Some long rate one-half binary convolutional codes with an optimum distance profile

Johannesson, Rolf

Published in:
IEEE Transactions on Information Theory

1976

where O is the M-by-M cyclic permutation matrix (28) and $A(i)$ is defined in (4).

Let us first consider the case $M = 2\nu - 1$. Define the following M-by-M matrices:

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{2(\nu-1)} \\ 1 & \bar{\epsilon} & \bar{\epsilon}^2 & \bar{\epsilon}^3 & \cdots & \bar{\epsilon}^{2(\nu-1)} \\ 1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \cdots & \epsilon^{4(\nu-1)} \\ 1 & \bar{\epsilon}^2 & \bar{\epsilon}^4 & \bar{\epsilon}^6 & \cdots & \bar{\epsilon}^{4(\nu-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \epsilon^{\nu-1} & \cdots & \cdots & \cdots & \cdots \\ 1 & \bar{\epsilon}^{\nu-1} & \cdots & \cdots & \cdots & \cdots \end{pmatrix} \tag{A.2}$$

$$T = \operatorname{diag}\left(1, \begin{pmatrix} 1 & 1 \\ j & -j \end{pmatrix}, \cdots, \begin{pmatrix} 1 & 1 \\ j & -j \end{pmatrix}\right) \tag{A.3}$$

and

$$B = M \operatorname{diag}(1,2,2,2,\cdots,2) \tag{A.4}$$

where

$$\epsilon = \exp j\frac{2\pi}{M} \qquad \bar{\epsilon} = \exp -j\frac{2\pi}{M}. \tag{A.5}$$

We have

$$P = B^{-1/2}TQ. \tag{A.6}$$

Proof: By direct computation, it is easy to show that

$$QOQ^T = M \operatorname{diag}\left(1, \begin{pmatrix} 0 & \epsilon \\ \bar{\epsilon} & 0 \end{pmatrix}, \begin{pmatrix} 0 & \epsilon^2 \\ \bar{\epsilon}^2 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & \epsilon^{\nu-1} \\ \bar{\epsilon}^{\nu-1} & 0 \end{pmatrix}\right). \tag{A.7}$$

Since T and QOQ^T exhibit a quasidiagonal form, to compute $T(QOQ^T)T^T$ it is sufficient to consider only the product

$$\begin{pmatrix} 1 & 1 \\ j & -j \end{pmatrix}\begin{pmatrix} 0 & \epsilon^h \\ \bar{\epsilon}^h & 0 \end{pmatrix}\begin{pmatrix} 1 & j \\ 1 & -j \end{pmatrix} = \begin{pmatrix} 2\cos\frac{2\pi}{M}h & 2\sin\frac{2\pi}{M}h \\ -2\sin\frac{2\pi}{M}h & 2\cos\frac{2\pi}{M}h \end{pmatrix} \tag{A.8}$$

Thus

$$TQOQ^TT^T = M \operatorname{diag}\left(1, \begin{pmatrix} 2\cos\frac{2\pi}{M} & 2\sin\frac{2\pi}{M} \\ -2\sin\frac{2\pi}{M} & 2\cos\frac{2\pi}{M} \end{pmatrix}, \cdots, \begin{pmatrix} 2\cos\frac{2\pi}{M}(\nu-1) & 2\sin\frac{2\pi}{M}(\nu-1) \\ -2\sin\frac{2\pi}{M}(\nu-1) & 2\cos\frac{2\pi}{M}(\nu-1) \end{pmatrix}\right) \tag{A.9}$$

Premultiplying and postmultiplying (A.9) by $B^{-1/2}$ and taking into account (A.6), we see that (A.1) holds true. Hence, we have only to show that P is orthogonal. By direct computation, we get

$$(TQ)(TQ)^T = B$$

so that

$$(B^{-1/2}TQ)(B^{-1/2}TQ)^T = I$$

and $P = B^{-1/2}TQ$ is orthogonal. Q.E.D.

