McMaster University

Inspiring Innovation and Discovery

On the Necessity of Evaluating Safety Evidence Weight and the Use of Baconian Reasoning

Silviya Grigorova, Tom Maibaum

McMaster Centre for Software Certification

McSCert

necsis

Assurance Cases and the Notion of Confidence

- Assurance cases are composed of:
  - Explicit safety goals
  - Evidence that these goals have been met, and
  - A structured argument linking evidence to safety goals
- Uncertainty associated with the elements of the assurance case gives rise to the notion of confidence
  - Safety goals and subgoals, expressed in probabilistic terms, versus the confidence we may place in their truth
  - Confidence is an important aspect in the construction and review of assurance cases

McSCert

The Nature of Evidence

- Not just data/facts
  - Has a bearing on a hypothesis
  - Crucial to explicitly encode argument
- Three characteristics of evidence
  - Credibility
  - Relevance
  - Evidence weight/strength/probative force

McSCert

Evidence Weight

- Two distinct uses of the word
  - "the degree to which a rational decision-maker is convinced of the truth of a proposition as compared to some competing hypothesis (which could be simply that the proposition is false)" [Nance]
  - "a balance, not between the favourable and the unfavourable evidence, but between the *absolute* amounts of relevant knowledge and relevant ignorance." [Keynes]
- Importance of the Keynesian evidence weight for confidence modeling

McSCert

Uncertainty

- Epistemic vs. aleatoric uncertainty
- Unknown unknowns (and black swans)
  - Emergence and epistemic uncertainty
  - Knowable unknowns and unknowable unknowns
  - How to stimulate uncovering them?
- Baconian approach for state space exploration

McSCert

Modeling Evidence Weight

- There seems to be an agreement that it is to be modelled using a probabilistic approach
- However, “probability” can refer to different things
- 4 distinct approaches, as outlined by Schum
  - His main research interest lies with evidence scholarship in the legal domain
  - The approaches are associated with varying interpretations of “evidence weight,” all contributing to our understanding of how evidence is perceived and evaluated

Classical Probability

- Three basic axioms (Kolmogorov):
  - Probabilities have a range [0,1].
  - The probability of a sure event is 1.0.
  - If two events cannot happen jointly, the probability that one or the other occurs is equal to the sum of their separate probabilities.

- Probabilities can be updated when new info becomes available, they are conditional
  - Bayes's Rule

The Bayesian Approach

- Prior probability, posterior probability and likelihood
- The weight of evidence is determined as a ratio of likelihoods
  - Used for single items of evidence, or for the entire mass of evidence
  - Important in determining how useful a piece of evidence is in building the assurance case
  - “Expanded forms of likelihood ratios allow us to combine all recognized sources of doubt in assessing the probative force or weight of evidence” [Schum]

Evidential Support and Evidential Weight

- Shafer's non-additive probabilistic beliefs
  - Rejects Kolmogorov's 3rd axiom
  - It is now possible to have uncommitted probabilistic beliefs
  - Having two mutually exclusive events (system being safe/not safe), the sum of their probabilities may be less than one
- Concept of evidential support
  - Shafer considers as "evidence weight" the support that the evidence provides for a hypothesis
  - In the range [0,1]
  - Non-additive

McSCert

Evidential Support and Evidential Weight Cont.

- Evidential support example
  - An agent can assign the following probabilistic beliefs based on evidence E – system is safe (0.7), system is not safe (0.1), system is either safe or not (0.2)
  - The degree of indecision can be modified as new evidence comes to light; it can also be 1 – complete indecision, one cannot read the evidence, as it is ambiguous

McSCert

Evidential Support Scale

- In classic probability theory, 0 stands for complete disbelief/disproof, in Shafer's theory, it stands for *lack of* belief
  - This lack of belief can be updated, it is done using Dempster's rule

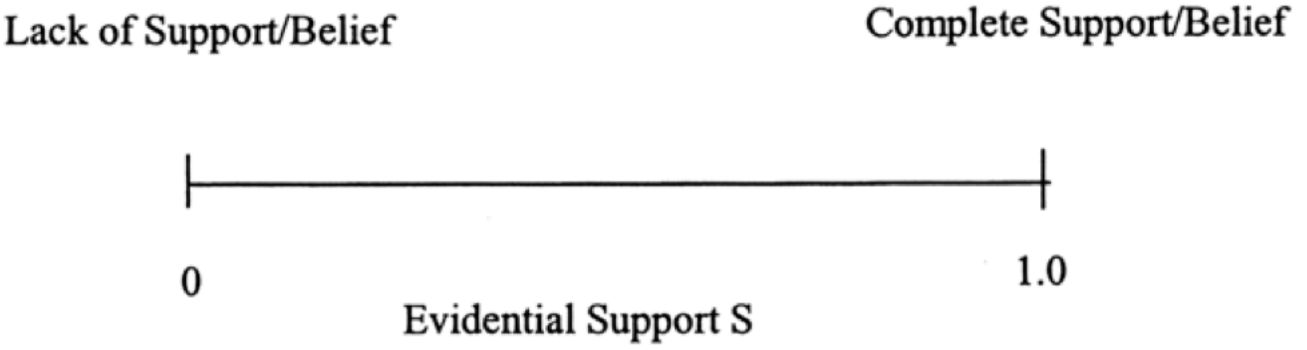

Fig. 2: Evidential Support Scale.

