A Zero-Error Source Coding Solution to the Russian Cards Problem

ESTEBAN LANDERRECHE
Institute of Logic, Language and Computation
January 24, 2017

Abstract

In the Russian Cards problem, Alice wants to communicate her hand from a deck of cards to Bob through one public announcement such that Cath does not learn her hand. In zero-error source coding, Alice's goal is to communicate her information to Bob with the least amount of bits. Both problems share the goal of Bob learning Alice's information in one announcement. However, they have additional objectives: in the Russian Cards case it is security against Cath, for source coding it is minimizing the communication complexity. At a first glance, these two additional properties are not mutually exclusive so we ask whether there is a solution that is both optimal and secure at the same time. This would permit us to model the Russian Cards problem as a zero-error source coding problem to find the optimal secure announcement and it will also enrich source coding by adding the knowledge that it is also secure for an attacker that holds some correlated information. Finally, we deal with the relationship between these two problems. To achieve this, we use results of graph theory and design theory, in particular block graphs and Steiner systems.

1 Introduction

There are many different approaches to the modelling of communication in mathematics. A fruitful area of study in this area is measuring the amount of information exchanged to communicate the most by saying the least. Another approach seeks to create communication that can only be understood by the intended recipients. It is possible to combine both goals in our modelling, to provide efficient and secure communication. Zero-error source coding is an example of the former approach which has some similarities with the Russian Cards problem, a member of the latter. We will try to

combine them to see if solutions for one also work for the other and to see what is necessary to achieve this.

Take a situation where three people (Alice, Bob and Cath) have a deck of cards. They randomly distribute the cards between themselves such that they only know their cards. Suppose everything that is said can be heard and understood by all three people, is there a way for Alice to tell Bob her hand without Cath finding out? This is the question that the Russian Cards problem tries to answer. In essence, what we have is three people with probabilistically correlated information in which two of them attempt to communicate their knowledge without the information reaching the third person. This seems to suggest a connection with zero-error source coding, which tries to construct the minimal announcement such that Bob can know all of Alice's information. To further study this connection, we first define each problem on its own.

1.1 The Russian Cards Problem

The Russian Card problem as it appeared in the 2000 Moscow Mathematical Olympiad is as follows

> Suppose we have three participants- Alice, Bob and Cath- who have a deck with 7 cards represented by the numbers 0 to 6. The cards are dealt within the three in a random manner in a way that only each player knows his or her cards. Both Alice and Bob receive 3 cards while Cath is given the remaining one. Alice gets cards 0, 1 and 2, Bob gets 3, 4 and 5 and Cath gets 6. Alice and Bob want to know each other's cards without Cath learning any of them. However, every communication between Alice and Bob can be heard and understood perfectly by Cath and it is impossible to encrypt the message in a traditional way. Is there a way that they can communicate each other's hand without Cath knowing the position of any card she doesn't hold?

What started as an Olympiad problem has been generalized for larger decks and different distributions of the cards. Other generalizations permit multiple announcements, which opens up a greater set of distributions that have a solutions. However, these examples no longer share the basic structure with zero-error source coding, so we do no take them into account.

1.2 Zero-error Source Coding

In zero-error source coding we have the following: Alice holds some information $x \in \Omega$ where Ω is commonly known by both Alice and Bob. She

wants to communicate x to Bob, who holds some correlated information u, of which Alice knows the form of (but not the content). The goal of a source coding problem is for Alice to communicate x to Bob with the least amount of bits possible, taking advantage that x and u are correlated. This is done by constructing a confusability graph $G = (V, E)$ where the vertices in V represent the possible values of x (that is each element of Ω) and two vertices v_1, v_2 are joined by an edge if and only if there is a certain value of u such that Bob would not be able to distinguish whether Alice holds v_1 or v_2. Given this graph, Alice must only find a minimal vertex coloring and communicate to Bob the color of the vertex x. Bob could now immediately distinguish which is the correct vertex through the information encoded in u, as no vertices of the same color are connected.

