New Construction of Deterministic Compressed Sensing Matrices via Singular Linear Spaces over Finite Fields

XUEMEI LIU
College of Science
Civil Aviation University of China
Tianjin,300300
CHINA
xm-liu771216@163.com

YINGMO JIE
College of Science
Civil Aviation University of China
Tianjin,300300
CHINA
asdfzxcv41371988@126.com

Abstract: As an emerging approach of signal processing, not only has compressed sensing (CS) successfully compressed and sampled signals with few measurements, but also has owned the capabilities of ensuring the exact recovery of signals. However, the above-mentioned properties are based on the (compressed) sensing matrices. Hence the construction of sensing matrices is the key problem. Compared with the intensive study of random sensing matrices, only a few deterministic constructions are known. In this paper, we provide a family of new construction of deterministic sensing matrices via singular linear spaces over finite fields, and show its better performance than Devore's construction using polynomials over finite fields.

Key–Words: Compressed sensing matrices, Singular linear spaces, Coherence, Restricted isometry property (RIP).

1 Introduction

The traditional Nyquist [1] 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 [2] and Candës [3] 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 $y = \Phi x$

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

This l_0-minimization is a combinatorial minimization problem and is normally NP-hard [4]. In fact, this kind of method [5] has been used widely. Whereas, CS provides a mighty method to reconstruct sparse signals with applicable algorithms and guarantees the number of measurements $s \ll t$.

A signal x is said to be k-sparse if the maximum number of nonzero entries of it equals to k. As we all know that the reconstruction of a sparse signal[6] plays a significant in the signal processing field. Pursuing greedy algorithms for l_0-minimization (1) is one method to reconstruct k-sparse signals. There is a famous pursuing greedy algorithm called orthogonal matching pursuit (OMP) [7]. 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 reconstruct x from (1) with probability surpassing $1 - 2\delta$. However, due to the success of the recovery process depending heavily on the property of the sensing matrix, sensing matrix plays an important role in the recovery of signals. There are two kinds of sensing 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 [8, 9, 10]. Another is named deterministic sensing matrices, whose properties are better than random sensing matrices'. Then another problem emerges: What kinds of matrices are appropriate? They must ensure that the prominent information in any k-sparse or compressible signal cannot be damaged by the dimensionality reduction from $x \in R^t$ down to $y \in R^s$. In order to guarantee this problem, Candés and Tao [11] have introduced a criterion, named restricted isometry property (RIP).

Definition 1. *[12] 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*

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

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.

Actually, suppose that a sensing matrix satisfies the RIP and its RIC is small enough, then OMP can recover sparse signals exactly [13]. Adversely, if a sensing matrix does not meet the RIP, we cannot ascertain if it could recover the signal or not. There is a relationship among sparsity k, s and t. Given a k-sparse signal $x \in R^t$, which can be accurately recovered from s measurements. Then an upper bound of the possible sparsity is

$$k \leq Cs/\log(t/s), \quad (3)$$

where C is a constant [14]. Thanks to the randomness of entries of random sensing matrices, the upper bound of k in (3) has been achieved by random sensing matrices, which could recover sparse signals with high probability[8]. Whereas, there are also some deficiencies about random sensing matrices. First, 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 or not, let alone with high probability. But the deterministic sensing matrices conquer those deficiencies.

Definition 2. *[15] Let Φ be a matrix with columns u_1, u_2, …, u_t, the coherence of Φ is defined as*

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

As a coherence can be looked as an equivalent form of the RIP, it is an important issue in the deterministic constructions.

Lemma 3. *[16] 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 [17]

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

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

Briefly, There are two steps about CS theory. In the first step, we design a CS matrix Φ that ensures 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 $y \in R^s$. In the second step, we develop a reconstruction algorithm to recover x from the measurements y. Here, we put our focus on the first step.

Recently, some deterministic constructions of sensing matrices have been presented. Devore's polynomials over finite fields[18]; Gao F's algebraic curves [19]; Amini and Marvasti's bipolar matrix by BCH code [20] and its generalization [21]; Bourgain's additive combinatorics[16]. In this paper, we construct one kind of deterministic construction based on singular linear spaces over finite fields, and show its excellent properties.

2 Singular linear spaces

In this section we shall introduce the concepts of subspaces of type (m, h) in singular linear space, (see Wang et al. [22]) and provide several lemmas. Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. For two non-negative integers n and l, $\mathbb{F}_q^{(n+l)}$ denotes the $(n+l)$-dimensional row vector space over $\mathbb{F}_q$. The set of all $(n+l) \times (n+l)$ nonsingular matrices over $\mathbb{F}_q$ of the form

$$\begin{pmatrix} T_{11} & T_{12} \\ 0 & T_{22} \end{pmatrix},$$

where T_{11} and T_{22} are nonsingular $n \times n$ and $l \times l$ matrices, respectively, forms a group under matrix multiplication, called the singular general linear group of degree $n + l$ over $\mathbb{F}_q$ and denoted by $GL_{n+l,n}(\mathbb{F}_q)$. If $l = 0$ (resp. $n = 0$), $GL_{n,n}(\mathbb{F}_q) = GL_n(\mathbb{F}_q)$ (resp. $GL_{l,0}(\mathbb{F}_q) = GL_l(\mathbb{F}_q)$) is the general linear group of degree n (resp. l) (See Wan [23]).

