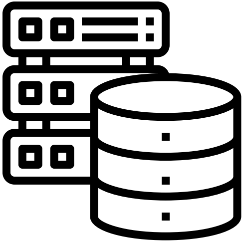
Implemented using the modelling language ProFeat[1] and the Model Checker Prism[2].

Successful self-adaptation on Prism case-study models:

- Real Time Voltage Scaling (Kwiatkowska, Norman, and Parker (2005))
- Human in the Loop UAV Mission Planning (Feng et al. (2015))
- Network Virus Infection (Kwiatkowska, Norman, Parker, and Vigliotti (2009))

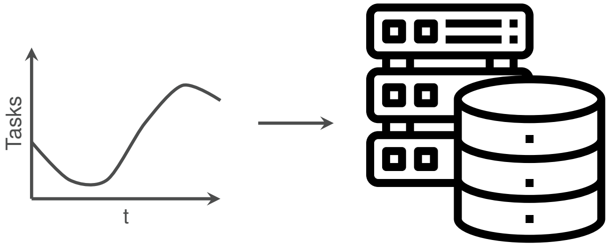
[1] Chrszon et al. (2018)
[2] Kwiatkowska, Norman, and Parker (2011)

Experiment Scenario



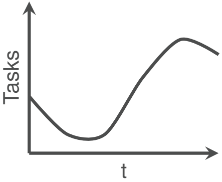
Adaptive DBMS

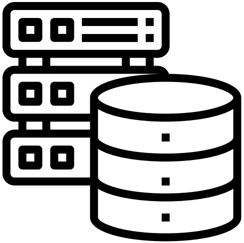
Experiment Scenario



Adaptive DBMS

Experiment Scenario





Adaptive DBMS

Adaptation

- Cores
- Frequency
- Hyper-Threading

Global Objective

Global Objective

Compute
all tasks

Global Objective

Compute all tasks

reduce Energy Costs

Global Objective

Global Objective

`Schedule:` $Pr(\text{all tasks computed})$

Global Objective

$\texttt{Schedule:} Pr(\text{all tasks computed})$ $\texttt{Costs:} Exp(\text{Costs})$

Global Objective

Compute all tasks ⟷ **Trade-off** ⟷ **reduce Energy Costs**

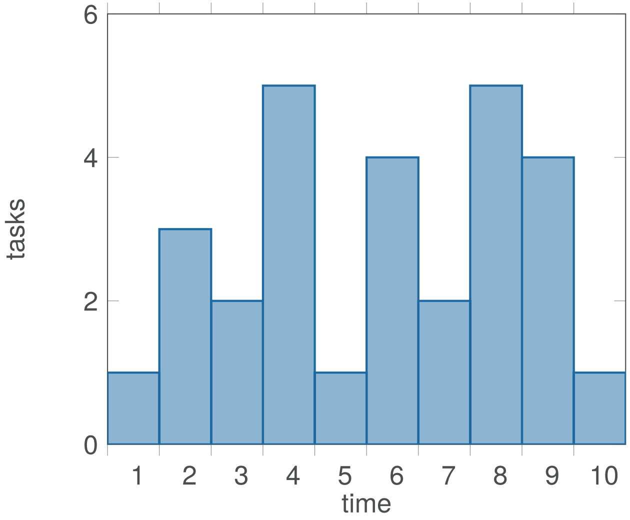
$\texttt{Schedule:} Pr(\text{all tasks computed})$

