EURASIP Journal on
Advances in Signal Processing
a SpringerOpen Journal

RESEARCH   **Open Access**

Deterministic construction of Fourier-based compressed sensing matrices using an almost difference set

Nam Yul Yu[*] and Ying Li

Abstract

In this paper, a new class of Fourier-based matrices is studied for deterministic compressed sensing. Initially, a basic partial Fourier matrix is introduced by choosing the rows deterministically from the inverse discrete Fourier transform (DFT) matrix. By row/column rearrangement, the matrix is represented as a concatenation of DFT-based submatrices. Then, a full or a part of columns of the concatenated matrix is selected to build a new $M \times N$ deterministic compressed sensing matrix, where $M = p^r$ and $N = L(M + 1)$ for prime p, and positive integers r and $L \leq M - 1$. Theoretically, the sensing matrix forms a tight frame with small coherence. Moreover, the matrix theoretically guarantees unique recovery of sparse signals with uniformly distributed supports. From the structure of the sensing matrix, the fast Fourier transform (FFT) technique can be applied for efficient signal measurement and reconstruction. Experimental results demonstrate that the new deterministic sensing matrix shows empirically reliable recovery performance of sparse signals by the CoSaMP algorithm.

1 Introduction

Compressed sensing (or compressive sampling) is a novel and emerging technology with a variety of applications in imaging, data compression, and communications. In compressed sensing, one can recover sparse signals of high dimension from incomplete measurements. Mathematically, measuring an N-dimensional signal $\mathbf{x} \in \mathbb{R}^N$ with an $M \times N$ measurement matrix Φ yields an M-dimensional vector $\mathbf{y} = \Phi\mathbf{x}$, where $M < N$. Imposing a requirement that $\mathbf{x}$ is s-sparse or the number of nonzero entries in $\mathbf{x}$ is at most s, one can recover $\mathbf{x}$ exactly with high probability by an l_1-minimization method or a greedy algorithm, which is computationally tractable.

Many research activities have been triggered on theory and practice of compressed sensing since Donoho, Candes, Romberg, and Tao published their marvelous theoretical works [1-3]. The efforts revealed that a measurement matrix Φ plays a crucial role in recovery of s-sparse signals. Although a random matrix provides many theoretical benefits [4], it has the drawbacks [5] of high

complexity and large storage in its practical implementation. As an alternative, we may consider a *deterministic* matrix, where well-known codes and sequences have been employed for the construction, e.g., chirp sequences [6], Alltop sequences [7,8], Kerdock and Delsarte-Goethals codes [9], second-order Reed-Muller codes [10], and BCH codes [11]. Other techniques for deterministic construction, based on finite fields, representation theory, characters and algebraic curves, and multicoset codes, can be also found in [12-18]. The deterministic matrices guarantee the recovery performance that is empirically reliable, allowing fast processing and low complexity.

In this paper, we study deterministic construction of a new class of Fourier-based compressed sensing matrices. Initially, a $p^r \times (p^{2r} - 1)$ basic partial Fourier matrix, equivalent to the partial Fourier codebook of [19], is introduced by selecting p^r rows from the $(p^{2r}-1)$-point inverse discrete Fourier transform (DFT) matrix according to an almost difference set, where p is a prime number and r is a positive integer. By rearranging the rows and/or columns, we show that the matrix is represented as a concatenation of DFT-based submatrices. Then, a full or a part of columns of the concatenated matrix is selected to build a new $M \times N$ sensing matrix for deterministic

*Correspondence: nam.yu@lakeheadu.ca
Department of Electrical and Computer Engineering, Lakehead University, Thunder Bay, Ontario P7B 5E1, Canada

compressed sensing, where $M = p^r$ and $N = L(M + 1)$ for $L \leq M - 1$. The concatenated structure allows the new sensing matrix to offer the various admissible column numbers while keeping it as an incoherent tight frame and enables efficient processing for measurement and reconstruction in compressed sensing. We would like to stress that it is not a trivial task to obtain the concatenated structure from the basic partial Fourier matrix by row/column rearrangement. With the parameters M and N, our new deterministic matrix can achieve the various permissible compression ratios of $\frac{M}{N} \approx \frac{1}{L}$ for a positive integer L, $2 \leq L \leq M - 1$.

Theoretically, the new sensing matrix forms a tight frame with small coherence. Moreover, our new sensing matrix theoretically guarantees unique recovery of sparse signals with uniformly distributed supports with high probability. From the structure of our new sensing matrix, the fast Fourier transform (FFT) technique can be applied for efficient signal measurement and reconstruction. Experimental results demonstrate that the new deterministic compressed sensing matrix, together with the CoSaMP recovery algorithm [20], empirically guarantees sparse signal recovery with high reliability. We observe that the empirical recovery performance of our new sensing matrices is similar to those of chirp sensing [6] and random partial Fourier matrices. However, our new matrices offer several practical benefits, requiring less storage and complexity than random partial Fourier matrices and providing more parameters of M and N than chirp sensing codes.

The rest of this paper is organized as follows. In Section 2, we introduce basic concepts and notations to understand this work. Section 3 modifies the structure of a basic partial Fourier matrix and presents a new sensing matrix for deterministic construction. We also discuss the efficient implementation and the theoretical recovery guarantee of the new sensing matrix. Section 4 describes the signal measurement process and the CoSaMP recovery algorithm by employing the FFT technique. In Section 5, we demonstrate the empirical recovery performance of our new sensing matrices in noiseless and noisy settings. Finally, concluding remarks will be given in Section 6.

2 Preliminaries

This section introduces fundamental concepts and notations for understanding this work. In subsections 2.1 and 2.2, we briefly introduce the concepts of finite fields, trace functions and cyclotomic cosets for signal processing researchers. For more details, see [21] and [22].

2.1 Finite fields and trace functions

Let p be prime and $m > 1$ a positive integer. A *finite field* $\mathbb{F}_{p^m}$ is generated by 0 and α^i, $i = 0, 1, \ldots, p^m - 2$, i.e.,

$\mathbb{F}_{p^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m - 2}\}$, where α is called a *primitive element* and $\alpha^{p^m - 1} = 1$. The primitive element α is a root of a primitive polynomial $f(x)$, i.e., $f(\alpha) = 0$, where $f(x)$ has the highest degree m and its coefficients are the elements of $\mathbb{F}_p = \{0, 1, 2, \ldots, p - 1\}$.

Let k be a positive integer that divides m. A *trace* function is a linear mapping from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_{p^k}$ defined by

$$\mathrm{Tr}_k^m(x) = \sum_{i=0}^{m/k-1} x^{p^{ki}}, \quad x \in \mathbb{F}_{p^m}$$

where the addition is computed modulo p. The trace function algebraically defines the well-known *m-sequences* or *pseudo-noise (PN) sequences*, which have been widely used in wireless communications. For instance, if $p = 2$ and $k = 1$, then $(\mathrm{Tr}_1^m(1), \mathrm{Tr}_1^m(\alpha), \mathrm{Tr}_1^m(\alpha^2), \ldots, \mathrm{Tr}_1^m(\alpha^{2^m - 2}))$ is a binary m-sequence of length $2^m - 1$, where each entry is 0 or 1. The m-sequence, defined by a trace function, is efficiently generated by a *linear feedback shift register (LFSR)*, which is a common method in communication standards.

