On the Number of Information Symbols in Bose-Chaudhuri Codes*

HENRY B. MANN

Department of Mathematics, Ohio State University

Let $\alpha$ be a primitive root of G. F. $(q^m)$. Let $I(m, v)$ be the number of information symbols of the code with parity check matrix $(\alpha^i)$, $i = 1, \cdots, v$, $j = 0, \cdots, q^m - 2$. Let $v = q^\lambda, m - \lambda = r$. Then for sufficiently large $m$ we have

$$I(m, v) = \langle \rho^m \rangle$$

where $\langle c \rangle$ denotes the nearest integer to $c$ and $\rho$ is the positive root of the equation $x^r = (q - 1)(x^{r-1} + \cdots + 1)$. For small values of $m$ we have $I(m, v) = \rho^m + \epsilon$ where $|\epsilon| \leq (r - 1)r^m, \quad |\epsilon| < 1$. Estimates for $\tau$ are given in the Appendix. Two other formulas, exact for all values of $m \geq r - 1$, are also given. The first contains $r$ terms, the second $\lfloor m/r + 1 \rfloor$ terms, where $[c]$ denotes the largest integer not exceeding $c$.

LIST OF SYMBOLS

G. F. = Galois field

$\langle x \rangle$ = nearest integer to $x$

$[x]$ = largest integer not exceeding $x$

The codes in the title were introduced by Bose and Chaudhuri (1960). An excellent account of them, including the necessary background in algebra has been given by Peterson (1960, 1961) and there is no need to give a detailed description of them here.

Let $\alpha$ be a primitive root of G. F. $(q^m)$. Let $H(x)$ be the polynomial of smallest degree with coefficients in G. F. $(q)$ which has $\alpha, \alpha^2, \cdots, \alpha^v$ among its roots. The degree $h$ of $H(x)$ is the number of check symbols of the code with parity check matrix $(\alpha^i)$, $i = 1, \cdots, v$, $j = 0, \cdots, q^m - 2$. The number $I(m, v)$ of information symbols is given by


153
\( I(m, v) = q^m - 1 - h. \) For \( q = 2 \) Peterson (1960) proved \( I(m, v) = o(2^m) \) for \( v/2^m \geq c > 0 \). We shall in this paper give two exact formulae for \( I(m, v) \) when \( v = q^\lambda \). One of our formulas immediately implies Peterson’s result.

If \( \alpha \) is a root of \( H(x) \) then \( \alpha q^j, \alpha q^{2j}, \ldots, \alpha q^{(m-1)j} \) are also roots of \( H(x) \). On the other hand the exponents of \( \alpha \) can be considered mod. \( q^m - 1 \). Hence given \( v \) we have to find the number of residues \( y \) mod. \( q^m - 1 \) which satisfy a congruence

\[
q^\mu y \equiv x \mod q^m - 1
\]

for some \( 0 \leq \mu \leq m - 1 \) and some \( 1 \leq x \leq v \). If we write the residues \( y \) in the notation to the base \( q \) then \( qy \) can be obtained from \( y \) by a cyclic permutation of its digits. We therefore have the following lemma:

**Lemma 1.** The degree of \( H(x) \) equals the number of integers \( y \) such that \( 0 \leq y < q^m - 1 \) and such that an integer \( y' \leq v \) may be obtained from \( y \) by permuting cyclically the digits of \( y \), when \( y \) is written in the notation to the base \( q \).

We now assume \( v = q^\lambda \). A number

\[
y = c_0 + c_1q + \cdots + c_{m-1}q^{m-1}
\]

is less than \( v = q^\lambda \) if and only if \( c_\lambda = \cdots = c_{m-1} = 0 \). Hence we have

**Lemma 2.** If \( v = q^\lambda \) and \( m - \lambda = r \), then the degree of \( H(x) \) is one less than the number of sequences of length \( m \) of \( q \) digits \( 0, 1, \ldots, (q - 1) \), which if placed on a circle contain a run of \( r \) or more \( 0 \)’s.

