Journal of Applied Logic 8 (2010) 62–81

Contents lists available at ScienceDirect

Journal of Applied Logic

www.elsevier.com/locate/jal

Group announcement logic

Thomas Ågotnes [a,*,1], Philippe Balbiani [b], Hans van Ditmarsch [c,2], Pablo Seban [b]

[a] Department of Information Science and Media Studies, University of Bergen, PB. 7802, N-5020 Bergen, Norway
[b] IRIT, Université Paul Sabatier, 118 Route de Narbonne, F-31062 Toulouse cedex 9, France
[c] Department of Logic, Faculty of Philosophy, University of Sevilla, Calle Camilo Jose Cela s/n, 41018 Sevilla, Spain

ARTICLE INFO

Article history:
Received 7 October 2008
Accepted 23 December 2008
Available online 10 July 2009

Keywords:
Dynamic epistemic logic
Agency
Coalitional ability
Information-based protocols

ABSTRACT

Two currently active strands of research on logics for multi-agent systems are dynamic epistemic logic, focusing on the epistemic consequences of actions, and logics of coalitional ability, focusing on what coalitions of agents can achieve by cooperating strategically. In this paper we bridge these topics by considering the question: "what can a coalition achieve by making public announcements?". We propose an extension of public announcement logic with constructs of the form $\langle G\rangle\phi$, where G is a group of agents, with the intuitive meaning that G can jointly execute a *publicly observable* action such that ϕ will be true afterwards. Actions here are taken to be *truthful public announcements*, but turn out also to include *sequences* of such joint actions as well as protocols with alternating actions by different agents, in response to the actions of others. We also study in detail the difference between 'knowing how' (knowing de re) and 'knowing that' (knowing de dicto) in our framework: both can elegantly be expressed in the single-agent case. We present several meta-logical properties of this *Group Announcement Logic*, including a sound and complete axiomatization, expressivity and the complexity of model checking.

1. Introduction

Analysis of the dynamics of knowledge has received some attention recently, see [20] for an overview. Van Benthem [18] and Balbiani et al. [4] suggested an interpretation of the standard modal diamond where $\Diamond\phi$ means "there is an announcement after which ϕ". This was in a setting going back to the Fitch-paradox [8]. The new interpretation of the diamond $\Diamond$ in the Fitch setting firstly interprets $\Diamond\phi$ as 'sometime later, ϕ', and secondly specifies this temporal specification as what may result of a specific event, namely a public announcement: 'after some announcement, ϕ'. In other words, the semantics is: $\Diamond\phi$ is true if and only if $\langle\psi\rangle\phi$ is true for some ψ; the expression $\langle\psi\rangle\phi$ stands for 'ψ is true and after ψ is announced, ϕ is true'. There are some restrictions on ψ. The resulting arbitrary announcement logic is axiomatizable and has various pleasing properties (again, see [4], and for more detail the extended journal version [5]).

Arbitrary announcement logic makes no assumption in the interpretation of $\Diamond\phi$ about *who* makes the announcement, or indeed whether or not the announcement *can* be truthfully made by anyone. In the current contribution we investigate a variant of arbitrary announcement logic. Instead of $\Diamond\phi$ we use a more specific operator, namely $\langle G\rangle\phi$. Here G is a subgroup of all agents *that simultaneously make truthful public announcements*, i.e., announcements of formulae they know. In other words, let $G = \{1,\ldots,k\}$, then: $\langle G\rangle\phi$ is true if and only if there exist formulae $\psi_1,\ldots,\psi_k$ such that $\langle K_1\psi_1 \wedge$

* Corresponding author.
E-mail addresses: thomas.agotnes@infomedia.uib.no (T. Ågotnes), hvd@us.es (H. van Ditmarsch), seban@irit.fr (P. Seban).

[1] Also affiliated with Bergen University College.

[2] The author acknowledges support of the Netherlands Institute of Advanced Study where he was Lorentz Fellow in 2008. He is also affiliated with the University of Otago, New Zealand, and during work for this article in 2008 he was affiliated with IRIT, France.

1570-8683/$ – see front matter
doi:10.1016/j.jal.2008.12.002

$\cdots K_k\psi_k\rangle\phi$ is true; now, the expression $\langle K_1\psi_1 \wedge \cdots K_k\psi_k\rangle\phi$ stands for $K_1\psi_1 \wedge \cdots K_k\psi_k$ is true and after agents $1,\ldots,k$, simultaneously announce $\psi_1,\ldots,\psi_k$, then ϕ is true'. Note that the remaining agents, not included in the set G of k agents, are not involved in making the announcement, although they are aware of that action happening. The resulting logic is called *Group Announcement Logic* (*GAL*).

Informally speaking, $\langle G\rangle\phi$ expresses the fact that coalition G has the ability to make ϕ come about. Logics modelling the coalitional abilities of agents have been an active area of research in multi-agent systems in recent years, the most prominent frameworks being Pauly's Coalition Logic [16] and Alur, Henzinger and Kupferman's Alternating-time Temporal Logic [3]. The main constructs of these logics are indeed of the form $\langle G\rangle\phi$ with the intuitive meaning that coalition G can achieve ϕ. In this paper we investigate these notions when the actions that can be performed are truthful public announcements.

Section 2 contains an introduction into public announcement logic, and arbitrary public announcement logic. Section 3 defines group announcement logic, presents various interaction axioms between the different modalities that express intuitive properties of such joint announcements, and the axiomatization. Section 4 is entirely devoted to expressivity matters, and Section 5 to model checking. The relation between group announcement logic and various notions of group ability, including knowledge 'de re' and knowledge 'de dicto', is discussed in detail in Section 6, which is followed by a more applied Section 7 that embeds these observations into security protocols for two agents (sender and receiver) in the presence of a finite number of eavesdroppers intercepting all communications between them. The paper is based on but greatly extend a part of [2].

2. Background

2.1. Structures

Let $N = \{1,\ldots,n\}$ be a finite set of agents, $n > 0$, and Θ be a countable set of primitive propositions. A *Kripke structure* (or *model*) over N and Θ is a tuple $\mathcal{M} = (S, \sim_1,\ldots,\sim_n, V)$ where S is a set of states, $\sim_i \subseteq S \times S$ is an epistemic indistinguishability relation and is assumed to be an equivalence relation for each agent $i \in N$, and $V : \Theta \to 2^S$ assigns primitive propositions to the states in which they are true. A *pointed Kripke structure* is a pair $(\mathcal{M}, s)$ where s is a state in $\mathcal{M}$.

Bisimulation is a well-known notion of structural similarity [6] that we will frequently use in examples and proofs, e.g. to achieve our expressivity results.

Let two models $\mathcal{M} = (S, \sim_1,\ldots,\sim_n, V)$ and $\mathcal{M}' = (S', \sim'_1,\ldots,\sim'_n, V')$ be given. A non-empty relation $\mathfrak{R} \subseteq S \times S'$ is a bisimulation between $\mathcal{M}$ and $\mathcal{M}'$ iff for all $s \in S$ and $s' \in S'$ with $(s, s') \in \mathfrak{R}$:

atoms for all $p \in \Theta$: $s \in V(p)$ iff $s' \in V'(p)$;

forth for all $i \in N$ and all $t \in S$: if $s \sim_i t$, then there is a $t' \in S'$ such that $s' \sim'_i t'$ and $(t, t') \in \mathfrak{R}$;

back for all $i \in N$ and all $t' \in S'$: if $s' \sim'_i t'$, then there is a $t \in S$ such that $s \sim_i t$ and $(t, t') \in \mathfrak{R}$.

We write $(\mathcal{M}, s) \underline{\leftrightarrow} (\mathcal{M}', s')$, iff there is a bisimulation between $\mathcal{M}$ and $\mathcal{M}'$ linking s and s', and we then call the pointed Kripke structures $(\mathcal{M}, s)$ and $(\mathcal{M}', s')$ bisimilar.

2.2. Public announcement logic

The language $\mathcal{L}_{pal}$ of public announcement logic (*PAL*) [17] over N and Θ is defined as follows, where $i \in N$ and $p \in \Theta$:

$$\varphi ::= p \mid K_i\varphi \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid [\varphi_1]\varphi_2$$

We write $\langle\phi_1\rangle\phi_2$ resp. $\hat{K}_i\varphi$ for the duals $\neg[\phi_1]\neg\phi_2$ and $\neg K_i\neg\varphi$.

The interpretation of formulae in a pointed Kripke structure is defined as follows (the other clauses are defined in the usual truth-functional way).

$$\mathcal{M}, s \models K_i\phi \text{ iff for every } t \text{ such that } s \sim_i t,\ \mathcal{M}, t \models \phi$$

$$\mathcal{M}, s \models [\phi]\psi \text{ iff } \mathcal{M}, s \models \phi \text{ implies that } \mathcal{M}|\phi, s \models \psi$$

where $\mathcal{M}|\phi = (S', \sim'_1,\ldots,\sim'_n, V')$ such that $S' = \{s' \in S:\ \mathcal{M}, s' \models \phi\}$; $\sim'_i = \sim_i \cap (S' \times S')$; $V'(p) = V(p) \cap S'$.

The purely epistemic fragment of the language (i.e., formulae not containing public announcement operators $[\phi]$) is denoted $\mathcal{L}_{el}$. It was already shown in Plaza's original publication on that logic [17] that the language of *PAL* is equally expressive as the purely epistemic fragment within the class of all models.

2.3. Arbitrary public announcement logic

Arbitrary public announcement logic (*APAL*) extends public announcement logic with an additional inductive construct $\Box\phi$. Its interpretation is:

$$\mathcal{M}, s \models \Box\phi \text{ iff for all } \psi \in \mathcal{L}_{el}:\ \mathcal{M}, s \models [\psi]\phi$$

In other words, $\Box\phi$ is true iff ϕ is true after announcement of any *epistemic formula*, i.e. after arbitrary model restriction *to epistemically definable submodels* containing the actual state. Two typical validities for the logic, which we will see recur in similar form in group announcement logic, are: $\models \Box\phi \rightarrow \Box\Box\phi$ (**4**) and $\models \Diamond\Box\phi \rightarrow \Box\Diamond\phi$ (**Church–Rosser**). A crucial semantic result, which we will also see reappear in different form, is that if $\Diamond\phi$ is true in some epistemic state $(\mathcal{M}, s)$, i.e., if a true epistemic formula ψ can be announced to make ϕ true, then, for some atom p not occurring in ϕ, $\langle p\rangle\phi$ is true in model $\mathcal{M}'$ that is exactly as model $\mathcal{M}$ except for the valuation of the announced p and of possibly other atoms not occurring in ϕ.

The logic *APAL* is more expressive than public announcement logic within the class of all models, it is not compact, and it has a complete axiomatization (see [4] and [5] for details). The axioms and inference rules involving arbitrary announcement are:

$$\Box\phi \rightarrow [\psi]\phi \qquad \text{where } \psi \in \mathcal{L}_{el}$$

From ϕ, infer $\Box\phi$

From $\psi \rightarrow [\theta][p]\phi$, infer $\psi \rightarrow [\theta]\Box\phi$ where $p \notin \Theta_\psi \cup \Theta_\theta \cup \Theta_\phi$

where Θ_ϕ denotes the set of atoms occurring in a formula ϕ.

3. Group announcement logic

The main construct of the language of *group announcement logic* (*GAL*) is $\langle G\rangle\varphi$, intuitively meaning that there is some announcement the group G can truthfully make after which φ will be true. Such a simultaneous announcement may sound like a lot of unintelligible noise. But in fact it merely means a *joint public action* – not necessarily involving talking. We will later even find ways to model subsequent announcements as sequences of simultaneous actions, making the basic semantic idea even less appear as shouting in groups.

3.1. Language

The language $\mathcal{L}_{gal}$ of *GAL* is defined by extending the language of *PAL* with a new operator $[G]$ for each coalition G:

Definition 1 *(Language).*

$$\varphi ::= p \mid K_i\varphi \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid [G]\varphi \mid [\varphi_1]\varphi_2$$

where i is an agent, G is a set of agents and $p \in \Theta$. We write $\langle G\rangle\varphi$ for the dual $\neg[G]\neg\varphi$ and $\langle i\rangle\phi$ for $\langle\{i\}\rangle\phi$. For the subset of atoms occurring in a formula ϕ we, again, write Θ_ϕ.

We adopt the standard definition for the notion of subformula.

3.2. Semantics

The interpretation of formulae in a pointed Kripke structure is defined by extending the definition for *PAL* with a clause for the new operator:

Definition 2 *(Semantics).* By induction on formula structure:

$\mathcal{M}, s \models p$ iff $p \in V(p)$

$\mathcal{M}, s \models K_i\phi$ iff for every t such that $s \sim_i t$, $\mathcal{M}, t \models \phi$

$\mathcal{M}, s \models \neg\phi$ iff not $\mathcal{M}, s \models \phi$

$\mathcal{M}, s \models \phi \wedge \psi$ iff $\mathcal{M}, s \models \phi$ and $\mathcal{M}, s \models \psi$

$\mathcal{M}, s \models [\phi]\psi$ iff $\mathcal{M}, s \models \phi$ implies that $\mathcal{M}|\phi, s \models \psi$ where $\mathcal{M}|\phi$ is as in Section 2.2

$\mathcal{M}, s \models [G]\phi$ iff for every set $\{\psi_i\colon i \in G\} \subseteq \mathcal{L}_{el}$, $\mathcal{M}, s \models [\bigwedge_{i\in G} K_i\psi_i]\phi$

We get the following meaning for the dual:

$\mathcal{M}, s \models \langle G\rangle\phi$ iff there exists a set $\{\psi_i\colon i \in G\} \subseteq \mathcal{L}_{el}$ such that $\mathcal{M}, s \models \langle\bigwedge_{i\in G} K_i\psi_i\rangle\phi$

If we write this out in detail, we get: $\mathcal{M}, s \models \langle G\rangle\phi$ iff there exists a set $\{\psi_i\colon i \in G\} \subseteq \mathcal{L}_{el}$ such that $\mathcal{M}, s \models \bigwedge_{i\in G} K_i\psi_i$ and $\mathcal{M}|\bigwedge_{i\in G} K_i\psi_i, s \models \phi$.

