Robustly-optimal rate one-half binary convolutional codes

Johannesson, Rolf

Published in:
IEEE Transactions on Information Theory

1975

TABLE II
ONE MAXPOL FOR GIVEN DEGREE

Degree	MAXPOL	Exponent	Degree	MAXPOL	Exponent
4	$P_0^{2}P_1$	6	20	$P_0^{6}P_1P_2P_4$	2040
5	$P_0^{3}P_1$	12	21	$P_0^{5}P_1P_2G_5$	3720
6	P_1P_2	15	22	$P_1P_2P_8$	3855
7	$P_0^{5}P_1$	24	23	$P_0^{3}P_1P_2G_7$	7620
8	$P_0^{2}P_1P_2$	30	24	$P_1P_2P_4G_5$	7905
9	$P_0^{3}P_1P_2$	60	25	$P_0^{3}P_1P_2P_8$	15420
10	$P_0^{4}P_1P_2$	60	26	$P_0^{2}P_1P_2P_4G_5$	15810
11	$P_0^{5}P_1P_2$	120	27	$P_0^{3}P_1P_2P_4G_5$	31620
12	$P_0^{6}P_1P_2$	120	28	$P_1P_2P_4G_7$	32385
13	$P_0^{3}P_1P_4$	204	29	$P_0^{5}P_1P_2P_4G_5$	63240
14	$P_1P_2P_4$	255	30	$P_1P_2P_4P_8$	65535
15	$P_0^{3}P_1P_2G_3$	420	31	$P_0^{3}P_1P_2P_4G_7$	129540
16	$P_0^{2}P_1P_2P_4$	510	32	$P_0^{2}P_1P_2P_4P_8$	131070
17	$P_0^{3}P_1P_2P_4$	1020	33	$P_0^{3}P_1P_2P_4P_8$	262140
18	$P_0^{4}P_1P_2P_4$	1020	34	$P_0^{4}P_1P_2P_4P_8$	262140
19	$P_0^{5}P_1P_2P_4$	2040			

This theorem establishes a reduced exhaustive search method for a MAXPOL of any given degree. One searches all k, the m_i, and the m_j such that $k \geq 0$, $r = k + 2(\Sigma m_i + \Sigma m_j)$, $m_i \geq 1$, $m_j \geq 3$, and $m_i \neq m_j$. Compute the exponent by

$$e = \lceil \log_2 k \rceil [\operatorname*{lcm}_{i,j} \{(2^{m_i} + 1),(2^{m_j} - 1)\}]$$

and keep the combination that yields the maximum e. ($\lceil x \rceil$ denotes the upper integer part of x.) This search was programmed in a simple APL routine that produced the list in Table II of one MAXPOL per given degree. We observe that the MAXPOL exponents are very near to $2^{(r+3)/2}$ for which we have no explanation at this time.

REFERENCES

[1] J. L. Massey, "Reversible codes," *Inform. Contr.*, vol. 7, pp. 369–380, 1964.
[2] W. W. Peterson, *Error-Correcting Codes*. Cambridge, Mass.: M.I.T. Press, 1961.
[3] P. Hsieh and M. Y. Hsiao, "Error-correcting codes—solutions," IBM TR00.1221, Dec. 14, 1964, p. 55.

Robustly Optimal Rate One-Half Binary Convolutional Codes

ROLF JOHANNESSON

Abstract—**Three optimality criteria for convolutional codes are considered in this correspondence: namely, free distance, minimum distance, and distance profile. Here we report the results of computer searches for rate one-half binary convolutional codes that are "robustly optimal" in the sense of being optimal for one criterion and optimal or near-optimal for the other two criteria. Comparisons with previously known codes are made. The results of a computer simulation are reported to show the importance of the distance profile to computational performance with sequential decoding.**

Manuscript received August 14, 1974. This work was supported by the National Aeronautics and Space Administration under Grant NGL 15-004-026 at the University of Notre Dame in liaison with the Communications and Navigation Division, Goddard Space Flight Center.
The author was with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, Ind. 46556. He is now with Telecommunication Theory, Lund Institute of Technology, Lund, Sweden.

