DETERMINISTIC CONSTRUCTIONS OF BINARY MEASUREMENT MATRICES WITH VARIOUS SIZES

Xin-Ji Liu, Shu-Tao Xia, Tao Dai

Graduate School at Shenzhen, Tsinghua University

ABSTRACT

We introduce a general framework to deterministically construct binary measurement matrices for compressed sensing. The proposed matrices are composed of (circulant) permutation submatrix blocks and zero submatrix blocks, thus making their hardware realization convenient and easy. Firstly, using the famous Johnson bound for binary constant weight codes, we derive a new lower bound for the coherence of binary matrices with uniform column weights. Afterwards, a large class of binary *base matrices* with coherence asymptotically achieving this new bound are presented. Finally, by choosing proper rows and columns from these base matrices, we construct the desired measurement matrices with various sizes and they show empirically comparable performance to that of the corresponding Gaussian matrices.

***Index Terms*—** Compressed sensing, deterministic measurement matrix, coherence, Johnson bound, Welch bound.

1. INTRODUCTION

Compressed sensing (CS) [1, 2] is a novel sampling technique that samples sparse signals at a rate far lower than the Nyquist-Shannon rate. Consider a k-*sparse* signal $\boldsymbol{x} \in \mathbb{R}^n$ with at most k nonzero entries, if we make a linear sampling $\boldsymbol{y} = A\boldsymbol{x}$ of $\boldsymbol{x}$ with the *measurement matrix* $A \in \mathbb{R}^{m\times n}$, where $m < n$, then $\boldsymbol{x}$ could be recovered by solving an ℓ_1-*minimization* problem [3] or by a greedy algorithm such as *orthogonal matching pursuit* (OMP) [4]. Actually, if A satisfies the *restricted isometry property* (RIP) [3] of order k with enough small $0 < \delta_k^A < 1$, signals with sparsity $O(k)$ can be exactly recovered by ℓ_1-minimization or OMP [5, pp. 26], where δ_k^A denotes the *restricted isometry constant* of A.

Many random matrices, such as the Gaussian matrices, have been proved to satisfy RIP of order k *with high probability* if $k \leq O(m/\log(n/k))$ [6]. However, there is no guarantee that a specific realization of a random matrix works and some random matrices require lots of storage space. In contrast, a deterministic matrix is often generated on the fly and RIP could be verified definitely. Therefore, deterministic measurement matrices are often preferable in practice.

The *coherence* $\mu(A)$ of a deterministic matrix A is often exploited to prove RIP since $\delta_k^A \leq (k-1)\mu(A)$ [7], where

$$\mu(A) \triangleq \max_{1\leq i\neq j\leq n} \frac{|\langle \boldsymbol{a}_i, \boldsymbol{a}_j\rangle|}{||\boldsymbol{a}_i||_2||\boldsymbol{a}_j||_2}, \tag{1}$$

$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ are the n columns of A, $\langle \boldsymbol{a}_i, \boldsymbol{a}_j\rangle \triangleq \boldsymbol{a}_i^T\boldsymbol{a}_j$ and for any $\boldsymbol{z} = (z_1, z_2, \ldots, z_m)^T \in \mathbb{R}^m$, $||\boldsymbol{z}||_2 \triangleq \sqrt{\sum_{i=1}^m z_i^2}$. Therefore, given $\mu(A)$, A satisfies RIP of order

$$k < 1 + \frac{1}{\mu(A)}. \tag{2}$$

Recently, binary deterministic matrices have been introduced into compressed sensing due to their simplicity [8, 9, 10, 11, 12, 13, 14, 15]. For example, let q be a prime power, DeVore proposed a class of binary (before column normalization) $q^2 \times q^{r+1}$ matrices satisfying RIP of order $k < q/r+1$, where $1 < r < q$ is a constant integer [8]. By using the codewords of orthogonal optical codes as the columns of matrices, Amini *et al.* constructed a class of binary measurement matrices [9]. In [13], the incidence matrices of several packing designs based on finite geometry are applied into compressed sensing. These matrices have relatively low coherence and show empirically good performance in compressed sensing.

