Safe communication for card players by combinatorial designs for two-step protocols

M. H. Albert* R. E. L. Aldred† M. D. Atkinson*
H. P. van Ditmarsch* C. C. Handley*

October 1, 2003

Abstract

Two parties A and B select a cards and b cards from a known deck and a third party C receives the remaining c cards. We consider methods whereby A can, in a single message, publicly inform B of her hand without C learning any card held by A or by B. Conditions on a, b, c are given for the existence of an appropriate message.

1 Introduction

At the Moscow 2000 Mathematical Olympiad the following problem was posed:

> *From a pack of seven known cards two players each draw in turn three cards. A third player gets the remaining card. How can the players with three cards openly inform each other about their cards without the third player learning any of the cards in their hands?*

This type of problem (with the same "card" terminology) has been studied in [1] as a model for communication among a team of computationally unlimited (perfectly rational) players including an eavesdropper, and this has been further explored in [4]. The communication protocols that such problems throw up are often rather subtle and they have been studied using dynamic epistemic logic in [9]. This has been used as a basis for a model checking approach in [10]. Also, various publications on the Russian cards problem intended for a more general audience have seen the light [6, 8, 3, 7].

In this paper we regard the Russian cards problem as the $(3, 3, 1)$ instance of the (a, b, c)-problem. We shall study solutions that are known to consist of two messages only. In such a solution the second message is trivial, because it may

*Department of Computer Science, University of Otago
†Department of Mathematics and Statistics, University of Otago

consist of revealing what the third player's c cards are, so our investigations focus on the first message only. We call this a *two-step protocol*.

We reformulate the problem in purely combinatorial terms, and show their equivalence to logical terms defined in [9]. We also give solutions for various (a, b, c), including one that applies in general when $a = O(\sqrt{b})$. Although our solutions succeed in preventing the third player from learning any particular card, they nevertheless reveal some information. Therefore we also give upper and lower bounds on how much information has to be revealed to the third player.

2 Notation and combinatorial formulation

We call the three players A, B, C, according to the number of cards a, b, c that they hold. We also let v denote the total number $a + b + c$ of cards, and Ω the set of those cards. All messages are supposed to be public and truthful announcements. Messages that enable A and B to learn each other's cards must originate from one of them. We shall suppose that the first message originates from A. The second message is just an announcement by B of C's card(s). All the complexity is therefore contained in A's announcement only.

Such an announcement may be of a very complex form ("I hold one of cards 1 and 4, if I hold card 3 then I do not hold card 6, moreover three of my cards are prime values,...") but, no matter how complex it is, it is tantamount to an announcement that simply lists a number of possible hands for A ("I hold one of the following sets of cards..."). This is because it is commonly known that a player's announcement is based on his/her information. For a proof, see [9]. We shall therefore take it that A announces a collection $\mathcal{L}$ of sets of size a ('A-hands'), one of which is her actual hand.

The collection $\mathcal{L}$ has to be such that B can (through knowing his own hand) rule out all but one A-hand in $\mathcal{L}$ as A's hand; yet C must not be able to infer any card in either of A or B's hands. The problem for A is to devise such an announcement that will be effective no matter what B (or C) holds. Informally, A's announcement must achieve the following three goals:

G1. B must be able to infer the actual hand of A

G2. C must not be able to infer any of A's cards

G3. C must not be able to infer any of B's cards

We assume the players to be perfectly rational, so for 'is able to infer' we may read 'know'.

These informal goals suffer from imprecision. One complication is that the meaning of A's announcement is partially determined by her intention to keep her cards a secret; and that intention depends on what the players consider an acceptable protocol. Another complication is, that so far we have only required that A's announcement is effective for a given actual A-hand, not that it is effective for any A-hand in $\mathcal{L}$. Before we continue, we give an example that illustrates these complications:

Example We name the seven cards $0, 1, 2, 3, 4, 5, 6$ and assume that the actual deal is that A holds $\{0, 1, 2\}$, B holds $\{3, 4, 5\}$ and C holds 6.

