Math 75 notes, Lecture 20 outline

P. Pollack and C. Pomerance

References below are to Pretzel's *Error-correcting codes and finite fields*:

- We reviewed the definition of a polynomial code and the left-shift criterion for recognizing one.

- We reviewed the definiton of a cyclic code and showed that this could be defined alternatively as (1) a polynomial code of block length n with generator polynomial $g(x)$ that divides $x^n - 1$; (2) a linear code closed under all left shifts.

- We went over an example where we have a length 15 binary code of dimension 7, with real word $(a_6, \ldots, a_0)$ encoded as
$$(a_6, \ldots, a_0, 0, a_6, \ldots, a_0).$$
This is clearly a linear code. It is closed under left shift if the leading entry is 0, so it is a polynomial code. The generator polynomial corresponds to the nonzero code word that starts with the most 0's, so it is
$$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1),$$
which corresponds to $x^8 + 1 = x^8 - 1$. Since $x^8 - 1 \nmid x^{15} - 1$ we see the code is not cyclic. Alternatively, the left shift of code word
$$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0),$$
is seen not to be a code word. (See the example of code K on pp. 226–228.)

- We showed how to write down the generator matrix with standard encoding for the polynomial code of block length n and generator polynomial $g(x)$. Recall that standard encoding of a real word $(a_{m-1}, \ldots, a_0)$ is to identify this with the polynomial $a(x) = a_{m-1}x^{m-1} + \cdots + a_0$, and form the code word $g(x)a(x)$. (Here the relation of $n, m, d = \deg(g(x))$ is that $n = m + d$.) The generator matrix corresponding to this encoding is $n \times m$ where the jth column for $j = 1, \ldots, m$ is $j - 1$ 0's, followed by the column vector $g_d, \ldots, g_0$ (the coefficients of the polynomial $g(x)$), followed by $n - d - j$ 0's. (This may not be in the book.)

- There is another way to encode real words with a polynomial code provided $m \le n/2$. This is called systematic encoding and it goes like this: Divide $g(x)$ into $a(x)x^{n-m}$ and find the remainder $r(x)$. Then real word $a(x)$ encodes as $a(x)x^{n-m} - r(x)$. The advantage of this encoder is that decoding (when there are no errors) is instantaneous—the top m coefficients of the code word are identical to the real word $a(x)$. There is a matrix formulation for systematic encoding; to find it, encode the standard basis vectors of real-word space, and put these as columns of a matrix.

- We reviewed the BCH code as a polynomial code. If α is a primitive element of $\mathbb{F}_{2^k}$ (it's multiplicative order is $2^k - 1$), let $p_i(x)$ be the minimum polynomial for α^i over $\mathbb{F}_2$. Then the generator polynomial is the product of the distinct $p_i(x)$ for $i = 1, \ldots, 2t$. Since $p_{2i}(x) = p_i(x)$, one need only consider odd values of i.

- The following claim was made in class: *When* $2t < n = 2^k - 1$, *the polynomials* $p_1(x)$, $p_3(x)$, *...,* $p_{2t-1}(x)$ *are all distinct, and so the generator polynomial* $g(x)$ *is their product.* In fact this claim is *not true*, sorry about that! Here's a counterexample: Consider BCH$(7, 9)$ and consider $p_9(x)$ and $p_{17}(x)$. We have the general principle for polynomials over $\mathbb{F}_2$ that if β is a root, then so too is $\beta^2, \beta^4, \beta^8$, etc. Well $\beta = \alpha^9$ is a root of $p_9(x)$, so $\beta^{16} = \alpha^{144}$ is a root as well. But in $\mathbb{F}_{2^7}$, the primitive element α has multiplicative order $2^7 - 1 = 127$, so $\alpha^{144} = \alpha^{17}$. Thus, $p_{17}(x) = p_9(x)$.

- So, there can be repeats among the $p_i(x)$, but these are not repeated in the generator polynomial $g(x)$ for BCK(k, t). It can be shown that there are no other repeats than the one listed above for BCH$(7, 9)$, so the generator polynomial is $p_1(x)p_3(x) \ldots p_{15}(x)$. Further, these all have degree 7 (do you know why?), so $g(x)$ has degree 56.

- Here is a corrected version of the claim from class. *In code* BCH(k, t), *if* $p_{2i-1}(x) = p_{2j-1}(x)$ *with* $i < j$, *then we must have* $(2i - 1)(2j - 1) > 2^k$. In particular, if $2t \leq 2^{k/2}$, then the polynomials $p_{2i-1}(x)$ are distinct for $i \leq t$. Can you prove this?

- The main point of all of this is that the individual polynomials $p_{2i-1}(x)$ all divide $x^{2^k} - x$, so they all divide $x^{2^k-1} - 1$ (assuming that $k \geq 2$), and so their least common multiple $g(x)$ also divides $x^{2^k-1} - 1$. Thus, the code BCH(k, t) is cylcic.

- We briefly went into Reed–Solomon codes. Here, we take the same matrix $V_{k,t}$ as for the BCH(k, t) code, and consider it's nullspace in $\mathbb{F}_{2^k}^n$ (as opposed to $\mathbb{F}_2^n$). See Ch. 17, where we covered briefly the first few sections. We noted that Reed–Solomon codes are good for handling "bursts" of single bit errors, since each vector coordinate in a code word has itself k bits, so if there are many bit-errors all occuring in a narrow interval, they will involve only a few coordinates of the code, and so will be correctable if the number of coordinates affected is $\leq t$.