Protocol Synthesis in the Dynamic Gossip Problem

Leo Poulson

April 6, 2019

1 Introduction

1.1 Motivation

1.1.1 Gossip

The gossip problem is a problem regarding peer-to-peer information sharing. A set of agents start out with some secret information, and their goal is to transfer this information across the whole network, thus finding out the secret of all of the other agents. This information is transferred through a phone call from one agent to another. When two agents communicate they tell each other all the secrets that they know; hence the name *gossip*.

In the original problem formulation (R.Tijdeman 1971), each agent began with the phone number of each other agent, and hence the starting network is a complete graph. Recently, there has been a lot of work in studying a variation of this problem named the *dynamic* gossip problem. In this, the agents start out with an incomplete set of phone numbers, and as they call the other agents, they exchange all of the phone numbers they know and so the graph's edges grow in number.

The dynamic gossip problem is a popular research topic (Ditmarsch et al. 2018, Ditmarsch et al. 2016), with applications in work in epidemics and research discoverd (Haeupler et al. 2016). In such scenarios, our network may be some peer to peer network, with our agents as computers and the goal to be finding the IP addresses of all of the other computers; or our network might be a social network, where we have people as agents who want to connect with everyone around them. In both cases, our network is updated as the agents communicate and they learn the contact details of other agents.

Applications of DEL here . . .

1.1.2 Planning

Automated planning is the act of computing a finite sequence of actions to take some system from a given initial state to some successful state. Recently, a variant of this has been studied by the dynamic epistemic logic community, called *epistemic* planning. Given an initial set of knowledge states of a set of agents, a finite set of available events, and an epistemic objective, the epistemic planning problem consists of computing the finite sequence of events whose occurence takes us from the initial state to a state satisfying the epistemic objective.

This problem is undecidable for many cases (Aucher and Bolander 2013), but by placing certain restrictions on the models we use it becomes decidable.

1.2 Contributions

In this thesis, we put forward a process to solve the decidable epistemic planning problem. We also give an implementation of this process in Haskell. This process also will solve the gossip problem, by finding a sequence of calls to make every agent know the secret of every other agent; however it is also capable of finding sequences of calls that lead to a situation in which every agent knows that every agent is a secret. **TODO: Find applications for this**.

Given that our software solves just the epistemic planning problem and not strictly the gossip problem, it can plan for any appropriate models. There is no other software currently that solves this problem.

2   Background

2.1   Dynamic Epistemic Logic

2.1.1   Epistemic Logic

Epistemic Logic is the logical language that we use to reason about knowledge. It is a modal logic; a logic with some operator, that can be used to model the passage of time, knowledge, obligation, or any other modality. The essential reference on epistemic logic is Fagin et al. 1995, and it is from here that most of the information in this section comes.

If we have some set of agents A and some set of propositions Λ, then we define the language of epistemic logic over this set of propositions, $\mathcal{L}(\Lambda)$, with the following BNF;

$$\phi ::= \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid K_i\phi$$

where $p \in \Lambda$ and $i \in A$. We also can define false, conjunction and implication in the classic way. We read $K_i\phi$ as "agent i knows that ϕ is true". We can give our epistemic logic a semantics through use of *Kripke models*.

A Kripke model $\mathcal{M}$ over a set of agents I and a set of propositions Λ is a triple (W, R, V), where W is a **(maybe)** finite set of worlds, R is a set of binary relations over W indexed by an agent, such that $R_i \subseteq W \times W$, and $V : W \to \mathcal{P}(\Lambda)$ is a valuation function that associates to every world in W some set of propositions that are true at it.

For epistemic logic, we think of R_i as being the set of pairs of worlds that an agent i cannot distinguish between, and thus considers possible. In our semantics, we use this relation to define knowledge in terms of possibility; agent i knows that something is true if it's true at all of the worlds that i cannot distinguish between.

When giving a semantics to a formula on a Kripke model, we need to use a *pointed Kriple model*. This is just a pair $(\mathcal{M}, w)$ where w is a world of $\mathcal{M}$. Then we read $(\mathcal{M}, w) \models \phi$ as "w satisfies ϕ". We define the evaluation as follows:

$$
\begin{aligned}
&(\mathcal{M}, w) \models \top \\
&(\mathcal{M}, w) \models p \text{ iff } p \in V(w) \\
&(\mathcal{M}, w) \models \neg\phi \text{ iff } (\mathcal{M}, w) \not\models \phi \\
&(\mathcal{M}, w) \models \phi \wedge \psi \text{ iff } (\mathcal{M}, w) \models \phi \text{ and } (\mathcal{M}, w) \models \psi \\
&(\mathcal{M}, w) \models K_i\phi \text{ iff for all } v \text{ such that } (w, v) \in R_i, (\mathcal{M}, v) \models \phi
\end{aligned}
$$

We need to give some properties to our knowledge operator in order to better understand it. We make all of our relations R_i equivalence relations. This means three things;

- R_i is *reflexive*; for all $w \in W$, $(w, w) \in R_i$.
- R_i is *symmetric*; for all $w, v \in W$, $(w, v) \in R_i$ iff $(v, w) \in R_i$.
- R_i is *transitive*; for all $w, v, u \in W$ if $(w, v) \in R_i$ and $(v, u) \in R_i$, then $(w, u) \in R_i$.

This is done in order to convey that agent i considers world v possible from world w if in both w and v agent i has the same information; that is, they are indistinguishable to the agent.
TODO: Perhaps we can write something about the K ϕ -> ϕ axiom here?

2.1.2 Event Models

Public announcement logic was the first development in epistemic logic to support information change in epistemic logic, and is described in Plaza 2007. However, in public annoucement logic, we may only model truthful, public communications; but we all know that there are many other types of communication and events after which some information has changed. An agent may communicate with another agent in a private phone call, or may be lying to them; furthermore, we may have some *physical* action, like a coin flip occuring, after which some knowledge has changed.

To model these more complicated events, we use *event models*. These treat events in a very similar way to how Kripke models treat worlds; we think of a set of possible events that can occur, and encode the events that an agent can tell apart.

Formally, an event model is a tuple $(E, R^E, \mathsf{pre}, \mathsf{post})$.

Bibliography

Aucher, Guillaume and Thomas Bolander (2013). "Undecidability in Epistemic Planning". In: *IJCAI - International Joint Conference in Artificial Intelligence*.

Ditmarsch, Hans van et al. (2016). "Epistemic Protocols for Dynamic Gossip". In: *Journal of Applied Logic,*

— (2018). "Dynamic Gossip". In: *Bulletin of the Iranian Mathematical Society*.

Fagin, Ronald et al. (1995). *Reasoning about Knowledge*. MIT Press.

Haeupler, Bernhard et al. (2016). "Discovery through Gossip". In: *Random Structures and Algorithms*.

Plaza, Jan (2007). "Logics of Public Communication". In: *Synthese*.

R.Tijdeman (1971). "On a telephone problem". In: *Nieuw Archief voor Wiskunde (3)* 19, pp. 188 –192.