

# Minimal generators for BCH codes

Jacob M. Farinholt\*      Keith E. Mellinger

October 14, 2009

## Abstract

We look at the construction of a particular subclass of cyclic codes known as the Bose-Chaudhuri-Hocquenghem (BCH) Codes. These codes are constructed with a prescribed minimum distance, which means that the codes can be designed to correct as many errors as are required for the intended application. Our goal is to construct classes of BCH codes in as simple a fashion as possible by using minimal sets of generators. An elementary upper bound on the number of generators necessary for our construction is fairly easy to obtain. Our main result shows that for sufficiently large length, the upper bound is actually sharp. Along the way, we provide a host of results on the structure of cyclotomic cosets, along with an introduction to algebraic coding theory.

## 1 Introduction to algebraic coding theory

In an age where reliance on communication systems is ever more rapidly growing, it is everyday becoming more necessary to develop methods to communicate more effectively. Suppose two individuals, Alice and Bob, are trying to communicate. When Alice sends Bob a message, the message is first converted into binary  $n$ -tuples, that is, binary “codewords” of length  $n$ , then transmitted to Bob, who then translates the codewords into the original message. During the transmission process, however, these codewords can be affected by outside elements that can flip certain bits of a codeword from zeros to ones and vice versa. In turn, the message that Bob receives is often different from the message that Alice sent. Rather than leaving Bob to guess what the message should have said, if the codewords are designed and chosen carefully, the errors can in fact be detected and corrected. The goal of algebraic coding theory is to use algebraic methods to design codes that detect and correct their own errors. We start by briefly looking at the relevant definitions and connections to ring theory, and we refer the interested reader to the introductory book by Pless [5] for more details.

By definition, a binary linear code,  $\mathcal{C}$ , is a collection of vectors that forms a subspace of the vector space  $V$  of all binary  $n$ -tuples. In this space, addition is defined component wise modulo 2. We define the (Hamming) distance between two vectors to be the number

---

\*The author acknowledges support by an Undergraduate Research Grant from the University of Mary Washington.

of coordinates in which they differ. The minimum weight, or minimum distance, of a code is the smallest distance between any two distinct codewords. If  $d$  is the minimum weight of a code  $\mathcal{C}$ , then  $\mathcal{C}$  can correct  $t = \lfloor \frac{d-1}{2} \rfloor$  or fewer errors, and conversely, under the decoding technique known as maximum likelihood decoding.

Rather than viewing a codeword as a vector in a vector space, we can instead view it as an element of a polynomial ring. We do this by treating each vector as the collection of coefficients of a polynomial. In other words, the vector  $(a_k \ a_{k-1} \ \dots \ a_1 \ a_0)$  represents the polynomial  $a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$ . Since the degrees of these polynomials cannot exceed the length of the vectors, we only consider those in the ring  $F[x]/f(x)$ , where  $F = GF(2)$  (the finite field with two elements, 0 and 1) and  $f(x)$  is some polynomial.

Multiplying by  $x$  results in a shifting of each of the coefficients. When every cyclic shift is also another codeword, we call the collection of all codewords a *cyclic code*. In other words, cyclic codes have the property that for any codeword  $(a_0 \ a_1 \ \dots \ a_{k-1} \ a_k)$ , the vector  $(a_k \ a_0 \ a_1 \ \dots \ a_{k-1})$  is also a codeword. For our purposes, we will consider the ring  $F[x]/(x^N - 1)$ , where  $N$  is some positive integer corresponding to the length of the code. Note that we use  $N$  for the length, rather than the more typical  $n$  which will be used later. Using this model, a set of elements  $S$  in  $F[x]/(x^N - 1)$  corresponds to a cyclic code  $\mathcal{C}$  if and only if  $S$  is an ideal in  $F[x]/(x^N - 1)$ . Moreover, if we let  $\mathcal{C}$  be an ideal in  $F[x]/(x^N - 1)$ , and let  $g(x)$  be the monic polynomial of smallest degree in  $\mathcal{C}$ , then  $g(x)$  is uniquely determined and  $\mathcal{C} = \langle g(x) \rangle$ .

The above result is more about algebra than it is about coding theory. It allows us to work with the algebra directly as it completely represents the code. In short, cyclic codes are extremely useful for several reasons. First, their implementation (through the use of a shift register) requires no storage making them attractive from a practical standpoint. Second, they are equivalent to ideals in  $F[x]/(x^N - 1)$  and can thus be studied from a purely algebraic perspective.

