

# A Distributed Computing Perspective of Unconditionally Secure Information Transmission in Russian Cards Problems

Sergio Rajsbaum

Instituto de Matemáticas  
Universidad Nacional Autónoma de México (UNAM)  
Mexico City 04510, Mexico  
rajsbaum@im.unam.mx

**Abstract.** The problem of  $A$  privately transmitting information to  $B$  by a public announcement overheard by an eavesdropper  $C$  is considered. To do so by a deterministic protocol, their inputs must be correlated. Dependent inputs are represented using a deck of cards. There is a publicly known *signature*  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , where  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ , and  $A$  gets  $\mathbf{a}$  cards,  $B$  gets  $\mathbf{b}$  cards, and  $C$  gets  $\mathbf{c}$  cards, out of the deck of  $n$  cards. Using a deterministic protocol,  $A$  decides its announcement based on her hand.

Using techniques from coding theory, Johnson graphs, and additive number theory, a novel perspective inspired by distributed computing theory is provided, to analyze the amount of information that  $A$  needs to send, while preventing  $C$  from learning a single card of her hand. In one extreme, the generalized Russian cards problem,  $B$  wants to learn all of  $A$ 's cards, and in the other,  $B$  wishes to learn *something* about  $A$ 's hand.

**Keywords:** Johnson graphs · Secret sharing · Distributed computing · Russian cards problem · Information Theoretic Security · Combinatorial cryptography · Binary Constant Weight Codes · Additive number theory.

## 1 Introduction

The idea that card games could be used to achieve security in the presence of computationally unbounded adversaries proposed by Peter Winkler [55] led to an active research line e.g. [26,27,28,29,39,44,45,46,55]. It motivated Fischer and Wright [28] to consider *card games*, where  $A, B, C$  draw cards from a deck  $D$  of  $n$  cards, as specified by a *signature*  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , with  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ . Nobody gets  $\mathbf{r}$  cards, while  $A$  gets  $\mathbf{a}$  cards,  $B$  gets  $\mathbf{b}$  cards, and  $C$  gets  $\mathbf{c}$  cards.

Fischer and Wright thought of the cards as representing correlated random initial local variables for the players, that have a simple structure. They were interested in knowing which distributions of private initial values allow  $A$  and  $B$  to obtain a key, that remains secret to  $C$ . Their protocols mostly use randomization, and they are information-theoretic secure. However, they do not keep the cards of  $A$  and  $B$  secret from  $C$ .

Another research line started with an in depth, combinatorial and epistemic logic study of van Ditmarsch [20] of the *Russian cards* problem, presented at the Moscow Mathematics Olympiad in 2000, where the cards of  $A$  and  $B$  should be kept secret from  $C$ . Here  $A$ ,  $B$  and  $C$  draw  $(3, 3, 1)$  cards, respectively, from a deck of 7 cards. First  $A$  makes an announcement that allows  $B$  to identify her set of cards, while  $C$  cannot deduce a single card of  $A$ . After the announcement of  $A$ ,  $B$  knows the cards of each player, and hence he may announce  $C$ 's card, from which  $C$  learns nothing, but allows  $A$  to infer the cards of  $B$ . The problem has received a fair amount of attention since then<sup>1</sup> e.g. [3,4,12,13,14,21,22,40,53,54], in its *generalized* form of signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , and other variants, including multi-round, multiplayer, and different security requirements. Solutions are based either on modular arithmetic or on combinatorial designs.

The original solution for  $(3, 3, 1)$  uses modular arithmetic, where  $A$  announces the sum of her cards modulo 7, and then  $B$  announces  $C$ 's card [42]. For the general case when  $\mathbf{c} = 1$  (and  $\mathbf{r} = 0$ ), solutions exist that announce the cards sum modulo an appropriate prime number greater or equal to  $n$  [12]. These solutions use only two announcements. A solution using three announcements for  $(4, 4, 2)$  is reported in [21], and a four-step protocol where  $C$  holds approximately the square of the number of cards of  $A$  is presented in [14].

The relation to Steiner triple system and combinatorial designs goes back to 1847 Kirkman [38]. Using combinatorial designs Cordón-Franco et al. [14] prove that solutions exist when  $\mathbf{a}$  is a power of a prime, and present the first solutions when  $\mathbf{c} > \mathbf{a}$ . The solution used 4 communication steps, as opposed to the usual 2-step protocols. Albert et al. [4] show that there is no 2-step solution if  $c \geq a - 1$ .

We provide an extensive discussion of related work in Appendix A. In addition to the papers mentioned above, through our new perspective on these problems, we have uncovered relations with other areas: intersecting families of sets, coding theory, additive number theory, and distributed computability.

*The new approach.* Given a publicly known signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , for a deck  $D$  of  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$  cards, the basic problem underlying the situations described above, is to design a safe protocol  $P_A$ , so that  $A$  makes a public announcement,  $P_A(a)$ , based on her hand,  $a$ . From the announcement  $P_A(a)$ , and using his own hand,  $b$ ,  $B$  should learn something about  $A$ 's hand. The announcement  $P_A(a)$  is deterministically determined by the input of  $A$ , and the knowledge of the signature. No randomized solutions are considered in this paper.

In the language of e.g. [12,14,21], a protocol  $P_A$  should be *informative* for  $B$  and *safe* from  $C$ . A protocol is *safe* if  $C$  does not learn any of the cards of  $A$ . It is *informative*, if  $B$  learns the hand of  $A$ .

We define the notion of a protocol being *minimally informative*, where the goal is that  $B$  learns *something* about the hand of  $A$ . We prove that the minimal information problem is a kind of oblivious transfer problem, in the sense that, when  $\mathbf{c} + \mathbf{r} = 1$ ,  $B$  learns one card of  $A$ , but  $A$  does not know which one. If

<sup>1</sup> The  $\mathbf{r} = 0$  case is mostly considered here, as well as in the secret key research line.

$\mathbf{c} + \mathbf{r} > 1$  then  $B$  learns even less; he learns that  $A$  has one of the cards of a set  $s$ ,  $|s| = \mathbf{c} + \mathbf{r}$ .

In Section 2 we formalize this setting based on distributed computability [36], and more specifically when the least amount of communication is studied [19].

In Section 3, using this formalization, we show that a protocol can be viewed as a coloring of the set of vertices  $\mathcal{P}_{\mathbf{a}}(D)$ , all subsets of size  $\mathbf{a}$  of  $D$ ,

$$P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathcal{M},$$

for the set of messages  $\mathcal{M}$  that  $A$  may send. Thus,  $\mathcal{P}_{\mathbf{a}}(D)$  is the set of vertices of a Johnson graph  $J(n, \mathbf{a})$ , where  $n = |D|$ . We are interested in the question of how small can  $\mathcal{M}$  be, i.e., the number of bits,  $\log_2 |\mathcal{M}|$ , that  $A$  needs to transmit to implement either an informative or a minimally informative safe protocol.

We show in Theorem 2 that  $P_A$  is informative if and only if  $P_A$  is a proper coloring of the  $d$ -distance Johnson graph  $J^d(n, \mathbf{a})$ ,  $d = \mathbf{c} + \mathbf{r}$ . Vertices  $a, a'$  of  $J^d(n, \mathbf{a})$  are adjacent whenever  $\mathbf{a} - d \leq |a \cap a'|$ . In particular, we have a Johnson graph when  $d = 1$ .

It is well-known that there is a family of maximal clicks of  $J(n, \mathbf{a})$  of size  $\mathbf{a} + 1$ , e.g. [32]. It turns out, that the inputs of  $A$  that  $B$  with input  $b$  considers possible, form a maximal click of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ , denoted  $K_p(\bar{b})$ . The click  $K_p(\bar{b})$  consists of all hands  $a \subset \bar{b}$ ,  $|a| = \mathbf{a}$ , and hence  $p = \binom{\mathbf{a}+\mathbf{c}+\mathbf{r}}{\mathbf{a}}$ . Similarly, the hands that  $C$  considers possible with input  $c$  form a click  $K_p(\bar{c})$  of  $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ , and such clicks are of size  $p = \binom{\mathbf{a}+\mathbf{b}+\mathbf{r}}{\mathbf{a}}$ .

We show also in Theorem 2 that  $P_A$  is minimally informative if and only if  $P_A$  colors at least one edge of each click  $K_p(\bar{b})$  with two different colors. In contrast, informative requires that  $P_A$  colors every edge of  $K_p(\bar{b})$  with two different colors.

Thus, the chromatic number of  $J^d(n, \mathbf{a})$  determines the number of messages needed for a protocol  $P_A$  to be informative. There are many interesting open questions concerning the chromatic number of Johnson graphs [32]. Upper bounds have been thoroughly studied for special cases, because they imply lower bounds on codes e.g. [10, 24]. In addition to some special cases, only the trivial lower bound implied by the maximal clicks is known. Briefly, it is known that  $n/2 \leq \chi(J(n, \mathbf{a})) \leq n$ , often the chromatic number is a little bit smaller<sup>2</sup>, more specifics are in Appendix B. Indeed, using coding theory techniques we show the easy result that there is an informative protocol when  $\mathbf{c} + \mathbf{r} = 1$  with  $n$  messages (Lemma 11), and the more difficult new result for the general case,  $\mathbf{c} + \mathbf{r} \geq 1$ , that  $(2n)^{\mathbf{c}+\mathbf{r}}$  messages suffice, i.e., to properly color  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$  (Lemma 15). It follows that  $\Theta((\mathbf{c} + \mathbf{r}) \log n)$  bits are needed and sufficient for an informative protocol; the lower bound is implied by the size of the maximal clicks of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ , more details in Section 8.

Remarkably, only 1 bit suffices for minimal information transmission, when  $\mathbf{b} < \lfloor n/2 \rfloor$ . We study the minimal information problem in Section 6, where we present this and other results. We show that if additionally  $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$  the 1-bit protocol is also safe. Also, we present a reduction from an informative protocol,

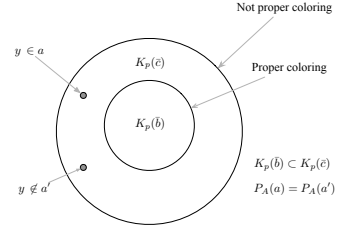
<sup>2</sup> Apparently there is no  $n, \mathbf{a}$  where it is known that  $\chi(J(n, \mathbf{a})) < n - 2$ . In some special cases the exact number has been determined, Figure 9.

showing that when  $\mathbf{c} + \mathbf{r} = 1$ , as  $\mathbf{a}$  grows from 3 up to roughly  $n/2$ , the number of different messages goes down from  $n/3$  to 2, for a safe and minimally informative protocol. We find it surprising that there is a safe minimally informative protocol for the classic Russian cards case  $(3, 3, 1)$  using 2 messages ( $n = 7$ ). Namely, with a message consisting of only one bit,  $A$  can transfer one of her cards to  $B$ , privately.

We study the classic Russian cards problem in Section 5, determined by colorings of  $J(7, 3)$ , as a concrete example of the previous ideas. There is an informative and safe solution with 7 messages (known since [42]), and one with 6 messages [53]. Namely, using 6 messages is optimal, since the chromatic number of  $J(7, 3)$  is known to be 6. There is also a safe informative solution using 6 messages for the *weak Russian cards* problem, i.e. when  $\mathbf{c} = 0$  and  $\mathbf{r} = 1$ .

While the informative property requires that all vertices of each maximal click  $K_p(\bar{b})$  are colored differently by  $P_A$ , the safety property requires the opposite, that not all vertices of each maximal click  $K_p(\bar{c})$  are colored differently. Thus, a protocol  $P_A$  can be informative and safe only if  $\mathbf{b} > \mathbf{c}$ . In this case, while  $K_p(\bar{c})$  induces a click in  $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ , it does not induce a click in  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ . Safety requires that for each card  $y$ , there is a hand of  $A$  that includes  $y$ , and another that does not include it, both equally colored, in the complement of the hand of  $C$ .

We consider the protocol  $\chi_{modn}$  in Section 7, that sends the sum of the cards modulo  $n$ , for  $\mathbf{c} + \mathbf{r} = 1$ , and show that it is informative and safe, for  $\mathbf{a}, \mathbf{b} \geq 3$ ,  $n \geq 7$ . Indeed, while informative is a coding theory property, safety is an additive number theory property. We prove safety using simple shifting techniques [32], getting a generalization and simplification of results of [12].<sup>3</sup> Thus, only two additional messages are needed to make an informative protocol, also safe (w.r.t. the best known solutions). We present an informative protocol for the general case  $\mathbf{c} + \mathbf{r} \geq 1$  based on more involved coding theory ideas and discuss safety, in Section 8, but a detailed treatment is beyond the scope of this paper.



**Organization.** In Section 2 we present the problems of secure information transmission that we study in this paper. In Section 3 we review some basic facts about Johnson graphs, and rephrase in such terms the secure information transmission problems. In Section 4 we discuss the relation with the generalized Russian cards problem, and some basic consequences of our formalization, e.g. there is a safe proper coloring of  $J(n, \mathbf{a})$  iff there is a safe proper coloring of  $J(n, n - \mathbf{a})$ . In Section 5 we present the results about six-message solutions for the weak and the classic Russian cards problem,  $n = 7$ . In Section 6 we present the minimal information transmission results. In Section 7 we show that  $n$  messages are sufficient for safe, informative information transmission, when

<sup>3</sup> Cordon-Franco et al. [12] show that  $\chi_{modn}$  is safe when  $n$  is prime using [17, Theorem 4.1], analogous to the Cauchy-Davenport theorem, except for  $(4, 3, 1)$ ,  $(3, 4, 1)$ .

$\mathbf{c} + \mathbf{r} = 1$ , and the general case is discussed in Section 8. The conclusions are in Section 9. Additional details are at the end: further related work discussion in Appendix A, Johnson graphs background in Appendix B, additional proofs and figures are in Appendix C and D.

## 2 Secure information transmission

The model and the problem are defined here, adapting the distributed computing formalization of [36] to the case of an eavesdropper. In Section 2.1 we present the representation of the inputs to  $A, B, C$  as a simplicial complex, which determines the Johnson graphs that will play a central role in this paper. In Section 2.2 the notions of protocol, and of a protocol being (minimally) informative and safe are defined.

### 2.1 The input complex

Let  $D = \{0, \dots, n-1\}$ ,  $n > 1$ , be the *deck* of  $n$  distinct cards. An element in the deck is a *card*. A subset  $x$  of cards is a *hand*,  $x \in \mathcal{P}(D)$ . We may say for short that  $x$ ,  $|x| = m$ , is an  $m$ -set or  $m$ -hand, namely, if  $x \in \mathcal{P}_m(D)$ , the subsets of  $D$  of size  $m$ . A *deal*  $= (a, b, c)$  consists of three disjoint hands, meaning that cards in  $a$  are dealt to  $A$ , cards in  $b$  to  $B$ , and cards in  $c$  to  $C$ . We say that the hand is the *input* of the process. 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 [27]. We assume that  $A, B$  and  $C$  are aware of the deck and the signature.

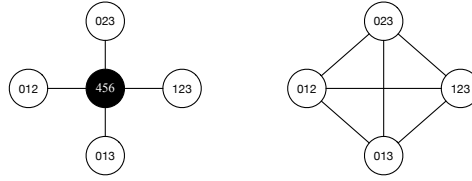
It has been often assumed that  $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$ , but as we shall see, it is natural to consider the case where nobody gets  $\mathbf{r}$  cards,  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ . While  $A$  and  $B$  get at least one card,  $\mathbf{a}, \mathbf{b} \geq 1$ ,  $C$  may get none  $\mathbf{c} \geq 0$ .

All possible deals for a given signature over  $D$  are represented by a simplicial complex. The vertices are of the form  $(Y, y)$ ,  $Y \in \{A, B, C\}$ , and  $y$  a hand. Such a vertex is called a  $Y$ -vertex. The *input complex*  $\mathcal{I}(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , or  $\mathcal{I}$  for short, for signature  $\gamma = (\mathbf{a}, \mathbf{b}, \mathbf{c})$  is defined as follows. The facets of  $\mathcal{I}$  are all the sets  $\{(A, a), (B, b), (C, c)\}$ , where  $a, b, c$  is a deal of signature  $\gamma$ . The input complex  $\mathcal{I}$  consists of all such facets, together with all their subsets.

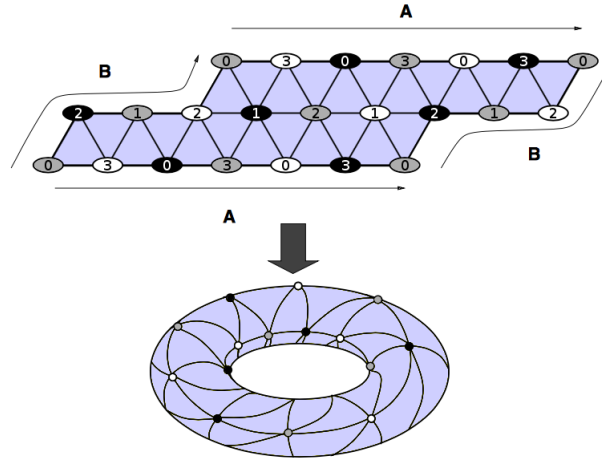
Notice that the  $A$ -vertices of  $\mathcal{I}$  are in a one-to-one correspondence with all subsets of size  $\mathbf{a}$  of  $D$ ,  $\mathcal{P}_{\mathbf{a}}(D)$ , the  $B$ -vertices with  $\mathcal{P}_{\mathbf{b}}(D)$ , the  $C$ -vertices with  $\mathcal{P}_{\mathbf{c}}(D)$ . Indeed, when  $\mathbf{c} = 0$ , there is a single vertex for  $C$  in  $\mathcal{I}$ .

The left part of Figure 1 illustrates the four  $A$ -neighbors of vertex  $(B, \{4, 5, 6\})$ , in  $\mathcal{I}$ , for signature  $(3, 3, 1)$ . For short, we omit the commas and parenthesis from the set notation, and write  $(B, \{456\})$ .

*Example 1.* In distributed computing the input complex with a signature  $\gamma = (1, 1, 1)$  for three processes has been considered, representing that processes get distinct input names from a set of  $n$  names [5]. The figure from [37] shows that in the case of  $n = 4$ , the complex is a torus subdivided into triangles. The vertices of each triangle are colored black, gray, and white to represent the three different processes. Inside the vertex is the card dealt to the corresponding process.



**Fig. 1.** White vertices correspond to  $A$ , and the black vertex correspond to  $B$ . The four  $A$ -neighbours of  $(B, 456)$  for signature  $(3, 3, 1)$  form a click on the right, the corresponding part of  $J(7, 3) = \mathcal{G}_B$ , defined in Section 3.2.



**Fig. 2.** Input complex for signature  $\gamma = (1, 1, 1)$  with  $n = 4$  (from [37]).

## 2.2 Informative and safe protocols

Fix an input complex  $\mathcal{I}$  over  $D$ ,  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ . In the language of e.g. [12, 14, 21], a protocol should be “informative” for  $B$  and “safe” from  $C$ . In the case of the Russian cards problem,  $B$  should learn the hand of  $A$ . We define also the notion of “minimally informative.”

The goal is that  $B$  learns something about the hand of  $A$ , after listening to an announcement  $m$  made by  $A$ . The announcement of  $A$  is defined by a deterministic function  $P_A(a) = M$ , for each input vertex  $(A, a) \in \mathcal{I}$ , where  $M$  belongs to  $\mathcal{M}$ , the domain of possible messages that  $A$  may send. We say that  $P_A$  is the *protocol* of  $A$ . For  $B$ , there is a *decision function*  $\delta_B(b, M)$  that produces a set of cards in  $\mathcal{P}(D)$ , based on the input  $b$  of  $B$ , and the message  $M$  received<sup>4</sup>.

The minimally informative notion (consider in Section 6) requires only that  $B$  learns *something* about the hand of  $A$ . As we shall see, the least one can

<sup>4</sup> Since we have fixed  $D$  and the input complex  $\mathcal{I}$ , implicitly  $P_A(a)$  and  $\delta_B(b, M)$  depend on these parameters, in addition to the specific input  $a$ , resp.  $(b, M)$ . This is what we mean when we say that the players know the input complex.

expect is that  $B$  learns that  $A$  has one of the cards of a set  $s$ ,  $|s| = n - \mathbf{a} - \mathbf{b}$ . Thus, if  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ , with  $\mathbf{c} + \mathbf{r} = 1$ , then  $B$  should learn one of the cards in the hand of  $A$ . When  $\mathbf{b} = 1$ ,  $B$  should learn that  $A$  has one of the cards in a set  $s$ ,  $|s| = n - \mathbf{a} - 1$ , more than the trivial guess  $s$ ,  $s = D \setminus b$ , where  $b$  is  $B$ 's input card. When  $\mathbf{c} + \mathbf{r} = 0$  without any communication  $B$  knows the hand of  $A$ , so it does not make sense to define a protocol where  $B$  learns less information. Notice that when  $\mathbf{c} + \mathbf{r} \geq 1$ , we have that  $n - \mathbf{a} - \mathbf{b} \geq 1$ , and the following minimally informative definition makes sense.

