

Challenge of the Week

February 24–March 2, 2009

Problem

This nifty problem was suggested by Tom Boothby. It arose while finding efficient algorithms to do arithmetic in finite fields for SAGE. A bit of background is necessary.

Define the four “inputs”

$$A = \begin{array}{|c|c|c|} \hline 0 & 1 & 1 \\ \hline 0 & 1 & 1 \\ \hline 0 & 1 & 1 \\ \hline \end{array} \quad a = \begin{array}{|c|c|c|} \hline 0 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline \end{array}$$
$$B = \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 1 & 1 & 1 \\ \hline 1 & 1 & 1 \\ \hline \end{array} \quad b = \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline 1 & 1 & 1 \\ \hline \end{array}$$

consisting of 3×3 arrays of 1's and 0's. We are allowed to combine these inputs together using the logical operations \wedge (and), \vee (or), \oplus (exclusive or). Associating “true” with a 1, and “false” with a 0, the following table summarizes the operations.

r	s	$r \wedge s$	$r \vee s$	$r \oplus s$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

We apply these operations to each of the cells in the 3×3 grids, so for example, we have

$$A \wedge b = \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline 0 & 1 & 1 \\ \hline \end{array} \quad A \vee b = \begin{array}{|c|c|c|} \hline 0 & 1 & 1 \\ \hline 0 & 1 & 1 \\ \hline 1 & 1 & 1 \\ \hline \end{array} \quad A \oplus b = \begin{array}{|c|c|c|} \hline 0 & 1 & 1 \\ \hline 0 & 1 & 1 \\ \hline 1 & 0 & 0 \\ \hline \end{array}$$

Suppose we wish to make the outputs V and W from combinations of A , a , B and b .

$$V = \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 1 \\ \hline \end{array} \qquad W = \begin{array}{|c|c|c|} \hline 0 & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline \end{array}$$

We can make V and W in four steps as follows:

1. Let $C = a \wedge B$
2. Let $D = b \wedge A$
3. Let $V = C \vee b$
4. Let $W = D \vee a$

But if we're clever, we can do it with only three steps, like this:

1. Let $E = a \vee b$
2. Let $V = E \wedge B$
3. Let $W = E \wedge A$

Now we're ready for the puzzle: Starting from the four inputs A , a , B and b , make outputs X and Y in the fewest number of steps.

$$X = \begin{array}{|c|c|c|} \hline 0 & 0 & 1 \\ \hline 0 & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline \end{array} \qquad Y = \begin{array}{|c|c|c|} \hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 1 \\ \hline \end{array}$$

Solution

It is possible to make X and Y in six steps, as shown below. Tom Boothby says that no solution with fewer than six steps exists, though proving this is difficult.

1. Let $C = a \oplus B$
2. Let $D = A \oplus b$
3. Let $X = C \wedge D$ (have X now)
4. Let $E = D \oplus a$
5. Let $F = C \oplus b$
6. Let $Y = E \vee F$ (have Y now)