# Partial State Space Generation for Fault Tree Analysis

Matthias Volk
RWTH Aachen University

Safety of Future Systems
Lorentz Workshop 2018, Leiden

UnRAVeL Research Training Group – Uncertainty and Randomness in Algorithms, Verification, and Logic
RWTH AACHEN UNIVERSITY

# Example: Server

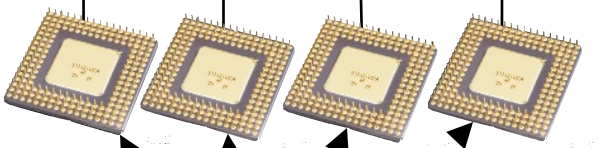
Server failure

CPU failure

2/4

Memory failure

Power failure



Cooling failure

# Example: Server

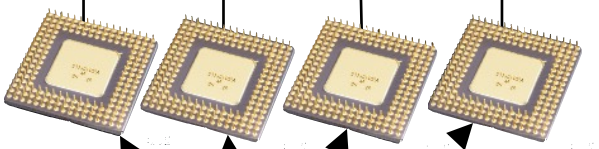
Server failure

CPU failure

2/4

Memory failure

Power failure



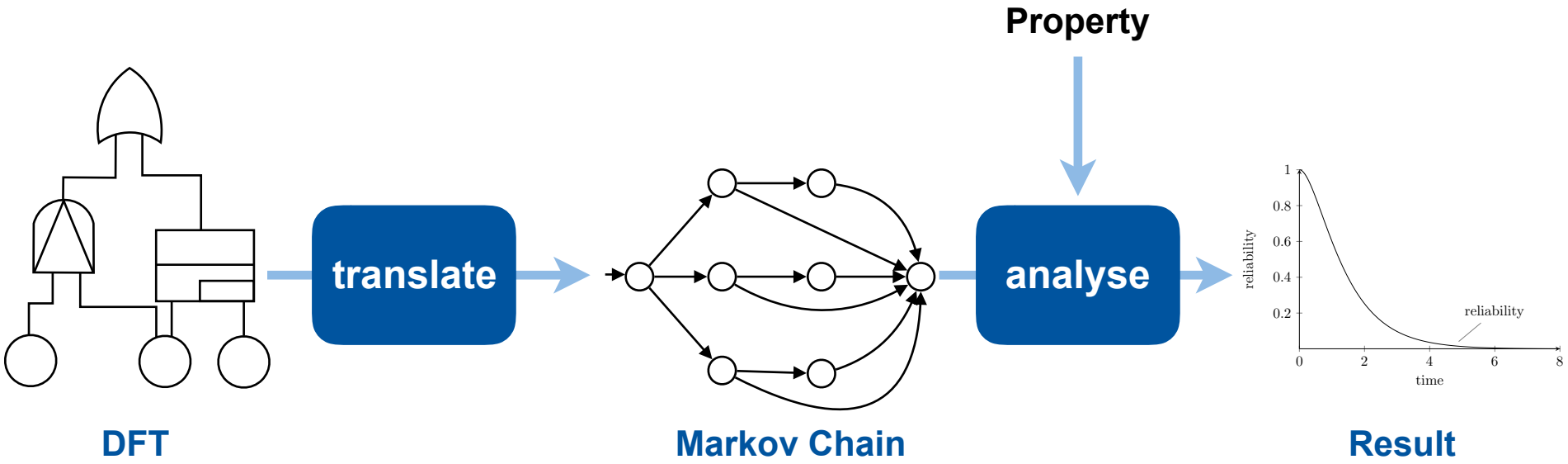
Cooling failure

Switch

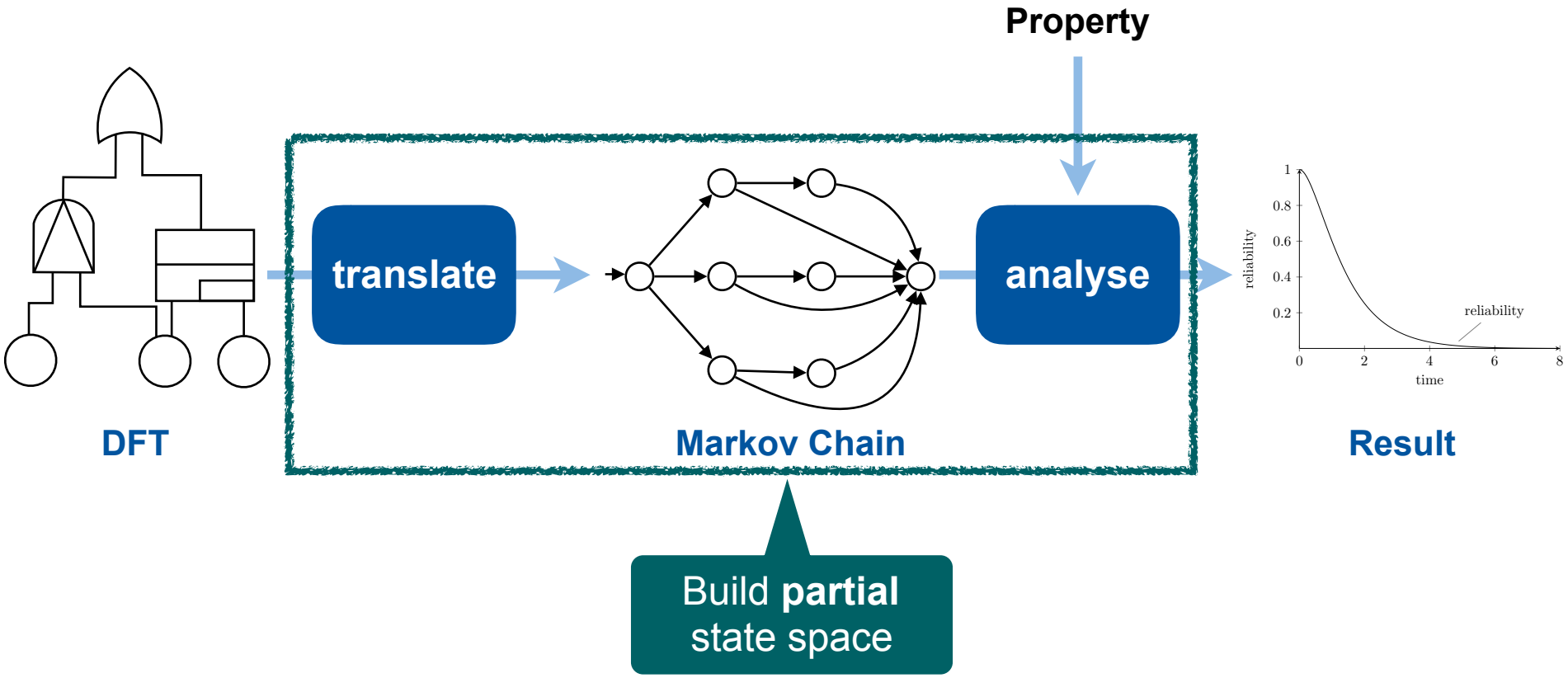
Power

UPS

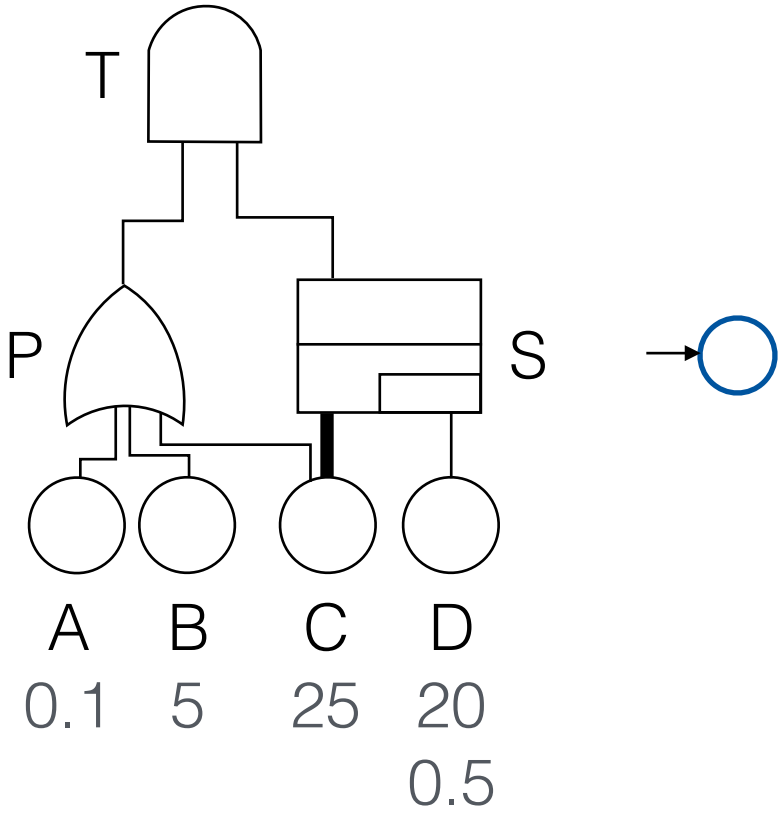
# Fault Tree Analysis



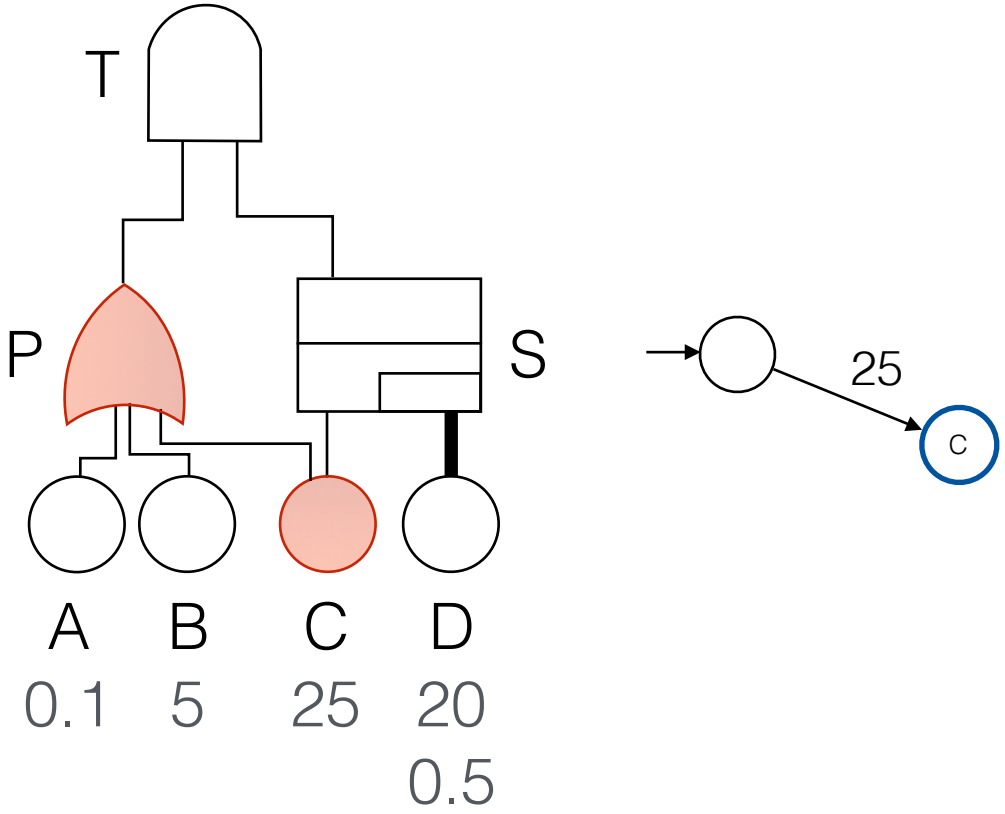
# Fault Tree Analysis



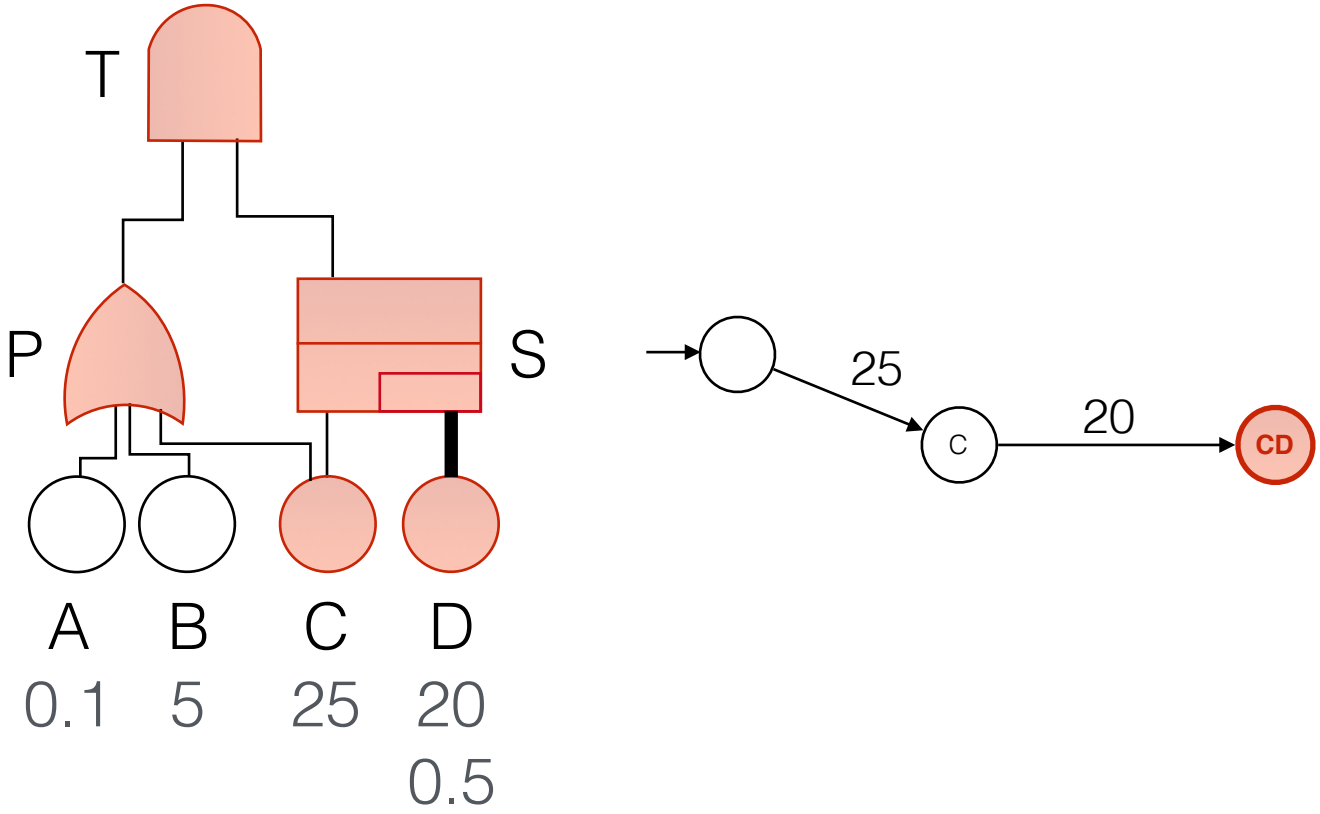
# State Space Exploration



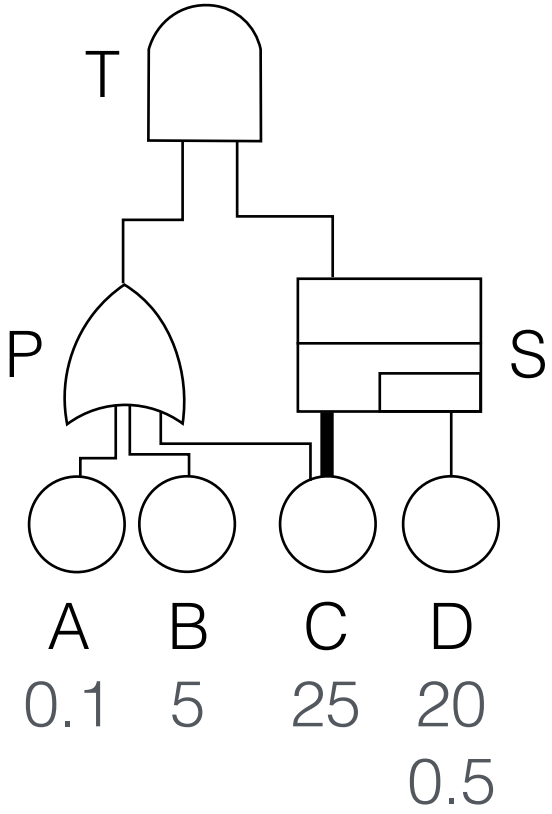
# State Space Exploration

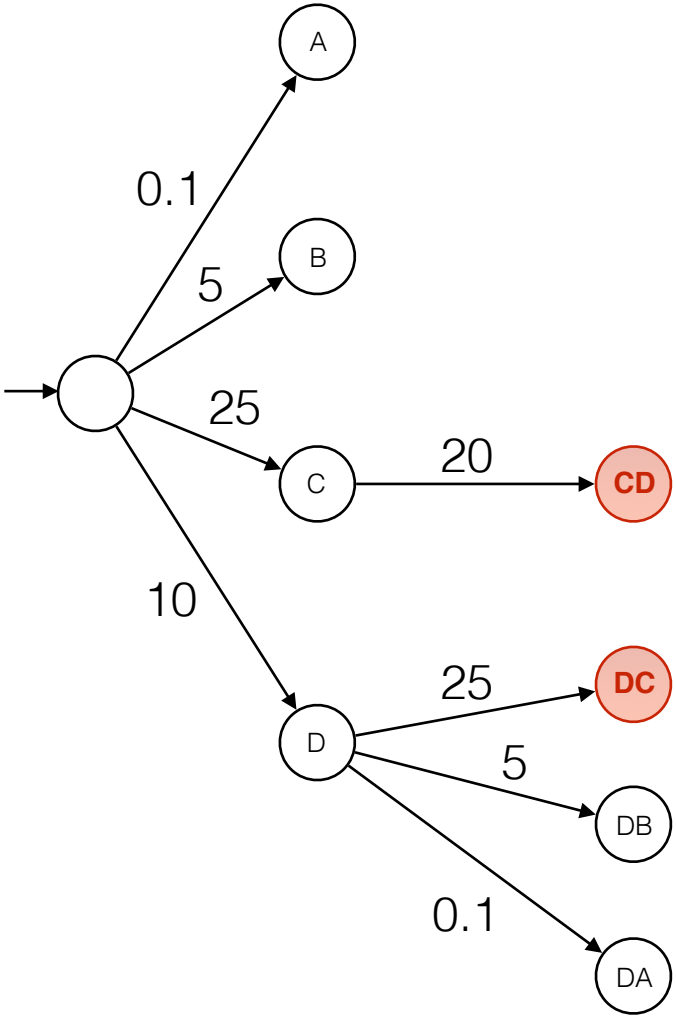


# State Space Exploration

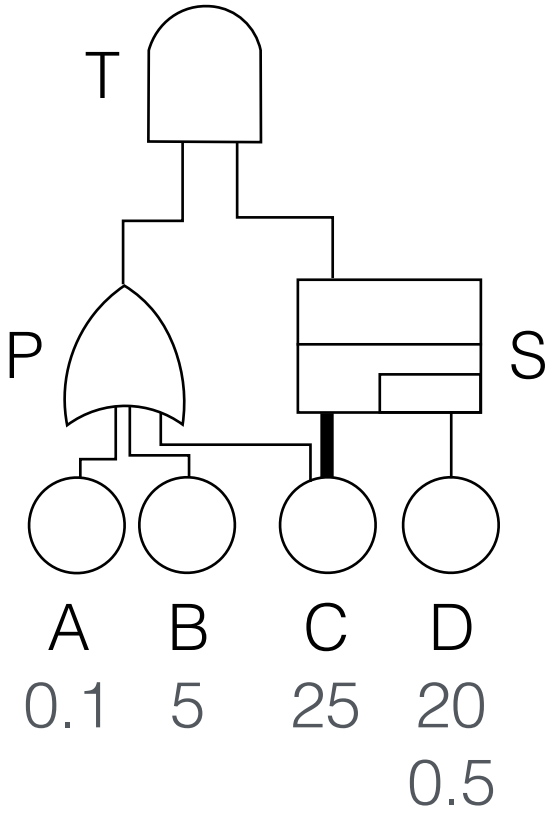


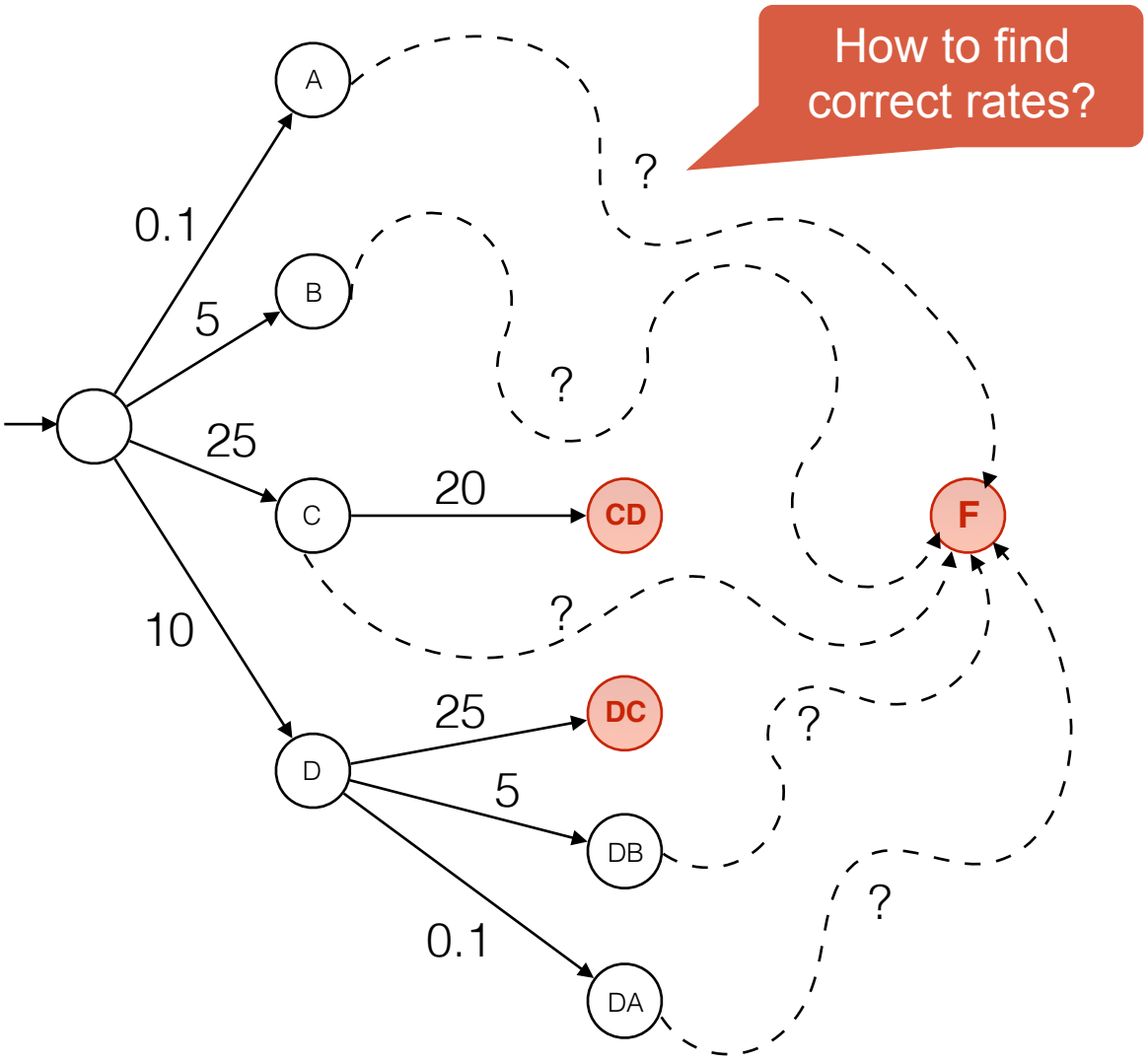
