High-Order Spectral-Null Codes—Constructions and Bounds

Ron M. Roth, *Member, IEEE,* Paul H. Siegel, *Senior Member, IEEE,* and Alexander Vardy, *Senior Member, IEEE*

***Abstract*—Let $\mathcal{S}(n,k)$ denote the set of all words of length n over the alphabet $\{+1,-1\}$, having a kth order spectral-null at zero frequency. A subset of $\mathcal{S}(n,k)$ is a spectral-null code of length n and order k. Upper and lower bounds on the cardinality of $\mathcal{S}(n,k)$ are derived. In particular we prove that $(k-1)\log_2(n/k) \le n - \log_2|\mathcal{S}(n,k)| \le O(2^k \log_2 n)$ for infinitely many values of n. On the other hand, we show that $\mathcal{S}(n,k)$ is empty unless n is divisible by 2^m, where $m = \lfloor \log_2 k \rfloor + 1$. Furthermore, bounds on the minimum Hamming distance d of $\mathcal{S}(n,k)$ are provided, showing that $2k \le d \le k(k-1)+2$ for infinitely many n. We also investigate the minimum number of sign changes in a word $\underline{x} \in \mathcal{S}(n,k)$ and provide an equivalent definition of $\mathcal{S}(n,k)$ in terms of the positions of these sign changes. An efficient algorithm for encoding arbitrary information sequences into a second-order spectral-null code of redundancy $3\log_2 n + O(\log\log n)$ is presented. Furthermore, we prove that the first nonzero moment of any word in $\mathcal{S}(n,k)$ is divisible by $k!$ and then show how to construct a word with a spectral null of order k whose first nonzero moment is any even multiple of $k!$. This leads to an encoding scheme for spectral-null codes of length n and any fixed order k, with rate approaching unity as $n \to \infty$.**

***Index Terms*—Input-constrained channels, spectral-null codes, spectral encoders.**

I. Introduction

Let Φ denote the bipolar binary alphabet $\{+1,-1\}$ regarded as a subset of the real field $\mathbb{R}$. We shall often use $+$ and $-$ as a shorthand notation for $+1$ and -1. With every word $\underline{x} = (x_1, x_2, \cdots, x_n) \in \Phi^n$, we associate a so-called *z-polynomial* in the indeterminate z,

$$X(z) = x_1 z + x_2 z^2 + \cdots + x_n z^n.$$

The discrete Fourier transform $X(e^{-j\omega})$ of $\underline{x}$ is then obtained by substituting $z = e^{-j\omega}$ in the z-polynomial of $\underline{x}$, where $j = \sqrt{-1}$. That is, $X(e^{-j\omega}) = \sum_{l=1}^{n} x_l e^{-j\omega l}$. The power spectrum of $\underline{x}$ is defined as $(1/n)|X(e^{-j\omega})|^2$.

Manuscript received September 16, 1993; revised March 16, 1994. The work of R. M. Roth and P. H. Siegel was supported in part by the United States–Israel Binational Science Foundation. The work of A. Vardy was supported in part by the Rothschild Fellowship. This paper was presented in part at the 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, June 1994.

R. M. Roth is with the Computer Science Department, Technion—Israel Institute of Technology, Haifa 32000, Israel.

P. H. Siegel is with the IBM Research Division, Almaden Research Center, San Jose, CA 95120.

A. Vardy was with the IBM Research Division, Almaden Research Center, San Jose, CA 95120. He is now with the Coordinated Science Laboratory, University of Illinois, Urbana, IL 61801.

IEEE Log Number 9406318.

A word $\underline{x} = (x_1, x_2, \cdots, x_n)$ in Φ^n is said to be a kth *order spectral-null word*, if its Fourier transform satisfies

$$\left.\frac{d^i X(e^{-j\omega})}{d\omega^i}\right|_{\omega=0} = 0 \qquad \text{for } i = 0, 1, \cdots, k-1.$$

It is fairly easy to verify that these k equalities hold if and only if

$$\left.\frac{d^i X(z)}{dz^i}\right|_{z=1} = 0 \qquad \text{for } i = 0, 1, \cdots, k-1. \tag{1}$$

Hence, a word over Φ is a kth order spectral-null word if and only if its z-polynomial is divisible by $(z-1)^k$. This property serves as an alternative common definition of kth order spectral-null words.

We let $\mathcal{S}(n,k) \subseteq \Phi^n$ denote the set of all kth order spectral-null words of length n over Φ. Any subset $\mathcal{C}$ of $\mathcal{S}(n,k)$ is called a *spectral-null code* of length n and order k. We shall refer to $\rho(\mathcal{C}) = n - \log_2|\mathcal{C}|$ as the redundancy of $\mathcal{C}$. The minimum distance $d(\mathcal{C})$ of $\mathcal{C}$ is the minimum Hamming distance between any two distinct words in $\mathcal{C}$.

Codes consisting of words with prescribed spectral-null properties have been extensively studied over the years. For instance, there is a vast body of literature on the first-order spectral-null codes, commonly known as dc-free codes. See for example [1]–[4], [6], [7], [9], [13], [18], [28]. High-order spectral-null codes—that is, subsets of $\mathcal{S}(n,k)$ for $k > 1$—have been recently considered in several works [5], [13]–[15], [22], for various applications. In particular, high-order spectral-null codes have been found useful for achieving a better rejection of the low-frequency components than is possible with the conventional dc-free codes [13], [14]. It is not too difficult to show (see [13, p. 241]) that for any kth order spectral-null word we have

$$\left.\frac{d^i |X(e^{-j\omega})|^2}{d\omega^i}\right|_{\omega=0} = 0 \qquad \text{for } i = 0, 1, \cdots, 2k-1$$

Thus, using kth order spectral-null words with larger values of k results in a power spectrum with a wider notch at zero frequency. Another notable application of high-order spectral-null codes for enhancing the error-correction capability of codes used in partial-response channels has been recently suggested in [5], [15].

The problem of analyzing and synthesizing high-order spectral-null codes has been dealt with in a number of papers [12], [14], [15], [22]. Some of the constructions [15], [22] are based on approaching the set $\mathcal{S}(n,k)$, when n

goes to infinity, by sets of words generated by all possible walks on certain labeled directed graphs. However, as the order of the spectral null increases, these graphs quickly become prohibitively complex. An alternative enumerative encoding scheme for $\mathcal{S}(n,2)$ was proposed in [12]. Still, there is no general construction of block codes that are subsets of $\mathcal{S}(n,k)$ with fairly small redundancy. The case of combining such constructions with prescribed error-correcting capability, and the design of efficient encoders and decoders for such codes, seem to be even more difficult problems that have yet to be explored.

This work has two main objectives. The first is to study the properties of the set $\mathcal{S}(n,k)$ and, in particular, derive upper and lower bounds on its cardinality and minimum distance. The second is to provide constructions of block codes that are subsets of $\mathcal{S}(n,k)$ with rate approaching unity as $n \to \infty$.

The case $k=0$ corresponds to unconstrained words and is therefore trivial. Thus $\mathcal{S}(n,0) = \Phi^n$ with $\rho(\mathcal{S}(n,0)) = 0$ and $d(\mathcal{S}(n,0)) = 1$. The set $\mathcal{S}(n,1)$ consists of all balanced, or dc-free, words with (cf. [13], [18])

$$\rho(\mathcal{S}(n,1)) = 0.5\log_2 n + O(1)$$
$$d(\mathcal{S}(n,1)) = 2$$

for all even n. Indeed, $\mathcal{S}(n,1)$ is empty if n is odd.

In general, no explicit expressions are presently known for the redundancy and minimum distance of $\mathcal{S}(n,k)$ for $k \geq 2$. However, in the next section we shall derive bounds on these parameters. We start in Section II-A with several equivalent presentations of the set $\mathcal{S}(n,k)$ in terms of null spaces of certain matrices. Such presentations will turn out to be instrumental in the sequel. Then we show in Section II-B that $\mathcal{S}(n,k) \neq \emptyset$ only if n is divisible by 2^m, where $m = \lfloor \log_2 k \rfloor + 1$. Next, we discuss in Section II-C a curious relationship between spectral-null codes and the so-called Morse sequences (cf. [8], [24]). In Section II-D we derive lower and upper bounds on the cardinality of $\mathcal{S}(n,k)$, showing that

$$\begin{aligned}(k-1)(\log_2(n) - \log_2(k-1)) \\ \leq \rho(\mathcal{S}(n,k)) \leq O\big((2^k-1)(\log_2(n) - k + 1)\big) \quad (2)\end{aligned}$$

for all n divisible by 2^k. Finally, in Section II-D we employ a well-known result from number theory (the Prouhet–Tarry problem cf. [10], [11]) to show that the minimum distance of $\mathcal{S}(n,k)$ is bounded by

$$2k \leq d(\mathcal{S}(n,k)) \leq k(k-1) + 2 \quad (3)$$

for all sufficiently large n divisible by 2^k.

In Section III we introduce yet another presentation of the set $\mathcal{S}(n,k)$ in terms of the positions of sign changes in every word $\underline{x} \in \mathcal{S}(n,k)$. An interesting feature of this presentation is that it characterizes $\mathcal{S}(n,k)$ as the set of all integer solutions of a certain system of Diophantine equations, without the additional constraint that these solutions belong to the binary alphabet $\Phi = \{+1, -1\}$, which is usually implicit in all other definitions. Using this characterization of $\mathcal{S}(n,k)$, we show that the lower bound of k on the number of sign changes in a kth order spectral-null word, given in [15], is not tight.

The remaining two sections are devoted to constructions of block spectral-null codes of length n and order k, for increasing values of k. Using enumerative encoding [12], [13], it is fairly easy to encode an arbitrary binary sequence of length $m = n - 0.5\log_2 n - O(1)$, regarded as an m-bit representation of an integer N, into a word $\underline{x}_N \in \mathcal{S}(n,1)$ indexed by N according to the standard lexicographic order on $\mathcal{S}(n,1)$. Henry [29] and independently Knuth [18] described a simpler encoding method into a subset of $\mathcal{S}(n,1)$ whose redundancy is about twice the redundancy of $\mathcal{S}(n,1)$. See also [1], [2], [9]. In Section IV we present an algorithm for encoding arbitrary sequences into a subset of $\mathcal{S}(n,2)$, which is, in some sense, a generalization of the encoding method of Knuth [18]. The redundancy of the resulting second-order spectral-null code is bounded from above by $3\log_2 n + O(\log\log n)$.

In Section V we present a general encoding scheme into a subset of $\mathcal{S}(n,k)$ for any fixed order k. First we describe in Section V-A an alternative algorithm for encoding arbitrary sequences into a subset of $\mathcal{S}(n,2)$. The redundancy of the resulting second-order spectral-null codes is substantially greater than $3\log_2 n + O(\log\log n)$. Hence these codes are inferior to the second-order spectral-null codes introduced in Section IV. Nevertheless, the rate of these codes still approaches unity as $n \to \infty$. Furthermore, unlike the construction of Section IV, the construction of Section V-A lends itself to generalization for values of k greater than 2. One of the key ingredients required for such generalization is the existence of an algorithm which, given a certain word $\underline{x} \in \mathcal{S}(n_1,k)$, produces a word $\underline{y}$ such that $(\underline{x}|\underline{y}) \in \mathcal{S}(n_2,k+1)$ for some $n_2 > n_1$, where $(\cdot|\cdot)$ denotes concatenation. Such an algorithm is derived in Section V-B. Finally, in Section V-C we employ this algorithm to describe a recursive encoding scheme for spectral-null codes of length n and any fixed order k. It is also shown in Section V-C that these codes are asymptotically optimal, in the sense that their rate approaches unity as $n \to \infty$.

II. Bounds on the Parameters of $\mathcal{S}(n,k)$

In this section we derive several equivalent presentations of the set $\mathcal{S}(n,k)$. We then show that $\mathcal{S}(n,k)$ is nonempty only if the length n satisfies a certain constraint. Following a discussion on Morse sequences as examples of spectral-null words, we devote the rest of the section to our main results herein—namely, upper and lower bounds on the cardinality and minimum distance of $\mathcal{S}(n,k)$.

