Exercise 2 - Reed-Muller Codes and HQC

Reed-Muller Codes

Q1. Given a Boolean function $f(x_0, x_1, x_2, x_3) = x_1 + x_3 + x_1x_2 + x_0x_1x_2 + x_1x_2x_3$, give the true table of f

Q2. Prove that the binary RM(r, m) code has minimum distance 2^{m-r}. Essentially, prove that all m-variate Boolean functions with algebraic degree smaller than m has even weight of its truth table

Q3. If we extend a binary RM(r, m) code to a p-ary RM(r, m) code, where p is an odd prime. What can we say about the minimum distance of a p-ary RM(r, m) code?

Q4. For the $(u, u + v)$ construction of a code C, where u, v are codewords of two codes C_1, C_2 of same code length, respectively, prove that the code C has minimum distance

$$d(C) = \min\{2d(C_1), d(C_2)\}$$

Q5. Consider a binary RM$(1, 4)$ code.

- List its generate matrix G
- Encode a message $(0, 1, 1, 0, 1)$
- Use the majority strategy to decode a noisy word with 2 errors;
- Use the fast Walsh-Hadamard transform to complete the above decoding

HQC

Q1. Given an $[n, k, d]_q$ linear code C, prove that the shortened code C_1 derived from C on the last t coordinates, $t < k$, has the same minimum distance

Q2. Use SageMath or other programming language to implement a decoder of RSRM concatenated code with parameters $[n_i, k_i, d_i] = [128, 8, 64]$ and $[n_2, k_2, d_2] = [255, 224, 31]$.