(For example the sequence 010100 contains a run of 3 zeros if placed on a circle.) From here on we shall drop the restriction that \( q \) is a prime power, \( h + 1 \) will denote the number of sequences of length \( m \) of \( q \) digits \( 0, 1, \ldots, (q - 1) \) which contain a “circular” run of at least \( r \) zeros.

One can reduce the enumeration of these “circular” runs to an enumeration of runs in the ordinary sense, which we shall call straight runs. Let \( r \) be fixed and let \( l(s) \) be the number of sequences of length \( s \) which contain a straight run of length \( r \). Put \( h + 1 - l(m) = d(m) \). Then \( d(m) \) is the number of sequences of length \( m \) which contain a circular run but no straight run of length \( r \). If \( 2r \leq m \) then such a sequence must contain a circular run of length \( r + k \), \( 0 \leq k \leq r - 2 \), bordered by a nonzero digit on both ends, while the remainder of the sequence does not contain a straight run of length \( r \). Moreover the \( r + k \) zeros must be placed in such a way that no straight run of length \( r \) results
and this can be done in \( r - k - 1 \) ways. Hence for \( m \geq 2r \)

\[
h + 1 = l(m)
\]

\[
+ (q - 1)^2 \sum_{k=0}^{r-2} (r - k - 1)(q^{m-r-k-2} - l(m - r - k - 2)).
\]

We now put \( \varphi(s) = q^s - l(s) \). The required number \( z(m) \) of sequences of length \( m \) without a circular run of length \( r \) is then given by

\[
z(m) = \varphi(m) - (q - 1)^2 \sum_{k=0}^{r-2} (r - k - 1)\varphi(m - r - k - 2).
\]

We proceed to compute \( l(s) \). A sequence \( S_1 \) of length \( s, s > r \) can be obtained from a sequence \( S \) of length \( s - 1 \) by addition of any of the \( q \) digits \( 0, 1, \ldots, q - 1 \). If \( S_1 \) has a run of length \( r \) while \( S \) does not have such a run then \( S_1 \) must have its last digit 0 and \( S \) must end with \( (r - 1) \) zeros preceded by a nonzero digit. Moreover, \( S \) cannot have a run of \( r \) zeros in its first \( s - r - 1 \) digits. Hence

\[
l(s) = ql(s - 1) + (q - 1)(q^{s-r-1} - l(s - r - 1)), \quad s > r,
\]

\[
l(r) = 1, \quad l(k) = 0 \quad \text{for } 0 \leq k < r.
\]

Hence

\[
\varphi(s) = q\varphi(s - 1) - (q - 1)\varphi(s - r - 1), \quad s > r,
\]

\[
\varphi(r) = q^r - 1, \quad \varphi(k) = q^k \quad \text{for } 0 \leq k < r.
\]

It is well known that we may put \( \varphi(s) = \rho^s \). Then

\[
\rho^{r+1} - q\rho^r + q - 1 = 0.
\]

For \( r = 1 \) we obviously have \( \varphi(s) = q - 1 \). Hence we may assume \( r > 1 \). A sketch of the curve \( y = x^{r+1} - qx^r + q - 1 = 0 \) shows that for \( r > 1 \) (5) has no double roots. Let now \( 1, \rho_1, \ldots, \rho_r \) be the roots of (5). We may put \( \varphi(s) = c_0 + c_1\rho_1^s + \cdots + c_r\rho_r^s \). The initial conditions of (4) give

\[
c_0 + c_1\rho_1^k + \cdots + c_r\rho_r^k = q^k, \quad 0 \leq k < r
\]

\[
c_0 + c_1\rho_1^r + \cdots + c_r\rho_r^r = q^r - 1.
\]

We divide (5) by \( \rho - 1, \rho \neq 1 \) and get

\[
\rho^r = (q - 1)(\rho^{r-1} + \cdots + 1).
\]
Subtracting the sum of the first \( r \) equations of (6) from the last and using (7) we find \( c_0 = 0 \) and the last equation of (6) may be deleted.