First, assume that A, B, C are told that A's single announcement should be sufficient for B to learn A's hand. (This makes it common knowledge.) Suppose A's announcement is

$$012, 034, 056, 135, 246, 235.$$

Player C can now reason as follows: "If A's hand is either 135 or 235, then if B's hand were 046, B would not have learnt A's hand. Player A knows that too. Therefore A would not have made that announcement if she actually held 135 or 235. Therefore she holds neither 135 nor 235. Further, from the remaining $012, 034, 056, 246$, A can obviously not hold 056 and 246 as I hold card 6 myself. So A's hand must be either 012 or 034, therefore A must hold card 0." So from the assumption that a *single* announcement by A (followed by a single announcement of B) should solve the problem, we can derive that this given announcement by A cannot be a solution.

Next, do not make that assumption. Instead, merely assume ('A, B, C are told') that solutions are finite sequences of announcements. From A's announcement $012, 034, 056, 135, 246, 235$ it can be concluded, by the argument above, that it is unclear to C if A knows that she has supplied enough information for B to learn her hand. As a matter of fact, A *has* supplied enough information, which becomes public from B now announcing in turn that C has card 6. But this only reduces the possible A-hands to $012, 034, 135, 235$ (C knew anyway that B's hand cannot be 046, so is not surprised by the outcome), and that is *not* enough information for C to determine the ownership of any specific card, other than card 6.

In other words: from the assumption that solutions are not required to consist of two announcements only, we can conclude that this is an acceptable solution that consists of two announcements. Now do we need to include this solution in the length-two solutions, or not? $\dashv$

Complications as illustrated in this example can be avoided by requiring that the problem constraints are *commonly known* to be met after an announcement, in a precise logical sense. For the problem domain that we investigate, this corresponds to requiring that the conditions are met regardless of the actual deal of cards or, in other words, that they are met *whenever* A can truthfully make that announcement [9, 10]. From this it follows that it is commonly known that A has informed B after her announcement, or, alternatively, that it is common knowledge that the protocol to be executed has length two. From now on, we will assume that this common knowledge requirement is *always* met.

The informal conditions given above can therefore be formalized as the following epistemic axioms:

EA1. Whenever A can announce $\mathcal{L}$, B knows A's hand after $\mathcal{L}$.

EA2. Whenever A can announce $\mathcal{L}$, C does not know any of A's cards after $\mathcal{L}$.

EA3. Whenever A can announce $\mathcal{L}$, C does not know any of B's cards after $\mathcal{L}$.

We can also formalize the informal conditions by means of three combinatorial axioms (a b-set is a set of b elements, etc.):

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

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

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

We now prove that the epistemic and combinatorial axioms correspond. We have to be careful in our formulations because of the interaction of different epistemic requirements. This is unavoidable as the epistemic requirements do not directly describe characteristics of the protocol but refer to its postconditions.

Theorem 1 *The Epistemic Axioms 1, 2, and 3 correspond to the Combinatorial Axioms 1, 2, and 3.*

Proof: Suppose that A announces a collection of possible hands $\mathcal{L}$.

CA1 $\Rightarrow$ EA1. Suppose that B's hand is X. If no member of $\mathcal{L}$ avoids X, A cannot have announced $\mathcal{L}$. If one member Y of $\mathcal{L}$ avoids X, B can infer that Y is A's hand.

CA1 $\Leftarrow$ EA1. Let X be a b-set such that there are unequal $Y_1, Y_2 \in \mathcal{L}$ with Y_1 and Y_2 both avoiding X. Then if B happened to hold X he would not know whether A held Y_1 or Y_2.

(CA1 &) CA2 $\Rightarrow$ EA2. Suppose that C's hand is Y. Player C can exclude, as hands for A, those members of $\mathcal{L}$ that intersect with his own. Also because of CA1, which implies EA1, these are the *only* A-hands he can exclude.* Therefore, in C's eyes the possible hands for A are those that are disjoint from his own. Since these possibilities have empty intersection, C cannot identify any card held by A.

*Without the presence of CA1, CA2 does not imply EA2. A typical counterexample is the one given above: for the given deal, after A-announcement $\mathcal{L} := 012, 034, 056, 135, 246, 235$, CA2 is satisfied but EA2 is not satisfied. Note that EA1 is indeed not satisfied, namely not for 135 and 235.