McSCert

Baconian Probability

- Induction by elimination
  - More meaningful than simply gathering evidence in support of a hypothesis
  - Confidence-building
  - Relies on evidential tests created with the purpose of eliminating alternative hypotheses
  - The testing has to be *variative* - the sources of evidence need to be diverse, covering different conditions
- "In Cohen's Baconian probability system, evidence is *relevant* only if it serves to eliminate one or more hypotheses or propositions being considered." [Schum]

McSCert

Baconian Probability Scale

- 0 stands for lack of proof, can be updated upward
- Cohen's Baconian probabilities have ordinal properties
  - No algebraic operations can be performed
  - Comparisons are usually not meaningful
  - No natural unit exists

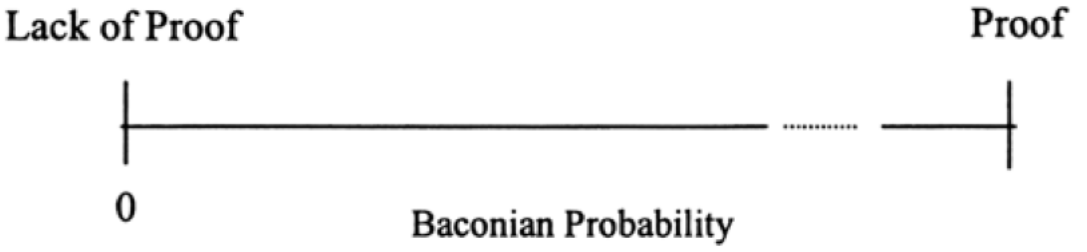

Fig. 3: Baconian Probability Scale.

McSCert

Keynesian Evidence Weight

- Evidential weight depends on how many evidential tests we have performed, and how many we have not
- It provides a measure of the completeness of the utilized evidence with regard to all relevant evidence

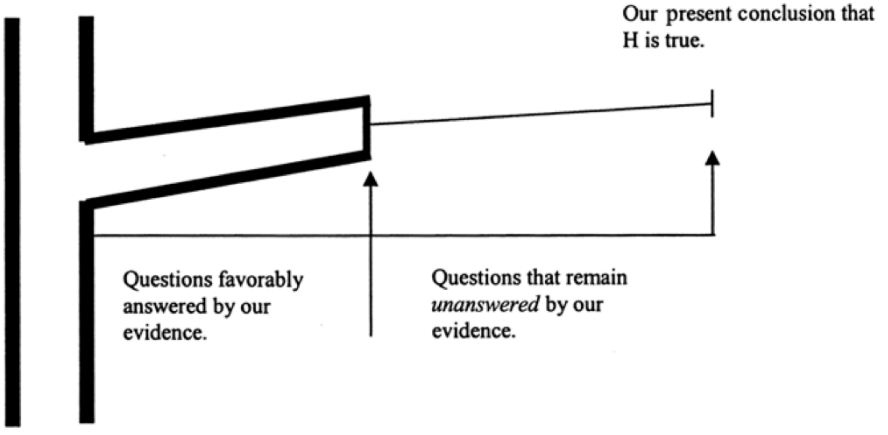

Fig. 4: Baconian Evidence Weight.

Wigmore and Fuzzy Evidence Weight

- Wigmore suggested a theory of verbal probabilistic force gradations
  - Did not provide a means for combining them
- Zadeh's fuzzy logic
  - Recognized the use of words rather than numbers when it is difficult to quantify probabilistic belief – fuzzy (imprecise) probabilities
  - Provided means of combining fuzzy gradations

Discussion

- All four approaches provide useful insight and modeling capabilities
- Can we use them in conjunction, to elicit maximal effect?
  - Use Baconian reasoning to expand state space coverage and model Keynesian evidence weight
  - Use Bayesian approach where the events we reason about are not idiosyncratic, and sufficient information is available
  - Utilize Shafer's evidential support when evidence is ambiguous
  - If it is not possible to elicit quantitative probabilities, use fuzzy logic

Conclusion

- Keynesian evidence weight is an important concept that should not be overlooked
  - It can provide one value in a tuple of confidence values
- The Baconian modeling approach appears to be best suited for its modeling
- Other probabilistic approaches are needed to complement the Baconian one in establishing assurance case confidence
  - Proper encoding of the safety case argument is a necessary initial step for each probabilistic approach