

The definition of BCH and RS codes

Definition. A **primitive n th root of unity** is a root of $x^n - 1$ that has multiplicative order n .

Example. Over the real numbers the 6th roots of unity are $\pm 1, \pm \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. A cyclic group of order 6 has 2 generators, so there are 2 primitive 6th roots of unity: $\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Note that $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ are primitive third roots of unity.

If β is a primitive n th root of unity over the field $\text{GF}(q)$, then β may or may not belong to $\text{GF}(q)$. If $\beta \in \text{GF}(q)$, then since it has order n its powers give n distinct roots of $x^n - 1$. Therefore in this case $x^n - 1$ factors over $\text{GF}(q)$ as $x^n - 1 = (x - 1)(x - \beta)(x - \beta^2) \cdots (x - \beta^{n-1})$. This happens, for instance, if β is an element of order $p - 1$ in \mathbf{Z}_p .

If $x^n - 1$ does not split in $\text{GF}(q)[x]$, then to actually get our hands on a primitive n th root of unity we need to construct an extension field of $\text{GF}(q)$ that is a splitting field for $x^n - 1$. More generally, we could use any extension $\text{GF}(q^m)$ in which $x^n - 1$ splits. Because we then have all roots of $x^n - 1$ within the field, it follows that $x^n - 1$ must be a factor of the polynomial $x^{q^m} - x$, for which $\text{GF}(q^m)$ is a splitting field over $\text{GF}(q)$.

Example. Over $\text{GF}(2) = \mathbf{Z}_2$, consider $\text{GF}(2^4) = \mathbf{Z}_2[x]/\langle x^4 + x + 1 \rangle$. If we let $\beta = [x]$, then β is a primitive 15th root of unity. A cyclic group of order 15 has $\varphi(15) = 8$ generators. The generators for $\langle \beta \rangle$ are $\beta, \beta^2, \beta^4 = \beta + 1, \beta^7 = \beta^3 + \beta + 1, \beta^8 = \beta^2 + 1, \beta^{11} = \beta^3 + \beta^2 + \beta, \beta^{13} = \beta^3 + \beta^2 + 1$, and $\beta^{14} = \beta^3 + 1$. The minimal polynomial for β over \mathbf{Z}_2 is $x^4 + x + 1$, while the minimal polynomial for β over $\text{GF}(16)$ is just $x - \beta$.

Definition. A cyclic code of length n over $\text{GF}(q)$ is called a **BCH code of designed distance δ** if its generator polynomial $g(x) \in \text{GF}(q)[x]$ is the least common multiple of the minimal polynomials of $\beta^\ell, \beta^{\ell+1}, \dots, \beta^{\ell+\delta-2}$, where β is a primitive n th root of unity.

Definition. If $n = q - 1$ in the definition of a BCH code, then it is called an **RS code of designed distance δ** .

If $\ell = 1$ in the definition of a BCH code, then it is called a *narrow-sense* BCH code. If $n = q^m - 1$, then the code is called a *primitive* BCH code (since this means that β is a primitive element of $\text{GF}(q^m)$).

The construction of BCH codes

These codes are cyclic codes, so the construction involves finding an ideal $\langle [g(x)] \rangle$ in $F[x]/\langle x^n - 1 \rangle$, for some finite field F . Given $g(x)$, we already know how to find a generator matrix and a parity check matrix for the code. We now outline how to construct a BCH code with designed distance δ .

1. Choose a finite field $\text{GF}(q)$ as the alphabet for the code.

Remember that $\text{GF}(q)$ has characteristic p for some prime p , so $q = p^s$ for some positive integer s , and all polynomials will have coefficients from this field.

