Department of Computer Science,
University of Otago

Technical Report OUCS-2002-08

The Russian cards problem: a case study in cryptography with public announcements

Author:
Hans van Ditmarsch
Department of Computer Science, University of Otago

Status: not yet submitted anywhere

Department of Computer Science,
University of Otago, PO Box 56, Dunedin, Otago, New Zealand

http://www.cs.otago.ac.nz/trseries/

The Russian cards problem: a case study in cryptography with public announcements

H.P. van Ditmarsch*

October 2002

Abstract

Suppose we have a stack of cards that is divided over some players. It may be possible to communicate your hand of cards to another player by public announcements, without yet another player learning any of your cards. A solution to this problem consists of some sequence of announcements and is called an *exchange*. It is called a *direct exchange* if it consists of (the minimum of) two announcements only. The announcements in an exchange have a special form: they are *safe communications*, an interesting new form of update. Certain unsafe communications turn out to be unsuccessful updates. A communication is a public announcement that is known to be true. Each communication may be about a set of alternative card deals only, and even about a set of alternatives to the communicating player's own hand only. There are 102 direct exchanges for a deal of seven cards where the two players holding three cards communicate their hands to each other. Our work can be used to design cryptographic protocols for 'perfect logicians' where secrets are not just computationally unfeasible to uncover but cannot be uncovered at all.

1 Introduction

In public/private key cryptography, secret information is safeguarded because of the too high complexity of factorizing a large product of primes. I.e., too high given the current state of the art of algorithmic techniques aiding that search for prime factors. One therefore may prefer alternative cryptographic protocols where, even though just as in public/private key cryptography the communication is public, secrets are guaranteed nevertheless. Such protocols have been studied recently in the cryptography and information theory community [FW96, Mak01], and a successful approach appears to be one where the communicating agents are card players, and the communicated secrets are (ownership of) cards. In our investigation we apply dynamic epistemic logic [Ger99, vD02a, Bal02] to the description of such protocols for card deals, aiming to continue a line of research where security and communication protocols have successfully been studied from a logical viewpoint [BAN90, FHMV95, SV02, AHV02]. There are at least two advantages to this approach: the logical analysis is particularly helpful in explaining why incorrect protocols do not work. We will go into that in detail. Beyond that, and using that card games can be seen as interpreted systems, standard logical techniques of finite model description, model checking, and theorem proving will be helpful in finding actual solutions (protocols) within the bounds of existing information theoretical results. This will be outlined only. Far from giving a well-tailored solution towards applications, we have chosen to thoroughly investigate a case-study, namely the Russian cards problem:

> *From a pack of seven known cards two players each draw three cards and a third player gets the remaining card. How can the players with three cards openly (publicly) inform each other about their cards, without the third player learning from any of their cards who holds it?*

*Computer Science, University of Otago, PO Box 56, New Zealand, hans@cs.otago.ac.nz

It was originally presented at the Moscow Mathematics Olympiad in 2000. I therefore propose to name it the 'Russian cards' problem. Originally, the cards were named $0, ..., 6$. Besides being public, all announcements are assumed to be truthful. One solution (somewhat suggested by the names of the cards) and a procedural requirement for solutions are presented in [MM01]. That same solution and various others are found in [vD01a, vD02b].

To start with, we present one 'bad' and one 'good' solution. Call the players Anne, Bill and Crow, and the cards $0, ..., 6$, and suppose Anne holds $\{0, 1, 2\}$, Bill $\{3, 4, 5\}$, and Crow card 6. If Anne says: "I or Bill have the cards 0,1, and 2," and Bill then says: "I or Anne have the cards 3,4, and 5," this may appear a solution. It appears that Anne and Bill learn each others' cards this way, but that Crow cannot distinguish between Anne (and Bill) holding either $\{0, 1, 2\}$ or $\{3, 4, 5\}$. So Crow doesn't know any of Anne's cards. We will explain why this is *not* a solution, and present even less trivial examples to the reader, where, unlike here, Anne knows that Crow doesn't know any of her cards after the announcements.

Next, consider the following solution: Anne says "I'll rename the cards as follows: 0 becomes 7, 1 becomes 3, 2 remains the same, 3 becomes 1, and the rest remains the same. The sum of my cards is now 12." This happens to enough for Bill to learn her cards, who therefore says: "Crow holds card 6." We will explain why this is indeed a solution. It is now common knowledge that Anne and Bill know each others' cards and that Crow doesn't know a single of theirs.

In the next section we introduce a logic to describe such problems and relevant structures to interpret it in. In section 3 we describe in the defined logic the formal requirements for a solution. In section 4 we present the solutions, called exchanges, for this specific seven cards problem. In section 5 we summarily present some generalizations.

2 Logic and structure

We successively introduce card deals, epistemic logic with announcements and its interpretation, and card game structures and their description in this logic.

2.1 Card deals

Given a stack of known cards and some players, the players blindly draw some cards from the stack. In a state where cards are dealt in that way, but where no game actions of whatever kind have been done, it is commonly known what the cards are, that they are all different, how many cards each player holds, and that players only know their own cards. From the last it follows that two deals are the same for an agent, if he holds the same cards in both, and if all players hold the same number of cards in both. This induces an equivalence relation on deals. See also [vDvdHK02].

Definition 1 *A* **card deal** d *is a function from* **cards** Q *to* **players** *(***agents***)* N*. The* **size** $\sharp d$ *of a deal of cards* d *lists for each player how many cards he holds. Two deals* $d, e \in (Q \to N)$ *are indistinguishable ('the same') for a player* $n \in N$ *if* $\sharp d = \sharp e$ *and* $d^{-1}(n) = e^{-1}(n)$*.*

Example 1 (Russian cards) *In the Russian cards problem, we (again) call the players Anne (or a), Bill (or b) and Crow (or c). For a convenient reference, these players are assumed to be, respectively, female, male, and neuter. Anne and Bill are the players holding three cards. Name the cards* $0, 1, 2, 3, 4, 5, 6$*. Assume that the actual card deal is: Anne holds* $0, 1, 2$*, Bill holds* $3, 4, 5$*, and Crow holds 6.*

We informally write $012|345|6$ *for that deal* d *(meaning that* $d(0) = a$*,* $d(1) = a$*,* $d(2) = a$*,* $d(3) = b$*, ...), and for its size – in bold –* $\mathbf{3}|\mathbf{3}|\mathbf{1}$*. The hand of Anne is* $\{0, 1, 2\}$ *(*$d^{-1}(a) = \{0, 1, 2\}$*). For Anne, deals* $012|345|6$ *and* $012|346|5$ *(*$= e$*) are the same, because they are both of size* $\mathbf{3}|\mathbf{3}|\mathbf{1}$*, and* $d^{-1}(a) = e^{-1}(a) = \{0, 1, 2\}$*.*

2.2 Epistemic logic with announcements

For the epistemic part of the language we follow standard notation as in, e.g., [FHMV95, MvdH95], for the dynamic part of the language we follow notation as in [GG97, vBDvE+02].

Definition 2 (Epistemic structures) *Given a set of* **agents** N *and a set of (propositional)* **atoms** P*, a (Kripke or modal or possible worlds)* **model** $M = \langle W, R, V\rangle$ *consists of a* **domain** W *of* **worlds** *or* **factual states**, **accessibility** $R : N \to \mathcal{P}(W \times W)$ *which for each agent* $n \in N$ *defines a binary accessibility relation* R_n *on* W*, and a* **valuation** $V : P \to \mathcal{P}(W)$ *which for each atom* $p \in P$ *defines a valuation* $V_p \subseteq W$*. If* $w \in W$*, then* (M, w) *is a* **pointed (modal) model** *or a* **modal state**.

Instead of '$w \in W$', we also write '$w \in \mathcal{D}(M)$' ('w is in the domain of M') or simply '$w \in M$'.

In an **epistemic model** or **information model**, commonly known as an $S5$ model, all accessibility relations are equivalence relations. We then write $\sim_n$ for the equivalence relation for agent n. If $w \sim_n w'$, we also say that 'w **is the same as** w' **for** n'. If M is an epistemic model, and $w \in M$, then (M, w) is an **epistemic state** or **information state**. World / factual state w is the **point** of the information state, and M the model **underlying** the information state.

Write $\mathcal{M}_N(P)$ for the class of all models for agents N and atoms P. Similarly, write $\mathcal{S}5_N(P)$ for the class of all such information ($S5$) models.

Definition 3 (Language of epistemic logic) *Given is a set* N *of agents and a set* P *of atoms.* $\mathcal{L}_N^{\Box}(P)$ *is the smallest set such that, if* $p \in P$*,* $\varphi, \psi \in \mathcal{L}_N^{\Box}(P)$*,* $n \in N$*, then*

$$p, \neg\varphi, (\varphi \wedge \psi), K_n\varphi, C\varphi, [\psi]\varphi \in \mathcal{L}_N^{\Box}(P)$$

Formula $K_n\varphi$ stands for 'agent n knows that φ', $C\varphi$ stands for 'it is common knowledge (to group N) that φ', and $[\psi]\varphi$ stands for 'after (truthful and public) announcement of ψ it holds that φ'. Other propositional connectives and modal operators are defined by abbreviations. Outermost parentheses of formulas are deleted whenever convenient. As we may generally assume an arbitrary P, we write $\mathcal{L}_N^{\Box}$ instead of $\mathcal{L}_N^{\Box}(P)$. If $|A| = m$, we also write $\mathcal{L}_m^{\Box}(P)$, and name the knowledge operators $K_1, K_2, \cdots, K_m$.

In $[\psi]\varphi$, operator $[\psi]$ is called the update. Sequences of, and nondeterministic choice between, announcements are defined by abbreviation as, respectively: $[\varphi\ ;\ \psi]\chi := [\varphi][\psi]\chi$ and $[\varphi \cup \psi]\chi := [\varphi]\chi \wedge [\psi]\chi$.