Several distance measures have been proposed for convolutional codes, each of which is important for particular applications. In this correspondence we report the results of the search for "robustly optimal" convolutional codes, i.e., codes that are optimal for one distance measure and are also optimal or near-optimal for the other two distance measures. We have limited the search to binary codes of rate $R = \frac{1}{2}$ as the case of greatest practical interest.

In a rate $R = \frac{1}{2}$ binary convolutional code, the information sequence $i_0,i_1,i_2,\cdots$ is encoded as the sequence

$$t_0^{(1)},t_0^{(2)},t_1^{(1)},t_1^{(2)},t_2^{(1)},t_2^{(2)},\cdots$$

where

$$t_u^{(k)} = \sum_{j=0}^{M} i_{u-j}\, g_j^{(k)}.$$

The parameter M is the code *memory* and

$$G^{(k)} = [g_0^{(k)},g_1^{(k)},\cdots,g_M^{(k)}]$$

for $k = 1,2$, are the code *generators*. The code is systematic when $G^{(1)} = [1,0,\cdots,0]$. The code is a *quick-look-in* (QLI) code [1] when

$$g_j^{(2)} = \begin{cases} g_j^{(1)}, & j \neq 1 \\ 1 + g_1^{(1)}, & j = 1. \end{cases}$$

QLI codes have some advantages in recovering the information sequence from the encoded sequence compared to general nonsystematic codes.

We shall find it convenient to write

$$\boldsymbol{t}_{[0,n]} = (t_0^{(1)},t_0^{(2)},t_1^{(1)},t_1^{(2)},\cdots,t_n^{(1)},t_n^{(2)})$$

for the encoded path containing the first $n + 1$ "branches" of the encoded sequence. The encoded path $\boldsymbol{t}_{[0,M]}$ is called the *first constraint length* of the code. The jth order *column distance* [2] d_j is the minimum Hamming distance between some $\boldsymbol{t}_{[0,j]}$ resulting from an information sequence with $i_0 = 1$ and some $\boldsymbol{t}_{[0,j]}$ with $i_0 = 0$. By linearity, d_j is also the minimum of the Hamming weights of the paths $\boldsymbol{t}_{[0,j]}$ resulting from information sequences with $i_0 = 1$.

The quantity d_M is called the *minimum distance* of the convolutional code and determines the guaranteed error-correcting capability when the code is decoded by a "feedback decoder" [3]. The quantity d_∞ is called the *free distance* of the code and has been found to be the principal determiner of decoding error probability when maximum-likelihood (or nearly so) decoding is used, i.e., for Viterbi decoding or sequential decoding [1], [4].

It has also been observed [1] that for good computational performance with sequential decoding, the column distances should "grow as rapidly as possible." We are led then to define the *distance profile* of the code as the $(M + 1)$-tuple

$$\boldsymbol{d} = [d_0,d_1,\cdots,d_M]$$

and to 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, $d_j < d_j'$.)

We notice that only in the range $0 \leq j \leq M$ is each branch on a path $\boldsymbol{t}_{[0,j]}$ affected by a new portion of the generator as one penetrates into the tree. The great dependence of the branches thereafter militates against the semi-infinite choice $\boldsymbol{d}_\infty =$

TABLE I
ODP SYSTEMATIC CONVOLUTIONAL CODES WITH RATE ½ WHICH ARE ALSO OMD CODES

M	$G^{(2)}$		d_M	#paths	d_∞	#paths
1	6	B	3	2	3	1
2	7	B	3	1	4	2
3	64	B	4	3	4	1
4	72	B	4	1	5	2
5	73	B	5	5	6	3
6	730	B	5	2	6	3
	734		5	3	6	1
7	714	B	6	11	6	2
8	715	B	6	5	7	2
	671		6	6	7	1
9	6710	B	6	1	7	1
	7154		6	3	8	4
10	6710	B	7	12	7	1
	7152		7	13	8	3
11	6711	B	7	5	8	2
	7153		7	6	9	3
12	67114	B	8	29	9	1
13	67114	B	8	12	9	1
14	67115		8	6	10	4

Note: B denotes that this generator was previously found by Bussgang [6].