A. Definitions of $\mathcal{S}(n,k)$

We start by summarizing several necessary and sufficient conditions for a given word to be a kth order spectral-null word. Thus, Lemmas 2.1–2.3 below provide characterizations of $\mathcal{S}(n,k)$ in the form of null spaces of certain matrices. As such, these matrices may be regarded as "parity-check" matrices of $\mathcal{S}(n,k)$. Most of these characterizations are essentially known and can be found in [5], [13, ch. 9], [14], [15], [22], among other works.

Lemma 2.1: Let

$$Q(n,k) \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \binom{1}{1} & \binom{2}{1} & \cdots & \binom{n}{1} \\ \binom{1}{2} & \binom{2}{2} & \cdots & \binom{n}{2} \\ \vdots & \vdots & \vdots & \vdots \\ \binom{1}{k-1} & \binom{2}{k-1} & \cdots & \binom{n}{k-1} \end{bmatrix}.$$

Then

$$\mathscr{S}(n,k) = \{\underline{x} \in \Phi^n : Q(n,k)\underline{x}^t = \underline{0}\} = \left\{\underline{x} \in \Phi^n : \sum_{l=1}^{n} \binom{l}{i} x_l = 0 \text{ for } i = 0,1,\cdots,k-1\right\}.$$

Proof: Let $\underline{x} = (x_1, x_2, \cdots, x_n)$ be a word over Φ and let $X(z)$ be the corresponding z-polynomial. It is straightforward to verify that

$$\left.\frac{d^i X(z)}{dz^i}\right|_{z=1} = i! \sum_{l=1}^{n} \binom{l}{i} x_l.$$

The lemma now follows immediately from (1). Note that the binomial coefficient $\binom{j}{i}$ is assumed to be zero for $j < i$. □

Let $\mathscr{V}(n,k)$ be the null space of $Q(n,k)$—that is, the vector space over the real field $\mathbb{R}$ of dimension $n-k$ consisting of all words $\underline{y} \in \mathbb{R}^n$ satisfying $Q(n,k)\underline{y}^t = \underline{0}$. Then, obviously, $\mathscr{S}(n,k) = \mathscr{V}(n,k) \cap \Phi^n$. It therefore follows that if M is any $k \times n$ matrix with entries from $\mathbb{R}$ such that the null space of M is equal to that of $Q(n,k)$, then

$$\mathscr{S}(n,k) = \{\underline{x} \in \Phi^n : M\underline{x}^t = \underline{0}\}. \tag{4}$$

We now specifically indicate two such matrices:

$$H(n,k;c) \stackrel{\text{def}}{=} \left[(j+c)^i\right]_{i=0,j=1}^{k-1,n}$$

$$D(n,k) \stackrel{\text{def}}{=} [d_{i,j}]_{i=0,j=0}^{k-1,n-1}$$

where

$$d_{i,j} = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j < k \text{ and } j \neq i. \\ (-1)^{k-i-1}\binom{j}{i}\binom{j-i-1}{k-i-1} & \text{if } j \geq k \end{cases} \tag{5}$$

Substituting these matrices into (4) leads to equivalent characterizations of $\mathscr{S}(n,k)$, which will prove to be useful in the sequel.

Lemma 2.2: For any constant $c \in \mathbb{R}$, let

$$H(n,k;c) \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1+c & 2+c & \cdots & n+c \\ (1+c)^2 & (2+c)^2 & \cdots & (n+c)^2 \\ \vdots & \vdots & \vdots & \vdots \\ (1+c)^{k-1} & (2+c)^{k-1} & \cdots & (n+c)^{k-1} \end{bmatrix}.$$

Then

$$\mathscr{S}(n,k) = \{\underline{x} \in \Phi^n : H(n,k;c)\underline{x}^t = \underline{0}\} = \left\{\underline{x} \in \Phi^n : \sum_{l=1}^{n} (l+c)^i x_l = 0 \text{ for } i = 0,1,\cdots k-1\right\}.$$

Proof: It is known [16, p. 55] that the polynomials

$$1, z, \frac{z(z-1)}{2}, \cdots, \frac{z(z-1)\cdots(z-i+1)}{i!}$$

form a basis of the $(i+1)$-dimensional linear space of all real polynomials of degree $\leq i$ in the indeterminate z. This linear space is also spanned by a shifted form of the standard basis $1, z+c, (z+c)^2, \cdots (z+c)^i$ for every real c. It thus follows that there is a nonsingular lower-triangular $k \times k$ matrix, $T = [t_{i,j}]_{i,j=0}^{k-1}$ say, such that

$$(j+c)^i = t_{i,0}\binom{j}{0} + t_{i,1}\binom{j}{1} + t_{i,2}\binom{j}{2} + \cdots + t_{i,i}\binom{j}{i}$$

for all integers j. Hence, the rows of $H(n,k;c)$ and $Q(n,k)$ span the same linear space and, so, the null spaces of $H(n,k;c)$ and $Q(n,k)$ must be equal. The lemma now follows from Lemma 2.1. □

The foregoing lemma shows that the spectral properties of a word $\underline{x} \in \Phi^n$ are position (or time, or shift) invariant. That is, a word $\underline{x}$ is a kth order spectral-null word if and only if so is any shifted version of $\underline{x}$. Indeed, this can as well be observed from the following simple fact. For any positive integer c, the z-polynomial $X(z)$ of $\underline{x}$ is divisible by $(z-1)^k$ if and only if $z^c X(z)$ is also divisible by $(z-1)^k$. This property will be of importance in Section II-D and also in Sections IV and V.

However, in most cases we will make use of Lemma 2.2 with $c = 0$. We shall employ the shorthand notation $H(n,k)$ for $H(n,k;0)$. For an integer $k \geq 0$ and a real vector $\underline{x} = (x_1, x_2, \cdots x_n)$, the *kth order moment* of $\underline{x}$ is defined as in [14], [15] by $m_k(\underline{x}) \stackrel{\text{def}}{=} \sum_{j=1}^{n} j^k x_j$. Substituting $c = 0$ in Lemma 2.2, we thus arrive at the same characterization of $\mathscr{S}(n,k)$ as in [14], [15], namely

$$\mathscr{S}(n,k) = \left\{\underline{x} \in \Phi^n : m_i(\underline{x}) = \sum_{j=1}^{n} j^i x_j = 0 \text{ for } i = 0,1,\cdots,k-1\right\}. \tag{6}$$

Lemma 2.3: Let $D(n,k)$ be the $k \times n$ matrix $[I_k \tilde{D}(n,k)]$, where I_k is the identity matrix of order k and

$$\tilde{D}(n,k) = \begin{bmatrix} (-1)^{k-1}\binom{k}{0} & (-1)^{k-1}\binom{k+1}{0}\binom{k}{k-1} & \cdots & (-1)^{k-1}\binom{n-1}{0}\binom{n-2}{k-1} \\ (-1)^{k-2}\binom{k}{1} & (-1)^{k-2}\binom{k+1}{1}\binom{k-1}{k-2} & \cdots & (-1)^{k-2}\binom{n-1}{1}\binom{n-3}{k-2} \\ (-1)^{k-3}\binom{k}{2} & (-1)^{k-3}\binom{k+1}{2}\binom{k-2}{k-3} & \cdots & (-1)^{k-3}\binom{n-1}{2}\binom{n-4}{k-3} \\ \vdots & \vdots & \vdots & \vdots \\ (-1)^{0}\binom{k}{k-1} & (-1)^{0}\binom{k+1}{k-1}\binom{1}{0} & \cdots & (-1)^{0}\binom{n-1}{k-1}\binom{n-k-1}{0} \end{bmatrix}.$$

Then

$$\begin{aligned}\mathcal{S}(n,k) &= \{\underline{x} \in \Phi^n : D(n,k)\underline{x}^t = \underline{0}\} \\ &= \Bigg\{\underline{x} \in \Phi^n : (-1)^{k-i-1}\sum_{j=k}^{n-1}\binom{j}{i}\binom{j-i-1}{k-i-1}x_{j+1} \\ &\qquad = -x_{i+1} \text{ for } i = 0,1,\cdots,k-1\Bigg\}.\end{aligned}$$

Proof: Let $B(k) = [b_{i,j}]_{i=0,j=0}^{k-1,k-1}$ be the $k \times k$ matrix whose entries are coefficients of the following polynomials in the indeterminate Z:

$$\begin{aligned} b_i(Z) &= \sum_{j=0}^{k-1} b_{i,j}Z^j \\ &= \frac{\prod_{l=0,\, l\neq i}^{k-1}(Z-l-1)}{\prod_{l=0,\, l\neq i}^{k-1}(i-l)}, \qquad \text{for } i = 0,1,\cdots,k-1. \end{aligned} \tag{7}$$

We now show that $D(n,k) = B(k)H(n,k)$. Denoting $B(k)H(n,k) = [c_{i,j}]_{i=0,j=0}^{k-1,n-1}$ and referring to (7), we have

$$c_{i,j} = \sum_{l=0}^{k-1} b_{i,l}(j+1)^l = b_i(Z)|_{Z=j+1} = \frac{\prod_{l=0,\, l\neq i}^{k-1}(j-l)}{\prod_{l=0,\, l\neq i}^{k-1}(i-l)} \tag{8}$$

for $i = 0,1,\cdots,k-1$ and $j = 0,1,\cdots,n-1$. Now, for $j < k$ we see from (8) that $c_{i,j}$ is equal to the Kronecker delta function $\delta(i,j)$ and therefore the first k columns of $B(k)H(n,k)$ form the identity matrix. That is, $B(k)$ is the inverse of $H(k,k)$, see [16, p. 36]. As for $j \geq k$, we have

$$\begin{aligned} c_{i,j} &= \frac{\prod_{l=0}^{i-1}(j-l)}{\prod_{l=0}^{i-1}(i-l)} \cdot \frac{\prod_{l=i+1}^{k-1}(j-l)}{\prod_{l=i+1}^{k-1}(i-l)} \\ &= (-1)^{k-i-1}\binom{j}{i}\binom{j-i-1}{k-i-1} = d_{i,j} \end{aligned}$$

where $d_{i,j}$ is as defined in (5). This shows that indeed $D(n,k) = B(k)H(n,k)$, and since $B(k)$ is nonsingular, the lemma now follows from (4). □

The matrix $D(n,k)$ is a "systematic" parity-check matrix of $\mathcal{S}(n,k)$, which allows us to express the first k positions of any word $\underline{x} \in \mathcal{S}(n,k)$ as a function of the last $n-k$ positions. In fact, since any $k \times k$ submatrix of $H(n,k)$ is a nonsingular Vandermonde matrix, any k positions in $\underline{x}$ may be expressed in terms of the remaining $n-k$ positions in a manner similar to that of Lemma 2.3. Furthermore, we have for $j \geq k$

$$\begin{aligned} d_{i,j} &= (-1)^{k-i-1}\binom{j}{i}\binom{j-i-1}{k-i-1} \\ &= (-1)^{k-i-1}\binom{k}{i}\binom{j}{k}\frac{k-i}{j-i}. \end{aligned}$$

Thus $\tilde{D}(n,k)$ is a generalized Cauchy matrix with *integer* entries (see [26]). All these properties of spectral-null codes resemble to a certain extent the properties of Reed–Solomon codes [19, ch. 11].

Lemma 2.3 will be employed in Section V-B to show that the kth moment of every $\underline{x}$ in $\mathcal{S}(n,k)$ is divisible by $k!$. This property is crucial for the construction of high-order spectral-null codes presented in Section V.

B. A Constraint on the Length of $\mathcal{S}(n,k)$

It is obvious that $\mathcal{S}(n,1) \neq \emptyset$ only if n is even, and it is well-known that $\mathcal{S}(n,2) \neq \emptyset$ only if n is divisible by 4 [14]. How does this constraint on the length of a (nonempty) spectral-null code of order k extend to values of k greater than two? In particular, is it true that as the order k of the null increases, the length of a spectral-null code of order k must be divisible by increasing powers of 2? In this section we settle the latter question affirmatively.

Theorem 2.4: The set $\mathcal{S}(n,k)$ is empty unless n is divisible by 2^m where $m = \lfloor \log_2 k \rfloor + 1$.

Proof: Let $\underline{x}$ be a kth order spectral-null word of length n. Then the z-polynomial $X(z)$ of $\underline{x}$ can be factored over the rationals into $(z-1)^k Y(z)$ for some polynomial $Y(z)$. In fact, by Gauss's lemma (cf. [17, p. 404]), the polynomial $Y(z)$ has integer coefficients. Reducing the equality $X(z) = (z-1)^k Y(z)$ modulo 2, we find that over GF(2) the polynomial $(z-1)^k$ divides the polynomial $z + z^2 + \cdots + z^n = z(z^n - 1)/(z-1)$. Thus, we may conclude that over GF(2) the polynomial $(z-1)^{k+1}$ divides the polynomial $z^n - 1$.

