Acyclic Phase-Type Distributions in Fault Trees

Pepijn Crouzen — Reza Pulungan

Dept. of Computer Science
Saarland University
Germany

Jurusan Ilmu Komputer
Universitas Gadjah Mada
Indonesia

The 9th International Workshop on Performability Modeling of Computer and Communication Systems

Reliability analysis

What is the likelihood of *system failure*?

given

the likelihood of *component failure*?

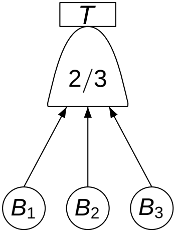
Reliability analysis

What is the likelihood of *system failure*?
given
the likelihood of *component failure*?

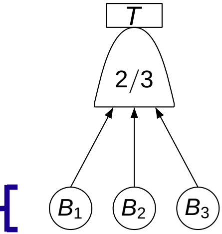
Outline

1. Theory
   - Fault Trees
   - Phase-Type distributions
2. Practice
   - Dynamic Fault Trees
   - Case study
3. Conclusion

Fault Trees - from component failure to system failure



Fault Trees - from component failure to system failure



Basic events

'Component Failure'

Failure probability is given

Fault Trees - from component failure to system failure

Gate

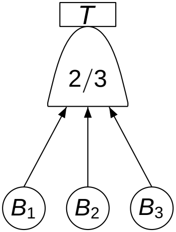
'T occurs after 2 of B_1, B_2, B_3 occur'

'T fails after 2 of its 3 subcomponents fail'

Basic events

'Component Failure'

Failure probability is given



Fault Trees - from component failure to system failure

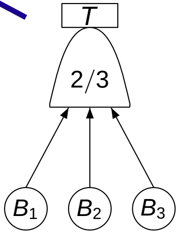
Top Event

'System Failure'

Gate

'T occurs after 2 of B_1, B_2, B_3 occur'

'T fails after 2 of its 3 subcomponents fail'



Basic events

'Component Failure'

Failure probability is given

Fault Trees - from component failure to system failure

Top Event

‘System Failure’

Gate

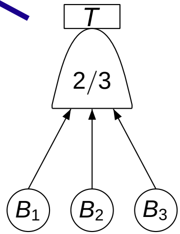
‘T occurs after 2 of B_1, B_2, B_3 occur’

‘T fails after 2 of its 3 subcomponents fail’

Basic events

‘Component Failure’

Failure probability is given



But actually...

A Fault Tree is a Boolean Function

Some terminology

- The state of the basic events is a random boolean vector $\vec{B} = (B_1, \ldots, B_n)$,
- The fault tree is a function f from $\{0,1\}^n$ to $\{0,1\}$. And now,

$$P(T = 1) = P(f(\vec{B}) = 1).$$

- This problem can be solved efficiently with binary decision diagrams.
- We only consider *coherent* fault trees where events are irrevocable.

Truth table of f

B_1	B_2	B_3	T
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	1

A Fault Tree is a Boolean Function

Some terminology

- The state of the basic events is a random boolean vector $\vec{B} = (B_1, \ldots, B_n)$,
- The fault tree is a function f from $\{0,1\}^n$ to $\{0,1\}$. And now,

$$P(T = 1) = P(f(\vec{B}) = 1).$$

- This problem can be solved efficiently with binary decision diagrams.
- We only consider *coherent* fault trees where events are irrevocable.

Truth table of f

B_1	B_2	B_3	T
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	1

Fault Trees with Time

Adding Time...

- State of BEs at time t is a stochastic process $\vec{B}^{(t)} = (B_1^{(t)}, \ldots, B_n^{(t)})$,
- $P(B_1^{(t)} = 1)$ is the probability that event B_1 has occurred on or before time-point t, and
- Again we have

$$P(T^{(t)} = 1) = P(f(\vec{B}^{(t)}) = 1).$$

But now:

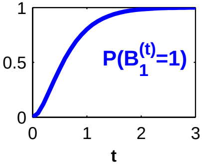
How do we represent the distribution of basic events and the top event?

Fault Trees with Time

Adding Time...

