Mathematics 392 – Seminar in Coding Theory
Discussion 5 – BCH Codes
April 12, 2002

Background

In class, we saw the construction of BCH codes with $n = 2^r - 1$, $k = 2^r - 2r - 1$, and $d = 5$ (so 2 errors in a received word can be corrected). Recall that the idea was:

- Let β be a primitive element of the field $\mathbf{F}_{2^r}$ (constructed using some particular irreducible polynomial of degree r).
- If the parity check matrix of a code is made up of columns

  $$(1, \beta^s, (\beta^s)^2, \ldots, (\beta^s)^{2^r-2})^{tr} \tag{1}$$

  ("tr" is the *transpose* to turn the row vector into a column – I wrote it this way for typographical reasons) for $s = 1, 2, 3, 4$, then every set of four rows is linearly independent (we proved this using properties of Vandermonde determinants).
- On the other hand, having the column (1) in the parity check matrix is equivalent to saying every codeword polynomial $c(x)$ has β^s as a root: $c(\beta^s) = 0$. And this is equivalent in turn to saying that the minimal polynomial, $m_{\beta^s}(x)$, of β^s divides $c(x)$.
- We also have that this is equivalent to saying β^ℓ is a root of $c(x) = 0$ for all ℓ in the cyclotomic coset C_s mod $n = 2^r - 1$.
- Hence if we make a cyclic code of length $n = 2^r - 1$ with generator polynomial $g(x) = m_\beta(x) m_{\beta^3}(x)$, then $\beta, \beta^2, \beta^3, \beta^4$ are roots of all the codeword polynomials, and we get from the above that $d \geq 5$.

In this discussion, you will consider how this construction can be generalized to yield BCH codes with "designed distance" as large as we like (provided $n = 2^r - 1$ is sufficiently large, of course). The actual minimum distance will be bigger than or equal to this designed distance.

Discussion Questions

A) Suppose we want $d \geq \delta = 2t + 1$ for a general t. To get that to be true, what columns of the form in (1) should appear in the parity check matrix? How do you know that rows of the corresponding parity check matrix satisfy the required linear independence conditions? (Hint: Think about the Vandermonde determinant argument we used in the case $\delta = 5$.)

B) Your columns in H from question A are equivalent to saying that every codeword polynomial has a particular set of elements of $\mathbf{F}_{2^r}$ as roots – which elements? Also: which minimal polynomials of field elements must divide every codeword polynomial?

C) Following these ideas, give a general "recipe" for making the generator polynomial of a cyclic code with $n = 2^r - 1$ and $d \geq \delta = 2t + 1$. Try to be as "economical" as

possible. For instance note that knowing β is a root of $c(x)$ implies that $\beta^2, \beta^4, \beta^8, \ldots$ are roots of $c(x)$ also (exponents from the cyclotomic coset of 1 mod $2^r - 1$). *Comment*

The codes you are constructing here are the $BCH(2^r, \delta)$ codes. The integer δ is called the *designed distance* of the BCH code. The actual minimum distance can be *strictly larger* if there is a longer string of consecutive powers of β that are roots of $g(x)$. This happens rather frequently because of the fact noted above that if β^t is a root of $g(x)$ then so are the β^ℓ for all ℓ in the cyclotomic coset of t mod $2^r - 1$. Next, you'll work out an example.

D) With $r = 5$, for instance, show that the actual minimum distance of $BCH(2^5, 7)$ satisfies $d \geq 11$. (That is we get a much larger minimum distance than we might expect!) (Hint: Don't work too hard: everything can be done by considering elements of cyclotomic cosets – you don't even need to write down what $g(x)$ is explicitly to see this!)

Assignment

Group writeups due Wednesday, April 17.