A colouring protocol for the generalized Russian cards problem

Andrés Cordón–Franco, Hans van Ditmarsch,
David Fernández–Duque, and Fernando Soler–Toscano[*]

March 27, 2014

Abstract

In the generalized Russian cards problem, Alice, Bob and Cath draw a, b and c cards, respectively, from a deck of size $a + b + c$. Alice and Bob must then communicate their entire hand to each other, without Cath learning the owner of a single card she does not hold. Unlike many traditional problems in cryptography, however, they are not allowed to codify or hide the messages they exchange from Cath. The problem is then to find methods through which they can achieve this. We propose a general four-step solution based on finite vector spaces, and call it the "colouring protocol", as it involves colourings of lines.

Our main results show that the colouring protocol provides a solution to the generalized Russian cards problem in cases where a is a power of a prime, $c = O(a^2)$ and $b = O(c^2)$. This improves substantially on the collection of parameters for which solutions are known. In particular, it is the first solution which allows the eavesdropper to have more cards than one of the communicating players.

---
[*]Emails and affiliations: {acordon,hvd,dfduque,fsoler}@us.es, University of Sevilla, Spain. Hans van Ditmarsch is also affiliated to IMSc, Chennai, India, as a research associate.

1 Introduction

The goal of this article is to provide a solution to the *generalized Russian cards problem* [1] based on finite vector spaces. The problem is parametrized by the triple (a, b, c), which we will often call its *size* and may be stated as follows:

The generalized Russian cards problem

> Alice, Bob and Cath each draw a, b and c cards, respectively, from a deck of $a + b + c$. All players know which cards were in the deck and how many of them the other players drew, but each player may only see the cards in their own hand.
>
> Alice and Bob, however, want to know exactly which cards the other holds. Moreover, they do not want for Cath to learn who holds *any* card whatsoever, aside of course from her own cards.
>
> However, they may only do so by making unencrypted public announcements, so that Cath can learn all the information that they exchange.
>
> Can Alice and Bob achieve this?

Some general assumptions are needed to make the problem precise, which we shall formalize in Section 2. First, the cards are dealt beforehand in a secure phase which we treat as a black box and gives the players no information about others' cards. The agents have no communication before this phase and cannot share secrets (such as private keys). Second, the agents have unlimited computational capacity.[1] This means, on one hand, that solutions via encryption are not valid, provided they are vulnerable to cryptanalisis (independently of its computational cost). It also means that we shall not be concerned with the feasibility of agents' strategies, although this is certainly an important line for future inquiry. Third, all strategies are public knowledge, in keeping with Kerckhoffs' principle [4]. These assumptions turn the problem into a challenging combinatorial puzzle.

---

[1]This assumption is unusual in traditional cryptography but is standard in information-theoretic approaches where *unconditional* rather than *probabilistic* security is sought [8].

A (possible) solution to the generalized Russian cards problem is a *protocol;* these shall also be discussed formally in Section 2. The solution we propose is, to the best of our knowledge, the first solution to the generalized Russian cards problem which works in cases where Cath holds more cards than Alice.

The Russian cards problem itself originates with Kirkman [5]. There, the solution takes the form of a *design*, a collection of subsets of a given set that satisfies certain regulaties [11]. The design consists of seven triples. Cryptography based on card deals is also investigated in various other (not necessarily related) publications, such as [9, 10].

Many instances of the generalized Russian cards problem have been studied. We remark that all of these protocols obtain a notion of security called *weak 1-security* by Swanson and Stinson [12], the notion we are concerned with in this paper. A stronger and more general notion of *perfect k-security* is also considered by them but we shall not treat it here. The known solutions are as follows.

1. The original $(3, 3, 1)$ case has been extensively studied and has many solutions [5, 7].

2. The case $(4, 4, 2)$ has a three-step solution given in [13], where it is also shown that there is no two-step solution.

3. All cases $(a, 2, 1)$ provided $a \equiv 0, 4 \pmod 6$ have been solved in [1].

4. All cases $(a, b, 1)$ with both $a, b > 2$ have been solved in [2].

5. If $c + 1 < a$ then there is a solution for $b = O(a^2)$ [1].

The case $(a, b, 1)$ with $a, b > 2$ subsumes the case $(3, b, 1)$ for $b \geq 3$, also covered previously in [1]; [12] demonstrates that, for the stronger notion of perfect 1-security, every announcement in a $(3, b, 1)$ solution is a Steiner triple. They have yet another characterization result for perfect k-security.

Our main contribution is to provide solutions for infinitely many cases where $b = O(c^2)$ and either $c = O(a^{3/2})$ or $c = O(a^2)$, the first known solutions for $c > a$. We remark that all but one of the previously known protocols are two-step protocols, whereas our protocol is in four steps. In [1] it is shown that there can be no two-step solution if $c \geq a - 1$. As we provide solutions with $c > a$, the protocol we propose is longer. We do not know if a shorter, three-step variant is possible.

The plan of the paper is as follows. Section 2 formalizes our model of security and our notion of protocol. Section 3 gives an informal description of the protocol, in order to motivate the more specific description given in Definition 3.6. This protocol depends on certain parameters which do not exist for all values of (a, b, c). The conditions under which such parameters exist are treated in Section 4. Finally, Section 5 computes explicit bounds on the parameters for which the protocol is executable.

2 Protocols and security

In this section we shall present the notion of *protocol* we shall use. Throughout this paper, we assume that D is a fixed, finite set of "cards". A *card deal* is a partition (A, B, C) of D; the deal has *size* (a, b, c) if A is an a-set, B a b-set and C a c-set, where by "x-set" we mean a set of cardinality x. The set of x-subsets of Y is written $\binom{Y}{x}$. We think of A as the *hand* of Alice, or that Alice *holds* A; similarly, B and C are the hands of Bob and Cath, respectively. In general we may simply assume that $D = \{1, \ldots, a + b + c\}$, and define $\mathrm{Deal}(a, b, c)$ to be the set of partitions of D of size (a, b, c).