Let P be a m-dimensional subspace of $\mathbb{F}_q^{(n+l)}$, denote also by P an $m \times (n+l)$ matrix of rank m whose rows span the subspace P and call the matrix P a matrix representation of the subspace P. There is an action of $GL_{n+l,n}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(n+l)}$ defined as follows

$$\begin{aligned} &\mathbb{F}_q^{(n+l)} \times GL_{n+l,n}(\mathbb{F}_q) \to \mathbb{F}_q^{(n+l)} \\ &((x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+l}), T) \mapsto \\ &(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+l})T. \end{aligned}$$

The above action induces an action on the set of subspaces of $\mathbb{F}_q^{(n+l)}$, i.e., a subspace P is carried by

$T \in GL_{n+l,n}(\mathbb{F}_q)$ to the subspace PT. The vector space $\mathbb{F}_q^{(n+l)}$ together with the above group action, is called the $(n+l)$-dimensional singular linear space over $\mathbb{F}_q$. For $1 \le j \le n+l$, let e_j be the row vector in $\mathbb{F}_q^{(n+l)}$ whose j-th coordinate is 1 and all other coordinates are 0. Denote by E the l-dimensional subspace of $\mathbb{F}_q^{(n+l)}$ generated by $e_{n+1}, e_{n+2}, \dots, e_{n+l}$. A m-dimensional subspace P of $\mathbb{F}_q^{(n+l)}$ is called a subspace of type (m,h) if $\dim(P \cap E) = h$. The collection of all the subspaces of types $(m,0)$ in $\mathbb{F}_q^{(n+l)}$, where $0 \le m \le n$, is the attenuated space. (see A.E. Brouwer et al. [24]

Lemma 4. *Let V denote the $(n+l)$-dimensional row vector space over a finite field $\mathbb{F}_q$, and fix a subspace W of type $(n+l-d,h)$ contained in V. Let $\mathcal{M}_+(i_1,h_1;d,h;n+l,n)$ denote the set of all subspaces U of type (i_1,h_1) contained in V satisfying $U+W=V$, and let $N_+(i_1,h_1;d,h;n+l,n)$ denote the size of $\mathcal{M}_+(i_1,h_1;d,h;n+l,n)$. Then*

$$N_+(i_1,h_1;d,h;n+l,n) = q^{d(n+l-i_1)} \begin{bmatrix} n+l-d-h \\ i_1-h_1-d \end{bmatrix}_q \begin{bmatrix} h \\ h_1 \end{bmatrix}_q . \quad (6)$$

Proof. By the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$ on the set of subspaces of the same type, we may choose the subspace W of type $(n+l-d,h)$ as the form

$$\begin{pmatrix} I^{(n+l-d-h)} & 0^{(n+l-d-h,d+h-l)} & 0 & 0 \\ 0 & 0 & I^{(h)} & 0^{(h,l-h)} \end{pmatrix}.$$

Let U has a matrix representation of the form

$$\begin{pmatrix} X^{(i_1-d-h_1,n+l-d-h)} & 0^{(i_1-d-h_1,d+h-l)} & 0 & 0 \\ Y^{(d,n+l-d-h)} & I^{(d+h-l)} & B^{(d,h)} & I^{(d,l-h)} \\ 0^{(h_1,n+l-d-h)} & 0 & A^{(h_1,h)} & 0^{(h_1,l-h)} \end{pmatrix}$$

where X is an $(i_1-d-h_1)\times(n+l-d-h)$ matrix of rank (i_1-d-h_1), Y is a $d\times(n+l-d-h)$ matrix, A is an $h_1 \times h$ matrix of rank h_1, B is a $d \times h$ matrix. Then X is an (i_1-d-h_1)-subspace which contained in $I^{(n+l-d-h)}$. By Wan ([23, 2002b, Theorem 1.7]), there are $\begin{bmatrix} n+l-d-h \\ i_1-h_1-d \end{bmatrix}_q$ choices for X. By the same token, A is an h_1-subspace which contained in $I^{(h)}$ and has $\begin{bmatrix} h \\ h_1 \end{bmatrix}_q$ choices. By the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$, we may let

$$X = (I^{(i_1-d-h_1)} \quad 0^{(i_1-d-h_1,n+l-h-i_1+h_1)}),$$

and

$$A = (I^{(h_1)} \quad 0^{(h_1,h-h_1)}).$$

Then U has the unique matrix representation of the form

$$\begin{pmatrix} I^{(\alpha)} & 0^{(\alpha,\beta)} & 0^{(\alpha,\gamma)} & 0^{(\alpha,h_1)} & 0 & 0 \\ 0 & Y_1^{(d,\beta)} & 0^{(d,\gamma)} & 0^{(d,h_1)} & B_1^{(d,h-h_1)} & 0^{(d,l-h)} \\ 0^{(h_1,\alpha)} & 0 & 0^{(h_1,\gamma)} & I^{(h_1)} & 0 & 0^{(h_1,l-h)} \end{pmatrix}.$$

where $\alpha = i_1-d-h_1$, $\beta = n+l-h-i_1+h_1$ and $\gamma = h+d-l$. Hence

$$N_+(i_1,h_1;d,h;n+l,n) = q^{d(n+l-i_1)} \begin{bmatrix} n+l-d-h \\ i_1-h_1-d \end{bmatrix}_q \begin{bmatrix} h \\ h_1 \end{bmatrix}_q .$$

