Logics of public announcements

An introductory talk

Jan Plaza

Computer Science Department

SUNY Plattsburgh

March 31, 2009

Welcome

This is a non-technical introduction to the Logic of Public Announcements and to Dynamic Epistemic Logics in general.

We will present

- basic concepts of any logic system:
  - proof,
  - semantics,
  - completeness,
- and logic systems:
  - classical logic,
  - modal logics,
  - epistemic logics,
  - dynamic epistemic logics.

Branches of philosophy

- **Epistemology**,
- **Logic**,
- Metaphysics (cosmology and ontology),
- Ethics,
- Aesthetics,
- ...

Logic has been also claimed by the 20th century mathematics.

Etymology

In Greek:

- $\eta\pi\iota\sigma\tau\eta\mu\eta$ [episteme] – knowledge,
- $\lambda o\gamma\iota\kappa o\varsigma$ [logikos] – reason.

So,

- **Epistemology** – investigates the nature and scope of knowledge;
- **Logic** – investigates reasoning.

When Harry met Sally ...

Epistemology and logic met in:

EPISTEMIC LOGIC

which allows us to reason about the knowledge of others
(e.g. I know that you know that he does not know that ...)

This talk will take you to a new area of formal logic:

DYNAMIC EPISTEMIC LOGIC

which allows us to reason about changes of knowledge resulting from communication.

Love and hate

“The grand book of universe is written in the language of mathematics.”

Galileo Galilei (1564-1642)

“One cannot understand the laws of nature, the relationship of things, without an understanding of mathematics.
There is no other way to do it.”

Richard Feynman (1918-1988)

So, we need to learn to love the mathematical approach to logic.

Classical logic

- Aristotle (384-322 B.C) – syllogism (350 B.C.E.)
- Gottfried Wilhelm Leibniz (1646-1716) – calculus ratiocinator, characteristica universalis
- George Boole (1815-1864) – algebra of logic
- **Gottlob Frege** (1848-1925) – Begriffsschrift (1879) predicate first order logic
- Emil Post (1897-1954) – completeness of propositional logic
- **Alfred Tarski** (1901-1983) – semantics, truth
- Stanislaw Jaśkowski (1906-1965) – natural deduction
- Gerhard Gentzen (1909-1945) – sequent calculus
- Adolf Lindenbaum (1904-1941) – Lindenbaum algebra
- Thoralf Skolem (1887-1963) – Skolem normal form
- **Kurt Gödel** (1906-1978) – completeness of first order logic (1921)
- Alonzo Church (1903-1995) – undecidability of first-order logic
- Leopold Löwenheim (1878-1957) – model theory
- Evert Willem Beth (1908-1964) – semantic tableaux, definability
- William Craig (b. 1918) - interpolation
- Robinson – joint consistency
- Helena Rasiowa (1917-1994) – algebraic methods
- Roman Sikorski (1920-1983) – algebraic methods
- Wilhelm Ackermann (1896-1962) – decidable fragments
- Per Lindstrom – classical first-order logic is THE logic
- Jacques Herbrand (1908-1931) – Herbrand universe
- John Alan Robinson (b. 1930) – resolution
- Robert Kowalski (b. 1941) – SLD resolution

Defining a logical system

- Syntax of formulas,
- Derivation system (proofs or refutations)
  – leads to: theorems,
- Semantics
  – leads to: valid statements and the notion of a formula being a consequence of other formulas.

(Sometimes just one of the last two.)

Semantics of propositional classical logic

α	$\neg\alpha$
false	true
true	false

α	β	$\alpha \longrightarrow \beta$
true	true	true
true	false	false
false	true	true
false	false	true

$\models \alpha$ or α **is valid** if α is true under every assignment of true/false to propositional symbols. For instance, $\models p \longrightarrow p$.

$\Gamma \models \alpha$ or α **is a consequence of** Γ if α is true under every assignment of true/false that makes formulas in Γ true.
For instance, $p \models \neg\neg p$.

Axiomatization of propositional classical logic

A Hilbert style axiomatization – after David Hilbert (1862-1943)

Axiom schemas:

1. $\alpha \rightarrow (\beta \rightarrow \alpha)$
2. $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$
3. $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$

Inference rule: Modus Ponens (MP) – from α and $\alpha \rightarrow \beta$ infer β:

$$\frac{\alpha, \alpha \rightarrow \beta}{\beta}$$

Formal proofs

Γ – a set of formulas
α – a formula
A formal proof of α from Γ is a sequence $\alpha_1, \ldots, \alpha_n$ of formulas such that $\alpha_n = \alpha$, and every α_k is

- either a logical axiom,
- or a member of Γ,
- or results by inference rules from formulas which precede α_k.