Central to this text is the notion of *protocol.* Roughly, a protocol is a family of rules or instructions that Alice and Bob must follow in order to send out a sequence of public announcements. Protocols are in principle non-deterministic, assigning only a probability measure to the announcements that an agent may make.

In [12] and other papers, an announcement has been modelled as a set of hands that one of the agents may hold. Thus Alice would announce a subset $\mathcal{A}$ of $\binom{D}{a}$, indicating that $A \in \mathcal{A}$. More specifically, an announcement is a pair $(i, \mathcal{A})$, where i is the agent making the announcement (either Alice or Bob). But for our proposed solution, agents' announcements are not in one-one correspondence to subsets of $\binom{D}{a}$. Because of this, it will be simpler to model announcements as elements of a countable or finite set, say $\mathbb{N}$; a similar setup is proposed in [12], where Alice enumerates all subsets of $\binom{D}{a}$ by $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_n$ and merely announces the appropriate subindex.

Thus we let $\mathrm{Ann} = \{Alice, Bob\} \times J$ be the set of announcements, where $J \subseteq \mathbb{N}$. A sequence of announcements $\vec{\alpha} = (i_0, \phi_0), (i_1, \phi_1), \ldots, (i_n, \phi_n)$ is a *run.* We shall write Run for the set of runs, including the empty sequence.

An (unusual) assumption of the problem is that there is a secure dealing phase which we treat as a black box. Initially, a card deal is selected

randomly and players have knowledge of their own cards and of the size (a, b, c) of the deal, but know nothing more about others' cards. Thus they are not able to distinguish between different deals where they hold the same hand. We model this by equivalence relations between deals; since from Alice's perspective, (A, B, C) is indistinguishable from (A, B', C'), we define $(A, B, C) \overset{Alice}{\sim} (A', B', C')$ if and only if $A = A'$. We also define analogous equivalence relations for Bob and Cath.

In [12], Swanson and Stinson define strategies of length two as assigning a probability distribution to Alice's possible announcements (after which Bob announces Cath's hand), and consider n-equitable strategies as a special case where Alice always has n possible announcements each with probability $1/n$. We will work with *equitable* strategies (and merely call them *protocols*), where probability is distributed evenly among the possible outcomes but the number of outcomes is left unspecified. This will allow us to dispense with probability measures and only determine a set of possible announcements at each stage of the protocol. On the other hand, we consider protocols which may have more than two steps, making our definition more elaborate than Swanson and Stinson's.

Definition 2.1 (Protocol)**.** *Let* Deal $=$ Deal(a, b, c).

A protocol *(with (a, b, c) as parameters) is a pair of functions (j, π) assigning to every deal $\delta \in$ Deal and every run $\vec{\alpha} \in$ Run an agent $j(\vec{\alpha}) \in \{Alice, Bob\}$ and a finite set $\pi(\delta, \vec{\alpha}) \subseteq \mathbb{N}$ such that if $\delta' \overset{j(\vec{\alpha})}{\sim} \delta$, then $\pi(\delta', \vec{\alpha}) = \pi(\delta, \vec{\alpha})$.*

Thus once a deal has been given, a protocol assigns to each run a player who is to make the next announcement and a set of possible announcements for the player to make. These announcements are determined exclusively by the information an agent has access to, which is assumed to be *only* (*i*) their hand, (*ii*) the parameters a, b, c, (*iii*) the announcements that have been made previously and (*iv*) the protocol being executed.

Protocols are non-deterministic in principle and hence may be executed in many ways; an *execution of a protocol* is a pair $(\delta, \vec{\alpha})$, where δ is a deal, $\vec{\alpha} = (i_0, \phi_0), \ldots, (i_n, \phi_n)$ a run and, for all $k < n$, $i_{k+1} = j\big((i_0, \phi_0), \ldots, (i_k, \phi_k)\big)$ and $\phi_{k+1} \in \pi\big(\delta, (i_0, \phi_0), \ldots, (i_k, \phi_k)\big)$.

The first property that a protocol needs to have in order to be successful is for its set of executions to be non-empty. This observation seems trivial but it will occupy a large portion of the paper.

5

Definition 2.2 (Executability). *Given a natural number N, a protocol is N-executable if for every deal δ there is an execution $(\delta, \vec{\alpha})$ where α has length N.*

We may omit the parameter N and let it be given by context; the protocol we propose has four steps so we take $N = 4$.

The second property that a protocol must have to be successful is that Alice and Bob know each other's cards (and hence the entire deal) after its execution:

Definition 2.3 (Informativity). *An execution $((A, B, C), \vec{\alpha})$ is informative for Alice if there is no execution $((A, B', C'), \vec{\alpha})$ with $C' \neq C$.*

Similarly, an execution $((A, B, C), \vec{\alpha})$ is informative for Bob if there is no execution $((A', B, C'), \vec{\alpha})$ with $C' \neq C$.

A protocol is informative if there exists N such that the protocol is N-executable and every execution of length N is informative both for Alice and for Bob.

The third property is that, given a card x which Cath does not hold, she should consider it possible that either Alice holds it or Bob holds it:

Definition 2.4 (Safety). *An execution $((A, B, C), \vec{\alpha})$ of a protocol (j, π) is safe if for every $x \notin C$ there is*

1. *a deal $\delta' = (A', B', C)$ such that $x \in A'$ and $(\delta', \vec{\alpha})$ is also an execution of (j, π), as well as*

2. *a deal $\delta'' = (A'', B'', C)$ such that $x \in B''$ and $(\delta'', \vec{\alpha})$ is also an execution of (j, π).*

The protocol (j, π) is safe if every execution of (j, π) is safe.

