Nuclear Arms Control: Optimising Verification Procedures Through Formal Modelling

An Overview

Paul Beaumont[1], Neil Evans[2], Michael Huth[1], and Tom Plant[2]

[1] Department of Computing, Imperial College London, London, SW7 2AZ, UK
{paul.beaumont, m.huth}@imperial.ac.uk
[2] AWE Aldermaston, Reading, Berkshire, RG7 4PR , UK
{Neil.Evans, Tom.Plant}@awe.co.uk

Abstract. We present an overview of the use of mathematical modelling in a nuclear arms verification regime. Modelling is a powerful tool that is particularly useful in domains where there is limited data on which to base decisions on, and where robust analysis is needed in order to give good decision-support. Models at varying levels of abstraction can mimic different facets of a regime; from the 'technical details of an information barrier system' during an inspection, through to 'how to schedule inspections' over a whole inspection regime. Arms control verification processes do not in practice allow the parties involved to gather complete information about each other, and therefore any model we use must be able to cope with the limited information, subjective assessment and uncertainty in this domain. We carry out an analysis of two such models using the capabilities of a Satisfiability Modulo Theory (SMT) solver [5]. We discuss the models briefly, before analysing pertinent questions of interest to give examples of the power of this approach.

1 Introduction

Arms control agreements are important tools that help nations to manage their security relationships with each other, particularly by reducing the risk of arms races, and which in some cases seek to eliminate particularly destructive classes of weaponry entirely.

One role of the Atomic Weapons Establishment (AWE) is to provide decision support to the UK Government on any potential nuclear arms treaty the UK may enter into. An arms control agreement would inevitably involve some level of verification mechanism or regime to ensure compliance with the treaty (for example: inspections, deployment of monitoring equipment, etc). Although verification in a treaty is not mandatory, the absence of any form of verification would be an absence of a deterrent to any nation that wished to 'cheat' the treaty. The design and implementation of verification processes are complicated, intrusive and expensive however - which imposes limits on the scale of that deterrent. This tension motivates the need for tools that model, analyse and optimise verification processes in this domain.

The Non-Proliferation Treaty (NPT) bans the transfer of knowledge or capabilities between nations that could enable them to build a nuclear weapon. During an arms control verification, it will be impossible, therefore for states to gain complete information about each other: an 'information barrier' will need to exist, and states will often, and in some circumstances must, withhold some information. Each must therefore make decisions about whether or not other parties are complying with their obligations on the basis of limited information. They must also make decisions during negotiation of a verification regime about the measures to be used, and how and when to use the tools at their disposal during the implementation of that regime. Decision-making under uncertainty is therefore a core element of the arms control verification problem.

AWE's approach to providing decision support in the face of this uncertainty is to use mathematical models to capture their degree of belief in events or propositions, and their

confidence in such beliefs. Our work extends and combines the mathematical modelling concepts and verification approaches AWE wish to use, such that they can cope with the inherent lack of available data in this domain, and potentially be used to support policy-makers in practice.

2 Scenarios of Interest

Our models of interest follow the technical setup from the UK-Norway Initiative [13, 16], which is an early 2007, collaboration between the UK Ministry of Defence, the UK Atomic Weapons Establishment, several Norwegian laboratories and the non-governmental organisation VERTIC (Verification Research, Training and Information Centre) to work on the technical verification of nuclear arms control. The verification techniques within the Initiative involve a radiation detector that is used to determine the radioactive make-up of an item under inspection. Models of this Initiative may be at varying levels of abstraction; ranging from the technical working of an *information barrier*, to the higher-level ideas about how to plan out limited inspections as part of a *verification regime*. We consider two such cases as examples.

2.1 Information Barrier

Consider the situation of two fictitious nations, **N1** and **N2**. **N2** is tasked with identifying whether an item belonging to **N1** and available to 'inspect' in a controlled inspection facility is a nuclear weapon. The purpose of this inspection within an arms control agreement may be that the item is on its way for decommissioning, destroying, storage, etc. Our mathematical model of the scenario does not reflect what may happen to the material post-inspection, but more detailed models may well reflect this.

