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

Secure information exchange protocols for Russian Cards problems

TESIS

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

PRESENTA:

EDUARDO PASCUAL ASEFF

Director de tesis

Dr. Sergio Rajsbaum
IMATE-UNAM

Ciudad Universitaria, CD. MX., Septiembre de 2021

Abstract

Two agents, Alice (A) and Bob (B) wish to privately exchange information by public announcements overheard by a computationally unlimited eavesdropper Cath (C). In order for them to achieve a certain level of confidentiality in their communication, their inputs must be correlated. Dependent inputs are represented using a deck of cards. There is a publicly known signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, meaning that A gets $\mathbf{a}$ cards, B gets $\mathbf{b}$ cards, and C gets $\mathbf{c}$ cards, out of the deck of n cards, where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. A and B want to learn each other's cards while preventing C from learning any card from A's or B's hand.

Our perspective is inspired by distributed computing and considers colorings of a generalization of Johnson graphs. We formally present the problem of information exchange in the Russian Cards problem scenario described above, where there are $\mathbf{r}$ cards not dealt to anyone. We present some general impossibility results and study the communication complexity of information transmission and information exchange protocols in this scenario. In doing so, we explore in detail links with a fundamental problem in Coding Theory regarding constant weight codes.

Agradecimientos

Muchísimas gracias ...

A mis padres Jorge y Neyibe, a mi abuela Victoria y mi hermana Luisa, por brindarme un gran apoyo, aún desde la distancia, con el que siempre puedo contar.

A Zoe Leyva, por su colaboración en el desarrollo de este trabajo. Nuestras discusiones en el problema estudiado han sido muy productivas y nos han ayudado a mejorar nuestros resultados.

A mi tutor Dr. Sergio Rajsbaum, por su enseñanza, su apoyo y sus consejos durante mis estudios y durante la elaboración de este trabajo.

A mis profesores Dr. Armando Castañeda Rojano, Dr. Rodolfo Conde Martínez, Dr. David Rosenbluth y Dr. Carlos Bruno Velarde Velázquez, por sus comentarios, sugerencias y correciones que han sido de gran ayuda para mejorar este trabajo.

A la UNAM, al Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas, y al Posgrado en Ciencia e Ingeniería de la Computación, por brindarme una educación de excelencia.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) por apoyarme económicamente durante mis estudios de posgrado.

A todos cuyos nombres no he mencionado aquí y que me han brindado su apoyo a lo largo de mis estudios, y a todos los que de una forma u otra han influido en mi desarrollo profesional y personal hasta el día de hoy.

A todos: ¡Muchísimas gracias!

Contents

Chapter 1

Introduction

The problem of two card players, Alice (A) and Bob (B), trying to publicly communicate their hands to the other, while preventing a third player, Cath (C), from learning any of their cards is often regarded as the Russian Cards problem, or one of its variants. From the problem statement, is clear that security, in the form of privacy, is an essential requirement, which immediately reveals a relation with cryptography. In particular, since one of the usual assumptions for the problem is that the agents involved (the card players) are computationally unlimited, solutions must aim for *unconditional security*.

In Section 1.1, we present the notion of unconditional security and discuss its role and relevance in the context of modern cryptography. We also discuss the reasons why the study of the Russian Cards problem and its generalizations could be of great importance for designing unconditional secure protocols for more general purposes, such as implementing well-known cryptographic primitives. In Section 1.2, we present the classic and generalized versions of the Russian Cards problem. The motivation and contributions of the present work are presented in Section 1.3. A related work discussion can be found in Section 1.4. Finally, the organization in chapters of the present work is documented at the end of this chapter.

1.1 Unconditional security in modern cryptography

Nowadays, *cryptography* is present in innumerable applications of our daily lives to provide confidential communications. Among these applications we can mention *online payments*, *digital currencies*, *computer passwords* and many others.

Most modern cryptosystems, whether they are symmetric or asymmetric, are designed around computational complexity assumptions; therefore, they are based on the model of *computational-security.* All such cryptosystems no matter if they use *private-* or *public-key cryptography*, although in practice are extremely hard to break, can be broken in principle given a sufficient amount of ciphertext by trying all of the possible keys. Hence, such systems are vulnerable to the development of science and technology, since computational power greatly increases and some of the previously considered hard problems, such as integer factorization, might not be hard enough in the future.

Thus, computer science and technology developments require for cryptosystems with computational security to be constantly reevaluated and, in occasions, they might need to be adapted. The permanent risk of being broken that these systems face, motivates the search for cryptosystems providing *unconditional security.* Unconditionally secure cryptosystems cannot be broken even if the adversary has unlimited computational resources; therefore, unconditional security will only become more and more relevant. The term unconditional security was used first by Diffie and Hellman in their seminal paper New Directions in Cryptography [9], as far as we know, although the area was born with Shannon. This type of security is based on the fact that there is not enough information available to the adversary that allows him to break the system. Then, in order for such cryptosystems to be proven secure the adequate framework is information theory rather than complexity theory.

A central notion in information-theoretic analysis of cryptosystems is Shannon's definition of *perfect secrecy*, which is without a doubt the strongest formulation of security one can find. However, despite the strong motivation for the search of unconditional security and the fact that such a nice formulation for what *perfect security* means (perfect secrecy) is already available, most research in past years focuses on the computational security of cryptosystems, rather than in unconditional security. This is also due to Shannon's well-known lower bound on the amount of a priori shared secret information (secret key length) for any perfectly secure cipher. This suggested that, in practical scenarios, such a high level of security was unfeasible. However, more recent research showed that unconditional security can in fact be achieved in various special but realistic scenarios, thus somewhat mitigating the pessimism surrounding unconditional security.

As observed in [22], almost every cryptographic primitive could be implemented in an unconditional secure manner; however, under certain conditions. As an example, *bit commitment* and *oblivious transfer* are two cryptographic primitives for which it is well known that there is no unconditionally secure scheme implementation in a two-player scenario. However, unconditional security has been achieved in both cases in the presence of a third party, namely a "trusted initializer" [20]. The role of the trusted initializer is to provide the participants with some sort of correlated inputs during a setup phase. Another example of when unconditional security has been achieved via correlated inputs is [13], in this case for *secret bit transmission*. Here, as well as in [14, 15] correlated inputs are modeled using a random deal of cards and the participants are modeled as card players such as in the Russian Cards problem scenario.

Since the statement of the Russian Cards problem, as we will see in the following section, is quite general, it is very likely that solutions for the problem could be useful for implementing several cryptographic primitives, such as the ones previously mentioned, in a unconditionally secure manner.

1.2 The classic and the generalized Russian Cards problems

Let D be a deck of n cards labeled from 0 to $n-1$, which are distributed among three players Alice (A), Bob (B) and Cath (C), so that A gets $\mathbf{a}$, B gets $\mathbf{b}$ and C gets the remaining $\mathbf{c}$ cards. A and B should communicate between them through a public channel, with the following two goals or requirements. First, following [19, 23], a solution or *protocol* should be *informative for* A, that is, A must learn B's hand and, on the other hand, it must be also *informative for* B, that is, B must also learn A's hand. The second requirement, regarded as *safety*, states that C cannot learn whether A or B has any particular card (except for the ones she owns).

A particular instance of this problem can be described by the signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, then $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$. This is usually regarded as the *generalized Russian Cards problem*, while the $(3, 3, 1)$ instance of the problem is known as the *Russian Cards problem* and was presented at the Moscow 2000 Mathematical Olympiad. We may also regard the latter as the classic Russian Cards problem, since it was the first instance of the problem that was actively studied.

All circumstances regarding the actual scenario, i.e., the deck composition, the signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ of the deal and the communication protocol, are assumed to be common knowledge among the players, except for which cards each player holds.

1.2.1 Problem solutions

Solutions to the problem may consist of only two announcements (one from A and one from B), and these solutions are regarded as *two-step protocols* [2, 11]. Then, in such solutions, both announcements from A and B must be informative for the other. On the other hand, we regard the protocol for A's announcement only, as a *one-step protocol.*

Whenever A can make an informative and safe announcement, since B

is informed about A's hand, he can always announce C's hand. Hence, B's announcement is informative for A and also safe, as the announcement does not give C any new information. This would be a two-step solution or, in other words, an informative and safe two-step protocol. Then, designing a two-step protocol for secure information exchange reduces to designing a one-step protocol for secure information transmission.

A one-step protocol for A's announcement is said to be *deterministic* when the hand that she holds uniquely determines the announcement that she makes [23]. Conversely, if for some hand there are different announcements that A could make, the protocol is said to be *non-deterministic* [23].

1.2.2 Announcements as alternative hands

It is well known that any public announcement from a player (no matter how the announcement is worded in natural language or coded) is always equivalent to the player making of public knowledge that he has one of the hands in a particular set $\mathcal{L}$, which we regard as an *announcement* [10].

As an example, consider the problem instance $(2, 2, 1)$ and A announcing "the sum of my cards is even". This is equivalent to the public announcement that A holds one of the hands in the set $\{\{0, 2\}, \{0, 4\}, \{1, 3\}, \{2, 4\}\}$.

In the following, when representing set of cards or hands we might omit the commas separating the elements of the set and even the brackets. Thus, we might write the set representing the previous announcement as $\{\{02\}, \{04\}, \{13\}, \{24\}\}$ or $\{02, 04, 13, 24\}$

1.2.3 Problem variants and generalizations

Over the generalized problem scenario variations in the requirements have also been considered, especially regarding the security (safety) requirement. The original requirement, as stated above is also regarded as *weak* 1*-security* [23]. Alternatively, if C cannot learn whether A or B holds any particular set of k cards, we are in the presence of *weak k-security.* Even a stronger security requirement regarded as *perfect k-security* [23] has also been considered. This is closer to Shannon's perfect secrecy notion [21], since C must not gain any probabilistic advantage in guessing who holds any set of k cards. Thus, for achieving *perfect* 1*-security*, C must consider, for any card x that she does not hold, that the probability of A or B holding x is the same as before the communication. Notice that, given the number of cards dealt, these probabilities are $\frac{\mathbf{a}}{n-\mathbf{c}}$ and $\frac{\mathbf{b}}{n-\mathbf{c}}$, respectively. Thus, although weak security is not concerned with giving C advantage in making educated guess, any of the aforementioned security conditions provides unconditional security in the sense that they do not relay on the assumption of a computationally limited adversary.

On the other hand, we can think of an even more general scenario, where there are $\mathbf{r}$ cards in the deck that are not dealt to anyone, i.e. $n = \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{r}$. This was recently considered for the first time in [19]. In this case, a problem instance is described by the signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, and additionally, the value of n, or alternatively, the value of $\mathbf{r}$. Hence, in the following, unless explicitly stated otherwise, we will consider $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$ for any problem instance with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

1.3 Motivation and contribution

What separates this work from others is mostly the fact that we consider the problem of information exchange in the more general Russian Cards scenario, in which there are $\mathbf{r}$ cards in the deck that are not dealt to any player, i.e., $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. This scenario was only considered recently in [19]; however, only the information transmission problem, i.e., one-way communication, was rigorously studied over the paper and only considering deterministic solutions. Most of the terminology and notation that we use in this work came from [19]

For this work we focus on both one-step and two-step protocols providing weak 1-security. We do not consider more lengthy solutions nor stronger security requirements. Hence, in the following, we might use the terms *security*, *safety* and *weak 1-security* interchangeably. Thus, our work is an extension of [19] in the sense that we now focus on studying the communication in both ways, i.e., two-step protocols, and also consider non-deterministic protocols.

Additionally, unlike other works that study the problem from an epistemic logic perspective, here we take a combinatorial approach, inspired by distributed computing.

Secure information exchange when $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. We provide a formal presentation of the problem of information exchange in the more general Russian Cards scenario, where $\mathbf{r}$ cards from the deck are not dealt to the players, as well as generalizations of several known results for this new scenario.

Additionally, we introduce the notion of *perfectly safe response* protocols, in which B's response is perfectly safe with respect to A's announcement. One of our main contributions is an impossibility result regarding perfectly safe response protocols. Namely, we prove that, unlike in the case where $n = \mathbf{a}+\mathbf{b}+\mathbf{c}$, when $\mathbf{r} > 0$, B cannot make an informative announcement for A without revealing any new information to C. Moreover, we also consider two-step protocols in which B's announcement is trivially informative for A and show that these protocols are proper solutions if and only if the protocol for A's announcement is informative and safe for the problem instance $(\mathbf{a}, \mathbf{b}, \mathbf{c} + \mathbf{r})$. Furthermore, we show that in this general scenario, a solution to the problem of secure information transmission does not always mean that we can solve the problem of secure information exchange, unlike in the case where $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$.

Good announcements and protocols. Some authors formulate the informative and safety requirements for individual announcements, instead of protocols [2, 3, 11]. Recall that an announcement is equivalent to a set of alternative hands for a player. In those works, the authors regard the announcement satisfying the informative and safety formulations as *good announcements*. About this approach, the authors in [23] argue that "*it is not possible to formally define or discuss the security of a scheme using definitions that focus on individual announcements*". Motivated by this claim, we argue that in fact this approach is valid, at least when considering weak 1-security, in the sense that good announcements can lead to a protocol construction, although not necessarily deterministic. Moreover, this protocol would inherit the informative and safety properties, and therefore can be considered a formal solution.

However, we also observe that the different strategies that can be used for the protocol construction, could have important implications on the communication complexity of the resulting protocol.

