**Math 75 notes, Lecture 17 outline**

P. Pollack and C. Pomerance

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

- We reviewed the definition of the Hamming codes Ham($k$) and some of their properties: that they have length $n = 2^k - 1$, dimension $m = 2^k - 1 - k$, are perfect codes, and have minimum distance 3. (See pp. 64, 66.)

- We showed that Ham($k$) can also be characterized as follows: Let $n = 2^k - 1$ as before, and $H'_k$ be the $1 \times n$ matrix whose entries are the nonzero elements of $\mathbb{F}_{2^k}$. Then Ham($k$) consists of those $x \in \mathbb{F}_2^n$ for which $x^T$ belongs to the nullspace of $H'_k$. (You should think of $H'_k$ as a generalized check matrix for Ham($k$); it is not a check matrix in the normal sense because its entries are from $\mathbb{F}_{2^k}$, not $\mathbb{F}_2$.)

- We defined the codes BCH($k, t$) for positive integers $k$ and $t$ with $t < 2^{k-1}$ as the binary code with generalized check matrix $V_{k,t}$ (see p. 206). Here $V_{k,t}$ is the $2t \times n$ matrix with $i$th row, $j$th column entry $\alpha^{i(n-j)}$, where $\alpha$ is a fixed generator of the multiplicative group $\mathbb{F}_{2^k}^{\times}$. (Note: the book incorrectly reverses the dimensions of $V_{k,t}$.)

- We saw that if we defined $H_{k,t}$ by just taking the odd rows of $V_{k,t}$, then for $x \in \mathbb{F}_2^n$, we have
$$H_{k,t}x^T = 0 \iff V_{k,t}x^T = 0.$$
(See Proposition, p. 211.) So either matrix could be used to define BCH($k, t$).

- We proved, using the $t \times n$ matrix $H_{k,t}$, that the dimension of BCH($k, t$) is at least $n - kt$. (See part (a) of the Theorem on p. 212.)

- We proved that every set of $2t$ columns of $V_{k,t}$ is linearly independent over $\mathbb{F}_{2^k}$ (and so also over $\mathbb{F}_2$). (See p. 213.) We deduced that the minimum distance of BCH($k, t$) exceeds $2t$, so that BCH($k, t$) can correct any error of weight at most $t$. (See part (b) of the Theorem on p. 212.)

A brief word on notation: The book's examples revolve around BCH(4, 3), so that elements of $\mathbb{F}_{16}$ come into play. Here (see p. 101) $\mathbb{F}_{16}$ is being identified with $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$, and to go from an integer $0 \le n < 15$ to an element of $\mathbb{F}_{16}$, one writes $n$ in binary, so
$$n = a \cdot 2^3 + b \cdot 2^2 + c \cdot 2 + d, \quad \text{where } a, b, c, d \in \{0, 1\},$$
and views $n$ as corresponding to the element
$$a\beta^3 + b\beta^2 + c\beta + d,$$
where $\beta = [x] \in \mathbb{F}_2[x]/(x^4 + x^3 + 1)$. It turns out that $\beta$ (which is '2' in this notation) is also a generator for $\mathbb{F}_{16}^{\times}$, and this is the generator that is used to define the generalized check matrices $H_{4,3}$ and $V_{4,3}$.