2. Choose integers n and m for which $x^n - 1$ is a factor of $x^{q^m} - x$.

One way to do this is to start with any n not divisible by p . Then $\text{gcd}(q, n) = 1$, so we can find the order m of q in \mathbf{Z}_n^\times . Then $q^m \equiv 1 \pmod{n}$, so $n \mid q^m - 1$, which guarantees that $x^n - 1$ is a factor of $x^{q^m - 1} - 1$ (and that $x^n - 1$ is a factor of $x^{q^m} - x$). This means that we can find the irreducible factors of $x^n - 1$ over $\text{GF}(q)$ by using the irreducible factors of $x^{q^m} - x$. From our general theory, the factors of $x^n - 1$ will be some of the irreducible polynomials over $\text{GF}(q)$ whose degree is a divisor of m .

3. Let β be a primitive n th root of unity in $\text{GF}(q^m)$.

We know that $\text{GF}(q^m)$ contains all roots of $x^n - 1$ since it is a factor of $x^{q^m} - x$, and then these roots form a subgroup of order n which must be cyclic. Therefore $\text{GF}(q^m)$ will actually contain $\varphi(n)$ primitive n th roots of unity.

4. Choose $\delta - 1$ consecutive powers of β , say $\beta^\ell, \beta^{\ell+1}, \dots, \beta^{\ell+\delta-2}$.

5. The BCH code we want is the ideal of $\text{GF}(q)[x]/\langle x^n - 1 \rangle$ consisting of all polynomials that have the consecutive powers of β as roots.

The generating polynomial for this ideal is the least common multiple of the minimal polynomials of $\beta^\ell, \beta^{\ell+1}, \dots, \beta^{\ell+\delta-2}$.

The construction of RS codes

1. Choose a finite field $\text{GF}(q)$ as the alphabet for the code.

2. Choose $n = q - 1$.

3. Let β be a primitive element of $\text{GF}(q)$.

Since $\text{GF}(q)$ consists of the roots of $x^q - x$, a primitive n th root of unity is just a generator of the multiplicative group of $\text{GF}(q)$.

4. Choose $\delta - 1$ consecutive powers of β , say $\beta^\ell, \beta^{\ell+1}, \dots, \beta^{\ell+\delta-2}$.

5. Since each β^i belongs to $\text{GF}(q)$, its minimal polynomial is $x - \beta^i$, and therefore the generator polynomial is $(x - \beta^\ell)(x - \beta^{\ell+1}) \dots (x - \beta^{\ell+\delta-2})$.

Note that this polynomial has coefficients in $\text{GF}(q)$, not in \mathbf{Z}_p .

Examples

The RS codes are easier to construct, but in order to increase the length of the code you must increase the size of the alphabet. With the BCH codes you can increase the length of the code by finding a primitive root of higher order.

In both cases, although we can create codes that correct more and more errors, what is important is the ratio of the number of errors corrected to the size of the code. As the number of corrected errors is increased, the block size goes up too fast, and the relative error correction goes to 0. Despite being used in many engineering applications, from a theoretical point of view the Hamming, RS, and BCH codes are limited successes.

One of the reasons for using them is that it is possible to determine the minimum distance of a code by checking the number of the columns of its parity check matrix that are linearly independent. This is where Vandermonde determinants play a crucial role, allowing us to construct a code that is guaranteed to have a minimum distance at least δ .

Example 4.1.4. (from the text) To define an RS code over \mathbf{Z}_7 with designed distance 4, choose the generator 3 and use three consecutive powers of 3. The generator polynomial $g(x) = (x - 3)(x - 3^2)(x - 3^3) = (x - 3)(x - 2)(x - 6)$ defines a $[6, 3, 4]$ cyclic code.

To increase the minimum distance by 1, we need to add another factor. Then $(x - 3)(x - 3^2)(x - 3^3)(x - 3^4) = (x - 3)(x - 2)(x - 6)(x - 4)$ generates a $[6, 2, 5]$ code.

