Implementing Linear Codes

With linear codes and their generator and parity check matrices, encoding and decoding can be carried out by operating on these matrices (instead of handling complete lists of possible codewords). Very large codes can therefore be handled.

The problem of recovering the data block from a codeword can be greatly simplified through the use of **systematic codes.**

Systematic Codes (1)

Using Gaussian elimination and column reordering it is always possible to get a generator matrix of the form

$$\mathbf{G} = [\mathbf{P} \mid \mathbf{I}_k] = \left[\begin{array}{cccc|cccc} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{array}\right],$$

so that the data block is embedded in the last k coordinates of the codeword: $\mathbf{c} = \mathbf{mG} = [m_0\ m_1\ \cdots\ m_{k-1}][\mathbf{P} \mid \mathbf{I}_k] = [c_0\ c_1\ \cdots\ c_{n-k-1} \mid m_0\ m_1\ \cdots\ m_{k-1}]$.

Systematic Codes (2)

The corresponding parity check matrix for systematic codes is $\mathbf{H} = [\mathbf{I}_{n-k} \mid -\mathbf{P}^T] =$

$$\left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & -p_{0,0} & -p_{1,0} & \cdots & -p_{k-1,0} \\ 0 & 1 & \cdots & 0 & -p_{0,1} & -p_{1,1} & \cdots & -p_{k-1,1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -p_{0,n-k-1} & -p_{1,n-k-1} & \cdots & -p_{k-1,n-k-1} \end{array}\right].$$

Standard Array Decoder (1)

A received word $\mathbf{r}$ is modeled by the summation $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c}$ is the transmitted codeword and $\mathbf{e}$ is the error pattern induced by the channel noise. The maximum likelihood decoder picks a codeword $\mathbf{c}'$ such that $\mathbf{r} = \mathbf{c}' + \mathbf{e}'$, where $\mathbf{e}'$ has the smallest possible weight. A look-up table called a **standard array decoder** can be used to implement this process.

Standard Array Decoder (2)

Consider all words in V_q^n in the following way:

1. Remove all codewords in C from V_q^n. List these in a single row, starting with the all-zero word.

2. Select (and remove) one of the remaining words of the smallest weight and write it in the column under the all-zero word. Add this word to all other codewords and write the results in the corresponding columns (and remove these from the set of remaining words).

3. With no remaining words, stop; otherwise, repeat Step 2.

▷ Each row in the table is a coset of C.

Example: Standard Array for a Small Code

With $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$, one possible standard array is

0000	1010	1101	0111
0001	1011	1100	0110
0010	1000	1111	0101
0100	1110	1001	0011

Properties of Standard Arrays

▷ The standard array is uniquely determined exactly when the code is perfect.

▷ A standard array for a q-ary code of length n has q^n entries, all of which are stored in memory.

▷ A standard array can be used only for small codes.

The next method to be presented reduces the entry table from size q^n to q^{n-k}.

Syndrome Vectors

For a received vector $\mathbf{r}$, where $\mathbf{r} = \mathbf{c} + \mathbf{e}$, we know that $\mathbf{r}\mathbf{H}^T = \mathbf{0}$ when $\mathbf{r} = \mathbf{c}$ ($\mathbf{e} = \mathbf{0}$); cf. Theorem 4-8. The matrix product $\mathbf{r}\mathbf{H}^T$ is called the **syndrome vector** $\mathbf{s}$ for the received vector $\mathbf{r}$.

$$\begin{aligned} \mathbf{s} &= \mathbf{r}\mathbf{H}^T \\ &= (\mathbf{c}+\mathbf{e})\mathbf{H}^T \\ &= \mathbf{c}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T \\ &= \mathbf{e}\mathbf{H}^T \end{aligned}$$

⇒ The syndrome vector depends only on the error pattern. Moreover, the syndrome vector is the same for all words in a row of a standard array (and different for words in different rows).

Example: Syndrome Table for a Small Code

The code used in the previous example has $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$.

Error pattern	Syndrome
0000	00
0001	11
0010	10
0100	01

If $\mathbf{r} = 1111$ is received, then $\mathbf{s} = \mathbf{r}\mathbf{H}^T = 10$, so $\mathbf{e} = 0010$ and $\mathbf{c} = 1101$.