Definition 4 (Semantics of epistemic logic) *Let* $M \in \mathcal{S}5_N(P)$*,* $w \in M$*, and* $\varphi \in \mathcal{L}_N(P)$*, where* $M = \langle W, \sim, V\rangle$*. We define* $M, w \models \varphi$ *by induction on the structure of* φ*.*

$$\begin{array}{lll}
M, w \models p & :\Leftrightarrow & w \in V_p \\
M, w \models \neg\varphi & :\Leftrightarrow & M, w \not\models \varphi \\
M, w \models \varphi \wedge \psi & :\Leftrightarrow & M, w \models \varphi \text{ and } M, w \models \psi \\
M, w \models K_n\varphi & :\Leftrightarrow & \forall w' : w \sim_n w' \Rightarrow M, w' \models \varphi \\
M, w \models C\varphi & :\Leftrightarrow & \forall w' : w \sim_N w' \Rightarrow M, w' \models \varphi \\
M, w \models [\psi]\varphi & :\Leftrightarrow & M, w \models \psi \Rightarrow M_\psi, w \models \varphi
\end{array}$$

In the clause for $C\varphi$*,* $\sim_N := (\bigcup_{n\in N} \sim_n)^*$ *(the transitive and reflexive closure of the union of all equivalence relations on* W*). In the last clause,* M_ψ *is the restriction of* M*, including access* $\sim$*, to those states where* ψ *holds, i.e.* $M_\psi = \langle W', \sim', V'\rangle$ *such that, for arbitrary* $n \in N$ *and* $p \in P$*:*

$$\begin{array}{l}
W' := \{v \in W \mid M, v \models \psi\} \\
\forall v, v' \in W' : v \sim'_n v' \Leftrightarrow v \sim_n v' \\
V'_p = V_p | W'
\end{array}$$

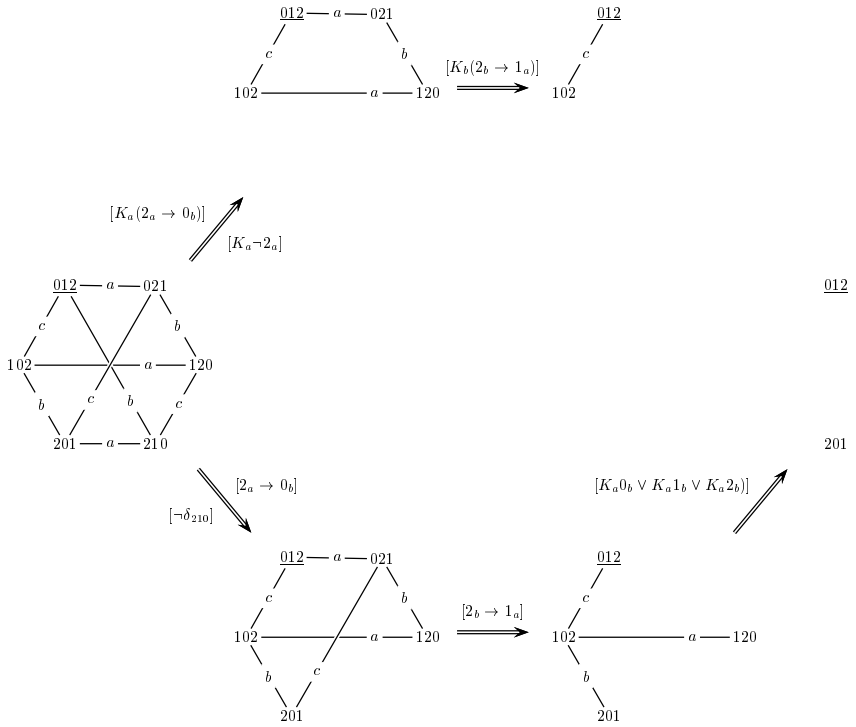

Figure 1: Updates in the information state $(Hexa, 0|1|2)$. Write 012 for $0|1|2$, etc. The actual deal has been underlined. Deals in the same n-equivalence class are linked, and are labeled with n. Formula $\neg\delta_{210}$ expresses that the deal of cards is not $2|1|0$, see Section 2.3.

Example 2 (Public updates in Hexa) *We illustrate the interpretation of updates by the simple example of an information state where there are only three cards* $0, 1, 2$ *and where every player holds one card. As there are six such deals of cards, we call the initial ('hexagonal') model* $I_{\mathbf{1|1|1}}$*: Hexa. Assume that the actual deal of cards is* $0|1|2$*, which for simplicity we now write as* 012*. Figure 1 pictures the information state* $(Hexa, 012)$ *and the result of some updates in this state. For example, we now have that*

$$(Hexa, 012) \models [K_a(2_a \to 0_b)]C\neg 2_a$$

which stands for 'After Anne says: "If I have 2, then Bill has 0," it is common knowledge that Anne doesn't have card 2 in the current information state'. This is, because it is commonly known to all players that Anne doesn't know any of Bill's cards at this state of the game. If Anne hadn't had card 0, she could have imagined both Bill and Crow to have card 0. Therefore, she can only truthfully make her announcement if the antecedent of the implication if false and she actually doesn't hold card 2. So, incidentally, Anne could also immediately have said: "I don't have card 2." For another example, we have that

$$(Hexa, 012) \models [K_a(2_a \to 0_b)][K_b(2_b \to 1_a)]C\neg K_c 0_a$$

which stands for 'After Anne says "If I have 2, then Bill has 0," and Bill says "If I have 2, then Anne has 1," it is common knowledge that Crow doesn't know that Anne has 0.

The remaining updates in Figure 1 result if an insider ('having access to all cards') says: "If Anne has 2, then Bill has 0," (or: "The deal of cards is not 210") and then says: "If Bill has 2, then Anne has 1." If Anne then says: "I know Bill's card," this update $[K_a 0_b \vee K_a 1_b \vee K_a 2_b]$ *results in Crow learning the deal of cards.*[1]

[1] Public updates in $Hexa$ can be performed online on

`http://www.science.uva.nl/projects/opencollege/cognitie/hexagon/`

Before we continue with the description of card game states in this logic in a more formal way than in Example 2, we give some of its revelant properties and concepts:

Proposition 1 (Combining two updates) *For all formulas in the language,* $[\varphi \wedge [\varphi]\psi]\chi$ *is equivalent to* $[\varphi][\psi]\chi$ *(also written as* $[\varphi\ ;\ \psi]\chi$*).*

In other words, if you say that 'φ and after that ψ', this is the same as first saying φ and then saying ψ. For an (elementary) proof, see the Appendix.

It is tempting to think that saying something is the same as making it common knowledge. This turns out to be false. A well-known complication of this logic (and basically, the reason that we need the update operator), is that you may announce something after which it is no longer true and therefore certainly not commonly known. The simplest example of this is a saying to b: "you don't know that (the fact) p (is true)." This corresponds to update $[K_a(p \wedge \neg K_b p)]$. After having said that, b of course knows that p. From $K_b p$ follows $\neg p \vee K_b p$, so $\neg K_a \neg(\neg p \vee K_b p)$, and the last is equivalent to $\neg K_a(p \wedge \neg K_b p)$, the negation of the update formula. This is just the most simple example of a regularly occurring phenomenon while establishing a common ground of information:

Definition 5 (Unsuccessful update) *Given an information state* (M, w)*, an unsuccessful update is a formula* φ *such that* $M, w \models [\varphi]\neg\varphi$*.*

Example 3 (Public updates in Hexa) *If in model Hexa the actual deal had not been 012 but 102, and if therefore in* $(Hexa_{2_a \to 0_b})_{2_b \to 0_a}, 120)$ *Anne announces that she doesn't know Bill's card, Crow can derive Bill's card from that announcement. Formally* $Hexa, 120 \models [2_a \to 0_b][2_b \to 0_a][\neg(K_a 0_b \vee K_a 1_b \vee K_a 2_b)](K_c 0_b \vee K_c 1_b \vee K_c 2_b)$*. The corresponding unsuccessful update actually is, that after Anne truthfully says that she doesn't know if some player knows the card deal, she knows that some player will know the card deal.*

The best-known example of an unsuccessful update is 'nobody knows whether (s)he is muddy' in the Muddy Children problem, in the last round [FHMV95]. The term is introduced in [Ger99] and used in [vD00]. Because some updates are successful and others aren't, the description of information states resulting from updates *may* be complex. It is therefore a useful result that updates with common knowledge are always successful:

Proposition 2 (Common knowledge updates are successful) *For all formulas in the language,* $[C\varphi]C\varphi$ *is valid.*

For an (elementary) proof, see the Appendix.

The logic for $\mathcal{L}_N^{\Box}(P)$ can be axiomatized and is complete [Pla89, vB01].

2.3 Logical description of card games

We continue by introducing information states that for a given deal of cards over players describe their knowledge [vDvdHK02]. Because two deals are the same for an agent if he holds the same cards in both, agents (at least) know their own local state. This makes card games examples of distributive or interpreted systems in the sense of [FHMV95]. These can statically be represented as information states, and dynamically by information state transitions. Because we merely investigate announcements for card deals, we can even restrict ourselves to information states where *different* worlds are about *different* deals. In general, we cannot restrict ourselves this way, e.g. after Anne shows one of her cards to Bill without Crow seeing it (even though he is aware of the action), Anne can distinguish the information state where she has shown card 1 from the state (same deal) where she has shown card 2.

Definition 6 (Public card game state) *A set of cards Q and a set of players N induce a set $P = Q \times N$ of atoms, such that q_n describes the fact that card q is held by agent n. A* **public card game state** *is an information state $(\langle D, \sim, V\rangle, d)$ such that: $D \subseteq (Q \to N)$, $d \in D$, for an arbitrary $n \in N$ and $d_1, d_2 \in D$: $d_1 \sim_n d_2$ only if $\sharp d_1 = \sharp d_2$ and $d_1^{-1}(n) = d_2^{-1}(n)$, and for an arbitrary $q_n \in P$: $V_{q_n} = \{d \in D \mid d(q) = n\}$.*

In particular, the information state where for a given deal d the players *only* know their own cards is a public card game state. It is represented by an **initial game state** $(I_{\sharp d}, d)$. The domain of $I_{\sharp d}$ consists of all deals of the same size as d, and for access we have that for an arbitrary $n \in N$ and $d_1, d_2 \in D$: $d_1 \sim_n d_2$ if and only if $d_1^{-1}(n) = d_2^{-1}(n)$.

