Problem 4. Column functions

Dung Le Quoc

October 22, 2023

1 Problem

Consider 2^n pairwise distinct vectorial one-to-one functions, $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $i = 1, 2, \ldots, 2^n$.

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, $i = 1, 2, \ldots, 2^n$, is a concatenation of values $G_i(0, 0, \ldots, 0, 0)$, $G_i(0, 0, \ldots, 0, 1)$, ..., $G_i(1, 1, \ldots, 1, 0)$, $G_i(1, 1, \ldots, 1, 1)$. 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 describe above there exist $2^{n/2}$ column funcions $f_1, f_2, \ldots, f_{2^{n/2}}$ 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 vector $\boldsymbol{x} \in \mathbb{F}_2^n$
$$f(f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \ldots, f_{2^{n/2}}(x)) = 0$$
- for every vector $\boldsymbol{y} \in \mathbb{F}_2^{2^{n/2}}$, the value $f(\boldsymbol{y})$ can be calculated using not more than $2^{n/2}$ addition and multiplication operations modulo 2.

2 Solution

I will prove that if exist 2^n pairwise distinct vectorial one-to-one functions $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $i = 1, 2, \ldots, 2^n$, then there also exist another 2^n functions $G_i' : \mathbb{F}_2^n \to \mathbb{F}_2^n$, which are genereted from G_i, and satisfy two conditions.

My purpose for this proof is that, from initial 2^n vectorial functions satisfying two conditions, then I can generate all combination of 2^n vectorial functions (among $(2^n)!$ one-to-one vectorial functions) that also satisfy two conditions.

Remark 1

For all $n = 2^n$, $m \geqslant 5$, there always exist 2^n vectorial one-to-one functions $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $i = 1, 2, \ldots, 2^n$, that satisfy two conditions.

Proof. We consider bijection

$$\begin{aligned}
G_1 &= (0, 1, 2, \ldots, 2^n - 2, 2^n - 1),\\
G_2 &= (1, 2, 3, \ldots, 2^n - 1, 0),\\
G_3 &= (2, 3, 4, \ldots, 0, 1),\\
\cdots &= \cdots,\\
G_{2^n-1} &= (2^n - 2, 2^n - 1, 0, \ldots, 2^n - 4, 2^n - 3),\\
G_{2^n} &= (2^n - 1, 0, 1, \ldots, 2^n - 3, 2^n - 2)
\end{aligned}$$

Here, $G_i(j)$ represent value of $G_i(\boldsymbol{x})$, where $\boldsymbol{x}$ is vector corresponding to number j. For example, $G_3(0, \ldots, 1, 0) = G_3(2) = 4$.

Now we consider matrix M. I number the columns from $1, 2, 3, \ldots, n2^n$.

1-st column is first bit of numbers $0, 1, 2, \ldots, 2^n - 2, 2^n - 1$. In other word

$$\underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}}, \underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}}$$

2-nd column is the second bit of numbers $0, 1, 2, \ldots, 2^n - 2, 2^n - 1$. In other word

$$\underbrace{0, \ldots, 0}_{2^{n-2}}, \underbrace{1, \ldots, 1}_{2^{n-2}}, \underbrace{0, \ldots, 0}_{2^{n-2}}, \underbrace{1, \ldots, 1}_{2^{n-2}}$$

Similarly, n-th column is the n-th bit of numbers $0, 1, 2, \ldots, 2^n - 2, 2^n - 1$. In other word

$$0, 1, 0, 1, \ldots, 0, 1, 0, 1$$

Now we consider following columns.
$(1 + 2^{n-1} \cdot n)$-th column is the first bit of numbers $2^{n-1}, 2^{n-1} + 1, \ldots, 2^n - 1, 0, 1, \ldots, 2^{n-1} - 1$. In other word

$$\underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}}, \underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}}$$

