# DD2552 - Seminars on Theoretical Computer Science, Programming Languages and Formal Methods, Seminar 7

Karl Palmskog (palmskog@kth.se)

2021-09-20

# Last Seminar and Today

Last seminar:

- error control for statistical model checking
- black box systems

Today:

- comparison of numerical and statistical methods
- statistical checking of unbounded untils

# Key properties of (PRISM) numerical checking

pros:

- iteratively improved precision of path probabilities
- lots of "symbolic tricks" can improve performance
- nesting of probability operator not an issue
- unbounded untils work fine

cons:

- needs white box, controllable model (rate matrix)
- no distributed checking
- problems scaling beyond state spaces of size $> 10^9$

# PRISM numerical approach for CTMC

- focus on formulas $P_{\geq\theta}(\phi\, U^{\leq t}\, \phi')$
- "uniformize" CTMC to a DTMC
- compute measure for path for *all* states simultaneously
- compare measure to $\theta$ for given state

# PRISM numerical measure computation

$$\overline{P}(\phi\, U^{\leq t}\, \phi') = \sum_{k=0}^{\infty} \gamma(k, q \cdot t) \cdot (\mathbb{P}^k \cdot f(s))$$

- $q$ is a "uniformization constant", $q \geq \max\{E'(s) \mid s \in S\}$
- $E'(s)$ is exit rate for $s$
- $f(s) = 1$ when $\mathcal{M}, s \models \phi'$, $f(s) = 0$ otherwise
- $\gamma(k, q \cdot t)$ is the $k$th Poisson probability with parameter $q \cdot t$
- $\gamma(k, q \cdot t) = e^{-q \cdot t} \cdot (q \cdot t)^k / k!$

# Numerical computation complexity

- introduce error tolerance $\epsilon$
- number of iterations grows very slowly as $\epsilon$ decreases
- for large $q \cdot t$, number of iterations is $O(q \cdot t)$
- each iteration takes $O(M)$ time, where $M$ is number of non-zero entries in rate matrix
- overall complexity: $O(q \cdot t \cdot M)$

# Statistical approach, abstractly

- select error probabilities $\alpha$ and $\beta$
- set up hypotheses $H_0$ and $H_1$ with indifference interval (half-width $\delta$)
- assume the underlying path measure (probability) is $p$
- main performance measure: number of samples/simulations (*sample size*)

# Statistical approach complexity

- we can stop analyzing a sample when we reach a state satisfying $\neg\phi \vee \phi'$
- in the worst case, we need time proportional to $t$, so expected time is $O(q \cdot t)$
- define $N_p$, the expected number of required samples
- overall complexity: $O(q \cdot t \cdot N_p)$
- key fact: no absolute dependency on state space size

# Combining numerical and statistical approaches

- can we get benefits of both approaches?
- need to consider models where numerical and statistical both work (DTMC, CTMC)
- nested probabilities: inner error bounds become terrible with sampling
- idea (Ymer): sample for outer operator, numerical for inner
- easy to transfer guarantees from numerical to statistical ($\alpha = \beta = 0$)

# Memory requirements

- for numerical: need to store the iteration vector
  - in case study: bottom out at 27 million states
- for statistical: only need to store current state
  - beyond 27 million states with ease