Knowledge transfer and information leakage in protocols

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

Formal Methods Update Meeting
IIT Mandi
July 18, 2017

Information exchange in protocols

- **Protocols**

Information exchange in protocols

- **Protocols**
    - Structured conversation to effect information exchange

Information exchange in protocols

- **Protocols**
  - Structured conversation to effect information exchange
  - **Informative**: Transmit relevant information to trusted partner

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)

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

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

Studying information leakage

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

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

Our approach

- Discrete measurement of information leakage
- Information consists of propositional facts

Our approach

- Discrete measurement of information leakage
- Information consists of propositional facts
- Represents knowledge to be shared among agents

Our approach

- Discrete measurement of information leakage
- Information consists of propositional facts
- Represents knowledge to be shared among agents
- Eavesdropper has no knowledge initially

Our approach

- Discrete measurement of information leakage
- Information consists of propositional facts
- Represents knowledge to be shared among agents
- Eavesdropper has no knowledge initially
- As messages are exchanged, agents learn more facts

Our approach

- Discrete measurement of information leakage
- Information consists of propositional facts
- Represents knowledge to be shared among agents
- Eavesdropper has no knowledge initially
- As messages are exchanged, agents learn more facts
- Measure how much eavesdropper knows at the end

Our approach

- Discrete measurement of information leakage
- Information consists of propositional facts
- Represents knowledge to be shared among agents
- Eavesdropper has no knowledge initially
- As messages are exchanged, agents learn more facts
- Measure how much eavesdropper knows at the end
- Check if honest agents know all they ought to know

SADI problems

- There are four agents A, B, C and D, with D being the eavesdropper

SADI problems

- There are four agents A, B, C and D, with D being the eavesdropper
- The deal

A	0, 1
B	2, 3, 4
C	5, 6, 7, 8

SADI problems

- There are four agents A, B, C and D, with D being the eavesdropper
- The deal

A	0, 1
B	2, 3, 4
C	5, 6, 7, 8

- Find a sequence of (truthful) announcements that help them learn the whole deal, while D does not know the whole deal

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

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??
- Other deals compatible with the announcement sequence

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??
- Other deals compatible with the announcement sequence
  - **(12, 056, 3478)**

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??
- Other deals compatible with the announcement sequence
  - $(\mathbf{12}, \mathbf{056}, \mathbf{3478})$
  - $(\mathbf{23}, \mathbf{178}, \mathbf{0456})$

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??
- Other deals compatible with the announcement sequence
  - $(\mathbf{12}, \mathbf{056}, \mathbf{3478})$
  - $(\mathbf{23}, \mathbf{178}, \mathbf{0456})$
  - $(\mathbf{23}, \mathbf{056}, \mathbf{1478})$

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??
- Other deals compatible with the announcement sequence
  - **(12, 056, 3478)**
  - **(23, 178, 0456)**
  - **(23, 056, 1478)**
- This announcement sequence does not work in those 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??
- Other deals compatible with the announcement sequence
  - **(12, 056, 3478)**
  - **(23, 178, 0456)**
  - **(23, 056, 1478)**
- This announcement sequence does not work in those cases
- The deal is leaked!

Protocols

Definition (Protocols)

A **protocol** (for a fixed deal type) is a function π assigning to every deal $\boldsymbol{H}$ of that type, and every run ρ a non-empty set of actions $\pi(\boldsymbol{H}, \rho)$ such that:

Protocols

Definition (Protocols)

A **protocol** (for a fixed deal type) is a function π assigning to every deal $\boldsymbol{H}$ of that type, and every run ρ a non-empty set of actions $\pi(\boldsymbol{H}, \rho)$ such that:

- $\boldsymbol{H}_p \in \alpha$ for all $\alpha \in \pi(\boldsymbol{H}, \rho)$ (**truthful**)

Protocols

Definition (Protocols)

A **protocol** (for a fixed deal type) is a function π assigning to every deal H of that type, and every run ρ a non-empty set of actions $\pi(H, \rho)$ such that:

- $H_p \in \alpha$ for all $\alpha \in \pi(H, \rho)$ (**truthful**)
- if $H \sim_p H'$, then $\pi(H, \rho) = \pi(H', \rho)$ (**view-based**)

Informativity of protocols

Definition (Informativity)

A run (H, ρ) of a protocol π is informative for an agent $\mathfrak{p}$ if there is no execution (H', ρ) of π with $H \sim_{\mathfrak{p}} H'$ and $H \neq H'$. A protocol π is