□

Lemma 5. *Let V denote the $(n+l)$-dimensional row vector space over a finite field $\mathbb{F}_q$, and fix a subspace W of type $(n+l-d,h)$ contained in V. For a given subspace U_2 of type (i_2,h_2) contained in V satisfying $U_2+W=V$, let $u(n+l,d,h;i_1,h_1;i_2,h_2)$ denote the number of subspaces U_1 of type (i_1,h_1) contained in V satisfying $U_1+W=V$ and $U_1 \subseteq U_2$. Then*

$$u(n+l,d,h;i_1,h_1;i_2,h_2) = q^{d(i_2-i_1)} \begin{bmatrix} i_2-d-h_2 \\ i_1-h_1-d \end{bmatrix}_q \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q . \quad (7)$$

Proof. Since the subgroup $GL_{n+l,n}(\mathbb{F}_q)_W$ of $GL_{n+l,n}(\mathbb{F}_q)$ fixing W acts transitively on the set $\{U|U+W=V, \dim U = i_2\}$, the number $u(n+l,d,h;i_1,h_1;i_2,h_2)$ depends only on i_1 and i_2. By Lemma 2.1 and (6), we get

$$u(n+l,d,h;i_1,h_1;i_2,h_2) = q^{d(i_2-i_1)} \begin{bmatrix} i_2-d-h_2 \\ i_1-h_1-d \end{bmatrix}_q \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q .$$

□

Lemma 6. *Let V denote the $(n+l)$-dimensional row vector space over a finite field $\mathbb{F}_q$, and fix a subspace W of type $(n+l-d,h)$ contained in V. For a given subspace U_1 of type (i_1,h_1) contained in V satisfying $U_1+W=V$, let $u'(n+l,d,h;i_1,h_1;i_2,h_2)$ denote the number of subspaces U_2 of type (i_2,h_2) contained in V satisfying $U_2+W=V$ and $U_1 \subseteq U_2$. Then*

$$u'(n+l,d,h;i_1,h_1;i_2,h_2) = \begin{bmatrix} n+l-h-i_1+h_1 \\ i_2-h_2-i_1+h_1 \end{bmatrix}_q \begin{bmatrix} h-h_1 \\ h_2-h_1 \end{bmatrix}_q . \quad (8)$$

Proof. Let

$$M = \left\{ (U_1, U_2) \middle| \begin{array}{l} U_1 \in \mathcal{M}_+(i_1, h_1; d, h; n+l, n), \\ U_2 \in \mathcal{M}_+(i_2, h_2; d, h; n+l, n), \\ U_1 \subseteq U_2 \end{array} \right\}.$$

We compute the size of M in the following two ways.

For a fixed subspace U_1 of type (i_1, h_1), there are $u'(n+l, d, h; i_1, h_1; i_2, h_2)$ subspaces of type (i_2, h_2) containing U_1. By Lemma 4

$$\begin{aligned} |M| &= u'(n+l, d, h; i_1, h_1; i_2, h_2) \\ &N_+(i_1, h_1; d, h; n+l, n). \end{aligned} \tag{9}$$

For a fixed subspace U_2 of type (i_2, h_2), there are $u(n+l, d, h; i_1, h_1; i_2, h_2)$ subspaces of type (i_1, h_1) contained in U_2. By Lemma 4

$$\begin{aligned} |M| &= u(n+l, d, h; i_1, h_1; i_2, h_2) \\ &N_+(i_2, h_2; d, h; n+l, n). \end{aligned} \tag{10}$$

Combining (9), (10), (7) and (6), (8) holds. □

Lemma 7. *Given integers* $0 \leq h_1 \leq h \leq l$ *and* $d \leq i - h_1 \leq n+l-h \leq n+d$*, the sequence* $N_+(i, h_1; d, h; n+l, n)$ *is unimodal and gets its peak at* $i = \lfloor \frac{n+l-h}{2} \rfloor + h_1$*.*

