Problem 9. «Metrical cryptosystem – 2»

Let $\mathbb{F}_2^n$ be an n-dimensional vector space over the field $\mathbb{F}_2 = \{0, 1\}$. Alice and Bob exchange messages using the following cryptosystem.

- First, they use a supercomputer to calculate two special large secret sets $A, B \subseteq \mathbb{F}_2^n$ which have the following property: there exists a constant ℓ ($\ell \geqslant 26$), such that for any $x \in \mathbb{F}_2^n$ it holds
$$d(x, A) + d(x, B) = \ell,$$
where $d(x, A)$ denotes Hamming distance from the vector x to the set A.

- Alice then saves the number ℓ, the set A and a set of vectors $a_1, a_2, \ldots, a_r$ such that for any $k : 0 \leqslant k \leqslant \ell$, there is a vector a_i at distance k from A. Similarly, Bob saves the number ℓ, the set B and a set of vectors $b_1, b_2, \ldots, b_s$ such that for any $k : 0 \leqslant k \leqslant \ell$, there is a vector b_i at distance k from B.

- Text messages are encrypted letter by letter. In order to encrypt a letter Alice replaces it with its number in the alphabet, say k. Then she chooses some vector a_i at distance k from the set A and sends this vector over to Bob. Bob then calculates the distance $d(a_i, B)$ and using the property of the sets A, B, calculates $k = \ell - d(a_i, B)$. So, he gets the letter Alice sent. If Bob wants to send an encrypted message to Alice, he does the same but using his saved vectors and the set B.

Eve was able to hack the supercomputer when it was calculating the sets A and B. She extracted the set C from its memory, which consists of all vectors of $\mathbb{F}_2^n$ that are at distance 1 or less from either A or B. She also learned that ℓ is even.

Help Eve to crack the presented cryptosystem (to decrypt any short intercepted message)! You know that she has an (illegal) access to the supercomputer, which can calculate and output the list of distances from all vectors of $\mathbb{F}_2^n$ to any input set D in reasonable (but not negligible) time.

Remark I. Recall several definitions and notions. The *Hamming distance* $d(x, y)$ between vectors x and y is the number of coordinates in which these vectors differ. Distance from vector $y \in \mathbb{F}_2^n$ to the set $X \subseteq \mathbb{F}_2^n$ is defined as $d(y, X) = \min_{x \in X} d(y, x)$.