

# Sparse Weighted Euclidean Superimposed Coding for Integer Compressed Sensing

Wei Dai and Olgica Milenkovic

Dept. of Electrical and Computer Engineering  
University of Illinois, Urbana-Champaign

**Abstract**—We address the problem of bounding the achievable rates of a new class of superimposed codes, termed weighted Euclidean superimposed codes (WESCs). WESCs generalize traditional Euclidean superimposed codes in so far that they allow for distinguishing bounded, integer-valued linear combinations of codewords. They can also be viewed as a bridge between superimposed coding and compressive sensing. In particular, we focus on sparse WESCs, for which one can devise low-complexity decoding algorithms and simple analytical constructions. Our results include a sufficient condition for meeting a minimum distance requirement of sparse WESCs, and a lower bound on the largest rate of sparse WESCs. Also included is a simple extension of DeVore’s deterministic construction for sparse compressed sensing matrices that meets the derived lower bound.

## I. INTRODUCTION

Superimposed coding [1], [2] represents a technique for distinguishing functions of codewords that are not necessarily linear nor defined over finite fields only. In their original setting, such codes were used to separate coordinate-wise OR functions of codewords over binary fields, to impose constraints on support-inclusions of such OR function, or to simply discriminate between sums of codewords over the field of real numbers. In the latter case, the scheme is known as *Euclidean* superimposed coding (ESC). Applications of these coding techniques have been broad and diverse, including user identification in wireless systems, quality-control and group testing, and database retrieval. It is the combination of group testing applications and the Euclidean coding strategy that provides a strong relationship between superimposed codes on one side and the emerging signal processing technique of compressed sensing (CS) on the other side.

The idea of compressed sensing is to recover a *sparse signal* via a small number of linear measurements [3]–[6]. In the CS framework, one samples a  $K$ -sparse, discrete,  $N$ -dimensional signal  $\mathbf{x}$  through  $m \ll N$  linear projections. The vector  $\mathbf{x}$  is termed  $K$ -sparse if it can be represented by a linear combination of at most  $K$  vectors from a fixed basis, with  $K \ll N$ . The result of the projections is a real-valued vector  $\mathbf{y} = \Phi\mathbf{x}$ , where  $\Phi$  denotes the  $m \times N$  “projection” matrix, usually over the field of real numbers. Under certain constraints on  $\Phi$  and the values of  $K$ ,  $m$  and  $N$ , compressed sensing guarantees accurate reconstruction of  $\mathbf{x}$  precisely through the measurement  $\mathbf{y}$ , despite the lack of knowledge about which columns of  $\Phi$  were sampled in the process.

Weighted Euclidean superimposed codes (WESCs) represents a simple link between ESCs and CS projection matrices. WESCs codes, introduced by the authors in [7], allow for distinguishing all bounded, integer-valued linear combination of at most  $K$  real-valued codewords. In comparison, one can view the columns of a compressive sensing matrix  $\Phi$  as real-valued codewords, and the gist of CS is to find codewords that allow for distinguishing all *real-valued linear combinations* of not more than  $K$  codewords. Similar to ESCs, WESCs are defined over the field of real numbers, they obey prescribed minimum Euclidean distance constraints, and therefore have deterministic performance guarantees in the presence of noise. However, unlike ESCs, which only distinguish between binary sums of codewords, WESCs can perform the same discrimination task for bounded integer-valued linear combinations of codewords. Similar to compressed sensing, WESCs allow for distinguishing linear combinations of codewords with non-binary coefficients; but, due to the fact that these coefficients are integer-valued, WESCs can meet prescribed minimum Euclidean distance properties that CS codes cannot achieve. Consequently, the WESCs framework provides certain advantages over both ESC and CS schemes: the minimum distance guarantee is desirable in many practical scenarios, especially when the measurement is contaminated by noise, at the same time, the assumption of bounded integer-valued coefficients can significantly reduce the decoding complexity [7].

Of course, these advantages come at the cost of a more limited range of applications of WESCs as compared to CS techniques. Nevertheless, there exist practical applications that motivate the study of WESCs. One example is our recent work on compressed sensing microarray design [8]. In whole-genome microarray experiments, the vector  $\mathbf{x}$  has entries that correspond to the number of different RNA molecules in a cell cytoplasm. Usually, the number of RNA macromolecules in a wild-type cell is used as the zero-level measurement, and deviations from this value (which can be both positive and negative, and integer-valued) represent the actual measurement. Since the number of RNA molecules in a cell at any point in time is upper bounded due to energy constraints, and due to intracellular space limitations, the deviations are assumed to be finite and relatively small compared to the number of different RNA types.

In this paper, we focus on *sparse* WESCs, for which one can implement low complexity decoding algorithm (see [9] for applications of belief propagation decoding for CS reconstruction) and design simple deterministic constructions.

\*This work is supported by NSF Grants CCF 0644427, 0729216 and the DARPA Young Faculty Award.

“Sparsity” imposes the requirement that the support sizes (i.e., the number of non-zero coordinates) of all codewords are significantly smaller than their length. We derive a sufficient condition that guarantees the minimum distance properties of sparse WESCs, and then proceed to derive a lower bound on the largest rate of sparse WESCs.

