ACKNOWLEDGMENT

The authors wish to thank Prof. T. S. Han for pointing out the game-theoretic aspect of the competitively optimal coding, and Prof. T. M. Cover and Prof. K. Itoh for their helpful comments.

REFERENCES

[1] T. M. Cover, "On the competitive optimality of Huffman code," *IEEE Trans. Inform. Theory*, vol. 37, no. 1, pp. 172–174, Jan. 1991.
[2] M. Feder, "A note on the competitive optimality of the Huffman code," *IEEE Trans. Inform. Theory*, vol. 38, no. 2, pp. 436–439, Mar. 1992.
[3] R. G. Gallager, "Variations on a theme by Huffman," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 6, pp. 668–674, Sept. 1978.
[4] G. Owen, *Game Theory*, 2nd ed. New York: Academic Press, 1982.

Constructions and Properties of Block Codes for Partial-Response Channels

Ludo M. G. M. Tolhuizen, *Member, IEEE*, Kees A. Schouhamer Immink, *Fellow, IEEE*, and Henk D. L. Hollmann, *Member, IEEE*

***Abstract*—We report on block-coding techniques for partial-response channels with transfer function $(1 \mp D^m)$, $m = 1, 2, \cdots$. We consider various constructions of block codes with prescribed minimum Euclidean distance. Upper and lower bounds to the size of a code with minimum squared Euclidean distance greater than unity are furnished. A table is presented of cardinalities of codes of small length with prescribed minimum squared Euclidean distance.**

***Index Terms*— Spectral null code, recording code, partial-response channel.**

I. INTRODUCTION

Partial-response (PR) channels can be fruitfully used to model certain magnetic and optical recording channels. A great variety of partial-response channels have been described. In this correspondence, we will specifically consider the simplest PR channel that can be described by the transfer function $(1 \mp D^m)$, $m = 1, 2, \cdots$, where D is the unit-delay operator.

Coding techniques for improving the reliability of digital transmission over noisy partial-response channels have received increasing attention in the literature [1]–[4]. Wolf and Ungerboeck [1] showed that conventional Hamming distance codes can be transformed, using a simple precoding operation, into codes that exhibit Euclidean distance. Karabed and Siegel [2] showed that Euclidean distance properties can be improved by matching the spectral nulls of both the power density function of the coded sequence and the partial response channel. Hole and Ytrehus [3] optimized the generator polynomials of convolutional codes with respect to Euclidean distance properties. Immink [4] considered the concatenation of Hamming distance improving codes and dc-balanced codes.

Given the complexity of the Euclidean distance measure, it is not a trivial task to find code sets with prescribed minimum distance. Useful tables that list the (upper or lower bound to the) maximum cardinality of code sets with prescribed minimum Hamming distance have been published [5]. Similar tables for codes with prescribed minimum Euclidean distance are not available.

After a section with preliminaries and definitions, we will proceed as follows. The precoding technique for trellis codes from [1] is applied to block codes. The distance properties of [2] will be shown to hold for codeword sets with fixed, not necessarily zero, moments as well. This offers the possibility to obtain code sets larger than in [2]. A new construction, generalizing the concatenation scheme from [4], will be given. It will be shown that, provided that $n \leq 10$ or $n = 12$, the set of words of minimum disparity is maximal, i.e., addition of a single word to the given set will reduce the minimum Euclidean distance. For $n = 11$ and $n \geq 13$, it will be shown that certain codewords having a constraint on the maximum runlength can be used to enlarge the set of words of minimum disparity without reduction of the minimum Euclidean distance. Upper and lower bounds to the size of codes with minimum squared Euclidean distance greater than unity will be furnished. We end by listing, for small code lengths, the maximum cardinality of sets achieving a given minimum Euclidean distance.

II. PRELIMINARY

Let $\boldsymbol{u} = (u_1, \cdots, u_n)$ and $\boldsymbol{v} = (v_1, \cdots, v_n)$ be two n-tuples over $\Phi = \{-1, 1\}$. Define the *difference* vector $\boldsymbol{e} = (e_1, \cdots, e_{n+m})$ for the PR channel with transfer function $(1 + aD^m)$, $m = 1, 2, \cdots$, and $a = \mp 1$, as

$$e_i = u_i + au_{i-m} - v_i - av_{i-m}. \tag{1}$$

By convention, the undeclared variables are set to unity. The squared Euclidean distance $d^2_{a,m}(\boldsymbol{u}, \boldsymbol{v})$ between $\boldsymbol{u}$ and $\boldsymbol{v}$ pertaining to the PR channel with transfer function $(1 + aD^m)$, $m = 1, 2, \cdots$, $a = \mp 1$, is defined by

$$d^2_{a,m}(\boldsymbol{u}, \boldsymbol{v}) = \frac{1}{8} \sum_{i=1}^{n+m} e_i^2. \tag{2}$$

The normalization constant $1/8$ has been chosen to ensure that the minimum distance between distinct n-tuples equals unity.

Obviously, the components of $\boldsymbol{e}$ are in $\{-4, -2, 0, 2, 4\}$. Their sum is a multiple of four, as

$$\sum_{i=1}^{n+m} e_i = \sum_{i=1}^{n+m} (u_i - v_i) + a \cdot \sum_{i=1}^{n+m} (u_{i-m} - v_{i-m}) = (1 + a) \sum_{i=1}^{n} (u_i - v_i).$$

Consequently, $e_i = \pm 2$ for an even number of indices i and hence $d^2_{a,m}$ as defined in (2) is an integer.

It is well known [2] that sets of words with certain distance properties for the $(1 + aD)$ channel can be transformed into corresponding sets for the $(1 + aD^m)$ channel, $m = 2, 3, \cdots$ by an m-fold interleaving operation. Sets matched to the $(1 - D)$ channel can be transformed to sets matched to the $(1 + D)$ channel by negating the odd- (or even)-numbered symbols of all their words. To that end, let $\hat{\boldsymbol{u}}$ and $\hat{\boldsymbol{v}}$ be two n-tuples found by negating the odd-numbered elements

Manuscript received July 22, 1994; revised March 24, 1995. The material in this correspondence was presented in part at the 4th Benelux-Japan Workshop on Coding and Information Theory, Eindhoven, The Netherlands, June 22–24, 1994.

The authors are with Philips Research Laboratories, 5656 AA Eindhoven, The Netherlands.

IEEE Log Number 9414734.

of the n-tuples $\boldsymbol{u}$ and $\boldsymbol{v}$, i.e., $\hat{u}_i = (-1)^i u_i$ and $\hat{v}_i = (-1)^i v_i$. After a simple substitution, we have

$$d^2_{-1,1}(\hat{\boldsymbol{u}}, \hat{\boldsymbol{v}}) = d^2_{1,1}(\boldsymbol{u}, \boldsymbol{v}).$$

Consequently, we can, without loss of generality, concentrate on the $(1-D)$ channel—and we will do so. In order to reduce clerical work, we will write $d^2(\boldsymbol{u}, \boldsymbol{v})$ in lieu of $d^2_{-1,1}(\boldsymbol{u}, \boldsymbol{v})$.

The minimum squared Euclidean distance of $\mathcal{S} \subset \Phi^n$, denoted by $d^2_{\min}(\mathcal{S})$, is defined as the minimum $d^2(\boldsymbol{u}, \boldsymbol{v})$ between any pair of distinct $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{S}$.

