Erotetic Epistemic Logic in Private Communication Protocol

PETR ŠVARNÝ[1], ONDREJ MAJER[2]
AND MICHAL PELIŠ[3]

Abstract:
The Russian Cards Problem is a toy model of safe communication via an open channel. It has been widely discussed in the literature, some of the recent approaches employ the apparatus of dynamic epistemic logic and represent communication of players by public announcements. In this article we propose a solution which adds questions to players communication toolkit. We compare it to the solutions using public announcements and provide some complexity bounds.

Keywords: russian cards problem, epistemic logic, erotetic logic, public announcement

1 Introduction

The Russian Cards Problem (RCP) is a coordination game between two agents with a third agent trying to eavesdrop on their exchange. The goal of cooperating agents is to publicly communicate each other's hand without providing any information to the third agent. The RCP problem was originally formulated on Russian Mathematics Olympiad at 2000 as a problem in information theory, but later it was introduced in the epistemic logic community by van Ditmarsch (2003). Together with his coauthors, he later presented mainly combinatorial solutions to the problem in (van Ditmarsch, van der Hoek, van der Meyden, & al., 2006). His original paper was, however, based on epistemic logic. A possible limitation of RCP is in its strict algorithm. Follow-up works to the original articles do explore the possible combinations of agents and cards involved in an RCP protocol, see (Albert,

[1]The work on this paper was supported by the Internal grant of the Faculty of Arts, Charles University in Prague, VG176.

[2]The work on this paper was supported by the grant GA13-21076S of the Grant Agency of the Czech Republic.

[3]The work on this paper was supported by Program for Development of Sciences at the Charles University in Prague no. 13 (Prvouk) Rationality in the Human Sciences, section Methods and Applications of Modern Logic.

Aldred, Atkinson, van Ditmarsch, & Handley, 2005; Duan & Yang, 2009). All these suggestions maintain the possibility of publicly sharing information without allowing an eavesdropper to cause harm. We will discuss the protocol in more detail later.

Nevertheless, there was no qualitative shift in the protocol. Our attempt in this article is to elaborate on the logical part of the protocol by adding tools from erotetic logic in the sense of (Peliš & Majer, 2011).

We have a few assumptions on which our work is based. First of all, agents are sincere. Hence they do not attempt any deception. They can only present true information. However, unless they are directly asked, they can choose to divulge only a part of the information available to them or add superfluous information.

Second, the agents are simple software agents. We do not assume that the agents are human-like. Hence, they do not have very complicated states and their information is stored in a well-defined system of finite statements. They also lack complex agendas to support their question posing strategies.

Last, we assume that the agents' knowledge can be represented by means of epistemic logic.

These assumptions are based on the view that a great deal of autonomous communication (for example on the Internet) can be performed by simple agents which need to deal with complex epistemic situations. An exemplar task can be the identification of a string like 20010db8142857ab. Questions enriched RCP agents could communicate such an information privately via public channels and discern, whether it is a Hexadecimal MAC address (20-01-0d-b8-14-28-57-ab), an IPv4 address (2001.0db8.1428.57ab), or an abbreviated IPv6 address (2001:0db8:0000:0000:0000:0000:1428:57ab). We will see now what obstacles we have to overcome in order to get this desired result and what we learn about questions when we use them for this purpose.

2 Russian Cards Problem

There are three agents named Anne, Bill, and Crow, abbreviated A, B, and C. Each of them receives some cards from a given stack of cards, which is known to all of them. In the case of the archetypal RCP, it is seven cards which are marked by numbers from 0 to 6. Anne and Bill get each three cards and Crow gets the last card. The state of the game can be represented as a pointed modal model over a propositional language extended with a knowledge operator K_i, common knowledge operator C, and a public an-

nouncement operator $[\psi]$. What we will call archetypal RCP can be summed up in the following way.

