Common knowledge in email exchanges

Sietsma, F.; Apt, K.R.

[Link to publication](#)

Common Knowledge in Email Exchanges

Floor Sietsma* and Krzysztof R. Apt*

Abstract

We consider a framework in which a group of agents communicates by means of emails, with the possibility of replies, forwards and blind carbon copies (BCC). We study the epistemic consequences of such email exchanges by introducing an appropriate epistemic language and semantics. This allows us to determine when a group of agents acquires common knowledge of the formula expressing that an email was sent.

We also show that in our framework from the epistemic point of view the BCC feature of emails cannot be simulated using messages without BCC recipients. Finally, we clarify the notion of a causal relationship between emails using the concept of properly terminating email exchanges.

1   Introduction

1.1   Motivation

Email is by now a prevalent form of communication. Its advantages speak for themselves. However, we rarely pause to reflect on its undesired consequences. Just to mention a few.

One occasionally reads about scandals caused by email leaks, see, e.g., [3]. On a smaller scale, users of the *blind carbon copy* feature (BCC) are sometimes confronted with an undesired situation in which a BCC recipient of an email reveals his status to others by using the *reply-all* feature. Further, many email systems allow one to edit a forwarded email, in particular allowing one to modify the content or the identity of the sender and of the recipients list.

Recently, a main Dutch daily, NRC Handelsblad, reported, see [10], that Wouter Bos, the Deputy Prime minister in the previous Dutch government,

---

*Centrum for Mathematics and Computer Science (CWI), Science Park 123, 1098 XG Amsterdam, the Netherlands, and University of Amsterdam

revealed the extensive network of his contacts by sending out his new email address to about four hundred of influential recipients whose email addresses were erronously put in the CC list instead of the BCC list. The list was leaked to the newspaper.

Epistemic consequences of email exchanges are occasionally raised by researchers in various contexts. For instance, the author of [2] mentions 'some issues of email ethics' by discussing a case of an email discussion in which some researchers were not included (and hence could not build upon the reported results).

Then consider the following recent quotation from a blog in which the writers call for a boycott of a journal XYZ: "We are doing our best to make the misconduct of the Editors-in-Chief a matter of common knowledge within the [...] community in the hope that everyone will consider whatever actions may be appropriate for them to adopt in any future associations with XYZ".

So when studying email exchanges a natural question arises: what are their knowledge-theoretic consequences? To put it more informally: after an email exchange took place, who knows what? Motivated by the above blog entry we can also ask: can sending emails to more and more new recipients ever create common knowledge? (Our Main Theorem shows that the answer is "No.")

To be more specific consider the following example to which we shall return later.

Example 1. Assume the following email exchange involving four people, Alice, Bob, Clare and Daniel:

- Alice and Daniel got an email from Clare,

- Alice forwarded it to Bob,

- Bob forwarded Alice's email to Clare and Daniel with a BCC to Alice,

- Alice forwarded the last email to Clare and Daniel with a BCC to Bob.

The question is:

Do all four people involved in this exchange have common knowledge of Bob's email? □

To answer such questions we study email exchanges focusing on relevant features that we encounter in most email systems.

More specifically, we study the following form of email communication:

- each email has a sender, a non-empty set of regular recipients and a (possibly empty) set of blind carbon copy (BCC) recipients. Each recipient receives a copy of the message and is only aware of the regular recipients and not of the BCC recipients (except himself),

- in the case of a reply to or a forward of a message, the *unaltered* original message is included,

- in a reply or a forward, one can append new information to the original message one replies to or forwards.

As a result, the email exchanges, as studied here, are essentially different from other forms of communication, in particular from multicasting, i.e., sending a message to a group of recipients. Also, the resulting model of email communication differs from the ones that were studied in other papers in which only limited aspects of emails have been considered. These papers are discussed below.

1.2   Contributions and plan of the paper

To study the relevant features of email communication we introduce in the next section a carefully chosen language describing emails. We make a distinction between a *message*, which is sent to a public recipient list, and an *email*, which consists of a message and a set of BCC recipients. This distinction is relevant because a *forward* email contains an earlier message, without the list of BCC recipients. We also introduce the notion of a legal state that captures the fact that there is a *causal ordering* on the emails. For example, an email needs to precede any forward of it.

To reason about the knowledge of the agents after an email exchange has taken place we introduce in Section 3 an appropriate epistemic language. Its semantics takes into account the uncertainty of the recipients of an email about its set of BCC recipients and the ignorance about the existence of emails that one neither sent nor received. This semantics allows us to evaluate epistemic formulas in legal states, in particular the formulas that characterize the full knowledge-theoretic effect of an email.

In Section 4 we present the main result of the paper, that clarifies when a group of agents can acquire common knowledge of the formula expressing the fact that an email has been sent. This characterization in particular sheds light on the epistemic consequences of BCC. The proof is given in Section 5.

Then in Section 6 we show that in our framework BCC cannot be simulated using messages without BCC recipients. Finally, in Section 7 we provide a characterization of legal states in terms of properly terminating email exchanges. This allows us clarify the notion of a causal relationship between emails.

1.3 Related work

The study of the epistemic effects of communication in distributed systems originated in the eighties and led to the seminal book [7]. The relevant literature, including [6], deals only with the customary form of communication, notably asynchronous send.

One of the main issues studied in these frameworks has been the analysis of the conditions that are necessary for acquiring common knowledge. In particular, [8] showed that common knowledge cannot be attained in the systems in which the communication is not guaranteed. More recently this problem was investigated in [4] for synchronous systems with known bounds on message transmission in which processes share a global clock. The authors proved that in such systems a so-called pivotal event is needed in order to obtain common knowledge. This in particular generalizes the previous result of [8] concerning acquisition of common knowledge in distributed systems with synchronous communication.

The epistemic effects of other forms of communication were studied in numerous papers. In particular, in [12] the communicative acts are assumed to consist of an agent j 'reading' an arbitrary propositional formula from another agent i. The idea of an epistemic contents of an email is implicitly present in [13], where a formal model is proposed that formalizes how communication changes the knowledge of a recipient of the message.

In [5] a dynamic epistemic logic modelling effects of communication and change is introduced and extensively studied. Further, in [17] an epistemic logic was proposed to reason about information flow w.r.t. underlying communication channels. [11] surveys these and related approaches and discusses the used epistemic, dynamic epistemic and doxastic logics.

Most related to the work here reported are the following two references. [1] studied knowledge and common knowledge in a set up in which the agents send and forward propositional formulas in a social network. However, the forward did not include the original message and the BCC feature was absent. More recently, in [15] explicit messages are introduced in a dynamic epistemic logic to analyze a similar setting, though BCC was simulated as discussed in Section 6. In both papers it is assumed that the number of

4

messages is finite. In contrast, in the setting of this paper the forward includes the original message, which results directly in an infinite number of messages and emails.