Now let m be an integer such that $2^{m-1} < k+1 \le 2^m$. That is, $m = \lfloor \log_2 k \rfloor + 1$ as in the statement of the theorem. Then $(z-1)^{k+1}$ obviously divides $(z-1)^{2^m}$. Note that in GF(2) we have $(z-1)^{2^m} = z^{2^m} - 1$. Hence, over GF(2) the polynomial $(z-1)^{k+1}$ divides both $z^n - 1$ and $z^{2^m} - 1$. As such, it must also divide $\gcd(z^n - 1, z^{2^m} - 1)$. Using Euclid's algorithm we obtain that $\gcd(z^n - 1, z^{2^m} - 1) = z^d - 1$ where $d = \gcd(n, 2^m)$. This, in fact, is true over any field. Therefore, $z^{k+1} - 1$ divides $z^d - 1$, which, in particular, implies that $k+1 \le d$. Now, d is a divisor of 2^m and so it is a power of 2. Recalling that $2^{m-1} < k+1 \le d \le 2^m$, it follows that d must be equal to 2^m. Thus $\gcd(n, 2^m) = 2^m$, which implies that 2^m divides n (see also [21, p. 103] for a slightly weaker statement). □

We shall see in the next section that Theorem 2.4 is tight for $k = 1,2,3,4,5$. Whether this bound is tight in general remains an open question. Equivalently, we have the following.

Question: Is it true that $\mathscr{S}(2^m q, 2^m - 1) \ne \varnothing$ for any fixed m and sufficiently large q?

We point out that it would suffice to show that $\mathscr{S}(2^m q_0, 2^m - 1) \ne \varnothing$ for one particular odd q_0, for any given m. Indeed, the set $\mathscr{S}(2^{2^m - 1}, 2^m - 1)$ is nonempty, as will be shown in the sequel. If q_0 is odd then $\gcd(q_0, 2^{2^m - 1 - m}) = 1$. Hence, by the conductor theorem of Frobenius [27, p. 276] every sufficiently large q can be written as $q = aq_0 + b2^{2^m - 1 - m}$, for some positive integers a and b. Therefore, by concatenating a copies of a word in $\mathscr{S}(2^m q_0, 2^m - 1)$ with b copies of a word in $\mathscr{S}(2^{2^m - 1}, 2^m - 1)$ we obtain a spectral-null sequence of length $2^m q$ and order $2^m - 1$.

C. Spectral-Null Codes of Short Length and Morse Sequences

The cardinality of the set $\mathscr{S}(n,k)$ for small values of n may be easily calculated, using for instance the generating function of [14] or direct enumeration. Table I below (which is calculated from the table in [14]) lists the values of $\rho(\mathscr{S}(n,k))$ for lengths $n \le 32$ that are divisible by 4. Empty entries in the table correspond to empty sets $\mathscr{S}(n,k)$.

TABLE I
REDUNDANCY OF $\mathscr{S}(n,k)$ FOR $n \le 32$ WITH $4|n$

$k \backslash n$	4	8	12	16	20	24	28	32
1	1.42	1.87	2.15	2.35	2.50	2.63	2.74	2.84
2	3	5	6.14	6.96	7.59	8.10	8.54	8.91
3		7	11	12.19	14.42	14.49	16.51	16.91
4				15		20		25.71
5								31

Several observations are evident from Table I. In particular, it readily follows from the table that the condition of Theorem 2.4 is not sufficient for $\mathscr{S}(n,k)$ to be nonempty. For example, taking $n = 16$, $k = 5$, and $m = \lfloor \log_2 k \rfloor + 1 = 3$, we see that 2^m divides n, and yet $\mathscr{S}(n,k) = \mathscr{S}(16,5) = \varnothing$. On the other hand, it follows from the table that $\mathscr{S}(4q,3) \ne \varnothing$ for $q = 2,3$. Since $\underline{x}_1 \in \mathscr{S}(n_1,k)$ and $\underline{x}_2 \in \mathscr{S}(n_2,k)$ can always be concatenated to produce $(\underline{x}_1|\underline{x}_2) \in \mathscr{S}(n_1+n_2,k)$, we deduce from Table I that $\mathscr{S}(4q,3) \ne \varnothing$ for $q \ge 2$ and $\mathscr{S}(4q,2) \ne \varnothing$ for $q \ge 1$. Furthermore, it can be verified by computer search that $\mathscr{S}(8q,5) \ne \varnothing$ for $q = 4,5,6,7$. Hence, $\mathscr{S}(8q,5) \ne \varnothing$ for $q \ge 4$ and $\mathscr{S}(8q,4) \ne \varnothing$ for $q \ge 2$.

We also point out that for $k \ge 1$ and $n \le 32$, the minimum distance of a nonempty set $\mathscr{S}(n,k)$ equals $2k$, except when the redundancy is $n-1$. In the latter case, the two words in $\mathscr{S}(n,k)$ are complements of each other and, therefore, the minimum distance is n.

The following two facts particularly stand out in Table I. For all $k \le 5$:

- the smallest integer n for which $\mathscr{S}(n,k) \ne \varnothing$ is $n = 2^k$;
- the set $\mathscr{S}(2^k,k)$ contains exactly two words.

We now show that these two words are (the truncations of) the binary Morse sequence (cf. [8], [24]) and its complement. The following lemma is slightly more general.

Lemma 2.5: For any $k \ge 0$ and any word $\underline{x} \in \Phi^n$ there exists a word $\underline{y} \in \mathscr{S}(2^k n, k)$ containing $\underline{x}$ as its prefix.

Proof: Let $X(z)$ be the z-polynomial of $\underline{x}$. Then

$$Y(z) = X(z)(1 - z^n)(1 - z^{2n})(1 - z^{4n}) \cdots (1 - z^{2^{k-1}n}) \tag{9}$$

is a z-polynomial of a word $\underline{y} \in \Phi^{n2^k}$ that contains $\underline{x}$ as a prefix. Since $(z-1)$ divides each of the k factors multiplying $X(z)$ in (9), it is clear that $Y(z)$ is divisible by $(z-1)^k$. Hence $\underline{y} \in \mathscr{S}(2^k n, k)$. □

Applying the construction of Lemma 2.5 to the word $\underline{x} = (+) \in \Phi^1$ produces, for $k \to \infty$, the infinite binary Morse sequence

$$+ - - + - + + - - + + - + - - + - + + - \\ + - - + + - - + - + + - \cdots$$

which is well-known in symbolic dynamics [8], [24]. It is easy to see that this sequence contains a $+$ in position i (starting at $i = 0$) if and only if the binary representation of i has even Hamming weight. We shall denote by $\mu(k)$ the truncation of the Morse sequence to its first 2^k positions. Then it follows from Lemma 2.5, in conjunction with Table I, that for all $k \le 5$ the Morse sequence $\mu(k)$ is the shortest spectral-null word of order k. Furthermore, for $k \le 5$, the Morse sequence $\mu(k)$ and its complement are the only elements in $\mathscr{S}(2^k,k)$.

It is tempting to ask whether the two properties of the Morse sequence exhibited in Table I extend beyond $k = 5$. Thus, we have the following.

Question: Is $\mu(k)$ the shortest spectral-null word of order k, for all k?

Question: Is it true that $\mathscr{S}(2^k,k) = \{\mu(k), \overline{\mu(k)}\}$ for all k?

While the first question remains open, the answer to the second question is, surprisingly, negative. For $k = 6$, the set $\mathcal{S}(2^6, 6)$ contains words other than the Morse sequence, e.g., the word

$$++----++-+--+-+++++--\\+--+--+--++$$

concatenated with its reflection. The construction of Lemma 2.5 may now be applied to this word to show that $\mathcal{S}(2^k, k) \neq \{\mu(k), \overline{\mu(k)}\}$ for all $k \geq 6$.

D. Bounds on Redundancy

Let $\mathcal{S}(k) = \bigcup_{n \geq 1} \mathcal{S}(n, k)$ denote the set of kth order spectral-null words over Φ. The set $\mathcal{S}(k)$ may be thought of as the set of all words admitted by the binary-input spectral-null channel of order k. The *capacity* of a spectral-null channel of order k is then defined by

$$\mathbf{cap}(\mathcal{S}(k)) = \limsup_{n \to \infty} \frac{\log_2 |\mathcal{S}(n,k)|}{n}.$$

It was noted in [15], using arguments based on canonical finite-state transition diagrams, that the capacity of a kth order spectral-null channel should be equal to unity for any fixed order k. We prove here that indeed $\mathbf{cap}(\mathcal{S}(k)) = 1$. Furthermore, we provide upper and lower bounds on $|\mathcal{S}(n,k)|$, or equivalently on $\rho(\mathcal{S}(n,k))$, establishing the stronger claim of (2).

The following theorem is essentially a sphere-packing upper bound on the cardinality of the set $\mathcal{S}(n,k)$.

Theorem 2.6: For all $n > k \geq 1$,

$$\rho(\mathcal{S}(n,k)) \geq (k-1)(\log_2(n) - \log_2(k-1)).$$

Proof: It is shown in [14], [15] that the minimum distance of $\mathcal{S}(n,k)$ is at least $2k$. Thus, by the sphere-packing bound [19, ch. 1] we have

$$\log_2 |\mathcal{S}(n,k)| \leq n - \log_2 V(n, k-1)$$

where $V(n,k) = \sum_{i=0}^{k} \binom{n}{i}$ denotes the volume of the Hamming sphere of radius k in Φ^n. The theorem now follows from the inequality $V(n, k-1) \geq \binom{n}{k-1} \geq (n/(k-1))^{k-1}$. □

The following theorem is a nonconstructive lower bound on the cardinality of $\mathcal{S}(n,k)$, which implies in particular that $\mathbf{cap}(\mathcal{S}(k)) = 1$. In Section V we present a construction of spectral-null codes that attains the capacity. However, the existence result of Theorem 2.7 provides a much better bound on the redundancy of $\mathcal{S}(n,k)$.

Theorem 2.7: For all $n \geq 1$ such that $2^k | n$,

$$\rho(\mathcal{S}(n,k)) \leq O\big((2^k - 1)(\log_2(n) - k + 1)\big).$$

Proof: The result is obviously true for $k = 0, 1$. Hence we hereafter assume that $k > 1$, in which case n is even. Write $n = 2h$ and let $\mathcal{S}(h, k; a)$ denote the set of all words $\underline{x}$ in $\mathcal{S}(h, k-1)$, such that $m_{k-1}(\underline{x}) = a$ for some fixed integer a. Further, let $A(h,k)$ denote the set of all the integers a for which $\mathcal{S}(h,k;a)$ is nonempty.

