On "The Optimal Linear Receiving Filter for Digital Transmission Over Nonlinear Channels"

William A. Gardner, *Senior Member, IEEE*

***Abstract*—A recent paper shows that the matched-filter/tapped-delay-line structure is optimum not only for linear pulse-modulated signals and linear channel distortion, but also for nonlinear finite-alphabet pulse-modulation and some nonlinear channel distortion. This has important practical applications. Therefore, its connection with other work reported in the literature is brought to light in this note.**

***Index Terms*—Optimum receivers, matched filters, nonlinear channels.**

The optimal linear receiving filter for digital transmission derived in the recent paper [1] is closely related to that derived in [2]. The structure of the filter derived in [1]—a parallel bank of matched filters, each followed by a tapped delay line—is identical to that derived in [2]. However, this structure is shown in [2] to be a special case of a more general structure that can be used for MMSE data-symbol estimation, MMSE signal-waveform estimation, or MMSE estimation of the *a posteriori* probabilities of the data symbols. Also, the solution presented in [1] is not as explicit as that presented in [2], which is expressed directly in terms of symbol correlation, pulse shape, and noise spectrum. The important practical ramifications of less than full dimensionality of the signal set, which is discussed briefly in [1], is treated at length in [3]. In addition, the derivation in [2] accommodates unlimited transmitted-signal pulse-duration and channel memory, whereas that in [1] is restricted to finite duration pulses (infinite excess bandwidth) and finite channel memory.

On the other hand, it is explained in [1] that the signal model adopted (in both [1] and [2]) can be used to model some nonlinear channels, which were not explicitly considered in [2], by expanding the symbol alphabet and reinterpreting the signal pulses. This has important practical applications.

Other work related to [1] includes [4], where the related signal-waveform estimation problem is studied and it is shown that the optimum waveform estimator functions like a regenerative repeater; [5], where an analogous receiver structure is derived for optical digital data transmission (which can be interpreted in terms of a random nonlinear channel); [6], where a novel interpretation delay of the matched-filter tapped-line structure as a means for exploiting the inherent frequency diversity in pulse-modulated signals that results from the spectral correlation that is characteristic of cyclostationary processes, is given, and the value of this for suppression of co-channel interference and distortion due to frequency-selective fading is explained, and where the role of the fractionally spaced equalizer for implementing this is clarified; and [7] and [8], where the functions $G_x^{(n)}(f)$ that arise in the receiving filter design equation [1, (2.8)] are shown to be spectral correlation density functions and are explicitly calculated for many types of communication signals.

References

[1] E. Biglieri, M. Elia, and L. Lopresti, "The optimal linear receiving filter for digital transmission over nonlinear channels," *IEEE Trans. Inform. Theory*, vol. 35, no. 3, pp. 620–625, May 1989.

Manuscript received September 18, 1989.

The author is with the Department of Electrical Engineering and Computer Science, University of California, Davis, CA 95616.

IEEE Log Number 9039290.

[2] W. A. Gardner, "The structure of least-mean-square linear estimators for synchronous M-ary signals," *IEEE Trans. Inform. Theory*, vol. IT-19, no. 2, pp. 240–243, Mar. 1973.

[3] ___, "Design of nearest prototype signal classifiers," *IEEE Trans. Inform. Theory*, vol. IT-27, no. 3, pp. 368–372, May 1981.

[4] W. A. Gardner and L. E. Franks, "Characterization of cyclostationary random signal processes," *IEEE Trans. Inform. Theory*, vol. IT-21, no. 1, pp. 4–14, Jan. 1975.

[5] W. A. Gardner, "An equivalent linear model for marked and filtered doubly stochastic Poisson processes with application to MMSE linear estimation for synchronous M-ary optical data signals," *IEEE Trans. Commun.*, vol. COM-24, pp. 917–921, Aug. 1976.

[6] W. A. Gardner and W. A. Brown, "Frequency-shift filtering theory for adaptive co-channel interference removal," in *Proc. Twenty-Third Asilomar Conf. Signals, Syst., and Comput.*, Oct.–Nov., 1989.

[7] W. A. Gardner, *Statistical Spectral Analysis: A Nonprobabilistic Theory*. Englewood Cliffs, NJ: Prentice-Hall, 1987.

[8] ___, *Introduction to Random Processes with Applications to Signals and Systems*, second ed. New York: McGraw-Hill, 1990.

Linear Codes with Covering Radius 2 and Other New Covering Codes

Ernst M. Gabidulin, Alexander A. Davydov, and Leonid M. Tombak

***Abstract*—This work gives infinite families of linear binary codes with covering radius $R = 2$ and minimum distance $d = 3$ and $d = 4$. Using the constructed codes with $d = 3$, $R = 2$, families of covering codes with $R > 2$ are obtained. The parameters of many constructed codes with $R \geq 2$ are better than the parameters of known codes. The parity check matrices of constructed codes with $d = 4$, $R = 2$ are equivalent to complete caps in projective geometry.**

I. Introduction

Covering codes are being extensively studied, see, e.g., [1], [2], [4]–[7], [10]–[12], and [17].

We consider linear binary covering codes.

Let an $[n, k, d]R$ code be a linear binary code of length n, dimension k, minimum distance d and covering radius R, Denote by $t[n, k]$ the smallest covering radius of any linear binary code of length n and dimension k. Let r be the number of check symbols of a code. Let $\mu_d[n, R]$ denote the density of the covering of binary n-dimensional space by spheres with radius R, whose centers correspond to the $[n, k, d]R$ codewords (cf. [5]). Let

$$\bar{\mu}_d[R] = \liminf_{n \to \infty} \mu_d[n, R]. \tag{1}$$

Manuscript received August 25, 1989; revised March 27, 1990. This work was presented in part at the Xth Symposium on Problem of Redundancy in Information Systems, Leningrad, USSR, June 1989, and at the IV International Sweden–Soviet Workshop on Information Theory "Convolutional Codes; Multi-user Communication," Gotland, Sweden, August 1989.