Example 1. Let $p = 2$ and $m = 4$. Then, the finite field $\mathbb{F}_{2^4}$ is defined by a primitive polynomial $f(x) = x^4 + x + 1$, where the root α is a primitive element of $\mathbb{F}_{2^4}$. Thus, $\mathbb{F}_{2^4} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, where $\alpha^4 + \alpha + 1 = 0$ and $\alpha^{15} = 1$. The trace function $\mathrm{Tr}_1^4(x)$ takes on either 0 or 1, since it is a linear mapping from $\mathbb{F}_{2^4}$ onto $\mathbb{F}_2$. For example,

$$\mathrm{Tr}_1^4(1) = 1 + 1 + 1 + 1 = 0,$$

$$\mathrm{Tr}_1^4(\alpha) = \alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0,$$

$$\mathrm{Tr}_1^4(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 = 1$$

where the addition is computed modulo $p = 2$.

2.2 Cyclotomic cosets

Let $\mathbb{Z}_v = \{0, 1, \ldots, v - 1\}$, where v is a positive integer. Also, p is a prime integer which is relatively prime to v, i.e., $\gcd(v, p) = 1$. For a nonnegative integer $s \in \mathbb{Z}_v$, a *cyclotomic coset* modulo v over p containing s is defined as

$$C_s = \{s, sp, sp^2, \ldots, sp^{n_s - 1}\}$$

where n_s is the smallest positive integer such that $sp^{n_s} \equiv s \pmod{v}$. It is conventional to define the *coset leader* of C_s as the smallest integer s. Then, $\mathbb{Z}_v$ is partitioned into cyclotomic cosets, i.e., $\mathbb{Z}_v = \bigcup_{s \in \Gamma_p(v)} C_s$, where $\Gamma_p(v)$ denotes a set of coset leaders in $\mathbb{Z}_v$. By definition, once an element is given, a cyclotomic coset containing it can be easily generated by successive multiplication by p to the element, which will be useful in generating the row index set for our new sensing matrix.

Example 2. Let $p = 2$ and $v = 15$. Then, the cyclotomic cosets modulo 15 over $p = 2$ are

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8\}, \quad C_3 = \{3, 6, 12, 9\},$$

$$C_5 = \{5, 10\}, \quad C_7 = \{7, 14, 13, 11\}$$

where the coset leaders are $\Gamma_2(15) = \{0, 1, 3, 5, 7\}$. With the cyclotomic cosets, $\mathbb{Z}_{15} = \{0, 1, \dots, 14\} = \bigcup_{s \in \Gamma_2(15)} C_s$.

2.3 Basic partial Fourier matrix $\widetilde{\mathbf{A}}$

In this subsection, we introduce a basic framework from which a new sensing matrix can be developed in Section 3. Throughout this paper, we set $M = p^r$ and $N' = p^{2r} - 1 = M^2 - 1$ for prime p and a positive integer r. Also, we assume that each column of a sensing matrix has unit l_2-norm, where the l_2-norm is denoted as $\|\mathbf{x}\| = \sqrt{\sum_{i=0}^{n-1} |x_i|^2}$ for an n-dimensional vector $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$. Table 1 summarizes all the variables and notations for the development of a new sensing matrix.

In [19], Yu, Feng, and Zhang presented a new class of (N', M) near-optimal partial Fourier codebooks using an *almost difference set* [23]. The codebook can be equivalently translated into an $M \times N'$ partial Fourier matrix, which contains M rows selected from the N'-point inverse DFT (IDFT) matrix according to the almost difference set.

Table 1 Variables and notations for the new sensing matrix

Variable or notation	Meaning
M	$M = p^r$ for prime p and a positive integer r
N'	$N' = p^{2r} - 1 = M^2 - 1$
L	positive integer, $2 \le L \le M - 1$
N	$N = (M + 1)L$
$\mathbb{F}_{p^m}$	$\mathbb{F}_{p^m} = \{0, 1, \alpha, \dots, \alpha^{p^m - 2}\}$ for the primitive element α
$\mathbb{Z}_v$	$\mathbb{Z}_v = \{0, 1, 2, \dots, v - 1\}$ for a positive integer v
C_s	cyclotomic coset with the coset leader s
$\Gamma_p(v)$	set of coset leaders of cyclotomic cosets modulo v over p
D	row index set, $D = \{d_0, d_1, \dots, d_{M-1}\} \equiv \{M, M - 1, \dots, 1\} \pmod{M + 1}$
$\widetilde{\mathbf{A}}$	$M \times N'$ partial Fourier matrix
$\mathbf{A}'$	$M \times N'$ matrix after row/column rearrangement of $\widetilde{\mathbf{A}}$
$\boldsymbol{\sigma}^{(l)}$	$M \times (M + 1)$ submatrix of $\mathbf{A}'$, $0 \le l \le L - 1$
$\gamma_k^{(l)}$	$\gamma_k^{(l)} = \exp\left(j\frac{\pi d_k l}{M - 1}\right) \times \exp\left(-j\frac{\pi d_k l}{M + 1}\right)$, $0 \le k \le M - 1$
$\boldsymbol{\Gamma}^{(l)}$	$M \times M$ diagonal matrix with diagonal entries of $\gamma_k^{(l)}$
$\mathbf{F}'_{M+1}$	$M \times (M + 1)$ DFT matrix without the first row
$\mathbf{A}$	$M \times N$ new sensing matrix, $\mathbf{A} = [\boldsymbol{\sigma}^{(0)} \mid \cdots \mid \boldsymbol{\sigma}^{(L-1)}]$

From the results of [19], Proposition 1 describes the basic partial Fourier matrix and its geometric properties with the notations of this paper.

Proposition 1. *For prime p and a positive integer r, let $M = p^r$ and $N' = p^{2r} - 1 = M^2 - 1$. Let $D = \{d_0, d_1, \dots, d_{M-1}\}$ be an index set defined in Lemma 2 of [19], which will be given below in Remark 1. Choosing M rows from the N'-point IDFT matrix according to D, we construct an $M \times N'$ matrix $\widetilde{\mathbf{A}}$, where each entry is given by*

$$\widetilde{a}_{k,n} = \frac{1}{\sqrt{M}} \exp\left(j\frac{2\pi d_k n}{N'}\right), \quad j = \sqrt{-1}$$

for $0 \le k \le M - 1$ and $0 \le n \le N' - 1$. Then, the coherence [24] of $\widetilde{\mathbf{A}}$ is given by

$$\mu = \max_{0 \le n_1 \ne n_2 \le N' - 1} \left| \widetilde{\mathbf{a}}_{n_1}^H \widetilde{\mathbf{a}}_{n_2} \right| = \frac{1}{\sqrt{M}}$$

where $\widetilde{\mathbf{a}}_{n_1}$ is a column vector of $\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{a}}_{n_1}^H$ denotes the transpose of its complex conjugate. The coherence nearly achieves the Welch bound equality [25] of $\sqrt{\frac{N' - M}{M(N' - 1)}} \approx \frac{1}{\sqrt{M+1}}$ for sufficiently large M. Moreover, $\widetilde{\mathbf{A}}$ forms a tight frame [26] as each row is mutually orthogonal.

