

S-72.341 Coding Methods

1. (6p.) Dual spaces.
- (a) Find a basis for the dual space to the vector space over $\text{GF}(2)$ spanned by $\{11100, 01110, 00111\}$.
 - (b) Find a basis for the dual space to the vector space over $\text{GF}(5)$ spanned by $\{12322, 14312, 41233\}$.
2. (4p.) Define maximum a posteriori (MAP) decoding and maximum likelihood (ML) decoding. When are these two decoders identical?
3. (5p.) Show that the binary code C of all *palindromes* of length n , that is, words that are the same read forwards or backwards, is linear. Describe the codewords (x_1, x_2, \dots, x_n) using equations, give a parity check matrix for C , and determine the number of errors it detects.
4. (6p.) Let $a = x^2 + x + 2$ and $b = x + 1$. Carry out the following calculations in the ring $\text{GF}(3)[x]/(x^3 - 1)$.
- (a) $a + b$,
 - (b) $a \cdot b$,
 - (c) Let $c = x + 2$ and now consider the ring $\text{GF}(3)[x]/(x^2 - 1)$. Calculate \sqrt{c} , that is, find the values of y that satisfy $y^2 = c$.
5. (6p.) Connect the following types of codes with the correct statements: BCH codes, convolutional codes, CRC codes, Hamming codes, Reed-Muller codes, Reed-Solomon codes (choose only one statement for each code type).
- (a) These have simple encoder and decoder implementations and are therefore perhaps the most frequently used error-detecting codes. CRC
 - (b) There are *narrow-sense* and *primitive* such codes. BCH
 - (c) These are codes of length $n = q - 1$ over $\text{GF}(q)$. Reed-Solomon
 - (d) There are such codes with unwanted properties which are said to be *catastrophic*. Convolutional
 - (e) These are perfect one-error-correcting codes. Hamming
 - (f) These are conveniently defined through Boolean functions. Reed-Muller
6. (3p.) Briefly describe the three basic retransmission protocols: stop-and-wait, go-back- N , and selective repeat.