Example 4.3.7. (from the text) To construct an RS code over $\text{GF}(8)$ that corrects ≤ 2 errors, we need a minimum distance of 5. Use $\text{GF}(8) = \mathbf{Z}_2[x]/\langle x^3 + x + 1 \rangle$, and let $\beta = [x]$, which is a primitive element for the field. We can use the successive powers β, β^2, β^3 , and β^4 , to define the polynomial

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

It is important to remember that this polynomial has coefficients in $\text{GF}(8)$, not in \mathbf{Z}_2 . The calculation in the text has $g(x) = x^4 + \beta^3 x^3 + x^2 + \beta x + \beta^3$.

Example. We will construct a BCH code of length 7 over \mathbf{Z}_2 with designed distance 3. The first question is whether 7 is a possible length of a BCH code. The answer is yes, because $x^7 - 1$ is a factor of $x^8 - x$, which defines $\text{GF}(8)$. Choose α as a primitive 7th root of unity (from the table on page 54 of the text) and use the successive powers α and α^2 . These powers both have minimal polynomial $x^3 + x + 1$, so the generating polynomial is $g(x) = x^3 + x + 1$ and we get the familiar Hamming $[7, 4, 3]$ code.

If we decide to pick α^2 and α^3 , then we have two different minimal polynomials, so $g(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. This produces the $[7, 1, 7]$ binary repetition code. We could have constructed this code by choosing all 6 of the consecutive nontrivial powers of α , and this is consistent with the general theory which guarantees a minimum distance of 7.

Example 4.3.4. (from the text) We can construct a binary BCH code of length 31 since $x^{31} - 1$ is a factor of $x^{32} - x$, the defining polynomial for $\text{GF}(32)$. In order for the code to correct ≤ 1 error, we need a minimum distance of 3, so we need to define the code using 2 consecutive powers of an element of order 31.

From the table on page 57 you can check that the choice α, α^2 corresponds to the polynomial $x^5 + x^2 + 1$, and α^9, α^{10} yields $x^5 + x^4 + x^2 + x + 1$, while α^{21}, α^{22} produces $x^5 + x^4 + x^3 + x + 1$, and the choice of α^{29}, α^{30} corresponds to $x^5 + x^3 + 1$.

To increase the minimum distance by choosing 3 consecutive powers requires either two or three minimal polynomials. For example, choosing $\alpha^3, \alpha^4, \alpha^5$ requires three different minimal polynomials, and produces a $[31, 16]$ code. The choice of $\alpha, \alpha^2, \alpha^3$ (as in the text) requires only two different minimal polynomials, and so this leads to a $[31, 21]$ BCH code.

Example. As the table for $\text{GF}(16)$ shows, the polynomial $x^5 - 1$ is a factor of $x^{16} - x$. That makes it possible to define a binary BCH code of length 5. Choose $\beta = u^3$ as a primitive 5th root of unity (the splitting field for $x^5 - 1$ over \mathbf{Z}_2 is $\text{GF}(16)$). The corresponding minimal polynomial is $x^4 + x^3 + x^2 + x + 1$, so we just get the binary $[5, 1]$ repetition code.

GF(16)

Construct GF(16) as $\mathbf{Z}_2[x]/\langle x^4 + x + 1 \rangle$. Let $u = [x]$, so that we have the relation $u^4 = 1 + u$. Thus u is a root of $x^4 + x + 1$, as are u^2, u^4 , and u^8 .

We know that GF(16) consists of the roots of $x^{16} - x$, which factors over \mathbf{Z}_2 as the product of all irreducible polynomials of degrees 1, 2, and 4 (the divisors of the exponent in $16 = 2^4$). We have already found these polynomials, so we can write

$$x^{16} - x = x(x-1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

We next show that u is a generator of the multiplicative group, and then list the elements of GF(16) as powers of u .