For each $a \in A(h,k)$ define the set $\mathcal{B}(n,k;a)$ by

$$\mathcal{B}(n,k;a) \stackrel{\text{def}}{=} \big\{ (\underline{x} | \underline{y}) \in \Phi^n : \underline{x} \in \mathcal{S}(h,k;a) \text{ and } \underline{y} \in \mathcal{S}(h,k;-a) \big\}.$$

It follows from Lemma 2.2 that $\mathcal{B}(n,k;a) \subseteq \mathcal{S}(n,k)$ for every $a \in A(h,k)$. Furthermore, $|\mathcal{B}(n,k;a)| = |\mathcal{S}(h,k;a)|^2$ since $|\mathcal{S}(h,k;a)| = |\mathcal{S}(h,k;-a)|$, and $\mathcal{B}(n,k;a) \cap \mathcal{B}(n,k;b) = \emptyset$ whenever $a \neq b$ since the sets $\mathcal{S}(h,k;a)$ form a partition of $\mathcal{S}(h, k-1)$. Hence we have

$$|\mathcal{S}(n,k)| \geq \sum_{a \in A(h,k)} |\mathcal{S}(h,k;a)|^2 \tag{10}$$

and

$$\sum_{a \in A(h,k)} |\mathcal{S}(h,k;a)| = |\mathcal{S}(h,k-1)|. \tag{11}$$

By the $\cup$-convexity of the function $f(z) = z^2$, the mean of the squares of real values is not smaller than the square of their mean. Hence,

$$\frac{\sum_{a \in A(h,k)} |\mathcal{S}(h,k;a)|^2}{|A(h,k)|} \geq \left(\frac{\sum_{a \in A(h,k)} |\mathcal{S}(h,k;a)|}{|A(h,k)|} \right)^2 = \frac{|\mathcal{S}(h,k-1)|^2}{|A(h,k)|^2}$$

where the last equality follows from (11). Therefore (10) implies

$$|\mathcal{S}(n,k)| \geq \frac{|\mathcal{S}(h,k-1)|^2}{|A(h,k)|} \tag{12}$$

Taking logarithms of both sides in (12) yields

$$\rho(\mathcal{S}(n,k)) \leq 2\rho(\mathcal{S}(h,k-1)) + \log_2 |A(h,k)|. \tag{13}$$

Obviously, $|A(h,k)| \leq 1 + 2\sum_{j=1}^{h} j^{k-1} \leq n^k$ whenever $k \geq 2$. Substituting this upper bound on $A(h,k)$ into (13), and writing $n = 2^m q$ for some $m \geq k$, we obtain

$$\rho(\mathcal{S}(2^m q, k)) \leq 2\rho(\mathcal{S}(2^{m-1} q, k-1)) + k(m + \log_2 q).$$

Taking into account that $\rho(\mathcal{S}(n,0)) = 0$ for all n, we can solve the above recursion to show that

$$\rho(\mathcal{S}(2^m q, k)) \leq \sum_{i=0}^{k-1} 2^i (k-i)(m - i + \log_2 q) = O\big((2^k - 1)(\log_2(q) + m - k + 1)\big)$$

as claimed. □

Remark: Theorem 2.7 can be slightly improved by using better estimates for the size of $A(n,k)$ and observing that the sizes of $\mathcal{S}(n,k;a)$ depend on a. In particular, an improvement can be obtained by taking into account that $k!$ must divide a for every $a \in A(n,k)$, as will be shown in Section V-B. However, such arguments will not get rid of the 2^k term in the bound of the Theorem 2.7, and are therefore omitted.

Remark: Referring to Table I, it is clear that Theorem 2.7 does not cover the entire range of values of n and k for which $\mathcal{S}(n,k) \neq \emptyset$. For instance, taking $n = 12$ and

$k = 3$, we see that 2^k does not divide n, and yet $\mathcal{S}(n,k) = \mathcal{S}(12,3) \neq \emptyset$.

E. Bounds on the Minimum Distance

It is shown in [14], [15] that the minimum distance of $\mathcal{S}(n,k)$ is bounded from below by $2k$. We present next an upper bound on the minimum distance of $\mathcal{S}(n,k)$ for infinitely many values of n, establishing (3).

Both [14] and [15] make use of a well-known result from number theory—The Prouhet–Tarry problem. Suppose that $A = \{a_1, a_2, \cdots, a_s\}$ and $B = \{b_1, b_2, \cdots, b_s\}$ are two disjoint sets of distinct positive integers and consider the system of k equations

$$a_1^i + a_2^i + \cdots + a_s^i = b_1^i + b_2^i + \cdots + b_s^i \qquad \text{for } i = 0, 1, \cdots, k-1. \quad (14)$$

Then the Prouhet–Tarry problem asks for the least value of s for which (14) has a solution. We shall use $P(k)$ to denote this value of s.

Lemma 2.8 (Prouhet–Tarry [10, p. 329]):

$$P(k) \le \tfrac{1}{2}k(k-1) + 1$$

The proof of the lower bound on $d(\mathcal{S}(n,k))$ in [15] is based on the lower bound $P(k) \ge k$. Herein we employ the upper bound on $P(k)$ of Lemma 2.8 to derive an upper bound on $d(\mathcal{S}(n,k))$.

Theorem 2.9: For any fixed k and any sufficiently large n that is divisible by 2^k,

$$d(\mathcal{S}(n,k)) \le 2P(k) \le k(k-1) + 2.$$

Proof: Set $s = P(k)$ and let $A = \{a_1, a_2, \cdots, a_s\}$ and $B = \{b_1, b_2, \cdots, b_s\}$ be the two solutions of (14) guaranteed by Lemma 2.8. Take N to be an integer greater than any of the elements in $A \cup B$, and consider the word $\underline{x} = (x_1, x_2 \cdots x_N) \in \Phi^n$, where $x_a = -1$ if $a \in A$ and $x_a = 1$ otherwise. Let $\underline{y} = (y_1, y_2, \cdots, y_N) \in \Phi^N$ be a similar word with respect to the set B. Clearly, $x_i = y_i$ for all the positions i that are not in $A \cup B$, and therefore the Hamming distance between $\underline{x}$ and $\underline{y}$ is $2P(k) \le k(k-1) + 2$. In view of Lemma 2.5, there exists a word $\underline{w} \in \mathcal{S}(2^kN, k)$ that contains $\underline{x}$ as its N-prefix. Replacing this prefix by $\underline{y}$, we obtain another word in $\mathcal{S}(2^kN, k)$ at distance $\le k(k-1) + 2$ from $\underline{w}$. □

Remark: It is known [11, p. 507] that $P(k) = k$ for all $k \le 10$. Hence, it follows from Theorem 2.9 that for $k \le 10$ the minimum distance of $\mathcal{S}(n,k)$ is exactly $2k$ for infinitely many values of n.

III. On Sign Changes in Spectral-Null Sequences

The characterizations of $\mathcal{S}(n,k)$ in the previous section may be recast into a form involving only the positions i where the component values in a word $\underline{x} = (x_1, x_2, \cdots, x_n) \in \mathcal{S}(n,k)$ change sign, that is $x_{i+1} = -x_i$. We shall denote these positions by the *sign-change list* $\tau = \{\tau_1, \tau_2, \cdots, \tau_l\}$, where $0 < \tau_1 < \tau_2 < \cdots < \tau_l < n$.

Let $f_k(n)$ denote the sum of kth powers of consecutive integers,

$$f_k(n) = \sum_{j=1}^{n} j^k.$$

It is well-known [16, p. 499] that $f_k(n)$ is an integer polynomial of degree $k+1$. Specifically,

$$f_k(n) = \frac{n^{k+1}}{k+1} + \frac{n^k}{2} + B_1\frac{kn^{k-1}}{2!} + B_2\frac{k(k-1)(k-2)n^{k-3}}{4!} + \cdots$$

where B_i is the ith Bernoulli number [16, p. 615], and the series terminates at the n^2 term if k is odd, or the n term if k is even. For example, since $B_1 = 1/6$ and $B_2 = -1/30$, we have

$$f_1(n) = \frac{n^2}{2} + \frac{n}{2} = \frac{n(n+1)}{2}$$

$$f_2(n) = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} = \frac{n(n+1)(2n+1)}{6}$$

$$f_3(n) = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4} = \frac{n^2(n+1)^2}{4}$$

$$f_4(n) = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30} = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

For a word $\underline{x}$ with sign-change positions $\{\tau_1, \tau_2, \cdots, \tau_l\}$, we can rewrite the moments $m_k(\underline{x}) = \sum_{j=1}^{n} j^k x_j$ in the form

$$m_k(\underline{x}) = \operatorname{sgn}(x_1)\big[f_k(\tau_1) - [f_k(\tau_2) - f_k(\tau_1)] + \cdots + (-1)^l[f_k(n) - f_k(\tau_l)]\big]$$

for all $k \ge 0$. This clearly reduces to

$$m_k(\underline{x}) = \operatorname{sgn}(x_1)\big[2f_k(\tau_1) - 2f_k(\tau_2) + \cdots + (-1)^{l-1}2f_k(\tau_l) + (-1)^l f_k(n)\big]. \quad (15)$$

When $\underline{x} \in \mathcal{S}(n,k)$, the expression above translates the vanishing moment conditions of (6) into simple conditions on the sign-change positions, as shown in the following lemma.

Lemma 3.1: Let $\underline{x}$ be a word over Φ with sign-change list $\tau = \{\tau_1, \tau_2, \cdots, \tau_l\}$. Then,

(a) The word $\underline{x}$ is in $\mathcal{S}(n,k)$ if and only if

$$(-1)^l n^{i+1} + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^{i+1} = 0 \qquad \text{for } i = 0, 1, \cdots, k-1.$$

(b) If $\underline{x} \in \mathcal{S}(n,k)$ then

$$m_k(\underline{x}) = \frac{\operatorname{sgn}(x_1)}{k+1}\left((-1)^l n^{k+1} + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^{k+1}\right).$$

Proof: We proceed by induction on k. Part (a) is vacuous when $k = 0$, while part (b) follows from (15) with $f_0(n) = n$. That is,

$$m_0(\underline{x}) = \operatorname{sgn}(x_1)\left[2\tau_1 - 2\tau_2 + \cdots + (-1)^{l-1}\tau_l + (-1)^l n\right].$$

This establishes the induction base.

Now assume that the lemma holds for $k - 1$. By part (a) we have that $\underline{x} \in \mathscr{S}(n, k-1)$ if and only if

$$(-1)^l n^{i+1} + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^{i+1} = 0 \quad \text{for all } i = 0, 1, \cdots, k-2. \tag{16}$$

Part (b) implies that for $\underline{x} \in \mathscr{S}(n, k-1)$ we have

$$m_{k-1}(\underline{x}) = \frac{\operatorname{sgn}(x_1)}{k}\left((-1)^l n^k + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^k\right). \tag{17}$$

Clearly, $\underline{x} \in \mathscr{S}(n,k)$ if and only if the following two conditions both hold: $\underline{x} \in \mathscr{S}(n, k-1)$ and $m_{k-1}(\underline{x}) = 0$. While the former condition is given by (16), the latter condition is equivalent to

$$(-1)^l n^k + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^k = 0$$

in view of (17). This completes the proof of part (a) of the lemma, and we now proceed with the proof of part (b). Write the polynomials $f_k(n)$ in the form (recall that these polynomials do not have a constant term):

$$f_k(n) = \sum_{i=0}^{k} f_{k,i} n^{i+1}$$

and rewrite the moment $m_k(\underline{x})$ as

$$m_k(\underline{x}) = \operatorname{sgn}(x_1)\left(2\sum_{i=0}^{k} f_{k,i}\tau_1^{i+1} + \cdots + (-1)^{l-1}2\sum_{i=0}^{k} f_{k,i}\tau_l^{i+1} + (-1)^l\sum_{i=0}^{k} f_{k,i}n^{i+1}\right).$$

Grouping terms of equal degree, we find

$$m_k(\underline{x}) = \operatorname{sgn}(x_1) \cdot \sum_{i=0}^{k} f_{k,i}\left((-1)^l n^{i+1} + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^{i+1}\right).$$

Now suppose that $\underline{x}$ is in $\mathscr{S}(n,k)$. By part (a), which has been already established above, the sums corresponding to $i \le k-1$ are all zero. Since $f_{k,k} = 1/(k+1)$, we conclude

$$m_k(\underline{x}) = \frac{\operatorname{sgn}(x_1)}{k+1}\left((-1)^l n^{k+1} + 2\sum_{j=1}^{l}(-1)^{j-1}\tau_j^{k+1}\right)$$

completing the induction step and the proof of the lemma. □

For small values of the null order k, the conditions on the sign-change positions in parts (a) and (b) of Lemma 3.1 may be used to determine elements $\underline{x} \in \mathscr{S}(n,k)$, as well as to find bounds on the first nonzero moment $m_k(\underline{x})$ for such $\underline{x}$.

For example, when $k = 1$ we have

$$2\tau_1 - 2\tau_2 + \cdots + (-1)^{l-1}2\tau_l + (-1)^l n = 0$$

implying that $\tau_1 \le n/2$. That is, the first sign change occurs not after the halfway point. Consequently, for any $\underline{x} \in \mathscr{S}(n,1)$, we have the bound

$$|m_1(\underline{x})| \le \frac{1}{2}\left(n^2 - 2\left(\frac{n}{2}\right)^2\right) = \frac{n^2}{4}. \tag{18}$$

We recall that a word with a kth order null must have at least k sign changes [15]. If we restrict attention to words in $\mathscr{S}(n,1)$ with precisely one sign change, the conditions of Lemma 3.1 produce the unique solution $\tau = \{n/2\}$, which attains both the lower bound on the number of sign changes and the upper bound (18) on $m_1(\underline{x})$.