**Definition 1 (Informative and minimally informative).** *Let  $P_A$  be a protocol. If there exists  $\delta_B$ , such that for any given input edge  $\{(A, a), (B, b)\} \in \mathcal{I}$ , with  $M = P_A(a)$ ,*

- $\delta_B(b, M) = a$ , *the protocol is informative,*
- *for  $\mathbf{c} + \mathbf{r} \geq 1$ ,  $\delta_B(b, M) = s \in \mathcal{P}_{\mathbf{c}+\mathbf{r}}(D)$ , such that  $a \cap s \neq \emptyset$ , the protocol is minimally informative.*

The previous definition does not talk about  $C$ . Indeed, it is based only on the graph which is the subcomplex of  $\mathcal{I}$  induced by the  $A$ -vertices and the  $B$ -vertices. A protocol is safe if  $C$  cannot tell who holds even a single card (that she does not hold). Consider a deal  $I = \{(A, a), (B, b), (C, c)\} \in \mathcal{I}$ . Let  $P_A(a) = M$  be the announcement sent by  $A$ , and denote it also by  $P_A(I)$ . Two deals  $I, I' \in \mathcal{I}$  are *initially indistinguishable* [6] to  $C$  with input  $c$  if  $(C, c) \in I, I'$ . And they are *indistinguishable after the protocol*, if additionally  $P_A(I) = P_A(I')$ . We require then that for  $C$  there are always two indistinguishable inputs of  $A$ ,  $a, a'$ , after the protocol, such that  $x \in a$  and  $x \notin a'$  or else  $x \notin a$  and  $x \in a'$ . More precisely, for a vertex  $(C, c)$ , let  $M$  be a *possible* message, namely, such that there exists  $I = \{(A, a), (B, b), (C, c)\} \in \mathcal{I}$ , and  $P_A(I) = M$ . For a hand  $c$ , let  $\bar{c} = D \setminus c$ , and  $\Delta$  the symmetric difference operator.

**Definition 2 (Safety).** *A protocol  $P_A$  is safe, if for any  $(C, c)$ , any  $x \in \bar{c}$ , and any possible message  $M$  for  $(C, c)$ , there are edges  $I = \{(A, a), (C, c)\} \in \mathcal{I}$ , and  $I' = \{(A, a'), (C, c)\} \in \mathcal{I}$ , with  $P_A(I) = P_A(I') = M$  such that  $x \in a \Delta a'$ .*

Notice that while  $\mathbf{a}, \mathbf{b} \geq 1$ , the previous definition applies even when  $\mathbf{c} = 0$ .

*Remark 1 (The  $\mathbf{c} + \mathbf{r} \geq 1$  assumption).* If  $\mathbf{c} = \mathbf{r} = 0$ , there is a single vertex for  $C$  in  $\mathcal{I}$ , and each vertex of  $A$  and of  $B$  belong to a single triangle; without any communication they know each other hands. Even when  $\mathbf{a} = \mathbf{b} = 1$ , the protocol  $P_A$  that always sends the same message, is informative and safe.

### 3 Protocol as vertex coloring

We represent subcomplexes of  $\mathcal{I}$  as Johnson graphs in Section 3.1, and some basic facts about these graphs are recalled in Section 3.2. We reformulate the information transmission problem as properties about vertex colorings of Johnson graphs in Section 3.3, and discuss corresponding chromatic number notions in Section 3.4.

### 3.1 Representing indistinguishability by Johnson graphs

The situation when  $B$  has input  $b$  is represented by a vertex  $(B, b) \in \mathcal{I}$ . The  $A$ -vertices that  $B$  considers possible with input  $b$ , are the  $A$ -neighbors of  $(B, b)$  in  $\mathcal{I}$ . Thus, we define (following [19]) the graph  $\mathcal{G}_B$  in terms of  $\mathcal{I}$ , as follows. The vertices of  $\mathcal{G}_B$  consist of all the  $A$ -vertices of  $\mathcal{I}$ . There is an edge joining two vertices  $(A, a), (A, a')$  if and only if there are edges in  $\mathcal{I}$  connecting them with the same vertex  $(B, b)$ . To analyze  $\mathcal{G}_B$ , we omit the id  $A$  from the vertices, and let  $V(\mathcal{G}_B) = \mathcal{P}_{\mathbf{a}}(D)$ . Thus, for two distinct  $a, a' \in \mathcal{P}_{\mathbf{a}}(D)$ ,  $\{a, a'\} \in E(\mathcal{G}_B)$  iff  $\exists b \in \mathcal{P}_{\mathbf{b}}(D)$  such that  $a, a' \subseteq \bar{b} = D - b$ . See Figure 1. If  $\mathbf{r} = \mathbf{c} = 0$ , and  $n = \mathbf{a} + \mathbf{b}$ , there are no two such distinct deals  $a, a'$ , and the graph has no edges (which is why it makes sense to assume  $\mathbf{c} + \mathbf{r} \geq 1$ , Remark 1).

The graph  $\mathcal{G}_C$  is defined analogously, on the same set of vertices,  $V(\mathcal{G}_C) = \mathcal{P}_{\mathbf{a}}(D)$ . When  $C$  has input  $c$  there is a vertex  $(C, c) \in \mathcal{I}$ . The  $A$ -vertices that  $C$  considers possible with input  $c$ , are the  $A$ -neighbors of  $(C, c)$  in  $\mathcal{I}$ . Thus, for two distinct  $a, a' \in \mathcal{P}_{\mathbf{a}}(D)$ ,  $\{a, a'\} \in E(\mathcal{G}_C)$  iff  $\exists c \in \mathcal{P}_{\mathbf{c}}(D)$  such that  $a, a' \subseteq \bar{c} = D - c$ .

**Lemma 1.** *For  $a, a' \in V(\mathcal{G}_B)$ ,  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ ,  $\mathbf{r} \geq 0$ , we have that  $\{a, a'\} \in E(\mathcal{G}_B)$  iff  $\mathbf{a} - (\mathbf{c} + \mathbf{r}) \leq |a \cap a'|$ . Similarly,  $\{a, a'\} \in E(\mathcal{G}_C)$  iff  $\mathbf{a} - (\mathbf{b} + \mathbf{r}) \leq |a \cap a'|$ .*

*Proof.* Recall that  $\{a, a'\} \in E(\mathcal{G}_B)$  iff  $\exists b \subseteq D$  such that  $|b| = \mathbf{b}$  and  $a, a' \subseteq \bar{b} = D - b$ .

Thus,  $\mathbf{b} \leq |D - (a \cup a')|$ . Now,  $|D - (a \cup a')| = (\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}) - |a \cup a'|$ . Also,  $|a \cup a'| = 2\mathbf{a} - |a \cap a'|$ . It follows that  $\mathbf{b} \leq \mathbf{b} + \mathbf{c} + \mathbf{r} - \mathbf{a} + |a \cap a'|$ . Finally,  $\mathbf{a} - \mathbf{c} - \mathbf{r} \leq |a \cap a'|$ .

The argument for  $\mathcal{G}_C$  is similar.

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

We have our basic theorem, for  $\mathbf{a}, \mathbf{b} \geq 1$ ,  $\mathbf{c}, \mathbf{r} \geq 0$ , and  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ . The basic, most studied case, is when  $\mathbf{c} = 1, \mathbf{r} = 0$ , or  $\mathbf{c} = 0, \mathbf{r} = 1$ .

**Theorem 1.** *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  $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ .*

Notice that when  $d = 0$  the graph  $J^d(n, m)$  has no edges. Thus, when  $\mathbf{c} + \mathbf{r} = 0$  the graph  $\mathcal{G}_B$  has no edges.

The vertices of  $A$  that  $B$  considers possible with input  $b$ , are the  $A$ -neighbors of  $(B, b)$  in  $\mathcal{I}$ . They are denoted  $K_p(\bar{b})$ , where  $\bar{b} = D - b$ . They induce a click in  $\mathcal{G}_B$  (overloading notation the click itself is also sometimes denoted by  $K_p(\bar{b})$ ). The vertices in  $K_p(\bar{b})$  are all  $a \subseteq \bar{b}$  with  $|a| = \mathbf{a}$ . Thus, when  $B$  has input  $b$ ,  $B$  considers possible that  $A$  has any input  $a$ ,  $a \in K_p(\bar{b})$ . Notice that if  $\mathbf{c} + \mathbf{r} = 0$  and  $n = \mathbf{a} + \mathbf{b}$ , then  $B$  with input  $b$  considers possible only one input for  $A$ , namely,  $\bar{b}$ . In this case,  $E(\mathcal{G}_B) = \emptyset$ .



**Lemma 2.** *For each hand  $b$  of  $B$ , the possible inputs of  $A$  induce a click  $K_p(\bar{b})$  in  $\mathcal{G}_B$ ,  $p = \binom{n-b}{a}$ , consisting of all  $a \in \mathcal{P}_a(D)$ , such that  $a \subset \bar{b}$ . Similarly, for  $\mathcal{G}_C$ , the vertices  $K_p(\bar{c})$  consisting of all  $a \in \mathcal{P}_a(D)$  such that  $a \subset \bar{c}$ , induce a click in  $\mathcal{G}_C$ .*

We have illustrated the following in the figure of the Introduction.

*Remark 2 (Subgraphs).* If  $\mathbf{b} \leq \mathbf{c}$  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. Hence, for each  $b \in \mathcal{P}_b(D)$ ,  $c \in \mathcal{P}_c(D)$ , both  $K_p(\bar{b})$  and  $K_p(\bar{c})$  induce clicks in  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ . Furthermore, if  $b \subseteq c$ , then  $K_p(\bar{c}) \subseteq K_p(\bar{b})$ .

### 3.2 Johnson graphs

Johnson graphs have been thoroughly studied, see Appendix B. We recall some basic notions here, which are especially relevant to this paper.

The vertices of a *Johnson graph*  $J(n, m)$  consist of the  $m$ -element subsets of an  $n$ -element set; two vertices are adjacent when the intersection of the two vertices consists of  $(m-1)$ -elements. We need the distance  $d$  version,  $J^d(n, m)$  of Definition 3. When  $d = 1$ ,  $J^d(n, m) = J(n, m)$ .

Let  $\delta(a, a')$  denote the distance between vertices  $a, a'$  in  $J(n, m)$ . Then,  $\delta(a, a') = k$  iff  $|a \cap a'| = m - k$ . Or, in terms of symmetric difference,  $\delta(a, a') = k$  iff  $|a \triangle a'| = 2k$ . One can show by induction that  $J(n, m)$  has diameter  $\min\{m, n - m\}$ . Thus, for all  $d \geq \min\{m, n - m\}$ ,  $J^d(n, m)$  is the complete graph on  $\binom{n}{m}$  vertices.

It is easy to see and well-known that  $J(n, m)$  is isomorphic to  $J(n, n - m)$ . The same holds for the distance  $d$  version.

**Lemma 3.** *The following are isomorphic graphs  $J^d(n, m) \cong J^d(n, n - m)$ .*

*Proof.* Consider vertices  $a, b$  of  $J^d(n, m)$ , and their complements  $\bar{a}, \bar{b}$ . Thus,  $|a| = |b| = m$ , and  $|\bar{a}| = |\bar{b}| = n - m$ . The isomorphism  $f$  is  $f(a) = \bar{a}$  and  $f(b) = \bar{b}$ . By definition,  $m - d \leq |a \cap b| \leq m - 1$  iff  $(a, b) \in E(J^d(n, m))$ . Let  $k = |a \cap b|$ . Then,  $|\bar{a} \cap \bar{b}| = n - m - k$ , hence,  $n - m - d \leq n - m - k \leq n - m - 1$ , so  $(\bar{a}, \bar{b}) \in E(J^d(n, n - m))$ , and the lemma follows.

*Remark 3 (Maximal clicks).* There are two families of maximal cliques in  $J(n, m)$ . For the first, take all  $n - m + 1$  of the  $m$ -subsets that contain a fixed  $(m - 1)$ -subset; for the second, take the  $m$ -subsets of a fixed set of size  $m + 1$ . When  $n = 2m$  the cliques in these two families have the same size. Maximality of the cliques is implied by Erdős–Ko–Rado Theorem [32, Chapter 6]. In the case of  $J^d(n, m)$ , we have already encountered one family in Lemma 2. For each  $(m + d)$ -subset  $\bar{b}$ , there is a click in  $J^d(n, m)$ , denoted  $K_p(\bar{b})$ . The vertices of  $K_p(\bar{b})$  are all  $m$ -subsets of  $\bar{b}$ . We will encounter the other family as well,  $K'_p(b)$ . A click  $K'_p(b)$  is obtained by taking the  $m$ -subsets that contain a fixed  $(m - d)$ -subset  $b$ .

We recall a simple but useful *shifting* technique in Johnson graphs, and even more generally in intersecting set families [32], we use the following version. For a hand  $a$ , and cards  $i, j$ , with  $i \notin a$ ,  $j \in a$ ,

$$a_{ij} = (a \setminus j) \cup \{i\},$$

denoted by an arc  $a \xrightarrow{ij} a_{ij}$ . Notice that,  $\{a, a_{ij}\} \in E(J(n, m))$ , and if  $a'$  is reachable from  $a$  by  $d$  arcs, then  $\{a, a'\} \in E(J^d(n, m))$ .

For a hand  $s$ , we say that  $a'$  is *s-reachable* from  $a$  if there is a directed path from  $a$  to  $a'$  defined by a (possibly empty) sequence of arcs  $\xrightarrow{ij}$ , all of them with  $i \in s$ . (For the following cf. [50, Lemma 1]).

**Lemma 4.** *Let  $a \in V(K_p(\bar{b}))$ . Let  $s = \bar{b} \setminus a$ . Thus,  $|s| = d$ . Then,  $V(K_p(\bar{b}))$  is the set of *s-reachable* vertices from  $a$ .*

*Proof.* First, notice that  $a$  is *s-reachable* from itself. Now, let  $a'$  be any other vertex of  $K_p(\bar{b})$ . If  $2d' = |a \triangle a'|$ ,  $d' \leq d$ , order the cards in  $a \setminus a'$  as  $x_1, \dots, x_{d'}$  and those in  $a' \setminus a$  as  $x'_1, \dots, x'_{d'}$ . Then,  $a'$  is reachable from  $a$  by the path

$$a = a_0 \xrightarrow{x'_1 x_1} a_1 \xrightarrow{x'_2 x_2} a_2 \cdots \xrightarrow{x'_{d'} x_{d'}} a_{d'} = a'.$$

We will need the following claims.

**Lemma 5.** *Let  $K_p(\bar{b})$  be a click of  $J^d(n, m)$ . For any set of  $k$  vertices,  $1 \leq k < p$ ,  $\{a_1, \dots, a_k\} \subset K_p(\bar{b})$ , there exists a set  $s \subset \bar{b}$ ,  $|s| = d$ , such that for any  $a_i$ ,  $a_i \cap s \neq \emptyset$ .*

*Proof.* Pick  $a \in K_p(\bar{b})$  not in  $\{a_i\}$ . Let  $s = \bar{b} \setminus a$ ,  $|s| = d$ . Since  $K_p(\bar{b})$  is the set of *s-reachable* vertices from  $a$  (Lemma 4), all other vertices in  $K_p(\bar{b})$  are *s-reachable* from  $a$ ,  $s = \bar{b} \setminus a$ . And hence, for the subset  $\{a_i\}$  of those vertices, we have that for any  $a_i$ ,  $a_i \cap s \neq \emptyset$ .

In particular, when  $d = 1$ , the following holds.

**Lemma 6.** *Consider  $J(n, m)$  and any  $K_{m+1}(\bar{b})$ . For any set of  $k$  vertices,  $1 \leq k \leq m + 1$ ,  $\{a_1, \dots, a_k\} \subseteq K_{m+1}(\bar{b})$ , it holds that  $|\cap a_i| = m + 1 - k$ .*

*Proof.* Consider the  $a_i$  vertices in order  $a_1, \dots, a_k$ , and the shiftings

$$a_1 \xrightarrow{x'_1 x_1} a_2 \xrightarrow{x'_2 x_2} a_3 \cdots a_{k-1} \xrightarrow{x'_{k-1} x_{k-1}} a_k,$$

where  $a_{i+1} \setminus a_i = x'_i$  and  $a_i \setminus a_{i+1} = x_i$ . Thus, by induction on  $i$ , for each  $i \geq 1$ ,  $|a_1 \cap a_2 \cap \dots \cap a_i| = m + 1 - i$ .

### 3.3 Protocol as vertex coloring of a Johnson graph

Consider a protocol  $P_A$  for signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , with  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ . In light of Theorem 1, we take the view of  $P_A$  as a vertex coloring,  $P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathcal{M}$ . For vertex  $(A, a) \in \mathcal{I}$ ,  $P_A(a)$  is the message  $M \in \mathcal{M}$ , sent by  $A$  when she has input  $a$ . We assume that  $P_A$  is surjective. The set of  $A$ -vertices colored  $M$  is  $P_A^{-1}(M)$ .<sup>5</sup>

Recall that a vertex coloring of a graph is *proper* if each pair of adjacent vertices have different colors. The following theorems reformulate the informative and safety notions of Definitions 1 and 2.

<sup>5</sup> Thus,  $P_A^{-1}(M)$  is equivalent to an “announcement” by  $A$  in the terminology of [4], or the “alternative hands” for  $A$ , in the notation of [20, Proposition 24].

**Theorem 2 (Informative characterization).** *Let  $P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathcal{M}$  be a protocol.*

- *$P_A$  is informative if and only if  $P_A$  is a proper vertex coloring of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ .*
- *When  $\mathbf{c} + \mathbf{r} \geq 1$ ,  $P_A$  is minimally informative if and only if for each  $b \in \mathcal{P}_{\mathbf{b}}(D)$  there is some edge  $\{a, a'\}$  in the click  $K_p(\bar{b})$  of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ , such that  $P_A(a) \neq P_A(a')$ .*

*Proof.* The first condition (informative) is clearly necessary for the protocol to be informative; if there is a vertex  $(B, b)$  such that two neighbours  $(A, a), (A, a')$  have the same color,  $M$ , then  $B$  cannot distinguish them, produces the same output,  $\delta_B(b, M)$ . Conversely, if all vertices in  $K_p(\bar{b})$  have different colors, then  $B$  with hand  $b$  will learn the hand of  $A$ . More formally, there is a function  $\pi_b$  of the colors of the  $A$ -neighbour of  $(B, b)$ , for each  $(B, b) \in \mathcal{I}$ , known a priori to  $B$ , such that  $\pi_b(M) = a$  when  $P_A(a) = M$ . The decision function for  $B$  is  $\delta_B(b, M) = \pi_b(M)$ .

The second condition (minimally informative) is defined only when  $\mathbf{c} + \mathbf{r} \geq 1$ , and hence  $K_p(\bar{b})$  has at least two vertices. The condition is clearly necessary, otherwise, when  $B$  has input  $b$ , he will output the same value on all of  $A$  possible hands (and there are at least two), independently of what the hand of  $A$  is. If  $B$ 's output is a set  $s$ ,  $|s| = n - \mathbf{a} - \mathbf{b}$ , then it could be that the input of  $A$  was actually  $a \in D \setminus s$ ,  $|a| = \mathbf{a}$ . Conversely, let  $V_M \subset K_p(\bar{b})$  be the subset of vertices  $a_i$  such that  $P_A(a_i) = M$ . Notice that  $0 < |V_M| < p$ , since there is an edge  $\{a, a'\} \in E(K_p(\bar{b}))$  with  $\chi(a) \neq \chi(a')$ . By Lemma 5 there exists a set  $s \subset \bar{b}$ ,  $|s| = \mathbf{c} + \mathbf{r} = n - \mathbf{a} - \mathbf{b}$ , such that for any  $a_i$ ,  $a_i \cap s \neq \emptyset$ . Thus, we may define  $\delta_B(b, M) = s$ .

*Remark 4 (Informative).* Some observations of the informative reformulation.

- Each edge of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$  is in some click  $K_p(\bar{b})$ . Thus,  $P_A$  being a *proper* vertex coloring is equivalent to the property that for all edges  $\{a, a'\} \in E(K_p(\bar{b}))$ , it holds that  $P_A(a) \neq P_A(a')$ , for any such click. In contrast, the minimally informative property requires only that not all edges of each click have both endpoints colored equally.
- By Lemma 3,  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a}) \cong J^{\mathbf{c}+\mathbf{r}}(n, n - \mathbf{a})$ , thus there is an informative protocol for one if and only if there is an informative protocol for the other. This equivalence does not generally hold for minimally informative protocols, e.g. the protocol  $\chi_2$  of Section 6.1.  
The reason is that a click  $K_p(\bar{b})$  in  $J^{\mathbf{c}+\mathbf{r}}(n, n - \mathbf{a})$  translates into a click  $K'_p(b)$  in  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$  (see Remark 3). When  $\mathbf{c} + \mathbf{r} = 1$  safety is preserved, see Theorem 5.
- If  $d = \mathbf{c} + \mathbf{r}$ ,  $d' = \mathbf{c}' + x'$ , and  $d \leq d'$ , then  $J^d(n, \mathbf{a})$  is a subgraph of  $J^{d'}(n, \mathbf{a})$  (Remark 2). 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  $n' > n$ ).

We have the following special case. By Lemma 6, for the case when  $\mathbf{c} + \mathbf{r} = 1$  (recall Theorem 1), we have that  $B$  learns at least one card of  $A$ .

