# A Verified Realization of a Dempster-Shafer-Based Fault Tree Analysis

Ekaterina Auer, Wolfram Luther, **Gabor Rebner**

Department of Computer and Cognitive Sciences (INKO)
University of Duisburg-Essen
Duisburg, Germany

# Table of Contents

# Motivation

Integrate verified Dempster-Shafer Theory in Fault tree analysis by using MATLAB and INTLAB[1]

## Issues

1. Use of intervals to express uncertainties in evidences
2. Computation of the verified upper bound of failure probability
3. New approach in Fault tree analysis
4. Fast evaluation of Dempster-Shafer-Functions

[1] http://www.ti3.tu-harburg.de/~rump/intlab/

# Motivation

Integrate verified Dempster-Shafer Theory in Fault tree analysis by using MATLAB and INTLAB[1]

## Issues

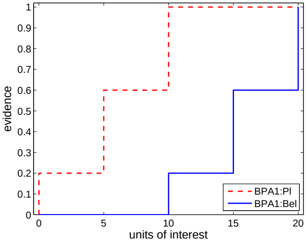
1. Use of intervals to express uncertainties in evidences
2. Computation of the verified upper bound of failure probability
3. New approach in Fault tree analysis
4. Fast evaluation of Dempster-Shafer-Functions

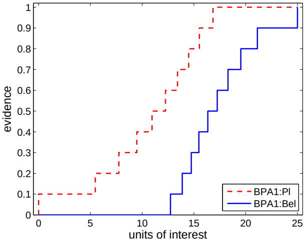
[1] http://www.ti3.tu-harburg.de/~rump/intlab/

# Motivation

## Uncertainties

- Lack of knowledge (failure probability is not available)
- Variations in system tests
- Different evidences by experts



# Dempster-Shafer Theory

Mathematical theory of evidence

Developed by A. Dempster and G. Shafer in 1976

## Features

- Uncertainty in evidence can be expressed as an interval
- Aggregation of evidence by different experts

# Introduction to DSI

## Fundamentals

$2^X$ is the power set of all probability assignments

# BPA

## Definition

Basic probability assignment (BPA) over all sets of interest $(A_1, \ldots, A_n)$

$$m : 2^{\widetilde{X}} \to [0,1]\,,\ \sum_{i=1}^{n} m(A_i) = 1,\ m(\emptyset) = 0,\ A_i \in 2^{\widetilde{X}}$$

In continuous case:

$$\boldsymbol{A}_i = \left[\underline{a_i}, \overline{a_i}\right]\,,\ -\infty < \underline{a_i} \leq \overline{a_i} < +\infty$$

# Solution Space

## Upper Bound

$$Pl(X) = \text{Plausibility}\left(X \in \widetilde{X}\right) = \sum_{A_i \cap X \neq \emptyset} m(A_i)$$

## Lower Bound

$$Bel(X) = \text{Belief}\left(X \in \widetilde{X}\right) = \sum_{A_i \subseteq X} m(A_i)$$

# Solution Space

## Upper Bound

$$Pl\left(X\right) = \text{Plausibility}\left(X \in \widetilde{X}\right) = \sum_{A_i \cap X \neq \emptyset} m\left(A_i\right)$$

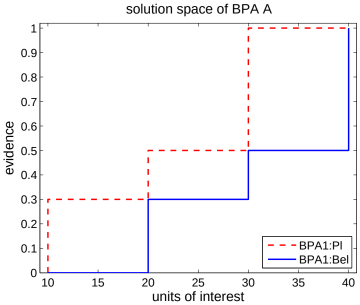
## Lower Bound

$$Bel\left(X\right) = \text{Belief}\left(X \in \widetilde{X}\right) = \sum_{A_i \subseteq X} m\left(A_i\right)$$

# Solution Space (Example)

**Example BPA**

$$\boldsymbol{A}_1 = [10, 20] \quad m(\boldsymbol{A}_1) = 0.3$$
$$\boldsymbol{A}_2 = [20, 30] \quad m(\boldsymbol{A}_2) = 0.2$$
$$\boldsymbol{A}_3 = [30, 40] \quad m(\boldsymbol{A}_3) = 0.5$$



# Dempster-Shafer with Intervals Toolbox

Implements verified Dempster-Shafer functions in MATLAB by using INTLAB

Based on the IPP-toolbox for R by P. Limbourg[2]

### Verified Computation

- Sampling of cumulative distribution functions
- Sampling of (non)monotonous system functions
- Monte Carlo sampling
- Aggregation of BPAs
- ...

