Further results on binary convolutional codes with an optimum distance profile

Johannesson, Rolf; Paaske, Erik

Published in:
IEEE Transactions on Information Theory

1978

[4] E. F. Assmus, Jr. and H. F. Mattson, Jr., "Majority decoding of the (24, 12) binary Golay code," G.T.E. Sylvania, Rep. Contract F-19628-69-C-0068, 1969.
[5] M. Rahman, "Combinatorial aspects of error correcting codes," Ph.d. thesis, Dep. Elec. Eng., Univ. Waterloo, Waterloo, ON 1975.
[6] R. T. Curtis, "A new combinatorial approach to M_{24}," *Math. Proc. Camb. Phil. Soc.*, vol. 79, pp 25–42, 1976.
[7] J. F. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam: North-Holland, 1977.
[8] J. A. Todd, "A representation of the Mathieu group M_{24} as a collineation group," *Ann. Mat. Pura Appl.*, series IV, vol. 71, pp. 199–238, 1966.

Further Results on Binary Convolutional Codes with an Optimum Distance Profile

ROLF JOHANNESSON AND ERIK PAASKE

***Abstract*—Fixed binary convolutional codes are considered which are simultaneously optimal or near-optimal according to three criteria: namely, distance profile d, free distance d_∞, and minimum number of weight d_∞ paths. It is shown how the optimum distance profile criterion can be used to limit the search for codes with a large value of d_∞. We present extensive lists of such robustly optimal codes containing rate $R = 1/2$ nonsystematic codes, several with d_∞ superior to that of any previously known code of the same rate and memory; rate $R = 2/3$ systematic codes; and rate $R = 2/3$ nonsystematic codes. As a counterpart to quick-look-in (QLI) codes which are not "transparent," we introduce rate $R = 1/2$ easy-look-in-transparent (ELIT) codes with a feedforward inverse $(1 + D,D)$. In general, ELIT codes have d_∞ superior to that of QLI codes.**

I. Introduction

It has been recently observed [1], [2], [3] that to obtain a good computational performance with sequential decoding, the column distance of the actual encoder should "grow as rapidly as possible." However, good computational performance does not exclude the choice of encoders with large free distances. On the contrary, the criterion of good computational performance can be used to limit the search for encoders with large free distance. In this correspondence, we report on some progress in finding such good binary fixed convolutional encoders (FCE's), i.e., encoders generating codes which are simultaneously optimal or near-optimal according to several criteria.

II. Notation and Definitions

For rates $R = (N-1)/N$, we can represent an FCE by the $(N-1) \times N$ matrix $\boldsymbol{G}(D)$, where

$$\boldsymbol{G}(D) = \begin{Bmatrix} G_1^1(D) & G_1^2(D) & \cdots & G_1^N(D) \\ G_2^1(D) & G_2^2(D) & \cdots & G_2^N(D) \\ \vdots & \vdots & & \vdots \\ G_{N-1}^1(D) & G_{N-1}^2(D) & \cdots & G_{N-1}^N(D) \end{Bmatrix},$$

and

$$G_i^j(D) = g_{0i}^j + g_{1i}^j D + g_{2i}^j D^2 + \cdots$$

is the transform of the generator sequence $g_{0i}^j, g_{1i}^j, g_{2i}^j \cdots 1 \le i \le N-1, 1 \le j \le N$. Each $G_i^j(D)$ is called a generator polynomial. Corresponding to the encoder, we can also write the parity matrix in polynomial form, i.e.,

$$\boldsymbol{H}(D) = \{H^1(D), H^2(D) \cdots H^N(D)\}$$

where each $H^j(D)$ is called a parity polynomial.

We consider only noncatastrophic codes [4], and we define the overall constraint length as

$$\nu = \max_{0<j\le N} \{\deg [H^j(D)]\}.$$

Then ν becomes also the number of memory elements in the corresponding minimal encoder.

