Tools for Gossip

Bachelor's Project

R.A. Meffert

Supervisor: Dr. B.R.M Gattinger

University of Groningen

Bachelor's Symposium, January 25, 2021

About this bachelor’s project

- The telephone problem [e.g. Tij71]

About this bachelor’s project

- The telephone problem [e.g. Tij71]
- Dynamic gossip [Dit+18]

About this bachelor’s project

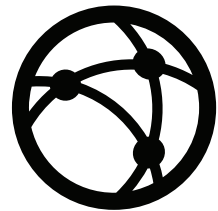
- The telephone problem [e.g. Tij71]
- Dynamic gossip [Dit+18]
- Goal: intuitive, educational tool

Why dynamic gossip?

Blockchain [Bai16]; [Ren16]

Social Media [Tar+19]

Genome analysis [Lib02]



Distributed databases [DGM02]; [DeC+07]

Some notation

Agents $A = \{a, b, \dots\}$

Some notation

Agents	$A = \{a, b, \dots\}$
Number relation	$N \subseteq A \times A$

Some notation

Agents	$A = \{a, b, \dots\}$
Number relation	$N \subseteq A \times A$
Secret relation	$S \subseteq A \times A$

Some notation

Agents	$A = \{a, b, \dots\}$
Number relation	$N \subseteq A \times A$
Secret relation	$S \subseteq A \times A$
Gossip graph	$G = (A, N, S)$

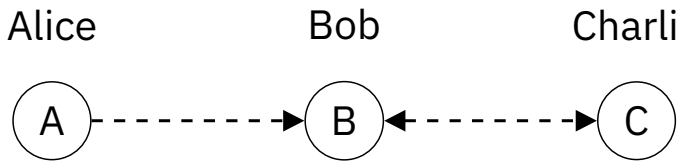
Some notation

Agents	$A = \{a, b, \dots\}$
Number relation	$N \subseteq A \times A$
Secret relation	$S \subseteq A \times A$
Gossip graph	$G = (A, N, S)$
Call	ab

Some notation

Agents	$A = \{a, b, \dots\}$
Number relation	$N \subseteq A \times A$
Secret relation	$S \subseteq A \times A$
Gossip graph	$G = (A, N, S)$
Call	ab
Identity relation	$I_A = \{\ (x, x) \mid x \in A\ \}$

Example

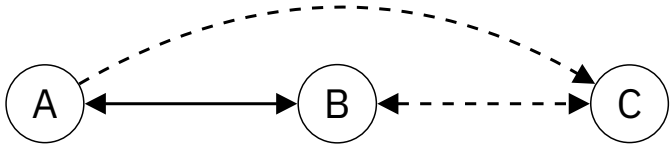


$N = \{(a, b), (b, c), (c, b)\}$

$S = I_A$

Example

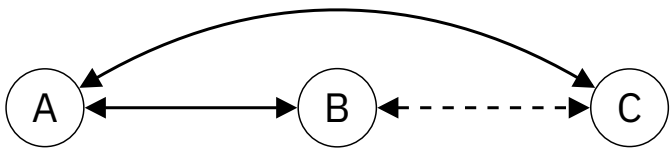
After call **ab**



$$N = I_A \cup \{(a,b),(a,c),(b,a),(b,c),(c,b)\}$$
$$S = I_A \cup \{(a,b),(b,a)\}$$