[2] http://www.uni-due.de/il/ipptoolbox.php

# Dempster-Shafer with Intervals Toolbox

Implements verified Dempster-Shafer functions in MATLAB by using INTLAB

Based on the IPP-toolbox for R by P. Limbourg[2]

## Verified Computation

- Sampling of cumulative distribution functions
- Sampling of (non)monotonous system functions
- Monte Carlo sampling
- Aggregation of BPAs
- ...

[2] http://www.uni-due.de/il/ipptoolbox.php

# Dempster-Shafer with Intervals Toolbox

Implements verified Dempster-Shafer functions in MATLAB by using INTLAB

Based on the IPP-toolbox for R by P. Limbourg[2]

## Verified Computation

- Sampling of cumulative distribution functions
- Sampling of (non)monotonous system functions
- Monte Carlo sampling
- Aggregation of BPAs
- ...

[2] http://www.uni-due.de/il/ipptoolbox.php

# Verified Normalization

## Definition

- Let $\{\boxed{+}, \boxed{-}, \boxed{\cdot}, \boxed{/}\}$ be interval operations
- Let $\mathrm{fl}_\triangle$ and $\mathrm{fl}_\triangledown$ be upward and downward directed roundings

## Formula

$$\underline{m}(A_i)\boxed{/}\left(\mathrm{fl}_\triangle\left(\sum_{j=1}^{n}\underline{m}(A_j)\right)\right), \quad \overline{m}(A_i)\boxed{/}\left(\mathrm{fl}_\triangledown\left(\sum_{j=1}^{n}\overline{m}(A_j)\right)\right)$$

# Verified Normalization

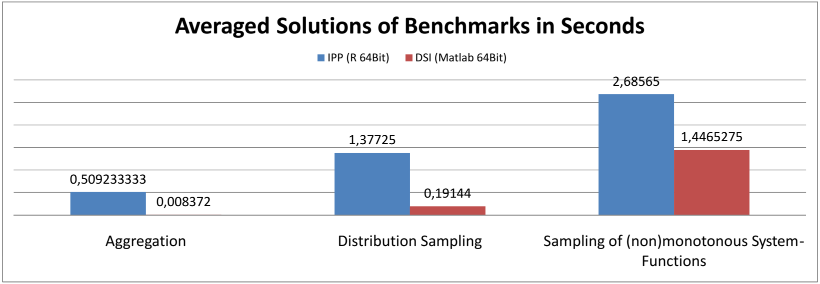
## Definition

- Let $\{\boxed{+}, \boxed{-}, \boxed{\cdot}, \boxed{/}\}$ be interval operations
- Let $\mathrm{fl}_\triangle$ and $\mathrm{fl}_\triangledown$ be upward and downward directed roundings

## Formula

$$\underline{m}(A_i)\boxed{/}\left(\mathrm{fl}_\triangle\left(\sum_{j=1}^{n}\underline{m}(A_j)\right)\right), \quad \overline{m}(A_i)\boxed{/}\left(\mathrm{fl}_\triangledown\left(\sum_{j=1}^{n}\overline{m}(A_j)\right)\right)$$

# Benchmarks


Averaged Solutions of Benchmarks in Seconds
IPP (R 64Bit)
DSI (Matlab 64Bit)
0,509233333
0,008372
1,37725
0,19144
2,68565
1,4465275
Aggregation
Distribution Sampling
Sampling of (non)monotonous System-Functions

