# Crossing Hands in the Russian Cards Problem

**Tor Hagland**

Dept. of Information Science and Media Studies
University in Bergen
Bergen, Norway

**Thomas Ågotnes**

Supervisor

# Abstract

When communicating using an unconditionally secure protocol, a sender and receiver is able to transmit secret information over a public, insecure channel without fear of the secret being intercepted by a third party. The Russian cards problem is an example of an unconditionally secure protocol where the communication is fully understandable for everyone listening in. Even though everyone can understand what is being said, only the sender and receiver are able to uncover the secrets being transmitted. In this thesis we investigate the interaction among the communicating parties. By extending existing problem-specific software we are able to more efficiently analyze protocols, and we are therefore able to provide an answer to an open problem in the literature. We provide a completely new solution to the Russian cards protocol and show that it fulfills all requirements by the problem. Discovering this new solution provides the person initiating the protocol two new strategies to choose from when constructing the initial announcement of the protocol.

# Contents

# Acknowledgments

I wish to thank my supervisor Thomas Ågotnes for his support and guidance throughout writing this thesis. Thomas Ågotnes allowed me to work independently and still provided interesting ideas and excellent feedback, especially in the last hectic weeks. He also initially introduced me to the problem, which made this thesis possible. I would also like to thank Marija Slavkovik and Truls André Pedersen for many useful discussions surrounding the problem.

I will never be able to thank my family enough for their endless support and motivation throughout the writing of the thesis, especially my mother who provided words of encouragement almost every day in the last weeks. Finally, I would like to thank Neil Anders for support and many useful discussions, not just throughout my thesis but throughout both my bachelor's and master's degree.

# Chapter 1

# Introduction

## 1 Communication protocols

Using the vast amounts of natural languages we have created to communicate with each other has been, and still is an essential part of the evolution of our species. It grants the possibility of discussing ideas, sharing knowledge or experiences and to express ourselves in ways other people can understand, interpret and apply to their own lives. Transmitting secret information has been of interest for a long time in many different settings, may that be secret communication among friends or national secrets being transmitted between several parties. Since the first use of Caesar's cipher some thousand years ago [Merkle, 1978], people have been trying to use different codes and ciphers to hide information transmitted between two parties over an insecure channel.

We can make two distinctions when talking about secure protocols, namely conditionally and unconditionally secure protocols. An example of conditionally secure protocols is the common RSA (Rivest–Shamir–Adleman) encryption schema which is based on private/public key encryption [Rivest et al., 1978]. In a private/public key protocol, the receiver (Anne) has a private and a public key. Anne initiates the protocol by sending her public key to the person that is sending her a message, in this case we name him Bob. Bob then encrypts the message using Anne's public key and sends the encrypted message back. Anne proceeds to use her private key to decrypt the message Bob sent and learns its content [Diffie and Hellman, 1976]. If Anne wants to send a message back to Bob, the protocol would be repeated symmetrically. Anne would need the public key of Bob, encrypt the message using his public key and Bob would be able to decrypt it using his private key. The private key is always kept secret as it is used for decryption, whereas the public key can be sent over public, insecure channels as its function is only to encrypt a message. The assumed security is due to the computational intractability, as it requires factoring a large product of primes [van Ditmarsch et al., 2006].

An unconditionally secure protocol does not rely on such assumptions, and an example is the one-time pad [Diffie and Hellman, 1976]. The one-time pad is a form of encryption that if executed perfectly is impossible to crack, even with unlimited computational power. It takes plain text and encrypts it using some key of the same length as the message. For each message sent using the one-time pad a new key must be generated. The keys are generated randomly and is secretly kept by the recipient(s) [Bellovin, 2011]. Its use is sub-optimal due to the amount of keys needed, which is why other conditionally secure protocols are more feasible [Diffie and Hellman, 1976]. The purpose of conditionally and unconditionally secure protocols are the same, to transmit some information across an insecure channel such that only the recipient and sender knows its content.

This thesis explores a different approach to an unconditionally secure protocol than the one-time pad. The protocol is named 'The Russian Cards Problem'. The problem was originally posed by Kirkman [1847], but garnered increased interest at the Russian mathematics olympiad in 2000 [van Ditmarsch, 2003]. Hans van Ditmarsch named it 'The Russian Cards Problem' in his paper published in 2003, as he thought the problem originated from the olympiad. After he discovered the origin of the problem he tried to rename it, but the name had already stuck in the community [van Ditmarsch and Kooi, 2015].

# 2 The Russian cards problem

The problem posed at the Russian mathematics olympiad in 2000 was as follows:

> *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?*

In the Russian cards problem, which will sometimes be abbreviated to RCP, the information transmitted between the players is modeled as cards. These can be seen as randomly dealt to the players by some third-party, or secretly drawn from a deck of seven cards by the players themselves. How the cards are distributed is not discussed in this thesis, it is rather a case study in the information exchange itself. Originally the cards were labeled from 0 to 6, which is required for some mathematical solutions [Shen et al., 2001]. However, using numbers is not a requirement with the formalization used in this thesis.

Even though the problem description presented above involves three agents and a deck of seven cards, the literature have also looked at a generalized version of the Russian cards problem [Albert et al., 2005, Swanson and Stinson, 2014b]. In the generalized Russian cards problem we might see more than three agents, and also decks of cards that are larger than seven cards [Van Ditmarsch and Soler–Toscano, 2011]. We might also see card distributions that are not equal for Anne and Bob, such as Anne holding an arbitrary amount of cards and Bob holding two cards [Albert et al., 2005]. We mainly focus on the classical version of the Russian cards problem in this thesis, but it is worth noting as there might be mentions of different card distributions throughout the paper.

We first present some attempts at solving the problem, which are not considered proper solutions to the Russian cards problem, some of which are less trivial than others.

Finally we present some actual solutions before going on to describe the language used to study the protocol and the contributions from this thesis.

**Default scenario** When discussing solutions, non-solutions or the problem at large, we must consider some concrete scenario where the players have been dealt their share of the cards. Consider the following naming of players and distribution of cards:

The two players holding three cards are named Anne and Bob. The person holding a single card is named Eve. Anne will be holding the cards 0, 1 and 2. Bob will be holding 3, 4 and 5. Eve is given the last card, 6.

This scenario will be considered the "default" scenario, meaning that if no other scenario is specified this is the card distribution used. It is the easiest to remember, as the cards are being dealt in ascending order and the players are named in a conventional manner when discussing secure protocols.

**Attempting to solve the Russian cards problem** We present three different attempts at solving the original problem, each with their own strategy behind the first announcement. We then discuss why they are not considered proper solutions.

**Attempt 1** Anne announces "I don't have card 6". This might appear as a solution, Eve is holding card 6 and therefore Bob learns Anne's cards - Bob knows he has the cards 345. The remaining cards in the deck from Bob's perspective are 0, 1, 2 and 6. He eliminates 6 from Anne's hand because of her announcement and then concludes that her hand is 012. However, consider the deal to be Anne: 0, 1, 2, Bob: 3, 4, 6 and Eve: 5. Anne does the same announcement: "I don't have card 6". When Eve hears this, she knows that Anne does not have card 6. Eve is now holding card 5, and can therefore conclude that Bob is the person holding card 6. Anne would never announce something that could potentially inform Eve of what cards Bob might hold - and can subsequently not announce any announcement similar to the one presented in this first attempt.

**Attempt 2** Anne announces "I have the cards 012 or Bob has the cards 012". It might seem that Eve is ignorant after this announcement, does she know after this announcement whether Anne or Bob is the person holding 012? Throughout this thesis, we require all players to announce truthful announcements - lying is not allowed in this context. A lie is not informative by nature, and we therefore exclude lies as possible announcements. As a consequence, for Anne to be able to announce this, she has to know that the announcement is true. This is also known by Eve, Eve is fully aware that Anne is unable to lie.

If Anne were to make this announcement she must know that either she is holding 012 or Bob is holding 012. Anne does not know anything about Bob's cards at this point, as Anne is the one initiating the protocol and no information regarding Bob's cards have been transmitted yet. Eve can therefore conclude that Anne's hand is 012, otherwise she would be unable to make the announcement. Anne can only announce something that she knows, and her announcements are therefore much more informative than it might seem because of her restricted amount of knowledge when the protocol is being initiated.

**Attempt 3** Anne announces "I have 012 or 345". This announcement is slightly different from the previous attempt at solving the problem. Here Anne announces two possible hands that she might have, instead of saying that her or Bob have the cards 012. Eve can't eliminate anything in a similar fashion as she could in the previous attempt, as no part of the announcement is considering Bob's cards. However, this announcement falls short in a similar way to the first attempt. Anne doesn't know that Eve might not hold 3, 4 or 5. Similar to the first announcement, this is Anne hoping that Eve is the one holding card 6. If Eve were to hold 3, 4 or 5 she could eliminate the second part of the announcement and conclude with Anne having the cards 0, 1 and 2.

Even though this announcement is not considered a solution, this approach to the problem yield solutions if we increase the amount of alternative hands. In the next section we show both the solution they had prepared at the Russian mathematics olympiad, and an extension of the way Anne constructed her announcement in attempt 3.

### Solving the Russian cards problem

**Solution 1** When the problem was first posed at the Russian mathematics olympiad, they had the following solution prepared [Shen et al., 2001].

> *Each of the players Anne and Bob declares the sum modulo 7 of the three cards they have, with Anne initiating the protocol and Bob following.*

This solution requires the cards to be labeled as integers from 0..6, as the modulo operator is a mathematical operator. It is not an intuitive solution to the problem, and it is rather hard to understand and reason around why this solves the problem. This solution is also not ideal, as it is only proven to work for card distributions where Anne and Bob have equal amount of cards and Eve has one card [Albert et al., 2011].

**Solution 2** If we extend attempt 3 presented earlier, we can show a solution that is much more intuitive because it bases itself on the elimination principle. Anne announces a collection of alternative hands that she might have, and Bob can eliminate all hands except the one Anne is holding. Consider the default scenario. A solution would then be:

> *Anne: My hand is one of 012 or 036 or 156 or 246 or 345*

In Anne's announcement we have that one of Bob's cards is present in all alternative hands except for 012. Bob can therefore eliminate all the alternative hands Anne are announcing except for 012, and conclude that Anne holds 012. As Bob learns Anne's cards, he also learns Eve's card, and can therefore announce it to Anne:

> *Bob: Eve's card is 6.*

Which results in Anne learning Eve's card, and therefore Bob's cards. The protocol is then said to be terminated, as both communicating players know each others cards and Eve is completely ignorant of any card the players hold. From Anne's initial announcement, Eve can eliminate the alternative hands that contain the card that she holds herself. This means that when Eve holds card 6, she can interpret Anne's announcement in the following way:

*Anne: My hand is one of 012 or 345*

Eve is thus not able to determine whether Anne is holding the cards 012 or 345, and the announcement is therefore safe.

But how did Anne know what to announce? Seeing as Anne doesn't know Bob's cards, it might seem like Anne got lucky when Bob could eliminate every hand but one. This is not the case. Anne's announcement is carefully constructed such that she *knows* that Bob can eliminate every hand but one. Notice that every hand in her announcement except the hand she is actually holding contains at most one card that is in her own hand. Therefore, each hand except her actual hand has two or more cards that Anne doesn't hold. Eve has only one card, and Anne therefore knows that even if a hand she announces contains Eve's card, it must also contain one of Bob's cards as there are at least two cards she doesn't hold. This is what guarantees the fact that Bob will learn Anne's cards after her announcement. When an announcement is constructed in this way, it is common knowledge among everyone that Bob is informed after Anne's announcement.

Contrary to the first solution where each player announces the sum modulo 7 of their cards, the labeling of the cards is irrelevant in solution 2 granted that the cards are uniquely identifiable and comparable. The second solution is based on the elimination principle. If Bob can match and eliminate hands based off the cards he is holding, a solution can be found. We could have labeled the cards as letters, sentences, or any other uniquely and comparable construct. Regardless, the convention of labeling the cards as numbers has stuck within the literature and will be used in this thesis as well.

**Problem** There exists an open problem within the literature of the Russian cards problem. It is described in detail in the paper 'The case of the hidden hand' [van Ditmarsch, 2005]. In solution 2 described above, we presented an announcement by Anne that was carefully constructed in such a way that she knew that Bob was going to be informed of which cards she held. Because of the structure of the announcement it was in fact common knowledge among everyone that Bob knew which cards Anne held. van Ditmarsch [2005] explores an announcement where it no longer is common knowledge among all players that Bob knows Anne's cards. He investigates an announcement where it is possible that Eve is unaware of the fact that Bob knows Anne's cards. Unfortunately, the protocol studied by van Ditmarsch was not a solution after all, but if the open problem is solved, we have an unconditionally secure protocol where Anne and Bob knows each others cards and Eve is unaware of this fact. Hans van Ditmarsch provides the following description in the introduction to 'The case of the hidden hand':

> *In case it can be proved that longer protocols can be really different, scenarios are conceivable wherein a sender and receiver have achieved common knowledge of a secret, but where the eavesdropper is uncertain whether this has been achieved and still considers it possible that the protocols has not been finished - thus having to waste resources by keeping an eye on the communicating agents, waiting for possible further communications to intercept [van Ditmarsch, 2005].*

The complexity of such a protocol is evident from the fact that van Ditmarsch initially published the paper in 2004 where he came to the wrong conclusion that it was safe protocol but that it was identical to a previous solution. He later came to the correct conclusion that the protocol wasn't safe after all, and the paper was republished in 2005 with the new conclusion [van Ditmarsch, 2004, 2005]. Finding a protocol that fits the description above, investigating the open problem from 'The case of the hidden hand' is what is tackled in this thesis.