In a companion paper [7], we derived asymptotic bounds on the largest rate of general WESCs. However, it is an open problem to find deterministic construction for WESC that achieve these bounds. Under the sparsity assumption, this construction problem becomes more tractable. We demonstrate this fact by extending a simple construction of sparse CS matrices, due to DeVore [10], and showing that it meets the derived lower bound for WESCs.

The paper is organized as follows. Section II introduces the relevant terminology and presents our main results. The corresponding proofs are included in Section III and IV. Finally, Section V contains the concluding remarks.

## II. DEFINITIONS AND MAIN RESULTS

### A. WESCs: The General Framework

A Euclidean code  $\mathcal{C}$  is a finite set of  $N$  code-vectors  $\mathbf{v}_i \in \mathbb{R}^m$ ,  $i = 1, 2, \dots, N$ , of fixed  $l_2$  norms,  $\|\mathbf{v}_i\| = c$  for some constant  $c$ . The code  $\mathcal{C}$  is specified by its *codeword matrix* (codebook)  $\mathbf{C} \in \mathbb{R}^{m \times N}$ , obtained by arranging the codewords as columns of the matrix. A submatrix of a codeword matrix  $\mathbf{C}$ , consisting of columns indexed by elements of an index set  $I \subset \{1, \dots, N\}$ , is denoted by  $\mathbf{C}_I$ .

Let

$$B_t = \{-t, -t+1, \dots, -1, 1, \dots, t-1, t\} = [-t, t] \setminus \{0\},$$

$t \in \mathbb{Z}^+$ , be a symmetric, bounded set of integers. For a given index set  $I \in [1, N]$  and a coefficient vector  $\mathbf{b} \in B_t^{|I|}$ , let

$$f(I, \mathbf{b}) = \sum_{i \in I} b_i \mathbf{v}_i,$$

where  $b_i$  is the  $i^{\text{th}}$  element of  $\mathbf{b}$ , and  $\mathbf{v}_i$  denotes the  $i^{\text{th}}$  column of  $\mathbf{C}$ . Define next a set of subsets over  $[1, N]$ ,

$$\mathcal{I}_K := \{I \subset \{1, \dots, N\} : |I| \leq K\},$$

and

$$d_E(\mathcal{C}, K) := \min_{((I_1, \mathbf{b}_1), (I_2, \mathbf{b}_2))} \|f(I_1, \mathbf{b}_1) - f(I_2, \mathbf{b}_2)\|_2,$$

where  $I_{1,2} \in \mathcal{I}_K$ ,  $(I_1, \mathbf{b}_1) \neq (I_2, \mathbf{b}_2)$ , and where  $\|\cdot\|_2$  denotes the Euclidean norm of a vector.

*Definition 1:* A code  $\mathcal{C}$  is said to be a WESC with parameters  $(N, m, K, d, B_t)$  if  $d_E(\mathcal{C}, K) \geq d$ , for some  $0 \leq d \leq c$ .

For simplicity, throughout the rest of the paper, we assume that  $c=1$ .

*Remark 1:* Notice that by using the set  $\{1\}$  instead of  $B_t$ , the definition above reduces to that of an Euclidean superimposed code.

Let

$$N(m, K, d, B_t) := \max \{N : \mathcal{C}(N, m, K, d, B_t) \neq \emptyset\},$$

and define the asymptotic code exponent as

$$R(K, d, B_t) := \limsup_{m \rightarrow \infty} \frac{\log N(m, K, d, B_t)}{m}.$$

In a companion paper [7], we derived lower and upper bounds on  $R(K, d, B_t)$ , summarized below in Lemma 1.

*Lemma 1:* For a constant  $t$ , the asymptotic code exponent of WESCs can be bounded as

$$\frac{\log K}{4K} (1 + o_{t,d}(1)) \leq R(K, d, B_t) \leq \frac{\log K}{2K} (1 + o_{t,d}(1)), \quad (1)$$

where  $o_{t,d}(1)$  is a function of  $t$  and  $d$ ,  $o_{t,d}(1) \rightarrow 0$  as  $K \rightarrow \infty$ .

However, the above bounds for general WESCs can not be met in general for certain subclasses of WESCs, such as sparse WESCs. This issue is addressed in the next section.

### B. Regular Sparse WESCs

For simplicity, throughout the remainder of the paper we consider *regular, sparse* WESCs, denoted by  $\mathcal{C}_s$ , and defined below.

*Definition 2:* A code  $\mathcal{C}_s$  is said to be a regular sparse code with sparsity  $s$  (where it is tacitly assumed that  $s|m$ ), if every codeword  $\mathbf{v} \in \mathcal{C}_s$  has support size  $m/s$ .