TABLE II
ODP SYSTEMATIC CONVOLUTIONAL CODES WITH RATE ½

M	$G^{(2)}$	d_M	#paths	d_∞	#paths
15	714474	8	1	10	1
16	714476	9	18	10	1
	671166	9	22	12	13
17	671145	9	7	11	1
	671166	9	13	12	13
18	6711454	9	3	12	4
19	7144616	10	31	12	3
20	7144616	10	13	12	3
	7144761	10	18	12	1
21	67114544	10	4	12	1
22	71446162	10	1	13	2
	71446166	10	6	14	6
23	67114543	11	27	14	6
	67115143	11	32	14	2
24	714461654	11	11	15	5
	671151434	11	16	15	4
25	714461654	11	5	15	5
	671145536	11	9	15	3
26	671145431	11	1	15	1
	671151433	11	4	16	8
27	7144616264	12	21	14L	1
	7144760524	12	26	16	7
28	6711454306	12	8	16	4
	6711514332	12	13	16	3
29	7144616573	12	2	17L	3
	7144760535	12	6	18	22
30	71446162654	13	43	16L	2
	67114543064	13	44	16L	1
31	71446162654	13	15	16L	2
	67114543066	13	24	18	11
32	71446162655	13	4	17L	2
	71447605247	13	13	18L	2
33	714461626554	13	1	18L	5
	671145430654	13	4	18L	1
34	714461626554	14	34	18L	5
	714461625306	14	42	18L	1
35	714461625313	14	14	18L	3
	714461626555	14	19	19L	2

Note: L denotes that this number is actually d_{71} which is a lower bound on d_∞.

$[d_1,d_2,\cdots,d_\infty]$, as does the fact that d_∞ is probably a description of the remainder of the column distances, which is quite adequate for all practical purposes.

We shall say that a code is an *optimum minimum distance* (OMD) code (or an *optimum free distance* (OFD) code or an *optimum distance profile* (ODP) code) when its minimum distance (or free distance or distance profile) is equal to or superior to that of any code with the same memory.

In Tables I–V we report the results of computer searches for binary convolutional codes that are robustly-optimal, i.e., optimal for one of the preceding distance measures and optimal or near-optimal for the other two. In cases where the optimum code is not unique, we have chosen a code with the fewest number of low-weight paths for the distance measure in question, e.g.,

TABLE III
ODP QLI CODES WITH RATE ½

M	$G^{(1)}$	$G^{(2)}$	d_M	#paths	d_∞	#paths
1	6	4	3	2	3	1
2	7	5	3	1	5	1
3	74	54	4	3	6	1
4	72	52	4	1	6	1
5	71	51	5	5	7	1
	75	55	5	6	8	2
6	704	504	5	2	7	1
	714	514	5	3	8	1
7	742	542	6	11	9	1
8	742	542	6	5	9	1
9	7404	5404	6	1	9	1
	7434	5434	6	2	10	2
10	7406	5406	7	12	10	1
	7422	5422	7	13	11	2
11	7421	5421	7	5	11	1
	7435	5435	7	6	12	5
12	74044	54044	8	29	11	1
13	74042	54042	8	12	11	1
	74046	54046	8	17	13	2
14	74042	54042	8	6	11	1
	74047	54047	8	7	14	2
15	740414	540414	8	1	13	1
	740470	540470	8	3	14	2
16	740416	540416	9	18	14	1
	740462	540462	9	22	15	3
17	740415	540415	9	7	15	3
	740463	540463	9	9	16	2
18	7404244	5404244	9	3	15	1
	7404634	5404634	9	4	16L	1
19	7404242	5404242	10	31	15	1
20	7404241	5404241	10	13	14L	1
	7404155	5404155	10	18	18L	2
21	74042404	54042404	10	4	15	1
	74041550	54041550	10	8	18L	2
22	74041566	54041566	10	1	18	1
	74042436	54042436	10	8	19L	2
23	74042417	54042417	11	27	18L	1
	74041567	54041567	11	32	19L	1

Note: L denotes that this number is actually d_{71} which is a lower bound on d_∞.