The coherence and the tightness of $\widetilde{\mathbf{A}}$ do not change if we select the rows from the DFT matrix, instead of the IDFT matrix. In this paper, we decide to use the IDFT matrix.

Remark 1. With the notations of this paper, the row index set D is defined by [19]

$$D = \{(M + 1)e_v - v \mid v \in I\} \text{ where}$$

$$I = \begin{cases} \mathbb{Z}_{M+1} \setminus \{0\}, & \text{if } p = 2 \\ \mathbb{Z}_{M+1} \setminus \{\frac{M+1}{2}\}, & \text{if } p > 2 \end{cases} \quad (1)$$

where all the operations in D are computed modulo N'. In Equation 1, D is an almost difference set, and e_v is a non-negative integer satisfying $\alpha^{(p^r + 1)e_v} = \mathrm{Tr}_r^{2r}(\alpha^v)$ for $v \in I$ [19], where α is a primitive element in $\mathbb{F}_{p^{2r}}$. To determine the index set D, one needs to compute e_v using a trace function, which might be difficult for signal processing researchers. In Section 3, we will present an alternative method to generate the indices of D by successive multiplication to predetermined values, which does not require the computation of e_v. Therefore, it suffices to assume that e_v is simply an integer in this paper.

3 Construction of new Fourier-based sensing matrices

To build a new $M \times N$ sensing matrix, we begin with the $M \times N'$ basic partial Fourier matrix $\widetilde{\mathbf{A}}$, and then choose

the N columns after a row/column rearrangement. Our approach is different from a conventional one of random or deterministic selection of M rows out of an $N \times N$ Fourier matrix, but we will show that it ultimately presents reliable recovery performance and practical benefits in implementation.

In deterministic compressed sensing, it is desired that a sensing matrix should be able to support a variety of admissible column numbers to sense a signal of various lengths. For this purpose, one needs to consider how to select the columns from $\widetilde{\mathbf{A}}$ for a new $M \times N$ sensing matrix with $N < N'$. In this section, we apply a row/column permutation to the partial Fourier matrix $\widetilde{\mathbf{A}}$ to obtain its variant $M \times N'$ matrix $\mathbf{A}'$. Then, we choose a full or a part of columns of $\mathbf{A}'$ to construct a new $M \times N$ sensing matrix $\mathbf{A}$, where $N = (M + 1)L$ for a positive integer L, $2 \leq L \leq M - 1$. The row/column rearrangement offers the following benefits for our new sensing matrix $\mathbf{A}$ in compressed sensing, which is the motivation:

1. If one selects the columns arbitrarily from $\widetilde{\mathbf{A}}$, the resulting sensing matrix may not be a tight frame in general. In fact, one needs to be careful in selecting the columns of $\widetilde{\mathbf{A}}$, to achieve the tightness of the resulting matrix. Through the row/column rearrangement, we will show that the new sensing matrix $\mathbf{A}$ has a *concatenated* structure of $(M + 1)$-point DFT-based submatrices. With the structure, $\mathbf{A}$ can be still a tight frame by choosing N as a multiple of $M + 1$, which will be shown in Lemma 2.

2. The concatenated structure of $\mathbf{A}$ also allows efficient $(M + 1)$-point FFT processing for measurement and recovery of sparse signals in compressed sensing. Note that if one selects the columns arbitrarily from the original $\widetilde{\mathbf{A}}$, the resulting matrix generally requires the N'-point FFT processing, which has more computational complexity. Moreover, one may enjoy fast processing via parallel FFT computations using the concatenated structure, which will be discussed in Section 4.

3.1 Structure

Recall the partial Fourier matrix $\widetilde{\mathbf{A}}$ in Proposition 1. If $p = 2$, we use the original index set D in Equation 1, i.e.,

$$D = \{(M + 1)e_\nu - \nu \mid \nu \in \mathbb{Z}_{M+1} \setminus \{0\}\}. \tag{2}$$

On the other hand, if $p > 2$, we redefine the index set D by adding $\frac{M+1}{2}$ to each original index in Equation 1, i.e.,

$$D = \left\{(M + 1)e_\nu - \nu + \frac{M + 1}{2} \mid \nu \in \mathbb{Z}_{M+1} \setminus \left\{\frac{M + 1}{2}\right\}\right\}. \tag{3}$$

The above modification for $p > 2$ ensures that each entry of D is nonzero when computed modulo $M + 1$, which

also holds for $p = 2$. See the proof of Lemma 1 for the implication.

Now, we suggest a column rearrangement of the original $\widetilde{\mathbf{A}}$. For given l, $0 \leq l \leq M - 2$, let us take the $M + 1$ column vectors of indices $n = (M - 1)t + l$ from $\widetilde{\mathbf{A}}$, where $0 \leq t \leq M$. With the column vectors, we then obtain an $M \times (M + 1)$ submatrix $\boldsymbol{\sigma}^{(l)} = \{\sigma_{k,t}^{(l)} \mid 0 \leq k \leq M - 1, 0 \leq t \leq M\}$, where each entry is given by

$$
\begin{aligned}
\sigma_{k,t}^{(l)} &= \frac{1}{\sqrt{M}} \exp\left(j\frac{2\pi d_k((M - 1)t + l)}{N'}\right) \\
&= \frac{1}{\sqrt{M}} \exp\left(j\frac{2\pi d_k t}{M + 1}\right) \times \exp\left(j\frac{2\pi d_k l}{N'}\right) \\
&= \frac{1}{\sqrt{M}} \exp\left(j\frac{2\pi d_k t}{M + 1}\right) \times \gamma_k^{(l)}.
\end{aligned}
\tag{4}
$$

In Equation 4, $\gamma_k^{(l)}$ is defined as

$$
\begin{aligned}
\gamma_k^{(l)} &= \exp\left(j\frac{2\pi d_k l}{N'}\right) = \exp\left(j2\pi d_k l \times \frac{1}{2}\left(\frac{1}{M - 1} - \frac{1}{M + 1}\right)\right) \\
&= \exp\left(j\frac{\pi d_k l}{M - 1}\right) \times \exp\left(-j\frac{\pi d_k l}{M + 1}\right).
\end{aligned}
$$

for each k, $0 \leq k \leq M - 1$.

Next, we show that the submatrix $\boldsymbol{\sigma}^{(l)}$ has a DFT-based structure if the row indices of D are arranged in appropriate order. In Lemma 1, we denote $\mathbf{F}'_{M+1}$ as the $M \times (M+1)$ DFT matrix without the first row, where each entry is $F'_{k,t} = \exp\left(-j\frac{2\pi(k+1)t}{M+1}\right)$ for $0 \leq k \leq M-1$ and $0 \leq t \leq M$.

Lemma 1. *In the index set of Equation 2 for $p = 2$ or Equation 3 for $p > 2$, the entries of $D = \{d_0, d_1, \ldots, d_{M-1}\}$ can be arranged such that $d_k \equiv -(k + 1) \pmod{M + 1}$ for $0 \leq k \leq M - 1$. With such D, let us define $\boldsymbol{\Gamma}^{(l)} = \{\Gamma_{k,t}^{(l)} \mid 0 \leq k, t \leq M - 1\}$ as an $M \times M$ diagonal matrix where each entry is*

$$
\Gamma_{k,t}^{(l)} = \begin{cases} \gamma_k^{(l)}, & \text{if } k = t, \\ 0, & \text{if } k \neq t \end{cases}
$$

for each l, $0 \leq l \leq L - 1$. Then, each submatrix $\boldsymbol{\sigma}^{(l)}$ can be expressed by

$$\boldsymbol{\sigma}^{(l)} = \frac{1}{\sqrt{M}} \boldsymbol{\Gamma}^{(l)} \mathbf{F}'_{M+1}, \tag{5}$$

which clearly shows the DFT-based structure of $\boldsymbol{\sigma}^{(l)}$.