**Lemma 7.** *Let  $\mathbf{c} + \mathbf{r} = 1$ . For a minimally informative protocol  $P_A$ , there exists a decision function for  $B$ ,  $\delta_B$ , such that when the hand of  $A$  is  $a$  and  $P_A(a) = M$ , then  $\delta_B(b, M) = x$ , for some  $x \in a$ .*

Recall from Section 3.1 the graph  $\mathcal{G}_C$ . The vertices of  $\mathcal{G}_C$  consist of all the  $A$ -vertices of  $\mathcal{I}$ . There is an edge joining two vertices  $(A, a), (A, a')$  if and only if there are edges in  $\mathcal{I}$  connecting them with the same vertex  $(C, c)$ . Then,  $V(\mathcal{G}_C) = V(\mathcal{G}_B) = \mathcal{P}_{\mathbf{a}}(D)$ , and for two distinct hands  $a, a'$  of size  $\mathbf{a}$ ,  $\{a, a'\} \in E(\mathcal{G}_C)$  iff  $\exists c \in \mathcal{P}_{\mathbf{c}}(D)$  such that  $a, a' \subseteq \bar{c} = D - c$ . Namely, we have the graph  $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ , where  $K_p(\bar{c})$  induces a click, for every  $c \in \mathcal{P}_{\mathbf{c}}(D)$ . In the following the set of colors of vertices of a click is denoted,  $P_A(K_p(\bar{c})) = \{M \mid P(a) = M, a \in K_p(\bar{c})\}$ .

**Theorem 3 (Safety characterization).** *Let  $P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathcal{M}$ . The following conditions are equivalent.*

1.  $P_A$  is safe.
2. Consider any  $c \in \mathcal{P}_{\mathbf{c}}(D)$ , and any  $y \in \bar{c}$ . For each  $M \in P_A(K_p(\bar{c}))$ , there exist  $a, a' \in K_p(\bar{c})$  with  $P_A(a) = P_A(a') = M$  such that  $y \in a \Delta a'$ .

*Proof.* The equivalence is straightforward, recalling the one-to-one correspondence between hands  $c$ ,  $|c| = \mathbf{c}$  and  $C$ -vertices of  $\mathcal{I}$ , and observing that  $c \cap a$  for an  $A$ -hand  $a$  is equivalent to the existence of a deal  $I \in \mathcal{I}$  including  $(A, a), (C, c)$ . Indeed, for any  $a$  in  $P_A^{-1}(M)$ , there exists one  $c$ ,  $|c| = \mathbf{c}$  with  $c \cap a = \emptyset$ .

*Remark 5 (Safety).*

- 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 coloring of  $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ .
- Thus, by Remark 2, a protocol can be informative and safe only if  $\mathbf{b} > \mathbf{c}$ . In this case, while  $K_p(\bar{c})$  induces a click in  $J^{\mathbf{b}+\mathbf{r}}(n, \mathbf{a})$ , it does not induce a click in  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ , by Remark 3. (cf. [4, Lemma 2]).
- Joining color classes  $P_A^{-1}[M] \cup P_A^{-1}[M']$  of a protocol preserves safety, but not necessarily informative properties (see Section 6.2).

Notice that it could be that there is a hand  $c$  for  $C$ , for which some message  $M$  is never sent by  $P_A$ . But as was observed in [12, Proposition 6], with protocols that send the sum of the cards modulo  $n$  this is not the case, see Section 6 and 7.

The following argument is similar to [20, Proposition 29].

**Lemma 8.** *Let  $\mathbf{a} \geq 2$ ,  $\mathbf{c} \geq 1$ ,  $P_A$  be a safe protocol. Consider any  $M$ . For any vertex  $a \in P_A^{-1}(M)$ , any  $z \in a$ , and any card  $y$ , there must be another vertex  $a' \in P_A^{-1}(M)$  that also includes card  $z$ , and  $y \in a \Delta a'$ .*

*Proof.* Suppose that  $y \in a$  (the other case is similar). Since  $P_A$  is safe, there must be another vertex in  $P_A^{-1}(M)$  that does not include  $y$ . Consider all vertices in  $P_A^{-1}(M)$  that do not include  $y$ , denoted  $V_{\bar{y}}$ . If one of them also includes  $z$  we are done.

Thus, suppose that none of them contains  $z$ . Let  $a' \in V_{\bar{y}}$  be such that  $y \notin a'$ . Thus,  $z$  is also not in  $a'$  (else we are done).

Consider a  $\mathbf{c}$ -hand  $c$  that contains  $y$  in the complement of  $a'$ . Thus,  $C$  with hand  $c$  may hear  $M$ , but if so she knows that  $A$  does not have card  $z$ , a contradiction to the safety of  $P_A$ .

Notice that  $\mathbf{c} \geq 1$  is necessary, otherwise, Lemma 8 may not hold; an example is protocol  $\chi_1$  of Theorem 8. And clearly,  $\mathbf{a} \geq 2$  is also necessary for the lemma to hold.

*Remark 6 (The assumption  $\mathbf{a} \geq 2$ ).* A simple consequence of Theorem 3 is that we should concentrate on the case that  $\mathbf{a} \geq 2$ . If  $\mathbf{a} = 1$  then a safe protocol  $P_A$  must always send the same message  $M$ . Otherwise, if  $P_A(y) \neq P_A(y')$  for  $y, y' \in D$ , then when  $C$  has a hand  $c$ , such that  $y, y' \in \bar{c}$ , then when  $C$  hears  $P_A(y)$  she knows that  $A$  does not have card  $y'$ . Thus a safe protocol  $P_A$  cannot be minimally informative, and thus cannot be informative either.

### 3.4 Chromatic numbers

For an informative, not necessarily safe protocol, the minimum number of bits to communicate her full hand is  $\log_2 \chi$ , where  $\chi$  is the chromatic number of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ . In the case of  $\mathbf{c} + \mathbf{r} = 1$ , namely a Johnson graph, computing the chromatic number is an important open question e.g. [32, Chapter 16]. It is however known that  $n/2 \leq \chi(J(n, \mathbf{a})) \leq n$  and hence, when  $\mathbf{c} + \mathbf{r} = 1$ , the number of bits necessary and sufficient for an informative protocol is  $\Theta(\log n)$ . We show in Section 8 that in general, the number of bit is  $\Theta((\mathbf{c} + \mathbf{r}) \log n)$ .

The *safe chromatic number* of  $J^d(n, m)$ ,  $d = \mathbf{c} + \mathbf{r}$ , denoted  $\chi^{sf}$ , is the cardinality of the smallest color set  $\mathcal{M}$  for which the graph has a safe proper coloring, or  $\infty$  if no such coloring exists. We will see cases where it is  $\infty$  in Theorem 6. Recall that the safety property depends on  $\mathbf{c}$ , which is why we have to specify that  $d = \mathbf{c} + \mathbf{r}$ . For the same  $\mathbf{c}$ , we have that  $\chi \leq \chi^{sf}$ . As we shall see in Section 5, there are cases where  $\chi < \chi^{sf}$ , namely,  $\chi(J(7, 3)) = 6$  and  $\chi(J(7, 3)) = 7$ .

Similarly,  $\chi_{min}$  is the cardinality of the smallest color set  $\mathcal{M}$  for which the graph has a minimal informative coloring, and if we require additionally safety, then it is denoted  $\chi_{min}^{sf}$ . Thus,  $\chi^{min} \leq \chi_{min}^{sf} \leq \chi^{sf}$ . We will see that  $\chi_{min}^{sf}$  can be much smaller than  $\chi^{sf}$ . In an extreme case, for  $n$  even, we have that  $\chi_{min}^{sf}(J(n, n/2)) = 2$  (Corollary 2), while  $\chi^{sf}(J(n, n/2)) \geq \chi(J(n, n/2)) > n/2$  (since  $\chi(J(n, m)) \geq \max\{n - m + 1, m + 1\}$ , see Appendix B).

## 4 Russian cards problems

In Section 4.1 we present the generalized Russian cards problem and discuss its relation with our information transmission problem. Some general bounds that will be useful later on are in Section 4.2.

#### 4.1 The problem statement

The Russian cards problem has signature  $(3, 3, 1)$ , and the generalized Russian cards problem has signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ . The players  $A$ ,  $B$  and  $C$  each draw  $\mathbf{a}$ ,  $\mathbf{b}$  and  $\mathbf{c}$  cards, respectively, from the deck  $D$  of  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$  cards. In this context, *two-step protocols* have been thoroughly studied, usually when  $\mathbf{r} = 0$ . First  $A$  and then  $B$  makes an announcement, both heard by  $C$ . If a protocol  $P_A$  is informative and safe, and  $\mathbf{r} = 0$ , one may assume that  $P_B$ , the protocol of  $B$ , is simply to announce  $C$ 's set of cards. First, since the protocol  $P_A$  is informative,  $B$  knows the cards of  $A$  after  $A$ 's announcement, and hence he can deduce the cards of  $C$ . After the announcement  $P_B$ ,  $A$  can deduce the cards of  $B$ . The announcement made by  $B$  is the set of cards of  $C$ , and hence does not give any new information to  $C$ .

We consider also the case where  $\mathbf{r} > 0$ . Then on input  $b$ , once  $B$  learns the hand  $a$  of  $A$ , he announces  $D \setminus (a \cup b)$ , a superset of  $C$ 's hand. We work under this security assumption for  $\mathbf{r} > 0$ . Namely, that we allow  $C$  to learn only cards that are not held by either  $A$  or  $B$ . Among the cards held jointly by  $A$  and  $B$ , she does not learn who holds which card. With this clarification, we continue to focus only in  $P_A$ , the protocol of  $A$ . We have the following consequence of Theorem 2.

**Theorem 4.** *There is a 2-step solution for the Russian problem  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ ,  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$  with  $A$  making the first announcement, if and only if there is a safe proper coloring of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ .*

#### 4.2 General bounds

In light of Theorem 4, we keep on presenting our results in terms of safe proper colorings of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ , but one should keep in mind that they are all bounds on when there is a 2-step solution for the Russian problem  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ ,  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$  with  $A$  making the first announcement.

Recall that when  $\mathbf{c} + \mathbf{r} = 1$  there are two cases:  $\mathbf{c} = 1, \mathbf{r} = 0$ , and  $\mathbf{c} = 0, \mathbf{r} = 1$ . Thus, the following has two instantiations. The cases  $(\mathbf{a}, \mathbf{b}, 1)$  and  $(\mathbf{b}+1, \mathbf{a}-1, 1)$ , and the cases  $(\mathbf{a}, \mathbf{b}, 0)$  and  $(\mathbf{b}+1, \mathbf{a}-1, 0)$ . Remarkably, the following result does not hold for minimally informative protocols (see Corollary 2).

For a protocol  $P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathcal{M}$ , the protocol  $\bar{P}_A : \mathcal{P}_{n-\mathbf{a}}(D) \rightarrow \mathcal{M}$  is defined by

$$\bar{P}_A(a) = P_A(\bar{a}),$$

where as usual,  $\bar{a} = D \setminus a$ .

The following shows that there is a safe proper coloring of  $J(n, \mathbf{a})$  iff there is a safe proper coloring of  $J(n, n - \mathbf{a})$ .

**Theorem 5 (duality).** *Assume  $\mathbf{c} + \mathbf{r} = 1$ , so  $n = \mathbf{a} + \mathbf{b} + 1$ . A protocol  $P_A$  is informative and safe for  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$  if and only if the protocol  $\bar{P}_A$  is informative and safe for  $(\mathbf{b} + 1, \mathbf{a} - 1, \mathbf{c})$ .*

*Proof.* There are two cases:  $\mathbf{c} = 1, \mathbf{r} = 0$ , and  $\mathbf{c} = 0, \mathbf{r} = 1$ . First we show the equivalence for the informative property, in both cases.

Notice that  $n - \mathbf{a} = \mathbf{b} + 1$ . By Lemma 3, we have that  $J(n, \mathbf{a}) \cong J(n, n - \mathbf{a})$ , under the isomorphism  $f(a) = \bar{a}$ . Thus, if  $P_A$  is an informative, i.e., proper vertex coloring of  $J(n, \mathbf{a})$ , then  $\bar{P}_A(a) = P_A(f(a))$  is a proper vertex coloring of  $J(n, n - \mathbf{a})$ .

Now, consider the case  $\mathbf{c} = 1, \mathbf{r} = 0$ , and assume that  $P_A$  is safe for  $(\mathbf{a}, \mathbf{b}, 1)$ . That is, for every card  $c \in \mathcal{P}_{\mathbf{c}}(D)$ ,  $\mathbf{c} = 1$ ,  $y \in \bar{c}$ , and  $M \in P_A(K_p(\bar{c}))$ , there exists  $a, a' \in K_p(\bar{c})$ ,  $P_A(a) = P_A(a') = M$  such that  $y \in a \Delta a'$ .

To prove that  $\bar{P}_A$  is safe, we need to consider a card  $c \in \mathcal{P}_{\mathbf{c}}(D)$ , and the vertices of  $K'_p(\bar{c})$  in  $J(n, n - \mathbf{a})$ , which are  $\bar{a} \in \mathcal{P}_{n-\mathbf{a}}(D)$ , such that  $\bar{a} \subseteq \bar{c}$ .

Let  $y \in \bar{c}$ ,  $\bar{a} \in K'_p(\bar{c})$  with  $\bar{P}_A(\bar{a}) = M$ . Suppose  $y \in a$  (the case when  $y \notin a$  is similar).

Thus,  $P_A(a) = M$  and  $c \in a$ . By Lemma 8 there exists  $a' \in \mathcal{P}_{\mathbf{a}}(D)$ ,  $y \notin a'$ ,  $P_A(a') = M$ , such that  $c \in a'$ .

Now, let  $a' \in \mathcal{P}_{\mathbf{a}}(D)$ ,  $y \notin a'$ ,  $P_A(a') = M$ , with  $c \in a'$ . Then,  $c$  is in both  $a$  and  $a'$ , and hence  $c$  is in neither  $\bar{a}$  nor  $\bar{a}'$ . Namely,  $\bar{a}, \bar{a}' \in K'_p(\bar{c})$ . But  $\bar{P}_A(\bar{a}) = P_A(a') = M$ . And we are done, because  $y \in \bar{a} \Delta \bar{a}'$ .

For the converse, assume  $P_A$  is safe for  $(\mathbf{b} + 1, \mathbf{a} - 1, 1) = (n - \mathbf{a}, \mathbf{a} - 1, 1)$ , and consider  $c \in \mathcal{P}_{\mathbf{c}}(D)$ , and the vertices of  $K_p(\bar{c})$  in  $J(n, \mathbf{a})$ , which are  $a \in \mathcal{P}_{\mathbf{a}}(D)$ , such that  $a \subseteq \bar{c}$ .

Let  $y \in \bar{c}$ ,  $a \in K_p(\bar{c})$  with  $P_A(a) = M$ . Suppose  $y \in a$  (the case when  $y \notin a$  is similar).

Consider  $\bar{a}$ , and hence  $\bar{P}_A(\bar{a}) = P_A(a)$ . Thus,  $c \in \bar{a}$ . By Lemma 8 there exists  $\bar{a}' \in \mathcal{P}_{n-\mathbf{a}}(D)$ ,  $y \notin \bar{a}'$ ,  $\bar{P}_A(\bar{a}') = M$ , such that  $c \in \bar{a}'$ .

Then,  $c$  is in both  $\bar{a}$  and  $\bar{a}'$ , and hence  $c$  is in neither  $a$  nor  $a'$ . Namely,  $a, a' \in K_p(\bar{c})$ . But  $P_A(a) = P_A(a') = M$ . And we are done, because  $y \in a \Delta a'$ .

Finally, we prove the safety equivalence, for the second case, where  $\mathbf{c} = 0, \mathbf{r} = 1$ . Solving the weak Russian cards problem for the case  $(\mathbf{a}, \mathbf{b}, 0)$  is equivalent to solving it for the case  $(\mathbf{b} + 1, \mathbf{a} - 1, 0)$ . This case is easier, it does not need Lemma 8. If  $P_A$  is safe for  $(\mathbf{a}, \mathbf{b}, 0)$ , then we take  $c$  and  $\bar{c}$  as the empty set. Then, for any  $y \in D$ , and  $M$ , there exists  $a, a'$  such that  $P_A(a) = P_A(a')$ , such that  $y \in a \Delta a'$ . Then,  $y \in \bar{a} \Delta \bar{a}'$ , which is what is needed for  $\bar{P}_A$  to be safe, since  $\bar{P}_A(\bar{a}) = \bar{P}_A(\bar{a}')$ .

And the converse is the same. If  $\bar{P}_A$  is safe, then for every  $M$ , and any  $y$ , it holds  $y \in \bar{a} \Delta \bar{a}'$  for some  $\bar{a}, \bar{a}'$  of size  $n - \mathbf{a}$  such that  $\bar{P}_A(\bar{a}) = \bar{P}_A(\bar{a}')$ . And thus,  $y \in a \Delta a'$ , with  $P_A(a) = P_A(a')$ .

For instance, there is solution for the  $(4, 2, 1)$  case, because it is equivalent to a solution to  $(3, 3, 1)$ , the classic Russian cards case<sup>6</sup>. However, there is no solution for the  $(2, 4, 1)$  case, as we show in the next theorem (and was observed in [4]). The reason is that in this case we get the graph  $J(7, 2)$ , which has no safe

<sup>6</sup> This is the example of [4], “we get a 7-line good announcement for  $(4, 2, 1)$ . It may further be observed that this is the complement of a 7-line good announcement for  $(3, 3, 1)$  as found above (for no apparent reason related to designs)”.

proper coloring. Thus, while we assume that  $A$  makes the first announcement; to analyze the other case, one may exchange values of  $\mathbf{a}$  and  $\mathbf{b}$ . It may be more convenient that  $A$  makes the first announcement, or that  $B$  makes it, in terms of both solvability and communication complexity. For the first case, a coloring has to be found for  $J(n, \mathbf{a})$ , and for the second case, one for  $J(n, \mathbf{b})$ .

**Theorem 6.** *If  $\mathbf{c} + \mathbf{r} \geq \min\{\mathbf{a}, n - \mathbf{a}\} - 1$ ,  $\mathbf{c} \geq 1$ , then there is no safe proper coloring of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ .*

*Proof.* Recall that the diameter of  $J(n, \mathbf{a})$  is  $\min\{\mathbf{a}, n - \mathbf{a}\}$ . If  $\mathbf{c} + \mathbf{r} = d \geq \min\{\mathbf{a}, n - \mathbf{a}\}$  then  $J^d(n, \mathbf{a})$  is a complete graph, and each vertex must have a different color, so if  $A$  announces  $M$  then  $C$  learns that her hand is the single hand in  $\chi^{-1}(M)$ .

Assume therefore that  $d = \min\{\mathbf{a}, n - \mathbf{a}\} - 1$ ,  $\mathbf{a} \geq 2$ . We have that  $\{a, a'\} \in E(J^d(n, \mathbf{a}))$  iff  $|a \cap a'| \geq 1$ . If  $\chi$  is a safe proper coloring, consider a vertex  $a \in \chi^{-1}(M)$  that includes some card  $x$ , for some color  $M$ . The safety requirement implies that there must be another vertex  $a' \in \chi^{-1}(M)$  that also includes card  $x$ , by Lemma 8, since  $\mathbf{c} \geq 1$ . A contradiction to the claim that  $\chi$  is a proper coloring, because then  $|a \cap a'| \geq 1$ .

The requirement that  $\mathbf{c} \geq 1$  is needed. Suppose  $\mathbf{c} = 0$ . For the case  $n = 4, \mathbf{a} = 2, \mathbf{b} = 1, \mathbf{r} = 1$ , the following  $P_A$  a safe proper coloring of  $J(4, 2)$ , with three messages 0, 1, 2.

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

Recall that a protocol can be informative and safe only if  $\mathbf{b} > \mathbf{c}$  (Remark 5). Thus, combining this fact with Theorem 6, we get the following.

**Corollary 1.** *There is no informative and safe protocol if  $\mathbf{c} \geq \mathbf{b}$  or if  $\mathbf{c} + \mathbf{r} \geq \min\{\mathbf{a}, n - \mathbf{a}\} - 1$ ,  $\mathbf{c} \geq 1$ .*

There are several particular cases of interest, some previously observed<sup>7</sup>.

## 5 Six messages solutions to the Russian cards problem

We study the classic Russian cards problem [20], with signature  $(3, 3, 1)$ , and also we consider the *weak* variant where  $C$  gets no cards at all,  $(3, 3, 0)$ , both with  $n = 7$ . By Theorem 1 in both the classic or the weak variant, we need to consider colorings of the Johnson graph  $J(7, 3)$ . These provide concrete examples of the previous ideas.

<sup>7</sup> Using two different proof techniques, it was shown that if  $\mathbf{a} \leq \mathbf{c} + 1$ , there is no informative and safe solution ( $\mathbf{r} = 0$ ), in [4, Corollary 2]) and [53, Theorem 6].