Weight Distribution of a Block Code

The weight distribution of an (n, k) code C is a series of coefficients $A_0, A_1, \ldots, A_n$, where A_i is the number of codewords of weight i in C.

The weight distribution is often written as a polynomial $A(x) = A_0 + A_1 x + \cdots + A_n x^n$. This representation is called the **weight enumerator**.

The MacWilliams Identity: Let $A(x)$ and $B(x)$ be the weight enumerators for an (n, k) code C and its $(n, n-k)$ dual code $C^\perp$. Then

$$B(x) = 2^{-k}(1+x)^n A\left(\frac{1-x}{1+x}\right).$$

Binary Hamming Codes

The binary Hamming codes are $(n = 2^m - 1, k = 2^m - m - 1)$ perfect one-error-correcting codes for any integer $m \geq 2$.

The columns of a parity check matrix (of size $m \times n$) of a binary Hamming code consist of all $2^m - 1$ nonzero vectors of length m. The smallest number of such vectors that sum to zero is three $\Rightarrow$ the minimum distance is $d = 3$.

Question. Prove that these codes are indeed perfect.

Decoding Hamming Codes

A received word corrupted by a single error in position i gives $\mathbf{s} = \mathbf{r}\mathbf{H}^T = \mathbf{d}_i^T$, where $\mathbf{d}_i$ is the ith column $\mathbf{H}$.

Decoding algorithm for Hamming code:

1. Compute the syndrome $\mathbf{s} = \mathbf{r}\mathbf{H}^T$.
2. Find the column $\mathbf{d}_i$ of $\mathbf{H}$ that matches the syndrome.
3. Complement the ith bit in the received word.

If the columns of $\mathbf{H}$ are in lexicographic order, the decimal value of the syndrome gives the position of the error (with the coordinates numbered $1, 2, \ldots, n = 2^m - 1$).

Weight Enumerator for Hamming Codes

The weight enumerator for the (n, k) binary Hamming code is

$$A(x) = \frac{(1+x)^n + n(1-x)(1-x^2)^{(n-1)/2}}{n+1}.$$

For example, for the $(15, 11)$ binary Hamming code we get
$A(x) = 1 + 35x^3 + 105x^4 + 168x^5 + 280x^6 + 435x^7 + 435x^8 + 280x^9 + 168x^{10} + 105x^{11} + 35x^{12} + x^{15}$.

Question. Why is $A_i = A_{15-i}$ in this formula?

The weight enumerator can be used to calculate exact probabilities of undetected error and decoder error as a function of the binary symmetric channel crossover probability; see [Wic, Fig. 4-9].

Nonbinary Hamming Codes

Hamming codes over GF(q) are
$(n = (q^m - 1)/(q-1), k = (q^m - 1)/(q-1) - m)$ perfect one-error-correcting codes for any integer $m \geq 2$.

The column vectors of a parity check matrix (of size $m \times n$) of such a code are selected from the set of $q^m - 1$ nonzero vectors of length m. Since for each such m-tuple, there are $q - 1$ other m-tuples that are multiples of that m-tuple, exactly one m-tuple is selected from each such set of multiples. For example, over GF(3),
$(1, 2, 0) + (1, 2, 0) = (2, 1, 0)$.

Modified Codes

puncturing Delete one of the redundant coordinates. An (n, k) codes becomes an $(n-1, k)$ code.

extending Add an additional redundant coordinate. An (n, k) code becomes an $(n+1, k)$.

shortening Delete a message coordinate. An (n, k) code becomes an $(n-1, k-1)$.

lengthening Add a message coordinate. An (n, k) code becomes an $(n+1, k+1)$ code.

These and two additional terms are illustrated in [Wic, Fig. 4-10].

Linear Cyclic Block Codes (1)

A (linear or nonlinear) code C of length n is said to be **cyclic** if for every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, there is also a codeword $\mathbf{c}' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

The **code polynomial** of a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. We know that if C is a q-ary (n, k) code, then the codewords form a vector subspace of dimension k within the space of all n-tuples over GF(q).

