Slide 1

COMP3152/9152
Lecture 1
Knowledge in Distributed Systems
(An Introduction)

Ron van der Meyden

Slide 2

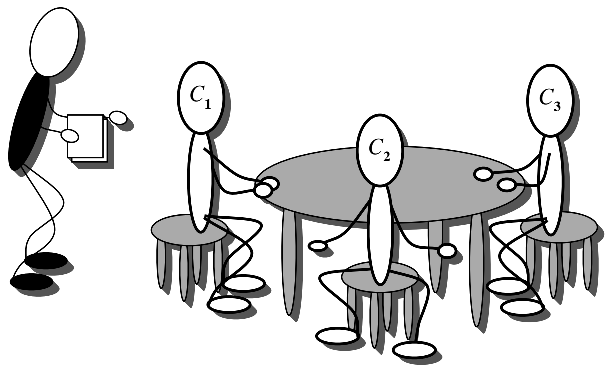
The main problem *unique* to distributed systems is a lack of (global) knowledge. It is difficult (probably impossible) for one node to know everything about the rest of the network. Yet global knowledge seems to be required to answer questions such as "Where is the file A", "Is there a deadlock", [or] "What is the best way to answer the question.... " (Gray, 1979)

"Once the sender receives the acknowledgement, it *knows* that the current packet has been delivered; it can then safely discard the current packet and send the next."

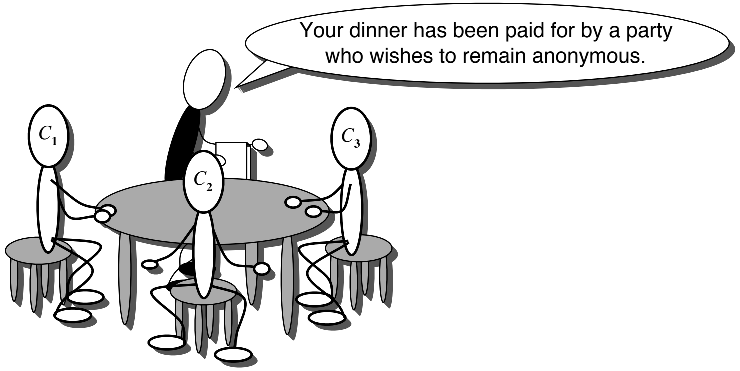
Slide 3

Chaum's Dining Cryptographers protocol

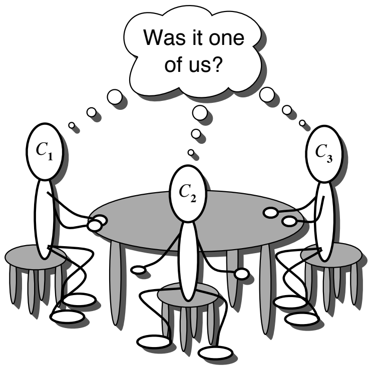
Slide 4



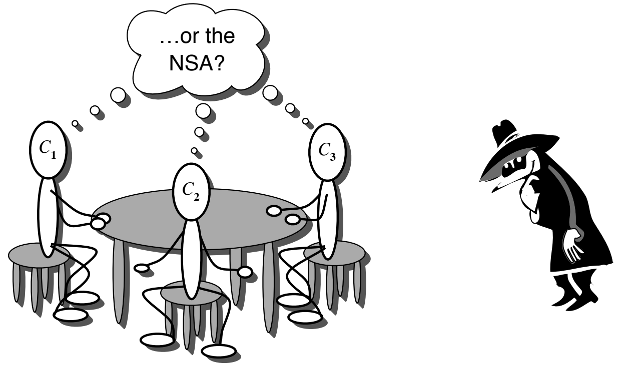
Slide 5



Slide 6



Slide 7



Slide 8

Knowledge Theoretic Specification

We want a protocol that will get us to a state where...

If C1 did not pay, then either

1. C1 knows that the NSA paid, or
2. C1 knows that either C2 or C3 paid, but does not know which one.

Similarly for the others ...

Slide 9

Knowledge Based Programs

A knowledge-based program:

```
wait until Know(position in Goal);
halt.
```

lide 10

The Muddy Children

n (very smart) children have been out playing in the garden. They were supposed to keep clean, but some of them have got mud on their forehead. They can't see their own forehead, but can see the forehead of every other child. Father comes along ....

Slide 11

Version 1: Father asks "Which of you know whether you have mud on your forehead?" Repeats the question....

Version 2: Father says "At least one of you has a dirty forehead." then asks "Which of you know whether you have mud on your forehead?" Repeats the question....

What happens? Why is there a difference?

Slide 12

Plan

Introduction, Semantic models for Knowledge
Logics of Knowledge - Axioms and Model Checking
Semantic Models for Knowledge and Time
Properties of Knowledge and Time
Dynamics of Common Knowledge
Model Checking Knowledge and Time
Knowledge-based programs
Applications to Distributed Algorithms
Applications to computer security
Variants of Common Knowledge
The logic of knowledge and probability
Connections to economics: epistemic game theory

lide 13

Textbook

Reasoning about Knowledge, Fagin, Halpern, Moses and Vardi, MIT Press, 2nd edition, 2003.