Observe that $\langle G\rangle$ quantifies only over purely epistemic formulae. The reason for this is as follows. First, in the semantics of $\langle G\rangle\phi$ the formulae ψ_i in $\bigwedge_{i\in G} K_i\psi_i$ *cannot* be unrestricted $\mathcal{L}_{gal}$ formulas, as that would make the definition circular: such a ψ_i could then be the formula $\langle G\rangle\phi$ itself that we are trying to interpret. We therefore avoid quantifying over formulae containing $\langle G\rangle$ operators. However, as public announcement logic is equally expressive as epistemic logic within the class of all models, the semantics obtained by quantifying over the fragment of the language without $\langle G\rangle$ operators is the same as the semantics obtained by quantifying only over epistemic formulae.

As usual, a formula ϕ is *valid on* $\mathcal{M}$, notation $\mathcal{M}\models\phi$, iff $\mathcal{M}, s\models\phi$ for all s in the domain of $\mathcal{M}$; and a formula ϕ is *valid*, $\models\phi$, iff $\mathcal{M}\models\phi$ for all $\mathcal{M}$. The denotation of ϕ on $\mathcal{M}$, notation $[\![\phi]\!]_{\mathcal{M}}$ is defined as $\{s\in S \mid \mathcal{M}, s\models\phi\}$. The set of validities of the logic is called *GAL* (group announcement logic).

Proposition 3. *Let two models $\mathcal{M}=(S,\sim_1,\ldots,\sim_n,V)$ and $\mathcal{M}'=(S',\sim'_1,\ldots,\sim'_n,V')$ be given. Let $\varphi\in\mathcal{L}_{gal}$ be a formula. For all $s\in S$ and for all $s'\in S'$, if $(\mathcal{M},s)\underline{\leftrightarrow}(\mathcal{M}',s')$ then $\mathcal{M},s\models\varphi$ iff $\mathcal{M}',s'\models\varphi$.*

Proof. As usual, the proof is done by induction on φ. □

3.3. Logical properties

To sharpen the intuition about the logic we mention some relevant validities, with particular attention to interaction between group announcement and epistemic modal operators. Examples are $\models[G]\phi\to[G][G]\phi$ (Corollary 6), $\models\langle G\rangle[G]\phi\to[G]\langle G\rangle\phi$ (Corollary 11), and $K_i[i]\phi\leftrightarrow[i]K_i\phi$ (Proposition 12).

3.3.1. Elementary validities

Proposition 4.

1. $\langle G\rangle p\to p$ *and* $\langle G\rangle\neg p\to\neg p$ (*atomic propositions do not change value*)
2. $\langle\emptyset\rangle\phi\leftrightarrow[\emptyset]\phi\leftrightarrow\phi$ (*the empty group is powerless*)
3. $\langle K_{j_1}\psi_{j_1}\wedge\cdots\wedge K_{j_k}\psi_{j_k}\rangle\phi\to\langle\{j_1,\ldots,j_k\}\rangle\phi$
4. $\phi\to\langle G\rangle\phi$ (*truth axiom*)

Proof.

1. In public announcement logic, and its 'derivatives', factual truths never change value.
2. The conjunction of an empty set of formulae is, as usual, taken to be a tautology.
3. Obvious (note that $\psi_{j_1},\ldots,\psi_{j_k}$ are purely epistemic formulas).
4. If all agents announce 'true', nothing changes to the system. □

An announcement by the empty group (the second property above) corresponds to a 'clock tick', a dynamic transition without informative effect. We could also see this as "nobody says a thing" (and this now happens...). In fact you could even see this as 'everybody says true', an announcement by the public (as in the fourth property): in other words, the group of all agents have the option *not* to exercise their power.

3.3.2. Sequences of group announcements

Intuitively, $\langle G\rangle\phi$ means that G can achieve a situation where ϕ is true in 'one step', by making a joint announcement. One can easily imagine situations where it could be interesting to reason about what a group can achieve by making *repeated* announcements, i.e., by a sequence of announcements, one after the other, or a communication protocol. A general example is a conversation over an open channel. We want to express that "there is some sequence, of arbitrary length, of announcements by G which will ensure that ϕ becomes true".

For arbitrary announcement logic (*APAL*), the validity of the principle $\Box\phi\to\Box\Box\phi$ follows from the simple observation that a sequence of two announcements ψ and χ is equivalent to the single announcement of $\psi\wedge[\psi]\chi$. Less obvious is that $[G]\phi\to[G][G]\phi$ is also valid, because now we have to show that two conjunctions of *known* formulas are again such a conjunction.

Proposition 5. $\models[G\cup H]\phi\to[G][H]\phi$.

Proof. The diamond version $\langle G\rangle\langle H\rangle\phi\to\langle G\cup H\rangle\phi$ of this validity makes clear that the requirement is that two successive announcements respectively by the agents in G simultaneously and in H simultaneously can also be seen as a single announcement by the agents in $G\cup H$ simultaneously. Let us prove how it can be done. Consider two successive announcements $\bigwedge_{i\in G}K_i\phi_i$ and $\bigwedge_{j\in H}K_j\psi_j$. Let a Kripke structure $\mathcal{M}$ and a state s in $\mathcal{M}$ be given such that $\mathcal{M},s\models\bigwedge_{i\in G}K_i\phi_i$, and similarly $\bigwedge_{j\in H}K_j\psi_j$ is true in state s in the restriction of $\mathcal{M}$ to the $\bigwedge_{i\in G}K_i\phi_i$-states: $\mathcal{M}|\bigwedge_{i\in G}K_i\phi_i, s\models\bigwedge_{j\in H}K_j\psi_j$.

Then we have:

$\mathcal{M}, s \models \langle \bigwedge_{i\in G} K_i\phi_i\rangle\langle \bigwedge_{j\in H} K_j\psi_j\rangle\theta$

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G} K_i\phi_i \wedge [\bigwedge_{g\in G} K_g\phi_g]\bigwedge_{j\in H} K_j\psi_j\rangle\theta$

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G} K_i\phi_i \wedge \bigwedge_{i\in H\setminus G} K_i\top \wedge [\bigwedge_{g\in G} K_g\phi_g](\bigwedge_{j\in H} K_j\psi_j \wedge \bigwedge_{j\in G\setminus H} K_j\top)\rangle\theta$

because for any agent i, $K_i\top$ is a valid formula

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G\cup H}(K_i\phi_i \wedge [\bigwedge_{g\in G} K_g\phi_g]K_i\psi_i)\rangle\theta$

with $\forall i \in H\setminus G,\ \phi_i = \top$ and $\forall j \in G\setminus H,\ \psi_j = \top$

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G\cup H}(K_i\phi_i \wedge (\bigwedge_{g\in G} K_g\phi_g) \to K_i[\bigwedge_{g\in G} K_g\phi_g]\psi_i)\rangle\theta$

by a reduction axiom of PAL

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G\cup H} K_i\phi_i \wedge \bigwedge_{i\in G\cup H}((\bigwedge_{j\in G} K_j\phi_j) \to K_i[\bigwedge_{j\in G} K_j\phi_j]\psi_i)\rangle\theta$

by distributing the $\wedge$

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G\cup H} K_i\phi_i \wedge \bigwedge_{i\in G\cup H} K_i[\bigwedge_{j\in G} K_j\phi_j]\psi_i\rangle\theta$

because $\bigwedge_{j\in G} K_j\phi_j$ is assumed true in the left conjunct of the announcement

only if $\mathcal{M}, s \models \langle \bigwedge_{i\in G\cup H} K_i(\phi_i \wedge [\bigwedge_{j\in G} K_j\phi_j]\psi_i)\rangle\theta$. □

Corollary 6. $\models [G]\phi \to [G][G]\phi$.

We thus get exactly the property alluded to above:

Corollary 7. *$\mathcal{M}, s \models \langle G\rangle\phi$ iff there is a finite sequence of announcements by agents in G after which ϕ is true.*

In Section 7 we discuss a security protocol example involving sequences of announcements. Note that our result does *not* mean that sequences of announcements can simply be replaced by a single announcement: whether agents are willing to do an announcement may depend on the postconditions of such announcements. These may be *known to be satisfied* after each announcement in the sequence, but not *known to be satisfied* initially after the entire sequence. These matters will be discussed in great detail later.

3.3.3. Church–Rosser

We prove that for all groups G and H of agents, for every formula $\phi \in \mathcal{L}_{gal}$, $\langle G\rangle[H]\phi \to [H]\langle G\rangle\phi$ is a valid formula. The principle is fairly intuitive: it says that when in a given epistemic state group G or group H make a group announcement, there are additional announcements by group H (after G's announcement) and group G (after H's announcement), in order to reach a new common state of information. Unfortunately, its proof is rather involved. This is because group announcements implicitly quantify over *all* propositional variables in the language. Towards the proof, we first define the *group-announcement depth* $d(\phi)$ of a formula ϕ:

Let $p \in \Theta$, $\psi, \psi_1, \psi_2 \in \mathcal{L}_{gal}$, $i \in N$, and $G \subseteq N$ be given; then $d(p) = 0$; $d(\neg\psi) = d(K_i\psi) = d(\psi)$; $d(\psi_1 \wedge \psi_2) = d([\psi_1]\psi_2) = \max(d(\psi_1), d(\psi_2))$; and $d([G]\psi) = d(\psi) + 1$. The following lemma holds for any number k, but we will only use it for $k \leqslant |N|$.

Lemma 8. *Let $Q = \{q_i\}_{i\in\mathbb{N}^*} \subseteq \Theta$ be pairwise distinct primitive propositions, and, for some $k \in \mathbb{N}$, $\theta_1, \ldots, \theta_k$ be epistemic formulas such that for $i = 1$ to $i = k$, $\Theta_{\theta_i} \cap Q = \emptyset$, and let $\phi \in \mathcal{L}_{gal}$ be such that $\Theta_\phi \cap Q = \emptyset$.*

For all $\psi \in \mathcal{L}_{gal}$, define

$$\begin{cases} \psi^{\alpha} = \psi(\theta_1/q_1, \ldots, \theta_k/q_k, q_1/q_{k+1}, q_2/q_{k+2}, \ldots) \\ \psi^{-\alpha} = \psi(q_{k+1}/q_1, q_{k+2}/q_2, \ldots) \end{cases}$$

Then, for all structures $\mathcal{M} = (S, \sim_1, \ldots, \sim_n, V)$ there is a valuation function $V' : \Theta \to 2^S$ such that

1. $[\![\phi^{\alpha}]\!]_{\mathcal{M}} = [\![\phi]\!]_{\mathcal{M}'}$,
2. *for all $\psi \in \mathcal{L}_{el}$,*
   - $[\![\psi]\!]_{\mathcal{M}'} = [\![\psi^{\alpha}]\!]_{\mathcal{M}}$,
   - $[\![\psi]\!]_{\mathcal{M}} = [\![\psi^{-\alpha}]\!]_{\mathcal{M}'}$,
3. *for all $i \leqslant k$, $[\![q_i]\!]_{\mathcal{M}'} = [\![\theta_i]\!]_{\mathcal{M}'} = [\![\theta_i]\!]_{\mathcal{M}}$,*

where $\mathcal{M}' = (S, \sim_1, \ldots, \sim_n, V')$.

Proof. We define V' as:

$$V'(p) = V(p), \qquad \text{for all } p \notin Q,$$
$$V'(q_i) = [\![\theta_i]\!]_{\mathcal{M}'}, \qquad \text{for all } i \leqslant k,$$
$$V'(q_{k+i}) = V(q_i), \qquad \text{for all } i \geqslant 1.$$

Items 2 and 3 follow directly from the definition of V'. We prove item 1 by induction on the group-announcement depth of ϕ, by showing the somewhat stronger:

For all subformulas ϕ_* of ϕ, for all submodels $\mathcal{M}_*$ of $\mathcal{M}$, and for all states $s \in \mathcal{M}_*$: $\mathcal{M}_*, s \models \phi_*^\alpha$ iff $\mathcal{M}'_*, s \models \phi_*$.

Base case main induction: The base case of this proof shows that this holds for all formulas without group announcement operators. This is itself a proof by induction on the structure of ϕ. We proceed:

Base case: $\phi = p \in \Theta$. Then the equivalence $\mathcal{M}_*, s \models p^\alpha$ iff $\mathcal{M}'_*, s \models p$ follows directly from the definition of V' and α.

Inductive cases: Let us suppose that the property is true for all subformulas of ψ, ψ_1 and ψ_2, and let us prove it for $\neg\psi$, $\psi_1 \wedge \psi_2$, $\hat{K}_i\psi$ and $[\psi_1]\psi_2$:

- $\neg\psi$:
  $\mathcal{M}_*, s \models (\neg\psi)^\alpha$ iff $\mathcal{M}_*, s \models \neg\psi^\alpha$ iff $\mathcal{M}_*, s \not\models \psi^\alpha$ iff (by IH) $\mathcal{M}'_*, s \not\models \psi$ iff $\mathcal{M}'_*, s \models \neg\psi$.
- $\psi_1 \wedge \psi_2$:
  $\mathcal{M}_*, s \models (\psi_1 \wedge \psi_2)^\alpha$ iff $\mathcal{M}_*, s \models \psi_1^\alpha \wedge \psi_2^\alpha$ iff ($\mathcal{M}_*, s \models \psi_1^\alpha$ and $\mathcal{M}_*, s \models \psi_2^\alpha$) iff (by IH) ($\mathcal{M}'_*, s \models \psi_1$) and $\mathcal{M}'_*, s \models \psi_2$) iff $\mathcal{M}'_*, s \models \psi_1 \wedge \psi_2$.
- $K_i\psi$:
  $\mathcal{M}_*, s \models K_i\psi^\alpha$ iff for all $t \sim_i s$, $\mathcal{M}_*, t \models \psi^\alpha$ iff for all $t \sim_i s$, $\mathcal{M}'_*, t \models \psi$ (by IH) iff (as $\sim_i = \sim'_i$) for all $t \sim'_i s$, $\mathcal{M}'_*, t \models \psi$ iff $\mathcal{M}'_*, s \models K_i\psi$.
- $[\psi_1]\psi_2$:
  $\mathcal{M}_*, s \models ([\psi_1]\psi_2)^\alpha$ iff $\mathcal{M}_*, s \models [\psi_1^\alpha]\psi_2^\alpha$ iff ($\mathcal{M}_*, s \models \psi_1^\alpha$ implies $\mathcal{M}_*|\psi_1^\alpha, s \models \psi_2^\alpha$) iff (using IH twice) ($\mathcal{M}'_*, s \models \psi_1$ implies $(\mathcal{M}_*|\psi_1^\alpha)', s \models \psi_2$) iff (using IH again for ψ_1^α and ψ_1, and that V' on the restriction is the restriction of V') ($\mathcal{M}'_*, s \models \psi_1$ implies $\mathcal{M}'_*|\psi_1, s \models \psi_2$) iff $\mathcal{M}'_*, s \models [\psi_1]\psi_2$.