$\texttt{Costs:} Exp(\text{Costs})$

$\texttt{Budget:} Pr(\text{all tasks computed} \wedge \text{costs in budget})$

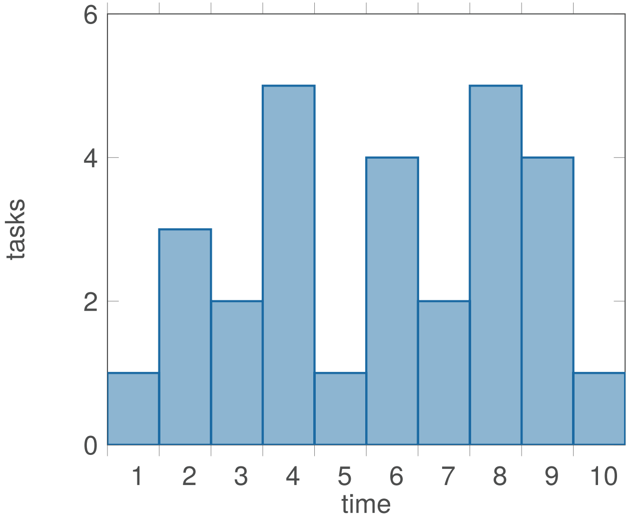
Experimental Setup

- Environment



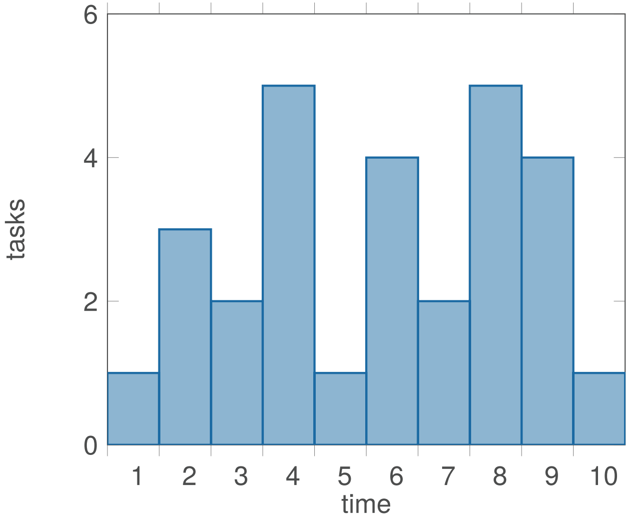
Experimental Setup

- Environment
- lookahead



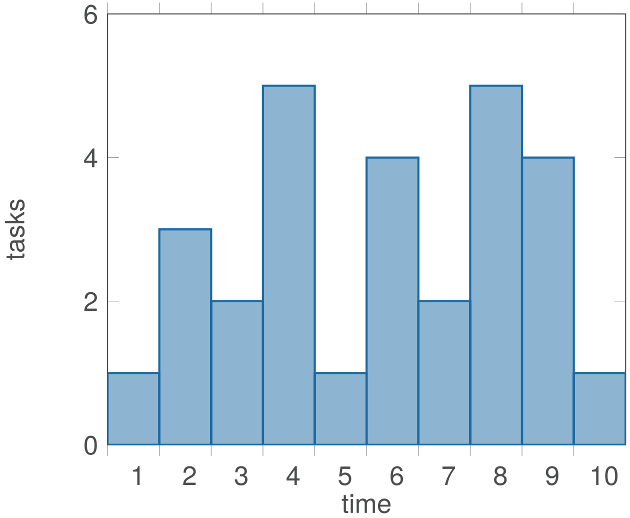
Experimental Setup

- Environment
- lookahead
- time between decisions



Experimental Setup

- Environment
- lookahead
- time between decisions
- noise-factor



Experimental Setup

- Environment
- lookahead
- time between decisions
- noise-factor
- Strategy

Experimental Setup

- Environment
- lookahead
- time between decisions
- noise-factor
- Strategy
  - `Max-Schedule`

`Max-Schedule:`

maximise `Schedule`

miminise `Costs`

Experimental Setup

- Environment
- lookahead
- time between decisions
- noise-factor
- Strategy
  - `Max-Schedule`
  - `Filter-Schedule`

`Filter-Schedule:`

keep `Schedule` $\geq$ 0.9

miminise `Costs`

Experimental Setup

RoSI

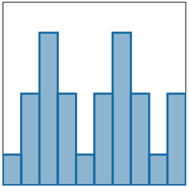
- Environment
- lookahead
- time between decisions
- noise-factor
- Strategy
  - `Max-Schedule`
  - `Filter-Schedule`
  - `Max-Budget`

