Deterministic Construction of Compressed Sensing Matrices over Finite Sets

Xuemei Liu *, Yingmo Jie
College of Science, Civil Aviation University of China, Tianjin, 300300, P.R. China

Abstract Compressed sensing (CS) has broken through the traditional Nyquist sampling theory in that it is a new technique of signal processing. According to CS theory, compressed sensing makes full use of sparsity so that a sparse signal can be reconstructed from very few measurements. It is well known that the construction of CS matrices is the central problem. In this paper, we provide one kind of deterministic sensing matrices by describing a combinatorial design, then we obtain two cases by instantiating the RIP framework with the obtained design, which the latter one is the majorization of the former one. At last, we show the better properties than DeVore's construction using polynomials over finite fields.

Keywords: Compressed sensing matrices, Finite sets, Coherence, Restricted isometry property (RIP).
AMS classification: 20G40 51D25

1. Introduction

The traditional Nyquist sampling theorem points out that in order to protect from losing information during sampling signals we have to sample at least two times faster than their bandwidth. However, it is too expensive to increase the sampling rate and it also brings complicated issues to our work. Therefore, it is high time to replace the conventional sampling and reconstruction operations with lower rate and keep the veracity about recovering signals. Meanwhile CS theorem has successfully tackled these problems. For a discrete signal x, which can be regarded as a vector in R^t with t entries. We want to capture this signal with t large by taking a small number s of linear measurements. Each linear measurement is to calculate the inner product $v \cdot x$ of x with vectors v. Then the $s \times t$ matrix Φ, which contains these vectors v, is called compressed sensing matrix, and the information $y = \Phi x$, which is extracted from x by Φ, is named the measurement vector. Here arises one question: For a given measurement vector y, how can we reconstruct the original signal x from $y = \Phi x$? Even though $y = \Phi x$ is usually ill-posed for $s < t$, Donoho[1] and Candès[2] make the most of sparsity to get that a sparse signal can be reconstructed from very few measurements. This problem is described as finding the sparsest solution of linear equations $y = \Phi x$

*Correspondence : College of Science, Civil Aviation University of China,Tianjin,300300, P.R.China; E-mail: xm-liu771216@163.com.

$$\min_{x \in R^t} \| x \|_0 \quad \text{s.t.}: \quad \Phi x = y. \tag{1}$$

This l_0-minimization is a combinatorial minimization problem and is normally NP-hard[3]. Whereas, CS presents a skillful way to recover sparse signals with suitable algorithms and the number of measurements $s \ll t$.

There are basic two ways to reconstruct k-sparse signals. One of them is pursuing greedy algorithms for l_0-minimization (1). Among these greedy algorithms, there is a famous one called orthogonal matching pursuit (OMP)[4]. If the number of measurements $s \geq Dk\log(\frac{t}{\delta})$, where D is a constant and $\delta \in (0, 0.36)$, OMP can recover x from (1) with probability surpassing $1 - 2\delta$. Namely, we can regard the recovery of sparse signals as an optimization problem with efficient algorithms available by choosing a stable sensing matrix. There are two kinds of CS matrices, one is called random sensing matrices whose entries are randomly drawn from certain probability distributions, which concludes Gaussian matrices; Bernoulli matrices; Random partial orthogonal matrices[5−7]. Another is named deterministic (compressed) sensing matrices, which successfully obtains a large number of attentions. Then we have another problem: What kinds of matrices are stable? They must ensure that the salient information in any k-sparse or compressible signal is not damaged by the dimensionality reduction from $x \in R^t$ down to $y \in R^s$. For the sake of figuring out this problem, Candès and Tao[8] have introduced a criterion, named restricted isometry property (RIP).

Definition 1.1.[9] Let Φ be an $s \times t$ matrix, if there exists a constant $\delta_k \in (0, 1)$, such that for any k-sparse signal $x \in R^t$, we have

$$(1 - \delta_k) \| x \|_2^2 \leq \| \Phi x \|_2^2 \leq (1 + \delta_k) \| x \|_2^2, \tag{2}$$

then the matrix Φ is said to satisfy the RIP of order k, and the smallest nonnegative number δ_k in (2) is called restricted isometry constant (RIC) of order k.

