

Communication Complexity of the Russian Cards Problem

Aiswarya Cyriac and K. Murali Krishnan

January 10, 2009

The Russian Cards Problem

- ▶ From a pack of seven known cards two players each draw three cards and the third player gets the remaining card. How can the players with three cards openly(publicly) inform each other about their cards, without the third player learning from any of their cards who holds it?

- ▶ The various solutions in the literature take at least two announcements.
- ▶ It is not possible to solve it in one announcement. Proof?

Modeling in Dynamic Epistemic Logic

- ▶ Let $U = \{0, 1, 2, 3, 4, 5, 6\}$ be the set of cards.
- ▶ $N = \{a, b, c\}$ (representing Anne, Bill and Cath) be the set of players.
- ▶ The basic propositions are 'card 0 is with Anne,' 'card 3 is with Bill' and so on. If i_x denotes 'card i is with x ' then the set of basic propositions $P = \{i_x \mid x \in N, i \in U\}$.

Modeling in Dynamic Epistemic Logic

- Initially Player a and Player b have three cards each and Player c has one card. The Kripke model for the initial game state is given by

$M = \langle W, R, V \rangle$ where,

$$W = \{(A, B, C) \mid |A| = |B| = 3, |C| = 1, A \cup B \cup C = U\}$$

$$R(a) = \{((A, B, C), (A', B', C')) \mid A = A'\}$$

$$R(b) = \{((A, B, C), (A', B', C')) \mid B = B'\}$$

$$R(c) = \{((A, B, C), (A', B', C')) \mid C = C'\}$$

$$V((A, B, C)) = \{i_a \mid i \in A\} \cup \{i_b \mid i \in B\} \cup \{i_c \mid i \in C\}$$

Modeling in Dynamic Epistemic Logic

- ▶ For each $A \subseteq U, |A| = 3$, let $T_A = \{(A', B', C') : A' = A, |B'| = 3, |C'| = 1 \text{ and } A' \cup B' \cup C' = U\}$.
- ▶ For each $B \subseteq U, |B| = 3$, let $S_B = \{(A', B', C') : B' = B, |A'| = 3, |C'| = 1 \text{ and } A' \cup B' \cup C' = U\}$
- ▶ For each $C \subseteq U, |C| = 1$, let $Q_C = \{(A', B', C') : C' = C, |A'| = |B'| = 3 \text{ and } A' \cup B' \cup C' = U\}$.

Modeling in Dynamic Epistemic Logic

Example: $A = \{0, 1, 2\}$,

$T_A = \{(\{0, 1, 2\}, \{3, 4, 5\}, \{6\}), (\{0, 1, 2\}, \{3, 4, 6\}, \{5\}),$
 $(\{0, 1, 2\}, \{3, 5, 6\}, \{4\}), (\{0, 1, 2\}, \{4, 5, 6\}, \{3\})\}$.

Player a cannot distinguish between these four states because in all the four states Player a 's hand is $\{0, 1, 2\}$.

Lemma 1

Lemma

Assume that RCP is solved in Kripke model $M = (W, R, V)$ and for all A, B and C such that $|A| = |B| = 3$ and $|C| = 1$, T_A, S_B and Q_C are components of $R(a), R(b)$ and $R(c)$ respectively. Let $\{w^*\}$ be the actual state. Then the following statements hold:

1. $\exists A, \exists B$ such that $T_A = S_B = \{w^*\}$
2. $\forall C, w^* \in Q_C \Rightarrow |Q_C| > 1$.

Theorem 1

Theorem

There exist no single announcement solution to the RCP.

A generalisation

- ▶ Consider a natural generalisation of the RCP in which Anne and Bill are holding k cards each and Cath is holding l cards from a pack of $2k + l$ cards. We denote this version of the RCP as $\text{RCP}(k; l)$. Hence the original RCP discussed before is $\text{RCP}(3; 1)$ in the new notation.

- ▶ The Kripke model is defined similar to the RCP(3; 1) case.
- ▶ T_A, S_B and Q_C are also defined similarly.
- ▶ $R(a)$ and $R(b)$ will have $\binom{2k+l}{k}$ components each with $\binom{k+l}{k} \times \binom{l}{l} = \binom{k+l}{k}$ elements each.
- ▶ Player a is making an announcement α for a set of components \mathcal{T}_α .

Player c should not learn even a single card with a or b .

Lemma

$$\bigcup_{T_A \in \mathcal{T}_\alpha} A = U \quad (1)$$

$$\bigcap_{T_A \in \mathcal{T}_\alpha} A = \emptyset \quad (2)$$

Lemma

For $k \geq 2$, $l > \frac{2k^2}{\ln k}$ for any announcement α satisfying the above Lemma $\exists s_1, s_2 \in \bigcup_{T_A \in \mathcal{T}_\alpha} T_A$ such that $s_1 \neq s_2$ and $(s_1, s_2) \in R(b)$

Theorem 2

Theorem

For $k \geq 2$, $l \geq \frac{2k^2}{\ln k}$, there exists no two announcement solution to the RCP($k; l$).

Conclusions and further directions

- ▶ The bound obtained is weaker than the result by Albert et. al. [Albert '05]
- ▶ Improve the bound.
- ▶ Find solutions which require more than two announcements.