However, many of them are often based on Galois fields (GF), thus having restrictions to the numbers of rows[1]. Recently, utilizing the parallel structure of Euclidean geometry, we proposed a class of binary measurement matrices with a bit more flexible sizes [16]. In this paper, we introduce more such matrices. In particular, we focus on the binary matrix H with a constant column weight. By viewing the columns of H as codewords of a *constant weight code* [17, p. 523–531], we derive a new lower bound for its coherence $\mu(H)$ with the help of the famous Johnson bound [18], which improves the traditional Welch bound [19]. Then we present a subclass of binary (often quasi-cyclic) matrices asymptotically achieving this new bound and some examples from structural low-density parity-check (LDPC) codes [20] are given. Based on these matrices, a general framework is proposed to obtain practical measurement matrices with various sizes. Finally, simulations show that the proposed matrices perform comparably to, sometimes even better than, the corresponding Gaussian matrices.

2. MAIN RESULTS

2.1. Coherence of Binary Matrices

In this part, we analyze the coherence of binary matrices which have uniform column weights $\gamma > 1$.

Firstly, some preliminaries are presented. For any matrix $H \in \{0,1\}^{m\times n}$, there is a *Tanner graph* G_H [21] corresponding to H. G_H is a bipartite graph comprised of n variable nodes labelled by the elements of $I = \{1, 2, \ldots, n\}$, m check nodes labelled by the elements of $J = \{1, 2, \ldots, m\}$, and the edge set $E \subseteq \{(i, j) : i \in I, j \in J\}$, where there is an edge $(i, j) \in E$ if and only if $h_{ji} = 1$. The *girth* $g(H)$ of H or G_H is defined as the minimum length of cycles in G_H. Girth is always an even number not smaller than 4. H

This research is supported in part by the 973 Program of China (No. 2012CB315803), the National Natural Science Foundation of China (Nos. 61371078, 61375054), and the Research Fund for the Doctoral Program of Higher Education of China (No. 20130002110051). Corresponding author: Shu-Tao Xia, xiast@sz.tsinghua.edu.cn.

[1] Generally, removing some columns from a matrix will not deteriorate its theoretical (such as coherence and RIP) and empirical performance.

is said to be (γ, ρ)-*regular* if H has uniform column weight γ and uniform row weight ρ.

A binary matrix H with uniform column weight γ can be viewed as a collection of codewords (as columns of H) of certain binary constant weight codes. An (m, d, γ) constant weight code $\mathcal{C}$ is a set of binary vectors of length m, weight γ and minimum distance d, where d is always an even number. Let $A(m, d, \gamma)$ be the largest number of codewords in any (m, d, γ) constant weight codes, $A(m, d, \gamma)$ could be bounded by the famous Johnson bound [18]:

$$A(m, 2\delta, \gamma) \leq \lfloor \frac{m}{\gamma} \lfloor \frac{m-1}{\gamma-1} \cdots \lfloor \frac{m-\gamma+\delta}{\delta} \rfloor \cdots \rfloor \rfloor, \quad (3)$$

where $\lfloor x \rfloor$ denotes the largest integer no larger than x.

Traditionally, the coherence of a matrix is bounded by the Welch bound [19]:

$$\mu(A) \geq \sqrt{\frac{n-m}{m(n-1)}}. \quad (4)$$

The equality in (4) achieves *if and only if* A is an *equiangular tight frame* (ETF), i.e., A should satisfy the following 3 conditions: (a) the columns of A have unit norm, (b) the rows of A are orthogonal with equal norm, and (c) the inner products between any two different columns of A are equal in modulus [22]. Therefore, for any binary[2] matrix H with uniform column weight $\gamma > 1$, the rows of H will not be orthogonal, thus the Welch bound (4) could not be achieved.