Safety is equivalent to *weak 1-security* as defined by Swanson and Stinson [12], but this is not the only notion of security they discuss. Weak security is equivalent to the statement that for all C, $x \notin C$ and every execution $\vec{\alpha}$ of the protocol,

$$0 < \Pr(x \in A | C, \vec{\alpha}) < 1$$

(where $\Pr(X|Y)$ denotes conditional probability). Stronger notions of security would demand that Cath does not gain probabilistic information, so that

$$\Pr(x \in A | C, \vec{\alpha}) = \frac{a}{a + b}$$

(perfect 1-security in [12]). In this paper we will only be concerned with weak security.

3   The protocol

In this section we shall describe the general colouring protocol, the central focus of this article. Before we do so, let us briefly describe some of the notation we shall use.

We will use p to denote a prime or a power of a prime, and $\mathbb{F}_p$ the field with p elements. If d is any natural number, $\mathbb{F}_p^d$ denotes the vector space of dimension d over $\mathbb{F}_p$. For a line $\ell = x + \lambda y$, we say y is a *directing vector* of ℓ. We denote by $\mathcal{L}_p^d$ the set of all lines in $\mathbb{F}_p^d$. The theory of finite fields and finite geometries has been extensively studied; see, for example, [6, 3].

For natural numbers d, n we define $\sigma_d(n)$ to be the sum $n^{d-1} + n^{d-2} + \ldots + n^0$. We know from basic algebra that $\sigma_d(n) = (n^d - 1)/(n - 1)$. This will be a very useful quantity to keep in mind; for example,

Lemma 3.1. *Given $x \in \mathbb{F}_p^d$, there are $\sigma_d(p)$ distinct lines passing through x.*

Let p be a prime or a prime power and $d \geq 2$. Assume that Alice holds as many cards as points in a line of $\mathbb{F}_p^d$ (i.e. $a = p$) and that Alice, Bob and Cath together hold as many cards as points in the whole space (i.e. $a + b + c = p^d$). Let K be a set of k colours, identified with the numbers $1, \ldots, k$. Colourings will be a crucial element in our protocol:

Definition 3.1 (Colouring). *A k–colouring is a function $\xi : \mathcal{L}_p^d \to K$.*

That is, ξ assigns a colour from $\{1, \ldots k\}$ to each line in $\mathbb{F}_p^d$.

Let us now give an informal account of the protocol; Definition 3.6 will give a formal version and Section 4 will study its executability. It consists of the following four steps:

1. Alice maps all the cards into $\mathbb{F}_p^d$ in such a way that her cards form a line and announces the mapping.

2. Bob announces a *suitably chosen* k-colouring ξ.

3. Alice announces the colour of her hand according to ξ.

4. Bob announces Cath's cards.

Of course, we have yet to specify what a suitable colouring is. This will be the focus of the rest of this section. In order to guarantee that the protocol is informative (Alice and Bob can deduce the card deal after the protocol's execution), the colouring must be *distinguished*, as defined below. For it to be safe (Cath cannot learn any of Alice or Bob's cards), the colouring should also be *rich*. However, colourings which are merely rich and distinguished may give Cath too much information, and thus we will have to replace the condition of being distinguished by the stronger version of being *very distinguished*. Once we have defined these notions the next question is for which a, b, c and k such colourings exist, i.e., when the protocol is executable; this shall be the topic of later sections.

First let us focus on making the protocol be informative. Given a card deal (A, B, C), we should design ξ in such a way that only A itself can be the line entirely contained in $A \cup C$ of whichever colour Alice announces. In this way, Bob can unequivocally identify A. But there may be many such spaces contained in $A \cup C$, and at the beginning of the protocol Bob has no way of telling them apart. Thus we arrive at the following:

Definition 3.2 (Distinguished colouring). *We say that a k–colouring ξ is* distinguished *for a set $E \subseteq \mathbb{F}_p^d$ if no two distinct lines contained entirely in E have the same colour.*
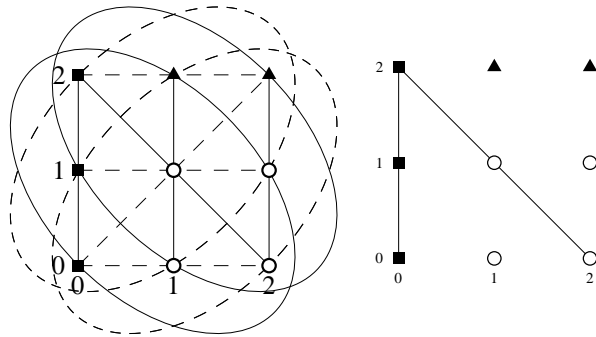

Figure 1: A simple 2-colouring.

Example 3.1. *Figure 1 illustrates the possible effects of a distinguished colouring. The left picture shows a 2-colouring that Bob announces after Alice maps the cards into $\mathbb{F}_3^2$. Throughout the examples we will continue to use black squares for Alice's cards, white circles for Bob's and black triangles*

for Cath's, so that cards held by Alice or Cath are black-filled shapes. Alice's cards A form the line $\{00, 01, 02\}$. Cath's cards C are $\{12, 22\}$. The set $A \cup C$ also contains the line $\{02, 12, 22\}$.

In order to enable Alice, by her later response, to distinguish between the lines, Bob announces the 2-colouring in the the left picture. It has two 'colours': solid lines and dashed lines. Ellipses in the figure are lines as well, e.g. $\{02, 10, 21\}$ is a dashed line.

Suppose Alice announces that her line is solid. Then, Bob will learn Alice's cards and he can announce Cath's cards. But the colouring that Bob announces is not safe. After Alice announces that her cards are a solid line, Cath discards all solid lines that meet some of her points. The right picture in Figure 1 shows the only two lines that Cath cannot discard. This makes Cath learn that Alice has 02 and that Bob has 10 and 21.

Hence, colourings that are merely distinguished will make the colouring protocol informative but not necessarily safe. To remedy this, we must have enough colours, and the colouring must be rich enough, so that for every card that Cath does not hold she should consider it possible both that Alice holds it and that Alice does not hold it.