TABLE IV
NONSYSTEMATIC QLI CODES WITH MAXIMUM FREE DISTANCE FOR QLI CODES

M	$G^{(1)}$	$G^{(2)}$		d_M	#paths	d_∞	#paths
1	6	4	1,2,3	3	2	3	1
2	7	5	1,2,3	3	1	5	1
3	74	54	1,2,3	4	3	6	1
4	66	46	1, 3	4	2	7	2
5	75	55	1,2,3	5	6	8	2
6	654	454	3	5	3	9	4
7	742	542	2,3	6	11	9	1
8	751	551	3	6	7	10	1
9	7664	5664		5	1	11	3
10	7506	5506	3	7	14	12	3
11	7503	5503		6	2	13	8
12	76414	56414		7	7	14	10
13	66716	46716		6	1	14	3

Notes: 1. This code is OFD.
2. This code is ODP.
3. This code is OMD.

TABLE V
NONSYSTEMATIC CODES WHICH ARE SIMULTANEOUSLY ODP, OMD, AND OFD

M	$G^{(1)}$	$G^{(2)}$	d_M	#paths	d_∞	#paths
1	6	4	3	2	3	1
2	7	5	3	1	5	1
3	74	54	4	3	6	1
4	62	56	4	2	7	2
5	75	55	5	6	8	2
6	634	564	5	3	10	12
7	626	572	6	11	10	1
8	751	557	6	6	12	10
9	7664	5714	6	2	12	1
10	7512	5562	7	13	14	19
11	-	-	7	-	15	-
12	-	-	8	-	16	-
13	60676	45662*	8	17	16	5

* The search for the code with the smallest number of d_∞=16 paths was not exhaustive and hence a slightly better code might exist.

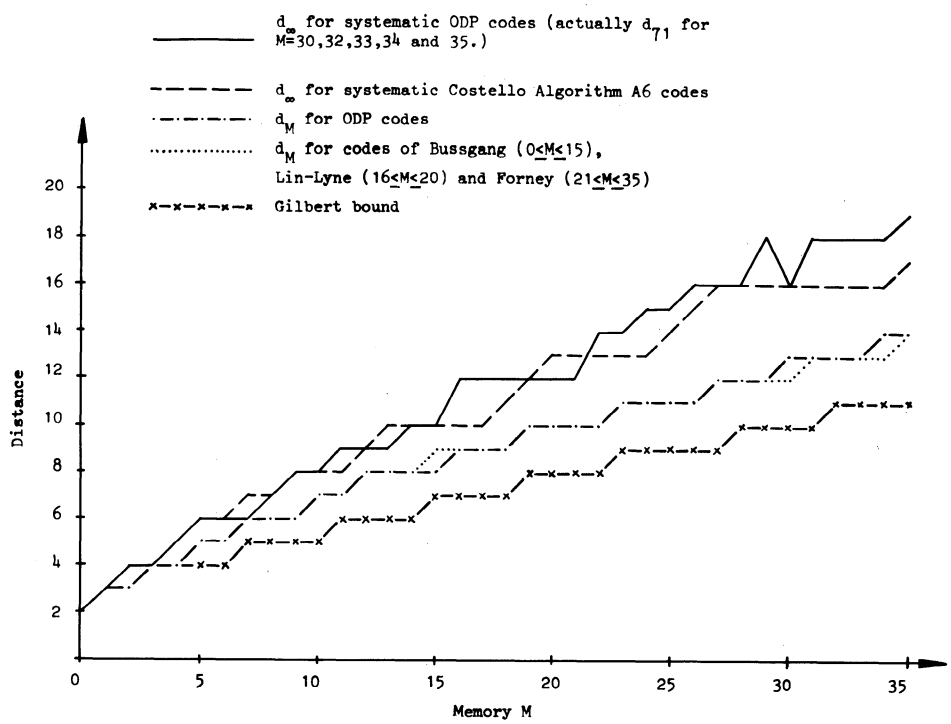

Fig. 1. Minimum distance d_M and free distance d_∞ for some rate $\frac{1}{2}$ convolutional codes.