- State of BEs at time t is a stochastic process $\vec{B}^{(t)} = (B_1^{(t)}, \ldots, B_n^{(t)})$,
- $P(B_1^{(t)} = 1)$ is the probability that event B_1 has occurred on or before time-point t, and
- Again we have

$$P(T^{(t)} = 1) = P(f(\vec{B}^{(t)}) = 1).$$



But now:

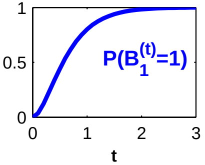
How do we represent the distribution of basic events and the top event?

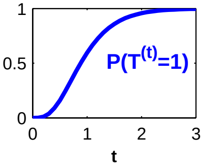
Fault Trees with Time

Adding Time...

- State of BEs at time t is a stochastic process $\vec{B}^{(t)} = (B_1^{(t)}, \ldots, B_n^{(t)})$,
- $P(B_1^{(t)} = 1)$ is the probability that event B_1 has occurred on or before time-point t, and
- Again we have

$$P(T^{(t)} = 1) = P(f(\vec{B}^{(t)}) = 1).$$





But now:

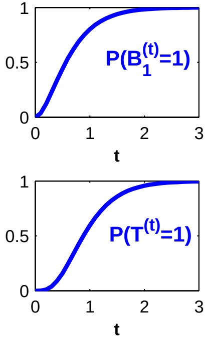
How do we represent the distribution of basic events and the top event?

Fault Trees with Time

Adding Time...

- State of BEs at time t is a stochastic process $\vec{B}^{(t)} = (B_1^{(t)}, \ldots, B_n^{(t)})$,
- $P(B_1^{(t)} = 1)$ is the probability that event B_1 has occurred on or before time-point t, and
- Again we have

$$P(T^{(t)} = 1) = P(f(\vec{B}^{(t)}) = 1).$$



But now:

How do we represent the distribution of basic events and the top event?

PH distribution overview

Properties

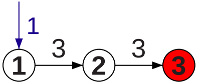
- A PH-distribution is represented by a CTMC with a single absorbing state,
- Matrix characterization,
- For a random variable Z PH-distributed with representation X we have,

$$P(Z \leq t) = P(X^{(t)} = 3) = \vec{\alpha} e^{Qt} \vec{\omega}.$$

- Infinitely many different representations,
- Acyclic PH-distributions (APH),
- For FTs:

$$P(B_1^{(t)} = 1) = P(X^{(t)} = 3).$$

X



PH distribution overview

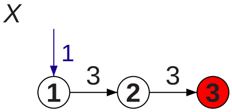
Properties

- A PH-distribution is represented by a CTMC with a single absorbing state,
- Matrix characterization,
- For a random variable Z PH-distributed with representation X we have,

$$P(Z \leq t) = P(X^{(t)} = 3) = \vec{\alpha} e^{Qt} \vec{\omega}.$$

- Infinitely many different representations,
- Acyclic PH-distributions (APH),
- For FTs:

$$P(B_1^{(t)} = 1) = P(X^{(t)} = 3).$$



$$\vec{\alpha} = (1, 0, 0)\,, \ \mathbf{Q} = \begin{pmatrix} -3 & 3 & 0 \\ 0 & -3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

PH distribution overview

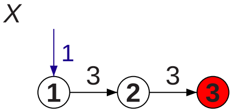
Properties

- A PH-distribution is represented by a CTMC with a single absorbing state,
- Matrix characterization,
- For a random variable Z PH-distributed with representation X we have,

$$P(Z \leq t) = P(X^{(t)} = 3) = \vec{\alpha} e^{Qt} \vec{\omega}.$$

- Infinitely many different representations,
- Acyclic PH-distributions (APH),
- For FTs:

$$P(B_1^{(t)} = 1) = P(X^{(t)} = 3).$$



$$\vec{\alpha} = (1, 0, 0)\,,\ \mathbf{Q} = \begin{pmatrix} -3 & 3 & 0 \\ 0 & -3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

PH distribution overview

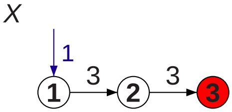
Properties

- A PH-distribution is represented by a CTMC with a single absorbing state,
- Matrix characterization,
- For a random variable Z PH-distributed with representation X we have,

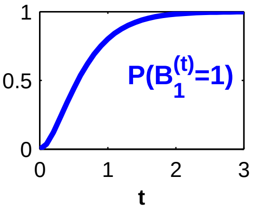
$$P(Z \leq t) = P(X^{(t)} = 3) = \vec{\alpha} e^{Qt} \vec{\omega}.$$