Proof. We investigate how $\exp\left(j\frac{2\pi d_k t}{M+1}\right)$ of Equation 4 is changed for $p = 2$ and $p > 2$, respectively.

Case. $p = 2$: In this case, each element of D in Equation 2 is represented as

$$d_k = (M+1)e_{k+1} - (k+1) \equiv -(k+1) \pmod{M+1}$$
$$(6)$$

for $0 \le k \le M-1$. Thus, $\exp\left(j\frac{2\pi d_k t}{M+1}\right) = \exp\left(-j\frac{2\pi(k+1)t}{M+1}\right)$ in Equation 4. Consequently, each entry of Equation 4 forms an $M \times (M+1)$ submatrix $\boldsymbol{\sigma}^{(l)}$ where each row is from the $(M+1)$-point DFT matrix excluding all one row and then masked by $\gamma_k^{(l)}$. Then, the structure of Equation 5 is straightforward.

Case. $p > 2$: In this case, each index of D in Equation 3 is

$$d_k' = \begin{cases} (M+1)e_k - k + \frac{M+1}{2}, & 0 \le k < \frac{M+1}{2} \\ (M+1)e_{k+1} - (k+1) + \frac{M+1}{2}, & \frac{M+1}{2} \le k \le M-1 \end{cases}$$

$$\equiv \begin{cases} -k - \frac{M+1}{2} \pmod{M+1}, & 0 \le k < \frac{M+1}{2} \\ -(k+1) + \frac{M+1}{2} \pmod{M+1}, & \frac{M+1}{2} \le k \le M-1 \end{cases}$$

where $-\frac{M+1}{2} \equiv \frac{M+1}{2} \pmod{M+1}$. Reordering the indices, we get

$$d_k = \begin{cases} d'_{k+\frac{M+1}{2}}, & 0 \le k < \frac{M-1}{2} \\ d'_{k-\frac{M-1}{2}}, & \frac{M-1}{2} \le k \le M-1 \end{cases}$$
$$(7)$$

$$\equiv -(k+1) \pmod{M+1}$$

for $0 \le k \le M-1$. Then, Equation 7 yields $\exp\left(j\frac{2\pi d_k t}{M+1}\right) = \exp\left(-j\frac{2\pi(k+1)t}{M+1}\right)$ in Equation 4. It is now clear why we introduced the modified index set D of Equation 3 for $p > 2$. By ensuring $d_k \not\equiv 0 \pmod{M+1}$ for any k, the modification guarantees that we can achieve the same DFT-based submatrix structure as that of $p = 2$. Finally, each entry of Equation 4 also forms an $M \times (M+1)$ submatrix $\boldsymbol{\sigma}^{(l)}$ where each row is from $\mathbf{F}'_{M+1}$ and then masked by $\gamma_k^{(l)}$, which yields Equation 5. □

Remark 2. In both cases of p, one needs to ensure that the entries of the index set $D = \{d_0, d_1, \ldots, d_{M-1}\}$ should satisfy $d_k \equiv -(k+1) \equiv M - k \pmod{M+1}$, to achieve the DFT-based submatrix structure in Lemma 1. If $p = 2$, the original entries of Equation 2 meet the condition from Equation 6. On the other hand, if $p > 2$, Equation 7 shows that we have to rearrange the entries of Equation 3 by circularly shifting the order by $\frac{M+1}{2}$. If the entries of D are generated by a different method, which will be introduced in Procedure 1, the index set

D should be sorted for both p such that the entries are in *decreasing* order when computed modulo $M + 1$, i.e., $D \pmod{M+1} \equiv \{M, M-1, \ldots, 1\}$, to satisfy the condition.

Finally, if l runs through $\{0, 1, \ldots, M-2\}$, we obtain the $M - 1$ submatrices $\boldsymbol{\sigma}^{(l)}$, and construct a variant $\mathbf{A}' = [\boldsymbol{\sigma}^{(0)} \mid \boldsymbol{\sigma}^{(1)} \mid \cdots \mid \boldsymbol{\sigma}^{(M-2)}]$ by concatenating them. Clearly, the $M \times N'$ matrix $\mathbf{A}'$ is equivalent to the original matrix $\widetilde{\mathbf{A}}$ under the row/column rearrangement. In what follows, Construction 1 presents a formal expression of the new sensing matrix $\mathbf{A}$.

Construction 1. *Let $M = p^r$ for prime p and a positive integer r. Let $D = \{d_0, d_1, \ldots, d_{M-1}\}$ be the row index set which satisfies $d_k \equiv -(k+1) \pmod{M+1}$ for $0 \le k \le M - 1$. Let L be a positive integer and $N = (M+1)L$, where $2 \le L \le M - 1$. For a given integer l, $0 \le l \le L - 1$, define an $M \times (M+1)$ submatrix $\boldsymbol{\sigma}^{(l)} = \{\sigma_{k,t}^{(l)} \mid 0 \le k \le M - 1, 0 \le t \le M\}$ where*

$$\sigma_{k,t}^{(l)} = \frac{1}{\sqrt{M}} \exp\left(-j\frac{2\pi(k+1)t}{M+1}\right) \times \gamma_k^{(l)}$$

and $\gamma_k^{(l)} = \exp\left(j\frac{\pi d_k l}{M-1}\right) \times \exp\left(-j\frac{\pi d_k l}{M+1}\right)$. An $M \times N$ sensing matrix $\mathbf{A}$ is a concatenation of the L submatrices i.e., $\mathbf{A} = [\boldsymbol{\sigma}^{(0)} \mid \boldsymbol{\sigma}^{(1)} \mid \cdots \mid \boldsymbol{\sigma}^{(L-1)}]$. In particular, if $L = M - 1$, then $\mathbf{A} = \mathbf{A}' = [\boldsymbol{\sigma}^{(0)} \mid \boldsymbol{\sigma}^{(1)} \mid \cdots \mid \boldsymbol{\sigma}^{(M-2)}]$.

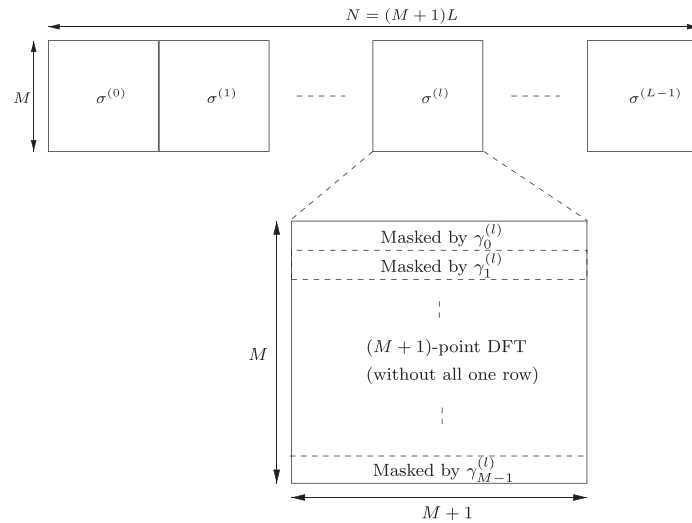Figure 1 illustrates the structure of our new sensing matrix $\mathbf{A}$ in Construction 1.