# Partial State Space Exploration



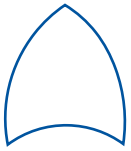
# Approximation idea

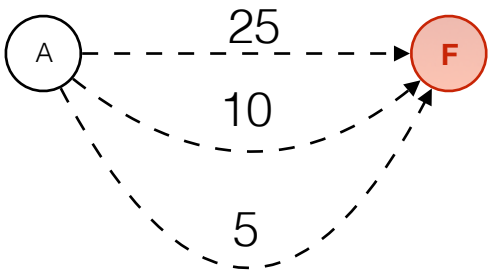


# Under and over approximation for MTTF

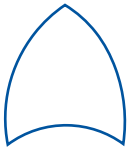
- **Under approximation:**
  - next BE leads to complete failure

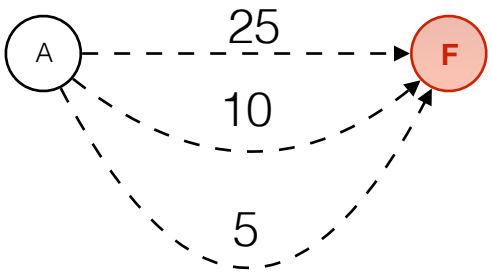




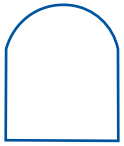
# Under and over approximation for MTTF

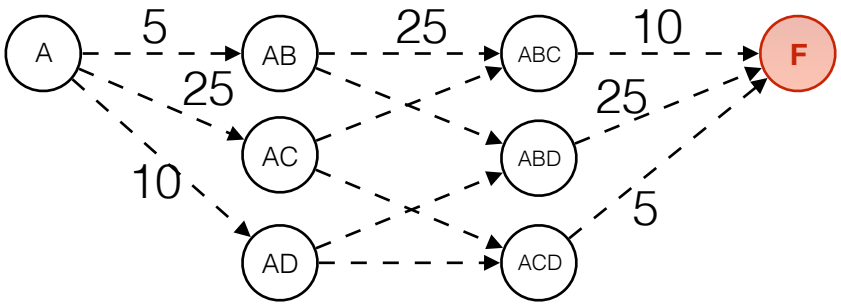
- **Under approximation:**
  - next BE leads to complete failure