Proposition 3 (Announcements and public card game states)
If (M, w) is a public card game state for players N and atoms P, and $\varphi \in \mathcal{L}_N^{\Box}(P)$ such that $M, w \models \varphi$, then $(M, w)_\varphi$ is a public card game state.

Proof. Every announcement results in a restriction of the domain. ⊣

The example above of Anne showing one of her cards to Bill (which can be done from information state $(I_{\mathbf{3|3|1}}, d)$), shows that Proposition 3 doesn't hold for all $S5$ state transitions.

Definition 7 (Description of a card deal) *Given is a deal $d : Q \to N$. Define by overloading: $d(q_n) = q_n$ iff $d(q) = n$, and $d(q_n) = \neg q_n$ iff $d(q) \neq n$. The (atomic)* **description of a deal** *d is the conjunction of atoms or their negations according to d: $\delta_d := \bigwedge_{q \in Q, n \in N} d(q_n)$ (it can be seen as the characteristic function of the valuation of atoms in world d). The* **description of the hand of** *n, is the conjunction of the atoms involving agent n: $\delta_d^n := \bigwedge_{q \in Q} d(q_n)$.*

Beyond that, there is a description Φ_d (characteristic formula) of $(I_{\sharp d}, d)$, that sums up the facts and the knowledge and ignorance of the players. More precisely, Φ_d describes the bisimulation class of $(I_{\sharp d}, d)$ with respect to the epistemic language without updates. The description Φ_d has the form $\delta_d \wedge C\mathsf{kgames}$, where kgames is the description of the model $I_{\sharp d}$. For details, see [vDvdHK02].

Example 4 *$(I_{\sharp 012|345|6}, 012|345|6)$ is the initial information state for the Russian cards problem. It consists of $\binom{7}{3}\binom{4}{3}\binom{1}{1} = 140$ deals. The atomic description of that deal is*

$$\delta_{012|345|6} := 0_a \wedge 1_a \wedge 2_a \wedge \neg 3_a \wedge \ldots \wedge \neg 0_b \wedge \ldots \wedge \neg 5_c \wedge 6_c$$

and the hand of player a is described by

$$\delta^a_{012|345|6} := 0_a \wedge 1_a \wedge 2_a \wedge \neg 3_a \wedge \neg 4_a \wedge \neg 5_a \wedge \neg 6_a \ .$$

For $\delta^a_{012|345|6}$ we also write 012_a, etc. Some typical formulas satisfied in the initial information state $(I_{\sharp 012|345|6}, 012|345|6)$ are: $K_a 0_a$ (Anne knows that she holds card 0), $K_b \neg K_a 3_b$ (Bill knows that Anne doesn't know that he holds card 3), and $C \bigvee_{\sharp d = \sharp 012|345|6} K_a \delta^a_d$ (It is common knowledge that Anne knows her own hand of cards).

Proposition 4 (Alternative deals) *Every announcement in a public card game state has the same denotation as one about alternative deals.*

Proof. Given a deal $d : Q \to N$, let (D, d) be a public card game state, $\varphi \in \mathcal{L}_N^{\Box}$, and assume $D, d \models \varphi$. Because all worlds $e \in D$ are different deals, each formula δ_e holds in exactly one information state (D, e) with underlying model D. Therefore, obviously, $D \models \varphi \leftrightarrow \bigvee_{e \in D_\varphi} \delta_e$. (Note that $\bigvee_{e \in D_\varphi} \delta_e \in \mathcal{L}_N$.) ⊣

The language and structures that we have introduced in this section are actually quite tailored towards an elegant description of the actions occurring in 'Russian cards' and related problems. For more complex dynamics, such as the action of showing a card, a more expressive dynamic epistemic logic is needed [Ger99, Bal02, vD00].

We are now ready to do battle with the Russian cards problem.

3 Safe communications

Let d be an arbitrary deal of cards Q over at least three players $N = \{a, b\} \cup O$, where O is the non-empty set of *O*ther players, e.g. Crow in the three player case. A solution of the cards problem is some sequence of announcements. A reasonable requirement for two communicating agents appears to be that uninformative statements are never consecutive as long as the problem is not solved ('epistemic liveness'). This means that the sequence will be finite: each informative announcement will reduce the number of deals in the model underlying the – finite – initial state. So the maximum length of a 'conversation' is twice the number of deals of that size. An announcement in such a sequence can be regarded as an 'epistemic programme', for which we therefore have to determine the (weakest) pre- and (strongest) postcondition.

After a solution sequence of announcements it should hold that: Anne knows Bill's cards (aknowsbs), Bill knows Anne's cards (bknowsas), and the other players don't know any of Anne's or Bill's cards (cignorant – for 'c (among Others) is ignorant'). The last is the same as 'If c doesn't hold a card, c can imagine both a and b to have it' (from which follows that c doesn't know a to have it, and doesn't know b to have it). For the given deal d this amounts to:

$$K_a\delta^b_d$$
$$K_b\delta^a_d$$
$$\bigwedge_{c\in O}\bigwedge_{q\in d^{-1}(a)\cup d^{-1}(b)}(\neg K_c\neg q_a \wedge \neg K_c\neg q_b)$$

Example 5 (Russian cards) *For Russian cards, for actual deal of cards* $012|345|6$*, we get:* K_a345_b *(Anne knows that Bill holds* $\{3,4,5\}$*),* K_b012_a *(Bill knows that Anne holds* $\{0,1,2\}$*), and* $\neg K_c\neg 0_a \wedge \neg K_c\neg 1_a \wedge \neg K_c\neg 2_a \wedge \neg K_c\neg 3_a \wedge \neg K_c\neg 4_a \wedge \neg K_c\neg 5_a$ *(Crow cannot eliminate any of the cards* $0,...,5$ *from consideration for Anne). In this case of three players only, the last entails that Crow can also imagine Bill to have any of the cards* $0,...,5$*.*

However, e.g. K_a345_b does not say that Anne knows Bill's cards (whatever they are) but only that Anne knows that Bill's cards are 3, 4, and 5. Obviously, we need a requirement on the model, that is independent from the actual deal, but from which the above follow:

Definition 8 (Postconditions) *Let* $d : Q \to \{a, b\} \cup O$ *be a card deal. In the information state* (D, d) *where the problem is solved it must hold that:*

$$\begin{array}{ll}\mathsf{aknowsbs} & \bigwedge_{e\in\mathcal{D}(D)}(\delta^b_e \to K_a\delta^b_e)\\ \mathsf{bknowsas} & \bigwedge_{e\in\mathcal{D}(D)}(\delta^a_e \to K_b\delta^a_e)\\ \mathsf{cignorant} & \bigwedge_{c\in O}\bigwedge_{q\in Q}\bigwedge_{n=a,b}(\neg q_c \to \neg K_c\neg q_n)\end{array}$$

The observant reader will immediately remark that, as these are requirements on the model, they are therefore independent of the actual deal, and part of the 'common ground' or context of the agents. Therefore, they should not just be true but commonly known. So we get: Caknowsbs, Cbknowsas, and Ccignorant. These are indeed, given that we see a solution sequence as an epistemic programme, the required (strongest) postconditions, and we further have to require that Ccignorant, the ignorance of the other (non-communicating) players, is an invariant under execution of each announcement in the sequence.[2]

The next issue is, by what sort of announcements the players obtain this common ground. For that, it is instructive to analyse example announcements that fail to establish it, such as the first announcement in the example of the introduction, that is repeated below as Example 6. In another example, Example 8, it becomes clear that Anne's intention to keep her hand

[2] A tempting, more abstract, formulation of the others' ignorance seems to be $\bigwedge_{c\in O}\bigwedge_{e\in\mathcal{D}(D)}(\delta^c_e \to \neg K_c\neg\delta_e)$ – every ('other') c can imagine every deal that extends his hand (in the given domain). This would nicely correspond to the 'private ignorance' of all players (including a and b) in $I_{\natural d}$, as described in Φ_d [vDvdHK02]. Unfortunately this formulation is too weak: it may hold as well when only a single deal is consistent with the current information, or only deals that correspond in one or more of a's or b's cards.

of cards secret is part of the meaning of her announcement, and that because of her intention she may actually unwillingly reveal her hand of cards: the opposite! The explanation of such 'non-solutions' involves unsuccessful updates. Generally the required ignorance cignorant has been established after the first announcement, but not common knowledge of cignorant. All examples are about the Russian cards problem, for actual deal 012|345|6. In all examples below it common knowledge after two announcements that all of cignorant, aknowsbs and bknowsas hold. One can easily construct yet other examples that do not have that property. The given examples are chosen for their simplicity.

First consider the sequence:

Example 6 *Anne says: "I have* $\{0,1,2\}$*, or Bill has* $\{0,1,2\}$*," and Bill says:"I have* $\{3,4,5\}$*, or Anne has* $\{3,4,5\}$*."*

Update of $(I_{\mathbf{3|3|1}}, 012|345|6)$ with $[012_a \vee 012_b]$ results in an information state that consists of eight card deals, and where cignorant holds but not common knowledge of it. Subsequent update with $[345_a \vee 345_b]$ results in an information state consisting of the two deals 012|345|6 and 345|012|6, that are the same for Crow and different for Anne and Bill, so that common knowledge of cignorant, aknowsbs and bknowsas holds. However, this is not a fair treatment of the information:

A *merely truthful* public announcement of φ by an agent n would indeed correspond to an update $[\varphi]$, but an announcement *based on n's information* corresponds to an update $[K_n\varphi]$. If Anne's announcements had been made by an *insider i*, a virtual player who can look in everybody's cards, or differently said, a player whose accessibility on the information state is the identity relation, the update would indeed have been $[\varphi]$, because in this case φ is equivalent to $K_i\varphi$. But Anne knows *much less* than an insider, and therefore her announcements are *much more* informative. Typically, φ can be true but not known by Anne, so $K_a\varphi$ holds in fewer worlds of the current information state than φ.

