182.703: Problems in Distributed Computing
(Part 7)
WS 2021

Ulrich Schmid
Institute of Computer Engineering, TU Vienna
Embedded Computing Systems Group E191-02
s@ecs.tuwien.ac.at
Outline (Part7)

Esoterics:

- Epistemic Logic in Distributed Computing
- Algebraic Topology in Distributed Computing
Epistemic Logic in Distributed Computing
Multi-Agent Systems

• Set of communicating **agents**
  – optional: **sensors**
  – optional: **actuators**

• Any means of communication
  – message passing
  – shared memory

• Evolution of global system state
The Cheating Husbands Problem [MDH86]

In an attempt to solve the male infidelity problem once and forever, Queen Henrietta I from Mamajorca, on the continent of Atlantis, summoned all of the women heads-of-households to the town square and read the following statement:

*There are (one or more) unfaithful husbands in our community. Although none of you knew before this gathering whether your own husband was unfaithful, each of you knows which of the other husbands are unfaithful. I forbid you to discuss the matter of your husband’s fidelity with anyone. However, should you discover that your husband is unfaithful, you must shoot him on the midnight of the day you find out about it.*

Thirty nine silent nights went by, and on the fortieth night, shots were heard.
Example: CHP as a Multi-Agent System

• Set of agents
  – Queen Henrietta
  – Women a, b, c

• Means of communication
  – Queen‘s public announcement
  – (almost) shared fidelity status („number on forehead“)
Kripke Model $M = <S, R, V>$ for Global States

- Set of states („possible worlds“ $S$) agents can be in

- Each state characterized by valuation of atomic propositions $h_a h_b h_c$
  - $h_a = 0$ ... $a$‘s husband is faithful
  - Fixed according to valuation function $V$

- Agents‘ indistinguishability relation $R$ between states
Basic Epistemic Logic

- $M,s \vDash \varphi$, for formulas $\varphi$ consisting of
  - atomic propositions
  - first-order propositional logic operators ($\neg$, $\land$)
  - Knowledge modality $K_a$

  $M,s \vDash K_a \varphi$ iff $\forall s'$ with $s R_a s'$ : $M,s' \vDash \varphi$

- $K_a$ is S5-type modality (= $R$ is equivalence relation):
  - Axiom K: $K_a (\varphi \to \psi) \to (K_a \varphi \to K_a \psi)$
  - Axiom T: $K_a \varphi \to \varphi$ (factivity)
  - Axiom 4: $K_a \varphi \to K_a K_a \varphi$ (positive introspection)
  - Axiom 5: $\neg K_a \varphi \to K_a \neg K_a \varphi$ (negative introspection)
Epistemic Logic Extensions

- Extended knowledge operators: For a group $G$ of agents (drop $G$ if $G$ are all agents)
  - "Everybody knows": $E_G \varphi \equiv \bigwedge_{a \in G} K_a \varphi$, $E_G^2 \varphi \equiv E_G (E_G \varphi)$, ...
  - "Common knowledge": $C_G \varphi \equiv \bigwedge_{k \geq 1} E_G^k \varphi$

- Epistemic logic allows to reason in one Kripke model
  - What about time evolution?
  - What about communication?

---

U. Schmid

Epistemic Logic and Topology
Runs and Systems Framework [HM90] (I)

• Most popular knowledge-based approach in distributed computing
  – Run $r$ of a protocol = sequence of global states $r(1), r(2), ...$
  – Run is equivalent to a sequence of Kripke models
  – System $I = \text{set of all possible runs}$

• Knowledge modality $K_a$ now reads:
  $$I, r, t \models K_a \varphi \iff \forall r' \in I, t' \geq 0 \text{ with } r_a(t') = r_a(t): I, r', t' \models \varphi$$

• Standard temporal modalities
  – $I, r, t \models \Box \varphi \iff \forall t' \geq t: I, r, t' \models \varphi$
  – $I, r, t \models \Diamond \varphi \iff \exists t' \geq t: I, r, t' \models \varphi$
Runs and Systems Framework [HM90] (II)

Main question: How to generate set of runs \( I \)?

- **Agent protocols**
  - Communicating state machines
  - Transition relation
    \( r(t) \rightarrow r(t+1) \)

- **Environment protocol**
  - External events
  - Agent scheduling
  - Message deliveries
  - Faults
Runs and Systems Framework [HM90] (III)

- Many interesting results:
  - Formalization
  - Connection between consensus and common knowledge
  - Impossibility of establishing common knowledge in the case of unreliable communication

- A lot of follow-up work:
  - Knowledge of precondition principle [Mos15]: If $\phi$ is necessary for $a$ to act, then $K_a \phi$ necessary for acting
  - Necessary & sufficient knowledge for solving ordered response problem [BM14]
  - Necessary & sufficient communication structures for achieving nested knowledge [BM14]
Cheating Husbands Protocol

*M before Queen‘s statement (t=0):*

- In state r(0), agent a knows "
  - $I, r, 0 \models \neg K_a (h_a = 1)$
  - $I, r, 0 \models \neg K_b (h_b = 1)$
  - $I, r, 0 \models \neg K_c (h_c = 1)$

- No action = No results
Cheating Husbands Protocol: 1 Unfaithful

$M'$ after Queen‘s statement ($t=1$):

On first day midnight:

$I,r,1 \models \neg K_a (h_a=1)$
$I,r,1 \models \neg K_b (h_b=1)$
$I,r,1 \models K_c (h_c=1)$
Cheating Husbands Protocol: 2 Unfaithful

\[
M' \text{ after Queen's statement (} t=1 \text{):}
\]

\[
\begin{align*}
I, r, 1 & \models \neg K_a (h_a=1) \\
I, r, 1 & \models \neg K_b (h_b=1) \\
I, r, 1 & \models \neg K_c (h_c=1)
\end{align*}
\]