## 2 BCH codes and results

Suppose there is a situation in which it is necessary to have a code that can correct a certain number of errors. An example of such a situation is in the coding of a compact disk. It is very easy for CDs to acquire marks, fingerprints, and scratches, all of which cause errors, or noise, when the disk is being read. In such a case, it is naturally desirable to have some code that can correct a large number of concentrated errors. Another example is found in deep space transmission, where it can take months for a single message to be received. In a situation like this, it is clearly desirable to have a code that can correct a very large number of errors without the need to retransmit any information. In order to correct a specified number of errors, this code must have a certain minimum distance,  $\delta$ . We run into a problem here. In general, determining the minimum distance of a code is an NP-hard problem. However, there is a special subclass of cyclic codes discovered by R. C. Bose and D. K. Ray Chaudhuri [1] in 1960, and independently by A. Hocquenghem [3] in 1959 that provides a solution to that problem. Rather than trying to determine the minimum distance of an already constructed code, this subclass of codes, called BCH codes, can be constructed for any prescribed minimum distance. We say that a code  $\mathcal{C}$  is a BCH code of

designed distance  $\delta$  if  $g(x)$ , the generator polynomial of  $\mathcal{C}$ , is the product of distinct minimal polynomials whose roots contain  $\delta - 1$  consecutive roots of  $x^N - 1$ ; say  $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ , where the powers of  $\alpha$  give all roots of  $x^N - 1$ .

## 2.1 The BCH construction

To construct a binary BCH code  $\mathcal{C}$  of prescribed distance  $\delta$ , first consider the roots of  $x^N - 1$  for some integer  $N \geq \delta$ , where  $x^N - 1$  is considered as a polynomial with coefficients in  $GF(2)$ . This collection of roots forms a cyclic subgroup of the multiplicative group of  $GF(2^m)$  for some  $m$ . It is known that such a field exists, so we choose  $m$  such that  $GF(2^m)$  is the smallest such field. Since the collection of roots is cyclic, all of the roots are generated by a particular root,  $\alpha$ , which we call the *primitive  $N^{\text{th}}$  root of unity*. All of the other roots will simply be powers of  $\alpha$ . Since  $\mathcal{C}$  is a cyclic code, it is an ideal in  $F[x]/(x^N - 1)$  with generator polynomial  $g(x)$ . Notice that  $g(x)$  divides  $x^N - 1$ . It follows that all of the roots of  $g(x)$  will also be roots of  $x^N - 1$ .

We now present a result about the minimum distance of a BCH code.

**Theorem 1** *The minimum weight of a BCH code of designed distance  $\delta$  is at least  $\delta$ .*

We avoid giving a complete proof of this important result. What the theorem tells us is that if the roots of  $g(x)$  contain  $\delta - 1$  consecutive roots of  $x^N - 1$ , then  $\mathcal{C}$  will have a minimum distance of at least  $\delta$ . This is important, since it then follows that a BCH code of designed distance  $\delta$  can correct at least  $t = \lfloor \frac{\delta-1}{2} \rfloor$  errors. Notice that if  $\delta$  is odd, then  $\delta$  and  $\delta + 1$  will both correct at least  $t$  errors. For the sake of simplicity, we will always assume that  $\delta$  is odd. We now see that in order to construct  $\mathcal{C}$  so that it can correct  $t$  errors, we simply choose monic irreducible polynomials that have at least  $\delta - 1$  consecutive roots, and let their product be the generator polynomial for  $\mathcal{C}$ . While the BCH construction works for any  $N$ , we will restrict our attention to the case where  $N$  is of the form  $2^n - 1$ . This gives us more structure since there exist finite fields of size  $2^n$  for any  $n$ . In general, if  $N = q^m - 1$  for some prime power  $q$ , then the code is called a *primitive BCH code*.