**Approach and research questions** Most of the previous work on the Russian cards problem have been purely analytical approaches using various ways of formalizing the problem. The two most common are combinatorics and formal logic [Albert et al., 2005, Swanson and Stinson, 2014b, Shen et al., 2001, van Ditmarsch, 2003, 2005, van Ditmarsch et al., 2007].

Since purely analytical approaches have been sometime unsuccessful and prone to error, my approach will be to develop a software tool that will augment traditional analytical methods. The goal of this tool is to (1) be able to exhaustively generate all possible announcements in various settings and (2) verify their properties. Such a tool will, if it is computationally efficient, allow us to decide whether or not there exists a solution to the open problem posed by van Ditmarsch, and to avoid mistakes.

1 Does the open problem in 'The case of the hidden hand' have a solution or not?

2 If a solution to the open problem exist, what is a concrete example of a protocol with the desired properties?

3 What is the correspondence between combinatorial axioms and logical formulas?

4 How can a software tool be developed and used to give further insight into the Russian Cards Problem?

**Contribution** In this thesis we try to answer and clarify all the preceding research questions. We provide a concrete solution to the open problem posed by van Ditmarsch in 'The case of the hidden hand'. This solution inhibits all desired properties, and is a completely new solution to the Russian cards problem. The correspondence between combinatorial axioms and logical formulas is important to clarify the connection between the formal language used in this thesis and combinatorial structures. It is also helpful in the context of the software tool that has been developed together with this thesis as it reduces computational complexity and thus the execution time of the software. The software presented in this thesis is an extension of existing software, but the existing software did not have sufficient functionality to uncover the results provided in this thesis in an effective manner as it only provides the possibility of manually constructing announcements and validating them [van Ditmarsch et al., 2006][1].

The solution to the open problem would not have been found without the software provided in this thesis, as it was required to exhaustively validate solutions based off the different criteria - separating them in the following way:

> *[..] How can the players with three cards openly (publicly) inform each other about their cards [..]*

This requirement can be separated from:

> *[..] without the third player learning from any of their cards who holds it?*

The extended software presented in this thesis is able to discern these criteria, and exhaustively generate solutions that only fulfills the first, but not the second and vice versa.

**Motivation** The motivation for pursuing this problem is to increase the understanding of the interaction between the communicating agents in an unconditionally secure protocol. In an unconditionally secure protocol, the communicating agents are able to exchange secret information with truthful and public announcements even though a third party is listening. Such a protocol is impossible to decipher, even with unlimited computational power, and it is therefore very interesting to dig deeper into the interaction among the communicating agents. Analyzing the Russian cards problem involves complex higher-order epistemic analysis. A framework to analyze and reason around the knowledge of the involved agents is therefore desired. This ties in with the motivation for research question 3, where we investigate the correlation between combinatorial axioms and logical formulas. Logical formulas represent this higher-order knowledge in a way that is easier to reason around and understand compared to combinatorial structures.

A fascinating aspect of this particular unconditionally secure protocol is that throughout the protocol the person listening in can understand everything the communicating agents are saying. This is not the case for the one-time pad. The one-time pad encrypts messages using one-time keys that are randomly generated. In the Russian cards problem the messages sent between the players are not even encrypted. They are understandable for everyone listening in. It is the structure of the messages that hides the true meaning of the communication between the players.

Another important distinction between the one-time pad and the Russian cards problem is that the one-time pad requires a pre-arranged set of randomly generated keys to be distributed to the recipient(s) of the message. This is not the case for the Russian cards

[1] http://www.cs.otago.ac.nz/staffpriv/hans/aoard/ has an updated version of the RCP software.

problem. There are no pre-arrangements needed between the two communicating agents, they are simply dealt their share of the cards and are able to share this information publicly, and not even encrypted, over an insecure channel.

The Russian cards problem exhibits an undecipherable protocol where all announcements are fully understandable by everyone, and from the contribution of this thesis the protocol may sometimes have the property that the communicating players have common knowledge of the card deal, but Eve does not know that and thus Eve does not know that the protocol has finished. This results in Eve having to continue to listen for announcements, even though the protocol has ended. The proposed solution of the Russian cards problem from this thesis therefore has some highly unique properties compared to other secure protocols.

**The rest of the thesis** In the next chapter we introduce the formal language and notation used to describe the problem. In chapter 3 we discuss some of the known results from existing literature. In chapter 4 we present the software tool and its place within the analysis of the problem. In chapter 5 we present the main results from this thesis, and finally in chapter 6 we conclude the thesis and project some future work on the Russian cards problem.

# Chapter 2

# Preliminaries

## 1 General concepts

Consider the problem description:

> *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?*

From the description there are certain elements of the protocol that are important to identify and distinguish throughout the thesis. The following list describes and identifies domain-specific aspects of the problem.

> **Players** The words player(s) and agent(s) will be used interchangeably from here on out. From the problem description we have that there are three agents. Two of them holding three cards, and a third holding one card. The agents holding three cards are named Anne and Bob. The third agent is named Eve, short for eavesdropper as this is the agent only listening in to the communication between Anne and Bob. Eve does not engage in any communication herself.
>
> **Deck** The deck of cards is always publicly known to every player. Each agent knows how big the deck is as well as what each card is labeled. For the original Russian cards problem we have a deck of size 7. The deck will always be represented as a set, denoted by $D$.
>
> **Cards** Let $|D|$ be the size of the deck. The cards will in this thesis be labeled from $0..(|D| - 1)$. For the original problem description with $|D| = 7$, we have that $D = \{0, 1, 2, 3, 4, 5, 6\}$.
>
> **Card distribution** In this thesis I mainly focus on the original card distribution in the theoretical part of the thesis. However, as the literature have expanded to

generalized versions of the Russian cards problem, there will sometimes be mentions of other card distributions. A card distribution is represented as an 3-tuple. The last element of the tuple is always Eve's amount of cards. Elements prior to Eve are respectively Anne and Bob's amount of cards. The card distribution representation for the original problem description is therefore $(3, 3, 1)$. If we take the 3-tuple $(4, 2, 1)$, it would indicate that Anne has four cards, Bob has two cards and Eve has one card.

Lastly, we separate the problem description's two criteria:

**Informative** Anne and Bob must know each other's cards at the end of the protocol.

**Safe** For any given card other than her own, Eve must not know whether Anne or Bob is the one holding it.

Informativity and safety are closely related, but separating them gives more granularity when describing why a solution is indeed a solution, and why one is not. Bundling them together is important as they collectively define the postconditions of the protocol, but when studying a specific information exchange they should be discussed separately from one another. Safety takes into account Eve's informativity and what knowledge the other agents have regarding Eve's informativity. Informativity only looks at what the communicating agents know about each other's cards. These two criteria have been linked together, saying that informativity is a requirement for safety [Albert et al., 2005]. We investigate this correspondence later, and show results that do not correlate with the assumption that safety necessarily is dependent on informativity.

# 2 Public Announcement Logic

## 2.1 Epistemic models

An epistemic model is a tuple $M = \langle A, S, \sim, V, PROP\rangle$. $A$ is the set of all agents in the epistemic model. $S$ is the set of all possible worlds (states). $\sim$ is a function giving every $a \in A$ a binary relation $\sim_a \subseteq S \times S$. More commonly called an "accessibility relation". $V$ is a valuation function, indicating which propositions are true in the different states. It is defined in the following way: $V : \mathrm{PROP} \to \wp(S)$. PROP is a finite set of atomic propositions [van Ditmarsch et al., 2007]. We can then list each of the sets with their respective description as follows:

**A** The set of all agents present in the model.

**S** The set of all states (possible worlds).

$\sim$ The accessibility relation for an agent $a$ ($\sim_a$) is a set of relations, where each relation connect two states. If there exists a relation between two states for an agent, this means that the agent deem these states as indistinguishable. If a relation among two states exist, it is because their valuation of propositions for an agent is equal in those two states.

**PROP** The set PROP is a finite set containing every atomic proposition that is present in the model.

**V** The valuation function determines in what possible worlds an atomic proposition is true. This way, we can give an atomic proposition as input, and the function will return a set of states where this proposition is true.

## 2.2 Language

Public Announcement Logic uses epistemic models as the foundation for the language. It specifically uses a strict subset of epistemic models called S5-models. An S5 model is an epistemic model where $\sim$ is an equivalence relation. An equivalence relation is a binary relation $R$ which satisfies the following three properties.

**Transitivity**: $\forall x \forall y \forall z((x,y) \in R \wedge (y,z) \in R) \Rightarrow (x,z) \in R$

**Symmetry**: $\forall x \forall y (x,y) \in R \Rightarrow (y,x) \in R$

**Reflexivity**: $\forall x (x,x) \in R$

Public announcement logic uses modal operators for knowledge and public announcements. We define the syntax of the language using BNF-notation [van Ditmarsch et al., 2007]. Consider $a \in A$, $K_a\varphi$ is then read as "Agent $a$ knows $\varphi$ to be true. Consider $B \subseteq A$, $C_B\varphi$ is read as "It is common knowledge among the agents that belong to group B that $\varphi$ is true.", $[\varphi_1]\varphi_2$ is read as "After $\varphi_1$ is announced, $\varphi_2$ is true."

$$\varphi ::= p|\neg\varphi|\varphi \wedge \varphi|K_a\varphi|C_B\varphi|[\varphi_1]\varphi_2 \tag{2.1}$$

The semantics of PAL is defined in the following way [van Ditmarsch et al., 2007]. $R^*$ is the reflexive-transitive closure on the relation R. The relation $s \sim_B t$ is short-hand for $(\bigcup_{a \in B} \sim_a)^*$. $M|\varphi$ is intuitively interpreted to be the epistemic model $M$ where $\varphi$ has been announced. $[[\varphi]]_M$ is the set of states in model $M$ where $\varphi$ is true. $M|\varphi = \langle S', \sim', V' \rangle$ is defined to be the following:

$$[[\varphi]]_M = \{s | s \in S \wedge M, s \models \varphi\}$$

$$S' = [[\varphi]]_M$$

$$\sim'_a = \sim_a \cap [[\varphi]]_M \times [[\varphi]]_M$$

$$V'(p) = V(p) \cap [[\varphi]]_M \times [[\varphi]]_M$$

We now recursively define when $M, s \models \varphi$ holds, for all $\varphi$:
$M, s \models p \Leftrightarrow s \in V(p)$
$M, s \models \neg\varphi \Leftrightarrow M, s \not\models \varphi$

$M, s \models \varphi_1 \wedge \varphi_2 \Leftrightarrow M, s \models \varphi_1 \wedge M, s \models \varphi_2$
$M, s \models K_a\varphi \Leftrightarrow \forall t \in S$ where $s \sim_a t : M, t \models \varphi$
$M, s \models C_B\varphi \Leftrightarrow \forall t \in S$ where $s \sim_B t : M, t \models \varphi$
$M, s \models [\varphi_1]\varphi_2 \Leftrightarrow M, s \models \varphi_1 \Rightarrow M|\varphi_1, s \models \varphi_2$

All other boolean connectives are defined using different combinations of negation ($\neg$) and conjunction ($\wedge$).

# 3 PAL and S5 models in RCP

## 3.1 An RCP S5 model

With the language defined, we can then look at how an RCP S5-model will look like. This model is equivalent to the one used when implementing the Russian cards problem in Haskell [van Ditmarsch et al., 2006]. If we take the list describing a generic S5-model from earlier, and change the description to fit RCP we get the following:

**A** The set of all agents present in the current problem. In this thesis we look at the three-agent case. This leaves $A$ to always consist of the following elements: $A = \{Anne, Bob, Eve\}$.

**S** The set of all states. These will in RCP correspond to different distributions of cards, such as in state 1 we have that Anne is holding $\{0, 1, 2\}$ whereas in state 6 she might be holding $\{2, 3, 4\}$. The complete description for a specific state will sometimes be represented in short-hand notation in the following way: 012.345.6. Here we have that Anne is holding $\{0, 1, 2\}$, Bob is holding $\{3, 4, 5\}$ and Eve is holding $\{6\}$.

**$\sim$** The accessibility relation for an agent $a$ ($\sim_a$) is a connection between two states for an agent. A connection between states $s$ and $t$ exists if and only if the cards that the appropriate agent is holding are the same in both $s$ and $t$. This way, the agent cannot discern these states, as the information the agent has is the same in both.

**PROP** The set PROP is a finite set containing every atomic proposition that might be used in the model. In RCP this set consists of $(|A| \cdot |D|)$ amounts of propositions. This is because for every agent in the model, we have one proposition for every card in the deck.