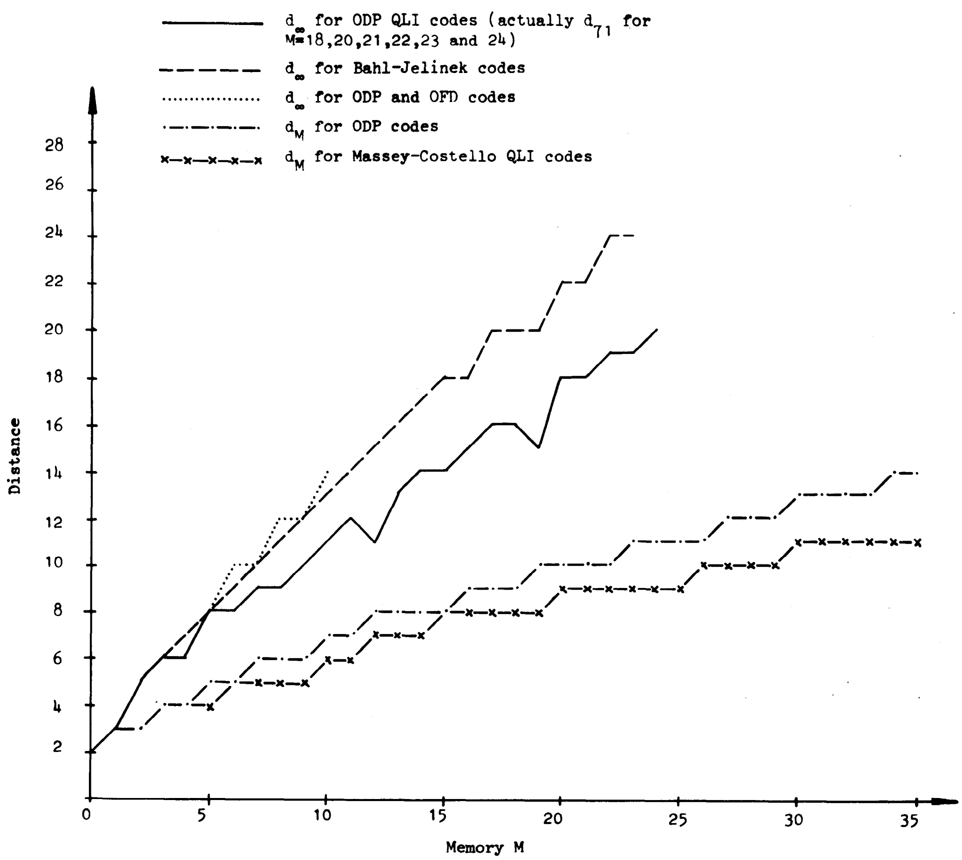

Fig. 2. Minimum distance d_M and free distance d_∞ for some rate $\frac{1}{2}$ convolutional codes.

the fewest number of paths $t_{[0,M]}$ with Hamming weight d_M resulting from information sequences with $i_0 = 1$ when d_M is the distance measure in question.

In Table I we list ODP systematic codes for the range $1 \leq M \leq 14$. In all the tables we write the generators in the octal form where the first octal digit denotes $[g_0^{(k)},g_1^{(k)},g_2^{(k)}]$, the second denotes $[g_3^{(k)},g_4^{(k)},g_5^{(k)}]$, etc. (It should be noted that the "customary" octal notation for generators [5] uses $[g_{M-2}g_{M-1}g_M]$ for the last octal digit, etc., so that the generators [1111] and [111101] become 17 and 75, respectively. In the notation here these would be 74 and 75, which we think better shows the fact that the former is a truncation of the latter.) In case of ties not resolved by the number of weight d_M paths, we have chosen for Table I a code with the greatest d_∞. The codes in Table I are all OMD codes as well as ODP codes. Since the "truncation" to smaller memory of an ODP code must give an ODP code for the reduced memory, the $M = 14$ code in Table I can be used to obtain an ODP code for all $M \leq 14$ but not necessarily one with the least number of low-weight paths.

