UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

Minimal information exchange in Russian Cards problems

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRA EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

PRESENTA:

ZOE LEYVA ACOSTA

Director de tesis

Dr. Sergio Rajsbaum
IMATE-UNAM

Ciudad Universitaria, CD. MX., Octubre de 2021

Abstract

We consider minimal information exchange in the Russian Cards problem scenario. Such scenario is usually considered as a promising model in studies about unconditionally secure protocols for general purposes, including the implementation of various cryptographic primitives.

Roughly, the problem scenario consists of two card players, Alice and Bob, trying to communicate to each other the cards they hold, through public announcements. The security requirement states that these announcements must not allow a third card player, Cath, to know who (Alice or Bob) is holding any of the cards that she does not have. The deck of cards is supposed to be known in advance and fully distributed among the three players so that all three know how many cards each one is holding. The communication protocol is also assumed to be common knowledge among the players, so that the only private information each player has is his own hand of cards.

In most related works, only informative announcement protocols are used for solving the problem. Then, such solutions consist of two steps or announcements, one from Alice and the other from Bob. In this work however, we mostly consider minimally informative and secure announcement protocols. We discuss possible advantages of using these, compared to their informative counterparts, in terms of communication complexity and the possibilities of them being used in scenarios where it is known that no simultaneously secure and informative protocols exist. Additionally, we are interested in using this type of announcement protocols for designing communication strategies with at least two steps, which allow the exchange of information between two agents in an unconditionally secure manner.

Agradecimientos

A toda mi familia, en especial a mi padre, Luis Eduardo, por su guía y constante apoyo; a mi madre, Zoe Acosta, cuyo recuerdo y enseñanzas son siempre una inspiración para mí; a mis abuelos, Zoe y Pepe y a mi hermano, William, quienes son siempre fuente de motivación para mi.

A Eduardo Pascual, por haber sido el mejor compañero y por su meritoria colaboración en todos los aspectos del desarrollo del presente trabajo.

A mi tutor, Sergio Rajsbaum, por su asesoría y orientación constante.

Al Posgrado en Ciencia e Ingeniería de la Computación de la UNAM y a todos mis profesores por compartir conmigo sus valiosos conocimientos.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) por el patrocinio durante mis estudios de maestría y al Programa de Apoyo a Proyectos de Investigación e Innovación Tecnológica (PAPIIT) de la UNAM[1].

[1] Investigación realizada gracias al Programa de Apoyo a Proyectos de Investigación e Innovación Tecnológica (PAPIIT) de la UNAM, IN106520. Agradezco a la DGAPA-UNAM la beca recibida.

Contents

Chapter 1

Introduction

Security is an usual and important requirement for information transmission protocols. Two agents A and B should be able to communicate with each other without an eavesdropper C being capable of learning secret information from the messages. A conventional approach for achieving this would be public-key cryptography. In this approach, information is safeguarded relying on the computational intractability of cryptanalysis for decryption of the messages. In other words, this approach works under the assumption that the agents have limited computational capabilities and therefore provides what is known as *conditional security*. On the other hand, another approach would be to get rid of this assumption and rather rely on what the agents *know* or not, i.e. the information available for each party. As opposite to the former, this *knowledge-based protocol* approach is information-theoretic secure, i.e. provides *unconditional security*.

A promising approach in studies about such unconditionally secure protocols appears to be modeling agents as card players [9, 10, 11, 12] and, in particular, using a scenario and constraints inspired by the *Russian Cards* problem [6]. In such scenario the cards are viewed as representing correlated input information for the participants.

The present work has been developed in collaboration with Eduardo Pascual Aseff. Pascual's work is focused on informative and secure protocols for a more general Russian Cards scenario, where there are $\mathbf{r}$ cards that are not dealt to anyone. Our discussions on the problem have been productive and helped us improving our results.

1.1 The Russian Cards problem

The *Generalized Russian Cards* problem scenario is usually described as follows: three players A, B and C, respectively named Alice, Bob and Cath, draw cards from a deck D of n cards labeled from 0 to $n-1$. A gets $\mathbf{a}$ cards, B gets $\mathbf{b}$ and C gets $\mathbf{c}$, as specified by a *signature* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$[1]. Then, the goal is for A and B to inform each other about which cards they hold while ensuring that C cannot know who holds any particular card (except for the ones she owns).

A particular instance of this problem can be described by the signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a}+\mathbf{b}+\mathbf{c}$. The $(3, 3, 1)$ instance of the generalized problem is regarded as the *Russian Cards* problem due to [6] and was first presented at the Moscow 2000 Mathematical Olympiad.

It is clear that the basic problem underling the situation described above is to design a *protocol* for Alice and Bob. Such protocol should be *informative* for each other and *safe* against Cath. The first condition, regards the first goal for the problem above, which is that Bob should learn Alice's hand from her announcement (and conversely, Alice should learn Bob's), in which case we also say this announcement is informative. On the other hand, the second condition, *safety*, deals with the goal of Cath not being able to infer a single card from Alice's hand neither Bob's, i.e. their announcements should be safe. The previous formulation of the safety requirement is also called *weak-1-security* [20], but stronger formulations have also been considered.

It is well known that any *announcement* from a player is equivalent to announcing that he holds one of the hands from a specific set of possible or *alternative* hands. Such set is also regarded as an *announcement* [6]. As the

[1]Recently, the case where $\mathbf{r}$ cards are not dealt, i.e. $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, was also considered in [18]

announcements are supposed to be truthful, the actual hand that the player holds must be contained in the set of alternative hands representing the announcement. This fact allows the study of the problem from a combinatorial perspective.

Moreover, when only informative announcements are considered, it is clear that the problem requirements are met with only two announcements (one from Alice and one from Bob), therefore *two-steps* protocols are sufficient for solving the problem when both announcements are informative. Additionally, in such cases, the second announcement can always be informative and safe. Given that Bob is informed about Alice's hand he can always announce Cath's hand, which is informative for Alice while being safe from Cath, as it doesn't give her any new information. Hence, in such cases, designing a communication strategy for solving the problem reduces to designing an announcement protocol for Alice's announcement. However, this is not the case when not fully informative announcements are considered. In such cases, the second announcement is not trivial, furthermore, solving the problem according to the classic requirements, demands communication strategies with more than two steps.

As it was early noted, a couple of assumptions are necessary to make the problem precise and therefore, formally distinguish between 'good' and 'bad' solutions [16]. First, all circumstances regarding the scenario are assumed to be public knowledge, except for which cards each player holds. This means it is assumed to be *common knowledge* among the three players, how many cards each player hold, the content of the announcements they make, as well as the communication *protocol* they use. Therefore, the only private information is what they wish to communicate. As is standard in modern cryptography, this assumption embraces *Kerckhoffs' principle*, i.e. rejects *security through obscurity.* The second assumption is that the player's computational capabilities are unlimited. As we previously remarked, this assumption, unlike the first, is not common in cryptography but it is in information theory approaches. This means, a 'good' solution can not be vulnerable to cryptanalisys. Finally, we assume that communication is completely reliable i.e., agents communicate via an *error-free* channel. When we take these assumptions into consideration, finding solutions becomes a challenging problem.

1.2 Zero-error source coding with side information

Now that we have presented the problem we are mainly concerned with, we want to discuss the relation between this and other problem from information theory, namely *zero-error source coding with side information* [21, 17]. Roughly, the *single instance*[2] scenario is the following: an informant Alice has some input information $a \in \Omega_A$ while the recipient Bob has some correlated information $b \in \Omega_B$. All possible input pairs (a, b) are defined by the elements in the *support set* S, which both Alice and Bob know. Then, the goal is for Alice to communicate a to Bob with zero probability of error and using the minimum amount of bits.

Its clear from the problem statement that *informativity* is a common requirement for solutions to this problem as well as for the Russian Cards case. On the other hand, both problem present additional requirements, namely *security*, for the Russian Cards case and *optimality* for zero-error source coding.

Although these last requirements are clearly different, there's no need for them to be mutually exclusive. In fact, it is reasonable to think that aiming for *optimality* for the transmission protocol i.e., a smaller set of possible messages, it may be the case that each individual message carries information about a bigger set of possible values for a and therefore more ambiguity, making it perhaps more *secure* against an eavesdropper.

The previous discussion and the similar structure of both problems makes it natural to think about the Russian Cards problem as a special kind of a zero-error source coding problem. This relation between both problems was also previously noted in [14]. Therefore, using some of the tools from the

[2]In general, the problem of *one-way communication* can also be considered in the *multiple instances* scenario i.e., with multiple communication rounds.

zero-error source coding literature appears to be a promising approach for the analysis of the Russian Cards problem.

1.3 Motivation

Recently, a weaker alternative for the *informative* requirement, called *minimally informative* was considered in [18]. For this variant of the problem, B is not required to learn A's entire hand, instead we need B to learn something about it. We regard this as the problem of minimal information transmission in the Russian Cards scenario.

In the present work, we are mostly interested in studying secure minimal information exchange in the Russian Cards scenario. Thus, while [18] only focuses on the problem of information transmission, i.e., only one-way communication; here, we also consider protocols for information exchange, i.e., we study the communication in both ways. In particular, as we are mostly concerned with the problem of secure minimal information exchange, we study protocols in which both, Alice and Bob communicate with each other with the goal of learning something about each other's hands, while preventing Cath from learning a single card of theirs.

The terminology we use is mostly that from [18]. Thus, this work extends the results presented in [18], specifically regarding the problem of minimal information transmission. Additionally, our approach for formalizing the problem is motivated by the links with the problem of zero-error source coding with side information, previously noted in [14].

In particular, we are interested in answering how much such protocols can help in reducing communication complexity with respect to (fully) informative ones.

Also, it is well known that no (fully) informative and safe announcement protocols exists for various problem instances, for example, when Alice or Bob have less information than Cath, i.e. when they hold less cards. It would be interesting to answer whether this weaker informative requirement could allow some information exchange between Alice and Bob in a safe manner even in such scenarios.

1.4 Contribution

In the present work, we provide a formal presentation of the problem of secure minimal information exchange in the Russian Cards scenario. Our main results, that we describe in this section, will be presented in the 23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'21)[15].

We present a two-message minimally informative solution in which Alice and Bob use the announcement protocol χ_2 proposed in [18], announcing both the sum of their cards modulo 2. We show this is a proper minimally informative solution to the problem whenever $1 \leq \mathbf{c} \leq \lfloor n/2 \rfloor - 2$, $2 \leq \mathbf{a}, \mathbf{b} < \lfloor n/2 \rfloor$. This is, exchanging only one bit, Alice and Bob can learn some information about each other's hand in a safe manner in several Russian Cards scenarios. However, such scenarios do not include the classic instance of the generalized problem, i.e., $(3, 3, 1)$.

We present another two-message minimally informative announcement protocol construction that could be used for the classic Russian Cards problem, unlike the first construction proposed. This construction is based on Singer sets and yields four different deterministic and safe protocols for Alice's announcement. We also verified the minimally informative requirement for this construction using the proof assistant system Coq. With such protocol, A can inform B one of her cards, privately.

Furthermore, we show that when $\mathbf{c} = 1$, any two-message minimally informative announcement protocol is also safe. This means that the announcement protocols resulting from the previously mentioned construction are also safe for $(3, 3, 1)$.

Finally, we show how these protocols can be used in a two-message minimally informative solution for the classic Russian Cards problem, allowing Alice and Bob to exchange information in a safe manner. Thus, using this protocol Alice and Bob can learn at least one card from each others hand, without Cath learning any, and this can be achieved by exchanging only one bit.

1.5 Related work

The Russian Cards problem, its generalizations and many variations have been subject of quite a few amount of studies since its appearance at the Moscow 2000 Mathematical Olympiad. However, its origins may be traced long back [13, 9, 10, 11, 12]. A well known solution for the classic $(3, 3, 1)$ problem uses modular arithmetic, where A announces the sum of her cards modulo 7, and then B announces C's card [16].

A seminal paper on this matter [6] models the classic Russian Cards problem via epistemic logic and shows that no matter how complex the construction of a player's announcement might be, it is always equivalent to the announcement of a set of possible hands for that player. In lights of this result, the author identifies 102 *direct exchange* solutions, i.e. two-steps solutions, for the deal $(\{123\}, \{345\}, \{6\})$ using combinatorial reasoning. Moreover, some important properties about informative and safe announcements are presented. The problem, as well as its generalized form, has received a fair amount of attention since then.

In [2] the authors focus on two-step solutions for various instances of the generalized problem. The authors state the problem requirements via some epistemic axioms and then reformulate these conditions in equivalent, but purely combinatorial terms. It is shown that there is no two-step solution when $\mathbf{c} \geq \mathbf{a} - 1$. Also, some bounds on the sizes of good announcements are given. Proposed solutions cover problem instances such as ($\mathbf{a}$, 2, 1), provided $a \equiv 0, 4 \mod 6$, and more interestingly, cases where $\mathbf{b} = O(\mathbf{a}^2)$. To this end, the authors propose constructions based in Singer difference sets and block designs, in particular, Steiner triple systems.

Unlike the previous works, which focus on the classic security condition, also known as *weak 1-security*, in [3] the authors strengthened the security requirement. In order to not give C probabilistic advantage in guessing the ownership of any card, this condition, also known as *perfect 1-security*, requires that all cards not held by C appear the same number of times in the hands C considers possible for A and also in the hands C considers B could hold. A good announcement construction satisfying this requirement is proposed using binary designs for parameters $(2^{k-1}, 2^{k-1}-1, 1)$, where $k \geq 3$.

A two-step protocol for $(\mathbf{a}, \mathbf{a}, 1)$ with $\mathbf{a} > 2$, where A announces the sum of her cards modulo $n = 2\mathbf{a} + 1$ is proposed in [1]. The paper also discus *state safe*, as a relaxed variant of the classic *card safe* security condition, in which Cath is only required to not learn the full hand of the other players. More recently, in [4], this *modulo-sum* protocol was generalized to provide a two-step solution for $(\mathbf{a}, \mathbf{b}, 1)$ with $\mathbf{a}, \mathbf{b} > 2$.

Although the solutions discussed above consist of two-step protocols, in [7] it is proved that no such solution exists for (4, 4, 2), therefore the authors proposed a three-step protocol for this problem instance. The first known solution for $\mathbf{c} > \mathbf{a}$ is reported in [5] via a four-step protocol based on finite vector spaces.

