

Public and Private Communication are Different: Results on Relative Expressivity*

Bryan Renne[†]

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 Kripke models, which provides a formal proof that public and private communication are fundamentally different in the presence of common knowledge. It is also shown that single-recipient private communication does not add expressive power to the language of modal logic with common knowledge for any class of *transitive* pointed Kripke models. The latter result provides a sense in which positive introspection—believing our own beliefs—induces a kind of self-dialog.

1 The Paradigmatic Approach in Formal Epistemology

Since Hintikka [8], the paradigmatic approach in formal epistemology has been to use modal logic to reason about the doxastic attitudes (that is, things like propositional knowledge and propositional belief) that are held by a number of individuals commonly called *agents*. The essence of this approach is to argue that a doxastic attitude is logically closed under certain principles that can be expressed in the language of modal logic. As an example, most authors agree that knowledge is veridical (meaning that there is no “false knowledge”: a statement φ must be true in the event agent i knows φ), and so such authors invite us to accept the modal scheme $K_i\varphi \supset \varphi$ (“if agent i knows φ , then φ is true”) as a principle of logical closure that is an essential component of a correct descriptive characterization of knowledge [5]. Such argumentation generally advocates that a particular modal logic ought to be accepted as the logic of the doxastic attitude in question on the basis that it is this logic that consists of exactly those principles of logical closure that were argued to be essential to that doxastic attitude. Examples: **S5** is often taken as the *logic of knowledge*, and **KD45** is often taken as the *logic of belief* [5].

*©2008 Springer Science+Business Media B.V. The original publication is available at www.springerlink.com. Citation: Bryan Renne. *Public and Private Communication are Different: Results on Relative Expressivity*. *Synthese*, 165(2):225–245, 2008.

[†]CUNY Graduate Center, New York, NY, USA. <http://bryan.renne.org/>

There are a number of straightforward objections to this particular analysis of knowledge, perhaps the most persistent and powerful of which is the observation that this analysis attributes *logical omniscience* to each of the agents, by which we mean that each agent knows all logical consequences of his knowledge (and so knows, in particular, all logical truths) [5, 11]. Hintikka himself made this observation.

Given a number of premises, logic does not tell us what conclusions we ought to draw from them; it merely tells us what conclusions we may draw from them—if we wish and if we are clever enough. [...] The applicability of our results may thus be said to presuppose a certain amount of rationality in the people whose attitudes are being discussed. In this respect, our logical theory is comparable with certain other theories (e.g., the theory of games) which may also be said to depend on an assumption of rationality. [...]

— Jaakko Hintikka, *Knowledge and Belief*, pp. 37–38 [8]

It is from this point of view that we begin the work of the present paper. In particular, we wish to understand how the expressive power of logical languages that describe the knowledge and beliefs of such ideally rational (that is, logically omniscient) agents is affected when we extend the language by including public and private communications to the agents. The basic idea is to try and see if there are certain propositions that can be expressed in a language with one kind of communication that cannot be expressed in a language with another kind of communication. Distinguishing these two languages in this way allows us to distinguish between these two types of communication, which helps us understand whether two intuitively distinct communicative types are in fact different for ideally rational agents and, if so, why.

Understanding the differences in communicative types for ideally rational agents provides important clues as to the fundamental communicative types that would constitute an account of the dynamics of our imperfect everyday knowledge, and it is in this spirit that we pursue the work of the present paper, understanding the word *agent* to refer to Hintikka’s ideally rational individual.

Let us now begin our work by describing how it is that we add communication to the language of modal logic.

2 Adding Communication to Modal Logic

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, immutable 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 the Hintikka-Kripke notion of belief [8, 9].

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

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

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_k, Γ_k) , then it ought to be common knowledge in the next moment (M_{k+1}, Γ_{k+1}) that p is true.¹
2. If no agent knows whether p is true in moment (M_k, Γ_k) , then the private communication to just those agents in group G that p is true ought to bring about a next moment (M_{k+1}, Γ_{k+1}) 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, 12, 14]. DEL uses modal logic as the basic language for describing knowledge, belief, and fact.² 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

$$[\varphi \rightarrow G]\psi$$

¹For present purposes, a basic statement p is an assertion about the world that is either eternally true or eternally false. So the truth of a basic statement does not change when a communication occurs. What does change is the agents' knowledge of the truth of basic statements, the agents' higher-order knowledge (that is, knowledge about knowledge), or some combination thereof. So in the case of the public communication of the basic statement p , the truth of p does not change, though the agents' mutual knowledge as to the truth of p does.

²For our purposes, the language of model logic is that obtained from the language of propositional logic by adding a knowledge modal K_i for each agent i .