Communication complexity bounds. We want to study the communication complexity of information transmission and information exchange protocols for Russian Cards problems. In doing so, we explore in detail the links between informative Russian Cards protocols and the fundamental problem regarding *binary constant-weight codes*. In particular, we follow ideas from [16] in order to present an informative one-step protocol for the general case $\mathbf{c}+\mathbf{r} > 1$, which therefore implies an upper bound on the number of messages needed for information transmission. To that effect, our approach and result is similar to that of [19]. Namely, we show that $O((\mathbf{c}+\mathbf{r})\log n)$ bits are sufficient for a one-step informative protocol, and $O((\mathbf{c}+\mathbf{r})\log n + \log \binom{n-\mathbf{a}}{\mathbf{b}})$ bits are sufficient for a two-step informative protocol. This bound for one-step informative protocols, generalizes a bound for informative and safe solutions when $\mathbf{c}+\mathbf{r} = 1$ and $\mathbf{a}, \mathbf{b} \geq 3$, in which $\log n$ bits are sufficient for the transmission [6].

1.4 Related work

The origins of the Russian Cards problem may be found in works such as [13, 14, 15]; however, the active study of the problem, as it is known today, and its generalizations started with [10]. Among other things, that paper was responsible for the name of the problem. Although in [10] the author takes an epistemic logic approach for modeling the problem, the author also shows that whenever a player makes an announcement, the announcement can be seen as the player making of public knowledge that he has one of the ha nds in a specific set $\mathcal{L}$ of *alternative hands.* Hence, in the present work, as well as in most works, such set $\mathcal{L}$ is regarded as an *announcement.* This is a useful and important result, since it allows the study of the problem with a combinatorial approach.

In [2] the authors focus on the scenario where all cards are dealt to the three players, i.e., $n = \mathbf{a}+\mathbf{b}+\mathbf{c}$ and in two-step solutions in which Alice makes the first announcement. Since the authors assume that Bob's announcement would be informing Alice about Cath's hand, they focus on designing a good announcement for Alice in some problem instances. The authors formalize the notion of a *good announcement* $\mathcal{L}$ via some epistemic axioms and equivalent combinatorial ones. These axioms or conditions are stated in such a way that, whenever Alice can make a (thoughtful) good announcement $\mathcal{L}$, the problem requirements (informative and safety) are met after Bob's response announcing Cath's hand. Then, the authors study some conditions for the existence of good announcements. Namely, they show that when $\mathbf{c} \geq \mathbf{a} - 1$ there is no *good announcement* for Alice and therefore, no two-step solution for the Russian Cards problem. Additionally, the authors present some lower and upper bounds on the sizes of good announcements.

Two-step solutions have been found for various instances of the generalized problem. Some solved instances are ($\mathbf{a}$, 2, 1), provided $\mathbf{a} \equiv 0, 4 \mod 6$, and more interestingly, those where $\mathbf{b} = O(\mathbf{a}^2)$, found in [2] with solutions via perfect difference sets and block designs. Also, ($\mathbf{a}$, $\mathbf{a}$, 1) with $\mathbf{a} > 2$ [1], where A announces the sum of her cards modulo $2\mathbf{a} + 1$. A generalized version of this result is presented in [6], for ($\mathbf{a}$, $\mathbf{b}$, 1) with $\mathbf{a}, \mathbf{b} > 2$.

Solutions consisting of more than two steps have also been studied, although not at the same extent that two-step solutions. In [11] the authors proposed a three-step solution for $(4, 4, 2)$ after proving that no two-step solution exists for this problem instance. Also, a four-step protocol based on finite vector spaces is presented in [7] as the first known solution when $\mathbf{c} > \mathbf{a}$.

In [23] the authors formalize the notions of *weak k-security* and *perfect k-security.* In such terminology, the classical security condition for the problem is called *weak 1-security.* Although most literature focus on this classical security requirement, some others have also been considered. For instance, in [3] the authors present a *perfect 1-security* good announcement construction for $(2^{k-1}, 2^{k-1} - 1, 1)$, where $k \geq 3$, via binary designs. Furthermore, the authors in [23] provide a characterization of informative and perfectly $(d-1)$-secure solutions for $(d+1, b, 1)$, with $b \geq d-1$, involving $d - (n, d+1, 1)$-designs.

Moreover, in [23] the authors also distinguish between *deterministic* solutions or protocols, in which A's hand uniquely determines her message, and non-deterministic ones.

Similarly, recently a weaker alternative for the *informative* requirement, known as *minimally informative* was considered in [19] where, instead of having to learn each other's hand, A and B only need to learn "something" about their respective hands. Additionally, in that paper, it is also considered the more general scenario for the Russian Cards problem in which there are $\mathbf{r}$ cards that are not dealt to the players. In that work the author takes a distributed-computing perspective based on Algebraic Topology, specifically, using simplicial complexes. Some of the results that we present in this work regarding only the information-transmission problem, i.e., one-way communication, were previously presented in [19], although only considering deterministic protocols. Moreover, in [19] the author exposes the link between comunication complexity of informative Russian Cards protocols and a fundamental problem in Coding Theory. In particular, this relation is a consequence of the characterization of informative protocols for Russian Cards problem as proper colorings of Johnson graphs. We also exploit this link in the present work in a similar fashion.

Organization. The present work consists of five chapters. In Chapter 2 we present the formal specification of both the secure information transmission and secure information exchange problems, in the general Russian Cards scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. Additionally, we present several general results, some of which are generalizations of known results and others which are novel.

In Chapter 3 we present a different approach to solutions, that focuses on announcements, instead of protocols [2, 3] and discuss the relation between both, in particular from the perspective of communication complexity.

In Chapter 4 we discuss the links between informative protocols for Russian Cards problem and the fundamental problem regarding constant weight codes. We also exploit this relation for presenting one of such protocols. Additionally, we provide a general upper bound for the communication complexity of such protocols.

Finally, the conclusions can be found in Chapter 5.

Chapter 2

The Russian Cards problem

In the first part of this chapter, Section 2.1, we formally present the problem of secure information exchange in the Russian Cards problem scenario in which there are $\mathbf{r}$ cards in the deck that are not dealt to any player. As we previously remarked this particular scenario has not been extensively studied. Following [19], the model of the problem is inspired by a distributed-computing approach [17] that relies on topological notions, such as simplicial complexes. Moreover, we use this model for defining the notions of informative and safe protocols.

In Section 2.2, we focus on *one-step protocols*. In particular, we show how they can be modeled as vertex-coloring functions of a Johnson graph. Additionally, we characterize the notions of informative and safe one-step protocols as properties of colorings for these graphs. Also, we present some generalizations of several known results which were originally stated when considering only the scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$ or solely deterministic protocols. Most of these results came as straightforward consequences of the characterizations that we present.

In Section 2.3, we study *two-step protocols* and present some general novel results for the more general scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$.

2.1 Modeling the problem

Let $D = \{0, \ldots, n-1\}$, $n > 1$, be a *deck* of n distinct *cards*. Each subset x of cards is a *hand*, $x \in \mathscr{P}(D)$. We may say for short that x, $|x| = m$, is an m-set or m-hand, namely, if $x \in \mathscr{P}_m(D)$, the subsets of D of size m. A *deal* $= (a, b, c)$ consists of three disjoint hands, meaning that the cards in a are dealt to A, the cards in b to B, and the cards in c to C. 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 $|c| = \mathbf{c}$, following the notation introduced by Fischer and Wright [14], although their notation did not used bold letters for the scalars. This notation may be seen as misleading for the readers, since scalars are usually used to represent vectors; however, we remind that we closely follow the terminology and notation from [19].

A given signature and the value of $\mathbf{r}$ (or alternatively n), with $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, determines an instance of the problem. We assume that the players A, B and C are aware of the deck and the signature. While A and B get at least one card ($\mathbf{a}, \mathbf{b} \geq 1$), C may get none ($\mathbf{c} \geq 0$). However, we assume $\mathbf{c} + \mathbf{r} \geq 1$. Otherwise, if $\mathbf{c} = \mathbf{r} = 0$, A and B would know each other's hands without the necessity of any communication.

When it is only required for A to inform B about her hand via a single announcement, we regard this as an *information-transmission* problem, and the protocol that A uses to that effect is a *one-step protocol*, denoted P_A.

When B is required to also inform A about his hand, we say this is an *information-exchange* problem. Solutions to this problem consisting of only two announcements (one from A and one from B), are regarded as *two-step protocols*, denoted as the pair (P_A, P_B), where P_A is the protocol for A's announcement, and P_B is the protocol for B's. We may also regard P_B as a *response protocol.*

In the following section, Section 2.1.1, we present the notions of deterministic and non-deterministic protocols for Russian Cards problems and discuss its communication complexity. In Section 2.1.2, we model the problem via an input simplicial complex, an approach that can be found in distributed-computing works. Finally, in Sections 2.1.3 and 2.1.4, we present the notions of informative and safe Russian Cards protocols relying on this model.

2.1.1 Deterministic and non-deterministic protocols

We are interested in studying both deterministic and non-deterministic protocols. If we denote by $\mathcal{M}_A$ the domain of messages that A may send, a one-step protocol P_A can be modeled by the function $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$ [1], meaning that A with hand a can announce M if and only if $M \in P_A(a)$. Similarly, if we denote by $\mathcal{M}_B$ the domain of messages that B may send, the protocol for B's announcement, P_B, would be a function $P_B : \mathscr{P}_{\mathbf{b}}(D) \times \mathcal{M}_A \to \mathscr{P}^*(\mathcal{M}_B)$.

As seen in Section 1.2, any public announcement of a player can be associated with a set of alternative hands that the player might hold [10]. Thus, since the number of different such sets is finite and the elements of $\mathcal{M}_A$ and $\mathcal{M}_B$ encode such sets, it makes sense to assume that both $\mathcal{M}_A$ and $\mathcal{M}_B$ are finite sets.

When considering *non-deterministic* protocols, the players' announcements are not uniquely determined by their hands and the messages that have been publicly announced (if any). Hence, if we consider a non-deterministic one-step protocol P_A for A, in which A holding hand a may announce one of several possible messages, then $|P_A(a)| > 1$.

On the other hand, in *deterministic* protocols, the communication between A and B is uniquely determined by their hands and the messages that have been publicly announced (if any). Hence, if we consider a deterministic one-step protocol P_A, then for any $a \in \mathscr{P}_{\mathbf{a}}(D)$, $|P_A(a)| = 1$. Similarly, for a deterministic protocol P_B for B's announcement, we have that for any $b \in \mathscr{P}_{\mathbf{b}}(D)$ and any $M \in \mathcal{M}_A$, $|P_B(b, M)| \leq 1$ [2].

In the following, we may also regard a deterministic one-step protocol P_A as a function from $\mathscr{P}_{\mathbf{a}}(D)$ to $\mathcal{M}_A$, meaning that $P_A(a) = M$ if M is A's message to B when she holds the hand a. Similarly, in a deterministic two-step protocol, we may say $P_B(b, M) = M'$, if M' is B's response to A's message, M, when he holds hand b.

[1] For a set S, $\mathscr{P}^*(S)$ denotes the power set of S without the empty set, i.e., $\mathscr{P}^*(S) = \mathscr{P}(S) - \emptyset$.

[2] Notice that $|P_B(b, M)| = 0$ exactly for the cases in which it is impossible that B with hand b may hear the message M.

Communication complexity. In distributed computing, an important matter is the amount of communication needed between the agents (or processes) to solve a problem or task. For a particular problem, the *communication complexity* is the minimum number of bits that the agents may communicate to solve the problem. One of the main goals for the present work is studying the communication complexity of several solutions to different variants of the Russian Cards problem.

For a one-step protocol $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$, whether it is deterministic or not, it is clear that what A needs to communicate is a message $M \in \mathcal{M}_A$. Since $\mathcal{M}_A$ is a finite set and it is also of public knowledge among all players (since it is part of the protocols definitions), then all elements in the set can be numbered from 0 to $|\mathcal{M}_A| - 1$. Hence, for communicating M to B, A only needs to transmit the index of M. In other words, $\mathcal{M}_A$ (as well as $\mathcal{M}_B$) can also be seen as a finite set of consecutive indexes starting from 0. This way, the number of bits for communication that P_A requires is $\log_2(|\mathcal{M}_A|)$. Hence, we can define the communication complexity of P_A to be $\log_2(|\mathcal{M}_A|)$.

Additionally, if we consider a two-step protocol, where B responds using the protocol $P_B : \mathscr{P}_{\mathbf{b}}(D) \times \mathcal{M}_A \to \mathscr{P}^*(\mathcal{M}_B)$, the communication complexity of (P_A, P_B) is $\log_2(|\mathcal{M}_A|) + \log_2(|\mathcal{M}_B|)$. Thus, it is clear that, from a communication-complexity perspective, the goal is to design protocols with the smallest possible sets $\mathcal{M}_A$ and $\mathcal{M}_B$.

2.1.2 The input complex

In this section, we present how the problem can be modeled, adapting the distributed-computing formalization of [17] to the case of an eavesdropper. A similar adaptation can be found in [19].

All possible deals for a given signature over D are represented by an *input complex* [17]. For a signature $\gamma = (\mathbf{a}, \mathbf{b}, \mathbf{c})$, the *input complex* $\mathcal{I}(\mathbf{a}, \mathbf{b}, \mathbf{c})$, or $\mathcal{I}$ for short, is defined as follows. It consists of all sets $\{(A, a), (B, b), (C, c)\}$, where (a, b, c) is a deal for signature γ, together with all their subsets. Each maximal set of $\mathcal{I}$, namely of size three, corresponds to a deal, and is called a *facet*. An element of the form (Y, y), where $Y \in \{A, B, C\}$ and y is a hand, is a vertex, an it is called Y-vertex. We say that the hand y is the *input* of the player Y. All vertices in a set of $\mathcal{I}$ are connected pair to pair.