Multi-player variations of the problem, i.e. involving more than three players, have also been considered [8].

In [20] the authors provide a formal definition of what they call *weak k-security* and *perfect k-security*. Most literature focus on what they refer to as *weak 1-security*, which is the original security condition. They also distinguish between *deterministic* announcement strategies, in which A's hand uniquely determines her message, and non-deterministic ones. Additionally, they give a characterization of informative strategies having optimal communication complexity, namely the set of announcements must be equivalent to a large set of $t-(n, \mathbf{a}, 1)$-designs, where $t = \mathbf{a} - \mathbf{c}$. They show that for a perfectly $(d-1)$-secure strategy for $(a, b, a-d)$, where $b \geq d-1$, $\mathbf{a} = d+1$ and hence $c = 1$. Moreover, the authors give a characterization of informative and perfectly $(d-1)$-secure strategies for $(d+1, b, 1)$, with $b \geq d-1$, involving $d-(n, d+1, 1)$-designs.

Also, in recent years the links between the problem and *zero-error source coding* were exposed in [14].

Building on the results from [18]. The results of this work are part of the research project about Russian Cards problems initiated by Rajsbaum in [18]. We stress that the present work takes mostly from [18] the basic framework and terminology; and also builds on some of the results from the cited paper. Here, we summarize the relation between both works.

In [18] the author focuses on the problem of information transmission, i.e., only one-way communication. Here, we also consider protocols for information exchange, i.e., we study the communication in both ways. Since we are mostly concerned with the problem of secure minimal information exchange, we present some preliminary results from [18] regarding the problem of minimal information transmission; and we build on such results for presenting our contributions. In that sense, our work is an extension of [18].

In this work, we present the notion of *minimally informative protocol*, analogous to that presented in [18, Definition 1]; however, our formulation is not limited to the Russian Cards scenario, instead we use the more general framework of source coding with side information, for Definition 1. Moreover, the preliminary results presented in Chapter 3 are mostly from [18]. Additionally, we present the results from [18, Section 4.1] in Section 5.1, Lemmas 3 and 4. Then, we build on these results for the proof of Theorem 5.

Moreover, in [18, Section 4.1] the author presented a minimally informative and safe protocol for $(3, 3, 1)$, using two messages, which allows Alice to use a single bit for informing one of her cards to Bob. This, was one of the $2 \times (76505394)$ two-message minimally informative and safe protocols for $(3, 3, 1)$ that we found using a computer program. We also present in this work one of these two-message protocols in Section 3.5.

1.6 Organization

The present work consists of six chapters. In Chapter 2 we present the problem of (one-way) information transmission using a similar framework to the one commonly used in studies about *zero-error source coding with side information* [21, 17]. In doing so, we present the notion of *informative protocol.*

Additionally, we also present the notion of *minimally informative protocol*, which therefore regards the problem of *minimal information transmission*. Such notion was previously presented in [18], although the author formulates the notion for the particular case of the Russian Cards scenario.

In Chapter 3 we show how the previous framework and notions can be used for formalizing the problem of information transmission in the Russian Cards scenario, as it was previously noted in [14]. Moreover, we present the notion of *safe* protocol for information transmission in this scenario, which therefore regards the problem of *secure information transmission*. Additionally, we present some preliminary known results, which we rephrase and prove using our framework and terminology.

In Chapter 4 we introduce the problem of secure information exchange for Russian Cards problems and present the notions of *one-step* and *two-step* protocols. Thus, in this chapter, we are concerned with the communication in both ways, rather than only with one-way communication.

In Chapter 5 we present some minimally informative solutions for several instances of the Russian Cards problem. Additionally we provide a novel result regarding safety in two-message minimally informative protocols when $\mathbf{c} = 1$. These are the main contributions of the present work, as discussed in Section 1.4.

Finally, the conclusions can be found in Chapter 6.

Chapter 2

One-way information transmission protocols

We already remarked the similarities between the Russian Cards problem and zero-error source coding with side information. Moreover, we exposed the reasons why we think the tools proved successful for the last problem may be suitable for the Russian Cards problem as well.

The *zero-error source coding with side information* problem, as we previously describe it, is determined by the *support set* S of all pairs (a, b) of possible input assignments for the informant A and the recipient B. Associated with S is a *characteristic graph* $\mathcal{G}_B$, also called *confusability* or *indistinguishability graph*. Hence, we can also associate with such problem the *characteristic graph* $\mathcal{G}_B$ associated to S.

We formally introduce these concepts in Section 2.1 and define in such terms the notion of *protocol*. In Section 2.2 we formalize what it means for a protocol to be *informative*. We also define in Section 2.2 the notion of *minimally informative* protocol, which was previously presented in [18]. In this case, the goal for Bob is to learn *something* about Alice's input, after her announcement, instead of her whole hand.

2.1 Characteristic graphs and protocols

Let S be a *support set*, defined over a discrete product set $\Omega_A \times \Omega_B$, i.e., $S \subseteq \Omega_A \times \Omega_B$, we define the *associated characteristic graph* $\mathcal{G}_B$ as follows. The vertex set of $\mathcal{G}_B$ is Ω_A and there is an edge (a, a') if and only if there is $b \in \Omega_B$ such that $(a, b), (a', b) \in S$.

We can also call $\mathcal{G}_B$ a *indistinguishability graph* because each edge (a, a') in $\mathcal{G}_B$ expresses the fact that when the recipient Bob has input b he can not distinguish between the informant Alice having input a or a', as he considers both values possible.

Then, for any edge (a, a') in $\mathcal{G}_B$ there is an input b for Bob, for which a and a' are indistinguishable, denoted by $a \overset{b}{\sim} a'$. For each $b \in \Omega_B$, this *indistinguishability* relation, $\overset{b}{\sim}$ is an equivalence relation, consisting of a single equivalence class, which we call the *indistinguishability class for b*. Therefore, for any $b \in \Omega_B$ we define its corresponding indistinguishability class to be the set denoted $K(\bar{b}) = \{a \mid (a, b) \in S\}$. Hence, for each $b \in \Omega_B$, the elements in $K(\bar{b})$ induce a clique in $\mathcal{G}_B$, overloading notation we also denote the clique itself by $K(\bar{b})$. Then, $K(\bar{b})$ is the set of all input values that Bob considers possible for Alice, given that his input is b.

Then, for a problem with *associated characteristic graph* $\mathcal{G}_B$, a *deterministic protocol* $P_A : \Omega_A \to \mathcal{M}$ for Alice's announcement is a vertex coloring function for $\mathcal{G}_B$, where $\mathcal{M}$ is the domain of possible messages that Alice may send. Thus, we say that P_A is an *m-message protocol* if $|\mathcal{M}| = m$.

Thus, when Alice has input $a \in \Omega_A$, $P_A(a) \in \mathcal{M}$ uniquely determines the message she send. Hence, for each $M \in \mathcal{M}$, $P_A^{-1}(M)$ denotes the set of vertices from $\mathcal{G}_B$ colored M.

Also, for any $b \in \Omega_B$ and any $M \in \mathcal{M}$, $\mathcal{P}(b, M) = \{a \mid a \in K(\bar{b}) \wedge a \in P_A^{-1}(M)\}$ denotes the set of inputs for A that B considers possible given that his input is b and A's announcement was M. We can also call this set the *indistinguishability class for b after M*.

In the following, the set of *compatible messages* with any $b \in \Omega_B$, is denoted $P_A(K(\bar{b})) = \{P_A(a) | a \in K(\bar{b})\}$. This is, the set of messages that B could possibly hear having input b.

2.2 Informative and minimally informative protocols

We can already formally define what it means for a protocol to be *informative* and also *minimally informative*. Recall that a vertex coloring of a graph is *proper* if each pair of adjacent vertices have different colors.

Definition 1 (Informative and minimally informative)**.** *Let $P_A : \Omega_A \to \mathcal{M}$ be a protocol for a problem with associated characteristic graph $\mathcal{G}_B$,*

- *P_A is* informative *if it is a proper vertex coloring of $\mathcal{G}_B$.*
- *P_A is* minimally informative *if for each $b \in \Omega_B$ such that $|K(\bar{b})| > 1$, there is some edge (a, a') in the clique $K(\bar{b})$ of $\mathcal{G}_B$, such that $P_A(a) \neq P_A(a')$.*

Notice that, according to the *informative* definition, P_A being informative is equivalent to $|\mathcal{P}(b, M)| \leq 1$, for all $b \in \Omega_B$ and for all $M \in \mathcal{M}$. This means that for any inputs assignment (a, b) for Alice and Bob, whenever Alice can announce M, i.e, if $M \in P_A(K(\bar{b}))$, Bob will know Alice's input is the only element a in $\mathcal{P}(b, M)$.

On the other hand, regarding the *minimally informative* definition, this is also equivalent to $\mathcal{P}(b, M) \subset K(\bar{b})$, for all $b \in \Omega_B$ and all compatible messages $M \in P_A(K(\bar{b}))$. Notice that $\mathcal{P}(b, M) \supset K(\bar{b})$ is impossible, by the definition of $\mathcal{P}(b, M)$ and if $\mathcal{P}(b, M) = K(\bar{b})$, for some $b \in \Omega_B$ and some $M \in P_A(K(\bar{b}))$, this would mean that if Bob has input b, the announcement M does not offer any new information to Bob. In other words, the least one can expect B to learn from an announcement is that A's input is in a proper subset of $K(\bar{b})$.

Also, it is clear that any informative protocol is also minimally informative. Moreover, if $\mathcal{G}_B$ has no edges no communication is needed for B to know A's input, since no matter what B's input is, he would only consider one possibility for A's input. Hence, in such case, any coloring function for $\mathcal{G}_B$ is an informative and therefore, also minimally informative protocol.

Chapter 3

Information transmission in Russian Cards problems

In this chapter, we formally present the problem of *secure information transmission* in the generalized Russian Cards problem scenario. Additionally, we present some known impossibility results regarding informative protocols, as well as a characterization for minimally informative protocols, previously shown in [18].

In Section 3.1 we introduce the problem and relate it to coloring functions of Johnson graphs.

In Section 3.2 we characterize the notions of *informative* and *minimally informative* announcement protocols for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$. The former notion corresponds to what we refer to as the problem of *full information transmission*; while the latter regards the problem of *minimal information transmission* in the Russian Cards scenario.

In Section 3.3 we define the notion of *secure* or *safe* announcement protocol. Hence, this notion regards what we refer to as the problem of *secure information transmission* in the Russian Cards scenario.

Some examples of announcement protocols for the Russian Cards problem, satisfying different requirements are presented in Section 3.5. We also discuss lower bounds on the number of messages for an informative Russian

Cards protocol in Section 3.4.

3.1 Representing Indistinguishability by Johnson graphs

Let $D = \{0, \ldots, n-1\}$, $n > 1$, denote the *deck* of n distinct *cards*. A subset a of D is a *hand*, $a \in \mathscr{P}(D)$. For a hand a, $\bar{a}$ denotes the set $D - a$, i.e., $\bar{a}$ is the complementary set of a with respect to D. If $|a| = m$, we may say that a is an m-set or m-hand. Thus, if $\mathscr{P}_m(D)$ stands for the set of all subsets of D of size m, $a \in \mathscr{P}_m(D)$.

A *deal* (a, b, c) consists of three disjoint hands, meaning that cards in a are dealt to A, cards in b to B, and cards in c to C. We say that the hand is the *input* of the agent. We call $\gamma = (\mathbf{a}, \mathbf{b}, \mathbf{c})$ the *signature* of the deal (a, b, c) if $|a| = \mathbf{a}$, $|b| = \mathbf{b}$ and $|c| = \mathbf{c}$. Hence, for the problem instance with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, the inputs of A, B and C, are the hands $a \in \mathscr{P}_{\mathbf{a}}(D)$, $b \in \mathscr{P}_{\mathbf{b}}(D)$ and $c \in \mathscr{P}_{\mathbf{c}}(D)$, respectively. As we previously remarked, it is assumed that A, B and C are aware of both, the deck and the signature. Also, while A and B get at least one card each, i.e. $\mathbf{a}, \mathbf{b} \geq 1$, C may get none, $\mathbf{c} \geq 0$ and $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$.

In the language of e.g. [4, 5, 7], A's announcement protocol should be "informative" for B and "safe" from the eavesdropper C. Thus, we can model the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ as two one-way information transmission problems, each with almost opposite requirements. First, is the communication between the informant Alice and the recipient Bob, which should be informative. Second, is the communication between Alice and the eavesdropper Cath (because Alice's announcement is public), which must not be informative, and additionally, must not allow Cath to learn a single card from Alice's hand. Then, Alice needs an informative announcement protocol for the first problem, such that it is also safe for the second problem. We already defined what it means for a protocol to be informative and, in the following sections, we will also define the notion of *safety* that the Russian Cards problem requires.

For the communication problem between Alice and Bob, we have the support set $S_B = \{(a,b)|(a,b) \in \mathscr{P}_{\mathbf{a}}(D) \times \mathscr{P}_{\mathbf{b}}(D) \wedge a \subseteq \bar{b}\}$. On the other hand, for modeling the communication between Alice and Cath, the support set is $S_C = \{(a,c)|(a,c) \in \mathscr{P}_{\mathbf{a}}(D) \times \mathscr{P}_{\mathbf{c}}(D) \wedge a \subseteq \bar{c}\}$.

With the support sets for each problem, we can now denote the *associated characteristic graphs* for S_B and S_C as $\mathcal{G}_B$ and $\mathcal{G}_C$, respectively. Thus, we say that $\mathcal{G}_B$ and $\mathcal{G}_C$ are the *indistinguishability graphs* for B and C, respectively, induced by the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

Notice that $(a, a') \in E(\mathcal{G}_B)$ iff $\exists b \in \mathscr{P}_{\mathbf{b}}(D)$ such that $a, a' \subseteq \bar{b}$. Such b exists iff $\mathbf{b} \leq |D - (a \cup a')|$, which is equivalent to $\mathbf{b} \leq (\mathbf{a}+\mathbf{b}+\mathbf{c}) - |a \cup a'|$. Then, since $|a \cup a'| = 2\mathbf{a} - |a \cap a'|$, it follows that $(a, a') \in E(\mathcal{G}_B)$ iff $\mathbf{b} \leq \mathbf{b} + \mathbf{c} - \mathbf{a} + |a \cap a'|$, and this is equivalent to $\mathbf{a} - \mathbf{c} \leq |a \cap a'|$. This is, $(a, a') \in E(\mathcal{G}_B)$ iff $\mathbf{a} - \mathbf{c} \leq |a \cap a'|$. By a similar argument we can show that $(a, a') \in E(\mathcal{G}_C)$ iff $\mathbf{a} - \mathbf{b} \leq |a \cap a'|$.

