



Problem 2. «Stairs-Box»

Nicole was climbing stairs and has found a box containing a curious permutation on the set of elements $\{0, 1, \dots, 63\}$:

$$S = [\begin{array}{l} 13, 18, 20, 55, 23, 24, 34, \quad 1, 62, 49, 11, 40, 36, 59, 61, 30, \\ 33, 46, 56, 27, 41, 52, 14, 45, \quad 0, 29, 39, \quad 4, \quad 8, \quad 7, 17, 50, \\ 2, 54, 12, 47, 35, 44, 58, 25, 10, \quad 5, 19, 48, 43, 31, 37, \quad 6, \\ 21, 26, 32, \quad 3, 15, 16, 22, 53, 38, 57, 63, 28, 60, 51, \quad 9, 42 \end{array}]$$

So, the element 0 it maps to 13, the element 1 to 18, etc.

Nicole understands that it is possible to consider such a permutation as a vectorial Boolean function $S : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^6$ if every number between 0 and 63 one replaces with a binary vector of length 6. For instance, $S(000010) = (010100)$, since S maps 2 to 20. She knows that S can be given in terms of coordinate functions as $S(x) = (s_1(x), \dots, s_6(x))$, and each Boolean function s_i can be represented in the algebraic normal form using binary operations XOR and AND in the following way: $s_i(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I (\prod_{i \in I} x_i)$, where $\mathcal{P}(N)$ is the power set of $N = \{1, \dots, 6\}$ and $a_I \in \mathbb{F}_2$.

A label on the box said that the function S can be represented as a composition of three maps in the following way:

$$S = A \circ X \circ B,$$

where $A, B : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^6$ are **linear maps** and X is a function with a **short arithmetic expression modulo 64**. Nicole knows that a linear map over $\mathbb{F}_2^6$ can be defined by multiplication with a 6×6 matrix over $\mathbb{F}_2$. But she wonders what is supposed by “a short arithmetic expression modulo 64”? Probably, Nicole also should consider maps as classical modular operations such as addition, subtraction, multiplication modulo 64?..

Help Nicole to find the secret function X and the respective maps A, B !