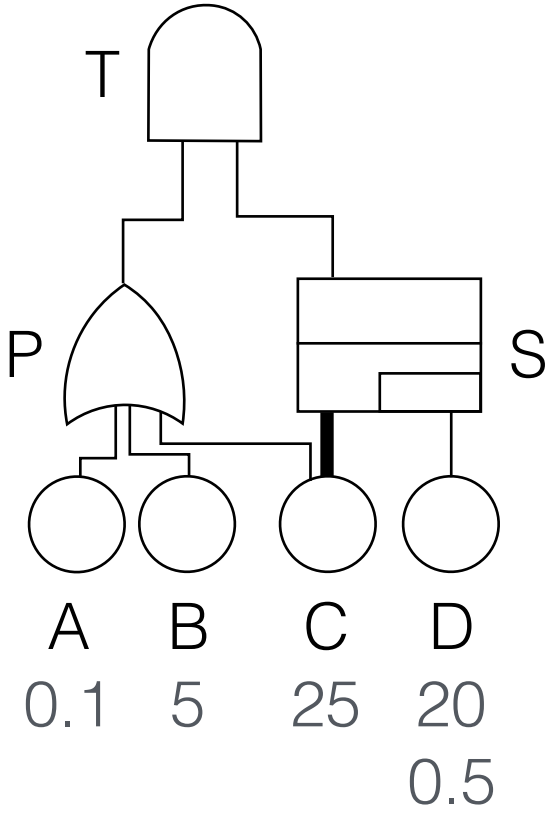


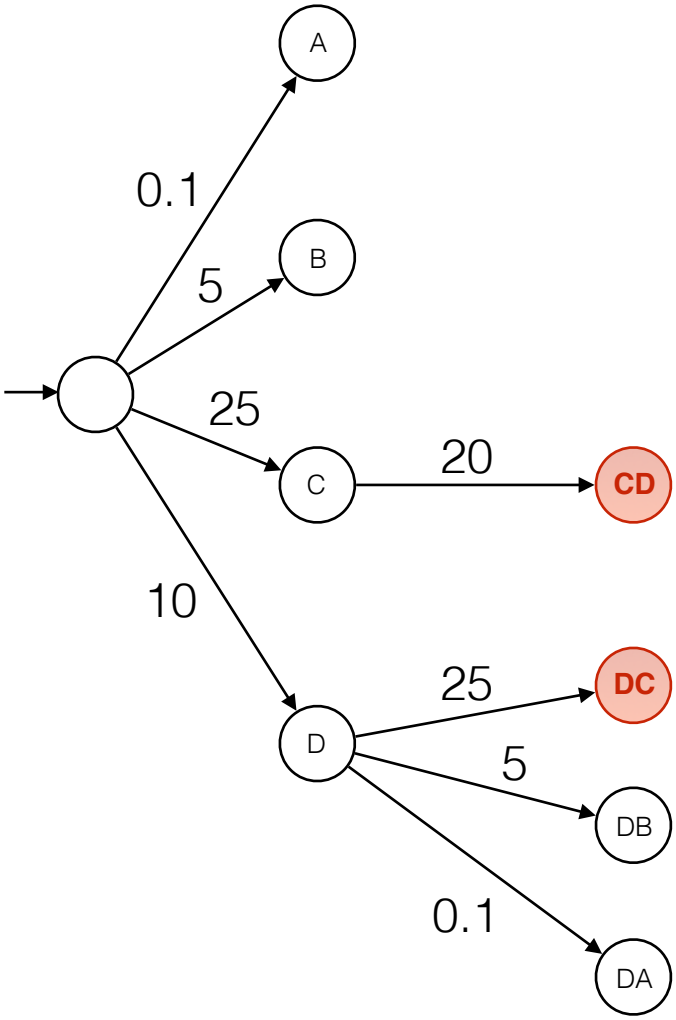

- **Over approximation:**
  - complete failure only if all remaining BEs have failed





# Approximation algorithm

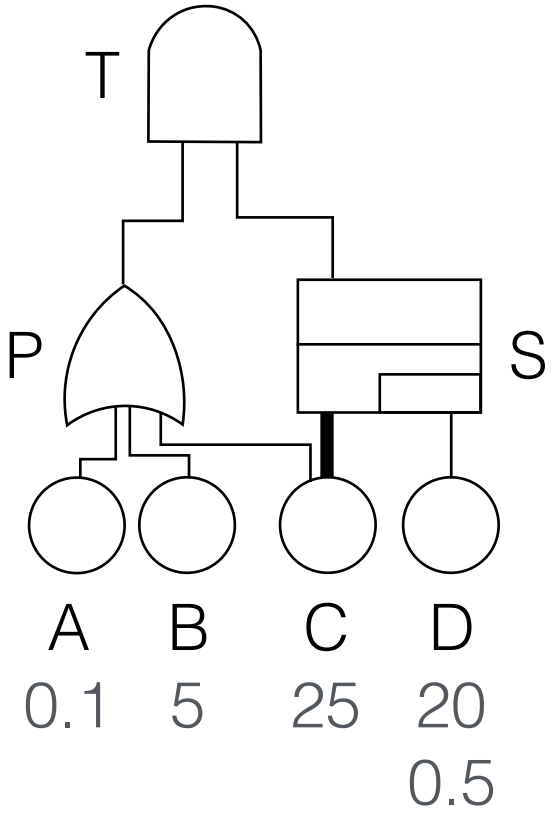


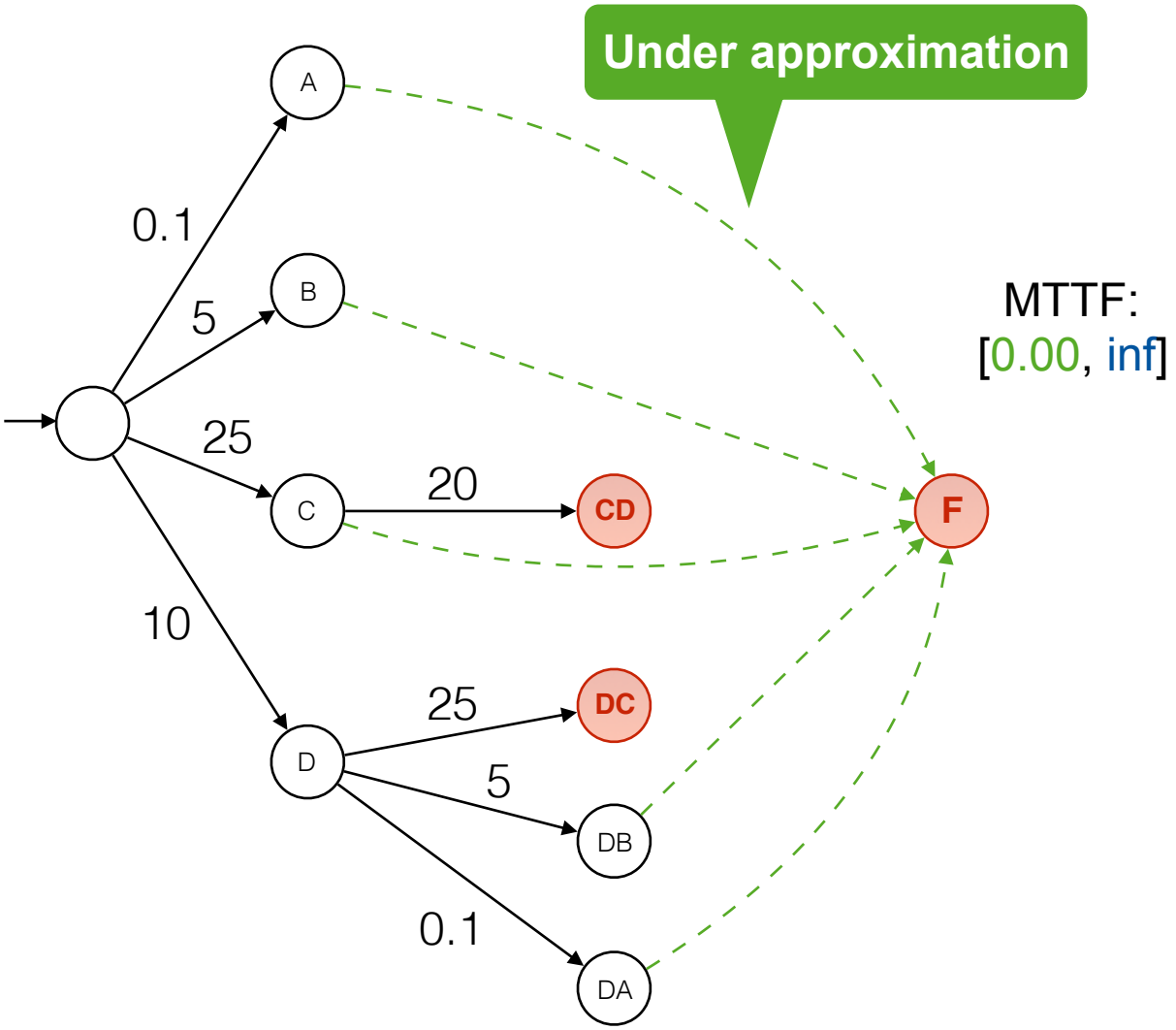




MTTF:
[0.00, inf]