Proof. By Lemma 4, if $i_1 < i_2$, then we have

$$\begin{aligned} & \frac{N_+(i_1, h_1; d, h; n+l, n)}{N_+(i_2, h_1; d, h; n+l, n)} \\ = & \frac{q^{d(n+l-i_1)} \begin{bmatrix} n+l-d-h \\ i_1 - h_1 - d \end{bmatrix}_q \begin{bmatrix} h \\ h_1 \end{bmatrix}_q}{q^{d(n+l-i_2)} \begin{bmatrix} n+l-d-h \\ i_2 - h_1 - d \end{bmatrix}_q \begin{bmatrix} h \\ h_1 \end{bmatrix}_q} \\ = & q^{d(i_2-i_1)} \cdot \frac{\prod_{i=i_1-h_1-d+1}^{i_2-h_1-d} (q^i - 1)}{\prod_{i=n+l-h-i_2+h_1+1}^{n+l-h-i_1+h_1} (q^i - 1)} \\ = & \frac{(q^{i_1-h_1+1} - q^d) \cdots (q^{i_2-h_1} - q^d)}{(q^{n+l-h-i_2+h_1+1} - 1) \cdots (q^{n+l-h-i_1+h_1} - 1)} \\ = & \frac{q^{i_1-h_1+1} - q^d}{q^{n+l-h-i_1+h_1} - 1} \cdots \frac{q^{i_2-h_1} - q^d}{q^{n+l-h-i_2+h_1+1} - 1}, \end{aligned}$$

where

$$\begin{aligned} & \frac{q^{i_1-h_1+1} - q^d}{q^{n+l-h-i_1+h_1} - 1} < \frac{q^{i_1-h_1+2} - q^d}{q^{n+l-h-i_1+h_1-1} - 1} \\ & < \cdots < \frac{q^{i_2-h_1} - q^d}{q^{n+l-h-i_2+h_1+1} - 1}. \end{aligned}$$

If $i_2 \leq \lfloor \frac{n+l-h}{2} \rfloor + h_1$, then

$$i_2 - h_1 < n + l - h - i_2 + h_1 + 1,$$

$$\frac{q^{i_2-h_1} - q^d}{q^{n+l-h-i_2+h_1+1} - 1} < 1.$$

Hence, when

$$h_1 + d \leq i_1 < i_2 \leq \lfloor \frac{n+l-h}{2} \rfloor + h_1,$$

we have

$$\frac{N_+(i_1, h_1; d, h; n+l, n)}{N_+(i_2, h_1; d, h; n+l, n)} < 1.$$

If $i_1 \geq \lfloor \frac{n+l-h}{2} \rfloor + h_1$, then

$$i_1 - h_1 + 1 > n + l - h - i_1 + h_1,$$

and

$$\frac{q^{i_1-h_1+1} - q^d}{q^{n+l-h-i_1+h_1} - 1} > 1.$$

Hence, when

$$\lfloor \frac{n+l-h}{2} \rfloor + h_1 \leq i_1 < i_2 \leq n + l - h + h_1,$$

we have $\frac{N_+(i_1,h_1;d,h;n+l,n)}{N_+(i_2,h_1;d,h;n+l,n)} > 1$. □

3 The construction

In this section, we will put forward a type of deterministic sensing matrix associated with subspaces of $\mathbb{F}_q^{(n+l)}$, and show it is superior to Devore's construction using polynomials over finite fields.

Definition 8. *Given integers* $0 \leq h_1 \leq h_2 \leq \lfloor \frac{h}{2} \rfloor$*,* $h \leq l$*, and* $d = i_1 - h_1 < i_2 - h_2 \leq \lfloor \frac{n+l-h}{2} \rfloor$*. Let* Φ_0 *be the binary matrix, whose rows are indexed by* $\mathcal{M}_+(i_1, h_1; d, h; n+l, n)$*, whose columns are indexed by* $\mathcal{M}_+(i_2, h_2; d, h; n+l, n)$*, and with a* 1 *or* 0 *in the* (b, j) *position of the matrix, if the* b*-th subspace which belongs to* $\mathcal{M}_+(i_1, h_1; d, h; n+l, n)$ *is or is not contained in the* j*-th subspace which belongs to* $\mathcal{M}_+(i_2, h_2; d, h; n+l, n)$*, respectively.*

By the Lemmas 4 and 5, Φ_0 is an $s \times t$ matrix, whose constant column weight is ω, where

$$\begin{aligned} s &= q^{(i_1-h_1)(n+l-i_1)} \begin{bmatrix} h \\ h_1 \end{bmatrix}_q, \\ t &= q^{(i_1-h_1)(n+l-i_2)} \begin{bmatrix} n+l-i_1+h_1-h \\ i_2-h_2-i_1+h_1 \end{bmatrix}_q \begin{bmatrix} h \\ h_2 \end{bmatrix}_q, \\ \omega &= q^{(i_1-h_1)(i_2-i_1)} \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q. \end{aligned} \tag{11}$$

Theorem 9. *Let* $0 \leq h_1 \leq h_2 \leq \lfloor \frac{h}{2} \rfloor$, $h \leq l$, $d = i_1 - h_1 < i_2 - h_2 \leq \lfloor \frac{n+l-h}{2} \rfloor$ *and* $\Phi = \frac{1}{\sqrt{\omega}}\Phi_0$, *then* Φ *is a matrix with coherence* $\mu(\Phi) = \frac{1}{q^{i_1-h_1}}$ *and satisfies the RIP of order* k *with* $\delta_k \leq \frac{(k-1)}{q^{i_1-h_1}}$, *whenever* $k < q^{i_1-h_1} + 1$.

