Task 9. «Add-Rotate-Xor»

Let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2 = \{0, 1\}$. A vector $x \in \mathbb{F}_2^n$ has the form $x = (x_1, x_2, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. This vector can be interpreted as the integer $x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \ldots + x_{n-1} \cdot 2 + x_n$.

Alice can implement by hardware the following functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ for all vectors $a, b \in \mathbb{F}_2^n$ and all integers r, $0 < r < n$:

1) $f_a(x) = x \boxplus a$ — addition of vectors x and a as integers modulo 2^n for a fixed a;

2) $g_r(x) = x \lll r$ — cyclic rotation of a vector x to the left by r positions for a fixed positive integer r;

3) $h_b(x) = x \oplus b$ — coordinate-wise sum of vectors x and b modulo 2 for a fixed b.

- Bob asks Alice to construct two devices that compute the functions S_1 and S_2 from $\mathbb{F}_2^2$ to $\mathbb{F}_2^2$ given by their truth table:

x	(00)	(01)	(10)	(11)
$S_1(x)$	(01)	(00)	(10)	(11)
$S_2(x)$	(01)	(11)	(00)	(01)

  Can Alice do it? If «yes», show how it can be done; if «no», give an explanation!

- Generalizing the problem above: can we construct any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ using only a finite number of compositions of functions f_a, g_r and h_b?

  And what about any permutation over $\mathbb{F}_2^n$?

  Consider at least the cases $n = 2, 3, 4$.

- Is it possible to compute every function h_b using only functions f_a and g_r?