.

Definition 2 (Distance d Johnson graph [18])**.** *For a set of n elements, the graph $J^d(n,m)$, $0 \leq d \leq m$, has as vertices all m-subsets. Two distinct vertices a, a' are adjacent whenever $m - d \leq |a \cap a'|$. When $d = 1$, we have a* Johnson graph, *denoted $J(n,m)$.*

Thus, from our previous observations, it is clear that the indistinguishability graph for B in the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ is the graph $J^{\mathbf{c}}(n, \mathbf{a})$, i.e. $\mathcal{G}_B = J^{\mathbf{c}}(n, \mathbf{a})$. In particular, $\mathcal{G}_B$ is a Johnson graph, $J(n, \mathbf{a})$, exactly when $\mathbf{c} = 1$. Similarly, the indistinguishability graph for C, $\mathcal{G}_C$, is equal to $J^{\mathbf{b}}(n, \mathbf{a})$.

As we previously remarked, for any $b \in \mathscr{P}_{\mathbf{b}}(D)$, the elements in $K(\bar{b})$ induce a clique in $\mathcal{G}_B$, and therefore in $J^{\mathbf{c}}(n, \mathbf{a})$. Thus, $K(\bar{b})$ denotes the set of hands that B considers possible for A, provided that he holds the hand b. Similarly, for any $c \in \mathscr{P}_{\mathbf{c}}(D)$, the elements in $K(\bar{c})$ induce a clique in $J^{\mathbf{b}}(n, \mathbf{a})$ representing the hands that C considers possible for A, given that she holds the hand c.

Notice that if $\mathbf{c} = 0$ and therefore $n = \mathbf{a}+\mathbf{b}$, then B with input b considers only one possible input for A, namely, $\bar{b}$. In this case, $E(\mathcal{G}_B) = \emptyset$.

3.2 Informative and minimally informative announcements

Previously, we proved that the *indistinguishablility graphs* for B and C induced by the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, are $J^{\mathbf{c}}(n, \mathbf{a})$ and $J^{\mathbf{b}}(n, \mathbf{a})$, respectively. Hence, for the problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ consider an announcement protocol for A, $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}$. We take the view of P_A as a vertex coloring of the graphs $J^{\mathbf{c}}(n, \mathbf{a})$ and $J^{\mathbf{b}}(n, \mathbf{a})$. A color class, $P_A^{-1}(M)$, for any message M, is an *announcement*, therefore we can also describe an m-message announcement protocol as a set of m announcements or color classes, i.e, $\{P_A^{-1}(M) | M \in \mathcal{M}\}$.

The following characterization is a reformulation of Definition 1 and it is similar to that presented in [18].

Theorem 1 (Informative characterization for Russian Cards)**.** *Let* $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}$ *be an announcement protocol for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$*.*

- P_A *is* informative *if and only if* P_A *is a proper vertex coloring of* $J^{\mathbf{c}}(n, \mathbf{a})$*.*
- P_A *is* minimally informative *if and only if for each* $b \in \mathscr{P}_{\mathbf{b}}(D)$ *such that* $|K(\bar{b})| > 1$*, there is some edge* (a, a') *in the clique* $K(\bar{b})$ *of* $J^{\mathbf{c}}(n, \mathbf{a})$*, such that* $P_A(a) \neq P_A(a')$*.*

The following result was previously shown in [2]:

Theorem 2. *Let* $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}$ *be an announcement protocol for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$*, then the following conditions are equivalent.*

1. *P_A is informative.*
2. *For any $M \in \mathcal{M}$ and any pair of distinct $a, a' \in P_A^{-1}(M)$, $|a \cap a'| < \mathbf{a} - \mathbf{c}$.*

Proof. P_A is informative iff it is a proper vertex coloring of $J^{\mathbf{c}}(n, \mathbf{a})$. Then, for any $M \in \mathcal{M}$, $a, a' \in P_A^{-1}(M)$ iff (a, a') is not and edge in $J^{\mathbf{c}}(n, \mathbf{a})$. As (a, a') is not and edge in $J^{\mathbf{c}}(n, \mathbf{a})$ iff $|a \cap a'| < \mathbf{a} - \mathbf{c}$, the theorem follows. $\square$

It follows from Theorem 2 that $\mathbf{a} > \mathbf{c}$ is a necessary condition for the existence of an informative protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

Corollary 1. *There is no informative announcement protocol for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ *if* $\mathbf{c} \geq \mathbf{a}$.

The following result expresses the fact that when $\mathbf{c} \geq 1$, the minimally informative condition is equivalent to B learning a set s, $|s| = \mathbf{c}$ which contains at least one of A's cards, after any possible announcement from A. Recall that the elements in $\mathcal{P}(b, M)$ are all $a \in K(\bar{b})$ such that $P_A(a) = M$.

Theorem 3. *Let* $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}$ *be an announcement protocol for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ *with* $\mathbf{c} \geq 1$, *then the following conditions are equivalent.*

1. P_A *is minimally informative.*
2. *For any* $b \in \mathscr{P}_{\mathbf{b}}(D)$ *and any compatible message* $M \in P_A(K(\bar{b}))$, *there is a set* $s \subset \bar{b}$, $|s| = \mathbf{c}$, *such that for any* $a \in \mathcal{P}(b, M)$, $a \cap s \neq \emptyset$.

Proof. Suppose P_A is minimally informative, then for any $b \in \mathscr{P}_{\mathbf{b}}(D)$ and any compatible message $M \in P_A(K(\bar{b}))$, $\mathcal{P}(b, M) \subset K(\bar{b})$, i.e., $|\mathcal{P}(b, M)| < |K(\bar{b})|$. Then, let a be an element in $K(\bar{b}) - \mathcal{P}(b, M)$ and let s be $\bar{b} - a$, so that $|s| = \mathbf{c}$. Assume for contradiction that there is an element $a' \in \mathcal{P}(b, M)$ such that $a' \cap s = \emptyset$. Then, $|a \cup a'| > \mathbf{a}$. Hence, $|b \cup a \cup a' \cup s| > n$, which is a contradiction since b, a, a' and s are all subsets of a deck of n cards. It follows that, for any $a \in \mathcal{P}(b, M)$, $a \cap s \neq \emptyset$.

On the other hand, for the second condition to hold, the protocol needs to be minimally informative. Otherwise, suppose there is $b \in \mathscr{P}_{\mathbf{b}}(D)$ such that all elements in $K(\bar{b})$ are colored M, i.e. the protocol is not minimally informative. Then, assume for contradiction that there is a set s, $|s| = \mathbf{c}$, such that for any $a \in K(\bar{b})$ with $P_A(a) = M$, $a \cap s \neq \emptyset$. Notice that $\bar{b} - s \in K(\bar{b})$, and therefore $\bar{b} - s \in \mathcal{P}(b, M)$ (as $\mathcal{P}(b, M) = K(\bar{b})$ in a not minimally informative protocol). This means that there is an element $a \in K(\bar{b})$ with $P_A(a) = M$, namely $a = \bar{b} - s$, such that $a \cap s = \emptyset$, which is a contradiction. □

Notice that for the previous equivalence to hold we need $\mathbf{c} \geq 1$. As we previously remarked if $\mathbf{c} = 0$, no protocol or communication is needed for B to learn A's hand, so that any protocol for this case is minimally informative. However, a set s, $|s| = 0$ can not contain any of A's cards, which does not make sense.

When $\mathbf{c} = 1$ and considering a minimally informative protocol, a direct consequence of Theorem 3 is that B learns at least one of A's cards. This fact can be formally stated as in the following corollary.

Corollary 2. *Let $P_A : \mathscr{P}_\mathbf{a}(D) \to \mathcal{M}$ be an announcement protocol for $(\mathbf{a}, \mathbf{b}, 1)$, then for any $b \in \mathscr{P}_\mathbf{b}(D)$ and any compatible message $M \in P_A(K(\bar{b}))$, there is a card $x \in \bar{b}$, such that for any $a \in \mathcal{P}(b, M)$, $x \in a$.*

3.3 Safe announcements

The security requirement we discuss here is known as *weak 1-security* [20], but we often call it for short *safety*. As we have seen, informativity is a requirement for the communication between Alice and Bob and therefore we formalize it as a property of a coloring function (protocol) for the graph $\mathcal{G}_B$, i.e. $J^\mathbf{c}(n, \mathbf{a})$. On the other hand, safety means that Cath can not be able to infer any of Alice's or Bob's cards after hearing Alice's announcement. Hence, we can formally define what it is a safe announcement protocol in terms of the properties of coloring functions for $J^\mathbf{b}(n, \mathbf{a})$ (recall $\mathcal{G}_C = J^\mathbf{b}(n, \mathbf{a})$).

Definition 3 (Safety)**.** *Let $P_A : \mathscr{P}_\mathbf{a}(D) \to \mathcal{M}$ be an announcement protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, then P_A is safe if for any $c \in \mathscr{P}_\mathbf{c}(D)$, any $y \in \bar{c}$ and any $M \in P_A(K(\bar{c}))$, there is some edge (a, a') in the clique $K(\bar{c})$ of $J^\mathbf{b}(n, \mathbf{a})$ with $P_A(a) = P_A(a') = M$, such that $y \in a \triangle a'$.*

Recall that for any $c \in \mathscr{P}_\mathbf{c}(D)$, $K(\bar{c})$ is the initial indistinguishability class of c, while $\mathcal{P}(c, M)$ is its indistinguishability class after the announcement M. The intuition behind the above definition is the following. We need Cath to not be able to distinguish between Alice having or not any of the cards in $\bar{c}$. Hence, for any such card $y \in \bar{c}$ we need to avoid two things:

- y being in all hands from $\mathcal{P}(c, M)$[1] (in which case Cath would know Alice holds the card y)
- y being in none of the hands from $\mathcal{P}(c, M)$ (in which case Cath would know Bob holds the card y).

Then, we need that whenever Cath can hear the message M, i.e. for any $c \in \mathscr{P}_{\mathbf{c}}(D)$ and any $M \in P_A(K(\bar{c}))$, for any card she does not hold, $y \in \bar{c}$, there are two hands for Alice $a, a' \in \mathcal{P}(c, M)$ (indistinguishable after M for Cath holding c) such that $y \in a$ and $y \notin a'$.

Remark 1 (Safety)**.** *Some consequences of the safety definition:*

- *When $\mathbf{b} \leq \mathbf{c}$, $J^{\mathbf{b}}(n, \mathbf{a})$ is a subgraph of $J^{\mathbf{c}}(n, \mathbf{a})$ on the same set of vertices. Thus, since P_A being informative is equivalent to being a proper vertex coloring of $J^{\mathbf{c}}(n, \mathbf{a})$ and safety requires P_A not to be a proper vertex coloring of $J^{\mathbf{b}}(n, \mathbf{a})$, it follows that, an announcement protocol can be informative and safe only if $\mathbf{b} > \mathbf{c}$. In this case, while $K(\bar{c})$ induces a clique in $J^{\mathbf{b}}(n, \mathbf{a})$, it does not induce a clique in $J^{\mathbf{c}}(n, \mathbf{a})$.*
- *Joining color classes $P_A^{-1}(M) \cup P_A^{-1}(M')$ of a protocol preserves safety, but not necessarily informative properties.*

Remark 2 (The assumption $\mathbf{c} \geq 1$)**.** *When $\mathbf{c} = 0$ any announcement protocol is trivially informative, and hence minimally informative, as in fact no communication is needed for B to know A's hand. Also, in this case, the protocol that always sends the same message ($P_A^{-1}(M) = \mathscr{P}_{\mathbf{a}}(D)$, with $\mathcal{M} = \{M\}$) is both informative and safe. Therefore, the interesting cases are those in which $\mathbf{c} \geq 1$.*

Remark 3 (The assumption $\mathbf{a} \geq 2$)**.** *Moreover, if $\mathbf{a} = 1$, a safe protocol P_A must always send the same message M. Otherwise, if $P_A(\{y\}) \neq P_A(\{y'\})$ for $y, y' \in D$, then when C has a hand c, such that $y, y' \in \bar{c}$, and hears the message $P_A(\{y\})$ she knows that A does not have card y'. Thus, in such case, when $\mathbf{c} \geq 1$, a safe protocol P_A cannot be minimally informative,*

[1]Notice that it could be that there is a hand c for C, for which some message M is never sent by P_A.

and thus cannot be informative either. Although regarding the informative requirement, this is also a consequence of Corollary 1, we can not say the same about the minimally informative condition.

From the previous remarks it is clear that we should concentrate in the cases where $\mathbf{b}, \mathbf{c} \geq 1$ and $\mathbf{a} \geq 2$ even when considering only minimally informative and safe protocols for Russian Cards problems.

The following argument is similar to [2, Lemma 3].