A key parameter used in the evaluation of the encoders is the column distance, which was originally defined by Costello [5]. The order j column distance d_j is the minimum Hamming weight of all codewords having a nonzero first branch and truncated after $(j+1)$ branches. In particular, d_∞ is called the free distance of the code. Also, in a previous paper [3], Johannesson introduced the distance profile as the $(\nu+1)$-tuple $\boldsymbol{d} = [d_0, d_1, \cdots d_\nu]$ and defined a distance profile $\boldsymbol{d}$ to be superior to $\boldsymbol{d}'$ if $d_j > d_j'$ for the smallest index j, $0 \le j \le \nu$, where $d_j \ne d_j'$. Hence an optimum distance profile (ODP) ensures that, for the first constraint length, the column distance "grows as rapidly as possible," which is not necessarily the case for the average column distance function [2].

III. How to Find Good Encoders

It is well known [6] that d_∞ is the principal determiner of decoding error probability when Viterbi decoding or sequential decoding is used, and further that the number of codewords with a nonzero first branch and weight d_∞ should be as small as possible. Also it has been observed [1], [2], [3] that, for good computational performance with sequential decoding, the column distance should "grow as rapidly as possible," i.e., an optimum distance profile is desirable. Since different criteria appear to be of fundamental importance for the error probability and for the computational performance, it seems reasonable to search for FCE's generating codes which are simultaneously optimal or near-optimal according to the mentioned criteria.

At first glance, one might believe it more difficult to search for FCE's which are optimal according to several criteria, but interestingly enough, a remarkable simplification in the search procedure may be obtained if the criteria are carefully chosen. As already discussed in [7], an exhaustive search becomes practically impossible even for rather small constraint lengths, and therefore some methods are needed to limit the search for good encoders. One approach is to select a subset in which the possibility of finding good encoders is "expected to be good." Another approach is to use rules that reject a large fraction of encoders from the complete ensemble either because they cannot be good encoders or because the distance properties of the codes generated equal the distance properties of some code in the remaining set.

We shall use the case of rate $R = 1/2$ nonsystematic codes to illustrate how a combination of the two approaches becomes very feasible when optimizing according to several criteria. Let us start with the first limitation approach and select the subset of ODP encoders. The justification to expect this subset to be good with regard to d_∞ lies mainly in Table V in [3], but also in the fact that, for most constraint lengths, ODP encoders have optimum d_ν which is of course a lower bound on d_∞. The subset of ODP encoders is also relatively small. Provided that both generator polynomials are monic, a general nonsystematic $R = 1/2$ encoder of constraint length ν is specified by 2ν coefficients implying an ensemble "size" of $2^{2\nu}$, while our subset "size" is $S(\nu)2^\nu$, where $S(\nu)$ is the number of systematic ODP encoders of constraint length

Manuscript received February 1, 1977; revised June 7, 1977. This work was supported in part by the Swedish Board for Technical Development under Grant 75-4165. A part of this paper was previously presented at the *IEEE International Symposium on Information Theory*, Ronneby, Sweden, June 21–24, 1976.

R. Johannesson is with the Department of Automata and General Systems Sciences, University of Lund, S-22007 Lund, Sweden.
E. Paaske is with the Institute of Circuit Theory and Telecommunications, Technical University of Denmark, DK-2800 Lyngby, Denmark.

0018-9448/78/0300-0264$00.75

ν. From the results leading to [3], $S(\nu)$ is known to be relatively small, and hence a substantial reduction in the search is obtained. Furthermore, the subset is easy to generate. Because of the restriction of the ODP to column distances up to ν, we can use well-known results of Bussgang [8] and Forney [9] to generate the subset of nonsystematic ODP encoders from the systematic ODP encoders in the following simple way. Let the systematic code with distance profile $\boldsymbol{d} = [d_0, d_1, \cdots, d_\nu]$ have parity matrix

$$\{H^1(D), H^2(D) \cdots H^{N-1}(D), 1\},$$

and let $*$ denote polynomial multiplication with truncation after degree ν. If $P(D)$ runs through all monic polynomials of degree $\leq \nu$, then

$$\begin{aligned}\boldsymbol{H}(D) &= \{P(D)\} * \{H^1(D), H^2(D) \cdots H^{N-1}(D), 1\} \\ &= \{P(D) * H^1(D), P(D) * H^2(D) \cdots P(D) * H^{N-1}(D), P(D)\}\end{aligned}$$

runs through the corresponding set of nonsystematic encoders with distance profile $\boldsymbol{d}$.