As it is common knowledge that Anne initially doesn't know any of Bill's cards, she can only truthfully announce "I have $\{0,1,2\}$, or Bill has $\{0,1,2\}$," if she actually holds $\{0,1,2\}$. E.g., if Anne's hand had been $\{0,3,4\}$ instead, the only way for the disjunction $012_a \vee 012_b$ to be true, given that 012_a is false, is that 012_b is true: Bill has $\{0,1,2\}$. But if Anne had held $\{0,3,4\}$, she couldn't have *known* 012_b to be true in the state where she only knows her own cards. In other words: execution of update $[K_a(012_a \vee 012_b)]$ in $I_{\mathbf{3|3|1}}, 012|345|6$ already restricts $I_{\mathbf{3|3|1}}$ to those four worlds where Anne's hand is 012. These are the deals $012|345|6, 012|346|5, 012|356|4, 012|456|3$, that are all different for Bill and for Crow. After that update, Crow knows all of Anne's cards, so cignorant is definitely false. A further update $[K_b(345_a \vee 345_b)]$ results in a state where it is common knowledge that 012|345|6 is the deal of cards. Formally:

$$I_{\mathbf{3|3|1}}, 012|345|6 \models [012_a \vee 012_b]\mathsf{cignorant}$$
$$I_{\mathbf{3|3|1}}, 012|345|6 \not\models [K_a(012_a \vee 012_b)]\mathsf{cignorant}$$

It is rather obvious that players' announcements should be based on their information. But it is now abundantly clear that a precondition for the execution of an announcement φ by player n is that $K_n\varphi$ holds in the current information state. We now move to the less obvious:

Example 7 *Anne says: "I don't have 6," and Bill says: "Neither have I."*

After the first announcement cignorant holds, and $\binom{6}{3}\binom{4}{3} = 80$ card deals remain. After Bill's announcement aknowsbs and bknowsas hold as well, and again all three are even commonly known, and 20 card deals remain. What is wrong here? In the initial information state, Anne cannot distinguish actual deal 012|345|6 from deal 012|346|4. If 012|346|4 had been the deal, after Anne's announcement Crow would have known the owner of one of the cards not held by itself, so cignorant fails again. So even though for the actual deal 012|345|6 postcondition cignorant holds after Anne's announcement, Anne doesn't know that, and it is indeed not commonly known: the stronger postcondition. Formally:

$$I_{\mathbf{3|3|1}}, 012|345|6 \models [K_a\neg 6_c]\mathsf{cignorant}$$
$$I_{\mathbf{3|3|1}}, 012|345|6 \not\models [K_a\neg 6_c]K_a\mathsf{cignorant}$$

It is irrelevant that Ccignorant holds after the second of both announcements. We have to require Ccignorant to be an invariant for *all* annoucements of a solution sequence.

It is even less obvious why the following is also a bad solution:

Example 8 *Anne says: "I have $\{0,1,2\}$, or I don't have any of these cards," and Bill says: "I have $\{3,4,5\}$, or I don't have any of these cards."*

After an update of $(I_{\mathbf{3|3|1}}, 012|345|6)$ with $[K_a(012_a \vee (\neg 0_a \wedge \neg 1_a \wedge \neg 2_a))]$ (=: $[K_a\mathsf{first}]$) we reach an information state that consists of 17 card deals, namely actual deal $012|345|6$ and $\binom{4}{3}\binom{4}{3} = 16$ others (Anne can have any of the four remaining cards $3,4,5,6$, and Bill any three of $0,1,2$ and the one Anne didn't get). By a further update $[K_b(345_b \vee (\neg 3_b \wedge \neg 4_b \wedge \neg 5_b))]$ we again, as in Example 6, reach the information state that consists of deals $012|345|6$ and $345|012|6$, that are the same for Crow and different for Anne and Bill. Example 7 can be said to be 'unsafe' in the sense that another execution of the apparently underlying protocol (namely Anne saying: "I don't have 4") would have resulted in Crow learning her cards. Instead, in the underlying Example 8, Anne's announcement seems 'safe' in that respect: no other execution of the underlying protocol would have resulted in Crow learning any of her cards. Therefore, indeed, Anne *knows* that Crow is ignorant of her cards after her announcement. However, Crow doesn't know *that*, and, surprisingly, Crow can derive factual knowledge from that ignorance. Crow rightfully assumes that Anne wouldn't dare make an unsafe communication: Anne wants to know that after her announcement Crow doesn't know any of her cards. Therefore, the update corresponding to first is not just $[K_a\mathsf{first}]$ but $[K_a\mathsf{first} \wedge [K_a\mathsf{first}]K_a\mathsf{cignorant}]$: "I know that first, and that after having said that, Crow doesn't know my cards."

For Crow, only deal $345|012|6$ is the same as $012|345|6$ after update $[K_a\mathsf{first}]$. If the deal had been $345|012|6$, Anne could have imagined it to have been, e.g., $345|016|2$. In that case it would have been informative for Crow when Anne had announced first: it would have known that Anne doesn't have 0, 1, and 2: so cignorant is not true. We now can wind up the argument: because cignorant doesn't hold after $[K_a\mathsf{first}]$ in $345|016|2$ (strictly: that deal in the restriction of the model), $K_a$cignorant doesn't hold after $[K_a\mathsf{first}]$ in $345|012|6$, therefore $K_a\mathsf{first} \wedge [K_a\mathsf{first}]K_a\mathsf{cignorant}$ doesn't hold in deal $345|012|6$ of the initial information state, so updating with that formula fails in deal $345|012|6$ of $I_{\mathbf{3|3|1}}$. But as this was the only alternative for Crow in that model, Crow now knows that the deal is $012|345|6$, so Crow knows all of Anne's cards! Formally:

$$
\begin{array}{l}
I_{\mathbf{3|3|1}}, 012|345|6 \models [K_a\mathsf{first}]\mathsf{cignorant} \\
I_{\mathbf{3|3|1}}, 012|345|6 \models [K_a\mathsf{first}]K_a\mathsf{cignorant} \\
I_{\mathbf{3|3|1}}, 012|345|6 \not\models [K_a\mathsf{first}]K_cK_a\mathsf{cignorant} \\
I_{\mathbf{3|3|1}}, 012|345|6 \models [K_a\mathsf{first} \wedge [K_a\mathsf{first}]K_a\mathsf{cignorant}]\neg\mathsf{cignorant}
\end{array}
$$

and therefore as well, just to make the unsuccessful update stand out:

$$(I_{\mathbf{3|3|1}})_{K_a\mathsf{first}}, 012|345|6 \models [K_a\mathsf{cignorant}]\neg K_a\mathsf{cignorant}$$

In other words: Crow does not learn Anne's cards from the mere fact that her announcement is based on her information. Instead, Crow learns Anne's cards from her intention to prevent Crow learning her cards. Without that intention, Crow would not have learnt Anne's cards. This is an interesting new type of unsuccessful update.

It is reassuring that with the intention to guarantee Ccignorant, such unsuccessful updates can be avoided:

$$
\begin{array}{ll}
M, w \models [K_n\varphi \wedge [K_n\varphi]C\mathsf{cignorant}]C\mathsf{cignorant} & \\
\Leftrightarrow & \text{proposition 1} \\
M, w \models [K_n\varphi][C\mathsf{cignorant}]C\mathsf{cignorant} & \\
\Leftarrow & \\
M_{K_n\varphi}, w \models [C\mathsf{cignorant}]C\mathsf{cignorant} & \\
\Leftrightarrow & \text{proposition 2} \\
\mathsf{true} &
\end{array}
$$

Because of Proposition 2 this intention of the communicating players has become invisible, so to speak: we merely have to test for the postcondition in the information state resulting from the simpler update $[K_n\varphi]$. It is therefore important to realize that this is a mere fortunate consequence of common knowledge updates being successful, and that the players 'really' have this intentional stance and execute the more complex update.

Without taking this intentional stance of agents into account, the information states reached by mere communications are unstable. If e.g. in Example 8 the announcements are interpreted as (only) communications, in the resulting information state aknowsbs and bknowsas both hold but are not commonly known: if Anne makes aknowsbs public (update $[K_a\mathsf{aknowsbs}]$), then Crow can derive the entire deal of cards. This is comparable to the result of Anne saying: "I know Bill's card" $(K_a 0_b \vee K_a 1_b \vee K_a 2_b)$ in the bottom right of Figure 1.

We summarize our results:

Definition 9 (Communicative updates) *Given is some public card game state where* Ccignorant *holds. There are three ways to interpret that an agent* n *(truthfully) says* φ *in that state. As not to confuse such announcements of formulas with the formulas themselves, we keep writing them as updates:*

$[\varphi]$	**announcement** *of* φ *(by an insider)*
$[K_n\varphi]$	**communication** *of* φ *(by player* n*)*
$[K_n\varphi \wedge [K_n\varphi]C\mathsf{cignorant}]$	**safe communication** *of* φ *(by player* n*)*

Note that $[K_n\varphi \wedge [K_n\varphi]C\mathsf{cignorant}]$ *is the same as* $[K_n\varphi][C\mathsf{cignorant}]$. *Alternatively, a safe announcement of* φ *by* n *is an update* $[K_n\varphi]$ *such that* Ccignorant *holds after its execution.*

Definition 10 (Exchange) *Given deal* $d : Q \to \{a, b\} \cup O$ *of cards (*O *non-empty), an* **exchange** *('secret exchange of hands') between two players* a *and* b *is a finite sequence* $\Pi := \pi_1, \pi_2, ..., \pi_m$ *of formulas* $\pi_i \in \mathcal{L}^{\Box}_{\{a,b\}\cup O}$ *that are interpreted as safe communications of* a *and* b*, such that after its execution in* $I^{\natural}_d, d$ *it holds that* $C\mathsf{aknowsbs} \wedge C\mathsf{bknowsas}$. *We assume that* a *is the player who speaks first, and that* a *and* b *take turns. So execution of* Π *corresponds to update sequence* $[K_a\pi_1][C\mathsf{cignorant}][K_b\pi_2][C\mathsf{cignorant}]...$ *(ending with either an* a*- or a* b*-announcement). A* **direct exchange** *is an exchange of length two.*

Observe that Ccignorant also holds after execution of the last announcement π_m of Π, so common knowledge of all three conditions of Definition 8 is satisfied.