$(2 + 2^{n-1} \cdot n)$-th column is the second bit of numbers $2^{n-1}, 2^{n-1} + 1, \ldots, 2^n - 1, 0, 1, \ldots, 2^{n-1} - 1$. In other word

$$\underbrace{0, \ldots, 0}_{2^{n-2}}, \underbrace{1, \ldots, 1}_{2^{n-2}}, \underbrace{0, \ldots, 0}_{2^{n-2}}, \underbrace{1, \ldots, 1}_{2^{n-2}}$$

Similarly, $(n + 2^{n-1} \cdot n)$-th column is the n-th bit of numbers $2^{n-1}, 2^{n-1} + 1, \ldots, 2^n - 1, 0, 1, \ldots, 2^{n-1} - 1$. In other word

$$0, 1, 0, 1, \ldots, 0, 1, 0, 1$$

Now we already have $2n$ column functions. We need $2^{n/2} - 2n$ more functions. Notice that $n = 2^m$, then $2^{n/2} = 2^{2^{m-1}}$, so the number $2^{n/2} - 2n$ is even. Next we will consider pair of column functions.
$(1 + n)$-th column is first bit of numbers $1, 2, 3, \ldots, 2^{n-1}, 0$. In other word

$$\underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}-1}, \underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}}, 0$$

and its corresponding column function is $(1 + (2^{n-1} + 1) \cdot n)$-th column.
$(1 + (2^{n-1} + 1) \cdot n)$-th column is the first bit of numbers $2^{n-1} + 1, 2^{n-1} + 2, \ldots, 2^n - 1, 0, 1, \ldots, 2^{n-1}$. In other word

$$\underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}-1}, \underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}}, 1$$

The reason why I choose this (and following) pair of column functions is to help us prove some property behind.
$(1 + 2n)$-th column is first bit of numbers $2, 3, 4, \ldots, 2^{n-1}, 0, 1$. In other word

$$\underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}-2}, \underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}}, 0, 0$$

and its corresponding column function is $(1 + (2^{n-1} + 2)\cdot)$-th column.
$(1 + (2^{n-1} + 2) \cdot n)$-th column is the first bit of numbers $2^{n-1} + 2, 2^{n-1} + 3, \ldots, 0, 1, \ldots, 2^{n-1}, 2^{n-1} + 1$. In other word

$$\underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}-2}, \underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}}, 1, 1$$

Let $t = \dfrac{2^{n/2} - 2n}{2} = \dfrac{2^{n/2}}{2} - n$. Then we do this until get $(1 + tn)$-th column and $1 + (2^{n-1} + t) \cdot n$-th column is the last pair.

Now, let f_i be

- f_1 is the 1-st column

$$f_1 = (\underbrace{0, 0, \ldots, 0, 0}_{2^{n-1}}, \underbrace{1, 1, \ldots, 1, 1}_{2^{n-1}})$$

- f_2 is the $(1 + 2^{n-1} \cdot n)$-th column

$$f_2 = (\underbrace{0, \ldots, 0}_{2^{n-2}}, \underbrace{1, \ldots, 1}_{2^{n-2}}, \underbrace{0, \ldots, 0}_{2^{n-2}}, \underbrace{1, \ldots, 1}_{2^{n-2}})$$

- for $i = 2, 3, 4, \ldots, n$, f_{2i-1} is the i-th column and f_{2i} is the $(i + 2^{n-1} \cdot n)$-th column

$$f_{2i-1} = f_{2i} = (\underbrace{0, \ldots, 0}_{2^{n-i}}, \underbrace{1, \ldots, 1}_{2^{n-i}}, \ldots, \underbrace{0, \ldots, 0}_{2^{n-i}}, \underbrace{1, \ldots, 1}_{2^{n-i}})$$

- for $i = n + 1, \ldots, t$ we pair column functions as above

Now we have $2^{n/2}$ column functions. Let $f(f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \ldots, f_{2^{n/2}}(\boldsymbol{x})) = f(x_1, x_2, \ldots, x_{2^{n/2}}) = x_1 \cdot x_2 \cdots x_{2^{n/2}}$.

We can see that, by the choice of f_1 and f_2, the product is always zero. Therefore value of f will always be zero, too. And there are $2^{n/2}$ operators, so we need $2^{n/2} - 1$ multiplication modulo 2. □

Next, I will prove a property that allow us to find another tuple of vectorial one-to-one functions.