For $M = 15$, we have found that an ODP code has $d_{15} = 8$ whereas an OMD code has $d_{15} = 9$ so there is no code that is both ODP and OMD for $M = 15$. We know of no other M in the range $15 \leq M \leq 35$ with this property. In Table II we list the systematic ODP codes that we have found for $15 \leq M \leq 35$. For $M \geq 16$, the value of d_M for OMD codes is unknown, but the codes in Table II have d_M as large as any previously known codes. In fact, for $M = 30$ and $M = 34$, the codes in Table II have larger d_M than any codes previously known. Moreover, the $M = 35$ code in Table II has d_∞ superior to the best previously known systematic code, viz., the adjoint [6] code of Forney's extension [7] of one of Bussgang's optimal codes [6].

The excellence as regards d_M of the systematic ODP codes in Tables I and II can be seen from Fig. 1 in which we have plotted d_M for these codes and for the best of the codes found previously by Bussgang [6], Lin–Lyne [8], and Forney [7]. For comparison, we have also plotted the Gilbert lower bound [3] on d_M. To show the excellence of their d_∞, we have also plotted d_∞ for the ODP systematic codes and for the systematic codes found by Costello [2].

It should be mentioned that, in Table II (as well as later in Table III), a notation of L indicates that d_{71} which is a lower bound on d_∞ is actually given rather than d_∞, which is unknown. It is likely, however, that $d_{71} = d_\infty$ in most, if not all, of these cases.

In Table III, we list the ODP QLI codes we have found for $1 \leq M \leq 23$. These codes, except when $M = 1$, are nonsystematic. QLI codes can generally achieve a greater d_∞ for a given M than is possible with systematic codes.

The excellence of the ODP QLI codes of Table III as regards d_M and d_∞ can be seen from Fig. 2 where we have plotted d_M and d_∞ for these codes and d_M for the QLI codes of Massey–Costello [1]. The ODP QLI codes of Table III appear very attractive for use with sequential decoding since 1) their QLI structure guarantees easy recovery of the information sequence from the encoded sequence with small "error amplification" [1]; 2) their ODP property ensures good computational performance; and 3) their large d_∞ ensures a small decoding error probability.

In Table IV, we list the QLI codes that we have found to have the greatest d_∞ for any QLI codes for $1 \leq M \leq 13$. For $M \leq 5$ these codes are also OFD, but for $M \geq 6$ larger d_∞ is possible only with more general nonsystematic codes. Ties were resolved using first d_∞ and then d_M as further optimality criteria. The codes of Table IV appear attractive for use with Viterbi decoders for $1 \leq M \leq 5$.

In Table V, we list ODP general nonsystematic convolutional codes with ties resolved first according to d_∞ and then according to d_M. The codes for $M \leq 10$ and $M = 13$ are all OFD codes [5], and it is surprising that the ODP property can be obtained over such a wide range at no sacrifice in free distance.

The excellence as regards d_∞ of the codes in Table V can be seen from Fig. 2 where we have plotted their d_∞ as well as that of the "complementary codes" found earlier by Bahl–Jelinek [9]. The codes of Table V are attractive candidates for use with Viterbi decoding when the QLI feature is of no interest. The $M = 5$ code in Table V is quite remarkable being simultaneously optimal for all three distance measures and also being QLI.

To illustrate the importance of the ODP property for sequential decoding computation, we have simulated the performance of a stack sequential decoder [10] on a binary symmetric channel (BSC) for 1) the ODP QLI code with $M = 23$, $d_\infty \geq d_{71} = 19$, and $d_M = 11$ of Table III; 2) the $M = 23$ Massey–Costello QLI code [1] with $d_\infty \geq d_{71} = 17$ and $d_M = 9$, which is currently being used by NASA in several deep-space programs; and 3) the $M = 23$ Bahl–Jelinek complementary code [9] with $d_\infty = 24$ and $d_M = 10$. The results of decoding 1000 frames of 256 information bits in length for each of these codes are given in Tables VI and VII for BSC's with crossover probability p of 0.045 and 0.057, respectively. No decoding errors were made in any case. It can be seen from Tables VI and VII that the computational performance of the ODP QLI code is far superior to the Massey–Costello QLI code and slightly better than the Bahl-Jelinek code that (while having larger d_∞) lacks the desirable QLI property.