Deleting the last equation of (6) we see that each \( c_i, \ i = 1, \ldots, r \) is given by a quotient of two Vandermond determinants and putting \( f(x) = x^r - (q - 1)(x^{r-1} + \cdots + 1) \) one finds

\[
c_i = \frac{\prod_{j \neq i} (q - p_j)}{\prod_{j \neq i} (p_i - p_j)} = \frac{f(q)}{(q - p_i)f'(p_i)}.
\]

(8)

Using (5) this can be simplified to

\[
c_i = \frac{\rho_i^r}{f'(p_i)(q - 1)}
\]

(9)

With \( (x - 1)f(x) = x^{r+1} - qx^r + q - 1 \) we easily find for \( \rho \neq 1 \) using (5)

\[
\rho(\rho - 1)f'(\rho) = \rho^{r+1} - (q - 1)r
\]

and

\[
c_i = \frac{\rho_i^{r+1}(\rho_i - 1)}{(\rho_i^{r+1} - (q - 1)r)(q - 1)} = \frac{\rho_i(\rho_i^r - 1)}{\rho_i^{r+1} - (q - 1)r},
\]

(10)

\( i = 1, \ldots, r \).

Hence

\[
\varphi(s) = \sum_{i=1}^{r} c_i \rho_i^s, \quad c_i = \frac{\rho_i(\rho_i^r - 1)}{\rho_i^{r+1} - (q - 1)r}.
\]

(11)

A sketch of the curve \( g(x) = x^{r+1} - qx^r + (q - 1) \) shows that \( g(x) \) has besides the root \( \rho = 1 \) only one other positive root which lies in the interval \((r/r + 1)q, q\). If \( \rho \) is a nonpositive (negative or complex) root of \( g(x) \) then from (5) we get with \( \tau = |\rho| \)

\[
\tau^{r+1} > q\tau^r - (q - 1)
\]

and from (7) for \( \tau > 1 \)

\[
\tau^{r+1} < q\tau^r - (q - 1).
\]

Hence

**Lemma 3.** If \( \rho \) is a nonpositive (negative or complex) root of (5) then \( |\rho| < 1 \).
We shall now prove

**Lemma 4.**

\[ |c, \rho_i^{r-1}| < \frac{1}{2(r-1)} \quad \text{if} \quad |\rho_i| < 1. \]  

(12)

From (11) we have

\[ |c, | \leq \frac{|\rho_i| |\rho_i' - 1|}{(q - 1)r - 1} \leq \frac{|\rho_i| |\rho_i' - 1|}{r - 1}. \]  

(13)

We put \( \rho_i = r^{e^\varphi} \). We may choose \( 0 < \varphi \leq \pi \). From (5) we get

\[ \tau^{r+1} \cos (r + 1)\varphi + q - 1 = q\tau' \cos (r\varphi), \]

\[ \tau \sin (r + 1)\varphi = q \sin (r\varphi). \]  

(14)

Substituting from the second equation of (14) into the first we get

\[ (q - 1) \sin (r\varphi) = \tau^{r+1} \sin \varphi, \]

\[ (q - 1) \sin (r + 1)\varphi = \tau'q \sin \varphi. \]  

(15)

From (14) and (15) we get

\[ \cos (r\varphi) > 0, \quad \sin (r\varphi) > 0, \quad \sin \varphi > (q - 1) \sin (r\varphi) \]

\[ \cos \varphi < \cos (r\varphi). \]  

(16)

Now

\[ |\rho_i' - 1|^2 = 1 - 2\tau' \cos (r\varphi) + \tau'^2. \]

If \( \sin \varphi = 0 \) then \( \cos (r\varphi) = 1 > \tau' \). If \( \sin \varphi \neq 0 \) we have from (15)

\[ (q - 1) \left( \frac{\sin (r\varphi)}{\sin \varphi} \cos \varphi + \cos (r\varphi) \right) = q\tau'. \]

