2012 3rd International Conference on Information Security and Artificial Intelligence (ISAI 2012)
IPCSIT vol. 56 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V56.24

The Russian Poker Game

Petr Švarný [+]

[1] University of Economics, Prague, Czech Republic

Abstract. The Russian cards problem is introduced in its classical form and thereafter it is generalized to a poker game. This serves as a preliminary basis for the investigation of public private communication.

Keywords: Dynamic epistemic logics; Russian cards problem; Multi-agent systems.

1. Introduction

One could wonder if there are possibilities to share knowledge without letting eavesdroppers gain any important information. There can be restrictive options of limiting unwanted access to private information, even when it is seemingly publicly available [1]. This paper, however, follows a different approach to the problem. This approach goes via the so called Russian cards problem. We first introduce the original problem and then generalize its ideas. Thereafter we present briefly a model based on the Russian cards problem to evaluate Texas hold'em poker games and present some suggestions of its use for secure public communication.

2. Russian Cards Problem

The Russian cards problem (RCP) was thoroughly studied by van Ditmarsch [2] and his colleagues [3]. The basic problem can be given by the following statement: "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?"

We will introduce RCP while still remaining in the context of card games and we will keep it informal.

2.1. Basic analysis of the problem

Van Ditmarsch has prepared a way how to treat RCP in a formal manner. Every deal of cards is described as a ordered list of numbers (representing cards), e.g. 012|345|6 is the distribution of cards where the first player, usually called Anne, gets the first three cards, the second player, Bill, has the next three cards and the last player, Crow, has the last card. The players only know their own hands for sure and they see the number of cards the other players have. There is an option for Anne to publicly announce a statement that would allow Bill to figure out Anne's card. This announcement is "I hold one of the following triplets: 012, 034, 056, 135, 246." After this announcement Bill knows Anne's cards and he can announce that Crow has the card 6. Therefore Anne will know also Bill's cards. It is only Crow who remains without knowing the precise distribution of cards between the two players. Yet, he knows now that Anne and Bill know their hands.

When we face the problem of RCP, we notice immediately that there are some limitations at place. Their exact nature was studied in the article [3] and it was shown that we can allow for different card distributions.

[+] Corresponding author. Tel.: + 420 736 227 887.
E-mail address: svarnypetr@gmail.com.

This means we do not have to distribute in the pattern 3|3|1, but it is enough to follow some limitations and Anne will be able to give a "good announcement", i.e. share her cards with Bill.

2.2. Generalization

We can, however, even continue on with these generalizations. In short we can find the following parameters of a RCP:

- Number of players – in RCP three: Anne, Bill, Crow.
- Relation of players – Anne and Bill collaborate, Crow is antagonistic.
- Positions – the pattern of cards, in RCP 3|3|1.
- Cards – the set of used cards, in RCP {0,…,6}.
- Card deal type – how the cards are distributed into the positions, in RCP it is the archetype 012|345|6, meaning every card is dealt and it is dealt only once.
- Knowledge – what do the players know about the situation, in RCP they know all the above mentioned, they only do not know which exact deal of cards is currently in play.
- Post-conditions – the conditions that have to be met at the end of the game, in RCP it is that Anne and Bill know each other's cards correctly and Crow remains ignorant of their cards.

The only assumption that evades these parameters and stays implicit is that there are no empty positions and that we have an unlimited supply of even identical cards if needed. Post-conditions were already introduced by van Ditmarsch as a necessity to assure that the protocol really tells us what we want to know. We can describe this in the following general formula for a generalized RCP: <#players; relation of players; positions; cards; card deal type; knowledge; post-conditions>.

3. Card games

RCP does not represent an actual card game. We could, however, use our general parameters to investigate actual card games and hence present already the first application of van Ditmarsch's work. Due to the presence of public information, we can for example think of Texas hold'em poker as an option. The traditional way how to solve this kind of card games is to use probability. Here we would use dynamic epistemic logic, the basis of RCP's analysis from van Ditmarsch.

