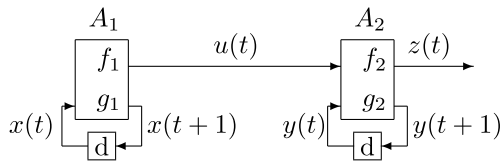
Problem 9. «Finite-state machines»

Problem for a special prize!

Alice decided to invent some generator that produces a sequence of maximal possible period relatively to its state size. Since she knows about finite-state machine, her generator G is constructed using two such machines A_1 and A_2:

- $A_1 = (\mathbb{F}_2^n, \mathbb{F}_2, g_1, f_1)$ with the state-transition function $g_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and the output function $f_1 : \mathbb{F}_2^n \to \mathbb{F}_2$, $n \geqslant 1$;
- $A_2 = (\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2, g_2, f_2)$ with the state-transition function $g_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ and the output function $f_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2$, $m \geqslant 1$.



For any $t = 1, 2, \ldots$, let

1. $x(t)$ and $y(t)$ be the states of A_1 and A_2 respectively, $x(1)$ and $y(1)$ be the initial states;
2. $x(t+1) = g_1(x(t))$ be the next state of A_1 and $u(t) = f_1(x(t))$ be the output bit of A_1;
3. $y(t+1) = g_2(u(t), y(t))$ be the next state of A_2 and $z(t) = f_2(u(t), y(t))$ be the output bit of A_2.

The sequence $z(1), z(2), z(3), \ldots$ is the output of the generator G. It is not difficult to see that it is eventually periodic whose the smallest period does not exceed 2^{n+m}.

Due to experiments, Alice noticed that the least period of the output sequence of G is less than 2^{n+m} if the Hamming weight of f_1 is even. Help Alice to prove or disprove this conjecture.

Remark. Recall that the Hamming weight of a Boolean function is the number of arguments on which it takes the value one.