The propositions are represented in the following way: $1_a$ indicating that Anne is holding card 1. The number represents the card, the subscript letter denotes the first letter in the agents name. $1_b$ represents Bob holding card 1, $1_e$ represents Eve holding card 1. The numbers might be chained together to describe the full hand of an agent. In which case, the representation: $012_a$ is used to say that Anne is holding the cards 0, 1 and 2. Writing $012_a$ to describe what cards an agent has is short-hand notation for the following logical formula:

$$0_a \wedge 1_a \wedge 2_a$$

**V** The valuation function determines in what possible worlds an atomic proposition is true. In RCP this function describes in what states an agent is holding a card. So for instance, if the proposition is: "Anne is holding card 0" and you give that as input to the valuation function it would return the states where Anne is holding card 0.

The amount of states in the Russian cards problem varies depending on the size of the deck and how many cards each agent is holding. For the original problem we have a deck of 7 cards, Anne and Bob holding 3 cards and Eve 1 card. This gives the model 140 states, from the following equation:

$$\binom{7}{3}\binom{4}{3}\binom{1}{1} = 140$$

Mathematically, the model looks like this, where $M$ is the Russian cards model with the card distribution (3,3,1).

$$M = \langle S, A, \sim V, PROP\rangle$$

$S = \{012.345.6, 012.346.5, 012.356.4, ...\}$
$A = \{\text{Anne, Bob, Eve}\}$
$\sim_a = \{(\mathbf{012}.345.6, \mathbf{012}.346.5), (\mathbf{012}.356.4, \mathbf{012}.345.6)...\}$
$\sim_b = \{(012.\mathbf{345}.6, 016.\mathbf{345}.2), (012.\mathbf{345}.6, 026.\mathbf{345}.1)...\}$
$\sim_e = \{(012.345.\mathbf{6}, 013.245.\mathbf{6}), (012.345.\mathbf{6}, 014.235.\mathbf{6})...\}$
$V(0_a) = \{\mathbf{0}12.345.6, \mathbf{0}13.245.6, \mathbf{0}14.235.6...\}$
$PROP = \{\ i_a \mid \forall a \in A,\ \forall i \in D\}$
Bold is used in the equivalence relations to clarify why the relation exists, and bold is also used in the valuation-function example to clarify why the state is included in the resulting set. In this case it is only used for visual presentation, and it provides no further syntactic or semantic meaning to the numbers beyond that.

When using epistemic operators that involve the agents such as $K$, instead of writing $K_{Anne}\varphi$ to indicate that Anne knows $\varphi$ to be true, the shorter version: $K_a\varphi$ will be used. This is true for Bob as well so that $K_{Bob}$ is shortened to $K_b$, and similarly for Eve, using $K_e\varphi$ when representing her knowledge.

Common knowledge represents the knowledge of some group of agents $B$ where $B \subseteq A$. In this thesis there are two different groups of agents used in combination with the common knowledge operator. Either the group of all agents, or only the communicating agents Anne and Bob. When representing common knowledge among all agents, we use $C_A\varphi$. When representing it only for Anne and Bob, we use $C_{\{ab\}}\varphi$. From here on out I will omit the curly braces, and use the short-hand notation $C_{ab}\varphi$ to indicate common knowledge among Anne and Bob.

When representing RCP in PAL, we can view the announcements as a collection of disjunctions, where each disjunct is a possible hand of cards the announcer can have [van Ditmarsch, 2003]. These are represented in natural language in the following way:

*Anne announces: "My hand of cards is 012 or 135 or 456"*

In PAL we must add the knowledge-operator $K$ before the disjunction of alternative hands. [van Ditmarsch, 2003, 2005, van Ditmarsch et al., 2006] This is because Anne is announcing that she *knows* that her hand of cards is one of the disjuncts. If we were to represent it in the following way:

$$(012_a \vee 135 \vee 456)$$

It would mean that some "insider" who has insight into every hand is announcing it. Anne knows much less than someone who has insight into every agents' hand. Anne is only aware of what cards the deck contains, and her own hand of cards in the initial state of the protocol. Her announcements are therefore much more informative to the other agents than some agent that has insight into everyone's hand [van Ditmarsch, 2003]. It is therefore important to include the knowledge operator before every collection of disjunctions - as it is Anne announcing that her hand is one of the alternative hands. The above is translated into PAL in the following way:

$$K_a(012_a \vee 135_a \vee 456_a)$$

# Chapter 3

# Related work

Representing the protocol has been done in many different ways. There has been built a geometrical protocol [Cordón-Franco et al., 2015], a colouring protocol [Cordón-Franco et al., 2013], combinatorial protocols viewing the communication as lines in the fano plane [Albert et al., 2005] and a formal representation using epistemic logic, which was first done by van Ditmarsch in his paper 'The Russian Cards Problem' published in 2003 [van Ditmarsch, 2003]. The representation in PAL has since been used in further research exploring the Russian cards problem, and its representation has been used together with the model checker DEMO built by Jan van Eijck [van Ditmarsch et al., 2006]. The model checker was made for epistemic models, and it can be used to validate whether announcements are considered to be solutions [van Ditmarsch et al., 2007, van Ditmarsch and Kooi, 2015, van Ditmarsch et al., 2006]. The main two constructs we focus on in this thesis is the basic combinatorial protocol, which uses set-theory to describe the protocol, and public announcement logic as it is the chosen language for this thesis to represent the problem. Public announcement logic provides a formalization that translates very well into natural language, and arguably a more intuitive structure for the Russian cards problem. Below I show an announcement represented in PAL, and its equivalent using set-theory, which is the construct often seen in the combinatorics literature. [Albert et al., 2005, Swanson and Stinson, 2014a,b]

**PAL**: $K_a(012_a \vee 034_a \vee 145_a \vee 246_a \vee 056_a)$

**Combinatorics**: $\{\{0,1,2\},\{0,3,4\},\{1,4,5\},\{2,4,6\},\{0,5,6\}\}$

When the PAL formula is announced, it is intuitively interpreted as "Anne knows that her hand of cards is either 012, 034, 145 or 056". As mentioned on the previous page, adding the knowledge operator is important here because of how the other agents interpret the announcement. This dimension is lost when representing the problem in combinatorics, as it is just a set of sets. PAL therefore exposes the intricate details of the Russian cards problem in a superior way compared to the combinatorial structure.

This chapter will discuss some of the known results regarding the Russian cards problem. It will also look at some of the concepts that are generally important when discussing the Russian cards problem. Firstly, we will formally define what is considered a solution to the Russian cards problem in PAL.

**Formal solution** The epistemic requirement for a solution is described as Anne and Bob having common knowledge of each others cards. It is also required that it is common knowledge among all agents that Eve is completely ignorant of any card an agent might hold - other than the card she is holding herself [van Ditmarsch, 2005]. We define three different formulae to help model these requirements [van Ditmarsch, 2005]:

$$aKnowsBs = \bigwedge_{i \neq j \neq k \in D} (ijk_b \rightarrow K_a ijk_b)$$

$$bKnowsAs = \bigwedge_{i \neq j \neq k \in D} (ijk_a \rightarrow K_b ijk_a)$$

$$eveIgnorant = \bigwedge_{d \in D} \bigwedge_{n = a,b} (\neg K_e d_n)$$

*aKnowsBs* is intuitively interpreted as "if Bob's hand is *ijk* then Anne knows that Bob's hand is *ijk*". Similarly for *bKnowsAs*. *eveIgnorant* is intuitively interpreted as "For any card in the deck, Eve does not know whether it is Anne or Bob holding that card."

We can then formally model the postconditions as the following [van Ditmarsch et al., 2006]:

$$postcondition = C_{ab}(aKnowsBs \wedge bKnowsAs) \wedge C_{abe} eveIgnorant$$

If this requirement is met, we say that a protocol is finished or terminated.

**Direct exchanges** One of the most central concepts in the Russian cards problem is a protocol that is considered a direct exchange as a large part of the literature only considers protocols that are defined to be direct exchanges [van Ditmarsch, 2003, Albert et al., 2005, van Ditmarsch et al., 2006, Swanson and Stinson, 2014a]. In the original setting of the Russian cards problem, a protocol is said to be a direct exchange if it finishes in two steps [van Ditmarsch, 2003]. In the classical setting, a direct exchange consists of a single announcement by Anne, which informs Bob of what cards Anne are holding. Bob then announces Eve's card, and the direct exchange is finished. The direct exchange property of the protocol is an important one, because it restricts the amount of possible announcements we need to consider and the complexity of the protocol vastly [Albert et al., 2005]. Direct exchanges is therefore a central concept of the literature.

If a protocol is to be considered a direct exchange, it must inhibit the following property:

$$M|An, s \models C_{ab} bKnowsAs \tag{3.1}$$

This means that after the initial announcement by Anne, it must be true that it is common knowledge among Anne and Bob that Bob knows Anne's cards. What this results in, is the common knowledge that Bob is informed of Anne's cards and Bob is therefore able to identify which card Eve holds. Bob can then announce Eve's card to terminate the protocol. We could also look at a direct exchange with the stronger property:

$$M|An, s \models C_A bKnowsAs \tag{3.2}$$

Here we require that it is common knowledge among all agents that Bob is informed of the card deal. We will see later in this thesis that the above formula is actually equivalent to another important concept of the RCP literature, namely *crossing hands.*

**Crossing hands** Crossing hands is another concept introduced by van Ditmarsch in his original paper on the Russian cards problem in 2003. It was originally presented as the following, in proposition 31 by van Ditmarsch [2003]. Here hands are different alternative hands in a single announcement:

> *We call hands that have a pair of cards in common: crossing hands [van Ditmarsch, 2003].*

An example of an announcement with crossing hands is the following:

$$K_a(0\mathbf{12}_a \vee \mathbf{12}3_a \vee 245_a \vee 036_a) \tag{3.3}$$

Formula (3.3) is an example of an announcement containing crossing hands, as the two cards 1 and 2 are present in two different alternative hands, expressed using bold text. The following is an announcement without crossing hands:

$$K_a(012_a \vee 245_a \vee 036_a \vee 135_a) \tag{3.4}$$

Mind that van Ditmarsch [2003] only considers the card distribution (3,3,1). However, as the literature have expanded to other card distributions, it has since been found a generalized definition of it. Consider $a$ to be Anne's amount of cards and $e$ to be Eve's amount of cards. The generalized definition of crossing hands is then:

> *Hands that have (a - e) cards in common [Albert et al., 2005].*

For (3,3,1) this would be 3 - 1 = 2 (a pair). Crossing hands has strong ties to a direct exchange. It has even been proven that if Anne makes an announcement without crossing hands, Bob will always be informed of what cards she hold after her initial announcement [Albert et al., 2005]. Therefore, after an announcement without crossing hands - Bob is informed of Anne's cards. He is therefore able to announce Eve's card(s), and we have a direct exchange. We also need to combine this with the requirement of safety, as there does exist announcements without crossing hands that are not safe announcements. An example being:

$$K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a)$$

This announcements does not fulfill Proposition 29 from van Ditmarsch [2003] which states:

> *Proposition 29. Every card occurs at least twice in a safe communication.*

Seeing as card the card 2 only occurs in the first alternative hand, it is not considered a safe announcement - it does however satisfy the crossing hands constraint. The crossing hands constraint is therefore not sufficient for safety. If we combine the crossing hands constraint with the requirement of safety in the classical RCP setting, we get the 102 direct exchanges that are considered proper solutions to the classical setting [van Ditmarsch, 2003]. We show later that not allowing crossing hands is equivalent with formula 3.2, which makes all safe announcements without crossing hands known direct exchanges for all agents.

Albert et al. [2005] describes another complexity of a direct exchange that is not as thoroughly studied. It describes an announcement by Anne that does include crossing hands. Even though it contains crossing hands it is a known direct exchange by the communicating agents in some cases. The slight difference being that it is not known to be a direct exchange by Eve. The announcement briefly described is the following:

$$K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a \vee 235_a)$$

However, it is not acceptable as a solution due to the complications expressed by van Ditmarsch [2005]. If the card deal is 012.345.6 and Anne makes the announcement above, then it is a direct exchange and it is common knowledge among the communicating agents that it is. But it is important to note that if the card deal is 135.046.2 then it is not common knowledge among the communicating agents that it is a direct exchange, because Bob is uncertain whether or not Anne is holding 135 or 235. In this case, it must be investigated whether or not there are protocols that eventually satisfies the postconditions. Albert et al. [2005] also states on the next page that it is not a safe announcement under an epistemic axiom that is informally defined in natural language. We will investigate this statement later, and explain why it not necessarily has to be true.

# Chapter 4

# Model checking Russian cards

## 1 Model Checking

Model checking is the practice of using software to model complex state systems [Clarke Jr et al., 2018]. It can be used to systematically verify formulae and augment traditional analytical methods of verifying logical formulas. Implementations have been done for various logical languages, such as Computation Tree Logic or Linear Temporal Logic [Clarke Jr et al., 2018]. In this thesis we use a model checker suitable for Public Announcement Logic. Model checking the Russian cards problem has previously been done using three different model checkers, MCK, MCMAS and DEMO [van Ditmarsch et al., 2006]. MCK and MCMAS are model checkers for temporal epistemic logics, whereas DEMO is an S5-model checker for dynamic epistemic logics, which is implemented in Haskell by Jan van Eijck [van Eijck, 2014].

