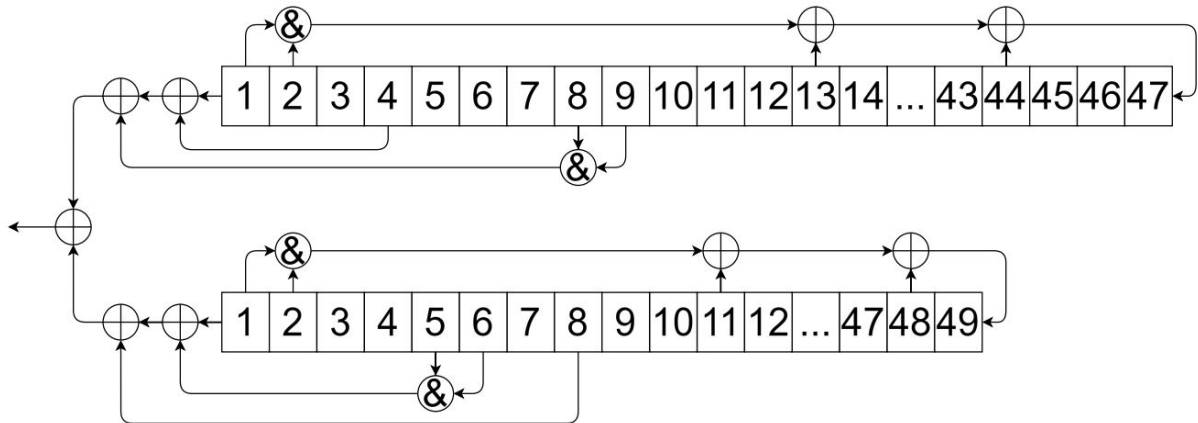




Problem 4. «A nonlinear generator»

Alice invented a keystream generator presented at the figure:



It consists of two shift registers of lengths 47 and 49 with non-linear feedback functions. The contents of the cells of a specific register at any time moment $t = 1, 2, \dots$ form the state number t of this register. At time t , each register first generates keystream bit number t and then transitions to the next state number $t + 1$. The states of the registers at moment t are denoted as

$$A(t) = (a_1(t), \dots, a_{47}(t)) \text{ and } B(t) = (b_1(t), \dots, b_{49}(t)) \text{ respectively.}$$

Both registers are shifted synchronously. For instance,

$$A(t + 1) = (a_2(t), \dots, a_{47}(t), (a_1(t) \& a_2(t)) \oplus a_{13}(t) \oplus a_{44}(t)).$$

The keystream Γ of length 8192, created by this generator, is given and can be found in [keystream.txt](#). Also, the states $A(8192)$ and $B(8192)$ are known:

$$A(8192) = (00101001110001001110111001100001010100000101110),$$

$$B(8192) = (0000010000101001000011000001010111001110000100101).$$

Could you find the initial states $A(1)$ and $B(1)$ of these registers?