Proof. According to Definition 3.1, we know that the number of ones in every column of Φ_0 is the same, that means the value of the denominator in (4) is given, which equals to $\omega = q^{(i_1-h_1)(i_2-i_1)} \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q$. Hence we only need to calculate the maximum value of $|\langle u_b, u_j \rangle|$, and then we can obtain the coherence μ of Φ. Let $P_1, P_2, \ldots, P_t$ be t distinct columns of Φ. For any two distinct columns P_b and P_j, this also means for any two different subspaces $\mathcal{P}_b$ and $\mathcal{P}_j$, where $\mathcal{P}_b, \mathcal{P}_j \in \mathcal{M}_+(i_2, h_2; d, h; n+l, n)$. As above-mentioned, we want to know the maximum value of $|\langle P_b, P_j \rangle|$, in other words, we want to know the maximum number of subspaces $\mathcal{U}$, where $\mathcal{U} \in \mathcal{M}_+(i_1, h_1; d, h; n+l, n)$ and contained in both $\mathcal{P}_b$ and $\mathcal{P}_j$. Actually, since the intersection of any two subspaces is also a subspace, hence let $\mathcal{P} = \mathcal{P}_b \bigcap \mathcal{P}_j$, where $|\mathcal{P}| = i_2 - 1$ and the left one is not contained in E, then $\mathcal{P} \in \mathcal{M}_+(i_2-1, h_2; d, h; n+l, n)$. Hence the maximum number of subspaces $\mathcal{U}$, which contained in $\mathcal{P}$, is equal to $q^{(i_1-h_1)(i_2-1-i_1)} \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q$. At last, as the definition of coherence, then

$$\mu(\Phi) = \frac{q^{(i_1-h_1)(i_2-1-i_1)} \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q}{q^{(i_1-h_1)(i_2-i_1)} \begin{bmatrix} h_2 \\ h_1 \end{bmatrix}_q} = \frac{1}{q^{i_1-h_1}}. \quad (12)$$

By the Lemma 3, then Φ satisfies the RIP of order k with $\delta_k \leq \frac{(k-1)}{q^{i_1-h_1}}$, whenever $k < q^{i_1-h_1} + 1$. This completes the proof. □

Example 10. *Given a construction of sensing matrix over* $\mathbb{F}_2$, *let* $i_2 - i_1 = 2, h_1 = h_2$ *and* $2(i_2 - h_2) = n + l - h$. *Then we obtain an* $s \times t$ *matrix* Φ *with*

$$s = 2^{(i_2-h_2-2)(i_2-2h_2+h+2)} \begin{bmatrix} h \\ h_2 \end{bmatrix}_2,$$

$$t = 2^{(i_2-h_2-2)(i_2-2h_2+h)} \begin{bmatrix} i_2 - h_2 + 2 \\ 2 \end{bmatrix}_2 \begin{bmatrix} h \\ h_2 \end{bmatrix}_2,$$

$$\mu(\Phi) = \frac{1}{2^{i_2-h_2-2}}.$$

Φ *satisfies the RIP of order* $k < 2^{i_2-h_2-2} + 1$. *So we can get that*

$$\frac{t}{s} = \frac{(2^{i_2-h_2+1} - 1)(2^{i_2-h_2+2} - 1)}{3 \cdot 2^{2(i_2-h_2-2)}},$$

then

$$2^{i_2-h_2} = \frac{\sqrt{48st + 256s^2} - 48s}{3t - 128s},$$

Φ *can be used to recover signals exactly with sparsity*

$$k \leq \frac{\sqrt{3st + 16s^2} - 12s}{3t - 128s}.$$

Next, Let's recall the Devore's construction[18]. Devore provides a kind of deterministic sensing matrix using polynomials over finite fields. For our comparison, we consider finite field of prime power order. Let $\mathbb{F}_{q'}$ be a finite field, where q' is a prime power. Given an integer r, where $0 < r < q'$, let $\mathbb{P}_r$ denotes the set $\{f(x) | \partial(f(x)) \leq r, x \in \mathbb{F}_{q'}\}$. Then there are $t' := {q'}^{r+1}$ such polynomials in it. Denote a null matrix by H with $q' \times q'$ large, and order the positions of H lexicographically as $(0,0), (0,1), \ldots, (q'-1, q'-2), (q'-1, q'-1)$. We classify the construction as three steps. First, insert one to a position of every row of H by the following way. Look $x \mapsto Q(x)$ as a mapping of $\mathbb{F}_{q'} \to \mathbb{F}_{q'}$, where $Q \in \mathbb{P}_r, x \in \mathbb{F}_{q'}$. then change the value of position $(x, Q(x))$ into 1. Every row exactly has a one. Second, Transform H into a column vector v_Q with $s' \times 1$ large, where $s' = {q'}^2$. Note that there are exactly q' ones in v_Q; one in the first q' entries, one in the next q'entries, and so on. Third, Recycle the above two steps for all the polynomials, which belongs to $\mathbb{P}_r$. Hence there are $t' := {q'}^{r+1}$ column vectors. At last, we obtain the matrix Φ_0' with $s' \times t'$ large.