The minimal colouring of this graph is an optimal solution for zero-error source coding because it is the smallest partition over the information that Alice holds which is still informative to Bob. The coloring of the graph is agreed and indexed beforehand so the communication consists only of the index of the color. If there are m colors, the announcement will be of length $\lceil \log_2 m \rceil$.

2 Informativity

We have presented two distinct problems from very different contexts and with very different goals. However, they have a similar structure. In both we have an agent attempting to communicate his information to the other. While each problem has additional desirable properties in the announcement, they both agree on the fact that an announcement must be informative for the receiving agent. After communication, the receiver must always know exactly what information the sender holds. We bridge the two problems through this idea.

It is very natural to see that the Russian Cards problem can be expressed as a zero-error source coding problem with an extra condition and a different goal. Ω is seen as all the possible hands for Alice, where x is the hand that she actually holds. Similarly, u becomes Bob's hand, which is clearly correlated to Alice's hand. Alice can clearly construct this graph, as she can think about all the possible hands that Bob can hold and build the edge set accordingly. In particular this means that any solution that is informative to Bob in the Russian Cards problem is also informative in the source coding context.

Looking for a connection between these two problems indirectly gives us a result for Russian Cards. The informativity of an announcement can be tested in a confusability graph, regardless of the way we construct the announcement. If an announcement contains two hands that are connected then there is at least one hand that Bob could hold that will consider both these hands as possible. Therefore, we must avoid this at all cost. The independence number of a graph represents the cardinality of the largest set of vertices in the graph such that all the vertices are not connected. Note that no announcement can have two connected vertices, as that would mean that for a certain card deal, Bob would not be able to distinguish the two connected hands. This gives us an upper bound on the size of an announcement which cannot be higher than the independence number of the confusability graph of that problem.

If our goal is to connect these two problems we will formally define what we mean by an announcement and informativity. The presentation follows the one seen in [LFD15] for the Russian Cards problem, but generalized so that it can also be applied. It is important to note that while generally zero-error source coding literature does not explicitly treat an announcement as a list of possible values for Alice's information, it can always be seen as such.

Definition 1. *Let $\Omega \subset \mathbb{N}$ be the set of the possible information and $A, B \subset \Omega$ be the information that Alice and Bob hold respectively, with $A \cap B = \varnothing$. An **announcement** $\mathcal{A} \subseteq \binom{\Omega}{A}$ is a list of possible values for A, with $\binom{\Omega}{A}$ representing all the subsets of Ω with cardinality equal to A.*

Definition 2. *Let $\binom{\Omega}{A}$ be the set of every possible information set that Alice may hold. An **announcement strategy** $\mathcal{S}$ is a set of announcements and a distribution function f over $\mathcal{S}$ such that for every set $A \in \binom{\Omega}{A}$ Alice will choose an appropriate announcement $\mathcal{A} \in \mathcal{S}$ with the probability dependent on f*

Definition 3. *Let A and B be the information that Alice and Bob hold respectively. An announcement $\mathcal{A}$ is **informative** if after the announcement Bob knows A, written in this way: $\mathcal{A} \setminus B = \{A\}$. An announcement strategy is informative if every announcement in it is informative.*

In the Russian Cards setting, Ω represents the deck of cards and A, B (and C) are the hands of each player. For the source coding perspective, each piece of information is encoded in a natural number. This differs from the classical presentation in the introduction, where Alice holds one element of Ω instead of a subset. It is easy to show that these two settings are equivalent, but we choose to present it in this way to show the similiarity with the Russian Cards problem. We define the notion of an announcement

strategy because the choice of an announcement depends on the particular information that Alice holds, however a strategy only depends on Ω and how the information is distributed. Therefore, we can define a strategy for any particular deal of cards/source coding problem. Note that we have a probability function to define which announcement Alice chooses for the case that there is more than one announcement for a particular hand. In the source coding paradigm, this function is unnecessary as we are trying to minimize the total number of announcements. It is natural to have only one possible announcement per hand, otherwise we could have redundancy. As a matter of fact, the solution using coloring of graphs ensures that there can only be one announcement per hand.