In particular, to derive lower bounds on the rate of sparse WESCs, we focus on codewords of the form  $\sqrt{\frac{s}{m}} \mathbf{v}_i$  for some  $\mathbf{v}_i \in \{0, 1\}^m$ ,  $i = 1, \dots, N$ , and such that  $\omega_H(\mathbf{v}_i) = \frac{m}{s}$ ,  $\forall i$ . In a more general setting, one could consider sparse codewords of the form  $\mathbf{v}_i / \|\mathbf{v}_i\|$  with fixed support size  $\frac{m}{s}$ , where  $\mathbf{v}_i \in \mathcal{V}^m$  and  $\mathcal{V}$  is a finite set such that  $|\mathcal{V}| \geq 2$ . Our constraint  $\mathcal{V} = \{0, 1\}$  does not impose an asymptotic rate loss when  $|\mathcal{V}| \ll s$ , as will be demonstrated later. Since our goal is to study sparse WESCs suitable for certain low complexity decoding algorithms, such as belief propagation decoding [9],  $s$  is assumed to increase with  $m$  and is therefore large.

*Definition 3:* A regular, sparse code  $\mathcal{C}_s$  is a WESC with parameters  $(N, m, K, d, B_t)$  if  $d_E(\mathcal{C}_s, K) \geq d$  for some  $0 \leq d \leq 1$ .

Similarly as for the case of general WESCs, for a given  $s$ , we also define

$$N_s(m, K, d, B_t) := \max \{N : \mathcal{C}_s(N, m, K, d, B_t) \neq \emptyset\},$$

as well as the corresponding asymptotic code rate exponent

$$R_s(K, d, B_t) := \limsup_{m \rightarrow \infty} \frac{\log N_s(m, K, d, B_t)}{m}.$$

We shall show next that the asymptotic exponent satisfies

$$R_s(K, d, B_t) = o\left(\frac{\log K}{4K}\right),$$

whenever the sparsity parameter  $s$  is allowed to increase with  $m$ . In this case, note that all the codewords are distinct and of fixed weight. The number of codewords is thus at most

$$\binom{m}{\frac{m}{s}} = \exp\left(m \cdot H\left(\frac{1}{s}\right) (1 + o(1))\right),$$

where

$$H\left(\frac{1}{s}\right) = -\frac{1}{s} \log \frac{1}{s} - \left(1 - \frac{1}{s}\right) \log \left(1 - \frac{1}{s}\right)$$

denotes Shannon's binary entropy function for the Bernoulli distribution with parameter  $1/s$ . Consequently,

$$R_s(K, d, B_t) \leq H\left(\frac{1}{s}\right),$$

independent on the choice of the parameter  $K$ .

Suppose now that  $d$  and  $t$  are fixed, while  $s$  is allowed to grow with  $m$ , but so that  $s = o(m)$ . Since  $H(1/s) \rightarrow 0$  as  $s \rightarrow \infty$ , sparse codes exhibits code exponent loss. Clearly, by introducing the sparse constraint, one loses some freedom in selecting feasible codewords; the asymptotic code exponent is therefore diminishing with increasing  $s$ .

The same argument holds for general regular sparse codes with entries defined on some arbitrary finite, discrete alphabet  $\mathcal{V}$ . For each nonzero element in a codeword, we have  $|\mathcal{V}|$  many choices. It can then be shown that

$$\frac{\log N'_s}{m} \leq \frac{\log(N_s \cdot |\mathcal{V}|^{\frac{m}{s}})}{m} = \frac{\log N_s}{m} + \frac{1}{s} \log |\mathcal{V}|.$$

As  $s$  increases with  $m$ ,

$$\frac{1}{s} \log |\mathcal{V}| \ll H\left(\frac{1}{s}\right)$$

for sufficiently large  $s$ , and consequently

$$R'_s \leq H\left(\frac{1}{s}\right) (1 + o(1)).$$

The main result of this paper is a lower bound on  $N_s$  that guarantees the existence of a code  $\mathcal{C}_s$ .

*Theorem 1:* For  $m, N, s \rightarrow \infty$  such that  $\frac{s}{m} \rightarrow 0$ , one has

$$\frac{\log N_s(m, K, d, B_t)}{m} \geq \frac{\log s}{s} \left( \frac{1}{2K} + o(1) \right).$$

This theorem is based on Lemma 2 and Theorem 2. Lemma 2 provides a sufficient condition for  $d_E(\mathcal{C}_s, K) \geq d$ , while Theorem 2 derives the lower bound under which the condition in Lemma 2 holds. The detailed proofs of these two results are presented in Section III.

*Lemma 2:* For a given  $k \in \mathbb{Z}^+$ , let  $\mathbf{v}_i \in \{0, 1\}^{m \times 1}$ ,  $i = 1, \dots, k$ , be vectors with constant weight  $\sum_{j=1}^m (\mathbf{v}_i)_j = \frac{m}{s}$ . Then

$$\frac{s}{m} \mathbf{v}_i^\dagger \mathbf{v}_j \leq \frac{1}{k} \text{ for all } 1 \leq i \neq j \leq k$$

is a sufficient condition for

$$\frac{s}{m} \left| \sum_{i=1}^k b_i \mathbf{v}_i \right|^2 \geq d^2.$$

Here,  $d^2 < 1$ , and  $b_i \in B_t$ ,  $i = 1, \dots, k$ , are arbitrary.