CA2 $\Leftarrow$ EA2. Suppose there is a c-set X such that $Z = \bigcap_{Y \cap X = \emptyset} Y$ is nonempty and let $q \in Z$. Then if C happened to hold X he would learn that A holds q.

(CA1 &) CA3 $\Rightarrow$ EA3. Suppose that C's hand is Y. Again, C can exclude, as hands for A, those members of $\mathcal{L}$ that intersect with his own. And in the presence of CA1, these are the *only* members of $\mathcal{L}$ that he can exclude. So he can deduce, as cards for B, only those cards not among such members of $\mathcal{L}$; but, by EA3, there are no such cards.

CA3 $\Leftarrow$ EA3. Suppose there is a c-set X such that (strictly) $Z = \bigcup_{Y \cap X = \emptyset} Y \subset \overline{X}$ and let $q \in \overline{X} \setminus Z$. Then if C happened to hold X he would learn that B held q. ■

In view of Theorem 1 we can, from now on, study two-step protocols using the language of Combinatorial Axioms 1, 2, 3.

Definition 1 *An announcement satisfying CA1, CA2, CA3 is called a* good announcement.

To give a foretaste of our results we consider the original Russian cards problem. Let us suppose that A's hand (three cards from $\{0, 1, \ldots, 6\}$) is actually $\{0, 1, 2\}$. Then A can announce that she holds one of the following: $012, 034, 056, 135, 146, 236, 245$. It is readily checked that this announcement satisfies the axioms.

It is not coincidental that the triples of this good announcement are the lines of the 7-point projective plane. As we shall see, many classical combinatorial configurations can be used to find such protocols. Motivated by the projective plane visualization of this Russian cards solution we shall henceforth refer to the members of any announcement as the *lines* of the announcement, and to the cards as the *points*.

We shall find it convenient sometimes to use an alternative formulation of CA1.

Lemma 1 *An announcement $\mathcal{L}$ satisfies CA1 if and only if for every pair of distinct lines $L_1, L_2 \in \mathcal{L}$ we have $|L_1 \cap L_2| < a - c$.*

Proof: Suppose that CA1 holds. Then for two lines $L_1, L_2 \in \mathcal{L}$, the set $\Omega \setminus (L_1 \cup L_2)$ consists of less than b cards, because any b-set can avoid only one but not two lines. We now have:

$$\begin{aligned} |\Omega \setminus L_1 \cup L_2| &< b \\ a + b + c - 2a + |L_1 \cap L_2| &< b \\ |L_1 \cap L_2| &< a - c \end{aligned}$$

Since this argument can be reversed the proof is complete. ■

A direct consequence of Lemma 1 is:

Corollary 1 *CA1 can only hold if $c < a$.*

We can also prove that c has to be strictly smaller than $a - 1$. For that, see Corollary 2, below. We further have that:

Lemma 2 *CA1 and CA2 can only hold simultaneously if $c < b$.*

Proof: If $c \geq b$, C can assume the role of B. Let CA1 hold for an announcement $\mathcal{L}$, and suppose $Z \in \mathcal{L}$ is the single line avoiding some b-subset X of C's actual hand Y. Then Z either also avoids Y or intersects with Y. In the first case CA2 will fail. In the second case A could not have made the announcement. ∎

There is no obvious size relation between a and b.

3 Bounds on the size of a good announcement

Having heard a good announcement by A, C will not be completely ignorant of what A holds. Initially, for a given C-hand, A could have had any one of $\binom{a+b}{a}$ hands within $\binom{a+b+c}{a}$ possibilities while, after the announcement, C knows A's hand to within $|\mathcal{L}|$ possibilities. Clearly, the least information is released to C if we maximise $|\mathcal{L}|$. Consequently, it will be of interest to give upper and lower bounds on the size $|\mathcal{L}|$ of good announcements. It is easy to verify that if an announcement satisfies CA1 then so does any subset of it. Also, if an announcement satisfies CA2 (or CA3) then so does any superset. From this it follows immediately that if $\mathcal{L}_1, \mathcal{L}_2$ satisfy CA1, CA2 and CA3, then also does any announcement such that $\mathcal{L}_1 \subseteq \mathcal{L} \subseteq \mathcal{L}_2$. So, in some cases, by finding a good announcement that meets a lower bound and another that meets an upper bound, we can infer the existence of good announcements having any value of $|\mathcal{L}|$ between these bounds.