Finally, the concept of a causal relation between messages in distributed systems is due to [9]. Lamport's analysis of causality was extended in the already cited paper [4] to synchronous systems with known bounds on message transmission.

2 Preliminaries

2.1 Messages

In this section we define the notion of a message. We assume non-empty and finite sets of **agents** $Ag = \{1, \ldots, n\}$ and of **notes** L. Each agent has a set of notes he holds initially.

We make a number of assumptions. Firstly, we assume that the agents do not know which notes belong to the other agents. Furthermore, we assume that the agents only exchange emails about the notes. In particular, they cannot communicate epistemic formulas. We also assume that an agent can send a message to other agents containing a note only if he holds it initially or has learnt it through an email he received earlier.

We inductively define **messages** as follows, where in each case we assume that $G \neq \emptyset$:

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

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

So the agents can send a message with a note or forward a message with a new note appended, where the latter covers the possibility of a reply or a reply-all. To allow for the possibility of sending a forward without appending a new note, we can assume there exists a note **true** that is held by all agents and identify **true**.m with m.

If m is a message, then we denote by $S(m)$ and $R(m)$, respectively, the singleton set consisting of the agent sending m and the group of agents receiving m. So for the above messages m we have $S(m) = \{i\}$ and $R(m) = G$. We do allow that $S(m) \subseteq R(m)$, i.e., that one sends a message to oneself.

Special forms of the forward messages can be used to model reply messages. Given $f(i, l.m, G)$, using $G = S(m)$ we obtain the customary *reply*

5

message and using $G = S(m) \cup R(m)$ we obtain the customary *reply-all* message. (In the customary email systems there is syntactic difference between a forward and a reply to these two groups of agents, but the effect of both messages is exactly the same, so we ignore this difference.) In the examples we write $s(i, l, j)$ instead of $s(i, l, \{j\})$, etc.

2.2 Emails

An interesting feature of most email systems is that of the blind carbon copy (BCC). We study here the epistemic effects of sending an email with BCC recipients and will now include this feature in our presentation.

In the previous subsection we defined messages that have a sender and a group of recipients. Now we define the notion of an email which allows the additional possibility of sending a BCC of a message. The BCC recipients are not listed in the list of recipients, therefore we have not included them in the definition of a message. Formally, by an **email** we mean a construct of the form m_B, where m is a message and $B \subseteq Ag$ is a possibly empty set of BCC recipients. Given a message m we call each email m_B a **full version** of m.

Since the set of BCC recipients is 'secret', it does not appear in a forward. That is, the forward of an email m_B with added note l is the message $f(i, l.m, G)$ or an email $f(i, l.m, G)_C$, in which B *is not mentioned*. This is consistent with the way BCC is handled in the email systems. However, this forward may be sent not only by a sender or a regular recipient of m_B, but also by a BCC recipient. Clearly, the fact that an agent was a BCC recipient of an email is revealed at the moment he forwards the message.

A natural question arises: what if someone is both a regular recipient and a BCC recipient of an email? In this case, no one (not even this BCC recipient himself) would ever notice that this recipient was also a BCC recipient since everyone can explain his knowledge of the message by the fact that he was a regular recipient. Only the sender of the message would know that this agent was also a BCC recipient. This fact does not change anything and hence we assume that for any email m_B we have $(S(m) \cup R(m)) \cap B = \emptyset$.

Re: Example 1.

Using the just introduced language we can formalize the story from Example 1 as follows, where we abbreviate Alice to a, etc.:

- Alice and Daniel got an email from Clare:

  $e := m_\emptyset$, where $m := s(c, l, \{a, d\})$,

6

- Alice forwarded it to Bob:

  $e' := m'_\emptyset$, where $m' := f(a, m, b)$,

- Bob forwarded Alice's email to Clare and Daniel with a BCC to Alice:

  $e'' := m''_{\{a\}}$, where $m'' := f(b, m', \{c, d\})$,

- Alice forwarded the last email to Clare and Daniel with a BCC to Bob.

  $f(a, m'', \{c, d\})_{\{b\}}$.

2.3   Legal states

Our goal is to analyze knowledge of agents after some email exchange took place. To this end we need to define a possible collection of sent emails.

First of all, we shall assume that every message is used only once. In other words, for each message m there is at most one full version of m, i.e., an email of the form m_B. The rationale behind this decision is that a sender of m_B and $m_{B'}$ might equally well send a single email $m_{B \cup B'}$. This assumption can be summarized as a statement that the agents do not have 'second thoughts' about the recipients of their emails. It also simplifies subsequent considerations.

In this work we have decided not to impose a total ordering on the emails in our model, for example by giving each email a time stamp. This makes the model a lot simpler. Also, many interesting questions can be answered without imposing such a total ordering. For example, we can investigate the existence of common knowledge in a group of agents after an email exchange perfectly well without knowing the exact order of the emails that were sent.

However, we have to impose some ordering on the sets of emails. For example, we need to make sure that the agents only send information they actually know. Moreover, a forward can only be sent after the original email was sent. We will introduce the minimal partial ordering that takes care of such issues.

First, we define by structural induction the ***factual information*** $FI(m)$ contained in a message m as follows:

$$
\begin{aligned}
FI(s(i, l, G)) &:= \{l\}, \\
FI(f(i, l.m, G)) &:= FI(m) \cup \{l\}.
\end{aligned}
$$

Informally, the factual information is the set of notes which occur somewhere in the message, including those occurring in forwarded messages.

We will use the concept of a **state** to model the effect of an email exchange. A state $s = (E, \mathrm{L})$ is a tuple consisting of a finite set E of emails that were sent and a sequence $\mathrm{L} = (L_1, \ldots, L_n)$ of sets of notes for all agents. The idea of these sets is that each agent i initially holds the notes in L_i. We use E_s and L_s to denote the corresponding elements of a state s, and $L_1, \ldots, L_n$ to denote the elements of L.

We say that a state $s = (E, \mathrm{L})$ is **legal** w.r.t. a strict partial ordering (in short, an spo) $\prec$ on E if it satisfies the following conditions:

L.1: for each email $f(i, l.m, G)_B \in E$ an email $m_C \in E$ exists such that $m_C \prec f(i, l.m, G)_B$ and $i \in S(m) \cup R(m) \cup C$,

L.2: for each email $s(i, l, G)_B \in E$, where $l \notin L_i$, an email $m_C \in E$ exists such that $m_C \prec s(i, l, G)_B$, $i \in R(m) \cup C$ and $l \in FI(m)$,

L.3: for each email $f(i, l.m', G)_B \in E$, where $l \notin L_i$, an email $m_C \in E$ exists such that $m_C \prec f(i, l.m', G)_B$, $i \in R(m') \cup C$ and $l \in FI(m')$.

