Gröbner Bases and Codes

Cyclic Codes

The **weight** of a vector $\mathbf{v}$ is $|\{i|v_i \neq 0\}|$. This is denoted $w(\mathbf{v})$.

The **Hamming distance** of two vectors, $\mathbf{x}$ and $\mathbf{y}$, of $GF(q)^n$ is $|\{i|x_i \neq y_i\}|$. This is denoted $d(\mathbf{x}, \mathbf{y})$.

The **distance** of a code C, normally denoted d, is $\inf_{\mathbf{x},\mathbf{y}\in C,\ \mathbf{x}\neq\mathbf{y}} \{d(\mathbf{x}, \mathbf{y})\}$.

A **linear code** is a code where the set of codewords, C, forms a vector subspace of $GF(q)^n$, with dimension k. If such a code has distance d, it is called a $[n, k, d]$-code. A $[n, k, d]$-code has q^k codewords. The distance of a linear code is $\inf_{\mathbf{w}\in C\setminus\{0\}} \{d(\mathbf{w}, \mathbf{0})\} = \inf_{\mathbf{w}\in C\setminus\{0\}} \{w(\mathbf{w})\}$.

We can consider a linear code as a function $\lambda : GF(q)^k \longrightarrow GF(q)^n$ with image C. An efficient way to calculate $\lambda(\mathbf{w})$ is $\mathbf{w}G$, for some matrix G. This matrix is called a **generator matrix** for the code.

The subspace may also be described as the set of solutions of a system of $n - k$ independent linear equations in n variables. The matrix of coefficients of such a system is called a **parity check matrix** for the code.

With a cyclic code, there is an isomorphism between codewords and polynomials

$$(a_0, a_1, \ldots, a_{n-1}) \longleftrightarrow a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

Then the cyclic shift of $(a_0, a_1, \ldots, a_{n-1})$ to $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is the same as multiplying $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ by x, and then taking the remainder on division by $x^n - 1$. Thus, we only need to consider polynomials of the ring $R = GF(q)[x]/\langle x^n - 1\rangle$.

Proposition 1. *Let $R = GF(q)[x]/\langle x^n - 1\rangle$. A subspace $C \subset R$ is a cyclic code if and only if C is an ideal of R.*

Proof. Suppose that C is a cyclic code. As it is linear, it is closed under addition, and constant multiplication. Now let $w(x) \in C$ and $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in R$. Then

$$\begin{aligned} w(x)f(x) &= w(x)(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \\ &= a_0w(x) + a_1w(x)x + \cdots + a_{n-1}w(x)x^{n-1} \end{aligned}$$

Each $a_iw(x)$ is in C, and then each element is multiplied by x a number of times. As C is cyclic, it is closed under multiplication by x, and so each summand is in C. Hence $w(x)f(x) \in C$, and C is an ideal.
Conversely, assume that C is an ideal. If $f(x)$ is a scalar, then the ideal conditions imply that C is linear. $x \in R$, so $xw(x) \in C$ for all $w(x) \in C$, and so C is cyclic. □

Proposition 2. *R is a principal ideal domain. That is, every ideal is generated by a single polynomial, g. Moreover, g is a divisor of $x^n - 1$ in $GF(q)[x]$.*

Proof. For the first statement, see Theorem 4.3, course notes. We can assume that g is the minimal such polynomial that generates the ideal I. Then, by the division algorithm, $x^n - 1 = q(x)g(x) + r(x)$, where $\deg(r) < \deg(g)$. But then $r(x) \equiv -q(x)g(x) \bmod(x^n - 1)$, and so $r(x) \in \langle g(x)\rangle$. By the minimality of $g(x)$, $r(x)$ must be 0, and so $x^n - 1 = q(x)g(x)$. □

The polynomial g in Proposition 2 is called a **generator polynomial** for the cyclic code.