- Infinitely many different representations,
- Acyclic PH-distributions (APH),
- For FTs:

$$P(B_1^{(t)} = 1) = P(X^{(t)} = 3).$$



$$\vec{\alpha} = (1, 0, 0)\ ,\ \mathbf{Q} = \begin{pmatrix} -3 & 3 & 0 \\ 0 & -3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$



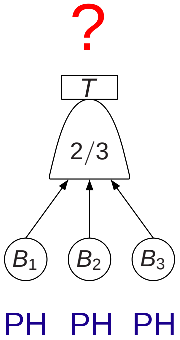
FT and PH

Theorem

The top event of a coherent fault tree with PH-distributed basic events is itself PH-distributed.

Corollary

The top event of a coherent fault tree with APH-distributed basic events is itself APH-distributed.



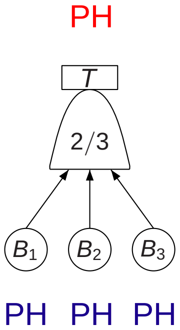
FT and PH

Theorem

The top event of a coherent fault tree with PH-distributed basic events is itself PH-distributed.

Corollary

The top event of a coherent fault tree with APH-distributed basic events is itself APH-distributed.



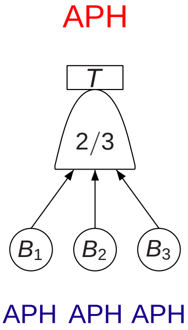
FT and PH

Theorem

The top event of a coherent fault tree with PH-distributed basic events is itself PH-distributed.

Corollary

The top event of a coherent fault tree with APH-distributed basic events is itself APH-distributed.

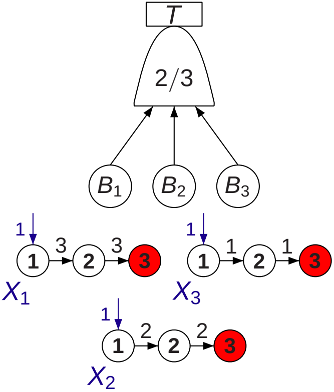


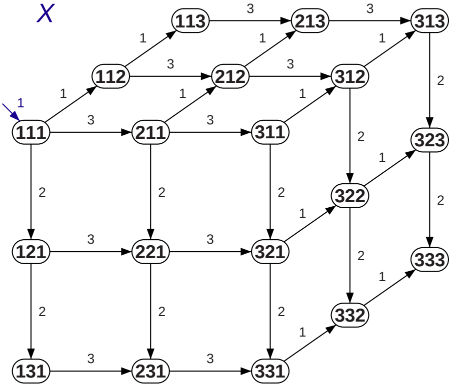
Proof by Construction

Constructing a representation for the top event

- For a coherent FT with n basic events,
- Parallel composition of representations: X
  Initial distribution $\vec{\alpha} = \vec{\alpha}_1 \otimes \ldots \otimes \vec{\alpha}_n$
  Generator matrix $\mathbf{Q} = \mathbf{Q}_1 \oplus \ldots \oplus \mathbf{Q}_n$.
- Mark occurrence of basic events. Per state a boolean vector $\vec{b} \in \{0, 1\}^n$,
- Group states by $f(\vec{b})$: Two sets S_0 and S_1,
- Collapse S_1 to a single state (Note: S_1 is absorbing),
- The resulting CTMC Y represents the PH distribution of the top event of the FT.

Construction example: parallel composition

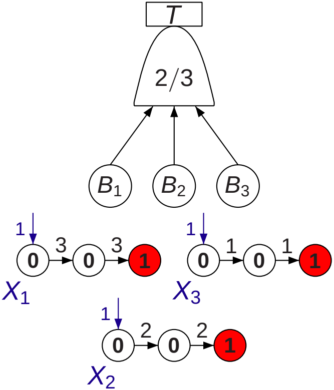


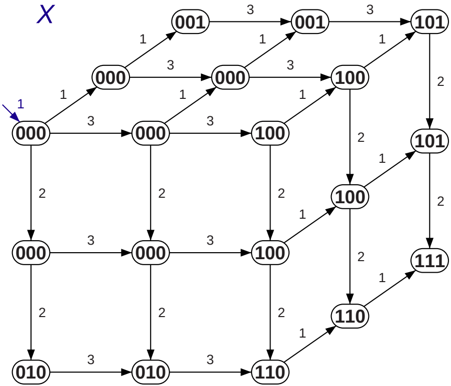


The connection

$$P(X_1^{(t)} = 3 \wedge X_2^{(t)} = 1 \wedge X_3^{(t)} = 2) = P(X^{(t)} = 312)$$

