Reasoning about Gossip

Hans van Ditmarsch
CNRS

- Dynamic Gossip

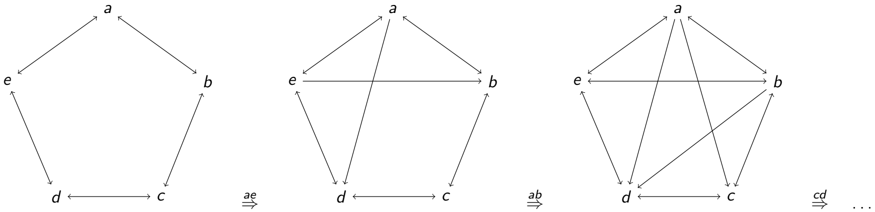
Materials found on http://reasoningaboutgossip.eu

Dynamic Gossip

On a complete gossip graph (all agents can call all agents / all agents are neighbours) $2n-4$ is optimal for all to become experts. On other connected graphs, only $2n-3$ may be optimal. For example, on a cycle $2n-3$ calls are optimal.

Example 5 agents: 6 calls is not optimal but 7 calls is optimal.

If the agents can also exchange numbers then 6 calls is optimal. (Only neighbours are displayed, not holdings of secrets.)

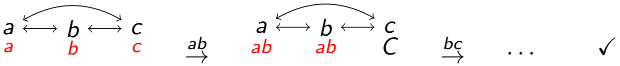


[vD, van Eijck, Pardo, Ramezanian, Schwarzentruber. *Dynamic Gossip*. Bulletin of the Iranian Mathematical Society, 2019]

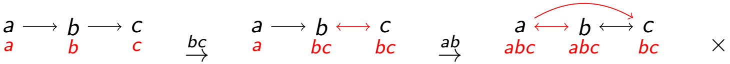
Dynamic Gossip — Learn New Secrets and Neighbours

Agents exchange all secrets and all numbers they know.

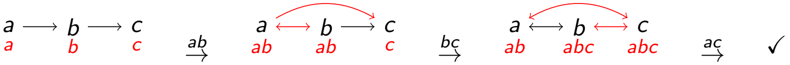
On fully connected graphs there is no difference.



On weakly connected graphs deadlock is possible. (After $bc.ab$ agent c cannot call agent a, because c does not have a's number.)



But on the same gossip graph deadlock can also be avoided. (After $ab.bc$ agent a calls agent c.)



When can deadlock sometimes or always be avoided and when not?

Dynamic Gossip — Characterization of success

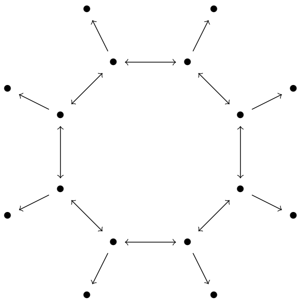
- A graph is weakly/strongly connected if there is an undirected/directed path between any two nodes.
- We distinguish gossip graphs by the properties of the neighbour relation, not the secret relation.
- No protocol is successful on a disconnected gossip graph.
- All presented protocols except LNS are strongly successful (maybe only fairly) on weakly connected gossip graphs.

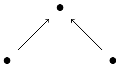
Relevant properties to show these results (let $G = (A, N, S)$):

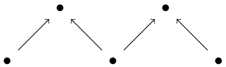
- $S \subseteq N$ you cannot know a secret without that number
- $S^\sigma \subseteq N^\sigma$ in non-dynamic gossip $N^\sigma \subset S^\sigma$ is fine!
- $S^\sigma \circ N \subseteq N^\sigma$ $(S^{\sigma.ab} \subseteq N^\sigma)$
- stable $\tau \sqsubset \sigma^\omega$ satisfy $S^\tau_x = S^\tau_y$ if for all x, y, then success
- in TOK and SPI every agent is a neighbour of a token holder

Dynamic Gossip — Characterization of LNS success

- If graph not weakly connected, unsuccessful. *Worse*:
  If graph a bush or double bush, unsuccessful.
- If graph strongly connected, strongly successful. *Better*:
  If graph a sun, strongly successful.



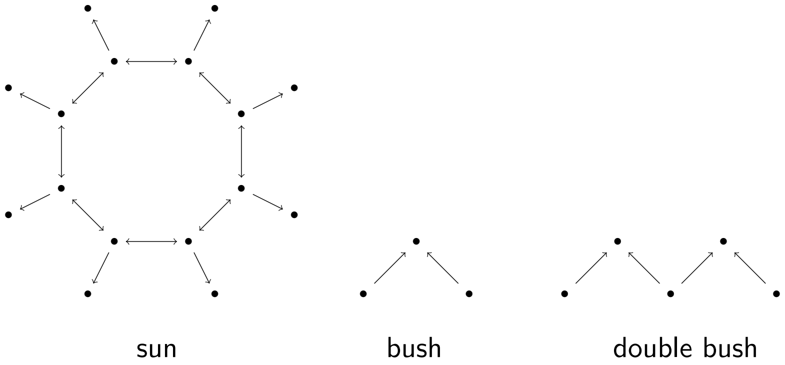




[vD, van Eijck, Pardo, Ramezanian, Schwarzentruber. *Dynamic Gossip*. Bulletin of the Iranian Mathematical Society, 2019]

Dynamic Gossip — Characterization of LNS success

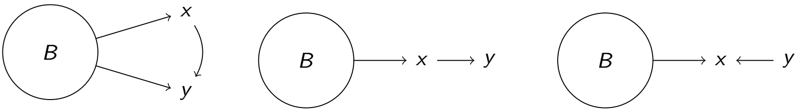
- sun: strongly connected graph linked to terminal (sink) nodes.
- bush: (converse) tree with root branching factor at least 2.
- double bush: two bushes joined in a leaf linked to their roots.