The Singleton Bound

Theorem 3 (Singleton bound)**.** *A code C of length n with distance d over an alphabet of size q can have at most q^{n-d+1} codewords.* □

Any code that meets Singleton bound with equality is called a **maximum distance seprable**, or **MDS code**.

Given a code C with q^k codewords over an alphabet of size q, a set of k coordinates is called an **information set** of C if the codewords run through all q^k possible k-tuples in that set of coordinates. That is, if there is a unique codeword associated with every possible set of symbol values in that set of coordinates. In other words, we may freely specify the symbols in these coordinates, and then the remainder of the codeword is uniquely specified.

Corollary 4. *A linear $[n, k, d]$-code over $GF(q)$ has $k \leq n - d + 1$. Equality holds if and only if every set of k coordinates is an information set of the code.* □

Reed-Solomon Codes

Choose a finite field $GF(q)$ and a primitive element of $GF(q)$, α. Fix $k < q$, and let $L_{k-1} = \{\sum_{i=0}^{k-1} a_i t^i \mid a_i \in GF(q)\}$ be the vectorspace of polynomials of degree at most $k-1$ in $GF(q)[t]$. To create codewords (in $GF(q)^{q-1}$), evaluate polynomials in L_{k-1} at the $q-1$ non-zero elements of $GF(q)$. Hence

$$C = \{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) \in GF(q)^{q-1} \mid f \in L_{k-1}\}$$

is the set of codewords of a code. This code is called a **Reed-Solomon** code, denoted by $RS(k, q)$. Another way to look at Reed-Solomon codes is as a mapping, $f(z) \mapsto \{f(\alpha^i) \mid 0 \leq i \leq q-2\} \cup \{f(0)\}$, where $f(z)$ is one of the q^k polynomials over $GF(q)$ of degree less than k.

Theorem 5. *$RS(k, q)$ is a linear $[n = q, k, d = n - k + 1]$ MDS code over $GF(q)$.*

Proof. The code is linear because the sum of the codewords corresponding to two polynomials $f(z)$ and $f'(z)$ is the codeword corresponding to the polynomial $f(z) + f'(z)$, and the multiple of the codeword corresponding to $f(z)$ by $\varpi \in GF(q)$ is the codeword corresponding to the polynomial $\varpi f(z)$.
A codeword has a 0 in the coordinate corresponding to α^i if and only if $f(\alpha^i) = 0$. That is, if and only if α^i is a root of the equation $f(z) = 0$. By the fundamental theorem of algebra, if $f(z) \neq 0$, then since $\deg(f(z)) \leq k - 1$, this equation can have at most $k - 1$ roots in $GF(q)$. Therefore a nonzero codeword can have at most $k-1$ symbols, so its weight is at least $n-k+1$. Since the code is linear, this implies that its distance is at least $n - k + 1$. But by the Singleton bound, the distance is at most $n-k+1$. Therefore $d = n-k+1$, and $RS(k, q)$ is a linear MDS code. □

To obtain a generator matrix for a Reed-Solomon code, take a basis of L_{k-1} and evaluate to form the corresponding codewords. The simplest basis is the monomial basis, $\{1, t, \ldots, t^{k-1}\}$.

For example, consider $RS(4,9)$. Using the monomial basis $\{1,t,t^2,t^3\}$ for L_4, the generator matrix for $RS(4,9)$ is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \end{bmatrix}$$

Proposition 6. *Let $RS(k,q)$ have distance $d = q - k$. Then the generator polynomial for $RS(k,q)$ has the form*

$$g = (x-\alpha)\cdots(x-\alpha^{d-1})$$

□

For example, the generator polynomial of $RS(4,9)$ is $(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$.

Multivariate polynomials

Let R be a quotient ring of $GF(q)[x_1,\ldots,x_m]$ of the form $R = GF(q)[x_1,\ldots,x_m]/\langle x_1^{n_1}-1,\ldots,x_m^{n_m}-1\rangle$, for some $n_i \in \mathbb{Z}^+ \cup \{0\}$. Any ideal I of R will be a linear code closed under multiplication by elements of R. We call any code obtained in this way a **m-dimensional cyclic code**.