If \( \cos \varphi < 0 \) then \( \cos (r\varphi) > \tau' \) is immediately obvious. If \( \cos \varphi > 0 \) we establish the inequality from the inequalities (16). Hence we have in all cases

\[ \cos (r\varphi) > \tau'. \]

We now get

\[ (|\rho_i' ||\rho_i' - 1|)^2 < \tau'^2(1 - \tau'^2) \leq \frac{1}{2}. \]

Lemma 4 now follows from (13). From (12) we find

\[ \sum_{|\rho_i'| < 1} c_ip_i^t < \frac{1}{2} \quad \text{for} \quad t \geq r - 1. \]
Denoting now by \(\langle x \rangle\) the nearest integer to \(x\) we therefore have:

**Theorem 1.** The number \(\varphi(m)\) of sequences of length \(m \geq r - 1\) of \(q\) digits 0, 1, \(\ldots\), \(q - 1\) which contain no straight run of \(r\) zeros is given by

\[
\varphi(m) = \langle c \rho^m \rangle
\]

where \(\rho\) is the largest positive root of Eq. (5) and

\[
c = \frac{\rho(r - 1)}{[\rho^{r+1} - (q - 1)r]};
\]

moreover \((r/r + 1)q < \rho < q\).

The last inequality follows from the fact that the polynomial

\[
x^{r+1} - qx^r + q - 1
\]

has a minimum at \(x = (r/r + 1)q\) where it is negative and the value 1 for \(x = q\).

From (2) we get the following corollary:

**Corollary 1.** Let \(z(m)\) be the number of sequences of length \(m\) of \(q\) digits 0, 1, \(\ldots\), \(q - 1\) which contain no circular run of \(r\) zeros. Then for \(m \geq 2r\)

\[
z(m) = \langle c \rho^m \rangle - (q - 1)^2 \sum_{k=0}^{r-2} (r - k - 1) \langle c \rho^{m-r-k-2} \rangle. \tag{18}
\]

From (7) and (11) we have

\[
z(m) = \sum_i c_i (\rho_i^m - (q - 1)^2 \sum_{k=0}^{r-2} (r - k - 1) \rho_i^{m-r-k-2})
\]

and since \(f'(\rho) = r \rho^{r-1} - (q - 1) \sum_{k=0}^{r-2} (r - k - 1) \rho^{r-k-2}\) this reduces to

\[
z(m) = \sum_i c_i (\rho_i^m + (q - 1)f'(\rho_i) \rho_i^{m-2r} - (q - 1)r \rho_i^{m-r-1}). \tag{19}
\]

Substituting for \(c_i\) its value from (9) and (11) one finally finds

\[
z(m) = \sum_i \rho_i^m, \tag{20}
\]

whence

**Corollary 2.** For \(m \geq 2r\) and \(|\rho_i| \leq r < 1\) for \(\rho_i | < 1\)

\[
z(m) = \rho^m + \epsilon, \quad |\epsilon| \leq (r - 1) r^m. \tag{21}
\]

For sufficiently large \(m\)

