Problem 10. «Close to permutations»

Bob wants to use a new function inside the round transformation of a cipher. He chooses a family $\mathcal{F}$ of functions F_α from $\mathbb{F}_2^n$ to itself of the form

$$F_\alpha(x) = x \oplus (x \boxplus \alpha), \text{ where}$$

- $x, \alpha \in \mathbb{F}_2^n$,
- $\oplus$ denotes the bit-wise XOR of binary vectors,
- $\boxplus$ denotes the addition modulo 2^n of integers whose binary representations are the given vectors.

Bob noted that functions from $\mathcal{F}$ are not bijective. So, he introduced a parameter that measures in some sense the closeness of a function to a permutation. For a given function F from $\mathbb{F}_2^n$ to itself, the parameter is

$$C(F) = \#\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \ : \ F(x) = F(y)\}.$$

The **smaller** the parameter value, the **better** the function. Bob wants to choose «**the best functions**» by this parameter among $\mathcal{F}$. Help Bob to find answers to the questions below!

Q1 How many «the best functions» exist in $\mathcal{F}$?

Q2 What α correspond to «the best functions» from $\mathcal{F}$?

Q3 What is $C(F_\alpha)$ for «the best functions» from $\mathcal{F}$?