Lemma 3 *In a good announcement every point lies in at least $c + 1$ lines.*

Proof: Suppose point x lies only in the lines $\{x, y_1, \ldots\}, \{x, y_2, \ldots\}, \ldots, \{x, y_t, \ldots\}$ where $t \leq c$. Consider a c-set X containing $\{y_1, y_2, \ldots, y_t\}$. Let L be a line that avoids X. Then $x \notin L$ (for otherwise L would contain one of $y_1, \ldots, y_t$). Hence

$$x \notin \bigcup_{L \cap X = \emptyset} L$$

This contradicts CA3 since the union in question is supposed to be the whole of $\Omega \setminus X$. ∎

Proposition 1 *The number of lines in a good announcement is at least*

$$(a + b + c)(c + 1)/a$$

Proof: The number of pairs (p, X) with point p in line X is exactly ka, where k is the number of lines. But, by Lemma 3, it is also at least equal to $(a+b+c)(c+1)$. ∎

Corollary 2 *If a good announcement exists then $c < a-1$.*

Proof: Corollary 1 shows that $c \leq a-1$. However, if $c = a-1$ then, for all lines $L_1 \neq L_2$, we have $L_1 \cap L_2 = \emptyset$ (by Lemma 1). Therefore every point lies in at most one line which contradicts Lemma 3. ∎

There is another lower bound argument that is better when a is relatively large and is particularly powerful for the parameters $(a, 2, 1)$. Suppose there are k lines. As above, there are ka point-line incidences and so there is some point p with at least ka/v lines through it and so with at most $k - ka/v = k(v-a)/v$ lines that avoid it. Now let X be any c-set that contains p and consider the lines that avoid X. These lines certainly avoid p and so there are $t \leq k(v-a)/v$ lines avoiding X. However, these t lines are subsets of the $(v-c)$-set $\Omega \backslash X$. This set of lines has, by CA2, trivial intersection but, if t a-subsets of a u-element set have empty intersection, then $t \geq u/(u-a)$. It follows that $t \geq (v-c)/(v-c-a) = (a+b)/b$. Putting this with the upper bound for t we have

Proposition 2 *The number of lines in a good announcement is at least*

$$\frac{(a+b)(a+b+c)}{b(b+c)}$$

For upper bounds on the number of lines we have two results.

Proposition 3 *The number of lines in a good announcement is at most*

$$\frac{(a+b+c)!(c+1)!}{(b+c)!(c+a+1)!}\left\lfloor\frac{a+c+1}{c+1}\right\rfloor$$

Proof: In this argument we will apply axiom CA1 for b-sets, when counting pairs (X, Y) where X is a $(b-1)$-set and Y is a line in $\mathcal{L}$ with $X \cap Y = \emptyset$. If there are k lines then there are k choices for Y and, for each Y, $\binom{b+c}{b-1}$ choices for X. So there are $k\binom{b+c}{b-1}$ such pairs. On the other hand we can choose X in $\binom{a+b+c}{b-1}$ ways. Having chosen X we want to bound the number $t = |\mathcal{T}|$ where $\mathcal{T}$ is the set of lines that avoid X. Given any $y \notin X$, $X \cup \{y\}$ has size b and so, by CA1, there is at most one line of $\mathcal{T}$ that avoids it. In other words at least $t-1$ of the lines of $\mathcal{T}$ contains y. Now we consider pairs (y, L) where $y \notin X$ and $L \in \mathcal{T}$ with $y \in L$. This gives the inequality

$$ta \geq (a+c+1)(t-1)$$

from which we have $t \leq \left\lfloor \frac{a+c+1}{c+1} \right\rfloor$. We therefore obtain

$$k\binom{b+c}{b-1} \leq \binom{a+b+c}{b-1}\left\lfloor \frac{a+c+1}{c+1} \right\rfloor$$

which gives the result. $\blacksquare$

Another upper bound on the number of lines is that

Proposition 4 *The number of lines in a good announcement is at most*

$$\frac{(a+b+c)!(c+1)!}{a!(b+2c+1)!}\left\lfloor \frac{b+2c+1}{c+1} \right\rfloor$$