3.2 Implementation

In Construction 1, generating the row index set D efficiently is a key issue in implementing the deterministic sensing matrix $\mathbf{A}$. In D, as $\alpha^{(p^r+1)e_v} = \mathrm{Tr}_r^{2r}(\alpha^v)$ is an element of a p^r-ary *m*-sequence of period $p^{2r} - 1$ [21], we can compute it by a 2-stage LFSR. Therefore, each element of D in Equation 1 can be generated by LFSR, log operation and other basic arithmetics over finite fields.

As the computation over finite fields is not trivial, we introduce an alternative method to generate the indices of D more efficiently. In the method, we use cyclotomic cosets modulo $p^r + 1$ and $p^{2r} - 1$ over p, respectively, which are always valid for any prime p, since $\gcd(p, p^r + 1) = \gcd(p, p^{2r} - 1) = 1$. In what follows, we describe the procedure, where the proof will be given in the Appendix.

Procedure 1.
1. Generate all cyclotomic cosets modulo $p^r + 1$ over p. When $p = 2$, identify a set of nonzero coset leaders

Figure 1 Concatenated structure of new sensing matrix A. It illustrates the concatenated structure of the new sensing matrix **A** in Construction 1.

by $\Gamma_2(2^r + 1) \setminus \{0\} = \{u_1, \ldots, u_\delta\}$. If $p > 2$, on the other hand, identify a set of coset leaders without $\frac{p^r+1}{2}$ by $\Gamma_p(p^r + 1) \setminus \{\frac{p^r+1}{2}\} = \{u_1, \ldots, u_\delta\}$. Note that $u_1 = 0$ if $p > 2$.

2. For each u_i, $1 \leq i \leq \delta$, compute a positive integer $z_i \in \mathbb{Z}_{p^{2r}-1}$ such that

$$\alpha^{z_i} = 1 + \alpha^{(p^r-1)u_i} \qquad (8)$$

where α is a primitive element in $\mathbb{F}_{p^{2r}}$.

3. For each z_i, $1 \leq i \leq \delta$, generate a cyclotomic coset modulo $p^{2r} - 1$ over p containing z_i by $C_{s_i} = \{z_i, z_i p, \ldots, z_i p^{n_{s_i}-1}\}$, where n_{s_i} is the smallest positive integer such that $z_i \equiv z_i p^{n_{s_i}} \pmod{p^{2r} - 1}$. Note that the coset leader s_i is not necessarily equal to z_i.

4. If $p = 2$,

$$D = \bigcup_{1 \leq i \leq \delta} C_{s_i},$$

and if $p > 2$,

$$D = \bigcup_{1 \leq i \leq \delta} C_{s_i} + \frac{M+1}{2}$$

where the addition is performed to each element of $\bigcup_{1 \leq i \leq \delta} C_{s_i}$, and computed modulo $p^{2r} - 1$. From Remark 2, the index set D should be sorted such that the entries are in decreasing order when computed

modulo $M + 1$, i.e., D
$(\text{mod } M + 1) \equiv \{M, M - 1, \ldots, 1\}$.

Example 3. Let $p = 2$ and $r = 3$. Also, let α be a primitive element in $\mathbb{F}_{2^6}$ satisfying $\alpha^6 + \alpha + 1 = 0$. Then, Procedure 1 generates $M = p^r = 8$ indices of D for our new sensing matrix:

1. From all cyclotomic cosets modulo 9 over $p = 2$, we identify nonzero coset leaders $\Gamma_2(9) \setminus \{0\} = \{1, 3\}$, where the cosets are $C'_1 = \{1, 2, 4, 8, 7, 5\}$ and $C'_3 = \{3, 6\}$, respectively.

2. From $u_1 = 1$, Equation 8 yields $\alpha^{z_1} = 1 + \alpha^7 = \alpha^{26}$, where $z_1 = 26$. Also, from $u_2 = 3$, we have $\alpha^{z_2} = 1 + \alpha^{21} = \alpha^{42}$ and $z_2 = 42$.

3. By successively multiplying $z_1 = 26$ by 2, we obtain its cyclotomic coset $C_{13} = \{26, 52, 41, 19, 38, 13\}$, where the coset leader is $s_1 = 13$. Note that the multiplication is computed modulo $p^{2r} - 1 = 63$. Similarly, we have $C_{21} = \{42, 21\}$ from $z_2 = 42$, where $s_2 = 21$.

4. Finally, the index set D is given by

$$D = \{d_0, d_1, \ldots, d_7\} = C_{13} \bigcup C_{21}$$

$$= \{26, 52, 42, 41, 13, 21, 38, 19\}$$

where we have sorted the indices such that they are in decreasing order when computed modulo 9, i.e., D $(\text{mod } 9) \equiv \{8, 7, 6, 5, 4, 3, 2, 1\}$.

Example 4. With the index set D of Example 3, we can construct an 8×18 matrix $\mathbf{A} = [\boldsymbol{\sigma}^{(0)} \mid \boldsymbol{\sigma}^{(1)}]$, where $M = 8$, $N = 18$ and $L = 2$. Denote $\omega = \exp\left(-j\frac{2\pi}{9}\right)$. Then,

$$\boldsymbol{\sigma}^{(0)} = \frac{1}{\sqrt{8}} \boldsymbol{\Gamma}^{(0)} \mathbf{F}_9' = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 & \omega^8 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} & \omega^{16} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} & \omega^{24} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} & \omega^{32} \\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} & \omega^{40} \\ 1 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} & \omega^{48} \\ 1 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49} & \omega^{56} \\ 1 & \omega^8 & \omega^{16} & \omega^{24} & \omega^{32} & \omega^{40} & \omega^{48} & \omega^{56} & \omega^{64} \end{bmatrix}$$

where $\boldsymbol{\Gamma}^{(0)}$ is the 8×8 identity matrix. Also,

$$\boldsymbol{\sigma}^{(1)} = \frac{1}{\sqrt{8}} \boldsymbol{\Gamma}^{(1)} \mathbf{F}_9'$$

$$= \frac{1}{\sqrt{8}} \begin{bmatrix} \gamma_0^{(1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \gamma_1^{(1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma_2^{(1)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \gamma_3^{(1)} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma_4^{(1)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \gamma_5^{(1)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \gamma_6^{(1)} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_7^{(1)} \end{bmatrix} \times \mathbf{F}_9'$$

