A t-error-correcting code is perfect if the covering radius is t.

The code is quasi-perfect if the covering radius is t + 1.

Let β be an element of order n = 2^m - 1. The largest cyclic code whose generator polynomial g(x) ∈ GF(2)[x] has the zeros β, β^2, ..., β^{2^m - 1} but not β^t is defined to be a primitive BCH code of designed distance d and is here denoted by B(d). Note that d must be odd if B(d) exists.

The code B(9) is the Hamming code, which is a one-error-correcting perfect code. Gorenstein, Peterson, and Zierler [1] proved that B(5) is a two-error-correcting quasi-perfect code. They also proved that B(7) is a three-error-correcting code which has covering radius at least five, and thus B(7) is not quasi-perfect. Later Van der Horst and Berger [2], Assmus and Mattson [3], and Helleseth [4] proved that B(7) has covering radius five.

In this correspondence we will prove a conjecture due to Gorenstein, Peterson, and Zierler [1], which says that B(d) is never quasi-perfect when d > 7.

Leont'ev [5] proved that B(d) is not quasi-perfect when (d - 1)/2 < √n/log n and m > 7.

We will need the following lemmas.

**Lemma 1:** If d = 2 - 1, r < m, then B(d) exists and has actual minimum distance d.

**Lemma 2:** If d = 2 - 2^t - 1, where 0 < (r - 1)/2 < s < r < m, then B(d) exists and has actual minimum distance d.

**Theorem 1:** No primitive binary t-error-correcting BCH code is quasi-perfect when t > 2.

Before proving Theorem 1 we prove the following stronger result.

**Theorem 2:** Let p_d and t_d denote the covering radius and actual error correcting ability of B(d), respectively, and let 3 < r < m - 1.

i) If 2^t - 2^t+1 - 1 < d < 2^t - 2^t - 1 where s is one of the numbers [2^t/2], [2^t/2] + 1, ..., r - 2, then

\[ p_d - t_d > \frac{2^t - s}{2} \cdot (t_d + 1). \]

ii) If 2^t - 2^{t/2} - 1 < d < 2^t - 2^t, then

\[ p_d - t_d > \frac{2^{(r - t)/2}}{2^{(r - t)/2} - 1} \cdot (t_d + 1). \]

**Proof:**

i) Let 2^t - 2^t+1 - 1 < d < 2^t - 2^t - 1 for some s = [2^t/2], [2^t/2] + 1, ..., r - 2, where 3 < r < m - 1. By Lemma 2, B(2^t - 2^t+1 - 1) and B(2^t - 2^t - 1) exist, and we have

\[ B(2^t - 2^t - 1) \subset B(d) \subset B(2^t - 2^t+1 - 1). \]

Since B(d) \subset B(2^t - 2^t+1 - 1), we can choose α ∈ B(2^t - 2^t+1 - 1) - B(d). Here α has distance at least 2^t - 2^t+1 - 1 from every element in B(d). From the definition of the covering radius it follows that

\[ p_d > 2^t - 2^t+1 - 1. \]

Since B(2^t - 2^t - 1) \subset B(d), we get by Lemma 2

\[ t_d < 2^t - 1 - 2^t - 1. \]

Combining (1) and (2) we have

\[ p_d - t_d > 2^{t-1} \cdot (2^t - s - 3) \]

which combined with (2) gives

\[ p_d - t_d > \frac{(t_d + 1)(2^t - s - 3)}{(2^t - 1)}. \]

This proves i).

\[ p_d - t_d > \frac{1}{2} (t_d + 1), \]

when d belongs to case i).

\[ p_d - t_d > \frac{1}{2} (t_d + 1), \]

when d belongs to case ii).

Hence we always have \( p_d - t_d > 1 \) since \( t_d > 3 \), and therefore \( B(d) \) is not quasi-perfect except when \( d = 3 \).

From the proof above we get the following corollary.

