Common Knowledge in Email Exchanges

Krzysztof R. Apt

CWI, Amsterdam, the Netherlands,
University of Amsterdam

based on joint work with

Floor Sietsma, CWI

(To appear in
ACM Transactions on Computational Logic.)
COMMON, something that belongs to all alike, in contradistinction to proper, peculiar.

KNOWLEDGE is defined, by Mr Locke, to be the perception of the connection and agreement, or disagreement and repugnancy, or our ideas.

Encyclopaedia Britannica
By a Society of GENTLEMEN in Scotland
Edinburgh
MDCCLXXI
p. 192: “As for the diplomatic informer, he worked, of course for the Deuxième Bureau, and the chief instructed us that we should carefully stick to the fiction that we didn’t know that he knew that we knew it."

p.2: “The final section, Economics, will deal with A thinks B thinks ... reasoning in formal games.”


p. 279: “It is *common knowledge* that if you plant a flag on a hitherto uncharted island or territory, you have staked a claim to that territory on behalf of the nation which the flag represents.”


p. 142: “It is *common knowledge* the political situation after the great victory over Germany began to deteriorate.”
History: Email

Story 1: Why BCC is Useful

FYI: Wouter Bos knows Trijntje Oosterhuis.

Source: Wouter Bos e-mailt per ongeluk zijn netwerk rond. NRC Handelsblad, 7th October 2010.
Story 2: Forwarding

I got an email from my Chinese postdoc Helen with a CC to her husband Bo.

I forwarded it to Floor.

Floor replied to my forward to Bo and Helen with a BCC to me.

I forwarded the last email to Helen and Bo with a BCC to Floor.

Do we all have common knowledge of Floor’s reply?
Messages

**Agents:** finite set $Ag$

**Notes:** further unspecified.

- $s(i, l, G)$;
  message containing note $l$, sent by agent $i$ to group $G$,

- $f(i, l.m, G)$;
  forwarding by $i$ of message $m$ with added note $l$, sent to group $G$,

$S(m) = \{\text{sender of } m\}$, $R(m) = \text{receivers of } m$.

**Special cases:**

- **reply:** $f(i, l.m, G)$, with $G = S(m)$, where $i \in R(m)$,

- **reply-all:** $f(i, l.m, G)$, with $G = S(m) \cup R(m)$, where $i \in R(m)$.
Emails

Email: $m_B$, with

$m$ a message, 

$B \subseteq Ag$ a set of BCC recipients.

Examples

- Passing a note further: 
  $s(i, l, G)_B, s(j, l, G')_{B'}$, where $j \in G \cup B$,

- Forwarding an email: 
  $m_B, f(i, l.m, G)_C$, where $i \in R(m) \cup B$,

- Forwarding one’s own email: 
  $m_B, f(i, l.m, G)_C$, where $S(m) = \{i\}$,

- BCC reply-all (grrr . . .): 
  $m_B, f(i, l.m, G)_C$, where $i \in B$ and $G = S(m) \cup R(m)$.
I got an email from my Chinese postdoc Helen with a CC to her husband Bo.
\[ e := m_{\emptyset}, \text{ where } m := s(H, l, \{B, K\}), \]

I forwarded it to Floor.
\[ e' := m'_{\emptyset}, \text{ where } m' := f(K, m, F'), \]

Floor replied to my forward to Bo and Helen with a BCC to me.
\[ e'' := m''_{\{K\}}, \text{ where } m'' := f(F, m', \{B, H\}), \]

I forwarded the last email to Helen and Bo with a BCC to Floor.
\[ f(K, m'', \{H, B\})_{\{F\}}.\]
Assumptions

Each agent

- has his set of notes,
- can send/forward his notes,
- also can send/forward notes he received,
- also can forward messages he received.
Some Considerations

- Are all sets of emails meaningful?
- **Nyet**: you can’t forward a note you did not receive.
- If one sends/forwards somebody’s else note, then one should have received it.
- If one forwards a message, then one should have received it.
States

- **Factual information:**

  \[
  FI(s(i, l, G)) := \{l\},
  FI(f(i, l.m, G)) := FI(m) \cup \{l\}.
  \]

- **State:** \( s = (E, L) \), where
  - \( E \): set of emails,
  - \( L = (L_1, \ldots, L_k) \): sets of agents’ notes.
Legal States

Legal state:
\( s = (E, L) \), such that for some partial ordering \( \prec \) on \( E \)