Linear Cyclic Block Codes (2)

Let C be a cyclic code, and let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ and $\mathbf{c}'$ be two codewords such that $\mathbf{c}'$ is obtained by a right cyclic shift of $\mathbf{c}$. Then

$$\begin{aligned} x \cdot c(x) &= x \cdot (c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \\ &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \\ &\equiv c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} \pmod{x^n - 1} \\ &\equiv c'(x) \pmod{x^n - 1}. \end{aligned}$$

Now $x^t c(x) \bmod (x^n - 1)$ corresponds to a shift of t places to the right. In general, $a(x)c(x) \bmod (x^n - 1)$, where $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathrm{GF}(q)[x]/(x^n - 1)$ is an arbitrary polynomial, is a linear combination of cyclic shifts of $\mathbf{c}$ and is a codeword.

Cyclic Codes and Ideals

We have that $a(x)c(x) \in C$ for all $a(x) \in \mathrm{GF}(q)[x]/(x^n - 1)$, $c(x) \in C$.

▷ A cyclic code is an ideal within $\mathrm{GF}(q)[x]/(x^n - 1)$ and vice versa.

Properties of Cyclic Codes

Let C be a q-ary (n, k) linear cyclic code.

1. Within the set of code polynomials in C there is a unique monic polynomial $g(x)$ with minimal degree $r < n$ called the *generator polynomial* of C.
2. Every codeword polynomial $c(x) \in C$ can be expressed uniquely as $c(x) = m(x)g(x) \bmod (x^n - 1)$, where $m(x) \in \mathrm{GF}(q)[x]$ is a polynomial of degree less than $n - r$.
3. The generator polynomial $g(x)$ of C is a factor of $x^n - 1$ in $\mathrm{GF}(q)[x]$.

Since $g(x)$ is monic, $g(x) = g_0 + g_1 x + \cdots + g_{r-1} x^{r-1} + x^r$.

Question. Why can we assume that $g_0 \neq 0$?

Possible Dimensions of Cyclic Codes (1)

The dimension of a cyclic code C is is $n - r$, where r is the degree of the generator polynomial of C. The factorization of $x^n - 1$ into irreducible polynomials in $\mathrm{GF}(q)[x]$ has been discussed earlier.

Example 1. Binary cyclic codes of length $n = 15$ $(= 2^4 - 1)$. The conjugacy classes formed by the powers of α, an element of order 15 in GF(16) are

$\{1\}$,
$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$,
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$,
$\{\alpha^5, \alpha^{10}\}$,
$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$.

Possible Dimensions of Cyclic Codes (2)

Example 1. (cont.) Hence, the binary polynomial $x^{15}-1$ factors into one binary polynomial of degree 1, one of degree 2, and three of degree 4. Therefore $x^{15}-1$ has factors of all degrees between 1 and 15 (for example, $11 = 4+4+2+1$), and there are binary cyclic $(15,k)$ codes for all $1 \leq k \leq 15$.

Example 2. In a previous lecture, it was shown that the binary polynomial $x^{25}-1$ factors into one polynomial of degree one, one of degree 4 and one of degree 20. Hence there are binary cyclic $(25,k)$ codes for $k \in \{1,4,5,20,21,24,25\}$.

Encoding Cyclic Codes (1)

Let $g(x)$ be the degree r generator polynomial for an (n,k) q-ary cyclic code C. An $(n-r)$-symbol data block $(m_0, m_1, \ldots, m_{n-r-1})$ is associated with a **message polynomial** $m(x) = m_0 + m_1 x + \cdots + m_{n-r-1}x^{n-r-1}$. Now

$$\begin{aligned} c(x) &= m(x)g(x) \\ &= m_0 g(x) + m_1 x g(x) + \cdots + m_{n-r-1}x^{n-r-1}g(x) \\ &= [m_0 \; m_1 \; \cdots \; m_{n-r-1}] \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1}g(x) \end{bmatrix}. \end{aligned}$$

Encoding Cyclic Codes (2)

A generator matrix for a cyclic code is then

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & & & \\ & g_0 & g_1 & \cdots & g_r & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & g_0 & g_1 & \cdots & g_r \end{bmatrix},$$

where the unmarked entries are zero.