# Comparison with IPP

## Comparison with IPP

1. Strict use of vector-matrix-operations (fast computation)
2. Verified computation (INTLAB)
3. Fault tree analysis
4. Fast sampling of (non)monotonous system functions

# Aim of Verified Fault Tree Analysis

## Main Objective

Computation of the biggest upper bound of failure probability

## Approach

1. Avoid limitations of floating-point numbers
   - Round-off errors
   - Approximation errors
2. Use of Dempster-Shafer Theory to express uncertainties
3. Use of INTLAB

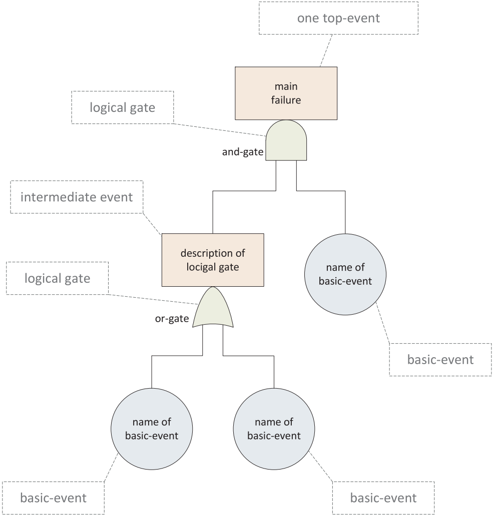
# Aim of Verified Fault Tree Analysis

## Main Objective

Computation of the biggest upper bound of failure probability

## Approach

1. Avoid limitations of floating-point numbers
   - Round-off errors
   - Approximation errors
2. Use of Dempster-Shafer Theory to express uncertainties
3. Use of INTLAB


one top-event
main
failure
logical gate
and-gate
intermediate event
description of
locigal gate
name of
basic-event
logical gate
or-gate
basic-event
name of
basic-event
name of
basic-event
basic-event
basic-event

# Basic Events

## Evidences

1. Only one evidence is given
2. More than one evidence is given
   - Aggregation is needed
   - Maybe loss of information

## Solution

Mixing based on arithmetic averaging

# Basic Events

## Evidences

1. Only one evidence is given
2. More than one evidence is given
    - Aggregation is needed
    - Maybe loss of information

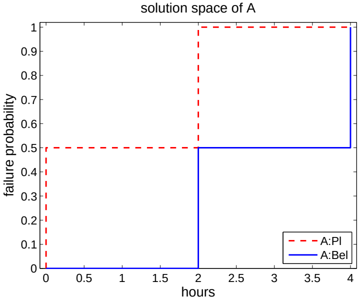
## Solution

Mixing based on arithmetic averaging

# Logical Gates Definitions

**Definition**

$$A_1 = [0,2] \quad m(A_1) = 0.5$$
$$A_2 = [2,4] \quad m(A_2) = 0.5$$



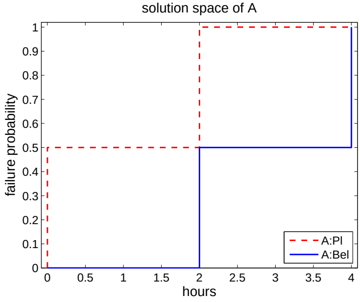
# Logical Gates (AND)

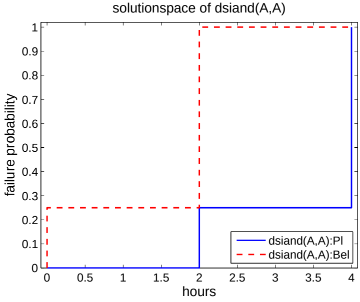
## AND-Gate

$C = A$ and $B = A \cap B$

$$C = A \cap B$$
$$PL(C) = PL(A) \cdot PL(B)$$
$$BEL(C) = BEL(A) \cdot BEL(B)$$

# AND-Gate (Example)



# OR-Gate

## Formula

$$A \vee B = 1 - (1 - P(A)) \cdot (1 - P(B))$$

# OR-Gate - Meaning in DST

## Evaluation Or-Gate in DST

$$C_1 = A \cap B$$
$$C_2 = A \backslash B$$
$$C_3 = B \backslash A$$
$$PL(C_1) = 1 - (1 - PL(A)) \cdot (1 - PL(B))$$
$$BEL(C_1) = 1 - (1 - BEL(A)) \cdot (1 - BEL(B))$$
$$PL(C_2) = PL(A)$$
$$BEL(C_2) = BEL(A)$$
$$PL(C_3) = PL(B)$$
$$BEL(C_3) = BEL(B)$$