Definition 3.3 (Rich colouring). *A k–colouring ξ is* rich *(or c–rich) if for any c-set C, colour i, and point $x \notin C$, there is an i-coloured line A containing x that avoids C and there also is an i-coloured line A' not containing x that avoids C.*

Rich and distinguished colourings are *almost* suitable, but we shall need an extra condition. Notice that Cath knows that Bob is to design the colouring so that it turns out to be informative. Thus, the colouring not only should be distinguished for the actual set of cards $A \cup C$ but also for every set of cards that Bob wants Cath to consider as possible. These will be the sets with the same *hue* as $A \cup C$:

Definition 3.4 (Hue). *Let ξ be a k-colouring.*

Given $E, F \subseteq \mathbb{F}_p^d$, we write $E \approx_1^\xi F$ if there are lines ℓ, h of the same colour such that $\ell \subseteq E$, $h \cap (E \setminus \ell) = \varnothing$ and $F = (E \setminus \ell) \cup h$. We will say E, F are one swap apart.

We then let $\approx^\xi$ be the reflexive and transitive closure of $\approx_1^\xi$, and define a hue *to be an equivalence class under $\approx^\xi$.*

9

Definition 3.5 (Very distinguished colouring)**.** *We say that a k–colouring ξ is* very distinguished *for $E \subseteq \mathbb{F}_p^d$ if ξ is distinguished for every F of the same hue as E.*
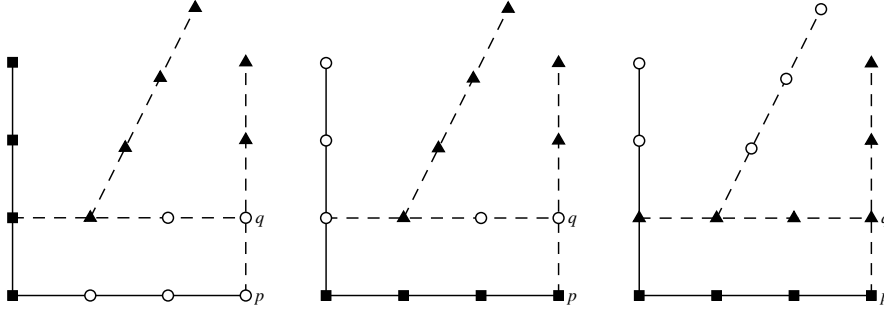

Figure 2: A 2-colouring which is distinguished but not very distinguished

Example 3.2. *Figure 2 shows an example of a 2-colouring in $\mathbb{F}_4^n$ for some n. We have represented only some points and lines in the space. Let's suppose that the colouring is 6–rich. In the situation represented on the left, the colouring is distinguished. $A \cup C$ contains two lines with different colours. But the sets of points shown in the middle and right pictures are of the same hue as $A \cup C$, and the set of points in the right picture contains two lines of the same colour. Then our colouring is not distinguished in the right picture, so it is not very distinguished in the left one.*

This means that the presented 2-colouring is not safe, even in the left picture. Cath may learn that the points p and q belong to Bob, reasoning as follows. Alice cannot have both points, because Alice's points are aligned, but she could have one of them, as can be seen in the center picture. However, if it were the case that Alice has one point (say, p), Bob should assign the line containing p, q a different colour to the other two lines in $A \cup C$, to keep Cath from learning that Bob has q. A similar reasoning applies to q, and thus Cath learns that Bob has both p and q.

With these considerations we know which kind of colouring Bob should use: a suitably chosen colouring is rich and very distinguished, and as we shall see, the protocol so defined is safe and informative. With this we may give a formal definition of our protocol. Note that it depends on a parameter k which will be specified later (see Sections 4, 5). Note also that the protocol is non-deterministic; recall that we are assuming all distributions to be uniform.

10

Definition 3.6 (Colouring protocol). *Let (a, b, c, k) be natural numbers such that a is a prime power and for some natural number d, $a + b + c = a^d$. Let $D = \{1, 2, \ldots, a+b+c\}$ and identify a natural number with (i) each bijection $f : D \to \mathbb{F}_a^d$ (ii) each k–colouring ξ, (iii) each of the k colours and (iv) each element of $\binom{D}{c}$.*

Let (A, B, C) be a deal of size (a, b, c). Then, the protocol is as follows.

1. *Alice randomly chooses a bijection $f : D \to \mathbb{F}_a^d$ in such a way that her cards form a line. She announces f.*

2. *Bob randomly chooses a k–colouring ξ which is rich and very distinguished for $A \cup C$ and announces ξ.*

3. *Alice announces the colour of her hand.*

4. *Bob announces Cath's cards C.*

Strictly speaking, when we state that "Alice announces f" it is understood that she announces the natural number assigned[2] to the function f, and similarly to other steps in the protocol. Thus an execution can be represented in the form

$$(Alice, f), (Bob, \xi), (Alice, n), (Bob, X)$$

where $f : D \to \mathbb{F}_a^d$, ξ is a colouring, n a colour and $X \in \binom{D}{c}$. Since the players take turns we may omit the agents and write (f, ξ, n, X).

With this in mind, let us see that the colouring protocol is indeed a protocol as defined in Section 2. Intuitively, we must show that every announcement depends only on information available to the respective player.

Lemma 3.2. *The colouring protocol satisfies Definition 2.1.*

Proof. Denote the colouring protocol by (j, π), where $j(\vec{\alpha}) = $ *Alice* if $\vec{\alpha}$ has even length and otherwise $j(\vec{\alpha}) = $ *Bob* and $\pi(\delta, \vec{\alpha})$ is the set of possible announcements as specified by Definition 3.6. We need to verify that π is invariant under $\overset{j(\vec{\alpha})}{\sim}$. Let us do this step by step:

---

[2]Alice's first announcement does not correspond one-one to sets of hands that she may hold, for many mappings may define the same set of lines (just compose f with an invertible linear transformation). A similar observation applies to Bob's colourings. This is why we do not model announcements as sets of hands, as is done, for example, in [1].