Note that $\mathcal{G} = \{x_1^{n_1}-1,\ldots,x_m^{n_m}-1\}$ is a Gröbner basis for $\langle\mathcal{G}\rangle$, with respect to all term orders. Therefore standard representations for elements of R can be computed by applying the division algorithm in $GF(q)[x_1,\ldots,x_m]$ and computing remainders with respect to $\mathcal{G}$. In this way, we obtain as representations of elements of R all polynomials whose degree in x_i is strictly less than n_i, for each i.

To define a m-dimensional cyclic code, it suffices to give a set of generators $\{f_1,\ldots,f_s\}$ for the ideal, I, of R. The corresponding ideal of $GF(q)[x_1,\ldots,x_m]$ is $J = \langle f_1,\ldots,f_s\rangle + \langle x_1^{n_1}-1,\ldots,x_m^{n_m}-1\rangle$. Pick a term order on $GF(q)[x_1,\ldots,x_m]$, and construct a Gröbner basis, $G = \{g_1,\ldots,g_t\}$ for J with respect to this term order. Now we have everything we need to determine whether a given element of R is in I.

Lemma 7. *A polynomial $h(x_1,\ldots,x_m)$ represents an element of I in R if and only if its remainder on division by G is zero.* □

One of the advantages of m-dimensional cyclic codes over generic linear codes is that their extra structure allows for a very compact representation of the encoding function. We only need to know a reduced Gröbner basis for J to perform encoding. Typically, a Gröbner basis will have fewer elements than a vectorspace basis for I, meaning that less information needs to be stored.

Monomials that are in $\langle \text{LT}(J)\rangle$ are known as **nonstandard monomials** for J. Monomials that are not in $\langle \text{LT}(J)\rangle$ are known as **standard monomials** for J.

During a systematic encoding, the **information positions** of a codeword refer to the k positions in the codeword that duplicate the components of the element of $GF(q)^k$ being encoded. These correspond to a certain subset of the coefficients in a polynomial representative for an element of R. Similarly, the parity check positions are the complementary collection of coefficients.

Theorem 8. *Let $R = GF(q)[x_1,\ldots,x_m]/\langle x_1^{n_1}-1,\ldots,x_m^{n_m}-1\rangle$, and let $I \subset R$ be a m-dimensional cyclic code. Let G be a Gröbner basis for the corresponding ideal J of $GF(q)[x_1,\ldots,x_m]$, with respect to some term order. Then there is a systematic encoding function for I constructed as follows:*

a. *The information positions are the coefficients of the nonstandard monomials for J in which each x_i appears to a power strictly less than n_i.*

b. *The parity check positions are the coefficients of the standard monomials for J.*

c. *The following algorithm gives a systematic encoder, E, for I:*

Input: G – the Gröbner basis for J;
w – a linear combination of nonstandard monomials for J.

Algorithm: $w' :=$ remainder of w after division by G.
$E(w) := w - w'$.

Output: $E(w) \in I$

Proof. The dimension of R/I as a vectorspace over $GF(q)$ is equal to the number of standard monomials for J since $R/I \cong GF(q)[x_1, \ldots, x_m]/J$. The dimension of I as a vectorspace over $GF(q)$ is equal to the difference $\dim(R) - \dim(R/I)$. But this is the same as the number of nonstandard monomials for J, in which each x_i appears to a power at most $n_i - 1$. Hence the span of those monomials is a subspace of R with the same dimension as I. Let w be a linear combination of only these nonstandard monomials. By the properties of the division algorithm, w' is a linear combination of only standard monomials, so the symbols from w are not changed in the process of computing $E(w)$. By Lemma 5, the difference $w - w'$ is an element of the ideal I, so it represents a codeword. Hence E is a systematic encoding function for I. □