Inductive case main induction: It remains to show the inductive case of the original induction on group-announcement operator depth. Suppose the property is true for all ψ such that $d(\psi) \leqslant n$. We prove that it is true for $\phi = \langle G\rangle\psi$.

$\mathcal{M}_*, s \models (\langle G\rangle\psi)^\alpha$

iff

$\mathcal{M}_*, s \models \langle G\rangle\psi^\alpha$

iff

there are $\chi_1, \ldots, \chi_{|G|}$ in $\mathcal{L}_{el}$ such that $\mathcal{M}_*, s \models \langle \bigwedge K_i\chi_i\rangle\psi^\alpha$

iff (**)

there are $\chi_1, \ldots, \chi_{|G|}$ in $\mathcal{L}_{el}$ such that $\mathcal{M}_*, s \models \langle(\bigwedge K_i\chi_i^{-\alpha})^\alpha\rangle\psi^\alpha$

iff (IH on depth)

there are $\chi_1, \ldots, \chi_{|G|}$ in $\mathcal{L}_{el}$ such that $\mathcal{M}'_*, s \models \langle \bigwedge K_i\chi_i^{-\alpha}\rangle\psi$

iff

$\mathcal{M}'_*, s \models \langle G\rangle\psi$.

In (**) we have used (the already shown) property 2 for epistemic formulas from which also follows that for all such ψ: $(\psi^{-\alpha})^\alpha = \psi$. □

Proposition 9 *(Diamond lemma). Let $k \geqslant 0$ and $G = \{i_1, \ldots, i_k\}$ be a set of agents. If $\mathcal{M}, s \models \langle G\rangle\psi$ and $p_1, \ldots, p_k \notin \Theta_\psi$, then there is an $\mathcal{M}''$ different from $\mathcal{M}$ only on the valuation of the atoms not appearing in ψ such that $\mathcal{M}'', s \models \langle K_{i_1}p_1 \wedge \cdots \wedge K_{i_k}p_k\rangle\psi$.*

Proof. We use the previous lemma twice:

1. Let Q be $\Theta\backslash\Theta_\psi$ and q_i be p_i for all $i \leqslant k$, θ_i be $\top$ for all $i \leqslant k$ and ϕ be $\langle G\rangle\psi$. By Lemma 8, there is V' such that $V'(p_i) = S$ and $[\![\langle G\rangle\psi]\!]_{\mathcal{M}'} = [\![\langle G\rangle\psi]\!]_{\mathcal{M}}$. As $\mathcal{M}, s \models \langle G\rangle\psi$, we have that $\mathcal{M}', s \models \langle G\rangle\psi$. Therefore there are $\tau_1, \ldots, \tau_k$ in $\mathcal{L}_{el}$ such that $\mathcal{M}', s \models \langle \bigwedge_{i\in G} K_i\tau_i\rangle\psi$.

2. Let Q be $\Theta \setminus (\Theta_\psi \cup \bigcup_{i \in G} \Theta_{\tau_i})$, $k = |G|$, q_i be p_i for all $i \leqslant k$, θ_i be τ_i for all $i \leqslant k$ and ϕ be $\langle \bigwedge_{i \in G} K_i \tau_i \rangle \psi$. By Lemma 8, there is V'' such that (with $\mathcal{M}''$ as $\mathcal{M}$ except for valuation V'') $[\![\langle \bigwedge K_i \tau_i \rangle \psi]\!]_{\mathcal{M}''} = [\![\langle \bigwedge K_i \tau_i \rangle \psi]\!]_{\mathcal{M}'}$ and for all $i \leqslant k$, $[\![p_i]\!]_{\mathcal{M}''} = [\![\tau_i]\!]_{\mathcal{M}''} = [\![\tau_i]\!]_{\mathcal{M}'}$. This last property implies that $\mathcal{M}'' \models \bigwedge K_i p_i \leftrightarrow \bigwedge K_i \tau_i$. As $\mathcal{M}', s \models \langle \bigwedge_{i \in G} K_i \tau_i \rangle \psi$ (by the first item), the first property implies that $\mathcal{M}'', s \models \langle \bigwedge_{i \in G} K_i \tau_i \rangle \psi$. The second one implies that $\mathcal{M}'' \models \bigwedge K_i p_i \leftrightarrow \bigwedge K_i \tau_i$. We now have that $\mathcal{M}'', s \models \langle \bigwedge_{i \in G} K_i p_i \rangle \psi$. □

A generalization of Proposition 9 indirectly proves the soundness of a derivation rule in the axiomatization of GAL. Here, we need Proposition 9 to prove the validity of the generalized Church–Rosser schema.

Proposition 10 *(Church–Rosser generalized). For any $G, H \subseteq N$: $\models \langle G \rangle [H] \phi \to [H] \langle G \rangle \phi$.*

Proof. Suppose the contrary: Let $\mathcal{M}$ be a model, s a state of $\mathcal{M}$, $\phi \in \mathcal{L}_{gal}$ and $G, H \subseteq N$ two groups of agents such that $\mathcal{M}, s \models \langle G \rangle [H] \phi \wedge \langle H \rangle [G] \neg \phi$. Then, using Proposition 9 twice, for $|G| = k$ and $|H| = k'$, we know that there are $\{p_i\}_{i \in G}$ and $\{q_i\}_{i \in H}$ subsets of Θ and $\mathcal{M}'$ differing from $\mathcal{M}$ only on the valuation of the p_i, q_i such that

$$\mathcal{M}', s \models \left\langle \bigwedge_{i \in G} K_i p_i \right\rangle [H] \phi \wedge \left\langle \bigwedge_{i \in H} K_i q_i \right\rangle [G] \neg \phi.$$

In particular,

$$\mathcal{M}', s \models \left\langle \bigwedge_{i \in G} K_i p_i \right\rangle \left[\bigwedge_{i \in H} K_i q_i \right] \phi \wedge \left\langle \bigwedge_{i \in H} K_i q_i \right\rangle \left[\bigwedge_{i \in G} K_i p_i \right] \neg \phi.$$

Note that $\langle \bigwedge_{i \in G} K_i p_i \rangle$ and $\langle \bigwedge_{i \in H} K_i q_i \rangle$ are conjunctions of known facts. As these are positive formulas, they remain true after further announcements. So we have

$$\mathcal{M}', s \models \left\langle \bigwedge_{i \in G} K_i p_i \wedge \bigwedge_{i \in H} K_i q_i \right\rangle \phi \wedge \left\langle \bigwedge_{i \in G} K_i p_i \wedge \bigwedge_{i \in H} K_i q_i \right\rangle \neg \phi$$

from which directly follows a contradiction. □

Corollary 11 *(Church–Rosser). $\models \langle G \rangle [G] \phi \to [G] \langle G \rangle \phi$.*

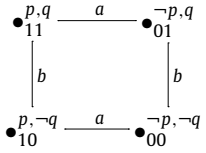
We cannot in general reverse the order of G and H in Proposition 10. A simple counterexample is the following model, where b cannot distinguish between two states but a can.

$$0 \bullet^{p} \overset{b}{\text{———}} 1 \bullet^{\neg p}$$

We now have that $\mathcal{M}, 0 \models \langle a \rangle [b] K_b p \wedge \langle a \rangle [b] \neg K_b p$ because $\mathcal{M}, 0 \models \langle K_a p \rangle [b] K_b p \wedge \langle K_a \top \rangle [b] \neg K_b p$. Therefore $\langle G \rangle [H] \phi \to [G] \langle H \rangle \phi$ is *not* valid if $G = \{a\}$ and $H = \{b\}$.

3.3.4. More validities

Just as for Church–Rosser, one would like to know whether the *APAL* validity $\Box \Diamond \phi \to \Diamond \Box \phi$ has a *GAL* generalization. We know that there exists $G, H \subseteq N$ such that the schema $[G] \langle H \rangle \phi \to \langle H \rangle [G] \phi$ is *not* valid. A simple counterexample is the following model $\mathcal{M}$, i.e. for $G = \{a\}$ and $H = \{b\}$, with $\phi = (K_a K_b p \vee K_b K_a q) \wedge \neg (K_a K_b p \wedge K_b K_a q)$.



Here we have $\mathcal{M}, 11 \models [a] \langle b \rangle \phi \wedge [b] \langle a \rangle \neg \phi$. We do not know whether $[G] \langle G \rangle \phi \to \langle G \rangle [G] \phi$ is valid.

For arbitrary announcement logic we have that $K_i \Box \phi \to \Box K_i \phi$, but not the other way round. Now, we can do more.

Proposition 12. *For arbitrary $i \in N$ and $G \subseteq N$:*

1. $\models K_i [i] \phi \leftrightarrow [i] K_i \phi$.
2. $\models K_i [G] \phi \to [G] K_i \phi$ *(but not the other way round).*

Proof.

1. In *APAL*, $\Box K_i\phi \rightarrow K_i\Box\phi$ is false because after going to an i-accessible state the subsequent model restriction may exclude the actual state. But for singleton announcements we have an equivalence. This is because any i-accessible state will be contained in the actual i-class.
2. As for arbitrary announcement logic. Agent i may but need not be in group G. □

Finally, a rather puzzling property on the interaction between the announcements and knowledge by two agents. The intuition behind it, is that announcements wherein you can make another agent learn facts even in the face of your own uncertainty, are rather rare. In other words, the conditions in the equivalence are fairly strong.

Proposition 13. *For any atomic proposition* $p \in \Theta$: $\models \langle a\rangle K_b p \leftrightarrow \langle b\rangle K_a p$.

Proof. Assume $\mathcal{M}, s \models \langle a\rangle K_b p$. Then there is a $\psi_a \in \mathcal{L}_{el}$ such that $\mathcal{M}, s \models \langle K_a\psi_a\rangle K_b p$. This formula is equivalent to $K_a\psi_a \wedge (K_a\psi_a \rightarrow K_b[K_a\psi_a]p)$ and thus to $K_a\psi_a \wedge K_b(K_a\psi_a \rightarrow p)$ – as p is an atom. Let us note $\mathcal{M}' = \mathcal{M}|K_b(K_a\psi_a \rightarrow p)$ and let us proof that $\mathcal{M}', s \models K_a p$. Indeed, let $t \in \mathcal{M}'$ s.t. $t \in \mathcal{R}'_a(x)$ (in the restricted model) and let us prove that $\mathcal{M}', t \models p$. But we have (1) $\mathcal{M}, t \models K_b(K_a\psi_a \rightarrow p)$ and (2) $t \in \mathcal{R}_a(x)$ (in the non-restricted model). But (1) implies that $\mathcal{M}, t \models K_a\psi_a \rightarrow p$ and (2) implies that $\mathcal{M}, t \models K_a\psi_a$ (because $\mathcal{M}, s \models K_a\psi_a$). Then $\mathcal{M}, t \models p$, and thus $\mathcal{M}', t \models p$. □

We now proceed to a more systematic treatment of validities.

3.4. Axiomatization

The following is a sound and complete axiomatization of group announcement logic.

Definition 14 *(GAL axioms and rules).*

Instantiations of propositional tautologies	
$K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$	distribution (of knowl. over impl.)
$K_i\phi \rightarrow \phi$	truth
$K_i\phi \rightarrow K_iK_i\phi$	positive introspection
$\neg K_i\phi \rightarrow K_i\neg K_i\phi$	negative introspection
$[\phi]p \leftrightarrow (\phi \rightarrow p)$	atomic permanence
$[\phi]\neg\psi \leftrightarrow (\phi \rightarrow \neg[\phi]\psi)$	announcement and negation
$[\phi](\psi \wedge \chi) \leftrightarrow ([\phi]\psi \wedge [\phi]\chi)$	announcement and conjunction
$[\phi]K_i\psi \leftrightarrow (\phi \rightarrow K_i[\phi]\psi)$	announcement and knowledge
$[\phi][\psi]\chi \leftrightarrow [\phi \wedge [\phi]\psi]\chi$	announcement composition
$[G]\phi \rightarrow [\bigwedge_{i\in G} K_i\psi_i]\phi$, where $\psi_i \in \mathcal{L}_{el}$	group and specific announcement
From ϕ and $\phi \rightarrow \psi$, infer ψ	modus ponens
From ϕ, infer $K_i\phi$	necessitation of knowledge
From ϕ, infer $[\psi]\phi$	necessitation of announcement
From ϕ, infer $[G]\phi$	necessitation of group announcement
From $\phi \rightarrow [\theta][\bigwedge_{i\in G} K_i p_i]\psi$, infer $\phi \rightarrow [\theta][G]\psi$ where $p_i \notin \Theta_\phi \cup \Theta_\theta \cup \Theta_\psi$	deriving group announcement/$R([G])$

Our axiomatization of *GAL* is based on the standard *S*5 axioms for the epistemic operators K_i, the standard reduction axioms for the public announcement operators $[\phi]$, and some additional axioms and derivation rules involving group announcement operators. These are the axiom *group and specific announcement*, and the derivation rules *necessitation of group announcement* and *deriving group announcement*. A formula $\phi \in \mathcal{L}_{gal}$ is derivable, notation $\vdash \phi$, iff ϕ belongs to the least set of formulas containing *GAL* axioms and closed with respect to the derivation rules.