The classic Russian cards problem with signature  $(3, 3, 1)$  and  $n = 7$  has been thoroughly studied, an exhaustive analysis can be found in [20]<sup>8</sup>. It is well-known that there is a uniform solution with seven messages (Theorem 12), each announcement of the same size. Only one solution is known that we are aware of with six messages [53], non-uniform. We show there is no uniform safe solution with 6 announcements (where all except one announcement are of the same size).

### 5.1 Upper bounds: information transmission with 6 messages

The chromatic number of Johnson graphs has been well studied e.g. [24], but in general, determining the chromatic number of a Johnson graph is an open problem [32, Chapter 16]. It is known that  $\chi(J(7, 3)) = 6$ , and hence there is an informative protocol with 6 messages, and no less<sup>9</sup>, by Theorem 2. We also present an explicit solution below, which is informative, but not safe for the weak version, and then a solution that is informative and safe for the weak version, but not for the classic version. At the end we prove there is no uniform solution with 6 messages for the classic version.

**Theorem 7.** *There is an informative (non-safe) protocol for the Russian cards problem sending 6 different messages, and this is optimal.*

While  $\mathcal{G}_B = J(7, 3)$  is the same for the Russian cards problem and for its weak version, for the protocol to be safe one needs to consider the possible inputs of  $C$ . In the Russian cards problem, the  $C$ -vertices are  $\mathcal{P}_{\mathbf{c}}(D)$ ,  $\mathbf{c} = 1$ , while in the weak version, there is a single  $C$ -vertex,  $(C, \emptyset)$ . We will show, that the graph  $J(7, 3)$  has a safe proper coloring in either version. Thus, there are solutions to the weak problems  $(3, 3, 0)$  and  $(4, 2, 0)$ , and similarly, for the classic problems,  $(3, 3, 1)$  and the  $(4, 2, 1)$ , by the duality Theorem 5.<sup>10</sup>

In the case of the weak Russian cards problem, there is a solution using 6 different messages. Namely, for  $J(7, 3)$ , the informative and safe chromatic number w.r.t.  $V(\mathcal{G}_C) = \emptyset$  is equal to the chromatic number  $\chi^p = \chi = 6$ . Complementary protocols (Theorem 5) solve the cases  $(3, 3, 1)$  and  $(4, 2, 1)$ , using 6 different messages, and this is optimal in terms of the number of messages (colors).

**Theorem 8.** *There is a solution for the weak Russian cards problem with 6 messages, and this is optimal.*

<sup>8</sup> Notice that for a given deal, there are 102 “direct exchanges” for the Russian cards problem [20, Corollary 41]. The direct exchanges are characterized in this paper, and the characterization can be naturally rephrased in our framework. A direct exchange corresponds in our notation to a color class,  $\chi^{-1}(M)$ , the set of hands of  $A$  on which the protocol sends message  $M$ .

<sup>9</sup> The same lower bound is [53, Theorem 4], proved by reduction to a combinatorial design theorem.

<sup>10</sup> This explains the issue raised in [4] (Example p.12): “Applying this construction, we get a 7-line good announcement for  $(4, 2, 1)$ . It may further be observed that this is the complement of a 7-line good announcement for  $(3, 3, 1)$  as found above (for no apparent reason related to designs).”

First, it is not hard to design proper 6-colorings of  $J(7, 3)$ , the following is an example:

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

For each  $i \in \{0, 1, 2, 3, 4\}$  the coloring is safe, because there are vertices  $a, a' \in \chi^{-1}[i]$ , with  $x \in a$  and  $x \notin a'$ , for each  $x \in \{0, \dots, 6\}$ . However, this coloring is not safe w.r.t.  $\mathbf{c} = 0$ , i.e. for the weak version, because there is no  $a \in \chi^{-1}[5]$ , with  $0 \in a$ . That is, if  $C$  listens to announcement 5 she learns that  $A$  does not have card 0.

To obtain a safe coloring w.r.t.  $\mathbf{c} = 0$ , we may fix  $\chi^{-1}[5]$  by adding a vertex  $a$  that contains card 0, but taking care that  $a$  is not adjacent to any vertex already there. We construct a safe variant  $\chi_1$  of  $\chi$ , by removing the vertex  $a_1 = \{012\}$  from  $\chi^{-1}[0]$  and adding it to  $\chi_1^{-1}[5]$ . We get the following 6 coloring, safe w.r.t.  $\mathbf{c} = 0$ , because by removing  $a_1$  from  $\chi^{-1}[0]$  we have not disrupted the safety of the announcement 0.

$$\begin{aligned}\chi_1^{-1}[0] &= \{034, 056, 135, 146, 236, 245\} \\ \chi_1^{-1}[1] &= \{016, 024, 035, 123, 145, 256, 346\} \\ \chi_1^{-1}[2] &= \{015, 023, 046, 124, 136, 345\} \\ \chi_1^{-1}[3] &= \{013, 026, 045, 125, 234, 356\} \\ \chi_1^{-1}[4] &= \{014, 025, 036, 126, 456\} \\ \chi_1^{-1}[5] &= \{012, 134, 156, 235, 246\}\end{aligned}$$

However, the previous coloring, is not safe w.r.t. the Russian cards problem, where the  $C$ -vertices are  $\mathcal{P}_{\mathbf{c}}(D)$ ,  $\mathbf{c} = 1$ . For example, if  $C$  has card 1 and  $A$  announces color 5, then  $C$  knows that  $A$  has hands 235 or 246, and can deduce that  $A$  has card 2 and also that she does not have card 0. Also, if  $C$  has card 0 and  $A$  announces color 4 then she knows that  $A$  has hands 126 or 456, and can deduce that  $A$  does not have 3 and she has 6.

There is an informative and safe coloring of the Russian cards problem with six messages [53],

$$\begin{aligned}\chi_2^{-1}[0] &= \{013, 026, 045, 124, 156, 235, 346\} \\ \chi_2^{-1}[1] &= \{015, 023, 046, 126, 134, 245, 356\} \\ \chi_2^{-1}[2] &= \{016, 024, 035, 123, 145, 256\} \\ \chi_2^{-1}[3] &= \{012, 036, 135, 234, 456\} \\ \chi_2^{-1}[4] &= \{056, 034, 125, 146, 236\} \\ \chi_2^{-1}[5] &= \{014, 025, 136, 246, 345\}\end{aligned}$$

## 5.2 Impossibility of uniform solutions

Here we discuss a new technique to study the structure of six message solutions to the Russian cards problem. The previous solution with six messages, partitions the 35 hands of  $A$  into color classes of size 5, 5, 5, 6, 7, 7. We prove now that this is optimal for a six message *uniform* solution, namely, two color classes must be of size 7. Thus, there is no solution with six messages with classes of sizes 5, 6, 6, 6, 6, 6 nor 5, 5, 6, 6, 6, 7.

**Theorem 9.** *There is no uniform solution to the Russian cards problem with six messages.*

*Proof.* Assume for contradiction that there is such a protocol  $P_A$ , which partitions all the 35 possible hands of  $A$  into 6 color classes. One class must have 5 hands, by a counting argument, not all can have at least 6, and it is not hard to check that a color class cannot have only 4 hands. Also, a color class cannot have more than 7 hands (as observed in [20]). Thus, the most uniform solution induces a partition of sizes 5, 6, 6, 6, 6, 6. And the less-uniform solutions are either of sizes 5, 5, 6, 6, 6, 7, or 5, 5, 5, 6, 7, 7.

A partition with 5 hands must have a single card, say 0, that appears in 3 hands. All other cards appear twice. There are 15 hands containing 0. Consider all remaining 12 hands containing 0 in the other color classes, say 2 through 6.

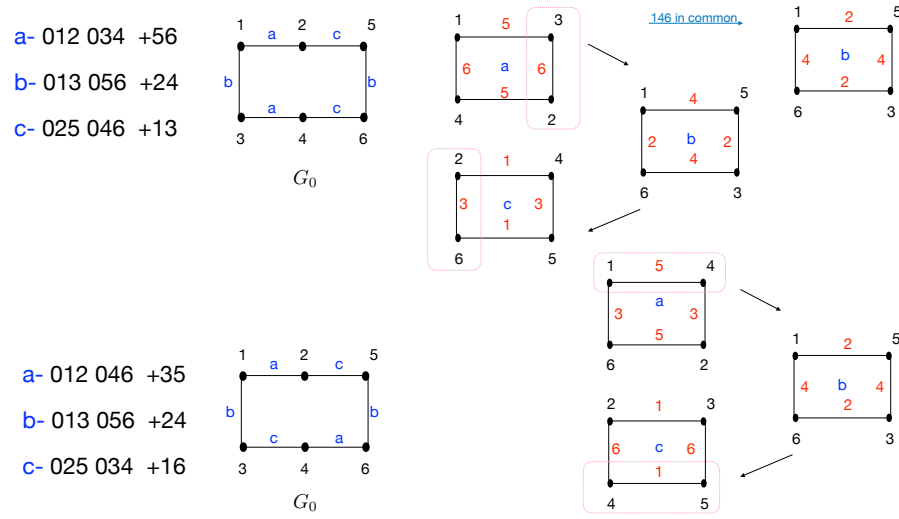
In the remaining 5 classes there must be 3 with two hands containing 0, and 2 classes with three hands containing 0. Recall that each card must appear at least twice in a color class, Lemma 8. Also, no color class can have 4 hands containing 0, because then two hands would have an intersection of 2 cards (and share an edge of  $J(7, 3)$ , violating the properness of the coloring).

Consider three color classes of size 6, denoted  $a, b, c$ , each one has exactly two hands containing 0. The case where one of these classes is of size 7, and hence it has three hands containing 0, is similar; it will be discussed at the end.

The 3 color classes  $a, b, c$  with two hands containing 0 define a graph  $G_0$  on the vertices  $D \setminus 0 = \{1, 2, 3, 4, 5, 6\}$ , each vertex representing a card. An edge of this graph is colored with an element from  $\{a, b, c\}$ , meaning that if an edge  $x, y$  is colored  $i$ , then the hand  $0xy$  is in class  $i \in \{a, b, c\}$ .

Since two hands in a class cannot have an intersection of more than one card, it follows that the edges of the same color are independent in  $G_0$ .

Now, assume for contradiction that a vertex, say 1, has degree 3. The three edges  $\{1, v_1\}, \{1, v_2\}, \{1, v_3\}$  are colored with different elements from  $\{a, b, c\}$ . As we shall see, this implies that 1 appears in three hands of each class,  $a, b, c$ . Therefore, it appears in two hands, of each of the remaining classes,  $d, e, f$ . We can thus consider the graph  $G_1$  on the vertices  $D \setminus 1$ , with edges colored with elements from  $\{d, e, f\}$ , meaning that if an edge  $x, y$  is colored  $i$ , then the hand  $1xy$  is in class  $i$ . The vertex 0 of  $G_1$  must then have degree 3, because as we shall see, this is needed for 0 to appear three times in each class  $d, e, f$ . But this implies that 0 is incident to one of  $v_1, v_2, v_3$ , say  $v_i$ , since the graph has only 6 vertices. Namely,  $\{0, v_i\}$  is an edge of  $G_1$ , and  $\{1, v_i\}$  is an edge of  $G_0$ ,



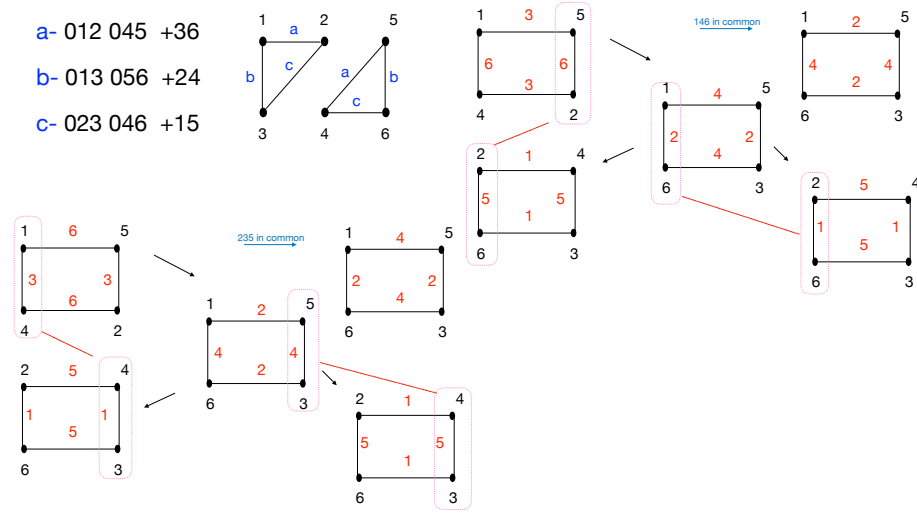
**Fig. 3.** First configuration on top 12, 34; 13, 56; 25, 46. Second configuration on bottom 12, 46; 13, 56; 25, 34. On the right part of the trees of possible ways of completing them.

so the hand  $01v_i$  appears twice, in a class of  $\{a, b, c\}$  and a class of  $\{d, e, f\}$ , a contradiction to the assumption that a vertex has degree three in  $G_0$ .

Thus, the edges of  $G_0$  either they form a cycle or two triangles. There are two types of cyclic configurations for the three classes  $a, b, c$  with two hands containing 0: either for each  $i \in \{a, b, c\}$ , the edges colored  $i$  are opposite in the cycle or not. For instance, 12, 34; 13, 56; 25, 46 (all plus 0) or else 12, 46; 13, 56; 25, 34 (all plus 0). See Figure 3 for these two cyclic configurations, and Figure 4 for the triangles case. These figures illustrate the case where 0 appears in exactly two hands, and the color classes are of size 6.

We need to complete each set of two hands to form a color class of 6 hands, by adding 4 more hands. These 4 more hands do not contain 0. The process to do it, is represented by three graphs,  $G_a, G_b, G_c$ . Now the vertices of the graph  $G_i$ ,  $i \in \{a, b, c\}$  are the four cards spanned by the two independent edges of the class  $G_i$ . There are four edges on these four vertices forming a cycle in each  $G_i$ ; each edge corresponds to a combination that *does not* appear in one of the two independent edges of  $G_i$  (because two cards that already appeared in a hand, cannot occur in another hand). The goal is to color these four edges, with the two remaining colors (0 is no longer available, because it already appears in two hands).

Notice that a loop on a vertex  $x$  could in principle be used, coloring it with the two remaining colors, giving the hand  $xyz$ , if the two remaining colors are  $yz$ . However, at most one such loop can be used (using two such loops, would give hands with intersection  $yz$ , with violets the requirement that the color is proper). And using a loop prevents using the two adjacent edges, leaving only



**Fig. 4.** The  $a, b, c$  classes define two triangles. On the right part are the trees of possible ways of completing first  $a$ , then  $b$  and then  $c$ , to have each 6 hands. Each hand is represented by an edge.

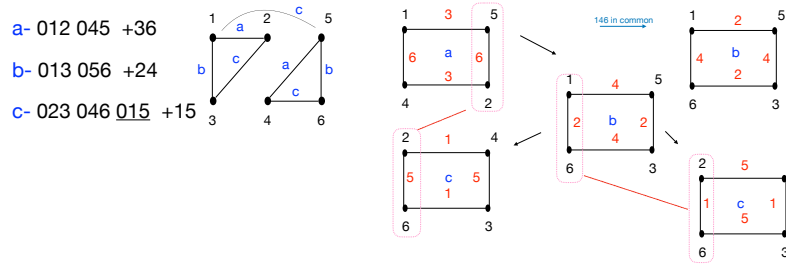
the other two, non-adjacent edges to be used, ie, coloring only 3 edges. It follows that no such loop can be used, because we need to color 4 edges, to obtain together with the 2 hands containing 0, the total number of hands which is 6 in the color class.

Consider all 4 combinations of taking one card from each pair (of 2 values different from 0). Then add each of the two remaining cards to complementary pairs, as illustrated in the figures. For example, in Figure 3, for the pairs (a) 12,34 one must add values 56. And there are only two options of getting independent edges. Add 5 to 13 and to 24; add 6 to 14 and to 23, as in the figure. Or else add 6 to 13 and to 24; add 5 to 14 and to 23.

Once 5 is added to 13 and to 24, and 6 to 14 and to 23, the next move is determined, to complete class (b). In the figure a blue arrow shows that 146 would be in common to the next class, if we added 2 to 15 and 36; and 4 to 16 and 35. Thus, the only option is the complementary choice. But then, either way, it is not possible to add 1 and 3 to class (c). In the figure one choice is shown, where 236 is repeated in classes (a) and (c). The reader can verify that in either of the two types of configurations, this process cannot be completed. The full tree for the first configuration is in Figure 11.

To complete the proof, we describe how to deal with a class of size 7, where 0 occurs in 3 hands. Actually, exactly the same argument is used, considering two hands that contain 0. This is illustrated in Figure 5, where the hand 015 of class  $c$  is underlined, to indicate that it does not play a role on the right side of the figure (in fact, this prevents it from using 15 to label a loop). Namely, in the figure, the two hands of class (c) are selected, 023,046, to complete them

with 4 hands not containing 0, into a color class of size 7 (together with 015). Thus, we have the vertices 1245 on the graph for color class (c) on the right, and the possible combinations represented by four edges forming a cycle. Each edge must be colored with 1 or 5, forming two independent edges colored 1 and 5. The tree of possibilities is therefore the same as before.



**Fig. 5.** Color class  $c$  is of size 7, where 0 is in three hands, 023, 046, 015. The first two hands 023, 046 play the same role, as in the other figures. They have to be completed with four more hands, to make a total of 7 hands.

## 6 Minimal information transmission

We study first the protocol,  $\chi_2$ , that sends the sum of the cards modulo 2. The techniques are simple, but serve as an introduction to the more complicated case of  $\chi_{mod n}$ , the mod  $n$  version of this protocol, studied in Section 7.

We show in Section 6.1 that  $\chi_2$  is minimally informative only if  $\mathbf{b} < \lfloor n/2 \rfloor$ . Thus,  $\chi_2$  is not minimally informative for the classic Russian cards case  $(3, 3, 1)$ .

In Section 6.2 we describe how to transform an informative protocol into a minimally informative protocol. Applying the reduction to  $\chi_{mod n}$ , when  $\mathbf{c} + \mathbf{r} = 1$ , as  $\mathbf{a}$  grows from 3 up to roughly  $n/2$ , the number of different messages goes down from  $n/3$  to 2.

This reduction shows that there is a safe minimally informative protocol for the Russian cards case  $(3, 3, 1)$  using 3 messages. Finally, we present a solution to the Russian cards case using only 2 messages, in Section 6.3. Given that there is no uniform safe informative protocol using 6 messages (Theorem 9), indeed this 2-message protocol splits color classes of an informative protocol.

### 6.1 Minimal information with 2 messages

For signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , with  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ , consider a protocol  $\chi_2 : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \{0, 1\}$ , defined by

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

**The protocol  $\chi_2$  is minimally informative** Recall Lemma 2. For each input vertex  $(B, b)$  denoting that  $B$  gets hand  $b$ , there are  $m = \binom{n-b}{a}$  possible hands  $a_i$  for  $A$ , corresponding to vertices  $(A, a_i)$ . In  $J^{c+r}(n, a)$  these vertices form a maximal click  $K_p(\bar{b})$  of  $\mathcal{G}_B$ ,  $p = \binom{n-b}{a}$ , consisting of all hands  $a \subset \bar{b}$ ,  $|a| = a$ . If  $b \geq \lfloor n/2 \rfloor$  then for  $b$  of size  $b$ ,  $\bar{b}$  may consist of cards of the same parity, and thus all  $a \subset \bar{b}$ ,  $|a| = a$  have the same parity, and  $\chi_2$  is not minimally informative.

**Lemma 9.** *Assume that  $c + r \geq 1$ ,  $a \geq 1$ ,  $b < \lfloor n/2 \rfloor$ . Then  $\chi_2$  is a minimally informative protocol.*

*Proof.* We use two facts. Since  $b < \lfloor n/2 \rfloor$  then  $|\bar{b}| > n - \lfloor n/2 \rfloor$ , for any  $b$  with  $|b| = b$ , and  $\bar{b}$  must contain both even and odd cards. Since  $c + r \geq 1$  (as required by the minimally informative definition), then  $a < |\bar{b}|$ .

To show that  $\chi_2$  is minimally informative, consider any click  $K_p(\bar{b})$ . Let  $a \subset \bar{b}$ ,  $|a| = a$ , be a vertex of  $K_p(\bar{b})$  with the largest number of odd cards. Since there are both even and odd cards in  $\bar{b}$ ,  $a$  contains at least one odd card,  $y$ . Since  $a$  contains the largest possible number of odd cards, it contains the minimum number of even cards. Thus, there is at least one even card  $y' \in \bar{b} \setminus a$ , given that  $|a| < |\bar{b}|$ . Let  $a' = (a \setminus y) \cup y'$ . Thus,  $a'$  is also a vertex of  $K_p(\bar{b})$ , and  $\chi_2(a) \neq \chi_2(a')$ .