E. M. Gabidulin is with the Moscow Institute of Physics and Technology, 141700 Dolgoprudnii, Moscow Region, USSR.

A. A. Davydov and L. M. Tombak are with the Institute for Problems of Cybernetics of Academy of Sciences of the USSR, Vavilov Street 37, 117312 Moscow, USSR.

IEEE Log Number 9036937.

This correspondence is mostly devoted to codes with $R = 2$. If $R = 2$ then $d = 3$ or $d = 4$ excepting the $[5, 1, 5]2$ code.

Graham and Sloane [7] described $[9, 4, 3]2$, $[13, 7, 3]2$, $[19, 12, 3]2$, $[59, 49, 3]2$ codes and the infinite family of codes with parameters

$$R = 2,\ d = 3,\ r \geq 7,\ n = 2^m + 2^{r-m} - 4,\ m = \lceil r/2 \rceil. \quad (2)$$

Brualdi, Pless, and Wilson [1] obtained $[13, 7, 4]2$, $[41, 29, 3]3$ codes and the infinite family of codes with parameters

$$R = 2,\ d = 3,\ r = 4u + \delta \geq 8,\ n = (2^u - 1)(2^{u+1} + 1) + \varphi(\delta), \quad (3)$$

where $\delta \in \{\overline{0,3}\}$, $\varphi(\delta) = 2^{2u+\delta-1} - 1$ if $\delta \geq 1$, $\varphi(0) = 0$.

Codes in (3) provide $t[27, 19] = t[42, 33] = t[58, 48] = 2$. Using results in [1], Calderbank and Sloane [2] proved that $t[56, 43] = t[57, 44] = 3$, $t[49, 30] = t[64, 44] = 5$, $t[63, 40] = 6$.

Codes with $R = 2$, $d = 4$, $n > 2^{r-2}$ were described in [6]. It is an open problem to establish an existence and to design all $[n, n - r, 4]2$ codes for $n < 2^{r-2}$.

Szönyi [16] described maximal 3-independent sets in the elementary abelian p-group of order p^r (see Section IV). For $p = 2$ these sets are parity check matrices of an infinite family of codes with parameters

$$R = 2,\ d = 4,\ r \geq 5,\ n = 2^m + 2^{r-m} - 3,\ m = \lceil r/2 \rceil. \quad (4)$$

Codes in (2) provide $\overline{\mu}_3[2] = 2$, where the limit in (1) is taken over a subsequence of codes with $r = 2m$, $n = 2^{m+1} - 4$, $m \to \infty$. Similarly, codes in (3) with $r = 4u$ and codes in (4) with $r = 2m$ provide respectively $\overline{\mu}_3[2] = 2$ and $\overline{\mu}_4[2] = 2$.

It is interesting to construct codes with $R = 2$, which provide $\overline{\mu}_d[2] < 2$ for $d = 3, 4$, and codes, which for fixed r have smaller length than the codes in (2), (3) (if $d = 3$) and than the codes in (4) (if $d = 4$).

Codes with $R = 2$, $d = 4$ are useful also for projective geometry (see Section IV).

In Sections III, IV we construct infinite families of codes with parameters

$$R = 2, \quad d = 3, \quad r \geq 7,$$
$$n = f(r) \triangleq \begin{cases} 7 \times 2^{m-2} - 2, & \text{if } r = 2m \\ 5 \times 2^{m-2} - 1, & \text{if } r = 2m - 1, \end{cases} \quad (5)$$

$$R = 2, \quad d = 4, \quad r \geq 10,$$
$$n = \begin{cases} 15 \times 2^{m-3} - 3, & \text{if } r = 2m \\ 23 \times 2^{m-4} - 3, & \text{if } r = 2m - 1. \end{cases} \quad (6)$$

In Sections IV we describe also $[28, 20, 4]2$, $[43, 34, 4]2$ codes and (using directly the methods from [16]) codes with parameters

$$R = 2, \quad d = 4, \quad r \geq 5, \quad n = 2^t + 2^{r-t} - 3, \quad r - 2 \geq t \geq 2. \quad (7)$$

For fixed r, the codes in (5) have smaller length than the codes in (2), (3) and the codes in (6) have smaller length than the codes in (4).

In Section V, using the codes in (5) and Hamming and Golay codes in amalgamated direct sum (ADS) constructions [7], we obtain families of codes with $d = 3$, $R > 2$.

Many improvements of Graham and Sloane's table [7] (see also [1], [2]) follow from results of Sections III and V:

$$t[26, 18] = t[39 + i, 30 + i] = t[54 + j, 44 + j] = 2. \qquad i = \overline{0,2},\ j = \overline{0,3}.$$
$$t[40, 28] = t[53 + i, 40 + i] = 3, \qquad i = \overline{0,2}.$$
$$t[51 + i, 35 + i] = t[64, 47] = 4, \qquad i = 0, 1.$$
$$t[48, 29] = t[61 + i, 41 + i] = 5, \qquad i = \overline{0,2}.$$
$$t[62, 39] = 6. \quad (8)$$

In the table in [7] of linear covering codes the respective values are $-2-3, 3-4, 4-5, 5-6, 6-7$, where the first item is the lower bound on $t[n, k]$ and the second one is the covering radius of the best known code.

In Section VI the density of a covering for codes described in Sections III, IV is determined.

If we use the codes in (5) with $n = 7 \times 2^{m-2} - 2$, $m \to \infty$, and the codes in (6) with $n = 15 \times 2^{m-3} - 3$, $m \to \infty$, then we obtain

$$\overline{\mu}_3[2] = 49/32, \qquad \overline{\mu}_4[2] = 225/128. \quad (9)$$

II. Notations

Throughout this correspondence all columns and matrices are binary. An upper index in denotation of a matrix (column) is the number of rows (coordinates) in the matrix (column).