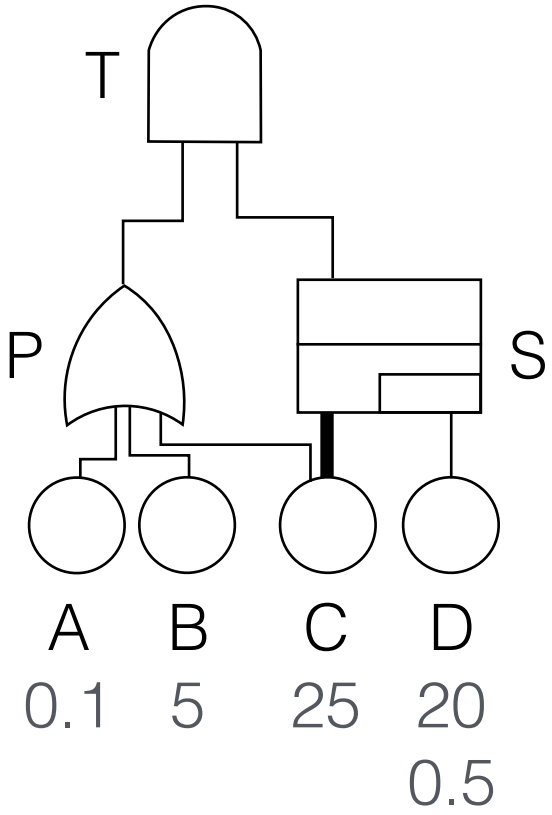
F

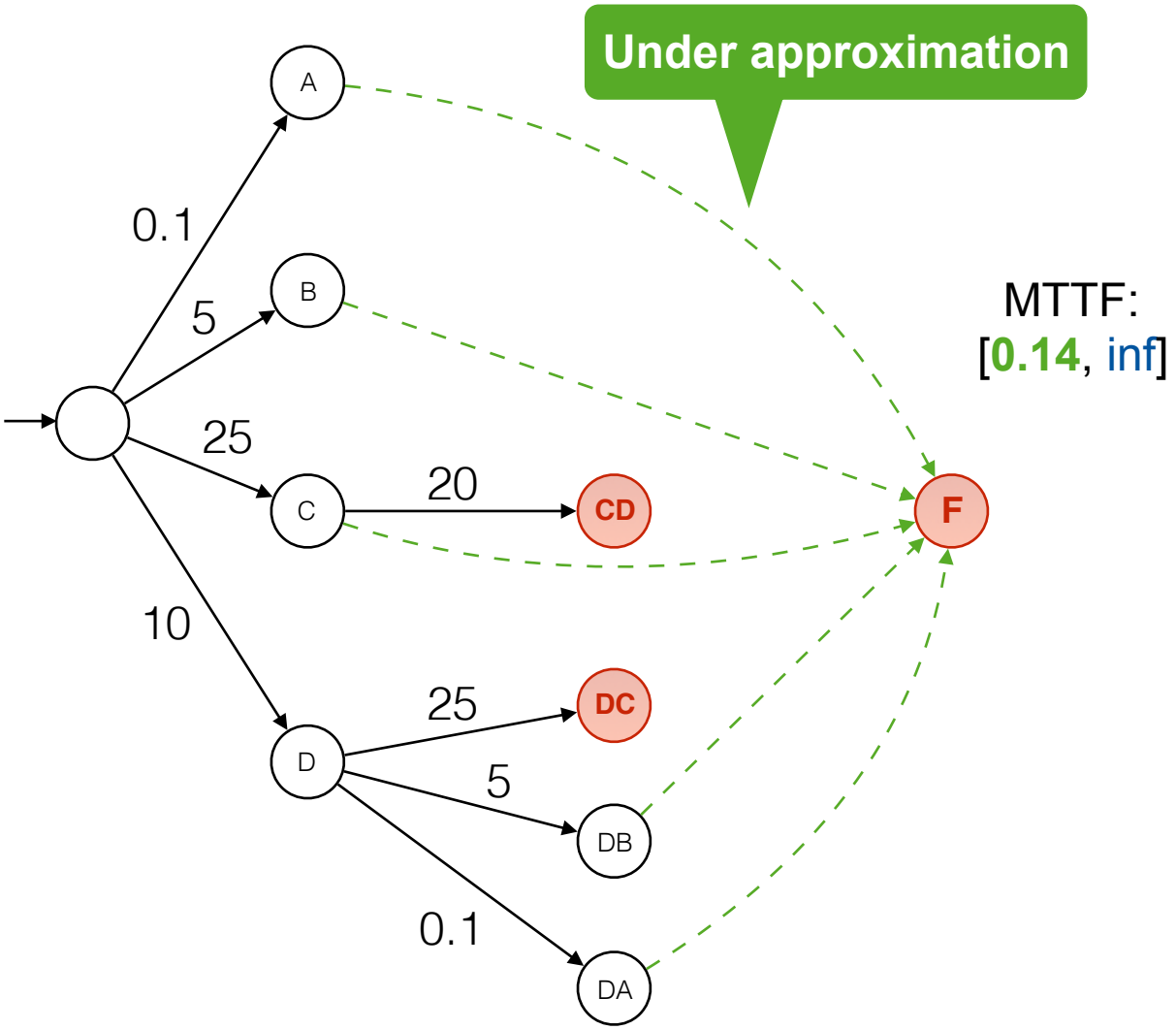
# Approximation algorithm



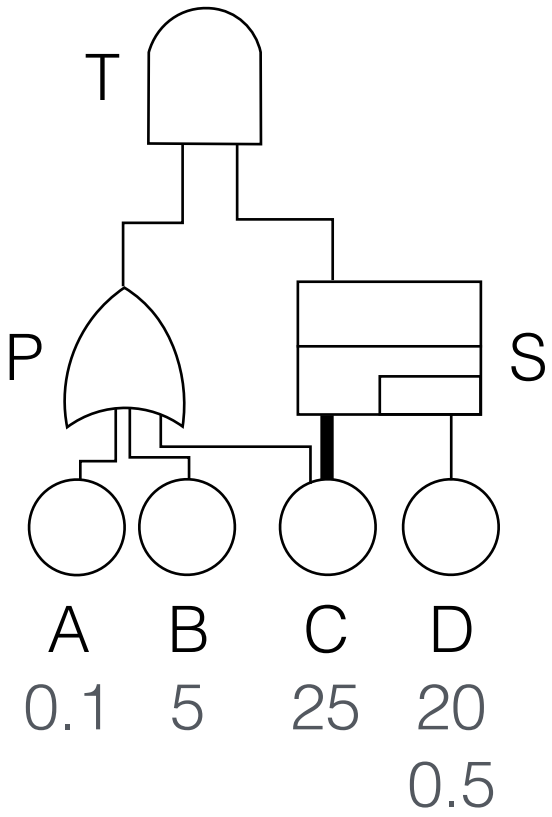



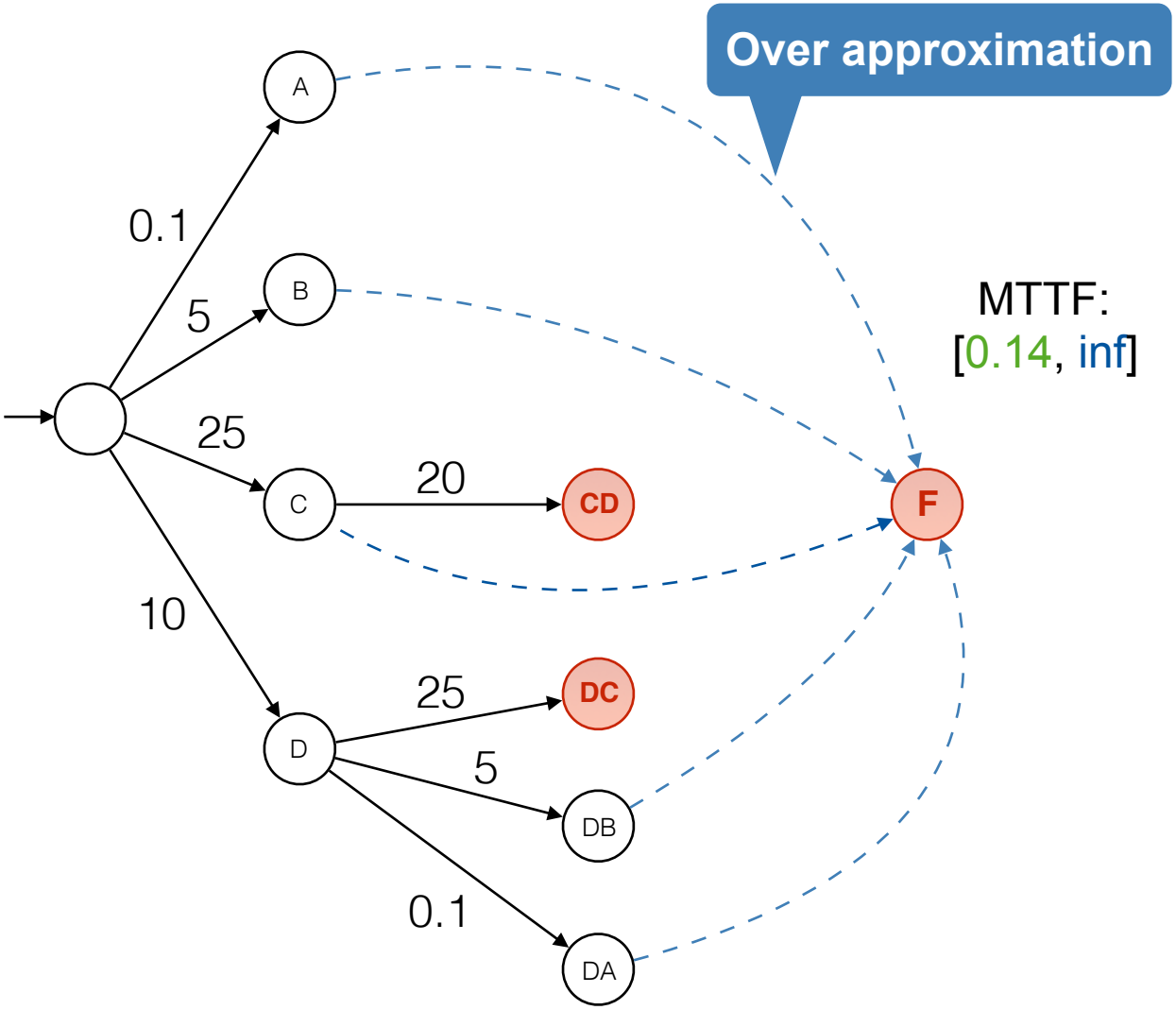