**The protocol  $\chi_2$  is safe** Lemma 9 implies that  $\chi_2$  is minimally informative when  $n = 7$ ,  $a = 3$ ,  $b = 2$ ,  $c = 2$ ,  $r = 0$ , namely, for  $J^2(7, 3)$ . But it is not safe, because if  $C$  has hand  $\{1, 3\}$  and the announcement is 0 she knows that  $A$  does not have card 5. Or if the announcement is 1, she knows that  $A$  has card 5. More generally, the number of odd cards in  $D$  is  $\lfloor n/2 \rfloor$ . If  $c = \lfloor n/2 \rfloor - 1$  then when  $C$  holds  $c$  odd cards she can deduce from the announcement whether  $A$  holds the remaining odd card. Thus, assume that  $c \leq \lfloor n/2 \rfloor - 2$ , and additionally,  $a \geq 2$  (Remark 6).

In Section 7.3 we discuss the modulo  $n$  case and the relation of proving safety with additive number theory. The proof here for the modulo 2 case provides a simple illustration of the ideas.

The safety characterization of Theorem 3(2) instantiated for protocol  $\chi_2$ , says that (cf. [12, Proposition 6])  $\chi_2$  is safe (with respect to  $c$ ) if and only if for each  $c$ -set  $c$ ,  $y \in \bar{c}$ , and  $M \in \{0, 1\}$ , there exists two  $a$ -sets  $a, a' \in \bar{c}$ ,  $\chi_2(a) = \chi_2(a') = M$  such that  $y \in a \Delta a'$ .

**Lemma 10.** *Assume that  $a, b \geq 2$  and  $c \leq \lfloor n/2 \rfloor - 2$ . Then  $\chi_2$  is a safe protocol.*

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

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

Combining Lemma 9 and Lemma 10 we get the following theorem.

**Theorem 10.** *Let  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ . If  $\mathbf{a}, \mathbf{b} \geq 2$ ,  $\mathbf{c} \leq \lfloor n/2 \rfloor - 2$ ,  $\mathbf{c} + \mathbf{r} \geq 1$ , and  $\mathbf{b} < \lfloor n/2 \rfloor$ , then  $\chi_2$  is minimally informative and safe.*

Thus, for example, when  $n = 7$ ,  $\mathbf{a} = 3$ ,  $\mathbf{b} = 2$ ,  $\mathbf{c} = 1$ ,  $\mathbf{r} = 1$ , namely,  $J^2(7, 3)$ , then  $\chi_2$  is both minimally informative and safe. Similarly for  $n = 7$ ,  $\mathbf{a} = 4$ ,  $\mathbf{b} = 2$ ,  $\mathbf{c} = 1$ ,  $\mathbf{r} = 0$ , namely,  $J(7, 4)$ . Which is interesting, because it shows that the duality Theorem 5 does not hold for minimally informative protocols; notice that  $J(7, 4) \cong J(7, 3)$ , but  $\bar{\chi}_2$  is not minimally informative for  $J(7, 3)$  (neither is  $\chi_2$ ). More generally, for the Russian cards case, we get the following.

**Corollary 2.** *Assume  $\mathbf{c} + \mathbf{r} = 1$ . Then,  $\chi_2$  is minimally informative and safe, whenever  $\mathbf{a} > \lceil n/2 \rceil - 1$  and  $\mathbf{b} < \lfloor n/2 \rfloor$ .*

## 6.2 Reducing informative to minimally informative protocols

As observed in Section 6.1, the protocol  $\chi_2$  is not minimally informative when  $\mathbf{a} \leq \lceil n/2 \rceil - 1$  or  $\mathbf{b} \geq \lfloor n/2 \rfloor$ , and thus, in particular, for the Russian cards problem  $(3, 3, 1)$ ,  $\mathbf{r} = 0$ . We present here a protocol for this case, based on the  $\chi_{modn}$  protocol studied in Section 7. Notice that the protocol  $\chi_{modn}$  is safe and informative when  $\mathbf{c} + \mathbf{r} = 1$ .

The protocol uses the idea that, merging two color classes of a protocol  $P_A$ ,  $P_A^{-1}[M] \cup P_A^{-1}[M']$ , leads to a new protocol that preserves safety (but possibly not informative properties). Actually, the idea works for any safe and informative protocol  $P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathcal{M}$ . If  $|\mathcal{M}| = m$ , let us denote  $\mathcal{M} = \mathbb{Z}_m$ .

If  $P_A : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathbb{Z}_m$  is a safe proper coloring of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ ,  $\mathbf{c} + \mathbf{r} \geq 1$ , define the protocol,  $P_A^{[p]} : \mathcal{P}_{\mathbf{a}}(D) \rightarrow \mathbb{Z}_{\lceil m/(p-1) \rceil}$ , where

$$P_A^{[p]}(a) = P_A(a) \pmod{\lceil m/(p-1) \rceil},$$

$$p = \binom{\mathbf{a}+\mathbf{c}+\mathbf{r}}{\mathbf{a}} = \binom{n-\mathbf{b}}{\mathbf{a}}.$$

**Theorem 11 (Information reduction).** *If  $P_A$  is a safe and informative protocol then  $P_A^{[p]}$  is a safe and minimally informative protocol. Thus, if  $m$  is the different number of messages used by  $P_A$ , then  $\lceil m/(p-1) \rceil$  is the number of messages used by  $P_A^{[p]}$ .*

*Proof.* Notice that each color class of  $P_A^{[p]}$  consists of a union of at most  $p-1$  color classes of  $P_A$ . Since the protocol  $P_A^{[p]}$  is defined in terms of merging color classes of  $P_A$ , if  $P_A$  is safe then  $P_A^{[p]}$  is safe (follows directly from Theorem 3).

Furthermore,  $P_A^{[p]}$  is minimally informative, because the number of vertices in a click  $K_p(\bar{b})$  is  $p = \binom{\mathbf{a}+\mathbf{c}+\mathbf{r}}{\mathbf{a}} = \binom{n-\mathbf{b}}{\mathbf{a}}$ . Since  $P_A$  is informative, any two vertices



of  $K_p(\bar{b})$  belong to different color classes of  $P_A$ . Since each color class of  $P_A^{[p]}$  consists of at most  $p - 1$  color classes of  $P_A$ , then not all such  $p$  vertices can be assigned the same color by  $P_A^{[p]}$ .

In the case of  $\mathbf{c} + \mathbf{r} = 1$ , the protocol  $\chi_{modn}$  studied in Section 7 is a safe and informative protocol (Theorem 12), using  $n$  different messages. In this case,  $p = \mathbf{a} + 1$ . Thus we have the following.

**Corollary 3.** *The protocol  $\chi_{modn}^{[\mathbf{a}+1]}$  is minimally informative and safe for  $\mathbf{a}, \mathbf{b} \geq 3$ ,  $\mathbf{c} + \mathbf{r} = 1$ , using  $\lceil n/\mathbf{a} \rceil$  different messages. In particular, it uses 3 messages for the case  $(3, 3, 1)$ ,  $\mathbf{r} = 0$ .*

Notice that not every minimally informative safe protocol can be obtained by reduction from an informative protocol. Theorem 10 states that  $\chi_2$  is minimally informative and safe in some cases where

$$\mathbf{c} \geq \mathbf{b} \text{ or } \mathbf{c} + \mathbf{r} \geq \min\{\mathbf{a}, n - \mathbf{a}\} - 1. \quad (1)$$

For instance, the case of signature  $(6, 6, 8)$ ,  $\mathbf{r} = 0$ , satisfies the hypothesis of the theorem and hence  $\chi_2$  is minimally informative and safe. But recall that in such cases (1) there is no informative and safe protocol (Corollary 1).

### 6.3 A solution to the Russian Cards problem with two messages

In this section we present a solution found by Zoe Leyva-Acosta and Eduardo Pascual-Aseff, using a computer program. The following protocol  $\chi$  is a minimally informative 2-coloring of  $J(7, 3)$ .

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

In Table 1 we show for each 3-set  $b$ , how  $\chi$  partitions the 3-set vertexes in  $K_p(\bar{b})$  into two color classes, so that the reader can verify that this is in fact a minimally informative coloring for  $J(7, 3)$ . To verify that  $\chi$  is also a safe coloring, in Table 2 we show how  $\chi$  partitions  $K_p(\bar{c})$  for each card  $c$  into two color classes. The reader can check that in all such partitions and for any card other than  $c$ , there is a hand which contains it and another that doesn't.

## 7 The modular protocol $\chi_{modn}$ for $\mathbf{c} + \mathbf{r} = 1$

For signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , with  $n = \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{r}$ , consider the protocol  $\chi_{modn} : \mathcal{P}_\mathbf{a}(D) \rightarrow \mathbb{Z}_n$ , defined by

$$\chi_{modn}(a) = \sum x \in a \pmod{n}.$$

All operations in this section are modulo  $n$ , working in  $\mathbb{Z}_n$ , even when not explicitly stated. We show that  $\chi_{modn}$  is informative and safe when  $\mathbf{c} + \mathbf{r} = 1$ . It is easy to see that  $\chi_{modn}$  is not informative when  $\mathbf{c} + \mathbf{r} > 1$ , and more complicated techniques are needed, discussed in Section 8.

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

**Table 1.** Color partitions of  $K_p(\bar{b})$  for each  $b$ , according to  $\chi$ 

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

**Table 2.** Color partitions of  $K_p(\bar{c})$  for each  $c$ , according to  $\chi$ 

### 7.1 $\chi_{modn}$ is informative and coding theory

The result that  $\chi_{modn}$  is informative when  $\mathbf{c} + \mathbf{r} = 1$  is known and easy [12]. But our perspective that this is equivalent to being a proper vertex coloring of

$J(n, \mathbf{a})$  exposes the connection with coding theory. It is actually the argument (generalized in Section 8 to  $\mathbf{c} + \mathbf{r} > 1$ ) behind a classic coding theory proof that shows a lower bound on  $A(n, 4, w)$ , the maximum number of codewords in any binary code of length  $n$ , constant weight  $w$ , and Hamming distance 4 [33, Theorem 1].

**Lemma 11.** *For  $\mathbf{c} + \mathbf{r} = 1$ ,  $\chi_{\text{mod}n}$  is a proper vertex coloring of  $J(n, \mathbf{a})$ , for  $1 \leq \mathbf{a} < n$ .*

*Proof.* Let  $a = \{x_1, x_2, \dots, x_{\mathbf{a}}\}$  and  $a' = \{x'_1, x_2, \dots, x_{\mathbf{a}}\}$  be adjacent vertices of  $J(n, \mathbf{a})$ ,  $x_1 \neq x'_1$ . Thus,  $a \cap a' = \{x_2, \dots, x_{\mathbf{a}}\}$  and  $a \triangle a' = \{x_1, x'_1\}$ . If  $\mathbf{a} \geq 2$ , let  $k = \sum x \in a \cap a' \pmod{n}$ , else remove  $k$  from the following equation. Then  $\sum x \in a \equiv x_1 + k \pmod{n}$ , and  $\sum x \in a' \equiv x'_1 + k \pmod{n}$ . Thus,  $\chi_{\text{mod}n}(a) \neq \chi_{\text{mod}n}(a')$ , since  $x_1 \neq x'_1$  and  $0 \leq x_1, x'_1 \leq n - 1$ .

Notice that taking the sum modulo a number smaller than  $n$  may not give a proper coloring. For example, for  $J(7, 3)$ ,  $a = \{012\}$ ,  $a' = \{126\}$ ,  $\sum x \in a \pmod{6} = \sum x \in a' \pmod{6} = 3$ . Yet, we know from Theorem 7 that there is a proper coloring of  $J(7, 3)$  with 6 colors.

## 7.2 Additive number theory for safety

We have already hinted in Section 6.1 that proving that the modular protocol is safe translates into a question about additive number theory. For each  $M \in \mathbb{Z}_n$ , we look for solutions to the following linear congruence in  $\mathbb{Z}_n$ ,

$$x_1 + x_2 + \dots + x_{\mathbf{a}} \equiv M \pmod{n} \quad (2)$$

with distinct  $x_i \in \mathbb{Z}_n$ . Additionally, for any given  $\mathbf{c}$ -subset  $c$  of  $\mathbb{Z}_n$ , we want that no  $x_i \in c$ . Such a solution is denoted  $a$ , since it corresponds to an  $\mathbf{a}$ -set, a vertex  $a \in K_p(\bar{c})$ , and it is said to *avoid*  $c$ . For  $y \in \mathbb{Z}_n$  and a solution  $a$  to the linear congruence, we say that  $y \in a$ , if  $y = x_i$  for some  $x_i$  in the solution. Finally, we need to show that for any  $y \in \mathbb{Z}_n$ ,  $y \notin c$  there are two  $c$ -avoiding solutions,  $a, a'$ , such that  $y \in a$  and  $y \notin a'$ .

The safety proofs are based on simple properties about solutions to equation (2), stated for the general case of  $\mathbf{c} + \mathbf{r} \geq 1$ . And Lemma 14, which does not talk about  $\mathbf{c} + \mathbf{r}$  at all.

We already used the shifting technique in Section 3.2. For a vertex  $a$ , and cards  $i, j$ , with  $i \notin a$ ,  $j \in a$ ,  $a_{ij} = (a \setminus j) \cup \{i\}$ , denoted by an arc  $a \xrightarrow{ij} a_{ij}$ . For set  $c$ , we say that  $a'$  is *c-avoiding-reachable* from  $a$  if there is a directed path defined by a (possibly empty) sequence of arcs  $\xrightarrow{ij}$ , all of them with  $i \notin c$ . The *weight* of arc  $a \xrightarrow{ij} a_{ij}$  is  $i - j$ , and the weight of a sequence of arcs is the sum of their weights. We are interested in zero-sum paths, because if there is a zero-sum path from  $a$  to  $a'$ , then  $\chi_{\text{mod}n}(a) = \chi_{\text{mod}n}(a')$ . We use the following simple idea repeatedly, illustrated in Figure 6.

**Lemma 12.** *Let  $c$  be a  $\mathbf{c}$ -set and  $a$  an  $\mathbf{a}$ -set,  $a \subseteq \bar{c}$ , with  $\mathbf{a} \geq 2$ . Consider two cards  $z_1, z_2 \in a$ . If there exists an integer  $i$ ,  $1 \leq i \leq \lfloor (z_2 - z_1 - 1)/2 \rfloor$  such that both  $z_1 + i \notin a \cup c$  and  $z_2 - i \notin a \cup c$ , then let  $y_1 = z_1 + i$  and  $y_2 = z_2 - i$ . The following is a zero-sum,  $c$ -avoiding path from  $a$  to  $a'$*

$$a \xrightarrow{y_1 z_1} a_1 \xrightarrow{y_2 z_2} a'.$$

Thus,  $\chi_{\text{mod } n}(a) = \chi_{\text{mod } n}(a')$ , and  $a' \cap (c \cup \{z_1, z_2\}) = \emptyset$  and  $a \cap (c \cup \{y_1, y_2\}) = \emptyset$ .

An immediate application of Lemma 12 is the following, illustrated in Figure 6.

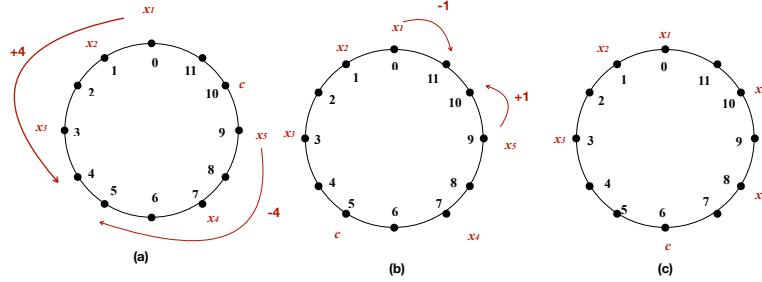
**Lemma 13.** *Assume  $\mathbf{a} \geq 2$ ,  $\mathbf{c} \geq 0$ , and  $\mathbf{a} + \mathbf{c} < n/2$ . Let  $c$  be a  $\mathbf{c}$ -set and  $a$  an  $\mathbf{a}$ -set,  $a \subseteq \bar{c}$ . For any two  $z_1, z_2 \in a$  there exist  $y_1, y_2$  such that the following is a zero-sum,  $c$ -avoiding path from  $a$  to  $a'$*

$$a \xrightarrow{y_1 z_1} a_1 \xrightarrow{y_2 z_2} a'.$$

Thus,  $\chi_{\text{mod } n}(a) = \chi_{\text{mod } n}(a')$ , and  $a' \cap (c \cup \{z_1, z_2\}) = \emptyset$  and  $a \cap (c \cup \{y_1, y_2\}) = \emptyset$ .

*Proof.* Let  $\ell_1 = z_2 - z_1 - 1$  and  $\ell_2 = z_1 - z_2 - 1$ . Thus,  $\ell_1$  is the number of cards in the interval  $(z_1, z_2)$  and  $\ell_2$  is the number of cards in the interval  $(z_2, z_1)$ .

Let  $i$ ,  $1 \leq i \leq \lfloor \ell_1/2 \rfloor$  be the smallest positive integer such that both  $z_1 + i \notin a \cup c$  and  $z_2 - i \notin a \cup c$ . If there exists such an integer, we are done, taking  $y_1 = z_1 + i$  and  $y_2 = z_2 - i$ , noticing that  $y_1 \neq y_2$ , since  $i \leq \lfloor \ell_1/2 \rfloor$ . Figure 6 illustrates three cases. Otherwise, repeat the same argument on the



**Fig. 6.** Case  $n = 12$ ,  $\mathbf{a} = 5$ ,  $\mathbf{c} = 1$ ,  $\mathbf{r} = 0$  of Lemma 13, where  $a = \{x_1, x_2, x_3, x_4, x_5\}$ . In case (c) there is no two-step  $c$ -avoiding path for  $x_1, x_5$

other side, and we are done if there exists  $i$ ,  $1 \leq i \leq \lfloor \ell_2/2 \rfloor$  such that both  $z_1 - i \notin a \cup c$  and  $z_2 + i \notin a \cup c$ . Thus (if we are not done), there is a subset  $a_1$  of  $\{z_1 + 1, z_1 + 2, \dots, z_2 - 1\}$  such that  $a_1 \subseteq a \cup c$ , and  $|a_1| \geq \lfloor \ell_1/2 \rfloor$ , and similarly, a subset  $a_2$  of  $\{z_1 - 1, z_1 - 2, \dots, z_2 + 1\}$  such that  $a_2 \subseteq a \cup c$ , and  $|a_2| \geq \lfloor \ell_2/2 \rfloor$ , and such that  $|a_1| + |a_2| + |\{z_1, z_2\}| = \mathbf{a} + \mathbf{c}$ .

Hence,  $\mathbf{a} + \mathbf{c} \geq \lfloor \ell_1/2 \rfloor + \lfloor \ell_2/2 \rfloor + 2$ . But recall that  $\ell_1 + \ell_2 = n - 2$ , and thus, a simple case analysis about the parity of  $\ell_1$  and  $\ell_2$  shows that  $\lfloor \ell_1/2 \rfloor + \lfloor \ell_2/2 \rfloor + 2 \geq n/2$ , a contradiction to the assumption that  $\mathbf{a} + \mathbf{c} < n/2$ .

The previous Lemma 13 does not apply for  $J(7, 3)$ , because in this case  $\mathbf{a} = 3, \mathbf{c} = 1$  and  $\mathbf{a} + \mathbf{c} > n/2$ . Indeed, the claim of the lemma is false in this case. For example, taking  $a = \{0, 1, 4\}$ , and selecting  $x_1 = 0, x_3 = 4$ , the only possible  $a'$  is  $a' = \{5, 6\}$ , so in this case neither 5 nor 6 can take the value for  $c$ , they cannot be avoided. To deal with the symmetric case, where  $\mathbf{a} + \mathbf{c} = \lfloor n/2 \rfloor$ , the following lemma will be useful.

Notice the effect of shifting by one a vertex  $a = \{x_1, x_2, \dots, x_{\mathbf{a}}\}$ . Namely,  $\chi_{\text{mod } n}(\{x_1 + 1, x_2 + 1, \dots, x_{\mathbf{a}} + 1\}) = \chi_{\text{mod } n}(\{x_1, x_2, \dots, x_{\mathbf{a}}\}) + \mathbf{a}$ . Thus,

*Remark 7 (Relatively prime).* If  $\mathbf{a}, n$  are relatively prime, then for each  $m \in \mathbb{Z}_n$ , there exists an  $x_m$ , such that  $a_m = \{x_m, x_m + 1, \dots, x_m + \mathbf{a} - 1\}$ ,  $\chi_{\text{mod } n}(a_m) = m$ .