In fact, the value of k is associated with the numbers of s and t. Assume x be a k-sparse signal, where $x \in R^t$, and it can be accurately recovered from s measurements. Then an upper bound of the possible sparsity is

$$k \leq Cs/\log(t/s), \tag{3}$$

where C is a constant[10]. Random sensing matrices have achieved the upper bound of k in (3), which could recover sparse signals with high probability[5]. However there are also some drawbacks about random sensing matrices. First of all, random sensing matrices need a lot of storage space to store their entries. Second, there is no efficient algorithm testing whether a random sensing matrix could satisfy the RIP, let alone with high probability. But the deterministic sensing matrices overcome those drawbacks.

Definition 1.2.[11] Let Φ be a matrix with columns u_1, u_2, $\ldots$, u_t, the coherence of Φ is defined as

$$\mu(\Phi) = \max_{i \neq j} \frac{|\langle u_i, u_j \rangle|}{\| u_i \|_2 \cdot \| u_j \|_2}, \quad \text{for} \quad 1 \leq i, j \leq t. \tag{4}$$

As coherence is associated with the RIP, therefore, it is one of essential ingredients in the deterministic constructions.

Lemma 1.3.[12] Suppose Φ is a matrix with coherence μ. Then Φ satisfies the RIP of order k with $\delta_k \leq \mu(k-1)$, whenever $k < \frac{1}{\mu} + 1$.

For an $s \times t$ matrix Φ, there is a famous Welch bound[13]

$$\mu(\Phi) \geq \sqrt{\frac{t-s}{s(t-1)}}, \tag{5}$$

which means that the deterministic constructions based on coherence can only obtain sensing matrices with the RIP of order $k = O(s^{1/2})$.

In recent years, there are some deterministic construction of compressed sensing matrices, which have been presented. DeVore's polynomials over finite fields[14]; Gao's algebraic curves[15]; Amini and Marvasti's bipolar matrix by BCH code[16] and its generalization[17]; Bourgain's additive combina torics[12]; Mahdi Cheraghchi[18] uses the notion of minimum L-wise distance of codes to capture the combinatorial structure of RIP-2 matrices. In this paper, we obtain two cases of deterministic sensing matrices associated with finite subsets of $[n]$ and partial mappings by describing a combinatorial design and instantiating the RIP framework where the latter one is majorization of the former one.

2. Notation

Given positive integers $m \leq n$, $\binom{[n]}{m}$ denote the collection of all m-subsets of $[n]$, where $[n] = \{1, 2, \ldots, n\}$. Then the number of $\binom{[n]}{m}$ equals to $\binom{n}{m}$, where

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}. \tag{6}$$

By convention $\binom{n}{0} = 1$ for all integers n and $\binom{n}{m} = 0$ whenever $m < 0$ or $n < m$.

Let $1 \leq d < m < n$. Note that the number of d-subsets of $[n]$, which are contained in a given m-subset of $[n]$, equals to $\binom{m}{d}$. Denote by $\mathcal{M}(m, n)$ the set of all m-pairs (A, f), where A is a m-subset of $[n]$ and $f : A \to [n]$ is a mapping. The pairs are called partial mappings. For $(A, f) \in \mathcal{M}(m, n)$

and $(B,g) \in \mathcal{M}(d,n)$, the pair (B,g) is called a d-pair of (A,f) if $B \subseteq A$ and $f|_B = g$, where $f|_B$ is the restriction of f on B. If (B,g) is a d-pair of (A,f), we also say that (A,f) contains (B,g).

3. The construction

In this section we obtain two cases of deterministic sensing matrices associated with finite subsets of $[n]$ and partial mappings by describing a combinatorial design and instantiating the RIP framework where the latter one is majorization of the former one, then let us compare the first construction with the case of DeVore and prove that the performance of the given construction is better than that of DeVore for meeting certain conditions.

Definition 3.1. An (t,d,n)-design is a set system $S_1,\cdots,S_t \subseteq [n]$ such that the size of each set is d, where $1 \le i \le t$.