It is immediate that $d^2(\boldsymbol{u}, \boldsymbol{v}) = 1$ if $\boldsymbol{u}$ and $\boldsymbol{v}$ have Hamming distance equal to 1. As a consequence, any set whose minimum squared Euclidean distance exceeds 1 has certain error-correcting or -detecting capabilities for the full response channel as well.

III. Coding Techniques

Three methods for constructing block codes for the PR channel are described. The first method uses a precoding technique for transforming Hamming-distance-based codes into codes matched to the PR channel. The second method is based on higher order spectral null codes, and the third one employs a concatenation of a code matched to the PR channel and a Hamming distance increasing code.

A. Precoding

In [1], a technique called *precoding* was used to transform Hamming-distance-based convolutional codes into trellis codes matched to the $1-D$ channel. The same technique can be fruitfully applied in conjunction with block codes. Indeed, let

$$\boldsymbol{c} = (c_1, c_2, \cdots, c_n) \in \{0, 1\}^n.$$

First, $\boldsymbol{c}$ is precoded to the word $\tilde{c}$ that has ith bit $c_1 \oplus c_2 \oplus \cdots \oplus c_i$, where $\oplus$ denotes modulo 2 addition. Subsequently, $\tilde{c}$ is transformed into $\boldsymbol{c}^*$ by substituting -1 for 0. As in [1], one can show that for two vectors $\boldsymbol{c}$ and $\boldsymbol{d}$ of length n with Hamming distance d_H, we have

$$d^2(\boldsymbol{c}^*, \boldsymbol{d}^*) = \left\lceil \frac{d_H}{2} \right\rceil + 2 \cdot |\{i \in \{1, 2, \cdots, n\} \mid c_i = d_i = 1 \text{ and } c_1 \oplus \cdots \oplus c_i \neq d_1 \oplus \cdots \oplus d_i\}|.$$

As a consequence, precoding a binary code C of minimum Hamming distance d yields a code with $d^2_{\min} \geq \lceil \frac{d}{2} \rceil$. If C is linear, equality holds.

If m and t are integers such that $2^m - mt \geq 2$, a primitive $[2^m - 1, k, d]$ BCH code exists with $k \geq 2^m - mt - 1$ and $d \geq 2t + 1$ [5]. Consequently, by choosing m sufficiently large, we find that for each fixed t, codes exist with $d^2_{\min} \geq t$ and rates arbitrarily close to unity.

B. Spectral Null Codes

Karabed and Siegel [2] showed that Euclidean distance can be generated by matching the spectral nulls of both the power density function of the coded sequence and the partial response channel. For the $(1-D)$ PR system at hand this means that coded sequences with a spectral null at zero frequency may serve our purpose. In this section, it will be shown that the idea above can be generalized. Let $\boldsymbol{u} = (u_1, \cdots, u_n) \in \Phi^n$. The kth-order *moment*, denoted by $M^{(k)}$, of $\boldsymbol{u}$ is defined by

$$M^{(k)} = \sum_{i=1}^{n} i^k u_i. \tag{3}$$

A word $\boldsymbol{u} = (u_1, \cdots, u_n) \in \Phi^n$ is said to have a Kth-order null at zero frequency [6] if the first $K+1$ moments are zero, i.e.

$$M^{(k)} = 0, \quad \text{for } k = 0, 1, \cdots, K. \tag{4}$$

TABLE I
Improved Codes with Constant Moments

n	a_0	a_1	a_2	size	size for zero moments
12	0	6	78	5	2
16	0	8	136	22	14
20	0	4	84	98	48
24	0	0	-12	617	592
28	0	2	58	4481	2886

The set of all Kth-order spectral null words is denoted by $\mathcal{S}^n_K$. It is obvious that $\mathcal{S}^n_0 \neq \emptyset$ if and only if n is even, and it is well known [6] that $\mathcal{S}^n_1 \neq \emptyset$ only if n is divisible by four. The relationship between the (non)emptiness of $\mathcal{S}^n_K$ and n has been explored by Roth *et al.* [7]. Karabed and Siegel [2] have shown, using results from number theory, that the minimum Euclidean distance of $\mathcal{S}^n_K$ is bounded from below by

$$d^2_{\min}(\mathcal{S}^n_K) \geq K + 2. \tag{5}$$

As the number of codewords rapidly decreases with increasing order K, the practical usefulness of higher order spectral null codes rapidly declines with increasing K.

The proof of (5) in [2] is based on the fact that for $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{S}^n_K$, the difference vector $\boldsymbol{e}$ as defined by (1) has $K+2$ zero moments, i.e.

$$\sum_{i=1}^{n+1} i^j e_i = 0, \quad \text{for } j = 0, 1, \cdots, K+1. \tag{6}$$

With an elementary substitution it can be verified that (6) also holds for code sets consisting of words with nonzero, but fixed, moments, i.e., words that satisfy

$$M^{(k)} = a_k, \quad \text{for } k = 0, 1, \cdots, K. \tag{7}$$

Consequently, the distance property (5) also applies to sets of words of fixed, not necessarily zero, moments. This result is of particular interest for values of K and n for which the set of zero-moment words is empty.

For $n = 8, 12, 16, 20$, and 24 we investigated by computer if the choice $a_k = 0$ for $k = 0, 1, \cdots, K$ in (7) maximizes the size of the codes. For $K = 1$, this is indeed the case. For $K = 2$, however, improvements were found, as depicted in Table I. For comparision, we tabulated in the rightmost column the size of the code for all moments equal to zero, a result taken from [8].

For $n = 12$, 16, and 20, we optimized over all triples (a_0, a_1, a_2); for $n = 24$ and 28, we fixed $a_0 = 0$ and optimized over all pairs (a_1, a_2).

C. Concatenation

In [4], good codes for the $1-D$ channel were constructed by a concatenation of binary random-error-correcting codes and the bi-phase code. This was accomplished by simply replacing the symbols 0 and 1 in the error-correcting code by the bi-phase words $1, -1$ and $-1, 1$, respectively. In this section, we elaborate on the idea of concatenating an error-correcting code and a code matched to the $1-D$ channel. Again, symbols from the error-correcting code are replaced by codewords from the code matched to the PR channel. After giving a more formal description, we will derive a lower bound on the minimum-squared Euclidean distance of the concatenated code.

Construction: Let $\mathcal{P} \subset \Phi^n$. Let C be a code of length m over a $|\mathcal{P}|$-ary alphabet A, and let ψ be a one-to-one mapping from A to $\mathcal{P}$. The code $\psi(C)$ is defined as

$$\psi(C) = \{(\psi(c_1), \psi(c_2), \cdots, \psi(c_m)) \mid (c_1, c_2, \cdots, c_m) \in C\}.$$

Clearly, $\psi(C)$ is a code of length mn over Φ with $|C|$ words. In order to give a lower bound on $d^2_{\min}(\psi(C))$, we require some simple results. We use the following notation: if $\boldsymbol{x} \in \Phi^n$, say $\boldsymbol{x} = x_1 \cdots x_n$, and $\boldsymbol{y} \in \Phi^m$, say $\boldsymbol{y} = y_1 \cdots y_m$, then $\boldsymbol{xy} \in \Phi^{n+m}$ is the vector $x_1 \cdots x_n y_1 \cdots y_m$.