Construction examples: From states to events



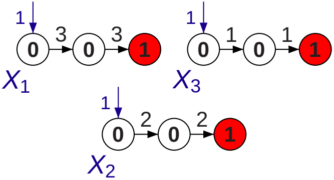


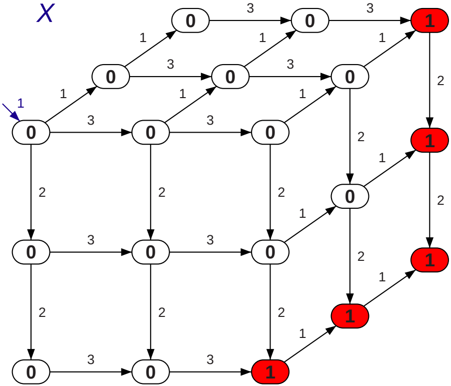
The connection

$$P(\vec{B}^{(t)} = (100)) = P(X_1^{(t)} \in S_1 \wedge X_2^{(t)} \in S_0 \wedge X_3^{(t)} \in S_0) = P(X^{(t)} \in S_{100})$$

Construction: Apply function f

B_1	B_2	B_3	T
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	1



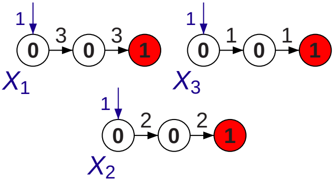


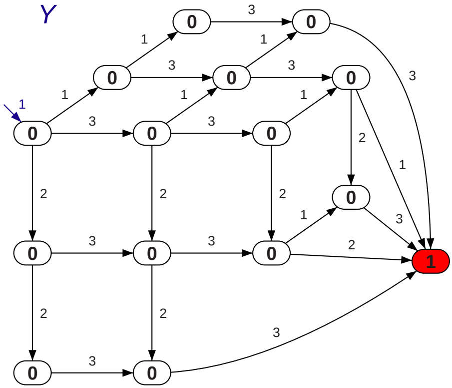
The connection

$$P(T^{(t)} = 1) = P(f(\vec{B}^{(t)}) = 1) = P(X^{(t)} \in S_1)$$

Construction: Collapse set ‘1’

B_1	B_2	B_3	T
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	1





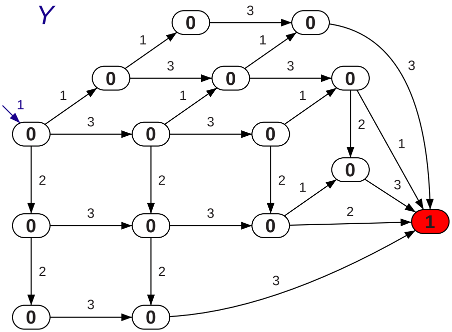
The connection

$$P(T^{(t)} = 1) = P(X^{(t)} \in S_1) = P(Y^{(t)} = 1)$$

Minimal Representation for APH

A better representation

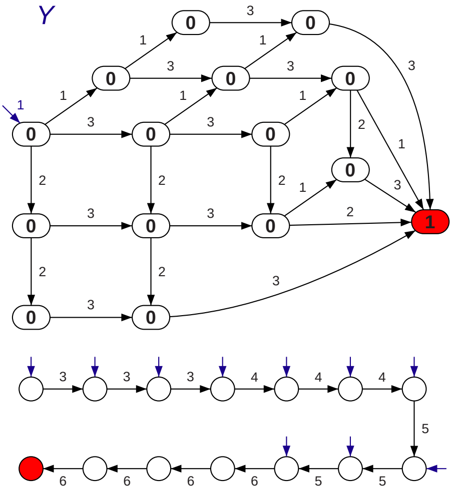
- Y has 21 states and 45 transitions,
- Smallest representation: 14 states and 13 transitions,
- For APH: find smallest representation with APHMIN.