Informativity of protocols

Definition (Informativity)

A run (H, ρ) of a protocol π is informative for an agent p if there is no execution (H', ρ) of π with $H \sim_p H'$ and $H \neq H'$. A protocol π is

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

Informativity of protocols

Definition (Informativity)

A run (H, ρ) of a protocol π is informative for an agent p if there is no execution (H', ρ) of π with $H \sim_p H'$ and $H \neq H'$. A protocol π is

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

Safety of cards

Definition (Safety of cards)

A run (H, ρ) of a protocol π is **safe** for the card c if for every agent p, there is another run (G, ρ) of π such that $c \notin G_p$.
A run (H, 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

Safety of protocols

Definition (Safety of Protocols)

A protocol π is

- **deal safe:** if every run of π is safe for some card $\boldsymbol{c}$.

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 an agent p):** if every run (H, ρ) of π is safe for all cards in H_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 an agent p):** if every run (H, ρ) of π is safe for all cards in H_p.
- **safe:** if every execution of π is safe for every card c.

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 an agent p):** if every run (H, ρ) of π is safe for all cards in H_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.

Our work (finally!)

- Represent the information state of agents as a set of valuations

Our work (finally!)

- Represent the information state of agents as a set of valuations
- Valuations for agent p

$$v : \{K_{pq}(c), K_{pNq}(c) \mid b \text{ an agent}, q \neq p, c \text{ a card}\} \to \{\top, \bot\}$$

Our work (finally!)

- Represent the information state of agents as a set of valuations
- Valuations for agent p

$$v : \{K_{pq}(c), K_{pNq}(c) \mid b \text{ an agent}, q \neq p, c \text{ a card}\} \to \{\top, \bot\}$$

- $v(K_{pq}(c)) = \top$ for all v in a's state means a knows that b has card c

Our work (finally!)

- Represent the information state of agents as a set of valuations
- Valuations for agent p

$$v : \{K_{pq}(c), K_{pNq}(c) \mid b \text{ an agent}, q \neq p, c \text{ a card}\} \rightarrow \{\top, \bot\}$$

- $v(K_{pq}(c)) = \top$ for all v in a's state means a knows that b has card c
- $v(K_{pNq}(c)) = \top$ for all v in a's state means a knows that b does not have card c

Our work (finally!)

- Represent the information state of agents as a set of valuations
- Valuations for agent p

$$v : \{K_{pq}(c), K_{pNq}(c) \mid b \text{ an agent}, q \neq p, c \text{ a card}\} \rightarrow \{\top, \bot\}$$

- $v(K_{pq}(c)) = \top$ for all v in a's state means a knows that b has card c
- $v(K_{pNq}(c)) = \top$ for all v in a's state means a knows that b does not have card c
- It is possible that $v(K_{pq}(c)) = \bot$ and $v(K_{pNq}(c)) = \bot$ for some v

Our work (finally!)

- Represent the information state of agents as a set of valuations
- Valuations for agent p

$$\nu : \{K_{pq}(c), K_{pNq}(c) \mid b \text{ an agent}, q \neq p, c \text{ a card}\} \to \{\top, \bot\}$$

- $\nu(K_{pq}(c)) = \top$ for all ν in a's state means a knows that b has card c
- $\nu(K_{pNq}(c)) = \top$ for all ν in a's state means a knows that b does not have card c
- It is possible that $\nu(K_{pq}(c)) = \bot$ and $\nu(K_{pNq}(c)) = \bot$ for some ν
- Natural constraints on valuations. For example

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

Measuring knowledge for runs

- Initial formula representing constraints on valuations

Measuring knowledge for runs

- Initial formula representing constraints on valuations
- Each announcement is a DNF formula

Measuring knowledge for runs

- Initial formula representing constraints on valuations
- Each announcement is a DNF formula
- Announcement sequence is a conjunction of these

Measuring knowledge for runs

- Initial formula representing constraints on valuations
- Each announcement is a DNF formula
- Announcement sequence is a conjunction of these
- Use a SAT solver (Z3) to compute all hands compatible with this formula φ

Measuring knowledge for runs

- Initial formula representing constraints on valuations
- Each announcement is a DNF formula
- Announcement sequence is a conjunction of these
- Use a SAT solver (Z3) to compute all hands compatible with this formula φ
- Collect statistics on this final state

Measuring knowledge for runs

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

Measuring knowledge for runs

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

Measuring knowledge for runs

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

Questions?

Thank you!