Short Shortened Binary Block Codes

{Jong-Kyu Kim°, Heunchul Lee, Inkyu Lee}* and Carl-Erik W. Sundberg¨
*Department of Communication Engineering, Korea University
Email : {jkkim, heunchul}@wireless.korea.ac.kr, inkyu@korea.ac.kr
¨SundComm, Chatham, NJ, USA Email : cews@ieee.org

Abstract

Among applications for short binary block codes are the transmission of header and control information in packets in e.g. digital audio broadcasting. In this paper, we give an inventory of good short binary block codes with information blocks of length equal to multiples of half bytes. We also compare these block codes with tailbiting convolutional codes. For high signal-to-noise ratios, the minimum Hamming distance and the corresponding error coefficient dominates the block error probability performance in the additive white Gaussian noise (AWGN) channel. We demonstrate that the choice of shortening affects the weight spectrum of the code when the length of shortening is greater than a certain number. We also show that some shortened codes are transparent. General properties of shortened $d_{\min}=3$ Hamming codes and extended $d_{\min}=4$ Hamming codes are illustrated. An upper bound on the error coefficient for all shortened codes is derived. We also present some code search results for the optimum shortened (19,8), (20,8) codes (shortened from the Golay code) and (26,16), (27,16) codes (shortened from the (31,21) BCH code) as well as short shortened Hamming codes.

1. Introduction

For many applications, e.g. in Digital Audio Broadcasting, there exist short packet headers that need protection by means of short binary block codes [1] [2] [3] [4], where error correction and detection applications are of interest. In this case, both hard decision decoding and soft decision maximum likelihood decoding (MLD) [4] are possible. For the soft decision MLD, tailbiting convolutional codes [5] with efficient decoding [6] [7] can be employed. In this paper, we will study the issues regarding the performance of shortened binary block codes. A code is shortened by deleting a message coordinate from the encoding process.

It turns out that independently of decoding methods, the minimum Hamming distance and the error coefficient A_d determine the performance for high signal to noise ratio (SNR) for the additive white Gaussian noise (AWGN) channel with coherent BPSK and QPSK modulation [8]. This is also the case for hard decision decoding in a binary symmetric channel with the low cross over probability p [4] [8]. Furthermore, for Rayleigh fading channels it is also of interest to keep A_d as small as possible.

Even with maximum *a posteriori* probability (MAP) decoder [9] [10] [11], A_d determines the probability of word errors for high SNR, thus we need to minimize A_d. We will see that for some shortened block codes, the weight spectrum for a given number of shortening bits is affected by the choice of the shortening pattern, when all other parameters such as code rate and code length are the same.

We are particularly interested in codes of size equal to multiples of half byte in the information bit field. An inventory of the minimum distance of such linear binary codes has been constructed in [12] [13] [14]. We present numerical search results of the weight spectra for the (19,8) codes shortened from the (23,12) Golay code and the (20,8) codes shortened from the extended (24,12) Golay code for different shortening patterns. We also illustrate results for shortened Hamming and BCH codes.

In the spirit of [1] where the impact of shortening on the weight spectrum and the performance of some short shortened Hamming block codes was studied, we also derive some simple general analytical bounds on the dominating components of the weight spectrum. For perfect codes, we arrive at a simple exact expression on A_d. We also discuss the impact of shortening in general on the weight

TABLE Ⅰ
MINIMUM CODEWORD LENGTH n FOR INFORMATION BITS k AND MINIMUM DISTANCE $d_{\min}$ FOR THE BEST CODES FROM [12]-[14]

k \ $d_{\min}$	3	4	5	6	7	8	9	10	11	12
8	12	13	16	17	19	20	25	26	28	29
12	17	18	21	22	23	24	30	31	33	34
16	21	22	26	27	30	31	35	36	39	40
20	25	26	30	31	35	36	40	41	43	44
24	29	30	35	36	40	41	45	46	47	48
28	34	35	39	40	44	45	51	52	55	56
32	38	39	43	44	49	50	56	57	59	60
36	42	43	47	48	53	54	60	61	53	54
40	46	47	52	53	57	58	64	65	70	74

spectra of codes. In particular, transparent codes where the all one sequence is a codeword are considered, since transparent codes have some advantages over nontransparent codes in designing diagnostic routines for semiconductor memories with error correcting codes [1].

In this paper we also compare short shortened block codes with short tailbiting convolutional codes with the same rate [15].