Minimal Representation for APH

A better representation

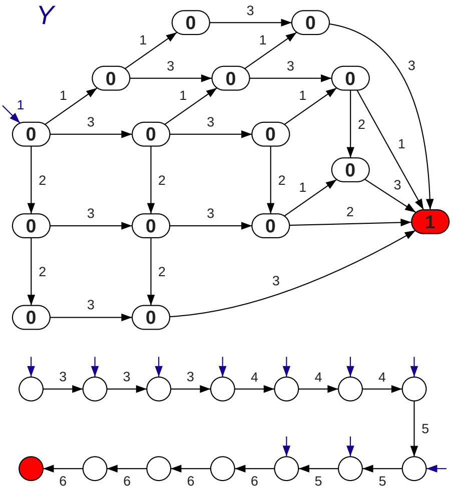
- Y has 21 states and 45 transitions,
- Smallest representation: 14 states and 13 transitions,
- For APH: find smallest representation with APHMIN.



Minimal Representation for APH

A better representation

- Y has 21 states and 45 transitions,
- Smallest representation: 14 states and 13 transitions,
- For APH: find smallest representation with APHMIN.



APHMIN Sketch

Computing the 'minimal' representation

1. Convert the APH representation to bidiagonal form,
2. Consider the Laplace-Stieltjens transform,
3. For each state:
    1. Check for states that are linear combinations of other states,
    2. Compute a new initial 'distribution',
    3. Check if the new initial 'distribution' is a distribution.

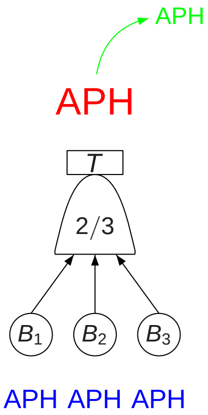
So far

We have seen...

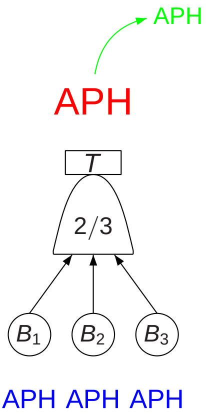
- Describe BEs with APH distributions,
- Top event is also APH distributed, and
- APH representations can be minimized.

But...

- Solving a FT is anyway easy!
- Perhaps FTs are too simple...



So far



We have seen...

- Describe BEs with APH distributions,
- Top event is also APH distributed, and
- APH representations can be minimized.

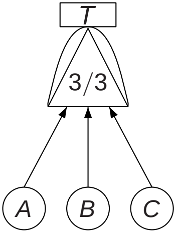
But...

- Solving a FT is anyway easy!
- Perhaps FTs are too simple...

Bringing order to FTs

Dynamic Fault Trees

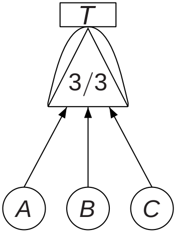
- Adds three gates to FTs,
- Example: T only occurs if A, B and C happen in the correct order,
- A DFT is not a boolean function!
- We must construct a representation of the distribution of event T.
- FT construction does not work.



Bringing order to FTs

Dynamic Fault Trees

- Adds three gates to FTs,
- Example: T only occurs if A, B and C happen in the correct order,
- A DFT is not a boolean function!
- We must construct a representation of the distribution of event T.
- FT construction does not work.

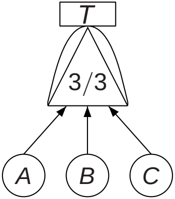


Compositional Aggregation

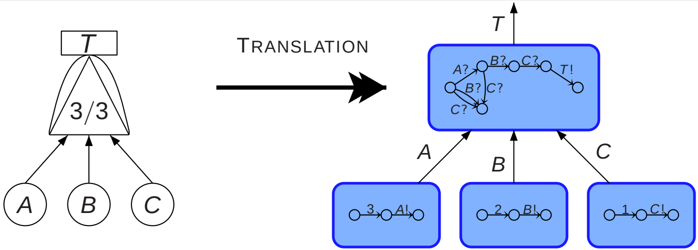
Generating the state space step by step

1. Translate syntactic elements to interactive models,
2. Select a subset of interactive models,
3. Compose them,
4. Minimize the result,
5. More than one model left: goto 2.