2.1 Example

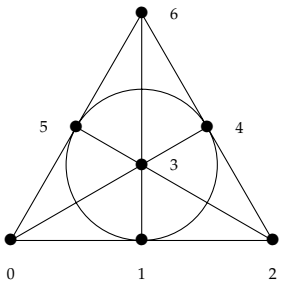
We will present an example to see that while the concept of informativity in both problems is equivalent, the problems are not. We will focus on the original problem with seven cards to show that the source coding protocol works. We will call this problem the $(3,3,1)$ problem, as this is how the cards are distributed. While this is a Russian Cards problem, we interpret it as a source coding problem and use the known solution for it. Then, we will see if it fulfills the requirements to be a good solution for the Russian cards problem.

The way to solve a zero-error source coding problem is through a confusability graph. Alice constructs a graph where each vertex represents the information that she may hold (in this case, every set of three cards) and joins every two vertices which could be confused by Bob if he held any valid hand (in this case, valid refers both to Bob having three cards and not having any card found in the vertices). While we could construct this graph vertex by vertex, there exists a class of graphs called Johnson Graphs which represent exactly that. A Johnson graph $J(n,k)$ is a graph where the vertices are the k-element subsets of an n-element set and there is an edge between two vertices if and only if they share a $k-1$ set. Lets take $J(7,3)$ and have every vertex represent one of Alice's possible hands. This is equivalent to the fact that two vertices are connected if they are indistinguishable for someone holding a $n-k-1$-set.

Therefore, the Johnson graph $J(7,3)$ is the confusability graph for the $(3,3,1)$ Russian cards problem, as Bob holds $7-3-1=3$ cards. Any coloring of this graph will give us a valid solution for the source coding problem within. We use sage to find the following coloring:

000	{0, 2, 6}, {2, 3, 4}, {1, 2, 5}, {0, 4, 5}, {0, 1, 3}
001	{1, 5, 6}, {3, 4, 6}, {0, 3, 5}, {0, 1, 4}
010	{3, 4, 5}, {2, 5, 6}, {0, 3, 6}, {1, 4, 6}, {0, 2, 4}, {1, 2, 3}
011	{2, 4, 6}, {2, 3, 5}, {1, 4, 5}, {0, 5, 6}, {0, 3, 4}, {1, 3, 6}, {0, 1, 2}
100	{4, 5, 6}, {2, 3, 6}, {0, 2, 5}, {0, 1, 6}, {1, 3, 5}, {1, 2, 4}
101	{2, 4, 5}, {1, 2, 6}, {3, 5, 6}, {0, 4, 6}, {1, 3, 4}, {0, 2, 3}, {0, 1, 5}

In the Olympiad problem, Alice held $\{0, 1, 2\}$. Therefore she would announce 011 as her hand is in the fourth announcement. In this particular case, Cath will not be able to learn the position of any of the cards that either Alice or Bob hold. We know this because it coincides with the projective geometric solution seen in the following example, where Alice holds a line:



This seems to show that the source coding strategy is secure, but this is not the case. Suppose instead of the original distribution of the cards, we have the following deal

- **Alice**: $1, 5, 6$
- **Bob**: $2, 3, 4$
- **Cath**: 0

In this case, Alice would announce the following:

$$\{1, 5, 6\}, \{3, 4, 6\}, \{0, 3, 5\}, \{0, 1, 4\}$$

At first glance we can see that Cath learns the position of some of the cards, as no hand in the announcement contains 2. This lets Cath know that Alice cannot hold 2, because it does not appear in any of the possible hands for Alice. Because Cath holds 0, she then knows Bob holds 2. It is even worse, as Cath can eliminate the last two hands which shows her that Alice holds 6. Therefore, source coding alone is not enough to solve the Russian Cards problem, as we need to add other restrictions to ensure security of the strategy.