- Players: Anne, Bill, Crow
- Card deals (in the order A, B, C) of the type: $3 \mid 3 \mid 1$ (if we want to display the actual card deal explicitly, then, e.g., $012 \mid 345 \mid 6$)
- Basic goals of the problem:
  - B must be able to infer the actual hand of A (and vice versa)
  - C must not be able to infer any of A's cards
  - C must not be able to infer any of B's cards
- Common knowledge among agents: All of here mentioned except the actual deal
- Tools: Pointed (modal) models over a propositional language containing $K_i\varphi$ (individual knowledge of an agent i), $C\varphi$ (common knowledge of the group of all agents), $[\psi]\varphi$ (after publicly announcing ψ the formula φ is valid)

We should mention, that a deal $012 \mid 345 \mid 6$ does not have to mean that the agents get exactly these cards. It signifies that the agents get all distinct cards and no card is repeated in the distribution. The numbers merely signify the type and are given starting from the first card of the first player. The given solutions of RCP do not depend on a particular card deal.

An example of the resulting pointed modal model is a Hexa model. This model is much simpler than a general RCP case, as it represents three agents sharing three cards. Each agent has only one card. The number sequence then shows how agents have their cards distributed. The card distribution 012 means that Anne holds the card 0, Bill the card 1 and Crow card 2. The formula describing this state is therefore:

$$012 \equiv 0_a \wedge \neg 1_a \wedge \neg 2_a \wedge \neg 0_b \wedge 1_b \wedge \neg 2_b \wedge \neg 0_c \wedge \neg 1_c \wedge 2_c \qquad (1)$$

The following Figure 1 shows three agents, each holding one card and not knowing about the distribution of the other cards.

Notice that each state represents a card deal and hence the main problem for the agents is to distinguish between card deals, i.e., states. Examples of

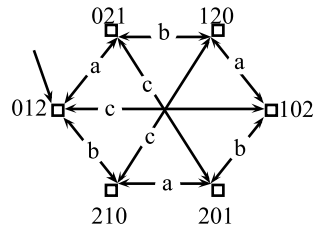

Figure 1: Hexa example from (van Ditmarsch, 2003)

simple formulae satisfied in this model are $K_a 0_a$(Anne knows she holds the card 0) or $K_b \neg K_a 1_b$ (Bill knows Anne does not know he holds the card 1).

The question that interested Albert et al. (2005) was what the conditions for *good announcements* are. A good announcement is such an announcement that the eavesdropper does not have a possibility to guess the cooperating agents' cards, but it helps the cooperating agents to advance in their goal. This is the main research question in RCP—for what card distributions are we able to get good announcements. Most of the cited works list different conditions on the numbers of cards for these safe distributions, i.e. those where a good announcement can be made. The main problem is that some of the possible card distributions do not allow for good announcements. Agents simply do not have enough cards to create an announcement that would satisfy these conditions.

In the case of an archetypal RCP, these are two examples of possible good announcements for the agent A:

- $[K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a \vee 245_a)]$
- $[K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a)]$

The study in (Albert et al., 2005) lists conditions for announcements and also the card distributions that make good announcements possible. If these conditions are not met, there is no announcement which would be safe from an eavesdropper.

Already van Ditmarsch (2003) addressed the question how to deal with the security aspect of the RCP protocol and presented the following example of its application.

Example 1. There are seven cards $0, 1, \ldots, 6$. Anne's hand is 125. She knows only her own cards now, that there are seven cards, and that either Bill or Crow hold the three cards 346. She wants to find out who holds the three cards. She realizes that both 251 and 643 are prime numbers. She can now either announce: "Who is the first to tell me the factorization of 161393?" which we may expect Bill to do faster than Crow, as Bill can simply divide that number by 634 (his 'private key', so to speak), or she may announce one of the direct exchanges for hand 125, e.g.: "My hand is one of $\{125, 023, 246, 045, 356, 016, 134\}$" after which only Bill, who actually holds 346, and not Crow, is able to tell her that she holds 125. In the first case, Crow is (presumably) not fast enough ('too complex') to pose as Bill with certainty, in the second case, it is impossible to pose as Bill with certainty.

This leads to the motivation to investigate the interaction of larger numbers of agents in later works, see (Duan & Yang, 2009). This is done still along the same basic lines of the original RCP problem. The world of agents, however, can be a lot more complicated. For this reason a generalization of RCP is a desired step for a more profound analysis of the protocol.

We obtain a generalization of RCP simply by loosening the rules connected to the RCP problem. For example the number or relations of players may be different or, more importantly, the card distribution can change and we can have cards that repeat themselves. It is also possible that the agents have only partial information available or none at all. Therefore generalized RCP cannot be solved with standard means. Questions could be a possible way of solving these generalized RCP problems. In order to do this, we need to learn about the role of questions in the archetypal RCP first.