Notice that the A-vertices of $\mathcal{I}$ are in a one-to-one correspondence with all subsets of size $\mathbf{a}$ of D, i.e., $\mathscr{P}_{\mathbf{a}}(D)$. Similarly, the B-vertices correspond to each of the elements from $\mathscr{P}_{\mathbf{b}}(D)$, and the C-vertices to the elements in $\mathscr{P}_{\mathbf{c}}(D)$. Indeed, when $\mathbf{c} = 0$, there is a single vertex for C in $\mathcal{I}$. Figure 2.1 shows that in the case of signature $\gamma = (1, 1, 1)$, $n = 4$, the complex is a torus subdivided into triangles. The vertices of each triangle are colored black, gray, and white to represent the three different players.Inside the vertex is the hand (consisting of a single card) dealt to the corresponding player.

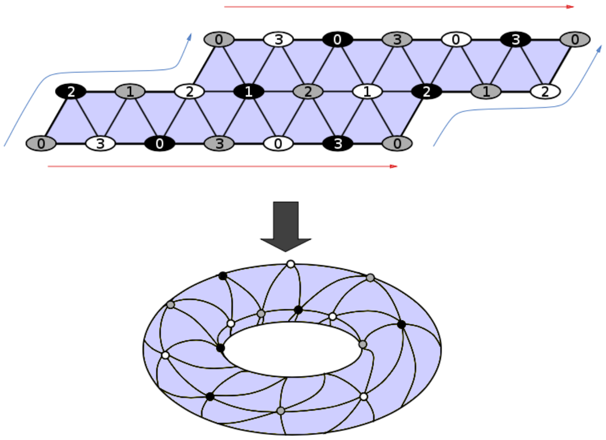

Figure 2.1: Input complex $\mathcal{I}$ for $(1, 1, 1)$ with $n = 4$

2.1.3 Informative protocols

In distributed systems, usually an agent is modeled as a state machine. Each agent starts in a state that depends only on its inputs. Then, they execute a protocol that may involve local computation or communication among agents and this may cause the agent to transit to another state. For a protocol, an *execution* is a sequence of agent state transitions [17].

In the Russian Cards problem, the initial state of a player X depends on x, the hand that the player holds. Since the communication is via public announcements, any communication may change the state of all players. In this problem, an *execution* of a protocol is given by the deal that the players hold, and the list of messages publicly announced by the players executing the protocol.

For a fixed protocol and a facet I, representing a specific deal (a, b, c), we denote all executions starting with I as $\alpha(I)$. Thus, for a facet I, since a deterministic protocol uniquely determines an execution, $\alpha(I)$ is a singleton set. However, in general, for a one-step protocol P_A and the facet I, $\alpha(I)$ is the set of executions determined by every possible $M \in P_A(a)$. Similarly, for a two-step protocol (P_A, P_B), $\alpha(I)$ denotes the set of executions determined by every possible $M \in P_A(a)$ and every possible message $M' \in P_A(b, M)$. For an execution $\alpha \in \alpha(I)$, we denote by $input_X(\alpha)$ the hand of player $X \in \{A, B, C\}$ in the deal determined by the facet I.

For a vertex (X, x), defining the input for the player X, we denote by $\alpha(X, x)$ the set of all the possible executions where X holds the hand x, i.e., $\alpha(X, x) = \{\alpha(I) : (X, x) \in I, I \in \mathcal{I}, |I| = 3\}$. For example, $\alpha(C, c)$ denotes all the executions that Cath considers possible when she holds hand c.

The *view* of a player in an execution consists of its input and the sequence of messages announced in the execution. Two executions α, α' are *indistinguishable* to $X \in \{A, B, C\}$, if the player X has the same view in both [4], denoted $\alpha \overset{X}{\sim} \alpha'$. On the contrary, if the executions are not indistinguishable, we say that they are *distinguishable*.

Definition 1 (Informative protocol)**.** *Let $X, X' \in \{A, B\}$, be two different players, and (X', x') be any X'-vertex in $\mathcal{I}$.*

- *A protocol P_X is* informative *for X' if any two executions $\alpha_1, \alpha_2 \in \alpha(X', x')$, such that $input_X(\alpha_1) \neq input_X(\alpha_2)$, are distinguishable to X'.*
- *A protocol (P_A, P_B) is* informative *if P_A and P_B are* informative *for B and A respectively.*

The previous definition guarantees that for any possible input, if P_X is informative, then X' may deduce the hand that X is holding. Notice that, when A or B learn the hand of the other, she or he may deduce the set of cards that were dealt to C or not dealt at all. Thus, when $\mathbf{r} = 0$ they could learn the hand held by C.

The informative notion does not consider the player C. Indeed, it is based only on the the subcomplex of $\mathcal{I}$ which is the graph induced by the A-vertices and the B-vertices.

2.1.4 Safe protocols

In this section, we formally define what it means for a Russian Cards protocol to be safe in the general scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. We want our definition to resemble as much as possible that of previous papers. However, previous papers considered only the case $\mathbf{r} = 0$. Some of the informal safety formulations that can be found in the literature are the following:

1. "C must not be able to infer any card in either of A or B's hands" [2]
2. "(...) without Cathy[3] learning the fate of any particular card" [23]
3. "the cards of A and B should be secret from C" [19]

These informal formulations are equivalent when $n = \mathbf{a}+\mathbf{b}+\mathbf{c}$; however, they are not when $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ with $\mathbf{r} > 0$. In fact, the first one (1) and the last (3) can be interpreted as being semantically equivalent in any context, but the second (2), when $\mathbf{r} > 0$, can hardly be interpreted as meaning the same as the other two. This is, when $\mathbf{r} = 0$, Cath not learning the fate of any card she does not own is equivalent to not knowing whether such a card is held by Alice or Bob. However, if $\mathbf{r} > 0$, even when Cath does not know any card in either of A or B's hands she may well know the fate of the remaining $\mathbf{r}$ cards. Thus, neither 1 nor 3 implies 2, but 2 does imply 1 and also 3. Therefore, 2 can be seen as a stronger formulation when considering the case of $\mathbf{r} > 0$.

[3] In [23] the authors use the name Cathy for the eavesdropper, which we call Cath in this work.

The following safety definition expresses the requirement that C must not be able to infer any card in either of A or B's hands, i.e., this is equivalent to formulations 1 and 3. In other words, when $\mathbf{r} > 0$, C may learn the fate of cards that neither A nor B hold, but for any other pair of cards x and y, she must not learn which party holds which card.

Definition 2 (Safe protocol)**.** *A protocol P_A (or a two-step protocol (P_A, P_B)) is* safe *if for any C-vertex (C, c) of $\mathcal{I}$, any protocol execution α in $\alpha(C, c)$, and any pair of cards x, y held by A and B, respectively, in α, there are two other executions of the protocol $\alpha_1, \alpha_2 \in \alpha(C, c)$, with $y \in input_A(\alpha_1)$ and $x \in input_B(\alpha_2)$, such that $\alpha \overset{C}{\sim} \alpha_1$ and $\alpha \overset{C}{\sim} \alpha_2$.*

Notice that the previous definition states when a one-step protocol, as well as a two-step protocol for a Russian Cards problem, should be considered safe when $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. However, when the definition is read for one-step protocols or, alternatively, for two-step protocols, it should be taken into consideration that the *execution* of a one-step protocol differs from the execution of a two-step protocol. Therefore, we must interpret the notion of execution in the definition according to the case.

The previous definition guarantees that, in a *safe* (one-step) protocol, C does not learn any of the cards held by A or B. That is, whenever C considers possible that A (B) holds any particular card, there is another scenario that looks the same for C, in which the card belongs to B (A) instead. However, for a safe two-step protocol it is still possible that C may learn the fate of any of the $\mathbf{r}$ cards that were not dealt to anyone. As we shall see later, this will allow in some cases that when there is an informative and safe one-step protocol P_A, B could answer to A announcing the set of cards that neither A nor B holds, and this would translate into an informative and safe two-step protocol.

On the other hand, for a safe one-step protocol P_A although it may seem possible also that Cath could learn the fate of any of the $\mathbf{r}$ cards that were not dealt to anyone, this is not the case, as we will show later. In fact, we will prove that safety for a one-step protocol means the satisfaction of the informal formulation 2.

2.2 One-step protocols

In the following sections, we focus on studying *one-step protocols*. Most of the terminology and notation that we use in this section is that from [19].

In Section 2.2.1, we show how we can represent indistinguishability in the Russian Cards scenario via Johnson graphs, as it was previously noted in [19].

In Section 2.2.2, we characterize the notions of informative and safe one-step protocols, i.e., Definitions 1 and 2, respectively, as properties of colorings of these particular graphs. These are generalizations of the informative and safety characterizations from [19], which only consider deterministic protocols.

In Section 2.2.3, we present some interesting remarks and observations, most of which came as straightforward consequences of the characterizations presented.

2.2.1 Representing indistinguishability by Johnson graphs

A one-step protocol $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$ is a function defined over the set of possible hands for A, i.e., the set $\mathscr{P}_{\mathbf{a}}(D)$. Such protocol assigns to each A-vertex (A, a) of $\mathcal{I}$, a set of labels or *colors*, $P_A(a)$. Thus, we can think of a one-step protocol as a *multicoloring* function (or simply a coloring function in the case of a deterministic protocol) of the A-vertices of $\mathcal{I}$.

The vertex $(B, b) \in \mathcal{I}$ represents that B has input b. The hands that B with input b considers possible for A are the $\mathbf{a}$-sets contained in the A-vertices connected to (B, b) in $\mathcal{I}$. Such A-vertices are the *A-neighbors* of the vertex (B, b).

Following [19], we define the graph $\mathcal{G}_B$ in terms of $\mathcal{I}$, as follows. The $\mathbf{a}$-sets contained in the A-vertices of $\mathcal{I}$ are the vertices of $\mathcal{G}_B$. Then, $V(\mathcal{G}_B) = \mathscr{P}_{\mathbf{a}}(D)$. The edge $\{a, a'\}$ is in $E(\mathcal{G}_B)$ if and only if (A, a) and (A, a') are A-neighbors of the same vertex (B, b) in $\mathcal{I}$, i.e., they are both connected to (B, b) in $\mathcal{I}$. Thus, for two distinct $a, a' \in \mathscr{P}_{\mathbf{a}}(D)$, the edge $\{a, a'\}$ is in $E(\mathcal{G}_B)$

if and only if there is $b \in \mathscr{P}_{\mathbf{b}}(D)$ such that $a, a' \subseteq \bar{b} = D - b$.

Similarly, we define the graph $\mathcal{G}_C$ considering the perspective of C instead of B. Both graphs have the same set of vertices: $V(\mathcal{G}_C) = V(\mathcal{G}_B) = \mathscr{P}_{\mathbf{a}}(D)$. When C has input c, this is represented by a vertex $(C, c) \in \mathcal{I}$, and the hands that C with input c considers possible for A are the **a**-sets contained in the A-neighbors of (C, c) in $\mathcal{I}$. Thus, for two distinct $a, a' \in \mathscr{P}_{\mathbf{a}}(D)$, the edge $\{a, a'\}$ is in $E(\mathcal{G}_C)$ if and only if there is $c \in \mathscr{P}_{\mathbf{c}}(D)$ such that $a, a' \subseteq \bar{c} = D - c$.

The following lemma can be found in [19]; however, we prove it here since it is fairly simple and it could be helpful in convincing the reader about the following observations.

Lemma 1. *[19] For $a, a' \in \mathscr{P}_{\mathbf{a}}(D)$, $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, we have that $\{a, a'\} \in E(\mathcal{G}_B)$ if and only if $\mathbf{a} - (\mathbf{c} + \mathbf{r}) \leq |a \cap a'|$. Similarly, $\{a, a'\} \in E(\mathcal{G}_C)$ if and only if $\mathbf{a} - (\mathbf{b} + \mathbf{r}) \leq |a \cap a'|$.*

Proof. Let a, a' be two hands in $\mathscr{P}_{\mathbf{a}}(D)$ such that $\{a, a'\} \in E(\mathcal{G}_B)$. Then, there exists a **b**-set b such that $a, a' \in \bar{b} = D - b$. Then, it holds:

$$|a \cup a'| \leq |D - b| = n - \mathbf{b}$$

$$|a \cup a'| \leq \mathbf{a} + \mathbf{c} + \mathbf{r}$$

By the inclusion-exclusion principle $|a \cup a'| = 2 \times \mathbf{a} - |a \cap a'|$, then we have:

$$2 \times \mathbf{a} - |a \cap a'| \leq \mathbf{a} + \mathbf{c} + \mathbf{r}$$

$$\mathbf{a} - (\mathbf{c} + \mathbf{r}) \leq |a \cap a'|$$

and this is exactly what we want to prove.

Let a, a' be two hands in $\mathscr{P}_{\mathbf{a}}(D)$ such that $\mathbf{a} - (\mathbf{c} + \mathbf{r}) \leq |a \cap a'|$. By a similar argument as the one used in the previous case, it holds that $|a \cup a'| \leq n - \mathbf{b}$. Then there exists a set b of cards of size $\mathbf{b}$ that is disjoint to both a and a', i.e. $a, a' \in \bar{b}$. This means that $a, a' \in E(\mathcal{G}_B)$.

The proof for the edges in $E(\mathcal{G}_C)$ is similar. □

The following is a generalization of Johnson graphs [19], and as we shall see in short, it can be used to represent the graphs $\mathcal{G}_B$ and $\mathcal{G}_C$.