$$= \frac{1}{\sqrt{8}} \begin{bmatrix} \gamma_0^{(1)} & \gamma_0^{(1)}\omega & \gamma_0^{(1)}\omega^2 & \gamma_0^{(1)}\omega^3 & \gamma_0^{(1)}\omega^4 & \gamma_0^{(1)}\omega^5 & \gamma_0^{(1)}\omega^6 & \gamma_0^{(1)}\omega^7 & \gamma_0^{(1)}\omega^8 \\ \gamma_1^{(1)} & \gamma_1^{(1)}\omega^2 & \gamma_1^{(1)}\omega^4 & \gamma_1^{(1)}\omega^6 & \gamma_1^{(1)}\omega^8 & \gamma_1^{(1)}\omega^{10} & \gamma_1^{(1)}\omega^{12} & \gamma_1^{(1)}\omega^{14} & \gamma_1^{(1)}\omega^{16} \\ \gamma_2^{(1)} & \gamma_2^{(1)}\omega^3 & \gamma_2^{(1)}\omega^6 & \gamma_2^{(1)}\omega^9 & \gamma_2^{(1)}\omega^{12} & \gamma_2^{(1)}\omega^{15} & \gamma_2^{(1)}\omega^{18} & \gamma_2^{(1)}\omega^{21} & \gamma_2^{(1)}\omega^{24} \\ \gamma_3^{(1)} & \gamma_3^{(1)}\omega^4 & \gamma_3^{(1)}\omega^8 & \gamma_3^{(1)}\omega^{12} & \gamma_3^{(1)}\omega^{16} & \gamma_3^{(1)}\omega^{20} & \gamma_3^{(1)}\omega^{24} & \gamma_3^{(1)}\omega^{28} & \gamma_3^{(1)}\omega^{32} \\ \gamma_4^{(1)} & \gamma_4^{(1)}\omega^5 & \gamma_4^{(1)}\omega^{10} & \gamma_4^{(1)}\omega^{15} & \gamma_4^{(1)}\omega^{20} & \gamma_4^{(1)}\omega^{25} & \gamma_4^{(1)}\omega^{30} & \gamma_4^{(1)}\omega^{35} & \gamma_4^{(1)}\omega^{40} \\ \gamma_5^{(1)} & \gamma_5^{(1)}\omega^6 & \gamma_5^{(1)}\omega^{12} & \gamma_5^{(1)}\omega^{18} & \gamma_5^{(1)}\omega^{24} & \gamma_5^{(1)}\omega^{30} & \gamma_5^{(1)}\omega^{36} & \gamma_5^{(1)}\omega^{42} & \gamma_5^{(1)}\omega^{48} \\ \gamma_6^{(1)} & \gamma_6^{(1)}\omega^7 & \gamma_6^{(1)}\omega^{14} & \gamma_6^{(1)}\omega^{21} & \gamma_6^{(1)}\omega^{28} & \gamma_6^{(1)}\omega^{35} & \gamma_6^{(1)}\omega^{42} & \gamma_6^{(1)}\omega^{49} & \gamma_6^{(1)}\omega^{56} \\ \gamma_7^{(1)} & \gamma_7^{(1)}\omega^8 & \gamma_7^{(1)}\omega^{16} & \gamma_7^{(1)}\omega^{24} & \gamma_7^{(1)}\omega^{32} & \gamma_7^{(1)}\omega^{40} & \gamma_7^{(1)}\omega^{48} & \gamma_7^{(1)}\omega^{56} & \gamma_7^{(1)}\omega^{64} \end{bmatrix}$$

where

$$\gamma_0^{(1)} = \exp\left(j\frac{26\pi}{7}\right) \times \exp\left(-j\frac{26\pi}{9}\right), \quad \gamma_1^{(1)} = \exp\left(j\frac{52\pi}{7}\right) \times \exp\left(-j\frac{52\pi}{9}\right),$$

$$\gamma_2^{(1)} = \exp\left(j\frac{42\pi}{7}\right) \times \exp\left(-j\frac{42\pi}{9}\right), \quad \gamma_3^{(1)} = \exp\left(j\frac{41\pi}{7}\right) \times \exp\left(-j\frac{41\pi}{9}\right),$$

$$\gamma_4^{(1)} = \exp\left(j\frac{13\pi}{7}\right) \times \exp\left(-j\frac{13\pi}{9}\right), \quad \gamma_5^{(1)} = \exp\left(j\frac{21\pi}{7}\right) \times \exp\left(-j\frac{21\pi}{9}\right),$$

$$\gamma_6^{(1)} = \exp\left(j\frac{38\pi}{7}\right) \times \exp\left(-j\frac{38\pi}{9}\right), \quad \gamma_7^{(1)} = \exp\left(j\frac{19\pi}{7}\right) \times \exp\left(-j\frac{19\pi}{9}\right).$$

We can further concatenate $\boldsymbol{\sigma}^{(2)}, \boldsymbol{\sigma}^{(3)}, \ldots, \boldsymbol{\sigma}^{(L-1)}$ for $L \leq 7$ so that $\mathbf{A}$ can take various column number $N = 9L$.

In practice, we can precompute $z_1, z_2, \ldots, z_\delta$ at items 1 and 2 of Procedure 1 and save them in memory to avoid the algebraic computation of Equation 8 in the hardware. Then, $M = p^r$ indices can be generated by items 3 and 4 of Procedure 1. In Example 3, for instance, $z_1 = 26$ and $z_2 = 42$ can be precomputed. Then, only the two elements need to be stored in the memory to generate eight row indices. Table 2 presents δ or the number of z_i's to be stored in the memory for various $M = p^r$. While a random partial Fourier matrix needs to save M indices, a storage space for δ ($\ll M$) elements is sufficient for our new sensing matrix. In conclusion, constructing our new sensing matrix requires a storage for δ elements and an additional circuit for successive multiplication, addition and sorting, which may present a practical benefit over random partial Fourier matrices.

3.3 Theoretical recovery performance

In this subsection, we discuss the geometric properties and the theoretical recovery guarantee of our new sensing matrix **A**.

Lemma 2. *The $M \times N$ sensing matrix **A** in Construction 1 has the following properties.*

1. *The coherence is upper bounded by $1/\sqrt{M}$.*
2. ***A** forms a tight frame.*
3. *All the row sums are equal to zero.*

Proof. Recall that $\mathbf{A}'$ is obtained by row/column rearrangement of $\widetilde{\mathbf{A}}$. Since the coherence of a matrix does not change by row/column permutation, the coherence of $\mathbf{A}'$ is also $1/\sqrt{M}$ from Proposition 1. Note that when $p > 2$, we have added the constant $\frac{M+1}{2}$ to each entry of the original D in Equation 1, which does not change the coherence [19] either. As **A** is a set of selected columns of $\mathbf{A}'$, the coherence of **A** is at most $1/\sqrt{M}$ from which item 1 is true. Moreover, $\boldsymbol{\sigma}^{(l)}\boldsymbol{\sigma}^{(l)H} = \frac{(M+1)}{M}\mathbf{I}_M$ from Equation 5, where $\mathbf{I}_M$ is the $M \times M$ identity matrix. Then, we have

$\mathbf{A}\mathbf{A}^H = \frac{(M+1)L}{M}\mathbf{I}_M = \frac{N}{M}\mathbf{I}_M$ by concatenating the L submatrices, which shows that item 2 is true. Finally, Equation 5 ensures that no submatrix $\boldsymbol{\sigma}^{(l)}$ has all one row masked by a constant factor, which concludes that all the row sums of each submatrix are equal to zero, due to the DFT-based structure. Consequently, item 3 is true from the concatenation. $\square$

The geometric properties of Lemma 2 meet the sufficient conditions for the new matrix **A** to achieve the *uniqueness-guaranteed statistical restricted isometry property (UStRIP)* [5]. See [27] for the proof of the UStRIP of **A**.