**DEMO S5** DEMO is short for Dynamic Epistemic MOdelling. For the purpose of this thesis we chose to extend the newest version of DEMO with two new functionalities. Common knowledge was present in the previous version of DEMO[1], however, it was removed in the newest version[2], and so it was necessary to extend the newest version with common knowledge. It was also necessary to add a new way to construct propositions. As DEMO is written in Haskell, every line of code presented in this thesis is Haskell code. Propositions were initially defined in the following way:

```
data Prp = P Int | Q Int | R Int | S Int deriving (Eq,Ord)
```

This implementation made it impossible to create generic RCP models, as each proposition P, Q, R or S was tied to an agent, and the integer was indicating whether or not the respective agent held that card. This would put the maximum allowed agents at

[1] https://homepages.cwi.nl/~jve/papers/04/demo/

[2] https://homepages.cwi.nl/~jve/software/demo_s5/

4, because there were only 4 propositions to choose from. The extended definition of propositions is the following:

```
  data Prp = P Int | Q Int | R Int | S Int | Prop Agent Int deriving (Eq,Ord)
```

The added structure of a proposition makes it possible to assign an integer to an agent, this way it is possible to create any amount of agents in an RCP model, indicating the cards that the agent holds. This is equivalent to first-order logic with the closed-world assumption.

The implementation of the RCP by van Ditmarsch et al. [2006] was specific only to the original problem description. This means that their generation of an RCP S5-model only supported the card distribution where Anne and Bob has three cards and Eve has one card. As the literature has expanded to the generalized Russian cards problem, I created a generic RCP S5-model generator. This model generator is able to generate any RCP S5-model, where you can have $n$ agents, and each agent can have any amount $x$ cards. Even though this thesis focuses on the classical setting of the Russian cards problem, the generation of Russian card models with arbitrary amount of agents and cards can be beneficial for further research. The function's signature is as follows:

```
generateRCPModel :: [Int] -> EpistM Int
```

Where the list of integers denotes the card distribution. To create the S5-model of the Russian cards problem as described in the original problem description, the syntax is as follows.

```
let model = generateRCPModel [3,3,1]
```

The resulting model is provided in the appendix. There is one limitation when generating the RCP model, which is that the list must be of some finite length $n$. Even though Haskell supports infinite lists due to lazy valuation, an S5 model requires a finite set of agents [van Ditmarsch et al., 2007] p.17. Because every element of the list represents the amount of cards an agent holds, this list cannot be infinite due to the limitation on S5-models. The following describes two valid uses of the function and one invalid, respectively.

```
VALID:
let model = generateRCPModel [5,4,3,2,1]
let model = generateRCPModel [100,100,50]

INVALID:
let model = generateRCPModel [1..]
```

It is important to note that the actual state of the model is always set to the state 012.345.6 when generating the model.

**Validating single solutions** I have implemented the possibility of constructing announcements. It is a function that takes as arguments a list of list of integers and an agent. The lists within the list are the alternative hands that are to be announced, the agent is the one announcing it.

```
integerAnnouncementToProp :: [[Int]] -> Agent -> Form a
```

If we wish to check whether an announcement satisfies all postconditions where crossing hands are not allowed, we can use the following function.

```
noCrossingHandsSuccess :: EpistM Int -> Form Int -> Bool
```

We therefore have the following workflow to manually check if one single announcement satisfies the conditions of the Russian cards problem.

```
> :l Solutions.hs
> let anne = Ag 0
> let announcement = integerAnnouncementToProp [[0,1,2], [3,4,5]] anne
> let model = generateRCPModel [3,3,1]
> EpistmProt.noCrossingHandsSuccess model announcement
> False
```

**Exhaustively generating solutions** To exhaustively generate and validate all possible solutions to the Russian cards problem have, to the best of my knowledge, not been done before. The amount of announcements Anne can make is extremely large, but can be reduced through propositions proven in the existing literature. Consider the card distribution (3,3,1), and the actual card deal to be 012.345.6. The following lists some of the restrictions we can make when generating all possible announcements for Anne.

> **Lower bound** If an announcement is to be considered a solution, it must contain at least five alternative hands [van Ditmarsch, 2003].
>
> **Upper bound** If an announcement is to be considered a solution it can at most consist of seven alternative hands. (Under the assumption that it is common knowledge that the protocol is a direct exchange) [van Ditmarsch, 2003].

There are $\binom{7}{3} = 35$ possible hands Anne can announce. If we are to check every possible announcement within the bounds of the (3,3,1) distribution, we have the following amount of announcements to check.

$$\binom{35}{5} + \binom{35}{6} + \binom{35}{7} = 8,672,312 \tag{4.1}$$

The reason we use combinations and not permutations is due to the fact that announcements are a collection of disjunctions. As a disjunction holds the commutative property, the ordering of them is irrelevant. Luckily, public announcement logic restricts us to only being able to announce true announcements. Anne's actual hand must therefore be in every announcement. This reduces the amount of announcements to the following.

$$\binom{35}{4} + \binom{35}{5} + \binom{35}{6} = 2,000,152 \tag{4.2}$$

Validating these 2,000,152 different possible announcements, and generating the 102 solutions that exist within the lower and upper bound of (3,3,1) takes vast amounts of time using the model checker, but using the combinatorial axioms described in Albert et al. [2005] is significantly faster due to it being simple boolean checks on the results of set-operations. We therefore show proof of their equivalence to public announcement logic, and we also point out a slight imprecision in their proof of the equivalence between the safety axioms in the next chapter. Proving this gives the possibility of interchangeably using the safety axioms from either PAL or combinatorics. There are two ways to calculate all the 102 known solutions to the Russian cards problem using the extended software, using the epistemic requirements or the combinatorial requirements respectively:

```
> :l Solutions.hs
> let anne = Ag 0
> let solutions = EpistmSol.solutions_epistm_all_withinBounds [3,3,1] anne
> length solutions
> 102
```

```
> :l Solutions.hs
> let anne = Ag 0
> let solutions = CombSol.solutions_comb_all_withinBounds [3,3,1] anne
> length solutions
> 102
```

The reason we specify the agent when calculating the combinatorial solutions is that we want the output to be structured as PAL formulae, so that they can be used in conjunction with the rest of the epistemic part of the software if needed.

It is also possible to specify the bounds explicitly, as done in the following way:

```
> :l Solutions.hs
> let anne = Ag 0
> let solutions = CombSol.solutions_comb_specifyLower_noCrossing [3,3,1] 5 anne
> length solutions
> 60
```

```
> :l Solutions.hs
> let anne = Ag 0
> let solutions = EpistmSol.solutions_epistm_specifyLower_noCrossing [3,3,1] 5 anne
> length solutions
> 60
```

# Chapter 5

# Results

## 1 Crossing Hands in the Russian Cards Problem

Crossing hands was first defined to be: ”Hands that have 2 cards in common” [van Ditmarsch, 2003]. The following is a formalization of proposition 32 given in van Ditmarsch [2003], where $H_{An}, G_{An}$ are alternative hands in some arbitrary announcement $An$. The announcement $An$ is in this case modeled using the combinatorial set of sets structure.

$$\forall H_{An} \forall G_{An} (H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2) \tag{5.1}$$

As the literature extended to the generalized Russian cards problem, so did the definition of crossing hands. Consider $a$ to be the amount of cards Anne is holding, and $e$ to be the amount of cards Eve is holding. The generalized version of crossing hands is ”Hands that have ($a$ - $e$) cards in common” [Albert et al., 2005]. The negated version of this formula is described in Theorem 5.1 in Swanson and Stinson [2014a], which is derived from lemma 1 in Albert et al. [2005]. Theorem 5.1 is defined to be the following:

> *The announcement An is informative for Bob if and only if there do not exist two distinct sets $H_{An}, H'_{An} \in An$ such that $|H_{An} \cap H'_{An}| \geq a - c$ [Swanson and Stinson, 2014a].*

We first prove the equivalence between a formula in public announcement logic and the definition of crossing hands as it is defined in (5.1). We then go on to discuss its place in the literature, and whether it is necessary for the safety of the protocol as is claimed by Albert et al. [2005]. We have the equivalence:

$$\forall H_{An} \forall G_{An} (H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2) \Leftrightarrow M, s \models [An_a] C_A bKnowsAs \tag{5.2}$$

But to prove this, we first prove that an announcement without crossing hands results in strictly singleton equivalence classes for Bob.

Consider the RCP (3,3,1) S5-model $M$ and its updated version with announcement $An$ respectively:

$$M = (S, A, V, \sim, Prop)$$

$$M|An = (S', A, V', \sim', Prop)$$

**Lemma 1**

$$\forall H_{An} \forall G_{An}(H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2) \Leftrightarrow \forall x, y \in S' : (x, y) \in \sim'_b \rightarrow x = y$$

$\Rightarrow$ Proof by contrapositivity:

Assumption: $\exists x, y \in S'$ s.t. $(x, y) \in \sim'_b$ and $x \neq y$

From our assumption we have that there exists two states, $x, y$ that $b$ deem indistinguishable. The valuation in these two states must then be of the following form:

$M, x \models ijk_a \wedge lmn_b \wedge o_{eve}$

$M, y \models ijo_a \wedge lmn_b \wedge k_{eve}$

Or some similar permutation of the variables, but $lmn_b$ must remain the same for Bob to consider them indistinguishable. This means that Anne will have two of the same variables in states $x$ and $y$, as Bob's cards must remain the same and Eve can only differ with the single card she holds. $x$ and $y$ would not be part of $M|An$ unless Anne had both $ijk_a$ and $ijo_a$ in her announcement, and the antecedent is therefore false as $|\{ijk\} \cap \{ijo\}| = 2$. Proof by contrapositivity holds.

$\Leftarrow$ Proof by contradiction. Assumptions:

Assumption 1: $\forall x, y \in S' : (x, y) \in \sim'_b \rightarrow x = y$

Assumption 2: $\exists H_{An} \exists G_{An}(H_{An} \neq G_{An} \wedge |H_{An} \cap G_{An}|) \geq 2$

From assumption 2 we can instead of $\geq 2$ just say $= 2$. If it is greater than two, namely 3, it will be removed because of idempotent law, as the announcement is a disjunction of alternative hands. It can never be larger than 3, as Anne's hand contains three cards and she can't announce an alternative hand that is larger than her actual hand as her announcement must be truthful. We therefore get:

Assumption 1: $\forall x, y \in S' : (x, y) \in \sim'_b \rightarrow x = y$

Assumption 2: $\exists H_{An} \exists G_{An}(H_{An} \neq G_{An} \wedge |H_{An} \cap G_{An}|) = 2$

From assumption 2 we get that in the announcement, there are two alternative hands that share two of the same cards. And as a consequence, in the resulting updated model, there will be two states $s, t$ where the following holds:

$M|An, s \models ijk_a \wedge lmn_b \wedge o_{eve}$

$$M|An, t \models ijo_a \wedge lmn_b \wedge k_{eve}$$

This leads to a contradiction, because of the fact that the states $s$ and $t$ have the same evaluation for Bob. He can not distinguish those states, and states $s$ and $t$ will be in the same equivalence class. We then have $(s,t) \in \sim'_b \wedge s \neq t$. Assumption 1 is therefore false, and the contradiction holds.

We can then prove that not allowing crossing hands is equivalent to the fact that after Anne's initial announcement, it is common knowledge among all agents that Bob knows Anne's cards.

Consider the RCP (3,3,1) S5-model $M$ updated with announcement $An$.

**Lemma 2**

$$M|An, s \models C_A bKnowsAs \Leftrightarrow \forall H_{An} \forall G_{An}(H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2)$$

$\Rightarrow$: Direct proof:

Assumption 1: $M|An, s \models C_A bKnowsAs$

If it is common knowledge among all agents that Bob knows Anne's cards, then in every state in the model $M|An$, Bob must know Anne's cards. This means that the following must hold:

$$\forall x, y \in S' : (x,y) \in \sim'_b \rightarrow x = y$$

Applying the truth of the above formula to Lemma 1 gives us:

$$\forall H_{An} \forall G_{An}(H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2)$$

Consequent must be true when assuming the truth of the antecedent, proof by direct proof holds.
$\Leftarrow$: Proof by contradiction:

Assumption 1: $\forall H_{An} \forall G_{An}(H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2)$

Assumption 2: $M|An, s \models \neg C_A bKnowsAs$

From Assumption 2:
There exists a pair $(s,x) \in \bigcup_{a \in A}^{*} \sim_a$ s.t. $(x,y) \in \sim_b$ and $x \neq y$. This would mean that in some state $b$ is unsure of the deal. Essentially meaning that there exists an equivalence class for $b$ that is not singleton in the updated model. Applying assumption 1 to Lemma 1 gives the contradiction.

## 1.1 Consequences

As previously mentioned, crossing hands is prevalent throughout the literature of RCP [van Ditmarsch, 2003, Albert et al., 2005, van Ditmarsch, 2005, Swanson and Stinson, 2014b]. From the equivalence proved in the previous lemma, we can then say that the assumption $M, s \models [An_a]C_A bKnowsAs$ is equally prevalent throughout the literature.

