Goals of the lecture

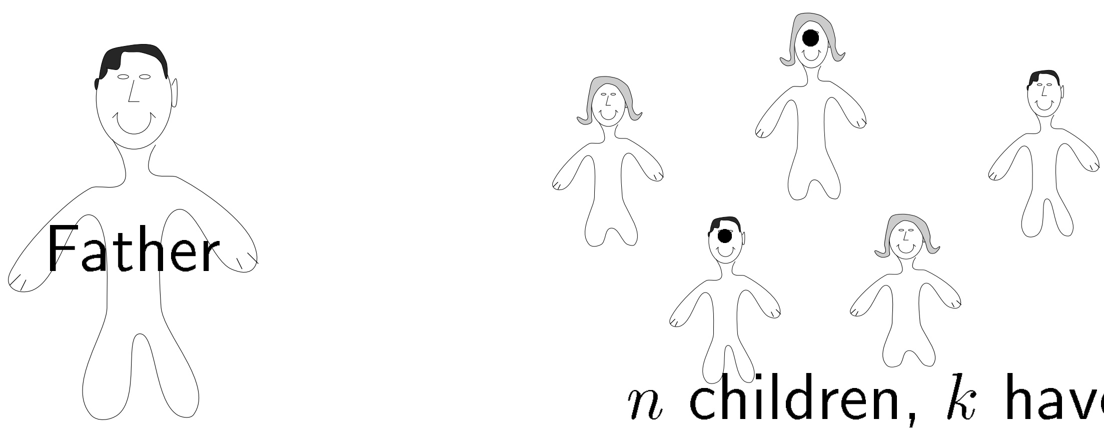
- Knowledge Hierarchy

- Relevance to Distributed Systems

- Impossibility of achieving common knowledge

Puzzle

- Father : at least one of you have mud on your forehead (S)
- He repeatedly asks the question: Do you know if you have mud on your forehead ?
- What happens ?



n children, k have mud

Solution

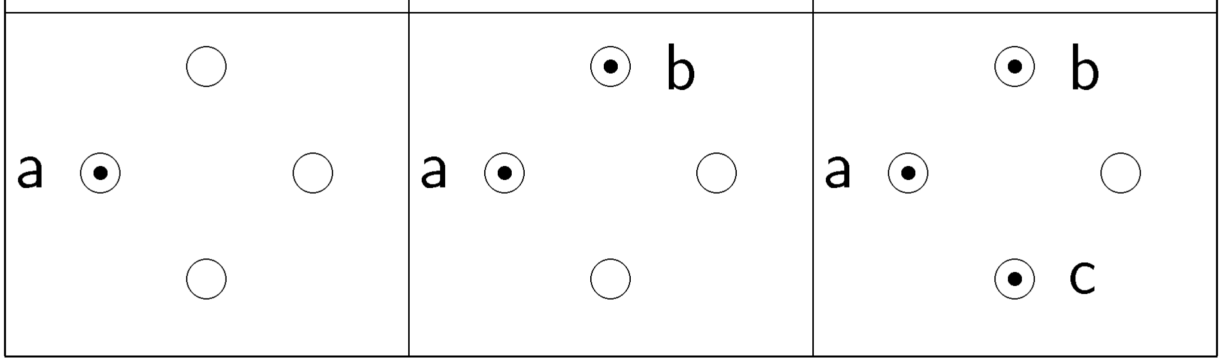
First $k-1$ times : all say "No".

k^{th} time : dirty children say "Yes".

Proof: (by induction on k)

$$k = 1, 2$$
$$k = i \rightarrow i + 1$$

$k = 1$	$k = 2$	$k = 3$



$\square$

Puzzle [Contd.]

- Let $k > 1 \quad \Rightarrow \quad$ Father did not tell the children anything they did not know.

- What if S was not stated ?

- What is the role of S ?

Assumptions

- Knowledge is monotone
  - no forgetting
  - p is true at t_0 $\Rightarrow$ p is always true.
- Processes are not faulty
  - honest processes

Definitions

$$K_i\, p \;\equiv\; \text{individual } \underline{i} \text{ knows } \underline{\text{p}}$$

Knowledge Axiom

$$K_i\, p \;\Rightarrow\; p$$

G: group of individuals

Levels of Knowledge

Implicit Knowledge : $I_G\, p$

$$\left.\begin{array}{c} K_i\, q \\ K_j\, (q \Rightarrow p) \end{array}\right\} \Rightarrow \; I_G\, p$$

Someone Knows : $S_G\, p$

$$S_G\, p \equiv \bigvee_{i \in G} K_i\, p$$

Everyone Knows : $E_G\, p$

$$E_G\, p \equiv \bigwedge_{i \in G} K_i\, p$$

Levels of Knowledge [Contd.]

Everyone$^{\mathrm{k}}$ Knows : $E_G^k\, p$

$$E_G^1\, p \equiv E_G\, p$$
$$E_G^{k+1}\, p = E_G\, E_G^k\, p$$

Common Knowledge : $C_G\, p$

$$C_G\, p \equiv p \wedge E_G\, p \wedge E_G^1\, p \wedge E_G^2\, p \wedge \cdots$$

Dirty Children

m : There are children with mud on their forehead.

Before S

- $k = 2$: m $(true)$, $E\,m$ $(true)$, $E^2\,m$ $(false)$
- $k = 3$: m $(true)$, $E\,m$ $(true)$, $E^2\,m$ $(true)$, $E^3\,m$ $(false)$.

Check : with $E^k\,m$ dirty children can prove
$E^{k-1}\,m$ they cannot.