We associate with a matrix A the set $\{A\}$ that has its columns as elements. In this case an expression of a form $\{A\} + \{G\}$, where A and G are matrices, is treated as

$$\{A\} + \{G\} = \{x : x = a + g,\ a \in \{A\},\ g \in \{G\}\}. \quad (10)$$

Let $(e_i)^b$ be the column vector that is the binary b-bit presentation of element e_i of the field $\mathrm{GF}(2^b)$, where $i \in \{\overline{0, B}\}$, $B = 2^b - 1$, $e_0 = 0$, and if $i \neq j$ then $e_i \neq e_j$.

For definiteness, in examples we assume that column $(e_i)^b$ is the b-bit binary number equal to i.

Let E^b and $F^{2b}(e_j)$ denote the following matrices,

$$E^b = \left[(e_0)^b \quad (e_1)^b \quad \cdots \quad (e_B)^b \right], \quad (11)$$

$$F^{2b}(e_j) = \begin{bmatrix} (e_0)^b & (e_1)^b & (e_2)^b & \cdots & (e_B)^b \\ (e_0)^b & \left(e_1^{-1}e_j\right)^b & \left(e_2^{-1}e_j\right)^b & \cdots & \left(e_B^{-1}e_j\right)^b \end{bmatrix}, \quad (12)$$

where $e_0, e_i, e_j, e_i^{-1}e_j \in \mathrm{GF}(2^b)$, $i = \overline{1, B}$, $B = 2^b - 1$ (cf. the parity check matrix of the Melas code [13, Section 7.6], [14]).

Let $E^b_{i,j}$ be a matrix E^b with punctured columns $(e_i)^b, (e_j)^b$. Let E^b_0 be a matrix E^b with punctured column $(e_0)^b$. Let $F^{2b}_0(e_j)$ be a matrix $F^{2b}(e_j)$ with punctured column $(e_0)^{2b}$.

Denote by $P^b(e_i)$ a matrix with unique repeated column $(e_i)^b$. The number of columns of this matrix is determined by context.

The following matrices and column are used later.

$$\Pi^b(v) = \left[\begin{array}{c} v \cdots v \\ \hline E^{b-1} \end{array} \right], \qquad v \in \{0, 1\}, \quad (13)$$

$$W^{2m-1}(t, u) = \left[\begin{array}{c} 0 \cdots 0 \\ \hline E^{2m-4} \\ \hline t \cdots t \\ u \cdots u \end{array} \right], \qquad t, u \in \{0, 1\}, \quad (14)$$

$$\left(v, e_i, e_j, t, u\right)^{2m-1} = \begin{bmatrix} v \\ (e_i)^{m-2} \\ (e_j)^{m-2} \\ t \\ u \end{bmatrix}, \qquad v, t, u \in \{0, 1\}. \quad (15)$$

III. Constructions of Codes with $R = 2$, $d = 3$, $r \geq 7$

A code with parity check matrix H^r has $R = 2$ if any column from $\{E^r\}$ is a sum of two or fewer columns of matrix H^r [4, p. 328], i.e.,

$$\{H^r\} \cup \{\{H^r\} + \{H^r\}\} = \{E^r\}. \quad (16)$$

Lemma 1: Let $w_1 + w_2 = w_3$, where $w_g \in \mathrm{GF}(2^b)$, $g = \overline{1,3}$, $w_1 \neq w_2$, $w_1, w_2 \neq 0$. Let

$$h_{ij} = \begin{bmatrix} (e_i)^b \\ (e_j)^b \end{bmatrix}. \quad (17)$$

Then

$$h_{ij} \in \bigcup_{g=1}^{3} \left\{ \left\{ F_0^{2^b}(w_g) \right\} + \left\{ F_0^{2^b}(w_g) \right\} \right\}, \qquad i,j = \overline{1,2^b-1}. \quad (18)$$

Proof: The relation (18) holds (see (12)) if for any pair e_i, e_j $(i,j \in \overline{1,2^b-1})$ there is an element w_g, $g \in \overline{1,3}$, such that equation $x^{-1}w_g + (x+e_i)^{-1}w_g = e_j$ is solvable for $x \in \mathrm{GF}(2^b)$. Changing a variable, $x = ze_i$, we get

$$z^2 + z + e_i^{-1}e_j^{-1}w_g = 0. \quad (19)$$

Let $T_b(e_i) = e_i + e_i^2 + e_i^{2^2} + \cdots + e_i^{2^{b-1}}$ be the trace of element e_i of the field $\mathrm{GF}(2^b)$. Since $w_1 + w_2 = w_3$, at least one trace $T_b(e_i^{-1}e_j^{-1}w_g)$, $g \in \overline{1,3}$, is equal to zero, i.e., (19) has a solution [13, Sections 4.8, 9.7]. □

Theorem 1: Let the parity check matrix of a code be

$$B^{2m-1} = [N \quad D \quad Q \quad M \quad G], \quad (20)$$

where $2m-1 = r \geq 7$ and

$$N = \begin{bmatrix} 0\cdots 0 \\ \hline E_0^{m-2} \\ P^m(e_0) \end{bmatrix}, \quad (21)$$

$$D = \begin{bmatrix} 1\cdots 1 \\ \hline F^{2(m-2)}(w_1) \\ \hline 0\cdots 0 \\ 0\cdots 0 \end{bmatrix}, \qquad Q = \begin{bmatrix} 1\cdots 1 \\ \hline F^{2(m-2)}(w_2) \\ \hline 0\cdots 0 \\ 1\cdots 1 \end{bmatrix}, \quad (22)$$

$$M = \begin{bmatrix} 1\cdots 1 \\ \hline F^{2(m-2)}(w_3) \\ \hline 1\cdots 1 \\ 0\cdots 0 \end{bmatrix}, \qquad G = \begin{bmatrix} 1\cdots 1 \\ \hline P^{m-2}(e_0) \\ \hline E^{m-2} \\ \hline 1\cdots 1 \\ 1\cdots 1 \end{bmatrix}. \quad (23)$$

Here $w_1, w_2, w_3 \in \mathrm{GF}(2^{m-2})$; $w_1, w_2 \neq 0$, $w_1 \neq w_2$; $w_3 = w_1 + w_2$. Then this code has parameters $R = 2$, $n = 5\times 2^{m-2} - 1$, $d = 3$.

