ARD: Accessible Reasoning with Diagrams*

Mateja Jamnik
University of Cambridge
Cambridge, UK
mateja.jamnik@cl.cam.ac.uk

Gem Stapleton
University of Brighton
Brighton, UK
g.e.stapleton@brighon.ac.uk

Introduction

Modelling modern high-technology systems is complex and involves multiple stakeholders. As these systems increasingly underpin our everyday lives, and are often safety or security critical, reasoning about correctness is paramount. Thus, modelling and formal reasoning is required in order to convey knowledge unambiguously and correctly. Whilst mathematical modelling adds great rigour, it is opaque to many of the stakeholders. This leads to errors in data handling, delays in product release, and even breaches in consumer privacy. We propose a solution: a new formal diagrammatic approach for developing, debugging, communicating and reasoning rigorously yet accessibly about domain models. Our aim is to make automated systems more human-like in their reasoning and consequently, more intuitive and accessible to their users.

Uniquely, the development of this diagrammatic approach will be guided by extensive empirical studies of what humans understand and find accessible. Whilst pushing forward research into diagrams and logic [2, 5], a major goal is also to bring usable reasoning tools to end-users who need to understand, develop and reason about models of their respective domains.

Our proposed solution represents a paradigm shift: we hypothesise that diagrams can be used instead of mathematical symbols to yield an accessible reasoning system. These diagrams are just as formal as the traditional mathematical approach. A particularly exciting aspect of our project is that it draws on both computer science and cognitive science, to address a long-held assumption that using diagrams makes modelling and reasoning accessible.

In addition to the rapid rise in quantity and availability of data, and the benefits this stands to bring to society if suitably understood, recent research has demonstrated that diagrams bring cognitive benefits over symbolic and textual notations. This cognitive offloading, identified using neuroscience approaches, shows that people find reasoning tasks significantly easier when using diagrams. These results mean that the time is right to design an accessible diagrammatic logic that reflects more the way humans reason, and that is suitable for real-world modelling and reasoning.

A Case Study: Privacy Requirements Modelling

To showcase practical relevance, we will apply our research to privacy requirements modelling [3]. This is an important topic from consumer, business and legal perspectives, and involves a wide range of stakeholders, including:

* This project is supported by the Leverhulme Trust Research Grant RPG-2016-082.

– software engineers, who must implement associated software systems,
– lawyers, who must ensure that data usage is legal,
– analysts, who need to understand the data for purposes such as product improvement,
– marketing personnel, who need information for targeted product advertising,
– managers, who need to understand what their teams are doing to ensure privacy is protected.

These stakeholders contribute specialist knowledge in the collaborative act of producing a model of privacy requirements, yet typically have no knowledge of symbolic logics. The diversity of stakeholders and the complexity of the domain make it an ideal area for study, in which we will collaborate with Nokia Networks. Their interest stems from the accessible nature of diagrams, allowing effective and accurate communication between their stakeholders.

$$\forall l \forall u \forall i \Big((RawLog(l) \wedge UID(u) \wedge IP(i)) \Rightarrow \Big(\big(source(l,i) \wedge uid(l,u) \wedge consent(u, Marketing) \wedge consent(u, Secondary) \wedge \forall x \big((source(l,x) \Rightarrow x = i) \wedge (uid(l,x) \Rightarrow x = u) \wedge (consent(u,x) \Rightarrow Consent(x)) \big) \big) \Rightarrow \Big(\exists x \big(hash(u,x) \wedge legallyCleanUID(u,x) \wedge \forall y ((hash(u,y) \Rightarrow y = x) \wedge ((legallyCleanUID(u,y) \Rightarrow y = x)))) \wedge \exists x \exists y \big(suburb(i,x) \wedge city(x,y) \wedge legallyCleanIP(u,y) \wedge \forall z ((suburb(i,z) \Rightarrow z = x) \wedge (city(x,z) \Rightarrow z = y) \wedge (legallyCleanIP(i,z) \Rightarrow z = y))) \big) \Big) \Big)$$

Fig. 1. A symbolic theorem about Nokia's privacy model.

Figure 1 shows a standard symbolically expressed example of a theorem that needs proving to establish that it complies with privacy laws (simplified from Nokia's privacy model).

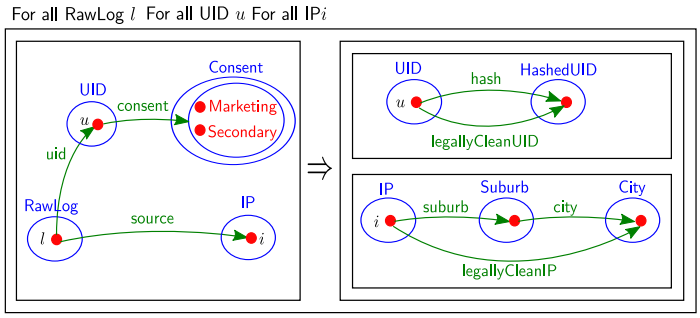

Fig. 2. A diagrammatic version of the theorem in Figure 1.

The same theorem is presented using a concept diagram [1] in Figure 2. It expresses that when users have consented for their data to be used for both

marketing and secondary purposes, the user IDs (UID) from the raw log need to be hashed (i.e., IDs are located and data associated with each is accessed), and their cities of origin must be extracted from their IP addresses to make the data legally 'clean'. Concept diagrams have an essential hierarchical structure that gives users the ability to abstract, for example, by referring to one diagram from another. This dividing of complexity between diagrams helps to keep each diagram simple and understandable. We have initial evidence from Nokia that such diagrams are more accessible to stakeholders than their symbolic counterparts [4], and our proposed diagrammatic logic will develop this much further.

Objectives

This project marries computer science and cognitive science, and a unique aspect is the use of empirical studies to guide the development of reasoning techniques towards more human-like computing. Research contributions fall into six objectives within two main streams:

Stream 1: diagrammatic reasoning,
Stream 2: empirical evaluation and layout.

The objectives are as follows:

O1. Develop case studies to identify core modelling and reasoning problems. [Streams 1 and 2]
O2. Qualitatively identify effective diagrammatic representations. [Stream 2]
O3. Design an accessible diagrammatic logic for modelling and visual reasoning. [Stream 1]
O4. Develop empirically informed layout algorithms for diagrams. [Stream 2]
O5. Implement a reasoning system for our diagrammatic representations. [Stream 1]
O6. Test and empirically evaluate the accessibility of our system. [Streams 2 and 1]

References

1. Howse, J., Stapleton, G., Taylor, K., Chapman, P.: Visualizing ontologies: A case study. In: International Semantic Web Conference. LNCS, vol. 7031, pp. 257–272. Springer (2011)
2. Jamnik, M.: Mathematical Reasoning with Diagrams: From Intuition to Automation. CSLI Press, Stanford, CA (2001)
3. Nissenbaum, H.F.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press (2009)
4. Oliver, I., Howse, J., Stapleton, G.: Protecting privacy: Towards a visual framework for handling end-user data. In: 2013 IEEE Symposium on Visual Languages and Human Centric Computing. pp. 67–74 (2013)
5. Urbas, M., Jamnik, M.: A framework for heterogeneous reasoning in formal and informal domains. In: Dwyer, T., Purchase, H., Delaney, A. (eds.) Diagrams. LNCS, vol. 8578, pp. 277–292. Springer (2014)