Condition L.1 states that the agents can only forward messages they previously received. Conditions L.2 and L.3 state that if an agent sends a note that he did not initially hold, then he must have learnt it by means of an earlier email.

We say that a state s is legal iff it is legal w.r.t. some spo. Given a legal state s, by its **causality ordering** we mean the smallest (so the least constraining) spo w.r.t. which s is legal.

So a state is legal if every forward was preceded by its original message, and for every note sent in an email there is an explanation how the sender of the email learnt this note.

3 Epistemic language and its semantics

We want to reason about the knowledge of the agents after an email exchange has taken place. For this purpose we use a language $\mathfrak{L}$ of communication and knowledge defined as follows:

$$\varphi \quad ::= \quad m \mid i \blacktriangleleft m \mid \neg\varphi \mid \varphi \wedge \varphi \mid C_G\varphi$$

Here m denotes a message. The formula m expresses the fact that m has been sent in the past, with some unknown group of BCC recipients. The formula $i \blacktriangleleft m$ expresses the fact that agent i was involved in a full version of the message m, i.e., he was either the sender, a recipient or a BCC recipient.

The formula $C_G\varphi$ denotes common knowledge of the formula φ in the group G.

We use the usual abbreviations $\vee$, $\to$ and $\leftrightarrow$ and use $K_i\varphi$ as an abbreviation of $C_{\{i\}}\varphi$. The fact that an email with a certain set of BCC recipients was sent can be expressed in our language by the following abbreviation:

$$m_B ::= m \wedge \bigwedge_{i \in S(m) \cup R(m) \cup B} i \blacktriangleleft m \wedge \bigwedge_{i \notin S(m) \cup R(m) \cup B} \neg i \blacktriangleleft m$$

Note that this formula expresses the fact that the message m was sent with exactly the group B as BCC recipients, which captures precisely the intended meaning of m_B.

We now provide a semantics for this language interpreted on legal states, inspired by the epistemic logic and the history-based approaches of [12] and [13]. For every agent i we define an indistinguishability relation $\sim_i$, where we intend $s \sim_i s'$ to mean that agent i cannot distinguish between the states s and s'. We first define this relation on the level of emails as follows (recall that we assume that senders and regular recipients are not BCC recipients):

$$m_B \sim_i m'_{B'}$$

iff one of the following contingencies holds:

(i) $i \in S(m)$, $m = m'$ and $B = B'$,

(ii) $i \in R(m) \setminus S(m)$ and $m = m'$,

(iii) $i \in B \cap B'$, and $m = m'$,

(iv) $i \notin S(m) \cup R(m) \cup B$ and $i \notin S(m') \cup R(m') \cup B'$.

Condition (i) states that the sender of an email confuses it only with the email itself. In turn, condition (ii) states that each regular recipient of an email who is not a sender confuses it with any email with the same message but possibly sent to a different BCC group. Next, condition (iii) states that each BCC recipient of an email confuses it with any email with the same message but sent to a possibly different BCC group of which he is also a member. Finally, condition (iv) states that each agent confuses any two emails in which he is not involved.

Example 2. Consider the emails $e := s(i, l, j)_\emptyset$ and $e' := s(i, l, j)_{\{k\}}$. We have then $e \not\sim_i e'$, $e \sim_j e'$ and $e \not\sim_k e'$. Intuitively, agent j cannot distinguish between these two emails because he cannot see whether k is a BCC recipient. In contrast, agents i and k can distinguish between these two emails. $\square$

Next, we extend the indistinguishability relation to legal states by defining

$$(E, \mathrm{L}) \sim_i (E', \mathrm{L}')$$

iff all of the the following hold:

- $L_i = L'_i$,

- for any $m_B \in E$ such that $i \in S(m) \cup R(m) \cup B$ there is $m_{B'} \in E'$ such that $m_B \sim_i m_{B'}$,

- for any $m_{B'} \in E'$ such that $i \in S(m) \cup R(m) \cup B$ there is $m_B \in E$ such that $m_B \sim_i m_{B'}$.

So two states cannot be distinguished by an agent if they agree on his notes and their email sets look the same to him. Since we assume that the agents do not know anything about the other notes, we do not refer to the sets of notes of the other agents. Note that $\sim_i$ is an equivalence relation.

Example 3. Consider the legal states s_1 and s_2 which are identical apart from their sets of emails:

$$
\begin{aligned}
E_{s_1} &:= \{s(i,l,j)_\emptyset, f(j, s(i,l,j), o)_\emptyset\}, \\
E_{s_2} &:= \{s(i,l,j)_{\{k\}}, f(j, s(i,l,j), o)_\emptyset, f(k, s(i,l,j), o)_\emptyset\}.
\end{aligned}
$$

We assume here that $l \in L_i$. The corresponding causality orderings clarify that in the first state agent i sends a message with proposition p to agent j and then j forwards this message to agent o. Further, in the second state agent i sends the same message but with a BCC to agent k, and then both agent j and agent k forward the message to agent o.

From the above definition it follows that $s_1 \not\sim_i s_2$, $s_1 \sim_j s_2$, $s_1 \not\sim_k s_2$ and $s_1 \not\sim_o s_2$. For example, the first claim holds because, as noticed above, $s(i,l,j)_\emptyset \not\sim_i s(i,l,j)_{\{k\}}$. Intuitively, in state s_1 agent i is aware that he sent a BCC to nobody, while in state s_2 he is aware that he sent a BCC to agent k. In turn, in both states s_1 and s_2 agent j is aware that he received the message $s(i,l,j)$ and that he forwarded the email $f(j, s(i,l,j), o)_\emptyset$. Intuitively, in state s_2 agent j does not notice the BCC of the message $s(i,l,j)$ and is not aware of the email $f(k, s(i,l,j), o)_\emptyset$. □

In order to express common knowledge, we define for a group of agents G the relation $\sim_G$ as the reflexive, transitive closure of $\bigcup_{i \in G} \sim_i$. Then we

define the truth of a formula from our language in a state inductively as follows, where $s = (E, \mathrm{L})$:

$$
\begin{array}{lll}
s \models m & \text{iff} & \exists B : m_B \in E \\
s \models i \blacktriangleleft m & \text{iff} & \exists B : m_B \in E \text{ and } i \in S(m) \cup R(m) \cup B \\
s \models \neg \varphi & \text{iff} & s \not\models \varphi \\
s \models \varphi \wedge \psi & \text{iff} & s \models \varphi \text{ and } s \models \psi \\
s \models C_G \varphi & \text{iff} & s' \models \varphi \text{ for any legal state } s' \text{ such that } s \sim_G s'
\end{array}
$$

We say that φ is ***valid*** (and often just write 'φ' instead of 'φ is valid') if for all legal states s, $s \models \varphi$.