Proof: Values of parameters n, d follow from (11), (12), (20)–(23). We show based on (16) that $R = 2$. Evidently (see (11), (13), (14)),

$$\{E^{2m-1}\} = \{\Pi^{2m-1}(1)\} \cup \{W^{2m-1}(0,0)\} \cup \{W^{2m-1}(0,1)\} \cup \{W^{2m-1}(1,0)\} \cup \{W^{2m-1}(1,1)\}. \quad (24)$$

Let

$$L = [D \quad Q \quad M \quad G]. \quad (25)$$

Since the last b rows of matrix $F^{2^b}(e_j)$ contain all different columns of length b, we have, from (11)–(13), (21), (25),

$$\{L\} \cup \{\{N\} + \{L\}\} = \{\Pi^{2m-1}(1)\}. \quad (26)$$

Evidently (see (14), (22), (23)),

$$\{M\} + \{G\} = \{W^{2m-1}(0,1)\}; \qquad \{Q\} + \{G\} = \{W^{2m-1}(1,0)\}; \quad (27)$$

$$\{D\} + \{G\} = \{W^{2m-1}(1,1)\}. \quad (28)$$

From (11), (15), (21), (23), it follows that

$$(0, e_i, e_0, 0, 0)^{2m-1} \in \{N\}, \qquad (0, e_0, e_j, 0, 0)^{2m-1} \in \{G\} + \{G\},$$

$i,j \in \overline{1,2^{m-2}-1}$. Now, by Lemma 1,

$$\{N\} \cup \{\{G\} + \{G\}\} \cup \{\{D\} + \{D\}\} \cup \{\{Q\} + \{Q\}\} \cup \{\{M\} + \{M\}\} = \{W^{2m-1}(0,0)\}. \quad \square \quad (29)$$

Example: Let $r = 7$, $m = 4$, $(w_1)^{4-2} = (01)^{\mathrm{tr}}$, $(w_2)^{4-2} = (10)^{\mathrm{tr}}$, $(w_3)^{4-2} = (11)^{\mathrm{tr}}$. Then the parity check matrix,

$$B^{2\times 4-1} = \left[\begin{array}{ccccc} 000 & 1111 & 1111 & 1111 & 1111 \\ \hline 011 & 0011 & 0011 & 0011 & 0000 \\ 101 & 0101 & 0101 & 0101 & 0000 \\ 000 & 0011 & 0101 & 0110 & 0011 \\ 000 & 0110 & 0011 & 0101 & 0101 \\ 000 & 0000 & 0000 & 1111 & 1111 \\ 000 & 0000 & 1111 & 0000 & 1111 \end{array}\right], \quad (30)$$

defines a [19, 12, 3]2 code.

Denote by B_1^{2m-1}, D_1 and L_1 respectively matrices B^{2m-1}, D and L (see (20), (22), (25)) with punctured column $(10\cdots 0)^{\mathrm{tr}}$.

Theorem 2: Let the parity check matrix of a code be

$$T^{2m} = [Z \quad Y], \quad (31)$$

where $2m = r \geq 8$ and

$$Z = \begin{bmatrix} 0\cdots 0 \\ \hline B_1^{2m-1} \end{bmatrix}, \qquad Y = \begin{bmatrix} 1\cdots 1 \\ \hline E^{m-1} \\ P^m(e_i) \end{bmatrix}, \qquad i \in \{\overline{0,2^m-1}\}.$$

Then this code has parameters $R = 2$, $n = 7\times 2^{m-2} - 2$, $d = 3$.

Proof: Values of parameters n, d are evident (see (11), (20), (31)). Similar to Theorem 1 we show that $R = 2$.

Because the last m rows of matrix B_1^{2m-1} contain all different columns of length m, it holds that $\{Z\} + \{Y\} = \{\Pi^{2m}(1)\}$.

We show that $\{\{Z\} + \{Z\}\} \cup \{\{Y\} + \{Y\}\} = \{\Pi^{2m}(0)\}$. The last relation is equivalent to relation

$$\left\{\left\{B_1^{2m-1}\right\} + \left\{B_1^{2m-1}\right\}\right\} \cup \{\{Y^*\} + \{Y^*\}\} = \{E^{2m-1}\}, \quad (32)$$

where Y^* is matrix Y with punctured first row. It is easy to see from (11)–(13), (21), (25), (31), that

$$\{L_1\} \cup \{\{N\} + \{L_1\}\} \cup \{\{Y^*\} + \{Y^*\}\} \supset \{\Pi^{2m-1}(1)\}. \quad (33)$$

The relation (29) holds if in place of matrix D we use matrix D_1, because Lemma 1 uses matrices $F_0^{2^b}(w_g)$. Now from (20), (24), (27), and (33), it can be seen that for proving relation (32) it is sufficient to show that

$$\{\{D_1\} + \{G\}\} \cup \{\{M\} + \{Q\}\} = \{W^{2m-1}(1,1)\}. \quad (34)$$

From (11), (12), (15), (22), and (23), it follows, that

$$(0, e_i, e_j, 1, 1)^{2m-1} \in \{D_1\} + \{G\}, \qquad \text{if } i \neq 0.$$

We show that

$$(0, e_0, e_j, 1, 1)^{2m-1} \in \{M\} + \{Q\}.$$

The column $(0, e_0, e_0, 1, 1)^{2m-1}$ is the sum of the first columns of matrices M and Q. If $j \neq 0$ then (since $w_2 + w_3 = w_1$):

$$(0, e_0, e_j, 1, 1)^{2m-1} = (1, w_1 e_j^{-1}, w_1^{-1} e_j w_2, 0, 1)^{2m-1} + (1, w_1 e_j^{-1}, w_1^{-1} e_j w_3, 1, 0)^{2m-1}. \quad \square$$

Example: Let $r = 8$, $m = 4$, $i = 12$ and let matrix $B_1^{2\times 4-1}$ be obtained from matrix (30). Then the parity check matrix,

$$T^{2\times 4} = \left[\begin{array}{cll} 000 & 000000000000000 & 11111111 \\ \hline 000 & 111111111111111 & 00001111 \\ 011 & 011001100110000 & 00110011 \\ 101 & 101010101010000 & 01010101 \\ 000 & 011010101100011 & 11111111 \\ 000 & 110001101010101 & 11111111 \\ 000 & 000000011111111 & 00000000 \\ 000 & 000111100001111 & 00000000 \end{array}\right], \quad (35)$$

defines a [26, 18, 3]2 code.