*Remark 2:* The bound on the column correlation

$$\left| \mathbf{v}_i^\dagger \mathbf{v}_j \right| \leq \frac{1}{k}$$

can be further improved to

$$\left| \mathbf{v}_i^\dagger \mathbf{v}_j \right| \leq \left(1 - \frac{d}{k}\right) \frac{1}{k-1}.$$

However, this refinement is marginal, especially when  $k$  is large. For convenience, we focus on the upper bound  $1/k$  only.

*Remark 3:* The sufficient condition in Lemma 2 simplifies the decoding algorithm. As we have shown in [7], given the measurement vector  $\mathbf{y} = \mathbf{C}_s \mathbf{x}$ , the  $i^{\text{th}}$  element of the input signal  $\mathbf{x}$  can be found via

$$x_i = \left\{ \mathbf{v}_i^\dagger \mathbf{y} \right\}.$$

The corresponding computational complexity of the underlying algorithm is only a  $1/K$  fraction of the standard orthogonal matching pursuit algorithm of [11].

*Theorem 2:* For a given  $\delta$ , let

$$N_{m,s,\delta} := \left\{ |\mathcal{C}_s| : \frac{s}{m} \mathbf{v}_i^\dagger \mathbf{v}_j \leq \delta \right. \\ \left. \text{for all } \mathbf{v}_i, \mathbf{v}_j \in \mathcal{C}_s \text{ s.t. } \mathbf{v}_i \neq \mathbf{v}_j \right\}.$$

For  $m, N, s$  large enough such that  $s \ll m$ , one has

$$\frac{\log s}{s} (\delta + o(1)) \leq \frac{\log N_{m,s,\delta}}{m} \leq \frac{\log s}{s} \left( \frac{1 + \delta}{2} + o(1) \right).$$

We postpone the proofs of Lemma 2 and Theorem 2 to Section III-B and III-C respectively.

### C. Deterministic Construction of Sparse WESCs

Given the lower bound on the code exponent, it is of importance to see whether there exist *deterministic* constructions of regular sparse codes that can achieve this bound. The answer is affirmative, provided the parameters  $m$ ,  $N$ , and  $s$ , satisfy some mild conditions. The construction itself is a simple extension of DeVore's method, described in [10].

Let  $p$  be a prime. Let  $m = p^l$ , so that  $\frac{m}{s} = p = m^{1/l}$  ( $s = p^{l-1}$ ), where  $l$  is an integer satisfying  $l \geq 2$ . Let  $\mathbb{P}$  denote the set of all polynomials in  $\mathbb{F}_p[x]$  of degree at most  $r$ , and let

$$(P_1(x), \dots, P_{l-1}(x)), \quad (2)$$

be a collection of  $l-1$  not necessarily distinct polynomials from  $\mathbb{P}$ . We index the rows of the superimposed code matrix by  $l$ -tuples of the form  $(x, y_1, y_2, \dots, y_{l-1})$ ,  $x, y_i \in \mathbb{F}_p$ ,  $\forall i$ , and the columns with all ordered collections of  $l-1$  polynomials of the form shown in (2). As a result, the coding matrix consists of  $p^l$  rows and  $p^{(r+1)(l-1)}$  columns. Now, in a column indexed by the collection  $(P_1(x), \dots, P_{l-1}(x))$ , we assign the value one to the rows indexed by  $(x, y_1, \dots, y_{l-1})$  provided that  $y_k = P_k(x)$  for all  $k = 1, \dots, l-1$ . For a given  $K$ , we set the maximum degree of the polynomials to

$$r = \left\lceil \frac{1}{2K} p \right\rceil - 1$$

where  $\lceil \cdot \rceil$  is the closest integer function. We use  $\mathbf{C}_s$  to denote the resulting codeword matrix, and  $\mathbf{v}_i$  ( $1 \leq i \leq N$ ) to denote the  $i^{\text{th}}$  codeword of the code (the  $i^{\text{th}}$  column of  $\mathbf{C}_s$ ). Then  $\mathbf{C}_s$  has the following properties.

*Theorem 3:* The codeword matrix  $\mathbf{C}_s$  satisfies

1) (constant codeword weight)

$$\sum_{j=1}^m v_{i,j} = \frac{m}{s} = m^{1/l}$$

for all  $1 \leq i \leq N$ ;

2) (small codeword correlations)

$$\frac{s}{m} \mathbf{v}_{i_1}^\dagger \mathbf{v}_{i_2} \leq \frac{1}{2K}$$

for all  $1 \leq i_1 \neq i_2 \leq N$ ;

3) (asymptotic code rate)

$$\frac{\log N}{m} \frac{s}{\log s} \rightarrow \frac{1}{2K}$$

as  $p \rightarrow \infty$  (and therefore  $m, N, s, r \rightarrow \infty$  simultaneously).

The proof of this theorem is given in Section IV. According to Lemma 2, since this code exhibits small correlations between codewords, it satisfies the minimum distance requirement  $d_E(\mathcal{C}_s, K) \geq d$ . We have thus shown that a deterministic construction of regular sparse WESCs achieves the lower bound of Theorem 1.