Assessment

6 problem sets, due weeks 2,4,6,8,10,12

Final Mark = best 5/6 each worth 20%

lide 14

Semantic Models for Knowledge

Reading, FHMV Ch 1 & 2

Slide 15

Propositional (Boolean) Logic

Let Φ be a set of atomic propositions, each intended to represent a sentence.

E.g.

$\texttt{muddy}_k$ representing "Child k is muddy"

$\texttt{holds}_a(c)$ representing "player a holds card c"

Slide 16

Logical operators

$\neg$ - Not

$\wedge$ - And

$\vee$ - Or

$\Rightarrow$ - implies, if ... then ...

$\iff$ – if and only if

lide 17

Formulas of Propositional Logic

The set of formulas of propositional logic are defined by

1. If $p \in \Phi$ then p is a formula.
2. If ϕ is a formula then $\neg\phi$ is a formula
3. If ϕ_1, ϕ_2 are formulas then so is $\phi_1 \wedge \phi_2$.
4. Nothing is a formula unless it can be shown to be a formula using the above.

lide 18

All other boolean operators can be defined using only $\neg$ and $\wedge$

$\phi_1 \vee \phi_2$ is $\neg((\neg\phi_1) \wedge (\neg\phi_2))$

$\phi_1 \Rightarrow \phi_2$ is $(\neg\phi_1) \vee \phi_2$

$\phi_1 \iff \phi_2$ is $(\phi_1 \Rightarrow \phi_2) \wedge (\phi_2 \Rightarrow \phi_1)$

Slide 19

Examples:

p

$p \wedge \neg p$

$(p \wedge q) \Rightarrow p$

Slide 20

Semantics of Propositional Logic

A *state of the world* determines which sentences are true.

Represent this by an *assignment* $\alpha : \Phi \to \{\texttt{true}, \texttt{false}\}$

Write $\alpha \models \phi$ for "ϕ is true with respect to assignment α"

$\alpha \models p$ if $\alpha(p) = \texttt{true}$, for $p \in \Phi$

$\alpha \models \neg\phi$ if not $\alpha \models \phi$

$\alpha \models \phi_1 \wedge \phi_2$ if $\alpha \models \phi_1$ and $\alpha \models \phi_2$

lide 21

Validity

A formula ϕ of propositional logic is *valid*, (or *a tautology*), written $\models \phi$, if $\alpha \models \phi$ for all assignments α.

Examples:

$\models p \Rightarrow p$

$\models \phi \vee \neg\phi$ (for all formulas ϕ)

$\models ((p \wedge q) \Rightarrow r) \iff (p \Rightarrow (q \Rightarrow r))$

lide 22

A Language for Knowledge

Suppose that there are n agents.

The formulas of the logic of knowledge are defined by

1. If $p \in \Phi$ then p is a formula
2. If ϕ is a formula then $\neg\phi$ is a formula
3. If ϕ_1, ϕ_2 are formulas then $\phi_1 \wedge \phi_2$, is a formula
4. **If ϕ is a formula, then so is $K_i\phi$, for $i = 1 \ldots n$**
5. Nothing is a formula unless it can be shown to be a formula using the above.

Slide 23

Examples:

$K_2\texttt{muddy}_3$

$K_1K_2\texttt{muddy}_3$

$K_1\neg K_2\texttt{muddy}_3$

$\neg K_1\neg K_2\texttt{muddy}_3$

Slide 24

Political Knowledge (Donald Rumsfeld, 2003)

As we know
There are known knowns
There are things we know we know
We also know
There are known unknowns
That is to say
We know there are some things
We do not know
But there are also unknown unknowns
The ones we don't know we don't know

lide 25

Semantics for Knowledge: Kripke Structures

A *Kripke structure for n agents* is a tuple $(S, \pi, \mathcal{K}_1, \dots, \mathcal{K}_n)$ where

1. S is a set of states,
2. $\pi : S \to \Phi \to \{\texttt{true}, \texttt{false}\}$ associates an assignment with every state,
3. $\mathcal{K}_i \subseteq S \times S$ is an *equivalence relation* on S, for each $i = 1 \dots n$

lide 26

$R \subseteq S \times S$ is an equivalence relation on S if

1. (Reflexivity) $(s, s) \in R$ for all $s \in S$.
2. (Symmetry) If $(s, t) \in R$ then $(t, s) \in R$, for all $s, t \in S$.
3. (Transitivity) If $(s, t) \in R$ and $(t, u) \in R$ then $(s, u) \in R$, for all $s, t, u \in S$.

Slide 27

Semantics

We now treat formulas as being true/false at a state in a Kripke structure.

Write $(M, s) \models \phi$ for "ϕ is true at state s in structure M."

