Problem 1. «Algebraic immunity»

Special Prize from the Program Committee!

A mapping F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called a *vectorial Boolean function* (recall that $\mathbb{F}_2^n$ is the vector space of all binary vectors of length n). If $m = 1$ then F is a *Boolean function* in n variables. A *component function* F_v of F is a Boolean function defined by a vector $v \in \mathbb{F}_2^m$ as follows $F_v = \langle v, F\rangle = v_1 f_1 \oplus \ldots \oplus v_m f_m$, where $f_1, \ldots, f_m$ are coordinate functions of F. A function F has its unique *algebraic normal form* (ANF)

$$F(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I \Big(\prod_{i \in I} x_i\Big),$$

where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$ and a_I belongs to $\mathbb{F}_2^m$. Here $\oplus$ denotes the coordinate-wise sum of vectors modulo 2. The *algebraic degree* of F is the degree of its ANF: $\deg(F) = \max\{|I| : \ a_I \neq (0, \ldots, 0),\ I \in \mathcal{P}(N)\}$.

Algebraic immunity $AI(f)$ of a Boolean function f is the minimal algebraic degree of a Boolean function g, $g \not\equiv 0$, such that $fg \equiv 0$ or $(f \oplus 1)g \equiv 0$. The notion was introduced by W. Meier, E. Pasalic, C. Carlet in 2004.

The tight upper bound of $AI(f)$. It is wellknown that $AI(f) \leqslant \lceil \frac{n}{2} \rceil$, where $\lceil x \rceil$ is the ceiling function of number x. There exist functions with $AI(f) = \lceil \frac{n}{2} \rceil$ for any n.

Component algebraic immunity $AI_{comp}(F)$ of a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is defined as the minimal algebraic immunity of its component functions F_v, $v \neq (0, \ldots, 0)$. Component algebraic immunity was considered by C. Carlet in 2009. It is easy to see that $AI_{comp}(F)$ is also upper bounded by $\lceil \frac{n}{2} \rceil$.

The problem. What is the tight upper bound of component algebraic immunity? For all possible combination of n and m, $n, m \leqslant 4$, vectorial Boolean functions with $AI_{comp}(F) = \lceil \frac{n}{2} \rceil$ exist.

Construct $F : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ with maximum possible algebraic component immunity 3 or prove that it does not exist.