When we are satisfied that  $a$  has only  $\mathbf{a} - 1$  consecutive cards, we can use the following stronger claim.<sup>11</sup>

**Lemma 14.** *Let  $2 \leq \mathbf{a} \leq n/2$ . For each  $M \in \mathbb{Z}_n$ , and each  $x_1 \in D$ , there is an  $\mathbf{a}$ -set  $a \in \chi_{\text{mod } n}^{-1}(M)$ , consisting of at least  $\mathbf{a} - 1$  consecutive cards, starting in either  $x_1$  or  $x_1 + 1$ .*

*Proof.* For the general case where  $\mathbf{a}, n$  may not be relatively prime, assume w.l.o.g. that  $x_1 = 0$ . We prove that there are  $n$  distinct  $\mathbf{a}$ -sets  $a_r$ , such that for each  $M$ , one of them is in  $\chi_{\text{mod } n}^{-1}(M)$ . Each vertex  $a_r$  consists of  $\mathbf{a} - 1$  consecutive values starting at either 0 or 1, plus one additional value. For  $\mathbf{a} - 1 \leq r \leq 2\mathbf{a} - 2$ , let  $a_r = \{0, 1, \dots, \mathbf{a} - 2, r\}$ . Thus,

$$\begin{aligned} a_{\mathbf{a}-1} &= \{0, 1, \dots, \mathbf{a} - 2, \mathbf{a} - 1\}, \\ a_{\mathbf{a}} &= \{0, 1, \dots, \mathbf{a} - 2, \mathbf{a}\}, \\ a_{\mathbf{a}+1} &= \{0, 1, \dots, \mathbf{a} - 2, \mathbf{a} + 1\}, \\ &\vdots \\ a_{2\mathbf{a}-2} &= \{0, 1, \dots, \mathbf{a} - 2, 2\mathbf{a} - 2\}. \end{aligned}$$

Notice that each  $a_r$  consists of a set of  $\mathbf{a}$  distinct values, since we are assuming  $\mathbf{a} \leq n/2$ . Now, for  $2\mathbf{a} - 1 \leq r \leq n + \mathbf{a} - 2$ , let  $a_r = \{1, 2, \dots, \mathbf{a} - 1, r - \mathbf{a} + 1\}$ . Thus,

$$\begin{aligned} a_{2\mathbf{a}-1} &= \{1, \dots, \mathbf{a} - 1, \mathbf{a}\}, \\ a_{2\mathbf{a}} &= \{1, \dots, \mathbf{a} - 1, \mathbf{a} + 1\}, \\ a_{2\mathbf{a}+1} &= \{1, \dots, \mathbf{a} - 1, \mathbf{a} + 2\}, \\ &\vdots \\ a_{n+\mathbf{a}-2} &= \{1, \dots, \mathbf{a} - 1, n - 1\}. \end{aligned}$$

<sup>11</sup> Lemma 14 is similar to [12, Lemma 5], except that this one gives additional structure to the  $\mathbf{a}$ -sets  $a$ , for  $\mathbf{a} \leq n/2$ .

Again, each  $a_r$  consists of a set of  $\mathbf{a}$  distinct values, since we are assuming  $\mathbf{a} \leq n/2$ . Notice that  $\chi_{modn}(a_{2\mathbf{a}-1}) = \chi_{modn}(a_{2\mathbf{a}-2}) + 1 \pmod{n}$ . And in general,  $\chi_{modn}(a_{r+1}) = \chi_{modn}(a_r) + 1 \pmod{n}$ . In total, we have that  $a_{\mathbf{a}-1}, \dots, a_{n+\mathbf{a}-2}$  are  $n$  distinct values  $\pmod{n}$ . Thus, for each  $M$ , there is one  $a_r \in \chi_{modn}^{-1}(M)$ .

### 7.3 If $\mathbf{c} + \mathbf{r} = 1$ then $\chi_{modn}$ is safe

Now we show that when  $\mathbf{c} + \mathbf{r} = 1$ , the well-known codes described in Section 7.1, defined by  $\chi_{modn}^{-1}$ , are safe. We prove it using the elementary additive number theory properties (the theorem generalizes and simplifies results of [12])<sup>12</sup> of Section 7.2.

Recall the safety characterization of Theorem 3. Instantiated for protocol  $\chi_{modn}$  it says that<sup>13</sup>  $\chi_{modn}$  is safe if and only if for each  $\mathbf{c}$ -set  $c$ ,  $y \in \bar{c}$ , and  $M \in \chi_{modn}(K_p(\bar{c}))$ , there exist  $\mathbf{a}$ -sets  $a, a' \subseteq \bar{c}$ ,  $\chi_{modn}(a) = \chi_{modn}(a') = M$  such that  $y \in a \triangle a'$ . Thus, we can assume that  $\mathbf{c} = 1, \mathbf{r} = 0$ , because proving that the protocol is safe in this case, implies that it is safe when  $\mathbf{c} = 0, \mathbf{r} = 1$ .

The conditions that  $\mathbf{a}, \mathbf{b} \geq 3$  are necessary, by Corollary 1. Also,  $n \geq 7$ , because if  $\mathbf{a} = 3$  and  $n = 6$ , then the protocol is not safe. For instance, if  $C$  has hand 5 and hears announcement 4 (because  $A$  has hand  $\{0, 1, 3\}$ ), then she can deduce that  $A$  does not have card 4.

In the proof we will assume that  $\mathbf{a} \leq \lfloor n/2 \rfloor$ , by the duality Theorem 5. Furthermore, to make the proof more elegant, we prove the (almost) symmetric cases where  $\mathbf{a} + \mathbf{c} \geq n/2$  separately, in Appendix D. Then, we can use Lemma 13 directly.

**Theorem 12.** *The protocol  $\chi_{modn}$  is informative and safe when  $\mathbf{c} + \mathbf{r} = 1$ ,  $\mathbf{a}, \mathbf{b} \geq 3$ ,  $n \geq 7$ .*

*Proof.* We already saw that  $\chi_{modn}$  is informative, in Lemma 11. To prove safety, as explained above, we may assume that  $\mathbf{c} = 1, \mathbf{r} = 0$ . Also, we may assume that  $\mathbf{a} \leq \lfloor n/2 \rfloor$ , by the duality Theorem 5.

We have considered the cases where:  $n = 2\mathbf{a} + 1$  in Lemma 17,  $\mathbf{a} = n/2 - 1$  with both  $n$  and  $\mathbf{a}$  even in Lemma 18, and  $2\mathbf{a} = n$  in Lemma 19. Thus, we may assume that  $\mathbf{a} + 1 < n/2$ , and we can use Lemma 13 directly.

Consider an  $M \in \mathbb{Z}_n$  and  $c \in D$ . Let  $y \in \bar{c}$ . First we show that there is an  $\mathbf{a}$ -set  $a_1 \subseteq \bar{c}$ , such that  $y \in a_1$  and  $\chi_{modn}(a) = M$ .

<sup>12</sup> In [12, Corollary 9] it is shown that the protocol is safe when  $n$  prime, with a proof based on a non-trivial theorem by Dias da Silva and Hamidoune [17, Theorem 4.1]. Which is analogous to the Cauchy–Davenport theorem, the first theorem in additive group theory [43]. Then, this result was extended to [12, Theorem 13], proving that a protocol that announces the sum of the cards modulo  $p$  is safe, except for  $(4, 3, 1)$ ,  $(3, 4, 1)$ , where  $p$  is the least prime greater than or equal to  $\mathbf{a} + \mathbf{b} + 1$ . For this, Bertrand’s postulate, as well as a theorem of Nagura [48] was used (stating that one can always find a prime number relatively close to a given integer).

<sup>13</sup> It is similar to [12, Proposition 6], except that this proposition also says that if  $\chi_{modn}$  is safe, then for each value  $M$  of  $D$ , there is an  $a \subseteq \bar{c}$  for which  $\chi_{modn}(a) = M$ .

For  $M \in \mathbb{Z}_n$  and  $x_1 = y - 1$ , let  $a_1 = \{x_1, x_2, \dots, x_a\}$  be the set defined by Lemma 14. Thus,  $\chi_{modn}(a_1) = M$ , and  $a_1$  consists of at least  $a - 1$  consecutive cards starting in either  $x_1$  or  $x_1 + 1$ , thus,  $y \in \{x_1, x_2\}$ , and in both cases,  $y \in a_1$ . If  $a_1 \subseteq \bar{c}$  we are done.

Thus, assume  $c \in a_1$ . Then, we use Lemma 13, to remove  $c$  from  $a_1$ , without touching  $y$ . Namely, we apply the lemma with  $c$  and any other card of  $a$  different from  $y$ . We have shown that there is an  $a$ -set  $a_1 \subseteq \bar{c}$ , such that  $y \in a_1$  and  $\chi_{modn}(a_1) = M$ . Figure 7 illustrates three cases, that can be dealt with, even when  $n/2 = a + 1$ .

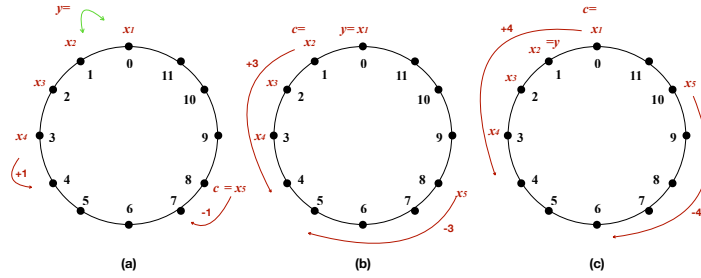


Fig. 7. Case  $n = 12$ ,  $a = 5$ ,  $c = 1$ ,  $r = 0$

To complete the proof, we need to show that there is an  $a$ -set  $a_2 \subseteq \bar{c}$ , such that  $y \notin a_2$  and  $\chi_{modn}(a_2) = M$ . This is done again by a direct application of Lemma 13, removing from  $a_1$  any two cards that include  $y$ , without including  $c$ .

## 8 Informative transmission: the general case $c + r \geq 1$

In this section we briefly discuss an informative solution when  $c + r \geq 1$ . As far as we know, this is the first informative protocol, and there is no safe and informative general solution known. Swanson et al. [54] discuss informative protocols and their relation to combinatorial designs. They explain the combinatorial difficulty of the case  $c + r \geq 1$ .

We have seen in Section 7.1 that  $\chi_{modn}$  is informative when  $c + r = 1$ , but not when  $c + r > 1$ , namely,  $\chi_{modn}$  is not a proper vertex coloring of  $J^{c+r}(n, a)$ . We are now behind the classic coding theory proof that shows a lower bound on  $A(n, 2\delta, w)$ , the maximum number of codewords in any binary code of length  $n$ , constant weight  $w$ , and Hamming distance  $2\delta$ . Namely, the proof that shows that the vertices in  $\chi_{modn}^{-i}$  in this case define a binary code of length  $n$ , constant weight  $w$ , and Hamming distance  $2\delta$ .

We rephrase the coding theory argument from [33, Theorem 4] in our notation. Let  $q$  be a primer power (positive integer power of a single prime number),  $q \geq n$ . Let the elements of the Galois field  $\text{GF}(q)$  be  $w_0, w_1, \dots, w_{q-1}$ . 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  $a = (a_0, \dots, a_{n-1}) \in \mathbb{F}_2^n$ . Define  $\bar{\chi}(a)$  to be the vector  $(\chi_1(a), \chi_2(a), \dots, \chi_d(a))$ ,

$$\begin{aligned}\chi_1(a) &= \sum_{a_i=1} w_i, \\ \chi_2(a) &= \sum_{\substack{i < j \\ a_i=a_j=1}} w_i w_j, \\ \chi_3(a) &= \sum_{\substack{i < j < k \\ a_i=a_j=a_k=1}} w_i w_j w_k, \\ &\dots\end{aligned}\tag{3}$$

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

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

**Lemma 15.**  $\bar{\chi}$  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  $\mathbb{F}_2^n$ , and such that  $\bar{\chi}(a) = \bar{\chi}(b)$ . Assume for contradiction that  $a$  and  $b$  are adjacent. Thus, there are  $2\gamma$  distinct coordinates  $r_1, \dots, r_\gamma, s_1, \dots, s_\gamma$ ,  $\gamma \leq d$ , 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

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

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

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

But a polynomial of degree  $\gamma$  over a field has at most  $\gamma$  zeros.

Thus, the set of colors needed is of size at most  $q^d$ . Which implies that there is always a set of size at most  $(2n)^d$  to properly color  $J^d(n, \mathbf{a})$ , because Bertrand's postulate states that there is a prime  $p$  such that  $n < p \leq 2n$ .

On the other hand, there is a corresponding (asymptotically in terms of  $n$ , for  $\mathbf{c} + \mathbf{r}$  constant) lower bound<sup>14</sup>. Namely, by Lemma 2, the clicks  $K_p(\bar{b})$  in  $\mathcal{G}_B$  have size  $p = \binom{\mathbf{a} + \mathbf{c} + \mathbf{r}}{\mathbf{a}}$ , and by Lemma 3,  $J^d(n, m) \cong J^d(n, n - m)$ . Thus,

<sup>14</sup> Recall that  $\binom{z+k}{k} = \frac{k^z}{\Gamma(z+1)}(1 + \frac{z(z+1)}{2k} + O(k^{-2}))$ , as  $k \rightarrow \infty$ . Thus, in more detail, the lower bound in the number of bits is  $\Theta((\mathbf{c} + \mathbf{r}) \log n - (\mathbf{c} + \mathbf{r}) \log(\mathbf{c} + \mathbf{r}))$ .



**Theorem 13.**  $\Theta((\mathbf{c} + \mathbf{r}) \log n)$  bits are needed and sufficient for an informative protocol.

## 9 Conclusions

We have presented a new perspective that brings closer together previous research on secret sharing and Russian card problems, by defining the underlying basic problem of safe information transmission from  $A$  to  $B$  in the face of an eavesdropper  $C$ . The new 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, and motivates developing new additive number theory proofs. We are able thus to prove new results, as well as explaining and unifying previously known results.

We have assumed, following these previous research lines, that the inputs are correlated, using a deck of cards. Considering a deterministic protocol  $P_A$  for  $A$ , we stayed with the common definition of safety, requiring that  $C$  does not learn any of the cards of  $A$  after listening to her announcement. Also, we considered the standard definition of informative, requiring the  $B$  learns her whole hand. We defined a new requirement, of minimal information transfer, requiring that always  $B$  learns *something* about  $A$ 's hand.

Many interesting avenues remain for future work. Some problems would imply solutions in coding theory, where much research has been done; the smallest number of messages needed for informative information transmission is equivalent to finding the chromatic number of a Johnson graph, a question of wide interest which is open even in the case of  $J(n, \mathbf{a})$ , not to mention the general case of  $J^d(n, \mathbf{a})$ . For  $d = \mathbf{c} + \mathbf{r} = 1$ , we have described solutions which show that no more than 2 additional messages are needed to go from the known proper coloring solutions with  $n - 2$  messages (or more), to a proper coloring that is additionally safe, with  $n$  messages. A thorough study of the general case  $d \geq 1$  is beyond the scope of this paper.

The colorings for minimal information transmission do not seem to have been studied before. Even very concrete cases remain open. We showed that there is a minimally informative safe protocol for the Russian cards problem  $(3, 3, 1)$  with only two messages, but the solution was found using a computer program. The modular algorithm  $\chi_2$  works only in the cases described by Theorem 10, and this solution uses 3 messages.

It would be of course interesting to consider randomized solutions, and the relation to the Fischer, Paterson and Rackoff [26] approach. They consider the problem of  $A$  and  $B$  agreeing on a bit that is secret from  $C$ , using randomized protocols. They then mention that it is not clear how to get rid of randomization, because the protocol itself is known also to  $C$ , and illustrate the difficulty with the following example, using the notion of *key set*  $\{x, y\}$ . This notion plays a crucial role in the algorithms of this paper, and subsequent ones. A key set consists of one card of  $A$  and one of  $B$ , equally likely, given the information available to  $C$ , that  $A$  holds  $x$  and  $B$  holds  $y$ , or the opposite. Then  $A$  and  $B$

can obtain a secret bit  $r$  from the key set, say  $r = 0$  if  $A$  holds the smaller card. If  $A$  announces a key set  $\{x, y\}$  by picking the smallest card in her hand for  $x$  and the smallest card not in her hand for  $y$ , then she may be revealing her entire hand by announcing  $\{x, y\}$ . Nevertheless, they describe a deterministic protocol where  $A$  and  $B$  exchange message several rounds to agree on a bit that is secret to  $C$ , that works when  $\mathbf{c} \leq \min(\mathbf{a}, \mathbf{b})/3$ ,  $\mathbf{a}, \mathbf{b} \geq 1$ . Notice that the solutions that we discuss do hide from  $C$  the location of the cards of  $A, B$ , while this is not the case for their protocol (but we have not shown that our solutions satisfy their requirement that all inputs are equally likely).

Our protocols that send one bit, by which  $B$  learns one of the cards of  $A$ , are somewhat reminiscent of the widely studied oblivious transfer problem [51], but passive, in the sense that the whole interaction consists of  $A$  sending a message to  $B$ , and  $A$  does not know which of her cards were learned by  $B$ . Namely,  $B$  has no say as to which card he wishes to learn.

Notice that a solution to the Russian cards problem implies a solution to the secret key problem. When  $\mathbf{c} = 1, \mathbf{r} = 0$ , consider the  $N = \binom{n-1}{\mathbf{a}}$  possible deals to  $A$  and  $B$ , all possible from the perspective of  $C$ , indexed from 0 to  $N - 1$  in some predetermined way, and let  $r$  the index of the actual deal. Both  $A$  and  $B$  can compute  $r$ , while  $C$  has no information about it [26]. Thus,  $A$  and  $B$  can share a string of  $\log_2 N$  bits, without revealing any of their cards to  $C$ , using the Russian cards protocol with signature  $(\mathbf{a}, \mathbf{b}, 1)$ , where  $A$  sends a string of  $\log_2(n)$  bits and  $B$  answers with a  $\log_2(n)$  bit string (again, not clear that they are all equally likely).

Many other interesting problems remain open, about the relation with combinatorial designs that has been thoroughly studied e.g. [54], about stronger security requirements e.g. [40], about fault-tolerant solutions [36], and more than two parties e.g. [22]. 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. [27], and from the Russian cards side [14,21], and of course in distributed computing, although without preserving privacy [19].

## Acknowledgements

We would like to thank Zoe Leyva-Acosta and Eduardo Pascual-Aseff for their many comments, and for finding the 2-message minimally informative solution to the Russian cards problem. Also, Jorge Armenta, for his help in the early stages of this research. This work was supported by the UNAM-PAPIIT project IN106520.

## References

1. A., H., N., O.: Quantum Probability and Spectral Analysis of Graphs. Springer, Berlin, Heidelberg (2007), chapter Johnson Graphs
2. Adams, D., Ponomarenko, V.: Distinct solution to a linear congruence. *Involve* **3**(3), 341–344 (2010). <https://doi.org/10.2140/involve.2010.3.341>, <https://doi.org/10.2140/involve.2010.3.341>

3. Albert, M., Cordon-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, Berlin, Heidelberg (2011)
4. 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)
5. Attiya, H., Bar-Noy, A., Dolev, D., Peleg, D., Reischuk, R.: Renaming in an asynchronous environment. *J. ACM* **37**(3), 524–548 (1990). <https://doi.org/10.1145/79147.79158>, <https://doi.org/10.1145/79147.79158>
6. Attiya, H., Rajsbaum, S.: Indistinguishability. *Commun. ACM* **63**(5), 90–99 (Apr 2020). <https://doi.org/10.1145/3376902>, <https://doi.org/10.1145/3376902>
7. Attiya, H., Welch, J.: *Distributed Computing: Fundamentals, Simulations and Advanced Topics*. John Wiley & Sons, Inc., USA (2004)
8. Biran, O., Moran, S., Zaks, S.: A combinatorial characterization of the distributed 1-solvable tasks. *J. Algorithms* **11**(3), 420–440 (1990). [https://doi.org/10.1016/0196-6774\(90\)90020-F](https://doi.org/10.1016/0196-6774(90)90020-F)
9. Brouwer, A.E., Shearer, J.B., Sloane, N.J.A., Smith, W.D.: A new table of constant weight codes. *IEEE Transactions on Information Theory* **36**(6), 1334–1380 (1990)
10. Brouwer, A.E., Etzion, T.: Some new distance-4 constant weight codes. *Advances in Mathematics of Communications* **5**, 417–424 (2011). <https://doi.org/10.3934/amc.2011.5.417>, <http://aimsciences.org//article/id/2563982d-5deb-4dda-aeb3-7b6d181a61a9>
11. Castañeda, A., Imbs, D., Rajsbaum, S., Raynal, M.: Generalized symmetry breaking tasks and nondeterminism in concurrent objects. *SIAM J. Comput.* **45**(2), 379–414 (2016). <https://doi.org/10.1137/130936828>, <https://doi.org/10.1137/130936828>
12. Cordon-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](http://ajc.maths.uq.edu.au/pdf/54/ajc_v54_p163.pdf)
13. Cordon-Franco, A., Ditmarsch, H., Fernández-Duque, D., Soler-Toscano, F.: A geometric protocol for cryptography with cards. *Des. Codes Cryptography* **74**(1), 113–125 (Jan 2015). <https://doi.org/10.1007/s10623-013-9855-y>, <https://doi.org/10.1007/s10623-013-9855-y>
14. Cordon-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 (Jul 2013). <https://doi.org/10.1016/j.tcs.2013.05.010>, <https://doi.org/10.1016/j.tcs.2013.05.010>
15. Correia, M., Neves, N.F., Veríssimo, P.: From consensus to atomic broadcast: Time-free byzantine-resistant protocols without signatures. *Comput. J.* **49**(1), 82–96 (Jan 2006). <https://doi.org/10.1093/comjnl/bxh145>, <https://doi.org/10.1093/comjnl/bxh145>
16. Cranston, D.W., Rabern, L.: A note on coloring vertex-transitive graphs. *The Electronic Journal of Combinatorics* **22**(2) (2015). <https://doi.org/https://doi.org/10.37236/4626>, <https://www.combinatorics.org/ojs/index.php/eljc/article/view/v22i2p1>
17. Da Silva, J.A.D., Hamidoune, Y.O.: Cyclic Spaces for Grassmann Derivatives and Additive Theory. *Bulletin of the London Mathematical Society* **26**(2), 140–146 (03 1994). <https://doi.org/10.1112/blms/26.2.140>, <https://doi.org/10.1112/blms/26.2.140>