3 Security

We have seen that solving the source coding problem related to a Russian Cards problem is not enough to solve the original problem. A generic solution for the source coding problem does not automatically ensure that Cath does not learn the position of a card. However, there are many different minimal colorings for a graph and while we found one that does not work, there may be another which does. For that, we must formalize the concept of security and see if it is reflected in some graph colorings. We want to ensure that, regardless of the cards that each person holds, Cath does not learn the exact position of any card she does not hold herself. This can be encoded in the following way.

Definition 4. *Let Ω be the set of cards, $\mathcal{A}$ an announcement and c the size of Cath's hand. If Y is a set of cards, let $\mathcal{A} \setminus Y$ be all the hands in $\mathcal{A}$ which do not contain an element of Y. We say $\mathcal{A}$ is **secure** if for all $C \in \binom{\Omega}{c}$ the following two properties hold*

- *The union of all the hands in $\mathcal{A}$ that avoid C is equal to $\Omega \setminus C$, that is*

$$\bigcup_{X_i \in \mathcal{A} \setminus C} X_i = \Omega \setminus C$$

.

- *The intersection of all hands in $\mathcal{A}$ that avoid C is the empty set, that is*

$$\bigcap_{X_i \in \mathcal{A} \setminus C} X_i = \varnothing$$

The first property ensures that Cath does not learn the position of any card in Alice's hand, the second one ensures the same does not happen for any card in Bob's hand. We can see that the insecure announcement in the example fails both, as $2 \notin \{1,5,6\} \cup \{3,4,6\}$ and $\{1,5,6\} \cap \{3,4,6\} = \{6\}$. As a matter of fact, no announcement for this case with four hands will be secure. This is because in an announcement every card must appear in at least two announcements. If it only appears in one, there might be the possibility that Cath holds a card in the same hand and can then conclude that that card is not held by Alice. The only way that Alice could prevent this is by having that one card only appear in the hand that she holds. However, this is not secure, as Cath will know that Alice's hand must be the one holding the card that appears only once. If Alice held any other card the announcement would not be secure, as we have seen previously, which means that Cath would know Alice's hand. That would mean that we must have at least $7 \times 2 = 14$ cards in the announcement, but an announcement with four hands has only 12. hence, by the pigeonhole principle, this is

impossible.

We can generalize this last fact: If Cath has c cards, each card must appear in at least $c+1$ hands in the announcement. From here, we get that a secure announcement must have at least $(a+b+c)(c+1)$ cards. This is necessary for our first condition to hold, but not sufficient. We can see this by looking at the first announcement in our previous example.

$$\{0,2,6\},\{2,3,4\},\{1,2,5\},\{0,4,5\},\{0,1,3\}$$

If Cath holds 0 she will know that Alice holds 2. Therefore we need stronger restrictions to ensure security. To do this, we must first properly characterize the graphs that we are constructing. To construct the confusability graph $G=(V,E)$ induced by the Russian Cards problem (a,b,c) with $V=\binom{\Omega}{k}$ and $E \subset V \times V$

- Create a vertex for each hand Alice can hold
- Join two vertices if there is a hand that Bob could hold such that he could not distinguish between the two hands. That is,

$$(H,K) \in E \Leftrightarrow |H \cup K| \leq a+c$$

Clearly G is regular and symmetric.

Lemma 5. *Let $G=(V,E)$ be a graph induced by the Russian Cards problem (a,b,c). For any $x \in V$, x has $\sum_{i=1}^{c}\binom{a}{i}\binom{b+c}{i}$ neighbors.*

Proof. If we want to see how many vertices y exist such that $x \cup y = a+i$ for any i we choose the i cards that we take away from x, which gives us $\binom{a}{i}$ and the cards with which we can replace them $\binom{b+c}{i}$. By adding all the vertices that differ from 1 to c cards we get exactly

$$\sum_{i=1}^{c}\binom{a}{i}\binom{b+c}{i}$$

□

To ensure security, we have to prevent the situation where Cath can eliminate all hands in an announcement that contain a particular card. Because we have to create announcements that work for every possible Cath hand, we have to make sure that if cards x and y appear together in a hand in the announcement, there must be a hand in the same announcement where x appears and y does not (and viceversa). However, as Cath's hands grow, so does this restriction. If Cath has two cards, then for every three cards

x, y and z in a hand in the announcement there must be at least one hand that contains x but not y and z. In general, if Cath has c cards, for each hand H in an announcement, there must be at least $c+1$ other hands in the announcement, each one containing exactly one of the elements of H. This condition is necessary to fulfill the second property of security, as we defined it previously. To fulfill the first property, for any $c+1$-set contained in a hand, there must be another hand in the announcement such that it contains none of the cards in the set.