Even though this definition does not specify the form of communication, one can deduce from it that the communication is synchronous, that is, that each email is simultaneously received by all the recipients. Namely, the condition of the form $m_B \in E$ present in the second clause implies that for every email m_B the following equivalence is valid for all $i, j \in S(m) \cup R(m) \cup B$:

$$
i \blacktriangleleft m \leftrightarrow j \blacktriangleleft m.
$$

This means that in every legal state (E, L) either all recipients of the email m_B received it (when $m_B \in E$) or none (when $m_B \notin E$).

However, it should be noted that the agents do not have a common 'clock' using which they could deduce how many messages have been sent. Also, there is no common 'blackboard' using which they could deduce how many messages have been sent by other agents between two consecutive messages they have received.

The following lemma clarifies when specific formulas are valid. In the sequel we shall use these observations implicitly.

Lemma 1.

(i) $m \rightarrow m'$ is valid iff $m = m'$ or m' is part of the message m.

(ii) $m \rightarrow i \blacktriangleleft m'$ is valid iff $i \in S(m') \cup R(m')$ or for some note l and group G, $f(i, l.m', G)$ is part of the message m.

The second item states that $m \rightarrow i \blacktriangleleft m'$ is valid either if i is a sender or a receiver of m' (in that case actually $i \blacktriangleleft m'$ is valid) or i forwarded the message m'. The latter is also possible if i was a BCC receiver of m'. The claimed equivalence holds thanks to condition L.1.

Example 4. To illustrate the definition of truth let us return to Example 3. In state s_2 agent j does not know that agent k received the message $s(i, l, j)$

since he cannot distinguish s_2 from the state s_1 in which agent k did not receive this message. So $s_2 \models \neg K_j k \blacktriangleleft s(i, l, j)$ holds.

On the other hand, in every legal state s_3 such that $s_2 \sim_o s_3$ both an email $f(k, s(i, l, j), o)_C$ and a 'justifying' email $s(i, l, j)_B$ have to exist such that $s(i, p, j)_B \prec f(k, s(i, l, j), o)_C$ and $k \in B$. Consequently $s_3 \models k \blacktriangleleft s(i, l, j)$, so $s_2 \models K_o k \blacktriangleleft s(i, l, j)$ holds, so by sending the forward agent k revealed himself to o as a BCC recipient.

We leave to the reader checking that both $s_2 \models C_{\{k,o\}} k \blacktriangleleft s(i, l, j)$ and $s_2 \models \neg C_{\{j,o\}} k \blacktriangleleft s(i, l, j)$ holds. In words, agents k and o have common knowledge that agent k was involved in a full version of the message $s(i, l, j)$, while the agents j and o don't. $\qquad\square$

4   Common knowledge

We now clarify when a group of agents acquires common knowledge of the formula expressing that an email was sent. This shows how we can use our framework to investigate epistemic consequences of email exchanges.

Given a set of emails E and a group of agents A, let

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

When $e \in E_A$ we shall say that the email e is **shared by the group** A. Note that when $|A| \geq 3$, then $e \in E_A$ iff $A \subseteq S(m) \cup R(m)$. When $|A| = 2$, then $e \in E_A$ also when $\exists j \in B : A = S(m) \cup \{j\}$, and when $|A| = 1$, then $e \in E_A$ also when $A = S(m)$ or $\exists j \in B : A = \{j\}$.

The following theorem summarizes our results.

Main Theorem Consider a legal state $s = (E, Ł)$ and a group of agents A.

(i) $s \models C_A m$ iff there is $m'_{B'} \in E_A$ such that $m' \to m$ is valid.

(ii) Suppose that $|A| \geq 3$. Then $s \models C_A m_B$ iff the following hold:

   C1 $Ag = S(m) \cup R(m) \cup B$,
   C2 for each $i \in B$ there is $m'_{B'} \in E_A$ such that $m' \to i \blacktriangleleft m$ is valid,
   C3 there is $m'_{B'} \in E_A$ such that $m' \to m$ is valid.

In words, $s \models C_A m_B$ iff

- the email m_B involves all agents,

- for every agent i that is on the BCC list of m_B there is an email shared by the group A that proves that i forwarded message m,

- there is an email shared by the group A that proves the existence of the message m.

The first of the above three items is striking and shows that common knowledge of an email is rare.

As an aside let us mention that there is a corresponding result for the case when $|A| < 3$, as well. However, it involves a tedious case analysis concerning the possible relations between $A, S(m), R(m)$ and B, so we do not present it here.

Re: Example 1.

We can use the above result to answer the question posed in Example 1. Let s be the state whose emails consist of the considered four emails, so

$e := m_\emptyset$, where $m := s(c, l, \{a, d\})$,
$e' := m'_\emptyset$, where $m' := f(a, m, b)$,
$e'' := m''_{\{a\}}$, where $m'' := f(b, m', \{c, d\})$,
$f(a, m'', \{c, d\})_{\{b\}}$.

Alice's set of notes in s consists of l while the sets of notes of Bob, Clare and Daniel are empty. Note that s is legal. We have then

$$s \not\models C_{\{a,b,c,d\}} f(b, m', \{c, d\})_{\{a\}}.$$

The reason is that condition **C2** does not hold since no email shared by $\{a, b, c, d\}$ exists that proves that Alice received m''. In contrast,

$$s \models C_{\{a,c,d\}} f(b, m', \{c, d\})_{\{a\}}$$

does hold, since the email $f(a, m'', \{c, d\})_{\{b\}}$ is shared by $\{a, c, d\}$. Further, if Alice used the forward $f(a, m'', \{b, c, d\})_\emptyset$, then condition **C2** would hold and we could conclude for this modified state s' that

$$s' \models C_{\{a,b,c,d\}} f(b, m', \{c, d\})_{\{a\}}.$$

5 Proof of the Main Theorem

We establish first a number of auxiliary lemmas. We shall use a new strict partial ordering on emails. We define

$$m_B < m'_{B'} \text{ iff } m \neq m' \text{ and } m' \to m.$$

Note that $m' \to m$ precisely if m' is a forward, or a forward of a forward, etc, of m. Then for two emails m_B and $m_{B'}$ from a legal state s with the causality ordering $\prec$, $m_B < m_{B'}$ implies $m_B \prec m_{B'}$ on the account of condition L.1. However, the converse does not need to hold since $m_B \prec m_{B'}$ can hold on the account of L.2 or L.3. Further, note that the $<$-maximal elements of E are precisely the emails in E that are not forwarded.

Given a set of emails E and $E' \subseteq E$ we then define the ***downward closure*** of E' by

$$E'_{\leq} := E' \cup \{e \in E \mid \exists e' \in E' : e < e'\}.$$

The set of emails E on which the downward closure of E' depends will always be clear from the context.

Next, we introduce two operations on states. Assume a state $(E, \mathbb{L})$ and an email $m_B \in E$.