In the following, we analyze the coherence of binary matrices by the Johnson bound. Consider the binary $m \times n$ matrix H with uniform column weight $\gamma > 0$, suppose the maximum inner product of any two columns of H is $\lambda > 0$, then H has coherence $\mu(H) = \frac{\lambda}{\gamma}$. In particular, when H has girth $g(H) > 4$, any two distinct columns of H have at most one pair of common '1' at the same row, i.e., $\lambda = 1$, we have

$$\mu(H) = \frac{1}{\gamma}. \quad (5)$$

By viewing the column vectors of H as the codewords of an (m, d, γ) constant weight code $\mathcal{C}$, then $d = 2\gamma - 2\lambda$. From the Johnson bound (3), we have the following fact.

Lemma 1. *For any binary matrix $H \in \{0,1\}^{m\times n}$ with uniform column weight $\gamma > 1$, maximum inner product $0 < \lambda < \gamma$ of any two distinct columns, m, n, γ and λ should satisfy:*

$$n \leq \lfloor \frac{m}{\gamma} \lfloor \frac{m-1}{\gamma-1} \cdots \lfloor \frac{m-\lambda}{\gamma-\lambda} \rfloor \cdots \rfloor \rfloor. \quad (6)$$

In particular, when H has girth $g(H) > 4$, we can obtain an explicit lower bound for the coherence of H.

Theorem 1. *Let $H \in \{0,1\}^{m\times n}$ be a binary matrix with uniform column weight $\gamma > 1$, girth $g(H) > 4$ and coherence $\mu(H) \neq 0$, then*

$$\mu(H) \geq \frac{2n}{n + \sqrt{n^2 + 4mn(m-1)}}. \quad (7)$$

Proof. When $g(H) > 4$ and $\mu(H) \neq 0$, $\lambda = 1$. By (6), $n \leq \lfloor \frac{m}{\gamma} \lfloor \frac{m-1}{\gamma-1} \rfloor \rfloor \leq \frac{m(m-1)}{\gamma(\gamma-1)}$, (7) follows since $\mu(H) = \frac{1}{\gamma}$. □

Remark 1. *By a simple deduction, it is easy to see that (7) is always tighter than the Welch bound (4) if $m < n$. In addition, throughout this paper, we call the binary matrix with uniform column weight $\gamma > 0$, girth $g > 4$ and coherence $\mu \neq 0$* (asymptotically) optimal *if the coherence of this matrix (asymptotically) achieves the lower bound (7).*

[2]Binary 0-1 matrices are mainly discussed here and all the discussions and conclusions in this paper only apply to binary 0-1 matrices.

Remark 2. *Similar to the Johnson bound, (7) could be achieved. For example, let H be the point-line incidence matrix (rows of H corresponding to the points and columns to the lines) of the Euclidean plane $EG(2, q)$, where q is a prime power. H is a $(q, q+1)$-regular matrix with the size $q^2 \times (q^2 + q)$, $g(H) = 6$, and it is easy to verify that (7) is achieved, see [16] for more details of H and its application to compressed sensing.*

2.2. A Subclass of Asymptotically Optimal Binary Matrices in Terms of Coherence

In this part, we show a subclass of binary matrices with coherence asymptotically achieving the lower bound (7). Later on, they will be used to obtain the desired measurement matrices with various sizes and empirically good performance.

Consider an $s^2 \times s^2$ *base matrix* as follows

$$H = [H_{i,j}], \quad 1 \leq i, j \leq s, \quad (8)$$

where $s > 1$ and $H_{i,j} \in \{0,1\}^{s\times s}$ is either a permutation block or a zero block $\mathbf{0} = \{0\}^{s\times s}$. A *permutation block* $B \in \{0,1\}^{s\times s}$ is a square matrix with each row and each column having exactly one element '1'. If B is also cyclic, then B is called a *circulant permutation block*. Each $[H_{i,1}, H_{i,2}, \ldots, H_{i,s}]$ (or $[H_{1,j}^T, H_{2,j}^T, \ldots, H_{s,j}^T]^T$) of H is called a *row-block* (or *column-block*) of H. H satisfies the following two properties.

