Background

The algebraic structure of linear codes and, in particular, cyclic linear codes, enables efficient encoding and decoding algorithms and fast implementations.

BCH (from the names of Bose, Ray-Chaudhuri, and Hocquenghem) and **Reed-Solomon** codes are even more powerful algebraic codes. Reed-Solomon codes can be described as certain nonbinary BCH codes (they are, however, discussed separately, as Reed-Solomon codes have some interesting properties that are not found in other BCH codes).

Minimum Distance of Cyclic Codes

When constructing an arbitrary cyclic code, there is no guarantee as to the resulting minimum distance. An exhaustive computer search is often needed to find the minimum-weight codewords of a linear code and thereby the minimum distance.

BCH codes, on the other hand, take advantage of a useful result that ensures a lower bound on the minimum distance given a particular constraint on the generator polynomial. This result is known as the *BCH bound*.

The BCH Bound

Theorem 8-1. Let C be a q-ary (n, k) cyclic code with generator polynomial $g(x)$. Let m be the order of q modulo n ($\mathrm{GF}(q^m)$ is thus the smallest extension field of $\mathrm{GF}(q)$ that contains a primitive nth root of unity), and let α be a primitive nth root of unity. Select $g(x)$ to be a minimal-degree polynomial in $\mathrm{GF}(q)[x]$ such that $g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0$ for some integers $b \geq 0$ and $\delta \geq 1$ (so $g(x)$ has $\delta - 1$ consecutive powers of α as zeros). Now the code C defined by $g(x)$ has minimum distance $d_{\min} \geq \delta$.

The parameter δ in this theorem is the **design distance** of the BCH code defined by $g(x)$.

Parity Check Matrix for BCH Code

The following matrix can be used as a parity check matrix for a BCH code from Theorem 8-1:

$$\begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{b+\delta-3} & \alpha^{2(b+\delta-3)} & \cdots & \alpha^{(n-1)(b+\delta-3)} \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}.$$

(Note: The first column can be written as $\alpha^{0 \cdot b}, \alpha^{0 \cdot (b+1)}, \ldots$.)

Design Procedure for BCH Codes

To construct a t-error-correcting q-ary BCH codes of length n:

1. Find a primitive nth root of unity $\alpha \in \mathrm{GF}(q^m)$, where m is minimal.
2. Select $\delta - 1 = 2t$ consecutive powers of α, starting with α^b for some nonnegative integer b.
3. Let $g(x)$ be the least common multiple of the minimal polynomials for the selected powers of α with respect to $\mathrm{GF}(q)$. (Each of the minimal polynomials should appear only once in the product.)

Types of BCH Codes

narrow-sense BCH code with $b = 1$.

primitive BCH code with $n = q^m - 1$ for some positive integer m (the nth root of unity α is a primitive element in $\mathrm{GF}(q^m)$).

A list of the generator polynomials for binary, narrow-sense, primitive BCH codes of lengths 7 through 255 can be found in [Wic, Appendix E].

Example: Binary BCH Codes of Length 31 (1)

Let α be a root of the primitive polynomial $x^5 + x^2 + 1 \in \mathrm{GF}(2)[x]$. Then α is a primitive element in GF(32), so these BCH codes are *primitive*. The cyclotomic cosets and minimal polynomials are

$$\begin{array}{lcl}
C_0 = \{0\} & \leftrightarrow & M_0(x) = x + 1, \\
C_1 = \{1, 2, 4, 8, 16\} & \leftrightarrow & M_1(x) = x^5 + x^2 + 1, \\
C_3 = \{3, 6, 12, 24, 17\} & \leftrightarrow & M_3(x) = x^5 + x^4 + x^3 + x^2 + 1, \\
C_5 = \{5, 10, 20, 9, 18\} & \leftrightarrow & M_5(x) = x^5 + x^4 + x^2 + x + 1, \\
C_7 = \{7, 14, 28, 25, 19\} & \leftrightarrow & M_7(x) = x^5 + x^3 + x^2 + x + 1, \\
C_{11} = \{11, 22, 13, 26, 21\} & \leftrightarrow & M_{11}(x) = x^5 + x^4 + x^3 + x + 1, \\
C_{15} = \{15, 30, 29, 27, 23\} & \leftrightarrow & M_{15}(x) = x^5 + x^3 + 1.
\end{array}$$

Example: Binary BCH Codes of Length 31 (2)

A narrow-sense one-error-correcting code: Now $b = 1$ and $\delta = 3$, so $g(x)$ must have α and α^2 as zeros. The minimal polynomial of both α and α^2 is $M_1(x)$, so the generator polynomial is

$$g(x) = \mathrm{LCM}(M_1(x), M_2(x)) = M_1(x) = M_2(x) = x^5 + x^2 + 1.$$

Since $\deg(g(x)) = 5$, the dimension of the code is $31 - 5 = 26$, so $g(x)$ defines a $(31, 26)$ binary single-error-correcting BCH code.