Dynamic Gossip — Characterization for LNS

- *LNS is strongly successful on a weakly connected gossip graph iff that gossip graph is a sun*

Sketch $\Rightarrow$: In all below there are LNS-maximal σ where y not expert:



σ': LNS-max for $A \backslash B$; σ'': LNS-max for B; $s(B)$: B-successors ($\notin B$)

— Bx everyone in B calls x left picture

— σ''': LNS-max for $B \cup (s(B) \backslash \{y\})$ after $\sigma'.\sigma''.Bx$

— then $\sigma'.\sigma''.Bx.\sigma'''$ is LNS-max and y is not expert

— σ''': LNS-max for $B \cup s(B)$ after $\sigma'.\sigma''$ middle/right picture

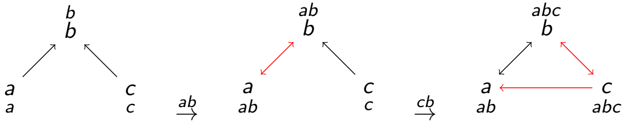
— then $\sigma'.\sigma''.\sigma'''$ is LNS-max and y is not expert

Sketch $\Leftarrow$: if σ is LNS-maximal, then $S^\sigma = N^\sigma$ and $S^\sigma \circ N^* = S^\sigma$

Dynamic Gossip — Characterization for LNS

- LNS *is weakly successful on a weakly connected gossip graph iff that gossip graph is not a bush or a double bush*

LNS is unsuccessful on the bush below. After two calls *ab.cb*:
— *b* and *c* cannot call *a* because they know the secret of *a*
— *a* does not know the secret of *c* but cannot call non-neighbour *c*



- The easy ⇒ part of the proof is to show that LNS is unsuccessful on a bush and on a double bush.
- The hard ⇐ part of the proof is to construct a successful LNS call sequence on a weakly connected gossip graph that is not a bush or a double bush. (Induction on the number of source nodes in the gossip graph and with many case distinctions.)

Dynamic Gossip — Characterization for LNS

- LNS *is weakly successful on a weakly connected gossip graph iff that gossip graph is not a bush or a double bush*

($\Rightarrow$) Sketch: One first shows the below property.

Given bush $G = (A, N, S)$ with root r, and LNS-permitted σ. Then:

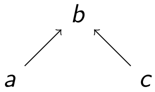
1. $G|N^\sigma_x$ is a tree.
2. $N^\sigma_x \setminus S^\sigma_x = \begin{cases} \text{root of } G|N^\sigma_x & \text{if not } S^\sigma xr \\ \emptyset & \text{otherwise} \end{cases}$

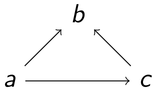
Once a child of the root calls the root, the subtrees generated by all other children are blocked, i.e., calls to those agents are not LNS-permitted. (Proof for double bush is similar to that for bush.)

($\Leftarrow$) By example only, see BIMS 2019 for full proof.

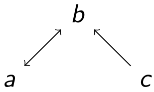
Dynamic Gossip — Characterization for LNS

Adding an edge to a bush permits LNS-successful sequences.
For example, the smallest bush.





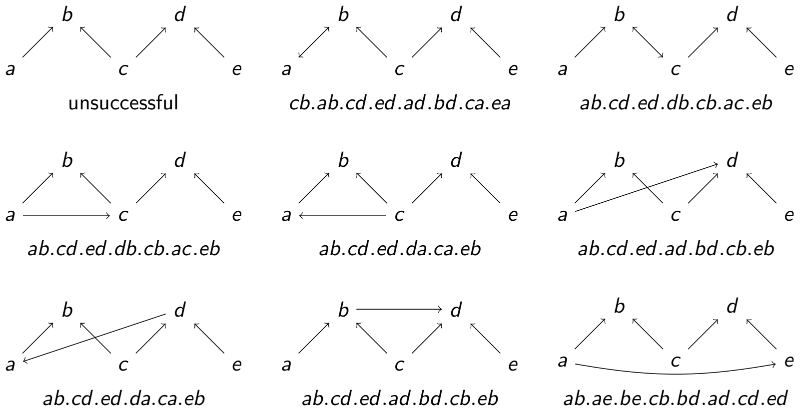
ab.ac.bc



cb.ab.ca

Dynamic Gossip — Characterization for LNS

Adding an edge to a double bush permits LNS-successful sequences. For example, the smallest double bush.



All for today!