Definition 3 (Distance d Johnson graph)**.** *For a set S of n elements, the graph $J^d(n, m)$, $0 \le d \le m$, has as vertices all m-subsets of S. Two vertices a, a' are adjacent whenever $m - d \le |a \cap a'|$. When $d = 1$, we have a* Johnson graph*, also denoted $J(n, m)$.*

From the previous definition and Lemma 1 it is straightforward that the graph $\mathcal{G}_B$ for signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ is equal to the graph $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$. In particular, $\mathcal{G}_B$ is a Johnson graph, $J(n, \mathbf{a})$, exactly when $\mathbf{c}+\mathbf{r} = 1$. Similarly, $\mathcal{G}_C$ is equal to $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$.

Figure 2.2 shows the graph $J(4, 2)$. Each vertex represents a possible 2-set out of a deck of 4 cards. In other words, the vertices are in one-to-one correspondence with all possible hands or inputs for A in the Russian Cards problem with signature $(2, 1, 1)$, $\mathbf{r} = 0$ or $(2, 1, 0)$, $\mathbf{r} = 1$. Additionally, two vertices are adjacent if they represent hands that B considers possible for A to have when he holds some hand b. As an example, consider the vertices for the hands $\{01\}$ and $\{02\}$, which are adjacent, meaning that, with input $\{3\}$, B considers both hands possible for A. Conversely, the vertices representing the hands $\{01\}$ and $\{23\}$ are not adjacent since there is not an input for B such that he would consider both hands as possible inputs for A.

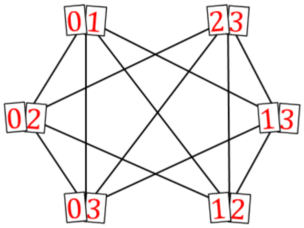

Figure 2.2: The Johnson graph $J(4, 2)$

For each hand b of B, the set of possible inputs for A, consisting of all $a \in \mathscr{P}_{\mathbf{a}}(D - b)$, is denoted $K_p(\bar{b})$. Similarly, for each hand c of C, the set of possible inputs for A, consisting of all $a \in \mathscr{P}_{\mathbf{a}}(D - c)$, is denoted $K_p(\bar{c})$. The elements in $K_p(\bar{b})$ and $K_p(\bar{c})$ induce a clique in $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ and $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$, respectively. Overloading notation, the respective cliques themselves are also sometimes denoted by $K_p(\bar{b})$ and $K_p(\bar{c})$.

Remark 1 (Subgraphs [19])**.** *When* $\mathbf{b} \leq \mathbf{c}$ *then* $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ *is a subgraph of* $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ *on the same set of vertices. Therefore, for any* $b \in \mathscr{P}_{\mathbf{b}}(D)$ *and any* $c \in \mathscr{P}_{\mathbf{c}}(D)$*, both* $K_p(\bar{b})$ *and* $K_p(\bar{c})$ *induce cliques in* $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$*. Additionally, if* $b \subseteq c$*, then* $K_p(\bar{c}) \subseteq K_p(\bar{b})$*.*

2.2.2 One-step protocols as vertex coloring of Johnson graphs

Consider a one-step protocol P_A for signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. In light of the results from the previous section we take the view of $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$ as a *multicoloring* of the graph $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$. Thus, P_A is a *proper* multicoloring of $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ if for any two adjacent vertices a, a' in $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$, $P_A(a)$ and $P_A(a')$ are disjoint. Notice that, if P_A is a deterministic protocol, then we may say it is simply a *coloring* of $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$, with $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}_A$.

Figure 2.3 represents a coloring of the graph $J(4, 2)$. Hence, this coloring represents a one-step deterministic protocol $P_A : \mathscr{P}_2(\mathbb{Z}_4) \to \mathcal{M}_A$ for the Russian Cards problem with signature $(2, 1, 1)$, $\mathbf{r} = 0$ or $(2, 1, 0)$, $\mathbf{r} = 1$. This protocol uses three colors or messages, namely, $\mathcal{M}_A = \{0, 1, 2\}$.

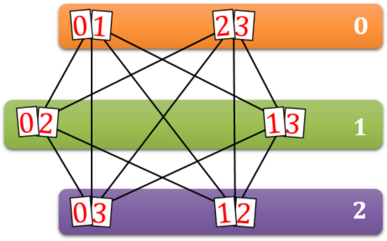

Figure 2.3: A coloring of the graph $J(4, 2)$ using three colors: ‘0’, ‘1’ and ‘2’.

Also, for a protocol P_A, we denote the *announcement* corresponding to a message or color M, by $P_A^{-1}(M)$ [4]. Then, for any $M \in \mathcal{M}_A$, the set $P_A^{-1}(M)$

[4] $P_A^{-1}(M)$ is equivalent to an “announcement” by A in the terminology of [2], or the “alternative hands” for A, in the notation of [10, Proposition 24].

is defined as follows:

$$P_A^{-1}(M) = \{a \mid M \in P_A(a)\}$$

As an example, consider the protocol P_A represented in Figure 2.3 and notice that the announcements for such protocol are the following:

$$\begin{aligned} P_A^{-1}(0) &= \{01, 23\} \\ P_A^{-1}(1) &= \{02, 13\} \\ P_A^{-1}(2) &= \{03, 12\} \end{aligned}$$

The following two theorems reformulate the informative and safety notions of Definitions 1 and 2 for one-step protocols, and generalize the characterizations [19, Theorem 2] and [19, Theorem 3], respectively.

Theorem 1 (Informative characterization)**.** *Let $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$ be a protocol, then P_A is informative for B if and only if P_A is a proper multicoloring of $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$.*

Proof. Let P_A be an informative protocol and assume for contradiction that P_A is not a proper multicoloring of $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$, then there is a vertex $(B, b) \in \mathcal{I}$ such that two different neighbors $(A, a), (A, a')$ share a color M. Therefore, there are two executions $\alpha, \alpha' \in \alpha(B, b)$ indistinguishable to B, with $input_A(\alpha) \neq input_A(\alpha')$, which is a contradiction with P_A being informative for B.

Conversely, if P_A is a proper multicoloring of $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$, then for any vertex $(B, b) \in \mathcal{I}$, any pair of neighbors $(A, a), (A, a')$ have a disjoint set of colors. Then any two executions $\alpha, \alpha' \in \alpha(B, b)$, with $input_A(\alpha) \neq input_A(\alpha')$, are distinguishable to B. Therefore P_A is an informative protocol. □

This theorem explains what B learns, formally defined by the notion of decision function from distributed computing [17]. A *decision function* δ_B consists of a function for B, where $\delta_B(\alpha)$ is the value that B decides in execution α. Clearly, if P_A is informative for B then there is a function δ_B, such that $\delta_B(\alpha) = input_A(\alpha)$.

Notice that, it follows from Theorem 1 that the protocol represented in Figure 2.3 is informative for the Russian Cards problem with signature $(2, 1, 1)$, $\mathbf{r} = 0$ or $(2, 1, 0)$, $\mathbf{r} = 1$, since it is a proper coloring of $J(4, 2)$.

Recall from Section 2.2.1 the graph $\mathcal{G}_C$, which is equivalent to the graph $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$, where $K_p(\bar{c})$ induces a clique, for every $c \in \mathscr{P}_{\mathbf{c}}(D)$. In the following, the set of messages or colors of the vertices of a clique $K_p(\bar{c})$ is denoted by:

$$P_A(K_p(\bar{c})) = \bigcup_{a \in K_p(\bar{c})} P_A(a)$$

Theorem 2 (Safety characterization)**.** *Let $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$ be a protocol, then the following conditions are equivalent.*

1. *P_A is safe.*
2. *Consider any $c \in \mathscr{P}_{\mathbf{c}}(D)$, and any $y \in \bar{c}$. For each $M \in P_A(K_p(\bar{c}))$, there are $a, a' \in K_p(\bar{c})$ with $M \in P_A(a) \cap P_A(a')$ such that $y \in a \triangle a'$ [5].*

Proof. (1) $\Rightarrow$ (2). Let P_A be a safe protocol. Then, for any $c \in \mathscr{P}_{\mathbf{c}}(D)$ and any $M \in P_A(K_p(\bar{c}))$, consider any card $y \in \bar{c}$ and an execution $\alpha \in \alpha(C, c)$ starting with $I = \{(A, a), (B, b), (C, c)\}$, in which A announces M ($M \in P_A(a)$). There are two possible cases, $y \in input_A(\alpha)$ and $y \notin input_A(\alpha)$.

- If $y \in input_A(\alpha)$, then as P_A is safe there exists an execution α' such that $y \in input_B(\alpha')$ and $\alpha \overset{C}{\sim} \alpha'$. It follows that $M \in P_A(input_A(\alpha)) \cap P_A(input_A(\alpha'))$ and $y \in input_A(\alpha) \triangle input_A(\alpha')$.
- If $y \notin input_A(\alpha)$, as $y \in \bar{c}$ then there exists an execution α' starting with input $I' = \{(A, a), (B, b'), (C, c)\}$ such that $y \in input_B(\alpha')$, and it holds $\alpha \overset{C}{\sim} \alpha'$. As P_A is safe, then there exists an execution α'' such that $y \in input_A(\alpha'')$ and $\alpha' \overset{C}{\sim} \alpha''$. It follows that $M \in P_A(input_A(\alpha)) \cap P_A(input_A(\alpha''))$ and $y \in input_A(\alpha) \triangle input_A(\alpha'')$.

(2) $\Leftarrow$ (1). Assume that for any $c \in \mathscr{P}_{\mathbf{c}}(D)$, any card $y \in \bar{c}$ and any message $M \in P_A(K_p(\bar{c}))$, there exists $a_1, a_2 \in K_p(\bar{c})$ with $M \in P_A(a) \cap P_A(a')$ such that $y \in a_1 \triangle a_2$.

[5] The symbol $\triangle$ stands for the symmetric difference operator.

Now let be c a $\mathbf{c}$-set and $\alpha \in \alpha(C,c)$ an execution, where the card x is held by A, and the card y is held by B. For any $M' \in P_A(K_p(\bar{c}))$, there must be an $\mathbf{a}$-set $a \in K_p(\bar{c})$ where $M' \in P_A(a) \cap P_A(input_A(\alpha))$ and $y \in a$, so, for any facet I with the vertices (C,c) and (A,a), there is an execution $\alpha_1 \in \alpha(I)$ such that $y \in input_A(\alpha_1)$ and $\alpha \overset{C}{\sim} \alpha_1$. There must be also an $a' \in K_p(\bar{c})$ with $M' \in P_A(a') \cap P_A(input_A(\alpha))$ and $x \notin a'$. As $x \in \bar{c}$, there is an execution $\alpha_2 \in \alpha(C,c)$, with $input_A(\alpha_2) = a'$ and $x \in input_B(\alpha_2)$, which also satisfies that $\alpha \overset{C}{\sim} \alpha_2$. Thus, P_A is safe. □

Following [23], we say that a non-deterministic one-step protocol is an γ-equitable protocol if $|P_A(a)| = \gamma$ for all $a \in \mathscr{P}_{\mathbf{a}}(D)$. Deterministic one-step protocols are equivalent to 1-equitable protocols.

2.2.3 Some consequences of the characterizations

Some observations regarding the informative and safety reformulations are the following:

Remark 2 (Communication Complexity)**.** *A simple consequence of the informative characterization for a one-step protocol, $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$ (Theorem 2), is that $|\mathcal{M}_A| \geq \chi(J^{\mathbf{c}+\mathbf{r}}(n,\mathbf{a}))$* [6]*. Then, $\chi(J^{\mathbf{c}+\mathbf{r}}(n,\mathbf{a}))$ is a lower bound on the* communication complexity *of the one-step protocol P_A.*

Remark 3 (Duality)**.** *Since $J^{\mathbf{c}+\mathbf{r}}(n,\mathbf{a}) \cong J^{\mathbf{c}+\mathbf{r}}(n,n-\mathbf{a})$*[7]*, there is an informative one-step protocol P_A for $(\mathbf{a},\mathbf{b},\mathbf{c})$ if and only if $\bar{P}_A(a) = P_A(\bar{a})$ is an informative one-step protocol for $(n-\mathbf{a},\mathbf{a}-(\mathbf{c}+\mathbf{r}),\mathbf{c})$.*

Remark 4. *If $d \leq d'$, then $J^d(n,\mathbf{a})$ is a subgraph of $J^{d'}(n,\mathbf{a})$ (Remark 1). Thus, if P_A is a proper vertex coloring of $J^{d'}(n,\mathbf{a})$ then it is also a proper vertex coloring of $J^d(n,\mathbf{a})$ (similarly, for $n \leq n'$).*

Remark 5 (Safety)**.** *Being Informative requires P_A to be a proper vertex coloring of $J^{\mathbf{c}+\mathbf{r}}(n,\mathbf{a})$, while safety requires that P_A is not a proper vertex*

[6] The notation $\chi(G)$ stands for the *chromatic number* of the graph G.

[7] This holds by [19, Lemma 3], and the isomorphism is the function $f : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}_{n-\mathbf{a}}(D)$ defined as $f(a) = \bar{a}$.

coloring of $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$. Thus, by Remark 1, if a protocol is informative and safe, then $\mathbf{b} > \mathbf{c}$.