Lemma 11. *[18] Suppose the matrix* $\Phi' = \frac{1}{\sqrt{q'}}\Phi_0'$, *then* Φ' *satisfies the RIP with* $\delta = (k-1)r/q'$ *for any* $k < q'/r + 1$.

Actually, Devore's polynomials deterministic matrix has been studied by many experts. They come up with that it has some deficiencies. First, due to the restriction of the finite field construction approach, the value range of measurement s is limited. Second, the time of construction is long. Third, every column exactly has q' nonzero entries. Hence, there are more nonzero values with the greater matrices, which makes the sparsity of the matrices adverse. Moreover, according to the practical application of image processing, we find that its result of reconstruction is superior to Gaussian matrix but inferior to Hadamard matrix (see [25]).

Inspired by the shortcomings of Devore's polynomials deterministic sensing matrix, we need to take sensing matrices into consideration, generally. Here we denote $a = \omega/s$, which means the rate of nonzero entries in every column of sensing matrices. Given the upper bound value of k, the sensing matrix is better when the parameter of sparse measurement a is smaller, which conduces to the recovery of signals (see [26]), the matrix is also better when the value of $\frac{t}{s}$ is larger, which means this matrix can provide powerfully compressed performance.

Consider the above-mentioned questions, carefully. Then we will draw a comparison between our construction and Devore's one and show our better properties than Devore's ones. Let $2(i_2-h_2)=n+l-h$ and $2h_2=h$, then by Theorem 9 and (11), we will obtain an $s\times t$ sensing matrix Φ with

$$s=q^{(i_1-h_1)(2i_2-i_1)}\begin{bmatrix}2h_2\\h_1\end{bmatrix}_q,$$
$$t=q^{(i_1-h_1)i_2}\begin{bmatrix}2i_2-2h_2-i_1+h_1\\i_2-h_2-i_1+h_1\end{bmatrix}_q\begin{bmatrix}2h_2\\h_2\end{bmatrix}_q,$$
$$k\le q^{i_1-h_1},$$

$$\begin{aligned}\frac{t}{s}&=\frac{q^{(i_1-h_1)i_2}\begin{bmatrix}2i_2-2h_2-i_1+h_1\\i_2-h_2-i_1+h_1\end{bmatrix}_q\begin{bmatrix}2h_2\\h_2\end{bmatrix}_q}{q^{(i_1-h_1)(2i_2-i_1)}\begin{bmatrix}2h_2\\h_1\end{bmatrix}_q}\\
&=\frac{1}{q^{(i_1-h_1)(i_2-i_1)}}\cdot\frac{\prod\limits_{i=i_2-h_2+1}^{2i_2-2h_2-i_1+h_1}(q^i-1)}{\prod\limits_{i=1}^{i_2-h_2-i_1+h_1}(q^i-1)}\cdot\frac{\prod\limits_{i=h_2+1}^{2h_2-h_1}(q^i-1)}{\prod\limits_{i=h_1+1}^{h_2}(q^i-1)}\\
&\ge\frac{1}{q^{(i_1-h_1)(i_2-i_1)}}\cdot\frac{\prod\limits_{i=i_2-h_2+1}^{2i_2-2h_2-i_1+h_1}q^i}{\prod\limits_{i=1}^{i_2-h_2-i_1+h_1}q^i}\cdot\frac{\prod\limits_{i=h_2+1}^{2h_2-h_1}q^i}{\prod\limits_{i=h_1+1}^{h_2}q^i}\\
&=q^{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)},\end{aligned}$$

and

$$\begin{aligned}a&=\frac{\omega}{s}\\
&=\frac{q^{(i_1-h_1)(i_2-i_1)}\begin{bmatrix}h_2\\h_1\end{bmatrix}_q}{q^{(i_1-h_1)(2i_2-i_1)}\begin{bmatrix}2h_2\\h_1\end{bmatrix}_q}\\
&=\frac{1}{q^{(i_1-h_1)i_2}}\cdot\frac{\prod\limits_{i=h_2-h_1+1}^{h_2}(q^i-1)}{\prod\limits_{i=2h_2-h_1+1}^{2h_2}(q^i-1)}\\
&\le\frac{1}{q^{(i_1-h_1)i_2}}\cdot\frac{\prod\limits_{i=h_2-h_1+1}^{h_2}q^i}{\prod\limits_{i=2h_2-h_1+1}^{2h_2}q^i}\\
&=\frac{1}{q^{(i_1-h_1)i_2+h_2h_1}}.\end{aligned}$$

Note that the value of a has been enlarged to $1/q^{(i_1-h_1)i_2+h_2h_1}$ and the value of $\frac{t}{s}$ has been reduced to $q^{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}$. In order to be convenient for comparison and make sure the absoluteness of results, here we may well let $a=1/q^{(i_1-h_1)i_2+h_2h_1}$ and $\frac{t}{s}=q^{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}$. Furthermore, we also have an $s'\times t'$ matrix Φ' of Devore with

$$s'=q'^2,\quad t'=q'^{r+1},\quad \frac{t'}{s'}=q'^{r-1},$$

$$k'\le\frac{q'}{r},\quad a'=\frac{q'}{s'}=\frac{1}{q'},$$

where $1<r<q'$ and q' is a prime power.

