Problem 5. «One more parameter»

There are several parameters in cryptanalysis of block ciphers that are used to measure the diffusion strength. In this problem, we study properties of one of them.

Let n, m be positive integers. Let $a = (a_1, \ldots, a_m)$ be a vector with coordinates a_i taken from the finite field $\mathbb{F}_2$. Denote the number of nonzero coordinates a_i, $i = 1, \ldots, m$, by $\mathrm{wt}(a)$ and call this number the **weight** of the vector a.

The inner product of $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$ in $\mathbb{F}_2^m$ is defined as

$$a \cdot b = a_1 b_1 \oplus \ldots \oplus a_m b_m.$$

For a Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$, we define the function *weight* wt as follows:

$$\mathrm{wt}(f) = \#\{a \in \mathbb{F}_2^m \mid f(a) = 1\}$$

The **special parameter** Q of a vectorial Boolean function $\varphi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is defined to be

$$Q(\varphi) = \min_{a,\, b,\, b \neq 0,\, \mathrm{wt}(a \cdot x \oplus b \cdot \varphi(x)) \neq 2^{m-1}} \{\mathrm{wt}(a) + \mathrm{wt}(b)\}.$$

- Rewrite (simplify) the definition of $Q(\varphi)$ when the function φ is linear (recall that a function ℓ is linear if $\ell(x \oplus y) = \ell(x) \oplus \ell(y)$ for any x, y).
- Rewrite the definition of $Q(\varphi)$ in terms of linear codes, when the linear function φ is given by an $m \times m$ matrix M over $\mathbb{F}_2$, i. e. $\varphi(x) = Mx$.
- Find the tight upper bound for $Q(\varphi)$ as a function of m.
- Can you give an example of the function φ with the maximal possible value of Q?