2.2.4 One-step protocol example

When $\mathbf{c} + \mathbf{r} = 1$, an example of solution for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ is the one-step protocol χ_{modn}, where A announces the sums of her cards modulo n. This protocol is presented in [6, 19]. Formally, the protocol is the function $\chi_{modn} : \mathscr{P}_{\mathbf{a}}(D) \to \mathbb{Z}_n$, defined as:

$$\chi_{modn}(x) = (\sum_{y \in x} y) \mod n$$

For example, in the classic instance of the Russian Cards problem, $(3, 3, 1)$ with $n = 7$, the protocol is specified by the following announcements:

$$\begin{aligned}
\chi^{-1}_{mod7}(0) &= \{016, 025, 034, 124, 356\} \\
\chi^{-1}_{mod7}(1) &= \{026, 035, 125, 134, 456\} \\
\chi^{-1}_{mod7}(2) &= \{036, 045, 126, 135, 234\} \\
\chi^{-1}_{mod7}(3) &= \{012, 046, 136, 145, 235\} \\
\chi^{-1}_{mod7}(4) &= \{013, 056, 146, 236, 245\} \\
\chi^{-1}_{mod7}(5) &= \{014, 023, 156, 246, 345\} \\
\chi^{-1}_{mod7}(6) &= \{015, 024, 123, 256, 346\}
\end{aligned}$$

2.3 Two-step protocols

In the previous sections, we formally presented the Russian Cards problem in its most general form. Additionally, we presented some general results regarding one-step protocols. In this section, we study more closely two-step protocols for solving the problem. As we mentioned earlier, two-step protocols have not been rigorously studied in the more general Russian Cards scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, so most of the formulations and results presented in this chapter are novel.

In particular, it is well known that in the generalized scenario with $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$, the existence of an informative and safe one-step protocol is equivalent to the existence of an informative and safe two-step protocol, in which B's announcement is trivially safe in the sense that it does not give C any new information. However, when $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, although, as we will see in Section 2.3.1, the existence of a two-step solution does mean a one-step solution for the particular problem instance, we will see in sections 2.3.2 and 2.3.3 that the implication in the other way does not hold.

2.3.1 One-step protocols for two-step solutions

It is straightforward that when $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$, the existence of an informative and safe one-step protocol P_A for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ is a necessary condition for the existence of a two-step solution for the same problem instance. As the following theorem states, this can be generalized also for the case where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$.

Theorem 3. *When $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, if there is an informative and safe two-step protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, then there is a one-step protocol P_A for the same problem instance, which is informative for B and safe.*

Proof. Consider a two-step informative and safe protocol $\rho = (P_A, P_B)$. Since ρ is informative, it is straightforward that P_A is informative for B. Consider for P_A an execution $\alpha \in \alpha(C, c)$ and any cards x, y such that $x \in input_A(\alpha)$ and $y \in input_B(\alpha)$. Now consider the execution $\beta \in \alpha(C, c)$ for protocol (P_A, P_B) starting with the same inputs as α. As (P_A, P_B) is safe, there exist executions $\beta_1, \beta_2 \in \alpha(C, c)$ such that $x \in input_B(\beta_1)$, $y \in input_A(\beta_2)$, $\beta \overset{C}{\sim} \beta_1$ and $\beta \overset{C}{\sim} \beta_2$. The executions $\alpha_1, \alpha_2 \in \alpha(C, c)$ for P_A with same input that β_1 and β_2 respectively, satisfy that $x \in input_B(\alpha_1)$, $y \in input_A(\alpha_2)$, $\alpha \overset{C}{\sim} \alpha_1$ and $\alpha \overset{C}{\sim} \alpha_2$ hence P_A is safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$. □

Moreover, in a two-step solution (P_A, P_B) for a specific problem instance with $\mathbf{r} = 0$, if the protocol P_A is informative for B and safe, one may assume that P_B consists in announcing C's hand. Notice that, since the protocol P_A is informative for B, B knows A's hand after her announcement, and hence he can deduce the cards of C. Thus, after B's announcement of C's hand, A can also deduce the cards from B's hand. Thus, this strategy is an informative two-step solution. Additionally, this is also safe since C does not learn anything new from B's announcement. Therefore, it is clear that when $\mathbf{r} = 0$, the existence of an informative and safe one-step protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ is not only a necessary condition, but additionally, a sufficient condition for the existence of a two-step solution for the specific problem instance. In the following sections we show that, unlike in the case when $\mathbf{r} = 0$, if we have that $\mathbf{r} > 0$, this last result cannot be generalized. That is, the existence of informative and safe one-step protocols for a problem instance is not a sufficient condition for the existence of two-step solutions.

However, if only informativeness is needed in a two-step protocol, the following theorem is straightforward.

Theorem 4. *An informative two-step protocol (P_A, P_B) exists if P_A is informative for B; and $|\mathcal{M}_B| >= \binom{n-\mathbf{a}}{\mathbf{b}}$, where $\mathcal{M}_B$ is the domain of messages for P_B.*

Proof. When A has input a, the hands that she considers possible for B are all the hands in $\mathscr{P}_{\mathbf{b}}(D - a)$. There are a total of $\binom{n-\mathbf{a}}{\mathbf{b}}$ such hands. Now, consider an informative protocol P_A. After A announces a message M, based on her input a, B knows a. Assume a pre-agreed order on the possible hands for B from A's perspective, so that they are referred to by the integers $1, \ldots, \binom{n-\mathbf{a}}{\mathbf{b}}$. Thus, we may define a protocol P_B by $P_B(b, M) = i$, where i is the index of B's hand in $\mathscr{P}_{\mathbf{b}}(D - a)$. The protocol P_B is informative and sends $\binom{n-\mathbf{a}}{\mathbf{b}}$ different messages, which is optimal for an informative two-step protocol. □

2.3.2 Perfectly safe response strategies

In this section, we have the intention to address what we think is an important difference between the generalized Russian Cards problem, as stated originally, and the more general form where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$.

It is well known that, when $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$, B's response strategy in two-step safe protocols may consist in announcing C's hand. The argument behind this claim is simple: it is because this announcement does not give C any new information. In other words, this means that, C could infer B's message even before hearing his announcement, only from her knowledge of the protocol and A's announcement. This observation also implies that in such cases, B's response protocol needs to be deterministic.

Thus, in fact, we could say that in such cases B's response protocol is *perfectly secure* in the strongest possible sense. This is, from C's perspective, the probability of A or B holding any set of cards, is exactly the same before and after B's announcement. Hence, for any informative and safe one-step protocol P_A, such a perfect secure response strategy would translate into a safe two-step protocol. Since we are interested in studying this particular kind of two-step protocols, we present the following definition in order to make this notion precise.

Definition 4 (Perfectly safe response). *Let (C, c) be any C-vertex of $\mathcal{I}$ and P_A be a one-step protocol. A response protocol P_B is* perfectly safe *with respect to P_A if for any two executions α, α' of the protocol P_A, with $\alpha, \alpha' \in \alpha(C, c)$ and $\alpha \overset{C}{\sim} \alpha'$, it holds that $P_B(input_B(\alpha), M) = P_B(input_B(\alpha'), M)$, for any $M \in P_A(input_A(\alpha))$.*

Intuitively, the previous definition states that a response protocol P_B is perfectly safe with respect to a one-step protocol P_A if any two scenarios indistinguishable to C after A's announcement according to P_A are still indistinguishable after B's announcement according to P_B.

Theorem 5. *When $\mathbf{r} > 0$, there is no two-step protocol (P_A, P_B) for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, where P_B is perfectly safe with respect to P_A and informative for A.*

Proof. Consider a two-step protocol (P_A, P_B), with P_B being perfectly safe with respect to P_A. Given that $\mathbf{r} > 0$, there are two facets in $\mathcal{I}$ (and corresponding deals), $I = \{(A, a), (B, b), (C, c)\}$ and $I' = \{(A, a), (B, b'), (C, c)\}$, with $b \neq b'$. Thus, there are two P_A executions $\alpha \in \alpha(I)$ and $\alpha' \in \alpha(I')$, and therefore $\alpha, \alpha' \in \alpha(C, c)$, such that $\alpha \overset{C}{\sim} \alpha'$. Now, since P_B is a perfectly safe with respect to P_A, it holds that $P_B(input_B(\alpha), M) = P_B(input_B(\alpha'), M)$ for any $M \in P_A(a)$. But then, P_B is not informative for A, since there are two

P_B executions in $\alpha(A, a)$ with different inputs for B, namely b and b', that are indistinguishable to A. □

Notice that for the previous result there is no assumption about the one-step protocol used for A's announcement, hence it does not matter whether this is an informative protocol or not. This means that, when $\mathbf{r} > 0$, if a two-step protocol is informative for A, then it always allows C to learn something from B's announcement. This is an important result because this means that, unlike in the case $\mathbf{r} = 0$, we cannot assume that designing an informative and safe one-step protocol for A's announcement means solving the problem of full-information exchange in the more general scenario where $\mathbf{r} > 0$. In these cases we must always consider what C learns from B's announcement in order to check that this new knowledge does not compromise the safety of the communication protocol or strategy.

Moreover, when $\mathbf{r} > 0$ the *trivially informative* response from B would be to announce all cards that both, he and A does not hold, which are those from C's hand and the ones not dealt to anyone. However, this is not a perfectly safe response protocol, neither would mean a secure two-step protocol, according to the informal safety formulation 2, because C will learn the fate of all the $\mathbf{r}$ cards that were not dealt. However, since our safety Definition 2 allows C to learn the fate of the cards that were not dealt, we cannot discard this response strategy yet, as it may translate into a two-step solution.

2.3.3 On the existence of two-step solutions

As seen in the previous section, when $\mathbf{r} > 0$, one may think that in a two-step solution (P_A, P_B), the response protocol P_B, could consist in announcing the set of cards not held by A nor B, which is a superset of C's hand. In the following, we may regard this particular kind of response protocol as *trivially informative*, and will be denoted by P_B^*.

The following theorem states a necessary and sufficient condition for a two-step protocol with trivially informative response to be a solution in the general Russian Cards scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$.

Theorem 6. *Let $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, then a two-step protocol (P_A, P_B^*) is informative and safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ if and only if P_A is an informative and safe one-step protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c} + \mathbf{r})$.*

Proof. Is straightforward that (P_A, P_B^*) is informative if and only if P_A is informative, so we are going to focus here on safety.

If (P_A, P_B^*) is safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, since B's announcement reveal the fate of the $\mathbf{r}$ remaining cards, after hearing both messages C can assume the role of a player containing $\mathbf{c} + \mathbf{r}$ cards, and still cannot learn any of the cards of either A or B. Then, if C initially held the $\mathbf{c} + \mathbf{r}$ cards, he could not either learn any card of A or B after hearing only A's announcement. Thus, P_A is safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c} + \mathbf{r})$.

If P_A is safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c}+\mathbf{r})$, then (P_A, P_B^*) is safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c}+\mathbf{r})$, because B announces exactly the cards that C holds, and this do not give to C any new information. Hence, (P_A, P_B^*) is also safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, because in this case C has even less information that in the previous case. □

The previous result means that if we want to consider the problem of information exchange in the Russian Cards scenario where $n = \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{r}$ different from the case with $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$, we need to design a response strategy for B apart from the trivially informative one.

The following result indicates that, when $\mathbf{r} > 0$, although there may be safe and informative one-step protocols for a problem instance $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, it could be the case that no safe and informative two-step protocol exists for the same problem instance.

Theorem 7. *There is no a safe and informative two-step protocol for $(2, 1, 0)$, with $\mathbf{r} = 1$.*

Proof. For an informative protocol P_A of this problem instance, it holds that $|\mathcal{M}_A| \geq 3$, because for any $b \in \mathscr{P}_1(D)$ the clique $K_p(\bar{b})$ has size 3. Given a safe protocol P_A of this problem instance, for any $M \in \mathcal{M}_A$ it holds that $|P_A^{-1}(M)| \geq 2$. Since $|\mathscr{P}_2(D)| = 6$, combining previous results, in a safe an informative protocol P_A for this instance, $|\mathcal{M}_A| = 3$, and for any $M \in \mathcal{M}_A$ it holds that $|P_A^{-1}(M)| = 2$. Indeed, for this instance, any safe and informative protocol is equivalent to the following one:

$$P_A^{-1}[0] = \{01, 23\} \quad P_A^{-1}[1] = \{02, 13\} \quad P_A^{-1}[2] = \{03, 12\}$$

Assume for contradiction that there is a protocol P_B such that (P_A, P_B) is informative and safe. Then, since P_B is informative for A, the executions $\alpha = \alpha(\{(A, 01), (B, 2), (C, \emptyset)\})$ and $\alpha' = \alpha(\{(A, 01), (B, 3), (C, \emptyset)\})$ must be distinguishable to A, hence $P_B(0, 2) \neq P_B(0, 3)$. Similarly, $P_B(0, 0) \neq P_B(0, 1)$. Since the protocol is safe, according to Definition 2 there must be two executions α_1, α_2 such that $\alpha \overset{C}{\sim} \alpha_1$, $\alpha \overset{C}{\sim} \alpha_2$, $0 \in \mathit{input}_B(\alpha_1)$ and $1 \in \mathit{input}_B(\alpha_2)$, but this is clearly impossible, given that $P_B(0, 0) \neq P_B(0, 1)$. Thus, this is a contradiction with (P_A, P_B) being safe. □

Thus, the previous result confirms that, unlike in the case when $\mathbf{r} = 0$, if we have that $\mathbf{r} > 0$ the existence of informative and safe one-step protocols for a problem instance is not a sufficient condition for the existence of two-step solutions.

