Problem 2. «Let's find permutations!»

A function F from $\mathbb{F}_{2^n}$ to itself is called **APN** (**almost perfect nonlinear**) if for any $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ the equation $F(x) + F(a + x) = b$ has at most 2 solutions. APN functions possess an optimum resistance to differential cryptanalysis and are under the extreme interest in cryptography! For example, when the unique 1-to-1 APN function in 6 variables was found in 2009, it was immediately applied in construction of the known lightweight cipher FIDES.

Let $F(x) = x^d$. It is known that F is APN for the following exponents d:

- $d = 2^{2i} - 2^i + 1$, $\gcd(i, n) = 1$, $i \geqslant 2$;
- $d = 2^t + 3$, $n = 2t + 1$;
- $d = 2^t + 2^{t/2} - 1$ for t even and $d = 2^t + 2^{(3t+1)/2} - 1$ for t odd with $n = 2t + 1$;
- $d = 2^{2t} - 1$, $n = 2t + 1$;
- $d = 2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$ with $n = 5i$.

Q1 Problem for a special prize! Describe (characterize or make a list of) all linear functions L_1 and L_2 for any one exponent above for $n = 7$ or $n = 8$, such that the function $L_1(x) + L_2(F(x))$ is a permutation.

Q2 Problem for a special prize! Consider any of the exponents d above. Find linear functions L_1 and L_2 (both different from 0 function) such that the function $L_1(x) + L_2(F(x))$ is a permutation ($n \geqslant 9$), or prove that such functions do not exist.

Remark. Let us recall the following definitions:

- $\mathbb{F}_{2^n}$ is the finite field of order 2^n;
- a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has the unique representation $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$, $c_i \in \mathbb{F}_{2^n}$;
- the algebraic degree of F is equal to the maximum binary weight of i such that $c_i \neq 0$;
- a linear function L has degree at most 1 and $L(0) = 0$ (that is $L(x) = \sum_{k=1}^{n} c_k x^{2^k}$).