Here, we run into a problem with our approach. Graph theory alone permits us to define local relationships and not the relationships that we have just mentioned. Therefore, we cannot represent these properties in the graph. Of course, we can find colorings and only accept one if these conditions are met, but we cannot affirm whether there exists a minimal coloring that fulfills these properties without checking all of them. Therefore, purely graph theoretic tools are not enough in this case and we need more robust mathematical structures, in particular Steiner systems, a type of block designs. These systems are a subset of $\binom{\Omega}{a}$ such that every $(a-c)$-set appears exactly in one element of the system. This is enough to ensure that the previous properties hold. These designs have graphs associated to them and they happen to be equivalent to the graphs we have constructed (when these designs exist). The Johnson Graph $J(7,3)$ is the block graph of the 2-$(7,3,1)$-design. In [SS14], it is shown that an optimal announcement strategy for a (a,b,c) deal is a large set of t-$(a+b+c,a,1)$-designs, with $t=a-c$. This is equivalent to the minimal coloring in such graph, whenever the large set exists.

Swanson & Stinson proved that the solution created by t-$(a+b+c,a,1)$-designs is not only informative and optimal, but also secure. Not content with the definition of security that we presented, they also proved a stronger notion of security. They showed that for any set X of t cards, the probability that Alice holds X according to Cath does not change before and after the announcement. This prevents Cath from gaining probabilistic information about Alice's hand, which might be desirable depending on the importance of the privacy of the information. They refer to this notion as t-perfect security.

Definition 6. *Let Ω be the set of cards, $\mathcal{S}$ an announcement strategy and c the size of Cath's hand. An announcement $\mathcal{A} \in \mathcal{S}$ for $A \in \binom{\Omega}{A}$ is* ***t-perfectly secure*** *if for every t-set Y and every $C \in \binom{\Omega}{c}$, if $Y \cap C = \varnothing$ then*

$$\frac{P(Y \subset A|C,\mathcal{A})}{P(Y \subset A|C)} = 1$$

An announcement strategy $\mathcal{S}$ is t-perfectly secure if every announcement in it is t-perfectly secure.

When the t is not directly relevant, we will refer to this simply as perfect security. This gives us a powerful tool to ensure security in our announcement. For that, we delve deeper into design theory, particularly in the study of Steiner systems. We will first return to our example to see some examples of security.

3.1 Continued Example

We go back to the $(3,3,1)$ case. Note that we have $\binom{7}{3} = 35$ possible hands and that the independence number of the associated Johnson graph $J(7,3)$ is 7. Our first instinct is that given that 7 divides 35, we might have a valid protocol with five announcements with seven cards each. Unfortunately, this is impossible, as the chromatic number of $J(7,3)$ is 6. Therefore, a protocol must have at least six different possible announcements. As a matter of fact, such announcement does exist and is the following 6-coloring of $J(7,3)$ (presented in [SS14]):

$$\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{0,4,5\},\{1,5,6\},\{0,2,6\}$$
$$\{0,2,3\},\{1,3,4\},\{2,4,5\},\{3,5,6\},\{0,4,6\},\{0,1,5\},\{1,2,6\}$$
$$\{0,2,4\},\{0,3,5\},\{1,2,3\},\{0,1,6\},\{1,4,5\},\{2,5,6\}$$
$$\{0,1,2\},\{2,3,4\},\{4,5,6\},\{1,3,5\},\{0,3,6\}$$
$$\{1,2,5\},\{0,5,6\},\{1,4,6\},\{0,3,4\},\{2,3,6\}$$
$$\{3,4,5\},\{0,1,4\},\{0,2,5\},\{2,4,6\},\{1,3,6\}$$