The axiom $[G]\phi \rightarrow [\bigwedge_{i\in G} K_i\psi_i]\phi$, where $\psi_i \in \mathcal{L}_{el}$, is obviously valid in all structures. Also the validity of 'from ϕ, infer $[G]\phi$' will be obvious. The derivation rule *deriving group announcement* ($R([G])$) is used to introduce group announcement operators in derivations:

From $\phi \rightarrow [\theta][\bigwedge_{i\in G} K_i p_i]\psi$ (where $p_i \notin \Theta_\phi \cup \Theta_\theta \cup \Theta_\psi$) infer $\phi \rightarrow [\theta][G]\psi$.

It needs some explanation. Consider some way to denote a unique occurrence of a subformula χ in an expression $\boldsymbol{\eta}$ containing an empty slot, in a way that the subformula does not appear just behind a negation, or similar awkward positions. We write $\boldsymbol{\eta}(\chi)$ for that formula $\boldsymbol{\eta}$ with the empty slot filled. The following is then the intuitively valid derivation rule that we need:

From $\boldsymbol{\eta}([\bigwedge_{i\in G} K_i\psi_i]\psi)$ for all $\psi_i \in \mathcal{L}_{el}$, infer $\boldsymbol{\eta}([G]\psi)$.

In other words, if you can get ψ after no matter what simultaneous announcement by no matter what agent in G, *then* it holds after group announcements by G. In the following section we show why this formulation can be simplified to the rule *deriving group announcement*, and why therefore our rule is sound. An outline of the completeness proof of *GAL* is also presented in the following section. The details for soundness and completeness are very similar to those for arbitrary announcement logic in [4,5].

Theorem 15 *(Soundness and completeness). Let $\phi \in \mathcal{L}_{gal}$. Then ϕ is a theorem iff ϕ is valid.*

3.4.1. Soundness and completeness

We show soundness of the rule $R([G])$, and we outline how the soundness and completeness proofs are interlinked. The completeness part of the proof uses the notion of necessity forms. it is very similar to the one for arbitrary announcement logic. For full details, see [5].

Necessity forms were introduced by Goldblatt [11]. A *necessity form* contains a unique occurrence of a special symbol $\sharp$. If $\boldsymbol{\psi}$ is such a necessity form and $\phi \in \mathcal{L}_{gal}$, then $\boldsymbol{\psi}(\phi)$ is obtained from $\boldsymbol{\psi}$ by substituting $\sharp$ in $\boldsymbol{\psi}$ for ϕ. The *necessity forms* are inductively defined as follows: $\sharp$ is a necessity form; if $\boldsymbol{\psi}$ is a necessity form then $(\phi \to \boldsymbol{\psi})$ is a necessity form; if $\boldsymbol{\psi}$ is a necessity form and φ is in $\mathcal{L}_{gal}$ then $[\phi]\boldsymbol{\psi}$ is a necessity form; if $\boldsymbol{\psi}$ is a necessity form then $K_i\boldsymbol{\psi}$ is a necessity form. We also use the dual notion of possibility form which can be defined by the dual clauses to a necessity form: $\sharp$ is a possibility form; if $\boldsymbol{\psi}$ is a possibility form then $(\phi \wedge \boldsymbol{\psi})$, $\langle\phi\rangle\boldsymbol{\psi}$ and $\hat{K}_i\boldsymbol{\psi}$ are possibility forms.

First, we prove a generalization of Proposition 9:

Lemma 16. *Let $n \geqslant 0$ and $G = \{i_1, \ldots, i_n\}$ be a set of agents. Let $\boldsymbol{\eta}(\sharp)$ be a possibility form. If $\mathcal{M}, s \models \boldsymbol{\eta}\{\langle G\rangle\psi\}$ and $p_1, \ldots, p_n \notin \Theta_\eta \cup \Theta_\psi$ then there is an $\mathcal{M}'$ differing only on the valuation of the p_i such that $\mathcal{M}', s \models \boldsymbol{\eta}\{\langle\bigwedge_{i\in G} K_i p_i\rangle\psi\}$.*

Proof. The base case where $\boldsymbol{\eta} = \sharp$, such that $\boldsymbol{\eta}\{\langle G\rangle\psi\} = \langle G\rangle\psi$, has been proved by Proposition 9. For the inductive cases: let $\boldsymbol{\eta}\{\sharp\}$ be a possibility form and suppose that the conditions for $\mathcal{M}, s \models \boldsymbol{\eta}\{\langle G\rangle\psi\}$ are met, and let $\phi \in \mathcal{L}_{gal}$. Then:

- If $\mathcal{M}, s \models \phi \wedge \boldsymbol{\eta}\{\langle G\rangle\psi\}$ and $p_1, \ldots, p_n \notin \Theta_{\boldsymbol{\eta}} \cup \Theta_\psi \cup \Theta_\phi$, then the construction made in the proof of Proposition 9 applies here too and gives us that $\mathcal{M}', s \models \phi$, and then, by IH, $\mathcal{M}', s \models \phi \wedge \boldsymbol{\eta}\{\langle\bigwedge_{i\in G} K_i p_i\rangle\psi\}$.
- If $\mathcal{M}, s \models \langle\phi\rangle\boldsymbol{\eta}\{\langle G\rangle\psi\}$ and $p_1, \ldots, p_n \notin \Theta_{\boldsymbol{\eta}} \cup \Theta_\psi \cup \Theta_\phi$ then $\mathcal{M}|\phi, s \models \boldsymbol{\eta}\{\langle G\rangle\psi\}$ and by induction hypothesis $(\mathcal{M}|\phi)', s \models \boldsymbol{\eta}\{\langle\bigwedge_{i\in G} K_i p_i\rangle\psi\}$. By definition of the valuation V', $(\mathcal{M}|\phi)' = \mathcal{M}'|\phi$.
- If $\mathcal{M}, s \models \hat{K}_i\boldsymbol{\eta}\{\langle G\rangle\psi\}$, then there is a t such that $s \sim_i t$ and $\mathcal{M}, t \models \boldsymbol{\eta}\{\langle G\rangle\psi\}$. Then, by IH, $\mathcal{M}', t \models \boldsymbol{\eta}\{\langle\bigwedge_{i\in G} K_i p_i\rangle\psi\}$. But we also have that $s \sim'_i t$ by construction of $\mathcal{M}'$. □

This lemma will help us to show soundness of the rule $R([G])$ in the axiomatization. Consider two variants of the axiomatization *GAL*, with instead of $R([G])$ either rule $R^\omega([G])$ or rule $R^1([G])$ as follows (where φ is an arbitrary necessity form):

- From $\boldsymbol{\varphi}([\bigwedge_{i\in G} K_i\theta_i]\psi)$ for all $\{\theta_i\}_{i\in G} \subset \mathcal{L}_{el}$, infer $\boldsymbol{\varphi}([G]\psi)$ $\quad (R^\omega([G]))$
- From $\boldsymbol{\varphi}([\bigwedge_{i\in G} K_i p_i]\psi)$ where $p_i \notin \Theta_{\boldsymbol{\varphi}} \cup \Theta_\psi$, infer $\boldsymbol{\varphi}([G]\psi)$ $\quad (R^1([G]))$

The inference rule $R^\omega([G])$ is not finitary, but its soundness is very obvious. The rule $R^1([G])$ is finitary (one premiss!), its soundness is not obvious, but fortunately it follows directly from Lemma 16. Here comes the convenient truth: the rule $R^1([G])$ is stronger than the rule $R^\omega([G])$: if, in the system based on $R^\omega([G])$, we can prove $\boldsymbol{\varphi}([\bigwedge K_i\theta_i]\psi)$ for all epistemic formulas θ_i then we can prove in particular $\boldsymbol{\varphi}([\bigwedge K_i p_i]\psi)$ for some atoms $p_1, \ldots, p_k \notin \Theta_{\boldsymbol{\varphi}} \cup \Theta_\psi$. As a result, we can derive the conclusion of the infinitary rule using only the finitary rule. Therefore, anything derivable in the infinitary axiomatization is also derivable in the axiomatization with $R^1([G])$.

One can also show that $R^1([G])$ and $R([G])$ are equally strong, in the sense that every derivation using the former can be transformed in one using the latter. The occurrence of $[\bigwedge_{i\in G} K_i p_i]\psi$ in the necessity form is always the last subformula (see the definition), but it can be preceded by any wild sequence of implications, epistemic operators, and announcement operators. All these can be pushed and merged such that the main operator becomes an implication, with as main operator on the right-hand side an announcement (for a proof, see [5] – the proof does not use that formulas may have arbitrary announcement operators):

Lemma 17. *Given a necessity form $\boldsymbol{\varphi}(\sharp)$, there are $\chi, \psi \in \mathcal{L}_{gal}$ such that for all $\theta \in \mathcal{L}_{gal}$: $\models \boldsymbol{\varphi}(\theta)$ iff $\models \psi \rightarrow [\chi]\theta$.*

This lemma indirectly shows the soundness of the derivation rule $R([G])$.

The omitted completeness proof demonstrates that all validities are derivable in the infinitary axiomatization, with the rule $R^{\omega}([G])$, and that then closes the circle, i.e.: if a formula is valid, we find an infinitary derivation, by just keeping the one premiss we get a finitary derivation (that can be transformed into one using the $R([G])$ version of the finitary rule $R^1([G])$), and soundness of that principle gives us validity again. See [5] for details.

4. Expressivity

Given languages X and Y and a model class Z, X is *at least as expressive as* Y with respect to Z iff, for every X-formula ϕ there is a logically equivalent Y-formula ψ. In other words, for every Z-model $\mathcal{M}$, $[\![\phi]\!]_{\mathcal{M}} = [\![\psi]\!]_{\mathcal{M}}$: the denotation of ϕ in $\mathcal{M}$ with respect to the X-semantics is the same as the denotation of ψ in $\mathcal{M}$ with respect to the Y-semantics. Two standard ways to determine that X is *at least as expressive as* Y are: the Y-formulas are a sublanguage of the X-formulas (i); there is a translation (reduction) such that every Y-formula is logically equivalent to an X formula (ii). Logic X is *more expressive than* Y with respect to Z if X is at least as expressive as Y, but Y is not at least as expressive as X (the notion is a partial order). The standard way to determine that Y is not at least as expressive as X is, that there are an X-formula ϕ and two Z-models $(\mathcal{M}, s)$ and $(\mathcal{M}', s')$ such that ϕ is true in $(\mathcal{M}, s)$ and false in $(\mathcal{M}', s')$, but any Y-formula ψ is true in $(\mathcal{M}, s)$ iff ψ is true in $(\mathcal{M}', s')$. We then also say that the logic X, but not Y, can *distinguish* between the models $(\mathcal{M}, s)$ and $(\mathcal{M}', s')$.

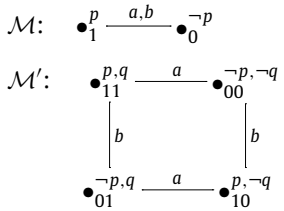
Known results are that *EL* is equally expressive as *PAL* [17], that in the single-agent situation *APAL* is equally expressive as *PAL*, and that in the multi-agent situation *APAL* is more expressive than *PAL* [4]. In this section we demonstrate that in the single-agent situation *GAL* is equally expressive as *EL*, and that in the multi-agent situation *GAL* is more expressive than *EL*, and *GAL* is not more expressive than *APAL*. We conjecture that *APAL* is not as least as expressive as (multi-agent) *GAL*.

Proposition 18. *For a single agent GAL is equally expressive as EL and PAL.*

Proof. Let a be the unique agent. For all ϕ in *GAL* we have that $\models [a]\phi \leftrightarrow \phi$, because in the single agent situation, each model is bisimilar to the restriction of that model to the a-equivalence class, from which directly follows that $\models [a]\phi \leftrightarrow \phi$. □

Theorem 19. *If $n \geqslant 2$, then GAL is more expressive than EL and PAL.*

Proof. *GAL* is obviously at least as expressive as *EL*. For the strictness part, consider the formula $\langle b\rangle K_a p$. Assume that there is an *EL* formula ψ equivalent to $\langle b\rangle K_a p$. Formula ψ can only contain a finite number of atoms. Let q be an atom not occurring in ψ. Consider the following models $\mathcal{M}$ and $\mathcal{M}'$ where a and b have common knowledge of their ignorance of p.

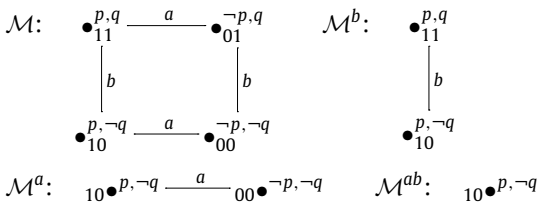


It is easy to see that $\mathcal{M}, 1 \not\models \langle b\rangle K_a p$, but that $\mathcal{M}', 11 \models \langle K_b q\rangle K_a p$, and thus that $\mathcal{M}', 11 \models \langle b\rangle K_a p$. On the other hand, $(\mathcal{M}, 1)$ and $(\mathcal{M}', 11)$ are bisimilar with respect to the epistemic language not including atom q, thus ψ cannot distinguish between these two pointed models. Therefore, ψ cannot be equivalent to $\langle b\rangle K_a p$. □

Theorem 20. *GAL is not at least as expressive as APAL.*

Proof. Consider the *APAL* formula $\Diamond(K_a p \wedge \neg K_b K_a p)$, and suppose there is an equivalent *GAL* formula χ. Assume an atomic proposition q not occurring in χ. We prove that the below pointed models $(\mathcal{M}, 10)$ and $(\mathcal{M}^a, 10)$ cannot be distinguished by any *GAL*-formula χ, whereas $\Diamond(K_a p \wedge \neg K_b K_a p)$ is true in the former but false in the latter, thus again deriving a contradiction.