In general, we consider $G_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Let $GL(n, 2)$ is the general linear group. Recall that general linear group is group of invertible matrices size $n \times n$, whose elements is in $\{0, 1\}$. For any n, this group contains $(2^n - 1) \cdot (2^n - 2) \cdots (2^n - 2^{n-1})$ elements.

Now let $\boldsymbol{x}_0 = G_1(0, 0, \ldots, 0, 0)$, $\boldsymbol{x}_1 = G_1(0, 0, \ldots, 0, 1)$, ..., $\boldsymbol{x}_{2^n-2} = G_1(1, 1, \ldots, 1, 0)$, $\boldsymbol{x}_{2^n-1} = G_1(1, 1, \ldots, 1, 1)$. We consider map

$$G_1' : \mathbb{F}_2^n \to \mathbb{F}_2^n, \quad \boldsymbol{x} \to \boldsymbol{x} \cdot A \oplus \boldsymbol{b} \tag{1}$$

where A is an element in $GL(n, 2)$ and $\boldsymbol{b}$ is vector in $\mathbb{F}_2^n$. This map is an affine map, so it is a permutation, or in other word, one-to-one vectorial Boolean function.

We see that $(\boldsymbol{x}_0 \cdot A \oplus \boldsymbol{b}) \oplus (\boldsymbol{x}_{2^{n-1}} \cdot A \oplus \boldsymbol{b}) = (\boldsymbol{x}_0 \oplus \boldsymbol{x}_{2^{n-1}}) \cdot A$. Because A is an invertible matrix, so product $(\boldsymbol{x}_0 \oplus \boldsymbol{x}_{2^{n-1}}) \cdot A = \boldsymbol{0}$ can happend if and only if $\boldsymbol{x}_0 \equiv \boldsymbol{x}_{2^{n-1}}$. Therefore $\boldsymbol{x}_0 \neq \boldsymbol{x}_{2^{n-1}}$.

Suppose that $\boldsymbol{x}_0$ is different from $\boldsymbol{x}_{2^{n-1}}$ at position i, $1 \leqslant i \leqslant n$. So from the choice of first n column functions as above and their corresponding n column functions from $(1 + 2^{n-1} \cdot n)$-th to $(n + 2^{n-1} \cdot n)$-th columns, because the i-th is different so product $x_{2i-1} \cdot x_{2i} = 0$. This means that, same as above, product of function f is always 0 and we need $2^{n/2} - 1$ multiplication modulo 2.

There are $(2^n - 1) \cdot (2^n - 2) \cdots (2^n - 2^{n-1})$ cases of matrix A, and 2^n cases of vector $\boldsymbol{b}$, in order to form affine map. So in total we can change G_1 to G_1' with

$$2^n \cdot (2^n - 1) \cdot (2^n - 2) \cdots (2^n - 2^{n-1})$$

different ways, and they all satisfy two conditions.

We also need to notice that

1. affine map G_1 to G_1' must not be same with any other $G_2, \ldots, G_{2^n}$, which means $G_1' \neq G_i$, $i = 2, 3, \ldots, 2^n$.
2. we can apply this property for G_2, G_3, ..., G_{2^n}. As mentioned above, G_i' must be different from G_j, where $i \neq j$.

Remark 2

If G_1, G_2, ..., G_{2^n} are vectorial one-to-one Boolean functions that satisfy two above conditions, then with any matrix A in $GL(n, 2)$ and any vector $\boldsymbol{b} \in \mathbb{F}_2^n$, the map

$$G_1' : \mathbb{F}_2^n \to \mathbb{F}_2^n, \quad G_1(\boldsymbol{x}) \to G_1(\boldsymbol{x}) \cdot A \oplus \boldsymbol{b}, \, \boldsymbol{x} \in \mathbb{F}_2^n$$

will also satisfy two conditions.

This means that G_1', G_2, ..., G_{2^n} are vectorial one-to-one Boolean functions that also satisfy two above conditions.