Problem 4. «Column functions»

Problem for a special prize!

Alice wants to construct a super strong symmetric cipher. On this way she solves some hard mathematical problems.

Consider 2^n pairwise distinct vectorial one-to-one functions, $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $i = 1, \ldots, 2^n$. Applying these functions we construct a special binary matrix and then try to determine some its properties.

For $n = 2^m$, $m \geqslant 5$, define a binary matrix M of size $2^n \times n2^n$ as follows. The i-th row, $i = 1, \ldots, 2^n$, is a concatenation of values $G_i(0, 0, \ldots, 0, 0)$, $G_i(0, 0, \ldots, 0, 1)$, $\ldots$, $G_i(1, 1, \ldots, 1, 1)$. The columns of the matrix M can be interpreted as vectors of values of $n2^n$ Boolean functions in n variables. We call them *column functions*.

Prove or disprove the following **conjecture** for at least one $m \geqslant 5$: for any matrix formed in the way described above there exist $2^{n/2}$ column functions $f_1, \ldots, f_{2^{n/2}}$ such that there is a nonzero Boolean function $f : \mathbb{F}_2^{2^{n/2}} \to \mathbb{F}_2$ satisfying the following conditions:

- for every $x \in \mathbb{F}_2^n$
$$f(f_1(x), f_2(x), \ldots, f_{2^{n/2}}(x)) = 0;$$
- for every $y \in \mathbb{F}_2^{2^{n/2}}$ the value $f(y)$ can be calculated using not more than $2^{n/2}$ addition and multiplication operations modulo 2.

Example. Let $m = 1$, then $n = 2$ and we construct matrix of size 4×8. Consider one-to-one vectorial Boolean functions G_1, G_2, G_3, G_4 from $\mathbb{F}_2^2$ to $\mathbb{F}_2^2$ defined by their vectors of values $(0, 1, 2, 3)$, $(0, 2, 1, 3)$, $(0, 3, 1, 2)$ and $(3, 2, 1, 0)$ respectively. Then the resulting matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

We need to find $2^{n/2} = 2$ column functions. Let f_1 and f_2 be defined as the first and the second columns of the matrix respectively, and $f(x_1, x_2) = x_1 \oplus x_2$ with the addition modulo 2. Then, $f(f_1(x), f_2(x)) \equiv 0$ since $f_1(x) = f_2(x)$ for any $x \in \mathbb{F}_2^n$.

Also, let f_1 and f_2 be the fifth and the sixth columns of the matrix. Then, giving $f(x_1, x_2) = x_1 x_2$ with the multiplication modulo 2, we obtain $f(f_1(x), f_2(x)) \equiv 0$ since $f_1(x) \neq f_2(x)$ for any $x \in \mathbb{F}_2^n$.

In the both cases the functions f can be calculated using only one operation. Note that the existence of such f implies that f_1 and f_2 are *algebraically dependent*.