- for each \( s(i, l, G)_B \in E \), where \( l \notin L_i \),
  \( m_C \in E \) exists such that
  \( m_C \prec s(i, l, G)_B \), \( i \in R(m) \cup C \) and \( l \in FI(m) \)
  \( (m_C \text{ justifies } s(i, l, G)_B) \),
Legal States

Legal state:
\( s = (E, L), \) such that for some partial ordering \( \prec \) on \( E \)

- for each \( s(i, l, G)_B \in E, \) where \( l \notin L_i, \)
  \( m_C \in E \) exists such that
  \( m_C \prec s(i, l, G)_B, i \in R(m) \cup C \) and \( l \in FI(m) \)
  \( (m_C \text{ justifies } s(i, l, G)_B), \)

- for each \( f(i, l.m, G)_B \in E, \) where \( l \notin L_i, \)
  some \( m'_C \in E \) exists such that
  \( m'_C \prec f(i, l.m, G)_B, i \in R(m') \cup C \) and \( l \in FI(m') \),
Legal States

Legal state:
$s = (E, L)$, such that for some partial ordering $\prec$ on $E$

- for each $s(i, l, G)_B \in E$, where $l \notin L_i$,
  $m_C \in E$ exists such that
  $m_C \prec s(i, l, G)_B$, $i \in R(m) \cup C$ and $l \in FI(m)$
  ($m_C$ justifies $s(i, l, G)_B$),

- for each $f(i, l.m, G)_B \in E$, where $l \notin L_i$,
  some $m'_C \in E$ exists such that
  $m'_C \prec f(i, l.m, G)_B$, $i \in R(m') \cup C$ and $l \in FI(m')$,  

- for each $f(i, l.m, G)_B \in E$
  some $m_C \in E$ exists such that
  $m_C \prec f(i, l.m, G)_B$ and $i \in S(m) \cup R(m) \cup C$. 

Common Knowledge in Email Exchanges – p. 16/31
Language to Discuss Emails

\[ \varphi ::= m \mid i \blacktriangleleft m \mid \neg \varphi \mid \varphi \land \varphi \]

Abbreviation:

\[ m_B ::= m \land \bigwedge_{i \in S(m) \cup R(m) \cup B} i \blacktriangleleft m \land \bigwedge_{i \notin S(m) \cup R(m) \cup B} \neg i \blacktriangleleft m \]

Semantics Take \( s = (E, L) \).

\[ s \models m \quad \text{iff} \quad \exists B : m_B \in E \]
\[ s \models i \blacktriangleleft m \quad \text{iff} \quad \exists B : m_B \in E \text{ and } i \in S(m) \cup R(m) \cup B \]
\[ s \models \neg \varphi \quad \text{iff} \quad s \not\models \varphi \]
\[ s \models \varphi \land \psi \quad \text{iff} \quad s \models \varphi \text{ and } s \models \psi \]
Epistemic Language

Add $C_A \varphi$ to the language discussing emails.

**Intuition:** $C_A \varphi$ iff group $A$ commonly knows $\varphi$.

**Semantics** Take $s = (E, L)$.

$$s \models C_A \varphi \iff s' \models \varphi \text{ for any legal } s' \text{ s.t. } s \sim_A s'.$$

$\sim_G$ is the reflexive, transitive closure of $\bigcup_{i \in A} \sim_i$.

How to define $\sim_i$?
$m_B \sim_i m'_{B'}$

iff

- $i \in S(m), B = B' \text{ and } m = m'$, or
- $i \in R(m) \setminus S(m) \text{ and } m = m'$, or
- $i \in B \cap B' \text{ and } m = m'$.

**Example** If $i \in B \cap B'$, then $i$ cannot distinguish $m_B$ from $m'_{B'}$. 
\[ (E, L) \sim_i (E', L') \]

iff

\begin{itemize}
  \item \( L_i = L'_i \),
  \item \( \forall m_B \in E \ (i \in S(m) \cup R(m) \cup B \to \exists m_{B'} \in E' \ m_B \sim_i m_{B'}) \),
  \item \( \forall m_{B'} \in E' \ (i \in S(m) \cup R(m) \cup B' \to \exists m_B \in E \ m_B \sim_i m_B) \).
\end{itemize}
Common Knowledge of a Message

Theorem

\[ s \models C_A m \iff \]  

there is an email shared by the group \( A \) that proves the existence of \( m \).