The construction of P when $M = 2\nu$ is similar, provided that the M-by-M matrices Q,T, and B are defined as follows:

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 1 & -1 & \cdots & -1 \\ 1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{2\nu-1} \\ 1 & \bar{\epsilon} & \bar{\epsilon}^2 & \bar{\epsilon}^3 & \cdots & \bar{\epsilon}^{2\nu-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \epsilon^{\nu} & \cdots & \cdots & \cdots & \cdots \\ 1 & \bar{\epsilon}^{\nu} & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

$$T = \operatorname{diag}\left(1,1, \begin{pmatrix} 1 & 1 \\ j & -j \end{pmatrix}, \cdots, \begin{pmatrix} 1 & 1 \\ j & -j \end{pmatrix}\right)$$

$$B = M \operatorname{diag}(1,1,2,2,\cdots,2).$$

References

[1] D. Slepian, "large signalling alphabets generated by groups," unpublished Memorandum, Bell Labs., 1951.

[2] ——, "Group codes for the Gaussian channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575–602, Apr. 1968.

[3] ——, "Permutation modulation," *Proc. IEEE*, vol. 53, pp. 228–236, Mar. 1965.

[4] I. Jacobs, "Comparison of M-ary modulation systems," *Bell Syst. Tech. J.*, vol. 46, pp. 843–864, May–June 1967.

[5] E. Biglieri and M. Elia, "On the existence of group codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 399–402, May 1972.

[6] J. S. Lomont, *Applications of Finite Groups*. New York: Academic, 1959.

[7] I. Ingemarsson, "Signal sets generated by orthogonal transformations of the signal space," Tech. Rep. 21, Royal Inst. Technol., Stockholm, Sweden, Feb. 1969.

[8] ——, "Commutative group codes for the Gaussian channel," Tech. Rep. 35, Royal Inst. Technol., Stockholm, Sweden, Apr. 1970.

[9] ——, "Commutative group codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 215–219, Mar. 1973.

[10] E. A. Guillemin, *The Mathematics of Circuit Analysis*. New York: Wiley, 1949.

[11] S. I. Gass, *Linear Programming*. New York: McGraw-Hill, 1958.

[12] M. Sakarovitch, *Notes on Linear Programming*. New York: Van Nostrand, 1972.

[13] G. Dantzig, *Linear Programming and Extensions*. Princeton: Princeton Univ. Press, 1963.

Some Long Rate One-Half Binary Convolutional Codes with an Optimum Distance Profile

ROLF JOHANNESSON, MEMBER, IEEE

***Abstract*—This correspondence gives a tabulation of long systematic, and long quick-look-in (QLI) nonsystematic, rate $R = \frac{1}{2}$ binary convolutional codes with an optimum distance profile (ODP). These codes appear attractive for use with sequential decoders.**

In this correspondence we report the results of computer searches for long rate $R = \frac{1}{2}$ fixed convolutional encoders (FCE's) with an *optimum distance profile* (ODP codes), i.e., with a distance profile equal to or superior to that of any other code with

Manuscript received September 2, 1975; revised January 26, 1976. This work was supported in part by the National Aeronautics and Space Administration under NASA Grant NSG 5025 at the University of Notre Dame in liaison with the Communications and Navigation Division of the Goddard Space Flight Center and in part by the Swedish Board of Technical Development under Grant 75-4165.

The author is with the Department of Automata and General Systems Sciences, University of Lund, Lund, Sweden.

TABLE I
ODP SYSTEMATIC CONVOLUTIONAL CODES WITH RATE $R = 1/2$

M	$G^{(2)}$	d_M	# paths
36	6711454544704	14	5
37	6711454544676	14	2
38	671145457556 4	15	31
39	7144616573 4534	15	12
40	671145457557 12	15	3
41	7144616573 4537	15	1
42	6711454575564 64	16	31
43	7144616265540 12	16	14
44	7144616265544 27	16	5
45	7144616265544 274	16	1
46	6711454575564666	17	39
47	6711454575564667	17	13
48	6711454575564 6674	17	4
49	6711454575564 6676	17	1
50	6711454575564 6676	18	38
51	6711454575564 66760	18	16
52	6711454575564 66760	18	7
53	7144616265532 60462	18	2
54	7144616265556 137204	19	43
55	7144616265556 137206	19	20
56	7144616265556 137206	19	7
57	7144616265556 1372064	19	2
58	7144616265556 1372064	20	60
59	6711454575564 6670367	20	25
60	6711454575564 66703670	20	10