Definition 3.2. Let $\mathcal{D} = \{S_1,\cdots,S_t\}$ be an (t,d,n)-design and $\mathcal{G} = \{T_1,\cdots,T_s\}$ be an (s,m,n)-design, consider the binary $s \times t$ matrix Φ induced by $\mathcal{D}$ and $\mathcal{G}$ where the ith row of Φ is supported on T_i and the jth column of Φ is supported on S_j. We define a_{ij} to denote the elements of Φ where

$$a_{ij} = \begin{cases} 1, & \text{if } T_i \subseteq S_j, \\ 0, & \text{if } T_i \nsubseteq S_j. \end{cases}$$

Construction 1[19] For $0 < d < m \le \lfloor \frac{n}{2} \rfloor$, we define d to denote the d-subsets of $[n]$ and m to denote the m-subsets of $[n]$. Then we obtain a binary $s \times t$ matrix Φ_0, whose constant column weight is ω,where

$$s = \binom{n}{d}, \quad t = \binom{n}{m}, \quad \omega = \binom{m}{d}. \tag{7}$$

Lemma 1 in Appendix tells us that Φ_0 always keeps $s < t$.

Theorem 3.1. Let $0 < d < m \le \lfloor \frac{n}{2} \rfloor$ and $\Phi = \frac{1}{\sqrt{\omega}}\Phi_0$, then Φ is a matrix with coherence $\mu(\Phi) = \frac{m-d}{m}$ and satisfies the RIP of order k with $\delta_k \le \frac{(m-d)(k-1)}{m}$, whenever $k < \frac{m}{m-d} + 1$.

Proof. By the Definition 3.1, we know the number of ones in every column of Φ_0 is the same, which means the value of the denominator in (4) is given, which equals to $\omega = \binom{m}{d}$. In order to obtain the coherence μ of Φ. We only need to calculate the maximum value of $|\ \langle u_i, u_j \rangle\ |$. Meanwhile, let P_1, P_2, $\ldots$, P_t be t distinct columns of Φ. For any two distinct columns P_i and P_j, this also means for any two different m-subsets of $[n]$, which are denoted by $\mathcal{P}_i$ and $\mathcal{P}_j$. As above-mentioned, we want to know the maximum value of $|\ \langle P_i, P_j \rangle\ |$, which also means we want to know the maximum number of d-subsets of $[n]$, which are contained in both $\mathcal{P}_i$ and $\mathcal{P}_j$. In fact, since the intersection of any two subsets is also a subset of $[n]$, hence let $\mid \mathcal{P}_i \bigcap \mathcal{P}_j \mid = m-1$, then the number of d-subsets of $[n]$ is equal to the maximum value $\binom{m-1}{d}$. At last, as the definition of coherence, then

$$\mu(\Phi) = \frac{\binom{m-1}{d}}{\binom{m}{d}} = \frac{m-d}{m}. \tag{8}$$

By the Lemma 1.3, then Φ satisfies the RIP of order k with $\delta_k \leq \frac{(m-d)(k-1)}{m}$, whenever $k < \frac{m}{m-d} + 1$. This completes the proof. □

Example 3.1. Let $n = 2m$ and $m - d = 2$. Then we obtain an $s \times t$ matrix Φ with

$$s = \binom{n}{d} = \binom{2m}{m-2}, \quad t = \binom{n}{m} = \binom{2m}{m}, \quad \mu(\Phi) = \frac{2}{m},$$

which satisfies the RIP of order $k < \frac{m}{2} + 1$. In the view of above-mentioned, we know that

$$\frac{t}{s} = \frac{(m+2)(m+1)}{m(m-1)},$$

then

$$m = \frac{t + 3s + \sqrt{t^2 + s^2 + 14st}}{2(t-s)},$$

Φ can be used to recover signals exactly with sparsity

$$k \leq \frac{t + 3s + \sqrt{t^2 + s^2 + 14st}}{4(t-s)}.$$

Construction 2 For $0 < d < m \leq n-1$, we define d to denote $\mathcal{M}(d, n)$ and m to denote $\mathcal{M}(m, n)$. Denote $t' := t, s' := s$, then we obtain a binary $s' \times t'$ matrix Φ_0', whose constant column weight is ω',where

$$s' = n^d \binom{n}{d}, \quad t' = n^m \binom{n}{m}, \quad \omega' = \binom{m}{d}. \tag{9}$$

Lemma 2 in Appendix tells us that Φ'_0 always keeps $s' < t'$.

