Problem 9. «Covering radius — 2»

In order to protect a new block cipher against some attack based on S-box approximations Alice needs to solve the following problem.

Let $\mathbb{F}_2^n$ be a n-dimensional vector space over the field $\mathbb{F}_2 = \{0, 1\}$. Let $n = 2k$, where k is a positive integer. Evaluate the covering radius and describe the metrical complement of the linear subspace spanned by rows of the following $k \times n$ matrix:

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \dots\dots\dots & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \dots\dots\dots & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \dots\dots\dots & 0 \\ & & & & & & \ddots & \ddots & \ddots & \\ 0 & \dots\dots\dots & & & & & & 0 & 1 \quad 1 \quad 1 & 0 \\ 1 & 0 & \dots\dots\dots & & & & & 0 & 0 \quad 0 \quad 1 & 1 \end{pmatrix}$$

Remark I. Recall several definitions and notions. A set $L \subseteq \mathbb{F}_2^n$ is called a *linear subspace* if for every $x, y \in L$ the sum $x \oplus y$ is also in L. The *Hamming distance* $d(x, y)$ between vectors $x, y \in \mathbb{F}_2^n$ is defined as the number of positions where they differ, i. e. $d(x, y) = |\{i \mid x_i \neq y_i\}|$. The Hamming distance from a vector y to a subset $X \subseteq \mathbb{F}_2^n$ is defined as $d(y, X) = \min_{x \in X} d(y, x)$. Since the distance between any two vectors is bounded by n, for an arbitrary subset X there exists the number $d(X)$ such that:

- for every $y \in \mathbb{F}_2^n$ it holds $d(y, X) \leqslant d(X)$;
- there exists a vector $z \in \mathbb{F}_2^n$ with $d(z, X) = d(X)$.

This number is called the *covering radius* of X. Set $\widehat{X} = \{z \in \mathbb{F}_2^n \mid d(z, X) = d(X)\}$ is called the *metrical complement* of 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 $d(X) = n$ and $\widehat{X} = \{x \oplus \mathbf{1}\}$, where $\mathbf{1}$ is the all-ones vector;
- Let Y be a ball of radius r centered at x: $Y = \{y \in \mathbb{F}_2^n \mid d(x, y) \leqslant r\}$. One can verify that $d(Y) = n - r$ and $\widehat{Y} = \{x \oplus \mathbf{1}\}$.