Lemma 1. *Assume $\mathbf{c} \geq 1$ and let $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}$ be an informative and safe announcement protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, then for any $y \in D$ and any $M \in \mathcal{M}$, card y is contained in at least $\mathbf{c}+1$ $\mathbf{a}$-sets from the announcement $P_A^{-1}(M)$.*

Proof. Assume for contradiction, there is an arbitrary $y \in D$ and $M \in \mathcal{M}$, such that card y is included in at most $t \leq \mathbf{c}$, $\mathbf{a}$-sets, $\{a_1, a_2, ..., a_t\}$ from the announcement $P_A^{-1}(M)$, i.e. $\{a_1, a_2, ..., a_t\} \subset P_A^{-1}(M)$. Since P_A is informative, by Corollary 1, it holds that $\mathbf{a} \geq \mathbf{c}$. Hence, for each $i \in \{1, 2, ..., t\}$ there is another card $y_i \in D$, $y_i \neq y$ such that $y_i \in a_i$. Thus, consider a c-set c, such that $\{y_1, y_2, ..., y_t\} \subseteq c$ and $y \in \bar{c}$, which exists given that $\mathbf{a} \geq 2$. Also, as P_A is safe there is also an $\mathbf{a}$-set a_{t+1} in $P_A^{-1}(M)$ such that $y \notin a_{t+1}$. Notice that it is always possible for c to be in the complement of a_{t+1}. Otherwise, it would be that for some $i \in \{1, 2, ..., t\}$, all elements in a_i except for y are included in a_{t+1}, i.e. $|a_i \cap a_{t+1}| = \mathbf{a} - 1$. But, as $\mathbf{a} - 1 \geq \mathbf{a} - \mathbf{c}$, by Theorem 2, this is a contradiction with P_A being informative. Therefore, $M \in P_A(K(\bar{c}))$, then for and any a in the clique $K(\bar{c})$ such that $P_A(a) = M$, we have that $y \notin a$, which is a contradiction with P_A being a safe protocol. □

Corollary 3. *When $\mathbf{c} \geq 1$, there is no informative and safe announcement protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ if $\mathbf{c} \geq \mathbf{a} - 1$.*

Proof. In light of Corollary 1 there is no informative protocol when $\mathbf{c} \geq \mathbf{a}$, so we only need to consider an informative and safe protocol P_A for the case $\mathbf{c} = \mathbf{a} - 1$. In such case, by Theorem 2, for any $M \in \mathcal{M}$ and any two hands

$a, a' \in P_A^{-1}(M)$, we have that $|a \cap a'| = \emptyset$. Hence, any card $y \in D$ appears at most once in every announcement, which by Lemma 1, is a contradiction with P_A being informative and safe. □

By Remark 1, an announcement protocol can be simultaneously informative and safe only if $\mathbf{b} > \mathbf{c}$. Combining this fact with Corollary 3, we get the following:

Corollary 4. *When* $\mathbf{c} \geq 1$*, there is no informative and safe announcement protocol for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ *if* $\mathbf{c} \geq \mathbf{b}$ *or* $\mathbf{c} \geq \mathbf{a} - 1$*.*

3.4 Lower bounds on the number of messages for informative protocols

It is clear now that, for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, the smallest m such that a fully informative m-message protocol exists, is the chromatic number of the graph $J^{\mathbf{c}}(n, \mathbf{a})$, denoted $\chi(J^{\mathbf{c}}(n, \mathbf{a}))$. However, such protocol will not necessarily be a safe protocol. Hence, the minimum number of bits needed for Alice to communicate her full hand to Bob is $\log_2 \chi(J^{\mathbf{c}}(n, \mathbf{a}))$.

Even in the case of $\mathbf{c} = 1$, computing the chromatic number of $J^{\mathbf{c}}(n, \mathbf{a})$, namely a Johnson graph, is an important open question. Apart from some special cases, only the trivial lower bound implied by the size of the maximal cliques is known.

In general, as all elements in the clique $K(\bar{b})$ of $J^{\mathbf{c}}(n, \mathbf{a})$ must have different colors, it holds that for an m-message informative protocol for the signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, $m \geq |K(\bar{b})|$, i.e., $m \geq \binom{\mathbf{a}+\mathbf{c}}{\mathbf{a}}$.

A less trivial general lower bound for m in the case of informative protocols follows from the next result which was previously shown in [20]:

Lemma 2. *If there is an* m*-message informative announcement protocol for the signature* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$*, then* $m \geq \binom{n-\mathbf{a}+\mathbf{c}}{\mathbf{c}}$*.*

Proof. Consider any $x \in \mathscr{P}_{\mathbf{a}-\mathbf{c}}(D)$. Then, there are exactly $\binom{n-\mathbf{a}+\mathbf{c}}{\mathbf{c}}$ **a**-sets $a \subset D$, such that $x \subset a$. By Theorem 2 all such **a**-sets must have different colors according to any informative protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$. $\square$

For the classic Russian Cards problem with signature $(3, 3, 1)$, this last bound yields $m \geq 5$, while the former yields $m \geq 4$, so in this case, the last is a tighter bound.

Combining the previous observation we have:

$$\max\left\{\binom{\mathbf{a}+\mathbf{c}}{\mathbf{a}}, \binom{n-\mathbf{a}+\mathbf{c}}{\mathbf{c}}\right\} \leq \chi(J^{\mathbf{c}}(n, \mathbf{a}))$$

In particular, for $J(n, \mathbf{a})$, we have $\max\{\mathbf{a}+1, n-\mathbf{a}+1\} \leq \chi(J(n, \mathbf{a}))$. Also, it is known that $\chi(J(n, \mathbf{a})) \leq n$. Hence, when $\mathbf{c} = 1$, the number of bits necessary and sufficient for an informative protocol is $\Theta(\log n)$.

In the following, we may say that a coloring of $J^{\mathbf{c}}(n, \mathbf{a})$ is *safe* if such coloring is a safe announcement protocol for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, according to Definition 3. Additionally, $\chi^{sf}(J^{\mathbf{c}}(n, \mathbf{a}))$ denotes the cardinality of the smallest color set $\mathcal{M}$ for which the graph $J^{\mathbf{c}}(n, \mathbf{a})$ has a safe proper coloring. It follows that $\chi(J^{\mathbf{c}}(n, \mathbf{a})) \leq \chi^{sf}(J^{\mathbf{c}}(n, \mathbf{a}))$. In particular, it is known that $\chi(J(7, 3)) = \chi^{sf}(J(7, 3)) = 6$.

Similarly, in the following we may regard a minimally informative announcement protocol for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, as a minimally informative coloring of $J^{\mathbf{c}}(n, \mathbf{a})$. Moreover, $\chi_{min}(J^{\mathbf{c}}(n, \mathbf{a}))$ denotes the cardinality of the smallest color set $\mathcal{M}$ for which the graph has a minimal informative coloring, and if we require such coloring to be also safe, then it is denoted χ^{sf}_{min}. Thus, $\chi_{min} \leq \chi^{sf}_{min} \leq \chi^{sf}$. We will see that χ^{sf}_{min} can be much smaller than χ^{sf}. In an extreme case, for n even, we have that $\chi^{sf}_{min}(J(n, n/2)) = 2$ (Corollary 5), while $\chi^{sf}(J(n, n/2)) \geq \chi(J(n, n/2)) \geq n/2$.

3.5 Protocol examples

As we previously mentioned, the $(3, 3, 1)$ instance of the Russian Cards problem was presented at the Moscow 2000 Mathematical Olympiad. The solution considered by the organizers can be stated as follows [16]: *Both, Alice and Bob, announce the sum modulo 7 of their three cards.*.

Thus, in this solution, Alice and Bob use the same announcement protocol, that we denote as sum_7. This sum_7 protocol is indeed a safe and proper 7-coloring for $J(7,3)$ and can be defined in our terminology as a function $sum_7 : \mathscr{P}_3(D) \to \mathbb{Z}_7$ as follows:

$$sum_7(a) = (\sum_{x \in a} x) \mod 7.$$

or alternatively, as a collection of 7 announcements as follows:

$sum_7^{-1}(0) = \{016, 025, 034, 124, 356\}$
$sum_7^{-1}(1) = \{026, 035, 125, 134, 456\}$
$sum_7^{-1}(2) = \{036, 045, 126, 135, 234\}$
$sum_7^{-1}(3) = \{012, 046, 136, 145, 235\}$
$sum_7^{-1}(4) = \{013, 056, 146, 236, 245\}$
$sum_7^{-1}(5) = \{014, 023, 156, 246, 345\}$
$sum_7^{-1}(6) = \{015, 024, 123, 256, 346\}$

As we shall see in Section 4.1, although sum_7 satisfies Theorem 1 (Informativity) and Definition 3 (Safety), some extra considerations are needed for guarantying that this announcement protocol is safe for Bob's response to Alice, and therefore a solution to the Russian Cards problem.

Let's analyze what happens for the deal $(\{236\}, \{015\}, \{4\})$. In this case, A's announcement is $sum_7^{-1}(4)$, i.e., she sends the message $'4'$. Figure 3.1 shows that every hand in the announcement, except for $\{236\}$, collides with B's hand. This means, that B can learn A's hand after the announcement. From C's perspective, A could have one of the hands in $\{013, 056, 236\}$. Figure 3.2 shows that, C considers possible for A to hold or not the card number 0 and also card 3. The same happens for the other cards that C doesn't hold, which means that the announcement is safe.

For the same instance, $(3, 3, 1)$, the following protocol χ is minimally informative and safe, i.e., a safe minimally informative 2-coloring for $J(7, 3)$.

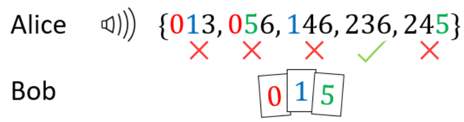

Figure 3.1: Perspective of B after A's announcement, for the deal $(\{236\}, \{015\}, \{4\})$

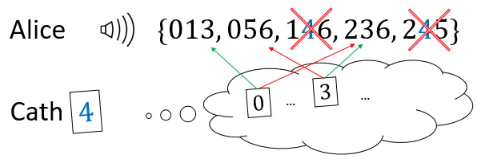

Figure 3.2: Perspective of C after A's announcement, for the deal $(\{236\}, \{015\}, \{4\})$

$$\begin{aligned}\chi^{-1}(0) = \{&012, 013, 014, 015, 016, 023, 024, 025, 036, 046, 126, 134, 135, 156,\\ &234, 245, 246, 256, 345\}\\ \chi^{-1}(1) = \{&026, 034, 035, 045, 056, 123, 124, 125, 136, 145, 146, 235, 236, 346,\\ &356, 456\}\end{aligned}$$

In Appendix A, Table A.1 we show for each 3-set b, how χ partitions the 3-sets in $K(\bar{b})$ into two color classes, so that the reader can check, that this is in fact a minimally informative coloring for $J(7, 3)$. Analogously, in Table A.2 we show how χ partitions $K(\bar{c})$ for each card c into two color classes. This way the reader can easily check that in all such partitions and for any card other than c, there is a hand which contains it and other that doesn't. Thus, χ is also a safe coloring for $J(7, 3)$.

Chapter 4

Information exchange in Russian Cards problems

So far we were mostly concerned with characterizing the informative and safety notions only for the announcement protocol of the agent starting the communication, i.e. for Alice. This is because, in some cases, the announcement protocol for Bob's response can be trivially informative and safe at the same time. As we already mentioned, such protocol could be the announcement of Cath's hand. Hence, in such cases, we can easily achieve (secure) *full information exchange* between Alice and Bob, once we have solved the problem of (secure) *full information transmission* in the Russian Cards scenario. However, such response strategy is only available for Bob when he is completely informed about Alice's hand, i.e. when Alice's announcement protocol is informative.

Thus, as we are mostly interested in studying minimally informative announcement protocols, we need to consider a different announcement protocol for Bob, that allows Alice to learn something about Bob's hand, while preventing Cath from learning the fate of any card she doesn't hold. Therefore, we need to consider the general problem of *information exchange* in the Russian Cards scenario. In this chapter, our main goal is to formally present this problem.

In Section 4.1 we introduce the problem of secure information exchange for Russian Cards problems and present the notions of *one-step* and *two-step* protocols.

In Section 4.2 we formally present the notions of *informative*, *minimally informative* and *safe* solutions for Russian Cards problems, from a combinatorial perspective.

In Section 4.3 we formally present the notion of *perfectly safe response protocol* as well as some well known examples.

4.1 One-step and two-step protocols

It may seem reasonable to think, that if A uses a safe announcement protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, and B answers to A according to a safe announcement protocol for parameters $(\mathbf{b}, \mathbf{a}, \mathbf{c})$, then, their cards could remain secret from C. However, this is not the case, as the following situation illustrates.

Consider the classic instance of the problem, $(3, 3, 1)$, and the deal $(\{245\}$, $\{136\}$, $\{0\})$. If both A and B use the announcement protocol from Appendix A, C learns who holds every card after Bob's announcement. What happens in this scenario is that A announces 0 and B announces 1. But then, there is only one hand in A's announcement that doesn't intersect with all hands in B's announcement. In other words, there is only a pair of compatible hands, i.e. disjoint hands, from both announcements. Thus, it is only possible for Alice and Bob to hold exactly one hand from their respective announcements, meaning that it is certain for Cath which cards they all hold.

Thus, although Bob is using a safe protocol for parameters $(3, 3, 1)$, according to Definition 3, his announcement reveals the ownership of all cards to Cath. Then, it is clear that, although Bob's protocol needs to be safe from Cath, this is not a sufficient condition for preventing Cath from learning the fate of the cards she doesn't hold. Intuitively, this happens because Definition 3, takes only into account the initial knowledge of C, while we need a formulation that also considers what C learned from A's announcement.

From the previous discussion, it is clear that we need a formal presentation of the problem of secure information exchange in Russian Cards problems, specially taking care of the formulation of the safety notion. Such presentation can also be found in [7] but from an epistemic logic perspective, while here we take a combinatorial approach.

In keeping with [7], there are two kinds of solutions to the Russian Cards problem consisting both of exactly one announcement from Alice and other from Bob. This two types of solutions are *one-step* protocols and *two-step* protocols. In *one-step* protocols, Bob's announcement does not depend on Alice's announcement. Hence it does not matter the order of the announcements as they even could be simultaneous. Conversely, in *two-step* protocols, Bob's announcement depends on hearing Alice's.

Then, we take the view of a *two-step* protocol ρ for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ as a pair $\rho = (P_A, P_B)$, where $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}_A$ is an announcement protocol for A, and $P_B : \mathscr{P}_{\mathbf{b}}(D) \times \mathcal{M}_A \to \mathcal{M}_B$ is the protocol for B's announcement, depending on his hand and also on Alice's previous message. Hence, $P_B^{-1}(M')$ denotes the set of pairs (b, M) such that $P_B(b, M) = M'$. Moreover, we say that ρ is an m-message protocol if $m = \max\{|\mathcal{M}_A|, |\mathcal{M}_B|\}$.