With the properties of ODP encoders in mind, it now becomes evident that we obtain a great simplification in the search for good encoders by chosing the criteria in the following way:

1) optimum distance profile (ODP),
2) optimum free distance (OFD) conditioned on 1),
3) minimum number of weight d_∞ paths conditioned on 2).

In the subset of ODP encoders, we can then use the second approach, viz. rejection rules, to limit the search for encoders with optimum d_∞. The rules which we have used are similar to those mentioned in [7]. On the average, they discarded about 99 percent of the encoders, and hence d_∞ need be calculated only for the remaining one percent of the FCE's in the subset of ODP encoders.

In Table I, we have listed the results of a computer search for nonsystematic rate $R = \frac{1}{2}$ FCE's. In all tables, the generators are given in octal form, as introduced in [3], where the first digit denotes $[g^j_{0i}, g^j_{1i}, g^j_{2i}]$, the second denotes $[g^j_{3i}, g^j_{4i}, g^j_{5i}]$, etc. All the codes are ODP and, except for a few cases where the search would become unreasonably large, they are also optimum according to criteria 2) and 3). For comparison, we have plotted the d_∞ of our codes in Fig. 1 together with d_∞ for: the OFD codes of Odenwalder [10], Larsen [11], and Paaske [12]; the complementary codes of Bahl and Jelinek [13]; and an upper bound on d_∞ calculated using the method given by Heller [14]. Four of the ODP codes, viz. those for $\nu = 18$, 19, 21, and 23 have d_∞ superior to that of any previously known rate $R = \frac{1}{2}$ code with the same constraint length. Furthermore, the $\nu = 23$ code has been recommended to NASA for use with sequential decoding on the deep-space channel [15], [16]. In general, a limitation of the search to the subset of ODP encoders seems to result in only a very small reduction in achievable d_∞, which is illustrated by the fact that encoders with a larger d_∞ are known only for $\nu = 11$, 12, 14, 15, and 16; these are listed in Table II for completeness. OFD encoders for $\nu = 11$ and 12 were previously found by Larsen [11], but the encoders listed here have a smaller number of weight d_∞ paths; the encoders for $\nu = 14$, 15, and 16 were hitherto unpublished, but were previously found by Paaske [12].

In Table III and Table IV, we have listed corresponding results for systematic and nonsystematic encoders of rate $R = \frac{2}{3}$. Table V shows the parity polynomials of the codes in Table IV. For this rate, $S(\nu)$ is much greater than the corresponding number for rate $R = \frac{1}{2}$, implying that the subset of nonsystematic ODP encoders is also much greater. Therefore, even with the rejection rules in effect, an exhaustive search according to criterion 2) was not reasonable in several cases. In Fig. 2 we have compared d_ν and d_∞ of our codes with d_∞ of the OFD codes by Paaske [7] and with an upper bound on d_∞ calculated using the method given by Heller [14].

TABLE I
ODP NONSYSTEMATIC CONVOLUTIONAL CODES WITH RATE $\frac{1}{2}$

ν	G_1^1	G_1^2	Notes	d_ν	#paths	d_∞	#paths
1	6	4	1,2	3	2	3	1
2	7	5	1,2	3	1	5	1
3	74	54	1,2	4	3	6	1
4	62	56	1,2	4	2	7	2
5	75	55	1,2	5	6	8	2
6	634	564	1,2	5	3	10	12
7	626	572	1,2	6	11	10	1
8	751	557	1,2	6	6	12	10
9	7664	5714	1,2	6	2	12	1
10	7512	5562	1,2	7	13	14	19
11	6643	5175	3	7	5	14	1
12	63374	47244	3	8	29	15	2
13	45332	77136	2	8	12	16	5
14	65231	43677	3	8	10	17	3
15	517604	664134	3,4	8	5	18	10
16	717066	522702	3	9	18	19	9
17	506477	673711	4	9	7	20	12
18	5653664	7746714	5	9	7	21	13
19	5122642	7315626	5	10	31	22	26
20	6567413	5322305	4	10	13	22	2
21	67520654	50371444	4,5	10	4	24	40
22	67132702	50516146	6	10	1	24	25
23	55346125	75744143	5,6	11	28	25	13

Notes:
1. This code was found by Johannesson [3] and is listed here for completeness.
2. This code is OFD.
3. An OFD code with the same memory is listed in Table II.
4. The search according to criterion 3) was not exhaustive, and hence a slightly better code might exist.
5. This code has a free distance superior to that of any previously known code with the same memory.
6. The search according to criterion 2) was not exhaustive, and hence a better code might exist.