Example: Binary BCH Codes of Length 31 (3)

A parity check matrix for the constructed code has the following general form:

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{29} & \alpha^{30} \\ 1 & \alpha^2 & \cdots & \alpha^{27} & \alpha^{29} \end{bmatrix}.$$

Since any binary polynomial having α as a zero must also have the other conjugates as zeros (including α^2), the matrix has redundant rows, so the second row may be deleted.

Note: This code is the binary Hamming code of length 31.

Example: Binary BCH Codes of Length 31 (4)

A narrow-sense two-error-correcting code: Now $b = 1$ and $\delta = 5$, so $g(x)$ must have α, α^2, α^3, and α^4 as zeros. The generator polynomial is

$$\begin{aligned} g(x) &= \mathrm{LCM}(M_1(x), M_2(x), M_3(x), M_4(x)) = M_1(x)M_3(x) \\ &= (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1. \end{aligned}$$

Since $\deg(g(x)) = 10$, the dimension of the code is $31 - 10 = 21$, so $g(x)$ defines a $(31, 21)$ binary double-error-correcting BCH code.

BCH Codes: Some Remarks

- ▷ The true minimum distance may be larger than the design distance.
- ▷ We want to maximize the dimension (and therefore the rate) with a given minimum distance. Therefore, it is sometimes worth considering codes that are not narrow-sense ($b > 1$).
- ▷ The weight distributions for most BCH codes are not known.
- ▷ The weight distributions for all double- and triple-error-correcting binary primitive BCH codes have been found.

Reed-Solomon Codes

Some trends:

1. For a fixed alphabet GF(q), the cardinality of the cyclotomic cosets modulo n is generally smaller for primitive codes ($n = q^m - 1$).
2. Large alphabets generally lead to smaller cyclotomic cosets.

BCH codes of length $n = q - 1$ over GF(q) are called **Reed-Solomon codes**.

Constructing Reed-Solomon Codes

We want to construct a t-error-correcting code of length $q-1$ over GF(q).

1. By Theorem 2-12, there exists a required primitive $(q-1)$th root of unity α in GF(q).

2. We want to construct the cyclotomic cosets modulo $q-1$ with respect to GF(q). Since $q \equiv 1 \pmod{q-1}$, we have $aq^s \equiv a \pmod{q-1}$, so all cyclotomic cosets have one element $\{a\}$ and the associated minimal polynomials are of the form $x - \alpha^a$.

The generator polynomial of a t-error correcting code is then

$$g(x) = (x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+2t-1}).$$

Example: Reed-Solomon Code over GF(8) (1)

Let α be a root of the primitive binary polynomial x^3+x+1 and therefore a primitive 7th root of unity. (The elements of GF(8) are then 0, 1, α, α^2, $\alpha^3 = \alpha+1$, $\alpha^4 = \alpha^2+\alpha$, $\alpha^5 = \alpha^2+\alpha+1$, and $\alpha^6 = \alpha^2+1$.)

We construct a 2-error-correcting code. Then $2t = 4$, and a narrow-sense generator polynomial is

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3.$$

Example: Reed-Solomon Code over GF(8) (2)

Since the generator polynomial has degree 4, we have a $(7,3)$ code over GF(8) and the following parity check matrix:

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{bmatrix}.$$

Minimum Distance of Reed-Solomon Codes

As the following theorem shows, we know the minimum distance of Reed-Solomon codes!

Theorem 8-2. An (n,k) Reed-Solomon code has minimum distance $n-k+1$.

Proof: Since the generator polynomial $g(x)$ is the product of $\delta-1$ minimal polynomials of the form $x-\alpha^a$, its degree is $\delta-1$. As we also know that the degree of $g(x)$ is $n-k$, we get that the minimum distance is at least $\delta = n-k+1$. The result now follows, since by the Singleton bound (Theorem 4-10), the minimum distance is at most $n-k+1$. □

Maximum Distance Separable Codes

An (n, k) code that satisfies the Singleton bound with equality is called **maximum distance separable (MDS)**. MDS codes have a number of interesting properties.

- ▷ If C is MDS, so is its dual $C^{\perp}$.
- ▷ Any combination of k coordinates in an MDS code may be used as message coordinates in a systematic representation.
- ▷ The weight distribution of MDS codes is known, see [Wic, Theorem 8-5].
- ▷ Punctured and shortened MDS codes are MDS.

Decoding BCH and Reed-Solomon Codes

The first explicit decoding algorithm for binary BCH codes was described by Peterson in 1960. Peterson's algorithm is useful only for correcting small numbers of errors.

Berlekamp introduced the first truly efficient decoding algorithm for both binary and nonbinary BCH codes in 1967. This was further developed by Massey and is usually called the *Berlekamp-Massey decoding algorithm*.

These and other decoding algorithms for BCH codes are considered in [Wic, Ch. 9].