Chapter 3

Communication complexity bounds for known solutions

So far, we have presented the modeling of solutions to the Russian Cards problem in the form of informative and safe *protocols*. In particular, solutions to the problem of information transmission, i.e. one-step protocols, can be seen as a collection of predefined *announcements*. In other words, a one-step protocol $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathscr{P}^*(\mathcal{M}_A)$, can also be regarded as the following set of announcements[1]:

$$\left\{P_A^{-1}(M) \mid M \in \mathcal{M}_A\right\}$$

Hence, the approach we have presented is analogous to those approaches in which a solution is modeled as a predefined set of (possible) announcements. Therefore, our approach is reminiscent of those from [19, 23]. However, there are other works on Russian Cards problems [3, 2], in which the authors define solutions to have the form of an announcement. Hence, in such works, the formulations of the informative and safety requirements do not focus on protocols, unlike ours do, but rather on individual announcements. An announcement satisfying such formulations is then said to be a *good announcement* and, consequently, it is regarded as a solution to the

[1] Recall that, for a protocol P_A, $P_A^{-1}(M) = \{a \mid M \in P_A(a)\}$, denotes the announcement corresponding to a message M.

problem. About such approach, the authors in [23] argue that "*it is not possible to formally define or discuss the security of a scheme using definitions that focus on individual announcements*".

Motivated by this claim, one of our goals for this chapter is to argue that this approach that focuses on announcements is indeed valid, at least when considering weak-1-secure solutions. To that effect, we first present this approach in Section 3.1 and discuss how it is comparable to our own approach and those from [19, 23]. We say that this approach is valid in the sense that, as we will see in Section 3.2, it could in fact lead, in a straightforward manner, to the construction of an informative and safe protocol, which would be compatible with our definition of what a solution to the problem is. Furthermore, in Section 3.3, we consider alternative ways in which an announcement could be translated into such solution, namely via different possible encodings. Additionally, we also discuss the communication complexity that such solutions might have.

3.1 Announcements and protocols

In this section, we present the approach from [2, 3] to solutions for the generalized Russian Cards problem. Since in these works the authors only consider the scenario where $n = \mathbf{a}+\mathbf{b}+\mathbf{c}$, they focus only on formalizing the problem of information transmission. Recall that in such scenario this would mean also a solution to the problem of information exchange with B announcing C's hand. Additionally, recall that, as shown in [10], any message from A can be modeled as the action of publicly announcing that she holds an $\mathbf{a}$-set from a set L of alternative hands, which is regarded as an announcement. In other words, an announcement is a non-empty subset of $\mathscr{P}_{\mathbf{a}}(D)$. In light of this, the authors regard solutions to the problem as a special kind of announcements. We say that an $\mathbf{a}$-set Y, maybe from an announcement L, avoids the set X if the sets X and Y are disjoint.

According to the formalism from [3, 2], an announcement L is said to be a *good announcement* for parameters $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ with $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$, if the following three axioms or properties hold:

CA1. For every $\mathbf{b}$-set X there is at most one member of L that avoids X.

CA2. For every $\mathbf{c}$-set X the members of L avoiding X have empty intersection.

CA3. For every $\mathbf{c}$-set X the members of L avoiding X have union consisting of all cards except those of X.

Then, the authors propose solutions to a particular problem instance $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$, by showing that a good announcement exists for such parameters.

These properties, considering that the actual hand of A is contained in L, guarantee that the announcement L solves the specific instance of the problem, even in the more general Russian Cards scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$.

The first property, **CA1**, is somehow related to Definition 1, at the level of a color class of a protocol, and only considering executions where A's hand is in L. For any $b \in \mathscr{P}_{\mathbf{b}}(D)$, if A's hand is the $\mathbf{a}$-set a contained in L, then a is the only member in L that avoids b, and there is not another execution indistinguishable to B in which A announces L. Therefore, from now on, we will refer to this axiom as the *informative announcement* property. To see this relation more clearly, we can rephrase **CA1** in the formalism from Section 2.2.1 as follows:

CA1x. For every $\mathbf{b}$-set X there is at most one member of (the color class) L in the clique $K_p(\bar{X})$ of $J^{c+r}(n, \mathbf{a})$.

Thus, an informative one-step protocol P_A, i.e., satisfying Theorem 1, would consist of a set of announcements all satisfying **CA1**.

For the case of both axioms **CA2** and **CA3**, they deal with the safety requirements for weak 1-security, which at the protocol level can be defined as in Theorem 2. Both axioms together can be rephrased in the formalism from Section 2.2.1 as follows:

CA2xCA3. For every $\mathbf{c}$-set X the members of L in the clique $K_p(\bar{X})$ of $J^{b+r}(n, \mathbf{a})$ have empty intersection and its union is $\bar{X}$.

Again, we can see that a *safe* protocol P_A, i.e., satisfying Theorem 2, would consist of a set of announcements all satisfying **CA2** and **CA3**.

Thus, for a protocol P_A to be *informative* and *safe*, we require that the induced color classes, or announcements, all satisfy **CA1**, **CA2** and **CA3**. This is, a protocol P_A is *informative* and *safe* if for any $M \in \mathcal{M}_A$ the announcement $P_A^{-1}(M)$ is a *good announcement*.

The following are examples of *good announcements* for $(3, 3, 1)$:

$$L_1 = \{013, 124, 235, 346, 045, 156, 026\}$$

$$L_2 = \{256, 035, 136, 046, 012, 145, 234\}$$

$$L_3 = \{014, 123, 246, 345, 036, 156, 025\}$$

Notice that even when these announcements are not disjoint sets (156 is in L_1 and L_3) and therefore cannot be part of a deterministic protocol, whenever A can announce $L \in \{L_1, L_2, L_3\}$, B would know A's hand after L, while C won't be able to tell any of A's cards nor B's.

Thus, for what we have seen so far, these *good announcements* only seem to be a solution *whenever A can announce* one of these, i.e., when it is the case that the actual hand of A is in the announcement L. Thus, for considering this approach for solving the problem, according to the notion of protocol from Section 2.1.1, we might need to assume that such *good announcements* exists for every possible hand of A; namely, that A can always make a *good announcement*, no matter which her actual hand is. However, about this matter, the authors in [23] point that: "*No assumption is made that, for every possible hand for Alice, an announcement is defined, or that a good announcement even exists*".

Indeed, such assumption is never explicitly made by the authors in [2], but we believe that in fact the constructions they propose for *good announcements* are not limited for some possible hands of A. The reason behind this is that, as we will see in the next section, a single good announcement can be easily transformed in a different good announcement for the same parameters by simply renaming the cards. In lights of this, we could always obtain a good announcement containing a specific hand, from any good announcement for the same parameters. This idea is also used in [11] for building a one-step protocol for $(4, 4, 2)$ from an individual announcement for these parameters.

3.2 From good announcements to protocols

As we discussed, a good announcement L helps to solve the problem when A's hand is contained in the announcement, and it is a good question whether this helps or not to solve the problem in other cases. In this section we propose a method for building a safe and informative one-step protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, starting from an already known good announcement L for the same parameters, which we regard as a *seed announcement* for this method.

The following is a method for obtaining a good announcement L' for parameters $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, with $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, containing an arbitrary $\mathbf{a}$-set, h. For this, we assume that we have a seed announcement L. The procedure is the following:

Announcement re-arrangement

1. If $h \in L$, then $L' = L$ and we are done.
2. Else,
   - Choose an arbitrary $\mathbf{a}$-set, h', from L.
   - Build any bijective endofunction f on D which transforms the cards in h' into the cards in h.
   - Define a bijective endofunction $f_{\mathbf{a}}$ for $\mathscr{P}_{\mathbf{a}}(D)$, such that for any $a \in \mathscr{P}_{\mathbf{a}}(D)$, $f_{\mathbf{a}}(a) = \{f(x) | x \in a\}$.
   - Let L' be the collection that results from the transformation of every $\mathbf{a}$-set in L according to $f_{\mathbf{a}}$, i.e. $L' = \{f_{\mathbf{a}}(X) | X \in L\}$.

Notice that the function f is simply a *card renaming function* or permutation of the cards, so for any k with $1 \leq k \leq n$, the function f_k that for any $X \in \mathscr{P}_k(D)$ is defined as $f_k(X) = \{f(x) \mid x \in X\}$, is also a bijective endofunction. Thus, $f_{\mathbf{a}}$ transforms $\mathbf{a}$-sets into $\mathbf{a}$-sets, and it is clear by the specification of the function f that the hand $h = f_{\mathbf{a}}(h')$ and therefore, $h \in L'$. Now we prove that L' is a good announcement.

Lemma 2. *The announcement L' obtained by an* announcement re-arrangement *is a good announcement.*

Proof. Since L is a good announcement, the axioms **CA1**, **CA2** and **CA3** hold for L. Assume for contradiction that **CA1** does not hold for L'. Thus, there is a **b**-set b such that at least two members in L' avoids Y. Let a_1 and a_2 be two of the hands in L' that are disjoint with b. Then, by the specification of the functions $f_{\mathbf{a}}$ and $f_{\mathbf{b}}$, we have that $f_{\mathbf{a}}^{-1}(a_1)$ and $f_{\mathbf{a}}^{-1}(a_2)$ are both different **a**-sets in L, avoiding the **b**-set $f_{\mathbf{b}}^{-1}(b)$, and this contradicts the fact that L is a good announcement.

In a similar way, we can prove that **CA2** and **CA3** also holds for L'. Thus, L' is a good announcement. □

As an example, consider that we want to find a good announcement for $(3, 3, 1)$ that contains the hand $\{2, 5, 6\}$, and that we already know the announcement L_1 from the previous section. Then, using the announcement re-arrangement method with the endofunction f defined in Table 3.1, we obtain the announcement L_2 (also from previous section), which contains the desired hand, and is a good announcement.

D	0	1	2	3	4	5	6
f	2	5	3	6	0	1	4

Table 3.1: Example of endofunction on D

The repetition of the previous method allows the construction of a general solution for the $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ instance of the Russian cards problem in the form of a *non-deterministic one-step protocol*. To that effect, we can repeat this procedure using different card renaming functions until every **a**-set not contained in L appears in at least one of the generated announcements.

It is important to notice that once this method results in a collection of good announcements which are not disjoint, the corresponding strategy or protocol might be non-deterministic. If there is a hand h contained in more than one announcement and we try to turn the protocol into a deterministic one by fixing the announcement i whenever A holds h, we might compromise the security of the protocol. That is, when A's hand is a, it needs to be possible that A announces any of the announcements that contains a. Otherwise, if there exists an announcement L' that contains a and is never announced by A when she has a, C can discard the hand a from the possibilities in L'. This could cause that **CA2** or **CA3** not longer holds for L'.

As an example of a non-deterministic protocol obtained by the previous method, we present the following solution for $(3, 3, 1)$, where the announcements from L_2 to L_7, were obtained from the seed announcement L_1 using the announcement re-arrangement method.

$$L_1 = \{013, 124, 235, 346, 045, 156, 026\}$$

$$L_2 = \{256, 035, 136, 046, 012, 145, 234\}$$

$$L_3 = \{014, 123, 246, 345, 036, 156, 025\}$$

$$L_4 = \{015, 126, 245, 356, 046, 134, 023\}$$

$$L_5 = \{016, 124, 346, 256, 023, 135, 045\}$$

$$L_6 = \{024, 056, 125, 236, 614, 130, 345\}$$

$$L_7 = \{043, 456, 531, 362, 610, 124, 025\}$$

This strategy for building an good announcement L', containing a specific hand, from a seed announcement L, is reminiscent of [11, Definition 2]. Here, the authors also use this announcement re-arrangement method for defining a one-step protocol. In their approach A may announce any L' containing her hand, obtained from a seed announcement via the re-arrangement method. That is, for any of the $n!$ possible renamings of the cards, there is a corresponding announcement in the protocol, that could be made. In their approach, the selection of h' and definition of f in a random manner is important; determinism for these steps could compromise safety. On the other hand, in our approach we might not need all the $n!$ announcements. Instead we define a one-step protocol by selecting a subset of these announcements, that represent a covering of all elements in $\mathscr{P}_{\mathbf{a}}(D)$.

So far we have seen how the announcement re-arrangement method can be used in order to obtain a new good announcement from a previously known one, or more generally, to obtain a protocol for a specific instance of the Russian Cards problem. From now on we will refer to an announcement or protocol generated by this method as a *re-arrangement generated announcement* or a *re-arrangement generated protocol*, respectively. The following theorem is straightforward considering the Definitions 1 and 2 and Lemma 2.

Theorem 8. *Given a good announcement L, any re-arrangement generated protocol obtained from L is an informative and safe non-deterministic one-step protocol.*

We can address now what the authors in [23] argue about the approach presented in [2]: "$(\ldots)$*the authors treat security on the announcement level (...) we argue that it is not possible to formally define or discuss the security of a scheme using definitions that focus on individual announcements.*"

Indeed, as we already discussed, in [2] the authors treat security on the announcement level. However, as it happens with our own formulation for the safety requirement, in [23], the authors' formulation of weak-1 security is equivalent to the requirement that **CA2** and **CA3** both hold for every announcement in the protocol or strategy. Thus, under the assumption that a good announcement does exist for any possible hand for A, these formal definition of security are in fact equivalent. Moreover, as we discussed, it is always safe to make the assumption that a good announcement for every possible hand exists, as long as a good announcement exists for the specific problem instance. What this means is that, both approaches are valid and the constructions that the authors in [2] proposed of good announcements for various problem instances represent indeed formal solutions, although, maybe in the form of non-deterministic protocols.

3.3 Complexity discussion

In this section we continue our discussion regarding the relation between the approach that focus on announcements and those, like our own, that focus on protocols. However, as we already saw that both approaches were valid for obtaining solutions to the Russian Cards problem, we now consider these approaches from the perspective of communication complexity.

