2008

TR-2008001: Public and Private Communication Are Different: Results on Relative Expressivity

Bryan Renne

Public and Private Communication are Different: Results on Relative Expressivity

Bryan Renne
Computer Science
CUNY Graduate Center
365 Fifth Avenue, Room 4319
New York NY 10016
USA

http://bryan.renne.org/

January 11, 2008

Abstract

Dynamic Epistemic Logic (DEL) is the study of how to reason about knowledge, belief, and communication. This paper studies the relative expressivity of certain fragments of the DEL language for public and private communication. It is shown that the language of public communication with common knowledge and the language of private communication with common knowledge are expressively incomparable for the class of all pointed models, which provides a formal proof that public and private communication are fundamentally different. It is also shown that single-recipient private communication does not add expressive power to the language of basic multi-modal logic with common knowledge for any class of *transitive* pointed models. The latter result provides a sense in which positive introspection—believing our own beliefs—induces a kind of self-dialog.

1 Introduction

In using modal logic to reason about the knowledge and belief of agents, we assume that a complete description of a certain moment in time is given by a *pointed Kripke model* [5, 8]. Now a *Kripke model* itself consists of a nonzero number of *worlds*—each having its own truth assignment describing the basic facts of that world—along with a number of binary relations, one for each agent, that may or may not hold between any two worlds. The binary relations represent agent uncertainty: if agent i's relation connects world Γ to world Δ, then agent i will consider it possible that the actual world is Δ whenever the world is in fact Γ. So for

agent i to believe something at world Γ, that something must be true at all those worlds i considers to be possible with respect to Γ. This is just Hintikka's notion of belief [8].

In this setup, knowledge is identified with correct belief: to say that agent i *knows* a statement φ at world Γ means that agent i believes φ at Γ and this belief is correct (that is, φ is true at Γ) [5].

Now a *pointed Kripke model* is a pair (M, Γ) consisting of a Kripke model M and a particular world Γ in M. The world Γ is to be thought of as the *actual* world. The truth assignment of the actual world Γ tells us the basic facts of the situation represented by (M, Γ). The purpose of the other worlds in M is to represent the agents' beliefs. An agent's beliefs may concern both the basic facts of the situation (M, Γ) and also higher-order beliefs (that is, beliefs about beliefs).

Since we have identified a pointed Kripke model (M, Γ) with a complete description of a certain moment in time, a natural way to represent the passage of time is to consider sequences of moments; that is, we consider sequences

$$(M_1, \Gamma_1), (M_2, \Gamma_2), (M_3, \Gamma_3), \ldots, (M_n, \Gamma_n)$$

consisting of pointed Kripke models. This view of time is discrete, with the complete description of the k-th moment in time given by the pointed Kripke model (M_k, Γ_k).

Thinking of our agents as a distributed system, such a sequence of moments represents a certain run of the system, where the $(k+1)$-st moment is generated from the k-th moment as a result of the occurrence of a communication to one or more of the agents. In reasoning about such runs, we often want to consider how the agents' knowledge and belief is affected by a given kind of communication. Here are two examples.

1. If all agents receive a public communication that some basic statement p is true at the actual world in moment (M, Γ), then it ought to be common knowledge in the next moment (M', Γ') that p is true.

2. If no agent knows whether p is true in moment (M, Γ), then the private communication to just those agents in group G that p is true ought to bring about a next moment (M', Γ') in which p is common knowledge among the agents in G and yet p is still unknown to the agents not in G.

Dynamic Epistemic Logic (DEL) is the study of how to reason about knowledge, belief, and communication [1, 2, 6, 9, 12]. DEL uses modal logic as the basic language for describing knowledge, belief, and fact. This basic language is then extended in various ways in order to describe what happens as a result of some communication. In this paper, we will consider extensions of the following kind: for a group G of agents and statements φ and ψ, we will write the statement

$$[\varphi{\rightarrow}\, G]\psi$$

to mean that ψ is true after φ is communicated privately to just those agents in group G. We will use A to represent the group consisting of all agents, so the statement

$$[\varphi{\rightarrow}\, A]\psi$$

says that ψ is true after φ is communicated publicly to all agents. Such statements allow us to express how communication affects knowledge and belief. In particular, we can express our example statements above.

1. $[p{\rightarrow}A]C_A p$

   In words: after the communication of p to the agents in A, we have that p is common knowledge among those in A.

2. $\big(\bigwedge_{i\in A}\neg K_i p\big) \supset [p{\rightarrow}G]\big(C_G p \wedge \bigwedge_{i\in A\setminus G}\neg K_i p\big)$

   In words: if no agent $i \in A$ knows p, then after the communication of p to just those agents in group G, we have that p is common knowledge among those in G and that no $i \in A\setminus G$ knows p.

   (Note: we always assume that A is finite.)

While we have only mentioned public and private communications, there is a natural way to define much more general kinds of communication that allow for complicated combinations of privacy and deceit [1]. With such a wide range of communications available, researchers have begun to try and classify how these many communications relate [1, 3, 6, 7, 9, 11]. For example, it has been shown that for the basic multi-modal language not containing common knowledge statements, adding statements $[\varphi{\rightarrow}A]\psi$ of public communication does not add expressive power [3, 6, 9]. Thus the basic multi-modal language without common knowledge can already express the concept of public communication. But it has also been shown that this is not true of the basic multi-modal language *with* common knowledge statements [3, 12].

Formally, such work is a study of the relative expressivity of the various languages obtained from basic multi-modal logic by adding additional syntax to represent various classes of communication. Most of the known DEL expressivity work has focused on public communication [3, 6, 9, 11, 12], though some work has been done on private communication [3]. In [3], it is shown that the language with common knowledge and private communication can express a concept that cannot be expressed using the language with common knowledge and public communication. In the present paper, we show that this result holds the other way around: the language with common knowledge and public communication can express a concept that cannot be expressed using any combination of private communications. Combining our result with that of [3], we obtain a proof that public and private communication with common knowledge are expressively incomparable. This provides a formal sense in which public and private communication are fundamentally different.

We also show that if our agents' beliefs satisfy the property of positive introspection (meaning each agent believes all of his beliefs), then the language of basic multi-modal logic with common knowledge can already express the concept of single-recipient private communication. A consequence of this curious result is that private communication to exactly one recipient is implicit in KD45, a logic typically used for reasoning about belief [5]. Thus there is a sense in which positively introspective belief already contains single-recipient private communication, which is a way of saying that believing our own beliefs induces a kind of self-dialog.

2 Public and Private Communication

In this section, we introduce the syntax and semantics of our formal language for reasoning about public and private communication.

2.1 Syntax

Definition 2.1. Let A be a finite nonempty set. The *language of public and private communication (over A)*, written $\mathfrak{L}^A$, consists of the formulas φ built by the following grammar.

$$\varphi \ ::= \ p_k \mid \bot \mid \varphi_1 \supset \varphi_2 \mid K_i\varphi \mid C_G\varphi \mid [\varphi_1 \to G]\varphi_2 \qquad \text{for each } k \in \mathbb{N},\ i \in A,\ \emptyset \neq G \subseteq A$$

$\{p_k : k \in \mathbb{N}\}$ is the set of *propositional letters*. A formula written using other logical connectives is understood as an abbreviation for an appropriate formula in this language. Abbreviation: for each $i \in A$, we set $[\varphi_1 \to i]\varphi_2 := [\varphi_1 \to \{i\}]\varphi_2$.

We read the formula $[\varphi \to G]\psi$ as "ψ is true after the communication of φ to just those in G."

It will be useful to define a few fragments of our language $\mathfrak{L}^A$, with the particular fragment determined by the various groups of agents that are allowed to receive a communication.

Definition 2.2. Let A be a finite nonempty set. If $\mathfrak{G} \subseteq 2^A \backslash \{\emptyset\}$ is a possibly empty collection of nonempty subsets of A, then the *$\mathfrak{G}$-fragment* of $\mathfrak{L}^A$, written $\mathfrak{L}^A(\mathfrak{G})$, is the language obtained from $\mathfrak{L}^A$ by restricting the rule $\varphi \mapsto [\varphi_1 \to G]\varphi_2$ of formula formation so that $G \in \mathfrak{G}$. Note: $\mathfrak{L}^A(\emptyset)$ simply omits the rule $\varphi \mapsto [\varphi_1 \to G]\varphi_2$ of formula formation all together. Notation: for a nonempty $G \subseteq A$, we let $\mathfrak{L}^A(G)$ denote $\mathfrak{L}^A(\{G\})$.

