The Importance of Being Formal

K.S. Makarychev, Yu.S. Makarychev

The following problem (suggested by A. Shapovalov) was given to the participants of Moscow Math Olympiad (spring 2000).

> The deck of cards contains 7 cards labeled $0, 1, 2, 3, 4, 5, 6$. Cards are shuffled and distributed among three people A, B, C. Both A and B receive three cards each; the remaining card is given to C. Show that A and B can exchange information about their cards (after that B knows A's cards and vice versa) speaking in presence of C in such a way that C still cannot name any card (different from his own) and say whether A or B has it.

The organizers of the Olympiad considered this problem as well posed having in mind the following solution:

> Each player (A and B) declares the sum modulo 7 of three cards he has.

The sum of two declared numbers will be the sum of all cards $(0+1+2+\ldots+5+6)$ minus C's card, so A and B know C's card and therefore know cards of each other.

It remains to show that C still has no information about any card (except for his own). Assume for example that C has card with 6 on it. The following table shows that any sum of (say) A's cards does not prevent him to have any specific card (each row contains combinations with any of the cards $0 \ldots 6$):

Sum	Possible combinations
0	(025), (034), (124)
1	(035), (125), (134)
2	(045), (135), (234)
3	(012), (145), (235)
4	(013), (245)
5	(014), (023), (345)
6	(015), (024), (123)

Therefore C cannot name one of B's cards. For the same reason C cannot name one of A's cards.

If C had any other card (instead of 6), the situation is similar (circular shift does not change anything).

However, the situation with problem is not so simple. To explain why, let us consider the following “solution”. Assume that A has cards $\{p, q, r\}$. Then he says to B:

> If you don't have card p, then I have cards $\{p, q, r\}$

Since B does not have p, he concludes that A has $\{p, q, r\}$. Then B make a similar statement about his cards $\{u, v, w\}$ and says “If you don't have u then I have $\{u, v, w\}$.”

Note that both statements remain true if A and B exchange cards (A has $\{u, v, w\}$ and B has $\{p, q, r\}$), so C cannot tell where any of the cards is.

Is this solution “good”? Probably you agree that something is wrong with it: in fact in his message A somehow discloses his cards though is an indirect way. But what does it mean and what is a “good” solution anyway?

We see that to make the problem clear one need a formal definition. It turns out that there are several natural definitions which are not equivalent. Let us describe two of them shortly.

(1) The solution is a pair of algorithms α and β that prescribe behavior of A and B during the game (what to say given the cards and the message of other player). We require that for any initial configuration of cards the protocol of exchange together with A's cards determine B's cards uniquely and vice versa. On the other hand, for any configuration and for each card x (except for C's card) there should exist another configuration that produces the same protocol but gives x to a different player.

(2) The solution is a rule that says what statements A and B made when seeing their cards. (A *statement* is any subset of the set of all configurations.)

We require that $A's$ statement together with B's cards determines A's card uniquely and vice versa, but A's and B's statements together with C's card do not determine the position of any other card.

These definition can be applied not only to this game but also to other similar games and one can prove that definition (1) is stronger. The first solution above satisfies both definitions (1) and (2) but the second (the "bad" one) satisfies only (2). If we had 5 cards instead of 7 (A and B have 2 cards, C has 1 card) the problem would be unsolvable according to the definition (1) but the "bad" solution still works for the definition (2).

Let us mention also that there is one more natural definition lying in-between (1) and (2).

What is the moral of this story? The importance of being formal is well understood in logic (and in computable cryptography which, by the way, can also provide a "solution" to our problem using public-key cryptosystems). But we see that even in very simple cases the absence of formal definition leads to ambiguity (better to be avoided, especially for a math competition problem!).