Note that as anticipated, this is not perfectly secure, as we can see with the fourth announcement. If Cath holds 6, the cards 1, 2 and 3 seem more likely than the rest as they appear twice in the reduced list while the other cards appear only once. On the other hand, we have the geometric protocol that was previously mentioned. This protocol is perfectly secure for the $(3,3,1)$ problem although it is pretty inefficient as there are four possible announcements per hand. However, we can optimize it by eliminating certain redundant announcements to have only two choices per hand (also from [SS14]):

$\{2,5,6\},\{2,3,4\},\{1,4,5\},\{1,3,6\},\{0,4,6\},\{0,3,5\},\{0,1,2\}$
$\{2,5,6\},\{2,3,4\},\{1,4,6\},\{1,3,5\},\{0,4,5\},\{0,3,6\},\{0,1,2\}$
$\{3,4,5\},\{2,4,6\},\{1,3,6\},\{1,2,5\},\{0,5,6\},\{0,2,3\},\{0,1,4\}$
$\{3,4,5\},\{2,4,6\},\{1,5,6\},\{1,2,3\},\{0,3,6\},\{0,2,5\},\{0,1,4\}$
$\{3,4,6\},\{2,3,5\},\{1,4,5\},\{1,2,6\},\{0,5,6\},\{0,2,4\},\{0,1,3\}$
$\{3,4,6\},\{2,3,5\},\{1,5,6\},\{1,2,4\},\{0,4,5\},\{0,2,6\},\{0,1,3\}$
$\{3,5,6\},\{2,4,5\},\{1,3,4\},\{1,2,6\},\{0,4,6\},\{0,2,3\},\{0,1,5\}$
$\{3,5,6\},\{2,4,5\},\{1,4,6\},\{1,2,3\},\{0,3,4\},\{0,2,6\},\{0,1,5\}$
$\{4,5,6\},\{2,3,6\},\{1,3,4\},\{1,2,5\},\{0,3,5\},\{0,2,4\},\{0,1,6\}$
$\{4,5,6\},\{2,3,6\},\{1,3,5\},\{1,2,4\},\{0,3,4\},\{0,2,5\},\{0,1,6\}$

This announcement is the best perfectly secure announcement, with a communication complexity of 10 (4 bits) while our previous solution is 6 (3 bits). Here, there is a trade off between perfect security and optimality. It is important to note that none of these options would qualify as optimal in the source coding paradigm, where the optimum is 5 (except for the particularity that the communication complexity of 5 and 6 are equivalent in bits).

4 Results in Steiner Systems

In the process of treating the Russian Cards problem as a zero-error source coding problem, we found that in order to ensure security we would need tools stronger than the ones given to us by graph theory. The graphs we are interested in corresponded to block graphs for Steiner systems, whenever these systems exist. We present a more formal treatment of these systems in the following work, noting that if we get a minimal coloring for our graph we will also get a large set of Steiner systems.

Definition 7. *A **block design** (or simply,* design*) t-(v,k,r) is a set X of v elements and a collection of k-subsets of X (called blocks) such that every t-subset of X appears in exactly r blocks.*

Definition 8. *A **Steiner system** $S(t,k,v)$ is a set X of v elements and a collection of k-subsets of X (called blocks) such that every t-subset of X appears in exactly one block. A Steiner system is equivalent to a t-$(v,k,1)$-design.*

Definition 9. *A **large set of Steiner systems** $S(t,k,v)$ is a set of Steiner systems such that every k-subset of X appears in exactly one Steiner system as a block.*

We know that these designs exist whenever we have the divisibility condition by [Kee14], and that the construction is not trivial. However, we do not know if the large sets exist. For example, designs of the form $S(2,7,3)$ do exist (the Fano plane). However, if we had a large set of $S(2,7,3)$ systems, we would have a strategy for the $(3,3,1)$ Russian Cards problem. However, as we have seen previously, this strategy does not exist. THis is consistent with results in design theory presented in [SS14].