Recall that, for the Russian Cards problem with signature $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, having a one-step protocol $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}_A$, A needs to transmit $\lceil \log_2(|\mathcal{M}_A|) \rceil$ bits for encoding her announcement. However, as discussed in the previous section, in the approach from [2] the problem can be solved instead with A communicating any good announcement, containing her hand, for the proper parameters. We already discussed why this is valid in terms of the informative and safety requirements, however, this alternative requires a different announcement encoding strategy and therefore differs from ours in terms of communication complexity.

Encoding announcements. In the following list, we describe several strategies for the encoding of A's announcement L', with $|L'| = k$. We regard these as *announcement encodings*. For the last element of the list we consider a good announcement L to be of public knowledge among the players, which A uses to build her announcement L', as a re-arrangement of L. We also describe how many bits are required for each encoding.

1. A may communicate L' as a list of $k \times \mathbf{a}$ integers in the range from 0 to $n - 1$. This encoding uses $k \times \mathbf{a} \times \lceil \log_2 n \rceil$ bits.
2. A may communicate a boolean array of size $\binom{n}{\mathbf{a}}$, where the i-th element in the array is true if and only if the i element of $\mathscr{P}_{\mathbf{a}}(D)$ is in L'. This encoding uses $\binom{n}{\mathbf{a}}$ bits.
3. A may communicate a single number, in the range from 0 to $n! - 1$, that represent the index of the function f used to build L', among all of the permutations of the cards. This encoding uses $\lceil \log_2(n!) \rceil$ bits.

We say that an encoding is more efficient than another one when it uses fewer bits than the other. We suspect that, in general, the encoding 3 is more efficient than the first two. This is because all announcement re-arrangements of a commonly known good announcement L conform a subset of all good announcements for the given parameters. This means that in this last case the number of elements that we will need to encode is at most the number of elements that we will need to encode in the first two cases. Although this reasoning is intuitive, in the following lemma we provide a formal proof.

Lemma 3. *The announcement encoding 3 is more efficient than the announcement encodings 1 and 2.*

Proof. By [2, Proposition 1], the numbers of hands in a good announcement is at least $n \times (\mathbf{c}+1)/\mathbf{a}$. Thus,

$$k \times \mathbf{a} \times \lceil \log_2 n \rceil \geq (\frac{n \times (\mathbf{c}+1)}{\mathbf{a}}) \times \mathbf{a} \times \lceil \log_2 n \rceil \geq n \times (\mathbf{c}+1) \times \log_2 n =$$

$$(\mathbf{c}+1) \times \sum_{i=1}^{n} \log_2 n \geq (\mathbf{c}+1) \times \sum_{i=1}^{n} \log_2 i = (\mathbf{c}+1) \times \log_2(n!) \geq \lceil \log_2(n!) \rceil$$

This means that the encoding 1 uses at least the same amount of bits than the encoding 3.

For a good announcement to exist, it must hold that $2 \leq \mathbf{a} \leq n-2$ and that $n \geq 4$. Thus, $\binom{n}{\mathbf{a}} \geq \binom{n}{2} = n \times (n-1)/2$, and $n/2 \geq \log_2 n$. Thus,

$$\binom{n}{\mathbf{a}} \geq n \times (n-1)/2 \geq (n-1) \times \log_2 n > \log_2(n!) + 1 \geq \lceil \log_2(n!) \rceil$$

This means that the encoding 3 uses fewer bits than encoding 2. □

It is clear that for deterministic solutions, the approach that focuses on protocols is better from the perspective of communication complexity than the approach that focuses on announcements. This is because for a protocol $P_A : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}_A$, $|\mathcal{M}_A| \leq \binom{n}{\mathbf{a}}$ and $\binom{n}{\mathbf{a}} < n!$. Moreover, when considering the approach that focuses on announcements, in order to obtain a better solution from a communication complexity perspective, it is always better to obtain a protocol from a seed announcement as described in the previous section. This is because the resulting protocol for the described method will always have at most $\binom{n}{\mathbf{a}} < n!$ announcements.

Chapter 4

Informative protocols for the general problem

This chapter presents a general bound for the communication complexity of informative (not necessarily safe) protocols for the Russian Cards problem. To that effect, we exploit previous results from the field of Coding Theory. In Section 4.1, we discuss in detail the link between informative protocols for Russian Cards problems and the fundamental problem regarding binary constant weight codes, exposed in [19]. In particular, we describe how we can discover in the literature new informative protocols for the Russian Cards problem by reinterpreting some proofs from works on Coding Theory. Additionally, in Section 4.2, we use the ideas from [16, Section III], for presenting an informative one-step protocol, for the general Russian Cards problem. In other words, such protocol would be informative for any instance of the Russian Cards problem. For completeness, in Section 4.3 we also present the results from [19, Section 8]. Finally, in Section 4.4, we present an upper bound on the communication complexity of information transmission in the general Russian Cards scenario, using the previously presented results.

4.1 Constant weight codes and informative protocols

Coding Theory studies properties of codes and how they can be used for several applications. A *code* can be seen as a mapping of elements from a *source alphabet* to strings in a *target alphabet*, regarded as *codewords.* For a *binary* code, the target alphabet is the set $\{0, 1\}$, thus, the codewords are binary strings. We are interested in a particular kind of codes, regarded as *fixed length* codes, where all the codewords have the same length.

Among the applications of codes we can mention *data compression*, *cryptography*, *data transmission.* When data is transmitted over a noisy or unreliable channel, it is useful to detect and correct errors that may be introduced during the transmission. To that effect, it is convenient that any pair of codewords "differ" as much as possible, and for this purpose, a distance measure is used to compare codewords. A commonly used distance measure in codes of fixed length is the *Hamming distance*, where the distance of the codewords x, y, denoted as $d_H(x, y)$, is the number of positions where x and y differ. On the other hand, for a codeword x, its *Hamming weight* is the number of symbols different from 0, or equivalently, the Hamming distance to the codeword where all elements are 0, i.e., $d_H(x, \bar{0})$.

Constant weight codes (CWC), for parameters $(n, d, \mathbf{a})$, are fixed length codes, where all codewords have length n, minimum Hamming distance d and constant Hamming weight $\mathbf{a}$. Thus, in a binary CWC of length n and weight $\mathbf{a}$, every codeword is equivalent to a hand with $\mathbf{a}$ cards from a deck of n cards: the n elements in the codeword represent each card in the deck, and the $\mathbf{a}$ non zero bits in the codeword indicate the cards of the hand. Thus, a CWC of length n and weight $\mathbf{a}$ can be represented by a subset of vertices of the Johnson graph $J(n, \mathbf{a})$.

By Definition 3, for the graph $J^d(n, \mathbf{a})$, any adjacent vertices a and a' represent codewords of length n, weight $\mathbf{a}$ and distance $d_H(a, a') \leq 2d$. Similarly, any *not* adjacent vertices a and a' represent codewords of length n, weight $\mathbf{a}$ and distance $d_H(a,a') \geq 2d+2$. Thus, any independent set[1] of $J^d(n,\mathbf{a})$ is a CWC for parameters $(n, 2d+2, \mathbf{a})$.

The central problem regarding constant-weight codes is founding the maximum number of codewords in a binary constant-weight code with length n, Hamming distance d, and weight w. This number is denoted $A(n,d,w)$, and Johnson graphs have been used to calculate bounds on it.

The chromatic number of a graph $\mathcal{G}$, denoted as $\chi(\mathcal{G})$, is the minimum number of disjoint independent sets of $\mathcal{G}$, such that the union of all them is the graph $\mathcal{G}$. In other words, $\chi(\mathcal{G})$ is the smaller size of a partition of the graph $\mathcal{G}$, where any element is an independent set. This means, that $\chi(J^d(n,\mathbf{a}))$, is the minimum number of disjoint constant weight codes, for parameters $(n, 2d+2, \mathbf{a})$, which union is the set of all n-tuples of weight $\mathbf{a}$. Lets denote the elements of this partition as $C_1, \ldots, C_{\chi(J^d(n,\mathbf{a}))}$. Since each C_i denotes an CWC, we have that:

$$\max_{i \in \left\{1,\ldots,\chi(J^d(n,\mathbf{a}))\right\}} |C_i| \leq A(n, 2d+2, w)$$

But, is easy to check that

$$\frac{\binom{n}{\mathbf{a}}}{\chi(J^d(n,\mathbf{a}))} \leq \max_{i \in \left\{1,\ldots,\chi(J^d(n,\mathbf{a}))\right\}} |C_i|$$

Thus, we have the following lower bound for $A(n, 2d+2, w)$:

$$\frac{\binom{n}{\mathbf{a}}}{\chi(J^d(n,\mathbf{a}))} \leq A(n, 2d+2, w)$$

In general, determining the chromatic number of a Johnson graph is an open problem. Thus, in Coding Theory literature, there are some proofs that show a lower bound on $A(n, 2\delta, w)$ using the following idea:

1. Define a coloring function $\bar{\chi} : \mathscr{P}_{\mathbf{a}}(D) \to \mathcal{M}$ for $J^{\delta-1}(n,\mathbf{a})$
2. Show that $\bar{\chi}$ is a proper coloring. Then, $\chi(J^{\delta-1}(n,\mathbf{a})) \leq |\mathcal{M}|$.

[1] An independent set of a graph is subset of vertices of the graph, where no two of them are adjacent.

3. Finally, since $\frac{\binom{n}{\mathbf{a}}}{|\mathcal{M}|} \leq \frac{\binom{n}{\mathbf{a}}}{\chi(J^{\delta-1}(n,\mathbf{a}))}$, $\frac{\binom{n}{\mathbf{a}}}{|\mathcal{M}|}$ is a lower bound for $A(n, 2\delta, w)$, given that $\frac{\binom{n}{\mathbf{a}}}{\chi(J^{\delta-1}(n,\mathbf{a}))} \leq A(n, 2\delta, w)$.

4.2 Information transmission via sets with distinct sums

In Section 2.2.4, we presented an informative protocol for $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ with $\mathbf{c}+\mathbf{r} = 1$. In this protocol, which we regard as χ_{modn}, A announces the sum of her cards modulo n. Thus, χ_{modn} is an n-message protocol. However, it is not difficult to check that for the general case $\mathbf{c} + \mathbf{r} > 1$, χ_{modn} is not an informative protocol.

In this section, we re-use the proof of a bound on $A(n, 2 \times d + 2, \mathbf{a})$, for describing informative solutions when $\mathbf{c} + \mathbf{r} > 1$. In particular, here we use the results from [16, Section III].

Definition 5. *A subset $S = \{s_1, s_2, \ldots, s_n\}$ of $\mathbb{Z}_m$ is called an S_t-set of size n and modulus m, if all the sums $s_{i_1} + s_{i_2} + \ldots + s_{i_t}$ for $i_1 < i_2 < \ldots < i_t$ are distinct in $\mathbb{Z}_m$.*

Proposition 1. *When $t \leq (n+1)/2$, an S_t-set is also an S_u-set for any $u \leq t$.*

Proof. This can be proven in a kind of backward induction, that is: trivially it holds for $u = t$, so suppose that it holds for $u+1 \leq t$ and then try to prove it holds for u. Assume for contradiction that an S_{u+1}*-set* S exists, but it is not an S_u*-set*. This means that in S there are two u-sums, $s_{i_1} + s_{i_2} + \ldots + s_{i_u}$ and $s_{j_1} + s_{j_2} + \ldots + s_{j_u}$, that are equal in $\mathbb{Z}_m$. As $u + 1 \leq (n+1)/2$, there is an element $s' \in S$ that is not included in any of this two sums. Thus, adding s' to each of these sums, give us two different $(u+1)$-sums that are equal, a contradiction with S being an S_{u+1}*-set*. □

Let q be a prime power (positive integer power of a single prime number), then there is an S_d*-set* of size $q+1$ and modulus $m = (q^{d+1} - 1)/(q-1)$ [16, Theorem 8]. Thus, as long as $q+1 \geq n$ we can associate each card $i \in D$ with a unique element s_i of such set $S = \{s_0, s_1, \ldots, s_q\}$. This way, given such S_d*-set* S, we can define a protocol $\chi_{modm} : \mathscr{P}_{\mathbf{a}}(D) \to \mathbb{Z}_m$ as follows:

$$\chi_{modm}(a) = (\sum_{i \in a} s_i) \mod m$$

Recall that if $d \geq \min\{\mathbf{a}, n-\mathbf{a}\}$, then $J^d(n, \mathbf{a})$ is a complete graph, and therefore any informative protocol must be equivalent to an identity function. Thus, we only consider the case $d < \min\{\mathbf{a}, n-\mathbf{a}\}$. In this case, $d < n/2$, and given that $q+1 \geq n$, we also have that $d \leq (q+2)/2$.

Theorem 9. *χ_{modm} is a proper vertex coloring of $J^d(n, \mathbf{a})$, $1 \leq d \leq \min\{\mathbf{a}, n-\mathbf{a}\}$.*

Proof. Assume for contradiction that there are two adjacent vertices a, b of $J^d(n, \mathbf{a})$ which are equally colored, that is, $\chi_{modm}(a) = \chi_{modm}(b)$. Namely,

$$(\sum_{i \in a} s_i) \mod m = (\sum_{i \in b} s_i) \mod m.$$

As a and b are adjacent, they differ in $\gamma \leq d$ elements. Namely $\gamma = |a-b| = |b-a|$, and therefore:

$$(\sum_{i \in a-b} s_i) \mod m = (\sum_{i \in b-a})s_i \mod m.$$

This two sums have γ different elements from S, so this means S is not a S_γ*-set*, and therefore, by Proposition 1, this is a contradiction with S being an S_d*-set*, given that $\gamma \leq d \leq (q+2)/2$. □

4.3 Information transmission via Galois field

For completeness, we present in this section the results from [19, Section 8] and compare these with those from the previous section. For this, we rephrase the coding theory argument from [16, Theorem 4] in our notation.