# Approximation algorithm



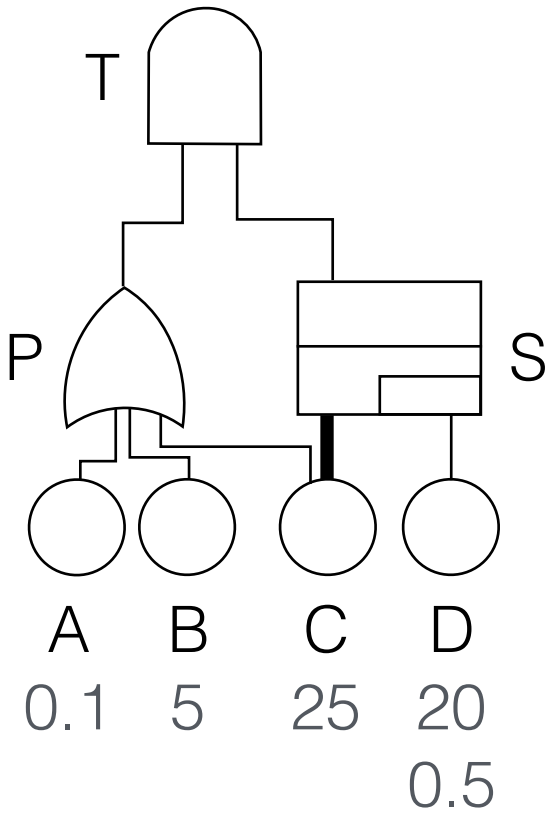



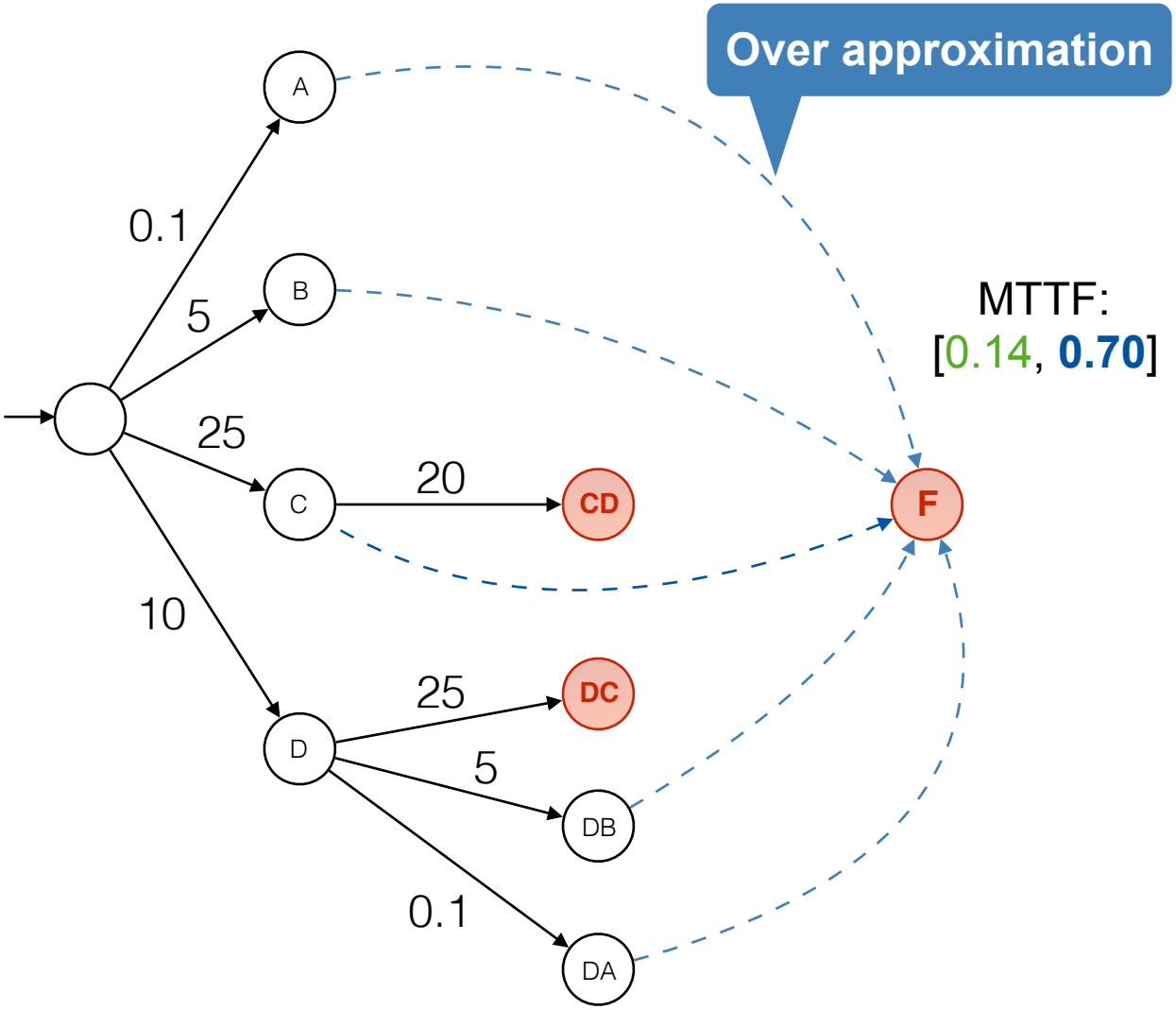
# Approximation algorithm



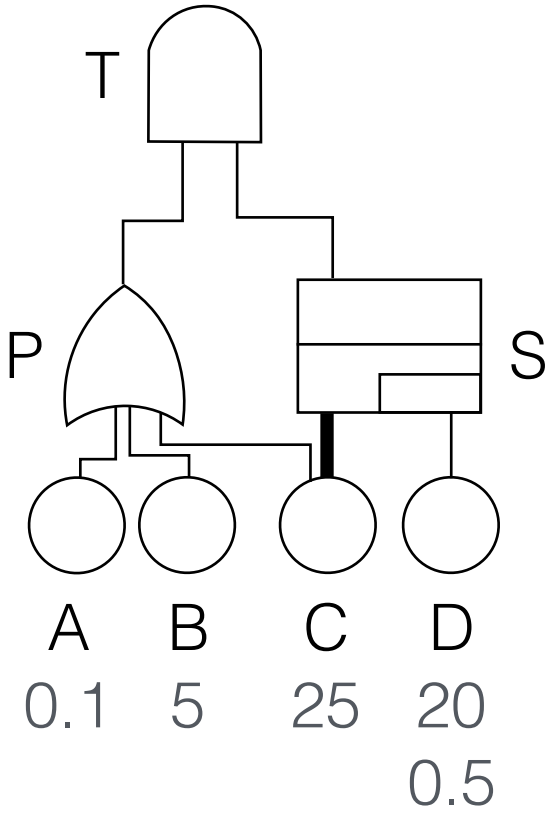