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

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

which we often abbreviate by $[\varphi]\psi$, 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. $[p]C_{AP}$

In words: after the communication of p (to all agents), we have that p is common knowledge (to all agents).

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

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 communication, 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, 12, 13]. For example, it has been shown that for the language of modal logic without common knowledge, adding statements $[\varphi]\psi$ of public communication does not add expressive power [3, 6, 12]. Thus the language of modal logic without common knowledge can already express propositions about public communication, even before we explicitly add public communication formulas $[\varphi]\psi$ to the language.³ But it has also been shown that this is not true of the language of modal logic *with* common knowledge statements [3, 14].

Formally, such work is a study of the relative expressivity of the various languages obtained from the language modal logic (with or without common knowledge) by adding additional syntax to represent various classes of communication. Most of the known DEL expressivity work has focused on public communication [3, 6, 12, 13, 14], though some work has been done on private communication [3], including a result that the language of private communication with common knowledge can express a proposition that cannot be expressed using the language of public communication with common knowledge. In the present paper, we show that this result holds the other way around: the language of public communication with common knowledge can express a proposition that cannot be expressed by the language

³A *proposition* is a set of pointed Kripke models. The *proposition expressed by a formula* consists of the set of all pointed Kripke models at which the formula is true. (Definition 3.6 says what it means to say that a formula in our to-be-defined language is true at a pointed Kripke model.) To say that a *formula expresses a proposition* S means that the proposition expressed by the formula is equal to S . To say that a *language can express a proposition* means that there is a formula in the language that expresses the proposition. To say that a *language cannot express a proposition* means that it is not the case that the language can express the proposition. To say that a *formula cannot be expressed in a language* means that the proposition expressed by the formula cannot be expressed in the language.

of private communication with common knowledge. When we combine these two results—the first from [3] and the second from our work in the present paper—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 in the presence of common knowledge.

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 modal logic with common knowledge can already express propositions about single-recipient private communication, even before we explicitly add single-recipient private communication formulas $[\varphi \rightarrow \{i\}]\psi$ to the language. A consequence of this curious result is that single-recipient private communication is implicit in KD45, the typical *logic of 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.

3 Public and Private Communication

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

3.1 Syntax

Our languages all concern the knowledge held by a finite, nonzero number of agents.

Definition 3.1. An *agent set* is a finite nonempty set.

Definition 3.2. Let A be an agent set.

- The *language of modal logic (for A)*, written ML^A , consists of the formulas φ built by the following grammar.

$$\varphi ::= p_k \mid \perp \mid \varphi_1 \supset \varphi_2 \mid K_i$$

$$k \in \mathbb{N}, i \in A$$

$\{p_k : k \in \mathbb{N}\}$ is the set of *propositional letters*. \perp is the propositional constant for falsity. A formula written using other logical connectives is understood as an abbreviation for an appropriate formula in this language. In particular, \top is an abbreviation for $\perp \supset \perp$.

- For each $G \subseteq A$, we make the following abbreviation:

$$E_G \varphi := \begin{cases} \bigwedge_{i \in G} K_i \varphi & \text{if } G \neq \emptyset, \\ \top & \text{if } G = \emptyset. \end{cases}$$

- The *language of public and private communication (for A)*, written COM^A , is the extension of ML^A obtained by adding the following rule of formula formation: if φ and ψ are formulas and $G \subseteq A$, then $[\varphi \rightarrow G]\psi$ is also a formula.

Abbreviations: for each $i \in A$, we let $[\varphi_1 \rightarrow i]\varphi_2$ abbreviate $[\varphi_1 \rightarrow \{i\}]\varphi_2$; we also let $[\varphi_1]\varphi_2$ abbreviate $[\varphi_1 \rightarrow A]\varphi_2$.

The modal formulas $K_i\varphi$, $E_G\varphi$, and $[\varphi \rightarrow G]\psi$ have the following intuitive readings.

- $K_i\varphi$ is read, “(agent) i knows φ .”
- $E_G\varphi$ is read, “everyone in G knows φ .”
- $[\varphi \rightarrow G]\psi$ is read, “ 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 COM^A , with the particular fragment determined by the various groups of agents that are allowed to receive a communication.

Definition 3.3. Let A be an agent set and let $\mathfrak{G} \subseteq 2^A$ be a possibly empty collection of subsets of A . Then the language $\text{COM}^A(\mathfrak{G})$ is the fragment of COM^A obtained by restricting all subformulas of the form $[\varphi \rightarrow G]\psi$ so that $G \in \mathfrak{G}$. Notation: for $G \subseteq A$ and $i \in A$, we let $\text{COM}^A(G)$ denote $\text{COM}^A(\{G\})$ and we let $\text{COM}^A(i)$ denote $\text{COM}^A(\{i\})$.

