Epistemic Logic with Common and Distributed Knowledge

Natasha Alechina   Brian Logan

Utrecht University

n.a.alechina@uu.nl   b.s.logan@uu.nl

Group or Collective Knowledge

A group of agents A can "know" that φ in several different epistemic modes:

- $E_A\varphi$: everybody in A knows that φ (or: A have mutual knowledge that φ)
- $C_A\varphi$: it is a common knowledge among A that φ
- $D_A\varphi$: A have distributed knowledge that φ

Language of epistemic logic with common and distributed knowledge

Definition (Syntax of ELCD)

$$\varphi := p \mid \neg\varphi \mid \varphi \wedge \psi \mid K_i\varphi \mid E_A\varphi \mid C_A\varphi \mid D_A\varphi$$

- where $p \in \mathcal{PV}$, $i \in Agt$ and $A \subseteq Agt$
- $E_A\varphi$ is not included in the name of the logic because it is easily definable as $\bigwedge_{i\in A} K_i\varphi$
- also, $K_i\varphi$ is definable as $D_{\{i\}}\varphi$

Group Knowledge: Semantics

or truth definitions

In state q, everybody in A knows ϕ if and only if for every state q prime which is indistinguishable from q by a group indistinguishability relation holds ϕ

- $\mathcal{M}, q \models E_A\varphi$ iff $\mathcal{M}, q' \models \varphi$ for every q' such that $q \sim_A^E q'$, where $\sim_A^E = \bigcup_{i \in A} \sim_i$

$$E_A\varphi = \bigwedge_{i \in A} K_i\varphi$$

- $\mathcal{M}, q \models C_A\varphi$ iff $\mathcal{M}, q' \models \varphi$ for every q' such that $q \sim_A^C q'$, where $\sim_A^C$ is the transitive closure of $\sim_A^E$

$$C_A\varphi = E_A\varphi \wedge E_A E_A\varphi \wedge E_A E_A E_A\varphi \wedge \ldots$$

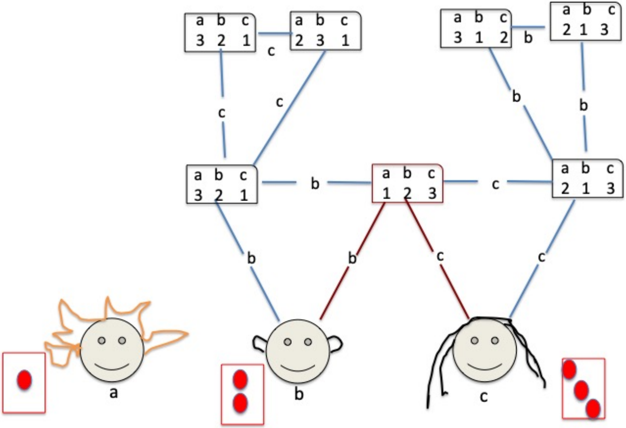
- $\mathcal{M}, q \models D_A\varphi$ iff $\mathcal{M}, q' \models \varphi$ for every q' such that $q \sim_A^D q'$, where $\sim_A^D = \bigcap_{i \in A} \sim_i$

Intuitions

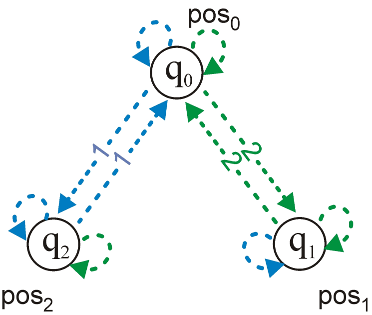
- $E_A\varphi$: everyone in A knows, but not necessarily know that others know
- $D_A\varphi$: if agents in A communicate their knowledge to each other, they will all come to know φ (actually: this is only true for positive knowledge and under some additional conditions)
- $C_A\varphi$: holds for example when all agents observe the same event φ and see each other observing it; or they are playing a game and have common knowledge of the rules of the game.