The nations' non-proliferation obligations and national security concerns dictate that the design details of the item must be protected, and therefore the inspecting party will have no visual access to the item. Instead the parties agree that the objects that they declare to be weapons contain Plutonium with the isotopic ratio 240Pu:239Pu below a certain threshold value, which they set at 0.1. In order to draw conclusions about whether an item presented for inspection is a weapon, the inspecting party uses an information barrier (IB) system comprising a HPGe detector and bespoke electronics with well-understood performance characteristics (see Figure 1, [16]) to conduct measurements on the object while the object is concealed in a box. The IB system displays a green light if it detects a gamma spectrum indicative of the presence of Plutonium with the appropriate isotopic ratio; if it does not detect this spectrum for whatever reason then it shows a red light. No other information is provided, and therefore weapon design information is protected [13].

Nation **N2** believes that it may be possible for nation **N1** to spoof a radioactive signal (or in some way provide a surrogate) to fool the detector, or that **N1** may have just placed Plutonium with the appropriate isotopic ratio in the box rather than a weapon. These subjective assessments should be reflected in the model alongside the error rates of the IB system. In order to deter cheating, **N2** is allowed to choose the IBs used in the verification from a pool of machines. They are also able to take some unused IBs away for authentication from the same pool. Authentication activities are designed to check whether or not the IB has been tampered with. It should be noted that **N2** are not allowed to take the IBs used in verification activities in case there is any residual information to be gained following their use. This selection process is designed to ensure that a nefarious host is held at risk of detection, because in order to tamper with the IBs used in verification it would have to run the risk of one or more tampered IBs being selected for authentication. Although authentication cannot be assumed to be perfect - and this too should be modelled - the prospect of detection may still give pause to such a host.

Fig. 1. The Information Barrier built as part of the UK-Norway Initiative [13, 16]. The option to 'calibrate', 'measure' and 'calibrate' again can be seen on the front of the panel, along with the corresponding (unlit) green and red lights.

2.2 Planning of an arms verification regime

Consider two fictitious nation states, who have agreed to increase transparency in their nuclear arsenals by exchanging information on the size of those arsenals on a regular basis. In our model, the two nations each hold a certain number of weapons, declare (not necessarily truthfully) to the other party that they have no more than a certain number of weapons, and hold beliefs about the size of the other nation's arsenal.

Two types of inspection are carried out by each nation to determine the consistency of the others' nuclear arsenals with their declarations: scheduled inspections, which occur at pre-agreed intervals; and surprise, unscheduled inspections which are carried out at the discretion of the inspecting nation. We assert the following:

- Neither type of inspection is perfect, given information barriers that exist, the qualitative nature of some of the information collected, and the error rate of detectors used in the inspections.
- Unscheduled inspections are more effective at detecting cheating. This comes intuitively down to the likelihood of the host being less prepared than for a scheduled inspection.

The inspections are assumed to follow a protocol similar to that described in Subsection 2.1. Let us here be more concerned with the dynamics of the system operating temporarily than with how the results are obtained for an inspection.

Each nation may build or dismantle nuclear weapons in this model. Their decisions in this respect are partly influenced by the ongoing arms control processes, and by a combination of their assessment of the difference between the two arsenals, their tendency to fear the other nation (or not), and – indirectly – by their overall strategy in relation to the verification process.

If one nation is found by the other to have made a false declaration then it will incur a cost of some kind. This might be financial (economic sanctions for example), reputational, diplomatic, or any mix of these or other factors. As with the inspection process, we do not model the details of the cost here because they are not particularly relevant to the analysis we are trying to carry out. Instead we are more interested in understanding "hidden" factors - such as the

actual number of weapons held by the other nation - and their dependencies, and in modelling the consequences of decisions - such as the frequency of scheduled inspections or the timing of the unscheduled inspections available to each nation.

3 Our Approach

There are of course multiple ways of modelling these scenarios. One advantage of our approach in general is that it is able to compare different such models analytically: as seen in [1] where we compare multiple models of varying levels of abstraction and assess how the abstraction process may lead to different insights and decision support.

Our approach is to model the various inspections control processes in a software tool known as a Satisfiability Modulo Theories (SMT) solver [14, 15]. SMT is uncomfortable with solving more advanced, non-linear mathematical concepts, however. The project itself has been concerned with engineering other languages to take up some of this load, so that SMT only has to check 'satisfiability' (and does a minimum of other computations itself). This is particularly important to AWE, because the mathematical models they are interested in using can be large and complicated.