1 *Alice announces a map* $f : D \to \mathbb{F}_p^d$ *in such a way that her cards form a line.* Suppose $(A, B, C) \overset{Alice}{\sim} (A', B', C')$ and $f \in \pi((A, B, C), ())$, so that $A = A'$ and f maps A into a line ℓ. Then, $f(A') = f(A) = \ell$ and hence $f \in \pi((A', B', C'), ())$, as required.

2 *Bob announces a rich and very distinguished k–colouring ξ.* Suppose that $(A, B, C) \overset{Bob}{\sim} (A', B', C')$ and $\xi \in \pi((A, B, C), (f))$, so that ξ is a rich and very distinguished colouring for $f(A \cup C)$. But since $B = B'$ we also have $A \cup C = A' \cup C'$ and thus ξ is also rich and very distinguished for $f(A' \cup C')$, so that $\xi \in \pi((A, B, C), (f))$, as required.

3 *Alice announces the colour of her hand according to ξ.* As before, suppose that $(A, B, C) \overset{Alice}{\sim} (A', B', C')$ and $n \in \pi((A, B, C), (f, \xi))$. Then, $\xi(f(A')) = \xi(f(A)) = n$ so we have that $n \in \pi((A, B', C'), (f, \xi))$.

4 *Bob announces Cath's cards.* Once again suppose that $(A, B, C) \overset{Bob}{\sim} (A', B, C')$. By our specification $X \in \pi((A, B, C), (f, \xi, n))$ if and only if $X = C$, so we must show that if $((A', B, C'), (f, \xi, n))$ is an execution of the protocol then $C = C'$.

Since ξ is distinguished there is a unique line $\ell \subseteq f(A \cup C) = f(A' \cup C')$ with $\xi(\ell) = n$. Since Alice's hand forms a line, we have $f^{-1}(\ell) = A = A'$. Thus $C = (D \setminus B) \setminus A = (D \setminus B) \setminus A' = C'$, as required. $\square$

It remains to check that the colouring protocol indeed provides a solution to the generalized Russian cards problem:

Theorem 3.1. *The colouring protocol is safe and informative, provided it is executable.*

Proof. The protocol is obviously informative given Bob's last announcement, so we focus on safety. Let $\vec{\alpha} = (f, \xi, n, C)$ be an execution of the colouring protocol.

First pick x that Cath does not hold. Because ξ is rich, there is a line ℓ with colour i passing through $f(x)$ and not meeting C. Further, note that $f(A) \cup f(C) \approx_1^\xi \ell \cup f(C)$, so that ξ is also very distinguished for $\ell \cup f(C)$. Then, setting $A' = f^{-1}(\ell)$ we see that $((A', B', C), \vec{\alpha})$ is also an execution of the protocol, but $x \in A'$.

The argument that Cath also considers it possible that Alice does not hold x is very similar. Since the set C has exactly c elements, there is a line h with colour i not meeting $f(C) \cup \{f(x)\}$, so that setting $A'' = f^{-1}(h)$ and reasoning as above, $((A'', B'', C), \vec{\alpha})$ is another execution of the protocol where Bob holds x.

Thus the colouring protocol is safe. □

We have so far worked under the assumption that the protocol is executable. The rest of the paper will be devoted to examining when this is the case, and determining the parameter k.

4 Executability

In what follows we will look for conditions to guarantee the existence of a rich and very distinguished k–colouring for some number of colours k. First, let us introduce the notion of *density:*

Definition 4.1 (Density). *Say a k–colouring ξ has density m if, given a point $x \in \mathbb{F}_p^d$ and a colour i, there are at least m i–coloured lines through x.*

There is a close connection between density and richness; to be precise, a colouring that is dense enough is automatically rich.

Lemma 4.1. *If ξ is a k–colouring of density $c + 2$, then ξ is rich.*

Proof. Let E be a subset of $\mathbb{F}_p^d$ with c elements. Fix a colour i and a point $x \notin E$. We note that if ℓ, h are two distinct lines passing through x, then $\ell \cap h = \{x\}$. Therefore, E contains the disjoint union

$$\bigcup \{E \cap \ell : x \in \ell \text{ and } \xi(\ell) = i\}.$$

It follows that for some ℓ with $\xi(\ell) = i$ and $x \in \ell$, $E \cap \ell$ must be empty, otherwise E would have at least $c + 2$ elements.

Similarly, if we pick $y \notin E$ different from x, we see that there is an i-coloured line through y not meeting $E \cup \{x\}$, satisfying the second requirement. □

Thus in order to construct rich colourings, we may focus on constructing dense colourings; this is not too difficult, as witnessed by the following:

Lemma 4.2. *Let $\ell_1, ..., \ell_k$ be distinct lines of $\mathbb{F}_p^d$ and assume that $\sigma_d(p) \geq k(m+1)$. Then, there is a k–colouring ξ of density m such that for $i \leq k$, $\xi(\ell_i) = i$.*

Proof. There are $\sigma_d(p) \geq k(m+1)$ non-collinear vectors in $\mathbb{F}_p^d$, and hence we can pick a set D of mk non–collinear vectors which are not directing vectors of any of the lines ℓ_i. Partition D into k disjoint sets D_i of m elements. Then, given a line $h \in \mathbb{F}_p^d$, put $\xi(h) = i$ if either $h = \ell_i$ or h has directing vector in D_i for some $i \leq k$. Otherwise put, for instance, $\xi(h) = 1$. It is easy to see that ξ satisfies the desired properties. $\qquad\square$

This will be sufficient for finding rich colourings. Now our goal is to construct a very distinguished k–colouring for $A \cup C$. As with richness, we will do so by introducing a stronger, approximate notion – that of a *perfect colouring*. It is not easy to tell under which conditions very distinguished colourings exist or how one may go about finding one, but finding perfect colourings will be straightforward.