18. Daven, M., Rodger, C.: The johnson graph  $j(n, k)$  has connectivity  $\delta$ . *Congressus Numerantium* **139**, 123–128 (1999)
19. Delporte, C., Fauconnier, H., Rajsbaum, S.: Communication complexity of wait-free computability in dynamic networks. In: Richa, A., Scheider, 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, Cham (2020). [https://doi.org/https://doi.org/10.1007/978-3-030-54921-3\\_17](https://doi.org/https://doi.org/10.1007/978-3-030-54921-3_17), [https://link.springer.com/chapter/10.1007/978-3-030-54921-3\\_17](https://link.springer.com/chapter/10.1007/978-3-030-54921-3_17)
20. van Ditmarsch, H.: The russian cards problem. *Studia Logica* **75**, 31–62 (10 2003). <https://doi.org/10.1023/A:1026168632319>
21. 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)
22. 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>, <https://doi.org/10.1007/s10878-009-9252-7>
23. ERD&, P., Heilbronn, H.: On the addition of residue classes mod  $p$ . *Arfa Arith* **9**, 149–159 (1964)
24. Etzion, T., Bitan, S.: On the chromatic number, colorings, and codes of the johnson graph. *Discrete Applied Mathematics* **70**(2), 163 – 175 (1996). [https://doi.org/https://doi.org/10.1016/0166-218X\(96\)00104-7](https://doi.org/https://doi.org/10.1016/0166-218X(96)00104-7), <http://www.sciencedirect.com/science/article/pii/0166218X96001047>
25. Fischer, M.J., Lynch, N.A., Paterson, M.: Impossibility of distributed consensus with one faulty process. *J. ACM* **32**(2), 374–382 (1985). <https://doi.org/10.1145/3149.214121>
26. 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>, <https://doi.org/10.1090/dimacs/002/11>
27. 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, Berlin, Heidelberg (1992)
28. Fischer, M.J., Wright, R.N.: An efficient protocol for unconditionally secure secret key exchange. In: *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*. p. 475–483. SODA '93, Society for Industrial and Applied Mathematics, USA (1993)
29. 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>, <https://doi.org/10.1007/BF00190803>
30. Friedman, R., Mostéfaoui, A., Rajsbaum, S., Raynal, M.: Asynchronous agreement and its relation with error-correcting codes. *IEEE Trans. Computers* **56**(7), 865–875 (2007). <https://doi.org/10.1109/TC.2007.1043>, <https://doi.org/10.1109/TC.2007.1043>
31. Godsil, C., Royle, G.F.: *Algebraic Graph Theory*, Graduate Texts in Mathematics, vol. 207. Springer (2001)

32. Godsil, C., Meagher, K.: *Erdős–Ko–Rado Theorems: Algebraic Approaches*. Cambridge Studies in Advanced Mathematics, Cambridge University Press (2015). <https://doi.org/10.1017/CBO9781316414958>
33. Graham, R., Sloane, N.: Lower bounds for constant weight codes. *IEEE Transactions on Information Theory* **26**(1), 37–43 (1980)
34. Gryniewicz, D.J., Philipp, A., Ponomarenko, V.: Arithmetic-progression-weighted subsequence sums. *Israel Journal of Mathematics* **193**(1), 359–398 (2013). <https://doi.org/10.1007/s11856-012-0119-8>, <https://doi.org/10.1007/s11856-012-0119-8>
35. Hegde, S.M., Murthy, T.S.: A partial solution to linear congruence conjecture. *National Academy Science Letters* **39**(6), 451–453 (2016). <https://doi.org/10.1007/s40009-016-0504-7>, <https://doi.org/10.1007/s40009-016-0504-7>
36. Herlihy, M., Kozlov, D., Rajsbaum, S.: *Distributed Computing Through Combinatorial Topology*. Elsevier-Morgan Kaufmann (2013). <https://doi.org/10.1016/C2011-0-07032-1>
37. Herlihy, M., Shavit, N.: The topological structure of asynchronous computability. *J. ACM* **46**(6), 858–923 (1999). <https://doi.org/10.1145/331524.331529>
38. Kirkman, T.: On a problem in combinations. *Camb. Dublin Math. J.* **2**, 191–204 (1847)
39. Koizumi, K., Mizuki, T., Nishizeki, T.: A revised transformation protocol for unconditionally secure secret key exchange. *Theory of Computing Systems* **42**(2), 187–221 (2008). <https://doi.org/10.1007/s00224-007-9052-3>, <https://doi.org/10.1007/s00224-007-9052-3>
40. Landerreche, E., Fernández-Duque, D.: A case study in almost-perfect security for unconditionally secure communication. *Des. Codes Cryptography* **83**(1), 145–168 (Apr 2017). <https://doi.org/10.1007/s10623-016-0210-y>, <https://doi.org/10.1007/s10623-016-0210-y>
41. Lynch, N.A.: *Distributed Algorithms*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1996)
42. Makarychev, Y.S., Makarychev, K.: The importance of being formal. *Mathematical Intelligencer* **23**(1) (2001)
43. Mann, H.: Additive group theory—a progress report. *Bull. Amer. Math. Soc.* **79**(6), 1069–1075 (11 1973), <https://projecteuclid.org:443/euclid.bams/1183535127>
44. Maurer, U.M., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory* **45**(2), 499–514 (1999)
45. Mizuki, T., Shizuya, H., Nishizeki, T.: Dealing necessary and sufficient numbers of cards for sharing a one-bit secret key (extended abstract). In: Stern, J. (ed.) *Advances in Cryptology — EUROCRYPT ’99*. pp. 389–401. Springer Berlin Heidelberg, Berlin, Heidelberg (1999), journal version in *Int. J. Inf. Sec.* 2002
46. Mizuki, T., Shizuya, H., Nishizeki, T.: A complete characterization of a family of key exchange protocols. *Int. J. Inf. Sec.* **1**(2), 131–142 (2002). <https://doi.org/10.1007/s102070100011>, <https://doi.org/10.1007/s102070100011>, an earlier version of the paper appears in *EUROCRYPT ’99*
47. Mostéfaoui, A., Rajsbaum, S., Raynal, M.: Conditions on input vectors for consensus solvability in asynchronous distributed systems. *J. ACM* **50**(6), 922–954 (2003). <https://doi.org/10.1145/950620.950624>, <https://doi.org/10.1145/950620.950624>

48. Nagura, J.: On the interval containing at least one prime number. *Proc. Japan Acad.* **28**(4), 177–181 (1952). <https://doi.org/10.3792/pja/1195570997>, <https://doi.org/10.3792/pja/1195570997>
49. Pease, M., Shostak, R., Lamport, L.: Reaching agreement in the presence of faults. *J. ACM* **27**(2), 228–234 (Apr 1980). <https://doi.org/10.1145/322186.322188>, <https://doi.org/10.1145/322186.322188>
50. Ramras, M., Donovan, E.: The automorphism group of a johnson graph. *SIAM Journal on Discrete Mathematics* **25**(1), 267–270 (2011). <https://doi.org/10.1137/090765596>, <https://doi.org/10.1137/090765596>
51. Schoenmakers, B.: Oblivious Transfer, pp. 884–885. Springer US, Boston, MA (2011). <https://doi.org/10.1007/978-1-4419-5906-5-9>, <https://doi.org/10.1007/978-1-4419-5906-5-9>
52. Smith, D.H., Hughes, L.A., Perkins, S.: A new table of constant weight codes of length greater than 28. *The Electronic Journal of Combinatorics* **13** (May 2006). <https://doi.org/10.37236/1162>, <https://www.combinatorics.org/ojs/index.php/eljc/article/view/v13i1a2>
53. Swanson, C.M., Stinson, D.R.: Combinatorial solutions providing improved security for the generalized russian cards problem. *Des. Codes Cryptography* **72**(2), 345–367 (Aug 2014). <https://doi.org/10.1007/s10623-012-9770-7>, <https://doi.org/10.1007/s10623-012-9770-7>
54. 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://doi.org/https://doi.org/10.37236/4019>, <https://www.combinatorics.org/ojs/index.php/eljc/article/view/v21i3p29>
55. Winkler, P.: The advent of cryptology in the game of bridge. *Cryptologia* **7**(4), 327–332 (1983). <https://doi.org/10.1080/0161-118391858053>, <https://doi.org/10.1080/0161-118391858053>

## A Related work.

There is related work in several domains: Russian card problems, Johnson graphs, coding theory, additive number theory, unconditionally secure key exchange, distributed computability and correlated inputs.

### A.1 Russian cards

Many instances of the generalized Russian cards problem have been studied, included where the cards are dealt over more than three agents and work on cryptography. The generalized Russian cards problem has close ties to the field of combinatorial designs, particularly for perfect security notions [40,54]. The traditional security requirement of the Russian cards problem, which is the one we consider,  $C$  may not know with certainty who holds any given card, that does not mean that she may not have a high probability of guessing this information correctly. To this end, stronger notions of security have been studied in these papers.

Cordón–Franco et al. [12] investigate conditions for when  $A$  or  $B$  can safely announce the sum of the cards they hold modulo the smallest prime greater than

or equal to  $n = \mathbf{a} + \mathbf{b} + \mathbf{c}$ . They hold whenever  $\mathbf{a}, \mathbf{b} > 2$  and  $\mathbf{c} = 1$ , except for the cases  $(3, 4, 1)$  and  $(4, 3, 1)$ . The exceptional cases  $(3, 4, 1)$  and  $(4, 3, 1)$  are treated separately using Haskell, and shown to work with modulo  $n$ . They observe that because  $C$  holds a single card, this also implies that  $A$  and  $B$  will learn the card deal from the announcement of the other player. For the general case when  $\mathbf{c} \geq 1$  they give a characterization of when the protocol is safe, but notice that the protocol is informative only when  $\mathbf{c} = 1$ .

Albert et al. [3] investigate both the problem of communicating the entire hand and communicating a secret bit. The analysis includes a sum announcement protocol for the case  $(k, k, 1)$ , where  $k \geq 3$ ; both players announce the sum of their cards modulo  $2k + 1$ . In addition, they show that state safe implies bit safe, and pose the open question of whether a protocol for sharing a secret bit implies the existence of a protocol for sharing states/card deals.

There are several additional ways of restating the safety property of Definition 2, such as CA2 and CA3 from [4].

**Lemma 16 (Safety characterization).** *Let  $P_A : \mathcal{P}_\mathbf{a}(D) \rightarrow \mathcal{M}$ . The following conditions are equivalent.*

1.  $P_A$  is safe.
2. For each  $M \in \mathcal{M}$ ,  $\mathbf{c}$ -set  $c$ , the following holds. Let  $X_{\bar{c}}$  be the subset of  $P_A^{-1}(M)$  avoiding  $c$ . If  $X_{\bar{c}} \neq \emptyset$  then for any  $y \notin c$ , there exist  $a, a' \in X_{\bar{c}}$  such that  $y \in a \Delta a'$ .
3. For each  $M \in \mathcal{M}$ ,
  - CA2** for every  $\mathbf{c}$ -set  $c$  the members of  $P_A^{-1}(M)$  avoiding  $c$  have empty intersection, and
  - CA3** for every  $\mathbf{c}$ -set  $c$  the members of  $P_A^{-1}(M)$  avoiding  $c$  have union consisting of all cards  $D$  except those of  $c$ .

## A.2 Johnson graphs and algebraic graph theory

As we show here, Johnson graphs capture the relations induced by correlated inputs defined by a deck of cards. Furthermore, certain vertex colorings of Johnson graphs turn out to capture essence behind information transmission with such correlated inputs. Johnson graphs, Kneser graphs and other related highly symmetric graphs have been well studied through algebraic methods [31], and in spectral analysis of graphs [1]. They are related to the Erdős–Ko–Rado Theorem, one of the fundamental results in combinatorics about intersecting families of sets. Its proof uses a simple yet useful operation called *shifting*, that we use too. The symmetry and algebraic properties of Johnson graphs are well understood, yet, although their chromatic number is important, especially in coding theory, it remains an open problem, see [32, Chapter 16] where there is a summary of known results, as well as in [10].

## A.3 Coding theory

Vertex colorings of Johnson graphs are closely related to coding theory. Coding theory captures necessary properties for information transmission with such cor-

related inputs; but the properties are not sufficient for the safety requirement that  $C$  does not learn about the inputs, for this, additional properties about the codes are needed. The independence number of the Johnson graph  $J(n, m)$  is the size of the largest constant weight code with word length  $n$ , weight  $m$ , and minimum distance 4. The chromatic number is the minimum number of parts in a partition into such constant weight codes. There is a lot of literature, due to its combinatorial interest and also applications. For instance, Smith et al. [52] extend known tables of constant weight codes of length  $n \leq 28$  up to 63, motivated by the generation of frequency hopping lists for use in assignment problems in radio networks. Large distance between codewords gives smaller overlap between lists. This leads to fewer clashes on the same frequency and so less interference. Similarly, a larger number of codewords allows larger list re-use distances in the network and again leads to lower interference.

A binary constant weight code of word length  $n$  and weight  $w$  and distance  $d$  is a collection of  $(0, 1)$ -vectors of length  $n$ , all having  $w$  ones and  $n - w$  zeros, such that any two of these vectors differ in  $d$  places. The Johnson graph  $J(n, w)$  is the graph on the binary vectors of length  $n$  and weight  $w$ , adjacent when they have Hamming distance 2.

The chromatic number of  $J(n, w)$  is the minimum number of disjoint constant weight codes of length  $n$ , weight  $w$ , and distance 4, for which the union is the set of all  $n$ -tuples with weight  $w$ . It is also the minimum number of disjoint packings of  $(w - 1)$ -subsets by  $w$ -subsets, for which the union is the set of all  $w$ -subsets of the  $n$ -set. Let  $(n, d, w)$  denote a code of length  $n$ , constant weight  $w$ , and distance  $d$ , and let  $A(n, d, w)$  denote the maximum size of an  $(n, d, w)$  code. Graham and Sloan [33] proved, for  $d = 4$ , that  $\chi(J(n, w)) \leq n$  for all  $0 \leq w \leq n$ . The proof is actually by the same algorithm of the Russian cards problem: putting the structure of abelian group on the coordinate positions, and all words with given sum of the elements in the support form a constant weight code with minimum distance 4. They present a generalization for all  $d$ , using an algorithm where a color is a vector, giving an upper bound for the number of colors need to color  $J^d(n, w)$ , and that we describe in Section 7. This and other more complicated methods, as well as explicit tables are described in [9], where the importance in combinatorics and coding of  $A(n, d, w)$  is emphasized. Although the chromatic number of Johnson graphs have been thoroughly studied, there seem to be no non-trivial general lower bounds. Apparently only a few cases are known where  $\chi(J(n, w)) < n$ , and in those cases,  $\chi(J(n, w)) \geq n - 2$ , see Brouwer and Etzion [10]. In general, determining the chromatic number of a Johnson graph is an open problem of wide interest [32].

#### A.4 Combinatorial Designs

Coding theory is an enormous topic in its own right, but some results are closely connected to another old and large topic: combinatorial designs. The theory of designs concerns itself with questions about subsets of a set possessing a high degree of regularity, thus, the generalized Russian cards problem has close ties to the field of combinatorial designs. The signature  $(3, 3, 1)$  was first considered by



Kirkman [38], who suggests a solution using a design. The design consists of seven triples, which are precisely the lines that form the projective geometric plane. Particularly for perfect security notions, designs are important, as demonstrated in [40,53,54]. Such notions require  $C$  not gaining any probabilistic advantage in guessing the fate of some set of  $\delta$  cards, *perfect  $\delta$ -security*. An equivalence between perfectly  $\delta$ -secure strategies and  $(c + \delta)$ -designs on  $n$  points with block size  $\mathbf{a}$ , when announcements are chosen uniformly at random from the set of possible announcements is established. Also, example solutions are provided, including a construction that yields perfect 1-security against when  $\mathbf{c} = 2$ , and a construction strategy with  $\mathbf{a} = 8$ ,  $\mathbf{b} = 13$ , and  $\mathbf{c} = 3$  that is perfectly 2-secure. Notice that such stronger security notions require protocols that use a larger set of possible messages.

### A.5 Additive number theory

While coding theory properties are necessary for informative properties of the protocol, to be safe, additional properties are needed, which define additive number theory problems, at least when working with additive protocols such as those in [12] and those we consider in Section 6 and 7. Announcing the cards modulo 7 was among the answers to a Moscow Mathematics Olympiad problem [42] that motivated subsequent work on Russian card problems.

Although finding solutions to a linear congruence is a classic problem, less seems to be known when the solution is required to be with distinct values [2,35], the question seems to have been studied first only fairly recently in [2], and a characterization of when a linear congruence

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots \alpha_n x_n \equiv \alpha \pmod{n}$$

with  $\alpha, \alpha_1, \dots, \alpha_n \in \mathbb{Z}$  has solutions with distinct values has been presented in [34]. The characterization implies that in our case (where the first  $\mathbf{a}$  coefficient  $\alpha_i = 1$  and the others are equal to 0) the congruence has a solution, for every  $\alpha \in \mathbb{Z}_n$ , a fact that can be proved directly rather easily (see [12, Lemma 5]), but to prove safety we need a more detailed analysis, as explained in Section 7.3. The question has interesting applications and relations to weighted subsequence sum questions, as described in these papers. Some work exists motivated by a 1964 conjecture by Erdős, and Heilbronn[23] giving lower bounds of the number of distinct sums of  $\mathbf{a}$ -subsets of  $\mathbb{Z}_n$ , later proven by Dias da Silva and Hamidoune [17], which is what is used to analyze the modular algorithm in [12].

### A.6 Unconditionally Secure Secret Key Exchange

The idea that card games could be used to achieve perfect cryptography without further assumptions proposed by Peter Winkler in 1981 in the context of the game of Bridge, led to a sequence of papers by Fischer and Wright. Peter Winkler [55] developed bidding conventions whereby one bridge player could send

her partner secret information about her hand that was totally unrelated to the actual bid and completely undecipherable to the opponents, even though the protocol was known to them. Much work has continued to be done, especially on the randomized setting, see e.g. for a more recent paper [39], and information theoretic [44].

Fischer and Wright’s [28] motivation of considering *card games*, where  $A, B, C$  draw cards from a deck of  $d$  cards, as specified by a signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , with  $\mathbf{a} + \mathbf{b} + \mathbf{c} = n = d$  (in [29] they also discuss a bit the case where there is a card which nobody gets), is as follows. It is desired correlated random initial local variables for the players, that have a simple structure and a small amount of initial information. By looking at her own cards, a player gains some information about the other players’ hands: a set of cards that appear in no other player’s hand. It is noted that if the initial local variables are uncorrelated, an eavesdropper can simulate any player over all random choices and all possible initial random values and learn the secret key. Thus, Fischer and Wright ask: We would like to know which distributions of private initial values allow any team that forms to obtain an  $n$ -bit secret key. Although their protocols use randomization, they require they *always* work, the key to be *completely* secret from a computational unbounded eavesdropper, and *exactly* known by all players (so standard techniques based on computational difficulty cannot be used).

Fischer and Wright [29] have explored in this and other papers the problem of players sharing a secret key using a deal of cards while their conversation is overheard by  $E$ , inspired by the work of Winkler. They present a general model for communication among players overheard by a passive eavesdropper  $E$ , in which all players including  $E$  are given private inputs that may be correlated. They study secret key exchange in this model. In particular, they consider the situation in which the team players are dealt hands of cards of prespecified sizes from a known deck of distinct cards. They consider both the cases where  $E$  gets the remaining card, and where she gets no card. They start with an example of a deck of four cards,  $A$  is given two, and  $B$  one. They explain that, if  $E$  does not see the remaining card or if  $A$  and  $B$  can use randomization, then  $A$  and  $B$  can agree on a perfectly secret bit. If  $E$  sees the remaining card or  $A$  and  $B$  are required to behave deterministically, then  $A$  and  $B$  cannot agree even on a weakly (strong requires equal probability) secret bit. More generally, in  *$N$ -valued multiparty secret key exchange* the players chose a value  $v$  from a known set of  $N$  values. In the *perfect* version  $E$  considers all  $N$  values equally likely, while in the *weak* version she considers all  $N$  values possible. They define it in terms of three requirements. *Agreement* is met if all parties know the secret key  $B$ ; *secrecy* is met if the eavesdropper’s probability of guessing  $B$  correctly is the same before and after hearing the communication; *uniformity* requires that  $B$  has equal probability of being any of the  $2^n$  possible  $n$ -bit sequences. Notice that there is no explicit requirement saying that the eavesdropper should not learn any of the input bits of the players (and indeed in some of their protocols the eavesdropper learns cards of the other players, e.g. the one-bit secret key exchange protocol in [27]), while this is a requirement for Russian cards games.

