university of groningen / faculty of science and engineering / bernoulli institute

Tools for Gossip

Bachelor's Project Thesis

R.A. Meffert, s2702207, r.a.meffert@student.rug.nl
Supervisors: Dr. B.R.M. Gattinger

Abstract:

1 Introduction

Gossip protocols are protocols that describe the way rumors—or, more generally, secrets—are shared in multi-agent environments. The goal of the protocols is to communicate all secrets to all agents. A lot of research has been done in this field, starting with research on the spread of infectious diseases (Kermack & McKendrick, 1927).

The definition of the gossip problem generally used nowadays was first introduced in 1972 by Hajnal et al.[*] In short, agents are represented as nodes in a graph, with the edges representing a "call"—that is, one agent transferring all of their secrets to another agent. When all agents can contact all other agents, Hajnal et al. proved that this can be done in $2n - 4$ calls, where n is the number of agents.

The problem as formulated above requires the oversight of a central authority in order to know whether all agents know all secrets. However, there are many applications where this is not feasible or desirable[†]. Another problem is that it often cannot be guaranteed that all agents can contact all other agents. This has led to the sub-fields of *distributed gossip*, addressing the first issue, and *dynamic gossip*, addressing the second. The combination of these fields, where there is no overseer and not all agents can contact all other agents, is called *distributed dynamic gossip*.

This paper will describe a tool that has been developed to aid research in distributed dynamic gossip. It is able to visualise the connections between agents, allows exploring the execution tree of different (semi-arbitrary) protocols and validate call sequences given a graph and/or a protocol[‡]

2 Method

2.1 Notation

The notation used in this paper is based off of the notation used in Van Ditmarsch et al. (2018) and for some part also on the notation used in van Ditmarsch et al. (2019). A summary of notation is given in Appendix A.

References

Hajnal, A., Milner, E. C., & Szemerédi, E. (1972). A cure for the telephone disease. *Canadian Mathematical Bulletin*, *15*(3), 447–450. https://doi.org/10/cpr4cv

Kermack, W. O., & McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London*, *115*(772), 700–721. https://doi.org/10.2307/94815

van Ditmarsch, H., Gattinger, M., Kuijer, L. B., & Pardo, P. (2019). Strengthening gossip protocols using protocol-dependent knowledge. *Journal of Applied Logics*, *6*(1), 157–203.

van Ditmarsch, H., van Eijck, J., Pardo, P., Ramezanian, R., & Schwarzentruber, F. (2018). Dynamic gossip. *Bulletin of the Iranian Mathematical Society*, *45*(3), 701–728. https://doi.org/10/cvpm

[*] TODO: Tijdeman (1971) might have been earlier, but I have not been able to find a pdf of that paper. It is referenced in Van Ditmarsch et al. (2018) though.

[†] TODO: maybe find a citation for this? Or just explain it better

[‡] TODO: check how possibility/permissibility depends on protocol

A Notation

Let A be a set of agents $\{a, b, \ldots\}$. Two binary relations on A are defined: $N, S \subseteq A^2$. The first denotes the *number* relation, the second the *secret* relation. A gossip graph G is then defined as the a triple (A, N, S).

A.1 Gossip graphs

Binary relation Pxy

Agent x has relation P to agent y.

$Pxy \equiv (x, y) \in P$

Identity relation I_A

The relations of all agents in A with themselves.

$I_A = \{(x, x) \mid x \in A\}$

Converse relation P^{-1}

The opposites of all relations in P.

$P^{-1} = \{(x, y) \mid Pyx\}$

Composition relation $P \circ Q$

The composition of the relations P and Q is a new relation such that the tuple (x, z) is in said new relation iff there exists another agent y such that $(x, y) \in P$ and $(y, z) \in Q$

$P \circ Q = \{(x, z) \mid \exists y((x, y) \in P \wedge (y, z) \in Q)\}$

P_x

The agents that agent x has a relation with.

$P_x = \{y \in A \mid Pxy\}$

P^i

The ith composition of relation P with itself

$$P^i = \begin{cases} P & \text{for } i = 1 \\ P^{i-1} \circ P & \text{for } i > 1 \end{cases}$$

P^*

All binary relations that are possible through (repeated) relation composition of P with itself.

$P_x = \{y \in A \mid Pxy\}$