We can in fact say that in any part of the literature where crossing hands is not allowed, we have common knowledge among all agents after the initial announcement by Anne that Bob knows Anne's cards. This in turn proves that any protocol without crossing hands in the first announcement is a known direct exchange by all agents. A weaker assumption is briefly described by van Ditmarsch [2003] as a footnote to the proof of Proposition 31 regarding the upper bound of an announcement, where they say:

> *Proposition 31: No direct exchange consists of more than seven hands.*

With the footnote:

> *This assumes that Eve knows that Anne knows that Bill knows her hand of cards after her announcement.*

If we represent this sentence as a formula in PAL we get:

$$M, s \models [An_a]K_{eve}K_a bKnowsAs$$

Which is weaker than the proven equivalence in lemma 2 presented above. Common knowledge of the fact that Bob knows Anne's cards after announcement $An$ means that all of them know that all of them know that all of them know ... to infinity that Bob knows Anne's cards [van Ditmarsch et al., 2007]. Albert et al. [2005] describes three epistemic axioms, and propose three combinatoric axioms that are equivalent to their corresponding epistemic axioms: (a $b$-set is a set of $b$ elements, in this case $b = 3$.) The first being the axiom regarding the informativity of Bob. **EA** means "epistemic axiom" and **CA** "combinatorial axiom". In the definition of the first combinatorial axioms the term "avoids" is used in. Two sets A and B "avoid" each other if the intersection of A and B is the empty set, formalized with the following formula:

$$A \cap B = \varnothing$$

**EA1.** Whenever Anne can announce $An$, Bob knows Anne's hand after $An$

**CA1.** For every $b$-set $X$ there is at most one member of $An$ that avoids $X$.

If we translate **EA1** literally from the description, we get:

$$M, s \models [An]bKnowsAs$$

If we translate **EA1** to the above formula, the equivalence does not hold. Consider the following card distribution:

$$A = \{0, 1, 2\}, B = \{3, 4, 5\}, C = \{6\}$$

**EA1** ⇒ **CA1** can then be falsified in the following way, taking the announcement they describe as a footnote in Albert et al. [2005] on the same page:

$$An = K_a(012_a \vee 034_a \vee 056 \vee 135_a \vee 246_a \vee 235_a)$$

We have that EA1 is satisfied, as Bob can exclude all hands that intersect with his, which leaves $012_a$ as the only remaining possible hand. However, we have that there are two hands that avoid the $b$-set $\{0, 4, 6\}$, namely $135_a$ and $235_a$. We therefore see an instance where **EA1** is satisfied, and **CA1** is not. However, Albert et al. [2005] notes in the section 'Notation and combinatorial formulation' that EA1 must be commonly known among all agents. Which is why I show the proof between crossing hands and $[An_a]C_A bKnowsAs$ and not the literal translation presented above. Consider lemma 1 from Albert et al. [2005]:

> *An announcement L satisfies CA1. if and only if for every pair of distinct lines* $L_1, L_2$ *we have* $|L_1 \cap L_2| < a - c$

Meaning that not allowing crossing hands is equivalent to **CA1**. Using Lemma 2 proven earlier in this thesis and Lemma 1 in Albert et al. [2005] we get:

$$M, s \models [An_a]C_A bKnowsAs \Leftrightarrow \forall H_{An} \forall G_{An}(H_{An} \neq G_{An} \Rightarrow |H_{An} \cap G_{An}| < 2) \Leftrightarrow \mathbf{CA1}$$

Applying transitivity of equivalence, we get:

$$M, s \models [An_a]C_A bKnowsAs \Leftrightarrow \mathbf{CA1}$$

Which is proof that my translation of **EA1** (with the requirement that it is common knowledge) to PAL is equivalent with **CA1**.

## 1.2 Epistemic Safety Axioms and Combinatorial Safety Axioms

Albert et al. [2005] gives descriptions of two epistemic safety-axioms, together with their respective combinatorial axioms. A $c$-set is a set with the cardinality of Eve's hand:

**EA2.** Whenever Anne can announce $An$, Eve does not know any of Anne's cards after $An$.

**CA2.** For every $c$-set $X$ the members of $An$ avoiding $X$ have empty intersection.

**EA3.** Whenever Anne can announce $An$, Eve does not know any of Bob's cards after $An$.

**CA3.** For every $c$-set $X$ the members of $An$ avoiding $X$ have union consisting of all cards except those of $X$.

The definition of *eveIgnorant* as presented earlier, is a conjunction of **EA2** and **EA3**. Let $An_a = K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a \vee 235_a)$. With this announcement, it is claimed in Albert et al. [2005] that without the presence of **CA1**, the epistemic axiom **EA2** is not satisfied. As shown below:

$$M, s \not\models [An_a]\mathbf{EA2}$$

However, that is not true. We do in fact have:

$$M, s \models [An_a]\mathbf{EA2}$$

The only axiom of the three combinatorial axioms that $An_a$ does not satisfy is **CA1**. However, it does satisfy the post-protocol informativity condition made by van Ditmarsch et al. [2006]:

$$C_{ab}(aKnowsBs \wedge bKnowsAs)$$

From this we have that $An_a$ does indeed satisfy all safety conditions. It also satisfies the fact that Bob knows Anne's cards after the first announcement. Specifically:

$$M, 012.345.6 \models [An_a]C_{ab}bKnowsAs$$

Bob can therefore truthfully announce Eve's card - and this is common knowledge among Anne and Bob. However, this is only true in the cases where Anne is not announcing crossing hands with her own hand, e.g state 012.345.6 Where this announcement falls short is the lack of investigation into whether or not the announcement always leads to a solution at some point. Regardless, **CA1** is not required together with **CA2** or **CA3** to ensure safety. **CA1** is a guarantee that all agents know that the protocol is of exactly length two, a direct exchange. It can also be viewed as a guarantee that every initiated protocol has a solution for every alternative hand announced by Anne. This is an important assumption in the Russian cards problem that has been thoroughly studied by Hans van Ditmarsch [van Ditmarsch, 2005].

### Safety axioms are equivalent

The safety axioms are in fact equivalent without **CA1**. In their proof of $(CA1\&)CA2/CA3$ they note:

> *"Eve can exclude, as hands for Anne, those members of the announcement that intersect with her own, also because of CA1, which implies EA1 these are the only Anne-hands she can exclude".*

This is somewhat true, but there is a slight imprecision here that is worth noting. If Eve were to eliminate other hands than those that contain cards she holds, then there are other assumptions surrounding the protocol that has been done. In the introduction to their paper they note that they only consider protocols that are commonly known to be direct exchanges, and that it is commonly known among all agents that the postconditions are satisfied after the direct exchange. This in turn means that they have assumed CA1 to be true at all times. van Ditmarsch [2005] describes the actual assumption needed for this equivalence to hold:

> *We assume that Anne and Bob take no risks: they are only willing to execute protocols that guarantee success, in the sense that, whatever one says, the other can make at least one safe reply to that which will bring a solution closer.*

CA1 is a strict subset of this assumption because CA1 is a guarantee that common knowledge of Bob's informativity is achieved. This means that the informativity requirement of the Russian cards problem always hold. CA1 restricts the solutions to only known direct exchanges for all agents. Combine CA1 with safety and we have 102 proper solutions to the Russian cards problem. However, CA2&3 is not dependent on CA1 for the equivalence between EA2&3 and CA2&3. The actual requirement for safety is the weaker assumption by van Ditmarsch. Every initiated protocol must have a solution at some point for every alternative hand in the announcement [van Ditmarsch, 2005]. This assumption is needed both for CA2&3 and EA2&3 - but this assumption is not reflected in EA2&3. The complexities mentioned in this paragraph illustrates even further the complexities of the Russian cards protocol, and the complexities of comparing epistemic axioms and combinatorial axioms.

You could even weaken the assumption made in van Ditmarsch [2005]. If the assumption is that some protocols might not terminate at all, then the announcement described in Albert et al. [2005] is a safe announcement because Eve is not able to remove any crossing hands if that is the case.

**Conclusion** If Eve is able to completely remove all crossing hands then the following three assumptions have been made:

1 CA1

2 Crossing hands is not allowed

3 $M|An, s \models C_A bKnowsAs$

Where 1 and 2 were proven equal by Albert et al. [2005] and the last was proven equal to 1 and 2 in this thesis.

If Eve can remove *some* crossing hands, then we have the assumption made by van Ditmarsch [2005] which states that all protocols must have a solution *at some point*. We can then say that Eve can remove the crossing hands that do not lead to a solution at some point. If the assumption is that some protocols don't terminate at all, then Eve is not able to eliminate any crossing hands at all.

We conclude that elimination of crossing hands is not based on the safety of the first announcement by Anne - elimination of crossing hands by Eve is a choice by those who are studying the Russian cards problem depending on which assumption they want to make. In the next section we present an exchange that does contain crossing hands, and we use the same assumption made in van Ditmarsch [2005], saying that all crossing hands must have a solution at some point.

## 2 Crossing hands exchange

To the best of our knowledge, only one protocol containing crossing hands has been studied extensively [van Ditmarsch, 2005]. The initial announcement by Anne is the following:

$$\psi_a = K_a(012_a \vee 034_a \vee 056 \vee 135 \vee 245 \vee 246) \tag{5.3}$$

This announcement contains the pair $(2,4)$ in the last two disjuncts, and as a consequence we have:

$$M|\psi_a, s \not\models C_A bKnowsAs \tag{5.4}$$

Ditmarsch proves that there exist no announcements that leads to a solution of the protocol in the state 245.013.6 and 246.013.5. There is an assumption that to the best of my knowledge has only been discussed thoroughly by van Ditmarsch [2005]. It is intuitively described in the following way:

> *"For every hand in Anne's announcement, there exists some sequence of announcements that leads to the postconditions of the protocol being satisfied"*

This can be represented pseudo-formally in PAL - consider $H$ to be an alternative hand in Anne's announcement $An$, M to be an arbitrary RCP S5-model and $s$ to be the state where Anne is holding $H$.

$$\forall H_{\in An} \exists \varphi_{1..i} \text{ s.t. } M, s \models [\varphi_1]..[\varphi_i] postconditions \tag{5.5}$$

Under this assumption, Eve can remove the alternative hands 245 and 246 from Anne's announcement, as these hands have no solutions. The announcement is therefore a 4-hand announcement, and no solution consists of less than 5 alternative hands [van Ditmarsch, 2003].

**Kerckhoff's Principle** All modern cryptography systems adheres to Kerckhoff's principle [Mousa and Hamad, 2006]. Kerckhoff's principle states that the inner workings of a cryptographic system should be publicly available [Mousa and Hamad, 2006]. It was originally a set of principles, but the term now commonly describes the following principle:

> *The system must not require secrecy and can be stolen by the enemy without causing trouble (what is nowadays referred to as Kerckhoffs' Principle)[Petitcolas, 2011].*

This principle is therefore highly appropriate for the Russian cards problem. We must assume that anyone can know how the Russian cards problem works. One way to break this principle in the Russian cards problem is by considering the announcement studied in detail by van Ditmarsch [2005]:

$$K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 245_a \vee 246_a) \tag{5.6}$$

This announcement contains the crossing hands $245_a$ and $246_a$. From lemma 2 we have that Eve is then unsure whether Bob learned the deal or not. It is a safe announcement without any further reasoning by Eve. Consider the assumption that every alternative hand must have a solution at some point.

We could say that Anne and Bob knows that every protocol terminates, and that they collectively know that Anne would not announce this if $245_a$ or $246_a$ was the case.

If this announcement was considered to be a solution, it would appear to any outsiders that Anne and Bob allow protocols that might not have a solution for some of the hands.

In this case we have a "secret" among Anne and Bob, they make it appear to Eve that they have protocols that could never terminate, even though they know that all protocols will terminate. If this secret were to be known by Eve at some later point in the protocol, the announcement discussed by van Ditmarsch [2005] would not be safe because Eve could go back and remove $245_a$ and $246_a$ from the announcement and learn the card distribution.

Kerckhoff's principle is therefore paramount when discussing the assumption that every alternative hand must have a solution at some point.

**7-hand crossing hands solution** I present a 7-hand solution that consists of crossing hands. The initial announcement is the following:

$$initAn = K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a \vee 025_a) \tag{5.7}$$

There are two crossing pairs in this announcement. $(0, 2)$ and $(0, 5)$. These are found in the hands $012_a$ and $025_a$, and in the hands $056_a$ and $025_a$ respectively. Bob is insecure of the deal in four states. Bob cannot tell apart the states $\{012.346.5, 025.346.1\}$, and he cannot tell apart the states: $\{025.134.6, 056.134.2\}$

As described in van Ditmarsch [2005], we must find solutions to the protocol for each of these four states. Taking each equivalence class separately:

## 2.1 012.346.5/025.346.1

**012.346.5** Bob can safely respond with "Eve has 5 or 1" [van Ditmarsch, 2005]. Represented in PAL as follows:

$$M|initAn, 012.346.5 \models [K_b(5_e \vee 1_e)]C_A eveIgnorant \tag{5.8}$$

As Anne hears this, she understands that she must 'narrow' down her announcement to help Bob understand which state we are actually in. Note that this does not remove the states where Bob knows the deal, he could have announced this even though he knew if Eve had 5 or Eve had 1, which is an important part of the security of the protocol.