Decoding Cyclic Codes (1)

Since $g(x) \mid (x^n - 1)$, there exists a **parity polynomial** $h(x)$ such that $g(x)h(x) = x^n - 1$. Moreover, since $g(x) \mid c(x)$, we have that $c(x)h(x) \equiv 0 \pmod{x^n - 1}$. We denote $s(x) := c(x)h(x) \bmod (x^n-1)$ with $s(x) = s_0 + s_1 x + \cdots + s_{n-1}x^{n-1} \in \mathrm{GF}(q)[x]/(x^n-1)$. Now

$$\begin{aligned} s(x) &= \sum_{t=0}^{n-1} s_t x^t \equiv c(x)h(x) \equiv \left(\sum_{i=0}^{n-1} c_i x^i\right)\left(\sum_{j=0}^{n-1} h_j x^j\right) \\ &\equiv 0 \bmod (x^n - 1) \;\Rightarrow \\ s_t &= \sum_{i=0}^{n-1} c_i h_{(t-i) \bmod n} \end{aligned}$$

Decoding Cyclic Codes (2)

Take the last $(n-k)$ of the parity check equations:

$$\mathbf{s}' = \begin{bmatrix} s_k \\ s_{k+1} \\ \vdots \\ s_{n-1} \end{bmatrix}^T = \begin{bmatrix} \sum_{i=0}^{n-1} c_i h_{(k-i) \bmod n} \\ \sum_{i=0}^{n-1} c_i h_{(k+1-i) \bmod n} \\ \vdots \\ \sum_{i=0}^{n-1} c_i h_{(n-1-i) \bmod n} \end{bmatrix}^T =$$

$$[c_0\, c_1\, \cdots\, c_{n-1}] \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & & & & \\ & h_k & h_{k-1} & \cdots & h_0 & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}^T = \mathbf{c}\mathbf{H}^T.$$

Decoding Cyclic Codes (3)

By a previous argument, if $\mathbf{c}$ is a codeword, then $\mathbf{s}' = \mathbf{c}\mathbf{H}^T = \mathbf{0}$, so the rows of $\mathbf{H}$ are vectors in $C^\perp$. Moreover, since the row rank of $\mathbf{H}$ is $n-k$ (as $h(x)$ is monic, the rows are linearly independent). Hence the row space spans $C^\perp$, and $\mathbf{H}$ is a valid parity check matrix.

Theorem 5-3. Let C be an (n,k) cyclic code with generator polynomial $g(x)$. Then $C^\perp$ is an $(n, n-k)$ cyclic code with generator polynomial $h^*(x)$, the reciprocal of the parity polynomial for C.

Proof: The parity check matrix has the same structure as the generator matrix. $\square$

Example: Binary Cyclic Code of Length 7 (1)

First, we need to factor $x^7 - 1$ over GF(2)[q]. Let α be a root of $p(x) = 0$, where $p(x)$ is the primitive polynomial $x^3 + x + 1$. The conjugacy classes and the corresponding polynomials are as follows:

$$\begin{array}{lcl} \{1\} & \leftrightarrow & x+1, \\ \{\alpha, \alpha^2, \alpha^4\} & \leftrightarrow & x^3+x+1, \\ \{\alpha^3, \alpha^6, \alpha^5\} & \leftrightarrow & x^3+x^2+1. \end{array}$$

The polynomial $g(x) = (x^3+x+1)(x+1) = x^4+x^3+x^2+1$ is one possible generator polynomial. The corresponding parity polynomial is $h(x) = (x^7+1)/g(x) = x^3+x^2+1$.

Example: Binary Cyclic Code of Length 7 (2)

(cont.) The message polynomials consist of all binary polynomials of degree less than or equal to 2. The code is a $(7,3)$ code (with $2^3 = 8$ words). A codeword of the code is, for example, $(x^2+1) \cdot g(x) = 1 + x^3 + x^5 + x^6 \to 1001011$. The following matrices are, respectively, a generator matrix and a parity check matrix of the code:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}, \; \mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$