ENEE626: Error-Correcting Codes

Instructor: Alexander Barg — Notes by: Juliana Belding

Lecture 13 (10/19/05). Cyclic Codes
(Algebraic Codes with Easy Decoding) — http://www.ece.umd.edu/~abarg/626

Motivation: Cyclic codes form a class of error-correcting codes that can correct errors up to $\frac{1}{2}$ the (estimated) minimum distance in a "reasonable" time-span. This is because, for a code length n, the decoding procedure involves solving a system of n equations which takes about $O(n^3)$ operations in the most pessimistic situation. In fact, shortcuts can reduce the time to $O(n^2)$ or better, making the decoding truly implementable, like in the case of Reed-Solomon codes used on CDs and in hard drives. Cyclic codes and their generalizations also continue to provide fascinating problems for theoretical research.

Definition: $\mathcal{C} \subset \mathbb{F}_q^n$ is a cyclic code if $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$. That is, $\mathcal{C}$ is closed under the cyclic shift mod n, which corresponds to multiplication by x^{n-1} of the $(n-1)$-degree polynomial with these coefficients, $\sum_{i=0}^{n-1} c_i x^i$.
Note: This definition does not require the code to be linear, though we will consider only the linear situation for the rest of the notes.

We will assume throughout that $(n, q) = 1$.

Definition: Let $R_n = \mathbb{F}_q[x]/(x^n - 1)$ be the ring of polynomials of degree $\leq n-1$ with coefficients in $\mathbb{F}_q$ with operations performed mod $(x^n - 1)$.

The formal definition of a ring is as follows:
Definition A ring R is an additive Abelian group with a multiplication operation which is commutative, associative and distributive and has an identity element.

Definition: An ideal $\mathcal{C} \subset R_n$ is a linear subspace of R_n such that

$$c(x) \in \mathcal{C} \Rightarrow r(x)c(x) \in \mathcal{C} \text{ for all } r(x) \in R_n. \text{ (*)}$$

Note: The condition (*) can be replaced by (**) $c(x) \in \mathcal{C} \Rightarrow xc(x) \in \mathcal{C}$ since $\mathcal{C}$ is a linear subspace and therefore contains all sums and scalar multiples of its elements.

Example 1: The integers, **Z**, are a ring. The subset of even integers, denoted $2\mathbf{Z}$, is an ideal of **Z** since any integer multiple of an even number is still an even number.

Definition: A cyclic code $\mathcal{C}$ is an ideal of R_n. Thus, $\mathcal{C}$ is a linear code.

In cyclic codes, we can represent codewords by polynomials as follows:
$c = (c_0 c_1 ... c_{n-1}) \longleftrightarrow c(x) = \sum_{i=0}^{n-1} c_i x^i$

Theorem Let $\mathcal{C}$ be a cyclic code of dimension k, $\mathcal{C} \subset \mathbb{F}_q^n$.
(1) There exists a unique monic polynomial $g(x)$ such that $\mathcal{C} = \langle g(x) \rangle$, i.e. every codeword is a multiple of $g(x)$. The degree of g is $n-k$. $g(x)$ is called the generator polynomial of $\mathcal{C}$.
(2) $g(x) | (x^n - 1)$.
(3) The generator matrix of $\mathcal{C}$ is

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ ... \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & ... & g_{n-k} & 0 & ... & ... & 0 \\ 0 & g_0 & g_1 & ... & g_{n-k} & 0 & ... & 0 \\ 0 & & & & & & & 0 \\ 0 & 0 & ... & 0 & g_0 & g_1 & ... & g_{n-k} \end{pmatrix}$$

Proof:
(1) Take $g(x)$, a monic polynomial of the smallest degree in $\mathcal{C}$. (Such a polynomial exists since the code is a finite set.) Let $c(x) \in \mathcal{C}$. Use the division algorithm to write $c(x) = g(x)q(x) + r(x)$ where $0 \leq \deg r < \deg g$. Since the code is linear, $r(x) = c(x) - g(x)q(x) \in \mathcal{C}$. If $r(x) \not\equiv 0$, since it has degree smaller than that of g, this would contradict the choice of g as a nonzero polynomial of the smallest degree in $\mathcal{C}$. Thus, $r(x) = 0$ and so $c(x)$ is a multiple of $g(x)$. Therefore $g(x)$ generates $\mathcal{C}$. It is unique since its leading coefficient must be 1.