## 2.2 Minimizing irreducible factors

It is important to note that the  $\delta - 1$  consecutive roots necessary to generate a BCH code need not start with  $\alpha$ . We can construct any such code with a sequence of the form  $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$  for some  $b$ . It is very rare that a collection of monic irreducible polynomials in the ring  $F[x]/(x^N - 1)$  will produce only the  $\delta - 1$  consecutive roots. For example, suppose you want a BCH code of designed distance  $\delta = 7$ . In the field  $F[x]/(x^{15} - 1)$ , where  $F = GF(2)$ , there are the following minimal polynomials:  $(x^4 + x^3 + 1)$ ,  $(x^4 + x + 1)$ ,  $(x^4 + x^3 + x^2 + x + 1)$ ,  $(x^2 + x + 1)$ , and  $(x + 1)$ . Since all the roots of  $x^{15} - 1$  form the multiplicative cyclic group of  $GF(16)$ , choose the smallest root of all of the monic irreducible polynomials listed, that is, the primitive  $N^{\text{th}}$  root of unity, to be  $\alpha$ . All the remaining roots will be powers of  $\alpha$ . The monic irreducible polynomials and their roots, as powers of  $\alpha$ , are enumerated in Table 1.

<u>Monic irreducible polynomials</u>	<u>Roots as powers of <math>\alpha</math></u>
$x^4 + x^3 + 1$	$\alpha, \alpha^2, \alpha^4, \alpha^8$
$x^4 + x + 1$	$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$
$x^4 + x^3 + x^2 + x + 1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$
$x^2 + x + 1$	$\alpha^5, \alpha^{10}$
$x + 1$	1

Table 1: monic irreducible polynomials and their roots

By looking at Table 1, we can determine that  $(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$  will have the roots  $\alpha, \alpha^2, \dots, \alpha^6$ , giving us a generator polynomial that will produce a BCH code of designed distance  $\delta = 7$ . Notice that in addition to those roots, the generator polynomial also contains the roots  $\alpha^8, \alpha^9, \alpha^{10}$ , and  $\alpha^{12}$ . Since these roots are not consecutive, they will not necessarily affect the minimum distance of the code and can thus be ignored.

In this example we see that starting with the root  $\alpha$ , it takes three monic irreducible polynomials in  $F[x]/(x^{15} - 1)$  to generate the desired BCH code. If we look at a different polynomial ring, however, we may not necessarily obtain the same result. In other words, suppose we are trying to obtain the  $\delta - 1 = 6$  consecutive roots  $\alpha, \alpha^2, \dots, \alpha^6$  of the polynomial  $x^N - 1$  for some  $N \neq 15$ . Then we will be looking for monic irreducible polynomials in  $F[x]/(x^N - 1)$  that divide  $x^N - 1$  and whose collective roots contain  $\alpha, \alpha^2, \dots, \alpha^6$ . Naturally, we will have a different set of monic irreducible divisors, and, depending on the value of  $N$ , fewer of them may be necessary in order to generate the desired BCH code.

Our work is motivated by the following problem. For various values of  $N$  we would like to determine the fewest number of monic irreducible polynomials necessary to produce a BCH code of a designed distance  $\delta$ . Our motivation is primarily drawn from an algebraic perspective, since few generators would result in a much more simplistic algebraic representation of our code. It is unclear whether a small number of generators would have a significant impact from the coding theoretic perspective. Fewer generators could mean that the codewords could be generated more quickly, but again it is not clear that this would be of any significant advantage from the coding perspective. In order to investigate our motivating question, we must first discuss cyclotomic cosets and their relationship to minimal polynomials.

By definition, a cyclotomic coset is a collection of integers of the form  $\{s, ps, p^2s, \dots, p^r s\}$  where each  $p^i s$  is reduced modulo  $(p^n - 1)$  for some prime  $p$  and some integer  $n$ . In this collection,  $s$  is some positive integer, and  $r$  the smallest positive integer such that  $p^{r+1}s \equiv s \pmod{p^n - 1}$ . We will only be focusing on the case where  $p = 2$ . A cyclotomic coset can then be equivalently described as the collection of elements  $m$  that satisfy

$$m \equiv s \cdot 2^k \pmod{2^n - 1}$$

for all nonnegative integers  $k$ , where  $s$  and  $n$  are some positive integers. All the cyclotomic cosets that satisfy this for a particular  $N = 2^n - 1$  are called the *cyclotomic cosets of  $N$* . Notice that  $s$  is a solution to the above congruence. If  $s$  is the smallest such solution for a given  $N$ , we say that the set of solutions to this congruence is the *cyclotomic coset of  $N$  generated by  $s$* , denoted  $C_s$ . For example, let  $n = 4$  so that  $2^n - 1 = 15$ . In this case the cyclotomic coset of 4 generated by 3 is  $\{3, 6, 12, 9\}$ . We can easily calculate the other four cyclotomic cosets in this example:  $\{1, 2, 4, 8\}$ ,  $\{5, 10\}$ ,  $\{7, 14, 13, 11\}$ , and  $\{0\}$ .