Proof: Again, we will apply CA1, but this time by counting pairs (U, L) where U is a $(a-c-1)$-set, L is a line from $\mathcal{L}$, and $U \subseteq L$. If $\mathcal{L}$ contains k lines, there are $k\binom{a}{a-c-1}$ such pairs. On the other hand, if we have a $(a-c-1)$-set U, of which there are $\binom{a+b+c}{a-c-1}$, and look for the lines that contain it, we see, by Lemma 1 (that is based on CA1), that these lines cannot overlap outside U. So the $b+2c+1$ points outside U get partitioned by the lines containing U. As the parts of such lines lying outside U have size $a-(a-c-1) = c+1$, at most $\left\lfloor \frac{b+2c+1}{c+1} \right\rfloor$ such lines can exist. We therefore obtain

$$k\binom{a}{a-c-1} \leq \binom{a+b+c}{a-c-1}\left\lfloor \frac{b+2c+1}{c+1} \right\rfloor$$

which gives the result. $\blacksquare$

It is routine to determine the better of these upper bounds: if $b+c \leq a$ then the bound of Proposition 3 should be used, otherwise the bound of Proposition 4 should be used. In a few rare cases the upper and lower bounds meet. In particular

Theorem 2 *For the parameter set* $(a, 2, 1)$ *a good announcement exists if and only if* $a = 0, 4 \mod 6$, *and such an announcement consists of exactly* $(a+3)(a+2)/6$ *lines.*

Proof: Note that $(a+3)(a+2)/6$, the lower bound according to Proposition 2, and $(a+3)/3\lfloor(a+2)/2\rfloor$, the upper bound according to Proposition 3, are only both integral if $a = 0, 4 \mod 6$, and if so are equal. Otherwise, the upper bound is smaller than the lower bound so a good announcement cannot exist. The fact that a good announcement indeed exists when $a = 0, 4 \mod 6$ is justified subsequently in Corollary 3. $\blacksquare$

Example Given these lower and upper bounds, we now can eliminate various conceivable candidates for good announcements. Those close to $(3, 3, 1)$ may be considered of interest: note that there are no good announcements for $(3, 3, 2)$ and for $(3, 2, 1)$. $\dashv$

4 Protocol constructions

In this section we give a number of constructions for producing two-step protocols for various parameter sets (a, b, c). They vary in the seriousness of the proof required: here we have to keep in mind that our goal is to *design* protocols, and that the various constructions appear to serve that goal equally well. We include some typical examples, and end the section with some examples outside the presented constructions.

4.1 Given a and c, for sufficiently large b

Suppose that a and c are given with $1 \leq c < a-1$. We shall construct a good announcement with $a+b+c = \Omega(a^2)$. Choose any prime p with $p \geq a-1$. In the interests of economy we may wish to choose p as small as possible; certainly we can take $p < 2a$ by Bertrand's postulate but much tighter bounds are known. There is a Singer difference set S of size $p+1$ for the modulus $v = p^2+p+1$ [5]. The defining property of S is that the $p(p-1)$ non-zero differences $\{s_1 - s_2 \mid s_1, s_2 \in S\}$ represent every non-zero number modulo v exactly once. In S we choose any subset T of size a and define the family of subsets

$$\mathcal{L} = \{x + T \mid x \in Z_v\}$$

Here Z_v denotes the set of integers modulo v and the addition $x+T$ denotes addition modulo v.

Theorem 3 *If $1 \leq c < a-1$ and $b = v-a-c$ then $\mathcal{L}$ is the set of lines of a good announcement for the parameters (a, b, c).*

Proof: We verify the axioms in turn.