The remainder of the paper is organized as follows: Section 2 presents an inventory of good short binary block codes and compare with tailbiting codes. In section 3 we discuss the performance of short block codes with hard and soft decoders. This leads to the search for the optimal shortened codes in section 4. Finally the paper is terminated by a conclusion.

2. Short block codes

In the literature there are a number of short linear binary block codes (see [12] [13] [14] and references therein). Table Ⅰ summarizes these results with the minimum block length n for given k and the minimum Hamming distance $d_{\min}$. Here we list the information bit block length k in the increment of half byte size (4bits) from $k=8$ to $k=40$ at the minimum Hamming distance of $d_{\min}=3,4,\dots,12$. The two left most columns ($d_{\min}=3$ and 4) in the table represent the shortened Hamming codes and the extended Hamming codes. Most of the codes in Table Ⅰ are obtained by shortening a full length code. For details, see [12] [13] [14]. Here we will pick a few of the codes in Table Ⅰ and optimize the shortening patterns in terms of the minimum error coefficient.

TABLE Ⅱ
COMPARISONS OF SOME OPTIMAL SHORTENED BLOCK CODES TO TAILBITING CODES FROM [15] WITH THE SAME RATE AND LENGTH

Rate	Block codes			Tailbiting codes		
	n	k	$d_{\min}$	m	$n_{d\min}$	$d_{\min}$
2/3	12	8	3	2	16	3
2/3	26	24	6	5	1048	6
1/2	48	24	12	8	372	10

Alternatives to the block codes in Table Ⅰ are tailbiting convolutional codes, [5] [6] [15]. Since these codes are convolutional, they have a trellis structure for Viterbi or MAP decoding [6] [15]. A few of the codes in Table Ⅰ are compared with tailbiting codes in Table Ⅱ. Table Ⅱ compares of some optimal shortened block codes to tailbiting codes from [15] with the same rate. Most of the code rates k/n in Table Ⅰ are not directly comparable to simple rational values like 2/3 and 1/2 but those in Table Ⅱ are. Table Ⅱ lists the tailbiting codes with the minimum distance $d_{\min}$, memory m (2^m states) and the number of error sequences of weight $d_{\min}$ equal to $n_{d_{\min}}$. We notice that the distance properties for the block codes and the tailbiting codes are quite comparable. For $k=24$, the tailbiting codes may be preferable for soft decoding because of lower decoder complexity.

3. Performance of short block codes with various decoding

For binary symmetric channels, we obtain the word error probability of an (n,k) binary block code with the minimum distance $d_{\min}$ (odd) and $2t+1=d$ using a bounded distance hard decision decoding [3] [4] as

$$P(E) \le \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j} \tag{1}$$

where the equality holds for perfect codes.

In [2], we show that for all shortened binary block codes

$$A_{d_{\min}} \le \frac{\binom{n}{t+1}}{\binom{d_{\min}}{t}} \tag{2}$$

with equality for a few perfect binary codes such as Hamming codes with $d_{\min}=3$ and Golay codes with $d_{\min}=7$. We have found empirically that the bound on A_d is quite tight for shortened perfect codes, while it is somewhat loose for nonperfect codes.

The probability of undetected error is given as

$$P_u = \sum_{j=d_{\min}}^{n} A_j p^j (1-p)^{n-j} \tag{3}$$

which can be approximated as for small p

$$P_u \sim A_{d_{\min}} p^{d_{\min}} \tag{4}$$

Thus it is of interest to choose a small A_d for a given $d = d_{\min}$.

For the hard decision MLD, the word error rate is upper bounded by

$$P(E) \leq \sum_{d=d_{\min}}^{n} A_d P_{u,d} \tag{5}$$

where $P_{u,j}$ for hard decision decoding is given as

$$P_{u,j} = \begin{cases} \sum_{e=\frac{j+1}{2}}^{j} \binom{j}{e} p^e (1-p)^{j-e}, & j \quad \text{odd} \\ \frac{1}{2}\binom{j}{j/2} p^{j/2}(1-p)^{j/2} & \\ + \sum_{e=j/2+1}^{j} \binom{j}{e} p^e (1-p)^{j-e}, & j \quad \text{even} \end{cases}$$

In contrast, with the soft MLD, the word error rate is upper bounded by [4] [16]

$$P(E) \leq \sum_{j=d_{\min}}^{n} A_j Q\left(\sqrt{2jR\frac{E_b}{N_0}}\right) \tag{7}$$

which is approximated for high SNR by

$$P(E) \sim A_{d_{\min}} Q\left(\sqrt{2d_{\min}R\frac{E_b}{N_0}}\right) \tag{8}$$

where $R = \frac{k}{n}$.