$\Gamma \vdash \alpha$ means: there exists a formal proof of α from Γ.

α **is a logical theorem** if $\vdash \alpha$ (with empty Γ).

A formal proof example

1. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$
   instance of Ax 2.

2. $p \to ((p \to p) \to p)$
   instance of Ax 1.

3. $(p \to (p \to p)) \to (p \to p)$
   by MP from 2 and 1.

4. $p \to (p \to p)$
   instance of Ax 1.

5. $p \to p$
   by MP from 4 and 3.

So, $\vdash p \to p$.

Metaproperties

- **Consistency** of the derivation system –
  no theorem is a negation of another;
- **Soundness** of the derivation system with respect to the semantics – every logical theorem is valid;
- **Completeness** of the derivation system with respect to the semantics – every valid statement is a logical theorem.

Theorem on soundness and completeness:
$\vdash \alpha$ iff $\models \alpha$
or a stronger version:
$\Gamma \vdash \alpha$ iff $\Gamma \models \alpha$.

They hold for classical propositional and first-order logics.

They are THE goals in investigations of (almost) any logical system.

Modal logics

- Aristotle (384-322 BC) – necessary, possible
- **Clarence Irving Lewis** (1883-1964) modal systems S1-S5
- **Cooper H. Langford** – modal systems S1-S5
- Kurt Gödel (1906-1978) – new axiomatizations
- Alfred Tarski (1901-1983) – algebrac semantics
- **Saul Kripke** (b. 1940) – Kripke semantics
- J.C.C. McKinsey – final model property
- Melvin Fitting – predicate abstraction

Modalities

Modality of α = mode of truth of α.

In different systems $\Box\alpha$ can mean:

- α is necessarily true (alethic modality),
- α will be always true (tense modality),
- α is obligatory (deontic modality),
- α is true after all terminating computations (dynamic modality),
- It is provable that α (metalogical modality),
- I believe that α (doxastic modality),
- I know that α (epistemic modality),
- It is a common knowledge that α (epistemic modality).

Modal logics

Modal logics extend classical logic
with new functors: $\Box$, $\Diamond$.

$\Diamond\alpha \Leftrightarrow \neg\Box\neg\alpha$
$\Box\alpha \Leftrightarrow \neg\Diamond\neg\alpha$

Unlike $\neg$, $\wedge$, $\vee$, $\rightarrow$, functors $\Box$ and $\Diamond$ are **not truth functional**:
the truth value of $\Box\alpha$ does not depend just on the truth value of α.

Semantics of modal logics

$\Diamond\alpha$ is read "α is possible"; $\Box\alpha$ is read "α is necessary".

Gottfried Wilhelm Leibniz (1646-1716):
we live in the best **possible world** God could have created.

Kripke models:

- depending on the world you are in you can imagine different possible worlds;
- $\Diamond\alpha$ is true in a world if α is true in **some** possible world;
- $\Box\alpha$ is true in a world if α is true in **every** possible world.

Given a world w, possible worlds are those w' which satisfy relation wRw'.

Different types of relations R yield different modal logics.
Equivalence relations yield S5.

Epistemic logics

- 1951 Georg Henrik von Wright (1916-2003) – logics of knowledge and belief,
- 1962 Jaakko Hintikka (b. 1929) – logics of knowledge and belief,
- 1977 E. J. Lemmon - hierarchy of epistemic systems,
- 1969 David Kellogg Lewis (1941-2001) – common knowledge vs. conventions,
- 1976 Robert Aumann (b. 1930) – common knowledge semantics,
- 1981 Kozen, Parikh – completeness of systems with common knowledge,
- 1992 Halpren, Moses – completeness of systems with distributed knowledge.

Monographs of epistemic logics

- Fagin, Halpern, Moses, Vardi, **Reasoning about Knowledge**, MIT Press 1995.

- Meyer, Ch, van der Hoek, **Epistemic Logic for AI and Computer Science**, Cambridge University Press, 1995.

- Rescher, **Epistemic Logic: survey of the logic of Knowledge**, University of Pittsburgh Press, 2005.