$(M, s) \models p$ if $\pi(s)(p) = \texttt{true}$, for $p \in \Phi$

$(M, s) \models \neg\phi$ if not $(M, s) \models \phi$

$(M, s) \models \phi_1 \wedge \phi_2$ if $(M, s) \models \phi_1$ and $(M, s) \models \phi_2$

$(M, s) \models K_i\phi$ if $(M, t) \models \phi$ for all t such that $(s, t) \in \mathcal{K}_i$

Slide 28

Example: Cards

Suppose there are three cards A, B, C. Players 1 and 2 get one card each, the other remains face down.

Represent a state by a tuple (x, y) where $x, y \in \{A, B, C\}$ and $x \neq y$.

x is the card held by player 1

y is the card held by player 2

Propositions: $\texttt{holds}_a(c)$ where $a \in \{1, 2\}$ is an agent and $c \in \{A, B, C\}$ is a card.

$\pi((x, y))(\texttt{holds}_a(c)) = \texttt{true}$ iff $(a = 1$ and $c = x)$ or $(a = 2$ and $c = y)$

$(x, y)\mathcal{K}_1(x', y')$ iff $x = x'$

$(x, y)\mathcal{K}_2(x', y')$ iff $y = y'$

lide 29

Why not just treat worlds as assignments to the basic propositions?

States also "contain information about what is known."

Example: suppose player 1 might be blind.

States are now tuples (x, y, b) where $x, y \in \{A, B, C\}$ and $b \in \{0, 1\}$ represents whether 1 is blind

$\pi((x, y, b))(\texttt{holds}_a(c)) = \texttt{true}$ iff $(a = 1$ and $c = x)$ or $(a = 2$ and $c = y)$

$(x, y, b)\mathcal{K}_1(x', y', b')$ iff $b = b'$ and $(x = x'$ or $b = 1)$

$(x, y, b)\mathcal{K}_2(x', y', b')$ iff $y = y'$

Note $\pi((x, y, 0)) = \pi((x, y, 1))$

lide 30

Properties of Knowledge

K1. $K_i\varphi \wedge K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\psi$

K2. $K_i\varphi \Rightarrow \varphi$

K3. $K_i\varphi \Rightarrow K_iK_i\varphi$

K4. $\neg K_i\varphi \Rightarrow K_i\neg K_i\varphi$

Slide 31

Validity

Write $\models \phi$ if $(M, s) \models \phi$ for all structures M and states s of M.

If $\models \varphi$ then $\models K_i\varphi$

If $\models \varphi$ and $\models \varphi \Rightarrow \psi$ then $\models \psi$.

Slide 32

Common and Distributed Knowledge

Add the following to the language: if ϕ is a formula and $G \subseteq \{1 \ldots n\}$ is a group of agents, then the following are formulas..

$E_G\phi$ — everyone in the group G knows ϕ

$C_G\phi$ — it is common knowledge in the group G that ϕ

$D_G\phi$ — it is distributed knowledge in the group G that ϕ

lide 33

Semantics

Define $E_G^k \phi$ by $E_G^0 \phi = \phi$ and $E_G^{k+1} \phi = E_G E_G^k \phi$.

Extend the semantics by the following clauses:

$(M, s) \models E_G \phi$ if $(M, s) \models K_i \phi$ for all $i \in G$

$(M, s) \models C_G \phi$ if $(M, s) \models E_G^k \phi$ for all $k = 1, 2, \ldots$

$(M, s) \models D_G \phi$ if $(M, t) \models \phi$ for all t such that $(s, t) \in K_i$ for all $i \in G$

lide 34

An alternate formulation of common knowledge

Let G be a group of agents.

Say state t is *G-reachable from state s in k steps* if there exists a sequence $s_0, s_1, \ldots, s_k$ of states such that $s_0 = s$, $s_k = t$ and for all $j = 0 \ldots k$ there exists $i \in G$ such that $s_j \, \mathcal{K}_i \, s_{j+1}$

Say state t is *G-reachable from state s* if there exists $k \geq 0$ such that t is *G-reachable from s in k steps.*

Slide 35

Lemma:

$(M, s) \models E_G^k \phi$ iff $(M, t) \models \phi$ for all t that are G-reachable from s in k steps

$(M, s) \models C_G \phi$ iff $(M, t) \models \phi$ for all t that are G-reachable from s

Slide 36

Properties of Common Knowledge

Write $M \models \phi$ if $M, s \models \phi$ for all states s of M.

C1. $M \models E_G \varphi \iff \bigwedge_{i=1}^m K_i \varphi$

C2. $M \models C_G \varphi \Rightarrow E_G(\varphi \wedge C_G \varphi)$

RC. If $M \models \varphi \Rightarrow E_G(\psi \wedge \varphi)$ then $M \models \varphi \Rightarrow C_G \psi$

lide 37

Properties of Distributed Knowledge

$\models D_{\{i\}}\phi \iff K_i\phi$

$\models D_G\phi \Rightarrow D_{G'}\phi$ if $G \subseteq G'$

lide 38

Kripke Structure for Muddy Children