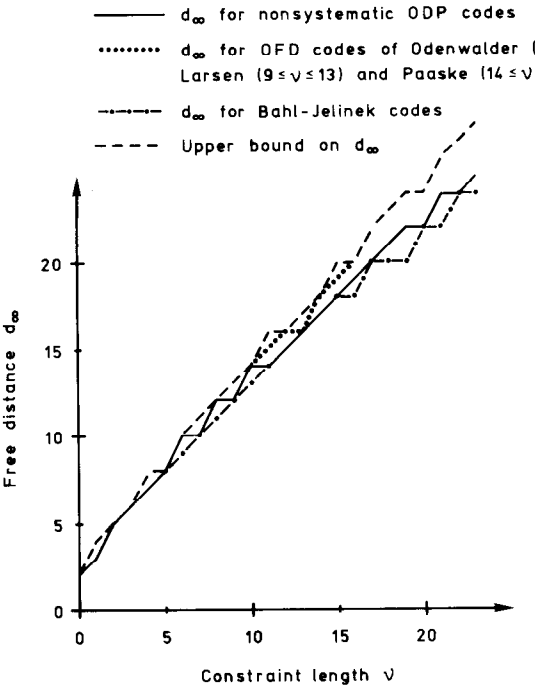

Fig. 1. Free distance d_∞ for some rate $\frac{1}{2}$ convolutional codes.

TABLE II
SOME NONSYSTEMATIC CONVOLUTIONAL CODES WHICH ARE OFD

ν	G_1^1	G_1^2	Note	d_ν	#paths	d_∞	#paths
11	7173	5261		7	6	15	14
12	53734	72304		7	3	16	14
14	63121	55367	1	8	12	18	29
15	447254	627324	1	7	2	19	30
16	716502	514576	1	8	5	20	53

Note:
1. The search for the code with the smallest number of weight d_∞ paths was not exhaustive, and hence a slightly better code might exist.

TABLE III
ODP SYSTEMATIC CONVOLUTIONAL CODES WITH RATE 2/3

ν	G_1^3	G_2^3	d_ν	#paths	d_∞	#paths
1	4	6	2	1	2	1
2	5	7	3	6	3	2
3	54	64	3	3	4	7
4	56	62	4	17	4	2
5	57	63	4	7	5	6
6	554	704	4	4	5	2
7	664	742	5	30	6	24
8	665	743	5	15	6	5
9	5734	6370	5	6	6	1
10	5736	6322	6	54	7	8
11	5736	6323	6	26	8	44
12	66414	74334	6	12	8	16
13	57372	63226	6	6	8	3
14	57371	63225	7	72	8	2
15	664150	743314	7	31	8	1
16	664072	743346	7	21	10	40
17	573713	632255	7	7	10	15
18	6640344	7431024	8	102	10	18
19	5514632	7023726	8	39	10	2
20	5514633	7023725	8	25	11	8
21	57361424	63235074	8	18	12	74
22	66415416	74311464	9	135	11	4
23	66415417	74311465	9	68	12	17

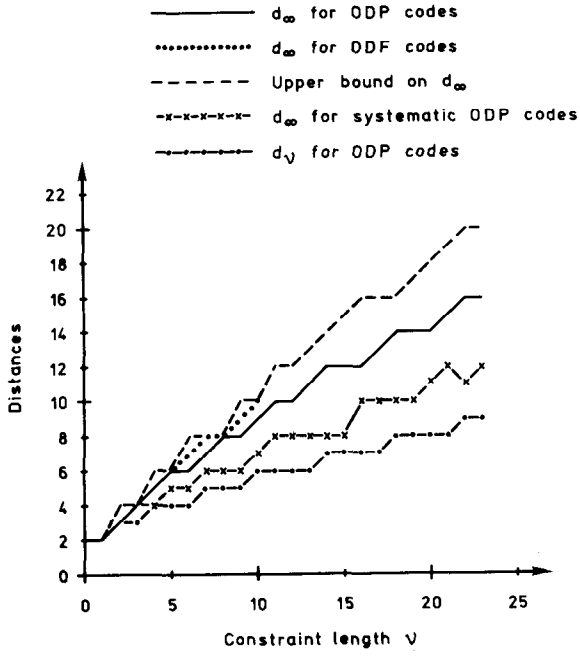

Fig. 2. Free distance d_∞ and column distance for some rate 2/3 convolutional codes.