We now define a few fragments of COM^A that are of particular interest in the present paper.

Definition 3.4. Let A be an agent set.

- The *language of public communication (for A)*, written PUB^A , is $\text{COM}^A(A)$.
- The *language of private communication (for A)*, written PRI^A , is $\text{COM}^A(2^A \setminus \{A\})$.
- The *language of single-recipient private communication (for A)*, written PRI1^A , is

$$\text{COM}^A\left(\{\{i\} : i \in A\}\right) .$$

Finally, we define the common knowledge extensions of the modal languages we defined above.

Definition 3.5. Let A be an agent set. For each

$$\mathfrak{L} \in \{\text{ML}^A, \text{COM}^A, \text{PUB}^A, \text{PRI}^A, \text{PRI1}^A\} ,$$

the extension of \mathfrak{L} *with common knowledge*, written \mathfrak{L}_C , is obtained from \mathfrak{L} by adding the following rule of formula formation: if φ is a formula and $G \subseteq A$, then $C_G\varphi$ is also a formula.

$C_G\varphi$ is read, “ φ is common knowledge to those in G .”

3.2 Semantics

COM_C^A -formulas are interpreted using an extension of Kripke's semantics for modal logic [9]. This extension is due to Baltag, Moss, and Solecki [1, 2].

Definition 3.6. Let A be an agent. A *Kripke 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 .⁴
- $V : \{p_k : k \in \mathbb{N}\} \rightarrow 2^W$ 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 Kripke model, then we write $\Gamma \in M$ to mean that $\Gamma \in W$. A *pointed Kripke model (for A)* is a pair (M, Γ) consisting of a Kripke model M and a world $\Gamma \in M$; the world $\Gamma \in M$ is called the *point* of (M, Γ) . To say that pointed Kripke 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 $i \in A$.⁵ For a pointed Kripke model (M, Γ) and a formula $\varphi \in \text{COM}_C^A$, 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 $\varphi \in \text{COM}_C^A$ at a pointed Kripke model (M, Γ) is given by the following induction on the construction of φ .

- $M, \Gamma \models p_k$ means that $\Gamma \in V(p_k)$.
- $M, \Gamma \not\models \perp$.
- $M, \Gamma \models \varphi_1 \supset \varphi_2$ 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 $M, \Gamma_n \models \varphi$.
- $M, \Gamma \models [\varphi_1 \rightarrow G] \varphi_2$ means that either we have $M, \Gamma \not\models \varphi_1$ or else we have both $M, \Gamma \models \varphi_1$ and $M[\varphi_1 \rightarrow G], (\Gamma, 0) \models \varphi_2$, where the Kripke model $M[\varphi_1 \rightarrow G]$ is the tuple

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

whose components are given as follows.

⁴ 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 $(\Gamma, \Delta) \in R$.

⁵Let 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 $\Gamma, \Delta, \Omega \in W$.

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

$$\left\{ ((\Gamma, a), (\Delta, b)) \in (W[\varphi_1 \rightarrow G])^2 : (\Gamma R_i \Delta) \wedge (a = b) \right\}$$

- For each $j \in A \setminus G$: $R_j[\varphi_1 \rightarrow G]$ is the set

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

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

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

The idea behind the construction of the Kripke 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 Kripke 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 $A \setminus G$ 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 to those in G that φ was communicated—while the agents in $A \setminus G$ 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 Kripke model (M, Γ) to a next moment in time given by the pointed Kripke model $(M[\varphi \rightarrow G], (\Gamma, 0))$. It is in this way that communication moves time from one moment to the next in this framework.

4 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 4.1. Let A be an agent set, \mathfrak{L}_1 and \mathfrak{L}_2 be sub-languages of COM_C^A , and \mathcal{I} be a set of pointed Kripke models for A . A *translation function (from \mathfrak{L}_1 to \mathfrak{L}_2 over \mathcal{I})* is a function $u : \mathfrak{L}_1 \rightarrow \mathfrak{L}_2$ 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 $(M, \Gamma) \in \mathcal{I}$, we have $M, \Gamma \models \psi$ if and only if $M, \Gamma \models \psi^u$. We write $\mathfrak{L}_1 \hookrightarrow_{\mathcal{I}} \mathfrak{L}_2$ to mean that there exists a translation function $u : \mathfrak{L}_1 \rightarrow \mathfrak{L}_2$ 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 4.2 (Relative Expressivity). We adopt the notation of Definition 4.1.

- 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 Kripke 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.