Example

After call **ac**

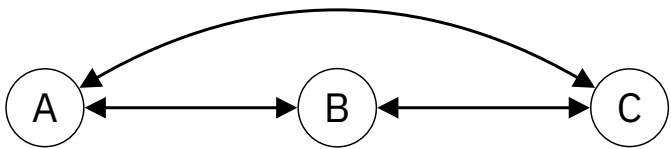


$N = A \times A$

$S = I_A \cup \{(a, b), (a, c), (b, a), (c, a)\}$

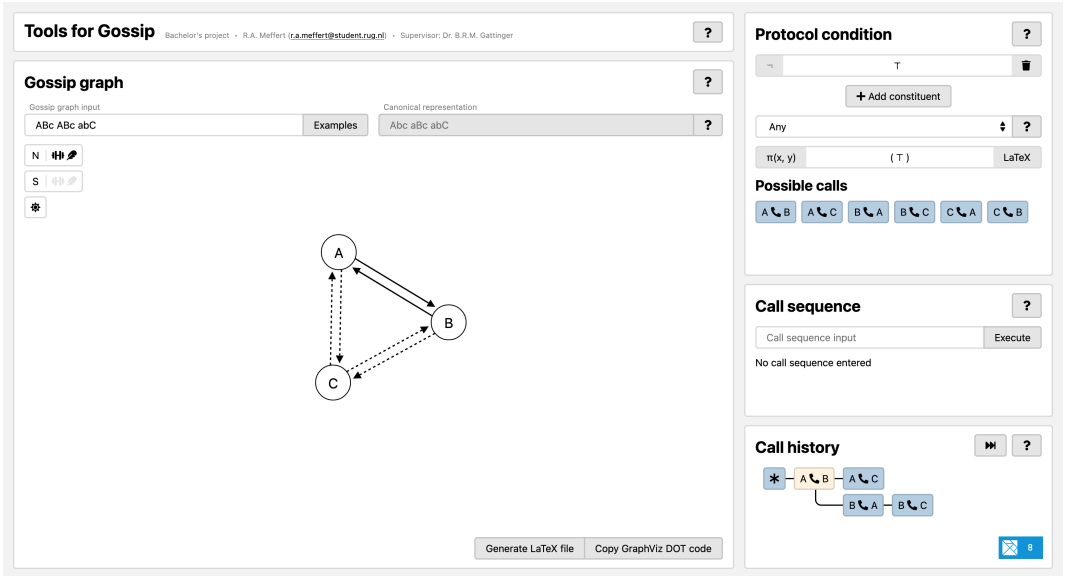
Example

After call **bc**



$$N = A \times A$$
$$S = A \times A$$

The tool


Tools for Gossip
Bachelor's project • R.A. Meffert (r.a.meffert@student.rug.nl) • Supervisor: Dr. B.R.M. Gattinger
?
Gossip graph
?
Gossip graph input
ABc ABc abC
Examples
Canonical representation
Abc aBc abC
?
N
S
A
B
C
Generate LaTeX file
Copy GraphViz DOT code
Protocol condition
?
¬
T
+ Add constituent
Any
?
π(x, y)
(T)
LaTeX
Possible calls
A B
A C
B A
B C
C A
C B
Call sequence
?
Call sequence input
Execute
No call sequence entered
Call history
?
A B
A C
B A
B C
8

Implementation

- Language: Elm [CC13]

Implementation

- Language: Elm [CC13]
- Graph visualisation & properties

Implementation

- Language: Elm [CC13]
- Graph visualisation & properties
- Execution tree

Implementation

- Language: Elm [CC13]
- Graph visualisation & properties
- Execution tree
- Call sequence validation & execution

Implementation

- Language: Elm [CC13]
- Graph visualisation & properties
- Execution tree
- Call sequence validation & execution
- Custom protocol creation*

*In last phase of development

Why Elm fits this project

- Pure functions
  - Easier to translate mathematical functions into code

Why Elm fits this project

- Pure functions
  - Easier to translate mathematical functions into code
- Compiled to Javascript
  - Free cross-platform compatibility

Why Elm fits this project

- Pure functions
  - Easier to translate mathematical functions into code
- Compiled to Javascript
  - Free cross-platform compatibility
- Static type checking
  - Zero runtime exceptions

Survey

- Short exploratory survey

Survey

- Short exploratory survey
- 12 respondents

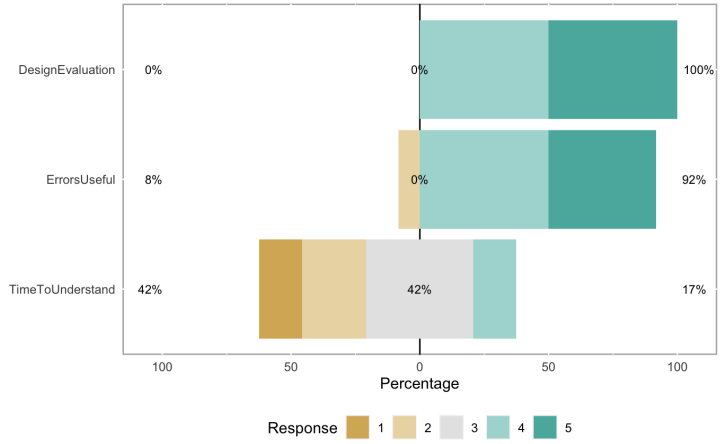
Survey

- Short exploratory survey
- 12 respondents
- General impression: positive

Survey

- Short exploratory survey
- 12 respondents
- General impression: positive
- Useful feedback

Survey



Some results from the survey. First question was (1 = very bad) to (5 = very good), second question was (1 = not useful at all) to (5 = very useful), last question was (1 = very little time) to (5 = very much time). For more results, please refer to the thesis.