For $k = 2$, we may solve for a word $\underline{x} \in \mathscr{S}(n,2)$ having exactly two sign changes. The conditions are

$$2\tau_1 - 2\tau_2 + n = 0$$

$$2\tau_1^2 - 2\tau_2^2 + n^2 = 0.$$

From these equations we easily derive $\tau = \{n/4, 3n/4\}$, which leads to

$$m_2(\underline{x}) = \frac{n^3}{16}$$

if we assume $x_1 = +1$. Note that if $\underline{y} \in \mathscr{S}(n,2)$ has more than two sign changes, then $m_2(\underline{y}) \le m_2(\underline{x})$. This follows from the observation that there must exist sign change positions $i < j$ such that $y_i = -1$ and $y_j = +1$. If we transpose the symbols y_i and y_{i+1}, and then transpose the symbols y_j and y_{j+1}, it is easily checked that the resulting word $\underline{y}'$ is again in $\mathscr{S}(n,2)$ and $m_2(\underline{y}') > m_2(\underline{y})$. Clearly, this procedure terminates when $\underline{y}'$ has only two sign changes. Hence the solution $\tau = \{n/4, 3n/4\}$ again achieves both the lower bound on the number of sign changes and the upper bound on $m_2(\underline{x})$. Note that the two solutions, $\{n/2\} \in \mathscr{S}(n,1)$ and $\{n/4, 3n/4\} \in \mathscr{S}(n,2)$, correspond to the Kronecker product of the word $(+ + \cdots + +)$ of appropriate length with the Morse sequences $\mu(1) \in \mathscr{S}(2,1)$ and $\mu(2) \in \mathscr{S}(4,2)$, respectively.

Application of Lemma 3.1 to the case $k = 3$ shows that the lower bound of k on the number of sign changes is not always tight. In particular, after some straightforward algebra, the conditions on sign change positions in part (a) of Lemma 3.1 reduce to the equation

$$8\tau_1^2 n^2 - 8\tau_1 n^3 + n^4 = 0.$$

The first sign change position τ_1 must be of the form αn, for some rational number α. The condition that α must therefore satisfy is

$$8\alpha^2 - 8\alpha + 1 = 0.$$

This quadratic equation has the two solutions

$$\alpha = \frac{2 \pm \sqrt{2}}{4}$$

neither of which is rational. It follows that there is no element of $\mathscr{S}(n,3)$ with only three sign changes.

Knowing that the Morse sequence $\mu(3) \in \mathscr{S}(8,3)$ has five sign changes, one might naturally inquire if five sign changes is the minimum number among the words with a null of order 3. If we assume that a word with four sign change positions $0 < \tau_1 < \tau_2 < \tau_3 < \tau_4 < n$ has a third-order null, and proceed as before, we obtain the following relations expressing τ_2, τ_3, and τ_4 in terms of τ_1:

$$\tau_2 = \alpha + \beta + \gamma$$

$$\tau_3 = \alpha + 2\beta$$

$$\tau_4 = \alpha + \beta - \gamma$$

where

$$\alpha = \frac{n + 2\tau_1}{2} \qquad \beta = \frac{2\tau_1^2}{n - 4\tau_1}$$

$$\gamma = \frac{\left(8(n - 4\tau_1)^3 n + (4\tau_1)^4\right)^{1/2}}{8(n - 4\tau_1)}.$$

This implies that $\tau_1 < n/4$, or else τ_3 would not be strictly in between τ_2 and τ_4. Further, to show that we cannot have a third-order spectral-null word with four sign changes it would suffice to show that γ is irrational whenever $0 < \tau_1 < n/4$. Write $p/q = 4\tau_1/n$, where $\gcd(p,q) = 1$. Then γ is irrational if and only if the following equation

$$p^4 + 8q(q-p)^3 = r^2 \tag{19}$$

does not have integer solutions in the range $0 < p < q$. The proof that (19) has indeed no integer solutions is rather elaborate, and is therefore deferred to Lemma A.1 in the Appendix. The foregoing discussion in conjunction with Lemma A.1 implies that five sign changes are indeed necessary for a binary word with a third-order null.

IV. An Encoder for Second-Order Spectral-Null Codes

While the previous two sections are devoted to the study of various properties of $\mathscr{S}(n,k)$, in this and the next section we present explicit constructions of encoders into subsets of $\mathscr{S}(n,k)$—viz. spectral-null codes of order k. We start with an encoding scheme for second-order spectral-null codes. In the next section we present an alternative encoding scheme, which extends to spectral-null codes of any fixed order.

One way of encoding an arbitrary word $\underline{y} = (y_1, y_2 \cdots, y_m)$ of length $m = n - \lceil \rho(\mathscr{S}(n,k)) \rceil$ over the alphabet $F = \{0,1\}$ into a word $\underline{x} \in \mathscr{S}(n,k)$ is by enumerative coding. For instance, assume that all the elements of $\mathscr{S}(n,k)$ have been arranged in lexicographic order, and a 1-1 map $b: F^m \to \{0, 1, \cdots 2^m - 1\}$ has been established, say $b(\underline{y}) = \sum_{i=1}^m y_i 2^{i-1}$. Then the enumerative encoder, presented with the word $\underline{y}$, encodes $\underline{y}$ into $\underline{x} \in \mathscr{S}(n,k)$ whose rank in the lexicographic ordering is equal to $b(\underline{y})$. In particular, such an enumerative encoder for $\mathscr{S}(n,2)$ was proposed in [12].

We note that the enumerative encoding technique can be, in principle, extended for $k \geq 2$. This, however, would require precomputing and storing a prohibitively large amount of information. For an integer vector $\underline{a} = (a_0, a_1, \cdots, a_{k-1}) \in \mathbb{Z}^k$ let

$$\mathscr{S}(n,k;\underline{a}) = \left\{\underline{x} \in \Phi^n : H(n,k)\underline{x}^t = \underline{a}\right\}.$$

Then the enumerative encoding algorithm requires the knowledge of the (nonzero) values of $|\mathscr{S}(l,k;\underline{a})|$ for all $\underline{a} \in \mathbb{Z}^k$ and all $l = 1, 2, \cdots, n$. These values may be precomputed using dynamic programming. However, for any fixed k, the ith entry a_i of $\underline{a}$ in $\mathscr{S}(l,k;\underline{a})$ may range over $\Theta(l^{i+1})$ values.[1] Hence, for each l we may end up with $\Theta(l^{k(k+1)/2})$ nonzero values $|\mathscr{S}(l,k;\underline{a})|$, and therefore the number of nonzero values we would need to compute and store in this way is $\Theta(n^{k(k+1)/2+1})$. This makes the enumerative method quite impractical even for small values of k.

In this section we concentrate on the case $k = 2$. The enumerative coding technique we have just outlined will require us to precompute and store $\Theta(n^4)$ values of $|\mathscr{S}(l,2;\underline{a})|$, and the redundancy of the encoded set of words of $\mathscr{S}(n,2)$ thus obtained is $\Theta(\log n)$. We now present an alternative encoding algorithm for $k = 2$ that requires $O(n \log n)$ bit operations for encoding, without any precomputation, and whose resulting redundancy is still $\Theta(\log n)$. In a way, this algorithm may be regarded as a generalization of one of the algorithms in Knuth's paper [18] for the case $k = 2$.

Let n be a positive integer and let m be the smallest integer such that $n + m + 1 \leq 2^m$. We further assume that $n + m + 1$ is divisible by 4, or else we may increase n by at most 3 to meet this condition. Thus, let h be the even integer $(m + n + 1)/2$. We now show how to encode an arbitrary word $\underline{y}$ in Φ^n into a word of $\mathscr{S}(2h,2)$.

As a first phase, we encode $\underline{y}$ into a word $\underline{x} = (x_{-h} x_{-h+1} \cdots x_0 x_1 \cdots x_{h-1})$ over Φ, which satisfies the equation $\sigma_1(\underline{x}) \overset{\text{def}}{=} \sum_{j=-h}^{h-1} j x_j = 0$. Note that $\sigma_1(\underline{x})$ is essentially the first moment of $\underline{x}$ with respect to the matrix $H(2h, 2; -(h+1))$. The encoding procedure may be specified as follows.

Phase A—Balancing $\sigma_1(\underline{x})$:

Step A1: Assign the entries of $\underline{y}$ to the entries x_j, where j ranges over all integers between $-h$ and $h - 1$

[1] Here, $\Theta(f(n))$ denotes a function in n that is bounded from below and above by $c_1 \cdot f(n)$ and $c_2 \cdot f(n)$, respectively, for some constants c_1 and c_2 independent of n.

that are not equal to $-1, 0, 1, 2, 4, \cdots, 2^{m-2}$. For the time being, set the $m+1$ unassigned entries of x_j to zero.

Step A2: For increasing values of $l = -h, -h+1, \cdots,$ flip the sign of x_l. Let $\sigma_1(\underline{x}; l)$ denote the value of $\sigma_1(\underline{x})$ just prior to flipping the sign of x_l. Proceed until the absolute value of $\sigma_1(\underline{x}; l)$ is not greater than h, and let l_0 denote the (smallest) index l for which this condition is met. Set $l_0 = h$ if the whole word $\underline{x}$ was negated.

Step A3: For $j = -1, 1, 2, 4, \cdots, 2^{m-2}$ set the entries x_j to $+1$ or -1 so that the resulting overall sum $\sigma_1(\underline{x}) = \sum_{j=-h}^{h-1} j x_j$ is zero.

We point out that the value of x_0 has not been set in the above procedure, neither does its value affect $\sigma_1(\underline{x}) = \sum_{j=-h}^{h-1} j x_j$.

We now show that the foregoing algorithm will always find an index $l < h$ for which $|\sigma_1(\underline{x}; l)| \le h$. Indeed, flipping the signs of *every* entry in $\underline{x}$ negates $\sigma_1(\underline{x})$ with respect to its initial value, that is $\sigma_1(\underline{x}; h) = -\sigma_1(\underline{x}; -h)$. Thus, there exists an l such that $\sigma_1(\underline{x}; l) \cdot \sigma_1(\underline{x}; l+1) \le 0$. Furthermore, $|\sigma_1(\underline{x}; l+1) - \sigma_1(\underline{x}; l)| \le 2h$ for all $l = -h, -h+1, \cdots, h-1$. Hence, we must reach in step A2 an index l_0 for which $|\sigma_1(\underline{x}; l_0)| \le h$.

Next, we show how to compute the entries x_j for $j = -1, 1, 2, 4, \cdots, 2^{m-2}$ in step A3 of the algorithm. Denote $S = \sigma_1(\underline{x}; l_0)$. First note that the value of $\sigma_1(\underline{x}; l)$ is always even. This is due to the fact that $j(x_j - x_{-j})$ is even for every $0 < j < h$, and so is $-h x_{-h}$. It remains to prove that every even integer S in the range $-2^{m-1} \le S \le 2^{m-1}$ can be written in the form

$$S = -x_{-1} + \sum_{s=0}^{m-2} x_{2^s} 2^s$$

where $x_{-1}, x_1, x_2, \cdots, x_{2^{m-2}} \in \Phi$.

Without loss of generality assume that S is nonnegative, or else apply the following argument to $-S$. The binary expansion of an odd integer $S + 2^{m-1} - 1$ may be written as

$$S + 2^{m-1} - 1 = 1 + \sum_{s=0}^{m-2} b_s 2^{s+1}$$

where $b_s \in \{0, 1\}$ for $s = 0, 1, \cdots, m-2$. Substituting $2^{m-1} - 1 = \sum_{s=0}^{m-2} 2^s$ in the expression above, we obtain

$$S = 1 + \sum_{s=0}^{m-2} (2b_s - 1) 2^s.$$

Hence we set $x_{-1} = +1$ and $x_{2^s} = 1 - 2b_s$ for $s = 0, 1, \cdots, m-2$.

Having encoded $\underline{y}$ into a word $\underline{x}$ that satisfies the condition $\sigma_1(\underline{x}) = 0$, we now apply the second phase of the algorithm that ensures that $\sigma_0(\underline{x}) \stackrel{\text{def}}{=} \sum_{j=-h}^{h-1} x_j = 0$.

Phase B—Balancing $\sigma_0(\underline{x})$:

Step B1: Call an index i qualifying if $x_i = x_{-i}$. For increasing values of qualifying indices $i \ge 1$ flip the signs of both x_i and x_{-i}, and let $\sigma_0(\underline{x}; i)$ denote the value of $\sigma_0(\underline{x})$ just prior to flipping x_i and x_{-i}. Proceed until $|\sigma_0(\underline{x}; i)| = 1$, and let i_0 denote the (smallest) index i for which this condition is met.