Theorem 3.2. Let $0 < d < m \leq n-1$ and $\Phi' = \frac{1}{\sqrt{\omega'}}\Phi'_0$, then Φ' is a matrix with coherence $\mu(\Phi') = \frac{m-d}{m}$ and satisfies the RIP of order k' with $\delta_{k'} \leq \frac{(m-d)(k'-1)}{m}$, whenever $k' < \frac{m}{m-d}+1$.

Proof. By the Definition 3.1, we know the number of ones in every column of Φ'_0 is the same, which means the value of the denominator in (4) is given, which equals to $\omega' = \binom{m}{d}$. In order to obtain the coherence μ of Φ'. We only need to calculate the maximum value of $|\langle u_i, u_j\rangle|$. Let (A_i, f_{ij}) be all the columns of Φ', where $(A_i, f_{ij}) \in \mathcal{M}(m,n), 1 \leq i \leq \binom{n}{m}, 1 \leq j \leq n^m$. For any two different columns $(A_{i_1}, f_{i_1j_1})$ and $(A_{i_2}, f_{i_2j_2})$, this also means for any two different m-pairs of $\mathcal{M}(m,n)$. As above-mentioned, we want to know the maximum value of $|\langle(A_{i_1}, f_{i_1j_1}),(A_{i_2}, f_{i_2j_2})\rangle|$. That is the maximum number of (B,g), where $(B,g) \in \mathcal{M}(d,n)$, which satisfy the conditions that $B \subset A_{i_1}$, $B \subset A_{i_2}$ and $f_{i_1j_1}|_B = f_{i_2j_2}|_B = g$. Firstly, we will think about the condition when $i_1 = i_2 = i$. So we just need to consider the mappings f_{ij_1} and f_{ij_2}. Let f_{ij_1} and f_{ij_2} have the same action on any $m-1$ elements of A_i, then (A_i, f_{ij_1}) and (A_i, f_{ij_2}) can be looked as a $(m-1)$-pair (C, f'), where C exactly has the above-mentioned $m-1$ elements and $f_{ij_1}|_C = f_{ij_2}|_C = f'$. At this moment, we can get the maximum number of (B,g), which equals to $\binom{m-1}{d}$. Secondly, we will consider another condition when $i_1 \neq i_2$. Then there are at most $m-1$ same elements in A_{i_1} and A_{i_2}, not to mention the mappings $f_{i_1j_1}$ and $f_{i_1j_2}$. Hence the maximum number of (B,g) is less than $\binom{m-1}{d}$ under this condition. As the Definition 1.2, then

$$\mu(\Phi') = \frac{\binom{m-1}{d}}{\binom{m}{d}} = \frac{m-d}{m}. \tag{10}$$

By the Lemma 1.3, then Φ' satisfies the RIP of order k' with $\delta_{k'} \leq \frac{(m-d)(k'-1)}{m}$, whenever $k' < \frac{m}{m-d}+1$. This completes the proof. □

Example 3.2. Let $n = m+d$ and $m-d = 2$, then we obtain an $s' \times t'$ matrix Φ' with

$$s' = n^d\binom{n}{d} = (2m-2)^{m-2}\binom{2m-2}{m-2}, \quad t' = n^m\binom{n}{m} = (2m-2)^m\binom{2m-2}{m},$$

$$\mu(\Phi') = \frac{2}{m},$$

which satisfies the RIP of order $k' < \frac{m}{2} + 1$. In view of above-mentioned, we know that

$$\frac{t'}{s'} = (2m-2)^2,$$

then

$$m = \frac{1}{2}\sqrt{\frac{t'}{s'}} + 1,$$

Φ' can be used to recover signals exactly with sparsity

$$k' \le \frac{1}{4}\sqrt{\frac{t'}{s'}} + \frac{1}{2}.$$

Next, we will find out some certain conditions when the performance of Construction 1 is better than that of DeVore.