CA1. Let $x+T$ and $y+T$ be distinct lines. An element in their intersection has the form $x+t_1$ and also the form $y+t_2$ with $t_1, t_2 \in T$. But if $x+t_1 = y+t_2 \mod v$ then $x-y = t_2-t_1 \mod v$ and this, by the difference set property, defines t_1 and t_2 uniquely so no further elements of the intersection can exist. Hence, for every two distinct lines L_1, L_2 we have $|L_1 \cap L_2| \leq 1 < a-c$ and we now appeal to Lemma 1.

CA2. Let $\{u_1, u_2, \ldots, u_c\}$ be an arbitrary c-set. Suppose there was a point p, such that in an arbitrary line $x+T$ that avoided this c-set, p was in it. Then we would have

$$\text{if } u_i \notin x+T \text{ for all } i \text{ then } p \in x+T$$

which we may rewrite as

$$\text{if } x \notin u_i - T \text{ for all } i \text{ then } x \in p-T$$

and this says that

$$\overline{\bigcup (u_i - T)} \subseteq p - T$$

Comparing the sizes of these sets we have

$$v - ca \leq a$$

which gives

$$v \leq ca + a \leq (a-2)a + a \leq (p-1)(p+1) + p + 1 = p^2 + p$$

a contradiction.

CA3. Again let $\{u_1, u_2, \ldots, u_c\}$ be an arbitrary c-set. This time suppose there was a point p not equal to any u_i in none of the lines that avoided this c-set. Then we would have

$$\text{if } u_i \notin x + T \text{ for all } i \text{ then } p \notin x + T$$

which we may rewrite as

$$\text{if } x \notin u_i - T \text{ for all } i \text{ then } x \notin p - T$$

and this condition is exactly that

$$p - T \subseteq \bigcup (u_i - T)$$

which we can write as

$$p - T = \bigcup ((u_i - T) \cap (p - T))$$

Since $p - T$ (a set of size a) is a union of c subsets one of them must have size at least $a/c > 1$. But each $(u_i - T) \cap (p - T)$ is the negative of $(T - u_i) \cap (T - p)$ which we saw above had size at most 1. Again, a contradiction. ∎

Example An example is the 13-line good announcement for $(4, 7, 2)$. Note that $(p = 3)$ $3^2 + 3 + 1 = 13$. We also get a 7-line announcement for $(3, 3, 1)$ this way $(p = 2)$, e.g. $\{012, 034, 056, 135, 146, 236, 245\}$. ⊣

4.2 Good announcements for $(3, b, 1)$

If $a = 3$ a good announcement can only exist if $c = 1$ (Corollary 2). Here we have

Proposition 5 *If $b \geq 3$ there is a good announcement with parameters $(3, b, 1)$.*

Proof: We give a constructive proof. First suppose that the number of points $b + 4$ is a multiple of 3, say $3m$. As points we take symbols x_i, y_i, z_i with $0 \leq i < m$. Consider the set of (altogether $2m$) lines

$$\{x_i, y_i, z_i\}, \{x_i, y_{i+1}, z_{i+2}\}$$

where $0 \leq i < m$ and subscripts are interpreted modulo m. It is readily checked that the conditions for a good announcement hold provided that $m \geq 3$. If $b + 4 = 2, 1 \mod 3$ we begin with the announcement above and remove one or two points respectively with a suitable adjustment of lines. In the first case we remove the single point z_{m-1}, and the lines $\{x_{m-1}, y_{m-1}, z_{m-1}\}$ and $\{x_{m-3}, y_{m-2}, z_{m-1}\}$ that contain it. Then we define new lines $\{x_{m-1}, y_{m-1}, y_{m-2}\}$ and $\{x_{m-3}, y_{m-2}, x_{m-1}\}$. In the second case we remove y_{m-1} and z_{m-1} and their three incident lines replacing them by $\{x_{m-3}, y_{m-2}, x_{m-1}\}$ and $\{x_{m-2}, x_{m-2}, z_0\}$. In both cases it is easy to verify that the resulting configurations are good announcements of the required types. ∎

Notice that the construction produces a good announcement whose number of lines meets the lower bound of Proposition 1.