The notion of a perfect colouring has the disadvantage that perfection is not hue-invariant. To deal with this issue, we will first need an intermediate concept: that of *critical colourings*. Every perfect colouring is critical and every critical colouring is very distinguished. Perfect colourings are the easiest to identify, but critical colourings are easier to work with than either perfect or very distinguished colourings.

Let us then begin by defining critical colourings:

Definition 4.2 (Critical colouring). *Given $E \subseteq \mathbb{F}_p^d$, we say that a k-colouring ξ is* critical *for E if there exists a set $L = \{\ell_1^*, \ldots, \ell_n^*\}$ of different colours such that, for every line $h \subseteq \mathbb{F}_p^d$, we have*

$$\left| (h \cap E) \setminus \bigcup_{i \leq n} \ell_i^* \right| < p - k,$$

where $|S|$ stands for the cardinality of a set S. We will say the lines in L are ξ-critical lines for E.

The notion of critical colouring in Definition 4.2 captures an important difference between the 2-colourings in Figures 2 and 3. The 2-colouring in Figure 2 is not critical for $E = A \cup C$, as for any set of lines L that we can select, there is a line h such that

$$\left| (h \cap E) \setminus \bigcup L \right| \geq 2 = p - k,$$

14

as the reader may verify by examination.

On the other hand, the colouring in the left-hand side of Figure 3 is critical for $E = A \cup C$, the union of the two lines and the fragment. We select L as the two complete lines in E. Then, for any line h, the property of Definition 4.2 holds. In particular, the line h with the three holes is the line outside of L with most points in E. For that line,

$$\left| (h \cap E) \setminus \bigcup L \right| = p - 3 < p - 2.$$

Recall Example 3.2, where we showed that the colouring in Figure 2 is unsafe. Intuitively, the insecurity of a k-colouring (in Figure 2 we have $k = 2$) is produced because $A \cup C$ contains k lines, along with a line fragment ℓ with k or less gaps – observe the line missing p and q in Figure 2. Then, though the k-colouring is distinguished, it might not be very distinguished, as we may be able to use several swaps to move the k lines and fill all the gaps in ℓ, thus generating $k + 1$ lines and repeating a colour.

However, when $A \cup C$ contains k or less lines and all fragments have more than k points missing, then a distinguished k-colouring ξ is always very distinguished. Figure 3 shows an example of this situation.
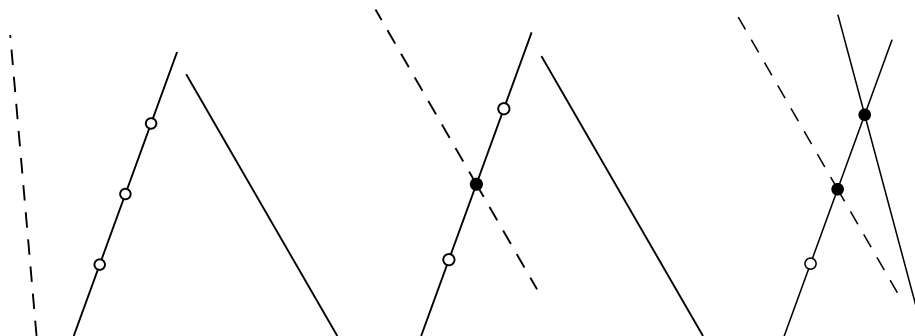

Figure 3: A critical 2-colouring

Example 4.1. *In the left-hand side of Figure 3, $A \cup C$ contains two lines and a fragment with three or more points missing. Alice has one of these lines, and Cath has the other line plus the segment. Then, a swap corresponds to moving a line to an empty position of the same colour, and it is not possible to arrange the two lines in $A \cup C$ in such a way that they fill the three gaps in the fragment. Thus there is no configuration of the same hue for which ξ is not distinguished, so that ξ is very distinguished.*

15

The above considerations suggest that critical colourings are very distinguished, and indeed this will turn out to be the case. Before we show this, let us make a simple observation:

Lemma 4.3. *If ξ is a critical k–colouring for E and $\ell \subseteq E$, then ℓ is a ξ–critical line for E, independently of how the other critical lines are chosen.*

Proof. Let $L = \{\ell_1^*, \ldots, \ell_n^*\}$ be ξ-critical lines for E. Notice that since they are lines of different colours, we have $n \leq k$. If ℓ is not ξ–critical then for every $i \leq n$, $\ell \cap \ell_i^*$ is either empty or a singleton. It therefore follows that

$$\left| (\ell \cap E) \setminus \bigcup L \right| = \left| \ell \setminus \bigcup_{i \leq n} \ell_i^* \right| \geq p - n \geq p - k,$$

which contradicts the definition of a critical k–colouring. $\square$

Now we will check that critical colourings are very distinguished. For this, it suffices to show that they are distinguished and that a critical colouring for E is critical for the entire hue of E; the former is straightforward, the latter rather involved.

Lemma 4.4. *Every critical k–colouring for E is distinguished for E.*

Proof. From Lemma 4.3 it follows that if $\ell \subseteq E$ then it is critical; but there is at most one critical line of each colour so there cannot be $h \neq \ell$ of the same colour both contained in E. $\square$

Lemma 4.5. *Suppose ξ is a critical k-colouring for E with $k < p$ and F has the same hue as E. Then, ξ is also a critical colouring for F.*

Proof. We shall prove this by induction on the number of swaps between E and F. The base case $(F = E)$ is vacuous. For the inductive step, suppose $F = (G \setminus \lambda_1) \cup \lambda_2$ with $\xi(\lambda_1) = \xi(\lambda_2) = j$ and G one swap closer to E than F is, so that by induction we may assume that there are ξ-critical lines $\ell_1^*, \ldots, \ell_n^*$ for G with $n \leq k$. Observe that $\ell_j^* = \lambda_1$; indeed, $\lambda_1 \subseteq G$, so that by Lemma 4.3, $\lambda_1 = \ell_i^*$ for some i. But $\xi(\lambda_1) = j$, and therefore $i = j$.