IV. TRANSPARENT CODES WITH A SIMPLE ENCODER INVERSE

Massey and Costello [1] introduced the class of quick-look-in (QLI) codes, nonsystematic codes of rate $R = 1/2$ in which the two generators differ only in the second position. The reason to prefer a QLI code rather than another nonsystematic code is the ease of extracting the information digits from the hard-decisioned received sequences, since a feedforward (FF) inverse $(P^1(D), P^2(D)) = (1,1)$ can be realized by a simple modulo 2 adder. Furthermore, since the FF-inverse has "weight" two, the "error amplification factor" $A = 2$ is the smallest possible for nonsystematic codes. However, if differential coding is used together with PSK, it is often desirable to use a "transparent" code [17], i.e., a code which has the all-one sequence as a codeword. Since the QLI codes are not transparent and since the smallest error amplification factor for a nonsystematic transparent code is $A = 3$, then, as a counterpart to the QLI codes, we are led to introduce *easy-look-in-transparent* (ELIT) codes such that

1E) $G_1^1(D)$ and $G_1^2(D)$ both have odd weight, and
2E) $(1 + D)G_1^1(D) + DG_1^2(D) = 1$.

Property 2E) specifies that ELIT codes have the FF-inverse $(P^1(D),P^2(D)) = (1 + D,D)$ with error amplification factor $A = 3$.

Although the subset of ODP QLI codes [3] is small, it contains FCE's with relatively large values of d_∞, and therefore one could expect the subset of ODP ELIT codes to have the same property. However, this turned out not to be the case. For several constraint lengths, the latter subset contains only bad codes, and in some cases, it is even empty. To overcome this problem, it is necessary to enlarge the subset which can be done systematically using a *generalized distance profile*:

$$\boldsymbol{d}_l = [d_0,d_1,d_2,\cdots,d_l].$$

Our first optimality criterion selects the subset of codes with an optimum $\boldsymbol{d}_\nu$, but we can of course enlarge the subset by requiring only an optimum $\boldsymbol{d}_l$, where $l < \nu$. For the case of ELIT codes we have chosen $l = \nu - 2$ for two reasons.

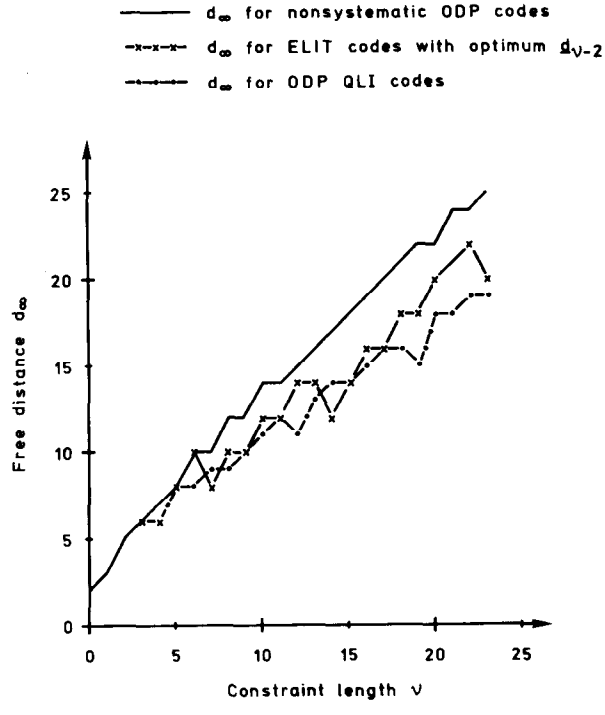

Fig. 3. Free distance d_∞ for some rate 1/2 convolutional codes with a simple encoder inverse.