- (P1) Every column-block of H has exactly t zero blocks, so does each row-block , i.e., H is $(s-t, s-t)$-regular, where $0 \leq t \ll s$ is a small constant.
- (P2) The girth of H is larger than 4, i.e., $g(H) > 4$.

Remark 3. *The $s^2 \times s^2$ base matrix H has coherence $\mu(H) = \frac{1}{s-t}$. According to Theorem 1, the (nonzero) coherence of any $s^2 \times s^2$ binary matrix with uniform column weight $\gamma > 1$ and girth larger than 4 has the lower bound $\frac{2}{1+\sqrt{4s^2-3}} \to \frac{1}{s}$ if $s \to \infty$. Since $t \geq 0$ is a small constant, the coherence of the base matrix H is asymptotically optimal.*

In addition, for some submatrices of the base matrices, their coherences are also asymptotically optimal. Let $A(\gamma, s, t)$ be a $\gamma s \times s^2$ submatrix of the base matrix H by simply choosing the first γ row-blocks of H, i.e.,

$$A(\gamma, s, t) \triangleq [H_{i,j}], \quad 1 \leq i \leq \gamma \leq s, \quad 1 \leq j \leq s. \quad (9)$$

Remark 4. *Suppose $\gamma = cs$, where $0 < c < 1$ is a constant such that cs is an integer. When $t = 0$, $A(cs, s, 0)$ is a (cs, s)-regular matrix with coherence $\mu(A(cs, s, 0)) = \frac{1}{cs}$. According to (7), for any binary $cs^2 \times s^2$ matrix with uniform column weight, girth larger than 4 and nonzero coherence, its coherence has the lower bound $\frac{1}{0.5+\sqrt{c^2s^2+0.25-c}} \to \frac{1}{cs}$ if $s \to \infty$. Therefore, the submatrix $A(cs, s, 0)$ is also asymptotically optimal in terms of coherence.*

In the following, we review several examples of satisfactory base matrices from structured (often quasi-cyclic) LDPC codes.

Example 1 ([23, 24])**.** *Let $H = H(q, q)$, where q is an odd prime and $H(q, q)$ is the binary matrix defined in (7) in [24] with $r = q$. Then $H \in \{0,1\}^{q^2\times q^2}$ is a (q, q)-regular base matrix with $t = 0$.*

Example 2 ([25, 26])**.** *Let $H = H^{(1)}(q, q, 0)$, where q is a prime power and $H^{(1)}(q, q, 0)$ is the parity-check matrix of a first class of B–J based LDPC code proposed in [25, Section III.A]. Then $H \in \{0,1\}^{q^2\times q^2}$ is a (q, q)-regular base matrix with $t = 0$.*

Let $GF(q) = \{\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha, \ldots, \alpha^{q-2}\}$ be a Galois field with primitive element α. Establish a one-to-one $(q-1)$-*fold correspondence* between the elements in $GF(q)$ and the matrices $P \in \{0,1\}^{(q-1)\times(q-1)}$ as follows:

- 0 is mapped to the zero block $\mathbf{0} = \{0\}^{(q-1)\times(q-1)}$;
- α^i is mapped to a circulant permutation block P_{q-1}^i, where $0 \le i \le q-2$,

$$P_{q-1} \triangleq \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}_{(q-1)\times(q-1)}, \quad (10)$$

P_{q-1}^i denotes the i-th power of P_{q-1} and $P_{q-1}^0 \triangleq I_{q-1}$ is the identity matrix of order $q-1$.

In the following Examples 3 and 4, we obtain the base matrix H by firstly constructing a matrix $L \in GF(q)^{(q-1)\times(q-1)}$ based on the *Latin square* and then replacing each element in L with a circulant permutation block or a zero block $P \in \{0,1\}^{(q-1)\times(q-1)}$.