Additionally, we take the view of a *one-step* protocol $\rho = (P_A, P_B)$ for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ as a special kind of two-step protocol in which for any pair of messages $(M_1, M_2) \in \mathcal{M}_A$, $P_B(b, M_1) = P_B(b, M_2)$, for any $b \in \mathscr{P}_{\mathbf{b}}(D)$. Thus, in a one-step protocol, it does not matter which message B receives with input b, since he will always send the same message regardless. Therefore, in the following, when referring specifically to a one-step protocol $\rho = (P_A, P_B)$, we may take the view of P_B as function depending only on B's input, i.e., $P_B : \mathscr{P}_{\mathbf{b}}(D) \to \mathcal{M}_B$.

Then, the solution presented in Section 3.5, in which Alice and Bob use the same announcement protocol sum_7, is an example of a one-step protocol for the classic instance of the Russian Cards problem. Therefore, this protocol can be denoted by the pair (sum_7, sum_7). On the other hand, the solutions in which Bob announces Cath's hand after an informative and safe announcement from Alice, are examples of two-step protocols and not one-step protocols.

4.2 Safe information exchange protocols

Consider a two-step protocol (P_A, P_B), where $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}_A$ and $P_B : \mathscr{P}_{\mathbf{b}}(D) \times \mathcal{M}_A \to \mathcal{M}_B$. Then, for all $M \in \mathcal{M}_A$, we define the function $P_{B,M} : \mathscr{P}_{\mathbf{b}}(D) \to \mathcal{M}_B$ by

$$P_{B,M}(b) = P_B(b, M)$$

Then, $P_{B,M}^{-1}(M')$ denotes the set $\left\{b \mid (b, M) \in P_B^{-1}\right\}$, which we regard as B's announcement after receiving message M from A. Notice that, in particular for a one-step protocol (P_A, P_B), $P_{B,M_1}^{-1}(M') = P_{B,M_2}^{-1}(M')$, for any pair of messages $M_1, M_2 \in \mathcal{M}_A$.

For an arbitrary two-step Russian Cards protocol (P_A, P_B) we will regard P_B as the *response protocol* for Bob. Observe that for all $M \in \mathcal{M}_A$, $P_{B,M}$ can be seen as an announcement protocol for $(\mathbf{b}, \mathbf{a}, \mathbf{c})$. Hence, we say P_B is *informative* if for all $M \in \mathcal{M}_A$, $P_{B,M}$ is an informative announcement protocol. Intuitively, this means that Bob's announcements according to P_B, will be informative for Alice. Similarly, we say P_B is *minimally informative* if for all $M \in \mathcal{M}$, $P_{B,M}$ is a minimally informative announcement protocol.

Definition 4 (Informative and minimally informative protocol)**.** *Let $\rho = (P_A, P_B)$ be a two-step protocol for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, then ρ is* (minimally) informative *if both P_A and P_B are (minimally) informative.*

As we previously discussed, the formulation of the safety notion for a Russian Cards protocol (P_A, P_B) is a bit more complex. However, it is easy to see that P_A needs to be a safe announcement protocol with respect to C and, while this suffices for P_A, we need a stronger requirement for the case of P_B, as it follows from the following definition. In the following, for any $\mathbf{c}$-set c, a pair of *compatible messages* with c, $(M, M') \in \mathcal{M}_A \times \mathcal{M}_B$, is such that there is a deal (a, b, c), with $P_A(a) = M$ and $P_B(b, M) = M'$.

Definition 5 (Safe protocol)**.** *Let* $\rho = (P_A, P_B)$ *be a protocol for the Russian Cards problem with signature* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$*. Then,* ρ *is* safe *if for any* $c \in \mathscr{P}_{\mathbf{c}}(D)$*, any* $y \in \bar{c}$ *and any compatible messages with c,* $(M, M') \in \mathcal{M}_A \times \mathcal{M}_B$*, there are two hands* a, a' *in* $\mathcal{P}(c, M)$ *such that* $y \in a \triangle a'$ *and* $P_B(D - c - a, M) = P_B(D - c - a', M) = M'$*.*

4.3 Perfectly safe response protocols

Previously, we remarked that whenever there is a safe and informative announcement protocol for Alice, there is a two-step safe and informative protocol for the corresponding Russian Cards problem, in which Bob announces Cath's hand. However, so far we have only claimed this is a safe two-step protocol based on an intuitive, but informal argument, i.e., the fact that this announcement does not give Cath any new information. Although, this argument may seem to be limited to this kind of response protocol, it is, in fact, the intuitive reason behind why other types of solutions also work well. For instance, we could also use this argument to explain why the aforementioned protocol (sum_7, sum_7) (in which Alice and Bob announce the sum of their cards modulo 7) is a solution to the classic Russian Cards problem, at least regarding the safety requirement. That is, in this case, Bob's response is something that Cath can infer at the moment she heard Alice's announcement, since she already knows the sum modulo 7 of his own cards and Alice's cards. Then, although in this case, Bob's response protocol is not explicitly the announcement of Cath's hand, his response protocol, sum_7, is equivalent to that, in the sense that he is informing nothing more than what Cath already knows.

The following definition formalizes this notion, that we call *perfectly safe response protocol.*

Definition 6 (Perfectly safe response)**.** *Let* $\rho = (P_A, P_B)$ *be a protocol for the Russian Cards problem with signature* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ *then, the response protocol* P_B *is* perfectly safe *with respect to* P_A *if for any* $c \in \mathscr{P}_{\mathbf{c}}(D)$*, any* $y \in \bar{c}$*, any compatible message* $M \in P_A(K(\bar{c}))$*, and any two hands* a, a' *in* $\mathcal{P}(c, M)$*, it* *holds that* $P_B(D-c-a, M) = P_B(D-c-a', M)$.

The intuition behind the previous definition is that the response protocol P_B is *perfectly safe* with respect to P_A if, from C's perspective, any two indistinguishable scenarios after A's announcement are still indistinguishable after B's announcement.

Chapter 5

Minimally informative protocols for Russian Cards

We present in Section 5.1 the two-message protocol χ_2, in which Alice announces the sum of her cards modulo 2. Such announcement protocol is minimally informative if and only if $\mathbf{b} < \lfloor n/2 \rfloor$. Thus, although χ_2 is not minimally informative for the classic Russian Cards problem $(3, 3, 1)$, it is for some cases in which it is known that no informative protocols exists, namely, cases where $\mathbf{a} \leq \mathbf{c}$. Moreover, this protocol is also safe for some of this instances. In particular, for the problem instance $(3, 4, 3)$ χ_2 is minimally informative and safe. This section is a presentation of the results from [18].

In Section 5.2 we present a two-message one-step solution in which Alice and Bob use the announcement protocol χ_2. This is, using only one bit, Alice and Bob can exchange some information in a safe manner in several Russian Cards scenarios. However, such scenarios do not include the classic instance of the generalized problem, i.e. $(3, 3, 1)$.

In Section 5.3 we present a two-message minimally informative announcement protocol construction for the classic problem $(3, 3, 1)$.

We show in Section 5.4 that, when $\mathbf{c} = 1$, any two-message minimally informative protocol is also a safe protocol. This means that the announcement protocol from Section 5.3 is also safe for $(3, 3, 1)$. Furthermore, in Section 5.5

we show how this protocol can be used in a two-message one-step minimally informative solution for the classic Russian Cards problem.

5.1 Two-message minimally informative protocol by modular arithmetic

This section is a presentation of the results from [18]. This results are presented here since in the following section we extend these results for obtaining a one step minimally informative solution for various instances of the Russian Cards problem.

For signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ consider the two-message protocol $\chi_2 : \mathscr{P}_{\mathbf{a}}(D) \to \{0, 1\}$, defined as follows:

$$\chi_2(a) = (\sum_{x \in a} x) \pmod 2.$$

5.1.1 χ_2 is minimally informative

Notice that, for each hand b for B, there are exactly $\binom{n-\mathbf{b}}{\mathbf{a}}$ possible hands for A. These are the vertices of a maximal clique $K(\bar{b})$ in $J^{\mathbf{c}}(n, \mathbf{a})$ consisting of all $a \subset \bar{b}$ such that $|a| = \mathbf{a}$.

The following lemma states the necessary and sufficient conditions for the protocol χ_2 to be minimally informative when $\mathbf{c} \geq 1$.

Lemma 3. *Assume that* $\mathbf{c} \geq 1$*, then the protocol* χ_2 *is minimally informative for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ *if and only if* $\mathbf{b} < \lfloor n/2 \rfloor$*.*

Proof. Notice that, if $\mathbf{b} \geq \lfloor n/2 \rfloor$, for $\mathbf{b} = |b|$, $\bar{b}$ may consist only of cards of the same parity, in which case, all $a \subset \bar{b}$ would have the same parity. Therefore, when $\mathbf{c} \geq 1$, $\mathbf{b} < \lfloor n/2 \rfloor$ is clearly a necessary condition for χ_2 to be minimally informative.

On the other hand, if we assume $\mathbf{b} < \lfloor n/2 \rfloor$, then $|\bar{b}| > n - \lfloor n/2 \rfloor$ for any b with $|b| = \mathbf{b}$, and $\bar{b}$ must consist of both even and odd cards. To show that χ_2 is minimally informative, consider any clique $K(\bar{b})$. Let $a \subset \bar{b}$, $|a| = \mathbf{a}$, be a vertex of $K(\bar{b})$ with the largest number of odd cards. Since there are both even and odd cards in $\bar{b}$, a contains at least one odd card, y. Since a contains the largest possible number of odd cards, it contains the minimum number of even cards. Thus, there is at least one even card $y' \in \bar{b} \setminus a$, given that $|a| < |\bar{b}|$. Let $a' = (a \setminus y) \cup y'$. Thus, a' is also a vertex of $K(\bar{b})$, and $\chi_2(a) \neq \chi_2(a')$. □

5.1.2 The protocol χ_2 is safe

Lemma 3 implies that χ_2 is minimally informative for $(3, 2, 2)$, namely, for $J^2(7, 3)$. However, it is not safe for this problem instance. Notice that, if C holds the hand $\{1, 3\}$ and A's message is 0, C knows A does not have card 5. Conversely, if the A's announcement is 1, C learns that A holds card 5.

The safety definition from Definition 3 instantiated for the protocol χ_2, says that (cf. [4, Proposition 6])χ_2 is safe (with respect to $\mathbf{c}$) if for each $\mathbf{c}$-set c, $y \in \bar{c}$, and $M \in \{0, 1\}$, there are two $\mathbf{a}$-sets $a, a' \in \bar{c}$, such that $\chi_2(a) = \chi_2(a') = M$ and $y \in a \triangle a'$. The following result states the necessary and sufficient conditions for χ_2 to be a safe protocol for the Russian Cards problem.

Lemma 4. *Assume that $\mathbf{c} \geq 1$, then the protocol χ_2 is safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ if and only if $\mathbf{a}, \mathbf{b} \geq 2$ and $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$.*

Proof. First, we prove that $\mathbf{a}, \mathbf{b} \geq 2$ and $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$ are necessary conditions when $\mathbf{c} \geq 1$.

Given that the number of odd cards in D is $\lfloor n/2 \rfloor$, if C holds $\mathbf{c} = \lfloor n/2 \rfloor - 1$ odd cards she can deduce from the announcement whether A holds the remaining odd card. Then, $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$ is clearly necessary.

As noted in Remark 3, if $\mathbf{a} = 1$, a safe protocol for $\mathbf{c} \geq 1$, needs to be a constant function for all possible cards that A may hold. As it is always possible that A's card is even or odd is clear that χ_2 does not always send the same message. Hence, $\mathbf{a} \geq 2$ is necessary.

Also, $\mathbf{b} \geq 2$ is necessary. Otherwise, if $\mathbf{b} = 1$, for any $\mathbf{c}$-set c, $|K(\bar{c})| = \mathbf{a} + 1$ and for any card $y \in \bar{c}$ there is only one hand a from $K(\bar{c})$ that does not contain y. Thus, since $\mathbf{a} \geq \lfloor n/2 \rfloor + 1$ its clear that $\{0, 1\} \in P_A(K(\bar{c}))$. Hence, w.l.o.g. suppose $P_A(a) = 0$, then all hands in $K(\bar{c})$ colored 1 do not contain y, which contradicts the safety requirement.

We prove now that the previous conditions are sufficient for χ_2 to be safe. Consider any $\mathbf{c}$-set c, and $y \in \bar{c}$. Let $z, z' \in D \setminus (c \cup y)$ be cards of different parity, which they exist because $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$. First, let a_1 be any $\mathbf{a}$-set in $\bar{c}$ that does not include y, and which includes z but not z', which exists because $\mathbf{b} \geq 2$. Let $a_2 = (a_1 \setminus z) \cup z'$. Thus, $\chi_2(a_1) \neq \chi_2(a_2)$. Similarly, let a'_1 be any $\mathbf{a}$-set in $\bar{c}$ which includes y, and which includes z but not z'. And let $a'_2 = (a'_1 \setminus z) \cup z'$. Thus, $\chi_2(a'_1) \neq \chi_2(a'_2)$.

We are done, because for each $M \in \{0, 1\}$, there is one $i \in \{1, 2\}$ such that $\chi_2(a_i) = M$ and does not include y, and there is one $i \in \{1, 2\}$ such that $\chi_2(a'_i) = M$ and does include y. □

Combining Lemma 3 and Lemma 4 we get the following theorem.

Theorem 4. *When $\mathbf{c} \geq 1$, the protocol χ_2 is minimally informative and safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ if and only if $\mathbf{a}, \mathbf{b} \geq 2$, $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$ and $\mathbf{b} < \lfloor n/2 \rfloor$.*

Remarkably, by the previous Theorem, χ_2 is minimally informative and safe in some cases where no informative and safe protocol exists. Recall that there is no informative and safe protocol (Corollary 4) in cases where

$$\mathbf{c} \geq \mathbf{b} \ \text{ or } \ \mathbf{c} \geq \mathbf{a} - 1. \tag{5.1}$$

Thus, for example, by Theorem 4, χ_2 is minimally informative and safe for $(3, 4, 3)$ and $(6, 6, 8)$, but there is no safe and informative solution in any of these cases. In particular, for the classic Russian Cards case χ_2 is not minimally informative. More generally, when $\mathbf{c} = 1$, we get the following.