We achieve this by integrating the solver with Python and other symbolic computation packages, leaving SMT to decide the satisfiability of logical formulas that capture the essence of questions we ask about models. This offers a general purpose approach to the automated analysis of mathematical models, and in our case we use SMT to deal with uncertainty in (or absence of) data in the model by expressing such uncertainty as the *under-specification* of probabilities or quantities in the models.

For instance, if we were unsure as to the probability of cheating by a party in a treaty, we could call such a probability x, instead of some concrete probability value 0 to 1. We would then limit x such that $0 \leqslant x \leqslant 1$. Similarly, if we were unsure on the initial number of weapons a state held before entering into a treaty, we could call this z, and constrain z by the lower and upper bounds of our estimations, say, $900 \leqslant z \leqslant 1100$. In other words, we don't have to choose values that we don't *know* for certain. We can assign a variable, and pick a range of possible values for that variable, and study the impact of such uncertainty in the model.

For this approach of under-specified parameter values, we have so far considered Bayesian Belief Networks (BBNs) [1, 4], Game theoretic models [2] and dynamical systems [3].

BBNs allow the representation and analysis of multiple variables, the causal relationships between them, and their associated conditional probabilities. They are particularly useful for making judgments under uncertainty, in representing probabilistic reasoning, and in handling objective and subjective data. This makes them attractive tools in principle for describing and analysing arms control processes.

Bayesian Belief Networks (BBNs) are probabilistic models that encode events of interest in a node-structure. BBNs are dependency graphs, displayed diagrammatically, as a directed acyclic graph (DAG) [11]. Dependencies of events are captured and expressed in probability tables, with observations of events influencing the chances of related events by "updating" the probabilities throughout the network. Nodes with 'parents' have probability tables that list the probability distributions conditionally on the aforementioned parent events. These have been used to assess the true value of beliefs held after observations of certain events in order to provide an untainted logical viewpoint on a situation.

It can be extremely difficult to set appropriate and defensible values for all conditional probabilities, which challenges their use in practice. At the 20th European Symposium on Research in Computer Security (ESORICS2015), the authors proposed a methodology to address this by

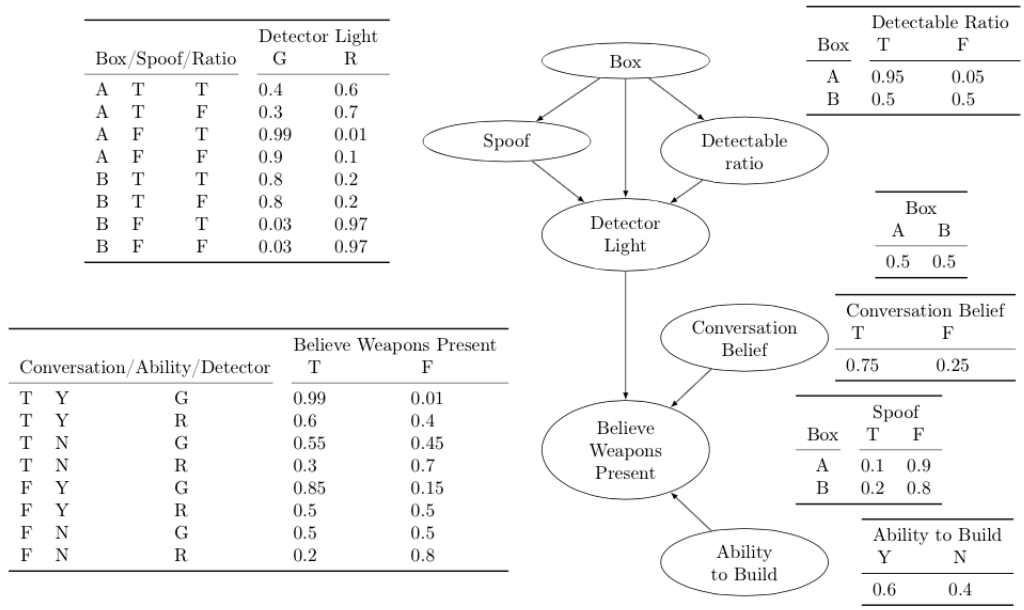

Fig. 2. A small, simplistic example Bayesian Belief Network model of an arms inspection. The item in the Box either is or isn't a weapon; depending on whether it is or isn't, the host may choose to Spoof the radiation with a surrogate source. Even if the Box does contain a weapon, the item in question may or may not have weapons grade material that is of a Detectable ratio for the detector; influencing whether the Detector light on the information barrier goes Green or Red. Along with whether or not the inspector believe what the host's facilities team are saying to them in their conversations with them (node Conversation Belief), and whether or not the inspecting nation believes the host has the Ability to Build a weapon, the Detector Light result feeds into whether, overall, the inspections Believe a Weapon is Present.