Epistemic operators

Write K instead of $\Box$.

$\mathsf{K}_i\alpha$ – "agent i implicitly **knows that** α".

$\mathsf{Kw}_i\alpha$ – "agent i implicitly **knows whether** α".

$\mathsf{Kw}_i\alpha \leftrightarrow \mathsf{K}_i\alpha \vee \mathsf{K}_i\neg\alpha$

$\mathsf{K}_i\alpha \leftrightarrow \alpha \wedge \mathsf{Kw}_i\alpha$

S5

Extend axiomatization of classical logic with:

K: $\mathsf{K}_i\alpha \wedge \mathsf{K}_i(\alpha \rightarrow \beta) \rightarrow \mathsf{K}_i\beta$ – knowledge closed under MP,

T: $\mathsf{K}_i\alpha \rightarrow \alpha$, – veradicity – agent knows only true things,

4: $\mathsf{K}_i\alpha \rightarrow \mathsf{K}_i\mathsf{K}_i\alpha$ – agent has positive introspection,

5: $\neg\mathsf{K}_i\alpha \rightarrow \mathsf{K}_i\neg\mathsf{K}_i\alpha$ – agent has negative introspection,

RN: $\frac{\vdash\alpha}{\mathsf{K}_i\alpha}$ – agent knows all theorems of logic.

S5 – a logic of an external observer who can reason about the world and about agents' knowledge, A perfect reasoner – will deduce everything that can be deduced.

Other epistemic systems

Other axiom schemas:

.2: $\neg \mathsf{K}_i \neg \mathsf{K}_i \alpha \rightarrow \mathsf{K}_i \neg \mathsf{K}_i \neg \alpha$,

.3: $\mathsf{K}_i(\mathsf{K}_i \alpha \rightarrow \mathsf{K}_i \beta) \vee \mathsf{K}_i(\mathsf{K}_i \beta \rightarrow \mathsf{K}_i \alpha)$

.4: $\alpha \rightarrow (\neg \mathsf{K}_i \neg \mathsf{K}_i \alpha \rightarrow \mathsf{K}_i \alpha)$,

Epistemic systems in order of increasing strength:

S4 = KT4 + RN

S4.2 = KT4.2 + RN

S4.3 = KT4.3 + RN

S4.4 = KT4.4 + RN

S5 = KT5 + RN

Byzantine generals

Two allied generals with their armies occupy two hills. They can defeat the enemy in the valley between them only if they attack simultaneously. The generals can send messengers to each other with encrypted messages. If the the enemy captures the messenger the message will not be delivered. Can the generals agree on a time to attack?

Answer: NO

Why?

Not only each general needs to know the attack time,
but needs to know that each one knows,
and needs to know that each one knows that each one knows,
and ...
(without an end)

They need a **common knowledge** of the attack time.

No finite number of messages can accomplish that.

Common knowledge

$\mathsf{E}\alpha = \mathsf{K}_1\alpha \wedge ... \wedge \mathsf{K}_m\alpha$ – "every agent knows that α ".

$\mathsf{E}^0\alpha = \alpha$,
$\mathsf{E}^{n+1}\alpha = \mathsf{E}\mathsf{E}^n\alpha$.

$\mathsf{E}^2\alpha$ – "everybody knows that everybody knows that α is true".

Common knowledge: $\mathsf{C}\alpha = \mathsf{E}^1\alpha \wedge \mathsf{E}^2\alpha \wedge \mathsf{E}^3\alpha \wedge ...$ (Informally)

Announcing α in a meeting makes it a common knowledge for all participants (provided that α is about the world, not knowledge).

In a Kripke model:

- $\mathsf{E}\alpha$ is true in a world w if α is true in all words accessible from w by the relation $R_\mathsf{E} = R_1 \cup ... \cup R_m$;
- $\mathsf{C}\alpha$ is true in a world w if α is true in all words accessible from w by the relation R_C that is the transitive closure of R_E.

S5C

extend the axiomatization of S5 with:

$$\mathsf{C}(\alpha \to \beta) \to (\mathsf{C}\alpha \to \mathsf{C}\beta)$$

$$\mathsf{C}\alpha \to (\alpha \wedge \mathsf{EC}\alpha)$$

$$\mathsf{C}(\alpha \to \mathsf{E}\alpha) \to (\alpha \to \mathsf{C}\alpha)$$

$$\frac{\alpha}{\mathsf{C}\alpha}$$

One can also consider common knowledge of different groups of agents.