Lemma 1: Let $\boldsymbol{a}, \boldsymbol{b} \in \Phi^n$, and let $\boldsymbol{u}, \boldsymbol{v} \in \Phi^m$. Let $\boldsymbol{x}$ and $\boldsymbol{y}$ denote the vectors $\boldsymbol{au}$ and $\boldsymbol{bv}$, respectively. We have

$$d^2(\boldsymbol{x},\boldsymbol{y}) = d^2(\boldsymbol{a},\boldsymbol{b}) + d^2(\boldsymbol{u},\boldsymbol{v}) - \frac{1}{4}(u_1 - v_1)(a_n - b_n).$$

Proof: By definition, we have

$$8d^2(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n+m+1} (x_i - y_i - x_{i-1} + y_{i-1})^2.$$

Splitting this summation, we obtain

$$\begin{aligned} 8d^2(\boldsymbol{x},\boldsymbol{y}) &= \sum_{i=1}^{n}(a_i - b_i - a_{i-1} + b_{i-1})^2 + (u_1 - v_1 - a_n + b_n)^2 \\ &\quad + \sum_{i=2}^{m+1}(u_i - v_i - u_{i-1} + v_{i-1})^2 \\ &= 8d^2(\boldsymbol{a},\boldsymbol{b}) - (a_n - b_n)^2 + (u_1 - v_1 - a_n + b_n)^2 \\ &\quad + 8d^2(\boldsymbol{u},\boldsymbol{v}) - (u_1 - v_1)^2. \end{aligned}$$

□

Corollary 1: Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be vectors of equal length over Φ, and let $\boldsymbol{x}$ and $\boldsymbol{y}$ be vectors of equal length over Φ. If $\boldsymbol{u}$ is a vector of length ≥ 1 over Φ, then

$$d^2(\boldsymbol{aux}, \boldsymbol{buy}) = d^2(\boldsymbol{a},\boldsymbol{b}) + d^2(\boldsymbol{x},\boldsymbol{y}).$$

Proof: As $\boldsymbol{au}$ and $\boldsymbol{bu}$ end in the same symbol, Lemma 1 implies that

$$d^2(\boldsymbol{aux}, \boldsymbol{buy}) = d^2(\boldsymbol{au}, \boldsymbol{bu}) + d^2(\boldsymbol{x},\boldsymbol{y}).$$

Lemma 1 also implies that

$$d^2(\boldsymbol{au}, \boldsymbol{bu}) = d^2(\boldsymbol{a},\boldsymbol{b}).$$

□

Remarks: Classical constructions for obtaining shorter codes from a given code include *shortening* and *puncturing* [5]. When shortening, one takes all words of a code that agree in a certain position and subsequently discards this position. Clearly, shortening does not decrease the minimum Hamming distance of a code. Lemma 1 implies that shortening a code in its first or final position does not decrease $d^2_{\min}$. Combining it with Corollary 1, we see that shortening in a position different from the first or final one decreases $d^2_{\min}$ by at most one. For example, if we shorten the code $\{111, -11-1\}$ in the second position, $d^2_{\min}$ drops from 2 to 1. When puncturing, one simply discards a certain position from all words of a code. Clearly, puncturing decreases the minimum Hamming distance of a code by at most one. Lemma 1 implies that puncturing a code in its first or final position may result in a decrease of $d^2_{\min}$ by two. Repeated application of Lemma 1 shows that puncturing a code in a postion different from the first or final one decreases $d^2_{\min}$ by at most four. For example, consider the code $C = \{1-11, -11-1\}$. If we puncture C in its first or final position, $d^2_{\min}$ drops from 5 to 3; if we puncture C in its second postion, $d^2_{\min}$ drops to 1.

By repeating codewords, the minimum Hamming distance of a code can be doubled; the rate of the code, of course, halves. A similar result can be obtained for $d^2_{\min}$. Let C be a code of length n. Clearly, the code

$$D = \{(c_1, \cdots, c_n, -c_n, \cdots, -c_1) \mid (c_1, \cdots, c_n) \in C\}$$

has length $2n$ and $|C|$ words. It readily follows from Lemma 1 that

$$d^2_{\min}(D) \in \{2d^2_{\min}(C), 2d^2_{\min}(C) + 1\}.$$

So while the rate of the code halves, $d^2_{\min}$ at least doubles.

Corollary 2: For $i = 1, 2, \cdots, m$, let $\boldsymbol{x}_i$ and $\boldsymbol{y}_i$ be vectors over Φ of equal length. If $\boldsymbol{x} = \boldsymbol{x}_1\boldsymbol{x}_2 \cdots \boldsymbol{x}_m$ and $\boldsymbol{y} = \boldsymbol{y}_1\boldsymbol{y}_2 \cdots \boldsymbol{y}_m$, then

$$\sum_{i=1}^{m} d^2(\boldsymbol{x}_i, \boldsymbol{y}_i) - (m-1) \leq d^2(\boldsymbol{x},\boldsymbol{y}) \leq \sum_{i=1}^{m} d^2(\boldsymbol{x}_i, \boldsymbol{y}_i) + (m-1).$$

Proof: Lemma 1 implies that

$$d^2(\boldsymbol{x},\boldsymbol{y}) \geq d^2(\boldsymbol{x}_1 \cdots \boldsymbol{x}_{m-1}, \boldsymbol{y}_1 \cdots \boldsymbol{y}_{m-1}) + d^2(\boldsymbol{x}_m, \boldsymbol{y}_m) - 1.$$

Iterating, we find that

$$d^2(\boldsymbol{x},\boldsymbol{y}) \geq \sum_{i=1}^{m} d^2(\boldsymbol{x}_i, \boldsymbol{y}_i) - (m-1).$$

The other inequality follows in the same way. □

Theorem 1: Let $\boldsymbol{x} = \boldsymbol{x}_1\boldsymbol{x}_2 \cdots \boldsymbol{x}_s$ and let $\boldsymbol{y} = \boldsymbol{y}_1\boldsymbol{y}_2 \cdots \boldsymbol{y}_s$ where $\boldsymbol{x}_i$ and $\boldsymbol{y}_i$ are vectors over Φ of equal length, and suppose that $\boldsymbol{x} \neq \boldsymbol{y}$. Let $I := \{i \mid \boldsymbol{x}_i \neq \boldsymbol{y}_i\}$. If k denotes the minimum number of disjoint intervals (=sets of consecutive integers) in which I can be partitioned, then

$$k + \sum_{i \in I} \left[d^2(\boldsymbol{x}_i, \boldsymbol{y}_i) - 1\right] \leq d^2(\boldsymbol{x},\boldsymbol{y}) \leq -k + \sum_{i \in I} \left[d^2(\boldsymbol{x}_i, \boldsymbol{y}_i) + 1\right].$$

Proof: Let I be partitioned into the intervals $I_1, I_2, \cdots, I_k$, where $I_i \cup I_j$ is not an interval if $i \neq j$. By $\boldsymbol{x}^{(j)}$ we denote the vector consisting of the components $\boldsymbol{x}_i$ with $i \in I_j$. Corollary 1 implies that

$$d^2(\boldsymbol{x},\boldsymbol{y}) = \sum_{j=1}^{k} d^2(\boldsymbol{x}^{(j)}, \boldsymbol{y}^{(j)}).$$

Application of Corollary 2 to $d^2(\boldsymbol{x}^{(j)}, \boldsymbol{y}^{(j)})$ for $j = 1, 2, \cdots, k$ proves the theorem. □

With the previous results, we are in a position to give a bound on $d^2_{\min}(\psi(C))$.

Theorem 2: The minimum squared Euclidean distance of $\psi(C)$ is at least $1 + d(C)(d^2_{\min}(\mathcal{P}) - 1)$, where $d(C)$ is the minimum Hamming distance of C.