3 Questions

We will use the framework developed in (Peliš & Majer, 2011). This framework is characterized by using set of answers methodology (a question is identified by a set of direct answers) and by an epistemic approach to questions. A question is understood as an epistemic statement, in which the inquirer informs the audience about her ignorance.

The language of erotetic epistemic logic is generated by the following BNF:

$$\psi ::= p \mid \neg\psi \mid (\psi \wedge \psi) \mid K_i\psi \mid ?_i \{\psi, ...\}$$

As in every normal modal logic we can define a dual operator $\hat{K}_i\psi \equiv \neg K_i \neg \psi$ with the meaning 'the agent *i* admits ψ'. A question is given by a set of direct answers $?_i\{\alpha_1, \alpha_2, \ldots \alpha_n\}$. In other words, an agent i asks : "Is it the case that α_1 or is it the case that α_2, ...?"[4] RCP allows only for public updates and therefore we assume that also questions are public. Our scenario presupposes that some agent in the audience eventually chooses one of these options and announces the correct answer. These questions should satisfy three basic conditions: (1) answers are syntactically distinct, (2) there are at least two direct answers, and (3) the set of direct answers dQ^i is finite. In short, answers should be distinguishable and if there is only one option to answer, then the agent does not need to ask a question.

The central semantic notion is the one of *askability* of a question. This replaces the notion of truth in the semantics of standard propositional languages as it makes sense to ask a question in a certain situation, but it never makes sense to say that a question is true. A question $?_i\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ is askable (for an agent i at a given state s of a model M)[5] iff it satisfies the following conditions:

1. $(M, s) \not\models K_i\alpha$, for each $\alpha \in dQ^i$
2. $(M, s) \models \hat{K}_i\alpha$, for each $\alpha \in dQ^i$
3. $(M, s) \models K_i(\bigvee_{\alpha \in dQ^i} \alpha)$

The first condition is called *non-triviality*—it is not reasonable to ask a question if the agent knows the answer. The second one, *admissibility*, requires that each direct answer is considered (by an agent i) as possible. And the third condition, *context*, means that at least one of the direct answers must be the right one (with respect to the knowledge of an agent i).

The third condition is problematic in some cases. It is superfluous for so called *safe questions*. For example, Anne's question "Does Bill hold 4?" is safe because the context of the question is given by tautology $(4_b \vee \neg 4_b)$.

Now, consider a question "Which natural number is greater than 13?", we can expect various answers to it, e.g., sets of some numbers greater than

[4] Representing a question as a set of direct answers does not correspond to the usual grammatical form of questions. A question can be more complex than just giving a list of direct answers. However, as our agents are simpletons, we can assume agents actually present the questions in this form.

[5] Our models are standard S5-models as it is usual in logics representing knowledge.

13, just one number greater than 13 or all the numbers greater than 13. Asking such a question an agent should only specify the form of expected answers (for example, she requires a singleton, some examples or a complete list), but she obviously does not list all possible answers.

Listing all the possible options in a real world situation could amount to a very long list. We could instead require that an agent lists a set of possible answers *she* has in mind and she is aware of the fact, that her list is incomplete. A new answer can be added by other agents and the agent then updates her knowledge. We allow this by omitting the context condition from the definition of askability.

This leads us to a generalization of the term *askability*. A *generally askable question* $?_i\{\alpha_1, \alpha_2, \ldots\}$ in a state s of a model M for an agent i is a question satisfying only the first two conditions of askability (non-triviality and admissibility).

4 Questionable RCP

Let us now combine RCP and questions. If we approach RCP with questions, we can get a system very similar to the original RCP. Now instead of announcing, Anne asks Bill, what cards he has. Does there exist an (RCP) *good question* that would allow Anne to learn about Bill's cards without Crow learning also?

First of all, Anne can ask Crow. We assumed all the agents are truth speaking and hence it is a valid option. This option is trivial, as Anne can ask single card questions (e.g., "Do you hold 4?") until she finds what card Crow has. The only necessary point is, Anne should ask also about her own cards. If she only asks about cards that she does not have, this protocol would not be safe. If done so, Crow cannot infer from Anne's questions what cards she has. However, in generalized RCP problems, Crow could have multiple cards. Depleting all the possibilities in that case could take a very long time.

