Uniform Codes

JAMES L. MASSEY, MEMBER, IEEE

Abstract—For any prime-power q, it is shown that there exist q-ary convolutional codes with the equidistance property that every code word is at the same distance from all code words disagreeing in the information digits to be decoded. These codes are called "uniform codes" and it is shown that they can be encoded in a very simple manner. The block codes most similar to uniform codes are the maximal-length codes which also have the equidistance property. It is shown that the error performance of these classes of codes is nearly identical but that the uniform codes have simpler encoding circuits. This latter fact is of importance in space applications, which is the most likely use for these codes.

I. Introduction

In earlier work[1] we demonstrated the existence of low rate *binary* convolutional codes with the property that each code word was at the same distance from every word that disagrees in the information digits to be decoded. We called these *uniform codes* and showed that they could be readily decoded, with correction of many error patterns beyond the error-correcting radius guaranteed by the minimum distance, by the technique of threshold decoding.

In this paper we show the existence of *q-ary* uniform convolutional codes where q is any prime-power, i.e., such that there exists a finite field of q elements $GF(q)$. Our approach will lead naturally to extremely simple encoding circuits for *all* of the uniform codes. It will be shown that the uniform codes have error-correcting ability comparable to the familiar maximal-length block codes but that the encoding circuit for a uniform code is less complex than that for the equivalent maximal-length code. This fact is of some practical importance, since the most likely application for such low rate codes is in space communication systems,[2] where encoder complexity in the space vehicle is a prime consideration.

II. Existence of Uniform Codes

Consider the digital circuit shown in Fig. 1. It will be shown in this section that this circuit is an encoder for a uniform convolutional code.

The information digits, $i_0, i_1, i_2, \cdots$, in Fig. 1 are taken to be elements of $GF(q)$. The device labelled *M-tuple generator* is any device which generates repetitively in any order all q^M distinct M-tuples of elements of $GF(q)$ commencing with $(0, 0, \cdots 0)$. The simplest realization of this device would generally be an M-stage ring counter. Since an information digit enters the upper shift-register in Fig. 1 only when $(0, 0, \cdots 0)$ is generated, it is clear that q^M transmitted digits are formed for each information digit. Hence, the code rate is $R = q^{-M}$ information digits per transmitted digit. When the transmitted digits are grouped into "blocks" of q^M digits as shown in Fig. 1, the first digit in block-j is just i_j. Thus, the encoder is systematic, i.e., the information digits appear unchanged among the transmitted digits. The other transmitted digits are linear combinations of the preceding information digits (the coefficients in the sum being determined by the M-tuple generated when such a digit is formed), and hence, the code is a true convolutional code. The first information digit, i_0, affects the encoded digits over the first $M + 1$ "blocks" so the code *constraint length* is $n_A = (M + 1)q^M$ digits.

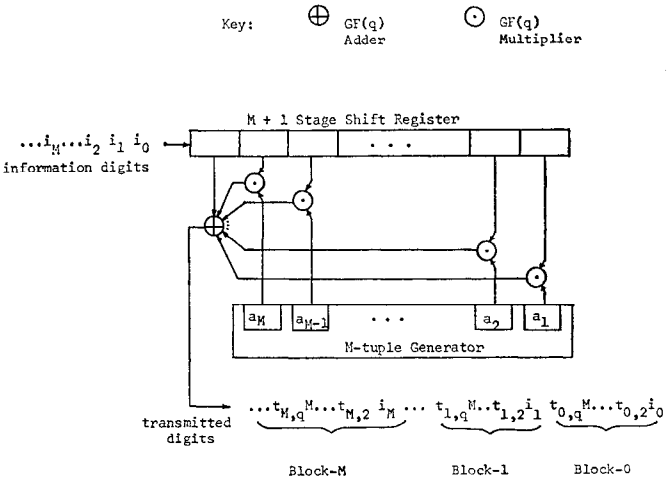

Fig. 1. Encoding circuit for uniform codes. NOTE: 1) The M-tuple generator is any device which generates repeatedly the set of all q^M M-tuples. 2) An information digit is shifted into the upper shift-register when and only when $\mathbf{a} = (0, 0, \ldots 0)$. 3) The upper shift-register is initially loaded with zeros.

The minimum distance $d_{\min}$ of a convolutional code is defined[3] to be the least number of positions in which there are disagreements among the first n_A encoded digits for any two encoded sequences corresponding to different values of i_0. Since the code is linear, it can be shown easily that $d_{\min}$ is also equal to the minimum Hamming weight $W_{\min}$ of all such sequences with $i_0 \neq 0$. Let W be the Hamming weight of some sequence of n_A digits with $i_0 \neq 0$. The average value of W is given by [4]

This work was supported by the Ames Research Center, National Aeronautics and Space Administration, under Contract NAS2-2874.

The author is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, Ind., and the Codex Corporation, Watertown, Mass.