**Corollary:** If \( t_d > 2 \) and \( t_d \neq 2^m - 1 \), then \( p_d - t_d > \frac{1}{2} (t_d + 1) \).

**REFERENCES**


Symbol Synchronization in Convolutionally Coded Systems

LEONARD D. BAUMERT, ROBERT J. McELIECE, MEMBER, IEEE, AND HENK C. A. VAN TILBORG

**Abstract—** Alternate symbol inversion is sometimes applied to the output of convolutional encoders to guarantee sufficient richness of symbol transitions in which arbitrarily long sequences of all zeros or all ones can cause temporary loss of synchronization and thus data loss. To avoid this problem, alternate symbols of the data stream are inverted; presumably a long alternating string is less likely than a long constant string.

Many digital communication systems derive symbol synchronization from the transitions in the received symbol stream. In such systems unusually long sequences of all zeros or all ones can cause temporary loss of synchronization and thus data loss. To avoid this problem, alternate symbols of the data stream are inverted; presumably a long alternating string is less likely than a long constant string.

Suppose the symbol stream is the alternately inverted output of a convolutional encoder. How long a constant string occurs?

**I. INTRODUCTION**

Many digital communication systems derive symbol synchronization from the transitions in the received symbol stream. In such systems unusually long sequences of all zeros or all ones can cause temporary loss of synchronization and thus data loss. To avoid this problem, alternate symbols of the data stream are inverted; presumably a long alternating string is less likely than a long constant string.

Suppose the symbol stream is the alternately inverted output of a convolutional encoder. How long a constant string occurs?
then? That is, how long a run of alternating symbols 
\[
\cdots 0101010101010101010101010101\cdots
\]
occurs in some codeword of a convolutional code? As we shall see, arbitrarily long alternating runs do occur in some codes; we characterize these codes in Section II. In Section III, for codes which do not have arbitrarily long alternating runs, we give upper bounds for the length of the longest run. In Section IV we consider examples which illustrate the use of these results and indicate how good the various upper bounds can be expected to be.

The reader is assumed to be familiar with the theory of convolutional codes and encoders as it appears, say, in Forney [1]. Thus terms like "overall constraint length," "minimal encoder," "dual code and dual encoder," etc., are assumed known and used without definition. However, we remind the reader that the convolutional encoders of concern operate on binary sequences of the form \( x = (x_1, x_2, x_3, \ldots) \) which, theoretically at least, extend to infinity in both directions. The index refers to discrete time intervals. In practice each sequence "starts" at some finite time; i.e., there is an index \( s \) such that \( t < s \) implies \( x_t = 0 \). The codewords produced by the encoders are of the same type. Using the delay operator \( D \), it is sometimes convenient to write \( x = x_1D^1 + x_2D^2 + \cdots \). We also use certain algebraic properties of these formal power series, e.g., \( D^s + D^{s+1} + \cdots = D^s/(1 + D) \).

II. CONVOLUTIONAL CODES WITH AN INFINITE RUN OF ALTERNATING SYMBOLS

**Theorem 1:** Let \( C \) be an \((n,k)\) convolutional code over \( \text{GF}(2) \) with generator matrix \( G \). Then \( C \) contains a codeword with an infinite run of alternating symbols if and only if there exists a linear combination \( v = [v_1, \ldots, v_n] \) of the rows \( g_i \) of \( G \) such that
\[
\begin{align*}
[0,1,0,\ldots,0] & \text{ modulo } 1 + D, \text{ } \text{n even} \\
[1,0,1,\ldots,0] & \text{ modulo } 1 + D, \text{ } \text{n odd}
\end{align*}
\]

Proof: (Sufficiency): When \( n \) is even, consider the codeword produced by the inputs \( a_i/(1 + D) \) applied to the rows \( g_i \), where \( v = \Sigma a_i g_i \). Note that this same codeword is produced by applying \( 1/(1 + D) = (1 + D)^n \) to each row of the equivalent encoder whose rows are \( \hat{g}_i \). Thus after an initial transient the output will be \( v_1(1), \ldots, v_n(1) \) and since \( v_i(D) = v_i(D) \) modulo \( 1 + D \) the result follows. For \( n \) odd note that \( v_i(D) = v_i(D) \) modulo \( 1 + D^2 \) means that the sum of its even coefficients is 0 and the sum of its odd coefficients is 1, whereas the situation is reversed for \( v_i(D) \) modulo \( 1 + D^2 \). Thus after an initial transient the input sequences \( a_i/(1 + D^2) \) will produce an infinite run of alternating symbols.