IV. Projective Geometry and Constructions of Codes with $R=2$, $d=4$

An s-dimensional projective geometry $PG(s,q)$ is described in [9], [13], [15]. We use also the papers [3], [6], [8], and [16].

Let a binary column c_i of length r be a point of the geometry $PG(r-1,2)$. Then a set of three columns c_1, c_2, and c_3 such that $c_1+c_2=c_3$ is a line of this geometry.

A cap in projective geometry is a set of points such that no three are collinear. A complete cap is a cap of n points that is not contained in any cap of $n+1$ points.

A bisecant of a cap of the geometry $PG(r-1,2)$ is a line such that two points belong to this cap but the third point is external, i.e., it does not belong to the cap. If a cap is complete then every external point lies on a bisecant of the cap.

On the other hand, for a parity check matrix $H^r=[c_1c_2\cdots c_n]$ of a binary linear code with $d=4$ it holds that

$$c_i+c_j\neq c_k, \qquad \forall i,j,k\in\{\overline{1,n}\}. \tag{36}$$

Hence (see also (16)) a parity check matrix of a code with $d=4$, $R=2$ is a complete cap.

An open problem is the structure of complete caps with a number of points smaller than 2^{r-2}. The results of paper [16] and our constructions of $[n,n-r,4]2$ codes for $n<2^{r-2}$ partially answer this question.

The following results are obtained in [16, p. 163–164]. Let G be an elementary abelian p-group of order p^r, $r\geq 4$ an integer. Subset X of this group is called a maximal 3-independent set if it holds that $x_1+x_2+x_3\neq 0$ for any three elements $x_1,x_2,x_3\in X$ and for any $y\in G\setminus X$ there exist $x_1,x_2\in X$ for which $y+x_1+x_2=0$.

The group G is isomorphic to $G_1\times G_2$, where $|G_1|=p^m$, $|G_2|=p^{r-m}$, $m=\lceil r/2\rceil$. Let $p\neq 3$; $\gamma_i\in G_i$, $\gamma_i\neq 0$, $i=1,2$; $X_1=\{(\gamma_1,\delta)|\delta\in G_2,\ \delta\neq 2\gamma_2\}$, $X_2=\{(\xi,\gamma_2)|\xi\in G_1,\ \xi\neq 2\gamma_1\}$; $X=X_1\cup X_2$. Then X is a maximal 3-independent set and

$$|X|=p^m+p^{r-m}-3, \qquad m=\lceil r/2\rceil. \tag{37}$$

On the other hand, let $p=2$ and let a binary column of length r be the binary representation of an element of G. Then (see (16), (36)) a parity check matrix of a code with $d=4$, $R=2$ is a maximal 3-independent set and relation (4) follows from (37).

If we take $p=2$, $|G_1|=p^t$, $|G_2|=p^{r-t}$, $r-2\geq t\geq 2$, then we obtain the codes in (7) with the construction described in Theorem 3.

Theorem 3 [16]: Let the parity check matrix of a code be

$$H^r=[K \quad A \quad S], \tag{38}$$

where $r\geq 5$ and

$$K=\begin{bmatrix} E_{0,i}^t \\ P^{r-t}(e_j)\end{bmatrix}, \qquad A=\begin{bmatrix}(e_i)^t\\ (e_j)^{r-t}\end{bmatrix}, \qquad S=\begin{bmatrix}P^t(e_i)\\ E_{0,j}^{r-t}\end{bmatrix},$$

$i,j\neq 0$, $r-2\geq t\geq 2$. Then this code has parameters $R=2$, $d=4$, $n=2^t+2^{r-t}-3$.

Proof: Code length $n=2^t-2+1+2^{r-t}-2$. Let

$$g_{a,c}=\begin{bmatrix}(e_a)^t\\ (e_c)^{r-t}\end{bmatrix}.$$

From (10), (11), and (38), it follows that

$$\{\{K\}\cup\{A\}\}+\{\{K\}\cup\{A\}\}=\{g_{a,0}\}, \qquad a=\overline{0,2^t-1},$$
$$\{\{A\}\cup\{S\}\}+\{\{A\}\cup\{S\}\}=\{g_{0,c}\}, \qquad c=\overline{0,2^{r-t}-1},$$
$$\{K\}+\{S\}=\{g_{a,c}\}, \qquad a=\overline{1,2^t-1}$$

and

$$a\neq i, \qquad c=\overline{1,2^{r-t}-1}$$

and

$$c\neq j.$$

Hence, relations (16) and (36) hold. □

Remark 1: The construction of (38) may be considered as a modification of ADS constructions [7] under requirement $d=4$.

Example: Let $r=6$, $t=3$, $i=2$ and $j=6$. The matrix

$$H^6=\begin{bmatrix}001111 & 0 & 000000\\ 010011 & 1 & 111111\\ 110101 & 0 & 000000\\ 111111 & 1 & 000111\\ 111111 & 1 & 011001\\ 000000 & 0 & 101011\end{bmatrix}$$

is the parity check matrix of a [13,7,4]2 code, which is equivalent to the [13,7,4]2 code from [1, p. 107].