On first day midnight:
Cheating Husbands Protocol: 2 Unfaithful

$M$“ after first night
(t=2):

On second day midnight:

$I,r,2 \models K_a (h_a=1)$
$I,r,2 \models K_b (h_b=1)$
$I,r,2 \models \neg K_c (h_c=1)$
Iterated Group Knowledge in CHP

Abbreviate

\[ m \equiv (h_a=1) \lor (h_b=1) \lor (h_c=1) \quad [\text{"there is at least one unfaithful husband"}] \]
\[ m(k) \equiv \text{"there are at least } k \text{ unfaithful husbands"} \quad [m = m(1)] \]

• After Queen’s public announcement [in case of } K \geq 1 \text{ unfaithful husbands}]:
  \[ I,r,1 \models C \ m, \text{ and hence also } I,r,1 \models E^k \ m, \text{ for every } k \geq 1 \]
  \[ I,r,1 \models E \ m(1) \land E \ m(K-1) \quad [\text{by } \text{"number on forehead"!}] \]

• At midnight of day } k:\n  \[ I,r,k \not\models E \ m(k) \quad \text{BUT} \quad I,r,K \models E \ m(K) \]

• For solving CHP, one actually only needs } I,r,K \models E^K \ m
Common Knowledge

• Achieving common knowledge $I, r, t \models C m$ of a fact $m$ in message-passing systems is difficult [HM90]:
  – impossible if messages may be lost
  – Even impossible for uncertain message delays $\delta \in \{0, \varepsilon\}$: $(K_R K_D)^k m$ cannot be attained before time $s+k\varepsilon$!

\[ K_R m \quad \rightarrow \quad K_R K_D m \quad \rightarrow \quad K_R K_D K_R K_D m \]

• Weaker forms: $\varepsilon$ and eventual common knowledge
Byzantine Faulty Agents [KPSFG19]

• Epistemic reasoning in the presence of Byzantine faulty agents

• Challenges:
  – Modeling framework
  – Necessary & sufficient knowledge for solving some DC problem
  – Necessary & sufficient communication structures

[BM14] I,r,t ⊨ K_c K_b K_a START
Dynamic Epistemic Logic

Incorporate communication in the logic itself

- Public announcement logic
- Action models [DHK08]
  - standard epistemic state model $M$
  - additional epistemic model for communication actions
Action Models and Communication Complexity

- Action models and communication complexity
  - Queen’s initial broadcast could be replaced by single point-to-point message!
  - Only sent in states with **single** unfaithful husband!
  - Less bits communicated system-wide

- Research questions:
  - Relation between a priori knowledge and communication complexity?
  - Relation between #components in Kripke model and communication complexity?
Topology in Distributed Computing
Indistinguishability (again)

- Remember Kripke model
- Alternative: Simplicial complex
Cheating Husbands Protocol: 3 Unfaithful

Before queen‘s statement

After queen‘s statement

After first night:

After second night:
Basics Simplicial Complexes

• **(Geometric) simplex** $S^n$
  – spanned by $n+1$ affinely independent vertices $\{v_0, v_1, \ldots, v_n\}$ (representing processors’ local states)
  – **Face** = simplex spanned by subset of vertices
  – **Boundary** = union of all proper faces

• **Simplicial complex** $C$
  – set of simplexes (colored by process ids)
  – $C$ closed w.r.t. faces
Complexes in Distributed Computing

- Associated complexes:
  - Input complex \( I \) (n-sphere)
  - Output complex \( O \)
  - Protocol complex \( P \): Evolution of input complex during protocol

- E.g. k-set agreement problem:
  - \( n+1 \) processes with local inputs \( \{x_0, \ldots, x_n\} \) (binary values)
  - every non-crashing process \( i \) computes output \( y_i \)
  - System-wide at most \( k \) different \( y_i \) for \( n=1, k=1: n=2, k=2 \)

- **Wait-free impossible** for \( k \leq n \)

U. Schmid  
Epistemic Logic and Topology  
TU Wien Informatics
Simplicial and Carrier Maps

- **Simplicial map** $\mu : P \rightarrow O$ maps simplex $\sigma \in P$ to simplex $\mu(\sigma)$ [this $\mu$ is called a decision map $\delta$]

- **Carrier map** $\Delta : I \rightarrow 2^O$ assigns to each input simplex $\sigma \in I$ a set of allowed output simplices $\Delta(\sigma)$
Chromatic Subdivision for IIS SHM Model (I)

- Protocol complex P (in Iterated Immediate Snapshot model):
  - Chromatic subdivision of input complex I
  - Carrier-preserving: Every simplex in P lies in some input simplex
Chromatic Subdivision for IIS SHM Model (II)

- Two subdivided neighboring simplices
Chromatic Subdivision for IIS SHM Model (III)

\[ \chi^2(I) : \text{two rounds of IIS} \]
Wait-free Impossibility of n-Set Agreement

- Sperner's lemma:
  - Color vertices of I differently
  - For any vertex map from P to I
  - There is some $\sigma^n \in P$ where all colors are different

- Existence of $\sigma^n$ contradicts n-set agreement requirement among n+1 processes
Relation Epistemic Logic and Topology

• Use simplicial complexes and algebraic topology for epistemic reasoning
  – Unlike Kripke models, simplicial complexes make indistinguishability relation explicit
  – Re-cast existing epistemic results may result in new insights
  – The powerful theorems of algebraic topology may give new results in epistemic reasoning
Outlook: Point-Set Topology [NSW19]

• Consider space of infinite executions of a distributed algorithm

• Define metric topologies on it to reason about solvability/impossibility
References (I)

The End

Thank you for your attention!