We define the state

$$s \setminus m_B := (E \setminus \{m_B\}, \mathbb{L}'),$$

with

$$L'_i := \begin{cases} L_i \cup FI(m) & \text{if } i \in R(m) \cup B \\ L_i & \text{otherwise} \end{cases}$$

Intuitively, $s \setminus m_B$ is the result of removing the email m_B from the state s, followed by augmenting the sets of notes of its recipients in such a way that they initially already had the notes they would have acquired from m_B. Note that $s \setminus m_B$ is a legal state if m_B is an $<$-maximal element of E.

Next, given $C \subseteq B$ we define the state

$$s[m_{B \mapsto C}] := (E \setminus \{m_B\} \cup \{m_C\}, \mathbb{L}'),$$

with

$$L'_i := \begin{cases} L_i \cup FI(m) & \text{if } i \in B \setminus C \\ L_i & \text{otherwise} \end{cases}$$

Intuitively, $s[m_{B \mapsto C}]$ is the result of shrinking the set of BCC recipients of m from B to C, followed by an appropriate augmenting of the sets of notes of the agents that no longer receive m.

Note that $s[m_{B \mapsto C}]$ is a legal state if there is no forward of m by an agent $i \in B \setminus C$, i.e., no email of the form $f(i, l.m, G)_D$ exists in E such that $i \in B \setminus C$.

We shall need the following lemma that clarifies the importance of the set E_A of emails.

14

Lemma 2. *Consider a legal state $s = (E, L)$ and a group of agents A. Then for some L' the state $s' := ((E_A)_\leq, L')$ is legal and $s \sim_A s'$.*

Proof. We prove that for all $<$-maximal emails $m_B \in E$ such that $m_B \notin E_A$ (so neither $A \subseteq S(m) \cup R(m)$ nor $\exists i \in B : (A \subseteq S(m) \cup \{i\}))$ we have $s \sim_A s \setminus m_B$. Iterating this process we get the desired conclusion.

Suppose m_B is a $<$-maximal email in E such that $m_B \notin E_A$. Take some $j \in A \setminus (S(m) \cup R(m))$. Suppose first $j \notin B$. Then $s \sim_j s \setminus m_B$ so $s \sim_A s \setminus m_B$.

Suppose now $j \in B$. Define

$$s_1 := s[m_{B \mapsto \{j\}}].$$

Then s_1 is a legal state and $s \sim_j s_1$. Next, define

$$s_2 := s[m_{B \mapsto \emptyset}].$$

Now take some $k \in A \setminus (S(m) \cup \{j\})$. Then $s_1 \sim_k s_2 \sim_j s \setminus m_B$ so $s \sim_A s \setminus m_B$. Note that both s_1 and s_2 are legal states since m_B is $<$-maximal. $\qquad \square$

Using the above lemma we now establish two auxiliary results concerning common knowledge of the formula $i \blacktriangleleft m$ or of its negation.

Lemma 3.

(i) $s \models C_A i \blacktriangleleft m$ iff $\exists m'_B \in E_A : (m' \to i \blacktriangleleft m)$
     or $(A \subseteq S(m) \cup \{i\}$ and $\exists m_B \in E_A : (i \in B))$.

(ii) $s \models C_A \neg i \blacktriangleleft m$ iff $s \models \neg i \blacktriangleleft m$ and $(A \subseteq S(m) \cup \{i\}$ or $s \models C_A \neg m)$.

To illustrate various alternatives listed in (i) note that each of the following emails in E ensures that $s \models C_{\{j\}} i \blacktriangleleft m$, where in each case m is the corresponding send message:

$$s(i, l, G)_{\{j\}}, f(k, q.s(i, l, G), H)_{\{j\}},$$
$$s(k, l, i)_{\{j\}}, \ f(i, q.s(k, l, G), H)_{\{j\}}, \ s(j, l, G)_{\{i\}}.$$

The first four of these emails imply $s \models C_{\{j\}} i \blacktriangleleft m$ by the first clause of (i), the last one by the second clause.

Proof. (i) $(\Rightarrow)$ Suppose $s \models C_A i \blacktriangleleft m$. Take the legal state s' constructed in Lemma 2. Then $s \sim_A s'$, so $s' \models i \blacktriangleleft m$.

Hence for some group B we have $m_B \in (E_A)_\leq$ and $i \in S(m) \cup R(m) \cup B$. Three cases arise.

15

Case 1. $i \in S(m) \cup R(m)$.

Then $m \to i \blacktriangleleft m$. So if $m_B \in E_A$, then the claim holds. Otherwise some email $m'_{B'} \in E_A$ exists such that $m_B < m'_{B'}$. Consequently $m' \to m$ and hence $m' \to i \blacktriangleleft m$. So the claim holds as well.

Case 2. $i \notin S(m) \cup R(m)$ and $A \subseteq S(m) \cup \{i\}$.

Then $i \in B$ since $i \in S(m) \cup R(m) \cup B$. Then by the definition of E_A, $m_B \in E_A$ so the claim holds.

Case 3. $i \notin S(m) \cup R(m)$ and $\neg(A \subseteq S(m) \cup \{i\})$.

If for some note l and groups G and C we have $f(i, l.m, G)_C \in (E_A)_{\leq}$, then either $f(i, l.m, G)_C \in E_A$ or for some $m'_{B'} \in E_A$ we have $f(i, l.m, G)_C < m'_{B'}$. In the former case we use the fact that the implication $f(i, l.m, G) \to i \blacktriangleleft m$ is valid. In the latter case $m' \to f(i, l.m, G)$ and hence $m' \to i \blacktriangleleft m$. So in both cases the claim holds.

Otherwise let $s'' = s'[m_{B \mapsto B \setminus \{i\}}]$. Note that s'' is a legal state because i does not forward m in s'. Take some $j \in A \setminus (S(m) \cup \{i\})$. Then $s' \sim_j s''$, so $s \sim_A s''$. Moreover, $s'' \models \neg i \blacktriangleleft m$, which yields a contradiction. So this case cannot arise.

($\Leftarrow$) The claim follows directly by the definition of semantics. We provide a proof for one representative case. Suppose that for some email $m'_B \in E_A$ both $A \subseteq S(m') \cup R(m')$ and $m' \to i \blacktriangleleft m$. Take some legal state s' such that $s \sim_A s'$. Then for some group B' we have $m'_{B'} \in E_{s'}$. So $s' \models m'$ and hence $s' \models i \blacktriangleleft m$. Consequently $s \models C_A i \blacktriangleleft m$.

(*ii*) Let $s = (E, \mathrm{L})$.