Formally:

\[ E_A := \{ m_B \in E \mid A \subseteq S(m) \cup R(m) \text{ or } \exists j \in B : (A \subseteq S(m) \cup \{j\}) \}. \]

\( E_A \) is the set of emails that group \( A \) shared.

\[ s \models C_A m \iff \exists m'_B \in E_A : m' \rightarrow m \text{ is valid.} \]
Common Knowledge of an Email

Main Theorem Assume $|A| \geq 3$.

$$s \models C_A m_B \iff$$

- there is an email shared by the group $A$ that proves the existence of $m$,

$$s \models C_A m \iff \exists m'_B \in E_A : m' \rightarrow m \text{ is valid.}$$

- for every agent $j \in B$ there is an email shared by $A$ that proves that $j$ forwarded $m$,

$$\forall j \in B \ \exists m'_B \in E_A : m' \rightarrow j \blacktriangleleft m \text{ is valid.}$$

- $m_B$ involves all agents,

$$Ag = S(m) \cup R(m) \cup B.$$
Conclusions Concerning Story 2

We have

\[ s \nsubseteq C_{B,H,K,F} f(F,m', \{B, H\})_K, \]

where

\[ m' := f(K, m, F), \]
\[ m := s(H, l, \{B, K\}). \]

I forwarded Floor’s reply to Helen and Bo with a BCC to Floor:

\[ f(K, m'', \{H, B\})_F, \]

where \[ m'' := f(F, m', \{B, H\}), \]

I should have forwarded Floor’s reply to Helen and Bo and Floor:

\[ f(K, m'', \{H, B, F\})_\emptyset. \]
Can one Simulate BCC?

- Yes and No.
- Yes:
  
  \[ m_B \equiv m, f(i, m, j_1), \ldots, f(i, m, j_k), \]
  
  where \( S(m) = \{i\} \) and \( B = \{j_1, \ldots, j_k\} \).
- No: the mailboxes of the BCC recipients differ. So for \( j \in B \)
  
  - \( \{m_B, f(j, m, G)\} \) is a legal state, while
  - \( \{m, f(i, m, j_1), \ldots, f(i, m, j_k), f(j, m, G)\} \) not.
Take state $s$ with

$$E_s = \{s(1, l, 2)_{\{3\}}\}.$$  

Then $s \models K_3 \neg K_2 K_3 s(1, l, 2)$.

Take the simulation state $t$. So

$$E_t = \{s(1, l, 2), f(1, s(1, l, 2), 3)\}.$$  

Then $t \not\models K_3 \neg K_2 K_3 s(1, l, 2)$.

This observation can be made more general.
Preliminaries

- $M$: the set of all messages (so not emails).
- **Mailbox**: a function $\sigma : Ag \rightarrow \mathcal{P}(M)$; $\sigma(i)$ is the mailbox of agent $i$.
- **Configuration**: $<s, \sigma>$, where $s$ is a legal state and $\sigma$ a mailbox.
Atomic transition between configurations:

\[ \langle s, \sigma \rangle \rightarrow \langle s', \sigma' \rangle, \]

- \( s := (E \cup \{m_B\}, L) \) and \( s' := (E, L) \),
- for \( j \in Ag \)

\[
\sigma'(j) := \begin{cases} 
\sigma(j) \cup \{m\} & \text{if } j \in R(m) \cup S(m) \cup B \\
\sigma(j) & \text{otherwise}
\end{cases}
\]

subject to the following conditions:

- **send** \( m = s(i, l, G) \).
  Then \( l \in L_i \) or for some \( m' \in \sigma(i) \) we have \( l \in FI(m') \).

- **forward** \( m = f(i, l.m', G) \).
  Then \( m' \in \sigma(i) \), and \( l \in L_i \) or for some \( m'' \in \sigma(i) \) we have \( l \in FI(m'') \).
Email exchange starting in a legal state \( s \): a maximal sequence of transitions starting in \( \langle s, \sigma_0 \rangle \), where \( \sigma_0 \) is the empty mailbox.

An email exchange **properly terminates** if its last configuration is of the form \( \langle s', \tau \rangle \), where \( s' = (\emptyset, L) \).

**Note:** The communication is synchronous.

**Theorem** The following statements are equivalent:

(i) \( s \) is a legal state,

(ii) an email exchange starting in \( s \) properly terminates,

(iii) all email exchanges starting in \( s \) properly terminate.
Future Research

- Decidability of semantics.
- Sound and complete axiomatization.
- Set up when the communication is asynchronous.
THANK YOU
Dziękuję za uwagę