TABLE VI
SIMULATION RESULTS FOR DECODING 1000 FRAMES OF 256 BITS EACH FOR THE BSC WITH $p = 0.045$ ($R = R_0 = 0.50$; $R_0 = R_{comp}$)

	Fraction of Frames with Computation More than N		
N	ODP QLI code M=23	Massey-Costello code M=23	Bahl-Jelinek code M=23
278	1.000	1.000	1.000
330	0.555	0.582	0.571
360	0.418	0.437	0.418
450	0.227	0.254	0.227
600	0.123	0.134	0.128
1100	0.047	0.051	0.047
1700	0.028	0.029	0.031
2700	0.017	0.019	0.018
	Fraction of Frames Decoded in Error		
	0.000	0.000	0.000

TABLE VII
SIMULATION RESULTS FOR DECODING 1000 FRAMES OF 256 BITS EACH FOR THE BSC WITH $p = 0.057$ ($R = 1.1R_0 = 0.50$)

	Fraction of Frames with Computation More than N		
N	ODP QLI code M=23	Massey-Costello code M=23	Bahl-Jelinek code M=23
278	1.000	1.000	1.000
330	0.851	0.869	0.860
360	0.731	0.757	0.731
450	0.532	0.553	0.537
600	0.359	0.377	0.365
1100	0.182	0.189	0.178
1700	0.125	0.134	0.128
2700	0.083	0.090	0.084
	Fraction of Frames Decoded in Error		
	0.000	0.000	0.000

Acknowledgment

I would like to acknowledge gratefully the assistance and encouragement of Prof. James L. Massey, who also suggested the names "distance profile" and "robustly optimal." Finally, I am indebted to the American-Scandinavian Foundation and the Swedish Telephone Company, L. M. Ericsson for their support.

References

[1] 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.
[2] D J. Costello, Jr., "A construction technique for random-error-correcting convolutional codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-15, pp. 631–636, Sept. 1969.
[3] J. L. Massey, *Threshold Decoding*. Cambridge, Mass.: M.I.T. Press, 1963.
[4] A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Commun. Technol.*, vol. COM-19, pp. 751–772, Oct. 1971.
[5] K. J. Larsen, "Short convolutional codes with maximal free distance for rates $\frac{1}{2}$, $\frac{1}{3}$, and $\frac{1}{4}$," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-19, pp. 371–372, May 1973.
[6] J. J. Bussgang, "Some properties of binary convolutional code generators," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 90–100, Jan. 1965.
[7] G. D. Forney, Jr., "Use of a sequential decoder to analyze convolutional code structure," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-16, pp. 793–795, Nov. 1970.
[8] S. Lin and H. Lyne, "Some results on binary convolutional code generators," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-13, pp. 134–139, Jan. 1967.
[9] L. R. Bahl and F. Jelinek, "Rate $\frac{1}{2}$ convolutional codes with complementary generators," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 718–727, Nov. 1971.
[10] F. Jelinek, "A fast sequential decoding algorithm using a stack," *IBM J. Res. Dev.*, vol. 13, pp. 675–685, Nov. 1969.

A Class of Binoid Single-Error-Correcting Codes

VASILE V. MASGRAS

***Abstract*—A new class of group binoid single-error-correcting codes is given. The codes are nonbinary group codes over the additive group of integers modulo q.**

I. Notation and Definitions

Let n and q $(n > q)$ be two positive integers. We denote by $(n)_q$ the radix-q representation of n. We suppose that this representation has s digits. Let I_k^j be the following set:

$$I_k^j = \{i \mid 1 \le i \le n,\ (i)_q = i_1,\cdots,i_{k-1}ji_{k+1},\cdots,i_s\},\qquad 1 \le j \le q-1,\quad 1 \le k \le s.$$

We denote by Z_q the additive group of integers (mod q).