TABLE II
ODP QLI CONVOLUTIONAL CODES WITH $R = 1/2$

M	$G^{(1)}$	$G^{(2)}$	d_M	# paths
24	740424174	540424174	11	11
25	740415562	540415562	11	5
26	740424173	540424173	11	1
27	7404241724	5404241724	12	23
28	7404241712	5404241712	12	8
29	7404241713	5404241713	12	2
30	74042402074	54042402074	13	43
31	74042402072	54042402072	13	15
32	74042402071	54042402071	13	4
33	74042402071 4	54042402071 4	13	1
34	74042402071 2	54042402071 2	14	34
35	74042402663 7	54042402663 7	14	14
36	74042402663 64	54042402663 64	14	5
37	74042402663 62	54042402663 62	14	2
38	74042402071 21	54042402071 21	15	31
39	74042417136 114	54042417136 114	15	12
40	74042402071 132	54042402071 132	15	3
41	74042417136 111	54042417136 111	15	1
42	74042402071 2164	54042402071 2164	16	31
43	74042402071 2166	54042402071 2166	16	14
44	74042402071 3351	54042402071 3351	16	5
45	74042402071 33514	54042402071 33514	16	1
46	74042402071 21636	54042402071 21636	17	39
47	74042402071 21635	54042402071 21635	17	13
48	74042402071 216354	54042402071 216354	17	4
49	74042402071 216356	54042402071 216356	17	1
50	74042402071 216357	54042402071 216357	18	38

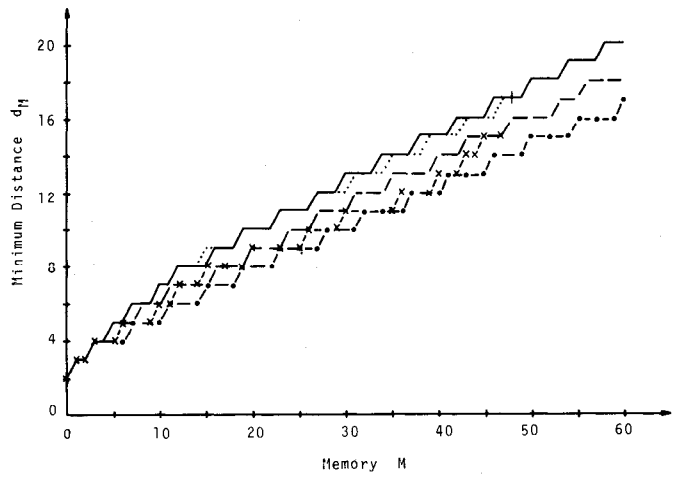

Fig. 1. Minimum distance d_M for some rate $1/2$ convolutional codes. — d_M for ODP codes; ····· d_M for codes of Bussgang ($0 \leq M \leq 15$), Lin–Lyne ($16 \leq M \leq 20$), and Forney ($21 \leq M \leq 48$); - - - - - d_M for systematic Costello A1 codes; x - x - x - x - d_M for Massey–Costello QLI codes ($0 \leq M \leq 47$); - - - - - - - Gilbert bound.

the same *memory* M. In a recent paper [1], we introduced the $(M + 1)$-tuple $\boldsymbol{d} = [d_0, d_1, \cdots, d_M]$ and called it the *distance profile* of the FCE, where d_j is the jth order *column distance* [2], i.e., the minimum Hamming distance between any two encoded paths of length $(j + 1)$ branches, in the infinitely long trellis defined by the FCE, resulting from information sequences with a differing first branch. In particular, d_M is called the *minimum distance* and d_∞ is called the *free distance* of the FCE. When comparing two codes of the same memory and rate, we say that a distance profile $\boldsymbol{d}$ is superior to a distance profile $\boldsymbol{d}'$ when there is some n such that

$$d_j \begin{cases} = d'_j, & j = 0,1,\cdots,n-1 \\ > d'_j, & j = n. \end{cases}$$

Thus $\boldsymbol{d} > \boldsymbol{d}'$ implies that the "early growth" of d_j with j is greater than that of d'_j with j. (It could, of course, happen that for sufficiently large j, $d_j < d'_j$.)

Systematic ODP codes are already known for $M \leq 35$ [1]. Newly found systematic ODP codes are listed in Table I for $36 \leq M \leq 60$. The code generators are given in an octal form according to the convention in [1]. In cases where the optimum code is not unique, ties were resolved using the number of low-weight paths as a further optimality criterion.

Massey and Costello [3] introduced a class of quick-look-in (QLI) nonsystematic codes in which the two generators differ only in the second position. In Table II, we list newly found ODP QLI codes for $24 \leq M \leq 50$. For $M \leq 23$ such codes are already known [1].