(Necessity): When \( n \) is even, an infinite run of alternating symbols results from the juxtaposition of \( n \)-tuples of the form \( 10\cdots10 \) or \( 01\cdots01 \). For definiteness, assume the former occurs. Then, if a codeword of \( C \) contains such an infinite run, there exists a codeword \( u \) such that
\[
u = h + \frac{D^2}{1 + D}[1,0,\ldots,1,0]
\]
Here \( h \) is an \( n \)-tuple of polynomials (of degrees \(<s) \) which describes the initial segment of \( u \). Let \( v(D) = (1 + D)u(D) \). Obviously, \( v(D) \) is polynomial and \( v(D) \equiv [1,0,\ldots,1,0] \) modulo \( 1 + D \).

Similarly, for \( n \) odd, \( C \) contains \( w = h' + \frac{D^2}{1 + D^2}[1,0,\ldots,1,1,0] \).

Define \( v(D) \) as \((1 + D^2)w(D)\). It follows as above that \( v(D) \equiv D^s[1,0,\ldots,1,1] \) modulo \( 1 + D^2 \) and the proof is complete.

Suppose an \((n,k)\) convolutional code \( C \) over \( \text{GF}(2) \) with generator matrix \( F \) for its dual code is given. Suppose \( F \) is a basic encoder, i.e., the gcd of its \( n-k \) by \( n-k \) subdeterminants is 1, then, if \( f_1, \ldots, f_n \) is any row of \( F \) it follows that \( (f_1, \ldots, f_n) = 1 \).

Let \( C_i \) be \((n,n-1)\) convolutional code dual to the \( i \)-th row of \( F \). Clearly, \( C = \bigcap_{i=1}^{n-k} C_i \) and the maximum run of alternating symbols in any codeword of \( C \) has length \( l = I(C) < \min I(C_i) \).
symbols if and only if every row of a basic generator matrix \( F \) for \( C \) satisfies the congruences of Theorem 2. When \( n \) is even it is further necessary that this be true for the same value of \( \alpha \) (0 or 1).

Note: Suppose \( n \) is even and \( L(C_i) = L(C) = \infty \) with \( \alpha \neq 1 \) for \( C_i \) and \( \alpha \neq 0 \) for \( C_j \). Add row \( j \) to row \( i \) in \( F \); this gives an equivalent basic encoder which has \( L(C) < \infty \).

### III. Bounds for Finite Runs of Alternating Symbols

If no codeword contains an infinite run of alternating symbols the question arises as to the maximum length \( L \) of such a finite run. It is easy to give a bound for \( L \) in terms of the generators for the dual code. From this bound it is possible to derive another bound (in general, weaker) which has the advantage that it can be applied directly without knowledge of the dual (see the Corollary to Theorem 3, below). In Section IV these bounds are applied to some specific examples.

Suppose \( \{f_1, \ldots, f_s\} \) is a generator matrix for an \((n,1)\) convolutional code \( C \) over \( \text{GF}(2) \) with \( d = \max(\deg(f_i)) \). Then

\[
1 + f_1 f_2 \cdots f_{s-1} f_s = 1 + f_1 f_2 \cdots f_{s-1} f_s
\]

is its associated bit pattern. Let \( s \) be the number of symbols occurring between the first and last nonzero symbols \( f_i \) inclusively. If \( (f_1, \ldots, f_s) = 1 \), \( s \) is the minimum length of any nonzero codeword of \( C \) and

\[
n(d-1) + 2 \leq s < n(d+1) + 1.
\]

**Theorem 3:** Let \( C \) be an \((n,n-1)\) convolutional code over \( \text{GF}(2) \) with generator matrix for its dual code given by \( \{f_1, \ldots, f_s\} \), where \( (f_1, \ldots, f_s) = 1 \). Suppose no codeword of \( C \) contains an infinite run of alternating symbols. Then the maximum run of alternating symbols in any codeword of \( C \) has length \( L = s + n - 2 \), when \( n \) is even or when \( n \) is odd and

\[
h(D) = \sum_{i=1}^{s+1} f_i D_i \equiv 1 + S \mod (1+D^2).
\]

If \( n \) is odd and \( h(D) = 1 \) or \( D \) modulo \( 1 + D^2 \), the maximum run of alternating symbols has length \( L = s + 2n - 2 \).