For $t=\lceil r/2\rceil=m$ the matrix in (38) defines the codes in (4), e.g., [9,4,4]2, [13,7,4]2, [21,14,4]2 codes. The first two codes have minimum length for any codes with $R=2$ and $r=5$, $r=6$ (see table in [7]). We conjecture that the [21,14,4]2 code has minimum length among codes with $R=2$, $d=4$, $r=7$. (But there is a [19,12,3]2 code [7].) For $r\geq 8$ we design codes with $R=2$, $d=4$, which have smaller length than the codes in (4).

Theorem 4: Let the parity check matrix of a code be

$$U^{2m}=[C \quad V \quad X \quad \Phi \quad \Lambda \quad Y], \tag{39}$$

where $2m=r\geq 10$; matrix Y is defined in (31);

$$C=\left[\begin{array}{c}0\cdots 0\\ 0\cdots 0\\ 0\cdots 0\\ \hline E_0^{m-3}\\ \hline P^{m-1}(\beta)\\ \hline 1\cdots 1\end{array}\right], \qquad V=\left[\begin{array}{c}0\cdots 0\\ 1\cdots 1\\ 0\cdots 0\\ \hline E^{m-3}\\ \hline P^{m-1}(\gamma)\\ \hline 1\cdots 1\end{array}\right], \qquad X=\left[\begin{array}{c}0\cdots 0\\ 1\cdots 1\\ 1\cdots 1\\ \hline E^{m-3}\\ \hline P^{m-1}(\delta)\\ \hline 0\cdots 0\end{array}\right], \tag{40}$$

$\beta,\gamma,\delta\in \mathrm{GF}(2^{m-1})$, $\beta\neq\gamma$, $\delta=\beta+\gamma$;

$$\Phi=\left[\begin{array}{c}0\cdots 0\\ 0\cdots 0\\ 1\cdots 1\\ \hline \Omega\\ \hline 0\cdots 0\end{array}\right], \qquad \Lambda=\left[\begin{array}{c}0\cdots 0\\ 0\cdots 0\\ 1\cdots 1\\ \hline \Omega(\beta)\\ \hline 1\cdots 1\end{array}\right], \tag{41}$$

$$\Omega=\left[\begin{array}{ccc:c}F_0^{2(m-3)}(w_1) & F^{2(m-3)}(w_2) & F^{2(m-3)}(w_3) & P^{m-3}(e_0)\\ & & & E^{m-3}\\ \hline 0\cdots 0 & 0\cdots 0 & 1\cdots 1 & 1\cdots 1\\ 0\cdots 0 & 1\cdots 1 & 0\cdots 0 & 1\cdots 1\end{array}\right], \tag{42}$$

$w_1,w_2,w_3\in \mathrm{GF}(2^{m-3})$, $w_1,w_2\neq 0$, $w_1\neq w_2$, $w_3=w_1+w_2$; $\Omega(\beta)$ is a matrix obtained by adding of column $(\beta)^{m-1}$ to the last $m-1$ coordinates of all columns of matrix Ω. Then this code has parameters $R=2$, $n=15\times 2^{m-3}-3$, $d=4$.

Proof: The value of length n follows from (11), (12), (39)–(42).

It is easy to see from (10)–(12), (39)–(42), that relation (36) holds, i.e., $d=4$. For example, $\{\{Y\}+\{Y\}\}\cap\{\{X\}\cup\{\Phi\}\}=\varnothing$, because $\delta\neq 0$, $w_1\neq 0$ and matrix Ω uses matrix $F_0^{2(m-3)}(w_1)$, i.e., the last m rows of matrix $[X\Phi]$ do not contain column $(e_0)^m$. $\{\{\Phi\}+\{\Lambda\}\}\cap C=\varnothing$, because matrix C uses matrix E_0^{m-3}, etc.

Similar to Theorems 1, 2 we show that $R=2$. Let $\Gamma=[\Phi\Lambda]$,

$$\Theta(v,t,u)=\begin{bmatrix} v\cdots v \\ t\cdots t \\ u\cdots u \\ \hline E^{2m-3} \end{bmatrix}, \qquad v,t,u\in\{0,1\}. \tag{43}$$

Let $\Theta(v,t,u;f)$ be a matrix containing all columns of matrix $\Theta(v,t,u)$, which have f on the last position, $f\in\{0,1\}$.

The following relations show that the relation (16) holds,

$$\{Y\}\cup\{\{Y\}+\{\{C\}\cup\{\Gamma\}\}\}=\Pi^{2m}(1), \tag{44}$$

$$\{X\}\cup\{\{C\}+\{X\}\}\cup\{\{V\}+\{\Gamma\}\}=\Theta(0,1,1), \tag{45}$$

$$\{V\}\cup\{\{C\}+\{V\}\}\cup\{\{X\}+\{\Gamma\}\}=\Theta(0,1,0), \tag{46}$$

$$\{\Gamma\}\cup\{\{C\}+\{\Gamma\}\}\cup\{\{V\}+\{X\}\}\cup\{\{Y\}+\{Y\}\}\supset\Theta(0,0,1), \tag{47}$$

$$\{\{C\}+\{C\}\}\cup\{\{\Phi\}+\{\Phi\}\}=\Theta(0,0,0;0), \tag{48}$$

$$\{C\}\cup\{\{\Phi\}+\{\Lambda\}\}=\Theta(0,0,0;1). \tag{49}$$

A proof of the relations (44)–(49) is analogous to the proofs of the Theorems 1, 2.

The last m rows of matrix Γ contain all columns of length m except the columns $(e_0)^m$ and $\mathscr{H}^m$, where $\mathscr{H}^m$ is column, contained $(\beta)^{m-1}$ on the first $m-1$ position and one on the last position. Hence, from (11), (13), (40), (41), we have (44)–(47).