extending the BBN framework to allow representation of sets of BBNs [1] using the replacement of probabilities with symbolic variables as described above. We refer to this as a *constrained* BBN (cBBN). A cBBN represents a set of Bayesian Belief Networks by symbolically expressing uncertainty about probabilities and scenario-specific constraints that are not representable by a conventional BBN, but can still be symbolically evaluated. This extension retains the advantages of BBNs, allows the incorporation of any scenario constraints, and assesses the robustness of models and their analyses when little or no contextual data are available.

In Figure 2, we include a small simplistic example for a reader to see, and encourage interested readers to view [4], which includes a much more detailed model designed by AWE.

The underspecification of pay-offs in game theory, or variables in a dynamical system allow us to model uncertainty in such models in a similar way to our cBBNs. Dynamical systems model the interactions and human decision making of parties in an arms control process through the updating of equations over time. Equations are written to model variables of interest, for instance, the arms stocks declared at each time point, the actual number of weapons, what each party to the treaty believes about each other, etc. Figure 3 details the equations of a sample system that models the use of scheduled and unscheduled inspections at varying time points in a treaty's lifetime. We refer to [3] for a detailed explanation of the system and its justifications.

Game theory - the 'study of mathematical models of conflict and cooperation between intelligent, rational decision makers' [7] - has an established history in defence analysis, perhaps most famously in the context of nuclear deterrence (see for example [8] or the normal form games of [9, 10] and Figure 4). In an arms control context, an inspecting party seeks data to support an assessment of another party's compliance with an agreed set of rules. Whilst both parties

$$
\begin{aligned}
W^i_{t+1} &= W^i_t\left(1-\gamma^i\right) + F_i\left(B^{ij}_t - W^i_t\right) \\
B^{ij}_{t+1} &= \begin{cases} \left(\alpha^i_B B^{ij}_t + \alpha^i_I I^{ij}_t + \alpha^i_D D^j_t\right)\mathcal{H}\left(D^j_t - I^{ij}_t\right) + \left(\beta^i_B B^{ij}_t + \beta^i_I I^{ij}_t + \beta^i_D D^j_t\right)\mathcal{H}\left(I^{ij}_t - D^j_t\right) \\ B^{ij}_t + \left(B^{ij}_t - B^{ij}_{t-1}\right) \end{cases} \\
I^{ij}_t &= \begin{cases} W^j_t\left(1-p^j_{f-}\right) + \left(\left(\frac{D^j_t + B^{ij}_t}{2}\right) - W^j_t\right)p^j_{f+}, & \text{if } D^j_t \geqslant W^j_t \\ W^j_t(1-\hat{p}^j_{f-}) + \left(\left(\frac{W^j_t + B^{ij}_t}{2}\right) - D^j_t\right)p^j_{f+}, & \text{if } D^j_t < W^j_t \\ I^{ij}_{t-1}, & \text{if no inspection} \end{cases} \\
\mathbb{P}(\text{found}^i_t) &= \begin{cases} 0, & \text{if } D^i_t \geqslant W^j_t \\ 1 - \sum_{i=0}^{N-D-1}\binom{n}{i}P^i_m(1-P_m)^{N-i}, & \text{if } D^i_t < W^i_t \text{ and } \theta = 1 \\ 1 - \sum_{i=0}^{N-D-1}\binom{n}{i}Q^i_m(1-Q_m)^{N-i}, & \text{if } D^i_t < W^i_t \text{ and } \Omega = 1 \end{cases} \\
D^i_{t+1} &= A^i_1 \cdot D^i_{t-1} + A^i_2 \cdot W^i_{t-1} + A^i_3 \cdot D^j_{t-1} + \mathbb{P}(\text{found}^i_t) \cdot \text{Penalty} \\
\theta^i_{t+1} &= 1 - \textstyle\sum_{i=0}^{n}\mathcal{H}\left(\theta_{t-i}\right) \text{ where } n \text{ is the period of inspections} \\
& p^j_{f-}, \hat{p}^j_{f-}, p^j_{f+} \text{ are modelled as constants}
\end{aligned}
$$

Fig. 3. A Dynamical Systems model that predicts the change in the number of nuclear weapons a state i has at time t, W^i_t, the beliefs about the number of weapons nations have about each other B^{ij}_t - based on inspection results I^{ij}_t and declarations D^i_t about the size of their arsenals. θ controls when to hold a scheduled inspection, according to the periodicity and shift defined in the model setup.