The crucial insight is that in *GAL*, unlike in *APAL*, the *only* definable model restrictions of $\mathcal{M}, 10$ are the four below displayed models. And to make the formula $\Diamond(K_a p \wedge \neg K_b K_a p)$ true in $\mathcal{M}, 10$, one needs to be able to define the restriction with domain $\{11, 10, 00\}$. The formal proof is by induction on the structure of ψ, and is formulated in terms also involving other points of other model restrictions of $\mathcal{M}$; of that proof we only give the formal proposition and for state 10 the inductive cases for announcement and for group announcement.



Let $\psi \in \mathcal{L}_{gal}$ with $q \notin \Theta_\psi$. Then:

$$\mathcal{M}, 10 \models \psi \quad \Leftrightarrow \quad \mathcal{M}^a, 10 \models \psi \quad \Leftrightarrow \quad \mathcal{M}, 11 \models \psi \qquad \text{(i)}$$

$$\mathcal{M}^{ab}, 10 \models \psi \quad \Leftrightarrow \quad \mathcal{M}^b, 10 \models \psi \quad \Leftrightarrow \quad \mathcal{M}^b, 11 \models \psi \qquad \text{(ii)}$$

$$\mathcal{M}, 00 \models \psi \quad \Leftrightarrow \quad \mathcal{M}^a, 00 \models \psi \quad \Leftrightarrow \quad \mathcal{M}, 01 \models \psi \qquad \text{(iii)}$$

Inductive case announcement:

- $\mathcal{M}, 10 \models [\chi]\psi$

$$\text{iff } \mathcal{M}, 10 \models \chi \text{ implies } \mathcal{M}|\chi, 10 \models \psi \qquad (*)$$

$$\text{iff } \mathcal{M}, 10 \models \chi \text{ implies } \begin{cases} \mathcal{M}, 10 \models \psi & \text{if } \mathcal{M}, 00 \models \chi \\ \mathcal{M}^b, 10 \models \psi & \text{otherwise} \end{cases}$$

$$\text{iff } \mathcal{M}^a, 10 \models \chi \text{ implies } \begin{cases} \mathcal{M}^a, 10 \models \psi & \text{if } \mathcal{M}, 00 \models \chi \\ \mathcal{M}^{ab}, 10 \models \psi & \text{otherwise} \end{cases} \qquad (**)$$

$$\text{iff } \mathcal{M}^a, 10 \models \chi \text{ implies } \mathcal{M}^a|\chi, 10 \models \psi$$

$$\text{iff } \mathcal{M}^a, 10 \models [\chi]\psi.$$

$(*)$: By induction hypothesis: $\mathcal{M}|\chi = \mathcal{M}$ if $\mathcal{M}, 00 \models \chi$, and $\mathcal{M}|\chi = \mathcal{M}^b$ otherwise.
$(**)$: By induction hypothesis: $\mathcal{M}^a|\chi = \mathcal{M}^a$ if $\mathcal{M}^a, 00 \models \chi$, and $\mathcal{M}^a|\chi = \mathcal{M}^{ab}$ otherwise.

Inductive case group announcement (there are four different coalitions):

- $\mathcal{M}, 10 \models [\emptyset]\psi$
  iff $\mathcal{M}, 10 \models \psi$
- $\mathcal{M}, 10 \models [a]\psi$
  iff $\mathcal{M}, 10 \models \psi$ and $\mathcal{M}^a, 10 \models \psi$
  iff $\mathcal{M}^a, 10 \models \psi$ (by IH)
  iff $\mathcal{M}^a, 10 \models [a]\psi$
- $\mathcal{M}, 10 \models [b]\psi$
  iff $\mathcal{M}, 10 \models \psi$ and $\mathcal{M}^b, 10 \models \psi$
  iff $\mathcal{M}^a, 10 \models \psi$ and $\mathcal{M}^{ab}, 10 \models \psi$ (by IH)
  iff $\mathcal{M}^a, 10 \models [b]\psi$
- $\mathcal{M}, 10 \models [a, b]\psi$
  iff $\mathcal{M}, 10 \models \psi$ and $\mathcal{M}^a, 10 \models \psi$ and $\mathcal{M}^{ab}, 10 \models \psi$ and $\mathcal{M}^b, 10 \models \psi$
  iff $\mathcal{M}^a, 10 \models \psi$ and $\mathcal{M}^{ab}, 10 \models \psi$ (by IH)
  iff $\mathcal{M}^a, 10 \models [a, b]\psi$. □

Conjecture 21. *APAL is not at least as expressive as GAL.*

Thus, we conjecture that the two logics are incomparable when it comes to expressivity.

Now consider a very special model class $\mathfrak{M}_g$, namely the class where an agent g has the identity relation on all models (there may be other agents). It is clear that the announcement made by g has the property that $K_g\phi \leftrightarrow \phi$: everything is known by g. Therefore $\Diamond\phi$ in *APAL* is equivalent to $\langle g\rangle\phi$ in *GAL* (ignoring a further translation downward in ϕ). If we restrict the model class of the logic to $\mathfrak{M}_g$, we say that *a super agent g exists*. This makes clear that:

Proposition 22. *If a super agent g exists, GAL is at least as expressive as APAL.*

Proof. Given a $\phi \in \mathcal{L}_{apal}$, replace every occurrence of $\Box$ in ϕ by $[g]$. The resulting formula is in $\mathcal{L}_{gal}$. □

5. Model checking

If a given system can be modeled as a finite model, one would like to verify if a given property written in a language for specifying desired properties of systems holds in the finite model. We speak of the model checking problem, an area of automated deduction that has been addressed for almost all logical languages, for example modal logic [12], temporal logic [10], etc. There is a need, on the theoretical side, to provide a sound mathematical basis for the design of algorithms devoted to the model checking problem. Hence, the question arises whether the following decision problem is decidable:

input: A finite structure $\mathcal{M} = (S, \sim_1, \ldots, \sim_n, V)$, a state $x \in S$ and a formula $\phi \in \mathcal{L}_{gal}$,
output: Determine whether ϕ is satisfied at x in $\mathcal{M}$.

This decision problem, denoted (MC(GAL)) is a variant of the well-known model checking problem. If one restricts to formulas $\phi \in \mathcal{L}_{el}$, then the above decision problem is known to be P-complete. The notion of a formula like $[\{1, \ldots, n\}]\phi$ being satisfied in a structure $\mathcal{M} = (S, \sim_1, \ldots, \sim_n, V)$ at state $x \in S$ relies on the satisfiability of all (infinitely many) formulas like $[K_1\varphi_1 \wedge \cdots \wedge K_n\varphi_n]\phi$ at x where $\varphi_1, \ldots, \varphi_n \in \mathcal{L}_{el}$. In Theorem 24 we show that (MC(GAL)) is in PSPACE and in Theorem 25 we show that it is PSPACE-hard.

5.1. Preliminary results

Let $Z_{\mathcal{M}}$ be the greatest bisimulation relation on $\mathcal{M}$. Note that $Z_{\mathcal{M}}$ is an equivalence relation on S. For all $s \in S$, let $\|s\|$ be the equivalence class of s modulo $Z_{\mathcal{M}}$. The bisimulation contraction of $\mathcal{M}$ is the structure $\|\mathcal{M}\| = (S', \sim'_1, \ldots, \sim'_n, V')$ such that:

- $S' = S|_{Z_{\mathcal{M}}}$, i.e. the quotient of S modulo $Z_{\mathcal{M}}$,
- $\|s\| \sim'_i \|t\|$ iff there exist $v, w \in S$ such that $sZ_{\mathcal{M}}v$, $tZ_{\mathcal{M}}w$ and $v \sim_i w$,
- $V'(p) = V(p)|_{Z_{\mathcal{M}}}$.

The following proposition will be obvious, because:

- the bisimulation contraction is bisimilar to the original structure;
- bisimilar structures have the same logical theory [6];
- public announcement and group announcement are bisimulation preserving operations.

Proposition 23. *For all $\phi \in \mathcal{L}_{gal}$, $\|\mathcal{M}\|, \|x\| \models \phi$ iff $\mathcal{M}, x \models \phi$.*

In $\|\mathcal{M}\| = (S', \sim'_1, \ldots, \sim'_n, V')$, every $\|s\| \in S'$ can be distinguished by a pure epistemic formula from all other (non-bisimilar) states. Hence, for any $i \in \{1, \ldots, n\}$, each union $\mathcal{C}'_i$ of classes of equivalence for $\sim'_i$ is distinguished from all other (non-bisimilar) states by a pure epistemic formula of the form $K_i\phi_i$. Therefore, a pure epistemic formula of the form $\bigwedge_{i \in G} K_i\phi_i$ defines a restriction $\mathcal{M}'' = (S'', \sim''_1, \ldots, \sim''_n, V'')$ where $S'' = \bigcap_{i \in G} \mathcal{C}'_i$.

5.2. Model checking algorithm

Theorem 24. (MC(GAL)) *is in* PSPACE.

Proof. Since APTIME = PSPACE [9], it suffices to prove that (MC(GAL)) is in APTIME. Let us consider the alternating Algorithm 1. This algorithm takes as input a finite model $\mathcal{M}$, a state s in $\mathcal{M}$, a formula φ in $\mathcal{L}_{gal}$ and b in $\{0, 1\}$. It stops with a reject iff either $b = 0$ and $\mathcal{M}, s \models \varphi$ or $b = 1$ and $\mathcal{M}, s \not\models \varphi$ whereas it stops with an accept iff either $b = 0$ and $\mathcal{M}, s \not\models \varphi$ or $b = 1$ and $\mathcal{M}, s \models \varphi$. Its execution depends primarily on (φ, b). Each case is either existential or universal. For example, the case $(\varphi_1 \vee \varphi_2, 1)$ is existential. It is an accepting case iff for some $\varphi' \in \{\varphi_1, \varphi_2\}$, the case $(\varphi', 1)$ is accepting, thus corresponding to the fact that $\varphi_1 \vee \varphi_2$ is true at s in $\mathcal{M}$ iff for some $\varphi' \in \{\varphi_1, \varphi_2\}$, φ' is true at s in $\mathcal{M}$. As well, the case $(\varphi_1 \vee \varphi_2, 0)$ is universal. It is an accepting case iff for every $\varphi' \in \{\varphi_1, \varphi_2\}$, the case $(\varphi', 0)$ is accepting, thus corresponding to the fact that $\varphi_1 \vee \varphi_2$ is false at s in $\mathcal{M}$ iff for every $\varphi' \in \{\varphi_1, \varphi_2\}$, φ' is false at s in $\mathcal{M}$. Cases labelled with $(\cdot)$ are both existential and universal. Obviously,

- $sat(\mathcal{M}, s, \phi, 1)$ accepts iff $\mathcal{M}, s \models \phi$,
- $sat(\mathcal{M}, s, \phi, 1)$ rejects iff $\mathcal{M}, s \not\models \phi$,
- $sat(\mathcal{M}, s, \phi, 0)$ accepts iff $\mathcal{M}, s \not\models \phi$,
- $sat(\mathcal{M}, s, \phi, 0)$ rejects iff $\mathcal{M}, s \models \phi$.

The only difficult case is $([G]\phi, 1)$. Computing $\|\mathcal{M}\|$ is easy and by Proposition 23 we have that $\mathcal{M}, s \models \langle G\rangle\phi$ iff $\|\mathcal{M}\|, \|s\| \models \langle G\rangle\phi$. Then we just have to prove it in the case where $\|\mathcal{M}\| = \mathcal{M}$. Let us suppose it, and let us see that, if there is a definable

Algorithm 1 $sat(\mathcal{M}, s, \phi, b)$

case (ϕ, b) of
$(\cdot)$ $(p, 1)$: **if** $s \in V(p)$ **then** accept **else** reject;
$(\cdot)$ $(p, 0)$: **if** $s \in V(p)$ **then** reject **else** accept;
$(\cdot)$ $(\bot, 1)$: reject;
$(\cdot)$ $(\bot, 0)$: accept;
$(\cdot)$ $(\neg\phi', 1)$: $sat(\mathcal{M}, s, \phi', 0)$;
$(\cdot)$ $(\neg\phi', 0)$: $sat(\mathcal{M}, s, \phi', 1)$;
$(\exists)$ $(\phi_1 \vee \phi_2, 1)$: choose $\phi' \in \{\phi_1, \phi_2\}$; $sat(\mathcal{M}, s, \phi', 1)$;
$(\forall)$ $(\phi_1 \vee \phi_2, 0)$: choose $\phi' \in \{\phi_1, \phi_2\}$; $sat(\mathcal{M}, s, \phi', 0)$;
$(\forall)$ $(K_i\phi', 1)$: choose $t \in \sim_i(s)$; $sat(\mathcal{M}, t, \phi', 1)$;
$(\exists)$ $(K_i\phi', 0)$: choose $t \in \sim_i(x)$; $sat(\mathcal{M}, t, \phi', 0)$;
$(\cdot)$ $([\phi_1]\phi_2, 1)$: compute the ϕ_1-definable restriction $\mathcal{M}' = (S', \sim_1, \ldots, \sim_n, V')$ of $\mathcal{M}$;
if $s \in S'$ **then** $sat(\mathcal{M}', s, \phi_2, 1)$ **else** accept;
$(\cdot)$ $([\phi_1]\phi_2, 0)$: compute the ϕ_1-definable restriction $\mathcal{M}' = (S', \sim_1, \ldots, \sim_n, V')$ of $\mathcal{M}$;
if $s \in S'$ **then** $sat(\mathcal{M}', s, \phi_2, 0)$ **else** reject;
$(\forall)$ $([G]\phi, 1)$: Compute $\|\mathcal{M}\|$, choose a definable restriction $\mathcal{M}'' = (S'', \sim''_1, \ldots, \sim''_n, V'')$
of $\|\mathcal{M}\|$ s.t. $S'' = \bigcap_{i\in G} \mathcal{C}_i$ where $\mathcal{C}_i$ are unions of classes of equivalence for $\sim'_i$;
if $s \in S''$ **then** $sat(\mathcal{M}'', s, \phi, 1)$ **else** accept;
$(\exists)$ $([G]\phi, 0)$: Compute $\|\mathcal{M}\|$, choose a definable restriction $\mathcal{M}'' = (S'', \sim''_1, \ldots, \sim''_n, V'')$
of $\|\mathcal{M}\|$ s.t. $S'' = \bigcap_{i\in G} \mathcal{C}_i$ where $\mathcal{C}_i$ are unions of classes of equivalence for $\sim'_i$;
if $s \in S''$ **then** $sat(\mathcal{M}'', s, \phi, 0)$ **else** reject;
end case

restriction $\mathcal{M}'' = (S'', \sim''_1, \ldots, \sim''_n, V')$ of $\mathcal{M}$ such that $S'' = \bigcap_{i\in G} \mathcal{C}_i$ where $\mathcal{C}_i$ are unions of classes of equivalence for $\sim_i$, if also $s \in S''$ and $\mathcal{M}', s \models \phi$, then $\mathcal{M}, s \models \langle G\rangle\phi$. Let us then suppose the first part of the implication.