Lemma 10. *A Steiner system $S(t,k,v)$ has $\frac{\binom{v}{t}}{\binom{k}{t}}$ blocks.*

Proof. Every t-subset of our set of v elements must appear in the system, so a design must have $\binom{v}{t}$ elements distributed within its blocks of k elements. Every block fits $\binom{k}{t}$ elements, so there must be $\binom{v}{t}/\binom{k}{t}$ for each t-subset to appear exactly once. □

Lemma 11. *A large set of Steiner systems $S(t,k,v)$ has $\binom{v-t}{k-t}$ designs.*

Proof. Every k-subset of our set of v elements must appear in the large set, so a large set must have $\binom{v}{k}$ elements distributed within its designs of $\binom{v}{t}/\binom{k}{t}$ elements. Every design fits $\binom{v}{t}$ elements, so there must be $\frac{\binom{v}{k}}{\binom{v}{t}/\binom{k}{t}}$ for each k-subset to appear exactly once. We can easily reduce this to $\binom{v-t}{k-t}$. □

It is important to know what the [SS14] refers to by an optimal strategy. We showed that the optimal announcement strategy for $(3,3,1)$ has 6 possible announcements. However this clearly is not a large set of Steiner systems. Therefore, an optimal strategy in this case refers not to the solution with lowest m, but specifically with the solution (which may or may not exist) equal to the following bound, presented in [SS14].

Lemma 12. *Suppose $a > c$ and there exists a strategy for Alice that is informative for Bob. Then the number of announcements m is bound by*

$$\binom{b+2c}{c} \leq m$$

.

Definition 13. *Let (a,b,c) be the sizes of Alice, Bob and Cath's hands. We say an announcement strategy is **design-optimal** if it contains exactly $\binom{b+2c}{c}$ announcements.*

With this, we present the following theorem from [SS14]

Theorem 14. *Suppose that $a > c$. A design-optimal (a, b, c)-strategy for Alice that is informative for Bob is equivalent to a large set of t-$(a + b + c, a, 1)$-designs, where $t = a - c$.*

To find a solution for the Russian Cards problem, we first generate the confusability graph G and then we find the chromatic number $\chi(G)$. An optimal informative announcement strategy has $\chi(G)$ possible announcements, any strategy with less announcements would either have uninformative announcements or not have relevant announcements for certain hands. If we want this minimal announcement to be t-perfectly secure then the graph must correspond to the block graph of a Steiner system. By [Kee14], a Steiner system $S(t, k, v)$ exists if and only if $\binom{k-i}{r-i}$ divides $\binom{v-i}{r-i}$ for every $0 \leq i \leq r - 1$. This means that there are certain Russian Cards problems that cannot be characterized by designs. While the graph exists, it does not correspond to a block graph and therefore we cannot apply these results to it. This does not mean a secure solution does not exist, only that it is not a design and it is not t-perfectly secure. Even if a Steiner system exists, the large set might not exist. There are no general proofs for the existence of large sets, but results exists for particular values, for example $k = 3$. The following theorem provides a necessary and sufficient condition to see if large sets of the form $S(a - c, a, a + b + c)$ exists.

Theorem 15. *Take $0 < c < a \leq b \in \mathbb{N}$ such that $\binom{a-i}{r-i}$ divides $\binom{a+b+c-i}{r-i}$ for every $0 \leq i \leq r - 1$. There is a large set of $S(a - c, a, a + b + c)$ Steiner systems if and only if the chromatic number of the graph G induced by the Russian Cards problem (a, b, c) is equal to $\binom{b+2c}{c}$*

Proof. $\Rightarrow$
Suppose such design exists. By Theorem 14 it is an optimal solution to the Russian Cards problem (a, b, c). Because a large set contains $\binom{b+2c}{c}$ designs, then we can color G by $\binom{b+2c}{c}$ colors and we cannot color it with less because the design is optimal.
$\Leftarrow$
By Theorem 14 we know that every informative announcement strategy with $\binom{b+2c}{c}$-coloring is a large set of $S(a - c, a, a + b + c)$ Steiner systems. □