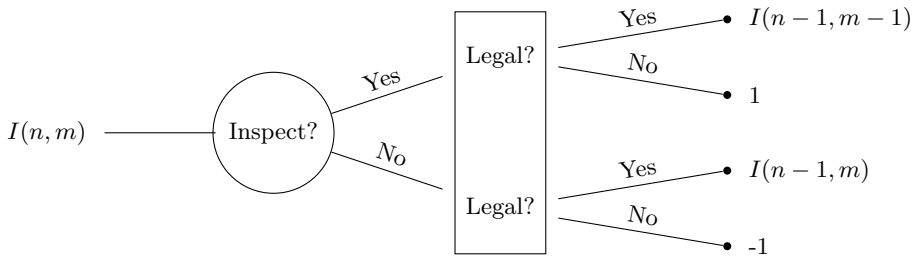

Fig. 4. Extensive form game theory model of how to best schedule inspections. This is based on the model of Dresher and assigns payoffs based on whether an inspection was used wisely to detect cheating, or not. The modeller decides whether to inspect or not based on the maximal utility of the system, and the the legality of the inspected nation's behaviour is left to chance (the probability of which can be the same throughout the model, set explicitly for different values of n and m, or can be assigned different probabilities randomly [6]).

have an interest in being seen to comply with this set of rules, other national interests may differ. This in turn leads to different objectives for the parties involved, the pursuit of which can be analysed by studying mathematical representations of inspections in a non-cooperative two-player game.

As BBNs, dynamical systems and game theory models can all be expressed as equations, we encode them as constraints in our tool. SMT is then able to apply logical formulae to the constraints, and check to see whether they are all satisfiable (in which case it returns a concrete realisation of such values that 'work'), or unsatisfiable (in which case it is impossible).

Using logical arguments, we can then extract more useful information. For instance, when we seek the maximum of a variable, we recursively add extra constraints to the SMT solver that seek a 'larger' value of that variable than the one it previously returned. Eventually, the model becomes unsatisfiable, meaning that the penultimate result was the maximum. Likewise we can see at which points satisfiable constraints become unsatisfiable, and how far we can push such constraints, to categorise 'impossible' scenarios. 'Impossible' may mean that we cannot realise something we expect to be realisable (detecting a problem of the model or proposed verification process that may then be re-addressed); or it may mean that all scenarios satisfy a desired invariant, where the formula analysed is the negation of that invariant.

4 Questions

We are now able to answer pertinent questions of our BBN inspection model. An example question could be of the following form. '*We observe no tamper abnormalities on the information barriers or detectors. What effect does uncertainty over whether a body scanner (to check for surrogate sources of radiation) is working correctly have on the likelihood of the information barrier reporting positively that nuclear material is present?*'. Over this uncertainty, we can then test our model and report back the range of results as under-specification, say x, varies. We can also compute how sensitive to change the results are, and whether any particular values of x are better or worse than others [12].

We can take multiple different BBN models at once and compare their results; checking for areas of agreement and disagreement between models. A decision maker could use the information gleaned to make an informed decision about how to authenticate the body scanner, weighing the cost of body scanner authentication against the cost of developing and employing more advanced information barrier authentication capabilities to conduct a cost-benefit analysis. They could also query in detail how the results of these cost-benefit analyses might change as new information is learned or new techniques deployed. This capability might help decision-makers to balance their priorities and to gain the best assurance possible without excessive cost that the verification regime they implement is effective.

Similarly, we can ask of our Dynamical Systems model: '*given uncertainty in our treaty partner's initial weapon stockpile, with scheduled inspections every 6 months and 3 other unscheduled inspections per year, what timing for unscheduled inspections leads to the minimum difference between our partners' declaration and our assessment of their actual arsenal?*'. The results to such a query would be returned along the lines of 'for all z covered by the range $low \leqslant z \leqslant high$ where z represents our treaty partner's initial weapon stockpile, assuming our model of how beliefs and weapon numbers change over time is correct, then we would be best holding inspections in months four, sixteen and eighteen, (say...) to achieve our goals'.

