Problem set 6. Due Thursday, April 5

Mathematics 342, Term 2, 2018. Instructor: Reichstein.

Questions 1-3 concern a general q-ary BCH code C defined by a parity check matrix of the form

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ \dots & \dots & \dots & \dots \\ a_1^{d-1} & a_2^{d-1} & \dots & a_n^{d-1} \end{pmatrix}.$$

Here $1 \leq d+1 \leq n \leq q$ and $a_1, \dots, a_n$ are distinct elements of F_q. We showed in class that $d(C) = d+1$.

Problem 1. Show that H can be row reduced to a matrix of the form $H' = (B \,|\, I_d)$, where B is a $d \times (n-d)$ matrix and I_d is the $d \times d$ identity matrix. Conclude that C has a generator matrix in standard form.

Hints: (i) See the discussion about standard forms for generator and parity check matrices on pp. 70-71 in the book. (ii) Use the fact that the last d columns of H form a $d \times d$ Vandermonde matrix and are therefore linearly independent. (iii) Note that the problem does not ask you to find B explicitly, just to show that it exists.

Problem 2. Show that if $d = n-1$, then C is equivalent to the q-ary repetition code of length n. Recall that the repetition code is a q-ary linear code with generator matrix $G = (1, 1, \dots, 1)$.

Problem 3. (a) How many binary BCH codes C are there? Find a generator matrix and the minimal distance for each C. (b) Same question for ternary codes.

Hints: "Binary" means that $q = 2$ and "ternary" means that $q = 3$. What are the possible choices of d, n and $a_1, \dots, a_n$ in each case?

Problem 4. Let $q > 2$ be a prime integer. Show that exactly half of the $q-1$ non-zero elements of F_q are squares, and the rest are non-squares. (For $q = 11$ the non-zero squares are 1, 3, 4, 5 and 9; see the table on p. 130.)

Problems 5–8 below concern the specific code in Example 11.3, with $q = 11$, $n = 10$, $d = 4$, and $a_1 = 1$, $a_2 = 2, \dots, a_{10} = 10$. In each problem use the decoding scheme in Example 11.3 to decode the received word $\mathbf{y} = (0, 0, 0, 8, 0, 0, 1, 7, 0, 0)$, if possible. Recall that decoding is possible if at most two errors occurred in transmission and impossible if three or more errors occurred.

Problem 5. $\mathbf{y} = (0, 0, 0, 8, 0, 0, 1, 7, 0, 0)$.

Problem 6. $\mathbf{y} = (1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$.

Problem 7. $\mathbf{y} = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$.

Problem 8. $\mathbf{y} = (2, 2, 2, 2, 0, 0, 0, 0, 0, 7)$.