The construction above is intimately tied to the well known class of Reed-Solomon (RS) codes over  $\mathbb{F}_p$ . In particular, the matrix  $\mathbf{C}_s$  is obtained through repetitive interleaving of codewords of an RS code. More details on this subject will be provided in the full version of the paper.

### III. ON THE CODE EXPONENT

#### A. Proof of Theorem 1

The lower bound on the code exponent in Theorem 1 is proved as follows.

Let  $I$  be an index set, let  $B_{2t} = [-2t, 2t] \setminus \{0\}$ , and  $\mathbf{b}' \in B_{2t}^{|I|}$ . Since  $\|f(I, \mathbf{b})\| = \|\mathbf{V}_I \mathbf{b}\|$ , it follows that

$$\begin{aligned} & \{ \|f(I_1, \mathbf{b}_1) - f(I_2, \mathbf{b}_2)\| : I_1, I_2 \in \mathcal{I}_K, (I_1, \mathbf{b}_1) \neq (I_2, \mathbf{b}_2) \} \\ & \subset \{ \|\mathbf{V}_I \mathbf{b}'\| : I \in \mathcal{I}_{2K}, \mathbf{b}' \in B_{2t}^{|I|} \}. \end{aligned}$$

Let  $N'(m, 2K, d, B_{2t})$  be the largest  $N$  such that there exists a codeword matrix  $\mathbf{C} \in \mathbb{R}^{m \times N'}$  with  $\|\mathbf{V}_I \mathbf{b}'\| \geq d$ , for all  $I \in \mathcal{I}_{2K}$ , and all  $\mathbf{b}' \in B_{2t}^{|I|}$ . The existence of such a code implies the existence of a  $(N, m, K, d, B_t)$  WESC, and  $N'$  is a lower bound on  $N$ .

For sparse WESC, according to Theorem 2, if

$$\frac{\log N'}{m} \geq \frac{\log s}{s} \left( \frac{1}{2K} + o(1) \right),$$

then there exists a  $\mathcal{C}_s$  such that

$$\mathbf{v}_i^\dagger \mathbf{v}_j \leq \frac{1}{2K} \frac{m}{s}$$

for all  $\mathbf{v}_i \neq \mathbf{v}_j$ . By Lemma 2,

$$\frac{s}{m} \left| \sum_{i \in I} \mathbf{v}_i b'_i \right| = \|\mathbf{V}_I \mathbf{b}'\|^2 \geq d^2$$

for all  $I \in \mathcal{I}_{2K}$  and  $\mathbf{b}' \in B_{2t}^{|I|}$ , which implies that  $d_E(\mathcal{C}_s, K) \geq d$ . By the definition of  $N_s$ , we conclude that

$$\frac{\log N_s(m, K, d, B_t)}{m} \geq \frac{\log N'}{m} \geq \frac{\log s}{s} \left( \frac{1}{2K} + o(1) \right).$$

#### B. Proof of Lemma 2

Note that

$$\frac{s}{m} \left| \sum_{i=1}^k \mathbf{v}_i b_i \right|^2 = \frac{s}{m} \sum_{j=1}^m \left( \sum_{i=1}^k v_{i,j} b_i \right)^2.$$

For a given  $j$ , if there is only one nonzero element in  $\{v_{1,j}, \dots, v_{k,j}\}$ , then

$$\left( \sum_{i=1}^k v_{i,j} b_i \right)^2 \geq 1;$$

for other cases, one clearly has

$$\left( \sum_{i=1}^k v_{i,j} b_i \right)^2 \geq 0.$$

Let  $\mathbf{v} = \sum_{i=1}^k b_i \mathbf{v}_i$ , and let

$$I_{\mathbf{v}} = \left\{ j : |v_j| = \left| \sum_{i=1}^k v_{i,j} b_i \right| \geq 1 \right\}.$$

Then

$$\frac{s}{m} \left| \sum_{i=1}^k \mathbf{v}_i b_i \right|^2 \geq \frac{s}{m} |I_{\mathbf{v}}|.$$

The quantity  $|I_{\mathbf{v}}|$  can be lower bounded as follows. Suppose that

$$|\mathbf{v}_i^\dagger \mathbf{v}_j| \leq \frac{1}{k} \frac{m}{s}$$

for all  $1 \leq i \neq j \leq k$ . Then at least

$$\frac{m}{s} - (k-1) \left( \frac{1}{k} \frac{m}{s} \right) = \frac{1}{k} \frac{m}{s}$$

entries from  $\mathbf{v}_i$  contribute to the set  $I_{\mathbf{v}}$ . Since we have  $k$  vectors, it follows that

$$|I_{\mathbf{v}}| \geq k \left( \frac{1}{k} \frac{m}{s} \right) = \frac{m}{s}.$$

Hence,

$$\frac{s}{m} \left| \sum_{i=1}^k \mathbf{v}_i b_i \right|^2 \geq \frac{s}{m} |I_{\mathbf{v}}| \geq 1 \geq d^2.$$

*Remark 4:* The same result can be obtained by using the Gershgorin Circle Theorem [12]. The derivations are omitted due to space limitation.