First of all, let's retrospect the DeVore's construction[14]. DeVore presents a construction of matrices using polynomials over finite fields. Let $\mathbb{F}_p$ be a finite field, where p is a prime. Given an integer r, where $0 < r < p$, let $\mathbb{P}_r$ be the set $\{f(x)|\partial(f(x)) \le r, x \in \mathbb{F}_p\}$. There are p^{r+1} such polynomials. Any polynomial $Q \in \mathbb{P}_r$, which is regarded as a mapping of $\mathbb{F}_p$ to $\mathbb{F}_p$, then its graph $\mathfrak{G}(Q)$ is the set of ordered pairs $(x, Q(x)), x \in \mathbb{F}_p$, which is a subset of $\mathbb{F}_p \times \mathbb{F}_p$. Let $\Phi_0{}^*$ be the binary matrix with rows indexed with ordering the elements of $\mathbb{F}_p \times \mathbb{F}_p$ lexicographically as $(0,1), (0,2), \ldots, (p-1, p-1)$ and columns indexed with the polynomials of $\mathbb{P}_r$, such that $\Phi_0{}^*(i,j) = 1$ if and only if $Q(i) = j$, where the j-th column is indexed by Q. Then $\Phi_0{}^*$ is a $p^2 \times p^{r+1}$ matrix.

Lemma 3.1.[14] Suppose the matrix $\Phi^* = \frac{1}{\sqrt{p}}\Phi_0{}^*$, then Φ^* satisfies the RIP with $\delta_{k^*} = (k^* - 1)r/p$ for any $k^* < p/r + 1$.

As a matter of fact, many experts have studied the properties of DeVore's polynomials deterministic matrices. They find that this construction has some drawbacks. First, the time to compute the matrix itself is long. Second, every column exactly has p ones. That means there are more nonzero entries in the larger matrices, which makes the compressed signals require a lot of storage space and expands large amounts of costing of transmission signals. (see [20])

As above-mentioned problems, we consider the performance of compressed sensing matrices by three kinds of parameters, they are a, k, and $\frac{t}{s}$. Here we define $a = \omega/s$ to denote the sparity of sensing matrices. Given the value of k, the sensing matrix is better when the value of a is smaller, which contributes to overcoming the above drawbacks(see [21]), the matrix is also better when the value of $\frac{t}{s}$ is larger, which means this matrix has more powerfully compressed properties.

By Theorem 3.1 and (7), we get an $s \times t$ sensing matrix Φ with

$$s = \binom{n}{d}, \quad t = \binom{n}{m}, \quad \frac{t}{s} = \frac{\binom{n}{m}}{\binom{n}{d}}, \quad k \leq \frac{m}{m-d}, \quad a = \frac{\omega}{s} = \frac{\binom{m}{d}}{\binom{n}{d}}.$$

Meanwhile, according to the description of Devore' construction, we also have an $s^* \times t^*$ sensing matrix Φ^* with

$$s^* = p^2, \quad t^* = p^{r+1}, \quad \frac{t^*}{s^*} = p^{r-1}, \quad k^* \leq \frac{p}{r}, \quad a^* = \frac{\omega^*}{s^*} = \frac{1}{p},$$

where $1 < r < p$ and p is a prime.

Theorem 3.3. Given the matrices Φ and Φ^*. Suppose k and k^* are equal to their upper bound values, respectively, which means $k = \frac{m}{m-d}$ and $k^* = \frac{p}{r}$. Let them be equal to each other and then $a < a^*$ when $r < \frac{(m-d)\binom{n}{d}}{m\binom{m}{d}}$.

Proof. As the description of conditions, since $k = k^*$, then $\frac{m}{m-d} = \frac{p}{r}$. Since $a^* = \frac{1}{p}$, then $a^* = \frac{m-d}{rm}$. Compare $a = \binom{m}{d}/\binom{n}{d}$ and $a^* = \frac{m-d}{rm}$. Then we have $a < a^*$ when $r < \frac{(m-d)\binom{n}{d}}{m\binom{m}{d}}$. So our construction has the better sparsity of sensing matrices. □

Theorem 3.4. Given the matrices Φ and Φ^*. Let k and k^* be equal to their upper bound values, respectively, which means $k = \frac{m}{m-d}$ and $k^* = \frac{p}{r}$. Denote $k = k^* = \frac{m}{m-d} = \frac{p}{r}$ and then $\frac{t}{s} > \frac{t^*}{s^*}$ when

$$r < \min\{\frac{(n-d)(m-d)}{m^2}, m-d+1\},$$

where $n > m + d + \frac{md}{m-d}$.