Distributed knowledge

Among the persons in this room, do any two have the same birthday? (Probably) nobody knows. Yet, we have a **distributed knowledge** of that – if we put our knowledge together we will know.

$\mathsf{D}_{1,2}\beta$ means that β is a distributed knowledge of agents 1 and 2.

$\mathsf{K}_1\alpha \wedge \mathsf{K}_2(\alpha \rightarrow \beta) \rightarrow \mathsf{D}_{1,2}\beta$

In a Kripke model $\mathsf{D}\alpha$ is true in a world w if α is true in all words accessible from w by the relation $R_1 \cap ... \cap R_m$.

How are these kinds of knowledge related?

$$\mathsf{C}\alpha \Rightarrow \mathsf{E}\alpha \Rightarrow \mathsf{K}_i\alpha \Rightarrow \mathsf{D}\alpha \Rightarrow \alpha$$

Dynamic Epistemic Logic

- 1989 Plaza – logic of public announcements PA
- 1993 Plaza – logic of semi-public announcements
- 1997 Gerbrandy and Groeneveld – PA
- 1998 Baltag, Moss, Solecki – PAC = PA + common knowledge
- 2000 van Ditmarsch – logic of epistemic actions EA
- 2003 van Ditmarsch, van der Hoek, Kooi – concurrent EA

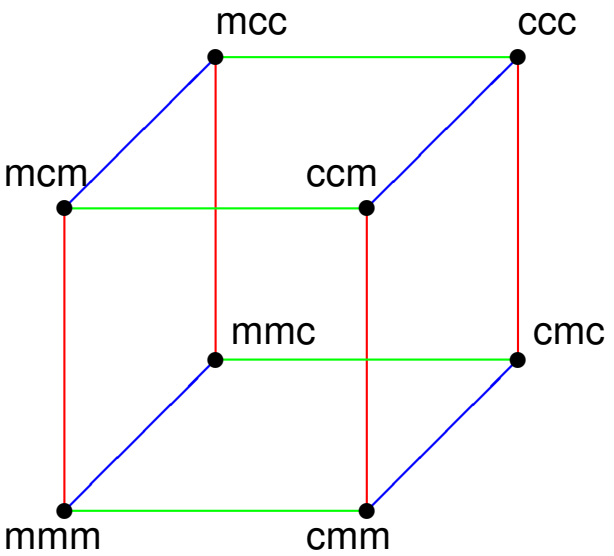
A monograph of the subject:
Dynamic Epistemic Logic,
by H. van Ditmarsch, W. van der Hoek, and B. Kooi,
Springer Verlag, 2007.

Muddy Children

Father: At least one of you has mud on the forehead.
Child 1: I do not know whether my forehead is muddy.
Child 2: I do not know whether my forehead is muddy.
Child 3: I know whether my forehead is muddy or not
but I won't tell you!

If the participants of the dialog can see each other (but no one can see own forehead), is the forehead of Child 3 muddy?

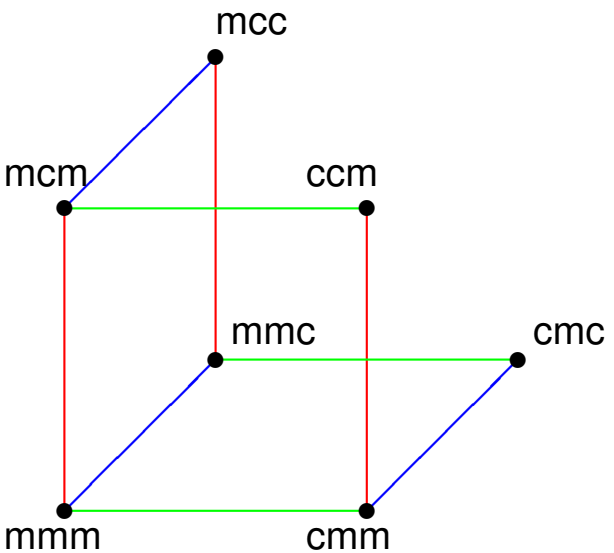
Initial model



Child 1
Child 2
Child 3

Next:
Father: At least one of you has mud on the forehead.