Let q be a primer power, $q \geq n$. Let the elements of the Galois field $\mathrm{GF}(q)$ be $w_0, w_1, \ldots, w_{q-1}$. For a vertex a of $J^d(n, \mathbf{a})$, let $a_i = 1$ if $i \in a$, and else $a_i = 0$. Namely, for the following lemma we view a as a vector $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}^n_{\mathbf{a}}$. Define $\bar{\chi}(a)$ to be the vector $(\chi_1(a), \chi_2(a), \ldots, \chi_d(a))$,

$$\begin{aligned}
\chi_1(a) &= \sum_{a_{i_1}=1} w_{i_1}, \\
\chi_2(a) &= \sum_{\substack{i_1<i_2 \\ a_{i_1}=a_{i_2}=1}} w_{i_1} w_{i_2}, \\
\chi_3(a) &= \sum_{\substack{i_1<i_2<i_3 \\ a_{i_1}=a_{i_2}=a_{i_3}=1}} w_{i_1} w_{i_2} w_{i_3}, \\
&\cdots \\
\chi_d(a) &= \sum_{\substack{i_1<i_2<\ldots<i_d \\ a_{i_1}=a_{i_2}=\ldots=a_{i_d}=1}} w_{i_1} w_{i_2} \ldots w_{i_d},
\end{aligned} \tag{4.1}$$

Then, for $\vec{v} \in \mathrm{GF}(q)^d$, the set of vertices colored $\vec{v}$ is $\bar{\chi}^{-1}(\vec{v})$.

Recall that if $d \geq \min\{\mathbf{a}, n - \mathbf{a}\}$ then $J^d(n, \mathbf{a})$ is a complete graph.

Theorem 10. *$\bar{\chi}$ is a proper vertex coloring of $J^d(n, \mathbf{a})$, $d \geq 1$, and $d < \min\{\mathbf{a}, n - \mathbf{a}\}$.*

Proof. Consider two vertices a, b of $J^d(n, \mathbf{a})$ viewed as vectors of $\mathbb{F}^n_{\mathbf{a}}$, and such that $\bar{\chi}(a) = \bar{\chi}(b)$. Assume for contradiction that a and b are adjacent. Thus, there are 2γ distinct coordinates $r_1, \ldots, r_\gamma$, $s_1, \ldots, s_\gamma$, $\gamma \leq d$, where a and b disagree, and on all other coordinates they agree. Say, $a_{r_i} = 1$ while $b_{r_i} = 0$, and conversely, $a_{s_i} = 0$ while $b_{s_i} = 1$ $(1 \leq i \leq \gamma)$. Write $\alpha_i = w_{r_i}$, $\beta_i = w_{s_i}$ $(1 \leq i \leq \gamma)$. Since $\bar{\chi}(a) = \bar{\chi}(b)$ we have

$$\begin{aligned}
\sigma_1 &= \sum_i \alpha_i = \sum_i \beta_i \\
\sigma_2 &= \sum_{i<j} \alpha_i \alpha_j = \sum_{i<j} \beta_i \beta_j \\
&\cdots \\
\sigma_d &= \sum_{i_1<\cdots<i_d} \alpha_{i_1} \cdots \alpha_{i_d} = \sum_{i_1<\cdots<i_d} \beta_{i_1} \cdots \beta_{i_d}
\end{aligned}$$

Therefore, $\alpha_1, \ldots, \alpha_\gamma, \beta_1, \ldots, \beta_\gamma$ are 2γ distinct zeros of the polynomial

$$x^\gamma - \sigma_1 x^{\gamma-1} + \sigma_2 x^{\gamma-2} - \cdots \pm \sigma_\gamma.$$

But a polynomial of degree γ over a field has at most γ zeros. □

4.4 Communication complexity of information exchange

For the informative protocol presented in Section 4.2, the amount of messages needed is at most $m = (q^{d+1} - 1)/(q - 1)$. As $q + 1 \geq n$ is needed, using Bertrand's postulate (there is always a prime in the interval $(x, 2x]$) we can say that there is always a solution with at most $((2n-2)^{d+1} - 1)/(2n-3)$ messages, that is $O(n^{\mathbf{c}+\mathbf{r}})$ messages. Thus, in terms of communication complexity, we have the following result.

Theorem 11. *$O((\mathbf{c}+\mathbf{r})\log n)$ bits are sufficient for an informative one-step protocol.*

As for the informative protocol from [19, Section 8] presented in the previous section, the amount of messages needed is at most q^d. Then, by Bertrand's postulate, there is always a set of size at most $(2n)^d$ to properly color $J^d(n, \mathbf{a})$. Then, in terms of communication complexity this bound is stronger than the other for some values of n, and for others, weaker. However, asymptotically, this approach yields the same upper bound of that from Theorem 11.

We just provided an upper bound for the communication complexity on the information transmission problem. Now we consider the communication complexity for the information exchange problem, i.e. when B responds after A's announcement. As is already mentioned in Section 2.1.1, for a two-step protocol (P_A, P_B), the communication complexity is $\log_2(|\mathcal{M}_A|)+\log_2(|\mathcal{M}_B|)$, where $\mathcal{M}_A$ and $\mathcal{M}_B$ are the set of messages of P_A and P_B, respectively.

Recall the proof of Theorem 4, where it is shown that if we have an informative one-step protocol P_A, there is always an informative two-step protocol

(P_A, P_B) such that $|\mathcal{M}_B| = \binom{n-\mathbf{a}}{\mathbf{b}}$. In light of this result and Theorem 11, the following theorem is straightforward.

Theorem 12. $O((\mathbf{c}+\mathbf{r}) \log n + \log \binom{n-\mathbf{a}}{\mathbf{b}})$ *bits are sufficient for an informative two-step protocol.*

Chapter 5

Conclusions

We have presented the problem of secure information exchange between two agents A and B in the face of an eavesdropper C. 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. Additionally, there are $\mathbf{r}$ cards from the deck that are not dealt to anyone, i.e. $n = \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{r}$. This scenario is reminiscent to that of the generalized Russian Cards problem, although for the last, it is usually considered that $n = \mathbf{a}+\mathbf{b}+\mathbf{c}$. Therefore, in this work we considered a more general Russian Cards scenario and formalized the informative and safety requirements of the classic problem in this new context.

The problem is an important case of study in the search for unconditionally secure implementations of several cryptographic primitives. In that sense, notice that a solution to the Russian Cards problem implies a solution to the secret key exchange problem. That is, consider all the possible deals of A and B from the perspective of C, indexed in a previously known manner from 0 to $N-1$, where $N = \binom{n-\mathbf{c}}{\mathbf{a}} \times \binom{n-\mathbf{c}-\mathbf{a}}{\mathbf{b}}$. Using a solution to the problem, both A and B can compute the value of k, the actual index of their deal from C's perspective, while C has no information about it [13]. Thus, k would be the shared secret key.

For this work, we focused on solutions to the general problem providing weak 1-security, which is a form of unconditional security, in the sense that the agents are regarded as computationally unlimited. Moreover we studied one-step and two-step protocols in both, deterministic and non-detrministic forms.

Our combinatorial perspective, inspired by distributed computing, is based on a formalization in terms of Johnson graphs, which facilitates using known results about these graphs, closely related to Coding Theory. Thus, we were able to prove novel results, as well as explaining and unifying previously known ones.

5.1 Repercussions

One of our main contributions is the impossibility result regarding the existence of two-step protocols, in which B's response is perfectly safe with respect to A's announcement. Namely, we proved that, when $\mathbf{r} > 0$, B cannot make an informative announcement for A without revealing any new information to C. This marks an important difference between the problem in this more general setting and the usually considered scenario with $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$ and this difference is not, in any sense, inconsequential. This is because, as far as we know, the response strategies used for the last step of all known solutions are in fact perfectly safe with respect to C's current knowledge. Examples of this are all solutions in which B's announces C's hand, as well as the well-known two-step solution for $(\mathbf{a}, \mathbf{b}, 1)$ ($n = \mathbf{a}+\mathbf{b}+\mathbf{c}$), where both A and B announce the sum of their cards modulo n. What happens in this last example is that, once C hears A's announcement, she can already predict B's announcement from her current knowledge. Notice that B's announcement can be determined by

$$\sum_{x \in b} x \mod n = (\sum_{x \in D} x - \sum_{x \in a} x - c) \mod n$$

Moreover, we also stated a necessary and sufficient condition under which B's announcement can be trivially informative for A in a two-step solution in terms of solutions to the information transmission problem in the scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$. This allows us to discard as a possible response strategy for B the announcing of the cards that he and A does not hold, whenever A's announcement is not safe for $(\mathbf{a}, \mathbf{b}, \mathbf{c} + \mathbf{r})$. Once again, this is an important observation since this response strategy was suggested in [19] without remarking such drawback.

Furthermore, we showed that in this general scenario where $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$, although we may find solutions to the problem of secure information transmission, it could be impossible to solve the problem of secure information exchange. This is also an interesting difference with respect to the most studied case where $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$.

On the other hand, our discussion regarding the approach to solutions that focus on individual announcements, or specifically, "good announcements", led us to argue that in fact these formulations define the security of a scheme in the same way that non-deterministic weak 1-secure protocols do. Additionally, we also discussed this approach from the point of view of communication complexity, which to the best of our knowledge, had not been done before formally.

Finally, we have shown how we can discover informative protocols for the general problem in the Coding Theory literature, by reinterpreting some of the most common methods for proving a bound on $A(n, d, w)$. By doing so, we were able to show an upper bound on the communication complexity of information transmission and exchange in the general Russian cards scenario. Namely, we showed that $O((\mathbf{c} + \mathbf{r}) \log n)$ bits are sufficient for a one-step informative protocol, and $O((\mathbf{c} + \mathbf{r}) \log n + \log \binom{n-\mathbf{a}}{\mathbf{b}})$ bits are sufficient for a two-step informative protocol.

5.2 Future work

There are still many questions without an answer about Russian Cards problem, particularly for the more general case where $\mathbf{r} > 0$. For example, for the cases when there is a safe and informative one-step protocol P_A and a trivially informative response protocol P_B^* is not possible, is there a two-step solution for the problem?

Additionally, as we have shown, even for the cases where $\mathbf{c} + \mathbf{r} > 1$, it is possible and not too difficult to find informative protocols using Coding Theory results. However, there still remains the question about how can we achieve security for these problem instances, for which only a few, such as $(4, 4, 2)$ with $n = 10$ [11], have (secure) solutions.

Many other interesting problems remain open. Some of them are the relation with combinatorial designs that has been thoroughly studied e.g. [24]; considering stronger security requirements e.g. [18]; about fault-tolerant solutions [17], more than two parties e.g. [12], etc. It would be interesting to understand the role of Johnson graphs in multi-round protocols; there exists work both from the secret sharing side e.g. [14], and from the Russian cards side [7, 11], and of course in distributed computing, although without preserving privacy [5, 8].

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] Attiya, H., Rajsbaum, S.: Indistinguishability. Comm. ACM **63**(5), 90–99 (April 2020), `https://doi.org/10.1145/3376902`

[5] Conde, R., Rajsbaum, S.: The complexity gap between consensus and safe-consensus. In: International Colloquium on Structural Information and Communication Complexity. pp. 68–82. Springer (2014)

[6] 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`

[7] 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

[8] Delporte, C., Fauconnier, H., Rajsbaum, S.: Communication complexity of wait-free computability in dynamic networks. In: Richa, A., Scheideler, C. (eds.) Proc. 27rd Int. Colloquium Structural Information and Communication Complexity (SIROCCO). pp. 291–309. No. 12156 in Lecture Notes in Computer Science, Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-54921-3_17, https://link.springer.com/chapter/10.1007/978-3-030-54921-3_17

[9] Diffie, W., Hellman, M.: New directions in cryptography. IEEE transactions on Information Theory **22**(6), 644–654 (1976)

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

[11] 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)

[12] 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

[13] 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

[14] 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)

[15] 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`

[16] Graham, R., Sloane, N.: Lower bounds for constant weight codes. IEEE Transactions on Information Theory **26**(1), 37–43 (1980)

[17] Herlihy, M., Kozlov, D., Rajsbaum, S.: Distributed Computing Through Combinatorial Topology. Elsevier-Morgan Kaufmann (2013), `https://doi.org/10.1016/C2011-0-07032-1`

[18] Landerreche, E., Fernández-Duque, D.: A case study in almost-perfect security for unconditionally secure communication. Des. Codes Cryptography **83**(1), 145–168 (April 2017), `https://doi.org/10.1007/s10623-016-0210-y`

[19] Rajsbaum, S.: A distributed computing perspective of unconditionally secure information transmission in Russian cards problems. Tech. rep., arXiv (2020), `https://arxiv.org/abs/2009.13644`, part of this work to appear in the 28th International Colloquium on Structural Information and Communication Complexity (SIROCCO) 2021, Springer Lecture Notes in Computer Science (LNCS).

[20] Rivest, R.: Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer (1999), `http://people.csail.mit.edu/rivest/Rivest-commitment.pdf`, MIT

[21] Shannon, C.E.: Communication theory of secrecy systems. The Bell System Technical Journal **28**(4), 656–715 (1949)

[22] Štika, P.: Unconditional security in classical cryptography. Masarykova universita, Fakulta informatiky (2010)

[23] 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

[24] Swanson, C.M., Stinson, D.R.: Additional constructions to solve the generalized Russian cards problem using combinatorial designs. The Electronic Journal of Combinatorics **21**(3) (2014), https://www.combinatorics.org/ojs/index.php/eljc/article/view/v21i3p29