Proof: Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two different words from $\psi(C)$. We partition $\boldsymbol{x}$ and $\boldsymbol{y}$ into m vectors of length n, say $\boldsymbol{x} = \boldsymbol{x}_1\boldsymbol{x}_2 \cdots \boldsymbol{x}_m$ and $\boldsymbol{y} = \boldsymbol{y}_1\boldsymbol{y}_2 \cdots \boldsymbol{y}_m$. Clearly, in Theorem 1, k is at least one, whence

$$d^2(\boldsymbol{x},\boldsymbol{y}) \geq 1 + \sum_{i \in I} \left[d^2(\boldsymbol{x}_i, \boldsymbol{y}_i) - 1\right]$$

where $I = \{i \mid x_i \neq y_i\}$. If $\boldsymbol{x}_i$ and $\boldsymbol{y}_i$ are different, then their contribution to the above sum is at least $d^2_{\min}(\mathcal{P})$. As $\boldsymbol{x}$ and $\boldsymbol{y}$ are two different words in $\psi(C)$, I has at least $d(C)$ elements. □

Example 1 [4]: Take $n = 2$, and take $\mathcal{P}$ to be the bi-phase code, that is, $\mathcal{P} = \{(1, -1), (-1, 1)\}$. Clearly, $d^2_{\min}(\mathcal{P}) = 3$. If we use a binary code C of length m and minimum distance d, we obtain a code for the $1 - D$ channel of length $2m$ with $|C|$ words and $d^2_{\min} \geq 1 + 2d$. A specific choice for C is the set of *all* binary words of length m. In this way, we obtain a code of length $2m$ with 2^m words and $d^2_{\min} \geq 3$. If we choose C to be the set of the even-weight binary words of length m, we obtain a code of length $2m$ with 2^{m-1} words and $d^2_{\min} \geq 5$.

Example 2: Let n be even, and take $\mathcal{P} = S_0^n$. We know that $d^2_{\min}(\mathcal{P}) = 2$. Let C be the code over $\mathbb{Z}_{|\mathcal{P}|}$ consisting of the m-tuples whose components add to a multiple of $|\mathcal{P}|$. We obtain a code of length nm with $d^2_{\min} \geq 1 + 2(2-1) = 3$. The number of codewords equals

$$|\mathcal{P}|^{m-1} = \binom{n}{n/2}^{m-1}.$$

As a consequence, a code rate arbitrarily close to unity can be obtained by choosing m and n sufficiently large.

We wish to add vectors to codes obtained by concatenation. The following proposition gives a lower bound on the Euclidean distance of a certain vector to any concatenation of bi-phase words.

Proposition 1: Let $\boldsymbol{x} \in \Phi^{2n}$ be such that $x_{2i} = -x_{2i-1}$, $i = 1, 2, \cdots, n$. Let $\boldsymbol{y}$ be the vector with $y_{2i} = y_{2i-1} = (-1)^{i-1}$. Then $d^2(\boldsymbol{x}, \boldsymbol{y}) \geq n$.

Proof: Let $e_i := x_i - y_i$. By definition, we have

$$8d^2(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{2n+1} (e_i - e_{i-1})^2 = 2 \cdot \sum_{i=1}^{2n} e_i^2 - 2 \cdot \sum_{i=2}^{n} e_i e_{i-1}. \quad (8)$$

From the properties of $\boldsymbol{x}$ and $\boldsymbol{y}$, it follows that

$$(e_{2i-1}, e_{2i}) \in \{(0, 2 \cdot (-1)^i), (2 \cdot (-1)^i, 0)\}.$$

As a consequence,

$$\sum_{i=1}^{2n} e_i^2 = 4n.$$

Moreover, if i is even, then $e_i e_{i-1} = 0$; if i is odd, then $e_i e_{i-1} \in \{0, -4\}$. Consequently, $e_i e_{i-1} \leq 0$. Plugging in these results into (8), we obtain the proposition. □

Corollary 3: If a binary code of length n with minimum Hamming distance d and with M words exists, then a code for the 1-D channel of length $2n$ exists with $M + 2$ words and $d^2_{\min} \geq \min\{2d + 1, n\}$.

Proof: Concatenate the binary code with the bi-phase code and add the words $11 - 1 - 111 \cdots$ and $-1 - 111 - 1 - 1 \cdots$. □

Example 3: Adding the words $11 - 1 - 111 \cdots$ and $-1 - 111 - 1 - 1 \cdots$ to the concatenation of the bi-phase code and the binary $[n, n, 1]$ code, we obtain a code of length $2n$ with $2^n + 2$ and $d^2_{\min} \geq \min\{n, 3\}$. So if $n = 3$, we obtain a code $\mathcal{P}$ of length six with ten words and $d^2_{\min} = 3$. A computer search revealed that $\mathcal{P}$ is unique in that no other set of ten words of length six has $d^2_{\min} \geq 3$. Concatenating $\mathcal{P}$ with the code consisting of all m-tuples over $\mathbb{Z}_{10}$, we obtain a code of length $6m$ with 10^m words with $d^2_{\min} \geq 1 + 1 \cdot (3 - 1) = 3$. Using the construction of Example 1, a code of length $6m$ with $d^2_{min} = 3$ would have been obtained with only 2^{3m} words. Similarly, concatenating $\mathcal{P}$ with the code over $\mathbb{Z}_{10}$ consisting of all words of length m whose components add to a multiple of ten, a code is obtained of length $6m$ with 10^{m-1} words and $d^2_{\min} \geq 1 + 2 \cdot (3 - 1) = 5$. For $m \geq 8$, this code has more words than the corresponding code obtained in Example 1.

IV. Codes with $d^2_{\min} \geq 2$

By application of the construction methods given in the previous sections, codes can be designed with prescribed length and minimum distance. It is not at all clear how "good" these constructions are. It would therefore be of interest to have an upper bound on the cardinality of codes with prescribed parameters. The main difficulty in deriving such an upper bound is the fact that the number of words at certain Euclidean distance from a given word $\boldsymbol{x}$ depends on $\boldsymbol{x}$, unlike in the Hamming distance case.

In this section, we study what might seem the simplest case, namely, codes with $d^2_{\min} \geq 2$. We will study the maximum cardinality $F(n)$ of a code of length n with minimum Euclidean distance at least two. We start with the construction of such codes. Next, we give an upper bound S_n on $F(n)$. The bounds so obtained are tabulated for $n \leq 24$. They are close for small n, but seem to diverge for larger n. The divergence is supported by the asymptotic behavior of the bounds. The asymptotic behavior of S_n is given without proof, as the derivation is lengthy and the applied methods are beyond the scope of this correspondence. Finally, we make a connection between codes with $d^2_{\min} \geq 2$ and codes detecting unidirectional errors.

A. Construction of Codes with $d^2_{\min} \geq 2$

From the results in the section on spectral null codes, it readily follows that sets with constant zeroth-order moment have $d^2_{\min} \geq 2$. That is, sets of words of fixed Hamming weight (= number of ones), have $d^2_{\min} \geq 2$. Hence we have the following bound on $F(n)$, where Stirling's approximation of $n!$ is used to obtain the asymptotical behavior.

Proposition 2:

$$F(n) \geq \binom{n}{\lfloor \frac{n}{2} \rfloor} \sim 2^n \Big/ \sqrt{\frac{\pi}{2} n}, \quad n \to \infty.$$

We will investigate if words can be added to the set of words of weight $\lfloor \frac{n}{2} \rfloor$ without reducing the minimum distance. We start with a characterization of the property that two words have Euclidean distance equal to 1. We denote the weight of the vector $\boldsymbol{x}$ by $\mathrm{wt}(\boldsymbol{x})$.