Combining this with the limits given above for \( s \) yields

\[
n(d-1) + 2 \leq s < n(d+1) + 1.
\]

**Proof:** Suppose \( n \) is even. Then, from Theorem 2, \( \Sigma f_{2i} = f_{2i+1} \equiv 1 \mod (1+D) \). If there were an alternating run of length \( > s + n - 1 \) it would have \( s \) consecutive symbols which would have inner product zero with the bit pattern of the \( f \). This contradicts \( \Sigma f_{2i} = \Sigma f_{2i+1} = 1 \), so \( L \leq s + n - 2 \). On the other hand, consider an alternating run of length \( s + n \). Change the first and last of these symbols; the inner products will be correct provided that they match up with the symbols \( f_1, \ldots, f_s \) and \( f_{s+1}, \ldots, f_{n-1} \). Clearly, this run can be extended to the right and the left to form a codeword of \( C \); it is merely necessary that symbols \( \pm jn \) of the inner products are zero. Such a codeword could conceivably extend infinitely in both directions; however, using an argument similar to that at the end of Theorem 2, it follows that there is a finite codeword with an alternating run of this length.

If \( n \) is odd then, from Theorem 2, \( h(D) \equiv 0 \mod (1+D) \). If \( h(D) \equiv 1 + D \mod (1+D^2) \) the proof above applies, so \( L = s + n - 2 \). If \( h(D) \equiv 1 \) or \( D \) then one of the inner products is zero but the other is not (see the display shown in the proof of Theorem 2). If there were a run of length \( s + 2n - 1 \) there would have to be a run of \( s \) consecutive symbols where the inner product was zero. On one side or the other of these symbols there would have to be \( n \) more symbols from the alternating run of size \( s + 2n - 1 \). These \( n \) symbols together with \( s - n \) of the original \( s \) symbols would also have to have inner product zero contrary to the hypothesis.

**Corollary:** Suppose \( L(C) = \infty \) for \( C \). Recall from the previous section the codes \( C \) \((n,n-1)\) convolutional codes dual to the rows of \( F \), where \( F \) is a basic generator matrix for \( C \)\(^{\perp} \) and the obvious property

\[
n-1
\]

from which it follows that the maximum run of alternating symbols in any codeword of \( C \) has length \( L = L(C) \leq \min \{ L(C_i) \} \). Suppose \( L(C_i) \) is finite for at least one value of \( i \). Then, if \( d \) is the maximum degree of any element in the \( j \)th row of \( F \), it follows that

\[
L(C) < L(C_i) < \begin{cases} n(d+2)-2, & n \text{ even} \\ n(d+3)-2, & n \text{ odd}. \end{cases}
\]

**Corollary to Theorem 3:** Let \( C \) be an \((n,n-1)\) convolutional code over \( \text{GF}(2) \) with generator matrix for its dual code given by \( \{f_1, \ldots, f_s\} \), where \( (f_1, \ldots, f_s) = 1 \). Suppose no codeword of \( C \) contains a finite codeword with an infinite run of alternating symbols. In fact, since the sum of rows 1 and 3 of \( F \) has degree \( d = 3 \) it follows that the maximum run of alternating symbols is bounded above by \( n(d+2) \equiv 11 \mod (1+D^2) \).

**Proof:** Under these conditions \( C \)\(^{\perp} \) has a generator matrix \( F \) (a so-called minimal encoder for \( C \)\(^{\perp} \)) all of whose entries are of degree \( < \mu \). Thus the result follows immediately except when \( n \) is even and \( L(C_i) = \infty \) for some \( i = 1, \ldots, n-k \). Here if \( L \) is finite, \( \mu \) can be determined by replacing row \( i \) of \( F \) in turn by the sum of row \( i \) and row \( j \), for \( j = 1, \ldots, n-k \). Of course in general all this work will not be required but the point is that such transformations do not increase the maximum degree of the elements of the dual encoder and so the bound given above is valid here also.