Example 9 (A five hand direct exchange for Russian cards) *Assume deal of cards* $012|345|6$. *The following is a direct exchange: Anne announces: "I have one of* $\{012, 034, 056, 135, 246\}$*," and Bill announces "Crow has card 6."*

We explain in detail why Example 9 constitutes a direct exchange. Let π $(= 012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a)$ be Anne's announcement. We have to show that all of the following hold. Note that the common knowledge requirements are translated into *model* requirements of the commonly known formula:

$I_{\mathbf{3\|3\|1}}, 012\|345\|6 \models K_a\pi$	i
$(I_{\mathbf{3\|3\|1}})_{K_a\pi} \models \mathsf{cignorant}$	ii
$(I_{\mathbf{3\|3\|1}})_{K_a\pi}, 012\|345\|6 \models K_b 6_c$	iii
$((I_{\mathbf{3\|3\|1}})_{K_a\pi})_{K_b 6_c} \models \mathsf{cignorant} \wedge \mathsf{bknowsas} \wedge \mathsf{aknowsbs}$	iv

To prove that cignorant holds on a given model, we proceed in the following systematic way:

For an arbitrary card of c, first we can remove all hands containing that card from the communication, because the actual a-hand cannot contain the actual c-card. Then we show that all other cards occur at least once and are absent at least once in the remaining hands. In other words: whatever the actual hand of a, for each of a's cards in that hand, there is still an alternative

remaining hand where that card does not occur. This guarantees that c remains ignorant of the ownership of other cards. Proving that bknowsas and aknowsbs hold in the model for the final information state, is almost directly observable: their access on this model is the identity.

We now prove conditions i to iv for this example:

- Hand 012 is in $\{012, 034, 056, 135, 246\}$. Therefore i holds.
- If c holds 0, the remaining hands are $\{135, 246\}$. Each of $1, 2, ..., 6$ both occurs in at least one of $\{135, 246\}$ and is absent in at least one of those (1 occurs in 135 and is absent in 246, 2 occurs in 246 and is absent in 135, etc.). If c holds 1, the remaining hands are $\{034, 056, 246\}$. Each of $0, 2, ..., 6$ both occurs in at least one of $\{034, 056, 246\}$ and is absent in at least one of those (0 occurs in 034 and is absent in 246, ...). Etc. for c holding 2, ..., 6. Therefore ii holds.
- From $\{012, 034, 056, 135, 246\}$, Bill can remove any hand that contains either 3, 4, or 5. This leaves only hand 012. In deal 012|345|6 Crow actually holds 6. Therefore iii holds.
- After both communications, the following deals are still possible:

  $$\{012|345|6, 034|125|6, 135|024|6\}.$$

  They are all different for Anne and Bill, therefore bknowsas and aknowsbs hold. They are all the same for Crow. Each of $0, 1, ..., 5$ both occurs in at least one of $\{012, 034, 135\}$ and is absent in at least one of those. Therefore iv holds.

We now know the 'meaning in context' of a player's announcement: the safe communication of φ is an update $[K_n\varphi \wedge [K_n\varphi]C\mathsf{cignorant}]$. Can we say anything about φ itself? So far, in the examples we didn't place any restrictions: 'my hand of cards is ...', 'I don't have the cards ...', 'player c doesn't have ...'. Indeed, anything appears to go, also complex epistemic statements such as 'I don't know the cards of player b yet', 'I know that it is not common knowledge whether player c has card 0', etc. Certainly not every update can be reduced to some non-epistemic one! In Proposition 4 however we have proved that the denotation of an arbitrary formula in a public card game state is the same as that of a statement about alternative deals. We can even go beyond that:

Proposition 5 (Alternative hands) *Given is an arbitrary sequence of communications executed in an initial card game state. The denotation of a communication in that sequence is the same as that of an announcement about alternative hands for that player.*[3]

Proof. A communication by player n is an update of the form $K_n\varphi$. By definition of the semantics of the epistemic operator, such formulas $K_n\varphi$ are either satisfied in all worlds of an n-equivalence class, or none at all. In other words, the denotation of $K_n\varphi$ in some given information state is a union of n-equivalence classes [4]. If we can prove that two different n-equivalence classes do not contain deals for the same n-hand, we are done: if different n-class means different hand, the denotation of every formula $K_n\varphi$ in some epistemic model is the same as that of 'a set of n-hands', i.e. in the language: some formula $\delta^n_d \vee \delta^n_e \vee ...$ (there is some D' such that $[\![K_n\varphi]\!] = [\![\bigvee_{d\in D'} \delta^n_d]\!]$). We now prove the proposition by simple induction on the number of communications:

In the initial information state for some deal d, where players only know their own cards, we therefore had that $d \sim_n e \Leftrightarrow d^{-1}(n) = e^{-1}(n)$, so here, hands and equivalence classes correspond by definition. But the rest is by now obvious: because communications are public announcements, they always result in a restriction of the domain. Therefore, the result of such an announcement is *either* that an n-class for player n is deleted, *or* that it is restricted. It is *never* refined, what would be required in order to get different n-classes for the same n-hand. ⊣

[3] Proposition 5 is by Ben Handley, who also provided a, rather different, proof.

[4] Differently said: every announcement by some player is a basic kind of *game action* in the sense of [vD01b]. Such propositions are called 'n-local' in [EvdMM98].

Example 10 *Bill's announcement "Crow has card 6" in Example 9 could* only in this example *also have been "My hand is one of* $\{345, 125, 024\}$*."*

Fact 6 (Last communication) *The last communication of an exchange may consist of b saying what all the cards are not held by a or b.*

Before we continue by presenting all direct exchanges for the Russian cards problem, a note on model checking. Both Proposition 4 and Proposition 5 allow systematic model checking procedures in order to find exchanges. Proposition 4 tells that one has 'merely' to check for all subsets of deals of the domain of an initial card game state whether common knowledge of cignorant is met, and so on, until also common knowledge of aknowsbs and bknowsas is met. It is much more efficient to use Proposition 5 for that:

Proposition 7 (Decision procedure for an exchange) *Given a deal of cards over more than two players, it can be determined whether there is an exchange between two of those players.*

Proof. Given deal $d : Q \to \{a, b\} \cup O$ of cards (O non-empty). The following crude algorithm computes all (possibly 0) exchanges of secrets:

Start with the set of deals equal to all deals of that size: $D := \mathcal{D}(I_{\natural d})$, and with model $M_D := I_{\natural d}$. For both player a and player b, for every subset $D' \subseteq D$ containing d that is a union of $\sim_a$ equivalence classes (or, respectively, $\sim_b$ equivalence classes), check whether $M_D|D' \models \mathsf{cignorant}$. If not, discard that subset. If so, check whether $M_D|D' \models \mathsf{aknowsbs} \wedge \mathsf{bknowsas}$. If so, we have found an exchange. If not, set $D := D'$ (and $M_D := M_D|D'$) and repeat the procedure. ⊣

Apart from this model checking perspective also a theorem proving perspective appears. We have seen that the information state $(I_{\natural d}, d)$ has a characteristic formula $\delta_d \wedge C\mathsf{kgames}$. A sequence of announcements $\Pi := \pi_1, \pi_2, ..., \pi_m$ is an exchange, if a number of *epistemic correctness statements* are valid such as:

$$(\delta_d \wedge C\mathsf{kgames}) \to [K_a \pi_1] C\mathsf{cignorant}$$

Both the model checking and theorem proving approach may provide alternatives to standard combinatorial / cryptographic approaches as in [GGL96] and [FW96]. For example, the last provides information theoretical upper and lower bounds for secret bit exchange for a given deal of cards, whereas we compute concrete exchanges for such deals.

The epistemic analysis of Definition 10 also applies to executions of cryptographic protocols, because these are sequences of announcements. For example, our analysis may correspond to a procedural requirement for such protocols that is given in [MM01]. The authors have provided me with a partial translation of their original work, in Russian [Mak01]. The infinitary flavour of what they define as a protocol appears to relate to the fixed-point character of common knowledge.

We continue with the presentation of solutions for the seven cards problem.

4 Overview of direct exchanges for seven cards

In this section we give an overview of all direct exchanges for card deal size **3**|**3**|**1**. From now on, assume all deals to be of that size. Assume that the actual deal is 012|345|6. In a direct exchange, Bill's announcement can always be "Crow has card 6," even though he could have made some equivalent statement in terms of his possible hands, see Fact 6. We therefore only mention Anne's communications in the following. Par abus de langage, we often refer to 'Anne's safe communication as the first of a direct exchange' as 'the direct exchange'.

Now if we merely used that all communications are about alternative deals (Proposition 4), we would have apply a procedure as in Proposition 7 check for 2^{139} subsets of deals (namely all subsets of card deals of size **3**|**3**|**1** containing actual deal 012|345|6). Because of Proposition 5, we

can see Anne's communication as a set of hands, namely the alternative hands for Anne. Write a hand as a sequence of three digits. Applying the procedure in Proposition 7 would still lead to checking 2^{34} subsets of hands (namely all subsets of Anne's hands that include her actual hand 012). Fortunately, by combinatorial reasoning (essentially using Proposition 5), we can be spared all that effort. We present our results in a number of Propositions:

Proposition 8 *Every card occurs at least once in a safe communication.*

Proof. By 'a card occurs in a communication' we mean: 'a card occurs in a hand of that communication'.