Example Applying this construction, we get a 5-line good announcement for $(3, 3, 1)$, e.g. $\{012, 034, 056, 135, 246\}$. It is not contained in a 7-line announcement as found above. Note that the initial example motivating the 'common knowledge' requirements is an extension of this announcement (with 235). ⊣

4.3 Good announcements for $(a, 2, 1)$ using block designs

The combinatorial axioms are reminiscent of design-theoretic definitions so it is perhaps not surprising that we can use designs to generate good announcements. We recall the definition of a t-design with parameters (v, k, λ). Relative to a v-set Ω this is a collection of k-subsets of Ω called *blocks* with the property that every t-subset of Ω is contained in exactly λ blocks.

Proposition 6 *If D is a $b - (a + 2b - 1, 2b - 1, 1)$-design, then $\overline{D}$ is a good announcement for $(a, b, b - 1)$ where $\overline{D}$ denotes the set of lines that are the complements of the blocks of D.*

Proof: We check each of the three axioms in turn.

CA1. Let X be an arbitrary b-set. If X avoids at least two lines in $\overline{D}$ then, as the lines in $\overline{D}$ are the complements of the blocks in D, there must be at least two blocks in D that contain X, a contradiction.

CA2. Let X be an arbitrary c-set (where $c = b - 1$) and consider the lines that avoid it. If this set of lines did not have empty intersection then some element x would belong to all of them. But that would mean that, in D, no block containing X would also contain x.

CA3. Let X be an arbitrary c-set (again $c = b - 1$) and consider the lines that avoid it. If the union of this set of lines was not $\Omega \setminus X$ we could find some $x \notin X$ belonging to none of them. So, in D, every block containing X would also contain x. But there is only one such block and therefore only one line avoiding X contradicting CA2. ∎

As a consequence we can complete the proof of Theorem 2.

Corollary 3 *There is a good announcement for* $(a, 2, 1)$ *if* $a = 0, 4 \mod 6$.

Proof: With $b = 2$ the designs of the previous proposition are exactly the Steiner triple systems; it is well known [2]that these exist if and only if $a = 0, 4 \mod 6$. ■

Example 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). $\dashv$

4.4 From $(a, b, c + 1)$ to (a, b, c)

Proposition 7 *If there is a good announcement for* $(a, b, c + 1)$*, then there is one for* (a, b, c).

Proof: In the case (a, b, c), player A starts by publicly introducing a virtual new card q. Player A then makes a good announcement for $(a, b, c + 1)$. ■

This proposition also applies when $c = 0$. However, cases $(a, b, 0)$ are trivial, because then A and B already know each other's hand without the need for any announcement at all. A non-trivial example is that there exists a good announcement for $(4, 7, 1)$, because (by Theorem 3) we have one for $(4, 7, 2)$.

4.5 From (a, b, c) to (b, a, c)

There is a good announcement for $(4, 2, 1)$, by Corollary 3. There is no good announcement for $(2, 4, 1)$, because $a - 1 \not< c$ (Corollary 2). What does this mean for players A and B that want to communicate their hand of cards to each other? From a communicative perspective, it is sufficient if at least one, if not both, of the players can make an informative announcement. As all players are aware of this, in the case of $(2, 4, 1)$ player A would simply wait for B to announce a $(4, 2, 1)$ protocol, and only then respond. Alternatively, A might have started by saying to B: "Please go ahead, B, you know I can't do anything."

4.6 Good announcements for $(4, 4, 1)$ and $(5, 5, 1)$

For values of $b \geq 3$, designs that satisfy the hypotheses of Proposition 6 are fairly rare. Rare designs also arise in the construction of good announcements for other parameter sets. However, we shall be content with giving just two further examples that, in some sense, are the 'next' larger versions of the original Russian cards problem.