#### C. Proof of Theorem 2

Theorem 2 is proved by sphere packing/covering arguments. Define

$$\mathcal{V}_s = \left\{ \mathbf{v} \in \{0, 1\}^{m \times 1} : \sum v_i = \frac{m}{s} \right\}.$$

For given  $\mathbf{v}_0 \in \mathcal{V}_s$  and constant  $\beta \in (0, 2)$ , define a Hamming ball in  $\mathcal{V}_s$  by

$$B_{\mathbf{v}_0} \left( \beta \frac{m}{s} \right) := \left\{ \mathbf{v} \in \mathcal{V}_s : d_h(\mathbf{v}_0, \mathbf{v}) \leq \beta \frac{m}{s} \right\},$$

where  $d_h(\cdot, \cdot)$  denotes the Hamming distance. Then we have the following lemma regarding the cardinality of the above defined Hamming ball.

*Lemma 3:* The cardinality of  $B_{\mathbf{v}_0}(\beta \frac{m}{s})$  is independent on  $\mathbf{v}_0$ . Furthermore, as  $m, s \rightarrow \infty$  with  $\frac{s}{m} \rightarrow 0$ ,

$$\log \left| B_{\mathbf{v}_0} \left( \beta \frac{m}{s} \right) \right| = \frac{m}{s} \left( \frac{\beta}{2} \log s + c + o(1) \right),$$

where

$$c = -\frac{\beta}{2} \log \frac{\beta}{2} + \frac{\beta}{2} + H \left( \frac{\beta}{2} \right).$$

*Proof:* See Appendix A.  $\blacksquare$

We describe next the relationship between the column correlation and the Hamming distance in  $\mathcal{V}_s$ . For any  $\mathbf{v} \in \mathcal{V}_s$ , let

$$I_{\mathbf{v}} = \{1 \leq i \leq m : v_i = 1\}.$$

For any  $\mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}_s$ , the condition  $\mathbf{v}_1^\dagger \mathbf{v}_2 \leq \delta \frac{m}{s}$  implies that

$$\left| I_{\mathbf{v}_1} \cap I_{\mathbf{v}_2} \right| \leq \delta \frac{m}{s},$$

which in turn implies that

$$\left| I_{\mathbf{v}_1} - I_{\mathbf{v}_1} \cap I_{\mathbf{v}_2} \right| \geq (1 - \delta) \frac{m}{s},$$

and

$$\left| I_{\mathbf{v}_2} - I_{\mathbf{v}_1} \cap I_{\mathbf{v}_2} \right| \geq (1 - \delta) \frac{m}{s}.$$

Thus,

$$d_h(\mathbf{v}_1, \mathbf{v}_2) \geq 2(1 - \delta) \frac{m}{s}.$$

Therefore, finding a regular sparse code  $\mathcal{C}_s$  such that

$$\mathbf{v}_i^\dagger \mathbf{v}_j \leq \delta \frac{m}{s},$$

where  $\mathbf{v}_i \neq \mathbf{v}_j$ , is equivalent to finding a code  $\mathcal{C}_s$  such that all its codewords are at Hamming distance at least  $2(1 - \delta) \frac{m}{s}$  from each other. According to the well known Hamming bound (sphere packing bound) and Gilbert-Varshamov bound (sphere covering bound), we get

$$\frac{|\mathcal{V}_s|}{\left| B \left( 2(1 - \delta) \frac{m}{s} \right) \right|} \leq N_{m,s,\delta} = \sup |\mathcal{C}_s| \leq \frac{|\mathcal{V}_s|}{\left| B \left( (1 - \delta) \frac{m}{s} \right) \right|}.$$

From Stirling's approximation formula, it follows

$$\log |\mathcal{V}_s| = \frac{m}{s} (\log s + 1 + o(1)).$$

As a result, the claim of Theorem 2 reduces to a straightforward application of Lemma 2.

For an interesting connection between this result and the theory of superimposed and spherical coding, the interested reader is referred to [13].

#### IV. PROOFS OF THEOREM 3

This section proves that the code construction in Section II-C has the claimed properties of Theorem 3.

According to the construction, it is clear that each column has exactly  $p$  non-zero entries. Thus,  $\mathbf{C}_s$  is a regular sparse code whose codewords have constant weight  $p = \frac{m}{s} = m^{1/l}$ .

Now, take any two columns  $\mathbf{v}_{i_1}$  and  $\mathbf{v}_{i_2}$  ( $i_1 \neq i_2$ ) from the codewords matrix  $\mathbf{C}_s$ . We shall show that

$$\frac{1}{p} \mathbf{v}_{i_1}^\dagger \mathbf{v}_{i_2} \leq \frac{1}{2K}.$$

With slight abuse of notation, we index the  $i_1$ -th and  $i_2$ -th column by  $(P_1(\cdot), \dots, P_{l-1}(\cdot))$  and  $(P'_1(\cdot), \dots, P'_{l-1}(\cdot))$ , respectively. If  $\alpha_0, \alpha_1, \dots, \alpha_{p-1}$  denotes an arbitrary ordering of the elements of  $\mathbb{F}_p$ , then  $v_{i_1,j} = v_{i_2,j} = 1$  if and only if

$$(P_1(\alpha_j), \dots, P_{l-1}(\alpha_j)) = (P'_1(\alpha_j), \dots, P'_{l-1}(\alpha_j))$$

as an ordered  $l$ -tuple.