### IV. Examples

Consider the \((3,2)\) code \( C \) generated by the encoder \( G \):

\[
\begin{bmatrix}
D^3 + D & D^3 + 1 & D^4 + D^2 + D + 1 \\
D & D^3 + D + 1 & D^2 + D^2 + 1 \\
D & D^2 + D + 1 & D \\
\end{bmatrix} \mod (1+D^2)
\]

Note that the sum of its rows is congruent to \([1, D, 1] \mod (1+D^2)\) and thus, by Theorem 1, \( C \) contains a codeword with an infinite run of alternating symbols.

As a second example, consider the \((4,1)\) code \( C \) with generator \( F \) of its dual code given by

\[
\begin{bmatrix}
D & D^2 + D + 1 & D^3 & D^3 + 1 \\
D^2 + D + 1 & D^3 + 1 & D^3 & D^3 + 1 \\
\end{bmatrix} \mod (1+D^2)
\]

Thus each row of \( F \) satisfies the congruences of Theorem 2 for some value of \( a \). But row 1 satisfies the congruence only for \( a = -1 \) and row 3 only for \( a = 1 \). Thus \( C \) does not contain a codeword with an infinite run of alternating symbols. In fact since the sum of rows 1 and 3 of \( F \) has degree \( d = 3 \) it follows that the maximum run of alternating symbols in any codeword of \( C \) is bounded above by \( n(d+2) \equiv 11 \mod (1+D^2) \). If we compute \( s \) here we get \( s = 14 \); so \( L < s + n - 2 = 16 \) is a little sharper. A basic generator for \( C \) is \([1+D^2+D^4+D^5+D^6+D^7+D^8, D^3+D^4]

### References

[364]

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-25, NO. 3, MAY 1979
Every permutation of the columns of this matrix yields a matrix whose row space contains \([1, 0, 1, 0]\) or \([0, 1, 0, 1]\).

ACKNOWLEDGMENT

The authors wish to thank M. K. Simon and J. G. Smith for bringing this problem to their attention and for suggesting several possible approaches.

REFERENCES


A Note on Optimal Quantization

JAMES A. BUCKLEW AND NEAL C. GALLAGHER, JR., MEMBER, IEEE

Abstract—For a general class of optimal quantizers the variance of the output is less than that of the input. Also the mean value is preserved by the quantizing operation.

I. INTRODUCTION

J. Max [1] is generally credited with being the first to consider the problem of designing a quantizer to minimize a distortion measure given that the input statistics are known. Max derives necessary conditions for minimizing the mean square quantization error. These results are summarized in the following equations:

\[ y_j = \int_{y_{j-1}}^{y_j} x f(x) \, dx / P(x_{j-1} < x < x_j) \]

\[ \frac{y_j + y_{j+1}}{2} = y_j \]

where \( f(x) \) is the probability density of the variable to be quantized and \( P(x_{j-1} < x < x_j) \) is the probability that \( x \) lies in the interval \( (x_{j-1}, x_j) \). The \( y_j \) are output levels and the \( x_j \) are the break points where an input value between \( x_{j-1} \) and \( x_j \) is quantized to \( y_j \). Fleischer [2] later gave a sufficient condition for Max’s equations to be the optimal set.

Typically, the above equations are intractable except for simple input densities, causing some researchers to derive approximate formulae for some common densities. Roe [3] derives an approximation for the input interval endpoints assuming that the signal and noise are independent and that no pseudo-independence of the sort considered by Widrow [4] is possible.

However, Wood’s derivation assumes the input density to be five times differentiable and that the quantizer input intervals be very small in order to truncate various Taylor series expansions. Furthermore, the derived expression for the output variance is dependent upon the input interval lengths and the input probability density function evaluated at the midpoints of these intervals.

In this note we derive a generalization of Wood’s results that eliminates a number of his approximations and generalizes the results to apply to more than just Max quantizers.

Manuscript received May 5, 1978; revised September 5, 1978. This work was supported in part by the National Science Foundation under Grant ENG-7682426 and in part by the Air Force Office of Scientific Research, Air Force Systems Command, USAF under Grant AFOSR-78-3605.

The authors are with the School of Engineering, Purdue University, West Lafayette, IN 47907.