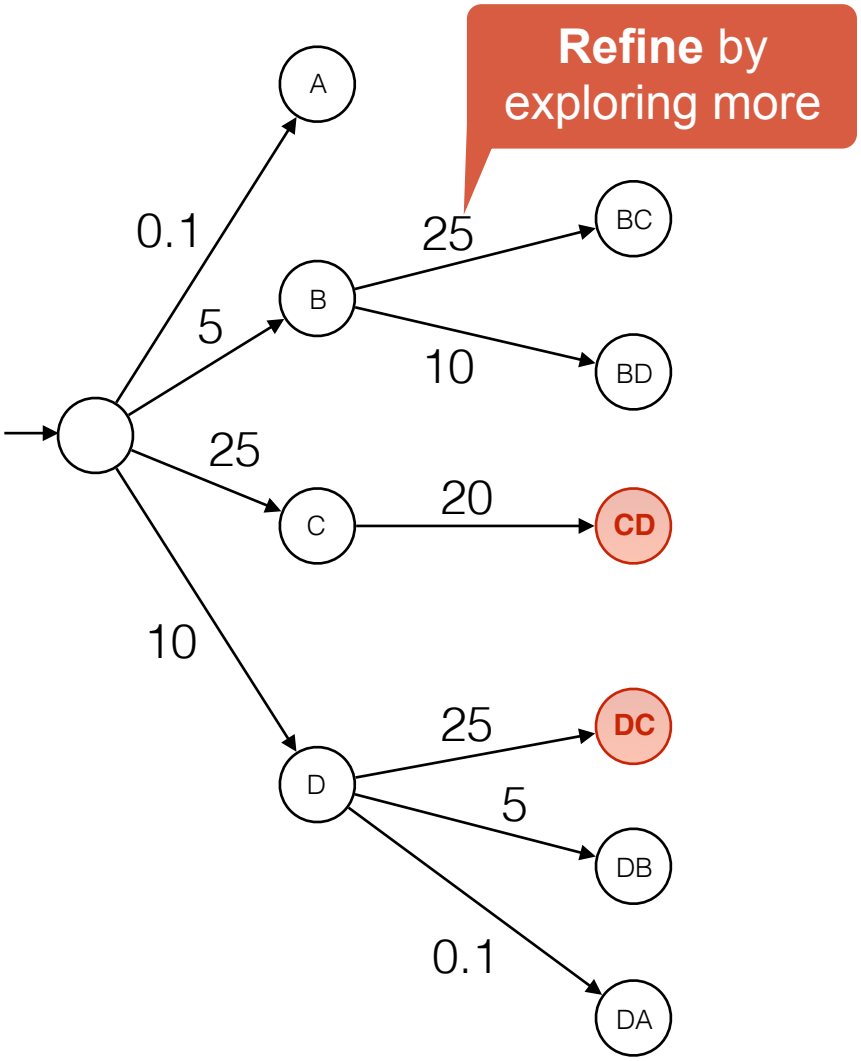
# Approximation algorithm



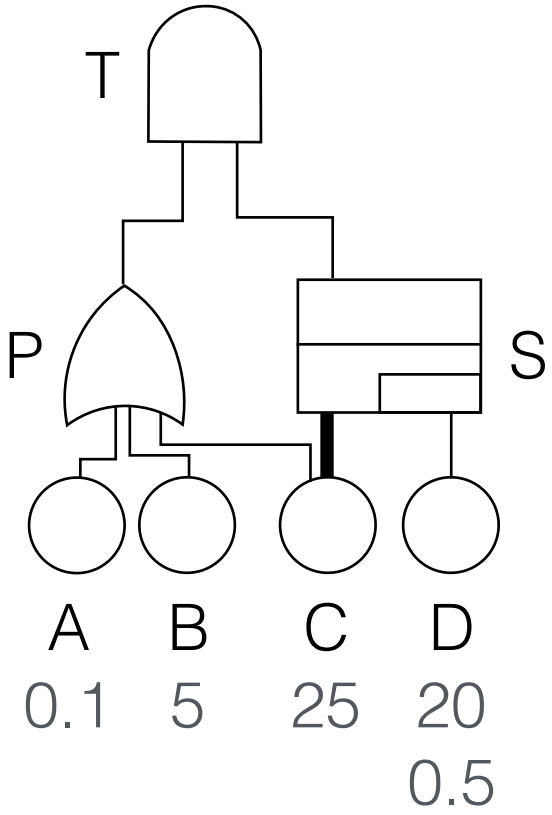
# Approximation algorithm

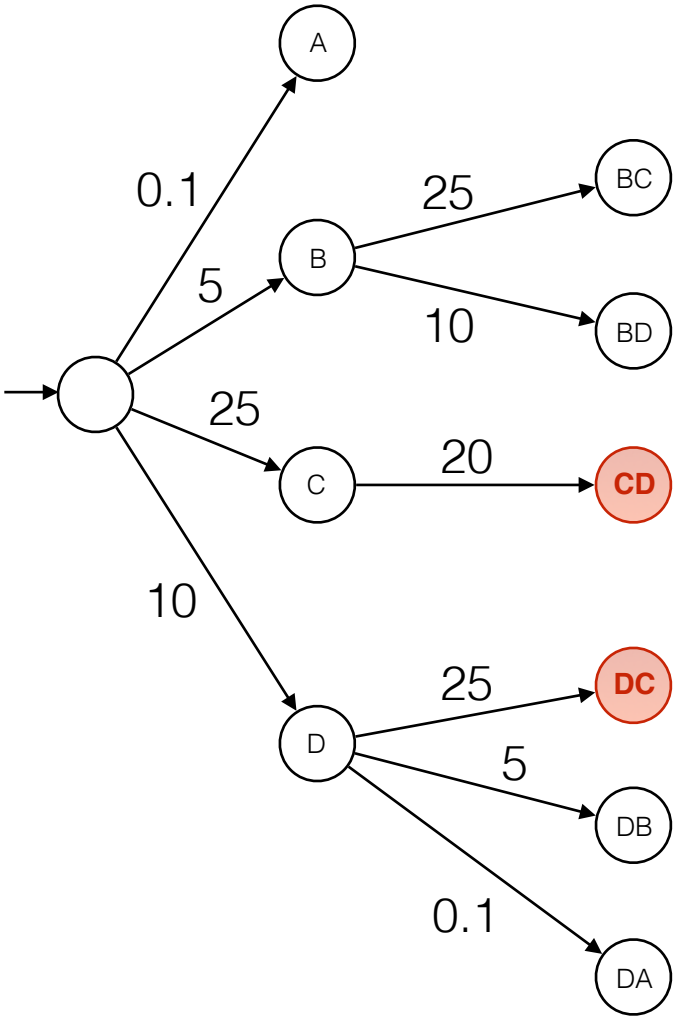



MTTF:
[0.14, 0.70]