With this result we know that, for given (a, b, c), if $\chi(G)$ is larger than $\binom{b+2c}{c}$, such large sets cannot exist. While this result is not new, we have built it from the connection of the Russian Cards problem and zero-error source coding. Design theory permits us to connect graph colorings with our notion of security, although unfortunately they do not work for all examples. The lack of existence of a large set of designs means that we have to take decisions regarding what we think is more important: optimality or security.

5 Conclusion and Further Research

We have found a connection between the Russian Cards problem and zero-error source coding. Both problems are seen extensions of the same problem in which Alice wants to communicate information to Bob, who holds some correlated information. However, each problem adds an additional condition: security in Russian cards and minimal communication complexity for source coding. We have seen that these two conditions are equivalent if the Steiner system $S(a-c, a, a+b+c)$ exists (in the source coding paradigm, Cath's hand represents Bob's uncertainty). We also saw that in other cases, this is not true and we must make a choice between security and optimality. This means that while the two problems are similar and occasionally equivalent, it is not always the case that an optimal solution will be secure.

While we saw that we can present a Russian Cards problem in the form a source coding problem, the opposite is not always true. In particular, Russian Cards problems have very well behaved confusability graphs (regular, symmetric). However, it could be interesting to see if the concept of security could be extended to all of source coding, seeing where security does not affect optimality. By adding an additional restriction to source coding we create a new problem in which optimality of communication is not the only concern, which might help model situations in which we do not want the method of data compression itself prevents the information from being compromised.

If there is no perfectly secure minimal coloring, then we are faced with one choice of what we value the most: optimality or security. For the first case, we know that every coloring will be informative, so we must look for the smallest (referring to the number of colors) secure coloring. However, this coloring would not be perfectly secure. If we want perfect security we will need a coloring that leads to an equitable protocol and for that we need all the sets to be of the same size. This means that the coloring must have a number of colors that divides the number of hands. We would then reject many possible colorings, some of which may have less colors, but not a number that divides the number of possible hands. A natural line to continue the research is finding whether optimal announcements preserve stronger notions of security (but weaker than perfect security), like ε-strong security presented in [LFD15], where the quotient of probabilities of a hand should be between $1-\varepsilon$ and $1+\varepsilon$.

If we are more interested in minimizing the number of announcements, it might be interesting to consider announcement strategies in which the distri-

bution function changes depending on Alice's hand. If a $S(a, a+b+c, c-a)$ system does not exist, we know that there is no coloring for the confusability graph such that it entails a perfectly secure announcement. Therefore, there is no perfectly secure strategy in which every hand appears exactly once, at least some hands appear in more than one announcement. This entails two possibilities, either some hands appear in more announcements than others or they all appear the same number of times. The second case would hardly be optimal, so it could be interesting to focus on what Swanson and Stinson call non equitable strategies to find strategies that can be secure and have a low number of possible announcements.

References

BJL99. Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory*, volume 69. Cambridge University Press, 1999.

Kee14. Peter Keevash. The existence of designs. *arXiv preprint arXiv:1401.3665*, 2014.

LFD15. Esteban Landerreche and David Fernández-Duque. A case study in almost-perfect security for unconditionally secure communication. *Designs, Codes and Cryptography*, pages 1–24, 2015.

OK98. Alon Orlitsky and J. Körner. Zero-error information theory. *IEEE Transactions on Information Theory*, 44(6):2207–2229, 1998.

RW. Todd Rowland and Eric W. Weisstein. Steiner system. `http://mathworld.wolfram.com/SteinerSystem.html`. From MathWorld–A Wolfram Web Resource.

SS14. Colleen M Swanson and Douglas R Stinson. Combinatorial solutions providing improved security for the generalized russian cards problem. *Designs, Codes and Cryptography*, 72(2):345–367, 2014.