To terminate the protocol, Anne announces a 4-hand announcement, satisfying all postconditions:

$$M|initAn|K_b(5_e \vee 1_e), 012.346.5 \models [K_a(012_a \vee 034_a \vee 056_a \vee 236_a)]C_A eveIgnorant \tag{5.9}$$

$$M|initAn|K_b(5_e \vee 1_e), 012.346.5 \models [K_a(012_a \vee 034_a \vee 056_a \vee 236_a)]C_{ab}(aKnowsBs \wedge bKnowsAs) \tag{5.10}$$

**025.346.1** Bob again responds with "Eve has 5 or 1":

$$M|initAn|K_b(5_e \vee 1_e), 025.346.1 \models C_A eveIgnorant \tag{5.11}$$

Anne reasons in the same fashion as described above, and announces a 4-hand announcement to terminate the protocol. It satisfies all postconditions:

$$M|initAn|K_b(5_e \vee 1_e)|K_a(025_a \vee 034_a \vee 146_a \vee 236_a), 025.346.1 \models postcondition \tag{5.12}$$

## 2.2 025.134.6, 056.134.2

**025.134.6** In this case, Bob responds with "Eve has 6 or 2".

$$M|initAn|K_b(6_e \vee 2_e), 025.134.6 \models C_A eveIgnorant \tag{5.13}$$

As Anne hears this, she again understands that she needs to narrow down her announcement to help Bob understand which state we are in. To terminate the protocol, Anne announces a 4-hand announcement, satisfying all postconditions:

$$M|initAn|K_b(6_e \vee 2_e)|K_a(025_a \vee 034_a \vee 135_a \vee 146_a), 025.134.6 \models postcondition \tag{5.14}$$

**056.134.2** Bob responds in the same manner, "Eve has 6 or 2".

$$M|initAn|K_b(6_e \vee 2_e), 056.134.2 \models C_A eveIgnorant \tag{5.15}$$

Anne reasons as she has done in the previous examples, and follows up with a narrowed down announcement to terminate the protocol:

$$M|initAn|K_b(6_e \vee 2_e)|K_a(056_a \vee 012_a \vee 034_a \vee 135_a), 056.134.2 \models postcondition \tag{5.16}$$

The resulting models from the 4 protocols described here are not found in any other RCP solution, unless Bob announces Eve's card to finish it off. This is not necessary, as we have already established common knowledge among the communicating agents that they know each others cards.

## 2.3 Approach

Finding this new solution would not have been possible without the extended software created for this thesis. The approach to finding this solution was as follows:

First, take the following 6-hand non-crossing solution:

$$K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a)$$

Then, extend it with a crossing hand, in this case we used 025 to get the initial announcement described in the solution above. This particular hand was chosen because it was crossing with Anne's own hand in the state 012.345.6. Due to the lack of previous work on establishing patterns in how these solutions are constructed, the easiest path to finding such a solution was to extend a previous solution with a crossing hand - attempting to have the least amount of crossing hands possible in the initial announcement. We then generate the announcement and the model as follows:

```
> :l Solutions.hs
> let model = generateRCPModel [3,3,1]
> let anne = (Ag 0)
> let an = [[0,1,2], [0,3,4], [0,5,6], [1,3,5], [1,4,6], [2,3,6], [0,2,5]]
> let announcement = integerAnnouncementToProp an anne
> let isSafe = commonKnowledgeOfSafety model announcement
> isSafe
> true
```

commonKnowledgeOfSafety validates whether updating the model with the announcement results in common knowledge of safety. We then update the model with the announcement, to see in which states Bob is insecure of the deal:

```
> let updatedModel = upd_pa model announcement
> show updatedModel
```

The result of showing the updated model is provided in the appendix (Model 2). From the model we see that all equivalence classes for Bob are singleton except for the two equivalence classes [1,31], and [28,58]. We then need to go to each of these states, and continue the protocol by having Bob announce what he believes to be Eve's cards (5 and 1).

```
> let updModel1 = changeCurrentStateInModel updatedModel 1
> let bob = (Ag 1)
> let bobAn1 = createDisjunctEveAnnouncement [5,1] bob
> commonKnowledgeOfSafety updModel1 bobAn1
> true
```

We then continue with the updated model after Bob's announcement, which is Model 3 in the appendix. Here is where the exhaustive generation of solutions is the important factor in solving these complex protocols. We are now able to generate any announcement, with any amount of alternative hands to find a solution. In this case we show a 4 hand announcement that solves the protocol.

```
> let afterBob1 = upd_pa updModel1 bobAn1
> let solutions = solutions_specifyLower_fromModel afterBob1 4 anne
> length solutions
> 1
```

Here we use the solutions_step3 function with the following signature:

```
solutions_specifyLower_fromModel :: EpistM Int -> Int -> Agent -> [Form Int]
```

It takes a model, then the amount of hands you want in the announcement and an agent. It then constructs all non-crossing announcements the agent can make, and validates that it Anne's announcement is safe, and that it is safe for Bob to announce Eve's card after Anne's announcement. It returns a list of formulae that satisfies the postconditions. The resulting formula is the announcement provided in the first solution of subsection 2.1 from this chapter (5.9). We can then view the final model in the following way:

```
> let finalAnnouncement1 = head solutions
> let finalModel1 = upd_pa afterBob1 finalAnnouncement1
> show finalModel1
```

The final model is found in the appendix (Model 4). Observe that Anne's equivalence classes are still not all singleton, we have the two equivalence classes [37,39] and [108, 110]. This is what makes this protocol unique. From Lemma 2 we prove that this is never the case when the initial announcement does not contain crossing hands - and Bob follows up by announcing Eve's card. If the protocol follows that structure, we always have common knowledge among all agents that Anne knows Bob's cards, Bob knows Anne's cards and Eve is ignorant. Here, Eve considers it possible that Anne is not yet aware of which cards Bob is holding. Regardless, both Anne and Bob have common knowledge that they know each others cards, because for both Anne and Bob the equivalence class for state 1 is singleton.

The process described above is subsequently repeated for each of the states that Bob is insecure of the deal in the following way:

```
> :l Solutions.hs
> let model = generateRCPModel [3,3,1]
> let anne = Ag 0
> let bob = Ag 1
> let an = [[0,1,2], [0,3,4], [0,5,6], [1,3,5], [1,4,6], [2,3,6], [0,2,5]]
> let announcement = integerAnnouncementToProp an anne
> let updatedModel = upd_pa model announcement
> let updatedModel31 = changeCurrentStateInModel updatedModel 31
> let updatedModel28 = changeCurrentStateInModel updatedModel 28
> let updatedModel58 = changeCurrentStateInModel updatedModel 58
> let bobAn1 = createDisjunctEveAnnouncement [5,1] bob
> let bobAn2 = createDisjunctEveAnnouncement [6,2] bob
> let afterBob31 = upd_pa updatedModel31 bobAn1
> let afterBob28 = upd_pa updatedModel28 bobAn2
> let afterBob58 = upd_pa updatedModel58 bobAn2
> let sols31 = solutions_specifyLower_fromModel afterBob31 4 anne
> let sols28 = solutions_specifyLower_fromModel afterBob28 4 anne
> let sols58 = solutions_specifyLower_fromModel afterBob58 4 anne
> let finalModel31 = upd_pa afterBob31 $ head sols31
> let finalModel28 = upd_pa afterBob28 $ head sols28
> let finalModel58 = upd_pa afterBob58 $ head sols58
```

The solutions from sols31, sols28 and sols58 are Anne's final announcement in (5.12), (5.14) and (5.16) respectively. The updated models updatedModel31, updatedModel28, updatedModel58 is equivalent with Model 2 in the appendix, as the only difference is the state being changed. The other models correspond to the following models in the appendix:

- afterBob31 = Model 5
- finalModel31 = Model 6
- afterBob28 = Model 7
- finalModel28 = Model 8
- afterBob58 = Model 9
- finalModel58 = Model 10

## 2.4 Consequences

The four 4-hand announcements described in section 2 that are the solutions to the different insecurity states of Bob are actually subsets of 5-hand solutions to the Russian cards problem. Below I give the 4-hand announcement that solves the state 012.346.5, and its corresponding superset which is a 5-hand (non-crossing) solution to the Russian cards problem.

012.346.5: $K_a(012_a \vee 034_a \vee 056_a \vee 236_a)$

012.346.5: $K_a(012_a \vee 034_a \vee 056_a \vee 145_a \vee 236_a)$

The reason $145_a$ is not needed in the 4-hand announcement is that $145_a$ is not part of Anne's initial announcement, and the state is therefore no longer part of the model, thus the disjunct is redundant. However, it can serve a very fascinating purpose.

Consider the actual deal to be 146.023.5. Anne can then start the protocol with the initial crossing hands announcement (5.7):

$$M, 146.023.5 \models [K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a \vee 025_a)]C_A eveIgnorant \quad (5.17)$$

We now have common knowledge among the communicating agents that Bob knows the deal of cards after the initial announcement! This is because Anne is not announcing any crossing hands with her own hand. This was not the case for state 012.345.6, because the pair (0,2) was present in two alternative hands - Anne announced a sequence of alternative hands that was crossing with her own hand. However, in state 146.023.5 this is not the case, and as a consequence the following is true:

$$M, 146.023.5 \models [K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a \vee 025_a)]C_{ab}(bKnowsAs) \quad (5.18)$$

Bob follows it up by announcing "Eve has 5 or 1". Bob knows that Anne is holding 146, and is therefore aware that Anne will learn the deal because he knows that Anne can eliminate the fact that Eve is holding 1. The announcement is both safe and fully informative for Anne:

$$M|initAn, 146.023.5 \models [K_b(5_e \vee 1_e)]C_{ab}(bKnowsAs \wedge aKnowsBs) \quad (5.19)$$

$$M|initAn, 146.023.5 \models [K_b(5_e \vee 1_e)]C_A eveIgnorant \tag{5.20}$$

Now, after this announcement by Bob, all postconditions are satisfied. The communicating agents know what the card deal is, and the ignorance of Eve is common knowledge. Eve does not know that the communicating agents know the card deal. She considers it possible that we are in state 012.346.5, where a second announcement by Anne is required to terminate the protocol.

After Bob's announcement, Anne can follow up with the 5-hand superset of the 4-hand announcement that finishes the protocol. This announcement can be a completely new protocol, or it can be the termination of the current protocol. This is only known by the communicating agents, based on the cards they were dealt.

In state 012.346.5 the 5-hand announcement $K_a(012_a \vee 034_a \vee 056_a \vee 145_a \vee 236_a)$ would be the termination of the protocol. In state 146.023.5 it would be the initiation of a completely new protocol. *Eve is not able to discern whether new information is being transmitted, or whether they are terminating a protocol.*

# Chapter 6

# Conclusions and Future work

## 1 Conclusion

It was previously only found to be one way to successfully initiate a Russian cards protocol, namely Anne announcing a sequence of alternative hands where none of them are crossing. The outcome of that announcement is known by everyone, and the protocol would always adhere to this structure. Each step of the protocol could be described in the following way:

1 Anne announces a sequence of alternative hands where none of the hands are crossing.

2 Everyone knows that Bob learns her cards.

3 Bob announces Eve's card.

4 Everyone knows that Anne and Bob knows each others cards, and Eve is completely ignorant of the card distribution.

With the findings from this thesis, it is now shown that there are in fact three different strategies that Anne can choose from when initiating the protocol, and they provide four different outcomes each described in detail below. The first is the same as the one described where Anne does not announce any crossing hands. The remaining two are more interesting however.

**Strategy 1** Anne initiates the protocol with an announcement containing a sequence of alternative hands where some are crossing with her actual hand. This initial announcement has two outcomes:

1 Bob learns which cards Anne are holding.

2 Bob does not know which cards Anne are holding.

Anne is unsure in both cases whether or not Bob learned which cards she is holding. This is because she announces one crossing with her own, and therefore she can imagine that Eve is holding the last card in the hand that is crossing with her own. If that is the case, Bob can't eliminate that hand and subsequently he considers two hands possible.

In the other case, Bob is the one holding the last card in the hand that is crossing with Anne's. He can therefore eliminate all hands except one, and learn the card distribution. Eve knows that both these cases are possible, and so Bob must announce a disjunction of two hands that Eve might hold. Finally, Anne learns the card distribution and then announces a subset of her initial announcement to terminate the protocol. As she is unsure of whether Bob learned her cards from the initial announcement, this protocol is known by both communicating agents to be a three-step protocol.

**Strategy 2** The other strategy Anne can choose from is announcing a sequence of alternative hands where some are crossing, but none are crossing with her own hand. In this case both communicating agents know that Bob learned Anne's card. When this is the case, Bob treats the protocol in the same way as in the previous scenario. However, when Anne initiates the protocol using this construct it is possible to initiate a new protocol without Eve knowing whether a new protocol is initiated or the previous is being continued.

Kerckhoff's principle was discussed earlier, and it might appear as if Anne and Bob has a secret among them if they are initiating a new protocol without Eve knowing. This is not the case here, as the inner workings of the system are not secret. It can be publicly known to everyone that this might happen from time to time, it does not affect the security of the protocol. For Eve to figure out whether or not a new protocol was initiated, she must know whether or not Anne's announcement contained crossing hands with Anne's own hand. For this to happen, Eve must know at least two of Anne's cards. That information is not given in the protocol, and so for Eve to acquire this knowledge, she must gain knowledge of Anne's hand outside of this protocol. The external security of the Russian cards problem is not discussed in this thesis. This thesis studies the protocol and its interaction only. Security measures surrounding the protocol is not relevant when concretely studying the announcements among the communicating agents. We can therefore say that Kerckhoff's principle is fulfilled. We have also fulfilled the requirement that for every hand announced in Anne's initial announcement, there is a sequence of announcements that lead to complete information among the communicating agents. Lastly, we have that the ignorance of Eve is preserved throughout the protocol.