With a deterministic sensing matrix of coherence μ, one can successfully recover *every* s-sparse signal from its measurement as long as $s = O(\mu^{-1})$ [24], which guarantees unique recovery of sparse signals with sparsity up to $O(\sqrt{M})$ by our new sensing matrix **A**. In an attempt to overcome the theoretical bottleneck, the authors of [28] discussed the *average* performance of compressed sensing under a *generic s-sparse model*, where the positions of nonzero entries of an s-sparse signal are distributed uniformly at random and their signs are independent and equally likely to be -1 or $+1$. In what follows, the average recovery performance of s-sparse signals with the generic s-sparse model is theoretically guaranteed by the sensing matrix **A**.

Theorem 1. *Consider the $M \times N$ sensing matrix **A** in Construction 1. Let $\mathbf{x} \in \mathbb{R}^N$ be an s-sparse signal with the generic s-sparse model. Then, if $s = O\left(\frac{M}{\log N}\right)$, it is possible to recover $\mathbf{x}$ with probability $1 - N^{-1}$ from the measurement $\mathbf{Ax}$.*

Proof. From Lemma 2, **A** is a tight frame with coherence $\mu = O\left(\frac{1}{\sqrt{M}}\right)$. For such a matrix, Theorem 2.2 of [29] presents the average recovery performance that if $s = O\left(\min\left\{\frac{\mu^{-2}}{\log N}, \frac{M}{\log N}\right\}\right) = O\left(\frac{M}{\log N}\right)$, it is possible to recover $\mathbf{x}$ with probability $1 - N^{-1}$ from $\mathbf{Ax}$, which completes the proof. $\square$

4 FFT-based signal measurement and recovery

This section describes measurement and recovery processes with the deterministic compressed sensing matrix **A** in Construction 1. With the DFT-based submatrix structure, we can make use of the FFT technique in the processes.

4.1 Measurement

The measurement process of compressed sensing is accomplished by $\mathbf{y} = \mathbf{Ax}$, where $\mathbf{x} = (x_0, x_1, \ldots, x_{N-1})^T$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{M-1})^T$. Let $b = M + 1$ and $\mathbf{x}_l =$

Table 2 The number of elements z_i's to be stored in memory for various $M = p^r$

p	r	M	δ	p	r	M	δ
2	6	64	6	5	3	125	23
	7	128	10		4	625	79
	8	256	16		5	3,125	315
	9	512	30	7	3	343	60
	10	1,024	52		4	2,401	301
3	4	81	11	11	2	121	31
	5	243	26		3	1,331	226
	6	729	63	13	2	169	43
	7	2,187	158		3	2,197	371

$(x_{bl}, x_{bl+1} \ldots, x_{bl+b-1})^T$ be a segment of $\mathbf{x}$ of length b, where $0 \leq l \leq L - 1$. From Equation 5, $\sigma^{(l)}\mathbf{x}_l = \frac{1}{\sqrt{M}}\mathbf{\Gamma}^{(l)}\mathbf{F}'_b\mathbf{x}_l$ for each l, which implies that the matrix-vector multiplication $\sigma^{(l)}\mathbf{x}_l$ includes to perform the b-point DFT of each segment $\mathbf{x}_l$ and then to multiply each DFT output by $\gamma_k^{(l)}$. Let $\widetilde{x}_k^{(l)}$ be the b-point DFT of $\mathbf{x}_l$, i.e.,

$$\widetilde{x}_k^{(l)} = \sum_{t=0}^{b-1} x_{bl+t}e^{-j\frac{2\pi tk}{b}}, \quad 0 \leq k \leq b-1$$

and $X_k^{(l)} = \widetilde{x}_{k+1}^{(l)}$, $0 \leq k \leq M - 1$ for each l. As $\mathbf{Ax} = \sigma^{(0)}\mathbf{x}_0 + \cdots + \sigma^{(L-1)}\mathbf{x}_{L-1}$, the measurement from $\mathbf{Ax}$ is equivalent to adding up each DFT output $X_k^{(l)}$ weighted by $\gamma_k^{(l)}$ for $0 \leq l \leq L - 1$. In other words,

$$y_k = \frac{1}{\sqrt{M}}\sum_{l=0}^{L-1} X_k^{(l)}\gamma_k^{(l)}, \quad 0 \leq k \leq M-1.$$

For fast implementation, the FFT algorithm can be applied to the L distinct segments of $\mathbf{x}$ simultaneously in a parallel fashion.

4.2 Reconstruction

For s-sparse signal recovery, we consider the CoSaMP algorithm presented in Algorithm 2.1 of [20], which is described in Algorithm 1 of this paper. At each iteration, it forms a signal proxy $\mathbf{f}$ and identifies a potential candidate Ω of the signal support by locating the largest $2s$ components of the proxy. The algorithm then merges the candidate Ω with the one from the previous iteration, to create a new support set T. To estimate the target signal $\widehat{\mathbf{x}}_i$, it solves a least-squares problem and takes only the largest s entries from the signal approximation $\mathbf{z}$. Finally, it updates the current sample $\mathbf{v}$ for the next iteration.

Algorithm 1: CoSaMP recovery algorithm [20]

$\widehat{\mathbf{x}}_0 \leftarrow \mathbf{0}, \mathbf{v} \leftarrow \mathbf{u}, \mathbf{z} \leftarrow \mathbf{0}, i \leftarrow 0$ Initialize

repeat
    $i \leftarrow i + 1$
    $\mathbf{f} \leftarrow \mathbf{A}^H\mathbf{v}$ Form signal proxy
    $\Omega \leftarrow \text{supp}(\mathbf{f}_{2s})$ Identify large components
    $T \leftarrow \Omega \cup \text{supp}(\widehat{\mathbf{x}}_{i-1})$ Merge supports
    $\mathbf{z}_{|T} \leftarrow \mathbf{A}_T^{\dagger}\mathbf{u}$ Estimate signal by least-squares
    $\widehat{\mathbf{x}}_i \leftarrow \mathbf{z}_s$ Take the largest s entries
    $\mathbf{v} \leftarrow \mathbf{u} - \mathbf{A}\widehat{\mathbf{x}}_i$ Update current samples

until a halting criterion is true

In Algorithm 1, the signal proxy is $\mathbf{f} = \mathbf{A}^H\mathbf{v} = (f_0, f_1, \ldots, f_{N-1})^T$, where $\mathbf{v} = (v_0, v_1, \ldots, v_{M-1})^T$ and $\mathbf{A}^H$ denotes

the conjugate transpose of $\mathbf{A}$. Initially, $\mathbf{v}$ is a (noisy) measurement vector $\mathbf{u}$. At each iteration, it will be updated by $\mathbf{v} = \mathbf{u} - \mathbf{A}\widehat{\mathbf{x}}_i$. Considering the submatrix structure of $\sigma^{(l)}$, the matrix-vector multiplication $\mathbf{A}^H\mathbf{v}$ is performed by the reverse operation of the measurement process, i.e., extracting the weight $\gamma_k^{(l)}$ from each measurement and then applying the b-point IDFT. For each l, $0 \leq l \leq L - 1$, we create a demasked version of $\mathbf{v}$ of length $b = M + 1$, i.e., $\widetilde{\mathbf{v}}^{(l)} = (\widetilde{v}_0^{(l)}, \widetilde{v}_1^{(l)}, \ldots, \widetilde{v}_M^{(l)})^T$ where $\widetilde{v}_0^{(l)} = 0$ and