Proof. According to the above description, since $\frac{m}{m-d} = \frac{p}{r}$ and $\frac{t^*}{s^*} =$

p^{r-1}, then $\frac{t^*}{s^*} = (\frac{rm}{m-d})^{r-1}$. In the meantime, since

$$\begin{aligned}\frac{t}{s} &= \frac{\binom{n}{m}}{\binom{n}{d}} \\ &= \frac{(n-m+1)(n-m+2)\cdot\cdots\cdot(n-d)}{(d+1)(d+2)\cdot\cdots\cdot m} \\ &= \frac{n-m+1}{d+1}\cdot\frac{n-m+2}{d+2}\cdot\cdots\cdot\frac{n-d}{m} \\ &\geq (\frac{n-d}{m})^{m-d},\end{aligned}$$

where $\frac{n-d}{m} < \cdots < \frac{n-m+2}{d+2} < \frac{n-m+1}{d+1}$, obviously, then let's compare $(\frac{n-d}{m})^{m-d}$ and $(\frac{rm}{m-d})^{r-1}$ by contrasting their base numbers and powers, respectively. Let $\frac{n-d}{m} \geq \frac{rm}{m-d}$ and $m-d > r-1$, then we have $r \leq \frac{(n-d)(m-d)}{m^2}$ and $r < m-d+1$. Hence we have $\frac{t}{s} \geq (\frac{n-d}{m})^{m-d} > \frac{t^*}{s^*}$ when $r < \min\{\frac{(n-d)(m-d)}{m^2}, m-d+1\}$. □

At the end of this section, we prove that Construction 2 is majorization of Construction 1. Given the integers $0 < d < m \leq \lfloor\frac{n}{2}\rfloor$, then by Theorem 3.1 and (7), we can get an $s \times t$ sensing matrix Φ with

$$s = \binom{n}{d}, \quad t = \binom{n}{m}, \quad \frac{t}{s} = \frac{\binom{n}{m}}{\binom{n}{d}}, \quad k \leq \frac{m}{m-d}, \quad a = \frac{\omega}{s} = \frac{\binom{m}{d}}{\binom{n}{d}}.$$

Meanwhile, by Theorem 3.2 and (9), we also obtain an $s' \times t'$ matrix Φ' with

$$s' = n^d\binom{n}{d}, \quad t' = n^m\binom{n}{m}, \quad \frac{t'}{s'} = n^{m-d}\frac{\binom{n}{m}}{\binom{n}{d}}, \quad k' \leq \frac{m}{m-d},$$

$$a' = \frac{\omega'}{s'} = \frac{\binom{m}{d}}{n^d\binom{n}{d}}.$$

Theorem 3.5. Given the matrices Φ and Φ'. Let k and k' be equal to their upper bound values, respectively, which means $k = k' = \frac{m}{m-d}$. Then $a' < a$.

Proof. As the above-mentioned, denote $k = k' = \frac{m}{m-d}$. Then compare $a = \binom{m}{d}/\binom{n}{d}$ and $a' = \binom{m}{d}/(n^d\binom{n}{d})$. Obviously, $a/a' = n^d > 1$, so the matrix Φ' has the better sparsity than Φ. □

Theorem 3.6. Given the matrices Φ and Φ'. Let k and k' be equal to their upper bound values, respectively, which means $k = k' = \frac{m}{m-d}$. Then $t/s < t'/s'$.

Proof. The same as above, denote $k = k' = \frac{m}{m-d}$. Then compare $t/s = \binom{n}{m}/\binom{n}{d}$ and $t'/s' = (n^m\binom{n}{m})/(n^d\binom{n}{d})$. Apparently, $\{(n^m\binom{n}{m})/(n^d\binom{n}{d})\}$: $(\binom{n}{m}/\binom{n}{d}) = n^{m-d} > 1$, therefore the matrix Φ' is better than Φ in terms of compressing signals. □

We find that the latter construction is perfectly better than the former one. By changing the numbers of d, m, n, we can obtain a family of distinct sensing matrices.

