Knowledge transfer and information leakage in protocols

Abdullah Abdul Khadir, Madhavan Mukund, S P Suresh
Chennai Mathematical Institute and UMI RELAX
{**abdullah**,madhavan,spsuresh}@cmi.ac.in

Formal Methods Update Meeting 2018
Goa, India
July 20, 2018

Information exchange in protocols

- **Protocols**
  - Structured conversation to effect information exchange
  - **Informative**: Transmit relevant information to trusted partner
  - **Safe**: Do not leak confidential data to eavesdropper(s)
- Full safety not always possible. e.g. rejecting a password
- Quantify information leakage

Studying information leakage

- **Qualitative**: Non-interference and allied notions / refinements
  - Low outputs not affected by high inputs

- **Quantitative**: Measure information leakage based on entropy

- **Our Approach**: Discrete measurement of information leakage

SADI problems

- Four agents A, B, C and E, with E being the eavesdropper
- The deal

$$\begin{array}{ll} A & 0,1 \\ B & 2,3,4 \\ C & 5,6,7,8 \end{array}$$

- Find a sequence of (truthful) announcements that help A, B, C learn the whole deal, while E does not know the whole deal

Informative and safe sequences

- A one-round protocol

A My hand is 01 or 08 or 18

Informative and safe sequences

- A one-round protocol

A	My hand is 01 or 08 or 18
B	Pass

Informative and safe sequences

- A one-round protocol

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

Informative and safe sequences

- A one-round protocol

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

- What is known at the end?

Informative and safe sequences

- A one-round protocol

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

- What is known at the end?

- Can this be promoted to a protocol?

Informative and safe sequences

- A one-round protocol

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

- What is known at the end?

- Can this be promoted to a protocol?

- Yes!

Another announcement sequence

- Another sequence

A	My hand is 01 or 12 or 23
B	My hand is 234 or 056 or 178
C	Pass

- Informative, but is it safe??

Another announcement sequence

- Another sequence

A	My hand is 01 or 12 or 23
B	My hand is 234 or 056 or 178
C	Pass

- Informative, but is it safe??
- All deals compatible with the announcement sequence
  - $(01, 234, 5678)$
  - $(12, 056, 3478)$
  - $(23, 056, 1478)$
  - $(23, 178, 0456)$

Another announcement sequence

- Another sequence

A	My hand is 01 or 12 or 23
B	My hand is 234 or 056 or 178
C	Pass

- Informative, but is it safe??
- All deals compatible with the announcement sequence
  - $(01, 234, 5678)$
  - $(12, 056, 3478)$
  - $(23, 056, 1478)$
  - $(23, 178, 0456)$
- This announcement sequence does not work in the other three cases

Another announcement sequence

- Another sequence

A	My hand is 01 or 12 or 23
B	My hand is 234 or 056 or 178
C	Pass

- Informative, but is it safe??
- All deals compatible with the announcement sequence
  - $(01, 234, 5678)$
  - $(12, 056, 3478)$
  - $(23, 056, 1478)$
  - $(23, 178, 0456)$
- This announcement sequence does not work in the other three cases
- The deal is leaked!

Another announcement sequence

- Another sequence

A	My hand is 01 or 12 or 23
B	My hand is 234 or 056 or 178
C	Pass

- Informative, but is it safe??
- All deals compatible with the announcement sequence
  - $(01, 234, 5678)$
  - $(12, 056, 3478)$
  - $(23, 056, 1478)$
  - $(23, 178, 0456)$
- This announcement sequence does not work in the other three cases
- The deal is leaked!

Informative and safe sequences - 2

- Another informative, safe sequence

  A My hand is 01 or 02 or 03 or 12 or 13 or 23

Informative and safe sequences - 2

- Another informative, safe sequence

A	My hand is	01	or 02	or 03	or 12	or 13	or 23
B	My hand is	456	or 678	or 158	or 378	or 236	or 014

Informative and safe sequences - 2

- Another informative, safe sequence

A	My hand is	01 or 02 or 03 or 12 or 13 or 23
B	My hand is	456 or 678 or 158 or 378 or 236 or 014
C	My hand is	2378 or 1345 or 2467 or 0456 or 4578 or 5678

Informative and safe sequences - 2

- Another informative, safe sequence

A	My hand is	01	or 02	or 03	or 12	or 13	or 23
B	My hand is	456	or 678	or 158	or 378	or 236	or 014
C	My hand is	2378	or 1345	or 2467	or 0456	or 4578	or 5678

- Let π_2 be a protocol obtained from above.

Informative and safe sequences - 2

- Another informative, safe sequence

A	My hand is	01	or 02	or 03	or 12	or 13	or 23
B	My hand is	456	or 678	or 158	or 378	or 236	or 014
C	My hand is	2378	or 1345	or 2467	or 0456	or 4578	or 5678

- Let π_2 be a protocol obtained from above.
- Recall the previous run (and let a protocol obtained from it be π_1)

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

Informative and safe sequences - 2

- Another informative, safe sequence

A	My hand is 01	or	02	or	03	or	12	or	13	or	23
B	My hand is 456	or	678	or	158	or	378	or	236	or	014
C	My hand is 2378	or	1345	or	2467	or	0456	or	4578	or	5678

- Let π_2 be a protocol obtained from above.
- Recall the previous run (and let a protocol obtained from it be π_1)

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

- Which is better, π_1 or π_2?