Suppose card q does not occur in the communication. Then obviously a doesn't have q (because a's actual hand is part of the communication). But then a can imagine c not to have q, in which case c would be able to conclude that a doesn't have q: $K_c\neg q_a$. Therefore $\neg$cignorant. (So Ccignorant doesn't hold after the communication.) ⊣

Proposition 9 *Every card occurs at least twice in a safe communication.*

Proof. Suppose card i occurs once only in communication π. Player c now reasons as follows:

Suppose a didn't have card i. Then she can imagine me not to have i. Let ijk be the hand in π containing i. Now suppose a didn't have j or k herself, say she didn't have j. Then she could imagine me to have j instead, in which case I would have been able to eliminate hand ijk and to conclude that a doesn't have card i. From $K_c\neg i_a$ follows that Ccignorant doesn't hold after the communication. Therefore a must have j. But from $K_c j_a$ also follows $\neg C$cignorant. Same for k. Because my assumption that a *did not* have card i leads to $\neg C$cignorant, a *must* have card i. But in that case we have $K_c i_a$ so again Ccignorant doesn't hold after the communication. ⊣

Proposition 10 *No direct exchange consists of less than five hands.*

Proof. Every card occurs at least twice in a direct exchange (Proposition 9). Therefore, (the first announcement of) a direct exchange must contain at least $7 \times 2 = 14$ occurrences of cards. An announcement of four hands consists of $4 \times 3 = 12$ occurrences of cards only. ⊣

Proposition 11 *No direct exchange consists of more than seven hands.*

Proof. We call hands that have a pair of cards in common 'crossing hands'. There are $\binom{7}{2} = 21$ different pairs of cards. Therefore, the maximum number of hands in an announcement without crossing hands is seven. Suppose that we extend such an announcement with one more hand (that is different from the seven in the announcement). This hand will cross with three of the seven hands (because the eighth hand introduces three pairs of cards).

We now prove that c can eliminate crossing hands in a's announcement from consideration after b's announcement. Suppose ijk and ijl are part of a's announcement. Crow can reason as follows:

If b had none of i, j, k, l but the remaining three cards, he would not have been able to determine which of ijk and ijl is the hand of a. But as he just announced my card, he was able to determine a's hand from her announcement. Therefore a's hand was neither ijk nor ijl.

Therefore we can remove the eighth hand and the three with which it crosses. Now only four hands remain: according to Proposition 10 this is not enough for a direct exchange.

Other cases (starting from fewer non-crossing hands) can be similarly treated (see also below). ⊣

Proposition 12 *No direct exchange contains crossing hands.*

Proof. Direct exchanges consisting of five or six hands cannot (if they exist at all: so far, we have only proved a five hand direct exchange in Example 9) contain a pair of crossing hands: applying the observation in the proof of Proposition 11, c can remove those from consideration after b's announcement of his card, after which three or four hands, respectively, remain: not

enough for a direct exchange. But also direct exchanges of seven hands cannot contain a pair of crossing hands. We omit the precise argument: it is somewhat similar to that in Proposition 11, with extra crucial observation that five non-crossing hands cannot be extended with two more hands that are crossing but not with those five. ⊣

A final observation is that:

Proposition 13 *Every card occurs at most thrice in a direct exchange.*

Proof. If a card were to occur in four hands, this would involve eight pairs containing that card: as there are only six other cards, there must therefore be two similar pairs. No direct exchange contains crossing hands (Proposition 11). ⊣

All the remaining possible five, six and seven hand combinations are indeed direct exchanges. We start with an informal overview of what they are:

Because every card occurs either twice or thrice in a direct exchange, and because there are no direct exchanges of less than five hands, some card must occur thrice.

First suppose this is one of a's actual cards. Assume w.l.o.g. that from a's actual cards $0, 1, 2$ card 0 occurs thrice. As the communication does not contain the same pair of cards more than once, we can assume it w.l.o.g. to contain 012, 034 and 056. Also w.l.o.g. we can assume the fourth hand to be 135. At this stage there are only four hands left that do not contain a pair of cards already used: 146, 246, 236, 245. We now have a moment of choice: **either** 1 occurs thrice in the message as well, in which case the fifth hand *must* be 146 (and we can then add either 236, or 245, or both), **or** there is no other card that occurs thrice in the message, in which case the fifth hand *must* be 246 and the message cannot (as one may observe) be extended further without crossing hands.

Next, suppose that none of a's actual cards $0, 1, 2$ occur thrice. Then they all occur twice. Starting from some seven hand announcement, where all cards occur thrice exactly, there are two ways to achieve that. The first is to remove a's actual hand from the announcement: in the remainder cards $0, 1, 2$ occur twice. But of course we cannot remove the actual hand! Therefore, two hands must be removed and we end up with five hands, where one of the remaining cards occurs thrice. An example of such an announcement is $\{012, 345, 036, 146, 256\}$. This turns out to be a symmetric variation of the one we already computed in the previous paragraph. And this should not surprise us, because if it were *not* a symmetric variation, c could observe that and possibly derive factual information from it.

We now prove that the communications we have found so far are direct exchanges. We found four different types: seven hands, six hands, five hands with an a-card thrice, five hands with a non a-card thrice. The proof follows the pattern outlined after Example 9. All other direct exchanges are merely symmetric variations on the above. We have seen in Proposition 12 that we cannot extend direct communications with hands that cross with it. We report on how they may be extended (or restricted) with non-crossing other hands. This, in other words, is a way of describing whether they are minimal or maximal with respect to deleting / adding hands. We then enumerate them. We close this section with some other interesting observations and descriptive versions of exchanges.

Proposition 14 *Anne announcing* $\{012, 034, 056, 135, 246\}$ *is a direct exchange. It is both minimal and maximal.*

Proof. This announcement is the one from Example 9. It was proven there that it is a direct exchange.

It is obviously minimal, because there is no exchange of four hands (Proposition 10).

This exchange is also maximal, because no hands can be added without sharing two cards with the five we already have: From the available non-crossing fifth hand candidates 146, 246, 236, 245, we chose to add 246. But then, adding either of 146, 236, 245 creates crossing hands (e.g., 246

and 236 share $(2, 6)$, etc.). Removing those from the announcement leaves an announcement of four hands: not an exchange. ⊣

Proposition 15 *Anne announcing* $\{012, 036, 146, 256, 345\}$ *is a direct exchange. It is both minimal and maximal.*

Proof. Almost identical to that of Proposition 14. ⊣

Proposition 16 *Anne announcing* $\{012, 034, 056, 135, 146, 236, 245\}$ *is a direct exchange. It is maximal, but not minimal.*

Proof. The proof that this is a direct exchange has been omitted (all such proofs are similar). The exchange is maximal, because there is no direct exchange of more than seven hands: Proposition 11. The exchange is not minimal: an arbitrary hand except the actual one can be deleted. See Proposition 18, below. ⊣

Proposition 17 *There are 6 direct exchanges of secrets consisting of seven hands.*

Proof. The first hand 012 is obligatory. The two other hands containing card 0 will contain all four other cards, therefore one of those two will contain card 3. We are free to choose the third card of that hand out of the remaining **three** cards. Then the other hand containing 0 is determined. One of the two other hands containing 1 will also contain card 3 (because the two other hands containing card 1 will contain all four other cards). We are free to choose the third card of that hand out of the remaining **two** cards: our choice must be different from the addition to 0 and 3. Therefore there are $3 \times 2 = 6$ direct exchanges of seven hands. ⊣

Proposition 18 *Anne announcing* $\{012, 034, 056, 135, 146, 236\}$ *is a direct exchange. It is minimal, but not maximal.*

Proof. We omit the proof that it is a direct exchange. Proof of the minimality:

Suppose we remove 236. Then cignorant doesn't hold on the model underlying the resulting state: if Crow had 0, it would learn that Anne has 1.

If we remove 146, cignorant doesn't hold either on the model underlying the resulting state: if Crow had 0, it would learn that Anne has 3. If we remove 135, similarly, if Crow had 0, it would learn that Anne has 6. If we remove 056, similarly, if Crow had 1, it would learn that Anne has 3. If we remove 034, similarly, if Crow had 1, it would learn that Anne has 6.

We can't remove actual deal 012. ⊣

Proposition 19 *There are 36 direct exchanges of secrets consisting of six hands.*

Proof. From all of the 6 direct exchanges consisting of seven hands we can delete an arbitrary hand (except the actual hand). This results in $6 \times 6 = 36$ exchanges. ⊣

Proposition 20 *There are 60 direct exchanges of secrets consisting of five hands.*

Proof. There are 24 direct exchanges where none of Anne's cards $0, 1, 2$ occur thrice, and therefore one of **four** other cards occur thrice (five hands contain 15 card occurrences: six cards occur twice – 12 – and one thrice – 3). If the remaining **three** occur together in one hand, then we can choose one of them to go with card 0 and from the remaining **two** one to go with 1.

There are 36 direct exchanges where one of Anne's cards $0, 1, 2$ occurs thrice: for each of those **three** cards, say 0, some other of these three hands containing that card must contain a 3, the remaining card of that hand may be chosen from one of the remaining **three** cards. This fixes the other hand containing 0. One of the remaining hands contains a 1 and the other a 2. For the hand containing 1 we may choose two out of the four cards not held by Anne, except the two combinations already used with 0. This leaves **four** combinations.

Altogether this makes 60.

Using the above, Proposition 18, and the minimality conditions mentioned before Definition 9, these are indeed all exchanges of five hands. ⊣

Corollary 21 *For given deal* 012|345|6 *there are 102 direct exchanges.*

For a list, see the Appendix.