4. Conclusion

In this paper, we present a new method to construct deterministic compressed sensing matrices by using finite subset and partial mappings. By meeting some certain conditions, our constructions are better than DeVore's method using polynomials over finite fields. We can also use subspaces over finite fields[22] to construct matrices based on this method, which gives great flexibility and offers more choices for the construction of sensing matrices. *Candès* and *Tao* once suggested that the CS framework leads to an encryption scheme[5], where a sensing matrix can be used as an encryption key. This may be highly valuable for the potential use of sensing matrix in the area of cryptography.

However, We believe that our construction still has much potential. Generally, binary sensing matrices are not good candidates in CS since all the entries are nonnegative. Using p-ary BCH codes, some contributions have been made in the direction to generate nonbinary sensing matrices[17]. Therefore, constructing nonbinary sensing matrices with algebraic curves is very interesting. At the same time, Mahdi Cheraghchi[18] uses the notion of minimum L-wise distance of codes to capture the combinatorial structure of RIP-2 matrices. These methods make great contribution and is worth studying in the future.

Appendix

Lemma 1 Given integers $0 \leq m \leq n$, the sequence $\binom{n}{m}$ is unimodal and gets its peak at $m = \lfloor \frac{n}{2} \rfloor$.

Proof. According to (6), we know that if $m_1 < m_2$, then

$$\frac{\begin{pmatrix} n \\ m_1 \end{pmatrix}}{\begin{pmatrix} n \\ m_2 \end{pmatrix}} = \frac{n!}{m_1!(n-m_1)!} \times \frac{m_2!(n-m_2)!}{n!}$$

$$= \frac{(m_1+1)(m_1+2)\ldots m_2}{(n-m_1)(n-m_1-1)\ldots(n-m_2+1)}$$

$$= \frac{m_1+1}{n-m_1} \cdot \frac{m_1+2}{n-m_1-1} \cdot \cdots \cdot \frac{m_2}{n-m_2+1},$$

where $\frac{m_1+1}{n-m_1} < \frac{m_1+2}{n-m_1-1} < \cdots < \frac{m_2}{n-m_2+1}$.

If $m_2 \leq \lfloor \frac{n}{2} \rfloor$, then $m_2 < n - m_2 + 1$, $\frac{m_2}{n-m_2+1} < 1$. Hence, when $0 \leq m_1 < m_2 \leq \lfloor \frac{n}{2} \rfloor$, we have $\frac{\begin{pmatrix} n \\ m_1 \end{pmatrix}}{\begin{pmatrix} n \\ m_2 \end{pmatrix}} < 1$.

If $m_1 \geq \lfloor \frac{n}{2} \rfloor$, then $m_1 + 1 > n - m_1$, $\frac{m_1+1}{n-m_1} > 1$. Hence, when $\lfloor \frac{n}{2} \rfloor \leq m_1 < m_2 \leq n$, we have $\frac{\begin{pmatrix} n \\ m_1 \end{pmatrix}}{\begin{pmatrix} n \\ m_2 \end{pmatrix}} > 1$. □

Lemma 2 Given integers $0 \leq m < n$, the sequence $n^m\binom{n}{m}$ is increasing strictly.

Proof. By (6), if $m_1 < m_2$, then we have

$$\frac{n^{m_1}\begin{pmatrix} n \\ m_1 \end{pmatrix}}{n^{m_2}\begin{pmatrix} n \\ m_2 \end{pmatrix}} = \frac{1}{n^{m_2-m_1}} \times \frac{(m_1+1)(m_1+2)\ldots m_2}{(n-m_1)(n-m_1-1)\ldots(n-m_2+1)}$$

$$= \frac{m_1+1}{n(n-m_1)} \cdot \frac{m_1+2}{n(n-m_1-1)} \cdot \cdots \cdot \frac{m_2}{n(n-m_2+1)},$$

where $\frac{m_1+1}{n(n-m_1)} < \frac{m_1+2}{n(n-m_1-1)} < \cdots < \frac{m_2}{n(n-m_2+1)}$.