The proof that these two strategies can result in proper solutions to the Russian cards problem would not have been possible without the extensions of the Russian cards software created for this thesis. It granted the possibility of generating any alternative hands announcement and validating them automatically. It has been proved that any announcement by some agent $n$ in the Russian cards problem is equivalent to an announcement of alternative hands [van Ditmarsch, 2003]. From this we have that the exhaustive generation of announcements with alternative hands is in fact a tool that is capable of validating any possible announcement made by an agent in the Russian cards problem. We can therefore use the software from this thesis to model and verify any protocol in the Russian cards problem, which is incredibly powerful when attempting to find new solutions to the problem.

**Contributions** In this thesis we have shed light on the relationship between crossing hands and common knowledge in the Russian cards protocol. This has, by transitivity, also shed light on the relationship between common knowledge of informativity modeled in PAL and a combinatorial axiom of informativity. The most important contribution from this thesis is the solution to the open problem posed and unsuccessfully attempted tackled in [van Ditmarsch, 2005] - and that has remained open since. The solution to this problem would not have been possible without the extended software specifically created for the Russian cards problem. We hope that this software might be used to find more protocols that inhibit the desired properties that van Ditmarsch was looking for, and that were found in this thesis.

# 2 Future work

**Crossing hands exchanges** With the proof by example that protocols with crossing hands exist, a lot of work is still to be done. Finding and proving characteristics of such protocols could help generating such protocols automatically. As of now, little knowledge around such protocols exist, and finding them is therefore a somewhat manual task. Further investigations into them could be done by extending the software presented in this thesis with automatic generation of these protocols too. The computational complexity is quite high as there are more than just one announcement by Anne and one by Bob to uncover a solution. However, it is possible to further build upon the software to generate these solutions. Further investigations into patterns and characteristics of crossing hands-solutions, similar to the crossing-hands restriction of a direct exchange would be the most convenient as it could restrict the generation of announcements before the protocol has been initiated - thus reducing the validation of common knowledge which is an expensive calculation compared to simple restrictions on how to generate announcements.

**Crossing hands in the generalized Russian cards problem** This thesis only looked at the classical setting of the Russian cards problem with the card distribution (3,3,1). Further investigation into crossing hands in the generalized Russian cards problem would be interesting as well, but establishing other proofs regarding the classical setting might be needed before this is possible.

# Chapter 7

# Appendix

Initial model (Model 1):

```
Non-changing parts of the models:
c = eve.
Prop = {a0, b0, c0 .. a6,b6,c6}
Ag = {a,b,c}

V = [(0,[a0,a1,a2,b3,b4,b5,c6]),(1,[a0,a1,a2,b3,b4,b6,c5]),
(2,[a0,a1,a2,b3,b5,b6,c4]),(3,[a0,a1,a2,b4,b5,b6,c3]),
(4,[a0,a1,a3,b2,b4,b5,c6]),(5,[a0,a1,a3,b2,b4,b6,c5]),
(6,[a0,a1,a3,b2,b5,b6,c4]),(7,[a0,a1,a3,b4,b5,b6,c2]),
(8,[a0,a1,a4,b2,b3,b5,c6]),(9,[a0,a1,a4,b2,b3,b6,c5]),
(10,[a0,a1,a4,b2,b5,b6,c3]),(11,[a0,a1,a4,b3,b5,b6,c2]),
(12,[a0,a1,a5,b2,b3,b4,c6]),(13,[a0,a1,a5,b2,b3,b6,c4]),
(14,[a0,a1,a5,b2,b4,b6,c3]),(15,[a0,a1,a5,b3,b4,b6,c2]),
(16,[a0,a1,a6,b2,b3,b4,c5]),(17,[a0,a1,a6,b2,b3,b5,c4]),
(18,[a0,a1,a6,b2,b4,b5,c3]),(19,[a0,a1,a6,b3,b4,b5,c2]),
(20,[a0,a2,a3,b1,b4,b5,c6]),(21,[a0,a2,a3,b1,b4,b6,c5]),
(22,[a0,a2,a3,b1,b5,b6,c4]),(23,[a0,a2,a3,b4,b5,b6,c1]),
(24,[a0,a2,a4,b1,b3,b5,c6]),(25,[a0,a2,a4,b1,b3,b6,c5]),
(26,[a0,a2,a4,b1,b5,b6,c3]),(27,[a0,a2,a4,b3,b5,b6,c1]),
(28,[a0,a2,a5,b1,b3,b4,c6]),(29,[a0,a2,a5,b1,b3,b6,c4]),
(30,[a0,a2,a5,b1,b4,b6,c3]),(31,[a0,a2,a5,b3,b4,b6,c1]),
(32,[a0,a2,a6,b1,b3,b4,c5]),(33,[a0,a2,a6,b1,b3,b5,c4]),
(34,[a0,a2,a6,b1,b4,b5,c3]),(35,[a0,a2,a6,b3,b4,b5,c1]),
(36,[a0,a3,a4,b1,b2,b5,c6]),(37,[a0,a3,a4,b1,b2,b6,c5]),
(38,[a0,a3,a4,b1,b5,b6,c2]),(39,[a0,a3,a4,b2,b5,b6,c1]),
(40,[a0,a3,a5,b1,b2,b4,c6]),(41,[a0,a3,a5,b1,b2,b6,c4]),
(42,[a0,a3,a5,b1,b4,b6,c2]),(43,[a0,a3,a5,b2,b4,b6,c1]),
(44,[a0,a3,a6,b1,b2,b4,c5]),(45,[a0,a3,a6,b1,b2,b5,c4]),
(46,[a0,a3,a6,b1,b4,b5,c2]),(47,[a0,a3,a6,b2,b4,b5,c1]),
(48,[a0,a4,a5,b1,b2,b3,c6]),(49,[a0,a4,a5,b1,b2,b6,c3]),
(50,[a0,a4,a5,b1,b3,b6,c2]),(51,[a0,a4,a5,b2,b3,b6,c1]),
(52,[a0,a4,a6,b1,b2,b3,c5]),(53,[a0,a4,a6,b1,b2,b5,c3]),
(54,[a0,a4,a6,b1,b3,b5,c2]),(55,[a0,a4,a6,b2,b3,b5,c1]),
(56,[a0,a5,a6,b1,b2,b3,c4]),(57,[a0,a5,a6,b1,b2,b4,c3]),
(58,[a0,a5,a6,b1,b3,b4,c2]),(59,[a0,a5,a6,b2,b3,b4,c1]),
(60,[a1,a2,a3,b0,b4,b5,c6]),(61,[a1,a2,a3,b0,b4,b6,c5]),
(62,[a1,a2,a3,b0,b5,b6,c4]),(63,[a1,a2,a3,b4,b5,b6,c0]),
(64,[a1,a2,a4,b0,b3,b5,c6]),(65,[a1,a2,a4,b0,b3,b6,c5]),
(66,[a1,a2,a4,b0,b5,b6,c3]),(67,[a1,a2,a4,b3,b5,b6,c0]),
(68,[a1,a2,a5,b0,b3,b4,c6]),(69,[a1,a2,a5,b0,b3,b6,c4]),
(70,[a1,a2,a5,b0,b4,b6,c3]),(71,[a1,a2,a5,b3,b4,b6,c0]),
(72,[a1,a2,a6,b0,b3,b4,c5]),(73,[a1,a2,a6,b0,b3,b5,c4]),
(74,[a1,a2,a6,b0,b4,b5,c3]),(75,[a1,a2,a6,b3,b4,b5,c0]),
(76,[a1,a3,a4,b0,b2,b5,c6]),(77,[a1,a3,a4,b0,b2,b6,c5]),
(78,[a1,a3,a4,b0,b5,b6,c2]),(79,[a1,a3,a4,b2,b5,b6,c0]),
(80,[a1,a3,a5,b0,b2,b4,c6]),(81,[a1,a3,a5,b0,b2,b6,c4]),
(82,[a1,a3,a5,b0,b4,b6,c2]),(83,[a1,a3,a5,b2,b4,b6,c0]),
(84,[a1,a3,a6,b0,b2,b4,c5]),(85,[a1,a3,a6,b0,b2,b5,c4]),
(86,[a1,a3,a6,b0,b4,b5,c2]),(87,[a1,a3,a6,b2,b4,b5,c0]),
(88,[a1,a4,a5,b0,b2,b3,c6]),(89,[a1,a4,a5,b0,b2,b6,c3]),
(90,[a1,a4,a5,b0,b3,b6,c2]),(91,[a1,a4,a5,b2,b3,b6,c0]),
(92,[a1,a4,a6,b0,b2,b3,c5]),(93,[a1,a4,a6,b0,b2,b5,c3]),
(94,[a1,a4,a6,b0,b3,b5,c2]),(95,[a1,a4,a6,b2,b3,b5,c0]),
(96,[a1,a5,a6,b0,b2,b3,c4]),(97,[a1,a5,a6,b0,b2,b4,c3]),
(98,[a1,a5,a6,b0,b3,b4,c2]),(99,[a1,a5,a6,b2,b3,b4,c0]),
(100,[a2,a3,a4,b0,b1,b5,c6]),(101,[a2,a3,a4,b0,b1,b6,c5]),
(102,[a2,a3,a4,b0,b5,b6,c1]),(103,[a2,a3,a4,b1,b5,b6,c0]),
(104,[a2,a3,a5,b0,b1,b4,c6]),(105,[a2,a3,a5,b0,b1,b6,c4]),
(106,[a2,a3,a5,b0,b4,b6,c1]),(107,[a2,a3,a5,b1,b4,b6,c0]),
(108,[a2,a3,a6,b0,b1,b4,c5]),(109,[a2,a3,a6,b0,b1,b5,c4]),
(110,[a2,a3,a6,b0,b4,b5,c1]),(111,[a2,a3,a6,b1,b4,b5,c0]),
(112,[a2,a4,a5,b0,b1,b3,c6]),(113,[a2,a4,a5,b0,b1,b6,c3]),
(114,[a2,a4,a5,b0,b3,b6,c1]),(115,[a2,a4,a5,b1,b3,b6,c0]),
(116,[a2,a4,a6,b0,b1,b3,c5]),(117,[a2,a4,a6,b0,b1,b5,c3]),
(118,[a2,a4,a6,b0,b3,b5,c1]),(119,[a2,a4,a6,b1,b3,b5,c0]),
(120,[a2,a5,a6,b0,b1,b3,c4]),(121,[a2,a5,a6,b0,b1,b4,c3]),
(122,[a2,a5,a6,b0,b3,b4,c1]),(123,[a2,a5,a6,b1,b3,b4,c0]),
(124,[a3,a4,a5,b0,b1,b2,c6]),(125,[a3,a4,a5,b0,b1,b6,c2]),
(126,[a3,a4,a5,b0,b2,b6,c1]),(127,[a3,a4,a5,b1,b2,b6,c0]),
(128,[a3,a4,a6,b0,b1,b2,c5]),(129,[a3,a4,a6,b0,b1,b5,c2]),
(130,[a3,a4,a6,b0,b2,b5,c1]),(131,[a3,a4,a6,b1,b2,b5,c0]),
(132,[a3,a5,a6,b0,b1,b2,c4]),(133,[a3,a5,a6,b0,b1,b4,c2]),
(134,[a3,a5,a6,b0,b2,b4,c1]),(135,[a3,a5,a6,b1,b2,b4,c0]),
(136,[a4,a5,a6,b0,b1,b2,c3]),(137,[a4,a5,a6,b0,b1,b3,c2]),
(138,[a4,a5,a6,b0,b2,b3,c1]),(139,[a4,a5,a6,b1,b2,b3,c0])])

  ------------------------------------------------------------------------
M =
S = [0..139]
Equivalence Classes:
a:
{[0,1,2,3],[4,5,6,7],[8,9,10,11],[12,13,14,15],[16,17,18,19],[20,21,22,23],
[24,25,26,27],[28,29,30,31],[32,33,34,35],[36,37,38,39],[40,41,42,43],
[44,45,46,47],[48,49,50,51],[52,53,54,55],[56,57,58,59],[60,61,62,63],
[64,65,66,67],[68,69,70,71],[72,73,74,75],[76,77,78,79],[80,81,82,83],
[84,85,86,87],[88,89,90,91],[92,93,94,95],[96,97,98,99],[100,101,102,103],
[104,105,106,107],[108,109,110,111],[112,113,114,115],[116,117,118,119],
[120,121,122,123],[124,125,126,127],[128,129,130,131],[132,133,134,135],
[136,137,138,139]}

b:
{[0,19,35,75],[1,15,31,71],[2,11,27,67],[3,7,23,63],[4,18,47,87],[5,14,43,83],
[6,10,39,79],[8,17,55,95],[9,13,51,91],[12,16,59,99],[20,34,46,111],[21,30,42,107],
[22,26,38,103],[24,33,54,119],[25,29,50,115],[28,32,58,123],[36,45,53,131],
[37,41,49,127],[40,44,57,135],[48,52,56,139],[60,74,86,110],[61,70,82,106],
[62,66,78,102],[64,73,94,118],[65,69,90,114],[68,72,98,122],[76,85,93,130],
[77,81,89,126],[80,84,97,134],[88,92,96,138],[100,109,117,129],[101,105,113,125],
[104,108,121,133],[112,116,120,137],[124,128,132,136]}
c:
{[0,4,8,12,20,24,28,36,40,48,60,64,68,76,80,88,100,104,112,124],
[1,5,9,16,21,25,32,37,44,52,61,65,72,77,84,92,101,108,116,128],
[2,6,13,17,22,29,33,41,45,56,62,69,73,81,85,96,105,109,120,132],
[3,10,14,18,26,30,34,49,53,57,66,70,74,89,93,97,113,117,121,136],
[7,11,15,19,38,42,46,50,54,58,78,82,86,90,94,98,125,129,133,137],
[23,27,31,35,39,43,47,51,55,59,102,106,110,114,118,122,126,130,134,138],
[63,67,71,75,79,83,87,91,95,99,103,107,111,115,119,123,127,131,135,139]}
```