Corollary 5. *The protocol χ_2 is minimally informative and safe for $(\mathbf{a}, \mathbf{b}, 1)$ if and only if $\mathbf{a} > \lceil n/2 \rceil - 1$ and $\mathbf{b} < \lfloor n/2 \rfloor$.*

5.2 One-step minimally informative solution by modular arithmetic

In the previous section we presented the announcement protocol χ_2, and stated when it is minimally informative and safe for A's announcement. Our purpose in this section, is to present a one-step minimally informative solution for some instances of the Russian Cards problem.

In this one-step protocol, both A and B use the announcement protocol χ_2, therefore we denote this solution by (χ_2, χ_2).

Theorem 5. *When* $1 \leq \mathbf{c} \leq \lfloor n/2 \rfloor - 2$, $2 \leq \mathbf{a}, \mathbf{b} < \lfloor n/2 \rfloor$, *the one-step protocol* (χ_2, χ_2) *is minimally informative and safe for* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

Proof. By Theorem 4, it is easy to see that χ_2 is minimally informative for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ and also for $(\mathbf{b}, \mathbf{a}, \mathbf{c})$, therefore (χ_2, χ_2) is minimally informative for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

Regarding the safety requirement, consider an arbitrary $\mathbf{c}$-set c, any card $y \in \bar{c}$ and any $M \in \{0, 1\}$. As χ_2 is a safe announcement protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, there are $a, a' \in \mathcal{P}(c, M)$ such that $y \in a \triangle a'$. Notice that when A announces M, B's message is fixed to be $\chi_2(D) - M - \chi_2(c) \pmod 2$. Thus, there is exactly one $M' = \chi_2(D) - M - \chi_2(c) \pmod 2$ such that (M, M') are compatible messages with c. Then, since $\chi_2(D-a-c) = \chi_2(D-a'-c) = M'$, (χ_2, χ_2) is safe. $\square$

The intuition behind why χ_2 is safe for Bob's response in this one-step protocol is that, once Alice announces according to χ_2, this information already allows Cath to infer Bob's announcement. Therefore, Bob's announcement does not give Cath any new information. Hence, what we have proved in fact is that, with respect to χ_2, Bob's response protocol is perfectly safe according to Definition 6.

Thus, we have our first one-step protocol for secure information exchange, which can be used for various instances of the generalized Russian Cards problem scenario, such as $(4, 4, 2)$, $(4, 3, 3)$ and $(5, 5, 2)$. Some of these instances can be described more generally as $(\mathbf{a}, \mathbf{a}, 2)$, with $\mathbf{a} \geq 4$. In particular, for cases in which $\mathbf{c} = 1$, such as the classic Russian Cards problem, this protocol would not be useful.

5.2.1 Two-step minimally informative protocol: first attempt

We know that, when $\mathbf{c} = 1$, a minimally informative announcement from Alice, allows Bob to learn at least one of the cards that Alice holds. The question we want to address now is whether it is safe for Bob to answer back to Alice saying: "You hold one of the cards x or y and I hold the other". This is obviously a minimally informative announcement to Alice, given that she will know one of Bob's cards. Therefore, at first glance, this may seem like a promising approach for not letting Cath to know which card belongs to who. However, this is not a trivial response since it reveals new information to Cath. This announcement allows Cath to know that neither A nor B, hold a hand containing both, x and y or a hand with neither x nor y.

Although this approach does not correspond to a trivial response, we cannot yet discard it as a possible response protocol. However, from the following analysis it is clear that in fact this approach does not always yield a solution. Consider the card deal $(\{456\} \,|\, \{012\} \,|\, \{3\})$ and the protocol from Appendix A. In this case, A announces $\chi(456) = 1$ and, after this, C considers possible for A to hold a hand in $\chi^{-1}(1) \cap K(\bar{3})$, i.e., $\mathcal{P}(\{3\}, 1) = \{026, 045, 056, 124, 125, 145, 146, 456\}$. On the other hand, B learns that A has card 6, so he can announce: "You hold one of the cards 0 or 6 and I hold the other". Let's call this message from Bob M'. After B's announcement, C knows that *Alice* cannot hold the hand 026, because it contains both 0 and 6. Also, C knows that *Alice* cannot hold the hand 124, because it does not contain either 0 or 6. Using similar analysis, we get that, after B's announcement, the only hands that C considers possible for *Alice* are those in $\{045, 146, 456\}$. Therefore, C can infer that A holds card 4, and also that Bob holds card 2. Hence, this is not an appropriate response protocol.

5.3 Two-message minimally informative protocol by Singer sets for (3,3,1)

In [18, Section 4.2] the author presented a construction that allows to obtain a minimally informative and safe protocol for $(3,3,1)$ using three messages. However, this is not optimal, namely there are minimally informative solutions for this problem instance using only two different messages. In fact, all these solutions could be easily computed by a program, which is what we did and found a total of $2 \times (76505394)$ 2-colorings. We already presented one of these two-message protocols in Section 3.5, which we found using our program. Although we were not able to find any protocol construction for that solution, here we present a construction for four of this two-message protocols.

The construction we present is based on Singer difference sets (or perfect difference sets) [19] and is inspired in the *good announcement* construction proposed in [2, Theorem 3].

First, we present the notions that we use for the protocol construction and then, some results that will be useful for proving that such construction yields a deterministic minimally informative protocol for $(3,3,1)$, using two messages.

Definition 7. *A set S of size $m+1$, is a perfect difference set if the differences $s_i - s_j$ module $m(m+1)+1$, with $i \neq j$, $s_i, s_j \in S$, are all the different integers from 1 to $m(m+1)$.*

In the following, the notation $x + S$ for a set S stands for the set $\{x + s \mod v \mid s \in S\}$.

The proof of the following lemma is similar to the one presented in [2, Theorem 3] for verifying that their announcement construction is informative.

Lemma 5. *Let S be a perfect difference set of size $m+1$ and $v = m(m+1)+1$, then for any two distinct elements $l_1, l_2 \in \{x + S \mid x \in \mathbb{Z}_v\}$, it holds that $|l_1 \cap l_2| = 1$.*

Proof. Let l_1 be $x+S$ and l_2 be $y+S$ with $x \neq y$. Assume for contradiction that $|l_1 \cap l_2| \neq 1$, then $|l_1 \cap l_2| = 0$ or $|l_1 \cap l_2| > 1$.

If it is the case that $|l_1 \cap l_2| = 0$, as S is a perfect difference set there are two elements $s_1, s_2 \in S$ such that $s_1 - s_2 = x - y \mod v$, then $y + s_1 = x + s_2 \mod v$, that is, an element from l_1 is equal to one from l_2, being a contradiction with $|l_1 \cap l_2| = 0$.

In the other case, any element in the intersection of l_1 and l_2 is equal to both $x + s_1$ and $y + s_2$, module v, for some $s_1, s_2 \in S$. Then $x - y = s_2 - s_1 \mod v$ and, as S is a perfect difference set, this uniquely define the pair s_1, s_2 so there is no more than one element in the intersection of l_1 and l_2, which contradicts $|l_1 \cap l_2| > 1$. $\square$

For a prime power m there is a perfect difference set of size $m+1$ [19], with all elements between 0 and $m(m+1)$. Thus, we know there is a perfect difference set S of size 3, such that $S \subseteq \mathbb{Z}_7$ which is what we need for the following protocol construction.

Let S be a perfect difference set of size 3 and S' a 3-*set* such that $S' \subseteq D - S$. Let L and L' be defined as follows:

$$L = \{x + S \mid x \in \mathbb{Z}_7\} \tag{5.2}$$

$$L' = \{x + S' \mid x \in \mathbb{Z}_7\} \tag{5.3}$$

Then, the protocol $\chi_S : \mathscr{P}_3(D) \to \mathbb{Z}_2$ is defined by,

$$\chi_S(0)^{-1} = L \cup L',$$
$$\chi_S(1)^{-1} = \mathscr{P}_3(D) - \chi_S(0)^{-1}.$$

Lemma 6. *The sets of cliques $K(\bar{a})$ of $J(7,3)$, $a \in L$ is a partition of $\mathscr{P}_3(D) - L$.*

Proof. For any $a \in L$, $K(\bar{a}) \subseteq \mathscr{P}_3(D) - L$, given that any element $a' \in L$ intersects with a by Lemma 5, it cannot be part of $K(\bar{a})$.

Let a and a' be two distinct elements of L, so by Lemma 5 $|a \cap a'| = 1$, then $|\bar{a} \cap \bar{a'}| = 2$. Thus, any 3-*set* in $K(\bar{a})$ intersects with any 3-*set* in $K(\bar{a'})$ in at most two elements, which means that $K(\bar{a})$ and $K(\bar{a'})$ are disjoint sets.

Finally, as $|\mathscr{P}_3(D) - L| = \binom{7}{3} - 7 = 28$ and $|K(\bar{a})| = 4$ for any 3-*set* a, we have that the union of the seven cliques $K(\bar{a})$ of $J(7,3)$, with $a \in L$, is the set $\mathscr{P}_3(D) - L$. $\square$

The main result of this section is stated in the following Theorem:

Theorem 6. *Let S be a perfect difference set of size 3 and S' a 3-set such that $S' \subseteq D - S$. The protocol χ_S is minimally informative for $(3, 3, 1)$.*

Proof. By Lemma 6, for any $b \in \mathscr{P}_3(D)$ we have two cases, namely $b \in L$ or $b \in K(\bar{a})$ for some $a \in L$.

Suppose $b \in L$, then there is $x \in \mathbb{Z}_7$, such that $b = x + S$. Therefore $x + S' \in K(\bar{b})$, otherwise if $x + S$ and $x + S'$ were to have common elements, it would mean that S and S' are not disjoint. Thus, as $|L| = |L'|$, for any $b \in L$ there is exactly one element $a \in L'$ such that $a \in K(\bar{b})$, given that all the cliques $K(\bar{b})$, $b \in L$ are disjoints by Lemma 6. Finally, let $a \in K(\bar{b})$ be $x + S'$ and a' be any element in $K(\bar{b}) - a$, then $\chi_S(a) = 0$ and $\chi_S(a') = 1$.

Now suppose $b \in K(\bar{a})$ for some $a \in L$. Then $a \in K(\bar{b})$ and $\chi_S(a) = 0$. Let a' be any element in $K(\bar{b}) - \{a\}$, then $dist(a, a') = 1$, i.e. $|a \cap a'| = 2$ and therefore $a' \notin L$, otherwise it would contradict Lemma 5. Now let a_1, a_2, a_3 be the three elements in $K(\bar{b}) - \{a\}$, and assume for contradiction that $\chi_S(a_1) = \chi_S(a_2) = \chi_S(a_3) = 0$, i.e. $a_1, a_2, a_3 \in L'$. Let $\bar{b} = \{x, y, z, k\}$, then w.l.o.g. $a_1 = \{x, y, z\}$, $a_2 = \{x, y, k\}$ and $a_3 = \{x, k, z\}$. Moreover, let s'_1, s'_2 and s'_3 be the three distinct elements in S', then w.l.o.g. $s'_1 + i = x$, $s'_2 + i = y$ and $s'_3 + i = z$, for some $i \in \mathbb{Z}_7$, so that $i + S' = \{x, y, z\} = a_1$. The following is a case analysis considering the different ways in which the other two sets, a_2 and a_3, could be obtained according to (5.3), so that $j + S' = \{x, y, k\} = a_2$ and $l + S' = \{x, k, z\} = a_3$, for distinct i, j, l with $j, l \in \mathbb{Z}_7$.

Notice that the following three ways for obtaining a_2 are impossible, since for any distinct $i, j \in \mathbb{Z}_7$ and any $r \in \mathbb{Z}_7$, $r + i \not\equiv r + j \mod 7$:

$$
\begin{array}{cccc|cccc|cccc}
 & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 \\
+i & x & y & z & +i & x & y & z & +i & x & y & z \\
+j & x & y & k & +j & x & k & y & +j & k & y & x
\end{array}
$$

Similarly, the following three ways for obtaining a_3 are also impossible:

$$
\begin{array}{cccc|cccc|cccc}
 & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 \\
+i & x & y & z & +i & x & y & z & +i & x & y & z \\
+l & x & k & z & +l & x & z & k & +l & k & x & z
\end{array}
$$

The following scenarios are also impossible since, for any distinct $r, t \in \mathbb{Z}_7$, $r - t \not\equiv t - r \mod 7$, given that 7 is a prime number:

$$
\begin{array}{cccc|cccc}
 & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 \\
+i & x & y & z & +i & x & y & z \\
+j & y & x & k & +l & z & k & x
\end{array}
$$

Then, we have only four possibilities left for obtaining a_2 and a_3 simultaneously, which are represented as follows:

$$
\begin{array}{cccc|cccc|cccc|cccc}
 & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 & & s'_1 & s'_2 & s'_3 \\
+j & k & x & y & +j & k & x & y & +j & y & k & x & +j & y & k & x \\
+l & k & z & x & +l & z & x & k & +l & k & z & x & +l & z & x & k
\end{array}
$$

These last four scenarios are also clearly impossible by the same arguments we mentioned earlier. Thus, since we have shown that in any of the previous scenarios we arrive to a contradiction, the theorem follows. $\square$

Additionally, we also verified Theorem 6 using the proof assistant system, Coq, for mechanically checking the arguments of the proof we presented here.

5.4 Safety for two-message minimally informative protocols

In the previous section we presented a two-message minimally informative protocol construction for $(3, 3, 1)$. Although we did not prove that this protocol is also safe, it is in indeed, in light of the following theorem, which is the main result of this section.

Theorem 7. *A two-message minimally informative announcement protocol for* $(\mathbf{a}, \mathbf{b}, 1)$ *is also safe if* $\mathbf{b} \geq 2$.