Let $\deg g = r$; we will show that $r = n - \dim \mathcal{C}$. We have seen that every codeword c is a multiple of g, i.e., has the form $c(x) = a(x)g(x)$ for some polynomial $a(x)$. All these multiples are different, moreover the polynomials $g(x), xg(x), x^2g(x), \ldots, x^{n-r-1}g(x)$ are linearly independent as vectors over $\mathbb{F}_q$ and span $\mathcal{C}$ as a linear space. Hence, $\dim \mathcal{C} = n - r$.
(2) Use the division algorithm to write $x^n - 1 = g(x)q(x) + r(x)$ with $0 \leq \deg r < \deg g$. Then in R_n, since $x^n - 1 = 0$, we have that $r(x) = -g(x)q(x)$, and hence $r(x) \in \mathcal{C}$. But again, if $r(x) \neq 0$, since it has degree smaller than that of g, this would contradict the choice of g as a polynomial of least degree in $\mathcal{C}$. Thus, $r(x) = 0$ and so $g(x)$ divides $x^n - 1$.

(3) Note that $g_0 \neq 0$. If it did, the codeword $x^{n-1}g(x) = x^{-1}g(x)$ has degree $\deg(g(x)) - 1$, and we would have a contradiction to the assumption that $g(x)$ has least degree in $\mathcal{C}$. So $g_0 \neq 0$ and thus because of the band form of the matrix, the k rows must be linearly independent.

Example 2: The Hamming Code $\mathcal{H}_3$ is a cyclic code $[7, 4, 3]$. Let α be a primitive element of $\mathbb{F}_8$, with minimal polynomial $m_1(x) = x^3 + x + 1$. Recall that the other roots of $m_1(x)$ are α^2 and α^4, since squaring is a linear operation over $\mathbb{F}_2$. Considering codewords of $\mathcal{H}_3$ as polynomials $c(x)$, we recall that $c(x) \in \mathcal{H}_3$ if and only if $c(\alpha) = 0$. Again, since squaring is linear, $c(\alpha)^2 = c(\alpha^2)$, so $c(\alpha^2) = 0$, and similarly, $c(\alpha^4) = 0$. Thus all the roots of $m_1(x)$ are roots of $c(x)$ so $m_1(x)$ divides $c(x)$ for all $c \in \mathcal{H}_3$. Thus every codeword is a multiple of $m_1(x)$. Since $\deg m_1 = 3 = n-k$, the polynomial m_1 is the generator polynomial. Thus $g(x) = m_1(x)$ is the generator polynomial of $\mathcal{H}_3$, and we have the following generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Definition: The <u>check polynomial</u> for a cyclic code $\mathcal{C} = \langle g(x) \rangle$ is $h(x) = \frac{x^n - 1}{g(x)}$. The degree of h equals k, where k is the dimension of $\mathcal{C}$.

Note: This definition makes sense since, if $c \in \mathcal{C}$, $c(x)h(x) = a(x)g(x)h(x) = 0 \bmod (x^n - 1)$. Furthermore, $c(x)h(x) = \left(\sum_{i=0}^{n-1} c_i x^i\right)\left(\sum_{i=0}^{n-1} h_i x^i\right) = 0$ implies that all the coefficients of this polynomial must be zero mod $(x^n - 1)$, and so we have n equations of the form

$$\sum_{j=0}^{n-1} c_j h_{(i-j) \bmod n} = 0, \quad (i = 0, 1, \ldots, n-1).$$

If we consider the equations corresponding to the coefficients of the terms $x^{n-1}, x^{n-2} \ldots, x^k$ and put $h_{k+1} = \cdots = h_{n-1} = 0$, we can make a parity check matrix as follows:

$$H = \begin{pmatrix} 0 & 0 & ... & 0 & h_k & h_{k-1} & ... & h_1 & h_0 \\ 0 & 0 & ... & h_k & h_{k-1} & ... & h_1 & h_0 & 0 \\ 0 & & & & & & & 0 & \\ h_k & h_{k-1} & ... & h_1 & h_0 & 0 & ... & 0 & 0 \end{pmatrix}$$