$\mathcal{M}$ is supposed to be bisimulation-contracted, then we know that for all $s \in \mathcal{M}$, there is $\phi_s \in \mathcal{L}_{gal}$, s.t. for all $t \in \mathcal{M}$, $\mathcal{M}, t \models \phi_s$ iff $s = t$. It implies that $s \in S''$ iff (for all $i \in G$, $s \in \mathcal{C}_i$) iff $\mathcal{M}, s \models \bigwedge_{i\in G}(\bigvee_{t\in\mathcal{C}_i} \phi_t)$ which is equivalent to $\mathcal{M}, s \models \bigwedge_{i\in G} K_i(\bigvee_{t\in\mathcal{C}_i} \phi_t)$. That means that $\mathcal{M}'' = \mathcal{M}|\bigwedge_{i\in G} K_i(\bigvee_{t\in\mathcal{C}_i} \phi_t)$ and then $\mathcal{M}, s \models \langle\bigwedge_{i\in G} K_i(\bigvee_{t\in\mathcal{C}_i} \phi_t)\rangle\phi$ (because $s \in S''$ and $\mathcal{M}', s \models \phi$). We obtain $\mathcal{M}, s \models \langle G\rangle\phi$.

Since *sat* can be implemented in polynomial time, (MC(GAL)) is in APTIME. □

Theorem 25. (MC(GAL)) *is* PSPACE-*hard.*

Proof. We prove that (MC(GAL)) is PSPACE-hard. Let $\Psi = Q_1x_1 \ldots Q_kx_k\Phi(x_1, \ldots, x_k)$ be an entry of the problem QBF-SAT:

- $Q_1, \ldots, Q_k \in \{\forall, \exists\}$,
- $x_1, \ldots, x_k$ are Boolean variables,
- $\Phi(x_1, \ldots, x_k)$ is a Boolean formula.

We will associate to Ψ a model $\mathcal{M}_{1;k} = (W_{1;k}, \mathcal{R}_1, \ldots, \mathcal{R}_k, V)$, a world $x \in W_k$ and a formula $\psi(\Psi) \in \mathcal{L}_{gal}$ such that $\models \Psi$ iff $\mathcal{M}_{1;k}, x \models \psi(\Psi)$ (P_k).

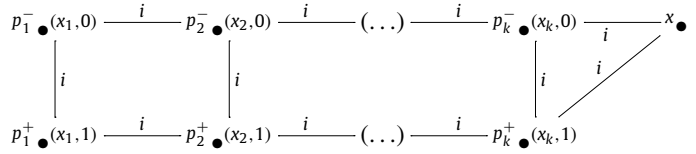
Let $1 \leqslant m \leqslant k$, $W_{m;k} = \{x\} \cup \{(x_l, 0), (x_l, 1)\}_{l\in\{m,\ldots,k\}}$ be the set of possible worlds, $\{p_m^-, p_m^+, \ldots, p_k^-, p_k^+\}$ be the set of atoms, with $V(p_l^-) = \{(x_l, 0)\}$ and $V(p_l^+) = \{(x_l, 1)\}$.

Let $i, g \in N$ and let us define

$$\begin{cases} \mathcal{R}_i = W_{m;k} \times W_{m;k}, \\ \mathcal{R}_g = \{(s, s) \text{ such that } s \in W_{m;k}\}. \end{cases}$$

(Note that g is omniscient and that i assumes this fact.)

$\mathcal{M}_{1;k}$:



(Note that i's relation is reflexive, symmetrical and transitive, and that g's reflexive arrows are omitted.)

Let us now define some formulae:

$$\text{for all } l \in \{1, \ldots, k\},\ q_l = \hat{K}_i(p_l^- \wedge K_i\neg p_l^+) \vee \hat{K}_i(p_l^+ \wedge K_i\neg p_l^-) \text{ and } r_l = \hat{K}_i p_l^+ \wedge \hat{K}_i p_l^-.$$

Intuitively, $\mathcal{M}_{1,k} \models r_l$ means that $(x_l, 0)$ and $(x_l, 1)$ are still possible worlds of the model (i.e. the truth value of x_l is not fixed) and $\mathcal{M}_{1,k} \models q_l$ means that one and only one of $(x_l, 0)$ and $(x_l, 1)$ is still a possible world (i.e. we have fixed the value of x_l).

We can now define the equivalence recursively:
Let $\psi_0 = \Phi(\hat{K}_i p_1^+, \ldots, \hat{K}_i p_k^+)$, suppose ψ_l is defined for some $l < k$, then

$$\psi_{l+1} = \begin{cases} K_i[g](q_1 \wedge \cdots \wedge q_{k-l} \wedge r_{k-l+1} \wedge \cdots \wedge r_k \rightarrow \psi_l) & \text{if } Q_{l+1} = \forall, \\ \hat{K}_i\langle g\rangle(q_1 \wedge \cdots \wedge q_{k-l} \wedge r_{k-l+1} \wedge \cdots \wedge r_k \wedge \psi_l) & \text{if } Q_{l+1} = \exists. \end{cases}$$

Finally, $\psi(\Psi) = \psi_k$.

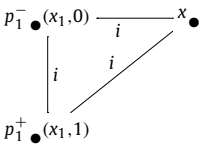
Example. If $\Psi = \forall x_1, \exists x_2, \forall x_3, \Phi(x_1, x_2, x_3)$ then:

$$\psi(\Psi) = K_i[g]\big(q_1 \wedge r_2 \wedge r_3 \rightarrow \hat{K}_i\langle g\rangle\big(q_1 \wedge q_2 \wedge r_3 \wedge K_i[g]\big(q_1 \wedge q_2 \wedge q_3 \rightarrow \Phi\big(\hat{K}_i p_1^+, \ldots, \hat{K}_i p_k^+\big)\big)\big)\big).$$

Intuitively, $K_i[g](q_1 \wedge r_2 \wedge r_3 \rightarrow \phi)$ means "After having fixed the value of x_1 only, ϕ" and $\hat{K}_i\langle g\rangle(q_1 \wedge r_2 \wedge r_3 \wedge \phi)$ as "There is a way of fixing the value of x_1 only, such that ϕ". We can now prove $\models \Psi \Leftrightarrow \mathcal{M}_{1;k}, x \models \psi(\Psi)$ by induction on k. The induction is quite technical, but the intuition is that something is true after having fixed the value of $k+1$ boolean variables if and only if it is true after having fixed the value of the first k variables, added the final one and then fixed its value. More precisely:

Base case: $k = 1$:

$\Psi = Q_1 x_1 \Phi(x_1)$, and $\mathcal{M}_1$:



- If $Q_1 = \forall$ then $\models \Psi$ iff ($\models \Phi(\top)$ and $\models \Phi(\bot)$) iff ($\models \Phi(\top) \leftrightarrow \top$ and $\models \Phi(\bot) \leftrightarrow \top$)
  iff ($p_1^+ \overset{i}{\bullet\!\!-\!\!\bullet}^x \models \Phi(\hat{K}_i p_1^+)$ and $p_1^- \overset{i}{\bullet\!\!-\!\!\bullet}^x \models \Phi(\hat{K}_i p_1^+)$)
  iff $\mathcal{M}_1, x \models K_i[g](q_1 \rightarrow \Phi(\hat{K}_i p_1^+))$, i.e. $\mathcal{M}_1, x \models \psi(\Psi)$
- Else, $Q_1 = \exists$ and $\models \Psi$ iff ($\models \Phi(\top) \vee \Phi(\bot)$) iff ($\models \Phi(\top) \leftrightarrow \top$ or $\models \Phi(\bot) \leftrightarrow \top$)
  iff ($p_1^+ \overset{i}{\bullet\!\!-\!\!\bullet}^x \models \Phi(\hat{K}_i p_1^+)$ or $p_1^- \overset{i}{\bullet\!\!-\!\!\bullet}^x \models \Phi(\hat{K}_i p_1^+)$)
  iff $\mathcal{M}_1, x \models \hat{K}_i\langle g\rangle(q_1 \wedge \Phi(\hat{K}_i p_1^+))$ i.e. $\mathcal{M}_1, x \models \psi(\Psi)$

Inductive case: $k \rightarrow k+1$:
Suppose that (P_k) is true, and let us note: $\Psi = Q_1 x_1 \ldots Q_k x_k Q_{k+1} x_{k+1} \Phi(x_1, \ldots, x_k, x_{k+1})$.
Then we have: $\models \Psi \Leftrightarrow \models Q_1 x_1 \underbrace{Q_2 x_2 \ldots Q_k x_k Q_{k+1} x_{k+1} \Phi(x_1, \ldots, x_k, x_{k+1})}_{\tilde{\Psi}(x_1)}$

- If $Q_1 = \forall$ then $\models \Psi$ iff ($\models \tilde{\Psi}(\top)$ and $\models \tilde{\Psi}(\bot)$)
  iff $\mathcal{M}_{2;k+1}, x \models \psi(\tilde{\Psi}(\top))$ and $\mathcal{M}_{2;k+1}, x \models \psi(\tilde{\Psi}(\bot))$ (by IH)
  iff $\mathcal{M}_{1;k+1}, x \models K_i[g](q_1 \wedge r_2 \wedge \cdots \wedge r_{k+1} \rightarrow \psi^*(\tilde{\Psi}(\hat{K}_i p_1^+)))$
  with ψ^* obtained by replacing any succession $q_2 \wedge \cdots$ by $q_1 \wedge q_2 \wedge \cdots$
- If $Q_1 = \exists$ then $\models \Psi$ iff ($\models \tilde{\Psi}(\top)$ or $\models \tilde{\Psi}(\bot)$)
  iff $\mathcal{M}_{2;k+1}, x \models \psi(\tilde{\Psi}(\top))$ or $\mathcal{M}_{2;k+1}, x \models \psi(\tilde{\Psi}(\bot))$ (by IH)
  iff $\mathcal{M}_{1;k+1}, x \models \hat{K}_i\langle g\rangle(q_1 \wedge r_2 \wedge \cdots \wedge r_{k+1} \wedge \psi^*(\tilde{\Psi}(\hat{K}_i p_1^+)))$

Agent g's announcement is just like a public announcement. Therefore, the same proof shows hat the model checking for *APAL* is PSPACE hard, namely by replacing $[g]$ by $\Box$, and $\langle g\rangle$ by $\Diamond$, above. □

We observe that our results also extend to *APAL*: the model checking problem for arbitrary public announcement logic is also PSPACE-complete. A relevant detail in the proof of Theorem 25 is that it involves an omniscient agent g, and that the role of $[g]$ is in *APAL* played by $\Box$, and that of $\langle g\rangle$ by $\Diamond$. (See also the expressivity result involving g, Proposition 22.)

6. Announcements and ability

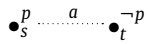
Our initial intuitive interpretation of a formula of the form $\langle C\rangle\phi$ was that coalition C has the ability to make ϕ come about by making some public announcement. We now have a better understanding of group announcement logic; let us discuss to what extent that intuition is precise.

Recent work on strategy logics have illuminated the fact that there are many subtly different notions of ability in the context of incomplete information [13,15,1,14] (see [14] for a recent summary). For example, does ability entail knowledge of ability? In [14, p. 433] three levels of ability in general strategy logics are discussed. We now discuss counterparts of these in the special context of truthful public announcements. In general strategy logics, such as ATL or STIT, agents and coalitions can perform arbitrary state-transforming actions. In our setting the actions are truthful *announcements*, and there is thus an intimate relationship between knowledge and ability. There are two main questions of interest related to the mentioned different variants of ability here: are they indeed different in this special context, and are they expressible in the logical language of *GAL*?

6.1. Singleton coalitions

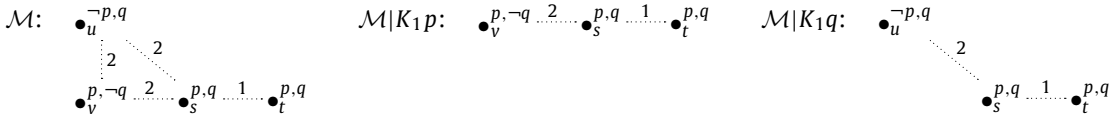
For simplicity we first consider a singleton coalition $\{a\}$. What does it mean that agent a has the ability to make a goal ϕ come about by making a public announcement? Let us begin with the weakest form of ability.