Updated model when solving the crossing hands exchange in state 1 (Model 2):

```
S = [0,1,2,3,28,29,30,31,36,37,38,39,56,57,58,
     59,80,81,82,83,92,93,94,95,108,109,110,111]
A = [a,b,c]
V = [(0,[a0,a1,a2,b3,b4,b5,c6]),(1,[a0,a1,a2,b3,b4,b6,c5]),
(2,[a0,a1,a2,b3,b5,b6,c4]),(3,[a0,a1,a2,b4,b5,b6,c3]),
(28,[a0,a2,a5,b1,b3,b4,c6]),(29,[a0,a2,a5,b1,b3,b6,c4]),
(30,[a0,a2,a5,b1,b4,b6,c3]),(31,[a0,a2,a5,b3,b4,b6,c1]),
(36,[a0,a3,a4,b1,b2,b5,c6]),(37,[a0,a3,a4,b1,b2,b6,c5]),
(38,[a0,a3,a4,b1,b5,b6,c2]),(39,[a0,a3,a4,b2,b5,b6,c1]),
(56,[a0,a5,a6,b1,b2,b3,c4]),(57,[a0,a5,a6,b1,b2,b4,c3]),
(58,[a0,a5,a6,b1,b3,b4,c2]),(59,[a0,a5,a6,b2,b3,b4,c1]),
(80,[a1,a3,a5,b0,b2,b4,c6]),(81,[a1,a3,a5,b0,b2,b6,c4]),
(82,[a1,a3,a5,b0,b4,b6,c2]),(83,[a1,a3,a5,b2,b4,b6,c0]),
(92,[a1,a4,a6,b0,b2,b3,c5]),(93,[a1,a4,a6,b0,b2,b5,c3]),
(94,[a1,a4,a6,b0,b3,b5,c2]),(95,[a1,a4,a6,b2,b3,b5,c0]),
(108,[a2,a3,a6,b0,b1,b4,c5]),(109,[a2,a3,a6,b0,b1,b5,c4]),
(110,[a2,a3,a6,b0,b4,b5,c1]),(111,[a2,a3,a6,b1,b4,b5,c0])])
Equivalence classes:
a:
{[0,1,2,3],[28,29,30,31],[36,37,38,39],[56,57,58,59],
[80,81,82,83],[92,93,94,95],[108,109,110,111]},
b:
{[0],[1,31],[2],[3],[28,58],[29],[30],[36],[37],[38],[39],[56],[57],
[59],[80],[81],[82],[83],[92],[93],[94],[95],[108],[109],[110],[111]},
c:
{[0,28,36,80],[1,37,92,108],[2,29,56,81,109],
[3,30,57,93],[31,39,59,110],[38,58,82,94],[83,95,111]}
```

Model after Bob's announcement of Eve's possible cards when solving the crossing hands exchange (Model 3):

```
S = [1,31,37,39,59,92,108,110]
A = [a,b,c]
V = [(1,[a0,a1,a2,b3,b4,b6,c5]),(31,[a0,a2,a5,b3,b4,b6,c1]),(37,[a0,a3,a4,b1,b2,b6,c5])
(39,[a0,a3,a4,b2,b5,b6,c1]),(59,[a0,a5,a6,b2,b3,b4,c1]),(92,[a1,a4,a6,b0,b2,b3,c5]),
(108,[a2,a3,a6,b0,b1,b4,c5]),(110,[a2,a3,a6,b0,b4,b5,c1])])
Equivalence classes:
a: {[1],[31],[37,39],[59],[92],[108,110]}
b: {[1,31],[37],[39],[59],[92],[108],[110]}
c: {[1,37,92,108],[31,39,59,110]}
```

Final model when solving the crossing hands exchange in state 1. (Model 4):

```
S = [1,37,39,59,108,110]
A = [a,b,c]
V = (1,[a0,a1,a2,b3,b4,b6,c5]),(37,[a0,a3,a4,b1,b2,b6,c5]),(39,[a0,a3,a4,b2,b5,b6,c1]),
(59,[a0,a5,a6,b2,b3,b4,c1]),(108,[a2,a3,a6,b0,b1,b4,c5]),(110,[a2,a3,a6,b0,b4,b5,c1])]
Equivalence classes:
a:
{[1],[37,39],[59],[108,110]}
b:
```

```
{[1],[37],[39],[59],[108],[110]}
c:
{[1,37,108],[39,59,110]}
```

After Bob's announcement in state 31 (Model 5):

```
S = [1,31,37,39,59,92,108,110]
A = [a,b,c]
V = (1,[a0,a1,a2,b3,b4,b6,c5]),(31,[a0,a2,a5,b3,b4,b6,c1]),
(37,[a0,a3,a4,b1,b2,b6,c5]),(39,[a0,a3,a4,b2,b5,b6,c1]),
(59,[a0,a5,a6,b2,b3,b4,c1]),(92,[a1,a4,a6,b0,b2,b3,c5]),
(108,[a2,a3,a6,b0,b1,b4,c5]),(110,[a2,a3,a6,b0,b4,b5,c1])
Equivalence classes:
a:
{[1],[31],[37,39],[59],[92],[108,110]}
b:,
{[1,31],[37],[39],[59],[92],[108],[110]}
c:
{[1,37,92,108],[31,39,59,110]}
```

After Anne's final announcement in state 31 (Model 6):

```
S = [31,37,39,92,108,110]
A = [a,b,c] (
V = (31,[a0,a2,a5,b3,b4,b6,c1]),(37,[a0,a3,a4,b1,b2,b6,c5]),
(39,[a0,a3,a4,b2,b5,b6,c1]),(92,[a1,a4,a6,b0,b2,b3,c5]),
(108,[a2,a3,a6,b0,b1,b4,c5]),(110,[a2,a3,a6,b0,b4,b5,c1])
Equivalence classes:
a:
{[31],[37,39],[92],[108,110]}
b:
{[31],[37],[39],[92],[108],[110]}
c:
{[31,39,110],[37,92,108]}
```

After Bob's announcement in state 28 (Model 7):

```
S = [0,28,36,38,58,80,82,94]
A = [a,b,c]
V = (0,[a0,a1,a2,b3,b4,b5,c6]),(28,[a0,a2,a5,b1,b3,b4,c6]),
(36,[a0,a3,a4,b1,b2,b5,c6]),(38,[a0,a3,a4,b1,b5,b6,c2]),
(58,[a0,a5,a6,b1,b3,b4,c2]),(80,[a1,a3,a5,b0,b2,b4,c6]),
(82,[a1,a3,a5,b0,b4,b6,c2]),(94,[a1,a4,a6,b0,b3,b5,c2])
Equivalence classes:
a:
{[0],[28],[36,38],[58],[80,82],[94]}
```

```
b:
{[0],[28,58],[36],[38],[80],[82],[94]}
c:
{[0,28,36,80],[38,58,82,94]}
```

After Anne's final announcement in state 28 (Model 8):

```
S = [28,36,38,80,82,94]
A = [a,b,c]
V = (28,[a0,a2,a5,b1,b3,b4,c6]),(36,[a0,a3,a4,b1,b2,b5,c6]),
(38,[a0,a3,a4,b1,b5,b6,c2]),(80,[a1,a3,a5,b0,b2,b4,c6]),
(82,[a1,a3,a5,b0,b4,b6,c2]),(94,[a1,a4,a6,b0,b3,b5,c2])
a:
{[28],[36,38],[80,82],[94]}
b:
{[28],[36],[38],[80],[82],[94]}
c:
{[28,36,80],[38,82,94]}
```

After Bob's announcement in state 58 (Model 9):

```
S = [0,28,36,38,58,80,82,94]
A = [a,b,c]
V = (0,[a0,a1,a2,b3,b4,b5,c6]),(28,[a0,a2,a5,b1,b3,b4,c6]),
(36,[a0,a3,a4,b1,b2,b5,c6]),(38,[a0,a3,a4,b1,b5,b6,c2]),
(58,[a0,a5,a6,b1,b3,b4,c2]),(80,[a1,a3,a5,b0,b2,b4,c6]),
(82,[a1,a3,a5,b0,b4,b6,c2]),(94,[a1,a4,a6,b0,b3,b5,c2])
Equivalence classes:
a:
{[0],[28],[36,38],[58],[80,82],[94]}
b:
{[0],[28,58],[36],[38],[80],[82],[94]}
c:
{[0,28,36,80],[38,58,82,94]}
```

After Anne's final announcement in state 58 (Model 10):

```
S = [0,36,38,58,80,82]
A = [a,b,c]
V = (0,[a0,a1,a2,b3,b4,b5,c6]),(36,[a0,a3,a4,b1,b2,b5,c6]),
(38,[a0,a3,a4,b1,b5,b6,c2]),(58,[a0,a5,a6,b1,b3,b4,c2]),
(80,[a1,a3,a5,b0,b2,b4,c6]),(82,[a1,a3,a5,b0,b4,b6,c2])
Equivalence classes:
a:
{[0],[36,38],[58],[80,82]}
b:
```

```
{[0],[36],[38],[58],[80],[82]}
c:
{[0,36,80],[38,58,82]}
```

# Bibliography

M. H. Albert et al. Safe communication for card players by combinatorial designs for two-step protocols. *Australasian journal of Combinatorics*, 33, 2005.

Michael Albert, Andrés Cordón-Franco, Hans van Ditmarsch, David Fernández-Duque, Joost J Joosten, and Fernando Soler-Toscano. Secure communication of local states in interpreted systems. pages 117–124, 2011.

Steven M. Bellovin. Frank miller: Inventor of the one-time pad. *Cryptologia*, 35(3): 203–222, 2011.

Edmund M Clarke Jr, Orna Grumberg, Daniel Kroening, and Helmut Veith. *Model checking*. Cyber-Physical Systems, 2018.

Andrés Cordón-Franco et al. A colouring protocol for the generalized russian cards problem. *Theoretical Computer Science*, 495:81–95, 2013.

Andrés Cordón-Franco et al. A geometric protocol for cryptography with cards. *Designs, Codes and Cryptography*, 74(1):113–125, 2015.

Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

T. Kirkman. On a problem in combinations. *Cambridge and Dublin Mathematics Journal*, 2(19120):4, 1847.

Ralph C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.

Allam Mousa and Ahmad Hamad. Evaluation of the rc4 algorithm for data encryption. *IJCSA*, 3(2):44–56, 2006.

Fabien Ap. Petitcolas. Kerckhoffs' principle. In U. S. Springer, editor, *Encyclopedia of cryptography and security*, pages 675–675. 2011.

Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

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

Colleen M. Swanson and Douglas R. Stinson. Additional constructions to solve the generalized russian cards problem using combinatorial designs. *arXiv preprint*, 2014a.

Colleen M. Swanson and Douglas R. Stinson. Combinatorial solutions providing improved security for the generalized russian cards problem. *Designs, Codes and Cryptography*, 72(2):345–367, 2014b.

H. Van Ditmarsch and F. Soler–Toscano. Three steps. *In International Workshop on Computational Logic in Multi-Agent Systems*, pages 41–57, 2011.

Hans van Ditmarsch. The russian cards problem. *Studia logica 75.1*, pages 31–62, 2003.

Hans van Ditmarsch and Barteld Kooi. *One hundred prisoners and a light bulb.* Copernicus, Cham 83-94, 2015.

Hans van Ditmarsch, Wiebe van der Hoek, R. van der Meyden, and J. Ruan. Model checking russian cards. *Electronic Notes in Theoretical Computer Science*, pages 105–123, 2006.

Hans van Ditmarsch, Wiebe van Der Hoek, and Barteld Kooi. *Dynamic epistemic logic.* Springer Science & Business Media, 2007.

Hans P. van Ditmarsch. The case of the hidden hand. *Liber Amicorum Dick de Jongh*, 2004. URL `http://www.illc.uva.nl/D65/`.

Hans P. van Ditmarsch. The case of the hidden hand. *Journal of Applied Non-Classical Logics*, 15(4):437–452, 2005.

Jan van Eijck. Demo-s5. 2014.