Theorem 12. *Given the matrices Φ and Φ'. Suppose k and k' are equal to their upper bound values, respectively, which means $k=q^{i_1-h_1}$, $k'=\lceil\frac{q'}{r}\rceil$. Let them be equal to each other and then $a<a'$ when*

$$r<q^{(i_1-h_1)i_2+h_2h_1-i_1+h_1}.$$

Proof. Since k=k', then $q^{i_1-h_1}=\frac{q'}{r}$. Since $a'=\frac{1}{q'}$, then $a'=\frac{1}{rq^{i_1-h_1}}$. Compare $a'=\frac{1}{rq^{i_1-h_1}}$ and $a=1/q^{(i_1-h_1)i_2+h_2h_1}$. We have $a<a'$ when $r<q^{(i_1-h_1)i_2+h_2h_1-i_1+h_1}$. □

Theorem 13. *Given the matrices Φ and Φ'. Suppose the value of $\frac{t}{s}$ and $\frac{t'}{s'}$ are the same, then $a<a'$ when*

$$\begin{aligned}r\ >\ &\frac{(i_2-i_1)(i_2-h_2-i_1+h_1)}{(i_1-h_1)i_2+h_2h_1}\\&+\frac{(h_2-h_1)(2h_2-h_1-i_2)}{(i_1-h_1)i_2+h_2h_1}+1.\end{aligned}$$

Proof. Since $\frac{t}{s}=\frac{t'}{s'}$, so

$$q'^{r-1}=q^{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}$$

and hence we get

$$q' = q^{[(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)]/(r-1)}$$

Since $a' = 1/q'$, we also obtain

$$a' = 1/q^{[(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)]/(r-1)}.$$

Compare $a = 1/q^{(i_1-h_1)i_2+h_2h_1}$ and

$$a' = 1/q^{[(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)]/(r-1)}.$$

Hence our parameter of sparse measurement a is better when

$$r > \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{(i_1-h_1)i_2+h_2h_1}+1.$$

□

For given two sensing matrices, one is our construction, another is Devore's construction. Let them satisfy the cases of Theorem 12 and 13, simultaneously. Then our construction has the better sparsity of sensing matrices when

$$\frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{(i_1-h_1)i_2+h_2h_1} +1 < r < q^{(i_1-h_1)i_2+h_2h_1-i_1+h_1}.$$

Theorem 14. *Given the matrices Φ and Φ'. Suppose the value of $\frac{t}{s}$ be equal to the value of $\frac{t'}{s'}$, then the upper bound value of k' is smaller than k's one, when*

$$r \geq \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)}{(i_1-h_1)i_2+h_2h_1} + \frac{(h_2-h_1)(2h_2-h_1-i_2)}{(i_1-h_1)i_2+h_2h_1}+1.$$

Proof. Since $\frac{t}{s} = \frac{t'}{s'}$, then

$$q'^{r-1} = q^{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)},$$

hence we obtain

$$q' = q^{[(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)]/(r-1)}.$$

For the sake of convenience, here we may let

$$x = \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{(r-1)}$$

where $x > 0$, then we can obtain $q' = q^x$,

$$1 < r = \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{x}+1 < q'.$$

Since $k' < \frac{q'}{r}+1$, then we can also get

$$k' < \frac{q^x}{\frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{x}+1}+1.$$

Draw a comparison between

$$\frac{q^x}{\frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{x}+1}+1$$

and $q^{i_1-h_1}+1$. In other words, we will compare k' and k's upper bound values. We notice that the upper bound value of k' will decrease with the value of $r = \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{x}+1$ increasing. So let $r = \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{x}+1 < q$, then we will obtain

$$q^{i_1-h_1} > \frac{q^x}{\frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{x}+1}$$

when $x \leq i_1-h_1$. As above-mentioned, we will obtain

$$\frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{(r-1)} \leq i_1-h_1.$$

Hence our construction is better when

$$r \geq \frac{(i_2-i_1)(i_2-h_2-i_1+h_1)+(h_2-h_1)(2h_2-h_1-i_2)}{i_1-h_1}+1$$

□

We have proved that our construction is superior to the construction of Devore under some conditions. By changing the numbers of parameters, we will obtain a type of different deterministic sensing matrices.