Definition 1. *An Latin square of order n is an $n \times n$ matrix with n distinct symbols, each of which occurrs exactly once in each row and exactly once in each column.*

Example 3 ([27, 28, 29])**.** *Let β be a nonzero element in $GF(q)$ and $L_{\mathrm{RS}}(\beta)$ be the following Reed-Solomon codes based (cyclic) Latin square of order $q-1$ over $GF(q) \setminus \{-\beta\}$:*

$$L_{\mathrm{RS}}(\beta) = \begin{bmatrix} 1-\beta & \alpha-\beta & \ldots & \alpha^{q-2}-\beta \\ \alpha^{q-2}-\beta & 1-\beta & \ldots & \alpha^{q-3}-\beta \\ \vdots & \vdots & \ddots & \vdots \\ \alpha-\beta & \alpha^2-\beta & \ldots & 1-\beta \end{bmatrix}.$$

Expand $L_{\mathrm{RS}}(\beta)$ by replacing each entry with a circulant permutation block or a zero block according to the $(q-1)$-fold correspondence, and then we could get a quasi-cyclic base matrix $H \in \{0,1\}^{(q-1)^2\times(q-1)^2}$ with $t = 1$. Note that no matter which nonzero β is chosen, there is exactly one 0 in each row and exactly one 0 in each column of $L_{\mathrm{RS}}(\beta)$. Therefore, the resulting H is a $(q-2, q-2)$-regular matrix. Finally, as there are $q-1$ nonzero elements $\beta \in GF(q)$, there will be $q-1$ such Latin squares $L_{\mathrm{RS}}(\beta)$ and thus $q-1$ such base matrices H.

Example 4 ([29])**.** *Let β be any nonzero element in $GF(q)$ and $\bar{L}(\beta) = W$ be the Latin square of order q over $GF(q)$ in [29, Equation (11)] with $\beta = \eta$. Choose the following $(q-1)\times(q-1)$ submatrix $L(\beta)$ of $\bar{L}(\beta)$, $L(\beta) =$*

$$\begin{bmatrix} \beta-1 & \beta-\alpha & \ldots & \beta-\alpha^{q-2} \\ \alpha\beta-1 & \alpha\beta-\alpha & \ldots & \alpha\beta-\alpha^{q-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-2}\beta-1 & \alpha^{q-2}\beta-\alpha & \ldots & \alpha^{q-2}\beta-\alpha^{q-2} \end{bmatrix}.$$

Expand $L(\beta)$ according to the $(q-1)$-fold correspondence. In this way, we obtain a quasi-cyclic and $(q-2, q-2)$-regular base matrix $H \in \{0,1\}^{(q-1)^2\times(q-1)^2}$ with $t = 1$.

Example 5 ([25, 26])**.** *Let q be a prime power. Let $H = H^{(2)}(q-1, q-1, 0)$, where $H^{(2)}(q-1, q-1, 0)$ is the parity-check matrix of a second class of B–J based LDPC code proposed in [25, Section III.B]. Then $H \in \{0,1\}^{(q-1)^2\times(q-1)^2}$ is a quasi-cyclic and $(q-2, q-2)$-regular base matrix with $t = 1$.*

2.3. General Framework of Matrix Constructions

In this part, we give the general framework to deterministically construct binary measurement matrices, see Algorithm 1. Note that in the second step of Algorithm 1, we choose the $s^2 \times s^2$ base matrix H in such a way as to make the resulting A have the smallest coherence. In practice, for the proposed construction, we often require $m \gg \sqrt{n}$, thus the outputted matrix will have small coherence and empirically good performance. For example, m scales linearly with n, i.e., $m = cn$, where $0 < c < 1$ is a constant. See the following Theorem 2 for a formalized explanation.

Algorithm 1 Deterministic Construction of Binary Measurement Matrices with Various Sizes

Input: Matrix size m and n.
Output: A binary measurement matrix $A \in \{0,1\}^{m\times n}$.
Steps:
(1) Base matrix construction: construct several classes of $\bar{s}^2 \times \bar{s}^2$ base matrices satisfying (P1) and (P2) with $t \ll \bar{s}$.
(2) Base matrix selection: choose an $s^2 \times s^2$ matrix H among these base matrices such that $s \ge \sqrt{n}$ and $(m/s - t)$ is as large as possible.
(3) Extra elements deletion: remove the last $s^2 - m$ rows and the last $s^2 - n$ columns of H and output the resulting submatrix as A.