Example 2 (revisited): For the Hamming code $\mathcal{H}_3$, we have the check polynomial $h(x) = (x^7-1)/m_1(x) = m_0(x)m_3(x) = x^4 + x^2 + x + 1$, which we can calculate using the factorization of $x^7 - 1$ into minimal polynomials determined by the cyclotomic cosets. We then get the parity-check matrix:

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Definition: The elements a of $\mathbb{F}_q$ such that $c(a) = 0$ for all codewords $c(x) \in \mathcal{C}$ are call the <u>zeros of the code $\mathcal{C}$</u>. In general, to get a generator polynomial for a cyclic code, we take the product of the minimal polynomials of the zeros of the code.

Interlude: We can use the notion of a reciprocal polynomial to determine some of the minimal polynomials $m_s(x)$ from previously calculated ones.

Definition: Let $f \in \mathbb{F}_q[x], f(0) \neq 0$. The polynomial $g(x) = x^{\deg f} f(\frac{1}{x})$ is called the <u>reciprocal</u> polynomial of f. Note that a is a zero of f if and only if $g(a^{-1}) = 0$. (a^{-1} exists since we're working in a field.)

Example 2 (revisited): Recall that for $\mathcal{H}_3$ we have α, a primitive 7th root of unity with minimal polynomial $m_1(x) = x^3 + x + 1$. The cyclotomic cosets are $C_0 = \{0\}, C_0 = \{1, 2, 4\}$, and $C_3 = \{3, 6, 5\}$. Note that $\alpha^6 = \alpha^{-1}$, so α^6 is a root of the reciprocal polynomial of $m_1(x)$, the minimal polynomial of α. Namely, α^6 is a root of $g(x) = x^3 + x^2 + 1$. Since $\alpha^5 = (\alpha^6)^2$ and $\alpha^3 = (\alpha^6)^4$, $g(x)$ has roots $\alpha^3, \alpha^6, \alpha^5$, and therefore must be the minimal polynomial of α^3, that is, $g(x) = m_3(x)$.

Example 3 (revisited from Lecture 12): Using the notion of reciprocal polynomial, we see that since $\alpha^{14} = \alpha^{-1}$, m_7 must be the reciprocal polynomial to $m_1(x) = x^4 + x + 1$. So $m_7(x) = x^4 m_1(x^{-1}) = x^4 + x^3 + 1$. This is more efficient than calculating $m_7(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11})$.

Recall that the parity-check matrix H of a code $\mathcal{C}$ with $\dim \mathcal{C} = k$ generates the dual code, $\mathcal{C}^\perp$, of dimension $n-k$. From the form of H, it's clear that the generator polynomial of $\mathcal{C}^\perp$ is $h^*(x)$, the reciprocal polynomial of $h(x)$. Since $h^*(x)$ is a polynomial in $\mathbb{F}_q[x]$ of degree $< n$, the set of multiples of h in R_n also forms a cyclic code.
To conclude: The dual of a cyclic code $\mathcal{C}$ is cyclic. The zeros of $\mathcal{C}^\perp$ are the inverses of the nonzeros of $\mathcal{C}$.

2-Error Correcting Binary BCH Codes

We construct a binary 2-error correcting code from the Hamming code $\mathcal{H}_m[n, n-m, 3]$ where $n = 2^m - 1$. Let α be a primitive n^{th} degree root of unity. Recall that the parity check matrix of $\mathcal{H}_m$ can be written as $(1, \alpha, \alpha^2, ..., \alpha^{2^m-2})$, where each column is expanded into a binary m-tuple. Consider the cyclotomic coset $C_1 = \{1, 2, 4, 8, 16, \ldots, 2^{m-1}\}$, representing the 2^k-powers of α. Since squaring is linear, $c(\alpha) = 0 \Rightarrow c(\alpha^{2^k}) = 0$ for all $0 \leq k \leq m-1$. Thus, all of the parity checks of the form $c(\alpha^{2^k}) = 0$ are linearly dependent. To correct more than one error, we must add some independent parity-check equations.