Another important feature comes to light already at this early stage. Questions differ from announcements in that they do not allow for triviality. Hence Anne could not ask Crow about her cards in this fashion because she already knows that Crow does not hold her cards. The violation is clearly visible in this case. However, we need to keep it in mind later, in the more complex situations.

Let us return to Crow as the passive eavesdropper. A straightforward

way how to introduce questions is to change the good announcement of Anne directly into a question. We demonstrate these options on the simple case of the archetypal seven card RCP.

Example 2. Anne's *good announcement* would be $[K_a(012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a)]$, hence the question would be $?_a\{K_b(012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a), \neg K_b(012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a)\}$. In other words, Anne asks Bill: "Do you think I hold one of these triplets?" Bill simply answers yes or no.

Here comes the twist. If he answers yes, Anne knows Bill knows her cards. However, because the question is based on the good announcement, Bill would never answer no. Therefore the question is trivial for Anne and it is unaskable according to the conditions. Let us try to construct a question that is askable for Anne. Anne could try to ask Bill about his cards instead of asking him about hers. Let us show the whole communication this time.

Example 3. Anne has her 012, Bill his 345, and Crow the 6. If Anne asks Bill over an open channel "Do you have one of these $\mathbf{02}5$, $\mathbf{0}34$, $\mathbf{0}56$, $\mathbf{12}3$, $\mathbf{1}45$, $\mathbf{2}36$, 346, 456?" Bill will respond with a simple "no". At this moment Anne knows that Bill does not have neither 346 nor 456 (the remaining combinations contain always a card from Anne). Bill has no idea what is going on. Crow eliminates combinations that have his card and the remaining combinations he knows Bill does NOT have. Crow still has to take into account 15 options. Anne has only two left, 345 and 356. Hence Crow has according to Anne either 4 or 6. So the follow-up question to Bill would be "Are your cards from these 012345?". Now Bill says "yes". Thus Anne knows Bill's cards.

Is the first question askable for Anne? Yes, it is in the form $?_a\{(025_b \vee 034_b \vee 056_b \vee 123_b \vee 145_b \vee 236_b \vee 346_b \vee 456_b), \neg(025_b \vee 034_b \vee 056_b \vee 123_b \vee 145_b \vee 236_b \vee 346_b \vee 456_b)\}$. Both answers are a genuine possibility for Anne so the question is not trivial. Bill can also know Anne's cards, because if the protocol is fixed, he knows that a yes answer for the second question means that the set of cards was composed only of Anne's and Bill's cards.

We can see that even if the first question would be different, the outcome would be the same.

Example 4. Anne asks Bill "Do you have one of these $\mathbf{02}5$, $\mathbf{0}34$, $\mathbf{0}56$, $\mathbf{12}3$, $\mathbf{1}45$, $\mathbf{2}36$, 345, 456?" Bill's answer is now positive. Hence for Anne, Bill

either has 345 or 456, the decisive cards being 3 and 6. She can make a similar second question as in the previous example. In the case of Crow this option presents a better outcome, as it has now five options to choose from.

Notice that the union of Crow's options covers the whole range of cards and that there is no intersection among the card sets. This is a property necessary for good announcements. However, it is *not* a necessity in the case of a good question. Natural language questions benefit from the possible incompleteness or even unintentional falsity of presented information. They also do suffer from this as we might need to construct a follow-up question.

If the second question is not as lucky, we can have a problem. The union of cards that are possible for Crow shows 012356. Crow learns that Anne does not know about 4. Hence she has 123 or 025.

Anne's original announcement can contain more options. This would worsen Crow's situation. Anne can construct her question based on the cards she takes as possible for Bill's hand, in our case 345, 346, 356, 456. She takes two of these and then she populates the length of the announcement (in the exemplar case up to eight cards) with random card combinations with approximately the same number of each card (in our case a card should be in the combinations three times on average).