We shall count next the number of the indices for which this equality can be met. Note that since  $i_1 \neq i_2$ , there exists at least one  $1 \leq k \leq l-1$  such that  $P_k(\cdot) \neq P'_k(\cdot)$ . The degree of the polynomial  $P_k(\cdot) - P'_k(\cdot)$  is at most  $r$ . Thus there are at most  $r$  many elements of the field  $\mathbb{F}_p$  for which  $P_k(x) = P'_k(x)$ . Hence, we have

$$\begin{aligned} \mathbf{v}_{i_1}^\dagger \mathbf{v}_{i_2} &= \sum_{j=1}^m \chi_{\{v_{i_1,j}=v_{i_2,j}\}} \\ &= \sum_{\alpha \in \mathbb{F}_p} \chi_{\{(P_1(\alpha), \dots, P_{l-1}(\alpha)) = (P'_1(\alpha), \dots, P'_{l-1}(\alpha))\}} \\ &\leq r = \left\lceil \frac{1}{2K} p \right\rceil - 1 \leq \frac{1}{2K} p, \end{aligned}$$

where  $\chi_A$  denotes the characteristic function of the event  $A$ .

Finally, we calculate the asymptotic code exponent. The number of columns of  $\mathbf{C}_s$  equals

$$N = p^{(r+1)(l-1)},$$

as there are  $p^{r+1}$  many choices for each  $P_k(\cdot)$   $1 \leq k \leq l-1$ , and a total of  $(p^{r+1})^{l-1}$  many choices for the tuple  $(P_1(\cdot), \dots, P_{l-1}(\cdot))$ . As already pointed out, the number of rows in the code matrix equals  $m = p^l$ . Thus,

$$\begin{aligned} \frac{\log N}{m} \cdot \frac{s}{\log s} &= \frac{(r+1)(l-1) \log p}{p^l} \cdot \frac{p^{l-1}}{(l-1) \log p} \\ &= \frac{r+1}{p} = \left\lceil \frac{1}{2K} p \right\rceil \rightarrow \frac{1}{2K} \end{aligned}$$

for  $p \rightarrow \infty$ , as claimed.

#### V. CONCLUSION

We studied sparse WESCs amenable for use with low complexity decoding algorithms, which also have simple deterministic constructions. We derived a sufficient condition that guarantees the minimum distance properties of these codes, and a lower bound on the largest rate of sparse WESCs. We also extended DeVore's deterministic construction and showed that it meets the derived lower bound.

#### APPENDIX

##### A. Proof of Lemma 3

For a  $\mathbf{v} \in \mathcal{V}_s$ , let  $I_{\mathbf{v}} = \{1 \leq i \leq m : v_i = 1\}$ . For any  $\mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}_s$  such that  $d_h(\mathbf{v}_1, \mathbf{v}_2) = \beta m/s$  (w.l.o.g., we suppose that  $\beta m/s$  is an even integer), one has

$$|I_{\mathbf{v}_1} - I_{\mathbf{v}_2}| = \frac{\beta m}{2s},$$

$$|I_{\mathbf{v}_2} - I_{\mathbf{v}_1}| = \frac{\beta m}{2s},$$

and

$$|I_{\mathbf{v}_1} \cap I_{\mathbf{v}_2}| = \frac{m}{s} \left(1 - \frac{\beta}{2}\right).$$

Thus, for an arbitrary  $\mathbf{v}_0 \in \mathcal{V}_s$ ,

$$|\{\mathbf{v} \in \mathcal{V}_s : d_h(\mathbf{v}_0, \mathbf{v}) = 2k\}| = \binom{\frac{m}{s}}{k} \binom{m - \frac{m}{s}}{k},$$

and

$$|B_{\mathbf{v}_0}(\beta \frac{m}{s})| = \sum_{k=0}^{\frac{\beta}{2} \frac{m}{s}} \binom{\frac{m}{s}}{k} \binom{m - \frac{m}{s}}{k}.$$

Let us first find the asymptotic expression for

$$\binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}}.$$

By Stirling's approximation formula,

$$\log \binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} = \frac{m}{s} \left( H\left(\frac{\beta}{2}\right) + o(1) \right),$$

where

$$H\left(\frac{\beta}{2}\right) = -\frac{\beta}{2} \log \frac{\beta}{2} - \left(1 - \frac{\beta}{2}\right) \log \left(1 - \frac{\beta}{2}\right),$$

and

$$\log \binom{m(1 - \frac{1}{s})}{\frac{\beta}{2} \frac{m}{s}} = \frac{\beta}{2} \frac{m}{s} \left( \log s - \log \frac{\beta}{2} + 1 + o(1) \right).$$

Thus

$$\log \left( \binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m(1 - \frac{1}{s})}{\frac{\beta}{2} \frac{m}{s}} \right) = \frac{m}{s} \left( \frac{\beta}{2} \log s + c + o(1) \right),$$

where  $c$  is a constant defined through

$$c = -\frac{\beta}{2} \log \frac{\beta}{2} + \frac{\beta}{2} + H\left(\frac{\beta}{2}\right).$$