Example: Distributed Knowledge

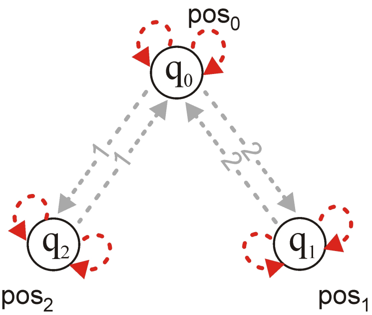
$D_{b,c}(a1 \wedge b2 \wedge c3)$



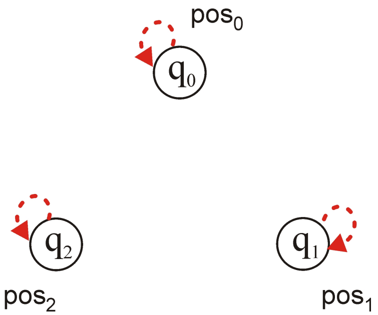
Example: Distributed Knowledge



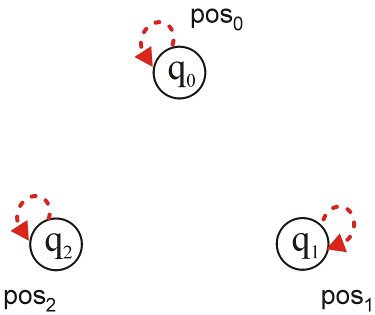
Example: Distributed Knowledge



Example: Distributed Knowledge

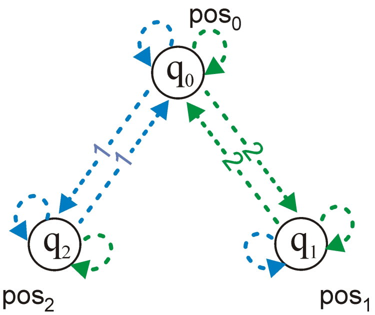


Example: Distributed Knowledge

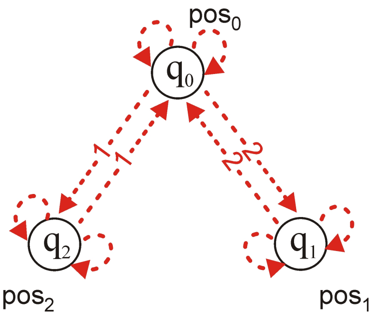


$$\text{pos}_2 \rightarrow D_{\{1,2\}}\text{pos}_2$$

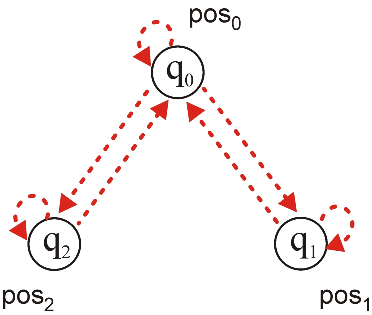
Example: Mutual Knowledge ("Everybody Knows")



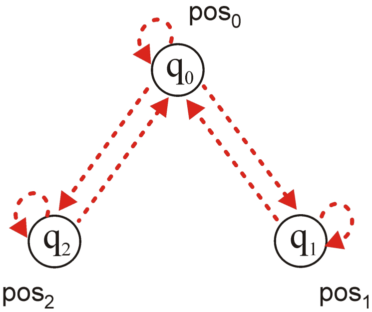
Example: Mutual Knowledge ("Everybody Knows")



Example: Mutual Knowledge ("Everybody Knows")

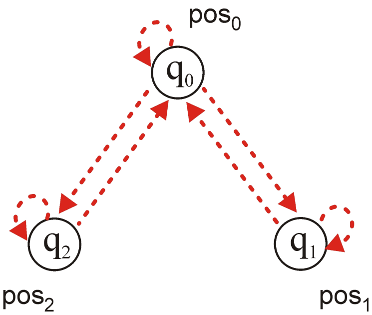


Example: Mutual Knowledge ("Everybody Knows")