Step B2: If $\sigma_0(\underline{x}; i_0) = +1$ set $x_0 = -1$. Otherwise, set $x_0 = +1$.

To verify that the condition of step B1 is indeed met for some $i < h$, notice that $\sigma_0(\underline{x}; i)$ is odd for every qualifying index i and, at each sign flip, the value of $\sigma_0(\underline{x}; i)$ may either increase or decrease by 4, or otherwise remain unchanged. Flipping the signs of x_i and x_{-i} for all qualifying indices i in the range $1 \le i < h$ will result in negating the initial value of $\sigma_0(\underline{x})$. Hence the condition of step B1 must be met for some $i < h$.

Note that Phase B of our algorithm essentially consists of one of the algorithms in Knuth's paper [18], applied only to those positions in $\underline{x}$ where the two (reflected) halves of $\underline{x}$ agree. Such a process guarantees that the value of $\sigma_1(\underline{x})$ will not be affected by the sign flippings performed in Phase B. Thus, at the output of Phase B we have a word $\underline{x} \in \Phi^{2h}$ such that $\sigma_0(\underline{x}) = \sigma_1(\underline{x}) = 0$. By Lemma 2.2 it therefore follows that $\underline{x} \in \mathscr{S}(2h, 2)$.

The final phase of our algorithm may be specified recursively as follows.

Phase C—Encoding the Indices:

Step C1: Apply Phase A and Phase B recursively to the binary representations of $l_0 + h$ and i_0 that were computed in steps A2 and B1, respectively. Concatenate the resulting word with $\underline{x}$ as the final output of the encoder.

Example: Assume that $n = 26$, in which case $m = 5$ and $h = 16$. Assume also that the word $\underline{y} \in \Phi^{26}$ to be encoded is given by

$$\underline{y} = (- - - - + + + + - - - - - + + + - - \quad + - - - + + + +).$$

After step A1 we have

$$\underline{x} = (- - - - + + + + - - - - - + + 0 0 0 0 \quad + 0 - - + 0 - - - + + + +)$$

with $\sigma_1(\underline{x}) = 64$. Applying the procedure of step A2 yields $l_0 = -14$ and we have

$$\underline{x} = (+ + - - + + + + - - - - - + + 0 0 0 0 \quad + 0 - - + 0 - - - + + + +)$$

with $S = \sigma_1(\underline{x}; -14) = 2 \le 16$. The binary representation of the integer $S + 2^4 - 1 = 17$ is given by $1 + 2^4$. Hence $(b_0, b_1, b_2, b_3) = (0, 0, 0, 1)$, and after step A3 we have

$$\underline{x} = (+ + - - + + + + - - - - - + + + 0 \quad + + + + - - + - - - - + + + +)$$

with $\sigma_1(\underline{x}) = 0$ as desired. Now $\sigma_0(\underline{x}) = 5$. Applying step B1 yields $i_0 = 2$ with

$$\underline{x} = (+ + - - + + + + - - - - - + + - 0 \quad - + + + - - + - - - - + + + +)$$

and $\sigma_0(\underline{x};2) = 1$. Thus at step B2 we set $x_0 = -1$, which produces the final encoded word

$$\underline{x} = (+ + - - + + + + - - - - - - + + - - - + + + - - + - - - - - + + + + +)$$

with $\underline{x} \in \mathscr{S}(32, 2)$. The binary representations of $l_0 + h = 2$ and $i_0 = 2$ are now encoded recursively and appended to $\underline{x}$.

It is clear from the foregoing description that, presented with an arbitrary word $\underline{y}$ of length n, our algorithm will encode $\underline{y}$ into a second-order spectral-null word of length $n + 3m + O(\log m)$, where m is the smallest integer such that $n + m - 1 \leq 2^m$. Obviously $m = O(\log n)$. Hence the redundancy of the second-order spectral-null code $\mathscr{C}$ that is the image of the proposed encoder is given by $\rho(\mathscr{C}) = 3\log_2 n + O(\log\log n)$.

V. A General Encoding Scheme

In this section we present a recursive encoding scheme for mapping arbitrary sequences over Φ into spectral-null words of order k, for any fixed value of k. We start in Section V-A with the description of this encoding scheme for the special case $k = 2$, which illustrates the basic ideas involved in our construction. The resulting second-order spectral-null codes have higher redundancy than the codes introduced in Section IV. However, unlike the construction of Section IV, the construction of Section V-A naturally extend to values of k greater than two. We first prove in Section V-B that $m_k(\underline{x})$ is divisible by $k!$ for any $\underline{x} \in \mathscr{S}(n, k)$ and, furthermore, that $m_k(\underline{x})$ is divisible by $2k!$ if $\mathscr{S}(n, k + 1) \neq \varnothing$. Then we show how to construct a word $\underline{y} \in \mathscr{S}(k)$ such that $m_k(\underline{y})$ is any prescribed even multiple of $k!$. These results are employed in Section V-C to present a recursive construction of spectral-null codes of order k, for any fixed k. Furthermore it is shown in Section V-C that the rate of these codes approaches $\mathbf{cap}(\mathscr{S}(k)) = 1$ as their length goes to infinity.

We point out that while the encoding scheme described herein is fairly simple to implement for the first few values of k (say, $k \leq 4$), it becomes impractical as the order of the null increases. Thus, for large values of k our encoder is best regarded as yet another way to prove that $\mathbf{cap}(\mathscr{S}(k)) = 1$. Such a proof differs from the existence result of Theorem 2.7, in the sense that it provides an explicit encoder from Φ^n into $\mathscr{S}(k)$ that achieves the capacity. Unlike the enumerative encoding scheme, the proposed encoder features complexity that is polynomial in both n and k (although n has to tend to infinity nonuniformly with respect to k in order for the rate to approach unity).

A. An Alternative Encoder for Second-Order Spectral-Null Codes

Let $\underline{v}$ be the word over Φ which is to be encoded into $\mathscr{S}(2)$, and further assume that the length of $\underline{v}$ is $n = n_1 n_2$, where n_1 is odd. We first partition this word as $\underline{v} = (\underline{v}_1 \mid \underline{v}_2 \mid \cdots \mid \underline{v}_{n_2})$, where $\underline{v}_1, \underline{v}_2 \cdots, \underline{v}_{n_2} \in \Phi^{n_1}$, and then extend each $\underline{v}_i$ by an extra coordinate fixed at $+1$ to obtain $\underline{v}_i' = (+ \mid \underline{v}_i)$ of length $n_1 + 1$. Subsequently, each $\underline{v}_i'$ is encoded into a word $\underline{x}_i \in \mathscr{S}(n_1 + 1 + r, 1)$, such that the first position in each $\underline{x}_i$ remains $+1$. This may be accomplished in a number of ways. To be specific, we assume that one of the algorithms of Knuth [18] is employed, in which case $\underline{x}_i = (\underline{v}_i' \cdot \underline{u}_j | \underline{a}_j)$, where $\cdot$ stands for bit-by-bit multiplication,

$$\underline{u}_j = \Big(\underbrace{+ + + \cdots + + +}_{j}\overbrace{- - - \cdots - - -}^{n_1 + 1 - j}\Big)$$

for some index j such that $\underline{v}_i' \cdot \underline{u}_j \in \mathscr{S}(n_1 + 1, 1)$, and $\underline{a}_j \in \mathscr{S}(r, 1)$ is a representation of j. Note that in this case, $r = \log_2 n_1 + O(1)$.

Now set $\underline{y}_1 = \underline{x}_1$. For $i = 2, 3, \cdots, n_2$ define the word $\underline{y}_i$ as follows:

$$\underline{y}_i = \begin{cases} (\underline{y}_{i-1} | \underline{x}_i) & \text{if } m_1(\underline{y}_{i-1}) \cdot m_1(\underline{x}_i) \leq 0 \\ (\underline{y}_{i-1} | -\underline{x}_i) & \text{if } m_1(\underline{y}_{i-1}) \cdot m_1(\underline{x}_i) > 0 \end{cases}. \quad (20)$$

Thus $\underline{y}_{n_2}$ is essentially a concatenation of the words $\underline{x}_1, \underline{x}_2, \cdots, \underline{x}_{n_2}$, with some of these words being negated. The first position in each such word indicates whether it has been negated or not. Note that the first position in $\underline{y}_{n_2}$ remains fixed at $+1$. Clearly $m_0(\underline{y}_{n_2}) = 0$. It is also clear from Lemma 2.2 that

$$m_1(\underline{y}_{n_2}) = m_1(\underline{x}_1) \pm m_1(\underline{x}_2) \pm \cdots \pm m_1(\underline{x}_{n_2}). \quad (21)$$

Furthermore, the simple polarity inversion technique of (20) ensures that the terms in (21) always add up in such a way that $|m_1(\underline{y}_{n_2})| \leq \max_{1 \leq i \leq n_2} |m_1(\underline{x}_i)| \leq (n_1 + 1 + r)^2/4$, where the second equality follows by (18). We shall assume that $n_1 + 1 + r \equiv 0 \pmod 4$, in which case $m_1(\underline{y}_{n_2})$ must be even. In order to complete the encoding we need a word $\underline{w} \in \mathscr{S}(1)$ with $m_1(\underline{w}) = -m_1(\underline{y}_{n_2})$. Such a word always exists, and has length at most $(n_1 + 1 + r)$ as is shown in the following lemma.

Lemma 5.1: Let $n \equiv 0 \pmod 4$. Then for any even integer t with $|t| \leq n^2/4$, there exists a word $\underline{w} \in \mathscr{S}(n, 1)$ with $m_1(\underline{w}) = t$.

Proof: Let $\underline{w} = (w_1, w_2, \cdots, w_n)$ and assume that either $(- +)$ or $(+ -)$ is contained in $\underline{w}$ at position j. We may then define $F_j\underline{w} = (w_1, w_2, \cdots, -w_j, -w_{j+1} \cdots w_n)$, where the effect of the flip operator F_j amounts to interchanging the positions of $+$ and $-$ in the coordinates j and $j + 1$. Now set $\underline{w}_0 = (- - \cdots - - + + \cdots + +) \in \mathscr{S}(n, 1)$. Clearly $m_0(\underline{w}_0) = 0$, $m_1(\underline{w}_0) = n^2/4$, and $(- +)$ is contained in $\underline{w}_0$ at position $n/2$. For $i = 1, 2, \cdots, n^2/4$ define $\underline{w}_i = F_j \underline{w}_{i-1}$, where j is the smallest index such that $(- +)$ is contained in $\underline{w}_{i-1}$ at position j. It is easy to see that as i varies from 0 to $n^2/4$, the first moment of $\underline{w}_i$ takes on all the even values in the range $+n^2/4$ to $-n^2/4$. □

Using the algorithm of Lemma 5.1, we can readily construct a word $\underline{w} \in \mathscr{S}(n_1 + 1 + r, 1)$ with

$m_1(\underline{w}) = -m_1(\underline{y}_{n_2})$. The output of the encoder then consists of the word $\underline{y} = (\underline{y}_{n_2}|\underline{w})$, which clearly satisfies $m_0(\underline{y}) = m_1(\underline{y}) = 0$.

Let $R(\mathscr{C})$ denote the rate of the second-order spectral-null code $\mathscr{C}$ consisting of all the words of length $(n_2+1)(n_1+r+1)$ obtained using this construction. Then obviously,

$$R(\mathscr{C}) = \frac{\log_2|\mathscr{C}|}{(n_2+1)(n_1+r+1)} = \frac{n_1 n_2}{(n_2+1)(n_1+r+1)}.$$

Since r approaches $\log n_1$ as $n_1 \to \infty$, it is easy to see that $\lim_{n_1,n_2\to\infty} R(\mathscr{C}) = 1$. We note that the optimal choice of parameters n_1, n_2 in this case is $n_2 = n_1/\log n_1$, which yields $\rho(\mathscr{C}) = O(\sqrt{n \log n})$.