5 Some Known Results on Relative Expressivity

The Plaza-Gerbrandy Theorem marks the beginning of Dynamic Epistemic Logic as an independent area of study.

Theorem 5.1 (Plaza-Gerbrandy [6, 12]). Let A be an agent set. Then $\text{PUB}^A \hookrightarrow_{\mathcal{I}} \text{ML}^A$ for each set \mathcal{I} of pointed Kripke models for A .

Since $\text{ML}^A \hookrightarrow_{\mathcal{I}} \text{PUB}^A$ for each set \mathcal{I} of pointed Kripke models for A , the Plaza-Gerbrandy Theorem implies that PUB^A and ML^A are equally expressive for any class of pointed Kripke models for A . Thus public communication does not add expressive power to the language of modal logic without common knowledge. But this does not tell us that the language PUB^A is useless; in fact, PUB^A is *exponentially more succinct* than ML^A , as the following theorem explains.

Theorem 5.2 ([10]). Let A be an agent set satisfying $|A| \geq 2$, let \mathcal{I} be the set of all pointed Kripke models for A , and let $u : \text{PUB}^A \rightarrow \text{ML}^A$ be a translation function over \mathcal{I} . Abbreviations: let $\langle \psi \rangle$ abbreviate $\neg[\psi]\neg$ and let \hat{K}_i abbreviate $\neg K_i \neg$. Choosing $i \in A$ and $j \in A$ such that $i \neq j$, define the sequence $\{\varphi_k\}_{k \in \mathbb{N}}$ of PUB^A -formulas by the following induction.

$$\varphi_k := \begin{cases} \top & \text{if } k = 0, \\ \langle \langle \varphi_{k-1} \rangle \hat{K}_i \top \rangle \hat{K}_j \top & \text{if } k > 0. \end{cases}$$

Then it follows that for each $k \in \mathbb{N}$, the number of symbols in φ_k^u is at least 2^k .

It remains open whether Theorem 5.2 holds if we choose for \mathcal{I} the set of all reflexive, transitive, and euclidean pointed Kripke models (for A), which is the set of pointed Kripke models corresponding to the logic **S5**, the typical *logic of knowledge* [5].

Theorem 5.3 ([1, 3]). Let A be an agent set. Then $\text{COM}^A \hookrightarrow_{\mathcal{I}} \text{ML}^A$ for each set \mathcal{I} of pointed Kripke models for A .⁶

Since $\text{ML}^A \hookrightarrow_{\mathcal{I}} \text{COM}^A$ for each set \mathcal{I} of pointed Kripke models for A , Theorem 5.3 implies that COM^A and ML^A are equally expressive for each set \mathcal{I} of pointed Kripke models for A . Thus public and private communication do not add expressive power to the language of modal logic without common knowledge.

We now survey results concerning the relative expressivity of fragments of COM_C^A .

Theorem 5.4 ([3, 14]). Let A be an agent set satisfying $|A| = 1$ and let \mathcal{I} be the set of all pointed Kripke models for A . Then $\text{PUB}_C^A \not\hookrightarrow_{\mathcal{I}} \text{ML}_C^A$.

Proof Hint. The PUB_C^A -formula $[p_0] \neg C_A \neg p_1$ cannot be expressed in ML_C^A [3]. \square

Since $\text{ML}_C^A \hookrightarrow_{\mathcal{I}} \text{PUB}_C^A$ for each set \mathcal{I} of pointed Kripke models for A , Theorem 5.4 implies that the language PUB_C^A of public communication with common knowledge is more expressive than the language ML_C^A of modal logic with common knowledge for the class of all pointed Kripke 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 5.5 ([3, 14]). Let A be an agent set satisfying $|A| \geq 2$ and let \mathcal{I} be the set of all reflexive, transitive, and euclidean pointed Kripke models for A . Then $\text{PUB}_C^A \not\hookrightarrow_{\mathcal{I}} \text{ML}_C^A$.

Proof Hint. The PUB_C^A -formula $[p_0] \neg C_G \neg p_1$ with $|G| = 2$ cannot be expressed in ML_C^A [3]. \square

Theorem 5.5 tells us that if there are at least two agents in the agent set A , then the language PUB_C^A of public communication with common knowledge is more expressive than the language ML_C^A of modal logic with common knowledge for the class of all pointed Kripke models for A that are reflexive, transitive, and euclidean.⁷ The latter trio of properties characterizes the class of frames valid for the logic **S5**, a logic generally thought of as the *logic of knowledge* [4, 5]. Thus public communication strictly increases the expressivity of the logic of knowledge when common knowledge is present. Contrasting this theorem with Theorem 5.3, we again see that common knowledge is necessary for the increase in expressive power.