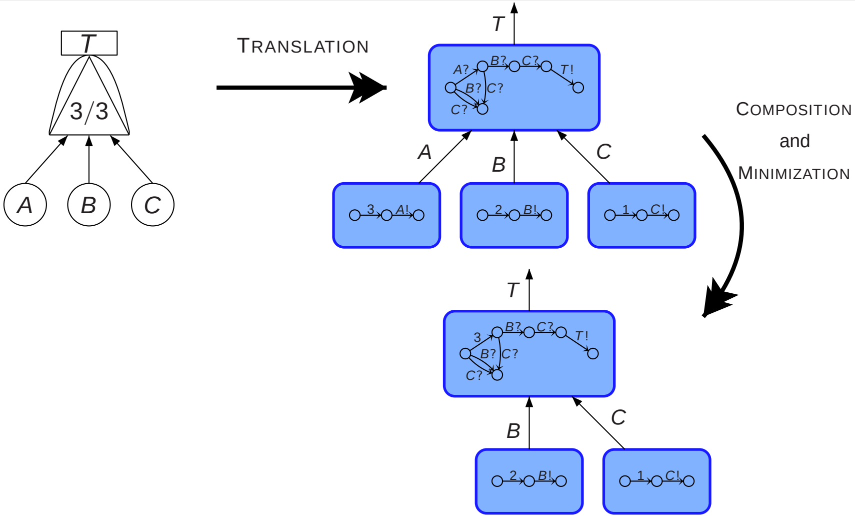
Constructing CTMC with CORAL



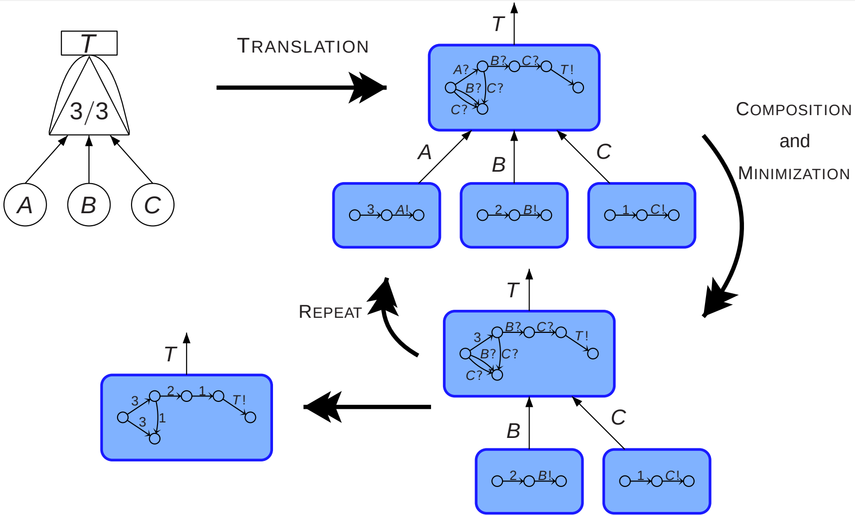
Constructing CTMC with CORAL



Constructing CTMC with CORAL

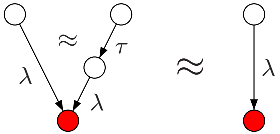


Constructing CTMC with CORAL



How to minimize?

Weak bisimulation

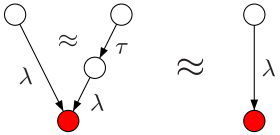


Properties

- Equality = same observable transitions,
- Eliminate equivalent states,
- For CTMCs and IOIMCs,
- Partition refinement algorithm.

How to minimize?

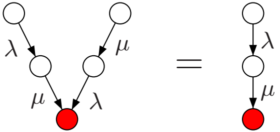
Weak bisimulation



Properties

- Equality = same observable transitions,
- Eliminate equivalent states,
- For CTMCs and IOIMCs,
- Partition refinement algorithm.

APHMIN



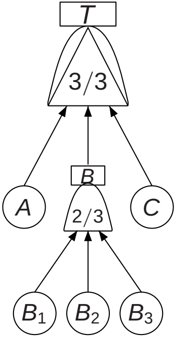
Properties

- Considers Laplace-Stieltjes transform,
- Eliminate states that are linear combinations of other states,
- For APH representations,
- Weaker than weak!

Improving Compositional Aggregation

Which minimization?

