Problem 7. «A unique decoding»

Problem for a special prize!

Consider a binary error-correcting code C of length n. Recall that it is just a subset of $\mathbb{F}_2^n$ and we transmit only elements of C over a noisy communication channel. Sending $x \in C$, some bits of x can be inverted in the channel. Getting $y \in \mathbb{F}_2^n$, a receiver decodes it into the nearest by Hamming metrics element of C. The Hamming weight $wt(x \oplus y)$ of $x \oplus y$ which is equal to the number of ones in $x \oplus y$ is the exact number of errors. Here $\oplus$ states for XORing. Error-correcting codes are of great interest in communication theory and post-quantum cryptography.

Consider the principle of the maximum-likelihood decoding. Obtaining some $y \in \mathbb{F}_2^n$, we suppose that the number of errors happened, say d_y, is minimal possible, i.e.

$$d_y = \min_{x \in C} wt(x \oplus y).$$

Next, let $\mathcal{D}(y) = \{x \in C : wt(x \oplus y) = d_y\}$. Finally, we decode y into any $x \in \mathcal{D}(y)$.

We are interested in all cases of codes for which $|\mathcal{D}(y)| = 1$ for all $y \in \mathbb{F}_2^n$. In other words for such code every binary vector $y \in \mathbb{F}_2^n$ can be decoded in the unique way.

Q1 What codes C can provide this property?

Q2 What codes C that are linear subspaces of $\mathbb{F}_2^n$ can provide this property?

Remarks.

1) An example. There are so-called perfect codes C that allow to divide $\mathbb{F}_2^n$ into non-intersecting balls $B_r(x) = \{y \in \mathbb{F}_2^n : wt(x \oplus y) \leqslant r\}$ of some radius r centered in all $x \in C$. In other words, C is *perfect* if for some r it holds

$$\bigcup_{x \in C} B_r(x) = \mathbb{F}_2^n \text{ and } B_r(x) \cap B_r(x') = \emptyset \text{ for } x \neq x', \text{ where } x, x' \in C.$$

It is not difficult to see that any such code provides $|\mathcal{D}(y)| = 1$ for all $y \in \mathbb{F}_2^n$. But what else?

2) Some notions related to *Voronoi diagrams* can be helpful, see general mathematical definitions at `https://en.wikipedia.org/wiki/Voronoi_diagram`. In our problem we are looking for codes with non-intersecting discrete Voronoi cells for all $x \in C$.