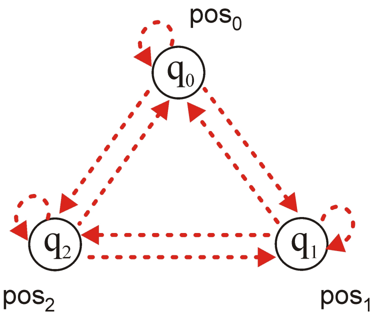
$$pos_2 \rightarrow \neg E_{\{1,2\}} pos_2$$

Example: Mutual Knowledge (“Everybody Knows”)



$$\text{pos}_2 \rightarrow \neg E_{\{1,2\}}\text{pos}_2$$
$$\text{pos}_2 \rightarrow E_{\{1,2\}}\neg\text{pos}_1$$

Example: Common Knowledge



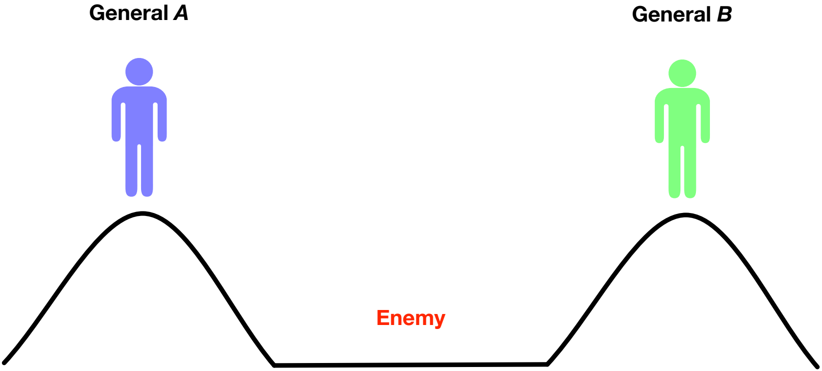
If there exists a path between states
(know about q2 -> q0 and then from q0 -> q1),
there exists a single edge.

That's why we create the connection between q2 and q1.

$$pos_2 \rightarrow \neg C_{\{1,2\}} pos_2$$
$$pos_2 \rightarrow \neg C_{\{1,2\}} \neg pos_1$$

Coordinated Attack Problem (aka Byzantine Generals)

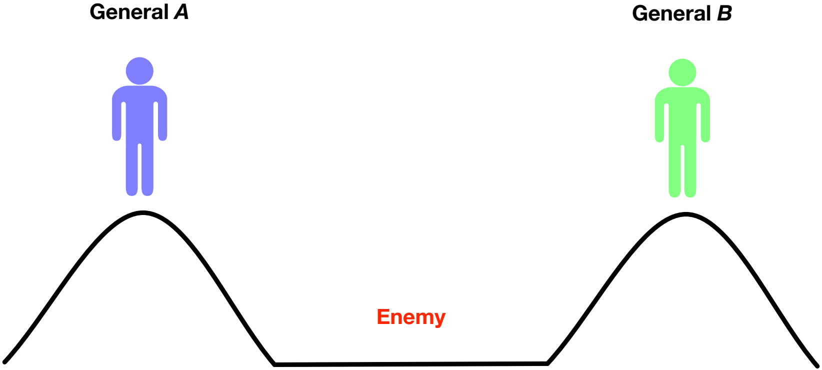
- only simultaneous attack will succeed
- suppose General *A* sends General *B* a proposal to attack at dawn and waits for confirmation from *B*
- messenger may be intercepted by the enemy