Definition 1 (Good question) *A* good question *is a question from a cooperating agent that after being answered by another cooperating agent does not allow the eavesdroppers to know any of the cards of the cooperating agents' hand and it allows a cooperating agent to reduce the amount of possible combinations in another cooperating agent's hand to at least a half of the original amount of options (rounded down).*

As there are results characterizing for good announcements in RCP, it would be suitable to profit from them. For this purpose let us construct a good question from a good announcement. The algorithm for Anne to achieve this goal is the following:

- Prepare a good announcement
- Add half of Bill's possible hands (rounded up)
- Add possible hands containing always at least one card from Anne to even out card occurrences or change cards in present hands, following:
  - avoid duplicity

- do not alter Bill's possible hands
- maintain in all the hands at least one card from Anne, unless they are possible hands for Bill
- do not add too many options

The last point, about adding too many options, will be discussed later. For now, let us concentrate on the RCP with three agents as before, with a general card distribution $a \mid b \mid c$. We start with a case, when both cooperating agents have the same number of cards.

Proposition 1 *It holds in an RCP with a symmetrical card distribution between the cooperating agents, that if there is a good announcement, then there is a good question.*

Proof. Let us have a good announcement. If Anne adds to the good announcement half of the hands she takes as possible for Bill and then adds possible hands to the question to have all the cards represented in almost the same number. This is a good question. Based on Bill's answer, Anne can eliminate at least half of the options for Bill (rounded down). Because of the equality of card numbers, Crow has multiple options for Anne's cards and Bill's cards. □

Example 5. Let's assume a $4 \mid 4 \mid 1$ case, where Anne has 0123, Bill 4567 and Crow 8. Anne has the following good announcement: "I have some of these: $\mathbf{0123}$, $\mathbf{01}46$, $\mathbf{01}58$, $\mathbf{01}67$, $\mathbf{02}46$, $\mathbf{03}46$, $\mathbf{03}68$, $\mathbf{03}78$, $\mathbf{12}48$, $\mathbf{13}45$, $\mathbf{13}56$, $\mathbf{1}457$, $\mathbf{23}57$, $\mathbf{2}457$, $\mathbf{2}478$, $\mathbf{2}678$, $\mathbf{3}458$, $\mathbf{3}567$". Anne adds to this good announcement the possible cards for Bill's hand, for example $4567, 4678, 5678$. The cards with the most occurrences are now 4 and 6, while 2 is with the least. Hence Anne does the following replacements: 1356 with 1235 and 0246 with 0236. Then she announces the question: "Do you have any of these: $\mathbf{0123}$, $\mathbf{01}46$, $\mathbf{01}58$, $\mathbf{01}67$, $\mathbf{023}6$, $\mathbf{03}46$, $\mathbf{03}68$, $\mathbf{03}78$, $\mathbf{12}48$, $\mathbf{13}45$, $\mathbf{123}5$, $\mathbf{1}457$, $\mathbf{23}57$, $\mathbf{2}457$, $\mathbf{2}478$, $\mathbf{2}678$, $\mathbf{3}458$, $\mathbf{3}567$, $4567, 4678, 5678$?"

Let us generalize to an RCP with a different number of cards but fulfilling the RCP conditions for card distribution from (Albert et al., 2005). We have two possible situations. Either Anne has more cards than Bill or Bill has more cards than Anne. The first case can be in the following form:

Example 6. For a $6 \mid 2 \mid 1$ case, the smallest with Anne having more cards that allows good announcements according to Albert et al. (2005), the original good announcement of Anne can be: 012345, 012356, 012347, 012348, 014567, 135678, and so on. For the question Anne takes the pairs of options for Bills cards, that is 67, 68, 78 and takes two of them. Then she takes her good announcement and from each set takes two cards, at least one being her card. For example from 012345 she gets 01 or 135678 makes 37.

The second case can end up like this:

Example 7. For the distribution $3 \mid 4 \mid 1$, a good announcement of Anne is 012, 034, 057, 136, 145, 235, 267. Anne adds to each of these an additional card from those she does not hold thus creating possibly the following question 0124, 0157, 0346, 1367, 1456, 2356, 3456, 3567 base is created, then she adds the possible cards of Bill, for example 3457, 3567, 4567 and finishes with the usual addition of new cards based on the quantity of the cards.

Proposition 2 *It holds in an RCP with an asymmetrical card distribution between the cooperating agents, that if there is a good announcement, then there is a good question.*

Proof. We need to distinguish the two cases, when Anne has more cards than Bill or vice versa.