What makes these cyclotomic cosets so important to BCH codes is the following property (which is stated as Theorem 44 in [5]). Let  $\alpha$  be a root of  $x^N - 1$  in the smallest finite field  $F$  of characteristic  $p$  that contains  $\alpha$  and let  $m(x)$  be its minimal polynomial. Let  $\beta$  be a primitive  $N$ th root of unity in  $F$ , and let  $\alpha = \beta^s$ . If  $u$  is the smallest element in the cyclotomic coset of  $N$  containing  $s$ , then  $m(x) = \prod_{i \in C_u} (x - \beta^i)$ .

What this says is that the degree of a minimal polynomial  $m(x)$  is the size of a cyclotomic coset. All the elements in the coset correspond to powers of the primitive  $N$ th root of unity that are roots of  $m(x)$ . Recall from our previous example that in the field  $F[x]/(x^{15} - 1)$  there are five minimal polynomials that contain all 15 primitive roots of  $x^{15} - 1$ . In that example, the minimal divisors of  $x^{15} - 1$  were calculated, and then their roots were given in Table 1. From that table, we could determine the number of minimal polynomials necessary to generate a BCH code of prescribed distance  $\delta = 7$ . We now see that we can determine this answer in a much easier manner. If we consider the cyclotomic cosets modulo  $15 = 2^4 - 1$ , we find that there are three that collectively contain the powers 1 through 6. It follows that there must be three minimal polynomials that produce the roots  $\alpha, \alpha^2, \dots, \alpha^6$ . The product of these three minimal polynomials will be the generator polynomial for the code. The same generator polynomial will also produce the roots  $\alpha^8, \alpha^9, \alpha^{10}$  and  $\alpha^{12}$ , but as mentioned earlier, these roots do not matter to us.

Just as the minimal polynomials change as we vary  $N$ , so do the cyclotomic cosets modulo  $2^n - 1$ . Recall our initial question. For a prescribed minimum distance  $\delta$ , can we vary  $N$  in  $F[x]/(x^N - 1)$  in order to produce a BCH code of prescribed distance  $\delta$  using the fewest monic irreducible polynomials possible? We can now see that an equivalent question is the following. By varying  $n$ , can we obtain  $\delta - 1$  consecutive integers contained in the fewest number of cyclotomic cosets modulo  $2^n - 1$ ? This is helpful in that it allows us to use number theoretic results about cyclotomic cosets to determine important results about BCH codes.

## 2.3 The structure of cyclotomic cosets

Before looking at our main result, we examine the structure of the cyclotomic cosets that are necessary for understanding the generators of BCH codes. Although each term in a cyclotomic coset is determined by multiplying the generator element by a power of two, working modulo  $2^n - 1$  allows the possibility for certain terms to be odd. As will become apparent later, it is important to know when terms in a particular cyclotomic coset are odd.

For the remainder of this paper, we will assume that every cyclotomic coset is arranged in the same form. When considering the cyclotomic coset  $C_s$ , it will have the form  $\{s, 2s, 2^2s, \dots, 2^r s\}$ , where  $s$  is odd and each of the terms is reduced modulo  $2^n - 1$ . In other words, we let  $s$  be the term in position 0,  $2s$  be in position 1, and in general,  $2^i s \pmod{2^n - 1}$  be in position  $i$ . We can determine the following.

**Theorem 2** *Let  $k_i$  be the integer representation of the element in  $C_s$  in position  $i$ . Then using the above terminology we have the following:*

i) *If  $k_i < \frac{2^n - 1}{2}$ , then  $k_{i+1}$  will be even.*

ii) *The last term in  $C_s$  is represented by the integer  $k_r = \frac{s + 2^n - 1}{2}$ .*

iii) If  $\frac{2^n-1}{2} < k_i < \frac{s+2^n-1}{2}$ , then  $k_{i+1}$  will be odd.

PROOF: We consider each case.

