

REPORT ON STSM ACTIVITIES BY FABRIZIO RUGGERI

1. Context

Fabrizio Ruggeri, from IMATI-CNR, visited David Rios Insua, from ICMAT-CSIC, in Madrid, during the period 9-13 November 2015. The visit was related to a previous visit, supported as STSM by the same COST project, by David Rios Insua to Milano in September/October 2015 and was meant to provide further advancements on the common work. The work should partially involve also Refik Soyer (George Washington University) who visited Milano during Rios Insua's visit and whom I visited in Washington at the end of October.

2. Overview

The bulk of the work developed referred mostly to adversarial risk analysis (ARA). This focuses on risk situations in which some of the threats come from intelligent adversaries. There is a need to forecast the adversaries' actions. This is complicated because of the intentionality involved and ARA may be seen as a methodology that allows to think and elicit such adversarial actions. Rather than asking an expert to think and provide direct information about such actions, we may ask him to think and provide judgements about what he believes is the problem that the adversary faces, his beliefs and preferences.

3. Papers

The following papers have been continued during the visit.

- Robustness for adversarial risk analysis (Rios Insua, Ruggeri). Elicitation of beliefs and preferences is a very crucial aspect in ARA. One possible way forward is to enhance ARA with sensitivity/robustness ideas, possibly applying previous work by both researchers. The approach we have adopted is as follows (with two players: a "defender" supported by us and an "attacker"). A) Start with the game theoretic solution, assuming common knowledge. B) Perform sensitivity analysis. If the problem is robust (i.e. there are "small" variations in expected utilities and decisions), then STOP. Otherwise, C) Perform an ARA approach. D) Perform sensitivity analysis considering attacker's probabilities and utilities drawn from classes of them. If the problem is robust, then STOP. Otherwise, E) Perform a gamma maxi-min analysis, looking for the decision which maximises, over all possible decisions, the minimum expected utility over all probability measures and utility functions in the entertained classes. We have used both the sequential Defend-Attack and the simultaneous Defend-Attack templates. The general theory has been written, a numerical example has been prepared and just computations are needed before we will send the paper to a Springer volume on Robustness. We have discussed also more complex, and more realistic, classes which should be the basis for a future paper.
- Adversarial hypothesis testing (Rios Insua, Ruggeri, Soyer). A new field encompassing many problems in cybersecurity is called adversarial signal processing. The approach adopted is based on minimax zero-sum games. We are developing an approach based on ARA which we called adversarial hypothesis testing. We have developed the theory,

discussed different scenarios, and prepared a numerical example. We have also worked out an applied example in relation with spam detection; the general ideas of the example have been set up and we need to complete the numerical part. We expect to complete the paper by end of year 2015 and submit it to a top statistical journal. Ideas for further works on the topic have been discussed as well.

- Adversarial life testing (Soyer, Rios Insua, Ruggeri). We aim here to provide a new approach to a series of papers by Lindley and Singpurwalla on life testing in relation with warranties and standards. The approach they proposed is essentially game theoretical and based on common knowledge assumptions. We have outlined an ARA strategy with trees and influence diagrams and need to work now on an example and how to relate this with standards. We expect to complete the paper by January 2016 and submit it to a journal in relation with quality and standards.
- Games and Decisions in Reliability (Soyer, Ruggeri, Wilson, Rios Insua). This is an invited review paper from EJOR due by February 2016. During Rios Insua and Soyer's visit to Milano we had sketched the contents and assigned sections to co-authors. During the current visit we discussed relations between different sections to have a coherent (and I had also the chance to discuss it with Wilson, visiting Madrid in the same days).

4. Other activities

We also discussed another topic to address from the beginning of next year:

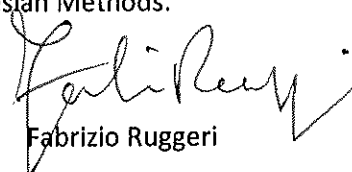
- Combination of expert opinions of project and unit managers and historical data in proposal bidding on behalf of a company, trying to revive an old research on the topic which had lead some years ago to a Ph.D. dissertation by Jesus Palomo.

We performed also some logistic planning including:

- I am organising, jointly with Soyer, a SAMSI workshop on Games and Decisions in Risk and Reliability (GDRR) in 2016 and we discussed the content of the courses that each of us will give and plans for submitting a year long programme at SAMSI on such topic. We also discussed about the possibility of organising the next GDRR in Madrid, possibly with invited talks stemming from the current COST project.
- We further discussed about a possible EJNET research kitchen around Multiple Experts, Multiple Attackers, Multiple Defenders to be held in Madrid in 2016.
- We performed further screening for possible H2020 bids in the new 2016-2017 work programme.

Finally, I also delivered a seminar on *New classes of priors based on stochastic orders and distortion functions*, a new contribution about sensitivity analysis, on November 11th within a session at ICMAT on Advances in Bayesian Methods.

Milano, November 18th 2015



Fabrizio Ruggeri