Definition: Linear Code

In this section, we study a class of error-correcting codes called linear codes. This type of code has a nice structure and can be encoded/decoded efficiently.

Definition: Linear code

A code C is linear if any linear combination of codewords is also a codeword.

For the definition of linearity to make sense, addition and multiplication by constants needs to be defined on $\mathcal{X}^n$ (formally, $\mathcal{X}^n$ needs to be a **vector space**). Then C is linear if it is a **linear subspace** of $\mathcal{X}^n$. In the following, we will assume that $\mathcal{X} = \{0, 1\}$: in that case, we are talking about **binary codes** and addition is simply bitwise addition modulo 2 (which is the exclusive OR function). Note that for binary codes, addition and subtraction are the same operation, as $-1 = +1$ modulo 2.