KRML 73 -0

The problem of the hidden card

K. Rustan M. Leino

4 October 1996

Digital Equipment Corporation Systems Research Center
130 Lytton Ave., Palo Alto, CA 94301, U.S.A.
rustan@pa.dec.com

In this problem, you and a partner are to come up with a scheme for communicating the value of a hidden card. The game is played as follows:

0. Your partner is sent out of the room.
1. The dealer hands you 5 cards from a standard 52 card deck.
2. You look at the cards, and hand them back to the dealer, one by one, in whatever order you choose.
3. The dealer takes the first card that you hand her and puts it, face up, in a spot labeled "0". The next three cards that you hand her, she puts, similarly, in spots labeled "1", "2", and "3". The last card that you hand her goes, face down, in a spot labeled "hidden". (While you control the order of the cards, you have no control over their orientations, sitting in their spots; so you can't use orientation to transmit information to your partner.)
4. Your partner enters the room, looks at the four face-up cards and the spots in which they lie and, from that information, determines the suit and value of the hidden card.

Question: What is the foolproof scheme that you and your partner settled on ahead of time?

(Turn for my solution...)

Observation A You're given more cards (5) than there are suits (4), so by the "the maximum is at least the average"-rule there exist two cards of the same suit. Call this suit S, and let s and t denote the values of two of the given cards of suit S such that $s < t$. We have

$$1 \leq s < t \leq 13 \quad . \qquad (*)$$

For any integers s and t satisfying (*), we have either

$$1 \leq t - s \leq 6 \qquad \text{(this holds if } t - s \leq 6\text{)}$$

or

$$1 \leq s - t + 13 \leq 6 \qquad \text{(this holds if } 6 < t - s\text{)} \quad .$$

Observation B You can permute the 3 remaining cards in 6 different ways. This lets you encode a number between 1 and 6.

For example, if, before the game begins, you and your partner agree on a total ordering of the 52 cards of a standard deck, then the order of the cards "1", "2", and "3" can be used to represent the numbers between 1 and 6 as follows.

order	number
card "1" $<$ card "2" $<$ card "3"	1
card "1" $<$ card "3" $<$ card "2"	2
card "2" $<$ card "1" $<$ card "3"	3
card "2" $<$ card "3" $<$ card "1"	4
card "3" $<$ card "1" $<$ card "2"	5
card "3" $<$ card "2" $<$ card "1"	6

Your play Pick cards (S, s) and (S, t) as described in Observation A above. If $t - s \leq 6$, then choose (S, s) as card "0", choose (S, t) as the hidden card, and encode the number $t - s$ using the remaining cards as described in Observation B. If $6 < t - s$, then choose (S, t) as card "0", choose (S, s) as the hidden card, and encode the number $s - t + 13$ using the remaining cards.

Your partner's play Let (S, r) denote card "0" and let n denote the number encoded by cards "1", "2", and "3". If $r + n \leq 13$, then the hidden card is $(S, r + n)$. If $13 < r + n$, then the hidden card is $(S, r + n - 13)$.

Proof To demonstrate that this strategy is foolproof, I will use techniques of program inversion. Using the variable names from above, your play is described by the program

$$
\begin{array}{lll}
P\text{:} & \{1 \le s < t \le 13\} & \\
& \textbf{if}\ \ t - s \le 6 \longrightarrow r, n := s, t - s & \{1 \le n \le 6 \ \wedge\ r + n \le 13\} \\
& \Box\ \ 6 < t - s \longrightarrow r, n := t, s - t + 13 & \{1 \le n \le 6 \ \wedge\ 13 < r + n\} \\
& \textbf{fi} \quad . &
\end{array}
$$

The assertions at the end of the two **if** branches can be proven from the precondition of P and the respective guards. Each of the two assertions implies $1 \le n \le 6$, which shows that the encoding is always possible.

Your partner's play is described by the program

$$
\begin{array}{ll}
Q\text{:} & \textbf{if}\ \ r + n \le 13 \longrightarrow s, t := r, r + n \\
& \Box\ \ 13 < r + n \longrightarrow s, t := r + n - 13, r \\
& \textbf{fi} \quad .
\end{array}
$$

To show that Q is the inverse of P, it suffices to notice the correspondence between the assertions in P and the guards in Q, that the guards are mutually exclusive, and that the following Hoare triples hold for any X and Y:

$$
\begin{array}{lll}
\{s = X \ \wedge\ t = Y\} & r, n := s, t - s\ ;\ s, t := r, r + n & \{s = X \ \wedge\ t = Y\} \\
\{s = X \ \wedge\ t = Y\} & r, n := t, s - t + 13\ ;\ s, t := r + n - 13, r & \{s = X \ \wedge\ t = Y\}
\end{array}
$$

The fact that program Q restores the values of s and t means that your partner can easily determine which of s and t is r and which is the value of the hidden card.

Omitted from the proof is the fact that the suit of card "0" is the same as the suit of the hidden card.

Acknowledgements Lyle Ramshaw communicated the problem to me, and the wording of the problem above is mostly his. I don't know who designed the problem.