Honours Project Proposal

Generalised Russian Cards Problem

Ruaan Kellerman

1 The original problem

The following problem was posed in the 2000 Moscow Mathematics Olympiad:

> From a deck of seven distinct cards, Alice and Bob are each dealt three cards and Cathy is dealt the remaining card. None of the players knows any of the cards of the other players. Describe how, using a series of truthful public announcements, Alice and Bob can exchange information about the hands they hold without Cathy being able to deduce the owner of any card other than her own.

Alice and Bob can exchange complete information about their hands without disclosing any of their cards to Cathy in just one round of announcements. A solution is as follows. Label the cards 0, 1, 2, 3, 4, 5 and 6. Suppose without loss of generality that Alice was dealt the cards 1, 2 and 3, Bob was dealt the cards 4, 5 and 6, and Cathy was dealt the card 0. Alice constructs a Fano plane having her hand as one of its lines (Figure 1).

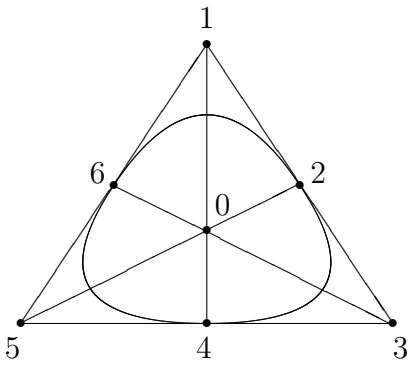

Figure 1: Alice's announcement

Alice starts by announcing that her hand corresponds to one of the lines of her Fano plane.

Alice: My hand is one of the following hands.

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

Since Bob holds the cards 4, 5 and 6, he deduces that Alice has the hand $\{1, 2, 3\}$. Cathy cannot conclude for any card other than her own whether Alice or Bob hold that card. Bob then makes the following announcement.

> Bob: Cathy holds the card 0.

Since Alice holds the cards 1, 2 and 3, she now deduces that Bob has the hand $\{4, 5, 6\}$. Cathy still cannot conclude for any card other than her own whether Alice or Bob hold that card.

Hence Alice and Bob have communicated their hands to each other without disclosing the ownership of any of their cards to Cathy.

2 A generalisation of the problem

The *generalised* Russian cards problem can be stated as follows:

> From a deck of $a + b + c$ distinct cards, three players Alice, Bob and Cathy are dealt a, b and c cards respectively. None of the players knows any of the cards of the other players. Describe how, using a series of truthful public announcements, Alice and Bob can exchange information about the hands they hold without Cathy being able to deduce the owner of any of the cards other than her own.

The generalised Russian cards problem can be formalised as a game $\mathrm{GRC}(a, b, c)$.

3 Encryption using public announcements

The most widely used encryption system for communicating electronic information is the RSA cryptosystem. Users who wish to communicate with each other using this system are both given a secret key (p, q) consisting of two large prime numbers p and q, while the product $n = pq$ of these two prime numbers is made public. The security of the RSA cryptosystem relies on the fact that it is computationally demanding to factorise n for large values of p and q, hence making it unfeasible, though not impossible, for an eavesdropper to decrypt messages for which they do not have the key (p, q). In 1994, Peter Shor developed a quantum algorithm that, were it ever to be implemented on a quantum computer, would allow for the factorisation of integers in polynomial time, hence making the RSA cryptosystem obsolete.

With the game $\mathrm{GRC}(a, b, c)$, Alice and Bob can be seen as two agents communicating sensitive information while Cathy is an eavesdropper. Since there are no private keys and all announcements are made publically, the game $\mathrm{GRC}(a, b, c)$ models a simple form of cryptography that is fully secure.

4 Goals of the project

In this project, the student will do a study of some of the important literature on the topic and will investigate solutions to $\mathrm{GRC}(a, b, c)$ for specific values of a, b and

c. The problem is finite but there is a combinatorial explosion that takes place even for small values of a, b and c so that the student should ideally have a programming background that would enable them to implement algorithms and check for solutions using a computer. A solid working understanding of basic combinatorics at the level of WTW 115 is essential. The project must be typeset using LaTeX. The project might be of interest to a student who enjoys combinatorics and who wishes to pursue interdisciplinary research between the fields of mathematics and computer science.