Proof. Let $\chi : \mathscr{P}_{\mathbf{a}}(D) \to \mathbb{Z}_2$ be a minimally informative announcement protocol for $(\mathbf{a}, \mathbf{b}, 1)$. Assume for contradiction that χ is not safe. That is, according to the safety Defitition 3, $\exists c \in D$[1], $\exists M \in \mathbb{Z}_2, \exists x \in \bar{c}$, such that for any **a**-sets $a, a' \subseteq \bar{c}$, it holds $\neg(\chi(a) = \chi(a') = M) \vee x \notin a \triangle a'$. Thus, for such c, M and x we have $\chi(a) = \chi(a') = M \Rightarrow x \in a \cap a' \vee x \notin a \cup a'$; so, if we consider any $a, a' \subseteq \bar{c}$ such that $a, a' \in \chi^{-1}(M)$, if $x \in a$ then $x \in a'$ or else if $x \notin a$ then $x \notin a'$. This means, for c, M and x one of the following should hold:

(1) for any $a \subseteq \bar{c}$, if $\chi(a) = M$ then $x \notin a$
(2) for any $a \subseteq \bar{c}$, if $\chi(a) = M$ then $x \in a$

Let $\{M'\} = \mathbb{Z}_2 - \{M\}$, then the previous is equivalent to:

(1) for any $a \subseteq \bar{c}$, if $x \in a$, then $\chi(a) = M'$
(2) for any $a \subseteq \bar{c}$, if $x \notin a$, then $\chi(a) = M'$

Suppose (1) holds. First, consider an arbitrary **a**-set $a' \subseteq \bar{c}$, such that $x \notin a'$. Let $\bar{b} = a' \cup \{x\}$, so that $\bar{b} \subseteq \bar{c}$ and for any $a \in K(\bar{b})$, $x \in a$ or $a = a'$. Thus, since χ is minimally informative, we have that $\chi(a') = M$; otherwise, all elements in $K(\bar{b})$, would be colored M' given that (1) holds. Thus, we have shown that for any **a**-set $a' \subseteq \bar{c}$, such that $x \notin a'$, it holds that $\chi(a') = M$. Now, let b be a **b**-set such that $c, x \in b$. Then, for any **a**-set $a \in K(\bar{b})$, we

[1] We also denote the singleton set with card c as c, as it is always clear from the context which case it is.

have that $a \subseteq \bar{c}$ and $x \notin a$; therefore, $\chi(a) = M$. This means that all **a**-sets in $K(\bar{b})$ are equally colored by χ, a contradiction to χ being a minimally informative coloring for $(\mathbf{a}, \mathbf{b}, 1)$.

Suppose (2) holds. Let b be a **b**-set such that $c, x \in b$. Then for any **a**-set $a' \in K(\bar{b})$, we have $\chi(a') = M'$. Then, all elements in $K(\bar{b})$ are equally colored by χ, thus we arrived to a contradiction with χ being a minimally informative coloring for $(\mathbf{a}, \mathbf{b}, 1)$.

Since, in any of the two cases we arrive to a contradiction, it holds that χ is safe and the theorem follows. $\square$

Notice that $\mathbf{c} = 1$ is necessary for the sake of the arguments in the proof. Otherwise, $D - a' - \{x\}$ is not a valid construction for a **b**-set b, and therefore $\bar{b}$ cannot be $a' \cup \{x\}$. Thus, for example, the previous lemma does not hold for the case $(2, 3, 2)$. For this case, even when there are minimally informative colorations for $J^2(7, 2)$, these may not be safe. For instance, in Appendix B we present a minimally informative coloring for this case, but it is not safe.

5.5 One-step minimally informative solution for (3,3,1)

In this section we present a one-step solution to the classic Russian Cards problem, with signature $(3, 3, 1)$. In this protocol, both Alice and Bob, use the same announcement protocol, based on the construction from Section 5.3, hence we denote this solution by (χ_S, χ_S).

Theorem 8. *Let S be a perfect difference set of size 3 and S' a 3-set such that $S' \subseteq D - S$. The one-step protocol (χ_S, χ_S) is minimally informative and safe for $(3, 3, 1)$.*

Proof. By Theorem 6, it is straightforward that (χ_S, χ_S) is minimally informative for $(3, 3, 1)$. Regarding the safety property, according to Definition 5, we must consider any card $c \in D$ [2] that C might hold, any card $y \in D - c$ that

[2] We also denote the singleton set with card c as c, as it is always clear from the context which case it is.

C does not hold, and any compatible messages $(M, M') \in \{0,1\} \times \{0,1\}$, and we must show that there are two 3-sets $a, a' \in \mathcal{P}(c, M)$ such that $y \in a \triangle a'$ and $\chi_S(D-a-c) = \chi_S(D-a'-c) = M'$. Note that there are exactly $\binom{6}{3} = 20$ 3-sets in $K(\bar{c})$. Hence, since there are exactly six elements in $\chi_S^{-1}(0)$ containing the card c, the remaining eight elements in $\chi_S^{-1}(0)$ are contained in $K(\bar{c})$, and therefore, these elements conform the set $\mathcal{P}(c, 0)$. Thus, the other twelve 3-sets in $K(\bar{c})$ (apart from the eight elements in $\chi_S^{-1}(0)$) are contained in $\chi_S^{-1}(1)$, and therefore, such elements conform the set $\mathcal{P}(c, 1)$.

In the following we analyze all four cases of possible pair of compatible messages $(M, M') \in \{0,1\} \times \{0,1\}$:

- Assume $(M, M') = (0, 0)$. Notice that, among the eight 3-sets in $\mathcal{P}(c, 0)$, by the construction of the set $\chi_S^{-1}(0)$, there must be two elements $a, a' \in \mathcal{P}(c, 0)$, such that $a = t + S$ and $a' = t + S'$, for some $t \in \mathbb{Z}_7$. Thus, a and a' are disjoint 3-sets in $\mathcal{P}(c, 0)$. Therefore, for any card $y \in D - c$, $y \in a \triangle a'$, since all cards in $D - c$ must appear in exactly one of the two 3-sets a and a'. Additionally, this also means that $D - a - c = a'$, therefore, $\chi_S(D - a - c) = \chi_S(a') = 0$ and $\chi_S(D - a' - c) = \chi_S(a) = 0$. Thus, it follows that $\chi_S(D - a - c) = \chi_S(D - a' - c) = 0$.
- Assume $(M, M') = (0, 1)$. Notice that, there are exactly three elements in $L' = \{x + S' \mid x \in \mathbb{Z}_7\}$ that contain card c. Let us say these elements are $t+S'$, $u+S'$ and $v+S'$. Then, the elements $t+S$, $u+S$ and $v+S$ from L are in $\mathcal{P}(c, 0)$. By Lemma 5, the intersection of any pair of elements from L is exactly one. Then, since $c \notin t + S \cup u + S \cup v + S$, from the inclusion-exclusion principle, it follows that $|t + S \cup u + S \cup v + S| = 6$ and $|t + S \cap u + S \cap v + S| = 0$. Then, for any card $y \in D - c$, there are two elements $a, a' \in \{t + S, u + S, v + S\}$, i.e., $a, a' \in \mathcal{P}(c, 0)$, such that $y \in a \triangle a'$. Without lost of generality, assume that $a = t + S$ and $a' = u + S$. Consider the 3-sets $b = D - a - c$ and $b' = D - a' - c$, so that $b \in K(\bar{a})$ and $b' \in K(\bar{a'})$. Notice that, by Lemma 5, $b, b' \notin L$, since $a \cap b = \emptyset$ and $a' \cap b' = \emptyset$. Assume for contradiction that there are at least two distinct elements in $K(\bar{a}) \cap L'$. Then, one of these elements must

be $t+S'$, and other must be $x+S'$ for some $x \in \mathbb{Z}_7$, with $x \neq t$. This means, that $K(\overline{t+S})$ and $K(\overline{x+S})$ are not disjoint, a contradiction with Lemma 6. Then, there is exactly one element in $K(\bar{a}) \cap L'$, which is $t+S'$. But, since $c \in t+S'$, it follows that $b \notin K(\bar{a}) \cap L'$, i.e., $b \notin L'$. Thus, $b \notin \chi_S^{-1}(0)$, which means $\chi_S(b) = 1$. Similarly, we can prove that $b' \notin L'$ then, $b' \notin \chi_S^{-1}(0)$, therefore $\chi_S(b') = 1$. It follows that $\chi_S(D-a-c) = \chi_S(D-a'-c) = 1$.

- Assume $(M, M') = (1, 0)$. Given that $\mathbf{a} = \mathbf{b}$, A and B use the same protocol, this follows from the previous case, i.e., they are symmetric.

- Assume $(M, M') = (1, 1)$. Notice that the 20 elements in $K(\bar{c})$ can be partitioned into ten pairs, such that the 3-sets in the pair are disjoint sets. Since twelve of these 3-sets conform the set $\mathcal{P}(c, 1)$, at least two of them must be disjoint, say a and a'. Thus, for any card $y \in D - c$, we have that $y \in a \triangle a'$. Then, by a similar argument to that from case $(M, M') = (0, 0)$, we have that $\chi_S(D-a-c) = \chi_S(D-a'-c) = 1$.

$\square$

Chapter 6

Conclusions

We have studied the problem of secure minimal information exchange between two agents A and B in the presence of an eavesdropper C. As in the Russian Cards problem scenario, the agents are modeled as card players, holding cards randomly dealt from a deck of n cards, according to a publicly known signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, specifying the number of cards dealt to A, B and C, respectively. Unlike in the classic Russian Cards problem, A and B are not required to learn the full hand of each other; instead, they only need to learn something about it. This way, their announcements must be minimally informative, but not necessarily informative. Additionally, the communication must be unconditionally secure, in the sense that the agents are treated as being computationally unlimited; in particular, the communication protocol must provide weak 1-security [20].

Our formalization, which is inspired in the framework from works about zero-error source coding, lead us to various formulations in terms of properties of Johnson graphs, similar to those from [18].

6.1 Repercussions

Reducing Communication Complexity. As we have seen, the minimum number of bits needed for an informative announcement protocol is

$\log_2 \chi(J^{\mathbf{c}}(n, \mathbf{a}))$, since the chromatic number of $J^{\mathbf{c}}(n, \mathbf{a})$ determines the number of different messages needed for an informative protocol. Although, in general, determining the exact chromatic number of Johnson graphs is still an open question, it is known that $\Theta(\mathbf{c} \log n)$ bits are needed and sufficient for information transmission in the Russian Cards scenario with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ [18]. However, as we have shown (see Section 5.2 and 5.5), only one bit suffices for achieving minimal information exchange and even security in various instances of the problem, and therefore, this is optimal in terms of communication complexity.

From informative to minimally informative protocols. In [18], the author presents a construction that produces a safe and minimally informative announcement protocol from a safe and informative one, for the same problem instance. The protocol construction uses the idea that merging two color classes of a protocol P_A, i.e., $P_A^{-1}[M]$ and $P_A^{-1}[M']$, leads to a new protocol that preserves safety, although possibly not informative properties. Therefore, this is a general propose strategy for obtaining a minimally informative protocol from known solutions to the problem. In particular, this construction allow us to obtain a three-message minimally informative and safe protocol for $(3, 3, 1)$, based on the well known modular protocol from [4].

In Section 5.3 we present a two-message safe and minimally informative protocol construction for $(3, 3, 1)$ based on Singer difference sets. This construction is also inspired in the informative solution proposed in [2, Theorem 3]. We believe this may serve as an example of how the techniques for informative protocol constructions can be creatively adapted for obtaining minimally informative protocols, using a more problem-specific approach compared to the previously mentioned, from [18].

Overcoming Impossibility Results. It is well known that no (fully) informative and safe announcement protocols exists for various problem instances, either when $\mathbf{c} \geq \mathbf{b}$ or $\mathbf{c} \geq \mathbf{a} - 1$. However, as we have shown, we can overcome this impossibility by weakening the informative requirement, namely, considering minimally informative announcements instead. Thus, for example, by Theorem 4, the protocol χ_2, presented in [18] is minimally informative and safe for $(3,4,3)$ and $(6,6,8)$, although there is no simultaneously safe and informative announcement protocol for any of these cases.

6.2 Future work

It is well known and easy to see that a solution for the classic Russian Cards problem implies a solution to the problem of unconditionally secure secret key exchange [9]. In general, it is quite likely that solutions for the classic problem could lead to unconditionally secure implementations of several cryptographic primitives. Notice that, in the problem scenario, the random deal of cards models correlated inputs for the participants, which are modeled as card players, such as in [9, 10, 11, 12], where the authors study unconditionally secure bit transmission and secret key exchange.

However, still remains the question of whether the minimally informative variant of the Russian Cards problem could also lead to unconditionally secure implementations of some general-purpose cryptographic primitive and in which scenarios.

Additionally, a full characterization of the deals for which minimally informative solutions and, in particular, two-message protocols exist could be also a subject of future investigation. For example, it is not known whether a secure minimally informative announcement protocol exists for the signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $\mathbf{b} > \mathbf{c} \geq \mathbf{a} > 1$ and $\mathbf{b} \geq \lfloor n/2 \rfloor$. Since no informative protocol exists for these problem instances with $\mathbf{c} \geq \mathbf{a}$, the protocol construction from [18, Section 4.2] would not work; additionally, since $\mathbf{b} \geq \lfloor n/2 \rfloor$, the protocol χ_2 from Section 5.1 would not be useful either. The further study of two-message protocols would be particularly interesting since such protocols are optimal in terms of communication complexity.

Moreover, it is also worthy to answer whether in future studies regarding minimally informative protocols we should keep the security requirement as weak 1-security. In other words, it might be reasonable to strengthen the security requirement since we are weakening the main classic goal of informativeness. Notice that, even when a minimally informative protocol is safe, in the sense of providing weak 1-security, it might well be the case that the eavesdropper C learns at least as much as B from A's announcement; in fact, it is clear that this would be the case whenever $\mathbf{c} \geq \mathbf{b}$. The intuition behind this can be expressed in terms of the initial knowledge of the agents, i.e, when $\mathbf{c} \geq \mathbf{b}$ the initial knowledge of C is at least as much as B's. Thus, it probably does not make much sense to use such protocols in those cases. As an alternative, we could study minimally informative protocols providing perfect k-security or weak k-security [20], for some $k > 1$. For practical purposes, such protocols would probably be more useful than the weak 1-secure ones in a wider amount of scenarios.

On the other hand, for future work, it might also be reasonable to study an alternative requirement for informativeness, but not as weak as the minimally informative requirement. To that effect, we could formulate the requirement so that it can be expressed in terms of the amount of cards that B should learn from A's announcement. This is because such formulation might be more consistent with the standard security formulations which are also concerned with the amount of cards that C must not learn. We believe that this decision would have important implications regarding the usefulness of such protocols for practical implementations of unconditionally secure cryptographic primitives.