We note that other than the minimum distance $d_{\min}$, it is also important to minimize $A_{d_{\min}}$. With a sequence MAP decoder [9] [10] [11], an expression similar to (5) can be derived, where individual *a priori* probabilities of the transmitted bits affect the metric values used in the decoder and the modified distance measure. However, *a priori* probabilities do not affect the performance for high SNR [9]. In summary, independently of the value of *a priori* probabilities, it is a good choice to select a code with maximum minimum distance $d = d_{\min}$ and the minimum number of codewords of weight $d_{\min}$, $A_{d_{\min}}$.

4. Optimal shortening and code search results

In [1] some transparent Hamming codes were studied and it was noticed that different shortening patterns with the same number of shortening bits s could produce codes with the same minimum distance $d_{\min}$ and rate (the same n and k) but with a different weight spectrum. It appears that this observation applies to any shortened code. For small s values, all our search results indicate that the weight spectrum is unique independently of the shortening pattern. However as s increases, a multiplicity of the weight spectra starts appearing with an growing number of different spectra. As was noted in [4], for shortened $d_{\min} = 3$ Hamming codes, there exists a shortening with $A_3 = 0$ which gives rise to $d_{\min} = 4$. This was also observed in [1]. Thus, if a multiplicity of weight spectra exists, it is expected that the one with the smallest $A_{d_{\min}}$ is in most cases preferable. The choice of such a shortened short code often comes with no extra cost.

A. Properties of shortenings

Any shortened single parity $d_{\min} = 2$ code has a unique weight spectrum. There are several properties associated with transparent codes. First, only codes with odd k are transparent. Also any perfect $d_{\min} = 3$ Hamming code is transparent. Shortenings with $s < d_{\min}$ yield a unique weight spectrum and nontransparent codes. For the case of any perfect (n,k) Hamming code, the parity check matrix H contains all binary column vectors of length $n-k$ bits except for the all zero sequence [3]. Using this fact, it is easy to show analytically that any shortening with $s = 1$ generates the same weight spectrum because the parity check matrices of any two codes with different $s = 1$ shortenings produce the same code word set. It is straightforward to apply the same reasoning to shortenings with $s = 2$ where one position overlaps in the two shortening patterns. For the case of two completely different $s = 2$ shortenings, we hypothesize that for all Hamming codes there is only one unique weight spectrum. The numerical results for short codes support this conjecture.

For $s = d_{\min}$, there exist a weight spectrum which corresponds to a transparent code and at least one other weight spectrum which corresponds to a nontransparent code. For the case of $d_{\min} = 4$, this is obtained by an overall parity check bit. If the weight spectrum is unique for the codes with $d_{\min} = 3$ case, the same is true for codes with $d_{\min} = 4$. For $d_{\min}$ greater than 4, e.g $d_{\min} \geq 5$, the same conclusion as above applies for transparent shortened codes. Thus for $s = d_{\min}$, at least one transparent shortened code exists if the full length code is transparent. At the same time, at least one nontransparent code with $s = d_{\min}$ also exists. As a result, there are at least two weight spectra for $s = d_{\min}$.

In contrast to the Hamming codes, a multiplicity of weight spectra may appear for codes with $d_{\min} \geq 5$ and $s \leq d_{\min}$, as we will see from the numerical results. In sections Ⅳ-B and Ⅳ-C below, we give some examples of results from the code search for the best shortening patterns for the (23,12) Golay code and the (31,21) BCH code. The more detailed codes are reported in [2], where we have also given some results for shortened $d_{\min}=3$ and $d_{\min}=4$ Hamming codes.

B. Code search results for the shortened (23,12) Golay code and the extended (24,12) Golay code

It should be noted that a time-reversed version of the generator polynomial exists for these codes yielding the same weight spectra set as those reported below for any shortening. Furthermore, any noncyclic code which can be formed from reordering of the bits in the full length codes used below also yields the same set of weight spectra for all corresponding shortened codes.

The generator polynomial for the (23,12) Golay code is given as

$$g_1(X) = 1 + X^2 + X^4 + X^5 + X^6 + X^{10} + X^{11}$$

The alternative generator polynomial

$$g_2(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$$

will give the same weight spectra results for all shortening values *s*, since $g_2(X)$ is a time-reversed version of $g_1(X)$. All shortened (19,8) codes have the same weight spectrum given in Table Ⅲ, which is not a transparent code as expected. In all the tables, P indicates shortening pattern. A zero in the P means that the code bit is not to be transmitted.