u	1		1
u^2		u	
u^3	1	$+u$	$= u^4$
$u^4 = 1 + u$		u^2	$= u^2$
$u^5 = u + u^2$	1	$+u^2$	$= u^8$
$u^6 = u^2 + u^3$		$u + u^2$	$= u^5$
$u^7 = u^3 + u^4 = 1 + u + u^3$	1	$+u + u^2$	$= u^{10}$
$u^8 = u + u^2 + u^4 = 1 + u^2$		u^3	$= u^3$
$u^9 = u + u^3$	1	$+u^3$	$= u^{14}$
$u^{10} = u^2 + u^4 = 1 + u + u^2$		$u + u^3$	$= u^9$
$u^{11} = u + u^2 + u^3$	1	$+u + u^3$	$= u^7$
$u^{12} = u^2 + u^3 + u^4 = 1 + u + u^2 + u^3$		$u^2 + u^3$	$= u^6$
$u^{13} = u + u^2 + u^3 + u^4 = 1 + u^2 + u^3$	1	$+u^2 + u^3$	$= u^{13}$
$u^{14} = u + u^3 + u^4 = 1 + u^3$		$u + u^2 + u^3$	$= u^{11}$
$u^{15} = u + u^4 = 1$	1	$+u + u^2 + u^3$	$= u^{12}$

The polynomial $x^3 - 1 = (x - 1)(x^2 + x + 1)$ is a factor of $x^{15} - 1$, so the two elements u^5 and u^{10} of order 3, which are roots of $x^3 - 1$, must be roots of $x^2 + x + 1$.

The polynomial $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ is also a factor of $x^{15} - 1$, so the elements u^3, u^6, u^9, u^{12} of order 5, which are roots of $x^5 - 1$, must be roots of $x^4 + x^3 + x^2 + x + 1$.

By process of elimination, the remaining powers of u , consisting of the generators $u^7, u^{11}, u^{13}, u^{14}$ must be roots of $x^4 + x^3 + 1$.

The generators u, u^2, u^4, u^8 and $u^7, u^{11}, u^{13}, u^{14}$ have as minimal polynomial $x^4 + x + 1$ and $x^4 + x^3 + 1$, respectively.

If r is a root of $f(x)$, then $r + 1$ is a root of $f(x - 1)$ since $f((r + 1) - 1) = f(r) = 0$. The automorphism $\theta(f(x)) = f(x - 1)$ leaves $x^4 + x + 1$ invariant, but permutes $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$. You can check that if α is a root of $x^4 + x + 1$, then so is $\alpha + 1$. On the other hand, if α is a root of $x^4 + x^3 + 1$, then $\alpha + 1$ is a root of $x^4 + x^3 + x^2 + x + 1$, and vice versa. This lets you check the calculations.

GF(9)

Construct GF(9) as $\mathbf{Z}_3[x]/\langle x^2 + 1 \rangle$. Let $i = [x]$, so that we have the relation $i^2 = -1$, where $\mathbf{Z}_3 = \{0, \pm 1\}$. Because GF(9) has characteristic 3, if a is a root of a polynomial $f(x)$, then so is a^3 . Thus $i^3 = -i$ is also a root of $x^2 + 1$.

We know that GF(9) consists of the roots of $x^9 - x$, which factors over \mathbf{Z}_3 as the product of all irreducible polynomials of degrees 1 and 2. Working from a list of all quadratic polynomials over \mathbf{Z}_3 , it is not difficult to check that the ones with no roots (and therefore irreducible) are $x^2 + 1$, $x^2 + x - 1$, and $x^2 - x - 1$. Therefore we have the factorization

$$x^9 - x = x(x - 1)(x + 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1).$$

Since $i^2 = -1$ we have $i^4 = 1$, and so i has order 4 and is *not* a generator of the multiplicative group of GF(9). We next show that $1 + i$ is a generator of the multiplicative group, and then list the elements of GF(9) as powers of $1 + i$.