TABLE IV
ODP NONSYSTEMATIC CONVOLUTIONAL CODES WITH RATE 2/3

ν	G_1^1	G_1^2	G_1^3	G_2^1	G_2^2	G_2^3	Notes	d_ν	#paths	d_∞	#paths
3	6	2	4	1	4	7	1	3	2	4	1
4	6	3	7	1	5	5	1	4	17	5	7
5	60	30	70	34	74	40	1	4	7	6	9
6	50	24	54	24	70	54		4	2	6	1
7	54	30	64	00	46	66		5	30	7	6
8	64	12	52	26	66	44	1	5	15	8	8
9	54	16	66	25	71	60		5	9	8	1
10	53	23	51	36	53	67		6	54	9	9
11	710	260	670	320	404	714		6	29	10	29
12	740	260	520	367	414	515	2	6	27	10	4
13	710	260	670	140	545	533		6	5	11	9
14	676	046	704	256	470	442		7	65	12	58
15	722	054	642	302	457	435	2	7	38	12	25
16	7640	2460	7560	0724	5164	4260	3	7	14	12	7
17	5330	3250	5340	0600	7650	5434	3	7	7	13	18
18	6734	1734	4330	1574	5140	7014	3	8	106	14	?
19	5044	3570	4734	1024	5712	5622	3	8	43	14	?
20	7030	3452	7566	0012	6756	5100	3	8	23	14	?
21	6562	2316	4160	0431	4454	7225	3	8	11	15	?
22	57720	12140	63260	15244	70044	47730	3	9	144	16	?
23	51630	25240	42050	05460	61234	44334	3	9	60	16	?

Notes:
1. This code is OFD.
2. The search according to criterion 3) was not exhaustive, and hence a slightly better code might exist.
3. The search according to criterion 2) was not exhaustive, and hence a better code might exist.

1) For most values of ν, this subset contains codes with reasonably large values of d_∞.

2) The subset is easy to generate. We denote codes with a FF-inverse $(1 + D,D)$, i.e., codes satisfying condition 2E), as *easy-look-in* (ELI) codes, and we denote by $C(\nu)$ the subset of ELI codes of constraint length ν with an optimum generalized distance profile $\boldsymbol{d}_{\nu-2}$. Then $C(\nu)$ can be easily generated from $C(\nu - 1)$ since, for each generator polynomial $G_1^1(D)$ in $C(\nu - 1)$, there are only two candidate codes for $C(\nu)$, namely $G_1^{1'}(D) = G_1^1(D) \oplus D^\nu$ and $G_1^{1''}(D) = G_1^1(D) \oplus D^{\nu-1} \oplus D^\nu$, each of which belongs to $C(\nu)$ if it also has optimum column distance $d_{\nu-2}$. Finally, the codes are also transparent if they satisfy condition 1E).

TABLE V
PARITY POLYNOMIALS OF THE CODES IN TABLE IV

ν	H^1	H^2	H^3
3	74	54	64
4	50	62	72
5	65	45	53
6	424	644	764
7	472	752	532
8	635	403	571
9	5014	4634	6664
10	7164	4136	5416
11	5755	7767	6601
12	70414	52464	60244
13	56502	76346	67772
14	71433	53241	61175
15	660004	575734	776554
16	461656	700006	630732
17	544463	433501	615256
18	4114444	5433454	7152024
19	6171512	5475256	4301002
20	7500021	6742327	4162245
21	72164254	45126324	61662214
22	55422416	42035332	60362506
23	45416327	51203765	76300111