We now define a few fragments of $\mathfrak{L}^A$ that are of particular interest in the present paper.

Definition 2.3. Let A be a finite nonempty set and $G \subseteq A$ be a nonempty subset.

- The *language of public communication (over A)*, written $\mathfrak{L}^A_{\to A}$, is $\mathfrak{L}^A(A)$.
- The *language of private communication (over A) to all but G*, written $\mathfrak{L}^A_{\not\to G}$, is $\mathfrak{L}^A\big(2^A \backslash \{\emptyset, G\}\big)$.
- The *language of private communication (over A)* is $\mathfrak{L}^A_{\not\to A}$.

Abbreviation: for each $i \in A$, we set $\mathfrak{L}^A_{\to i} := \mathfrak{L}^A_{\to \{i\}}$.

2.2 Semantics

$\mathfrak{L}^A$-formulas are interpreted using an extension of Kripke's semantics for modal logic. This extension is due to Baltag, Moss, and Sołecki [1, 2].

Definition 2.4. Let A be a finite nonempty set. A *model (for A)* is a tuple $(W, \{R_i\}_{i \in A}, V)$ whose components are given as follows.

- W is a nonempty set whose elements are called *worlds (in M)*.
- For each $i \in A$: R_i is a binary relation on W.[1]
- $V : \{p_k : k \in \mathbb{N}\} \to 2^W$ is a function mapping each propositional letter p_k to a possibly empty set $V(p_k)$ of worlds.

If $M = (W, \{R_i\}_{i\in A}, V)$ is a model, then we write $\Gamma \in M$ to mean that $\Gamma \in W$. A *pointed model (for A)* is a pair (M, Γ) consisting of a model M and a world $\Gamma \in M$; the world $\Gamma \in M$ is called the *point* of (M, Γ). To say that pointed model (M, Γ) for A has a property P of binary relations—examples include reflexivity, transitivity, seriality, or being euclidean—means that for $M = (W, \{R_i\}_{i\in A}, V)$, we have that R_i has property P for each $i \in A$.[2] For a pointed model (M, Γ) and a formula $\varphi \in \mathfrak{L}^A$, we write $M, \Gamma \models \varphi$ to mean that φ is *true at* (M, Γ). The negation of $M, \Gamma \models \varphi$ is written $M, \Gamma \not\models \varphi$. Truth of a formula $\varphi \in \mathfrak{L}^A$ at a pointed model (M, Γ) is given by the following induction on the construction of φ.

- $M, \Gamma \models p_k$ means that $\Gamma \in V(p_k)$.
- $M, \Gamma \not\models \bot$.
- $M, \Gamma \models \varphi_1 \supset \varphi_2$ means that $M, \Gamma \not\models \varphi_1$ or $M, \Gamma \models \varphi_2$.
- $M, \Gamma \models K_i\varphi$ means that $M, \Delta \models \varphi$ for each $\Delta \in M$ satisfying $\Gamma R_i \Delta$.
- $M, \Gamma \models C_G\varphi$ means that for each non-negative integer $n \in \mathbb{N}$, if $\{\Gamma_k\}_{k=0}^n$ is a sequence of worlds in M such that $\Gamma_0 = \Gamma$ and each $k \in \mathbb{N}$ satisfying $k < n$ has an $i \in G$ such that $\Gamma_k R_i \Gamma_{k+1}$, then $M, \Gamma_n \models \varphi$.
- $M, \Gamma \models [\varphi_1 \to G]\varphi_2$ means that either we have $M, \Gamma \not\models \varphi_1$ or else we have both $M, \Gamma \models \varphi_1$ and $M[\varphi_1 \to G], (\Gamma, 0) \models \psi$, where the model $M[\varphi_1 \to G]$ is the tuple

$$\big(W[\varphi_1 \to G], \{R_i[\varphi_1 \to G]\}_{i\in A}, V[\varphi_1 \to G]\big)$$

  whose components are given as follows.

  - $W[\varphi_1 \to G] \;:=\; \{(\Gamma, 0) \in W \times \{0\} : M, \Gamma \models \varphi_1\} \cup \{(\Gamma, 1) \in W \times \{1\} : \Gamma \in W\}$
  - For each $i \in G$: $R_i[\varphi_1 \to G]$ is the set

$$\Big\{\big((\Gamma, a), (\Delta, b)\big) \in (W[\varphi_1 \to G])^2 : (\Gamma R_i \Delta) \wedge (a = b)\Big\}$$

[1] R is a binary relation on a set W iff $R \subseteq W^2$. If R is a binary relation on a set W and $\Gamma, \Delta \in W$, then we write $\Gamma R \Delta$ to mean that $(\Gamma, \Delta) \in R_i$.

[2] Let R be a binary relation on a set W. R is *reflexive* iff $\Gamma R \Gamma$ for each $\Gamma \in W$. R is *transitive* iff $\Gamma R \Delta$ and $\Delta R \Omega$ together imply $\Gamma R \Omega$ for each $\Gamma, \Delta, \Omega \in W$. R is *serial* iff for each $\Gamma \in W$, there is a $\Delta \in W$ such that $\Gamma R \Delta$. R is *euclidean* iff $\Gamma R \Delta$ and $\Gamma R \Omega$ together imply $\Delta R \Omega$ for each $\Gamma, \Delta, \Omega \in W$.

– For each $j \in A\backslash G$: $R_j[\varphi_1{\rightarrow}\, G]$ is the set

$$\Big\{\big((\Gamma, a), (\Delta, b)\big) \in (W[\varphi_1{\rightarrow}\, G])^2 : (\Gamma R_j \Delta) \wedge (b = 1)\Big\}$$

– $V[\varphi_1{\rightarrow}\, G](p_k) := \big\{(\Gamma, a) \in W[\varphi_1{\rightarrow}\, G] : \Gamma \in V(p_k)\big\}$

If $\mathcal{I}$ is a set of pointed models for A, then to to say that a formula $\varphi \in \mathfrak{L}^A$ is *valid for* $\mathcal{I}$, written $\mathcal{I} \models \varphi$, means that $M, \Gamma \models \varphi$ for each pointed model $(M, \Gamma) \in \mathcal{I}$. To say that a formula $\varphi \in \mathfrak{L}^A$ is *valid*, written $\models \varphi$, means that φ is valid for the set of all pointed models for A.

The idea behind the construction of the model $M[\varphi{\rightarrow}\, G]$ may be understood as follows. The worlds in $M[\varphi{\rightarrow}\, G]$ of the form $(\Gamma, 0)$ are just those worlds of M at which φ is true, while the worlds in $M[\varphi{\rightarrow}\, G]$ of the form $(\Gamma, 1)$ make up a copy of the model M. The binary relations in $M[\varphi{\rightarrow}\, G]$ are then defined so that from a world $(\Gamma, 0)$, agents in G will only consider possible worlds of the form $(\Delta, 0)$ while agents in $A\backslash G$ will only consider possible worlds of the form $(\Delta, 1)$. Thus the agents in G jointly eliminate from consideration all worlds in M at which φ is not true—and in this sense it becomes common knowledge among G that φ was communicated—while the agents in $A\backslash G$ are effectively unaware that the communication of φ to G ever occurred. So in case we have that $M, \Gamma \models \varphi$, then the construction of $M[\varphi{\rightarrow}\, G]$ takes us from the moment in time given by the pointed model (M, Γ) to a next moment in time given by the pointed model $\big(M[\varphi{\rightarrow}\, G], (\Gamma, 0)\big)$. It is in this way that communication moves time from one moment to the next in this framework.

3 Relative Expressivity

Expressivity is the comparative study of the propositions expressible in two languages that share a common semantics. The intuitive question this study attempts to answer is the following: can one language say everything that the other language can say?

