Problem 5. «Super dependent S-box»

Harry wants to find a super dependent S-box for his new cipher. He decided to use a permutation that is strictly connected with every of its variables. He tries to estimate the number of such permutations.

A vectorial Boolean function $F(x) = (f_1(x), f_2(x), \dots, f_n(x))$, where $x \in \mathbb{F}_2^n$, is a *permutation* on $\mathbb{F}_2^n$ if it is a one-to-one mapping on the set $\mathbb{F}_2^n$. Its coordinate function $f_k(x)$ (that is a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$), *essentially depends* on the variable x_j if there exist values $b_1, b_2, \dots, b_{j-1}, b_{j+1}, \dots, b_n \in \mathbb{F}_2$ such that

$$f_k(b_1, b_2, \dots, b_{j-1}, 0, b_{j+1}, \dots, b_n) \neq f_k(b_1, b_2, \dots, b_{j-1}, 1, b_{j+1}, \dots, b_n).$$

In other words, the essential dependence on the variable x_j of a function f means the presence of x_j in the algebraic normal form of f (the unique representation of a function in the basis of binary operations AND, XOR, and constants 0 and 1).

An example. Let $n = 3$. Then the Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3$ essentially depends on all its variables; but $g(x_1, x_2, x_3) = x_1x_2 \oplus x_2 \oplus 1$ essentially depends only on x_1 and x_2.

The problem. Find the number of permutations on $\mathbb{F}_2^n$ such that all their coordinate functions essentially depend on all n variables, namely

Q1 Solve the problem for $n = 2, 3$.

Q2 **Problem for a special prize!** Solve the problem for arbitrary n.