TABLE Ⅲ

SHORTENED (19,8) GOLAY CODE ($d_{\min}$=7, s=4)

A_d ($d=d_{\min},d_{\min}+1,\dots,20$)	52 78 0 0 72 48 0 0 4 1 0 0 0
P	1 1 1 1 1 1 1 1 0 0 0 0

TABLE Ⅳ

SHORTENED (20,8) GOLAY CODE ($d_{\min}$=8, s=4)

A_d ($d=d_{\min},d_{\min}+1,\dots,21$)	130 0 0 0 120 0 0 0 5 0 0 0 0
P	1 1 1 1 1 1 1 1 0 0 0 0

The extended (24,12) Golay code is obtained by adding an overall parity bit to the cyclic (23,12) Golay code. The shortened (20,8) code also has only one weight spectrum given in Table Ⅳ. This code is also nontransparent. More detailed results about shortened Golay codes with other shortening values are given in [2].

C. Code search results for the shortened (31,21) BCH code and the extended (32,21) BCH code

The (31,21) BCH code used is generated by

$$g(X) = 1 + X^3 + X^5 + X^6 + X^8 + X^9 + X^{10}$$

The extended (32,21) BCH code is obtained by adding an overall parity bit. Various power spectra for the shortened (26,16) code with $d_{\min}=5$ are shown in the Table V where A_5 varies from 69 to 76. We note that the best and worst codes are nontransparent. The best transparent (26,16) code with $A_5=70$ is also given in Table V with its corresponding shortening pattern.

Corresponding results are repeated for the shortened (27,16) code with $d_{\min}=6$. In contrast to the shortened Golay code results, we now get a multitude of weight spectra since the shortening is beyond the minimum distance $d_{\min}$. For detailed results for a different number of shortening bits, see the search results in [2]. In Table V, we also show the weight spectra for two shortened codes with $s=9$ from the (31,21) BCH code above, namely the (22,12) code with $d_{\min}=5$ and the (23,12) code with $d_{\min}=6$. Note that the difference in A_d between the best and the worst cases with $s=9$ now increases compared to the case with $s=5$. For the Golay code, multiple weight distributions are demonstrated in [2], where we also give data for short shortened Hamming codes as well as short shortened extended Hamming codes.

5. Discussion and Conclusion

We have studied short shortened binary codes and conclude that in some cases there is a room for an improved performance by selecting the best shortening. We have drawn some general conclusions of the impact of different shortenings on the weight spectrum and on the transparency of the shortened codes. A general upper bound have been derived on the dominant error coefficient A_d for any shortened code. Numerical code search results are given for a few selected shortened codes. A simple comparison has also been made to tailbiting convolutional codes. We notice that in most cases the choice of shortening patterns affects the weight spectrum. Since this gain normally comes for free, we might as well use it. For illustrative purposes, we choose to perform computer search for some selected codes only. These results imply, however, that if shortened