Theorem 5.6 ([3]). Let A be an agent set satisfying $|A| \geq 2$ and let \mathcal{I} be the set of all pointed Kripke models for A . Then $\text{PRI}_C^A \not\hookrightarrow_{\mathcal{I}} \text{PUB}_C^A$.⁸

Proof Hint. The PRI_C^A -formula $[p_0 \rightarrow i] \neg C_i K_j p_0$ with $i \neq j$ cannot be expressed in PUB_C^A . \square

⁶Theorem 5.3 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 ML^A for any set of pointed Kripke models.

⁷Theorem 5.5 fails in the case $|A| = 1$, since $|A| = 1$ implies that $\text{PUB}_C^A \hookrightarrow_{\mathcal{I}} \text{ML}_C^A$ for any set \mathcal{I} of transitive pointed Kripke models for A [3].

⁸Theorem 5.6 fails in the case $|A| = 1$ for a trivial reason: $|A| = 1$ implies that $\text{PRI}_C^A = \text{PUB}_C^A$ (see Definition 3.4).

Theorem 5.6 tells us that if there are at least two agents in the agent set A , then the language PUB_C^A of public communication with common knowledge cannot say everything that can be said by the language PRI_C^A of single-recipient private communication with common knowledge for the set of all pointed Kripke models for A . Comparing this result with Theorem 5.3, we again see the necessity of common knowledge for an increase in expressive power.

6 Our Results on Relative Expressivity

Our first result, Theorem 6.2, is the strongest possible form for the reverse direction of Theorem 5.6. But before we state our theorem, we make the following auxiliary definition for use in our proof.

Definition 6.1. 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 Kripke 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 Kripke model $(W', \{R'_i\}_{i \in A}, V')$ for A whose components are given as follows.

- $W' := W \cup \{(\Gamma, \Delta, i) : (\Gamma, \Delta) \in R, i \in \mathbb{N} \text{ with } 1 \leq i \leq |G| - 1\}$
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 $1 \leq i \leq |G|$:

$$R'_{g_i} := R_{g_i} \cup \left\{ ((\Gamma, \Delta, i - 1), (\Gamma, \Delta, i)) : (\Gamma, \Delta) \in R \right\}$$

- For each $i \in A \setminus G$: set $R'_i := R_i$.
- $V'(p_k) := V(p_k) \cup \{(\Gamma, \Delta, i) \in W' : i \leq |G| - 1 \text{ and } \Gamma \in V(p_k)\}$

The expansion of M at R by $\{g_i\}_{i=1}^{|G|}$ 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,

$$\begin{aligned} & \Gamma \xrightarrow{R} \Delta \\ & \text{expands to} \\ & \Gamma \xrightarrow{g_1} (\Gamma, \Delta, 1) \xrightarrow{g_2} (\Gamma, \Delta, 2) \xrightarrow{g_3} \dots \xrightarrow{g_{|G|-1}} (\Gamma, \Delta, |G| - 1) \xrightarrow{g_{|G|}} \Delta \end{aligned}$$

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 5.6.

Theorem 6.2. Let A be an agent set. Then $\text{PUB}_C^A \not\leftrightarrow_{\mathcal{I}} \text{PRI}_C^A$ for the set \mathcal{I} of all pointed Kripke models for A .

Proof. If $|A| = 1$, then we have that PRI_C^A and ML_C^A are equally expressive for any set of pointed Kripke models for A (since $\models [\varphi \rightarrow \emptyset]\psi \equiv \varphi \supset \psi$), and so the result follows by Theorem 5.4. So we may assume that $|A| \geq 2$. For each non-negative integer $n \in \mathbb{N}$, we define the Kripke model $B^n := (W^n, S^n, V^n)$ for A and the relation $R^n \subseteq W^n \times W^n$ as follows.

- $W^n := \{\Omega_k^L : k \in \mathbb{N} \text{ and } 1 \leq k \leq n+1\} \cup \{\Omega_k^R : k \in \mathbb{N} \text{ and } 1 \leq k \leq n+1\} \cup \{\Gamma, \Delta\}$
- Abbreviations: we set $\Omega_0^L := \Omega_{n+2}^R := \Gamma$ and $\Omega_{n+2}^L := \Omega_0^R := \Delta$.
- For each $i \in A$, set $R_i^n := \emptyset$.
- $V^n(p_k) := \begin{cases} W^n \setminus \{\Delta\} & \text{if } k = 0 \\ \{\Gamma\} & \text{if } k = 1 \\ \emptyset & \text{if } k \geq 2 \end{cases}$
- $R^n := \{(\Omega_{k-1}^L, \Omega_k^L) : 1 \leq k \leq n+2\} \cup \{(\Omega_{k-1}^R, \Omega_k^R) : 1 \leq k \leq n+2\}$

Now fix an enumeration $\{a_i\}_{i=1}^{|A|}$ of A . For each $n \in \mathbb{N}$, we define the Kripke model C^n as the expansion of B^n at R^n by $\{a_i\}_{i=1}^{|A|}$ (Definition 6.1). See Figure 1 for a picture of C^n .