In the first case, Anne takes at least half of Bill's possible hands. She adds hands created from each of hands in the good announcement. Each such hand has to contain at least one card from Anne's hand. Thereafter she adds more hands to keep the occurrence of individual cards even.

This is a good question. Anne added the possible cards of Bill. If she added Bill's actual hand, then she successfully eliminated half of the possible options. If she did not list the actual hand, she still eliminated half of the options. Because of the equal representation of cards, Crow has still enough possible hands and hence does not know which hand is the correct one.

In the second case, Anne adds possible Bill's cards to her good announcements and then adds at least half of the possible Bill's hands to the question. In the end, Anne has to compensate for the number of cards by adding additional hands. This again will be a good question. Bill can identify his hand if it is present or not. Anne, thanks to the construction of her question, eliminates half of the options from possible Bill's cards. Thanks to the equal distribution of cards, Crow remains again with multiple options. □

Corollary 1 *In RCP, if the card distribution has a good announcement, we can create a good question.*

The opposite does not hold and therefore good questions and good announcements are not equivalent. We can see this on the following example.

Example 8. The distribution $012 \mid 34 \mid 5$ allows Anne to ask a good question. This can be done by asking Bill about the cards 02, 03, 12, 14, 25, 35, 45.

The feature that distinguishes a good announcement from a good question is that the proposition in the question can be false, but that answer is still informative. In the example, Bill will answer no. Thanks to that Anne knows Bills cards and hence can announce Crows card. A good announcement in this case would fail on the lack of cards. When Anne holds 012 and announces the options for her hand, she has little options before introducing triplets with two cards from her hand. Due to the limited amount of options, Anne will be able to present cards that contain the 5, hence get eliminated by Crow (any ending with 5), or repeat Bill's cards (i.e. 034, 134, 234). She cannot use two cards from her hand because she risks announcing a triple Bill would take as a possible hand for Anne (015, 025, 125).

5 Complexity

We promised to address also the problem of the amount of hands in a good question. Anne needs enough cards to make the question confusing for Crow and have a possibility to ask follow-up questions if necessary.

Observation 1 *Let us have an RCP problem with a distribution $a \mid b \mid c$. Then the upper bound for the number of hands for a good question is*

$$\binom{a+b+c}{b} \cdot \frac{1}{b-1} \tag{2}$$

The idea is to take all the combinations of cards for Bill's hand size and limit the amount in proportion to that hand size. The limitation is necessary, because the larger the amount of cards held by Bill is, the larger the amount of possibilities will be. However, for a good question we do not need to list all of them. Obviously, the other constrains from the transformation algorithm still apply. Hence we try to have the same occurrence of cards and the question also contains at least half of the possible hands of Bill.

Because we are able to construct good questions from good announcements, we can use the bounds set for the size of good announcements in (Albert et al., 2005). We can alter these bounds by adding at least half of the number of cards based on Bill's possible hands. This follows straight from the way we constructed our good questions.

Observation 2 *Let us have an RCP problem with a distribution $a \mid b \mid c$. Then the lower bound for the number of hands for a good question is*

$$\frac{(a+b)(a+b+c)}{b(b+c)} + \left\lceil \frac{1}{2}\binom{b+c}{b} \right\rceil \tag{3}$$

Albert et al. (2005) presented two upper bounds. The first equation is a bound for the case when $b + c \leq a$, the second one is for all the other cases of good announcements.

$$\frac{(a+b+c)!(c+1)!}{(b+c)!(c+a+1)!} \left\lfloor \frac{a+c+1}{c+1} \right\rfloor \tag{4}$$

$$\frac{(a+b+c)!(c+1)!}{a!(b+2c+1)!} \left\lfloor \frac{(b+2c+1)}{(c+1)} \right\rfloor \tag{5}$$

We can construct our upper bounds based on these two equations.