($\Rightarrow$) Suppose $s \models C_A \neg i \blacktriangleleft m$. Then $s \models \neg i \blacktriangleleft m$. Assume $A \nsubseteq S(m) \cup \{i\}$ and $s \nvDash C_A \neg m$. Then there is some legal state $s' = (E', \mathrm{L}')$ such that $s \sim_A s'$ and $s' \models m$. Then there is some group B such that $m_B \in E'$. Let $j \in A \setminus (S(m) \cup \{i\})$ and let $s'' = (E' \setminus \{m_B\} \cup \{m_{B \cup \{i\}}\}, \mathrm{L}')$. Then $s' \sim_j s''$ so $s \sim_A s''$. But $s'' \models i \blacktriangleleft m$ which contradicts our assumption.

($\Leftarrow$) Suppose that $s \models \neg i \blacktriangleleft m$ and either $A \subseteq S(m) \cup \{i\}$ or $s \models C_A \neg m$. We first consider the case that $A \subseteq S(m) \cup \{i\}$. Let s' be any legal state such that $s \sim_A s'$. Assume $s' \models i \blacktriangleleft m$. Then $m_B \in E_{s'}$ for some group B such that $i \in B$. Since $A \subseteq S(m) \cup \{i\}$, any legal state s'' such that $s' \sim_A s''$ contains an email $m_C \in E_{s''}$ for some group C such that $i \in C$. So $s'' \models i \blacktriangleleft m$. In particular, this holds for the state s, which contradicts our assumption. So $s' \models \neg s(i, n, G)$ and hence $s \models C_A \neg s(i, n, G)$.

Now we consider the case that $s \models C_A \neg m$. Let s' be such that $s \sim_A s'$. Then $s' \models \neg m$. Since $i \blacktriangleleft m \to m$ is valid, we get $s' \models \neg i \blacktriangleleft m$. So

$s \models C_A \neg i \blacktriangleleft m.$ $\hfill\square$ $\hfill\blacksquare$

We are now ready to prove the Main Theorem.

Proof (i) $(\Rightarrow)$ Suppose $s \models C_A m$. Take the legal state s' constructed in Lemma 2. Then $s \sim_A s'$, so $s' \models m$. So for some group B we have $m_B \in (E_A)_\leq$.

Hence either $m_B \in E_A$ or some email $m'_{B'} \in E_A$ exists such that $m_B < m'_{B'}$. In both cases the claim holds.

$(\Leftarrow)$ Suppose that for some email $m'_B \in E_A$ we have $m' \to m$. Take some legal state s' such that $s \sim_A s'$. Then by the form of E_A and the definition of semantics for some group B' we have $m'_{B'} \in E_{s'}$. So $s' \models m'$ and hence $s' \models m$. Consequently $s \models C_A m$.

(ii) By the definition of m_B, the fact that the C_A operator distributes over the conjunction, part (i) of the Main Theorem and Lemma 3 we have

$$s \models C_A m_B \text{ iff } \textbf{C3-C6},$$

where

C4 $\bigwedge_{i \in S(m) \cup R(m) \cup B} ((A \subseteq S(m) \cup \{i\} \text{ and } \exists B' : (m_{B'} \in E_A \text{ and } i \in B')) \text{ or } \exists m'_{B'} \in E_A : (m' \to i \blacktriangleleft m)),$

C5 $\bigwedge_{i \notin S(m) \cup R(m) \cup B} (A \subseteq S(m) \cup \{i\} \text{ or } s \models C_A \neg m),$

C6 $s \models \bigwedge_{i \notin S(m) \cup R(m) \cup B} \neg i \blacktriangleleft m.$

$(\Rightarrow)$ Suppose $s \models C_A m_B$. Then properties **C3-C6** hold. But $|A| \geq 3$ and $s \models C_A m$ imply that no conjunct of **C5** holds. Hence property **C1** holds.

Further, since $|A| \geq 3$ the first disjunct of each conjunct in **C4** does not hold. So the second disjunct of each conjunct in **C4** holds, which implies property **C2**.

$(\Leftarrow)$ Suppose properties **C1-C3** hold. It suffices to establish properties **C4-C6**.

For $i \in S(m) \cup R(m)$ we have $m \to i \blacktriangleleft m$. So **C2** implies property **C4**. Further, since **C1** holds, properties **C5** and **C6** hold vacuously. $\hfill\square$

6 Analysis of BCC

In our framework we built emails out of messages using the BCC feature. So it is natural to analyze whether and in what sense the emails can be reduced to messages without BCC recipients.

Given a send email $s(i, l, G)_B$, where $B = \{j_1, \ldots, j_k\}$, we can simulate it by the following sequence of messages:

$$s(i, l, G), f(i, s(i, l, G), j_1), \ldots, f(i, s(i, l, G), j_k).$$

Analogous simulation can be formed for the forward email $f(i, l.m, G)_B$. At first sight, it seems that this simulation has exactly the same epistemic effect as the original email with the BCC recipients. In both states, agents $j_1, \ldots, j_k$ receive a copy of the message and only each of them separately and the sender of the message are aware of this. However, there are two subtle differences.

First of all, there is a syntactic difference between message that agents $j_1, \ldots, j_k$ receive in the original case and in the simulation. In the original case they receive exactly the message m, and in the simulation they receive a forward of it. This also means that if they reply to or forward the message, there is a syntactic difference in this reply or forward. This difference is purely syntactic and does not essentially influence the knowledge of the agents, even though it clearly influences the truth value of the formula $j \blacktriangleleft m$ which is true for $j \in \{j_1, \ldots, j_k\}$ in the original case but not in the simulation.

The second difference is more fundamental. If agents $j_1, \ldots, j_k$ are BCC recipients of m and they do not send a reply to or a forward of m, then each of them can be sure that no other agent but the sender of m knows he was a BCC recipient. Indeed, in our framework there is no message the sender of m could send to another agent, that expresses that agents $j_1, \ldots, j_k$ were the BCC recipients of m.

In the case of the simulation however, these recipients do not receive a BCC but a forward. Since these forwards may have additional BCC recipients of which agents $j_1, \ldots, j_k$ are unaware, they cannot be sure that the other agents do not know that they received a forward of the message. Furthermore, the sender of m could also forward the forward he sent to $j_1, \ldots, j_k$ without informing them about it, thus also revealing their knowledge of m.

A concrete example that shows this difference is the following.

Example 5. Let
$$E_s = \{s(1, l, 2)_{\{3\}}\}.$$

Then $s \models K_3 \neg K_2 K_3 s(1, l, 2)$, that is, agent 3 is sure that agent 2 does not know about his knowledge of the message $s(1, l, 2)$. A simulation of this email without a BCC recipient would result in the state t with (we abbreviate here each email $m_\emptyset$ to m)

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

Now consider a state t' with:

$$E_{t'} = \{s(1, l, 2), f(1, s(1, l, 2), 3), f(1, f(1, s(1, l, 2), 3), 2)\}.$$

Clearly $t \sim_3 t'$ and $t' \models K_2 K_3 s(1, l, 2)$. This shows that $t \not\models K_3 \neg K_2 K_3 s(1, l, 2)$.
$\square$

This argument can be made more general as follows. Below, in the context of a state we identify each message m with the email $m_\emptyset$. Then we have the following result.