A poker game can be given by RCP's parameters as follows: < N; no one collaborates; 5|…|5; the poker card pack; all the cards are different, none is dealt twice, not all cards are dealt; players know all the above mentioned, they only do not know which exact deal of cards is currently in play; a given player knows that he has the winning hand>.

Obviously a poker game has quite different dynamics than RCP. However, we can impose RCP like rules on a poker game and hence assure private communication. The reason why private communication would be appropriate is that the table can be viewed as the $N+1^{st}$ player who cooperates with every agent-player in order to guess the cards of the other agent-players. Actually, as poker rules are concerned, we do not even need to bother with ordering the preferences of agents-players on all possible combinations of cards. It is enough to order all possible winning combinations of cards, i.e. cards stronger than what the possible hand of the agent-player. One additional feature of poker is that the old cards are not reshuffled into the deck. Therefore the amount of relevant cards can be lower than 52. Surely also other scenarios can be made. These are, however, already instances of this problem.

We are able to formalize a poker game based on RCP's parameters but that does not allow us to use the 'good announcement' criteria from RCP in this altered environment. This is because one of the basic mechanisms hidden behind RCP, as we can see also in [3], is that Crow has the least information from the three players.

What we can do, however, is to model the epistemic state of the player. Our work is based on dynamic epistemic logics, hence every agent has a set of possible states represented by the possible stronger deals of cards. An agent obviously knows only his own cards and the cards present on the table. The usual way how a player thinks can be modelled by making a structure of relations between winning card combinations. In this

structure the less mathematically probable combinations will be taken as less plausible. The agent thereafter evaluates according to the signals from other agents what card deal she has. These signals can be captured via their betting behaviour or in a more complicated scenario by a set of possible performatives accompanying their betting behaviour. All the available signals need to be evaluated by the agent in a similar way as public announcements are evaluated in RCP in order to determine her actions. As poker presents a turn-based game, the order in which agents proceed is given. Therefore it is also always clear what signals ought to be taken into consideration.

A seeming drawback of the connection between poker and RCP is the possible use of contrafactual signals from the players as they try to bluff. The original framework is built upon the assumption that agents announce only true announcements.

These ideas are implemented in a simple NetLogo model [4] using a BDI framework [5]. The agents are dealt a random set of cards, evaluate their options, and based on their knowledge do their bets. In our example performatives aren't used yet. To evaluate the plausibility of a hand the agents compare their threshold to a product of the probability of a given stronger hand and to the betting behaviour of the other agents (if already available) and their possible knowledge. The agents in our examples compared the product of the inverse of the probability of an outcome and truth value based on the raising of the bet by others with their threshold. This was only a simple threshold function that was meant to capture some property distinct from the cards themselves and it certainly could be replaced by a more elaborate function. The result of single agents is then added and compared with the studied agent's threshold and if lower or equal, the agent chooses to raise the bet also. If the agent lacks knowledge about the betting behaviour of other agents, he assumed that the other agents would raise their bet. As one can see, our simple example did not account for agents that would leave the game and focused only on the last step of the game. We show a basic example to demonstrate these points.

3.1. Example

Let us have a small poker game. We describe the situation by mentioning only those parameters that have changed and using abbreviations for poker cards: < {Anne, Bill, Crow, table}; table cooperates, other relations are antagonistic; 2|2|2|5; poker card pack; D10, D9 | S9, HA | CA, D6 | D7, S8, SA, H9, C9; … >.

The players have the following strongest hands at this moment – Anne: Three of a Kind: D9, H9, C9, D10, SA; Bill: Full House S9, H9, C9, HA, SA; Crow: Two Pair CA, SA, H9, C9, S8. Hence the winner would be Bill. We focus now on Bill. The other players are still in play after the river; therefore they supposedly have some viable card combination that seems worth staying in game. As we told before Bill has to worry only about stronger (or equal) hands of cards than his hand. Stronger would be a Straight Flush or a Four of a Kind. But as Bill knows the table's cards (those are common knowledge), he sees that a Four of a Kind is not possible as he holds one of the nines and a Straight Flush is not possible because there are neither enough cards of the same suit nor are the ranks of the cards suited for a Straight. There still can be another Full House as strong as Bill's (for ex.: H9, C9, D9, SA, DA). The probability of being there at least one such hand is according to Bill's knowledge 0.2%. Let Anne raise and Crow not. Hence the values according to our function would be in Anne's case 5 and in Crow's case 0. If the threshold for Bill is low, for example 4, then he would suppose that Anne has a winning hand. However, Bill would be very gullible or too careful in that case. A more reasonable threshold according to our trials is at least 20. If Crow would also rise, Bill with his threshold of 20 would still raise the bet.