TABLE V

(26,16), (27,16), (22,12) and (23,12) SHORTENED BCH CODE

(26,16) SHORTENED BCH CODE $d_{\min}=5$, $s=5$	best code	A_d	1 0 0 0 0 69 255 671 1554 2920 4992 7792 9776 9882 9110 7750 5349 2944 1496 680 216 57 19 3 0 0 0
		P	1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 0
	worst code	A_d	1 0 0 0 0 76 251 640 1570 2960 4976 7808 9760 9800 9150 7808 5333 2960 1480 640 232 76 15 0 0 0 0
		P	1 1 1 1 1 0 1 1 1 0 0 1 1 1 1 1 1 1 1 0 1 0
	best transparent code	A_d	1 0 0 0 0 70 256 680 1530 2840 5117 8024 9480 9540 9480 8024 5117 2840 1530 680 256 70 0 0 0 0 1
		P	1 1 1 1 1 0 1 1 1 1 1 1 1 0 1 1 1 0 1 0 0
(27,16) SHORTENED BCH CODE $d_{\min}=6$, $s=5$	best code	A_d	1 0 0 0 0 0 322 0 2235 0 7896 0 17568 0 19020 0 13071 0 4440 0 912 0 66 0 5 0 0 0
		P	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 0 0
	worst code	A_d	1 0 0 0 0 0 327 0 2210 0 7936 0 17568 0 18950 0 13141 0 4440 0 872 0 91 0 0 0 0 0
		P	1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 0 0 0 0
(22,12) SHORTENED BCH CODE $d_{\min}=5$, $s=9$	best code	A_d	1 0 0 0 0 20 101 160 329 460 577 768 619 460 335 160 74 20 11 0 1 0 0
		P	1 0 1 1 0 1 0 1 1 1 1 1 0 0 1 1 0 1 0 0 0
	worst code	A_d	1 0 0 0 0 37 84 157 332 467 570 719 668 467 328 179 55 21 10 1 0 0 0
		P	1 1 0 1 1 0 0 0 0 1 0 1 0 1 1 1 1 1 1 0 0
	best transparent code	A_d	1 0 0 0 0 26 85 180 306 454 632 728 632 454 306 180 85 26 0 0 0 0 1
		P	0 1 1 1 1 1 1 0 0 1 1 1 1 1 0 0 1 0 0 0 0
(23,12) SHORTENED BCH CODE $d_{\min}=6$, s=9	best code	A_d	1 0 0 0 0 0 104 0 516 0 1044 0 1366 0 800 0 227 0 36 0 2 0 0 0
		P	1 1 0 1 0 1 1 1 1 1 1 1 1 0 1 0 0 0 0 0 0
	worst code	A_d	1 0 0 0 0 0 123 0 477 0 1067 0 1347 0 825 0 222 0 33 0 1 0 0 0
		P	1 1 1 1 1 1 0 1 0 1 0 0 1 1 1 1 0 0 0 0 0

codes are preferred for certain applications, an optimization of the shortening pattern is worthwhile.

6. Reference

[1] C.-E. W. Sundberg, "Properties of transparent shortened codes for memories with stuck-at faults.", IEEE Transactions on Computers, vol.28, pp.686-690, September 1979.

[2] H. Lee, J.-K. Kim, I. Lee, and C.-E. Sundberg, "On Short Shortened Binary Block Codes", In submission to Journal of Communications and Networks, January 2006.

[3] S. Lin and D. J. Costello Jr, Error Control Coding : Fundamentals and Applications. Second Edition, Pearson / Prentice Hall, 2004.

[4] S. B. Wicker, Error Control Systems for Digital Communication and Storage. Prentice Hall, 1995.

[5] H. Ma and J. Wolf, "On Tail Biting Convolutional Codes", IEEE Transactions on Communications, vol. 34, pp. 104-111, February 1986.

[6] R. Cox and C.-E. W. Sundberg, "An efficient adaptive circular Viterbi algorithm for decoding generalized tailbiting convolutional codes", IEEE Transactions on Vehicular Technology, vol. 43, pp. 57-68, February 1994.

[7] R. Shao, S. Lin, and M. Fossorier, "Two decoding algorithms for tailbiting codes", IEEE Transactions on Communications, vol. 51, pp. 1658-1665, October 2003.

[8] J. G. Proakis, Digital Communications. Fourth Edition, McGraw-Hill Series in Electrical and Computer Engineering 2001.

[9] C. Leanderson and C.-E. W. Sundberg, "Performance Evaluation of List sequence Map Decoding", IEEE Transactions on Communications, vol. com-53, pp. 422-432, March 2005.

[10] J. Hagenauer, "Source-controlled channel decoding", IEEE Transactions on Communications, vol. 43, pp. 2449-2457, September 1995.

[11] J. Kroll and N. Phamdo, "Analysis and design of trellis codes optimized for a binary symmetric Markov source with MAP detection", IEEE Transactions on Information Theory, vol. 44, pp. 2977-2987, November 1998.

[12] E. Agrell, A. Vardy and K. Zeger, "A table of upper bounds for binary codes", IEEE Transactions on Information Theory, vol. 47, pp. 3004-3006, November 2001.

[13] A. E. Brouwer, "Bounds on the minimum distance of linear codes", in *www.win.tue.nl/aeb/voorlincod.html*

[14] D. B. Jaffe, "Information about binary linear codes", in *www.math.unl.edu/djaffe/codes/webcodes/codeform/html*.

[15] P. Stahl, "On Tailbiting Codes from Convolutional Codes", in Ph.D. Thesis Lund University, Lund, Sweden, December 2001.

[16] P. O. Borjesson and C.-E. W. Sundberg, "Simple Approximation of the Error Function Q(x)", IEEE Transactions on Communications, vol. COM-27, pp. 639-643, March 1979.