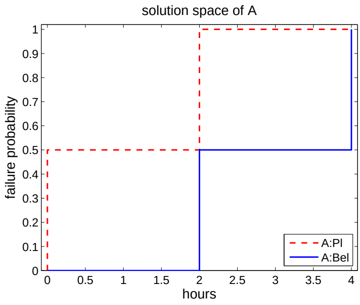
# OR-Gate - Meaning in DST

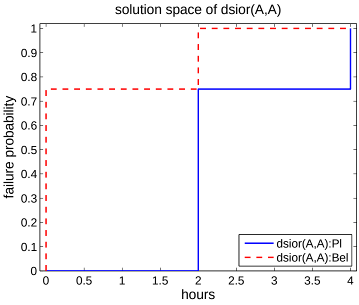
## Evaluation Or-Gate in DST

$$C_1 = A \cap B$$
$$C_2 = A \backslash B$$
$$C_3 = B \backslash A$$
$$PL(C_1) = 1 - (1 - PL(A)) \cdot (1 - PL(B))$$
$$BEL(C_1) = 1 - (1 - BEL(A)) \cdot (1 - BEL(B))$$
$$PL(C_2) = PL(A)$$
$$BEL(C_2) = BEL(A)$$
$$PL(C_3) = PL(B)$$
$$BEL(C_3) = BEL(B)$$

# OR-Gate (Example)

$$A \lor B = 1 - (1 - P(A)) \cdot (1 - P(B))$$



# Conclusion

## Development

DSI-Toolbox:

- Fast and verified Dempster-Shafer computation
- Use of INTLAB

New approach in Fault tree analysis:

- Verified computation of the biggest failure probability
- Uncertainties in failure distributions can be expressed as intervals
- Based on DSI (fast computation)

# Further Work

## Further Work

Combination of verified Dempster-Shafer Theory and Markov chains, with possible application to Fault tree analysis.

# Literature


- AUER, K. ; LUTHER, W. ; REBNER, G. ; LIMBOURG, P.: *A Verified MATLAB Toolbox for the Dempster-Shafer Theory*, 2010. – http://www.ensieta.fr/belief2010/papers/p83.pdf
- LIMBOURG, P. ; SAVIC, R. ; PETERSEN, J. ; KOCHS, H. D.: *Modelling uncertainty in fault tree analyses using evidence theory*. In: Journal of Risk and Reliability 222 (2008),S. 291–302
- RUMP, S.: *INTLAB - INTerval LABoratory*. In Tibor Csendes, editor, Developments in Reliable Computing, pages 77–104. Kluwer Academic Publishers, Dordrecht, 1999.
- GUTH, M.: *A probability foundation for vagueness and imprecision in fault tree analysis*. In: IEEE Transactions on Reliability (1991), Nr. 40, S. 563–570
- CHEN, Y.: *Uncertainties in Fault Tree Analysis*. – http://www2.tku.edu.tw/tkjse/3-1/3-1-3.pdf
- TONON, F.: *Using random set theory to propagate epistemic uncertainty through a mechanical system*. In: Reliability Engineering and System Safety 85 (2004), Nr. 1–3, S. 169–181
- SHAFER, G.: *A Mathematical Theory of Evidence*. Princeton, USA : Princeton University Press, 1976
- ROBERT, C. ; CASELLA, G.: *Monte Carlo statistical methods*. 2. ed. New York, NY : Springer, 2004 (Springer texts in statistics). – ISBN 0387212396

# Thank you for your attention