Theorem 3: Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two vectors of equal length. If $\mathrm{wt}(\boldsymbol{x}) \geq \mathrm{wt}(\boldsymbol{y})$, then $d^2(\boldsymbol{x}, \boldsymbol{y} = 1)$ if and only if $\mathrm{wt}(\boldsymbol{x}) > \mathrm{wt}(\boldsymbol{y})$ and there exist vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ (possibly of length 0) such that

$$\boldsymbol{x} = \boldsymbol{a}11 \cdots 1\boldsymbol{b} \text{ and } \boldsymbol{y} = \boldsymbol{a} - 1 - 1 \cdots - 1\boldsymbol{b}. \quad (9)$$

Proof: From Lemma 1, it is immediate that $\boldsymbol{x}$ and $\boldsymbol{y}$ have Euclidean distance 1 if they satisfy (9). Conversely, suppose $d^2(\boldsymbol{x}, \boldsymbol{y}) = 1$.Let i and j be the smallest and largest indices, respectively, of the positions in which $\boldsymbol{x}$ and $\boldsymbol{y}$ differ. If $i = j$, then (9) holds. Suppose that $i < j$. By definition, we have

$$8 = 8d^2(\boldsymbol{x}, \boldsymbol{y}) = \sum_{k=i}^{j+1} (x_k - x_{k-1} - y_k + y_{k-1})^2.$$

As $x_{i-1} = y_{i-1}$, $x_i = -y_i$, $x_j = -y_j$, and $x_{j+1} = y_{j+1}$, the first and the last term of the sum above both equal 4. Hence, $x_k - x_{k-1} = y_k - y_{k-1}$ for $i + 1 \leq k \leq j$ and so, if $i + 1 \leq m \leq j$, then

$$x_m - x_i = \sum_{k=i+1}^{m} (x_k - x_{k-1}) = \sum_{k=i+1}^{m} (y_k - y_{k-1}) = y_m - y_i.$$

Hence, $x_m - y_m = x_i - y_i = 2x_i$ for $i + 1 \leq m \leq j$. As x_m and y_m are in $\{-1, 1\}$, we infer that for $i + 1 \leq m \leq j$, $x_m = x_i$ and $y_m = -x_i = y_i$. □

Note that Theorem 3 implies that words of equal weight cannot have Euclidean distance equal to 1, confirming Proposition 2.

The following lemma answers the question whether words can be added to the set of words of weight $\lfloor \frac{n}{2} \rfloor$ without reducing its minimum Euclidean distance. In order to improve readability, we will use in the remainder of this section the alphabet $\Omega = \{0, 1\}$ instead of the alphabet $\Phi = \{-1, 1\}$.

Lemma 2: A word of weight w has Euclidean distance at least two to *all* words of weight v if and only if $v \neq w$ and it does not have a run of at least

$$\begin{cases} w - v \text{ consecutive ones,} & \text{if } w > v \\ v - w \text{ consecutive zeros,} & \text{if } v > w. \end{cases}$$

Proof: Let $\boldsymbol{x}$ be a word of weight w. We only consider the case $w > v$, the other case being similar. Theorem 3 implies that $d^2(\boldsymbol{x},\boldsymbol{y}) \geq 2$ for all vectors $\boldsymbol{y}$ of weight v if $\boldsymbol{x}$ does not have a run of at least $p = w - v$ ones. Conversely, suppose $\boldsymbol{x}$ does contain a run of at least p consecutive ones, say $x_i = 1$ for $i = a, a+1, \cdots, a+p-1$. The word $\boldsymbol{y}$ having zeroes in the same positions $a, a+1, \cdots, a+p-1$ and agreeing with $\boldsymbol{x}$ in the other positions, has weight v and, according to Theorem 3, distance one to $\boldsymbol{x}$. □

In the following example, we use Lemma 2 to construct, for certain values of n, sets of words of length n that can be added to the set of all words of weight $\lfloor \frac{n}{2} \rfloor$ without reducing $d^2_{\min}$.

Example 4: We use notation $(a_0, a_1, \cdots, a_m)$ for the vector $1^{a_0}01^{a_1}0\cdots 1^{a_m}$. Here, as usual, 1^p denote a string of p ones. This vector has weight

$$\sum_{i=0}^{m} a_i$$

and length

$$m + \sum_{i=0}^{m} a_i.$$

Its maximum l's runlength is the maximum of the numbers $a_0, a_1, \cdots, a_m$. Take $n = 11$. The words $(3,3,3)$ and $(2,2,2,2)$ have Euclidean distance at least two to all words of weight 5. As their mutual distance is larger than one, we have

$$F(11) \geq \binom{11}{5} + 2 = 464.$$

Take $n = 13$. The following words have Euclidean distance at least two to all words of weight $v = 6$.

$w = 11 : (4,4,3), (4,3,4)$, and $(3,4,4)$.

$w = 10 : (3,3,3,1)$, $(3,3,1,3)$, $(3,1,3,3)$, and $(1,3,3,3)$; $(3,3,2,2)$, $(3,2,3,2)$, $(3,2,2,3)$, $(2,3,3,2)$, $(2,3,2,3)$, and $(2,2,3,3)$.

$w = 9 : (2,2,2,2,1), (2,2,2,1,2), (2,2,1,2,2), (2,1,2,2,2)$, and $(1,2,2,2,2)$.

It is easy to check that all 18 words listed above have Euclidean distance at least two to each other; hence they can *all* be added to the set of words of weight six without lowering the minimum Euclidean distance. We conclude that

$$F(13) \geq \binom{13}{6} + 18 = 1734.$$

Similarly, consider the case $n = 14$. The following words have Euclidean distance at least two to all words of weight $v = 7$.

$w = 10 : (2,2,2,2,2)$.

$w = 11 : (3,3,3,2), (3,3,2,3), (3,2,3,3)$, and $(2,3,3,3)$.

$w = 12 : (4,4,4)$.

Also the complements of these words have Euclidean distance at least two to all words of weight seven. Again, it is easy to check that all these twelve words have Euclidean distance at least two to each other; consequently,

$$F(14) \geq \binom{14}{7} + 12 = 3444.$$

Unfortunately, two words at distance at least two from all codewords of fixed weight can have distance one to each other. For example, the words $(2,2,2,2,2,0)$ and $(2,2,2,3)$ have Euclidean distance one, but both words have Euclidean distance at least two to all words of weight seven. However, the set of words of weight v can be extended with all words of a *fixed* weight w that have distance at least two to all words of weight v without lowering $d^2_{\min}$. By combining Lemma 2 and the following proposition, it is easy to count the number of such words.

TABLE II
NUMBER OF WORDS THAT CAN BE ADDED TO WEIGHT $\lfloor \frac{n}{2} \rfloor$ WORDS

n	w	number of words
15	11	65
16	12	35
17	12	336
18	13	216
19	13	1554
20	15	1246
21	14	6728
22	16	7140
23	16	38165
24	17	37080

Proposition 3: The number of words of length n and weight w without any run of more than p ones equals the coefficient of x^w in $(1 + x + x^2 + \cdots + x^p)^{n-w+1}$.