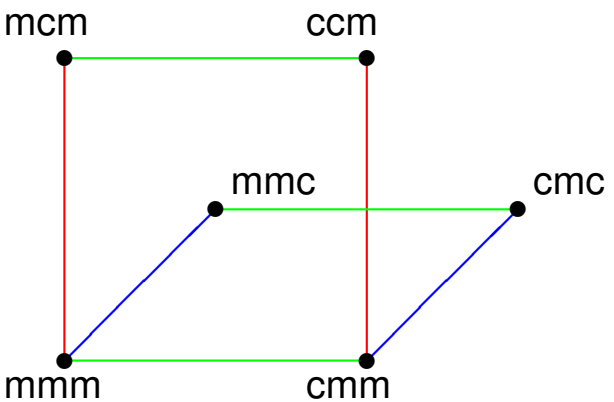
After father's statement



Child 1
Child 2
Child 3

Next:
Child1: I don't know if my forehead is muddy.

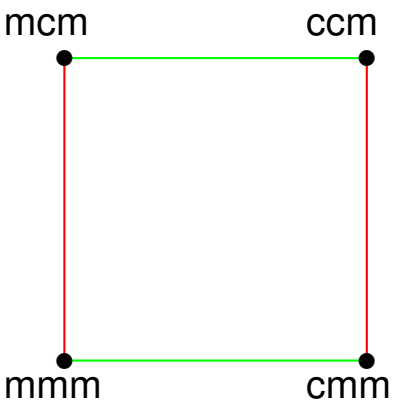
After the statement of Child 1



Child 1
Child 2
Child 3

Next:
Child2: I don’t know if my forehead is muddy.

After the statement of Child 2



Child 1
Child 2
Child 3

Now Child 3 can say:
I know if my forehead is muddy!

Now, assume that the situation is mmm.
Does Father say anything the children did not know before?

Now, assume that the situation is mmm.
Does Father say anything the children did not know before?

Answer: NO

Is Father's statement superfluous?

Now, assume that the situation is mmm.
Does Father say anything the children did not know before?

Answer: NO

Is Father's statement superfluous?

Answer: NO

Why?

Now, assume that the situation is mmm.
Does Father say anything the children did not know before?

Answer: NO

Is Father's statement superfluous?

Answer: NO

Why?

It creates common knowledge!

Functor $+$

Define: $\alpha+\beta$ **is true at a world** w **of a model** M
if β is true at a world w of M'
where M' is contains only those worlds where α was true.

β will be true after a (honest) public communication of α by agent i iff $\mathsf{K}_i\alpha + \beta$ is true at the present.

β will be true after (honest) parallel public communications of α_1 by agent 1 and of α_2 by agent 2 iff $(\mathsf{K}_1\alpha_1 \wedge \mathsf{K}_2\alpha_2) + \beta$ is true at the present.

In current literature the notation for $\alpha + \beta$ is $\langle\alpha\rangle\beta$.

Axiomatization of PA

To obtain Logic of Public Announcements (PA)
extend the axiomatization of S5 with:

$\alpha + p \leftrightarrow \alpha \wedge p$ (for any propositional letter p)
$\alpha + \top \leftrightarrow \alpha$
$\alpha + \bot \leftrightarrow \bot$
$\alpha + (\beta_1 \wedge \beta_2) \leftrightarrow (\alpha + \beta_1) \wedge (\alpha + \beta_2)$
$\alpha + (\beta_1 \vee \beta_2) \leftrightarrow (\alpha + \beta_1) \vee (\alpha + \beta_2)$
$\alpha + \neg\beta \leftrightarrow \alpha \wedge \neg(\alpha + \beta)$
$\alpha + (\beta_1 \rightarrow \beta_2) \leftrightarrow \alpha \wedge (\alpha + \beta_1 \rightarrow \alpha + \beta_2)$
$\alpha + (\beta_1 \leftrightarrow \beta_2) \leftrightarrow \alpha \wedge (\alpha + \beta_1 \leftrightarrow \alpha + \beta_2)$
$\alpha + \mathsf{K}_i\beta \leftrightarrow \alpha \wedge \mathsf{K}_i(\alpha \rightarrow \alpha + \beta)$

Muddy children in PA

$$K_{Father}\text{atLeastOneMuddy} + K_{Child1}\neg Kw_{Child1}\text{muddy1} + \\ + K_{Child2}\neg Kw_{Child2}\text{muddy2} + K_{Child3}Kw_{Child3}\text{muddy3}$$

which is equivalent to:

$$K_{Father}\text{atLeastOneMuddy} + \neg Kw_{Child1}\text{muddy1} + \\ + \neg Kw_{Child2}\text{muddy2} + Kw_{Child3}\text{muddy3}$$

which is equivalent to:

$$\text{atLeastOneMuddy} + \neg Kw_{Child1}\text{muddy1} + \\ + \neg Kw_{Child2}\text{muddy2} + Kw_{Child3}\text{muddy3}.$$

To find the situations in which the dialog could have taken place it is enough to test this formula in the worlds of our Kripke model.