In particular, they show that secret key exchange is not possible if the player's inputs are not correlated. A *signature*  $(s_1, \dots, s_k; d)$  specifies the hands size  $s_i$  for each player and the deck size  $d$ . The perfect (resp. weak) capacity of a signature is the largest  $N$  such that  $N$ -valued perfect (resp.) weak) secret key exchange is possible when the deal is chosen randomly as specified by the given signature. Previous work was informal, and some studied the case of  $N = 2$  and two players.

Fischer and Wright [28] proposed a method for reducing the problem of a multi-party  $n$ -bit secret key exchange to the problem of a 2-party  $n$ -bit secret key exchange. They present a simulation (that needs randomization), and needs that the deals in the multiparty signature are large enough. Hence, using this method, one can easily extend a protocol from  $A, B$  so that it performs a  $p$ -party  $n$ -bit secret key exchange with  $p \geq 3$ . In this paper they also describe the *transformation protocol* for two parties. This protocol is later improved in [39], where a detail and clear analysis is presenting, showing that the improved transformation protocol establishes an  $n$ -bit secret key exchange for a signature  $(a, b; e)$  if and only if  $\Psi(a, b; e) \geq n$ ,  $\Psi$  a function which is approximately proportional to  $d$ , where  $d$  is the number of distinct cards in the deck. For *key set* protocols, Fischer and Wright show that  $A$  and  $B$  can share a bit if and only if  $\mathbf{a} + \mathbf{b} \geq \mathbf{c} + 2$ , this is reported in [46] (journal version of [45]), where a characterization for the signatures that are solvable by key set protocols is presented, and observe that actually the transformation protocol of Fischer and Wright [28] can deal with a case that is not solvable by key set, namely  $(3, 2; 4)$ . All this is for randomized protocols, the only case of deterministic protocols that we are aware of is Fischer, Paterson and Rackoff [26], where they give a protocol for secret bit transmission, and show it works if  $\mathbf{c} \leq \min(a, b)/3$ . Notice that this protocol is not private against the deal:  $A, B$  reveal some of their cards in the process.

## A.7 Distributed Computability

In a distributed system a set of processes communicate with each other to solve problems. The simplest kind is one where they start with input values, and decide on output values, once. In a *task* the domain is a set of input assignments to the processes, the range is a set of output assignments, and the task specification  $\Delta$  is an input/output relation between them. An input vector  $I$  specifies in its  $i$ -th entry the (private) input to the  $i$ -th process, and an output vector  $O \in \Delta(I)$  states that it is valid for each process  $i$  to produce as output the  $i$ -th entry of  $O$ , whenever the input vector is  $I$ . In more detail, a task  $\mathcal{T} = (\mathcal{I}, \mathcal{O}, \Delta)$  is defined by an input complex  $\mathcal{I}$ , an output complex  $\mathcal{O}$ , and a carrier map  $\Delta$ . An important example of a task is *consensus*, where each process is given an input from a set of possible input values, and the participating processes have to agree on one of their inputs.

Delporte et al. [19] observed that the least amount of communication that  $A$  and  $B$  need to send to each other, one has to consider a vertex coloring of the graphs  $\mathcal{I}_A$  and  $\mathcal{I}_B$ . As explained here, when  $\mathcal{I}$  corresponds to a signature  $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ , the proper coloring needed is of  $J^{\mathbf{c}+\mathbf{r}}(n, \mathbf{a})$ . This is the minimum needed so that  $A$  and  $B$  can learn each other inputs, otherwise there will be input vectors

indistinguishable to them. Here we explore the additional requirement that input vectors are indistinguishable to  $C$  after listening to the conversation.

Notions of *indistinguishability* are central in computer science, particularly in distributed computing. Representing the indistinguishability structure appropriately, exposes what can and cannot be done in a given situation [6].

A *distributed computing model* has to specify various details related to how the processes communicate with each other and what type of failures may occur, e.g. [7,41]. It turns out that different models may have different power, i.e., solve different sets of tasks.

The theory of distributed computability has been well-developed since the early 1990's [37], with origins even before [8,25], and overviewed in a book [36]. It was discovered that the reason for why a task may or may not be computable is of a topological nature. The input and output sets of vectors are best described as *simplicial complexes*, and a task can be specified by a relation  $\Delta$  from the input complex  $\mathcal{I}$  to the output complex  $\mathcal{O}$ . The main result is that a task is solvable in the layered message-passing model if and only if there is a certain subdivision of the input complex  $\mathcal{I}$  and a certain simplicial map  $\delta$  to the output complex  $\mathcal{O}$ , that respects the specification  $\Delta$ .

Notice that the requirement that  $A$  and  $B$  decide on each others inputs is closely related to the *interactive consistency* problem (and other vector consensus variants e.g. [15]), introduced early on [49] in a system where processes may fail, and has continued to be studied up to day due to its practical importance. Once a solution to interactive consistency is obtained, a solution to consensus can be obtained, if each process decides e.g. on the majority of the inputs it has received.

## A.8 Correlated input complex

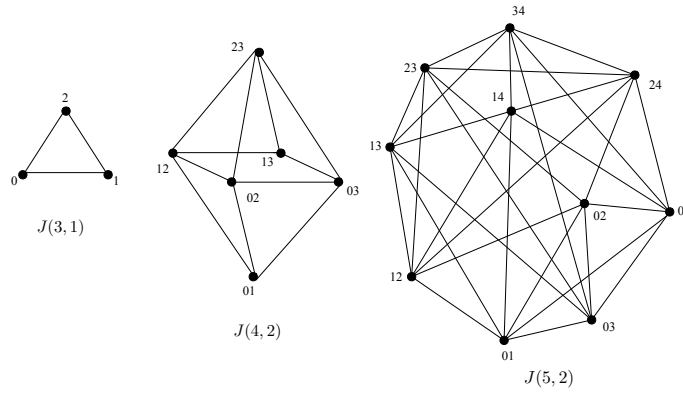
In distributed computing a common situation is when the inputs are not correlated. The input complex  $\mathcal{I}$  is called *colorless*: any input may be assigned to any process. Colorless tasks have both input and output complex colorless. Correlated inputs make the task computability analysis much more complicated. Thus, the book [36] treats first colorless tasks, and then presents more advanced topological techniques to deal with the general setting.

In various situations related to renaming, the input complex consists of assigning distinct input names to the processes, from some domain on input names. This leads to a card game where each process gets a single card. Correlated outputs have been considered for this input complex, many encompassed by the Generalized symmetry breaking family of tasks [11]. In this paper the question is considered of which correlated inputs are sufficient to solve other tasks, especially set agreement, in a wait-free read/write context.

The condition-based approach started in [47] studies subcomplexes of tasks that have a colorless input complex (consensus or set agreement), that make an unsolvable task either solvable or more efficiently solvable. Namely, how much correlation among inputs is required to solve a given task. Relations with coding theory are investigated in [30].

## B Johnson graphs

In a *Johnson graph*  $J(n, m)$  the vertices are  $m$ -subsets of a  $n$ -set, and two vertices  $a, a'$  are adjacent when  $a \cap a' = m - 1$ . In Figure B some examples are depicted. In other words, when the symmetric difference is  $|a \Delta a'| = 2$ . The special case of  $J(7, 3)$  corresponds to  $\mathcal{G}_B (= \mathcal{G}_B)$  of the classic Russian cards problem. The *Johnson distance*  $d$  of two  $m$ -sets is half the size of their symmetric difference. Thus, the graph  $J^d(n, m)$  describes the distance- $d$  relation, and  $J^1(n, m)$  is denoted  $J(n, m)$ .



**Fig. 8.** Some Johnson graphs.

Notice that the *Kneser graph*,  $K(n, m)$  is the graph on the  $m$ -subsets of an  $n$ -set, adjacent when they are disjoint. And the *generalized Johnson graph*  $J(n, m, i)$  is the graph on the  $m$ -subsets of an  $n$ -set, adjacent whenever their intersection is  $i$ . The graphs  $J(n, m, m - 1)$  are the Johnson graphs, the graphs  $J(n, m, 0)$  are the Kneser graphs. The Kneser graph  $J(5, 2, 0)$  is the famous Petersen graph. All these are highly symmetric graphs that recur throughout the book [31]. It is observed there that the following are isomorphic graphs  $J(n, m, i) \cong J(n, n - m, n - 2m + i)$ ,  $i \leq m \leq n$ , by the function that maps an  $m$ -set to its complement.

Johnson graphs are related to coding theory, Quantum probability [1, Chapter 6: Johnson Graphs] and Steiner systems, and have been thoroughly studied. Some of the more relevant facts to our study are (we provide citations unless they are easy to prove):

1. The following are isomorphic graphs  $J(n, m) \cong J(n, n - m)$ . Also,  $J(n, 1) \cong J(n, n - 1) \cong K_n$ .  $J(n, 2)$  called a *triangular graph*, which is the line graph of  $K_n$ .
2. Let  $\delta(a, a')$  denote the distance between vertices  $a, a'$  in  $J(n, m)$ . Then,  $\delta(a, a') = k$  iff  $a \cap a' = m - k$ . Thus two  $k$ -subsets are adjacent in the

Kneser graph  $K(n, k)$  if and only if they are at maximum possible distance in  $J(n, k)$ .

3.  $J(n, m)$  is distance-regular of diameter  $\min\{m, n-m\}$ .
4. The set of maximal cliques in  $J(n, m)$  are of size  $n-m+1$  and  $m+1$  see [50].
5. The chromatic number of Johnson graphs have been well studied e.g. [24], see Figure 9. But in general, determining the chromatic number of a Johnson graph is an open problem [32, Chapter 16]. For the triangular graph,  $\chi(J(n, 2)) = n$  for odd  $n$ , and  $\chi(J(n, 2)) = n-1$  for even  $n$ . It is known that  $\chi(J(n, m)) \leq n$ . Often the chromatic number is a little bit smaller. For  $n \equiv 1, 3 \pmod{6}$ ,  $n > 7$ ,  $\chi(J(n, 3)) = n-2$ . For the Russian cards case, notice that it is known that  $\chi(J(7, 3)) = 6$ .
6. As far as we know the only general (for specific instances, there are others) lower bound on the chromatic number is  $\chi(J(n, m)) \geq \max\{n-m+1, m+1\}$ , implied by the maximal cliques in the Johnson graph.
7. The Johnson graph is vertex transitive and distance transitive. For  $J(7, 3)$ , its automorphism group is  $S_7$ .
8.  $J(n, m)$  is regular of degree  $m(n-m)$ . Thus, it has vertex connectivity  $m(n-m)$ . See [18].
9. For vertex-transitive graphs with maximum degree  $\Delta \geq 13$  and clique number  $\omega$ , the Borodin-Kostochka conjecture,  $\chi \leq \max\{\omega, \Delta-1\}$  was proved in [16]. Also, if  $\omega < \Delta$  then  $\chi \leq \Delta-1$ .

$n \backslash w$	1	2	3	4	5	6	7	8
5	5	5						
6	6	5	6					
7	7	7	6					
8	8	7	7	6				
9	9	9	7	8				
10	10	9	10	8-9	8			
11	11	11	10	10	8-9			
12	12	11	11	10-11	10-11	8-9		
13	13	13	11	11-13	10-13	10-13		
14	14	13	13	11-13	11-14	10-14	10-14	
15	15	15	13	13-14	12-15	11-15	10-15	
16	16	15	16	13-14	13-15	12-15	11-16	10-15

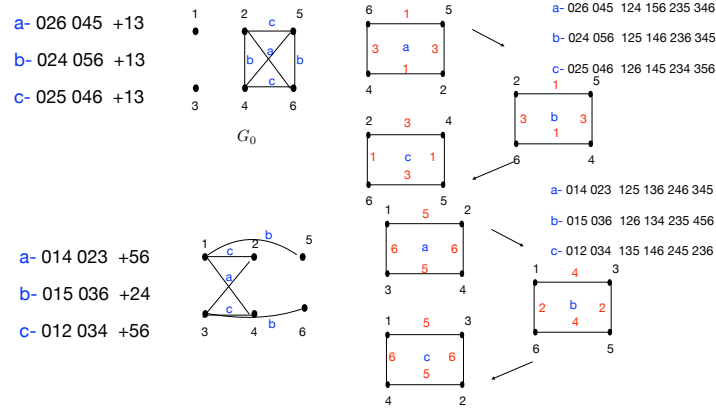
**Fig. 9.** Bounds on the chromatic number of Johnson graphs [10, Table 4]

## C Impossibility of uniform solutions to the Russian cards problem

Here we present additional details about six-message solutions to the Russian cards problem, and the impossibility of Section 5.2, in which Theorem 9 states

that there is no uniform solution to the Russian cards problem with only six messages, namely, where at most one color class is of size 7.

In the proof of Theorem 9, it is shown that it is not possible to design three color classes, where all vertices of  $G_0$  are of degree two. Figure 10 shows that it is possible, using vertices of degree 3.



**Fig. 10.** It is possible to design three color classes with vertices of degree 3, here are two examples.

The full tree is of configurations 12, 34; 13, 56; 25, 46 is in Figure 11.

## D Symmetric cases of the $\chi_{modn}$ protocol

We begin with the case of Remark 7 where  $\mathbf{a}, n$  are relatively prime (which includes [12, Corollary 9]). In particular, this takes care of cases where  $n = 2\mathbf{a} + 1$ , such as the classic<sup>15</sup> (3, 3, 1).

**Lemma 17.** *The protocol  $\chi_{modn}$  is safe when  $\mathbf{c} + \mathbf{r} = 1$ ,  $\mathbf{a}, \mathbf{b} \geq 3$ ,  $n \geq 7$  and  $\mathbf{a}, n$  are relatively prime.*

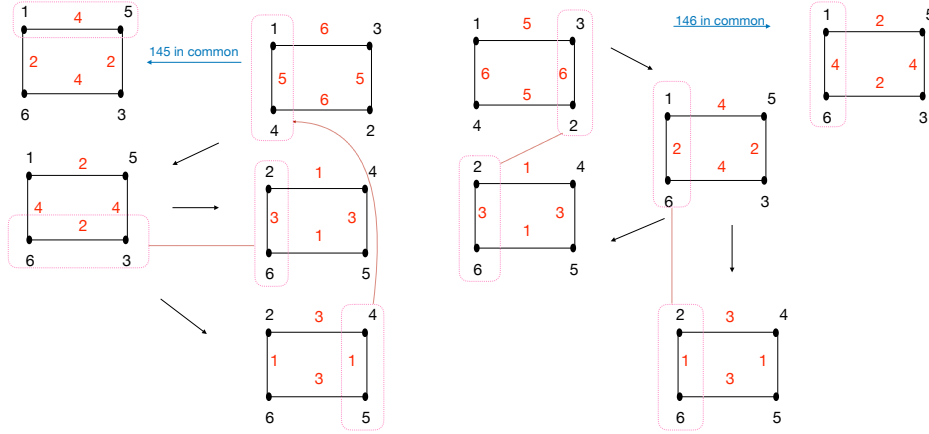
*Proof.* Assume that  $\mathbf{a} \leq \lfloor n/2 \rfloor$ , by the duality Theorem 5.

Consider an  $M \in \mathbb{Z}_n$  and  $c \in D$ . Let  $y \in \bar{c}$ .

Since  $\mathbf{a}, n$  are relatively prime (Remark 7), there exists an  $x$ , such that  $a = \{x, x + 1, \dots, x + \mathbf{a} - 1\}$  satisfies  $\chi_{modn}(a_m) = m$ . Assume w.l.o.g. that  $x = 0$ .

We consider several easy, similar cases, where we use Lemma 12 to obtain  $a'_1, a'_2 \in \bar{c}$  such that  $y \in a'_1 \triangle a'_2$ .

<sup>15</sup> Interestingly, this is the case that had to be treated separately in [12]. The cases (4, 3, 1) and (3, 4, 1) were checked using a Haskell script.



**Fig. 11.** The full tree for configuration 12, 34; 13, 56; 25, 46

Case 1: assume that both  $y$  and  $c$  are in  $a$ .

Let  $z_1 = c$  and  $z_2 = y$ , and apply the Lemma 12 to obtain  $a'_1 \in \bar{c}$ , such that  $y \notin a'_1$ . Then, let  $z_1 = c$  and  $z_2$  any card from  $a$  different from  $y$ , and apply Lemma 12 to obtain  $a'_2 \in \bar{c}$ , such that  $y \in a'_2$ .

Case 2: assume that  $y \in a$  and  $c \notin a$ .

In this case, we already have  $a = a'_2 \in \bar{c}$ , such that  $y \in a'_2$ . Thus, let  $z_1 = \mathbf{a} - y - 1$  and  $z_2 = y$ . Notice that if  $z_1 \neq z_2$  then there exists an integer  $i$ ,  $1 \leq i \leq \lfloor \ell_1/2 \rfloor$  such that both  $z_1 + i \notin a \cup c$  and  $z_2 - i \notin a \cup c$ , and we can apply Lemma 12 to obtain  $a'_1 \in \bar{c}$ , such that  $y \notin a'_1$ . Else, the conditions of the lemma hold for either  $z_1 = y - 1$  or  $z_1 = y + 1$ , with  $z_2 = y$ , to obtain  $a'_1 \in \bar{c}$ , such that  $y \notin a'_1$ .

Case 3: assume that  $y \notin a$  and  $c \notin a$ .

In this case, we already have  $a = a'_1 \in \bar{c}$ , such that  $y \notin a'_1$ . Thus, let  $z_1 = 0$  and  $z_2 = \mathbf{a} - 1$ . If there exists an integer  $i$ ,  $1 \leq i \leq \lfloor \ell_1/2 \rfloor$  such  $z_1 + i = y$  and  $z_2 - i \neq c$ , we can apply Lemma 12 to obtain  $a'_2 \in \bar{c}$ , such that  $y \in a'_2$ . Else, the conditions of the lemma hold for  $z_1 = 0$  and  $z_2 = \mathbf{a} - 2$ , to obtain  $a'_2 \in \bar{c}$ , such that  $y \in a'_2$ .

Case 4: assume that  $y \notin a$  and  $c \in a$  is similar.

We now prove the symmetric case<sup>16</sup> where  $\mathbf{a} = n/2$ .

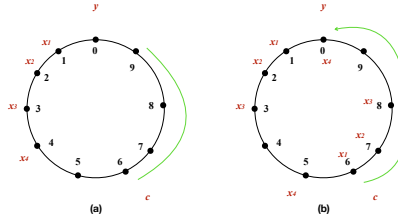
**Lemma 18.** *If  $\mathbf{a} = n/2 - 1$  with both  $n$  and  $\mathbf{a}$  even, the protocol  $\chi_{modn}$  is safe when  $\mathbf{c} + \mathbf{r} = 1$ ,  $\mathbf{a} \geq 3$ ,  $n \geq 7$ .*

*Proof.* We have that  $\gcd(n, \mathbf{a}) = 2$ , and hence for half of the values in  $z_n$  there is an  $m$  there are exactly two opposite sequences of  $\mathbf{a}$  cards,  $a$  and  $a'$  with

<sup>16</sup> Interestingly, this is the case that had to be treated separately in [12]. The cases (4, 3, 1) and (3, 4, 1) were checked using a Haskell script.



$\chi_{mod n}(a) = \chi_{mod n}(a')$ , all even. For the other half, there is a sequence of  $\mathbf{a} - 1$  consecutive, separated at the end by 1, all odd. Thus, in either case, there are exactly two values that are not covered by these opposite  $\mathbf{a}$ -sets. And it is then easy to reach these two values. Figure 12 illustrates the two cases.



**Fig. 12.** Symmetric case  $n = 10$ ,  $\mathbf{a} = 4$ ,  $\mathbf{c} = 1$ ,  $\mathbf{r} = 0$

**Lemma 19.** *If  $n = 2\mathbf{a}$ , the protocol  $\chi_{mod n}$  is safe when  $\mathbf{c} + \mathbf{r} = 1$ ,  $\mathbf{a} \geq 3$ ,  $n \geq 7$ .*

*Proof.* The arguments are similar to the above, we present only a sketch. We use Remark 7, to choose without loss of generality  $c = n/2$ . Consider the two  $\mathbf{a}$ -sets  $a_1 = \{0, 1, \dots, c-1\}$ , and  $a_2 = \{c+2, c+3, \dots, 0, 1\}$ . Notice that  $\chi_{mod n}(a_1) = \chi_{mod n}(a_2)$ , because  $a_2 = a_1 + (n/2 + 2)\mathbf{a}$ . Thus, for each card  $y \notin \{c, 0, 1\}$ ,  $y \in a_1 \triangle a_2$ . To complete the proof of this case, we use Lemma 12 as follows. Consider  $y = 0$ , and let  $a'_1$  be

$$a_1 \xrightarrow{-2,0} a_1 \xrightarrow{c+1,c-1} a'_1.$$

Thus,  $y = 0 \in a_1 \triangle a'_1$ , and  $\chi_{mod n}(a_1) = \chi_{mod n}(a'_1)$ . Similarly, consider  $y = 1$ , and let  $a'_2$  be

$$a_2 \xrightarrow{2,1} a_1 \xrightarrow{c+1,c+2} a'_2.$$

Thus,  $y = 1 \in a_2 \triangle a'_2$ , and  $\chi_{mod n}(a_2) = \chi_{mod n}(a'_2)$ .