Theorem 2. *For any measurement matrix $A \in \{0,1\}^{m\times n}$ constructed by Algorithm 1, we have*

$$\mu(A) \le \frac{1}{\gamma - t}, \quad (11)$$

where $\gamma = \left\lfloor \frac{m}{s} \right\rfloor$, $0 \le t \ll s$ is a fixed integer.

Proof. According to (P1), the minimum possible column weight of A is $\gamma - t$. From (P2), the inner product of any two columns of A is at most 1. By (1), (11) follows directly. □

Remark 5. *As stated in Remark 4, when $\gamma = \frac{m}{s} = cs$, $n = s^2$ and $t = 0$, the binary matrix $A(cs, s, 0)$ outputted by Algorithm 1 is asymptotically optimal in terms of coherence. In other cases, the structure (and thus the coherence) of the resulting matrix A with $m = cn$ and $n = s^2$ is very close to that of $A(cs, s, 0)$. Moreover, removing columns of a measurement matrix will not deteriorate its empirical performance. Therefore, it is reasonable to conjecture that the measurement matrices obtained by Algorithm 1 will often perform well in practice and this will be verified by the following experimental results.*

3. EXPERIMENTAL RESULTS

In the following simulations, for each measurement matrix A and each k-sparse signal $\boldsymbol{x}$, we conduct an experiment using $M = 1000$ Monte Carlo trials. In the i-th trial, a relative recovery error $e_i = ||\boldsymbol{x}^* - \boldsymbol{x}||_2/||\boldsymbol{x}||_2$ is computed, where $\boldsymbol{x}^*$ denotes the recovered signal. If $e_i \le 0.001$, we declare this recovery to be "perfect". Finally, an average percentage of perfect recovery over the M trials is obtained and shown as a point in the figures.

At first, we give an example to show the empirical effectiveness for the base matrix selecting strategy in the second step of Algorithm 1. Suppose only one class of base matrices are constructed in the first step, such as the base matrices in Example 3, and now we want to construct a 100×300 binary measurement matrix. Since $\sqrt{300} = 17.32$, we can set q to be 19, 23, or even larger prime

power. The OMP recovery performance of the desired measurement matrices obtained by setting $q = 19$, $q = 23$ and the Gaussian matrix ('Rnd') with the same size are shown in Fig. 1. It is clear that

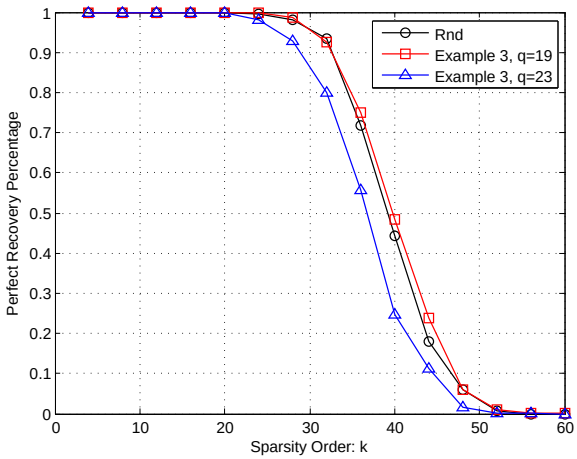

Fig. 1. Empirical performance of the 100×300 measurement matrices obtained by Example 3 by setting $q = 19$ and $q = 23$ and the corresponding Gaussian random matrix under OMP recovery.

the matrix based on Example 3 with $q = 19$ is better than that with $q = 23$, which agrees with the base matrix choosing strategy in the second step of Algorithm 1.

In the following, we consider several binary measurement matrices based on the base matrices in Examples 1–5, see Fig. 2 for the empirical performance of these matrices with small sizes and Fig. 3 for that of matrices with larger sizes.