Some results

New logical system:
Logic of public announcements with common knowledge PAC

For S5, PA, PAC the following hold:

- Strong soundness and completeness: $\Gamma \vdash \alpha$ iff $\Gamma \models \alpha$.
- Decidability: it is decidable if $\Gamma \models \alpha$.

Expressibility: PA = S5 $<$ S5C $<$ PAC

Mr. Sum and Mr. Product

Mr. Puzzle: I chose two whole numbers greater than 1. I will tell their sum only to Mr. Sum and their product only to Mr. Product.
He tells them.
Mr. Product: I do not know the numbers.
Mr. Sum: I knew you didn't.
Mr. Product: But now I know!
Mr. Sum: So do I!

What can be the numbers if they are not greater than 100?

$Kv_{Product}$numbers – Mr. Product knows the value of numbers –
if in all worlds accessible from the current world the numbers are the same.

Mr. Sum and Mr. Product in logic

Possible worlds: $\langle a, b\rangle$ where $1 < a \leq b$.

Mr. Sum does not distinguish two worlds if they have the same sum;
Mr. Product — if they have the same product:
$\langle a, b\rangle R_{\mathsf{Sum}} \langle a', b'\rangle$ iff $a + b = a' + b'$,
$\langle a, b\rangle R_{\mathsf{Product}} \langle a', b'\rangle$ iff $a * b = a' * b'$.

$(\mathsf{K}_{\mathsf{Product}} \neg \mathsf{Kv}_{\mathsf{Product}} \mathsf{numbers} \wedge \mathsf{K}_{\mathsf{Sum}} \neg \mathsf{Kv}_{\mathsf{Product}} \mathsf{numbers}) +$
$+ \mathsf{K}_{\mathsf{Product}} \mathsf{Kv}_{\mathsf{Product}} \mathsf{numbers} + \mathsf{K}_{\mathsf{Sum}} \mathsf{Kv}_{\mathsf{Sum}} \mathsf{numbers}$

this can be reduced to:

$\mathsf{K}_{\mathsf{Sum}} \neg \mathsf{Kv}_{\mathsf{Product}} \mathsf{numbers} + \mathsf{Kv}_{\mathsf{Product}} \mathsf{numbers} + \mathsf{Kv}_{\mathsf{Sum}} \mathsf{numbers}.$

Employ a computer to test in which worlds the formula is satisfied.

Another version of of the puzzle:

First, Mr. Puzzle tells Mr. Sum and Mr. Product in a public communication that the numbers are not greater than 100.

Now the model is finite. The formula representing dialog stays the same.

This change affects solutions.

Russian cards

Seven cards have numbers 1..7 on them.
Anne and Bill draw three cards each.
Cath gets the remaining card.

Can Anne and Bill make a sequence of public announcements so that they learn each other's cards but Cath still does not know their cards?

Epistemic actions

Anne and Bill are in a cafe. A letter is delivered to Anne.
They both see “ABCD stock value update” on the envelope.

Alternative scenarios:

- **tell=public announcement** Anne reads the letter aloud.
- **read=semi-public announcement** Bill sees that Anne reads the letter (not aloud).
- **may-read** Bill leaves the table. Anne may have read the letter when he was away.
- **both-may-read** Bill leaves the table. Anne may have read the letter when he was away. Bill returns. Anne leaves the table. Bill may have read the letter when she was away.

Such actions can be combined resulting in new states of agents’ knowledge. They are described by **logic of epistemic actions**.

Possible Applications of Dynmic Epistemic Logics

"Prediction is always difficult, especially of the future"

Niels Bohr

- cryptography, codes, protocols – extending the ideas of Russian cards,
- proofs of equivalence of different versions of a protocol which use epistemic actions, or proofs of correctness of a protocol with respect to specification,
- game theory (where agents communicate and cooperate or oppose each other to win a game).