# Approximation algorithm



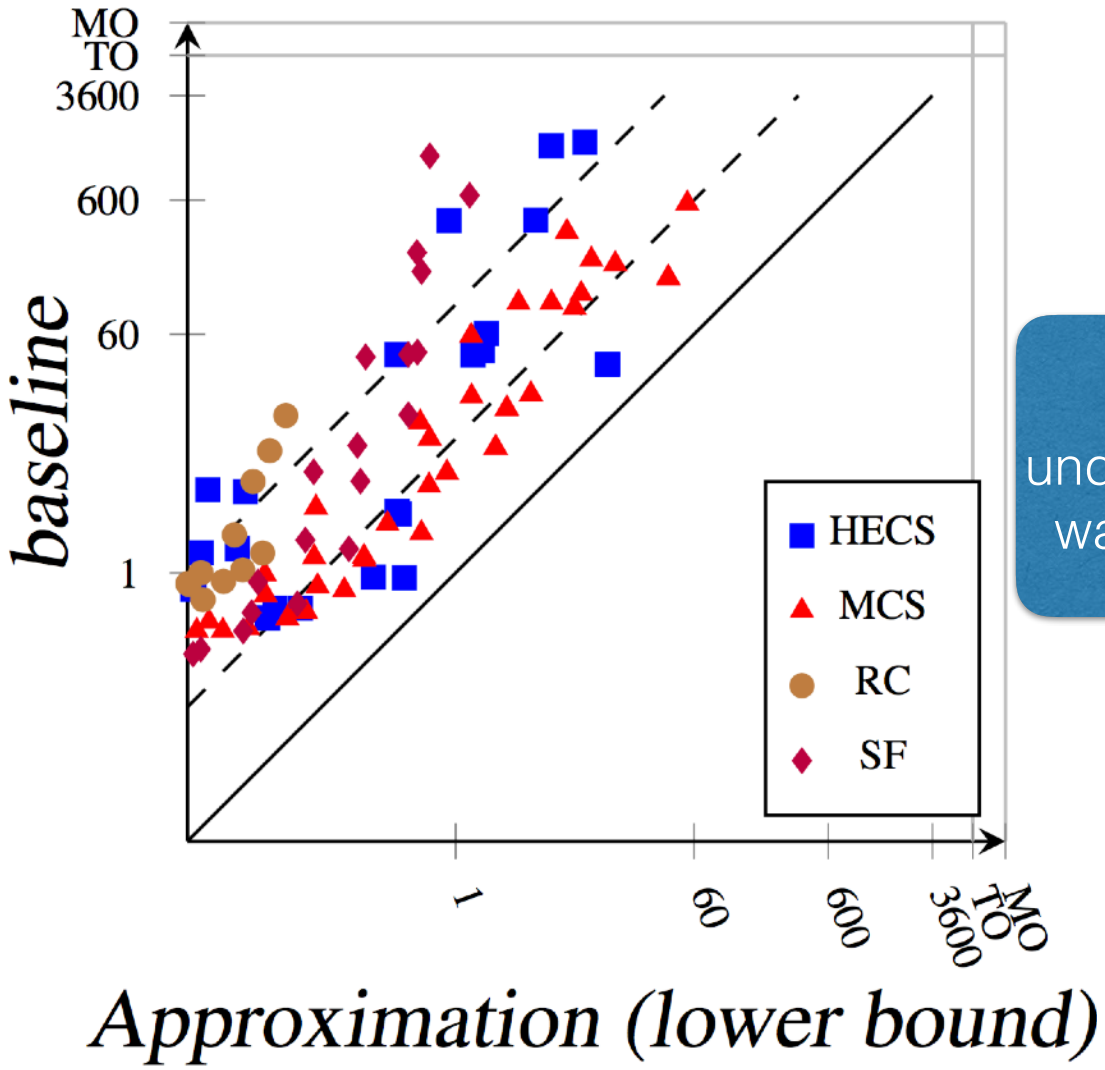

**Stop if precision suffices**

MTTF:
[0.27, 0.28]

F

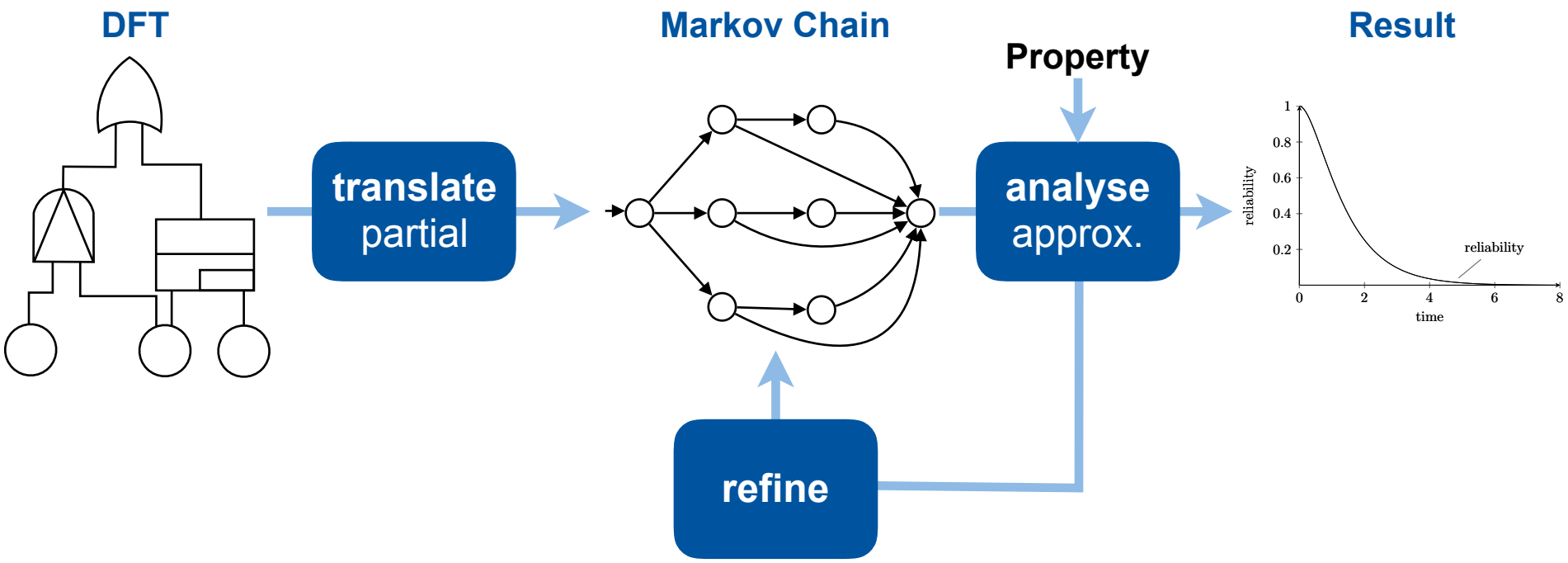
# Evaluation: run times

[Volk, Junges, Katoen, IEEE TII 2018]

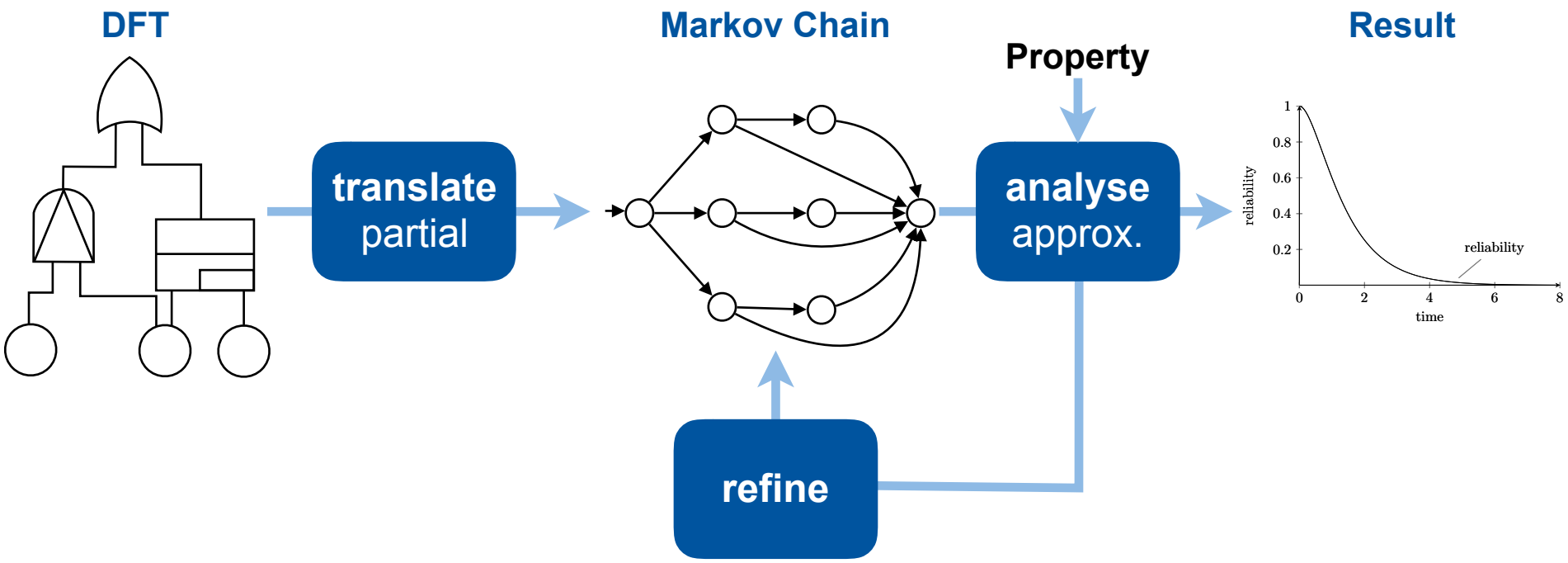



Time until under approximation was **95% of MTTF**

# Summary


DFT
translate
partial
Markov Chain
Property
analyse
approx.
Result
refine
reliability
time
reliability
1
0.8
0.6
0.4
0.2
0
2
4
6
8

# Summary




Storm

http://www.stormchecker.org