Definition 3.1. Let A be a finite nonempty set, $\mathfrak{L}_1$ and $\mathfrak{L}_2$ be sub-languages of $\mathfrak{L}^A$, and $\mathcal{I}$ be a set of pointed models for A. A *translation function (from* $\mathfrak{L}_1$ *to* $\mathfrak{L}_2$ *over* $\mathcal{I}$*)* is a function $u : \mathfrak{L}_1 \to \mathfrak{L}_2$ that maps each formula $\varphi \in \mathfrak{L}_1$ to a formula $\varphi^u \in \mathfrak{L}_2$ such that for each $\psi \in \mathfrak{L}_1$ and each $I \in \mathcal{I}$, we have $I \models \psi$ if and only if $I \models \psi^u$. We write $\mathfrak{L}_1 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ to mean that there exists a translation function $u : \mathfrak{L}_1 \to \mathfrak{L}_2$ over $\mathcal{I}$. The negation of $\mathfrak{L}_1 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ is written $\mathfrak{L}_1 \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$.

Our informal reading of $\mathfrak{L}_1 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ is "$\mathfrak{L}_2$ can say at least as much as $\mathfrak{L}_1$." This reading leads us to the following definition of relative expressivity.

Definition 3.2 (Relative Expressivity)**.** We adopt the notation of Definition 3.1.

- To say that $\mathfrak{L}_1$ is *more expressive (for* $\mathcal{I}$*)* than $\mathfrak{L}_2$ means that $\mathfrak{L}_1 \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ and $\mathfrak{L}_2 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_1$.

- To say that $\mathfrak{L}_1$ and $\mathfrak{L}_2$ are *equally expressive (for $\mathcal{I}$)* means that $\mathfrak{L}_1 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ and $\mathfrak{L}_2 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_1$.
- To say that $\mathfrak{L}_1$ and $\mathfrak{L}_2$ are *expressively incomparable (for $\mathcal{I}$)* means that $\mathfrak{L}_1 \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ and $\mathfrak{L}_2 \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}_1$.

Our definition of $\mathfrak{L}_1 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ is our formalization for the notion of $\mathfrak{L}_2$ saying at least as much as $\mathfrak{L}_1$. This gives us a partial ordering on languages, from which we defined the strict partial ordering that is relative expressivity. But note that these definitions all depend on a given set $\mathcal{I}$ of pointed models for A. In particular, we will show in the last section how a specific choice of $\mathcal{I}$ affects the outcome of an expressivity result.

4 Some Known Results on Relative Expressivity

We recall the first expressivity theorems in DEL.

Theorem 4.1 (Plaza-Gerbrandy [6, 9])**.** Let A be a finite nonempty set. For each $\mathfrak{G} \subseteq 2^A \backslash \{\emptyset\}$, let $\mathfrak{L}^A_{\mathscr{C}}(\mathfrak{G})$ be the language obtained from $\mathfrak{L}^A(\mathfrak{G})$ by omitting the rule $\varphi \mapsto C_G\varphi$ of formula formation. Then $\mathfrak{L}^A_{\mathscr{C}}(\emptyset)$ and $\mathfrak{L}^A_{\mathscr{C}}(A)$ are equally expressive for any class of pointed models for A.

The Plaza-Gerbrandy Theorem says that public communication does not add expressive power to the basic language of multi-modal logic without common knowledge.

Theorem 4.2 ([1, 3])**.** Let A be a finite nonempty set. Adopting the notation of the Plaza-Gerbrandy Theorem, we have that $\mathfrak{L}^A_{\mathscr{C}}(\emptyset)$ and $\mathfrak{L}^A_{\mathscr{C}}(2^A \backslash \{\emptyset\})$ are equally expressive for any class of pointed models for A.[3]

Theorem 4.2 says that public and private communication do not add expressive power to the basic language of multi-modal logic without common knowledge.

We now recall a few known results concerning the relative expressivity of certain fragments of $\mathfrak{L}^A$.

Theorem 4.3 ([3, 12])**.** Let A be a set satisfying $|A| = 1$ and let $\mathcal{I}$ be the set of all pointed models for A. Then $\mathfrak{L}^A_{\to A} \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}^A(\emptyset)$.

Since $\mathfrak{L}^A(\emptyset) \hookrightarrow_{\mathcal{I}} \mathfrak{L}^A_{\to A}$ for each finite nonempty set A, Theorem 4.3 tells us that public communication strictly increases the expressivity of the language $\mathfrak{L}^A(\emptyset)$ of basic multi-modal logic with common knowledge for the class of all pointed models for A. Contrasting this theorem with the Plaza-Gerbrandy Theorem, we see that common knowledge is necessary for this expressivity increase to occur.

Theorem 4.4 ([3, 12])**.** Let A be a finite set satisfying $|A| \geq 2$ and let $\mathcal{I}$ be the set of all reflexive, transitive, and euclidean pointed models for A. Then $\mathfrak{L}^A_{\to A} \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}^A(\emptyset)$.

[3] Theorem 4.2 is actually a special case of a more general theorem from [1, 3]: no collection of the general communication types in [1, 3] adds expressivity to $\mathfrak{L}^A_{\mathscr{C}}(\emptyset)$.

Theorem 4.4 tells us that if there are at least two agents in the finite set A, then public communication strictly increases the expressivity of the language $\mathfrak{L}^A(\emptyset)$ of basic multi-modal logic with common knowledge for the class of all pointed models for A that are reflexive, transitive, and euclidean.[4] The latter trio of properties characterizes the class of frames valid for the logic $\mathsf{S5}$, a logic typically used for reasoning about knowledge [5]. Thus public communication strictly increases the expressivity of the (typical) logic of knowledge when common knowledge is present. Contrasting this theorem with Theorem 4.2, we again see that common knowledge is necessary for the increase in expressive power.

Theorem 4.5 ([3])**.** Let A be a finite set satisfying $|A| \geq 2$ and let $\mathcal{I}$ be the set of all pointed models for A. Then $\mathfrak{L}^A_{\rightarrow i} \not\leftrightarrow_{\mathcal{I}} \mathfrak{L}^A_{\rightarrow A}$ for each $i \in A$.[5]

Theorem 4.5 says that if there are at least two agents in the finite set A, then the language $\mathfrak{L}^A_{\rightarrow A}$ of public communication with common knowledge cannot say everything that can be said by the language of single-recipient private communication with common knowledge. Contrasting this theorem with Theorem 4.2, we again see the necessity of common knowledge for an increase in expressive power.

5 Our Results on Relative Expressivity

Our first result, Theorem 5.2, is the strongest possible form for the reverse direction of Theorem 4.5. But before we state our theorem, we make the following auxiliary definition for use in our proof.

Definition 5.1. Let A be a finite nonempty set and $G \subseteq A$ be a nonempty subset. Let $\{g_i\}_{i=1}^{|G|}$ be a fixed enumeration of G. Then given a model $M = (W, \{R_i\}_{i\in A}, V)$ for A and binary relation R on W, the *expansion of M at R by $\{g_i\}_{i=1}^{|G|}$* is the model $(W', \{R'_i\}_{i\in A}, V')$ for A whose components are given as follows.

- $W' := W \cup \big\{(\Gamma, \Delta, i) : (\Gamma, \Delta) \in R,\ i \in \mathbb{N} \text{ with } 1 \leq i \leq |G| - 1\big\}$
  Abbreviations: for each $(\Gamma, \Delta) \in R$, we set $(\Gamma, \Delta, 0) := \Gamma$ and $(\Gamma, \Delta, |G|) := \Delta$.
- For each $i \in \mathbb{N}$ satisfying $1 \leq i \leq |G|$:
$$R'_{g_i} := R_{g_i} \cup \left\{\big((\Gamma, \Delta, i-1), (\Gamma, \Delta, i)\big) : (\Gamma, \Delta) \in R\right\}$$
- For each $i \in A \backslash G$: set $R'_i := R_i$.
- $V'(p_k) := V(p_k) \cup \big\{(\Gamma, \Delta, i) \in W' : i \leq |G| - 1 \text{ and } \Gamma \in V(p_k)\big\}$

[4] Theorem 4.4 fails in the case $|A| = 1$, since we then have $\mathfrak{L}^A_{\rightarrow A} \hookrightarrow_{\mathcal{I}} \mathfrak{L}^A(\emptyset)$ for $\mathcal{I}$ the class of all reflexive, transitive, and euclidean pointed models for A [3].

