Finite Degradation Structures

Liu Yang[1,2] and Antoine Rauzy[1,3]

[1] Department of Mechanical and Industrial Engineering, Norwegian University of
Science and Technology, Trondheim, Norway
[2] zf_yangliu@126.com
[3] antoine.rauzy@ntnu.no

Introduction

This tutorial aims at presenting finite degradation structures, a unifying algebraic framework for combinatorial probabilistic risk assessment models recently introduced by the authors [1, 2].

Probabilistic risk assessment is widely applied for evaluating the risk in industrial systems. Probabilistic risk assessment models can be essentially divided into two categories: combinatorial models and state automata [3]. Fault trees, event trees and reliability block diagrams belong to the first category. They are called combinatorial because they describe the state of a system as a combination of the states of its components. Markov chains, Petri nets and guarded transition systems [4] belong to the second category. They describe the dynamic behavior of the system by defining not only its states (which are, as in combinatorial models, combinations of states of components), but also the possible transitions between these states.

State automata have indeed a higher expressive power than combinatorial models. This additional power comes however with a price: not only models are much more difficult to design, to validate and to maintain, but the computational cost of calculating risk indicators is also much higher. In other words, there is no silver bullet: the choice a modeling formalism results always a tradeoff between the expressive power and the computational resources one can dedicate to the assessment of the model, given that even the most basic calculations, e.g. the assessment of probability of the top event of a fault tree, are already very resource consuming (technically #P-hard, as shown by Valiant [5]). The question is thus "given my limited modeling and calculation capacities, which formalism is the most appropriate to obtain indicators that ensure a reasonably correct and robust decision process?" [3].

With that respect, all of the formalisms within one class are not equally good. For instance, guarded transition systems have a stricty more expressive power than Petri nets, while algorithms used to assess both are the same, up to minor details, and have thus the same theoretical and practical efficiencies.

In the same vein, significant efforts have been made in the recent years to enrich Boolean formalisms, fault trees in particular, without increasing the complexity of assessments. This led to so-called multistate systems, i.e. models in which variables can take more, but still a finite (and in general small) number of values [6–8]. The question remained however of how to lift up central concepts of fault tree analysis, notably the notion of minimal cutsets, to these models.

This is precisely where finite degradation structures make a major breakthrough. In finite degradation structures, values of variables are organized into a meet-semilattice. The partial order over the values reflect the degree of degradation of components. Moreover, the product of two (or more) finite degradation structures is a finite degradation structure. Technically, finite degradation structures form a monoidal category. The key result is that the notion of minimal states (for the degradation order) satisfying a predicate generalizes and explains the notion of the minimal cutsets of fault trees. In other words, finite degradation structures shed a new light onto the whole system reliability theory.

From a practical point of view, finite degradation structures can be turned into a full fledged modeling language thanks to the S2ML+X paradigm introduced with AltaRica 3.0 [9, 10]. Moreover, efficient assessment algorithms can be designed for this language by extending the binary decision diagram technology [11] in a suitable way.

In this tutorial, we shall give a snapshot of these different results and illustrate the key concepts by means of examples.

References

1. Rauzy, A., Yang, L.: Finite degradation structures. Journal of Applied Logics – IfCoLog Journal of Logics and their Applications **6**(7), 1471–1495 (2019)
2. Rauzy, A., Yang, L.: Decision diagram algorithms to extract minimal cutsets of finite degradation models. Information **10**(368), 1–28 (2019). https://doi.org/10.3390/info10120368
3. Rauzy, A.: Notes on computational uncertainties in probabilistic risk/safety assessment. Entropy **20**(3) (2018). https://doi.org/10.3390/e20030162
4. Rauzy, A.: Guarded transition systems: a new states/events formalism for reliability studies. Journal of Risk and Reliability **222**(4), 495–505 (2008). https://doi.org/10.1243/1748006XJRR177
5. Valiant, L.G.: The complexity of enumeration and reliability problems. SIAM Journal of Computing **8**(3), 410–421 (1979). https://doi.org/10.1137/0208032
6. Lisnianski, A., Levitin, G.: Multi-State System Reliability. Quality, Reliability and Engineering Statistics, World Scientific, London, England (2003)
7. Natvig, B.: Multistate Systems Reliability Theory with Applications. Wiley, Hoboken, NJ, USA (2010)
8. Zaitseva, E., Levashenko, V.: Reliability analysis of multi-state system with application of multiple-valued logic. International Journal of Quality and reliability Management **34**, 862–878 (2017). https://doi.org/10.1108/IJQRM-06-2016-0081
9. Rauzy, A., Haskins, C.: Foundations for model-based systems engineering and model-based safety assessment. Journal of Systems Engineering (2018). https://doi.org/10.1002/sys.21469
10. Batteux, M., Prosvirnova, T., Rauzy, A.: Altarica 3.0 in 10 modeling patterns. International Journal of Critical Computer-Based Systems **9**(1–2), 133–165 (2019). https://doi.org/10.1504/IJCCBS.2019.098809
11. Bryant, R.S.: Symbolic Boolean Manipulation with Ordered Binary Decision Diagrams. ACM Computing Surveys **24**, 293–318 (September 1992)