3.2. No more (card) games

We only shifted our attention from one card problem to another and suddenly there is a completely different perspective. Although a poker game application uses different principles and introduces probability as an important part of reasoning, it can still be described using only the framework and ideas given by RCP. Although different approaches can be used in the case of poker games to simulate the behaviour of players (e.g. Bayesian networks, game theory approaches), an approach based on the generalization of RCP allows us to work with the epistemic states of agents and gives us the possibility to abstract from cards and move to chunks of information. We saw this partially in the provided example as information different from the cards

themselves was also provided, namely the betting behaviour of the other agents. Poker games, with their use of bluff, serve as a good proving ground to test the agent's capability to deal with contrafactual and unreliable information. And they present an environment complex enough to work as a good first step in the direction of real-life communication while they still maintain some level boundaries given by exact rules.

Our main aim would be to work in the context of a social network and automatize the process of information acquisition and evaluation. The user Anne wonders who knows a certain piece of information marked and who doesn't know. She then can attempt to share her knowledge with Bill or she can try to find out what Crow knows based on its statements. If we would create a protocol for good announcements based on the generalized RCP and its application in poker games, this protocol could allow messages that can be spread publicly without the risk of losing the transmitted information to some eavesdropper or a man-in-the-middle. At the same time, these ideas could serve as a basis for a bot capable of not only collecting but also synthesizing information.

4. Conclusions

We saw how generalization of RCP can present new options of interaction evaluation and that it might one day be used in the construction of dynamically changing protocols for public private communication. We stayed in this article only in card games, but we have shown how these games can serve as an example for the evaluation and testing of communication protocols and can add interesting results. It would be suitable to have a strong logical tool to be able to capture all the statements and their relations. For example we would like to capture uncertainty, false signals, and trust between players. One could capture some properties also by introducing performatives that would enrich the vocabulary of the agent-players with gestures that could be interpreted by the other players. Although the logic used by van Ditmarsch is able to capture problems directly related to RCP, it is not enough to describe the possibilities present in real communication. Nonetheless, RCP presents an option how to possibly approach the construction of protocols that allow public communication while maintaining the privacy of the transferred messages content.

5. Acknowledgements

I would like to thank my supervisor prof. Vladimír Mařík from the Czech Technical University in Prague. Gratitude also goes to the 'Prague dynamic group' of O. Majer and M. Peliš at the Institute of philosophy of the Czech academy of sciences.

6. References

[1] M. Jakob, Z. Moler, M. Pěchouček, and R. Vaculín. Content-Based Privacy Management on the Social Web. In: *Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2011 IEEE/WIC/ACM International Conference on, vol. 3, pp. 277-280, 2011.

[2] H. van Ditmarsch. The Russian cards problem: a case study in cryptography with public announcements. University of Otago, Otago, Technical OUCS-2002-08, Oct. 2002.

[3] H. van Ditmarsch, W. Van Der Hoek, R. Van Der Meyden, and J. Ruan. Model checking Russian cards. In: *Electronic Notes in Theoretical Computer Science*, vol. 149, no. 2, pp. 105-123, Elsevier, 2006.

[4] U. Wilensky. NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University. Evanston, IL. 1999.

[5] I. Sakellariou, P. Kefalas, I. Stamatopoulou. Enhancing NetLogo to simulate BDI communicating agents, In: *Artificial Intelligence: Theories, Models and Applications*, pp. 263-275, Springer, 2008.