[5] Theorem 4.5 fails in the case $|A| = 1$ for a trivial reason: $|A| = 1$ implies that $\mathfrak{L}^A_{\rightarrow i} = \mathfrak{L}^A_{\rightarrow A}$ for each $i \in A$.

The expansion of M at R by $\{g_i\}_{=1}^{|G|}$ simply takes each edge $(\Gamma, \Delta) \in R$ and expands it to a path whose edges are the enumeration $\{g_i\}_{i=1}^{|G|}$ of G; that is,

$$\Gamma \xrightarrow{R} \Delta$$

expands to

$$\Gamma \xrightarrow{g_1} (\Gamma, \Delta, 1) \xrightarrow{g_2} (\Gamma, \Delta, 2) \xrightarrow{g_3} \cdots \xrightarrow{g_{|G|-1}} (\Gamma, \Delta, |G| - 1) \xrightarrow{g_{|G|}} \Delta$$

For $i \leq |G| - 1$, the set of propositional letters true at (Γ, Δ, i) is exactly the set of propositional letters true at Γ.

We may now state and prove our first theorem of this section. Compare our theorem with Theorem 4.5.

Theorem 5.2. Let A be a finite nonempty set. Then $\mathfrak{L}^A_{\to A} \not\to_{\mathcal{I}} \mathfrak{L}^A_{\not\to A}$ for the set $\mathcal{I}$ of all pointed models for A.

Proof. If $|A| = 1$, then $\mathfrak{L}^A_{\not\to A} = \mathfrak{L}^A(\emptyset)$, and the result then follows from Theorem 4.3. So we may assume that $|A| \geq 2$. For each non-negative integer $n \in \mathbb{N}$, we define the model

$$B^n := (W^n, \{R^n_i\}_i, V^n)$$

for A and the relation $R^n \subseteq W^n \times W^n$ as follows.

- $W^n := \{\Omega^L_k : k \in \mathbb{N} \text{ and } 1 \leq k \leq n+1\} \cup \{\Omega^R_k : k \in \mathbb{N} \text{ and } 1 \leq k \leq n+1\} \cup \{\Gamma, \Delta\}$

  Abbreviations: we set $\Omega^L_0 := \Omega^R_{n+2} := \Gamma$ and $\Omega^L_{n+2} := \Omega^R_0 := \Delta$.

- For each $i \in A$, set $R^n_i := \emptyset$.

- $V^n(p_k) := \begin{cases} W^n \backslash \{\Delta\} & \text{if } k = 0 \\ \{\Gamma\} & \text{if } k = 1 \\ \emptyset & \text{if } k \geq 2 \end{cases}$

- $R^n := \big\{(\Omega^L_{k-1}, \Omega^L_k) : 1 \leq k \leq n+2\big\} \cup \big\{(\Omega^R_{k-1}, \Omega^R_k) : 1 \leq k \leq n+2\big\}$

Now fix an enumeration $\{a_i\}_{i=1}^{|A|}$ of A. For each $n \in \mathbb{N}$, we define the model C^n as the expansion of B^n at R^n by $\{a_i\}_{i=1}^{|A|}$. See Figure 1 for a picture of C^n.

We now define a depth function $d : \mathfrak{L}^A_{\not\to A} \to \mathbb{N}$ by the following induction on $\mathfrak{L}^A_{\not\to A}$-formula construction.

- $d(p_k) := 0$ for $k \in \mathbb{N}$
- $d(\bot) := 0$
- $d(\varphi_1 \supset \varphi_2) := \max\big\{d(\varphi_1), d(\varphi_2)\big\}$

- $d(K_i\varphi) := 1 + d(\varphi)$ for $i \in A$
- $d(C_G\varphi) := |A| + d(\varphi)$
- $d\big([\varphi_1 \rightarrow G]\varphi_2\big) := |A| + \max\big\{d(\varphi_1), d(\varphi_2)\big\}$

We will prove the following statement that we call S: for each $\varphi \in \mathfrak{L}^A_{\not\rightarrow A}$, each $n \in \mathbb{N}$ satisfying $d(\varphi) < (n+1)\cdot|A|$, each positive integer $k \in \mathbb{N}^+$ satisfying $d(\varphi) + (k-1)\cdot|A| < (n+1)\cdot|A|$, and each $i \in \mathbb{N}$ satisfying both $0 \leq i \leq |A| - 1$ and $d(\varphi) + i + (k-1)\cdot|A| < (n+1)\cdot|A|$, we have that

$$C^n, (\Omega^L_k, i) \models \varphi \quad \text{iff} \quad C^n, (\Omega^R_k, i) \models \varphi \ .$$

Observe that for the $\mathfrak{L}^A_{\rightarrow A}$-formula $\theta := [p_0 \rightarrow A]\neg C_A \neg p_1$ we have $C^n, \Omega^L_1 \not\models \theta$ and $C^n, \Omega^R_1 \models \theta$ for each $n \in \mathbb{N}$. Applying Statement S, it then follows that no function $u : \mathfrak{L}^A_{\rightarrow A} \rightarrow \mathfrak{L}^A_{\not\rightarrow A}$ satisfies the property that the two equivalences

$$\begin{array}{lll} C^n, \Omega^L_1 \models \theta & \text{iff} & C^n, \Omega^L_1 \models \theta^u \quad \text{and} \\ C^n, \Omega^R_1 \models \theta & \text{iff} & C^n, \Omega^R_1 \models \theta^u \end{array}$$

both hold for each $n \in \mathbb{N}$. Since $\mathcal{I}$ is the set of all pointed models for A, we then have that $\mathfrak{L}^A_{\rightarrow A} \not\rightarrow_{\mathcal{I}} \mathfrak{L}^A_{\not\rightarrow A}$, which completes our proof. So what remains is for us to prove Statement S. We proceed by an induction on the construction of $\mathfrak{L}^A_{\not\rightarrow A}$-formulas. The Boolean cases of this induction are straightforward, so we will only handle the non-Boolean cases.

- Case: $K_j\varphi$ for some $j \in A$.

  Suppose that $C^n, (\Omega^L_k, i) \not\models K_j\varphi$ and that $d(K_j\varphi) + i + (k-1)\cdot|A| < (n+1)\cdot|A|$.

  In case $i < |A| - 1$, we then have that $C^n, (\Omega^L_k, i+1) \not\models \varphi$. Since $d(K_j\varphi) = 1 + d(\varphi)$, it follows that $d(\varphi) + (i+1) + (k-1)\cdot|A| < (n+1)\cdot|A|$ and so $C^n, (\Omega^R_k, i+1) \not\models \varphi$ by the induction hypothesis. But then $C^n, (\Omega^R_k, i) \not\models K_j\varphi$.

  In case $i = |A| - 1$, we have from our assumptions that $C^n, (\Omega^L_{k+1}, 0) \not\models \varphi$ and $d(\varphi) + k\cdot|A| < (n+1)\cdot|A|$. It follows from the induction hypothesis that $C^n, (\Omega^R_{k+1}, 0) \not\models \varphi$ and thus that $C^n, (\Omega^R_k, i) \not\models K_j\varphi$.

  The argument that $C^n, (\Omega^R_k, i) \not\models K_j\varphi$ implies $C^n, (\Omega^L_k, i) \not\models K_j\varphi$ is shown similarly.

- Case: $C_A\varphi$.

  $C^n, (\Omega^L_k, i) \not\models C_A\varphi$ is equivalent to $C^n, w \not\models \varphi$ for some $w \in C^n$. But the latter is equivalent to $C^n, (\Omega^R_k, i) \not\models C_A\varphi$.

- Case: $C_G\varphi$ for some nonempty $G \subsetneq A$.

  It follows from our assumption $G \subsetneq A$ that $C^n, (\Omega^L_k, i) \not\models C_G\varphi$ is equivalent to $C^n, w \not\models \varphi$ for some $w \in C^n$ satisfying the property the number of edges between (Ω^L_k, i) and w is at most $|G|$. w may have one of two forms and we consider a separate case for each form.

Suppose w is of the form (Ω^L_k, i') with $i' \in \mathbb{N}$ satisfying $i \leq i' \leq |A| - 1$ and further that $d(C_G\varphi) + i + (k-1) \cdot |A| < (n+1) \cdot |A|$. Since $d(C_G\varphi) = |A| + d(\varphi)$, it follows that $d(\varphi) + i' + (k-1) \cdot |A| < (n+1) \cdot |A|$ because $i' < i + |A|$. Applying the induction hypothesis, we have $C^n, (\Omega^R_k, i') \not\models \varphi$, from which it follows that $C^n, (\Omega^R_k, i) \not\models C_G\varphi$.