Theorem 6. *Take a legal state $s = (E, L)$, an email $m_B \in E$ and an agent $j \in B$ such that E does not contain a forward of m by j or to j. Then for any set of messages M such that (M, L) is a legal state we have for any agent $k \notin S(m) \cup \{j\}$*

$$s \models K_j m \wedge K_j \neg K_k K_j m,$$

while

$$(M, Ł) \not\models K_j m \wedge K_j \neg K_k K_j m.$$

Proof. Agent j is a BCC recipient of m in s, so by the definition of the semantics $s \models K_j m$. We will first show that $s \models K_j \neg K_k K_j m$. Take some state t such that $s \sim_j t$. Then by the definition of the semantics there is some group C such that $m_C \in E_t$ and $j \in C$. Suppose that m is a send email, say $m = s(i, l, G)$. For the case that m is a forward email the reasoning is analogous. Let u be the state like t, but with

$$E_u = E_t \backslash \{s(i, l, G)_C\} \cup \{s(i, l, G)_{C \backslash \{j\}}, s(i, l, j)\}.$$

Note that we implicitly assume that no full version of $s(i, l, j)$ is already present in E_t. If there were such a full version, we could do the same construction without adding $s(i, l, j)$ to E_t.

Since there are no forwards of m by j or to j in E, and $s \sim_j t$, there are no forwards of m by j or to j in E_t. This shows that u is a legal state and that there are no forwards of m to j in E_u so $u \not\models K_j m$. Clearly, for any $k \notin S(m) \cup \{j\}$ we have $t \sim_k u$. So $t \not\models K_k K_j m$, which shows that $s \models K_j \neg K_k K_j m$.

Take now any set of messages M such that $(M, Ł)$ is legal and suppose $(M, Ł) \models K_j m$. Then by the Main Theorem there is some message m' in which agent j was involved that implies that message m was sent. By the requirements on the legal states we know that there is such a message

m' of which agent j was a recipient, and not the sender, since agents can only send information they initially knew or received through some earlier message. Since there are no BCC recipients in M, we conclude that agent j is a regular recipient of m' that he received from some other agent and that $m' \to m$ is valid.

Define the set of messages M' by

$$M' := M \cup \{f(S(m'), m', k)\}.$$

Note that $(M', Ł)$ is a legal state, and $(M', Ł) \models K_k m'$. Since j is a regular recipient of m', $m' \to K_j m'$ is valid and since $m' \to m$ is also valid this implies that $(M', Ł) \models K_k K_j m$. Also, since j is not involved in $f(S(m'), m', k)$, $(M, Ł) \sim_j (M', Ł)$. This shows that $(M, Ł) \not\models K_j \neg K_k K_j m$. In view of our assumption that $(M, Ł) \models K_j m$ we conclude that $(M, Ł) \not\models K_j m \wedge K_j \neg K_k K_j m$. $\square$

In this theorem we assume that for the BCC recipient j of the message m there are no forwards of m to j or by j. The theorem shows that under these assumptions, s and (M, L) can be distinguished by an epistemic formula concerning the message m. We will now show that these assumptions are necessary.

Example 7. Take a legal state $s = (E, Ł)$ with

$$E = \{s(1, l, 2)_{\{3\}}, f(2, s(1, l, 2), 3)\}$$

and

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

We can see that $(M, Ł)$ is a perfect BCC-free simulation of s: for any formula φ that holds in s, if we replace the occurrences of $3 \blacktriangleleft s(1, l, 2)$ in φ by $f(1, s(1, l, 2), 3)$ then the result holds in $(M, Ł)$. The reason that we can find such a set M is that in E there is a forward of $s(1, l, 2)$ to agent 3. This reveals the "secret" that agent 3 knows about $s(1, l, 2)$ and then the fact that agent 3 was a BCC recipient of $s(1, l, 2)$ is no longer relevant.

Example 8. A similar example shows the importance of the assumption that there are no forwards by a BCC recipient. Take a legal state $s = (E, Ł)$ with

$$E = \{s(1, l, 2)_{\{3\}}, f(3, s(1, l, 2), 2)\}$$

and

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

Again, for any formula φ that holds in s, if we replace the occurrences of $3 \blacktriangleleft s(1, l, 2)$ in φ by $f(1, s(1, l, 2), 3)$ then the result holds in (M, L). Now the reason is that agent 3 informed agent 2 that he was a BCC recipient of $s(1, l, 2)$ in s by sending a forward of this message, so again the fact that agent 3 knows $s(1, l, 2)$ is not secret anymore.

It is interesting to note that the impossibility of simulating BCC by means of messages is in fact caused by our choice of uninterpreted notes as the basic contents of the messages. If our framework allowed one to send messages containing more complex information, for example a formula of the form $j \blacktriangleleft m$, the sender of m could have informed other agents who were the BCC recipients. Then in Example 5 we could consider a state s' with

$$E_{s'} = \{s(1, n, 2)_{\{3\}}, s(1, 3 \blacktriangleleft s(1, n, 2), 2)\}.$$

By appropriately extending our semantics we would have then $s \sim_3 s'$ and $s' \models K_2 K_3 s(1, n, 2)$, and hence $s \not\models K_3 \neg K_2 K_3 s(1, n, 2)$, so the difference between the above two states s and t would then disappear. We leave an analysis of this extension of our framework and the role of BCC in this extended setting as future work.

7 Email exchanges

In this section we provide a characterization of the notion of a legal state in terms of email exchanges. In this setting emails are sent in a nondeterministic order, each time respecting the restrictions imposed by the legality conditions L.1 – L.3 of Subsection 2.3.

We define first an operational semantics in the style of [14], though with some important differences concerning the notions of a program state and the atomic transitions. Let M be the set of all messages (so *not* emails). By a **mailbox** we mean a function $\sigma : Ag \to \mathcal{P}(M)$; $\sigma(i)$ is then the mailbox of agent i. If for all i we have $\sigma_0(i) = \emptyset$, then we call σ_0 the **empty mailbox**. A **configuration** is a construct of the form $< s, \sigma >$, where s is a legal state and σ is a mailbox.

Atomic transitions between configurations are of the form

$$< s, \sigma > \to < s', \sigma' >,$$

where

- $s := (E \cup \{m_B\}, \text{L})$,

- $s' := (E, Ł)$,

- for $j \in Ag$

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

We say that the above transition **processes** the email m_B. This takes place subject to the following conditions depending on the form of m, where $Ł = (L_1, \ldots, L_n)$:

- **send** $m = s(i, l, G)$.

  We stipulate then that $l \in L_i$ or for some $m' \in \sigma(i)$ we have $l \in FI(m')$. In the second case of the second alternative we say below that m **depends on** m'.