Further research and extensions

- Unreliable gossip [BG20]

Further research and extensions

- Unreliable gossip [BG20]
- Higher level knowledge [HM17]

Further research and extensions

- Unreliable gossip [BG20]
- Higher level knowledge [HM17]
- Temporal gossip [Coo+19]

Further research and extensions

- Unreliable gossip [BG20]
- Higher level knowledge [HM17]
- Temporal gossip [Coo+19]
- And more!

Demo

Thanks for your attention!

Questions?

	Result	Source code
Tool	r3n.nl/bsc/gossip	r3n.nl/bsc/src/gossip
Thesis[†]	r3n.nl/bsc/thesis	r3n.nl/bsc/src/thesis
Slides	r3n.nl/bsc/slides	r3n.nl/bsc/src/slides

[†] From February 1

References I

[Bai16] Leemon Baird. ‘The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance’. In: *Swirlds, Inc. Technical Report SWIRLDS-TR-2016* 1 (2016).

[BG20] Line van den Berg and Malvin Gattinger. ‘Dealing with Unreliable Agents in Dynamic Gossip’. In: *Dynamic Logic. New Trends and Applications*. Ed. by Manuel A. Martins and Igor Sedlár. Vol. 12569. Series Title: Lecture Notes in Computer Science. Springer International Publishing, 2020, pp. 51–67. DOI: fp2t.

[CC13] Evan Czaplicki and Stephen Chong. ‘Asynchronous Functional Reactive Programming for GUIs’. In: *SIGPLAN Not.* 48.6 (June 2013), pp. 411–422. DOI: 10/f45mkb.

[Coo+19] Martin C. Cooper et al. ‘Temporal Epistemic Gossip Problems’. In: *Multi-Agent Systems*. Ed. by Marija Slavkovik. Vol. 11450. Springer International Publishing, 2019, pp. 1–14. DOI: fp2v.

References II

[DeC+07] Giuseppe DeCandia et al. ‘Dynamo: Amazon’s Highly Available Key-value Store’. In: *Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles*. SOSP ’07. Association for Computing Machinery, 2007, pp. 205–220. DOI: 10/bj8wqc.

[DGM02] A. Das, I. Gupta and A. Motivala. ‘SWIM: scalable weakly-consistent infection-style process group membership protocol’. In: International Conference on Dependable Systems and Networks. IEEE Comput. Soc, 2002, pp. 303–312. DOI: 10/dfvrrz.

[Dit+18] Hans van Ditmarsch et al. ‘Dynamic Gossip’. In: *Bulletin of the Iranian Mathematical Society* 45.3 (Sept. 2018), pp. 701–728. DOI: 10/cvpm.

[HM17] Andreas Herzig and Faustine Maffre. ‘How to share knowledge by gossiping’. In: *AI Communications* 30.1 (27th Mar. 2017), pp. 1–17. DOI: 10/f94qxh.

References III

[Lib02] David Liben-Nowell. ‘Gossip is synteny: Incomplete gossip and the syntenic distance between genomes’. In: *Journal of Algorithms* 43.2 (May 2002), pp. 264–283. DOI: 10/bkq8p9.

[Ren16] Robbert van Renesse. ‘A Blockchain Based on Gossip? – A Position Paper’. In: *Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016)*. July 2016.

[Tar+19] Dominic Tarr et al. ‘Secure Scuttlebutt: An Identity-Centric Protocol for Subjective and Decentralized Applications’. In: ICN ’19: 6th ACM Conference on Information-Centric Networking. ACM, 24th Sept. 2019, pp. 1–11. DOI: 10/ghrvm9.

[Tij71] Robert Tijdeman. ‘On a telephone problem’. In: *Nieuw Archief voor Wiskunde* 3.19 (1971), pp. 188–192.