Our goal is to show that ξ is also critical for F; we will do this by proving that the lines $h_1^*, \ldots, h_n^*$ defined by $h_i^* = \ell_i^*$ for $i \neq j$ and $h_j^* = \lambda_2$ are critical. For this it will suffice to check that if ℓ is any line,

$$(\ell \cap F) \setminus \bigcup_{i \leq n} h_i^* \subseteq (\ell \cap G) \setminus \bigcup_{i \leq n} \ell_i^*; \tag{1}$$

16

this inclusion would then imply that

$$\left| (\ell \cap F) \setminus \bigcup_{i \leq n} h_i^* \right| \leq \left| (\ell \cap G) \setminus \bigcup_{i \leq n} \ell_i^* \right| < p - k,$$

showing that $h_1^*, \ldots, h_n^*$ (and hence ξ) are critical for F.

To establish (1), pick $x \in (\ell \cap F) \setminus \bigcup_{i \leq n} h_i^*$. It is obvious that $x \in \ell \cap G$, except perhaps in the case that $x \in \lambda_2$. But $\lambda_2 = h_j^*$, so this cannot be, and therefore we always have $x \in \ell \cap G$.

Next, we need to check that $x \notin \ell_i^*$ for any $i \leq k$. This is obvious if $i \neq j$, since $\ell_i^* = h_i^*$. Thus it remains to rule out that $x \in \ell_j^*$. If we had $x \in \ell_j^* = \lambda_1$, we would also have that $x \in \lambda_1 \setminus h_j^* = \lambda_1 \setminus \lambda_2$. But F does not intersect this set, so this is impossible.

We conclude that (1) holds, and thus ξ is critical for F, as desired. $\qquad \square$

As promised, we now have the following:

Lemma 4.6. *Every critical colouring is very distinguished.*

Proof. If ξ is critical for E, then by Lemma 4.5, it is also critical for every set of the same hue as E; thus, by Lemma 4.4, it is also distinguished for every such set. $\qquad \square$

We have seen that in order to construct very distinguished colourings, it suffices to construct critical colourings. This has the advantage that the notion of being critical depends only on a set E and not on the entire hue of E. However, it is still not entirely obvious when exactly critical colourings exist or how one is to go about building one.

This is where perfect colourings come into play. Although perfect colourings are not perfect for their entire hue, they are very easy to identify, and every perfect colouring is automatically critical.

Definition 4.3 (Perfect k–colouring). *Given $E \subseteq \mathbb{F}_p^d$, let $L_m(E)$ denote the set of all lines ℓ such that $|\ell \cap E| \geq m$.*

We say that a k-colouring ξ is perfect *for E if different elements of $L_{p-k}(E)$ have different colours.*

Perfect colourings, when they exist, are quite easy to identify and construct, yet they are always very distinguished:

Proposition 4.1. *If ξ is a perfect colouring for E, then ξ is very distinguished for E.*

Proof. First we note that ξ is critical, since we can take all of $L_{p-k}(E)$ as critical lines, given that they are all of different colour. Then, by Lemma 4.6, we have that ξ is very distinguished, as required. □

Now for the main result of this section:

Theorem 4.1. *Assume that a, b, c, d, k satisfy the following conditions:*

1. *a is a prime or a prime power,*

2. *$a + b + c = a^d$,*

3. *$k < a$,*

4. *for every $S \subseteq \mathbb{F}_a^d$ with $|S| \leq a + c$, we have $|L_{a-k}(S)| \leq k$;*

5. *$\sigma_d(a) \geq k(c + 3)$.*

Then, the colouring protocol is executable.

Proof. Assume that Alice has announced f and for this proof let A, B, C denote the images of each player's hand under f. By assumption, $|L_{a-k}(A \cup C)| \leq k$, so Bob can enumerate $L_{a-k}(A \cup C)$ by $\vec{\ell} = \langle \ell_1, \ldots, \ell_n \rangle$, with $n \leq k$. Then, by Lemma 4.2, there exists a colouring ξ with density $c + 2$ and such that $\xi(\ell_i) = i$, which by construction is perfect for $A \cup C$, so that by Proposition 4.1, it is also very distinguished. Further, by Lemma 4.1, we see that ξ is rich, as needed. □

The above proof should be seen as a theoretical argument that very distinguished colourings exist under the above conditions – but never as an algorithm for constructing them. It is essential for our protocol that Bob choose randomly among all possible colourings. We leave the specification of feasible algorithms for doing so for future work.

18

5 Finding suitable parameters

The conditions given by Theorem 4.1, while rather general, remain somewhat implicit. In this subsection we shall compute some explicit bounds on the parameters which guarantee that these conditions are met. The computations we will make are a bit rough, but will nevertheless give us a large family of parameters for which the protocol is guaranteed to work.

They are based on the following counting lemma:

Lemma 5.1. *If a set $E \subseteq \mathbb{F}_p^d$ is such that*

$$|E| < (k+1)(p-k) - \frac{k(k+1)}{2},$$

then $|L_{p-k}(E)| \leq k$.

Proof. We argue by contrapositive, assuming that $|L_{p-k}(E)| > k$.