TABLE VI
ELIT CODES WITH OPTIMUM $\boldsymbol{d}_{\nu-2}$

ν	G_1^1	G_1^2	Notes	$d_{\nu-1}$	#paths	d_ν	#paths	d_∞	#paths
3	54	64	1	3	1	3	1	6	2
4	52	76		3	1	3	1	6	1
5	51	73	1,2	4	2	5	6	8	3
6	564	634	1,2	5	6	6	5	10	12
7	576	602		5	2	5	1	8	1
8	513	735		5	1	6	7	10	3
9	5114	7324	2	6	5	6	3	10	2
10	5646	6352	2	6	1	7	12	12	7
11	5643	6345		6	3	7	11	12	1
12	51154	73264		7	8	7	4	14	6
13	51162	73226		7	4	8	22	14	2
14	51101	73303		8	12	8	6	12	2
15	564614	635224		8	10	8	3	14	2
16	511016	733022		8	3	8	1	16	5
17	511015	733027	2	9	18	9	7	16	1
18	5646044	6352154	2	9	11	9	4	18	8
19	5646042	6352146	2	9	3	10	31	18	5
20	5110135	7330347		9	2	9	1	20	11
21	-	-	3						
22	56460366	63520432	2	10	11	10	3	22	?
23	56460365	63520437		10	3	10	2	20	1

Notes:
1. This code is also OFD.
2. This code is also ODP.
3. The subset of ELIT codes with optimum $\boldsymbol{d}_{\nu-2}$ is empty for $\nu = 21$.

TABLE VII
SOME ELI CODES WITH FREE DISTANCE SUPERIOR TO THAT OF ELIT AND QLI CODES WITH THE SAME MEMORY

ν	G_1^1	G_1^2	Notes	$d_{\nu-1}$	#paths	d_ν	#paths	d_∞	#paths
4	56	62	1,2	4	3	4	2	7	2
8	511	733	2	6	11	6	6	10	2
15	564604	635214	2	8	6	8	1	15	1
16	511012	733036		8	1	8	1	17	3
17	564601	635203		8	2	8	1	17	3
21	56460424	63521474	2	10	18	10	8	20	4
23	56460367	63520431	2	10	8	11	29	21	3

Notes:
1. This code is also OFD.
2. This code is also ODP.

The result of a computer search using the above mentioned criteria is given in Table VI. In Fig. 3 we compare the free distance of the ELIT codes in Table VI with the ODP QLI codes found by Johannesson [3] and with the ODP nonsystematic codes in Table I. Finally, we remark that some nontransparent ELI codes are ODP and have a free distance superior to that of ODP QLI codes with the same memory. These ELI codes are given in Table VII, which also contains two ELI codes with optimum $d_{\nu-2}$ and free distance superior to any QLI code with optimum $d_{\nu-2}$.

V. CONCLUSION

The ODP criterion seems important for two reasons. One is the improvement observed in the computational performance for sequential decoding of ODP codes. The other is that, in a search for "good" encoders, the ODP criterion can be used to limit the ensemble size without serious degradation in the attainable values of d_∞.

REFERENCES

[1] J. L. Massey and D. J. Costello, Jr., "Nonsystematic convolutional codes for sequential decoding in space applications," *IEEE Trans. Commun. Technol.*, Pt II, vol. COM-19, pp. 806–813, Oct. 1971.
[2] P. R. Chevillat and D. J. Costello, Jr., "Distance and computation in sequential decoding," *IEEE Trans. Commun. Technol.*, vol. COM-24, pp. 440–447, Apr. 1976.
[3] R. Johannesson, "Robustly optimal rate one-half binary convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 464–468, July 1975.
[4] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Trans. Comput.*, vol. C-17, pp. 330–337, Apr. 1968.
[5] 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.
[6] A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Commun. Technol.*, vol. COM-19, pp. 751–772, Oct. 1971.
[7] E. Paaske, "Short binary convolutional codes with maximal free distance for rates ⅔ and ¾," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 683–689, Sept. 1974.
[8] J. J. Bussgang, "Some properties of binary convolutional code generators," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 90–100, Jan. 1965.
[9] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.
[10] J. P. Odenwalder, "Optimal decoding of convolutional codes," Ph. D. dissertation, Dep. Syst. Sci, Sch. Eng. Appl. Sci., Univ. California, Los Angeles, 1970.
[11] K. J. Larsen, "Short convolutional codes with maximal free distance for rates ½, ⅓, and ¼," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 371–372, May 1973.
[12] E. Paaske, unpublished results.
[13] L. R. Bahl and F. Jelinek, "Rate ½ convolutional codes with complementary generators," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 718–727, Nov. 1971.
[14] J. A. Heller, "Sequential decoding: Short constraint length convolutional codes," Jet Propulsion Lab., California Inst. Technol., Pasadena, Space Program Summary 37–54, vol. 3, pp. 171–174, Dec. 1968.
[15] J. L. Massey, "Comparison of rate one-half, equivalent constraint length 24, binary convolutional codes for use with sequential decoding on the deep-space channel," Tech. Rep. no. EE-762. Univ. Notre Dame, Notre Dame, IN, 1976.
[16] J. L. Massey, "Performance of the Johannesson–Paaske $K = 24$, $R = ½$, binary, convolutional code on the deep-space channel," Tech. Rep. no EE-764, Univ. Notre Dame, Notre Dame, IN, 1976.
[17] G. D. Forney and E. K. Bower, "A high speed sequential decoder: prototype design and test," *IEEE Trans. Commun. Technol.*, vol. COM-19, Part II, pp. 821–835, Oct. 1971.