We will end up this paper with a comparison between a matrix formed by singular linear space over $\mathbb{F}_2$ and a Devore's sensing matrix formed by polynomials over $\mathbb{F}_3$ via numerical simulation. For a signal x, we choose OMP to solve l_0-minimization (1) and denote the solution by x'. Define the reconstruction signal-to-noise ratio (SNR)[27] of x as

$$\mathrm{SNR}(x) = 10 \cdot \log_{10}\left(\frac{\| x \|_2}{\| x-x' \|_2}\right)\mathrm{dB}. \quad (13)$$

If SNR (x) is no less than 100 dB, we say the recovery of x is perfect.

Consider a matrix over $\mathbb{F}_2$, where

$$n+l-h=4, \quad i_2-h_2-(i_1-h_1)=1,$$

$$d=i_1-h_1=1, \quad h_1=h_2=h=0.$$

Then we obtain an $s \times t$ sensing matrix with $s = 8, t = 28$. Furthermore, by Devore's construction

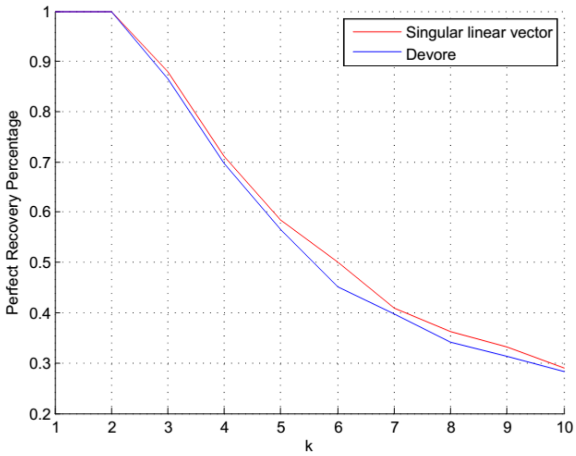

Figure 1: Perfect recovery percentage of a 8×28 matrix formed by singular linear space over $\mathbb{F}_2$ and that of a 9×27 Devore's sensing matrix over $\mathbb{F}_3$. For each k, 5000 input signals are used to compute the percentage.

using polynomials over finite fields, when $r = 2$ we also get an $s' \times t'$ sensing matrix over $\mathbb{F}_3$ with $s' = 9, t' = 27$. Figure shows the perfect recovery percentage of those two matrices. For each sparsity k, we input 5000 random signals to compute the perfect recovery percentage.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grant No.61179026 and supported by the Fundamental Research Funds for the Central Universities (3122015L008).

References:

[1] K. Long, Intercept of Frequency Agility Signal using Coding Nyquist Folding Receiver, *WSEAS Transactions on Signal Processing*, 7, 2011, pp.82-91.

[2] D. Donoho, Compressed sensing, *IEEE Trans. Inf. Theory*, 52(4), 2006, pp.1289-1306.

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

[4] B. K. Natarajan. Sparse approximate solutions to linear systems, *SIAM J. Comput.*, 24(2), 1995,pp.227-234.

[5] A. Keller, l_p-Norm Minimization Method for Solving Nonlinear System of Equations, *WSEAS Transactions on Mathematics*, 13, 2014, pp.654-665.

[6] X. Ren, J. Wang, S. Lin, A Sparse Signal Reconstruction Perspective for Direction-of-Arrival Estimation with Minimum Redundancy Linear Array, *WSEAS Transactions on Signal Processing*, 10, 2014, pp.374-381.

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

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

[9] E. Candés, J. Romberg, T. Tao, Stable signal recovery from incomplete and inaccurate measurement, *Communications on Pure and Applied Mathematices*, 59(8), 2006, pp.1207-1223.

[10] Y. Tsaig, D. Donoho, Extensions of compressed sensing, *Signal Processing*, 86(3), 2006, pp.549-571.

[11] E. Candés, T. Tao, Decoding by linear programming, *IEEE Trans. Inf. Theory*, 51(12), 2005, pp.4203-4215.

[12] E. Candés, The restricted isometry property and its implications for compressed sensing, *Comptes Rendus Math. Acad. Sci. Paris*, 346(9-10), 2008, pp.589-592.

[13] M. Davenport, M. Wakin, Analysis of orthogonal matching pursuit using the restricted isometry property, *IEEE Trans. Inf. Theory*, 56(9), 2010, pp.4395-4401.

[14] A. Cohen, W. Dahmen, R. DeVore, Compressed sensing and best k-term approximation, *J. Amer. Math. Soc.*, 22(1), 2009, pp.211-231.

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

[16] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, Explicit constructions of RIP matrices and related problems, *Duke Math. J*, 159(1), 2011, pp.145-185.

[17] L. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inf. Theory*, 20(3),1974, pp.397-399.

[18] R. Devore, Deterministic constructions of compressed sensing matrices, *J. Complexity*, 23(4-6), 2007, pp.918-925.

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

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

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

[22] K. Wang, J. Guo, F. Li, Singular linear space and its applications, *Finite Fields Appl*, 17, 2011, pp.395-406.

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

[24] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin, Heidelberg, 1989.

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

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

[27] D. Needell, J. Tropp, CoSaMP: Iterative signal recovery from incomplete and inaccurate samples, *Appl. Comput. Harmon. Anal.*, 26(3), 2009, pp.301-321.