[1] J. Massey, *Threshold Decoding*. Cambridge, Mass.: M.I.T. Press, 1963, pp. 46–48.

[2] A. Viterbi, "Phase-coherent communication over the continuous Gaussian channel," in *Digital Communication with Space Application*, S. W. Golomb, Ed. Englewood Cliffs, N. J.: Prentice-Hall, 1964, pp. 106–134.

[3] Massey, *op. cit.*,[1] p. 15.

[4] Massey, *ibid.*, p. 53.

$$W_{\text{avg}} = \frac{q-1}{q} n_A + q^{M-1}. \tag{1}$$

Substituting $n_A = (M+1)q^M$ into (1), we obtain

$$W_{\text{avg}} = [(M+1)(q-1)+1]q^{M-1}. \tag{2}$$

We next show that for the encoder in Fig. 1 every encoded sequence of length n_A with $i_0 \neq 0$ has Hamming weight $W = W_{\text{avg}}$. Hence, it follows $W_{\min} = W_{\text{avg}} = d_{\min}$ and the resulting convolutional code is a uniform code.

Let W_j be the Hamming weight of block-j in the encoded sequence formed by the encoder in Fig. 1, $j = 0, 1, \cdots M$. Clearly,

$$W = \sum_{j=0}^{M} W_j. \tag{3}$$

When $i_0 \neq 0$, all q^M digits in block-0 are nonzero, and hence,

$$W_0 = q^M. \tag{4}$$

Lemma

For $i_0 \neq 0$

$$W_j = (q-1)q^{M-1}, \qquad j = 1, 2, \cdots M. \tag{5}$$

Proof: The q^M digits in block-j are given by

$$i_j + a_M i_{j-1} + \cdots + a_1 i_{j-M} \tag{6}$$

where $\mathbf{a} = (a_1, a_2, \cdots a_M)$ ranges over the set of all q^M M-tuples of elements of $GF(q)$, and we take $i_k = 0$ for $k < 0$. We next show that this sum takes on each value of $GF(q)$ exactly q^{M-1} times. Without loss of generality, we may then suppose $i_j = 0$ in what follows.

Consider the sum

$$\sum(\mathbf{a}) = a_M i_{j-1} + a_{M-1} i_{j-2} + \cdots + a_1 i_{j-M}. \qquad 1 \leqq j \leqq M.$$

The M-tuples $\mathbf{a}$ such that $\sum(\mathbf{a}) = 0$ form a subgroup of the additive group of all M-tuples. Since $i_0 \neq 0$, there is at least one $\mathbf{a}$ such that $\sum(\mathbf{a})$ takes on any specified element β of $GF(q)$. For $\beta \neq 0$, the set of M-tuples $\mathbf{a}$ such that $\sum(\mathbf{a}) = \beta$ is a coset of the above subgroup, and hence, has the same number of M-tuples as the subgroup. Hence, $\sum(\mathbf{a})$ and thus the sum in (6) assumes each value of $GF(q)$ exactly $q^M/q = q^{M-1}$ times. There are $q-1$ nonzero elements in $GF(q)$ so that $W_j = (q-1)q^{M-1}$ as was to be shown.

Combining (3), (4), and (5), we obtain

$$W = q^M + M(q-1)q^{M-1}$$

or

$$W = [(M+1)(q-1)+1]q^{M-1}.$$

From (2), it then follows that $W = W_{\text{avg}}$, and hence, we have shown the following.

Theorem

For any integer M and any prime-power q, there exists a uniform convolutional code having

$$R = q^{-M}$$
$$n_A = (M+1)q^M$$

and

$$d_{\min} = W_{\text{avg}} = [(M+1)(q-1)+1]q^{M-1}.$$

This theorem can be generalized slightly as follows. Suppose that the information digits are read into the shift-register in Fig. 1 only every Ith time that $\mathbf{a} = (0, 0, \cdots 0)$. Clearly, this has the effect of repeating each transmitted block I times. Thus, the rate is divided by I while the constraint length and minimum distance are multiplied by I.

Corollary: For all integers I and M and any prime-power q, there exists a uniform convolutional code having

$$R = I^{-1}q^{-M}$$
$$n_A = I(M+1)q^M$$
$$d_{\min} = W_{\text{avg}} = I[(M+1)(q-1)+1]q^M.$$

III. Comparison to Maximal-Length Codes

The uniform codes are characterized by the "equidistance" structure of their code-word sets. In this section, the *convolutional* uniform codes are compared to the *block* maximal-length codes, a second class of codes with an equidistance property.