Addition to "A Method for Decoding of Generalized Goppa Codes"

DAVID M. MANDELBAUM

***Abstract*—In a previous correspondence,[1] a decoding procedure which uses continued fractions and which is applicable to a wide class of algebraic codes including Goppa codes was presented. The efficiency of this method is significantly increased.**

The efficiency of the decoding method in the above correspondence[1] can be significantly increased. In the following, all references will be to the equations and bibliography of the original paper.[1]

In the decoding process, the test (18) with the associated multiplications is not required; instead, the test for the correct convergent can be taken as

$$\deg (r_{i+1}(x)) < k + \deg (q_i(x)), \tag{18'}$$

and therefore no multiplication is needed.

This is shown as follows. From [6], we have

$$q_{i-1}(x)r_{i+1}(x) + q_i(x)r_i(x) = m(x)$$
$$p_{i-1}(x)r_{i+1}(x) + p_i(x)r_i(x) = v(x).$$

Multiplying the above two equations by $p_i(x)$ and $q_i(x)$, respectively, and subtracting the first from the second yields

$$\begin{aligned} &q_i(x)v(x) - p_i(x)m(x) \\ &\quad = q_i(x)p_{i-1}(x)r_{i+1}(x) + q_i(x)p_i(x)r_i(x) \\ &\quad - p_i(x)q_{i-1}(x)r_{i+1}(x) - p_i(x)q_i(x)r_i(x) \\ &\quad = r_{i+1}(x)(q_i(x)p_{i-1}(x) - p_i(x)q_{i-1}(x)) = r_{i+1}(x)(-1)^i. \end{aligned}$$

Since for the correct convergent

$$u(x) = v(x) - m(x)p_i(x)/q_i(x) \text{ and } \deg (u(x)) < k,$$

the rule (18′) follows. Also, $u(x)$ can be obtained by means of $u(x) = (-1)^i r_{i+1}(x)/q_i(x)$ when (18′) is satisfied. This is a particularly attractive method of obtaining $u(x)$ for low-rate codes.

As a result of the new test (18′), it is seen that this procedure is of equivalent complexity to that given in [4].

It can also be easily seen that the method presented in the above correspondence[1] can be used for decoding Goppa and Bose–Chandhuri–Hocquenghem (BCH) codes using the standard syndrome $S(z)$ as developed in [9]. That is, if $S(z) = \eta(z)/\sigma(z) \bmod g(z)$, then, if we set $S'(x) = x^r S(1/x)$ where $r = \deg S(z)$; we can use the syndrome $S'(x)$ in the decoding method in the above correspondence[1]. It will be noticed that this method, like the Berlekamp–Massey algorithm, starts with the "end" of the syndrome while the method of [4] starts in the "middle" of the syndrome.

Two corrections should be made in the example in the above correspondence[1]; namely, the remainders $r_2(x)$ and $r_3(x)$ should read $r_2(x) = \beta^2x^6 + \beta^2x^5 + x^4 + x^3 + \beta^4x^2 + \beta^6x + \beta$ and $r_3(x) = \beta^5x^5 + \beta^2x^4 + \beta^4x^3 + \beta^3x^2 + \beta^6x + 1$, respectively.

Manuscript received February 28, 1977; revised June 1, 1977.
The author is at P.O. Box 645, Eatontown, NJ 07724.
[1] D. M. Mandelbaum, *IEEE Trans. Inform Theory*, vol. IT-23, pp. 137–140, Jan. 1977.