We have harnessed a supercomputer to analyse over 134 million possible inspection timelines, allowing the software to compute an inspection schedule over a treaty lifespan of over 2 years

for which performance against one or more measures of interest is optimised. The results can then be studied to assist in decision-making regarding proposed arms control regimes.

These new modelling and analysis methods allow for a much more sophisticated approach to modelling arms control where we accept that there are somethings we just can't know, but we account for them and can still prove that the decision advice given holds true irrespective of the actual concrete value those variables take.

5 Conclusions

In this paper, we have provided an overview of the work done on the analysis of inspection regime models. We have introduced a methodology for dealing with uncertainty in Bayesian Belief Networks, Dynamical Systems and Game Theoretic models. The result is an automated approach that could allow a decision maker to ask pertinent questions of an arms control scenario, under uncertainty.

Overall, we have explained how we can generalise models of historic importance in the study of nuclear arms dynamics, whilst effectively addressing the non-linear modelling concerns of selecting 'correct' pay-off values, probabilities, or values of variables and automatically analysing questions of interest for a range of possible values. This allows us to support decision making in particular in our scenario of interest. We believe that analysis of this type was not previously supported; and the capability to do this is useful for scenarios such as the one discussed here as a case study; in supporting decision making.

Acknowledgements: The authors from Imperial College London would like to thank AWE for sponsoring a PhD studentship under which the research reported in this paper was carried out.

References

1. Beaumont, P., Evans, N., Huth, M., Plant, T.: Confidence analysis for nuclear arms control: SMT abstractions of Bayesian Belief Networks, Computer Security – ESORICS 2015, Lecture Notes in Computer Science, Springer, 2015
2. Beaumont, P., Evans, N., Huth, M., Plant, T.: Confidence analysis for nuclear arms control: SMT abstractions of Game Theoretic Models, INMM57, 24-28 July, Atlanta, USA, 2016
3. Beaumont, P., Evans, N., Huth, M., Plant, T.: Bounded Analysis of Constrained Dynamical Systems: A Case Study in Nuclear Arms Control, INMM57, 24-28 July, Atlanta, USA, 2016
4. Beaumont, P., Day, E., Evans, N., Haworth, S., Huth, M., Plant, T., Roberts, C.: An in-depth case study: modelling an information barrier in Bayesian Belief Networks, INMM57, 24-28 July, Atlanta, USA, 2016
5. Barrett, C., de Moura, L.M., Ranise, S., Stump, A., Tinelli, C.: The SMT-LIB initiative and the rise of SMT, Hardware and Software: Verification and Testing - 6th International Haifa Verification Conference, HVC, 2010
6. Dresher, M., A sampling inspection problem in arms control agreements: a game theoretic analysis. Memorandum No. RM-2972-ARPA, The RAND Corporation, Santa Monica, California (1962)
7. Myerson, R. B: Game Theory: Analysis of Conflict - Harvard University Press, p. 1. Chapter-preview links, pp. vii-xi, 1991
8. Schelling, T., The Strategy of Conflict, Harvard University Press, reprinted May 1981
9. Saaty, T. L.: Mathematical models of arms control and disarmament: application of mathematical structures in politics, Publications in operations research, Wiley, 1968
10. von Stengel, B. : Recursive Inspection Games, CoRR, 2014
11. Fenton, N., Neil, M.: Risk Assessment and Decision Analysis with Bayesian Networks. CRC Press (2013)
12. Kwan, M.Y.K., Overill, R.E., Chow, K., Tse, H., Law, F.Y.W., Lai, P.K.Y.: Sensitivity analysis of bayesian networks used in forensic investigations, Advances in Digital Forensics, 2011
13. UK MoD: Ministry of Defence of the United Kingdom. the UK/Norway initiative: report on the UKNI nuclear weapons states workshop (March 2010)
14. de Moura, L.M., Bjørner, N.: Z3: An efficient SMT solver. In: TACAS. pp. 337–340 (2008)
15. De Moura, L., Bjørner, N.: Satisfiability Modulo Theories: Introduction and Applications, Communications of the ACM, Vol. 54 No. 9, Pages 69-77, 2011
16. UKNI: http://ukni.info/