`Max-Budget:`

maximise `Budget`

miminise `Costs`

Effect of Lookahead

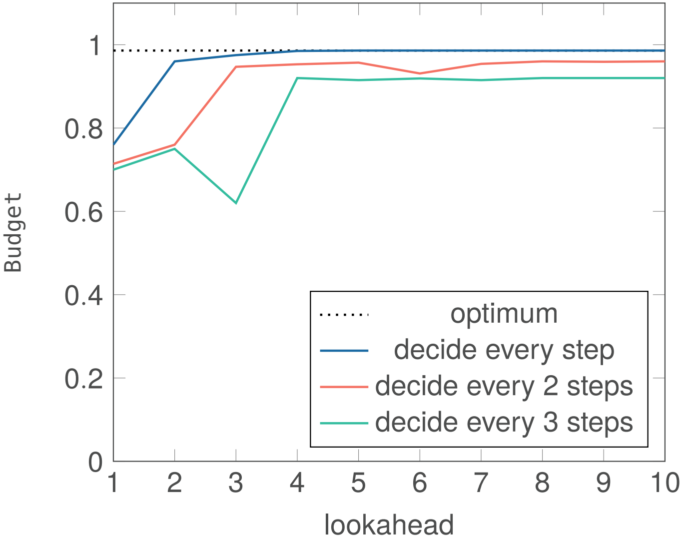


Lookahead: ∗

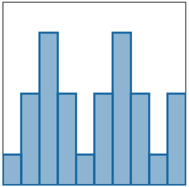
Decisions: ∗

Noise: 0

Strategy: `Max-Budget`



Effect of Noise

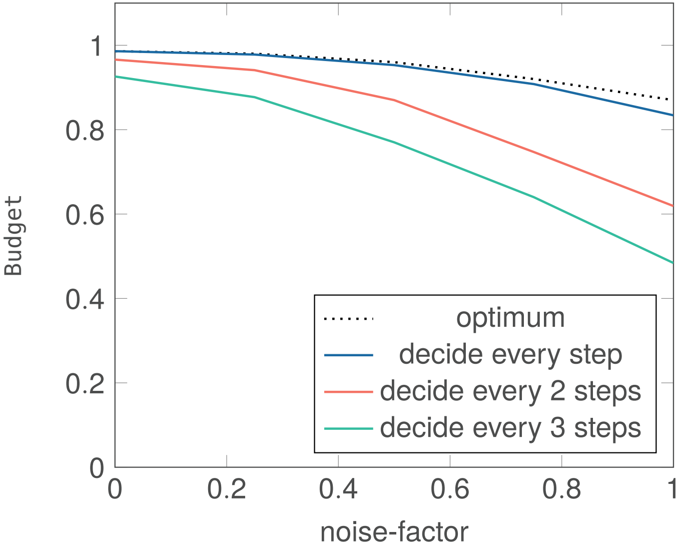


Lookahead: 10

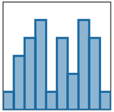
Decisions: ∗

Noise: ∗

Strategy: `Max-Budget`



Strategy Comparison

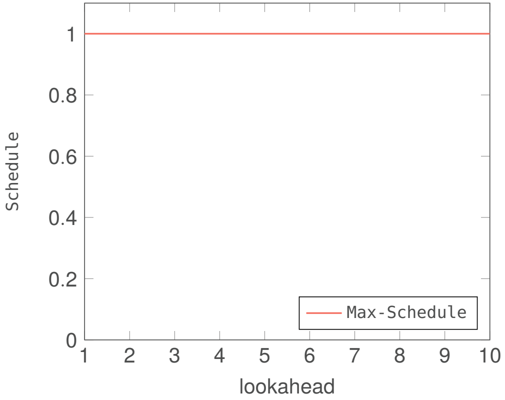


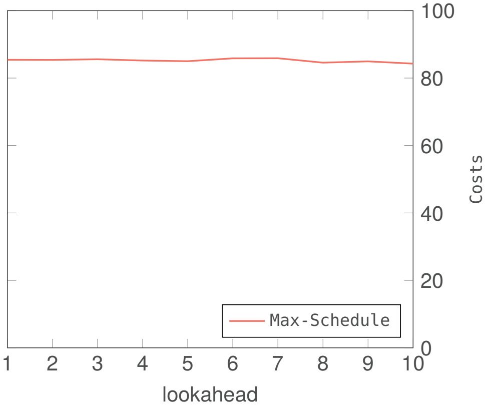
Lookahead: ∗

Decisions: every step

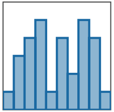
Noise: 0

Strategy: ∗





Strategy Comparison

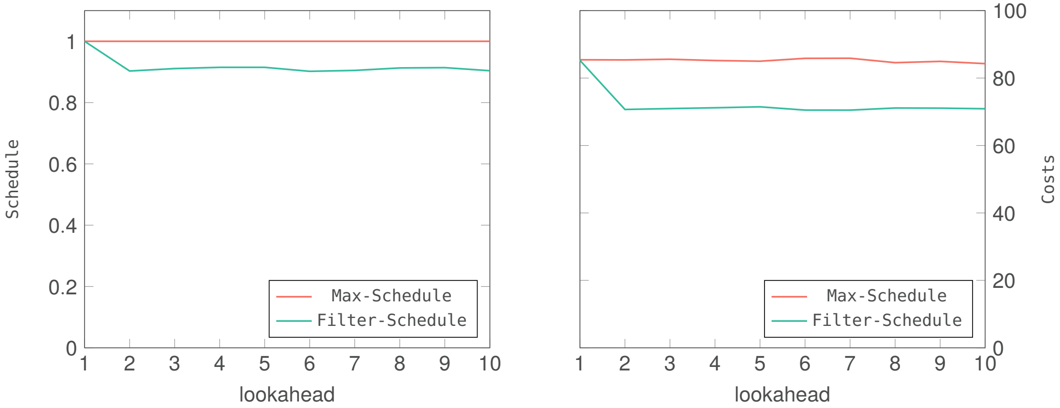


Lookahead: ∗

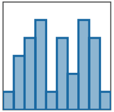