Suppose w is of the form (Ω^L_{k+1}, i') with $i' \in \mathbb{N}$ satisfying $0 \leq i' \leq |G| - \big(|A| - i\big)$ and further that $d(C_G\varphi) + i + (k-1) \cdot |A| < (n+1) \cdot |A|$. Since $d(C_G\varphi) = |A| + d(\varphi)$, it follows that $d(\varphi) + i' + k \cdot |A| < (n+1) \cdot |A|$ because we have $i' + |A| \leq |G| + i < |A| + i$ by our assumption $G \subsetneq A$. Applying the induction hypothesis, we have $C^n, (\Omega^R_{k+1}, i') \not\models \varphi$, from which it follows that $C^n, (\Omega^R_k, i) \not\models C_G\varphi$.

The argument that $C^n, (\Omega^R_k, i) \not\models C_G\varphi$ implies $C^n, (\Omega^L_k, i) \not\models C_G\varphi$ is shown similarly.

- Case: $[\varphi \rightarrow G]\psi$ for some nonempty $G \subsetneq A$.

  Suppose that $d\big([\varphi \rightarrow G]\psi\big) + i + (k-1) \cdot |A| < (n+1) \cdot |A|$. Since $d\big([\varphi \rightarrow G]\psi\big) = |A| + \max\big\{d(\varphi), d(\psi)\big\}$, we have each of the following.

  - $d(\varphi) + i' + (k-1) \cdot |A| < (n+1) \cdot |A|$ for each $i' \in \mathbb{N}$ satisfying $i \leq i' \leq |A| - 1$
    Applying the induction hypothesis, we have that
    $$C^n, (\Omega^L_k, i') \models \varphi \quad \text{iff} \quad C^n, (\Omega^R_k, i') \models \varphi$$
    for each $i' \in \mathbb{N}$ satisfying $i \leq i' \leq |A| - 1$.
  - $d(\varphi) + i' + k \cdot |A| < (n+1) \cdot |A|$ for each $i' \in \mathbb{N}$ satisfying $0 \leq i' \leq |G| - \big(|A| - i\big)$
    Applying the induction hypothesis, we have that
    $$C^n, (\Omega^L_{k+1}, i') \models \varphi \quad \text{iff} \quad C^n, (\Omega^R_{k+1}, i') \models \varphi$$
    for each $i' \in \mathbb{N}$ satisfying $0 \leq i' \leq |G| - \big(|A| - i\big)$.

  Without loss of generality, we may assume that
  $$C^n, (\Omega^L_k, i) \models \varphi \quad \text{and} \quad C^n, (\Omega^R_k, i) \models \varphi \ ,$$
  for otherwise the desired result follows trivially. Now let s^L be the longest sequence of worlds in C^n such that the first member of s^L is (Ω^L_k, i) and s^L satisfies each of the following: $C^n, w \models \varphi$ for each world w in s^L and each pair (w_1, w_2) of consecutive worlds in s^L satisfies $w_1 R_j w_2$ for some $j \in G$. Since $G \subsetneq A$, the nonempty sequence s^L is necessarily finite. Now let s^R be the sequence of worlds in C^n obtained by replacing each occurrence of a superscript L in a world in s^L by a superscript R. It follows from what we showed in the two bulleted items above that s^R is the longest sequence of worlds in C^n such that the first member of s^R is (Ω^R_k, i) and s^R satisfies each of the following: $C^n, w \models \varphi$ for each w in s^R and each pair (w_1, w_2) of consecutive worlds in s^L satisfies $w_1 R_j w_2$ for some $j \in G$. Now if the unique outgoing edge of the last member in s^L is labeled by some $j \in G$, then the tree model generated by
  $$\big(C^n[\varphi \rightarrow G], ((\Omega^L_k, i), 0)\big)$$

is isomorphic to the sub-model of C^n consisting of those worlds in the sequence s^L and, by what we showed in the two bulleted items above, the tree model generated by

$$\big(C^n[\varphi\!\rightarrow\! G], ((\Omega^R_k, i), 0)\big)$$

is also isomorphic to the sub-model of C^n consisting of those worlds in the sequence s^L.[6] But it then follows that

$$\begin{array}{l} C^n[\varphi\!\rightarrow\! G], \big((\Omega^L_k, i), 0\big) \models \psi \text{ iff} \\ C^n[\varphi\!\rightarrow\! G], \big((\Omega^R_k, i), 0\big) \models \psi \ , \end{array}$$

as desired. So let us assume that the unique outgoing edge of the last member in s^L is labeled by some $j \in A\backslash G$. We then have that the tree model generated by

$$\big(C^n[\varphi\!\rightarrow\! G], ((\Omega^L_k, i), 0)\big)$$

is isomorphic to the tree model generated by $\big(C^n, (\Omega^L_k, i)\big)$. Thus

$$C^n[\varphi\!\rightarrow\! G], \big((\Omega^L_k, i), 0\big) \models \psi \quad \text{iff} \quad C^n, (\Omega^L_k, i) \models \psi \ .$$

By similar reasoning, we also have

$$C^n[\varphi\!\rightarrow\! G], \big((\Omega^R_k, i), 0\big) \models \psi \quad \text{iff} \quad C^n, (\Omega^R_k, i) \models \psi \ .$$

Since $d\big([\varphi\!\rightarrow\! G]\psi\big) + i + (k-1)\cdot|A| < (n+1)\cdot|A|$ and $d\big([\varphi\!\rightarrow\! G]\psi\big) = |A| + \max\big\{d(\varphi), d(\psi)\big\}$, we have that $d(\psi) + i + (k-1)\cdot|A| < (n+1)\cdot|A|$. Applying the induction hypothesis, we have that

$$C^n, (\Omega^L_k, i) \models \psi \quad \text{iff} \quad C^n, (\Omega^R_k, i) \models \psi \ ,$$

which completes the proof of this theorem (Theorem 5.2). □

Theorem 5.2 tells us that the language $\mathfrak{L}^A_{\not\rightarrow A}$ of private communication with common knowledge cannot say everything that can be said in the language $\mathfrak{L}^A_{\rightarrow A}$ of public communication with common knowledge. Applying this to Theorem 4.5 yields the following result.

Theorem 5.3. Let A be a finite set satisfying $|A| \geq 2$ and let $\mathcal{I}$ be the set of all pointed models for A. Then the languages $\mathfrak{L}^A_{\rightarrow A}$ and $\mathfrak{L}^A_{\not\rightarrow A}$ are expressively incomparable for $\mathcal{I}$.

Proof. Since we have that $\mathfrak{L}^A_{\rightarrow i} \hookrightarrow_{\mathcal{I}} \mathfrak{L}^A_{\not\rightarrow A}$ for each $i \in A$, it follows from Theorem 4.5 that $\mathfrak{L}^A_{\not\rightarrow A} \not\hookrightarrow_{\mathcal{I}} \mathfrak{L}^A_{\rightarrow A}$. Applying Theorem 5.2, the result follows. □

Finally, we show that in contrast to Theorem 4.5, we have that single-recipient private communication does not add expressivity to the language of basic multi-modal logic with common knowledge for any class of *transitive* pointed models for A.

[6] The tree model generated by a pointed model is sometimes called the *unraveling* generated by a pointed model. See [10] for definitions and results relevant to a language extending $\mathfrak{L}^A$, and see [4] for definitions and results relevant to modal logic in general.