To get a new parity check, we look at the next cyclotomic coset, $C_3 = \{3, 6, 12, \ldots, 3 \cdot 2^{m-1}\}$. If we require that the codewords have α^3 as a zero, this gives us another set of parity checks, namely

$$(1, \alpha^3 \alpha^6, \alpha^9, \ldots, \alpha^{3 \cdot 2^m - 2}),$$

with every power of α^3 as an m-column. So together we obtain the parity check matrix:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \ldots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \ldots & \alpha^{3 \cdot 2^m - 2} \end{pmatrix}$$

Remark: A binary cyclic code with zeros α and α^3 is called a <u>2-error correcting BCH code</u>. What makes this a BCH code is that the degrees of α used as parity checks are consecutive: $\alpha, \alpha^2, \alpha^3, \alpha^4$. Note that α^2 doesn't contribute any new parity checks since it is automatically a zero of any polynomial which has α as a zero.

Example 4 Consider the Hamming Code $\mathcal{H}_4[15, 11, 3]$. Let α be a primitive 14th root of unity. We can construct a BCH code $\mathcal{C}$ with zeros α and α^3. The parity check matrix is:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \ldots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \ldots & \alpha^{12} \end{pmatrix}$$

This is a 8 by 15 parity check matrix with all eight rows linearly independent. So we have a $[15, 7]$ code. Note that the dimension is $n - 2m$, which will be true for any BCH code. It remains to prove that $d = 5$.

Claim: $d = 5$.

Proof: Let $c(x)$ be a codeword of $\mathcal{C}$. Then $c(\alpha) = c(\alpha^3) = 0$. Suppose c is sent over a channel and received as $y(x) = c(x) + e(x)$, where $e(x)$ is the error. Number the columns of the parity check matrix by the elements of $\mathbb{F}_{16}$ in the increasing order of the powers of the primitive element: $1, \alpha, \alpha^2, \ldots \alpha^{14})$. Since we are assuming at most 2 errors, $e(x) = x^i + x^j$, where i, j stand for the locations of the errors in the list $1, \alpha, \alpha^2, \ldots \alpha^{14}$. Let $S_1 = y(\alpha) = e(\alpha) = \alpha^i + \alpha^j$ and $S_3 = (\alpha^3) = e(\alpha^3) = \alpha^3 i + \alpha^3 j$. Let X_1, X_2 be the "error locators," that is $X_1 = \alpha^i$ and $X_2 = \alpha^j$. The locators satisfy the following system of equations:

$$\begin{array}{ccccc} S_1 & = & X_1 & + & X_2 \\ S_3 & = & X_1^3 & + & X_2^3. \end{array}$$

Note that $S_1^3 + S_3 = X_1^3 + X_1^2 X_2 + X_1 X_2^2 + X_2^3 + X_1^3 + X_2^3 = X_1 X_2 (X_1 + X_2)$, so we have the revised set of equations:

$$\begin{array}{ccc} S_1 & = & X_1 + X_2 \\ S_1^3 + S_3 & = & X_1 X_2 (X_1 + X_2) \end{array}$$

which imply that X_1, X_2 correspond to the roots of the quadratic

$$z^2 + S_1 z + \frac{S_1^3 + S_3}{S_1} = 0.$$

Thus we need to solve the quadratic over $\mathbb{F}_2$. We have the following three cases: **(1)** If $S_1 = S_2 = 0$, both roots X_1, X_2 are zero, so we conclude there were no errors (since X_1, X_2 correspond to the powers of α which were incorrectly received.) **(2)** If $S_1 \neq 0$ and $S_3 = S_1^2$, then one root is zero and the other is S_1, so we conclude there was just one zero in the spot S_1 and we flip that coordinate. **(3)** If there are two distinct roots, $X_1, X_2 \in \mathbb{F}_{q^m}$, then we declare 2 errors and and flip their respective coordinates. **(4)** If there are no zeros in $\mathbb{F}_{q^m}$, we conclude that there were more than 2 errors.

Remark: In general, to correct 2 errors in a code of length $n \approx 2^m$, we need $2m \approx 2 \log_2 m$ parity checks.