B. Construction of the Balancing Sequence

It is evident that in order to extend the construction of the previous section beyond $k = 2$, we need the analogue of Lemma 5.1 for arbitrary values of $k > 2$. More specifically, let $\underline{x}_1, \underline{x}_2, \cdots, \underline{x}_s \in \mathscr{S}(n,k)$ and let $S = m_k(\underline{x}_1) \pm m_k(\underline{x}_2) \pm \cdots \pm m_k(\underline{x}_s)$ with $|S| \le \max_{1\le i\le s}|m_k(\underline{x}_i)|$. Then we have to be able to construct a word $\underline{w} \in \mathscr{S}(k)$, whose length *does not depend* on s, such that $m_k(\underline{w}) = S$. To this end we proceed as follows. First we show that $k!|S$. Furthermore, if $\mathscr{S}(ns, k+1) \ne \varnothing$ then $2k!|S$. Then we show how to construct a word $\underline{w} \in \mathscr{S}(k)$, such that $m_k(\underline{w})$ is any prescribed multiple of $2k!$.

Lemma 5.2: Let $\underline{x} \in \mathscr{S}(n,k)$. Then $m_k(\underline{x})$ is divisible by $k!$.

Proof: Let $D(n, k+1)$ be the "systematic" parity-check matrix for $\mathscr{S}(n, k+1)$ as in Lemma 2.3 and let $B(k+1)$ be the inverse of $H(k+1, k+1)$, as defined in Lemma 2.3. Also, for any $\underline{x} \in \Phi^n$ let $\underline{s}(\underline{x}) = (s_0(\underline{x}), s_1(\underline{x}), \cdots, s_k(\underline{x}))^t \stackrel{\text{def}}{=} D(n, k+1)\underline{x}^t$. Now, if $\underline{x} \in \mathscr{S}(n,k)$ then obviously $H(n, k+1)\underline{x}^t = (0, 0, \cdots, 0, m_k(\underline{x}))^t$. Hence we have

$$\begin{aligned}\underline{s}(\underline{x}) &= D(n,k+1)\underline{x}^t = B(k+1)H(n,k+1)\underline{x}^t \\ &= B(k+1)(0,0,\cdots,0,m_k(\underline{x}))^t.\end{aligned}$$

Thus, $s_k(\underline{x}) = b_{k,k} m_k(\underline{x}) = m_k(\underline{x})/k!$ where the second equality follows from (7). Yet, it was shown in Lemma 2.3 that $D(n, k+1)$ is an integer matrix and, hence, $s_k(\underline{x})$ must be an integer. It follows that $k!$ divides $m_k(\underline{x})$ for all $\underline{x} \in \mathscr{S}(n,k)$. □

Lemma 5.3: If $\mathscr{S}(n, k+1) \ne \varnothing$, then $m_k(\underline{x})$ is divisible by $2k!$ for all $\underline{x} \in \mathscr{S}(n,k)$.

Proof: As we have seen, if $\underline{x} \in \mathscr{S}(n,k)$ then $s_k(\underline{x}) = m_k(\underline{x})/k!$. On the other hand, $s_k(\underline{y}) = 0$ for any $\underline{y} \in \mathscr{S}(n, k+1)$. Since $\underline{x} \equiv \underline{y} \pmod 2$ for all $\underline{x}, \underline{y} \in \Phi^n$ it follows that $s_k(\underline{x}) \equiv s_k(\underline{y}) \equiv 0 \pmod 2$, provided $\mathscr{S}(n, k+1) \ne \varnothing$. In other words, $m_k(\underline{x})/k! = s_k(\underline{x}) \equiv 0 \pmod 2$, and therefore $2k!$ must divide $m_k(\underline{x})$. □

We point out that there are examples of words $\underline{x} \in \mathscr{S}(n,k)$ such that $m_k(\underline{x})$ is divisible by $k!$ but not by $2k!$, where by Lemma 5.3 we must have $\mathscr{S}(n, k+1) = \varnothing$. One such example is the word $\overline{\mu(1)} = (-+) \in \mathscr{S}(2,1)$ with $m_1(\overline{\mu(1)}) = 1$. For a less trivial example, take the word $\underline{x} \in \mathscr{S}(20,3)$ with $m_3(\underline{x}) = 6$, obtained by concatenating $+--+-+-+++$ with the complement of its reflection. Similar examples exist for $k = 3$ and $n = 28$. In general, however, it can be verified by induction on k that $m_k(\mu(k)) = (-1)^k 2^{k(k-1)/2} k!$ and, hence, $m_k(\mu(k))$ is divisible by $2k!$ for all $k > 1$. In fact, for $k > 3$, we do not know of any word $\underline{x} \in \mathscr{S}(n,k)$ for which $m_k(\underline{x})$ is an odd multiple of $k!$. On the other hand, it is relatively easy to construct a series of *ternary* words $\underline{u}_1, \underline{u}_2, \cdots, \underline{u}_k$, over the alphabet $\{-1, 0, 1\}$, such that $m_i(\underline{u}_k) = 0$ for all $i = 0, 1, \cdots, k-1$ and $m_k(\underline{u}_k)$ is an odd multiple of $k!$ for all $k > 1$. Set $\underline{u}_1 = (-+)$ and for $k = 1, 2, \cdots,$ define

$$\underline{u}_{k+1} = \begin{cases} (\underline{u}_k \mid -\underline{u}_k) & k \equiv 0 \bmod 2 \\ (\underline{u}_k \mid 0 \mid -\underline{u}_k) & k \equiv 1 \bmod 2 \end{cases}. \tag{22}$$

Using Lemma 2.2, it is easy to see that $m_i(\underline{u}_k) = 0$ for all $i = 0, 1, \cdots, k-1$ and

$$m_k(\underline{u}_k) = -k \cdot \left(\ell(\underline{u}_{k-1}) + \frac{1-(-1)^k}{2}\right) \cdot m_{k-1}(\underline{u}_{k-1}) \tag{23}$$

where $\ell(\underline{u}_k)$ is the length of $\underline{u}_k$. Furthermore, we have

$$\ell(\underline{u}_k) = \frac{4\cdot 2^k + (-1)^{k+1}}{3} + \frac{1-(-1)^k}{2}. \tag{24}$$

Substituting this into (23) and solving the recursion, we obtain

$$m_k(\underline{u}_k) = k! \cdot \prod_{i=1}^{k-1}\left[\frac{(-1)^i - 4\cdot 2^i}{3}\right] \stackrel{\text{def}}{=} k! \cdot W(k) \tag{25}$$

the empty product being 1 by convention. It is easy to see that $m_k(\underline{u}_k)$ is indeed an odd multiple of $k!$.

We now employ the series of ternary words $\underline{u}_1, \underline{u}_2, \cdots, \underline{u}_k$ in order to construct a series of (binary) words $\underline{w}_1, \underline{w}_2, \cdots, \underline{w}_k$, such that $\underline{w}_k \in \mathscr{S}(k)$ and $m_k(\underline{w}) = 2k!$.

Lemma 5.4: For any $k \ge 1$, there exists a word $\underline{w}_k \in \mathscr{S}(k)$ with $m_k(\underline{w}_k) = 2k!$.

Proof: For $k = 1, 2$ the lemma follows by considering $\underline{w}_1 = (-+-+) \in \mathscr{S}(4,1)$ and $\underline{w}_2 = (+--+) \in \mathscr{S}(4,2)$. As an induction hypothesis, assume the existence of a word $\underline{w}_{k-1} \in \mathscr{S}(k-1)$ such that $m_{k-1}(\underline{w}_{k-1}) = 2(k-1)!$. We now construct the following ternary word

$$\underline{v} = \left(\cdots \underset{\substack{\uparrow \\ j_1}}{\underline{u}_{k-1}} \cdots \underset{\substack{\uparrow \\ j_2}}{-\underline{u}_{k-1}} \cdots \underset{\substack{\uparrow \\ j_3}}{-\underline{w}_{k-1}} \cdots \underset{\substack{\uparrow \\ j_4}}{\underline{w}_{k-1}} \cdots\right)$$

meaning that $\underline{u}_{k-1}$ and $-\underline{u}_{k-1}$, given by (22), are contained in $\underline{v}$ starting at positions j_1 and j_2, while $-\underline{w}_{k-1}$ and $\underline{w}_{k-1}$ are contained in $\underline{v}$ starting at positions j_3 and j_4. Let $\underline{e}$ be an arbitrary ternary word, such that $e_i = 0$ if and only if $v_i \ne 0$. Note that $\pm\underline{v} + \underline{e}$ are both words over Φ. Hence by Lemma 2.5 there exists a word $\underline{y} \in \mathscr{S}(k)$ such that $\underline{v} + \underline{e}$ is a prefix of $\underline{y}$. Consider the binary word

$\underline{w}$ of length $\ell(\underline{w}) = \ell(\underline{y})$ obtained from $\underline{y}$ by changing the prefix $\underline{v} + \underline{e}$ to $-\underline{v} + \underline{e}$. From the construction of $\underline{w}$ and $\underline{y}$ it follows that

$$m_i(\underline{w}) = m_i(\underline{y}) + 2\sum_{l=0}^{i}\binom{i}{l}(j_4^l - j_3^l)m_{i-l}(\underline{w}_{k-1}) - 2\sum_{l=0}^{i}\binom{i}{l}(j_2^l - j_1^l)m_{i-l}(\underline{u}_{k-1}).$$

Since all the moments of $\underline{w}_{k-1}$ and $\underline{u}_{k-1}$ vanish up to order $k-2$, $m_i(\underline{w})$ is obviously 0 for $i = 0, 1, \cdots, k-2$. Furthermore, substituting $i = k-1$ into the expression above we obtain $m_{k-1}(\underline{w}) = 0$ and hence $\underline{w} \in \mathscr{S}(k)$. A similar argument now shows that

$$m_k(\underline{w}) = 2k(j_4 - j_3)m_{k-1}(\underline{w}_{k-1}) - 2k(j_2 - j_1) \cdot m_{k-1}(\underline{u}_{k-1}) = 2k! \cdot 2\delta_2 - 2k! \cdot W(k-1) \cdot \delta_1$$

where $W(k)$ is given by (25), while $\delta_1 = j_2 - j_1$ and $\delta_2 = j_4 - j_3$. W.l.o.g. we may assume that $W(k-1)$ is positive, otherwise exchange the roles of $\underline{u}_{k-1}$ and $-\underline{u}_{k-1}$ in the foregoing construction. Clearly δ_1 and δ_2 could not be less than the lengths of $\underline{u}_{k-1}$ and $\underline{w}_{k-1}$, respectively, but otherwise are arbitrary. Thus we may take δ_1 to be the smallest odd integer $\geq \ell(\underline{u}_{k-1})$, such that $W(k-1)\delta_1 > 2\ell(\underline{w}_{k-1})$. Since both δ_1 and $W(k-1)$ are odd, we may furthermore take $2\delta_2 = W(k-1)\delta_1 + 1$. In this case we have $m_k(\underline{w}) = 2k!$ and thereby the lemma is proved. □

It is clear from (24) and (25) that $\ell(\underline{u}_k) = O(2^k)$ and $W(k) = O(2^{k(k+1)/2})$. Substituting this in the construction of Lemma 5.4 we see that $\ell(\underline{w}_k) = O(\ell(\underline{w}_{k-1})2^k) = 2^{(1/2)k^2 + O(k)}$. Hence we have the following lemma.

Lemma 5.5: For any $k \geq 1$ and any integer t, there exists a word $\underline{w} \in \mathscr{S}(k)$ of length at most $t \cdot 2^{(1/2)k^2 + O(k)}$ with $m_k(\underline{w}) = 2tk!$.

Proof: In the construction of Lemma 5.4, let δ_1 be odd if t is odd and even otherwise, and let $2\delta_2 = W(k-1)\delta_1 + t$. Take $\delta_1 \equiv t \pmod 2$ and $2\delta_2 = W(k-1)\delta_1 + t$ in the construction of Lemma 5.4. □

Lemma 5.5 is the required generalization of Lemma 5.1.

