Problem 9. «Masking»

It is known that there are attacks on cryptosystems that use information obtained from the physical implementation of a cryptosystem, for example, timing information, power consumption, electromagnetic leaks or even sound. To protect cryptosystems from such attacks cryptographers can use a countermeasure known as **masking**.

Correlation immune Boolean functions can reduce the masking cost. Therefore, we need to search for Boolean functions satisfying the following conditions: they should have **small Hamming weight** and **high correlation immunity**.

Let f be a non-constant Boolean function in 12 variables of correlation immunity 6.

- What is the lowest possible Hamming weight k of f?
- Give an example of such a function f with Hamming weight k.

Remark I. Hamming weight $\mathrm{wt}(f)$ of a Boolean function f in n variables is the number of vectors $x \in \mathbb{F}_2^n$ such that $f(x) = 1$.

Remark II. A Boolean function f in n variables is called *correlation immune of order* t, where t is an integer such that $1 \leqslant t \leqslant n$, if

$$\mathrm{wt}(f_{i_1,\ldots,i_t}^{a_1,\ldots,a_t}) = \mathrm{wt}(f)/2^t$$

for any set of indexes $1 \leqslant i_1 < \ldots < i_t \leqslant n$ and any set of values $a_1, \ldots, a_t \in \mathbb{F}_2$. Here $f_{i_1,\ldots,i_t}^{a_1,\ldots,a_t}$ denote the subfunction of f in $n - t$ variables that is obtained from $f(x_1, \ldots, x_n)$ by fixing each variable x_{i_k} by the value a_k, $1 \leqslant k \leqslant t$.