Proof: The set of such words equals the set of words of the form

$$1^{a_0}01^{a_1}\cdots 01^{a_{n-w}}, \qquad \text{with } 0 \leq a_i \leq p \text{ and } \sum_{i=0}^{n-w} a_i = w. \quad \square$$

By virtue of Lemma 2 and Proposition 3, we can determine the number of words of weight w that can be added to the set of words of weight $\lfloor \frac{n}{2} \rfloor$ without lowering the minimum distance of that set (the case $v > w$ in Lemma 2 can be handled by taking complements). Using a software package to expand the appropriate power series in Proposition 3, we obtained the results shown in Table II. The table lists that value of w that maximizes the number of words that can be added.

It appeared that for $n \leq 10$ and $n = 12$, no words could be added, a fact that can also be proved analytically. For $n = 11, 13$, and 14, the number of codewords that can be added is 2, 18, and 12, respectively—see Example 4.

B. An Upper Bound on $F(n)$

For deriving an upper bound on $F(n)$, we will define a mapping f from Ω^n to itself such that $d^2(\boldsymbol{x},\boldsymbol{y}) = 1$ whenever $f(\boldsymbol{x}) = f(\boldsymbol{y})$. Clearly, for each $\boldsymbol{x} \in \Omega^n$, any code with $d^2_{\min} \geq 2$ has at most one element from the set $\{\boldsymbol{y} \in \Omega^n \mid f(\boldsymbol{y}) = \boldsymbol{x}\}$. Consequently, $F(n)$ is at most the cardinality of the range of f, that is

$$F(n) \leq |\{f(\boldsymbol{x}) \mid \boldsymbol{x} \in \Omega^n\}|. \tag{10}$$

We now proceed to define f. Let $\boldsymbol{x} \in \Omega^n$. We write $1\boldsymbol{x}0$ as

$$1^{a_1}0^{b_1}\cdots 1^{a_m}0^{b_m},$$

$$\text{where } a_i \geq 1, b_i \geq 1 \text{ and } \sum_{i=1}^{m}(a_i + b_i) = n + 2.$$

We define

$$M = M(\boldsymbol{x}) = max\{(a_i + b_i) \mid 1 \leq i \leq m\}$$

and j as the smallest integer such that $a_j + b_j = M$. The vector $f(\boldsymbol{x})$ is given by the equation

$$1f(\boldsymbol{x})0 = 1^{a_1}\cdots 0^{b_{j-1}}10^{M-1}1^{a_{j+1}}\cdots 0^{b_m}.$$

The vectors $\boldsymbol{y}$ such that $f(\boldsymbol{x}) = f(\boldsymbol{y})$ are the vectors satisfying

$$1\boldsymbol{y}0 = 1^{a_1}\cdots 0^{b_{j-1}}1^a0^b1^{a_{j+1}}\cdots 0^{b_m},$$

$$\text{with } a \geq 1, b \geq 1 \text{ and } a + b = M.$$

Consequently, words with equal image have Euclidean distance equal to 1. Moreover, $M(\boldsymbol{x})-1$ vectors are mapped onto $f(\boldsymbol{x})$, from which we conclude that

$$|\{f(\boldsymbol{x}) \mid \boldsymbol{x} \in \Omega^n\}| = \sum_{\boldsymbol{x}\in\Omega^n} \frac{1}{M(\boldsymbol{x})-1} =: S_n. \quad (11)$$

We give an efficient procedure for computing S_n, the sum in (11). To this end, we define

$$s(n,r) = |\{\boldsymbol{x} \in \Omega^n \mid M(\boldsymbol{x}) \le r+1\}|. \quad (12)$$

With (12), we have

$$S_n = \sum_{\boldsymbol{x}\in\Omega^n} \frac{1}{M(\boldsymbol{x})-1} = \sum_{r=1}^{n+1} \frac{1}{r}(s(n,r)-s(n,r-1)). \quad (13)$$

Clearly, we have

$$s(n,0)=0 \text{ and } s(n,r)=2^n \text{ if } r \ge n+1. \quad (14)$$

Moreover, the words $\boldsymbol{x} \in \Omega^n$ with $M(\boldsymbol{x}) = n+2$ are $0^n, 10^{n-1}, \cdots, 1^{n-1}0$ and 1^n, so $s(n,n+1)-s(n,n)=n+1$. Finally, $s(n,1)=0$ if n is odd and $s(n,1)=1$ if n is even: the unique word with $M(\boldsymbol{x})=1$ is $0101\cdots01$. We now proceed with a recurrence formula for $s(n,r)$.

Theorem 4: If $r \le n$, then

$$s(n,r) = \sum_{l=n-r-1}^{n-2} (n-l-1)s(l,r).$$

If $r \ge n+1$, then

$$s(n,r) = n+1+\sum_{l=n-r-1}^{n-2} (n-l-1)s(l,r).$$

Proof: Let $\boldsymbol{x} \in \Omega^n$ be such that $M(\boldsymbol{x}) \le r+1$. We write

$$1\boldsymbol{x}0 = 1^{a_1}0^{b_1}\cdots 1^{a_m}0^{b_m}$$

where $a_i \ge 1, b_i \ge 1$ and

$$\sum_{i=1}^{m}(a_i+b_i) = n+2.$$

We first consider the case $m > 1$. We have

$$\boldsymbol{x}0 = 1^{a_1-1}0^{b_1}1\boldsymbol{y}0, \quad \text{where } 1\boldsymbol{y}0 = 1^{a_2}\cdots 0^{b_m}.$$

It is easy to see that $M(\boldsymbol{x}) \le r+1$ if and only if $a_1+b_1 \le r+1$ and$M(\boldsymbol{y}) \le r+1$. The length l of $\boldsymbol{y}$ equals $n-(a_1+b_1)$; hence, if $M(\boldsymbol{x}) \le r+1$, then $l \ge n-r-1$. As $a_1 \ge 1$ and $b_1 \ge 1$, l is at most $n-2$. If $n-r-1 \le l \le n-2$, there are $(n-l-1)$ choices for (a_1,b_1) and $s(l,r)$ choices for $\boldsymbol{y}$.

Clearly, $m=1$ exactly if $M(\boldsymbol{x})=n+2$. As there are $n+1$ vectors $\boldsymbol{x}$ with $M(\boldsymbol{x})=n+2$, the case $m=1$ has no contribution if $r+1 \le n+1$, and its contribution equals $n+1$ if $r+1 \ge n+2$. □

For $n \le 24$, we evaluated S_n with (11), (13), (14), and Theorem 4. The results are shown in Table III. For comparison, we also listed a lower bound to $F(n)$. For $n \le 10$ and for $n=12$, the lower bound equals the number of words of weight $\lfloor \frac{1}{2}n \rfloor$ (cf. Propostion 2). For $n = 11$, 13, and 14, the lower bounds are taken from Example 4. For $n \ge 15$, the lower bound follows from Table II. The rightmost column of Table III lists the quotient of upper and lower bound.

From this table, we see that the upper and lower bounds are close for small n. For large n, the upper bound seems to diverge from the lower bound.

TABLE III
BOUNDS ON CODES WITH $D^2_{min} = 2$

n	upper bound	lower bound	quotient
4	6	6	1.000
5	10	10	1.000
6	20	20	1.000
7	36	35	1.029
8	70	70	1.000
9	133	126	1.056
10	256	252	1.016
11	494	464	1.065
12	960	924	1.039
13	1861	1734	1.073
14	3632	3444	1.055
15	7091	6500	1.091
16	13872	12905	1.075
17	27185	24646	1.103
18	53352	48836	1.092
19	104825	93932	1.116
20	206202	186002	1.109
21	405998	360591	1.126
22	800138	712572	1.123
23	1578118	1390243	1.135
24	3114816	2741236	1.136

C. Asymptotics of S_n

For fixed r, the generating function $s_r(z)$ is defined by

$$s_r(z) = \sum_{n=0}^{\infty} s(n,r)z^n.$$

With Theorem 4, we find

$$s_r(z) = \frac{1+2z+3z^2+\cdots+rz^{r-1}}{1-z^2-2z^3\cdots-rz^{r+1}}, \quad \text{and so}$$

$$z^2 s(z,r) = -1 + \frac{(1-z)^2}{q_r(z)},$$

where $q_r(z) = 1-2z+(r+1)z^{r+2}-rz^{r+3}$.