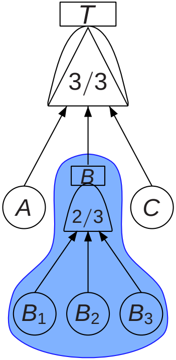
- Compositional aggregation uses minimization,
- For DFTs: weak bisimulation minimization,
- Can we use APHMIN instead?
- For FT-subtrees we can!
- 14 states instead of 21 states.



Improving Compositional Aggregation

Which minimization?

- Compositional aggregation uses minimization,
- For DFTs: weak bisimulation minimization,
- Can we use APHMIN instead?
- For FT-subtrees we can!
- 14 states instead of 21 states.



Case Study

Case Study

- FTPP case study (20 basic events, 21 gates),
- Three variants with 1,2, or 3 FT subtrees,
- Compare normal CA (CORAL) with enhanced CA (APHMIN),
- For FT subtrees: 21 states (CORAL) vs. 14 states (APHMIN).

#	Tool	States	Transitions	Time (s)	Unreliability
1	CORAL	1,672	12,303	10.37	$1.13 \cdot 10^{-7}$
	APHMIN	1,119	7,410	10.42	$1.13 \cdot 10^{-7}$
2	CORAL	59,739	598,524	24.52	$3.21 \cdot 10^{-4}$
	APHMIN	26,006	219,310	14.14	$3.21 \cdot 10^{-4}$
3	CORAL	1,777,955	21,895,068	14,047.99	0.209
	APHMIN	507,067	5,010,000	367.71	0.209

Case Study

Case Study

- FTPP case study (20 basic events, 21 gates),
- Three variants with 1,2, or 3 FT subtrees,
- Compare normal CA (CORAL) with enhanced CA (APHMIN),
- For FT subtrees: 21 states (CORAL) vs. 14 states (APHMIN).

#	Tool	States	Transitions	Time (s)	Unreliability
1	CORAL	1,672	12,303	10.37	$1.13 \cdot 10^{-7}$
	APHMIN	1,119	7,410	10.42	$1.13 \cdot 10^{-7}$
2	CORAL	59,739	598,524	24.52	$3.21 \cdot 10^{-4}$
	APHMIN	26,006	219,310	14.14	$3.21 \cdot 10^{-4}$
3	CORAL	1,777,955	21,895,068	14,047.99	0.209
	APHMIN	507,067	5,010,000	367.71	0.209

Conclusion

We have seen...

- Describe BEs with APH distributions,
- Top event is also APH distributed,
- APH representations can be minimized, and
- APHMIN can be effectively used in compositional aggregation.

Future work

- Fully integrate APHMIN into CORAL,
- Identify dynamic fault trees that are APH distributed,
- Prove a conjecture about almost-sure minimality,
- Find APH-like structures in other Markovian models.

Conclusion

We have seen...

- Describe BEs with APH distributions,
- Top event is also APH distributed,
- APH representations can be minimized, and
- APHMIN can be effectively used in compositional aggregation.

Future work

- Fully integrate APHMIN into CORAL,
- Identify dynamic fault trees that are APH distributed,
- Prove a conjecture about almost-sure minimality,
- Find APH-like structures in other Markovian models.

References

Fault Trees:

- W.E. Vesely, F.F. Goldberg, N.H. Roberts and D.F. Haasl, *Fault Tree Handbook*. United States Nuclear Regulatory Commision, 1981, vol. (NUREG-0492).

Phase-Type Distributions:

- M.F. Neuts, *Matrix-Geometric Solutions in Stochastic Models: An Algorithmic Approach*. Dover, 1981.
- R. Pulungan and H. Hermanns, "Acyclic minimality by construction–almost," in *Fifth International Conference on the Quantitative Evaluation of Systems (QEST 2009)*. IEEE Computer Society, 2009.

Dynamic Fault Trees:

- J.B. Dugan, S.J. Bavuso, and M.A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," in *IEEE Transactions on Reliability*, vol. 41, no. 3, pp. 363–377, 1992.
- H. Boudali, P. Crouzen, and M. Stoelinga, "A compositional semantics for Dynamic Fault Trees in terms of Interactive Markov Chains," in *Proceedings of the 5th International Symposium on Automated Technology for Verification and Analysis*, pp 441–456, 2007.