\[
z(m) = \langle \rho^m \rangle. \tag{22}
\]
**Table I**

**Values of \( p \) and \( cp^r \) for \( q = 2 \)

<table>
<thead>
<tr>
<th>( r )</th>
<th>( p )</th>
<th>( cp^r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.618034</td>
<td>3.065248</td>
</tr>
<tr>
<td>3</td>
<td>1.839287</td>
<td>7.07522</td>
</tr>
<tr>
<td>4</td>
<td>1.927562</td>
<td>15.07028</td>
</tr>
<tr>
<td>5</td>
<td>1.965948</td>
<td>31.05669</td>
</tr>
<tr>
<td>6</td>
<td>1.983583</td>
<td>63.04252</td>
</tr>
<tr>
<td>7</td>
<td>1.991964</td>
<td>127.0302</td>
</tr>
<tr>
<td>8</td>
<td>1.996031</td>
<td>255.0206</td>
</tr>
<tr>
<td>9</td>
<td>1.998029</td>
<td>511.0136</td>
</tr>
<tr>
<td>10</td>
<td>1.999019</td>
<td>1023.009</td>
</tr>
<tr>
<td>11</td>
<td>1.999510</td>
<td>2047.005</td>
</tr>
<tr>
<td>12</td>
<td>1.999756</td>
<td>4095.003</td>
</tr>
</tbody>
</table>

**Corollary 3.** The number \( I(m, q^X) \) of information symbols of a code with parity check matrix \( (\alpha^{ij}) \), \( i = 1, \ldots, q^X; j = 0, 1, \ldots, q^{m-2} \), \( \alpha \) a primitive root of \( G. F.(q^m) \) is given by

\[
I = z(m), \tag{23}
\]

where \( z(m) \) is given by (18) with \( r = (m - \lambda) \). Within the given error \( z(m) \) may of course also be computed from (21).

Table I shows the values of \( p \) and \( cp^r \) for \( q = 2 \) and \( 2 \leq r \leq 12 \).

In the applications to coding \( r \) is usually not large, so that (18) will be convenient to use. If \( m \) is large compared to \( r \), then Eq. (22) can be used. We shall therefore give another formula for \( h + 1 \) which is a sum of \( [m/r + 1] \) terms, so that it can be used when \( r \) is too large to use (18) and \( m \) too small to use (22). We shall need the following lemma.

**Lemma 5.** Suppose we have \( N \) sets of objects, say balls to fix ideas. The sets containing either 1, 2, \ldots balls. Let \( a_1 \) be the number of balls, \( a_2 \) the number of pairs of balls that occur together in one set, \( a_3 \) the number of triples etc. Then

\[
N = a_1 - a_2 + a_3 \ldots \tag{24}
\]

**Proof:** Number the balls. \( N_i = 1 \) is the number of sets containing the \( i \)th ball, \( N_{ij} \) (either 0 or 1) the number of sets containing the \( i \)th and \( j \)th ball etc. Then \( N \) is the number of sets containing at least one ball and by a well known formula

\[
N = \sum N_i - \sum N_{ij} + \ldots
= a_1 - a_2 + \ldots .
\]
If a sequence does not consist entirely of zeros and if it contains a circular run of \( r \) zeros then it must contain a nonzero digit followed (in a circular sense) by \( r \) zeroes. We shall call a nonzero digit followed by \( r \) zeros a string. We can place such a string in \( m \) positions and then fill the remaining positions by digits in \( q^{m-r-1} \) ways. Hence \( a_1 \), the number of strings occurring in all sequences is \( mq^{m-r-1}(q-1) \). The number \( a_k \) of \( k \)-tuples \( (k(r+1) \leq m) \) of strings is obtained by placing the first string in \( m \) positions. The other strings can now be considered as units and can be distributed in \( \binom{m-kr-1}{k-1} \) ways over the \( m-kr-1 \) places still to be filled. The remaining places can be filled by digits in \( q^{m-k(r+1)} \) ways and the initial terms of the strings can be chosen in \( (q-1)^k \) ways. Each \( k \)-tuple has now been counted \( k \) times since each of its strings can be considered the first. Hence

\[
a_k = \frac{m}{k} (q-1)^k \binom{m-kr-1}{k-1} q^{m-k(r+1)}.
\]

By (24) we therefore have:

\[
h = m \sum_{k=1}^{\lfloor m/r+1 \rfloor} (-1)^{k-1} \frac{(q-1)^k}{k} \binom{m-kr-1}{k-1} q^{m-k(r+1)} \quad (25)
\]

and

\[
z(m) = q^m - h - 1. \quad (26)
\]