- i) If  $k_i < \frac{2^n-1}{2}$ , then it is clear that  $2k_i$  will be less than the modulus and will thus be even.
- ii) If the last term is represented by  $k_r$ , then it must be the case that  $2k_r \equiv s \pmod{2^n-1}$ . But since  $2k_r$  is larger than the modulus and less than twice the modulus, it follows that  $2k_r - (2^n - 1) = s$ , and the result follows.
- iii) If  $\frac{2^n-1}{2} < k_i < \frac{s+2^n-1}{2}$ , then  $2k_i$  will clearly be larger than the modulus but less than twice the modulus. But then  $k_{i+1}$  is equal to  $2k_i - (2^n - 1)$  and will thus be an odd number.

QED

The next theorem gives us particular information about the parity of the last term in a cyclotomic coset.

**Theorem 3** *The last term in  $C_s$  will be even iff  $s \equiv 1 \pmod{4}$ .*

PROOF: By the previous theorem, we know that the last term can be described by the integer  $k_r = \frac{s+2^n-1}{2}$ . Since  $s$  is odd,  $s - 1$  is even. So we say  $s - 1 = 2t$ , for some integer  $t$ . We can then say  $k_r = 2^{n-1} + t$ . We can clearly see that  $k_r$  is even iff  $t$  is even, that is, if  $4|(s - 1)$ , or  $s \equiv 1 \pmod{4}$ . QED

**Theorem 4** *Consider the cyclotomic coset  $C_s$ . If  $k_r$  is the integer representation of the last term in  $C_s$ , then*

$$k_{r-1} = \begin{cases} \frac{s+2^n-1}{4}, & \text{if } s \equiv 1 \pmod{4}, \\ \frac{s+3(2^n-1)}{4}, & \text{otherwise.} \end{cases}$$

PROOF: If  $s \equiv 1 \pmod{4}$ , then  $k_r$  is even, which means that  $k_{r-1} = \frac{k_r}{2} = \frac{s+2^n-1}{4}$ . If  $s \not\equiv 1 \pmod{4}$ , then  $k_r$  is odd, so we can determine that  $k_r = 2k_{r-1} - (2^n - 1)$ , and solving for  $k_{r-1}$  we obtain the given result. QED

The next theorem was given as a corollary to a theorem in [4]. It is useful as another result about the structure of cyclotomic cosets so we include it here.

**Theorem 5** *If two consecutive odd integers,  $2j + 1$  and  $2j + 3$ , are in the same cyclotomic coset modulo  $2^n - 1$  for  $n > 5$ , then  $n \not\equiv 0 \pmod{5}$ , and  $n \equiv 2u \pmod{5}$ , or  $n \equiv 3u \pmod{5}$ .*

It is also important to understand how many times the values in a particular cyclotomic coset “loop around.” We use this expression to describe when a particular integer value  $2^i \cdot s$  is larger than the modulus and therefore gets reduced to a value less than the modulus. The “loop around terms” begin with the first term in the cyclotomic coset in which the integer value is larger than the least residue modulo  $2^n - 1$  and continues through the last term in the coset. Our next result shows us how to determine exactly how many loop around terms will be in any cyclotomic coset generated by a particular  $s$ .

**Theorem 6** *If  $\gamma$  is the largest integer such that  $2^\gamma < s$ , then the last  $\gamma$  terms will “loop around” in the cyclotomic coset  $C_s$ .*

PROOF: We can rewrite  $s$  as  $2^\gamma + c$  for some positive integer  $c < 2^\gamma$ . In  $C_s$ , the last term is  $s \cdot 2^{n-1} \pmod{2^n - 1}$ . We claim that the first term to “loop around,” that is, the first term whose least residue is not itself, is  $2^{n-\gamma} \cdot s \pmod{2^n - 1}$ . It suffices to show that  $2^{n-\gamma} \cdot s > 2^n$  and  $2^{n-\gamma-1} \cdot s < 2^n$ . We know  $s = 2^\gamma + c$ , so  $2^{n-\gamma} \cdot s = 2^n + 2^{n-\gamma} \cdot c$ , clearly larger than  $2^n$ . Also,  $2^{n-\gamma-1} \cdot s = 2^{n-1} + 2^{n-\gamma-1} \cdot c$ . We can see that  $2^{n-\gamma-1} \cdot c < 2^{n-1}$ , so  $2^{n-\gamma-1} \cdot s = 2^{n-1} + 2^{n-\gamma-1} \cdot c < 2 \cdot 2^{n-1} = 2^n$ . QED

We note that in the above proof we assumed that  $C_s$  has  $n$  terms. When  $C_s$  has less than  $n$  terms, we let the set repeat itself until it has  $n$  terms. All of those repeats will be considered “loop around” terms.