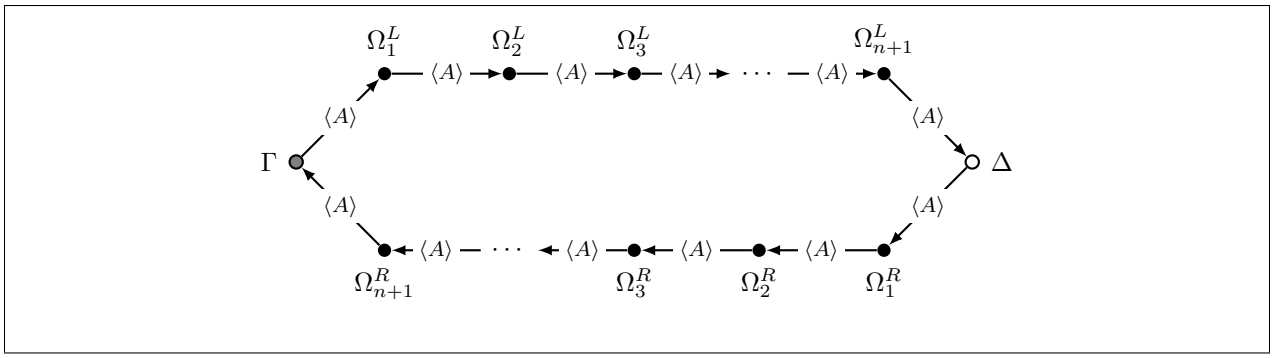

Figure 1. Picture representing the model C^n defined in the proof of Theorem 5.2. An edge from w to w' labeled "$\langle A\rangle$" represents a path from w to w' whose edges enumerate A in some fixed order.

Theorem 5.4. Let A be a finite nonempty set, $\mathfrak{G} := \big\{\{i\} : i \in A\big\}$, and $\mathcal{I}$ be any set of transitive pointed models for A. Then $\mathfrak{L}^A(\mathfrak{G}) \hookrightarrow_{\mathcal{I}} \mathfrak{L}^A(\emptyset)$.

Proof. For each formula $\varphi \in \mathfrak{L}^A$ and each nonempty $G \subseteq A$, we let $E_G\varphi$ abbreviate the conjunction $\bigwedge_{i\in G} K_i\varphi$. In Figure 2, we define a function $u : \mathfrak{L}^A(\mathfrak{G}) \to \mathfrak{L}^A(\emptyset)$. For each formula $\chi \in \mathfrak{L}^A$, we show that $\mathcal{I} \models \chi \equiv \chi^u$. Our argument proceeds by an induction on the depth of announcement modals in χ (that is, modals of the form $[\psi{\to}i]$ for $\psi \in \mathfrak{L}^A(\mathfrak{G})$ and $i \in A$) with a sub-induction on the number of symbols in χ. This induction follows the inductive definition in Figure 2 of the function u. Many cases of the induction are straightforward, so we will only handle the non-straightforward cases. (Note that the condition of transitivity is used only in the second half of the last case we handle.)

- $\mathcal{I} \models [\varphi{\to}i]K_j\psi \equiv \varphi^u \supset K_j\psi^u$ when $j \neq i$

  Suppose $M, \Gamma \not\models [\varphi{\to}i]K_j\psi$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi$ and $M[\varphi{\to}i], (\Gamma, 0) \not\models K_j\psi$. Thus $M[\varphi{\to}i], (\Delta, 1) \not\models \psi$ for some $\Delta \in M$ satisfying $\Gamma R_j\Delta$. It follows from the induction hypothesis that $M, \Gamma \models \varphi^u$ and $M[\varphi{\to}i], (\Delta, 1) \not\models \psi^u$. But the tree model generated by $\big(M[\varphi{\to}i], (\Delta, 1)\big)$ is isomorphic to the tree model generated by (M, Δ), so it then follows that $M, \Delta \not\models \psi^u$. Since $\Gamma R_j\Delta$, we then have that $M, \Gamma \not\models K_j\psi^u$. Taken together, we have shown that $M, \Gamma \not\models \varphi^u \supset K_j\psi^u$.

  Conversely, suppose $M, \Gamma \not\models \varphi^u \supset K_j\psi^u$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi^u$ and $M, \Delta \not\models \psi^u$ for some $\Delta \in M$ satisfying $\Gamma R_j\Delta$. It follows from the induction hypothesis that $M, \Gamma \models \varphi$ and $M, \Delta \not\models \psi$. But the tree model generated by (M, Δ) is isomorphic to the tree model generated by $\big(M[\varphi{\to}i], (\Delta, 1)\big)$, so it then follows that $M[\varphi{\to}i], (\Delta, 1) \not\models \psi$. Since $M, \Gamma \models \varphi$ and $\Gamma R_j\Delta$, we have that $(\Gamma, 0) \in M[\varphi{\to}i]$ and $(\Gamma, 0)R_j[\varphi{\to}i](\Delta, 1)$ and thus that $M[\varphi{\to}i], (\Gamma, 0) \not\models K_j\psi$. Taken together, we have shown that $M, \Gamma \not\models [\varphi{\to}i]K_j\psi$.

- $\mathcal{I} \models [\varphi{\to}i]K_i\psi \equiv \varphi^u \supset K_i\big([\varphi{\to}i]\psi\big)^u$

  Suppose $M, \Gamma \not\models [\varphi{\to}i]K_i\psi$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi$ and $M[\varphi{\to}i], (\Gamma, 0) \not\models K_i\psi$. Thus $M[\varphi{\to}i], (\Delta, 0) \not\models \psi$ for some $\Delta \in W$ satisfying $\Gamma R_i\Delta$. But this means that $M, \Delta \not\models [\varphi{\to}i]\psi$. Now it follows from the sub-induction hypothesis

that $M, \Delta \not\models \big([\varphi \to i]\psi\big)^u$, and the induction hypothesis implies that $M, \Gamma \models \varphi^u$. So we have $M, \Gamma \not\models \varphi^u \supset K_i\big([\varphi \to i]\psi\big)^u$ because $\Gamma R_i \Delta$.

Conversely, suppose that $M, \Gamma \not\models \varphi^u \supset K_i\big([\varphi \to i]\psi\big)^u$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi^u$ and $M, \Delta \not\models \big([\varphi \to i]\psi\big)^u$ for some $\Delta \in M$ satisfying $\Gamma R_i \Delta$. It follows by the sub-induction hypothesis that $M, \Delta \not\models [\varphi \to i]\psi$. But this means that $M, \Delta \models \varphi$ and $M[\varphi \to i], (\Delta, 0) \not\models \psi$. Applying the induction hypothesis, we have that $M, \Gamma \models \varphi$ and thus that $(\Gamma, 0) \in M[\varphi \to i]$. But then $(\Gamma, 0) R_i [\varphi \to i](\Delta, 0)$ and thus $M[\varphi \to i], (\Gamma, 0) \not\models K_i\psi$, which is what it means to say that $M, \Gamma \not\models [\varphi \to i]K_i\psi$.

- $\mathcal{I} \models [\varphi \to i]C_G\psi \equiv \big([\varphi \to i]\psi\big)^u \wedge (\varphi^u \supset E_G C_G \psi^u)$ when $i \notin G$

  Suppose $M, \Gamma \not\models [\varphi \to i]C_G\psi$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi$ and there is a sequence $\big\{(\Gamma_k, a_k)\big\}_{k=0}^n$ of worlds in $M[\varphi \to i]$ such that $(\Gamma_0, a_0) = (\Gamma, 0)$, each $k \in \mathbb{N}$ satisfying $0 < k \leq n$ has $a_k = 1$, each $k \in \mathbb{N}$ satisfying $k < n$ has a $j \in G$ with $(\Gamma_k, a_k) R_j [\varphi \to i](\Gamma_{k+1}, a_{k+1})$, and $M[\varphi \to i], (\Gamma_n, a_n) \not\models \psi$. In case $n = 0$, we then have that $M, \Gamma \not\models [\varphi \to i]\psi$ and thus that $M, \Gamma \not\models \big([\varphi \to i]\psi\big)^u$ by the sub-induction hypothesis. So suppose that $n > 0$. We then have that $M, \Gamma_n \not\models \psi$ because the tree model generated by $\big(M[\varphi \to i], (\Gamma_n, 1)\big)$ is isomorphic to the tree model generated by (M, Γ_n). Applying the induction hypothesis, it follows that $M, \Gamma_n \not\models \psi^u$. But $\{\Gamma_k\}_{k=1}^n$ is a nonempty sequence of worlds in M such that each $k \in \mathbb{N}$ satisfying $1 \leq k < n$ has a $j \in G$ with $\Gamma_k R_j \Gamma_{k+1}$, so $M, \Gamma_1 \not\models C_G\psi^u$. We also have that $\Gamma R_j \Gamma_1$ for some $j \in G$, and thus $M, \Gamma \not\models E_G C_G \psi^u$. Further, the induction hypothesis implies that we may conclude $M, \Gamma \models \varphi^u$ from the fact that $M, \Gamma \models \varphi$, and thus $M, \Gamma \not\models \varphi^u \supset E_G C_G \psi^u$. So no matter whether $n = 0$ or $n > 0$, we have shown that $M, \Gamma \not\models \big([\varphi \to i]\psi\big)^u \wedge (\varphi^u \supset E_G C_G \psi^u)$.