- **forward** $m = f(i, l.m', G)$.

  We stipulate then that $m' \in \sigma(i)$, and $l \in L_i$ or for some $m'' \in \sigma(i)$ we have $l \in FI(m'')$.

  In the case of the first alternative we say below that m **depends on** m' and in the case of the second alternative that m **depends on** m' and m''.

Given a legal state s an **email exchange starting in** s is a maximal sequence of transitions starting in the configuration $< s, \sigma_0 >$, where σ_0 is the empty mailbox. An email exchange **properly terminates** if its last configuration is of the form $< s', \tau >$, where $s' = (\emptyset, Ł)$.

Note that messages are never deleted from the mailboxes. Further, observe that in the above atomic transitions we augment the mailboxes of the recipients of m_B (including the BCC recipients) by m and *not* by m_B. So the recipients of m_B only 'see' the message m in their mailboxes. Likewise, we augment the mailbox of the sender by the message m and *not* by m_B. As a result when in an email exchanges a sender forwards his own email, the BCC recipients of the original email are not shown in the forwarded email. This is consistent with the discussion of the emails given in Subsection 2.2.

Observe that from the form of a message m in the mailbox $\sigma(i)$ we can infer whether agent i received it by means of a BCC. Namely, this is the case iff $i \notin R(m) \cup S(m)$. (Recall that by assumption the sets of regular recipients and BCC recipients of an email are disjoint.)

The following result then clarifies the concept of a legal state.

Theorem 9. *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.*

The equivalence between (i) and (ii) states that the property of a legal state amounts to the possibility of processing all the emails in an orderly fashion.

Proof. Suppose $s = (E, \mathrm{L})$.
$(i) \Rightarrow (ii)$. Suppose s is legal w.r.t. an spo $\prec$. Extend $\prec$ to a linear ordering $\prec_l$ on E. (Such an extension exists on the account of the result of [16].) By the definition of the atomic transitions we can process the emails in E in the order determined by $\prec_l$. The resulting sequence of transitions forms a properly terminating email exchange starting in s.

$(ii) \Rightarrow (iii)$. Let ξ be a properly terminating email exchange starting in s and ξ' another email exchange starting in s. Let m_B be the first email processed in ξ that is not processed in ξ'. The final mailbox of ξ' contains the message(s) on which m depends on, since their full versions were processed in ξ before m_B and hence were also processed in ξ'. So m_B can be processed in the final mailbox of ξ', i.e., ξ' is not a maximal sequence. This is a contradiction.

$(iii) \Rightarrow (ii)$. Obvious.

$(ii) \Rightarrow (i)$. Take a properly terminating email exchange ξ starting in s. For two emails $e_1, e_2 \in E$ let $e_1 \prec e_2$ iff e_1 is processed in ξ before e_2. By the definition of the atomic transitions s is legal w.r.t. $\prec$. $\qquad\square$

8 Conclusions and future work

Email is by now one of the most common forms of group communication. This motivates the study here presented. The language we introduced allowed us to discuss various fine points of email communication, notably forwarding and the use of BCC. The epistemic semantics we proposed aimed at clarifying the knowledge-theoretic consequences of this form of communication. Our presentation focused on the issue of common knowledge allowed us to determine when a group of agents has a common knowledge of an email.

This framework also leads to natural questions concerning axiomatization of the introduced language and the decidability of its semantics. Currently we work on

- a sound and complete axiomatization of the epistemic language $\mathfrak{L}$ of Section 3; at this stage we have such an axiomatization for the non-epistemic formulas,

- the problem of decidability of the truth definition given in Section 3; at this stage we have a decidability result for positive formulas,

- a comparison of the proposed semantics with the one based on sequences ('histories') of emails rather than partially ordered sets of emails.

In our framework, as explained in Section 3, communication is synchronous. We plan to extend our results to the more general framework of [4], by assuming for each agent a time bound by which he reads his emails.

Another extension worthwhile to study is one in which the agents communicate richer basic statements than just notes. We already indicated in Section 6 that sending messages containing a formula $i \blacktriangleleft m$ increases the expressiveness of the messages from the epistemic point of view. One could also consider in our framework sending epistemic formulas, a feature recently studied in a different setting in [15].

Acknowledgements

References

[1] K. R. Apt, A. Witzel, and J. A. Zvesper. Common knowledge in inter-action structures. In *Proceedings of TARK XII*, pages 4–13. The ACM Digital Library, 2009.

[2] L. Babai. E-mail and the unexpected power of interaction. In *Fifth Structure in Complexity Theory Conference*, pages 30–44, 1990.

[3] E-mail leak of degree inflation. BBC News, 2008. Available at `http://news.bbc.co.uk/2/hi/uk_news/education/7483330.stm`.

[4] I. Ben-Zvi and Y. Moses. Beyond lamport's *Happened-Before*: On the role of time bounds in synchronous systems. In *Proceedings of DISC 2010)*, pages 421–436, 2010.

[5] J. v. Benthem, J. van Eijck, and B. Kooi. Logics of communication and change. *Information and Computation*, 204(11):1620–1662, 2006.

[6] K. M. Chandy and J. Misra. How processes learn. *Distributed Computing*, 1(1):40–52, Mar. 1986.

[7] R. Fagin, J. Halpern, M. Vardi, and Y. Moses. *Reasoning about knowledge*. MIT Press, Cambridge, MA, USA, 1995.

[8] J. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM*, 37.

[9] L. Lamport. Time, clocks, and the ordering of events in a distributed system. *Commun. ACM*, 21(7):558–565, 1978.

[10] Wouter Bos e-mailt per ongeluk zijn netwerk rond. NRC Handelsblad, 7th October 2010, 2010. In Dutch.

[11] E. Pacuit. Logics of informational attitudes and informative actions. Manuscript, University of Tilburg, 2010.

[12] E. Pacuit and R. Parikh. Reasoning about communication graphs. *Interactive Logic. Proceedings of the 7th Augustus de Morgan Workshop*, pages 135–157, 2007.

[13] R. Parikh and R. Ramanujam. A knowledge based semantics of messages. *Journal of Logic, Language and Information*, 12(4):453–467, 2003.

[14] G. D. Plotkin. An operational semantics for CSP. In D. Bjørner, editor, *Formal Description of Programming Concepts II*, pages 199–225, Amsterdam, 1982. North-Holland.

[15] F. Sietsma and J. van Eijck. Message passing in a dynamic epistemic logic setting. In *Proceedings of TARK XIII*, pages 212–220. The ACM Digital Library, 2011.

[16] E. Szpilrajn. Sur l'extension de l'ordre partiel. *Fundamenta Mathematicae*, 16:386–389, 1930.

[17] Y. Wang, F. Sietsma, and J. van Eijck. Logic of information flow on communication channels. In *Proceedings of AAMAS-10*, pages 1447–1448, 2010.