Let $\ell_1, \ldots, \ell_{k+1}$ be distinct lines such that $|E \cap \ell_i| \geq p-k$. Then, we have

$$
\begin{aligned}
|E| &\geq \left| \bigcup_{i \leq k+1} (\ell_i \cap E) \right| \\
&\geq \sum_{i \leq k+1} |\ell_i \cap E| - \sum_{i < j \leq k+1} |\ell_i \cap \ell_j| \\
&\geq (k+1)(p-k) - \tfrac{1}{2}k(k+1).
\end{aligned}
$$

$\square$

Thus in view of Theorem 4.1, in order to find suitable parameters, it suffices to solve the system of inequalities

1. $a + c < (k+1)(a-k) - \frac{1}{2}k(k+1)$,

2. $\dfrac{a^d - 1}{a - 1} \geq k(c+3)$

or, simplifying a bit,

1. $c < ak - \frac{3}{2}k(k+1)$,

2. $a^d > k(a-1)(c+3)$.

From this we immediately obtain the following asymptotic result:

Theorem 5.1. *If a is a large enough prime power, the colouring protocol is executable with*

1. $c < O(a^{3/2})$ and $d = 3$ or

2. $c < O(a^2)$ and $d = 4$.

Proof. In view of Theorem 4.1 and Lemma 5.1, it suffices to show that the above inequalities hold.

For the first result, set $k \approx \sqrt{a}$ and $c \approx {}^{a^{3/2}}\!/_2$. Then, we have that $ak - {}^{3k(k+1)}\!/_2 = a^{3/2} + O(a)$, which for large a is greater than ${}^{a^{3/2}}\!/_2$. Meanwhile, $k(a-1)(c+3) = {}^{a^3}\!/_2 + O(a^2)$, which for large a is bounded by a^3.

The second is similar; here, set $k \approx {}^a\!/_2$ and $c \approx {}^{a^2}\!/_9$. $\square$

A nice conclusion we obtain from the above result is that indeed c can be larger than a by any order of magnitude we desire, provided a is large enough:

Corollary 5.1. *Given any natural number N, there exist a, c such that ${}^c\!/_a > N$ and the colouring protocol is executable, sound and informative for $(a, a^3 - a - c, c)$.*

Proof. If $a \gg N^2$ then $a^{3/2} = (a^{1/2})a \gg Na$ and, by Theorem 5.1.1, the required inequalities hold and the protocol is executable. $\square$

Note that we may use Theorem 5.1.1 or Theorem 5.1.2 depending on whether we wish to keep b relatively small with respect to a or a relatively small with respect to c. In either case, $b = O(c^2)$.

6 Conclusions and further research

The colouring protocol we have presented gives a new and flexible solution to the generalized Russian cards problem. Our protocol solves the problem in many cases where the eavesdropper has more cards than one of the players, and is the first known solution to achieve this. If the generalized Russian cards problem is to be understood as *Find triples (a, b, c) for which a safe and informative protocol of any length exists,* then the current work is a giant stride over what had been previously achieved.

There are many variations that could be analyzed and might yield important results. Alice may have more than one line, there may be more players, Cath may be allowed to learn a few of the cards, etc. Along these lines, a particularly promising direction would be to replace lines by other algebraic

curves. This could, potentially, reduce the size of the whole space (and hence Bob's hand) without compromising the existence of suitable colourings.

A different direction to pursue involves cases where either a or $a+b+c$ are not prime powers. There are already standard techniques to deal with these; one finds a prime which is not much larger than the desired parameter and works with that instead. Such techniques have already been used to extend a different protocol to many new triples in [2] but have not been worked out in our context.

Meanwhile, the generalized Russian cards problem may have a recreational flavour to it, but it has potential for serious applications in secure communication. These protocols have an advantage over most traditional encryption methods in that they are "unconditionally secure", meaning that an eavesdropper is unable to decipher messages even when granted unlimited computational capacity. The presupposition of a "dealing stage" is not so different to authentication systems using security tokens, where the user receives a physical device that generates one-time passwords. A possible application is the development of challenge-response authentication systems. The user Bob is authenticated against the server Alice by running a Russian cards protocol. If Alice checks that Bob's responses are coherent with the key he should have (Bob's hand) then the authentication succeeds.

Real-world implementation of these protocols would also require an additional computational and probabilistic analysis. What is the complexity of running the colouring protocol? Are there good algorithms for finding suitable colourings? Even if Cath does not learn any cards, how do we minimize the probability that she guesses them correctly?

To summarize, there is much to be done indeed!

Acknowledgements

References

[1] M.H. Albert, R.E.L. Aldred, M.D. Atkinson, H. van Ditmarsch, and C.C. Handley. Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, 33:33–46, 2005.

[2] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque, J.J. Joosten, and F. Soler-Toscano. A secure additive protocol for card players. *Australasian Journal of Combinatorics.*, 54:163–175, 2012.

[3] P. Dembowski. *Finite Geometries (reprint)*. Springer, 1997.

[4] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38 and 161–191, 1883.

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

[6] R. Lidl. *Finite Fields*. Cambridge University Press, 1997.

[7] K.S. Makarychev and Yu.S. Makarychev. The importance of being formal. *Mathematical Intelligencer*, 23(1):41–42, 2001.

[8] U. Maurer. Information-theoretic cryptography. In M. Wiener, editor, *Advances in Cryptology — CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 47–64. Springer-Verlag, August 1999.

[9] T. Mizuki, H. Shizuya, and T. Nishizeki. A complete characterization of a family of key exchange protocols. *International Journal of Information Security*, 1:131–142, 2002.

[10] A. Stiglic. Computations with a deck of cards. *Theoretical Computer Science*, 259(1–2):671–678, 2001.

[11] D.R. Stinson. *Combinatorial Designs – Constructions and Analysis*. Springer, 2004.

[12] C. M. Swanson and D. R. Stinson. Combinatorial solutions providing improved security for the generalized russian cards problem. *arXiv*, 1207.1336 [math.CO], 2012.

[13] H. van Ditmarsch and F. Soler-Toscano. Three steps. In J. Leite, P. Torroni, T. Ågotnes, G. Boella, and L. van der Torre, editors, *Computational Logic in Multi-Agent Systems - 12th International Workshop, CLIMA XII. Proceedings*, pages 41–57. Springer, 2011. LNCS 6814.