It may be observed that all numbers

\[
v, q^k \leq v < q^k + q^{k-r} + \cdots + q^{k-(\lambda-1)/r} = n(\lambda)
\]

contain in their representation to the base \( q \) a sequence of at least \( r \) zeros. Hence the number \( I(m, v) \) of information symbols for the corresponding Bose-Chaudhuri code will be \( z(m) \) as given by (18). Formula (21), (22), or (26) may also be used if more convenient. It is also obvious that all numbers obtainable from \( n(\lambda) \) by cyclic permutation of its digits are distinct and larger than \( n(\lambda) \), so that \( I(m, n(\lambda)) = z_m - m \). Similarly one sees that \( I(m, q^k - 1) = z_m + m \).

APPENDIX

Let \( re^{iq} \) be a nonpositive root of (5). We may assume \( 0 < \varphi \leq \pi \). Put \( r\varphi \equiv \alpha \) (mod \( 2\pi \)). From (14) we have \( 0 \leq \alpha < \pi/2 \), \( \sin \alpha < 1/q \leq \sin (\pi/2q) \), hence \( q\alpha < \pi/2 \). Furthermore \( \sin (\alpha + \varphi) > q \sin \alpha \leq q\alpha \) and so

\[
\alpha + \varphi > q\alpha, \quad \varphi > (q-1)\alpha. \quad (27)
\]
We shall need the following Lemma:

**Lemma 6.** For \(0 < k\varphi \leq \pi/2, k > 1\), the function

\[
\psi(\varphi) = \frac{\sin (k\varphi)}{\sin \varphi}
\]

decreases with \(\varphi\).

One proves Lemma 6 easily using the convexity of \(\tan \varphi\).

From (27) we have \(r_\varphi \geq 2\pi\), hence

\[
\varphi \geq \frac{2\pi}{r}.
\]  

(28)

If \(\sin \varphi = 0\) we must have \(\varphi = \pi\) and (14) gives

\[
\tau^{r+1} < \frac{q - 1}{q + 1}.
\]

For \(\sin \varphi \neq 0\) we have from (15)

\[
\frac{\sin \alpha + \varphi}{\sin \varphi} \frac{q - 1}{q} = \tau^r,
\]  

(29)

From (27), (28), (29), and Lemma 6 one easily establishes the following inequalities:

\[
\tau^r < \frac{q - 1}{q} \quad \text{if} \quad \pi > \varphi \geq \frac{\pi}{2},
\]

\[
\tau^r < \frac{q - 1}{q} \frac{1}{\sin(q - 1/q)} \quad \text{if} \quad \frac{\pi}{2} \geq \varphi \geq \frac{q - 1}{q} \frac{\pi}{2},
\]

\[
\tau^r < \frac{q - 1}{q} \frac{\sin [(q/q - 1)2\pi/r]}{\sin(2\pi/r)} \quad \text{if} \quad \varphi \leq \frac{q - 1}{q} \frac{\pi}{2}.
\]  

(30)

This gives the following estimates for \(\tau^r\):

\[
\tau^r < \left(\frac{q - 1}{q + 1}\right)^{r+1} \quad \text{for} \quad \varphi = \pi,
\]

\[
\tau^r < \frac{q - 1}{q} \quad \text{for} \quad 2 \leq r \leq 4,
\]

\[
\tau^r < \frac{q - 1}{q} \frac{1}{\sin(2\pi/r)} \quad \text{for} \quad \frac{4q}{q - 1} \geq r \geq 4,
\]

\[
\tau^r < \frac{q - 1}{q} \frac{\sin [(q/q - 1)2\pi/r]}{\sin(2\pi/r)} \quad \text{for} \quad r \geq \frac{4q}{q - 1}.
\]
For $q = 2$ a short calculation shows that for $r = 2, 3, 4, 5, 6$ Eq. (22) is exact for $m \geq 2, 6, 10, 18, 24$, respectively.

Received: October 9, 1961

References