Let $q = 31$ in Example 1, $q = 32$ in Examples 2–5, $\beta = 1$ in Examples 3 and 4. For each Example 1–5, construct 3 measurement matrices with sizes 190×940, 225×950, and 260×960 by removing the last extra rows and columns from the 5 different base matrices. See Fig. 2 for their empirical performance and the corresponding Gaussian matrices.

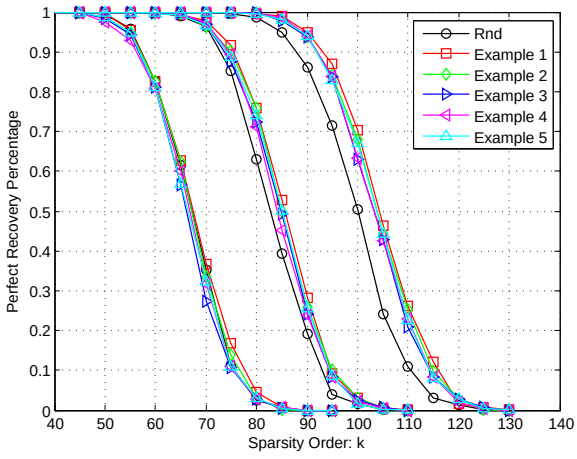

Fig. 2. Empirical performance of the proposed measurement matrices and the corresponding Gaussian random matrices with sizes 190×940, 225×950, and 260×960 (the three curve bundles from left to right, respectively) under OMP recovery.

Let $q = 61$ in Example 1 and $q = 64$ in Example 2–5. For each Example 1–5, construct 3 matrices with sizes 450×3500, 500×3600, and 550×3700. See Fig. 3 for their empirical performance.

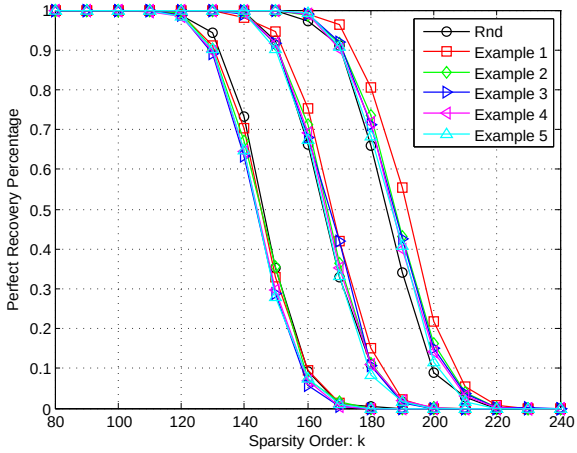

Fig. 3. Empirical performance of the proposed measurement matrices and the corresponding Gaussian matrices with sizes 450×3500, 500×3600, and 550×3700 (the three curve bundles from left to right, respectively) under OMP recovery.

In Figs. 2 and 3, all of the proposed matrices perform as well as, sometimes even better than, the corresponding Gaussian matrices. In addition, it is easy to see that the matrices from Example 1 often perform slightly better than those from Example 2–5 due to the specific matrix sizes. Simple computations on the upper bounds of coherence (according to Theorem 2) show that each coherence upper bound of the six matrices obtained by Example 1 is smaller than (or sometimes equal to) that of other examples. This also agrees with the base matrix selecting strategy in the second step of Algorithm 1.

4. CONCLUSIONS AND DISCUSSIONS

This paper has introduced a general framework to deterministically construct binary measurement matrices with various sizes and empirically good performance. In particular, some of them are also shown to be asymptotically optimal according to a new lower bound of coherence derived with the help of the famous Johnson bound. Moreover, these matrices are binary, sparse, and mostly quasi-cyclic, which will benefit the hardware implementation.