Informative and safe sequences - 2

- Another informative, safe sequence

A	My hand is	01 or 02 or 03 or 12 or 13 or 23
B	My hand is	456 or 678 or 158 or 378 or 236 or 014
C	My hand is	2378 or 1345 or 2467 or 0456 or 4578 or 5678

- Let π_2 be a protocol obtained from above.
- Recall the previous run (and let a protocol obtained from it be π_1)

A	My hand is 01 or 08 or 18
B	Pass
C	My hand is 0234 or 1237 or 5678

- Which is better, π_1 or π_2?
- Why?

Our work

- Represent the information state of agents using atomic propositions
- Atomic propositions for agents p, q ($p \neq q$) and card c
  - $K_{pq}(c)$: p knows that q has card c
  - $K_{pNq}(c)$: p knows that q does not have c.
- Valuations for agent p assign $\top$ or $\bot$ for every proposition.
- Natural constraints on valuations. For example

$$\forall q, c: \text{ either } v \not\models K_{pq}(c) \text{ or } v \not\models K_{pNq}(c)$$

Measuring knowledge for runs

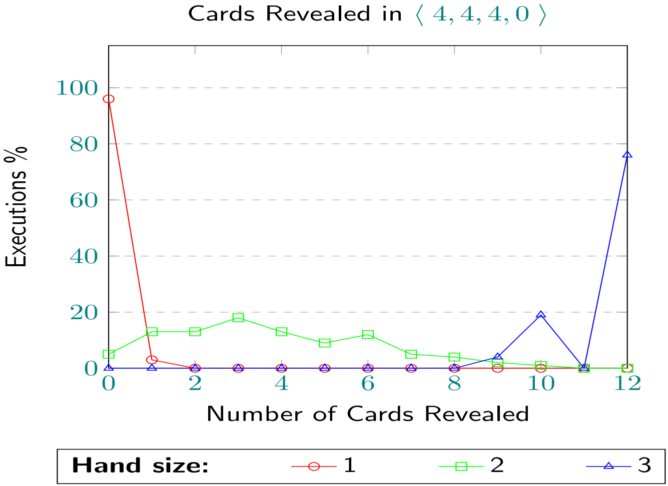
- Initial formula representing constraints on valuations
- Each announcement is a DNF formula
- Announcement sequence is a conjunction of these (ϕ)
- Use a SAT solver (Z3) to compute all hands compatible with ϕ
- Collect statistics on this final state
- E.g. if $\neg K_{pq}(c) \wedge \phi$ is unsat, it means that p knows that q has c
- Use this to search for informative and safe runs
- Coming up with a protocol – harder problem

Experiment Setup

In order to evaluate the tool we built, we

- Identified the following parameters for generating a run,
  - The size of the hand in each announcement
  - The number of disjuncts in each announcement
  - The number of announcements
- Fixed the initial distribution type as $\langle 4, 4, 4 \rangle$).
- Generate a set of runs for specific values.
- Compute statistics for each set of runs.

Results (for three disjuncts, two rounds)



Questions?

Protocols

- For deal d, let d_p denote the hand of agent p.
- An announcement is a disjunction of hands
- A protocol π is a function that
  - assigns a subset of announcements to a run ρ for deal d.
  - is turn-based : agents take turns in making announcements.
- Further, $\pi(d, \rho)$ is :
  - (**truthful**) Any announcement made by agent p must be true.

    $$\text{for all } ann \in \pi(d, \rho),\ d_p \in ann$$

  - (**view-based**) Same response if hand and sequence are the same,

    $$(d_p = f_p) \implies (\pi(d, \rho) = \pi(f, \rho))$$

Informativity

Definition (Informative run)

Run (d, ρ) of protocol π is informative for agent p if d is the only deal compatible with ρ and p's hand

Formally: For every execution (f, ρ) of π, $(d \neq f) \implies (d_p \neq f_p)$

Definition (Informative Protocols)

A protocol π is

- **weakly informative (WI):** if every (maximal) run of π is informative for some agent.
- **informative (I):** if every (maximal) run of π is informative for every agent.

Safety of cards

A card is safe if its status is not known to eavesdropper, E

Definition (Safety of cards)

A run (d, ρ) of a protocol π is **safe** for the card c, if for any agent p, if $c \in d_p$, then, there is another run (f, ρ) of π such that $c \notin f_p$.

Definition (Strong Safety of cards)

A run (d, ρ) of a protocol π is **strongly safe** for the card c if for every agent p, there are two runs $(f, \rho), (g, \rho)$ of π such that $c \in f_p$ and $c \notin g_p$.

Safety of protocols

Definition (Safety of Protocols)

A protocol π is

- **deal safe:** if every run of π is safe for some card c.
- p**-safe (for** p**):** if every run (d, ρ) of π is safe for all cards in d_p.
- **safe:** if every execution of π is safe for every card c.
- **strongly safe:** if every execution of π is strongly safe for every card c.