We then show that

$$\log |B(\beta \frac{m}{s})| = (1 + o(1)) \log \left( \binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m(1 - \frac{1}{s})}{\frac{\beta}{2} \frac{m}{s}} \right).$$

For any integers  $n, k$  such that  $k < n$ , we have

$$\frac{\binom{n}{k-1}}{\binom{n}{k}} = \frac{k}{n - k + 1},$$

which is a monotone increasing function of  $k$ . A direct consequence of this observation is that for any  $k \leq \frac{\beta}{2} \frac{m}{s}$ ,

$$\frac{\binom{\frac{m}{s}}{k-1} \binom{m - \frac{m}{s}}{k-1}}{\binom{\frac{m}{s}}{k} \binom{m - \frac{m}{s}}{k}} \leq \frac{\binom{\frac{\beta}{2} \frac{m}{s} - 1}{\frac{\beta}{2} \frac{m}{s} - 1} \binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s} - 1}}{\binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}}}.$$

The right side can be bounded via

$$\frac{\binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s} - 1} \binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s} - 1}}{\binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}}} = \frac{\frac{\beta}{2} \frac{m}{s}}{\left(\frac{m}{s} - \frac{\beta}{2} \frac{m}{s} + 1\right)} < \frac{\frac{\beta}{2}}{1 - \frac{\beta}{2}},$$

and

$$\begin{aligned} & \frac{\binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s} - 1} \binom{m - \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}}}{\binom{\frac{\beta}{2} \frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}}} < \frac{\frac{\beta}{2} \frac{m}{s}}{m \left(1 - \frac{1}{s} - \frac{\beta}{2s} + \frac{1}{m}\right)} < \frac{\frac{\beta}{2s}}{1 - \frac{1}{s} - \frac{\beta}{2s}}. \end{aligned}$$

For any given  $\beta < 2$ , as  $s$  is large enough, one has

$$\frac{\frac{\beta}{2}}{1 - \frac{\beta}{2}} \frac{\frac{\beta}{2s}}{1 - \frac{1}{s} - \frac{\beta}{2s}} < 1.$$

This implies that for any  $k \leq \beta \frac{m}{s}$ ,

$$\binom{\frac{m}{s}}{k} \binom{m - \frac{m}{s}}{k} \leq \binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m(1 - \frac{1}{s})}{\frac{\beta}{2} \frac{m}{s}}$$

for large enough  $s$ , and therefore,

$$\begin{aligned} & \log \left( |B(\beta \frac{m}{s})| \right) \\ &= \log \left( \sum_{k=0}^{\frac{\beta m}{2s}} \binom{\frac{m}{s}}{k} \binom{m - \frac{m}{s}}{k} \right) \\ &\leq \log \left( \binom{\frac{m}{s}}{\frac{\beta}{2} \frac{m}{s}} \binom{m(1 - \frac{1}{s})}{\frac{\beta}{2} \frac{m}{s}} \frac{\beta m}{2s} \right) \\ &= \frac{m}{s} \left( \frac{\beta}{2} \log s + c + o(1) \right) + \log \frac{\beta m}{2s} \\ &= \frac{m}{s} \left( \frac{\beta}{2} \log s + c + o(1) \right). \end{aligned}$$

This completes the proof of the lemma.

## REFERENCES

- [1] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 363–377, 1964.
- [2] T. Ericson and L. Györfi, "Superimposed codes in  $\mathbf{R}^n$ ," *IEEE Trans. Inform. Theory*, vol. 34, no. 4, pp. 877–880, 1988.
- [3] D. Donoho, "Compressed sensing," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.
- [4] E. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 489–509, 2006.
- [5] E. J. Candès, J. K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Comm. Pure Appl. Math.*, vol. 59, no. 8, pp. 1207–1223, 2006.
- [6] E. J. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inform. Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.
- [7] W. Dai and O. Milenkovic, "Weighted euclidean superimposed codes for integer compressed sensing," in *IEEE Information Theory Workshop (ITW)*, 2008, submitted.
- [8] M. Sheikh, O. Milenkovic, and R. Baraniuk, "Designing compressive sensing DNA microarrays," *Proceedings of the IEEE Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, St. Thomas, U.S. Virgin Islands, submitted, Dec. 2007.
- [9] S. Sarvotham, D. Baron, and R. Baraniuk, "Compressed sensing reconstruction via belief propagation." *Preprint*, 2006.
- [10] R. A. DeVore, "Deterministic constructions of compressed sensing matrices," *Preprint*, 2007.
- [11] J. A. Tropp, "Greed is good: algorithmic results for sparse approximation," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2231–2242, 2004.
- [12] R. S. Varga, *Geršgorin and His Circles*. Berlin: Springer-Verlag, 2004.
- [13] D. Danev, Z. Füredi, and M. Ruzinkó, *Multiple Access Channels - Theory and Practice*. IOS Press, 2007, ch. Multiple Access Euclidean Channel, pp. 54 – 72.