Problems

Problem 1

• How many information sets has [7,4] Hamming code?
• How many information sets has [8,4] extended Hamming code?
• Estimate complexity of information set decoding for the above two codes

Problem 2

• Find a primitive element of GF(7)
• Find multiplicative orders of all elements of GF(7)
• Find the order of the multiplicative group of GF(7)
• Show that for GF(7) multiplicative orders are divisors of the multiplicative order of the group.
• Prove that for any element $a \in GF(q)$, $q$ is prime the following equality holds:

$$a^{q-1} = 1$$

Problem 3

• Construct extension field GF($2^5$) by using primitive polynomial $x^5 + x^2 + 1$ (express each element of the field as a power of primitive element)
• Write the MATLAB program for constructing extension field, summation, multiplication, and finding the inverse element for each element of the extension field

Problem 4

• Draw a scheme generating the maximal length sequence with the polynomial $x^5 + x^2 + 1$ or equivalently a scheme of the encoder of [31,5]-code
• Starting with the initial state 00001, show that 31 sequential states of the generator (encoder) are different

Problem 5.
• Construct cyclic codes of lengths $n = 3 \ldots 7$. Compute code rate and minimum distance of the constructed codes and their duals

• Let $g(x)$ be a generator polynomial of a cyclic code. Denote by $r(x)$ a noisy codeword and by $s(x)$ the corresponding syndrome. Prove that cyclic shifts of $s(x)$ are syndromes of the corresponding cyclic shifts of $r(x)$. How this observation can be used for simplifying the syndrome decoding?