C. An Encoder for kth-Order Spectral-Null Codes

It is now clear how the encoder of Section V-A may be extended for null orders greater than two. Let $\mathscr{E}(k)$ denote such a general encoder from Φ^n into $\mathscr{S}(k)$. Then $\mathscr{E}(k)$ may be specified recursively as follows. Assume that the length of the information word $\underline{v}$ to be encoded is given by $n = n_k n_{k-1} \cdots n_1$, and denote $m = n/n_k = n_{k-1}n_{k-2} \cdots n_1$. First, $\underline{v}$ is partitioned into n_k blocks $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_{n_k}$ of length m. Subsequently, each $\underline{v}_i$ is mapped into a word $\underline{x}_i \in \mathscr{S}(m + r, k-1)$, where r is the redundancy associated with the encoder $\mathscr{E}(k-1)$ applied to words of length m. The words $\underline{x}_i$ are then concatenated, and possibly negated, to obtain the series $\underline{y}_1, \underline{y}_2, \cdots, \underline{y}_{n_k}$ where $\underline{y}_1 = \underline{x}_1$ and

$$\underline{y}_i = \begin{cases} (\underline{y}_{i-1}|\underline{x}_i) & m_k(\underline{y}_{i-1}) \cdot m_k(\underline{x}_i) \leq 0 \\ (\underline{y}_{i-1}| - \underline{x}_i) & m_k(\underline{y}_{i-1}) \cdot m_k(\underline{x}_k) > 0 \end{cases}.$$

This ensures that

$$|m_k(\underline{y}_{n_k})| \leq \max_{1 \leq i \leq n_k} |m_k(\underline{x}_i)| \leq (m + r)^{k+1}.$$

Clearly, $\underline{y}_{n_k} \in \mathscr{S}(n_k(m+r), k-1)$ and, therefore, Lemma 5.3 implies that $m_k(\underline{y}_{n_k})$ is divisible by $2k!$ provided $\mathscr{S}(n_k(m+r), k) \neq \varnothing$. In view of Lemma 2.5, to satisfy the latter condition it would suffice to choose any value of n_k that is divisible by 2^k. Hence, using Lemma 5.5 we may construct a word $\underline{w}_k \in \mathscr{S}(k-1)$ of length

$$\ell(\underline{w}_k) = O\left(\frac{(m+r)^{k+1} \cdot 2^{(1/2)k^2 + O(k)}}{2k!}\right) \tag{26}$$

such that $m_k(\underline{w}_k) = -m_k(\underline{y}_{n_k})$. The output of the encoder $\mathscr{E}(k)$ then consists of a word $\underline{y} = (\underline{y}_{n_k}|\underline{w}_k) \in \mathscr{S}(k)$.

Let $\mathscr{C}$ denote the kth-order spectral-null code at the output of $\mathscr{E}(k)$, which is the set of all words obtained by applying $\mathscr{E}(k)$ to Φ^n. Then clearly

$$\begin{aligned}\rho(\mathscr{C}) &= \ell(\underline{w}_k) + n_k \ell(\underline{w}_{k-1}) + n_k n_{k-1} \ell(\underline{w}_{k-2}) + \cdots \\ &= \sum_{i=1}^{k} \ell(\underline{w}_i) \prod_{j=0}^{k-i-1} n_{k-j}.\end{aligned}$$

The rate of $\mathscr{C}$ is given by

$$R(\mathscr{C}) = \frac{n}{n + \rho(\mathscr{C})} = \frac{1}{1 + \dfrac{\rho(\mathscr{C})}{n}}$$

and we have

$$\frac{\rho(\mathscr{C})}{n} = \sum_{i=1}^{k} \ell(\underline{w}_i) \frac{\prod_{j=0}^{k-i-1} n_{k-j}}{\prod_{j=1}^{k} n_j} = \sum_{i=1}^{k} \frac{\ell(\underline{w}_i)}{\prod_{j=1}^{i} n_j}. \tag{27}$$

Note that, in view of (26), the value of $\ell(\underline{w}_i)$ depends on $n_1, n_2, \cdots, n_{i-1}$ but *not* on n_i. Hence by taking n_i sufficiently large for all $i = 1, 2, \cdots, k$ we can make each of the k terms in (27) as close to zero as desired. Therefore, $\limsup_{n_1, n_2, \cdots, n_k \to \infty} R(\mathscr{C}) = 1$, as claimed.

Appendix

This Appendix establishes the fact that (19) does not have nontrivial integer solutions, which was employed in Section III to show that the number of sign-changes in a word $\underline{x} \in \mathscr{S}(n, 3)$ is at least 5.

Lemma A.1: The equation

$$p^4 + 8q(q-p)^3 = r^2$$

does not have integer solutions in the range $0 < p < q$.

Proof By clearing common factors, we may assume without loss of generality that $\gcd(p, q) = 1$, for if a prime b divides both p and q then b^2 must divide r. We now verify that p must be odd. Indeed, if p were even then q would have to be odd and r would be divisible by 4. Reducing (19) modulo 16, we would then find that the left-hand side is congruent to 8 whereas the right-hand side is congruent to 0, which is a contradiction. Hence, we conclude that p is odd, and therefore so is r. This makes it possible to rewrite (19) as

$$2q(q-p)^3 = \xi \cdot \eta$$

where

$$\xi = \frac{r+p^2}{2} \quad \text{and} \quad \eta = \frac{r-p^2}{2}$$

and both ξ and η are positive integers. We thus have

$$p^2 = \xi - \eta = \xi - \frac{2q(q-p)^3}{\xi}. \tag{28}$$

Writing $p = q - a$ for a positive integer a, we can transform (28) into the following quadratic equation in q:

$$\xi q^2 - 2a(\xi - a^2)q - \xi(\xi - a^2) = 0. \tag{29}$$

The discriminant Δ of (29) is given by

$$\begin{aligned}\Delta &= 4a^2(\xi - a^2)^2 + 4\xi^2(\xi - a^2)\\ &= 4(\xi - a^2)(\xi^2 + a^2\xi - a^4)\\ &= 4(\xi^3 - 2a^4\xi + a^6).\end{aligned}$$

The solution q for (29) is an integer. Therefore, ξ and a must be such that $\Delta = 4x^2$ for some integer x, namely,

$$(\xi - a^2)(\xi^2 + a^2\xi - a^4) = \xi^3 - 2a^4\xi + a^6 = x^2. \tag{30}$$

To verify whether such integers ξ and a exist, we can assume without loss of generality that $\gcd(a, \xi) = 1$. Otherwise, if a prime b divides both ξ and a then b^3 divides x^2 in view of (30). Thus, x is divisible by b^2, which implies by (30) that b^4 divides ξ^3. Hence, ξ is divisible by b^2 and so x^2 is divisible by b^6. We can therefore substitute $\xi' = \xi/b^2$, $a' = a/b$, and $x' = x/b^3$ into (30) and then clear the common factor b^6.

Next we claim that $\xi - a^2$ is positive. Otherwise, we could multiply both sides of

$$a^2(\xi - a^2) \le \xi^2 + a^2\xi - a^4$$

by the nonpositive value $4(\xi - a^2)$ to obtain

$$\begin{aligned}(2a(\xi - a^2))^2 &= 4a^2(\xi - a^2)^2\\ &\ge 4(\xi - a^2)(\xi^2 + a^2\xi - a^4) = \Delta.\end{aligned}$$

This, in turn, would imply $|2a(\xi - a^2)| \ge \sqrt{\Delta}$. Solving (29) for q, we would thus have

$$q = \frac{2a(\xi - a^2) \pm \sqrt{\Delta}}{2\xi} \le 0$$

which is a contradiction.

It is easy to see that $\gcd(a, \xi) = 1$ also implies $\gcd(\xi - a^2, \xi^2 + a^2\xi - a^4) = 1$. Combining this with (30) and with the fact that $\xi - a^2$ is positive, we conclude that there must be an integer factorization $x = y \cdot z$ such that

$$\xi - a^2 = y^2 \quad \text{and} \quad \xi^2 + a^2\xi - a^4 = z^2. \tag{31}$$

Eliminating ξ from (31), we obtain the equation

$$a^4 + 3a^2y^2 + y^4 = z^2 \tag{32}$$

where both a and y must be nonzero to avoid the trivial solutions $p = q$ or $q = 0$. It is known that (32) has no integer solutions for nonzero a and y. See [23, pp. 19–22] for the mention of this result and [25, p. 115] for its proof. This completes the proof that (19) has no integer solutions in the range $0 < p < q$. □

Acknowledgment

The authors wish to thank the anonymous referees for their valuable comments. In particular, we have adopted the suggestion of one of the referees to revise part of the presentation so that it will be based on the characterization of kth-order spectral-null words through the divisibility of their z-polynomials by $(z-1)^k$. We would also like to thank T. Etzion for helpful discussions.

References

[1] S. Al-Bassam and B. Bose, "On balanced codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 406–408, 1990.

[2] N. Alon, E. E. Bergmann, D. Coppersmith, and A. M. Odlyzko, "Balancing sets of vectors," *IEEE Trans. Inform. Theory*, vol. 34, pp. 128–130, 1988.

[3] M. Blaum, "A (16, 9, 6, 5, 4) error-correcting DC-free block code," *IEEE Trans. Inform. Theory*, vol. 34, pp. 138–141, 1988.

[4] A. M. Barg and S. N. Litsyn, "DC-constrained codes from Hadamard matrices," *IEEE Trans. Inform. Theory*, vol. 37, pp. 801–807, 1991.

[5] E. Eleftheriou and R. Cideciyan, "On codes satisfying Mth order running digital sum constraints," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1294–1313, 1991.

[6] T. Etzion, "Constructions of error-correcting DC-free block codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 899–905, 1990.

[7] H. C. Ferreira, Lower bounds on the minimum Hamming distance achievable with runlength constrained or DC-free block codes and the synthesis of a (16, 8), $D_{\min} = 4$, DC-free block code," *IEEE Trans. Magnetics*, vol. 20, pp. 881–883, 1984.

[8] W. H. Gottschalk and G. A. Hedlund, "Topological dynamics," *Colloq. AMS*, vol. 36, Providence, RI: Amer. Math. Soc., 1955.

[9] H. D. L. Hollman and K. A. Schouhamer Immink, "Performance of efficient balanced codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 913–918, 1991.

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford: Oxford Univ. 1979.

[11] L. K. Hua, *Introduction to Number Theory*. Berlin: Springer-Verlag, 1982.

[12] K. A. Schouhamer Immink, Spectrum shaping with DC^2-constrained channel codes, *Phillips J. Res.*, vol. 40, (1985), pp. 40–53.

[13] ——, *Coding Techniques for Digital Recorders*. London: Prentice-Hall, 1991.

[14] K. A. Schouhamer Immink and G. Beenker, "Binary transmission codes with higher order spectral zeros at zero frequency," *IEEE Trans. Inform. Theory*, vol. 33, pp. 452–454, 1987.

[15] R. Karabed and P. H. Siegel, "Matched spectral-null codes for partial-response channels," *IEEE Trans. Inform. Theory*, vol. 37, pp. 818–855, 1991.

[16] D. E. Knuth, *The Art of Computer Programming, Vol. 1: Fundamental Algorithms*, 2nd ed. Reading, MA: Addison-Wesley, 1973.

[17] ——, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 2nd ed. Reading, MA: Addison-Wesley, 1981.

[18] ——, "Efficient balanced codes," *IEEE Trans. Inform. Theory*, vol. 32, pp. 51–53, 1986.

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

[20] B. H. Marcus and P. H. Siegel, "On codes with spectral nulls at rational submultiples of the symbol frequency," *IEEE Trans. Inform. Theory*, vol. 33, pp. 557–568, 1987.

[21] J. L. Massey, D. J. Costello, Jr., and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inform. Th.*, vol. 19, pp. 101–110, pp. 1973.

[22] C. M. Monti and G. L. Pierobon, "Codes with a multiple spectral null at zero frequency," *IEEE Trans. Inform. Theory*, vol. 35, pp. 463–472, 1989.

[23] L. J. Mordell, *Diophantine Equations*. London: Academic, 1969.

[24] M. Morse, "Recurrent geodesics on a surface of negative curvature," *Trans. Amer. Math. Soc.*, vol. 22, pp. 84–100, 1921.

[25] H. C. Pocklington, "Some diophantine impossibilities," *Proc. Cambridge. Phil. Soc.*, vol. 17, pp. 110–118, 1914.

[26] R. M. Roth and G. Seroussi, "On generator matrices of MDS codes," *IEEE Trans. Inform. Theory*, vol. 31, pp. 826–830, 1985.

[27] A. Schrijver, *Theory of Linear and Integer Programming*. New York: Wiley, 1986.

[28] H. C. A. van Tilborg and M. Blaum, "On error-correcting balanced codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1091–1095, 1989.

[29] P. S. Henry, "Zero disparity coding system," U.S. Patent 4,309,694 (1982).