Now apart from these 102 direct exchanges for Russian cards, are there any other, non-direct, exchanges, consisting of more than two safe communications? Yes, there are. To give a trivial example: Anne could have started by saying "I have one of all possible hands," after which Bill could have given a seven hand announcement from the above (but computed for his own hand, which is 345), after which Anne declares Crow's card. But are such exchanges essentially different? This one isn't. But in general that is not entirely clear. An exchange starting with a communication that is not an extension of any of the 102 direct exchanges, could be said to be 'really' different. Also an exchange ending in an information state that was not reached by any of the 102 direct exchanges can be said to be 'really' different. For example, none of the 102 above reach the information state consisting of $\{012|345|6, 345|012|6\}$ only, where common knowledge of the postconditions holds. Is there an exchange that results in that state? We have not been able to prove that such 'really' different exchanges do not exist. In due time, we hope to confirm this conjecture by exhaustive model checking. Instead, we give some partial results towards this conjecture:

Proposition 22 (Extension of safe communications) *Let π be a safe a-communication announced in some initial state $(I_{\mathbf{3|3|1}}, d)$, and h an a-hand that is described by $\delta^a_{d'}$. Then $\pi \vee \delta^a_{d'}$ $(\pi \cup \{h\})$ is also safe.*

Proof. Because π is safe, $(I_{\mathbf{3|3|1}})_{K_a\pi}, d \models C\mathsf{cignorant}$, therefore $(I_{\mathbf{3|3|1}})_{K_a\pi} \models \mathsf{cignorant}$. Let $e \in (I_{\mathbf{3|3|1}})_{K_a\pi}$, and $q \in Q \setminus d^{-1}(c)$, then $[e]_{\sim_c}$ contains both a deal where Anne holds q and one where Anne doesn't hold q. Now the only way that $\mathsf{cignorant}$ may fail to hold on the extended model $(I_{\mathbf{3|3|1}})_{K_a(\pi\vee\delta^a_{d'})}$ is when removing one less class $[d']_{\sim_a}$ from the initial model (or more), results in leaving a class $[d']_{\sim_c}$ that does not occur in $(I_{\mathbf{3|3|1}})_{K_a\pi}$ and where c knows some of a's cards. But this cannot be the case: $[d']_{\sim_c} \subseteq (I_{\mathbf{3|3|1}})_{K_a(\pi\vee\delta^a_{d'})}$ must be the extension to that model of some $[e]_{\sim_c} \subseteq (I_{\mathbf{3|3|1}})_{K_a\pi}$ that contains both a deal where Anne holds q and one where Anne doesn't hold q (Anne's first announcement, whatever it is, will not publicly rule out *any* specific card for Crow). Therefore, also $(I_{\mathbf{3|3|1}})_{K_a(\pi\vee\delta^a_{d'})} \models \mathsf{cignorant}$, so $(I_{\mathbf{3|3|1}})_{K_a(\pi\vee\delta^a_{d'})}, d \models C\mathsf{cignorant}$. ⊣

Proposition 22 may hold for non-initial card game states as well. Unfortunately the value of such extended safe communications is questionable, because Bill may very well be unable to say anything informative after it:

Example 11 *For example, suppose that in deal* 012|345|6*, instead of communication* {012, 034, 056, 135, 146, 236, 245}*, a had added another hand, say 345. What can Bill still say after Anne says that?*

Bill learns Anne's hand, because he can remove all hands that contain 3, 4, or 5. That includes 345. However, if Bill now announces that Crow's card is 6, as before, Crow now learns, unlike before, that Anne's hand of cards cannot have been any of {034, 135, 245, 345} *(as all of the first three cross with 345), because in that case Bill would not have learnt Crow's card. From the remaining hands* {012, 056, 146}*, Crow can eliminate 056 and 146 because they contain 6, so it can derive the hand of Anne. So Bill cannot say that he knows Crow's card.*

Now suppose that Anne had added hand 016 to her announcement. In this case Bill would not *have learnt Anne's hand. If Bill announces that (or, somewhat similarly, that he doesn't know Crow's card yet), Crow learns that Anne's hand must have been one of 012, 016, 056, 146. From those it can eliminate all but 012, so once again Crow learns Anne's hand. So Bill cannot say that he doesn't know Crow's card.*

Other cases are similar. It is unclear if Bill can say anything at all after this Anne's extended 'safe' announcement. The least he can say is: "Please say something else, Anne," and in consideration of the previous, it may well be commonly known that this is all *he can say.*

We close this section with some observations on variants of direct exchanges for **3|3|1** and other matters of logical interest.

Fact 23 *Each direct exchange results in factual knowledge for Crow.*

Fact 24 *Suppose Crow tries to cheat and privately (i.e., without Anne or Bill noticing) peeks into one or more of Anne's cards. In a seven hand exchange such as* $\{012, 034, 056, 135, 146, 236, 245\}$ *it has in this way to learn privately* **two** *of Anne's cards before it learns her hand. In a five hand exchange where Crow's card is the card occurring thrice, e.g. for deal* $012|345|6$ *the communication* $\{012, 056, 146, 236, 345\}$*, Crow has to learn privately just* **one** *of Anne's cards to learn her entire hand.*

Example 12 (Modulo 7 and sum 12 solutions) *Instead of announcing "My hand is one of* $\{012, 046, 136, 145, 235\}$*" Anne could have said: "The sum of my cards modulo 7 is 3." Announcing the sum modulo seven of your cards is always a direct exchange consisting of five hands.*

If the sum modulo 7 is 5 (and only *in that case) we can even do better. An example of that is* $\{014, 023, 156, 246, 345\}$*. If card 0 had been named 7 instead, all sums would have been 12. See the similar example in section 1: Anne's public renaming of cards to* $1, ..., 7$ *does not provide information. After that, she executes a five hand direct exchange.*

Example 13 *Instead of announcing "My hand is one of* $\{012, 034, 056, 135, 146, 236, 245\}$*," Anne could have said as well: "I have one of* $\{0, 1, 2\}$*, and one of* $\{0, 3, 4\}$*, and one of* $\{0, 5, 6\}$*, and one of* $\{1, 3, 5\}$*, and one of* $\{1, 4, 6\}$*, and one of* $\{2, 3, 6\}$*, and one of* $\{2, 4, 5\}$*." In logic, slightly simplified: instead of*

$$(0_a \wedge 1_a \wedge 2_a) \vee (0_a \wedge 3_a \wedge 4_a) \vee ... \vee (2_a \wedge 4_a \wedge 5_a)$$

Anne could have said

$$(0_a \vee 1_a \vee 2_a) \wedge (0_a \vee 3_a \vee 4_a) \wedge ... \wedge (2_a \vee 4_a \vee 5_a).$$

The two announcements are logically equivalent, the first is a disjunctive normal form of the announcement, so to speak, and the second a conjunctive normal form.

Finally, note that the hands of a seven hand direct exchange can be seen as the seven lines of a projective geometric plane consisting of seven points. The apparent symmetry is an automorphism property of that plane.

5 Generalizations, conclusions, and applications

For the case of three players of which two hold three cards we have exhaustively described the ways in which these two agents can exchange their hands by public communications. Some logical properties of such communications have been proved for arbitrary card deals, most notably that all communications can be about alternative hands for the communicating player.

We have some tentative results for arbitrary card deals. For some deals of cards no exchange exists. An example is the deal where each player holds one card (Example 2). Direct exchanges also exist for deals of size **4|2|1** and **4|7|2** (starting with 7 and 13 hand a-announcements, respectively). If there is an exchange for size **x|y|z**, then there is one for size **x|y|z-1**: in the second case, the first player introduces a virtual extra card for the third player (and the players commonly know that the third player has that card). A trivial application of that, is that we can solve the 3|3|0 'problem': assume that a seventh card named 6 exists as well and that Crow holds it. Then execute one of **3|3|1** direct exchanges. It is trivial, because if Crow doesn't hold any card, Anne and Bill *already* know each other's hand in the initial game state. A non-trivial example is that there is an exchange for **4|7|1** (because there is one for **4|7|2**).

We conjecture the following: If there is an exchange for a given deal of some size, there is a direct exchange. If the conjecture holds, it would greatly simplify the algorithm in Proposition 7

for determining whether an exchange exists for a given deal of cards. There is some suggestive evidence that the conjecture holds: If any update is allowed, and secrecy is no issue, n agents can pool their distributed knowledge in a maximum of n communications. For card deals this may be done by each but the last player saying what their cards are, i.e.: $n-1$ communications. For three players this means: two communications.

Our results are relevant for the analysis of distributed (interpreted) systems [FHMV95] where the agents' local state is interdependent. Can two agents communicate their local state to each other without the remaining agents getting to know those states? This is weaker than the requirement for the Russian cards problem, because it is now allowed to learn *some* of the cards of the communicating players, but just not *all* of them. For the Russian cards problem, this weaker requirement results in shorter solutions:

Example 14 *In* $012|345|6$*, after Anne says: "My hand is one of* $\{012, 034, 056\}$*," and Bill says: "Crow has card 6," it is commonly known that Anne and Bill know each other's hand, and that Crow doesn't. Even though Crow knows that Anne holds card 0, it does not know her hand.*

A general treatment of exchanges for players in card deals is relevant for cryptology. In public/private key cryptography for example, the non-communicating (listening in) agents cannot discover the secrets that are exchanged, because of the unfeasible complexity of factorising a product of large primes. Our cryptographic protocols apply to 'computationally unlimited' agents ('perfect logicians'). An example:

Example 15 *There are seven cards* $0, 1, ..., 6$*. Anne's hand is 125. Unlike before, she now only knows her own cards, that there are seven cards, and that either Bill or Crow hold the three cards 346. She wants to find out who holds the three cards. She realizes that both 251 and 643 are prime numbers... She can now* either *announce: "Who is the first to tell me the factorization of 161393," which we may expect Bill to do faster than Crow, as Bill can simply divide that number by 643 (his 'private key', so to speak),* or *she may announce one of the direct exchanges for hand 125, e.g.: "My hand is one of* $\{125, 023, 246, 045, 356, 016, 134\}$*," after which only Bill, who actually holds 346, and not Crow, is able to tell her that she holds 125. In the first case, Crow is (presumably) not fast enough ('too complex') to pose as Bill with certainty, in the second case, it is impossible to pose as Bill with certainty.*

In Russian cards, Crow has a (commonly known) 25% probability of correctly guessing Anne's hand if she chooses a seven hand exchange, and an expected probability of 33% or 50% of correctly guessing her hand if she chooses a five hand exchange. For larger deals of cards, the probability of guessing correctly decreases. If one choose the card deal large enough, outsiders such as Crow will have a probability below a preferred threshold, say 5%, of correctly guessing the secret. In other words: we design a cryptographic protocol based on card deals that suits our security requirements.

Acknowledgements

A great number of people contributed more or less directly to the research resulting in this article. I want to thank the following people for their contributions: Mike Atkinson, Ben Handley, Wiebe van der Hoek, Gerard van Kempen, Lambrecht Kok, Barteld Kooi, Jarda Opatrny, Rohit Parikh, Marc Pauly, Alexander Shen, B. Vorselaars, Rineke Verbrugge. Marc Pauly originally brought the Russian cards problem to my attention. Lambrecht Kok came up with the 'modulo seven' solution at the time I didn't yet know of the Russian Olympiad solution. Mike Atkinson came up with the 'projective plane' solution. (Its equivalent in conjunctive normal form is my own.) Gerard van Kempen en B. Vorselaars both came up with the 'sum is 12' solution in the prize competition of the journal Natuur & Techniek. Alexander Shen provided valuable comments on my motivation of the common knowledge requirements. Proposition 5 is by Ben Handley. Jarda Opatrny pointed out the validity of the six hand solutions. Wiebe van der Hoek's intensive reading was invaluable at the stage of finishing this article.