Coordinated Attack Problem

$$\Leftarrow$$

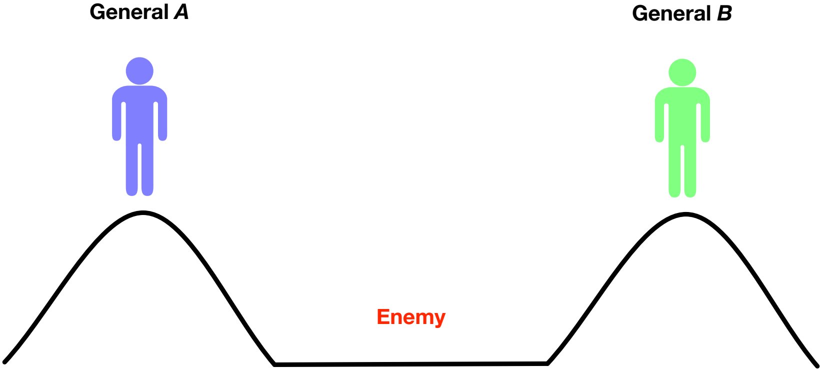
$$E_{A,B}\text{attack\_at\_dawn} \wedge \neg K_B K_A E_{A,B}\text{attack\_at\_dawn}$$



Coordinated Attack Problem

$$\Rightarrow$$

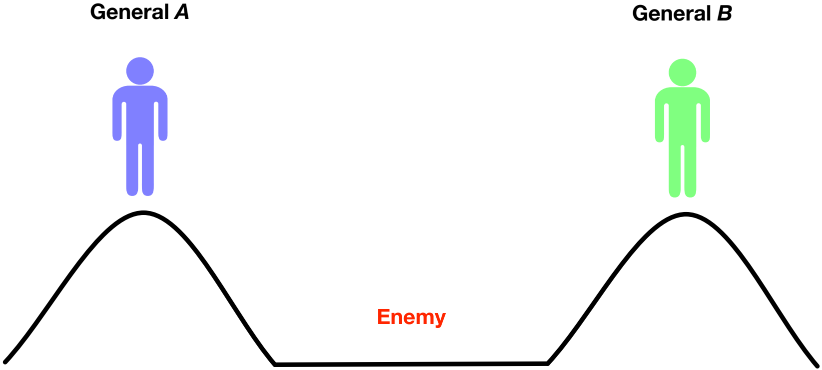
$$E_{A,B}E_{A,B}\text{attack\_at\_dawn} \wedge \neg K_A K_B E_{A,B}E_{A,B}\text{attack\_at\_dawn}$$



Coordinated Attack Problem

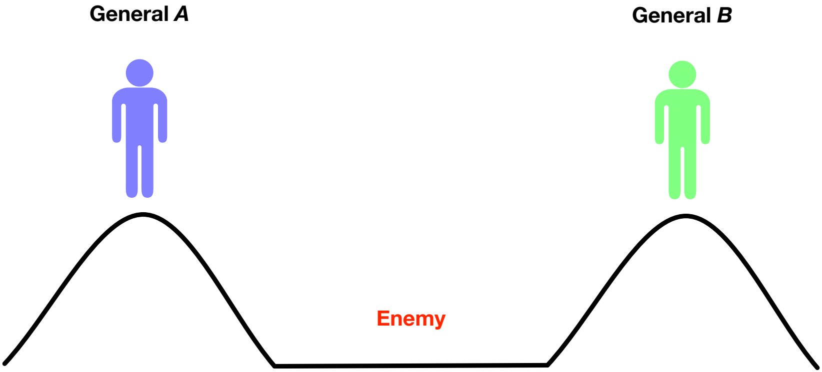
$$\Leftarrow$$

$$E_{A,B}E_{A,B}E_{A,B}\text{attack\_at\_dawn} \wedge \neg K_B K_A E_{A,B}E_{A,B}E_{A,B}\text{attack\_at\_dawn}$$



Coordinated Attack Problem

$$E^k_{A,B}\text{attack\_at\_dawn} \ldots \wedge \neg C_{A,B}\text{attack\_at\_dawn}$$



Application of epistemic logic in distributed systems

- the paper using the notion of knowledge to analyse distributed systems received Gödel prize in 1997:
- see Halpern and Moses Knowledge and Common Knowledge in a Distributed Environment. Journal of the ACM 37(3): 549-587 (1990)