Proposition 8 *Name the cards* $1, 2, 3, 4, 5, 6, 7, 8, 9$. *The* 18 *quadruples*

$$2468, 4579, 2347, 1679, 1456, 1389, 3678, 2359, 1258$$

$$1357, 1236, 5689, 3458, 2789, 2567, 1249, 1478, 3469$$

are a good announcement for the parameter set $(4,4,1)$. *Every good announcement for* $(4,4,1)$ *has at most* 18 *lines.*

Proof: The fact that a good announcement cannot have more than 18 lines is a consequence of Proposition 4. It may be verified directly that the stated announcement satisfies CA1, CA2, and CA3. However we shall give a brief indication of how this announcement was discovered. Let F be the field of 9 elements. The multiplicative group of F is the disjoint union $G \cup H$ of its subgroup of order 4 with its other coset. The announcement then consists of the additive translates of G and H by elements of F. This algebraic definition makes it somewhat easier to check the axioms. ∎

Proposition 9 *There exists a set of* 66 *quintuples that are a good announcement for the parameter set* $(5,5,1)$. *No good announcement for* $(5,5,1)$ *has more than* 66 *lines.*

Proof: Proposition 4 gives the upper bound. The good announcement meeting this upper bound is the set of 66 blocks of the $4-(11,5,1)$ design whose automorphism group is the quadruply transitive group M_{11}. Two distinct blocks cannot intersect in a set of size 4 as that contradicts the defining property of the design so CA1 holds by Lemma 1. Axioms CA2 and CA3 are also easily proved. Let x be any point and let $\mathcal{L}_0$ be the set of blocks that avoid x. If there exists a point y in the intersection of this set of blocks then, as the stabiliser of x in M_{11} permutes the members of $\mathcal{L}_0$ and acts transitively on the set of points not equal to x, *every* point y lies in the intersection; this contradicts CA1. The same argument reaches a contradiction from the assumption that there exists a point $y \neq x$ in none of the blocks of $\mathcal{L}_0$. ∎

5 Conclusions and further research

Given three players A, B, C that hold, respectively, a, b, c cards from a deck of known cards, A can sometimes publicly inform B of her hand without C learning any card held by A or by B. General combinatorial requirements have been shown to be equivalent to known logical terms. We have given solutions, called 'good announcements' for various (a,b,c), including one that applies in general when $a = O(\sqrt{b})$. We have also given upper and lower bounds on how much information has to be revealed to the third player.

We are not yet able to determine for an arbitrary (a,b,c) if a good announcement exists and if so, to construct one.

There are two main reasons why our results may be considered relevant for cryptology. First, the upper and lower bounds on revealed information can also be turned around: based on a security requirement for A and B, e.g., that an eavesdropper C should have a less than 5% chance to guess their secrets correctly after having intercepted the message, one may design a protocol by appropriate choices of (a, b, c). Note that the underlying scenario is not very specific for card deals but rather generally applicable to distributed systems where a scarce resource is known to be distributed over the agents. Second, the initial example in which it was not assumed that the protocol is commonly known to be of length two, illustrates that we may weaken good announcements so that they are still effective for A and B but even less informative to C, as C may not even learn that A has succeeded in informing B, before B confirms that. In other words: a rational eavesdropper does not yet have enough reason to break into B's computer in order to gather the secret, but may still consider to await further messages from either A or B. This is to the advantage of A and B.

References

[1] M.J. Fischer and R.N. Wright. Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology*, 9(2):71–99, 1996.

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

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

[4] 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.

[5] J. Singer. A theorem in finite projective geometry and some applications in number theory. *Trans. Amer. Math. Soc.*, 43:377–385, 1938.

[6] H.P. van Ditmarsch. Killing cluedo. *Natuur & Techniek*, 69(11):32–40, 2001.

[7] H.P. van Ditmarsch. Het zeven-kaartenprobleem (the seven cards problem). *Nieuw Archief voor Wiskunde*, 5/3(4):326–332, 2002.

[8] H.P. van Ditmarsch. Oplossing van het mysterie (solution of the murder mystery). *Natuur & Techniek*, 70(2):17, 2002.

[9] H.P. van Ditmarsch. The russian cards problem. *Studia Logica*, 75:31–62, 2003.

[10] S. van Otterloo, W. van der Hoek, and M. Wooldridge. Model checking; a knowledge exchange scenario. In xx, editor, *Proceedings of the Second International Workshop on Model Checking and Artificial Intelligence (MOCHART-2003)*, 37–44.