Observation 3 *Let us have an RCP problem with a distribution $a \mid b \mid c$, where $b + c \leq a$. Then the suitable upper bound for the number of hands for a good question is*

$$\frac{(a+b+c)!(c+1)!}{(b+c)!(c+a+1)!} \left\lfloor \frac{a+c+1}{c+1} \right\rfloor + \left\lceil \frac{1}{2}\binom{b+c}{b} \right\rceil \tag{6}$$

Observation 4 *Let us have an RCP problem with a distribution $a \mid b \mid c$, where $b + c \not\leq a$. Then the lower bound for the number of hands for a good question is*

$$\frac{(a+b+c)!(c+1)!}{a!(b+2c+1)!} \left\lfloor \frac{(b+2c+1)}{(c+1)} \right\rfloor + \left\lceil \frac{1}{2}\binom{b+c}{b} \right\rceil \tag{7}$$

A proof that this works in the case of good announcement based questions is trivial. An interesting observation is that these boundaries work also for cases without good announcements.

Example 9. The distribution $012 \mid 34 \mid 5$ has an upper boundary for the questions given based on the equation (6) and the calculation gives us 7 as answer. The lower bound is 6. The example used the good question of length 7, namely 02, 03, 12, 14, 25, 35, 45. A shorter version can be 02, 03, 12, 14, 35, 45.

The protocol how to make a good question without using a good announcement is very simple and quite similar to the original protocol.

- Take randomly half of the possible hands of Bill (rounded up)
- Add hands composed of at least one card from Anne's hand while
  - not repeating any hand
  - maintaining an approximately equal occurrence of cards in the question
  - do not exceed the number of cards given by the upper bound

The fact that we have this protocol does not mean we can construct a good question for any card distribution (for example $1 \mid 1 \mid 1$ is still an unsolvable case). However, it does allow us to address a larger number of card distributions than the good announcements did. At least for this reason, it is worth thinking about questions in the RCP.

6 Conclusion

We explored the possibility of using questions instead of announcements in the protocol of the Russian Cards Problem. We concentrated on the RCP class with two cooperating agents and one eavesdropper without repetition of cards. We showed that questions provide more general solutions for this class: for any solution in the form of a good announcements there is a solution in the form of a good question, but not vice versa. We presented an example for which a good question exists, but a good announcement does not. We also gave some complexity bounds for the amount of hands necessary for a good questions.

We plan to use questions in more general Russian cards problems which include more players and allow for card repetitions. This might require extension of the framework of questions and employing weaker background epistemic systems than from S5. A useful step to elaborate on the topic

is also the introduction of trust among agents. The basic inspiration comes from the article (Baltag & Smets, 2009). There general plausibility frames are endowed with 'Radical' Upgrade and 'Conservative' Upgrade. This would allow the agents to have a hierarchy similar to the contemporary hierarchy of trust protocol servers.

References

Albert, M., Aldred, R., Atkinson, M., van Ditmarsch, H., & Handley, C. (2005). Safe Communication for Card Players by Combinatorial Designs for Two-step Protocols. *Australasian Journal of Combinatorics*, *33*, 33–46.

Baltag, A., & Smets, S. (2009). Talking Your Way into Agreement: Belief Merge by Persuasive Communication. In *Proceedings of the Second Multi-Agent Logics, Languages, and Organisations.* Aachen: Federated Workshops.

Duan, Z., & Yang, C. (2009). Generalized Russian Cards Problem. In D.-Z. Du, X. Hu, & P. Pardalos (Eds.), *Combinatorial Optimization and Applications* (pp. 85–97). Berlin: Springer.

Peliš, M., & Majer, O. (2011). Logic of Questions and Public Announcements. In *Eighth International Tbilisi Symposium on Logic, Language and Computation 2009, Lecture Notes in Computer Science* (pp. 145–157). Berlin: Springer.

van Ditmarsch, H. (2003). The Russian Cards Problem: A Case Study in Cryptography With Public Announcements. *Studia Logica*, *75*, 1–32.

van Ditmarsch, H., van der Hoek, W., van der Meyden, R., & al. (2006). Model Checking Russian Cards. *Electronic Notes in Theoretical Computer Science*, *149*, 105–123.

Ondrej Majer
Institute of Philosophy, Czech Academy of Sciences
The Czech Republic
E-mail: majer@flu.cas.cz

Michal Peliš
Charles University in Prague
Institute of Philosophy, Czech Academy of Sciences
The Czech Republic
E-mail: michal.pelis@ff.cuni.cz

Petr Švarný
Charles University in Prague
The Czech Republic
E-mail: svarnypetr@gmail.com