$1 + i$	1	1
$(1 + i)^2 = 1 + 2i + i^2 = -i$	-1	$= (1 + i)^4$
$(1 + i)^3 = (1 + i)(-i) = -i - i^2 = 1 - i$	i	$= (1 + i)^6$
$(1 + i)^4 = (1 + i)(1 - i) = 1 - i^2 = -1$	$1 + i$	$= (1 + i)^1$
$(1 + i)^5 = (1 + i)(-1) = -1 - i$	$-1 + i$	$= (1 + i)^7$
$(1 + i)^6 = (1 + i)^2(-1) = i$	$-i$	$= (1 + i)^2$
$(1 + i)^7 = (1 + i)^3(-1) = -1 + i$	$1 - i$	$= (1 + i)^3$
$(1 + i)^8 = (1 + i)^4(-1) = 1$	$-1 - i$	$= (1 + i)^5$

Since the characteristic is 3, it is possible to use the quadratic formula. In this case $\frac{1}{2} = (2)^{-1} = (-1)^{-1} = -1$. The roots of $ax^2 + bx + c$ are therefore $x = b \pm \sqrt{b^2 - ac}$.

Elements	Minimal polynomial
$\pm i$	$x^2 + 1$
$1 \pm i$	$x^2 + x - 1$
$-1 \pm i$	$x^2 - x - 1$

If r is a root of $f(x)$, then $r + 1$ is a root of $f(x - 1)$ since $f((r + 1) - 1) = f(r) = 0$. We can check the minimal polynomials by observing that if we define $\theta(f(x)) = f(x - 1)$, then $\theta(x^2 + 1) = x^2 + x - 1$, $\theta(x^2 + x - 1) = x^2 - x - 1$, and $\theta(x^2 - x - 1) = x^2 + 1$. Adding 1 to the roots of $x^2 + 1$ does in fact give us the roots of $x^2 + x - 1$, etc.

The Golay codes

Over \mathbf{Z}_2 it can be shown that

$$x^{23} - 1 = (x - 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1).$$

We can use $g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$ as the generating polynomial for a $[23, 12]$ cyclic code. Note that the other 11-degree factor of $x^{23} - 1$ will generate an equivalent code.

This code is called the **binary Golay code**, and is denoted by G_{23} . Since $g(x)$ has 7 nonzero terms, the code has minimum distance ≤ 7 . It can be proved that G_{23} actually has minimum distance 7, so it is a $[23, 12, 7]$ cyclic code and can correct ≤ 3 errors.

Over \mathbf{Z}_3 , $x^{11} - 1 = (x - 1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x + 1)$. We can use $g(x) = x^5 + x^4 - x^3 + x^2 - 1$ as the generating polynomial for an $[11, 6]$ cyclic code over \mathbf{Z}_3 . The other factor of degree 5 generates an equivalent code.

This code is called the **ternary Golay code**, denoted by G_{11} . It takes some work to show that G_{11} is an $[11, 6, 5]$ code, but then it can correct ≤ 2 errors.

Proposition. G_{23} and G_{11} are perfect codes.

Proof. We have the following calculations.

$$\begin{aligned} 1 + 23 + \binom{23}{2} + \binom{23}{3} &= 1 + 23 + 253 + 1771 = 2048 = 2^{11} \\ 2^{12} \left(1 + 23 + \binom{23}{2} + \binom{23}{3} \right) &= 2^{23} \\ 1 + 11 \cdot 2 + \binom{11}{2} \cdot 2^2 &= 1 + 22 + 220 = 241 = 3^5 \\ 3^6 \left(1 + 11 \cdot 2 + \binom{11}{2} \cdot 2^2 \right) &= 3^{11} \end{aligned}$$

The calculations show that for both codes the sphere packing bound is satisfied exactly. \square

If n is odd, then the binary repetition code of length n is a perfect code that corrects $\leq (n - 1)/2$ errors. On the other hand, the binary code of length n consisting of all of \mathbf{Z}_2^n is a perfect code with minimum distance 1 that corrects 0 errors. These are called the trivial perfect codes.

Theorem. The only nontrivial perfect codes are the Hamming codes and the two Golay codes.