We now define a depth function $d : \text{PRI}_C^A \rightarrow \mathbb{N}$ by the following induction on PRI_C^A -formula construction.

- $d(p_k) := 0$ for $k \in \mathbb{N}$
- $d(\perp) := 0$
- $d(\varphi_1 \supset \varphi_2) := \max\{d(\varphi_1), d(\varphi_2)\}$
- $d(K_i \varphi) := 1 + d(\varphi)$ for $i \in A$
- $d(C_G \varphi) := |A| + d(\varphi)$
- $d([\varphi_1 \rightarrow G]\varphi_2) := |A| + \max\{d(\varphi_1), d(\varphi_2)\}$

We will prove the following statement that we call S : for each $\varphi \in \text{PRI}_C^A$, 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

$$C^n, (\Omega_k^L, i) \models \varphi \quad \text{iff} \quad C^n, (\Omega_k^R, i) \models \varphi .$$

Observe that for the PUB_C^A -formula $\theta := [p_0] \neg C_A \neg p_1$ we have $C^n, \Omega_1^L \not\models \theta$ and $C^n, \Omega_1^R \models \theta$ for each $n \in \mathbb{N}$. Applying Statement S , it then follows that no function $u : \text{PUB}_C^A \rightarrow \text{PRI}_C^A$ satisfies the property that the two equivalences

$$\begin{aligned} C^n, \Omega_1^L \models \theta & \quad \text{iff} \quad C^n, \Omega_1^L \models \theta^u & \quad \text{and} \\ C^n, \Omega_1^R \models \theta & \quad \text{iff} \quad C^n, \Omega_1^R \models \theta^u \end{aligned}$$

both hold for each $n \in \mathbb{N}$. Since \mathcal{I} is the set of all pointed Kripke models for A , we then have that $\text{PUB}_C^A \not\rightarrow_{\mathcal{I}} \text{PRI}_C^A$, which completes our proof. So what remains is for us to prove Statement S . We proceed by an induction on the construction of PRI_C^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 $C^n, (\Omega_k^L, i) \not\models K_j\varphi$ and that $d(K_j\varphi) + i + (k-1) \cdot |A| < (n+1) \cdot |A|$.

In case $i < |A| - 1$, we then have that $C^n, (\Omega_k^L, i+1) \not\models \varphi$. 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 $C^n, (\Omega_k^R, i+1) \not\models \varphi$ by the induction hypothesis. But then $C^n, (\Omega_k^R, i) \not\models K_j\varphi$.

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

The argument that $C^n, (\Omega_k^R, i) \not\models K_j\varphi$ implies $C^n, (\Omega_k^L, i) \not\models K_j\varphi$ is shown similarly.

- Case: $C_A\varphi$.

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

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

It follows from our assumption $G \subsetneq A$ that $C^n, (\Omega_k^L, i) \not\models C_G\varphi$ is equivalent to $C^n, w \not\models \varphi$ for some $w \in C^n$ satisfying the property the number of edges between (Ω_k^L, 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_k^L, 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 $C^n, (\Omega_k^R, i') \not\models \varphi$, from which it follows that $C^n, (\Omega_k^R, i) \not\models C_G\varphi$.

Suppose w is of the form (Ω_{k+1}^L, i') with $i' \in \mathbb{N}$ satisfying $0 \leq i' \leq |G| - (|A| - i)$ 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 $C^n, (\Omega_{k+1}^R, i') \not\models \varphi$, from which it follows that $C^n, (\Omega_k^R, i) \not\models C_G\varphi$.

The argument that $C^n, (\Omega_k^R, i) \not\models C_G\varphi$ implies $C^n, (\Omega_k^L, i) \not\models C_G\varphi$ is shown similarly.

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

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

$$- d(\varphi) + i' + (k-1) \cdot |A| < (n+1) \cdot |A| \text{ for each } i' \in \mathbb{N} \text{ satisfying } i \leq i' \leq |A| - 1$$

Applying the induction hypothesis, we have that

$$C^n, (\Omega_k^L, i') \models \varphi \quad \text{iff} \quad C^n, (\Omega_k^R, i') \models \varphi$$

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 $0 \leq i' \leq |G| - (|A| - i)$

Applying the induction hypothesis, we have that

$$C^n, (\Omega_{k+1}^L, i') \models \varphi \quad \text{iff} \quad C^n, (\Omega_{k+1}^R, i') \models \varphi$$

for each $i' \in \mathbb{N}$ satisfying $0 \leq i' \leq |G| - (|A| - i)$.