As $s(n,r)=2^n$ for $r \ge n+1$, it follows from (13) that

$$S_n = \sum_{r=1}^{\infty} \frac{1}{r}[s(n,r)-s(n,r-1)] = \sum_{r=1}^{\infty} \frac{s(n,r)}{r(r+1)}.$$

Consequently, the generating function

$$S(z) = \sum_{n=0}^{\infty} S_n z^n$$

satisfies

$$S(z) = \sum_{n=0}^{\infty}\sum_{r=1}^{\infty} \frac{1}{r(r+1)} s(n,r)z^n = \sum_{r=1}^{\infty} \frac{1}{r(r+1)} s_r(z)$$

and so

$$z^2 S(z) = -1 + \sum_{r=1}^{\infty} \frac{1}{r(r+1)} \frac{(1-z)^2}{q_r(z)}. \quad (15)$$

In a private correspondence, our colleague A. J. E. M. Janssen applied techniques from complex analysis to (15) to obtain the asymptotic behavior of S_n, namely

$$S_n \sim 2^{n+1}/\log n, \quad n \to \infty.$$

Hence, asymptotically, S_n is far from the asymptotic form of the lower bound

$$\binom{n}{\lfloor \frac{1}{2}n \rfloor} \sim 2^n \Big/ \sqrt{\frac{\pi}{2}n}$$

(cf. Proposition 2).

Remark: Codes with minimum squared Euclidean distance larger than one may prove useful on a bursty unidirectional channel. In the classical binary-symmetric-channel model, both symbols 1 and -1 have equal probability of being corrupted. In the unidirectional channel model, only one of the symbols 1 or -1 can be corrupted—but it is not known which one. It is well known [9] that the words of length n and weight $\lceil \frac{n}{2} \rceil$ form a code of maximal cardinality for detecting all unidirectional errors.

With Theorem 3, it is readily verified that a code has minimum squared Euclidean distance larger than one if and only if it detects all single bursts of unidirectional errors.

In [10] and [11], systematic codes are constructed that detect all bursts up to a given length. It seems that nonsystematic codes that detect *all* single unidirectional burst errors have not been studied before.

V. Codes with Small Cardinality

In this section, we give explicit constructions of codes with small cardinality. Specific instances of these codes will be detailed in the next section.

Clearly, the word of length n with ith component $(-1)^i$ has distance $2n-1$ to its complement. Hence, there is a code of length n with two words with distance $d^2_{\min} = 2n-1$.

Next, we construct a code with four words. Let p, q, and r be integers and let the vectors $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, and $\boldsymbol{d}$ of length $n = p+q+r$ be defined as follows:

$$a_i = (-1)^i$$

$$b_i = \begin{cases} (-1)^i, & \text{if } 1 \le i \le p \\ (-1)^{i+1}, & \text{otherwise} \end{cases}$$

$$c_i = \begin{cases} (-1)^i, & \text{if } p+1 \le i \le p+q \\ (-1)^{i+1}, & \text{otherwise} \end{cases}$$

and

$$d_i = \begin{cases} (-1)^{i+1}, & \text{if } 1 \le i \le p+q \\ (-1)^i, & \text{otherwise.} \end{cases}$$

It is easy to verify the following table.

$\boldsymbol{x}, \boldsymbol{y}$	$d^2(\boldsymbol{x}, \boldsymbol{y})$
$\boldsymbol{a}, \boldsymbol{b}$	$2q+2r-1$
$\boldsymbol{a}, \boldsymbol{c}$	$2p+2r-2$
$\boldsymbol{a}, \boldsymbol{d}$	$2p+2q-1$
$\boldsymbol{b}, \boldsymbol{c}$	$2p+2q-3$
$\boldsymbol{b}, \boldsymbol{d}$	$2p+2r-2$
$\boldsymbol{c}, \boldsymbol{d}$	$2q+2r-3$

Consequently, the minimum squared Euclidean distance of the code equals $\min\{2q+2r-3, 2p+2r-2, 2p+2q-3\}$. Given n, this minimum is maximized by choosing $p = r$ and q as close to p as possible. That is, choose

- $p = q = r = \frac{1}{3}n$, if $n \equiv 0 \pmod 3$; $d^2_{\min} = \frac{4n}{3} - 3$
- $p = r = \lfloor \frac{n}{3} \rfloor, q = \lceil \frac{n}{3} \rceil$, if $n \equiv 1 \pmod 3$; $d^2_{\min} = 4\lfloor \frac{n}{3} \rfloor - 2$
- $p = r = \lceil \frac{n}{3} \rceil, q = \lfloor \frac{n}{3} \rfloor$, if $n \equiv 2 \pmod 3$; $d^2_{\min} = 4\lfloor \frac{n}{3} \rfloor - 1$.

Summarizing these results, we find that a code of length n exists with cardinality four and $d^2_{\min} = n + \lfloor \frac{n}{3} \rfloor - 3$. After discarding the word $\boldsymbol{c}$, we obtain a 3-word code whose minimum squared Euclidean distance equals $\min\{2q+2r-1, 2p+2q-1, 2p+2r-2\}$. The minimum distance is maximized by choosing $p = \lceil \frac{n}{3} \rceil$ and $q = \lfloor \frac{n}{3} \rfloor$. The minimum distance of the code so obtained equals $n - 2 + \lfloor \frac{1}{3}(n+1) \rfloor$, i.e., the minimum distance of the code with four words of length $n+1$ constructed above.

TABLE IV
Maximum $|\mathcal{S}^n|$ with Prescribed $d^2_{\min}(\mathcal{S}^n)$

d^2_{min} \ (n)	2	3	4	5	6	7	8
2	2	3	$\underline{6}$	10	$\underline{20}$	≥ 35	70
3	$\underline{2}$	2	$\underline{4}$	5	$\underline{10}$		≥ 18
4		2	2	3	5	8	≥ 10
5		$\underline{2}$	2	3	4	5	≥ 8
6			2	2	3	4	
7			$\underline{2}$	2	2	3	≥ 4
8				2	2	2	
9				$\underline{2}$	2	2	≥ 3
10					2	2	
11					$\underline{2}$	2	
12						2	
13						$\underline{2}$	

VI. Enumeration

In this section, we will list the cardinality of code sets achieving a prescribed Euclidean distance. The constructions described in the previous section will be used to provide lower bounds to the cardinality. In order to get some insight into the particular properties of optimal codes, we have conducted exhaustive computer searches. The results of the search programs are listed in Table IV. The figures are underscored if they relate to unique sets.

Several observations are imminent from Table IV.

The computer searches revealed that, for n even and $n \le 6$, (the maximum codeword length for which exhaustive searches were made) zeroth-order spectral null codes are maximum (and unique) sets that have a minimum distance of two. For n odd and $n \le 6$, the sets of fixed-weight codewords of weight $(n+1)/2$ or $(n-1)/2$ are optimum sets with a minimum distance of two.

