Problem 5. «Metrical cryptosystem»

Alice and Bob exchange messages using the following cryptosystem. Let $\mathbb{F}_2^n$ be an n-dimensional vector space over the field $\mathbb{F}_2 = \{0, 1\}$. Alice has a set $A \subseteq \mathbb{F}_2^n$ and Bob has a set $B \subseteq \mathbb{F}_2^n$ such that both A and B are metrically regular sets and they are metrical complements of each other. Let d be the Hamming distance between A and B. To send some number a $(0 \leqslant a \leqslant d)$ Alice chooses some vector $x \in \mathbb{F}_2^n$ at distance a from the set A and sends this vector to Bob. To obtain the number that Alice has sent Bob calculates the distance b from x to the set B and concludes that the initial number a is equal to $d - b$.

Is this cryptosystem correct? In other words, does Bob correctly decrypt all sent messages, regardless of initial sets A, B satisfying given conditions and of the choice of vector x?

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 $d(y, X) = \min_{x \in X} d(y, x)$. The *metrical complement* of a set $X \subseteq \mathbb{F}_2^n$ (denoted by $\widehat{X}$) is the set of all vectors $y \in \mathbb{F}_2^n$ at maximum possible distance from X (this maximum distance is also known as *covering radius* of a set). A set $X \subseteq \mathbb{F}_2^n$ is called *metrically regular*, if its second metrical complement $\widehat{\widehat{X}}$ coincides with X.

Remark II. Let us consider several examples:

- Let X consist of a single vector $x \in \mathbb{F}_2^n$. It is easy to see that $\widehat{X} = \{x \oplus \mathbf{1}\}$, where $\mathbf{1}$ is the all-ones vector, and therefore $\widehat{\widehat{X}} = \{x \oplus \mathbf{1} \oplus \mathbf{1}\} = \{x\} = X$, so X is a metrically regular set; it is also easy to see that cryptosystem based on $A = \{x\}$, $B = \{x \oplus \mathbf{1}\}$ is correct;
- Let Y be a ball of radius $r > 0$ centered at x: $Y = B(r, x) = \{y \in \mathbb{F}_2^n : d(x, y) \leqslant r\}$. You can verify that $\widehat{Y} = \{x \oplus \mathbf{1}\}$, but $\widehat{\widehat{Y}} = \{x\} \neq Y$, and Y is not metrically regular;
- Let X be an arbitrary subset of $\mathbb{F}_2^n$. Then, if we denote $X_0 := X$, $X_{k+1} = \widehat{X_k}$ for $k \geqslant 0$, there exists a number M such that X_m is a metrically regular set for all $m > M$. You can prove this fact as a small exercise, or simply use it in your solution.