For any integer m and prime-power q, the well-known[5] maximal-length codes are q-ary block codes for which every code word is at the same distance from every other code word. Thus, $d_{\min} = W_{\text{avg}}$ for these codes where W_{avg} is the average Hamming weight of the nonzero code words. The rate R, constraint length n, and minimum distance $d_{\min}$ are given by:

$$R = \frac{m}{q^m - 1}$$
$$n = q^m - 1$$

and

$$d_{\min} = (q-1)q^{m-1}.$$

The maximal-length codes with $m = q^L$ have $R \approx q^{-(m-L)}$, and hence, are *equivalent in rate* to a uniform q-ary code with $M = m - L$. The minimum distance, $(q-1)q^{m-1}$, of the maximal length codes, for $qL > L + q$, slightly exceeds the minimum distance,

$$(q-1)q^{m-1} - (qL - q - L)q^{m-L-1},$$

of the equivalent uniform codes. However, the constraint length $q^m - 1$ of the maximal-length codes, for $L > 1$,

[5] W. Peterson, *Error-Correcting Codes*. Cambridge, Mass.: M.I.T. Press, and New York: Wiley, 1961, pp. 147–148.

TABLE I
COMPARISON OF EQUIVALENT BINARY UNIFORM CONVOLUTIONAL CODES AND MAXIMAL-LENGTH BLOCK CODES

Maximal-Length Codes						Uniform Codes					
m	R	n	$d_{\min}$	$\frac{d_{\min}}{n}$	Encoding Stages	M	R	n_A	$d_{\min}$	$d_{\min}/n_A$	Encoding Stages
4	4/15	15	8	2/3	8	2	1/4	12	8	3/4	5
8	8/255	255	128	128/255	16	5	1/32	192	112	7/12	11
16	$\sim 2^{-12}$	$2^{16} - 1$	2^{15}	$\sim 1/2$	32	12	2^{-12}	13×2^{12}	7×2^{12}	7/13	25
32	$\sim 2^{-27}$	$2^{32} - 1$	2^{31}	$\sim 1/2$	64	27	2^{-27}	7×2^{29}	29×2^{26}	29/56	55

exceeds slightly the constraint length $q^m - (L-1)q^{m-L}$ of the equivalent convolutional codes. A table of equivalent binary codes is given in Table 1 and shows that the $d_{\min}/n_A$ ratio favors the uniform codes slightly. For both classes of codes, any error pattern of weight $(d_{\min} - 1)/2$ or less is guaranteed correctable.

The best criterion for code comparison is generally the error probability per decoded digit on a standard channel. When a decoding error occurs in the binary block maximal-length codes, half of the m information digits will be decoded incorrectly on the average. Thus, the block error probability, which is the quantity determined by the minimum distance, should be multiplied by $m/2$ to give the decoded bit error probability. The minimum distance of the convolutional code, on the other hand, determines the probability of incorrectly decoding a single information bit. Because of the error propagation effect[6] in convolutional codes, this quantity must be multiplied by the average number of decoding errors triggered by the first decoding mistake. Experimental evidence for binary codes suggests that this number is on the order of M. Since $M = m - L$ for the equivalent rate uniform code, the multiplying factor M of the equivalent uniform code is not substantially different from that of the maximal length code. The over-all conclusion is that equivalent rate maximal-length codes and uniform codes do not differ significantly in error-correcting power since they have very nearly the same constraint length and minimum distance.

There is a difference, however, in encoder complexity for equivalent rate codes. A maximal-length code can be encoded by means of an m-stage maximal-length shift-register in which the m information digits are initially loaded and which is then shifted $q^m - 1$ times. An m-stage counter is thus required to determine when the encoding is completed. Thus, a total of $2m$ register stages are required. The equivalent uniform code, when encoded by the circuit in Fig. 1, requires an $(M+1)$-stage feedback-free shift register plus an M-stage counter or a total of $2M + 1 = 2(m - L) + 1$ stages of register which is always less than that of the block code. Since $m = q^L$, the difference is about $2 \log_q m$ stages which can be a significant savings in space applications.

We have neglected to this point the complexity of the $GF(q)$ multipliers required in the encoding circuit of Fig. 1 for the uniform codes. For the binary case, each of these units is a two-input AND gate, but can be an appreciable circuit for larger q. For $q > 2$, the encoder for the maximal-length codes requires circuits which multiply by a constant in $GF(q)$, but these circuits are easier to build than full multipliers. We have also neglected the timing circuitry and buffering of information digits that is required in the encoding circuit for the maximal-length codes because of the block format. This is not required for the uniform codes, since the encoding circuit of Fig. 1 accepts the information digits in a continuous periodic stream and acts simply as a digital filter. In general, quantitative comparison of these neglected factors is difficult because they are highly dependent on the specific logical circuitry chosen for the encoder. There seems to be no evidence that these factors would negate the conclusion that the encoding circuit for the uniform codes is simpler than that for the maximal-length codes.

ACKNOWLEDGMENT

The author is indebted to Dr. R. G. Gallager of the Codex Corporation for a valuable suggestion in connection with the encoding circuit of Fig. 1.

[6] J. Massey and R. Liu, "Application of Lyapunov's direct method to the error-propagation effect in convolutional codes," *IEEE Trans. on Information Theory (Correspondence)*, vol. IT-10, pp. 248–250, July 1964.