### 3 Main results

We are now ready to apply knowledge of the cyclotomic cosets. Our goal is to completely understand the number of irreducible factors necessary for a prescribed  $\delta$  and a fixed value of  $N = 2^n - 1$ . The fact that more than one BCH code can be constructed to have the same prescribed distance makes the general answer to our question much more complicated. To simplify the problem slightly, we start by considering BCH codes generated by polynomials that contain the consecutive roots  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$  (although we will return to the more general construction later).

First, we note that there is an almost trivial upper bound on the number of required irreducible factors. Since  $\alpha^{2^s}$  is always in the cyclotomic coset generated by  $\alpha^s$ , one only needs to consider the powers of  $\alpha$  that are odd. Hence, the number of required generators will never be greater than  $\frac{\delta-1}{2}$ . However, it is certainly possible that one would not need a new generator for every odd power. We look at when certain values  $a$  lie in the cyclotomic coset generated by other odd values  $d$ .

**Theorem 7** *Suppose  $d$  is odd and that  $d = 2^\gamma + s$ , where  $\gamma$  is as large as possible. Then an integer  $a > d$  is an element of the cyclotomic coset generated by  $d$  modulo  $2^n - 1$ ,  $C_d$ , iff one of the following is true:*

- 1)  $a = d \cdot 2^k$  for some positive integer  $k < n$ , or
- 2)  $(2^n - 1) \mid (a \cdot 2^m - d)$ , for some  $m \in \{1, 2, \dots, \gamma\}$ .

PROOF: Case 1) is true by definition. If  $a \neq d \cdot 2^k$  for some  $k$ , then  $a$  can only be in  $C_d$  if it is a loop around term. Only the last  $\gamma$  terms are loop around terms from Theorem 6, so this will only be the case if  $k = n - m$ , for some  $m \in \{1, 2, \dots, \gamma\}$ . Then consider the congruence  $d \cdot 2^{n-m} \equiv a \pmod{2^n - 1}$ . Multiplying both sides by  $2^m$  and then subtracting  $d$  from both sides, it follows that  $a$  is in  $C_d$  only if  $2^n - 1$  divides  $2^m \cdot a - d$ . QED

Notice that if  $n$  is large enough, an odd  $a$  will not be an element of any cyclotomic coset generated by a number smaller than itself, so each odd integer up through  $\delta - 2$  will generate its own cyclotomic coset. What this means in terms of BCH codes is that if  $n$  is large enough,

we will need a separate monic irreducible polynomial in order to generate each odd-powered root. Suppose we want to generate a BCH code of prescribed distance  $\delta$ . We now provide a sufficient condition for  $n$  to be “large enough.”

**Theorem 8** *Let  $\gamma$  be the largest integer such that  $2^\gamma < (\delta - 4)$ . If  $2^n > (\delta - 2)(2^\gamma - 1) + 3$ , then each positive odd integer less than  $\delta$  will generate a different cyclotomic coset modulo  $2^n - 1$ . Hence, for sufficiently large  $n$ , the roots  $\alpha, \dots, \alpha^{\delta-1}$  will be generated by precisely  $\frac{\delta-1}{2}$  minimal polynomials.*

PROOF: Considering Theorem 7, if  $2^n - 1$  is larger than  $(a \cdot 2^m - d)$  for all possible odd values of  $a$  and  $d$  and all  $m$ , then it cannot divide any of them, and hence each odd integer  $a$  will generate its own cyclotomic coset. By definition,  $d$  is always the smallest number in the cyclotomic coset generated by  $d$ . Hence, any value  $a \neq d$  that could be an element of  $C_d$  must be larger than  $d$ . Since  $2^n - 1$  must be larger than every  $(a \cdot 2^m - d)$ , we want to consider the case when  $(a \cdot 2^m - d)$  is as large as possible. Clearly, the largest odd integer smaller than  $\delta$  is  $\delta - 2$  since we always assume  $\delta$  is odd. Thus we let  $a = \delta - 2$ . Since  $m$  is determined by  $d$ , in order to have  $m$  as large as possible,  $d$  must be as large as possible. The largest value of  $d$  is  $a - 2$ , that is,  $\delta - 4$ . Since  $m$  is determined by  $d$ , the largest value for  $m$  is  $\gamma$ , where  $\gamma$  is the largest integer such that  $2^\gamma < d$ . Thus,  $(a \cdot 2^m - d)$  is largest when  $a = \delta - 2$ ,  $d = \delta - 4$ , and  $\gamma$  is the largest integer such that  $2^\gamma < (\delta - 4)$ . Notice that it is clear that  $(\delta - 2) \cdot 2^\gamma$  is always larger than  $d$ . Plugging these values in and simplifying, we obtain the desired result. QED