From (20), (22), (23), (25), (42), it follows that matrix Ω is matrix L_1 with punctured first row, where L_1 is obtained from B_1^{2m-3}. Hence, we can prove relations (48) and (49), using (27), (29), and (34). (The relation (29) holds if instead of matrix D we use matrix D_1.) The set $\{\Phi\}+\{\Phi\}$ in (48) (respectively $\{\Phi\}+\{\Lambda\}$ in (49)) contains all columns from $\Theta(0,0,0;0)$ (respectively $\Theta(0,0,0;1)$) except columns such that the last m positions equal to $(e_0)^m$ (respectively $\mathscr{H}^m$). But these columns are contained in the set $\{C\}+\{C\}$ (respectively $\{C\}$). □

Example: Let $r=10$, $m=5$, $i=8$ (for matrix Y), $(\beta)^4=(1111)^{\mathrm{tr}}$, $(\gamma)^4=(1011)^{\mathrm{tr}}$, $(\delta)^4=(0100)^{\mathrm{tr}}$, $(w_1)^2=(01)^{\mathrm{tr}}$, $(w_2)^2=(10)^{\mathrm{tr}}$, $(w_3)^2=(11)^{\mathrm{tr}}$. Then the parity check matrix

$$U^{10}=\left[\begin{array}{lllll} 000 & 0000 & 0000 & 000000000000000 & 000000000000000 & 1111\cdots 1 \\ 000 & 1111 & 1111 & 000000000000000 & 000000000000000 & 0000\cdots 1 \\ 000 & 0000 & 1111 & 111111111111111 & 111111111111111 & 0000\cdots 1 \\ 011 & 0011 & 0011 & 011001100110000 & 011001100110000 & 0011\cdots 1 \\ 101 & 0101 & 0101 & 101010101010000 & 101010101010000 & 0101\cdots 1 \\ 111 & 1111 & 0000 & 011010101100011 & 100101010011100 & 0000\cdots 0 \\ 111 & 0000 & 1111 & 110001101010101 & 001110010101010 & 1111\cdots 1 \\ 111 & 1111 & 0000 & 000000011111111 & 111111100000000 & 0000\cdots 0 \\ 111 & 1111 & 0000 & 000111100001111 & 111000011110000 & 0000\cdots 0 \\ 111 & 1111 & 0000 & 000000000000000 & 111111111111111 & 0000\cdots 0 \end{array}\right]$$

defines a $[57,47,4]2$ code.

Theorem 5: Let the parity check matrix of a code be

$$\Psi^{2m-1}=[\pi \quad J], \tag{50}$$

where $2m-1=r\geq 11$ and

$$\pi=\begin{bmatrix} 0\cdots 0 \\ \hline U^{2(m-1)} \end{bmatrix}, \qquad J=\begin{bmatrix} 1\cdots 1 \\ \hline P^{m-1}(e_u) \\ \hline E^{m-1} \end{bmatrix}, \qquad u\in\overline{\{0,2^{m-1}-1\}}.$$

Then this code has parameters $R=2$, $n=23\times 2^{m-4}-3$, $d=4$.

Proof: Value of length n follow from (11), (39), (50).

By Theorem 4, $\{\pi\}+\{\pi\}=\Pi^{2m-1}(0)$. From (39)–(42), it follows that the first $m-1$ rows of matrix $U^{2(m-2)}$ contain all columns of length $m-1$ except the column $(e_0)^{m-1}$. Hence, $\{\{J\}+\{J\}\}\cap\{\pi\}=\varnothing$, $\{\{\pi\}+\{J\}\}\cap\{J\}=\varnothing$, i.e., $d=4$, and $\{J\}\cup\{\{\pi\}+\{J\}\}=\Pi^{2m-1}(1)$, i.e., $R=2$. □

Remark 2: The matrix U^8 is not the parity check matrix of a code with $R=2$, but the matrix Ψ^9 is the parity check matrix of a $[43,34,4]2$ code. The parity check matrix

$$H_1=\left[\begin{array}{lllllll} 0 & 00 & 00 & 0000000 & 0000000 & 11111111 & 0 \\ 0 & 11 & 11 & 0000000 & 0000000 & 00001111 & 0 \\ 0 & 00 & 11 & 1111111 & 1111111 & 00110011 & 0 \\ 1 & 00 & 11 & 1010100 & 1010100 & 01010101 & 0 \\ 1 & 10 & 10 & 1010101 & 0101010 & 11111111 & 0 \\ 1 & 01 & 01 & 0001111 & 1110000 & 00000000 & 0 \\ 1 & 01 & 01 & 0110011 & 1001100 & 00000000 & 0 \\ 1 & 11 & 00 & 0000000 & 1111111 & 00000000 & 1 \end{array}\right], \tag{51}$$

designed by using the ideas of the constructions described in (39), defines a $[28,20,4]2$ code. These facts can be proved similar to Theorems 4, 5 or can be examined by a computer.

Remark 3: The parity check matrices (39), (50), treated as a maximal 3-independent set, can be used to design small complete caps in plane $PG(2,2^r)$ by the methods of Szönyi [16, p. 169–170].

V. Codes with Covering Radius $R>2$

Since linear codes with $R=2$ are normal [5, Theorem 22], the codes in (20), (31) can be used in ADS construction [7], which forms an $[n_1+n_2-1,k_1+k_2-1]R_1+R_2$ code from an $[n_1,k_1]R_1$ and an $[n_2,k_2]R_2$ code. Using ADS construction codes in (20) and (31) with the parameters in (5) as $[n_1,k_1]2$ codes, we obtain families of codes with parameters

$$R=3, \qquad n=f(r_1)+2^{r_2}-2, \qquad r=r_1+r_2, \qquad r_1\geq 7, \tag{52}$$

$$R=4, \qquad n=f(r_1)+f(r_2)-1, \qquad r=r_1+r_2, \qquad r_1,r_2\geq 7, \tag{53}$$

$$R=5, \qquad n=f(r_1)+22, \qquad r=r_1+11, \qquad r_1\geq 7, \tag{54}$$

$$R=6, \qquad n=f(r_1)+2^{r_2}+20, \qquad r=r_1+r_2+11, \qquad r_1\geq 7. \tag{55}$$

Here the $[n_2, k_2]R_2$ code is the $[n = 2^{r_2} - 1, n - r_2]1$ Hamming code (52) or an $[n = f(r_2), n - r_2]2$ code (53) or the [23, 12]3 Golay code (54). In (55) the ADS construction is used twice. Equation (8) follows from (52)–(55).