This paper mainly focuses on binary matrices with girth larger than 4. However, as has been indicated by Lu [10], some empirically even better binary matrices lie in the region of girth $g = 4$. In addition, a $(q^2 + 1) \times q(q^2 + 1)$ binary measurement matrix with uniform column weight $\gamma = q + 1$ and $\lambda = 2$ (thus girth $g = 4$) has been proposed in [13]. It is easy to verify that this matrix achieves the Johnson bound and Equation (6) in this paper and they are also shown to perform empirically well in [13]. As a result, it will be interesting to carry out some theoretical analysis explicitly on binary matrices with $g = 4$ and construct more such (asymptotically) optimal matrices which may show perhaps better performance in practice.

5. REFERENCES

[1] E. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.

[2] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[3] E. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[4] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.

[5] S. Foucart and H. Rauhut, *A mathematical introduction to compressive sensing*. Springer, 2013.

[6] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constructive Approximation*, vol. 28, no. 3, pp. 253–263, 2008.

[7] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova *et al.*, "Explicit constructions of RIP matrices and related problems," *Duke Mathematical Journal*, vol. 159, no. 1, pp. 145–185, 2011.

[8] R. A. DeVore, "Deterministic constructions of compressed sensing matrices," *Journal of Complexity*, vol. 23, no. 4, pp. 918–925, 2007.

[9] A. Amini and F. Marvasti, "Deterministic construction of binary, bipolar, and ternary compressed sensing matrices," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2360–2370, Mar. 2011.

[10] W. Lu, K. Kpalma, and J. Ronsin, "Sparse binary matrices of LDPC codes for compressed sensing," in *Data Compression Conference (DCC)*, Snowbird (Utah), United States, Apr. 2012, pp. 405–405.

[11] A. Dimakis, R. Smarandache, and P. Vontobel, "LDPC codes for compressed sensing," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3093–3114, 2012.

[12] A. Tehrani, A. Dimakis, and G. Caire, "Optimal deterministic compressed sensing matrices," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Vancouver, BC, May 2013, pp. 5895–5899.

[13] S. Li and G. Ge, "Deterministic construction of sparse sensing matrices via finite geometry," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2850–2859, Jun. 2014.

[14] P. Indyk, "Explicit constructions for compressed sensing of sparse signals," in *ACM-SIAM Symposium on Discrete Algorithms(SODA)*, San Francisco, California, USA, Jan. 2008.

[15] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 358–374, April 2010.

[16] S.-T. Xia, X.-J. Liu, Y. Jiang, and H.-T. Zheng, "Deterministic constructions of binary measurement matrices from finite geometry," *IEEE Trans. Signal Process.*, 2015.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland., 1979.

[18] S. Johnson, "A new upper bound for error-correcting codes," *IRE Transactions on Information Theory*, vol. 8, no. 3, pp. 203–207, 1962.

[19] L. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, Mar. 1974.

[20] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[21] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, May 1981.

[22] A. Bandeira, M. Fickus, D. Mixon, and P. Wong, "The road to deterministic matrices with the restricted isometry property," *Journal of Fourier Analysis and Applications*, vol. 19, no. 6, pp. 1123–1149, 2013.

[23] M. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[24] X.-J. Liu and S.-T. Xia, "Constructions of quasi-cyclic measurement matrices based on array codes," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 479–483.

[25] X. Ge and S.-T. Xia, "LDPC codes based on Berlekamp-Justesen codes with large stopping distances," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Chengdu, China, Oct. 2006, pp. 214–218.

[26] D.-D. Li, X.-J. Liu, S.-T. Xia, and Y. Jiang, "A class of deterministic construction of binary compressed sensing matrices," *Journal of Electronics (China)*, vol. 29, no. 6, pp. 493–500, Dec. 2012.

[27] L. Lan, L. Zeng, Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2429–2458, Jul. 2007.

[28] L. Zeng, L. Lan, Y. Tai, S. Song, S. Lin, and K. Abdel-Ghaffar, "Constructions of nonbinary quasi-cyclic LDPC codes: A finite field approach," *IEEE Trans. Commun.*, vol. 56, no. 4, pp. 545–554, Apr. 2008.

[29] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. Blake, "Quasi-cyclic LDPC codes: An algebraic construction, rank analysis, and codes on latin squares," *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3126–3139, Nov. 2010.