Being able to, but not necessarily knowing it. The formula $\langle a\rangle\phi$ means that there is something which a knows, and if the fact that a knows it is announced, ϕ is a consequence. However, it might be the case that *a doesn't know this*, i.e., that $K_a\langle a\rangle\phi$ is not true. As an example, first observe that $\langle K_a\psi_a\rangle\phi \to K_a\langle K_a\psi_a\rangle\phi$ is not a principle of public announcement logic. As a counterexample take state s of the following model



and take $\psi_a = \top$ and $\phi = p$. However, this does not mean that a cannot achieve ϕ in all her accessible states by some *other* announcements (possibly different ones in different states). But in group announcement logic, we have in the model above that $s \models \langle a\rangle p$ (a can announce $K_a\top$), but $t \not\models \langle a\rangle p$ and thus, $s \models \neg K_a\langle a\rangle p$. So, $\langle a\rangle\phi \to K_a\langle a\rangle\phi$ is not a principle of group announcement logic. This is a first illustration of the fact that we must be careful when using the term 'ability': in some (but not necessarily all) circumstances it might be counter-intuitive to say that a has the ability make ϕ come about, when she is not aware that she is; when she cannot discern between the actual situation and a situation in which she does not have this ability.

Being able to, knowing that, but not knowing how. Consider the following model $\mathcal{M}$ (some model updates are also shown):



and let

$$\phi = K_2 q \wedge \big(\neg K_2 p \vee \hat{K}_1(K_2 p \wedge \neg K_2 q)\big).$$

If we take the current state to be s, we have a situation where 1 is able to make ϕ come about and where she in addition knows this; a stronger type of ability than in the example above. Formally: $s \models \langle 1\rangle\phi$, because $s \models \langle K_1 q\rangle\phi$, and $t \models \langle 1\rangle\phi$ because $t \models \langle K_1 p\rangle\phi$. Thus, $s \models K_1\langle 1\rangle\phi$. However, we argue, it might still be counter-intuitive to say that 1 can make ϕ come about in this situation. The reason is that she has to use *different announcements in indiscernible states*. Observe that $s \models \langle K_1 p\rangle\neg\phi$ and $t \models \langle K_1 q\rangle\neg\phi$: while the same announcements can be made in both states, they don't have the same consequences. In fact, there exists *no* single announcement agent 1 can make which will ensure that ϕ will be true in both s and t. To see this, we can enumerate the possible models resulting from 1 making an announcement in s or t. Because such a model must include 1's equivalence class $\{s, t\}$, there are four possibilities. First, the starting model itself (e.g., 1 announces a tautology), in which ϕ does not hold in s. Second, the model where only state u is removed (e.g., 1 announces $K_1 p$), in which ϕ does not hold in s (as we saw above). Third, the model where only state v is removed (e.g., 1 announces $K_1 q$), in which ϕ does not hold in t (as we saw above). Fourth, the model where both u and v are removed, in which ϕ holds in neither s nor t.

Since agent 1 cannot discern state s from state t, she has the ability to make ϕ come about only in the sense that she depends on guessing the correct announcement. In other words, she can make ϕ come about, knows that she can make ϕ come about, but does not know *how* to make ϕ come about.

Being able to, knowing that, knowing how. Thus, we can formulate a strong notion of the ability of a to achieve ϕ by public announcements: there exists a formula ψ such that a knows ψ and in any state a considers possible, $\langle K_a\psi\rangle\phi$ holds.

Compare this version of ability, "there is an announcement which a knows will achieve the goal", with the previous version above, "a knows that there is an announcement which will achieve the goal". We can call these notions, respectively, *knowing de re* and *knowing de dicto* that the goal can be achieved, following [15] who use the same terminology for general strategy logics, after the corresponding notion used in quantified modal logic. In our framework these notions are more formally defined as follows:

Knowledge de dicto: Agent i knows *de dicto* that she can achieve the goal ϕ in state s of model $\mathcal{M}$ iff

$$\forall t \sim_i s \; \exists \psi \in \mathcal{L}_{el} \; (\mathcal{M}, t) \models \langle K_i \psi \rangle \phi. \tag{1}$$

Knowledge de re: Agent i knows *de re* that she can achieve the goal ϕ in state s of model $\mathcal{M}$ iff

$$\exists \psi \in \mathcal{L}_{el} \; \forall t \sim_i s \; (\mathcal{M}, t) \models \langle K_i \psi \rangle \phi. \tag{2}$$

Note, however, that it is not prima facie clear that there is a distinction between these notions in *GAL*, because of the intimate interaction between knowledge and possible actions (announcements), but the model and formula above show that there indeed is.

We have seen how to express knowledge *de dicto*. In the most popular general strategy logics such as ATL, where actions are not necessarily truthful announcements, extended with epistemics, knowledge *de re* is not expressible. Several recent works have focused on extending such logics in order to be able to express knowledge *de re* and other interaction properties between knowledge and ability [15,1,14,7]. In the special case of *GAL*, however, it turns out that knowledge *de re* in fact *is* already expressible (in the single agent case, at least), as the following proposition shows.

Proposition 26.

1. *Knowledge de dicto* (1) *is expressed by the formula* $K_i \langle i \rangle \phi$.
2. *Knowledge de re* (2) *is expressed by the formula* $\langle i \rangle K_i \phi$.

Proof.

1. Immediate.
2. Let $\mathcal{M}$ be a model and s a state in $\mathcal{M}$. Agent i knows *de re* that she can achieve ϕ iff $\exists \psi \in \mathcal{L}_{el}((\mathcal{M}, s) \models K_i \psi$ and $\forall t \in S \; (s \sim_i t \Rightarrow (\mathcal{M}, t) \models \langle K_i \psi \rangle \phi))$ iff $\exists \psi \in \mathcal{L}_{el}((\mathcal{M}, s) \models K_i \psi$ and $\forall t \in S \; (s \sim_i t \Rightarrow (\mathcal{M}, t) \models K_i \psi$ and $\mathcal{M}|K_i \psi, t \models \phi))$ iff, since $\mathcal{M}, s \models K_i \psi$ and $s \sim_i t$ implies that $\mathcal{M}, t \models K_i \psi$, $\exists \psi \in \mathcal{L}_{el}((\mathcal{M}, s) \models K_i \psi$ and $\forall t \in S \; (s \sim_i t \Rightarrow \mathcal{M}|K_i \psi, t \models \phi))$ iff $\exists \psi \in \mathcal{L}_{el}((\mathcal{M}, s) \models K_i \psi$ and $\forall t \in S \; (\mathcal{M}, t \models K_i \psi$ and $(s \sim_i t \Rightarrow \mathcal{M}|K_i \psi, t \models \phi)))$ iff, again since $\mathcal{M}, s \models K_i \psi$ and $s \sim_i t$ implies that $\mathcal{M}, t \models K_i \psi$, $\exists \psi \in \mathcal{L}_{el}((\mathcal{M}, s) \models K_i \psi$ and $\forall t \in S \; (\mathcal{M}, t \models K_i \psi$ and $((\mathcal{M}, t \models K_i \psi$ and $s \sim_i t) \Rightarrow \mathcal{M}|K_i \psi, t \models \phi)))$ iff $\exists \psi \in \mathcal{L}_{el}((\mathcal{M}, s) \models K_i \psi$ and $\mathcal{M}|K_i \psi, s \models K_i \phi)$ iff $(\mathcal{M}, s) \models \langle i \rangle K_i \phi$. □

Thus, i knows *de re* that she can achieve ϕ iff she can achieve the fact that she knows ϕ. This depends crucially on the fact that by 'achieve' we mean achieve by truthful public announcements; it is not true if we allow general actions. As an illustration of the latter case, take the following example. An agent i is in front of a combination lock safe. The agent does not know the combination. The available actions correspond to dialing different codes. The agent is *able* to open the safe, $\langle i \rangle open$, because there is a successful action (dial the correct code). She knows *de dicto* that she can open the safe, $K_i \langle i \rangle open$, because this is true in all the states she considers possible (a possible state correspond to a possible correct code). But she does not know *de re* that she can open the safe, because there is no code that will open the safe in all the states she considers possible. However, $\langle i \rangle K_i open$ *does* hold: there is some action she can perform (dial the correct code) after which she will know that the safe is open. In *GAL*, the fact that $\langle i \rangle K_i \phi$ expresses (2) is a result of the inter-dependence between knowledge and actions (announcements) and the S5 properties of knowledge. The following are some properties of knowledge *de dicto* and *de re* in *GAL*.

Proposition 27. *The following are valid.*

1. $K_i \langle i \rangle \phi \rightarrow \langle i \rangle \phi$. *Knowledge de dicto of ability implies ability*; *if you know that you can do it then you can do it.*
2. $\langle i \rangle K_i \phi \rightarrow K_i \langle i \rangle \phi$. *Knowledge de re implies knowledge de dicto*; *if you know how to do it you know that you can do it.*
3. $\langle i \rangle K_i \phi \leftrightarrow K_i \langle i \rangle K_i \phi$. *Knowledge de re holds iff knowledge of knowledge de re holds*; *you know how to do it iff you know that.*

Proof. The first point is immediate from reflexivity of the accessibility relations. The second point is also immediate; let ψ be fixed by (2). For the third point, the direction to the left is immediate by point 1, so consider the direction to the right. Assume that $\mathcal{M}, s \models \langle i \rangle K_i \phi$, i.e., that (2) holds. Let $u \sim_i s$. We must show that $\exists \psi \in \mathcal{L}_{el} \; \forall t \sim_i u \; (\mathcal{M}, t) \models \langle K_i \psi \rangle \phi$. Let ψ be as in (2), and let $t \sim_i u$. By transitivity of $\sim_i$ we have that $t \sim_i s$, and thus that $(\mathcal{M}, t) \models \langle K_i \psi \rangle \phi$ by (2). □

On first sight the expression $\langle i \rangle K_i \phi$ of knowledge *de re* might seem to suffer from a similar problem as the expression of 'mere' ability of the first type we discussed above, $\langle i \rangle \psi$, namely that while i has the ability to make ψ come about she does not necessarily know this (*de dicto*). However, as the last point in the proposition above shows, if ψ is of the special form $K_i \phi$ (for the *same* agent i), then ability does in fact imply knowledge of ability. In every circumstance where you can achieve a state where you know ϕ, you know that you can.

As illustrated above, the other direction of the second property in Proposition 27 does not hold; knowledge *de dicto* does not imply knowledge *de re*. Given our expressions of these two properties, we thus have that

$K_i\langle i\rangle\phi \rightarrow \langle i\rangle K_i\phi$ is not valid

that you know that you can achieve ϕ does not necessarily mean that you can achieve a state where you know ϕ.

6.2. More than one agent

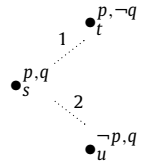
In the case of more than one agent, there are even more subtleties. In particular, what does it mean that a group knows how to achieve something, i.e., knows which joint announcement will be effective? That everybody knows it? That they have common knowledge of it?

In [15] it is argued that the answer depends on the situation. It might be the case that the agents have common knowledge (although they then need some resolution mechanism for cases when there are more than one effective announcement, in order to coordinate); that every agent knows the effective announcement; that the agents have distributed knowledge about the effective announcement and thus can pool their knowledge together to find out what they should do; that a particular agent (the 'leader') knows the effective announcement and can communicate it to the others.

In *GAL* we do not have distributed or common knowledge in the language, but "everybody knows" can be defined: $E_G\phi \equiv \bigwedge_{i\in G} K_i\phi$, where G is a coalition. The following generalization of (2) says that in state s coalition G can make a truthful announcement which all the members of G know will achieve the goal ϕ:

$$\exists\{\psi_i\}_{i\in G} \subseteq \mathcal{L}_{el} \quad \forall(t,s) \in \bigcup_{i\in G} \sim_i (\mathcal{M},t) \models \left\langle \bigwedge_{i\in G} K_i\psi_i \right\rangle \phi. \tag{3}$$

However, while the single agent case (2) is expressed by $\langle i\rangle K_i\phi$, it is *not* in general the case that (3) is expressed by $\langle G\rangle E_G\phi$. The following is a counterexample. Let $\mathcal{M}$ and ϕ be the following model and formula.



$\phi = p \wedge q$

Let $G = \{1,2\}$. It is easy to see that group G in s does not know *de re* that they can achieve ϕ in the sense of (3): it would imply, for instance, that it is possible to make an announcement in state t which at the same time eliminates state t – which is impossible. However, $\langle 1,2\rangle E_G\phi$ holds in s – $\{1,2\}$ can announce $K_1p \wedge K_2q$.

Let us consider distributed and common knowledge. Assume for a moment that the language is extended with operators C_G and D_G where G is a coalition, such that $\mathcal{M},s \models D_G\phi$ iff for all $(s,t) \in \bigcap_{i\in G} \sim_i \mathcal{M},t \models \phi$ and $M,s \models C_G\phi$ iff for all $(s,t) \in \sim_G{}^*\mathcal{M},t \models \phi$, where $\sim_G{}^*$ is the reflexive transitive closure of $\bigcup_{i\in G} \sim_i$. The following version of (3) says that in s, G can make a truthful announcement which G distributively know will achieve the goal ϕ:

$$\exists\{\psi_i\}_{i\in G} \subseteq \mathcal{L}_{el} \quad \forall t \in S\left((s,t) \in \bigcap_{i\in G} \sim_i \Rightarrow (\mathcal{M},t) \models \left\langle \bigwedge_{i\in G} K_i\psi_i \right\rangle \phi\right). \tag{4}$$

Contrary to the case for "everybody knows", this property *is* in fact expressed by the analogue to the expression for the single-agent case (can be shown similarly to Proposition 27 – observe that $(s,t) \in \bigcap_{i\in G}$ and $\mathcal{M},s \models \bigwedge_{i\in G} K_i\psi_i$ implies that $\mathcal{M},t \models \bigwedge_{i\in G} K_i\psi_i$):

Proposition 28. *The property (4) is expressed by the formula* $\langle G\rangle D_G\phi$.