Without loss of generality, we may assume that

$$C^n, (\Omega_k^L, i) \models \varphi \quad \text{and} \quad C^n, (\Omega_k^R, i) \models \varphi ,$$

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_k^L, 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_k^R, 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^R 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

$$(C^n[\varphi \rightarrow G], ((\Omega_k^L, i), 0))$$

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

$$(C^n[\varphi \rightarrow G], ((\Omega_k^R, i), 0))$$

is also isomorphic to the sub-model of C^n consisting of those worlds in the sequence s^L .⁹ But it then follows that

$$\begin{aligned} C^n[\varphi \rightarrow G], ((\Omega_k^L, i), 0) \models \psi & \text{ iff} \\ C^n[\varphi \rightarrow G], ((\Omega_k^R, i), 0) \models \psi & , \end{aligned}$$

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

$$(C^n[\varphi \rightarrow G], ((\Omega_k^L, i), 0))$$

is isomorphic to the tree model generated by $(C^n, (\Omega_k^L, i))$. Thus

⁹The tree model generated by a pointed Kripke model is sometimes called the *unraveling* generated by a pointed Kripke model. See [4] for definitions and results relevant to modal logic in general.

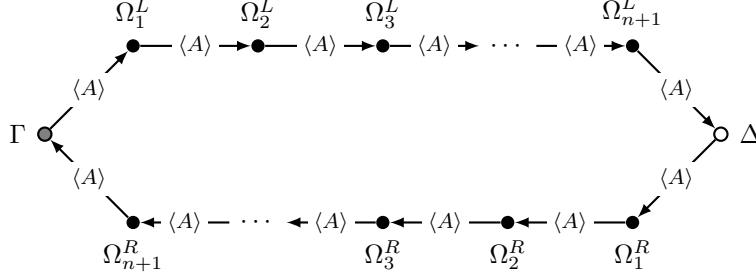


Figure 1: Picture representing the Kripke model C^n defined in the proof of Theorem 6.2. An edge from w to w' labeled “ $\langle A \rangle$ ” represents a path from w to w' whose edges enumerate A in some fixed order.

$$C^n[\varphi \rightarrow G], ((\Omega_k^L, i), 0) \models \psi \quad \text{iff} \quad C^n, (\Omega_k^L, i) \models \psi .$$

By similar reasoning, we also have

$$C^n[\varphi \rightarrow G], ((\Omega_k^R, i), 0) \models \psi \quad \text{iff} \quad C^n, (\Omega_k^R, i) \models \psi .$$

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

$$C^n, (\Omega_k^L, i) \models \psi \quad \text{iff} \quad C^n, (\Omega_k^R, i) \models \psi ,$$

which completes the proof of this theorem (Theorem 6.2). \square

Theorem 6.2 tells us that the language PRI_C^A of private communication with common knowledge cannot say everything that can be said in the language PUB_C^A of public communication with common knowledge for the set of all pointed Kripke models for A . Since we have that $\text{PRI}_C^A \hookrightarrow_{\mathcal{I}} \text{PRI}_C^A$ for each set \mathcal{I} of pointed Kripke models for A , combining Theorems 5.6 and 6.2 yields the following result.

Theorem 6.3. Let A be an agent set satisfying $|A| \geq 2$ and let \mathcal{I} be the set of all pointed Kripke models for A . Then the languages PUB_C^A and PRI_C^A are expressively incomparable for \mathcal{I} .

Finally, we show that in contrast to Theorem 5.6, we have that single-recipient private communication does not add expressivity to the language of modal logic with common knowledge for any class of *transitive* pointed Kripke models for A .

Theorem 6.4. Let A be an agent set and let \mathcal{I} be any set of transitive pointed Kripke models for A . Then $\text{PRI}_C^A \hookrightarrow_{\mathcal{I}} \text{ML}_C^A$.

Proof. In Figure 2, we define a function $u : \text{PRI1}_C^A \rightarrow \text{ML}_C^A$. For each formula $\chi \in \text{PRI1}_C^A$, 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 $[\psi \rightarrow i]$ for $\psi \in \text{PRI1}_C^A$ 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.)