Bibliography

[1] Albert, M., Cordón-Franco, A., van Ditmarsch, H., Fernández-Duque, D., Joosten, J.J., Soler-Toscano, F.: Secure communication of local states in interpreted systems. In: Abraham, A., Corchado, J.M., González, S.R., De Paz Santana, J.F. (eds.) International Symposium on Distributed Computing and Artificial Intelligence. pp. 117–124. Springer Berlin Heidelberg (2011)

[2] Albert, M.H., Aldred, R.E.L., Atkinson, M.D., van Ditmarsch, H., Handley, C.C.: Safe communication for card players by combinatorial designs for two-step protocols. Australas. J. Comb. **33**, 33–46 (2005)

[3] Atkinson, M.D., van Ditmarsch, H.P., Roehling, S.: Avoiding bias in cards cryptography. arXiv preprint cs/0702097 (2007)

[4] Cordón-Franco, A., van Ditmarsch, H., Fernández-Duque, D., Joosten, J.J., Soler-Toscano, F.: A secure additive protocol for card players. Australas. J. Comb. **54**, 163–176 (2012), `http://ajc.maths.uq.edu.au/pdf/54/ajc_v54_p163.pdf`

[5] Cordón-Franco, A., Van Ditmarsch, H., Fernández-Duque, D., Soler-Toscano, F.: A colouring protocol for the generalized Russian cards problem. Theor. Comput. Sci. **495**, 81–95 (July 2013), `https://doi.org/10.1016/j.tcs.2013.05.010`

[6] van Ditmarsch, H.: The Russian cards problem. Studia Logica **75**, 31–62 (October 2003), `https://doi.org/10.1023/A:1026168632319`

[7] van Ditmarsch, H., Soler-Toscano, F.: Three steps. In: Proc. of CLIMA XII. Lecture Notes in Computer Science, vol. 6814, pp. 41–57. Springer, New York, NY, USA (2011)

[8] Duan, Z., Yang, C.: Unconditional secure communication: a Russian cards protocol. Journal of Combinatorial Optimization **19**(4), 501–530 (2010), `https://doi.org/10.1007/s10878-009-9252-7`

[9] Fischer, M.J., Paterson, M.S., Rackoff, C.: Secret bit transmission using a random deal of cards. In: Feigenbaum, J., Merritt, M. (eds.) Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 2, pp. 173–182. DIMACS/AMS (1989), `https://doi.org/10.1090/dimacs/002/11`

[10] Fischer, M.J., Wright, R.N.: Multiparty secret key exchange using a random deal of cards. In: Feigenbaum, J. (ed.) Advances in Cryptology — CRYPTO '91. LNCS, vol. 576, pp. 141–155. Springer Berlin Heidelberg (1992)

[11] Fischer, M.J., Wright, R.N.: An efficient protocol for unconditionally secure secret key exchange. In: Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms. p. 475–483. SODA '93, Society for Industrial and Applied Mathematics, USA (1993)

[12] Fischer, M.J., Wright, R.N.: Bounds on secret key exchange using a random deal of cards. Journal of Cryptology **9**(2), 71–99 (1996), `https://doi.org/10.1007/BF00190803`

[13] Kirkman, T.: On a problem in combinations. Camb. Dublin Math. J. **2**, 191–204 (1847)

[14] LANDERRECHE, E.: A zero-error source coding solution to the russian cards problem (2017)

[15] Leyva-Acosta, Z., Pascual-Aseff, E., Rajsbaum, S.: Information exchange in the Russian Cards problem, to appear in the 23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'21), November 17-20, 2021. Lecture Notes in Computer Science (LNCS), Springer

[16] Makarychev, Y.S., Makarychev, K.: The importance of being formal. Mathematical Intelligencer **23**(1) (2001)

[17] Orlitsky, A.: Worst-case interactive communication. i. two messages are almost optimal. IEEE Transactions on Information Theory **36**(5), 1111–1126 (1990)

[18] Rajsbaum, S.: A distributed computing perspective of unconditionally secure information transmission in Russian cards problems. In: Jurdzinski, T., Schmid, S. (eds.) Structural Information and Communication Complexity - 28th International Colloquium, SIROCCO 2021, Wrocław, Poland, June 28 - July 1, 2021, Proceedings. Lecture Notes in Computer Science, vol. 12810, pp. 277–295. Springer (2021). https://doi.org/10.1007/978-3-030-79527-6_16, `https://doi.org/10.1007/978-3-030-79527-6_16`

[19] Singer, J.: A theorem in finite projective geometry and some applications to number theory. Transactions of the American Mathematical Society **43**(3), 377–385 (1938)

[20] Swanson, C.M., Stinson, D.R.: Combinatorial solutions providing improved security for the generalized Russian cards problem. Des. Codes Cryptography **72**(2), 345–367 (August 2014), `https://doi.org/10.1007/s10623-012-9770-7`

[21] Witsenhausen, H.: The zero-error side information problem and chromatic numbers (corresp.). IEEE Transactions on Information Theory **22**(5), 592–593 (1976)

Appendix A

An example of minimally informative coloring for J(7,3)

The following is an example of a minimally informative coloring for $J(7,3)$, which we previously presented in Section 3.5.

$$\chi^{-1}(0) = \{012, 013, 014, 015, 016, 023, 024, 025, 036, 046, 126, 134, 135, 156, 234, 245, 246, 256, 345\}$$
$$\chi^{-1}(1) = \{026, 034, 035, 045, 056, 123, 124, 125, 136, 145, 146, 235, 236, 346, 356, 456\}$$

b	$\chi^{-1}(0) \cap K(\bar{b})$	$\chi^{-1}(1) \cap K(\bar{b})$	b	$\chi^{-1}(0) \cap K(\bar{b})$	$\chi^{-1}(1) \cap K(\bar{b})$
012	{345}	{346, 356, 456}	013	{245, 246, 256}	{456}
014	{256}	{235, 236, 356}	015	{234, 246}	{236, 346}
016	{234, 245, 345}	{235}	023	{156}	{145, 146, 456}
024	{135, 156}	{136, 356}	025	{134}	{136, 146, 346}
026	{134, 135, 345}	{145}	034	{126, 156, 256}	{125}
035	{126, 246}	{124, 146}	036	{245}	{124, 125, 145}
045	{126}	{123, 136, 236}	046	{135}	{123, 125, 235}
056	{134, 234}	{123, 124}	123	{046}	{045, 056, 456}
124	{036}	{035, 056, 356}	125	{036, 046}	{034, 346}
126	{345}	{034, 035, 045}	134	{025, 256}	{026, 056}
135	{024, 046, 246}	{026}	136	{024, 025, 245}	{045}
145	{023, 036}	{026, 236}	146	{023, 025}	{035, 235}
156	{023, 024, 234}	{034}	234	{015, 016, 156}	{056}
235	{014, 016, 046}	{146}	236	{014, 015}	{045, 145}
245	{013, 016, 036}	{136}	246	{013, 015, 135}	{035}
256	{013, 014, 134}	{034}	345	{012, 016, 126}	{026}
346	{012, 015, 025}	{125}	356	{012, 014, 024}	{124}
456	{012, 013, 023}	{123}			

Table A.1: Color partitions of $K(\bar{b})$ for each b, according to χ

c	$\chi^{-1}(0) \cap K(\bar{c})$	$\chi^{-1}(1) \cap K(\bar{c})$
0	{126, 134, 135, 156, 234, 245, 246, 256, 345}	{123, 124, 125, 136, 145, 146, 235, 236, 346, 356, 456}
1	{023, 024, 025, 036, 046, 234, 245, 246, 256, 345}	{026, 034, 035, 045, 056, 235, 236, 346, 356, 456}
2	{013, 014, 015, 016, 036, 046, 134, 135, 156, 345}	{034, 035, 045, 056, 136, 145, 146, 346, 356, 456}
3	{012, 014, 015, 016, 024, 025, 046, 126, 156, 245, 246, 256}	{026, 045, 056, 124, 125, 145, 146, 456}
4	{012, 013, 015, 016, 023, 025, 036, 126, 135, 156, 256}	{026, 035, 056, 123, 125, 136, 235, 236, 356}
5	{012, 013, 014, 016, 023, 024, 036, 046, 126, 134, 234, 246}	{026, 034, 123, 124, 136, 146, 236, 346}
6	{012, 013, 014, 015, 023, 024, 025, 134, 135, 234, 245, 345}	{034, 035, 045, 123, 124, 125, 145, 235}

Table A.2: Color partitions of $K(\bar{c})$ for each c, according to χ

Appendix B

An example of minimally informative not safe coloring for $J^2(7,2)$

Here we present an example of minimally informative not safe coloring for $J^2(7,2)$.
$\varphi^{-1}(0) = \{01, 02, 03, 04, 05, 06, 12, 13, 14, 25, 26, 35, 36, 45, 46\}$
$\varphi^{-1}(1) = \{15, 16, 23, 24, 34, 56\}$

b	$\varphi^{-1}(0) \cap K(\bar{b})$	$\varphi^{-1}(1) \cap K(\bar{b})$	b	$\varphi^{-1}(0) \cap K(\bar{b})$	$\varphi^{-1}(1) \cap K(\bar{b})$
012	$\{35, 36, 45, 46\}$	$\{34, 56\}$	013	$\{25, 26, 45, 46\}$	$\{24, 56\}$
014	$\{25, 26, 35, 36\}$	$\{23, 56\}$	015	$\{26, 36, 46\}$	$\{23, 24, 34\}$
016	$\{25, 35, 45\}$	$\{23, 24, 34\}$	023	$\{14, 45, 46\}$	$\{15, 16, 56\}$
024	$\{13, 35, 36\}$	$\{15, 16, 56\}$	025	$\{13, 14, 36, 46\}$	$\{16, 34\}$
026	$\{13, 14, 35, 45\}$	$\{15, 34\}$	034	$\{12, 25, 26\}$	$\{15, 16, 56\}$
035	$\{12, 14, 26, 46\}$	$\{16, 24\}$	036	$\{12, 14, 25, 45\}$	$\{15, 24\}$
045	$\{12, 13, 26, 36\}$	$\{16, 23\}$	046	$\{12, 13, 25, 35\}$	$\{15, 23\}$
056	$\{12, 13, 14\}$	$\{23, 24, 34\}$	123	$\{04, 05, 06, 45, 46\}$	$\{56\}$
124	$\{03, 05, 06, 35, 36\}$	$\{56\}$	125	$\{03, 04, 06, 36, 46\}$	$\{34\}$
126	$\{03, 04, 05, 35, 45\}$	$\{34\}$	134	$\{02, 05, 06, 25, 26\}$	$\{56\}$
135	$\{02, 04, 06, 26, 46\}$	$\{24\}$	136	$\{02, 04, 05, 25, 45\}$	$\{24\}$
145	$\{02, 03, 06, 26, 36\}$	$\{23\}$	146	$\{02, 03, 05, 25, 35\}$	$\{23\}$
156	$\{02, 03, 04\}$	$\{23, 24, 34\}$	234	$\{01, 05, 06\}$	$\{15, 16, 56\}$
235	$\{01, 04, 06, 14, 46\}$	$\{16\}$	236	$\{01, 04, 05, 14, 45\}$	$\{15\}$
245	$\{01, 03, 06, 13, 36\}$	$\{16\}$	246	$\{01, 03, 05, 13, 35\}$	$\{15\}$
256	$\{01, 03, 04, 13, 14\}$	$\{34\}$	345	$\{01, 02, 06, 12, 26\}$	$\{16\}$
346	$\{01, 02, 05, 12, 25\}$	$\{15\}$	356	$\{01, 02, 04, 12, 14\}$	$\{24\}$
456	$\{01, 02, 03, 12, 13\}$	$\{23\}$			

Table B.1: Color partitions of $K(\bar{b})$ for each b, according to φ

c	$\varphi^{-1}(0) \cap K(\bar{c})$	$\varphi^{-1}(1) \cap K(\bar{c})$
01	$\{25, 26, 35, 36, 45, 46\}$	$\{23, 24, 34, 56\}$
02	$\{13, 14, 35, 36, 45, 46\}$	$\{15, 16, 34, 56\}$
03	$\{12, 14, 25, 26, 45, 46\}$	$\{15, 16, 24, 56\}$
04	$\{12, 13, 25, 26, 35, 36\}$	$\{15, 16, 23, 56\}$
05	$\{12, 13, 14, 26, 36, 46\}$	$\{16, 23, 24, 34\}$
06	$\{12, 13, 14, 25, 35, 45\}$	$\{15, 23, 24, 34\}$
12	$\{03, 04, 05, 06, 35, 36, 45, 46\}$	$\{34, 56\}$
13	$\{02, 04, 05, 06, 25, 26, 45, 46\}$	$\{24, 56\}$
14	$\{02, 03, 05, 06, 25, 26, 35, 36\}$	$\{23, 56\}$
15	$\{02, 03, 04, 06, 26, 36, 46\}$	$\{23, 24, 34\}$
16	$\{02, 03, 04, 05, 25, 35, 45\}$	$\{23, 24, 34\}$
23	$\{01, 04, 05, 06, 14, 45, 46\}$	$\{15, 16, 56\}$
24	$\{01, 03, 05, 06, 13, 35, 36\}$	$\{15, 16, 56\}$
25	$\{01, 03, 04, 06, 13, 14, 36, 46\}$	$\{16, 34\}$
26	$\{01, 03, 04, 05, 13, 14, 35, 45\}$	$\{15, 34\}$
34	$\{01, 02, 05, 06, 12, 25, 26\}$	$\{15, 16, 56\}$
35	$\{01, 02, 04, 06, 12, 14, 26, 46\}$	$\{16, 24\}$
36	$\{01, 02, 04, 05, 12, 14, 25, 45\}$	$\{15, 24\}$
45	$\{01, 02, 03, 06, 12, 13, 26, 36\}$	$\{16, 23\}$
46	$\{01, 02, 03, 05, 12, 13, 25, 35\}$	$\{15, 23\}$
56	$\{01, 02, 03, 04, 12, 13, 14\}$	$\{23, 24, 34\}$

Table B.2: Color partitions of $K(\bar{c})$ for each c, according to φ