The situation for common knowledge is, however, similar to that of "everybody knows". The following version of (4) says that in s G can make a truthful announcement which G commonly know will achieve the goal ϕ:

$$\exists\{\psi_i\}_{i\in G} \subseteq \mathcal{L}_{el} \quad \forall t \sim_G{}^* s(\mathcal{M},t) \models \left\langle \bigwedge_{i\in G} K_i\psi_i \right\rangle \phi. \tag{5}$$

The model $\mathcal{M}$, formula ϕ and coalition $G = \{1,2\}$ above is a counterexample showing that (5) is not expressed by $\langle G\rangle C_G\phi$: (5) does not hold in state s, but $\mathcal{M},s \models \langle G\rangle C_G\phi$.

Summing up, it can be argued that *all* of the different notions of ability discussed in this section are *useful*. For example, in different contexts it might be useful to reason about what an agent can achieve by *guessing* the right actions to perform, while in others what she can achieve by *identifying* the correct actions with certainty. It is, however, of vital importance to discern between these different notions, for example in the analysis of security protocols.

7. Security protocols

Consider a sender and a receiver attempt to communicate a secret to each other without an eavesdropper learning it. A very powerful eavesdropper is one that intercepts all communications. This creates the setting where sender, receiver, and eavesdropper are three agents that can be modelled in a multi-S5 system and where all communications are public announcements by sender and receiver. One specific example of such a setting is known as the Russian Cards Problem [19]. The setting is one where a pack of all different cards are distributed over the three 'players', where every player only knows his own cards, where sender and receiver have an informational advantage over the eavesdropper because they hold more cards, and where the 'secrets' that should not be divulged are about card ownership. Posed as a riddle it looks as follows – Anne and Bill are sender and receiver, Cath the eavesdropper:

> From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ Anne and Bill each draw three cards and Cath gets the remaining card. How can Anne and Bill openly (publicly) inform each other about their cards, without Cath learning from any of their cards who holds it?

To simplify matters, assume that Anne has drawn $\{0, 1, 2\}$, that Bill has drawn $\{3, 4, 5\}$ and that Cath therefore has card 6. The initial Kripke model $\mathcal{D}$ describing this setting consists of all possible card deals (valuations). In that model an epistemic class for an agent can be identified with the hand of cards of that agent. For example, given that Anne holds $\{0, 1, 2\}$, she cannot distinguish the four deals – allow us to use some suggestive notation – 012.345.6, 012.346.5, 012.356.4, and 012.456.3 from one another.

Given that all announcements that can be made by a player are known by that player, they consist of unions of equivalence classes for that player and can therefore be identified with sets of alternative hands for that player. One solution is where

> Anne says "My hand of cards is one of $012, 034, 056, 135, 246$" after which Bill says "My hand of cards is one of $345, 125, 024$."

The last is equivalent in that information state to Bill saying "Cath has card 6". Anne and Bill in fact execute a protocol here, not in the sense of sets of sequences of announcements but in the sense of functions from local states of agents to nondeterministic choice between announcements. For example, Anne is executing "given cards i, j, k, the first of my five hands is that actual hand ijk; the second of my five hands to announce is ikl where k, l are chosen from the five remaining cards; the third is imn where m, n are the remaining two cards; etc.; shuffle the hands before announcing them."

We can describe this solution in logic. Agent a stands for Anne, b for Bill, and c for Cath. Let q_i stand for 'agent i holds card q' and let klm_i stand for $k_i \wedge l_i \wedge m_i$. The information and safety requirements are as follows – the conjunction in the formula suggests a conjunction over all hands of cards, 'Cath does not learn any card' means 'Cath does not learn the ownership of any card except her own card.'

Anne learns Bill's cards	$\bigwedge_{ijk}(ijk_b \to K_a ijk_b)$	(*one*)
Bill learns Anne's cards	$\bigwedge_{ijk}(ijk_a \to K_b ijk_a)$	(*two*)
Cath does not learn any card	$\bigwedge_{q=0}^{6}((q_a \to \neg K_c q_a) \wedge (q_b \to \neg K_c q_b))$	(*three*)

These requirements should hold throughout the model after protocol completion (i.e., they should be common knowledge between Ann and Bill). The safety requirement should be satisfied both at the end and in all intermediate stages: after any announcement that forms part of such a protocol.

All protocols are finite, because the model is finite and all informative announcements result in proper model restriction. But it is unclear how long such protocols need to be. The above solution was of length two, but settings that require strictly longer protocols are also known. The uncertain but finite length cannot be described in public announcement logic, but it can be described in group announcement logic. The diamond in $\langle ab\rangle\phi$ refers to arbitrarily finite length protocols taking place between sender a and receiver b in the presence of other agents, such as the eavesdropper, as was discussed in Section 3.3.2.

Let us see how this works for the length-two protocol above that solves the Russian Cards Problem. First, we model the solution in public announcement logic. In the solution, first Anne announces $012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a$ (*anne*). Then Bill announces $345_b \vee 125_b \vee 024_b$ (*bill*). After these two announcements the solution requirements are satisfied. This can now be described in various ways: as a sequence of two announcements by different agents, as a sequence of two simultaneous announcements by Anne and Bill, or as a single announcement by Anne and Bill.

$$\mathcal{D}, 012.345.6 \models \langle K_a anne\rangle\langle K_b bill\rangle(one \wedge two \wedge three)$$

$$\mathcal{D}, 012.345.6 \models \langle K_a anne \wedge K_b\top\rangle\langle K_a\top \wedge K_b bill\rangle(one \wedge two \wedge three)$$

$$\mathcal{D}, 012.345.6 \models \langle K_a(anne \wedge [K_a anne \wedge K_b\top]\top) \wedge K_b(\top \wedge [K_a anne \wedge K_b\top]bill)\rangle(one \wedge two \wedge three)$$

The last one implies that we have, in this case:

$$\mathcal{D}, 012.345.6 \models \langle ab \rangle (one \wedge two \wedge three)$$

Given that we should be able to realize the three postconditions after any execution of the underlying protocol, and regardless of the initial card deal, the existence of a successful protocol to realize them can be expressed all at once by the model validity

$$\mathcal{D} \models \langle ab \rangle (one \wedge two \wedge three)$$

or in other words

"$\langle ab \rangle (one \wedge two \wedge three)$ *is* valid in the initial model for card deals" (6)

In principle, we can now model check this formula in that model, thus establishing that a secure exchange is possible under the uncertainty conditions about card ownership in a fully automated way.

We have so far overlooked one aspect of the meaning of announcements executing such protocols. The security requirement *three* should be an invariant: its validity throughout the model should be preserved after every good announcement. In this particular case we can enforce that, because its negation is a positive formula: if it is ever not preserved, then it is lost forever afterwards. Therefore, it suffices to guarantee it after the execution of the protocol. Thus the above expression also incorporates that invariance.

One must be careful when interpreting the meaning the existence of sequences of announcements. If we can replace the two successive announcements: Anne says "My hand of cards is one of 012, 034, 056, 135, 246" after which Bill says "My hand of cards is one of 345, 125, 024", by a single one, does that not mean that all protocols can be reduced to length 1? And what would in this case that single simultaneous announcement be? Well: as both agents are announcing facts and not knowledge, their single announcement is simply the conjunction of their successive announcements. As the second one for Anne and the first one for Bill was 'true' (vacuous), this means that they could *simultaneously* have made their successive announcements: Anne says "My hand of cards is one of 012, 034, 056, 135, 246" and simultaneously Bill says "My hand of cards is one of 345, 125, 024". Unfortunately, even though this indeed solves the problem, the agents do not know the public consequences of their joint action merely from the public consequences of their individual part in it. This situation was discussed in the previous section: there *is* a simultaneous announcement by Ann and Bill which will achieve the goal, but Ann and Bill do not *know* that their respective announcements will achieve the goal – they will not achieve the goal in all the states they consider possible. A different execution of the protocol for Anne, when she holds cards $\{0, 1, 2\}$, is the announcement "My hand of cards is one of 012, 035, 046, 134, 256". From that with Bill's above announcement Cath can deduce straightaway that the card deal is 012.345.6. And, obviously, Bill does not know whether Anne is going to announce the original or the alternative set of five hands, or any of many others. In epistemic terms,we can sum up our achievements for this security setting as follows, also using the discussion and results of Section 6.

$$\mathcal{D} \models \langle ab \rangle (one \wedge two \wedge three) \tag{7}$$

$$\mathcal{D} \not\models \langle ab \rangle K_a (one \wedge two \wedge three) \tag{8}$$

$$\mathcal{D} \not\models \langle ab \rangle K_b (one \wedge two \wedge three) \tag{9}$$

$$\mathcal{D} \models \langle a \rangle K_a \big(two \wedge three \wedge \langle b \rangle K_b (one \wedge two \wedge three)\big) \tag{10}$$

Recall (Proposition 26.2) that a formula of the form $\langle i \rangle K_i \phi$ expresses the fact that agent i knows *de re* that she can achieve ϕ; that she can make an announcement that will ensure that ϕ is true in any state that i considers possible. Thus, the last formula above, (10), expresses the fact that there is an announcement that Anne can make after which Bill has learnt her cards and Cath remains ignorant, no matter which of the four card deals Anne considers possible is the actual one, and such that Bill then can make an announcement after which all three requirements hold. Thus, it is rational for Ann to make that announcement, and for Bill to make a proper counter announcement in the resulting state. Unlike the property (6), (10) shows that Ann and Bill know *how* to execute a successful protocol.

8. Conclusions

We proposed an extension of public announcement logic with constructs $\langle G \rangle \phi$, where G is a group of agents, with the intuitive meaning that G can jointly execute a *publicly observable* action such that ϕ will be true afterwards. This included *sequences* of such joint actions and also protocols with alternating actions by different agents, in response to the actions of others. The logic is completely axiomatizable, using the same method as for arbitrary announcement logic. The model checking problem for public announcement logic is PSPACE-complete. Both 'knowing how' (knowing de re) and 'knowing that' (knowing de dicto) can be expressed in our framework. Requirements for finite-length protocols can also be investigated in group announcement logic.

We anticipate some further research. A simple extension to the language would also allowing factual change, apart from informational change. This would make the correspondence with multi-player games even more direct. A different,

and further, generalization would be with non-public actions, such as private messages involving subgroups, card showing actions, etc. This is also technically conceivable, but slightly further down the road, we think.

References

[1] T. Ågotnes, Action and knowledge in alternating-time temporal logic, Synthese (Special Section on Knowledge, Rationality and Action) 149 (2) (2006) 377–409.
[2] T. Ågotnes, H.P. van Ditmarsch, Coalitions and announcements, in: L. Padgham, D. Parkes, J. Muller, S. Parsons (Eds.), Proceedings of the Seventh International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2008), Estoril, Portugal, May 2008, IFAMAAS, 2008, pp. 673–680.
[3] R. Alur, T.A. Henzinger, O. Kupferman, Alternating-time temporal logic, Journal of the ACM 49 (2002) 672–713.
[4] P. Balbiani, A. Baltag, H.P. van Ditmarsch, A. Herzig, T. Hoshi, T. De Lima, What can we achieve by arbitrary announcements? A dynamic take on Fitch's knowability, in: D. Samet (Ed.), Proceedings of TARK XI, Louvain-la-Neuve, Belgium, Presses Universitaires de Louvain, 2007, pp. 42–51.
[5] P. Balbiani, A. Baltag, H.P. van Ditmarsch, A. Herzig, T. Hoshi, T. De Lima, 'Knowable' as 'known after an announcement', Review of Symbolic Logic 1 (3) (2008) 305–334.
[6] P. Blackburn, M. de Rijke, Y. Venema, Modal Logic, Cambridge Tracts in Theoretical Computer Science, vol. 53, Cambridge University Press, Cambridge, 2001.
[7] J. Broersen, A complete STIT logic for knowledge and action, and some of its applications, in: Proceedings of DALT@AAMAS08, in: Lecture Notes in Artificial Intelligence, Springer, 2008.
[8] B. Brogaard, J. Salerno, Fitch's paradox of knowability, http://plato.stanford.edu/archives/sum2004/entries/fitch-paradox/, 2004.
[9] A.K. Chandraa, D.C. Kozen, L.J. Stockmeyer, Alternation, Journal of the ACM 28 (1981) 114–133.
[10] E.M. Clarke, O. Grumberg, D.A. Peled, Model Checking, MIT Press, Cambridge, MA, USA, 1999.
[11] R. Goldblatt, Axiomatising the Logic of Computer Programming, Springer-Verlag, 1982.
[12] E. Gradel, M. Otto, On logics with two variables, Theoretical Computer Science 224 (1999) 73–113.
[13] W. Jamroga, Some remarks on alternating temporal epistemic logic, in: FAMAS'03 – Formal Approaches to Multi-Agent Systems, Proceedings, Warsaw, Poland, 2003, pp. 133–140.
[14] W. Jamroga, T. Ågotnes, Constructive knowledge: What agents can achieve under imperfect information, Journal of Applied Non-Classical Logics 17 (4) (2007) 423–475.
[15] W. Jamroga, W. van der Hoek, Agents that know how to play, Fundamenta Informaticae 63 (2004) 185–219.
[16] M. Pauly, A modal logic for coalitional power in games, Journal of Logic and Computation 12 (1) (2002) 149–166.
[17] J.A. Plaza, Logics of public communications, in: M.L. Emrich, M.S. Pfeifer, M. Hadzikadic, Z.W. Ras (Eds.), Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems: Poster Session Program, Oak Ridge National Laboratory, 1989, pp. 201–216, ORNL/DSRD-24.
[18] J.F.A.K. van Benthem, What one may come to know, Analysis 64 (2) (2004) 95–105.
[19] H.P. van Ditmarsch, The Russian cards problem, Studia Logica 75 (2003) 31–62.
[20] H.P. van Ditmarsch, W. van der Hoek, B.P. Kooi, Dynamic Epistemic Logic, Synthese Library, vol. 337, Springer, 2007.