This result naturally leads us to another question. Can we extend this result to a BCH code generated using an arbitrary collection of roots? In other words, is the maximum number of monic irreducible polynomials necessary to generate a BCH code of prescribed distance  $\delta$  dependent upon which sequence of roots we choose? The answer to this question is yes. Notice that when considering a BCH code generated by the roots  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ , we have the convenience of knowing that a cyclotomic coset containing one of the necessary even powers will have as its generator one of the necessary odd powers of  $\alpha$ . We do not in general have this luxury. An even power in any other consecutive set is often generated by a smaller number not in the set.

For example, suppose we are considering the powers 8 through 13 (for  $\delta = 7$ ), and that  $n$  is large enough that each odd power requires its own cyclotomic coset. In addition to needing separate cyclotomic cosets for the powers 9, 11, and 13, we also need separate cyclotomic cosets for 8, 10, and 12. While using the powers 1 through 6 would only require three cyclotomic cosets, using the powers 8 through 13 requires six. We can see from this example that in the worst case scenario, we could need a separate cyclotomic coset for each power, that is,  $\delta - 1$  cyclotomic cosets.

## 4 Some concluding remarks

Using the roots  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$  in the BCH construction, we determined that if the underlying field is large enough (i.e., the power of  $N$  meets the requirement in Theorem 8), then each odd-powered root needed will be generated by a separate polynomial. If it is smaller than this, then it is sometimes possible for a single polynomial to generate multiple odd-powered

roots. If we use an arbitrary collection of roots, we could need up to twice as many monic irreducible polynomials. We can conclude that the simplest construction of a BCH code, that is, the construction that requires the fewest number of monic irreducible polynomials, is in general a BCH code constructed using the roots  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .

Recall that throughout this paper we restricted our attention to BCH codes constructed in the polynomial ring  $F[x]/(x^N - 1)$  where  $N$  is a power of 2 minus 1. While this is helpful in that it gives us more structure since there exist finite fields of size  $2^k$  for any  $k$ , it is not necessary. It would be interesting to see if we can determine similar results for the case when  $N$  is a power of some other prime minus 1, or even when  $N$  is arbitrary.

**Acknowledgment:** The authors would like to thank the referee for some very helpful suggestions that strengthened the quality of this article.

## References

- [1] R. C. Bose and D. K. Ray-Chaudhuri, On a class of error-correcting binary group codes, *Info. and Control*, **3** (1960) 68–79, 279–290.
- [2] J. Durbin, *Modern Algebra: An Introduction*, fifth edition, John Wiley & Sons, Inc., 2005.
- [3] A. Hocquenghem, Codes correcteurs d’erreurs, *Chiffres* (Paris) **2** (1959) 147–156.
- [4] D. Mandelbaum, Two applications of cyclotomic cosets to certain BCH codes, *IEEE Transactions on Information Theory*, Vol. IT-26, No. 6, November 1980.
- [5] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, third edition, Wiley-Interscience Series in Discrete Mathematics, 1998.

## About the authors:

Jacob Farinholt graduated from the University of Mary Washington with a Bachelor of Science degree in mathematics in the spring of 2009. While a senior, the work presented here was completed as part of an honors project directed by Dr. Keith E. Mellinger, associate professor and chair of the department of mathematics. Jake currently works as an operations research analyst at the Naval Surface Warfare Center, Dahlgren Division.

### Jacob M. Farinholt

Naval Surface Warfare Center, Dahlgren Division, W63, 5409 First Street, Building 1510, Dahlgren, VA 22448, jfarinholt@gmail.com

### Keith E. Mellinger

Department of Mathematics, University of Mary Washington, 1301 College Avenue, Trinkle Hall, Fredericksburg, VA 22401, kmelling@umw.edu