  Conversely, suppose that $M, \Gamma \not\models \big([\varphi \to i]\psi\big)^u \wedge (\varphi^u \supset E_G C_G \psi^u)$ for some $(M, \Gamma) \in \mathcal{I}$. In case $M, \Gamma \not\models \big([\varphi \to i]\psi\big)^u$, the sub-induction hypothesis implies that $M, \Gamma \not\models [\varphi \to i]\psi$ and thus $M[\varphi \to i], (\Gamma, 0) \not\models \psi$. The latter implies that $M[\varphi \to i], (\Gamma, 0) \not\models C_G\psi$ and thus that $M, \Gamma \not\models [\varphi \to i]C_G\psi$. In case $M, \Gamma \not\models \varphi^u \supset E_G C_G \psi^u$, then $M, \Gamma \models \varphi^u$ and for some $n \in \mathbb{N}$ with $n > 0$, there is a sequence $\{\Gamma_k\}_{k=0}^n$ of worlds in M such that $\Gamma_0 = \Gamma$, each $k \in \mathbb{N}$ with $k < n$ has a $j \in G$ with $\Gamma_k R_j \Gamma_{k+1}$, and $M, \Gamma_n \not\models \psi^u$. Applying the induction hypothesis, we have that $M, \Gamma_n \not\models \psi$ and thus that $M[\varphi \to i], (\Gamma_n, 1) \not\models \psi$ because the tree model generated by $\big(M[\varphi \to i], (\Gamma_n, 1)\big)$ is isomorphic to the tree model generated by (M, Γ_n). Again applying the induction hypothesis, it follows that $M, \Gamma \models \varphi$ from the fact that $M, \Gamma \models \varphi^u$, and thus $(\Gamma, 0) = (\Gamma_0, 0) \in M[\varphi \to i]$. Defining the sequence $\{a_k\}_{k=0}^n$ by setting $a_0 := 0$ and $a_k := 1$ for $k > 0$, we have that $\big\{(\Gamma_k, a_k)\big\}_{k=0}^n$ is a sequence of worlds in $M[\varphi \to i]$ such that $(\Gamma, 0) = (\Gamma_0, a_0)$, each $k \in \mathbb{N}$ satisfying $k < n$ has a $j \in G$ with $(\Gamma_k, a_k) R_j [\varphi \to i](\Gamma_{k+1}, a_{k+1})$, and $M[\varphi \to i], (\Gamma_n, a_n) \not\models \psi$. But then we have shown that $M, \Gamma \not\models [\varphi \to i]C_G\psi$.

- $\mathcal{I} \models [\varphi \to i]C_G\psi \equiv \varphi^u \supset C_i\big([\varphi \to i]\psi\big)^u \wedge C_i(\varphi^u \supset E_{G \setminus \{i\}} C_G \psi^u)$ when $i \in G$

  Suppose that $M, \Gamma \not\models [\varphi \to i]C_G\psi$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi$ and for some $n \in \mathbb{N}$ and some $m \in \mathbb{N}$ with $m \leq n$, there is a sequence $\big\{(\Gamma_k, a_k)\big\}_{k=0}^n$ of worlds in $M[\varphi \to i]$ such that $(\Gamma_0, a_0) = (\Gamma, 0)$, each $k \in \mathbb{N}$ satisfying $k < m$ has

$(\Gamma_k, a_k)R_i[\varphi{\rightarrow}i](\Gamma_{k+1}, a_{k+1})$, each $k \in \mathbb{N}$ satisfying $m < k < n$ has a $j \in G$ with $(\Gamma_k, a_k)R_j[\varphi{\rightarrow}i](\Gamma_{k+1}, a_{k+1})$, and $M[\varphi{\rightarrow}i], (\Gamma_n, a_n) \not\models \psi$. Note that we have $a_k = 0$ for each $k \in \mathbb{N}$ satisfying $k \leq m$ and $a_k = 1$ for each $k \in \mathbb{N}$ satisfying $m < k \leq n$. Now it follows from the induction hypothesis that $M, \Gamma \models \varphi^u$ by the fact that $M, \Gamma \models \varphi$. So what remains is for us to show that

$$M, \Gamma \not\models C_i\big([\varphi{\rightarrow}i]\psi\big)^u \wedge C_i(\varphi^u \supset E_{G\setminus\{i\}}C_G\psi^u) \ .$$

We consider two cases.

- Case: $n = 0$ or $0 < m = n$.

  We have $M, \Gamma_n \not\models [\varphi{\rightarrow}i]\psi$ and thus the sub-induction hypothesis yields $M, \Gamma_n \not\models \big([\varphi{\rightarrow}i]\psi\big)^u$. Since $m = n$, it follows that $\{\Gamma_k\}_{k=0}^n$ is a sequence of worlds in M such that $\Gamma_0 = \Gamma$ and each $k \in \mathbb{N}$ satisfying $k < n$ has $\Gamma_k R_i \Gamma_{k+1}$. Thus $M, \Gamma \not\models C_i\big([\varphi{\rightarrow}i]\psi\big)^u$.

- Case: $0 < m < n$.

  $(\Gamma_m, 0) \in M[\varphi{\rightarrow}i]$ implies that $M, \Gamma_m \models \varphi$ and thus that $M, \Gamma_m \models \varphi^u$ by the induction hypothesis. Since $m < n$, the sequence $\{\Gamma_k\}_{k=m}^n$ of worlds in M is nonempty and satisfies each of the following: $\Gamma_m R_{j_0} \Gamma_{m+1}$ for some $j_0 \in G\setminus\{i\}$, and each $k \in \mathbb{N}$ satisfying $m + 1 \leq k < n$ has a $j \in G$ with $\Gamma_k R_j \Gamma_{k+1}$. Now $m < n$ implies that $a_n = 1$, and thus $M, \Gamma_n \not\models \psi$ follows from the fact that the tree model generated by (M, Γ_n) is isomorphic to the tree model generated by $\big(M[\varphi{\rightarrow}i], (\Gamma_n, a_n)\big)$. Applying the induction hypothesis, we have that $M, \Gamma_n \not\models \psi^u$. But then we have shown that $M, \Gamma_m \not\models \varphi^u \supset E_{G\setminus\{i\}}C_G\psi^u$. Since $\{\Gamma_k\}_{k=0}^m$ is a sequence of worlds in M such that each $k \in \mathbb{N}$ satisfying $k < m$ has $\Gamma_k R_i \Gamma_{k+1}$, we then have that $M, \Gamma \not\models C_i(\varphi^u \supset E_{G\setminus\{i\}}C_G\psi^u)$.

Conversely, suppose that

$$M, \Gamma \not\models \varphi^u \supset C_i\big([\varphi{\rightarrow}i]\psi\big)^u \wedge C_i(\varphi^u \supset E_{G\setminus\{i\}}C_G\psi^u)$$

for some $(M, \Gamma) \in \mathcal{I}$. Thus $M, \Gamma \models \varphi^u$, from which it follows by the induction hypothesis that $M, \Gamma \models \varphi$. So what remains is for us to show that $M[\varphi{\rightarrow}i], (\Gamma, 0) \not\models C_G\psi$. We consider two cases.