Decisions: every step

Noise: 0

Strategy: ∗



Strategy Comparison

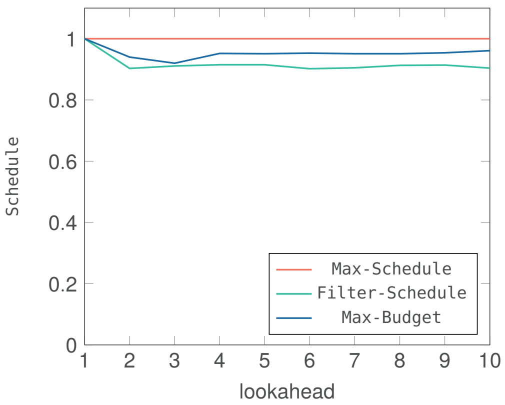


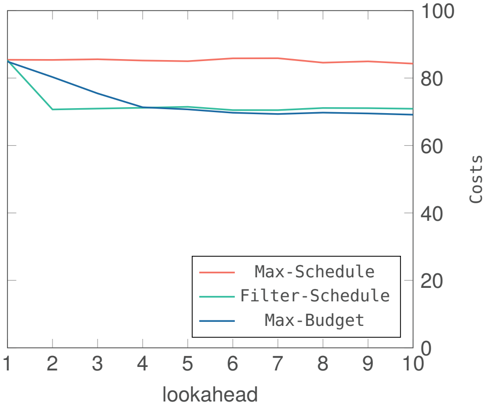
Lookahead: *

Decisions: every step

Noise: 0

Strategy: *





Conclusion

Conclusion

- Decision making approach using offline PMC

Conclusion

- Decision making approach using offline PMC
- Analysis tool using statistic MC

Conclusion

- Decision making approach using offline PMC
- Analysis tool using statistic MC

Conclusion

- Decision making approach using offline PMC
- Analysis tool using statistic MC

Paper in progress

Conclusion

- Decision making approach using offline PMC
- Analysis tool using statistic MC

Paper in progress

Further analysis:

- effects of environmental changes

Conclusion

- Decision making approach using offline PMC
- Analysis tool using statistic MC

Paper in progress

Further analysis:

- effects of environmental changes
- separating global objective in local metrics

Related Work I

- Becker, Matthias, Markus Luckey, and Steffen Becker (2013). "Performance Analysis of Self-Adaptive Systems for Requirements Validation at Design-Time". In: *Proceedings of the 9th International ACM Sigsoft Conference on Quality of Software Architectures*. QoSA '13. Vancouver, British Columbia, Canada: Association for Computing Machinery, pp. 43–52. ISBN: 9781450321266. DOI: 10.1145/2465478.2465489. URL: https://doi.org/10.1145/2465478.2465489.
- Calinescu, R. et al. (2011). "Dynamic QoS Management and Optimization in Service-Based Systems". In: *IEEE Transactions on Software Engineering* 37.3, pp. 387–409. DOI: 10.1109/TSE.2010.92.
- Cámara, J. and R. de Lemos (2012). "Evaluation of resilience in self-adaptive systems using probabilistic model-checking". In: *2012 7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, pp. 53–62. DOI: 10.1109/SEAMS.2012.6224391.
- Chrszon, Philipp et al. (2018). *ProFeat: feature-oriented engineering for family-based probabilistic model checking*. DOI: 10.1007/s00165-017-0432-4.

Related Work II

- Feng, Lu et al. (2015). "Controller Synthesis for Autonomous Systems Interacting with Human Operators". In: *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*. ICCPS '15. Seattle, Washington: Association for Computing Machinery, pp. 70–79. ISBN: 9781450334556. DOI: 10.1145/2735960.2735973. URL: https://doi.org/10.1145/2735960.2735973.
- Filieri, Antonio, Carlo Ghezzi, and Giordano Tamburrelli (2011). "Run-Time Efficient Probabilistic Model Checking". In: *Proceedings of the 33rd International Conference on Software Engineering*. ICSE '11. Waikiki, Honolulu, HI, USA: Association for Computing Machinery, pp. 341–350. ISBN: 9781450304450. DOI: 10.1145/1985793.1985840. URL: https://doi.org/10.1145/1985793.1985840.
- Güdemann, M., F. Ortmeier, and W. Reif (2006). "Safety and Dependability Analysis of Self-Adaptive Systems". In: *Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (isola 2006)*, pp. 177–184. DOI: 10.1109/ISoLA.2006.38.

Related Work III

- Iftikhar, M. Usman and Danny Weyns (2014). "ActivFORMS: Active Formal Models for Self-Adaptation". In: *Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*. SEAMS 2014. Hyderabad, India: Association for Computing Machinery, pp. 125–134. ISBN: 9781450328647. DOI: 10.1145/2593929.2593944. URL: https://doi.org/10.1145/2593929.2593944.
- Kwiatkowska, M., G. Norman, and D. Parker (2005). "Probabilistic Model Checking and Power-Aware Computing". In: *Proc. 7th International Workshop on Performability Modeling of Computer and Communication Systems (PMCCS'05)*, pp. 6–9.
- – (2011). "PRISM 4.0: Verification of Probabilistic Real-time Systems". In: *Proc. 23rd International Conference on Computer Aided Verification (CAV'11)*. Ed. by G. Gopalakrishnan and S. Qadeer. Vol. 6806. LNCS. Springer, pp. 585–591.
- Kwiatkowska, M., G. Norman, D. Parker, and M.G. Vigliotti (2009). "Probabilistic Mobile Ambients". In: *Theoretical Computer Science* 410.12–13, pp. 1272–1303.

Related Work IV

Saller, Karsten, Malte Lochau, and Ingo Reimund (2013). "Context-Aware DSPLs: Model-Based Runtime Adaptation for Resource-Constrained Systems". In: *Proceedings of the 17th International Software Product Line Conference Co-Located Workshops*. SPLC '13 Workshops. Tokyo, Japan: Association for Computing Machinery, pp. 106–113. ISBN: 9781450323253. DOI: 10.1145/2499777.2500716. URL: https://doi.org/10.1145/2499777.2500716.