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

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

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

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

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

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

Suppose $M, \Gamma \not\models [\varphi \rightarrow i]C_G\psi$ for some $(M, \Gamma) \in \mathcal{I}$. This means that $M, \Gamma \models \varphi$ and there is a sequence $\{(\Gamma_k, a_k)\}_{k=0}^n$ of worlds in $M[\varphi \rightarrow i]$ 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 $(\Gamma_k, a_k) R_j [\varphi \rightarrow i](\Gamma_{k+1}, a_{k+1})$, and $M[\varphi \rightarrow i], (\Gamma_n, a_n) \not\models \psi$. In case $n = 0$, we then have that $M, \Gamma \not\models [\varphi \rightarrow i]\psi$ and thus that $M, \Gamma \not\models ([\varphi \rightarrow i]\psi)^u$ 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 $(M[\varphi \rightarrow i], (\Gamma_n, 1))$ 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 $M, \Gamma \not\models ([\varphi \rightarrow i] \psi)^u \wedge (\varphi^u \supset E_G C_G \psi^u)$.

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

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

Suppose that $M, \Gamma \not\models [\varphi \rightarrow i] C_G \psi$ 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 $\{(\Gamma_k, a_k)\}_{k=0}^n$ of worlds in $M[\varphi \rightarrow i]$ 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

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

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 $M, \Gamma_n \not\models ([\varphi \rightarrow i] \psi)^u$. 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 $M, \Gamma \not\models C_i([\varphi \rightarrow i] \psi)^u$.

- 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 $(M[\varphi \rightarrow i], (\Gamma_n, a_n))$. 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

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

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: $M, \Gamma \not\models C_i([\varphi \rightarrow i]\psi)^u$

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 $M, \Gamma_n \not\models ([\varphi \rightarrow i]\psi)^u$. 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 $i \in G$.

– 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 $(\Gamma_n, 0) \in M[\varphi \rightarrow i]$, from which it follows that $(\Gamma, 0) R_i [\varphi \rightarrow i](\Gamma_n, 0)$ 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

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

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

By choosing \mathcal{I} as a set of transitive pointed Kripke models for A , we choose those Kripke models for which the agents' beliefs are *introspective*, meaning each agent believes his own beliefs. Since each single-recipient communication of agent i 's knowledge to a group G having $i \in G$ is in fact a communication received only by i himself, Theorem 6.4 provides a sense in which believing our own beliefs imposes a kind of self-dialog.

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

Figure 2: Inductive definition of a function $u : \text{PRI1}_C^A \rightarrow \text{ML}_C^A$ used in the proof of Theorem 6.4.

7 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 6.2: the language PRI_C^A of private communication with common knowledge cannot say everything that can be said in the language PUB_C^A of public communication with common knowledge for the class of all pointed Kripke models for A .

In Theorem 6.3, we combined Theorem 6.2 with a known result—Theorem 5.6 [3]—to show that for $2 \leq |A| < \omega$, the languages PRI_C^A and PUB_C^A are expressively incomparable for the class of all pointed Kripke models for A . This provides us with a formal proof that public and private communication are fundamentally different in the presence of common knowledge.

2. Theorem 6.4: the language PRI1_C^A of single-recipient private communication with common knowledge and the language ML_C^A of modal logic with common knowledge are equally expressive for any class of *transitive* pointed Kripke models, which says that single-recipient private communication does not add expressivity to the language of modal logic with common knowledge for any class of *transitive* pointed Kripke models.

As a consequence, single-recipient private communication is implicit in **KD45**, the typical *logic of 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, 14]. Given the extremely limited collection of known expressivity results that have been discovered since the Plaza-Gerbrandy Theorem became well-known in 1999 [6, 12],

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 that the many DEL languages make available to ideally rational agents. Understanding this gamut will provide important clues as to the fundamental communicative types that would constitute an account of the dynamics of our imperfect everyday knowledge, and so it is our hope that our small contributions here will be of use in this pursuit as well.

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] Saul A. Kripke. A completeness theorem in modal logic. *The Journal of Symbolic Logic*, 24(1):1–14, 1959.
- [10] Carsten Lutz. Complexity and succinctness of public announcement logic. In Peter Stone and Gerhard Weiss, editors, *Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'06)*, pages 137–144. Association for Computing Machinery (ACM), 2006.
- [11] Rohit Parikh. Logical omniscience and common knowledge: What do we know and what do we know? In R. van der Meyden, editor, *Proceedings of the 10th Conference on Theoretical Aspects of Rationality and Knowledge (TARK-2005)*, pages 62–77, Singapore, 2005.

- [12] 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.
- [13] Johan van Benthem, Jan van Eijck, and Barteld Kooi. Logics of communication and change. *Information and Computation*, 204(11):1620–1662, 2006.
- [14] Hans van Ditmarsch, Wiebe van der Hoek, and Barteld Kooi. *Dynamic Epistemic Logic*. Springer, 2007.