References

[AHV02] N. Agray, W. van der Hoek, and E. de Vink. On ban logics for industrial security protocols. In B. Dunin-Keplicz and E. Nawarecki, editors, *From Theory to Practice in Multi-Agent Systems*, pages 29–38. LNAI 2296, 2002.

[Bal02] A. Baltag. A logic for suspicious players: Epistemic actions and belief updates in games. *Bulletin of Economic Research*, 54(1):1–45, 2002.

[BAN90] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8:18–36, 1990.

[EvdMM98] K. Engelhardt, R. van der Meyden, and Y. Moses. Knowledge and the logic of local propositions. In I. Gilboa, editor, *Proceedings of TARK VII*, pages 29–41. Morgan Kaufmann, 1998.

[FHMV95] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge MA, 1995.

[FW96] M.J. Fischer and R.N. Wright. Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology*, 9(2):71–99, 1996.

[Ger99] J.D. Gerbrandy. *Bisimulations on Planet Kripke*. PhD thesis, University of Amsterdam, 1999. ILLC Dissertation Series DS-1999-01.

[GG97] J.D. Gerbrandy and W. Groeneveld. Reasoning about information change. *Journal of Logic, Language, and Information*, 6:147–169, 1997.

[GGL96] R. L. Graham, M. Grotschel, and L. Lovasz, editors. *Handbook of Combinatorics*. MIT Press, Cambridge MA, 1996.

[Mak01] K. Makarychev. Logicheskie voprosy peredachi informacii (logical issues of information transmission). Master's thesis, Moscow State University, 2001. Diplomnaja rabota, part 1.

[MM01] K.S. Makarychev and Yu.S. Makarychev. The importance of being formal. *Mathematical Intelligencer*, 23(1):41–42, 2001.

[MvdH95] J.-J.Ch. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge Tracts in Theoretical Computer Science 41. Cambridge University Press, Cambridge, 1995.

[Pla89] J.A. Plaza. Logics of public communications. In M.L. Emrich, M.S. Pfeifer, M. Hadzikadic, and Z.W. Ras, editors, *Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems*, pages 201–216, 1989.

[SV02] F. Stulp and L.C. Verbrugge. A knowledge-based algorithm for the internet transmission control protocol (tcp). *Bulletin of Economic Research*, 54(1):69–94, 2002.

[vB01] J.F.A.K. van Benthem. Logics for information update. In J.F.A.K. van Benthem, editor, *Proceedings of TARK VIII*, pages 51–88, Los Altos, 2001. Morgan Kaufmann.

[vBDvE+02] J.F.A.K. van Benthem, P. Dekker, J. van Eijck, M. de Rijke, and Y. Venema. *Logic in Action*. ILLC, Amsterdam, 2002.

[vD00] H.P. van Ditmarsch. *Knowledge games*. PhD thesis, University of Groningen, 2000. ILLC Dissertation Series DS-2000-06.

[vD01a] H.P. van Ditmarsch. Killing cluedo. *Natuur & Techniek*, 69(11):32–40, 2001.

[vD01b] H.P. van Ditmarsch. Knowledge games. *Bulletin of Economic Research*, 53(4):249–273, 2001.

[vD02a] H.P. van Ditmarsch. Descriptions of game actions. *Journal of Logic, Language and Information*, 11:349–365, 2002.

[vD02b] H.P. van Ditmarsch. Oplossing van het mysterie (solution of the murder mystery). *Natuur & Techniek*, 70(2):17, 2002.

[vDvdHK02] H.P. van Ditmarsch, W. van der Hoek, and B.P. Kooi. Descriptions of game states. In I. van Loon, G. Mints, and R. Muskens, editors, *Proceedings of LLC9 (2000)*, Stanford, 2002. CSLI Publications. To appear.

Appendix

Proof of Proposition 1: For all formulas in the language, $[\varphi \wedge [\varphi]\psi]\chi$ is equivalent to $[\varphi][\psi]\chi$.

Proof. Let M, w be arbitrary. Then:

$$
\begin{array}{l}
M, w \models [\varphi \wedge [\varphi]\psi]\chi \\
\Leftrightarrow \\
M, w \models \varphi \text{ and } M, w \models [\varphi]\psi \text{ implies } M_{\varphi \wedge [\varphi]\psi}, w \models \chi \\
\Leftrightarrow \\
M, w \models \varphi \text{ and } M_\varphi, w \models \psi \text{ implies } M_{\varphi \wedge [\varphi]\psi}, w \models \chi \\
\Leftrightarrow \qquad\qquad\qquad \text{as } M_{\varphi \wedge [\varphi]\psi} = (M_\varphi)_\psi, \text{ see below} \\
M, w \models \varphi \text{ and } M_\varphi, w \models \psi \text{ implies } (M_\varphi)_\psi, w \models \chi \\
\Leftrightarrow \\
M, w \models \varphi \text{ implies } M_\varphi, w \models [\psi]\chi \\
\Leftrightarrow \\
M, w \models [\varphi][\psi]\chi
\end{array}
$$

We have that $M_{\varphi \wedge [\varphi]\psi} = (M_\varphi)_\psi$, since:

$$
\begin{array}{l}
\mathcal{D}(M_{\varphi \wedge [\varphi]\psi}) \\
= \\
\{v \mid M, v \models \varphi \wedge [\varphi]\psi\} \\
= \\
\{v \mid M, v \models \varphi \text{ and } (M, v \models \varphi \text{ implies } M_\varphi, v \models \psi)\} \\
= \qquad\qquad v \in \mathcal{D}(M_\varphi) \text{ presupposes that } M, v \models \varphi \\
\{v \mid M_\varphi, v \models \psi\} \\
= \\
\mathcal{D}((M_\varphi)_\psi)
\end{array}
$$

⊣

Proof of Proposition 2: For all formulas in the language, $[C\varphi]C\varphi$ is valid.

Proof. Define $\sim_N := (\bigcup_{n \in N} \sim_n)^*$, and $M^w_{\sim_N}$ as the $\sim_N$-generated submodel of M with point w (i.e. with $\mathcal{D}(M^w_{\sim_N}) := \{v \in \mathcal{D}(M) \mid v \sim_N w\}$). Obviously, for all formulas and states, $M, w \models \psi$ iff $M^v_{\sim_N}, w \models \psi$.

Let M, w be arbitrary, and suppose $M, w \models C\varphi$. Let $v \sim_N w$. Then $M, v \models C\varphi$ (using the validity of $C\varphi \to CC\varphi$), and therefore $\mathcal{D}(M^w_{\sim_N}) \subseteq \mathcal{D}(M_{C\varphi})$. Also $M, v \models \varphi$, so $M^v_{\sim_N}, v \models \varphi$, and also $M_{C\varphi}, v \models \varphi$. As $v \in M_{C\varphi}$, it follows that $M_{C\varphi}, w \models C\varphi$. We have now shown that $M, w \models C\varphi$ implies $M_{C\varphi}, w \models C\varphi$, in other words: $M, w \models [C\varphi]C\varphi$. As M and w were arbitrary, it follows that $\models [C\varphi]C\varphi$. ⊣

Direct exchanges for Russian cards:

012 034 056 135 146 236
012 034 056 135 146 236 245
012 034 056 135 146 245
012 034 056 135 236 245
012 034 056 135 246
012 034 056 136 145 235
012 034 056 136 145 235 246
012 034 056 136 145 246
012 034 056 136 235 246
012 034 056 136 245
012 034 056 145 235 246
012 034 056 145 236
012 034 056 146 235
012 034 056 146 236 245
012 034 135 146 236 245
012 034 135 146 256
012 034 135 236 456
012 034 136 145 235 246
012 034 136 145 256
012 034 136 235 456
012 034 145 246 356
012 034 146 245 356
012 034 156 235 246
012 034 156 236 245
012 035 046 134 156 236
012 035 046 134 156 236 245
012 035 046 134 156 245
012 035 046 134 236 245
012 035 046 134 256
012 035 046 136 145 234
012 035 046 136 145 234 256
012 035 046 136 145 256
012 035 046 136 234 256
012 035 046 136 245
012 035 046 145 234 256
012 035 046 145 236
012 035 046 156 234
012 035 046 156 236 245
012 035 134 156 236 245
012 035 134 156 246
012 035 134 236 456
012 035 136 145 234 256
012 035 136 145 246
012 035 136 234 456
012 035 145 256 346
012 035 146 234 256
012 035 146 236 245
012 035 156 245 346
012 036 045 134 156 235
012 036 045 134 156 235 246
012 036 045 134 156 246
012 036 045 134 235 246
012 036 045 134 256
012 036 045 135 146 234
012 036 045 135 146 234 256
012 036 045 135 146 256
012 036 045 135 234 256
012 036 045 135 246
012 036 045 146 234 256
012 036 045 146 235
012 036 045 156 234
012 036 045 156 235 246
012 036 134 156 235 246
012 036 134 156 245
012 036 134 235 456
012 036 135 146 234 256
012 036 135 146 245
012 036 135 234 456
012 036 145 234 256
012 036 145 235 246
012 036 146 256 345
012 036 156 246 345
012 045 134 156 235 246
012 045 134 156 236
012 045 134 246 356
012 045 135 146 234 256
012 045 135 146 236
012 045 135 234 256
012 045 135 256 346
012 045 136 235 246
012 045 146 234 356
012 045 156 235 346
012 046 134 156 235
012 046 134 156 236 245
012 046 134 245 356
012 046 135 236 245
012 046 136 145 234 256
012 046 136 145 235
012 046 136 234 256
012 046 136 256 345
012 046 145 234 356
012 046 156 236 345
012 056 134 235 246
012 056 134 236 245
012 056 135 146 234
012 056 135 146 236 245
012 056 135 245 346
012 056 136 145 234
012 056 136 145 235 246
012 056 136 246 345
012 056 145 235 346
012 056 146 236 345