- Case: $M, \Gamma \not\models C_i\big([\varphi{\rightarrow}i]\psi\big)^u$

  This means that there is a sequence $\{\Gamma_k\}_{k=0}^n$ of worlds in M such that $\Gamma_0 = \Gamma$, each $k \in \mathbb{N}$ satisfying $k < n$ has $\Gamma_k R_i \Gamma_{k+1}$, and $M, \Gamma_n \not\models \big([\varphi{\rightarrow}i]\psi\big)^u$. Applying the sub-induction hypothesis, we have that $M, \Gamma_n \not\models [\varphi{\rightarrow}i]\psi$. The latter implies that $M, \Gamma_n \models \varphi$, and hence $(\Gamma_n, 0) \in M[\varphi{\rightarrow}i]$. Now it follows by the transitivity of R_i that $\Gamma R_i \Gamma_n$, and thus $(\Gamma, 0)R_i[\varphi{\rightarrow}i](\Gamma_n, 0)$. But $M, \Gamma_n \not\models [\varphi{\rightarrow}i]\psi$ also implies that $M[\varphi{\rightarrow}i], (\Gamma_n, 0) \not\models \psi$, so we have $M[\varphi{\rightarrow}i], (\Gamma, 0) \not\models C_G\psi$ by the fact that $i \in G$.

$$
\begin{array}{lcl}
p_k^u & := & p_k \\
\bot^u & := & \bot \\
(\varphi \supset \psi)^u & := & \varphi^u \supset \psi^u \\
(K_i\varphi)^u & := & K_i\varphi^u \\
(C_G\varphi)^u & := & C_G\varphi^u \\
\big([\varphi{\to}\, i]p_k\big)^u & := & \varphi^u \supset p_k \\
\big([\varphi{\to}\, i]\bot\big)^u & := & \varphi^u \supset \bot \\
\big([\varphi{\to}\, i](\psi \supset \chi)\big)^u & := & \big([\varphi{\to}\, i]\psi\big)^u \supset \big([\varphi{\to}\, i]\chi\big)^u \\
\big([\varphi{\to}\, i]K_j\psi\big)^u & := & \begin{cases} \varphi^u \supset K_j\psi^u & \text{if } j \neq i \\ \varphi^u \supset K_i\big([\varphi{\to}\, i]\psi\big)^u & \text{if } j = i \end{cases} \\
\big([\varphi{\to}\, i]C_G\psi\big)^u & := & \begin{cases} \big([\varphi{\to}\, i]\psi\big)^u \wedge (\varphi^u \supset E_G C_G\psi^u) & \text{if } i \notin G \\ C_i\big([\varphi{\to}\, i]\psi\big)^u \wedge C_i(\varphi^u \supset E_{G\setminus\{i\}} C_G\psi^u) & \text{if } i \in G \end{cases} \\
\big([\varphi{\to}\, i][\psi{\to}\, j]\chi\big)^u & := & \big([\varphi{\to}\, i]([\psi{\to}\, j]\chi)^u\big)^u
\end{array}
$$

Figure 2. Inductive definition of a function $u : \mathfrak{L}^A(\mathfrak{G}) \to \mathfrak{L}^A(\emptyset)$ used in the proof of Theorem 5.4.

– Case: $M, \Gamma \not\models C_i(\varphi^u \supset E_{G\setminus\{i\}} C_G\psi^u)$
This means that there is a sequence $\{\Gamma_k\}_{k=0}^n$ of worlds in M such that $\Gamma_0 = \Gamma$, each $k \in \mathbb{N}$ satisfying $k < n$ has $\Gamma_k R_i \Gamma_{k+1}$, and $M, \Gamma_n \not\models \varphi^u \supset E_{G\setminus\{i\}} C_G\psi^u$. Thus $M, \Gamma_n \models \varphi^u$, and so the induction hypothesis implies that $M, \Gamma_n \models \varphi$. We therefore have that $(\Gamma_n, 0) \in M[\varphi{\to}\, i]$, from which it follows that $(\Gamma, 0) R_i [\varphi{\to}\, i](\Gamma_n, 0)$ by the transitivity of R_i. Applying the induction hypothesis again, we have that $M, \Gamma_n \not\models E_{G\setminus\{i\}} C_G\psi$, which means that there is a sequence $\{\Gamma_k\}_{k=n}^m$ for some $m \in \mathbb{N}$ with $m > n$ such that $\Gamma_n R_{j_0} \Gamma_{n+1}$ for some $j_0 \in G\setminus\{i\}$, each $k \in \mathbb{N}$ satisfying $n+1 \leq k < m$ has a $j \in G$ with $\Gamma_k R_j \Gamma_{k+1}$, and $M, \Gamma_m \not\models \psi$. But then

$$(\Gamma, 0), (\Gamma_n, 0), (\Gamma_{n+1}, 1), (\Gamma_{n+2}, 1), \ldots, (\Gamma_m, 1)$$

is a sequence of worlds in $M[\varphi{\to}\, i]$ such that each pair (w, w') of consecutive worlds in the sequence has a $j \in G$ such that $w R_j [\varphi{\to}\, i] w'$. Further, $M[\varphi{\to}\, i], (\Gamma_m, 1) \not\models \psi$ by the fact that the tree model generated by $\big(M[\varphi{\to}\, i], (\Gamma_m, 1)\big)$ is isomorphic to the tree model generated by (M, Γ_m). But then $M[\varphi{\to}\, i], (\Gamma, 0) \not\models C_G\psi$. □

6 Conclusion

We have surveyed public and private communication in Dynamic Epistemic Logic (DEL) with a focus on questions of relative expressivity. Our work adds the following to the list of known results.

1. Theorem 5.2: the language $\mathfrak{L}^A_{\not\to A}$ of all private communications with common knowledge cannot say everything that can be said in the language $\mathfrak{L}^A_{\to A}$ of public communication with common knowledge for the class of all pointed models for A.

In Theorem 5.3, we combined Theorem 5.2 with a known result—Theorem 4.5 [3]—to show that for $2 \leq |A| < \omega$, the languages $\mathfrak{L}^A_{\not\to A}$ and $\mathfrak{L}^A_{\to A}$ are expressively incomparable for the class of all pointed models for A. This provides us with a formal proof that public and private communication are fundamentally different.

2. Theorem 5.4: single-recipient private communication does not add expressivity to the language of basic multi-modal logic with common knowledge for any class of *transitive* pointed models.

   As a consequence, single-recipient private communication is implicit in KD45, a logic typically used for reasoning about belief [5]. This provides us a sense in which positive introspection—believing our own beliefs—induces a kind of self-dialog.

More generally, the work of this paper is a small step in a larger project whose eventual goal is to provide a complete characterization of the relative expressivity for the many DEL languages [1, 12]. Given the extremely limited collection of known expressivity results that have been discovered since the Plaza-Gerbrandy Theorem became well-known in 1999 [6, 9], this task may turn out to be quite difficult. But the task will nonetheless be of use in getting a better understanding of the gamut of communicative types available through the many DEL languages.

References

[1] Alexandru Baltag and Lawrence S. Moss. Logics for epistemic programs. *Synthese*, 139(2):165–224, 2004.

[2] Alexandru Baltag, Lawrence S. Moss, and Sławomir Solecki. The logic of common knowledge, public announcements, and private suspicions. In Itzhak Gilboa, editor, *Proceedings of the 7th Conference on Theoretical Aspects of Rationality and Knowledge (TARK VII)*, pages 43–56, Evanston, IL, USA, 1998.

[3] Alexandru Baltag, Lawrence S. Moss, and Sławomir Solecki. Logics for epistemic actions: completeness, decidability, expressivity. Manuscript, 2005.

[4] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*. Cambridge University Press, 2001.

[5] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge*. The MIT Press, 1995.

[6] Jelle Gerbrandy. *Bisimulations on Planet Kripke*. PhD thesis, University of Amsterdam, 1999.

[7] Jelle Gerbrandy and Willem Groeneveld. Reasoning about information change. *Journal of Logic, Language, and Information*, 6:147–169, 1997.

[8] Jaakko Hintikka. *Knowledge and Belief*. Cornell University Press, 1962.

[9] Jan A. Plaza. Logics of public communications. In Zbigniew W. Ras, editor, *Proceedings of the Fourth International Symposium on Methodologies for Intelligent Systems (ISMIS 1989)*. North-Holland, 1989.

[10] Bryan Renne. The relative expressivity of public and private communication in BMS logic. Technical Report TR-2007012, CUNY Ph.D. Program in Computer Science, 2007.

[11] Johan van Benthem, Jan van Eijck, and Barteld Kooi. Logics of communication and change. *Information and Computation*, 204(11):1620–1662, 2006.

[12] Hans van Ditmarsch, Wiebe van der Hoek, and Barteld Kooi. *Dynamic Epistemic Logic*. Springer, 2007.