We will describe codes whose main parameters are listed in Table IV. For notational convenience, we will use the alphabet $\{0, 1\}$ rather than the alphabet$\{-1, 1\}$.

The optimal set of length $n = 4$ and distance $d^2_{\min} = 3$ is unique, and it is a subset of $\mathcal{S}^4_0$, namely$\{0101, 0110, 1001, 1010\}$. The other codes of cardinality 4, as well as the codes of cardinality 2 and 3, are constructed in the previous section.

The optimal set of length $n = 6$ and distance $d^2_{\min} = 3$, obtained in Example 3, is unique. A five-word code of length five and $d^2_{\min} = 3$ can be constructed by taking the five words of the latter code that end with a zero, and subsequent deletion of this symbol.

The code of length 8 with eight words and $d^2_{\min} = 5$ is obtained by concatenation of the bi-phase code and the binary $[4, 3, 2]$ code—see Example 1. Adding the words 11001100 and 00110011 to this code, we obtain a code with ten words and $d^2_{\min} = 4$–see Corollary 3. Adding these two words to the concatenation of the bi-phase code and the binary $[4, 4, 1]$ code, we obtain a code of length 8 with 18 words and $d^2_{\min} = 3$—again we used Corollary 3. An example of a code with $n = 7$, $d^2_{\min} = 5$ is

$$\{100100, 1010010, 1010101, 0100010, 0100100\}.$$

An example of a code with $n = 7$, $d^2_{\min} = 4$ is provided by the set

$$\{0010101, 0100100, 0101001, 0110011, 1000110, 1001101, 1011011, 1101010\}.$$

A code of length $n = 6$ with $d^2_{\min} = 4$ can be obtained from the latter code by taking the five words ending in a one and subsequently discarding the last symbol.

VII. Conclusions

We have investigated Euclidean distance properties of bipolar block codes in conjunction with simple partial-response channels with transfer function $(1 \mp D^m)$, $m = 1, 2, \cdots$. Lower bounds to the cardinality of sets with prescribed minimum Euclidean distance have been provided. Matched spectral null codes of zeroth order are constructions offering large code sets, for small word length even optimal sets. Spectral null codes of higher order, $K \geq 1$, are far from optimal for the small values of the codeword lengths that have been investigated. Upper and lower bounds have been furnished to the size of codes with minimum squared Euclidean distance greater than unity.

ACKNOWLEDGMENT

The authors wish to thank A. J. E. M. Janssen for finding the asymptotical behavior of S_n described in Section IV-C.

REFERENCES

[1] J. K. Wolf and G. Ungerboeck, "Trellis coding for partial-response channels," *IEEE Trans. Commun.*, vol. COM-34, pp. 765–773, Aug. 1986.
[2] R. Karabed and P. H. Siegel, "Matched spectral-null codes for partial-response channels," *IEEE Trans. Inform. Theory,* vol. 37, no. 3, pp. 818–855, May 1991.
[3] K. Hole and Ø. Ytrehus, "Improved coding techniques for precoded partial-response channels," *IEEE Trans. Inform. Theory,* vol. 40, no. 2, pp. 482–493, Mar. 1994.
[4] K. A. S. Immink, "Coding techniques for partial-response channels," *IEEE Trans. Commun.,* vol. 36, pp. 1163–1165, Oct. 1988.
[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, New York: North-Holland, 1981.
[6] K. A. S. Immink and G. F. M. Beenker, "Binary transmission codes with higher order spectral zeros at zero frequency," *IEEE Trans. Inform. Theory,* vol. IT-33, no. 3, pp. 452–454, May 1987.
[7] R. M. Roth, P. H. Siegel, and A. Vardy, "Higer-order spectral-null codes—Constructions and bounds," *IEEE Trans. Inform. Theory,* vol. 40, no. 6, pp. 1826–1840, Nov. 1994.
[8] K. A. S. Immink, *Coding Techniques for Digital Recorders.* Englewood Cliffs, NJ: Prentice-Hall, 1991.
[9] B. Bose and T. R. N. Rao, "Theory of unidirectional error correcting/detecting codes," *IEEE Trans. Comput.*, vol. C-31, no. 6, pp. 521–530, June 1982.
[10] B. Bose, "Burst unidirectional error detecting codes," *IEEE Trans. Comput.*, vol. C-35, no. 4, pp. 350–353, Apr. 1986.
[11] M. Blaum, "Systematic unidirectional burst detecting codes," *IEEE Trans. Comput.*, vol. 37, no. 4, pp. 453–457, Apr. 1988.

An Efficient Block-Based Addressing Scheme for the Nearly Optimum Shaping of Multidimensional Signal Spaces

A. K. Khandani, *Associate Member, IEEE*, and P. Kabal, *Member, IEEE*

***Abstract*—We introduce an efficient addressing scheme for the nearly optimum shaping of a multidimensional signal constellation. The 2-D (two-dimensional) subspaces are partitioned into K energy shells of equal cardinality. The average energy of a 2-D shell can be closely approximated by a linear function of its index. In an $N = 2n$-D space, we obtain K^n shaping clusters of equal cardinality. Shaping is achieved by selecting $T \leq K^n$ of the N-D clusters with the least sum of the 2-D indices. This results in a set of T integer n-tuples with the components in the range $[0, K-1]$ and the sum of the components being at most a given number L. The problem of addressing is to find a one-to-one mapping between the set of such n-tuples and the set of integers $[0, T-1]$ such that the mapping and its inverse can be easily implemented. In the proposed scheme, the N-D clusters are grouped into blocks of identical binary weight vectors. This results in a simple rule for the addressing of points within the blocks. The addressing of the blocks is based on some recursive relationship which allows us to decompose the problem into simpler parts. The overall scheme requires a modest amount of memory and has a small computational complexity.**

***Index Terms*—Optimum shaping, addressing decomposition, recursive addressing, binary weight vectors, shell mapping.**

I. INTRODUCTION

A digital communication system is usually modeled as a discrete-time system. In the discrete model, the channel provides us with a given number of dimensions, say N, per signaling interval. In each signaling interval, the input data are encoded such that one of M equiprobable symbols is produced. To transmit these symbols, we select M points over the channel space. Each of the source symbols is represented by one of these points. This collection of points is called a signal constellation.

A signal constellation is usually selected as a finite subset of a regular array of points (packing) bounded within a shaping region. The main objective in selecting a shaping region is to minimize the average energy of the constellation for a given number of points from the given packing. The reduction in the average energy per two dimensions due to using a region $\mathcal{C}$ as the boundary instead of a hypercube is called the shaping gain of $\mathcal{C}$ and is denoted as $\gamma_s(\mathcal{C})$.

The price to be paid for a shaping gain $\gamma_s > 1$ involves: i) an increase in the factor CER_s (Constellation-Expansion Ratio) which is defined as the ratio of the employed number of points per two dimensions to the minimum necessary number of points per two dimensions [1], ii) an increase in the factor PAR_s (Peak-to-Average-power Ratio) which is defined as the ratio of the peak of energy per two dimensions to the average energy per two dimensions [1], and iii) an increase in the addressing complexity where addressing is the assignment of the input data to the constellation points.

Manuscript received November 2, 1992; revised December 10, 1994. This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). This work was presented in part at the IEEE International Conference on Communications, ICC'93.

A. K. Khandani is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, N2L 3G1.
P. Kabal is with the Department of Electrical Engineering, McGill University, Montreal, PQ, Canada, H3A 2A7.

IEEE Log Number 9414736.