After S

$$C\,m \;\Rightarrow\; E^k\,m$$

Knowledge and Distributed Systems

- Knowledge hierarchy

$$C\,p \Rightarrow \cdots \Rightarrow E^{k+1}\,p \Rightarrow \cdots \Rightarrow E\,p \Rightarrow S\,p \Rightarrow I\,p \Rightarrow p$$

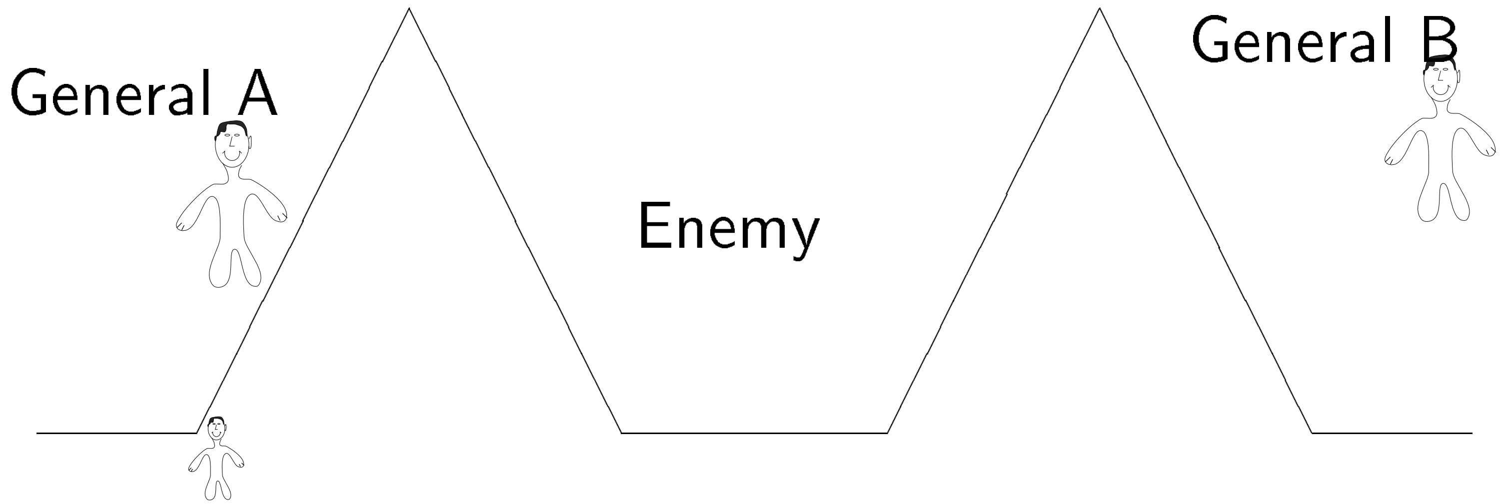
How does the level of knowledge of a fact p changes ?

- Examples:
  - fact discovery (I_p to S_p)

    deadlock detection
  - fact publication (S_p to C_p)

    new common protocol

Coordinated Attack Problem



Message Delivery not guaranteed

Q: Can the generals coordinate their attack ?

Coordinated Attack [Contd.]

Theorem 1 *There is no protocol for attaining common knowledge if communication is not guaranteed.*

Proof: no message delivered □

Q: How about any run of protocol instead of all runs of protocol ?

Coordinated Attack [Contd.]

Theorem 2 *If q is not common knowledge then no run of any protocol ever attains $C\,q$.*

Proof: Let p have n messages.
Induction on n. $\square$

Q: What if communication is guaranteed ?

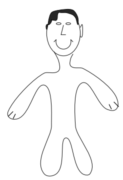
- any message takes either 0 time or ϵ time.

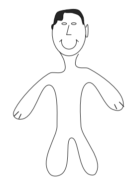
Coordinated Attack [Contd.]

Theorem 3 *Common knowledge is still unattainable*

Proof:

R_2 D_2





t_r	m is true	t_d	
$t_r + \epsilon$	D_2 knows m	$\vdots$	
$t_r + 2\epsilon$	D_2 knows R_2 knows D_2 knows m	$t_d + \epsilon$	R_2 knows D_2 knows m

$$\left.\begin{array}{cc} m & t_r \\ K_R\, K_D\, m & t_r + \epsilon \\ K_R\, K_D\, K_R\, K_D\, m & t_r + 2\epsilon \\ \vdots & \\ (K_R\, K_D)^n\, m & t_r + n\epsilon \end{array}\right\} \Rightarrow$$

m can never be common knowledge

$\square$

ϵ-Common Knowledge

Common Knowledge : any message will arrive in at most ϵ time.

- R_2 initially knows m.
- within ϵ both will know $m \equiv m_1$
- within ϵ both will know m_1

$O^\epsilon = \epsilon$ time units later

$$C^\epsilon\, p \equiv p \wedge O^\epsilon E\, p \wedge \cdots \wedge (O^\epsilon E)^n\, p \cdots$$

Asynchronous Communication

Every message sent will eventually reach

$$R_2 \xrightarrow{m} D_2$$

R_2 knows

m
eventually D_2 will know m
eventually D_2 will know that
R_2 will know that D_2 will know m

$$C^{\diamond}\, p \equiv p \wedge \diamond E\, p \wedge \cdots \wedge (\diamond E)^n\, p \wedge \cdots$$

$\diamond \equiv$ eventually

Cheating to Attain $C\,m$

R_2 sends "$C\,m$" instead of "m" and asserts $C\,m$.

message takes 0 time	message takes ϵ time
both assert $C\,m$ simultaneously	inconsistency for ϵ time

Weak Common Knowledge

Examples:

- within ϵ
- eventually
- with probability π
- likely

can be attained

- and then you can cheat to get common knowledge.

Conclusions

Common Sense may be uncommon but

Common Knowldege is Impossible

(in a distributed system)