VI. Density of a Covering

An $[n, n-r, d]R$ code provides a density of a covering

$$\mu_d[n, R] = 2^{n-r} V_R(n)/2^n = \sum_{i=0}^{R} \binom{n}{i} \Big/ 2^r, \qquad (56)$$

where $V_R(n)$ is the number of points in a sphere of radius R in a n-dimensional binary space.

For the codes of (5), (6), it holds respectively that

$$\mu_3[n, 2] = \frac{49}{32} - \frac{21}{2^{m+3}} + \frac{1}{2^{2m-1}} \quad \text{for } n = 7 \times 2^{m-2} - 2, \qquad (57)$$

$$\mu_4[n, 2] = \frac{225}{128} - \frac{75}{2^{m+4}} + \frac{1}{2^{2m-2}} \quad \text{for } n = 15 \times 2^{m-3} - 3. \qquad (58)$$

Equation (9) follows from (57), (58).

VII. Conclusion

New constructions of infinite families of linear binary codes with covering radius $R = 2$ and minimum distance $d = 3$, $d = 4$ are proposed. Using new codes with $d = 3$ in the ADS construction we obtained infinite families of covering codes with $R \geq 3$. Parameters of many constructed codes with $R \geq 2$ are better than parameters of previously known codes. The parity check matrices of constructed codes with $d = 4$, $R = 2$ are equivalent to complete caps in projective geometry.

Acknowledgment

The authors thank the anonymous referees for suggestions improving their exposition.

References

[1] R. A. Brualdi, V. S. Pless, and R. M. Wilson, "Short codes with a given covering radius," *IEEE Trans. Inform. Theory*, vol. 35, no. 1, pp. 99–109, Jan. 1989.

[2] A. R. Calderbank and N. J. A. Sloane, "Inequalities for covering codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1276–1280, Sept. 1988.

[3] R. C. Di Cocco, "On thick $(Q+2)$-sets," *Annals Discrete Math.*, vol. 30, pp. 115–124, 1986.

[4] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Shatz, "Covering radius—Survey and recent results," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 3, pp. 328–343, May 1985.

[5] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-32, no. 5, pp. 680–694, Sept. 1986.

[6] A. A. Davydov and L. M. Tombak, "Quasi-perfect linear binary codes with distance 4 and complete caps in projective geometry," *Probl. Peredach. Inform.*, vol. 25, no. 4, pp. 11–23, Oct.–Dec. 1989 (in Russian).

[7] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 3, pp. 385–401, May 1985.

[8] R. Hill, "Caps and codes," *Discrete Math.*, vol. 22, pp. 111–137, 1978.

[9] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford: Clarendon Press, 1979.

[10] I. S. Honkala, "Modified bounds for covering codes," Univ. of Turku, preprint.

[11] K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for codes I. Bounds on normalized covering radius," *SIAM J. Alg. Disc. Meth.*, vol. 8, no. 4, pp. 604–618, Oct. 1987.

[12] ____, "On the covering radius problem for codes II. Of low dimension; normal and abnormal codes," *SIAM J. Alg. Disc. Meth.*, vol. 8, no. 4, pp. 619–627, Oct. 1987.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[14] C. M. Melas, "A cyclic code for double error correction," *IBM J. Res. Dev.*, vol. 4, pp. 364–366, 1960.

[15] B. Segre, "Introduction to Galois geometries," *Atti. Accad. Naz. Lincei, Memorie*, vol. 8, pp. 133–236, 1967.

[16] T. Szönyi, "Small complete arcs in Galois planes," *Geometriae Dedicata*, vol. 18, pp. 161–172, 1985.

[17] G. J. M. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 237–245, Mar. 1988.

Correction to "On the Diameter of a Class of Random Graphs"

Thomas K. Philips, Don F. Towsley, *Member, IEEE*, and Jack K. Wolf, *Fellow, IEEE*

In the above paper[1] Don Coppersmith[2] has pointed out a typographical error. Equation (1) should have read

$$\binom{N}{k} \leq \min\left(\frac{N^k}{k!}, 2^N\right). \qquad (1)$$

None of the results are affected by this change.

Manuscript received August 9, 1990.

T. K. Philips is with the IBM T. J. Watson Research Center, H2-A13, P.O. Box 704, Yorktown Heights, NY 10598.

D. F. Towsley is with the Department of Computer and Information Science, University of Massachusetts, Amherst, MA 01003.

J. K. Wolf is with the Center for Magnetic Recording Research, S-008, University of California—San Diego, La Jolla, CA 92093.

IEEE Log Number 9039344.

[1] T. K. Philips, D. F. Towsley, and J. K. Wolf, "On the diameter of a class of random graphs," *IEEE Trans. Inform. Theory*, vol. 36, no. 2, pp. 285–288, Mar. 1990.

[2] Private Communication.

Correction to "General Entropy Criteria for Inverse Problems, with Applications to Data Compression, Pattern Classification and Cluster Analysis"

Lee K. Jones, *Member, IEEE*, and Charles L. Byrne, *Member, IEEE*

In the above paper[1], on page 27. Fig. 3 is incorrect. It should be replaced with the revised Fig. 3.

Manuscript received August 10, 1990.

The authors are with the Department of Mathematics, University of Lowell, Lowell, MA 01854.

IEEE Log Number 9039345.

[1] L. K. Jones and C. L. Byrne, *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 23–30, Jan. 1990.

0018-9448/91/0100-0224$01.00 © 1991 IEEE