Definition 1: The set $C \subset Z_q^n$ is the nonbinary group code [3], such that

$$c = (c_1,\cdots,c_n) \in C$$

if and only if

$$\sum_{i \in I_k^j} c_i \equiv 0 \pmod q,\qquad 1 \le j \le q-1,\quad 1 \le k \le s. \tag{1}$$

If we let $r = \#\{I_k^j \mid I_k^j \ne \phi, 1 \le j \le q-1, 1 \le k \le s\}$, then the group code has r check symbols and $m = n - r$ information symbols.

Manuscript received February 25, 1974; revised February 11, 1975.
The author is with the Department of Mathematics, Polytechnic Institute, Bucharest, Rumania.

For $q = 2$ and $n = 2^s - 1$, C is a binary Hamming code [1], [2]. For $q > 2$, C represents another nonbinary generalization of the Hamming code [3].

Definition 2: A pair of sets $\langle A,M \rangle$ is a binoid [4], if the following two conditions are satisfied:

i) there are two operations $\oplus: A \times A \to A$ and $\otimes: A \times M \to A$;
ii) the set A is a group with respect to the $\oplus$ operation.

A binoid $\langle A,M \rangle$ is called distributive if the $\otimes$ operation is distributive with respect to the $\oplus$ operation, and it will be termed commutative if A is a commutative group. The set $A^* = \{a \mid a \in A, a \otimes m \ne a \otimes m'; \forall m, m' \in M, m \ne m'\}$ is called the univalence domain. If, in addition, we have $A^* = A - \{0\}$, $\langle A,M \rangle$ is termed a completely univalent binoid.

Definition 3: A set $C \subset A^n$ is a binoid code [4], if there is a set M such that following conditions are satisfied:

i) $\langle A,M \rangle$ is a binoid;
ii) C is a nonbinary group code (of length n);
iii) the parity check matrix of C has its components from M.

II. Link Theorem

Taking into account Definitions 1 and 3, we may formulate the following theorem.

Theorem 1: The nonbinary group code C of Definition 1 is always a binoid code for $M = \{0,1\}$, where $\oplus$ is modulo q addition and $\otimes$ is ordinary multiplication.

Proof: This is obvious if we note that the code C is the null space of the matrix $H = [\delta_{(j,k)}{}^i]$, where $\delta_{(j,k)}{}^i \in M = \{0,1\}$ are defined in the following way:

$$\delta_{(j,k)}{}^i = \begin{cases} 1, & \text{if } i \in I_k^j \\ 0, & \text{if } i \notin I_k^j. \end{cases}$$

Q.E.D.

Any group code C may be regarded as a binoid code. The binoid $\langle A,M \rangle$ is completely univalent.

III. Detection and Correction of Single Error

Theorem 2: The nonbinary group code $C \subset Z_q^n$ of Definition 1 is a single-error-correcting code.

Proof: Let $c = (c_1,\cdots,c_n)$ be a codeword and $b = (b_1,\cdots,b_n)$ be the received vector. We define

$$d_k^j = \sum_{i \in I_k^j} b_i \pmod q. \tag{2}$$

If we assume that no more than a single error occurred, then we suppose

$$b_i = \begin{cases} c_i, & \text{for } i \ne h \\ c_h + p \pmod q, & \text{for } i = h \end{cases}$$

where p and h are the value and position of the error. We have $b_i = c_i \oplus \delta_{ih} p$, where δ_{ih} is the Kronecker symbol.

From the (2) congruences we have

$$\begin{aligned} d_k^j &= \sum_{i \in I_k^j} b_i = \sum_{i=1}^{n} \delta_{(j,k)}{}^i \otimes b_i \\ &= \sum_{i=1}^{n} \delta_{(j,k)}{}^i \otimes c_i \oplus \sum_{i=1}^{n} \delta_{(j,k)}{}^i \otimes \delta_{ih} p \\ &= 0 + \delta_{(j,k)}{}^h p = \begin{cases} p, & \text{if } h \in I_k^j \\ 0, & \text{if } h \notin I_k^j. \end{cases} \end{aligned}$$