Since $m_2 < n$, then $m_2(n+1) < n(n+1)$, $m_2 < n^2 + n - nm_2$,

$\frac{m_2}{n(n-m_2+1)} < 1$. Hence, when $0 \leq m_1 < m_2 < n$, we have $\frac{n^{m_1}\binom{n}{m_1}}{n^{m_2}\binom{n}{m_2}} <$ 1. □

Acknowledgements This work is supported by the Fundamental Research Funds for the Central Universities (3122015L008).

References

[1] D. Donoho. Compressed sensing. IEEE Trans. Inf. Theory, 2006, 52(4) : 1289 – 1306.

[2] E. Candès, J. Romberg, T. Tao. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory, 2006, 52(2) : 489 – 509.

[3] B. K. Natarajan. Sparse approximate solutions to linear systems. SIAM J. Comput, 1995, 24(2) : 227 – 234.

[4] J. Tropp, A. Gilbert. Signal recovery from random measurements via orthogonal matching pursuit. IEEE Trans. Inf. Theory, 2007, 53(12) : 4655 – 4666.

[5] E. Candès, T. Tao. Near-optimal signal recovery from random projections: Universal encoding strategies. IEEE Trans. Inf. Theory, 2006, 52(12) : 5406 – 5425.

[6] E. Candès, J. Romberg, T. Tao. Stable signal recovery from incomplete and inaccurate measurement. Communications on Pure and Applied Mathematices, 2006, 59(8) : 1207 – 1223.

[7] Y. Tsaig, D. Donoho. Extensions of compressed sensing. Signal Processing, 2006, 86(3) : 549 – 571.

[8] E. Candès, T. Tao. Decoding by linear programming. IEEE Trans. Inf. Theory, 2005, 51(12) : 4203 – 4215.

[9] E. Candès. The restricted isometry property and its implications for compressed sensing. Comptes Rendus Math. Acad. Sci. Paris, 2008, 346(9 – 10) : 589 – 592.

[10] A. Cohen, W. Dahmen, R. Devore. Compressed sensing and best k-term approximation. J. Amer. Math. Soc, 2009, 22(1) : 211 – 231.

[11] J. Troop. Greed is good: Algorithmic result for sparse approximation. IEEE Trans. Inf. Theory, 2004, 50(10) : 2231 – 2242.

[12] J. Bourgain, S. Dilworth, K. Ford, D. Kutzarova. Explicit constructions of RIP matrices and related problems. Duke Math. J, 2011, 159(1) : 145 – 185.

[13] L. Welch. Lower bounds on the maximum cross correlation of signals. IEEE Trans. Inf. Theory, 1974, 20(3) : 397 – 399.

[14] R. Devore. Deterministic constructions of compressed sensing matrices. J. Complexity, 2007, 23(4 – 6) : 918 – 925.

[15] Li S, Gao F, Ge G, Zhang S. Deterministic construction of compressed sensing matrices via algebraic curves. IEEE Trans. Inf. Theory, 2012, 58(8) : 5035 – 5041.

[16] A. Amini, F. Marvasti. Deterministic construction of binary, bipolar and ternary compressed sensing matrices. IEEE Trans. Inf. Theory, 2011, 57(4) : 2360 – 2370.

[17] A. Amini, V. Montazerhodjat, F. Marvasti. Matrices with small coherence using *p*-ary block codes. IEEE Trans. Signal Processing, 2012, 60(1) : 172 – 181.

[18] M. Cheraghchi. Coding-theretic method for sparse recovery. arXiv: 2012, 1110.0279.

[19] A.J. Macula. A simple construction of *d*-disjunct matrices with certain constant weights. Discrete Math, 1996, 162 : 311 – 312.

[20] Li X. Research on measurement matrix based on compressed sensing. Beijing Jiaotong University, thesis of Master Degree, 2010 : 25 – 31.

[21] Wu H, Zhang X, Chen W. Measurement matrices in compressed sensing theory. Journal of military communication technology, 2012, 33(1) : 90 – 94.

[22] Wan Z. Geometry of classical groups over finite fields, 2nd edn. Science, Beijing. 2002.