The excellence as regards d_M for the ODP codes can be seen from Fig. 1 in which we have plotted d_M for these codes; the best of the systematic codes found by Bussgang [4], Lin–Lyne [5], and Forney [6]; Costello's Algorithm A1 systematic codes [2]; and Massey–Costello's QLI codes [2], [3]. The codes are also compared with the Gilbert bound [2], [4]. We notice that the newly found codes have d_M equal to or superior to that of any previously known code with the same memory.

REFERENCES

[1] R. Johannesson, "Robustly-optimal rate one-half binary convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 464–468, July 1975.
[2] D. J. Costello, Jr., "A construction technique for random-error-correcting convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 631–636, Sept. 1969.
[3] J. L. Massey and D. J. Costello, Jr., "Nonsystematic convolutional

codes for sequential decoding in space applications," *IEEE Trans. Commun. Technol.*, vol. COM-19, pp. 806–813, Oct. 1971.
[4] J. J. Bussgang, "Some properties of binary convolutional code generators," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 90–100, Jan. 1965.
[5] S. Lin and H. Lyne, "Some results on binary convolutional code generators," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 134–139, Jan. 1967.
[6] G. D. Forney, Jr., "Use of a sequential decoder to analyze convolutional code structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 793–795, Nov. 1970.

Some Two-Weight Codes with Composite Parity-Check Polynomials

TOR HELLESETH

***Abstract*—The Hamming weight enumerator polynomials of some two-weight codes are presented. The codes have parity-check polynomials which are products of two irreducible polynomials.**

I. Introduction

Let ψ be a primitive element of $GF(q^k)$. Let $h_d(x) \in GF(q)[x]$ denote the minimum polynomial of ψ^d. Then $h_d(x)$ is a primitive polynomial if and only if gcd $(d,q^k - 1) = 1$.

It is well known that codes which have primitive parity-check polynomials are equidistant in the Hamming metric. In Kjeldsen [2] and Oganesyan, Yagdzyan, and Tairyan [3], some other cyclic equidistant codes are found. From the papers of Semakov and Zinov'ev [4] and Semakov, Zinov'ev, and Zaitsev [5], it can be concluded that every equidistant cyclic code has an irreducible parity-check polynomial.

Here we study codes that have parity-check polynomials which are the product of two irreducible polynomials. Since the codes do not have an irreducible parity-check polynomial, at least two nonzero Hamming weights must occur in the codewords. We present here a family of nonbinary cyclic codes with composite parity-check polynomials such that only two nonzero weights occur.

Some of the codes have parity-check polynomials which are a product of two primitive polynomials of the same degree. The complete weight enumerator of such codes has been studied indirectly by studying the cross-correlation function between two maximal-length linear sequences. In Helleseth [1], it is proved that, for $q = p^n$, where p is a prime and $n = 1$, at least three different nonzero weights occur in the complete weight enumerator. In particular, if we consider instead the Hamming weight enumerator, it is possible to achieve only two nonzero weights.

II. The Two-Weight Codes

Let deg $h(x)$ denote the degree of $h(x)$ and let per $h(x)$ denote the least positive integer r such that $h(x)$ divides $x^r - 1$.

Lemma: Let gcd (k,N_1) = gcd (k,N_2) = gcd $(t,N_2) = 1$, where N_1 and N_2 divide $q - 1$. Let $d_1 = (q^k - 1)/N_1 + 1$ and $d_2 = t(q^k - 1)/N_2 + 1$. Then we have that

i) deg $h_{d_1}(x)$ = deg $h_{d_2}(x) = k$;
ii) per $h_{d_1}(x) = (q^k - 1)/\gcd(d_1,N_1)$,
per $h_{d_2}(x) = (q^k - 1)/\gcd(d_2,N_2)$;
iii) let $d_1 \not\equiv q^i d_2 \pmod{q^k - 1}$, for all $i \geq 0$; let $h(x) = h_{d_1}(x)h_{d_2}(x)$, then per $h(x) = (q^k - 1)/\gcd(d_1,d_2,N_1,N_2)$.

Proof: i) Let deg $h_{d_1}(x) = m$. By definition, m is the least positive integer such that

$$(\psi^{(q^k-1)/N_1+1})^{q^m-1} = 1.$$

Therefore

$$((q^k - 1)/N_1 + 1)(q^m - 1) \equiv 0 \pmod{q^k - 1}.$$

Since N_1 divides $q - 1$, this means

$$q^m - 1 \equiv 0 \pmod{q^k - 1}.$$

Hence $m \geq k$ and, therefore, $m = k$. The proof that deg $h_{d_2}(x) = k$ is similar.

ii) Since gcd $(d_i,q^k - 1)$ = gcd (d_i,N_i), for $i = 1, 2$, we have

$$\begin{aligned}\text{per } h_{d_i}(x) &= (q^k - 1)/\gcd(d_i,q^k - 1)\\ &= (q^k - 1)/\gcd(d_i,N_i).\end{aligned}$$

iii) Since $d_1 \not\equiv q^i d_2 \pmod{q^k - 1}$, for all $i \geq 0$, we have gcd $(h_{d_1}(x),h_{d_2}(x)) = 1$. Hence

$$\begin{aligned}\text{per } h(x) &= \text{lcm}(\text{per } h_{d_1}(x), \text{per } h_{d_2}(x))\\ &= \frac{(q^k - 1)^2/(\gcd(d_1,N_1)\gcd(d_2,N_2))}{\gcd((q^k - 1)/\gcd(d_1,N_1),(q^k - 1)/\gcd(d_2,N_2))}\\ &= (q^k - 1)/\gcd(d_1,d_2,N_1,N_2).\end{aligned}$$

We are now able to prove the main theorem.

Theorem: Let d_1 and d_2 be defined as in the lemma. Put $N = \text{lcm}(N_1,N_2)$. Suppose gcd $(d_1,d_2,N_1,N_2) = 1$. Let V be the $(q^k - 1,2k)$ cyclic code with parity-check polynomial $h(x) = h_{d_1}(x)h_{d_2}(x)$. Then the weight enumerator polynomial of V is

$$A(z) = 1 + (q^k - 1)\frac{N}{u} z^{q^{k-1}(q-1)-q^{k-1}(q-1)u/N} + \left(q^{2k} - 1 - (q^k - 1)\frac{N}{u}\right) z^{q^{k-1}(q-1)}$$

where

$$u = \gcd\left(N, \frac{N}{N_1} - t\frac{N}{N_2}\right).$$

Proof: By iii) of the lemma, we have per $h(x) = q^k - 1$. Let $a_1,a_2 \in GF(q^k)$. Let $\mathbf{v}(a_1,a_2) = (v_0,v_1,\cdots,v_{q^k-2})$ with

$$v_j = \text{tr}_1^k(a_1\psi^{d_1 j} + a_2\psi^{d_2 j}),$$

where

$$\text{tr}_1^k(x) = \sum_{i=0}^{k-1} x^{q^i}.$$

We then have

$$V = \{\mathbf{v}(a_1,a_2) | a_1,a_2 \in GF(q^k)\}.$$

Let $j = Nj_2 + j_1$, with $0 \leq j_2 < (q^k - 1)/N$ and $0 \leq j_1 < N$. Then

$$\begin{aligned}v_j &= \text{tr}_1^k(a_1\psi^{d_1(Nj_2+j_1)} + a_2\psi^{d_2(Nj_2+j_1)})\\ &= \text{tr}_1^k(a_1\psi^{Nj_2+d_1 j_1} + a_2\psi^{Nj_2+d_2 j_1}),\end{aligned}$$

since $d_i N = ((q^k - 1)/N_1 + 1)N \equiv N \pmod{q^k - 1}$, for $i = 1,2$. Therefore

$$v_{Nj_2+j_1} = \text{tr}_1^k(\psi^{Nj_2}(a_1\psi^{d_1 j_1} + a_2\psi^{d_2 j_1})).$$

Let $T(a) = |\{j | tr_1^k(a\psi^{Nj}) \neq 0, 0 \leq j < (q^k - 1)/N\}|$. From Oganesyan, Yagdzyan, and Tairyan [3, p. 220] we have

$$T(a) = \begin{cases}0, & \text{if } a = 0\\ q^{k-1}(q-1)/N, & \text{if } a \neq 0.\end{cases}$$

Let

$$S(a_1,a_2) = |\{j_1 | a_1\psi^{d_1 j_1} + a_2\psi^{d_2 j_1} = 0, 0 \leq j_1 < N\}|.$$

Manuscript received October 28, 1975.
The author is with the Matematisk Institutt, Universitetet i Bergen, Bergen, Norway.