$$\widetilde{v}_{k+1}^{(l)} = v_k\gamma_k^{(l)*}, \quad 0 \leq k \leq M-1$$

where '$*$' denotes the complex conjugate. Applying the b-point IDFT to $\widetilde{\mathbf{v}}^{(l)}$ with normalization then yields a segment of $\mathbf{f}$ of length b, i.e., $\mathbf{f}_l = (f_{bl}, f_{bl+1}, \ldots, f_{bl+b-1})^T$, where

$$f_{bl+t} = \frac{1}{\sqrt{M}}\sum_{k=0}^{b-1} \widetilde{v}_k^{(l)}e^{j\frac{2\pi tk}{b}}, \quad 0 \leq t \leq b-1.$$

For fast implementation, the FFT algorithm can be applied to the L distinct demasked versions of $\mathbf{v}$ simultaneously in a parallel fashion. Finally, concatenating the L segments forms $\mathbf{f} = (\mathbf{f}_0^T \mid \cdots \mid \mathbf{f}_{L-1}^T)^T$.

While updating current samples at each iteration, the matrix-vector multiplication $\mathbf{A}\widehat{\mathbf{x}}_i$ is also performed by the FFT algorithm in a similar manner to the measurement process. One may stop the iterations of the CoSaMP algorithm if the norm of updated samples is sufficiently small or the iteration counter reaches a predetermined value.

Table one of [20] claimed that forming a signal proxy dominates the algorithm complexity by the cost of matrix-vector multiplication. Thus, each iteration of the FFT-based CoSaMP recovery algorithm has the complexity of $O(L \times b \log b) \approx O(N \log M)$, which is smaller than that of random partial Fourier matrices.

5 Empirical recovery performance

In this section, we compare our new sensing matrices to chirp sensing [6] and random partial Fourier matrices in terms of empirical recovery performance in noiseless and noisy scenarios. For comparison, we assume that a random partial Fourier matrix has the same parameters M and $N = (M + 1)L$ as those of our new sensing matrix. To obtain it, we made ten trials to select M rows randomly from the N-point IDFT matrix, where the coherence was checked at each trial. Then, we chose the one with the smallest coherence for our experiments. For a chirp sensing matrix, on the other hand, M is set to a prime number closest to the parameter used in our new sensing matrix, and $N = ML$. Each submatrix of the partial chirp sensing matrix has an alternating polarity as in [30].

Through experiments, we measured an *s*-sparse signal **x**, where the *s* nonzero entries are either $+1$ or -1, and their positions and signs are chosen uniformly at random. For signal reconstruction, the FFT-based CoSaMP algorithm was applied to a total of $2,000$ sample vectors measured by the three sensing matrices. In Algorithm 1, the iterations are stopped if either $||\mathbf{v}|| < 10^{-4}$ or the iteration counter reaches the sparsity level *s*.
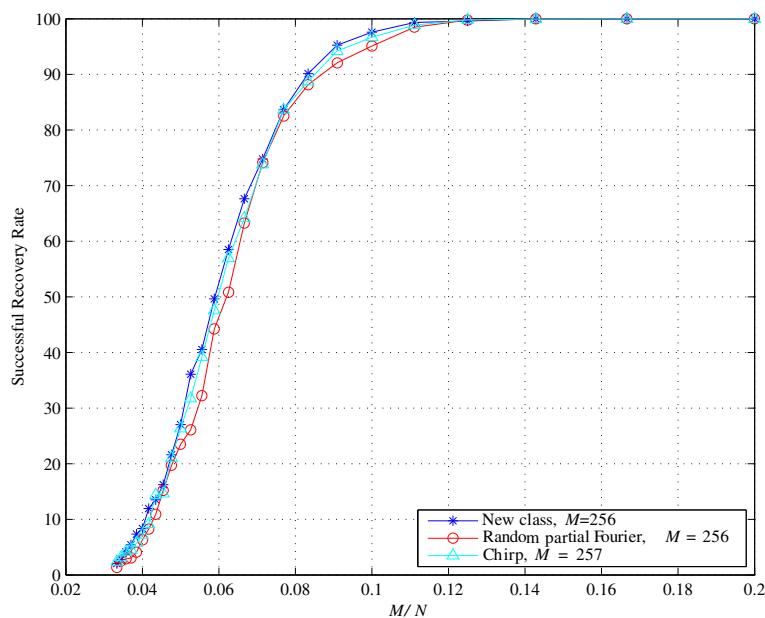
Figure 2 displays successful recovery rates of the three sensing matrices from noiseless measurements at various compression ratios, where the sparsity level is $s = 64$. In the figure, for $5 \leq L \leq 30$, $M = 256$ and $N = (M + 1)L$ for our new sensing and random partial Fourier matrices, while $M = 257$ and $N = ML$ for chirp sensing matrices. With the parameters, each sensing matrix achieves the compression ratios of $0.0333 \leq \frac{M}{N} \approx \frac{1}{L} \leq 0.2$. A success is declared in reconstruction if $||\mathbf{x} - \widehat{\mathbf{x}}|| < 10^{-6}$ for the estimate $\widehat{\mathbf{x}}$. The figure shows that our new sensing matrices have slightly higher recovery rates than the random partial Fourier matrices but have almost the same recovery rates as those of chirp sensing codes.

In noisy compressed sensing, a measured signal is corrupted by additive noise, i.e., $\mathbf{u} = \mathbf{y} + \mathbf{n} = \mathbf{Ax} + \mathbf{n}$, where **n** is the additive white Gaussian noise of zero mean and variance σ^2. Then, the *input signal-to-noise ratio (SNR)* is defined as $\text{SNR}_{input}(dB) = 10\log_{10}\frac{||\mathbf{y}||^2}{\sigma^2}$. Also,

we define the *reconstruction SNR* as $\text{SNR}_{reconst}(dB) = 10\log_{10}\frac{||\mathbf{x}||^2}{||\mathbf{x}-\widehat{\mathbf{x}}||^2}$, to measure the recovery performance in noisy compressed sensing. In the experiments, we fixed $L = 8$, where $M = 256$ and $N = L(M + 1) = 2,056$ for our new sensing and random partial Fourier matrices, while $M = 257$ and $N = ML = 2,056$ for chirp sensing matrices. Figure 3 shows an example of original and reconstructed signals for our new sensing matrix in noisy compressed sensing, where the sparsity level is $s = 15$ and the input SNR is 15 dB.

Figure 4 sketches the reconstruction SNR of the three sensing matrices from noisy measurements. In the figure, the input SNR is 15 dB. The figure reveals that our new sensing matrix outperforms the random partial Fourier and the chirp sensing matrices at high sparsity levels, but the differences are negligible. Figure 5 demonstrates reconstruction SNR versus input SNR of the three matrices in noisy compressed sensing, where the sparsity level of an original signal is 70. At the sparsity level, we observed that the relationship between reconstruction and input SNR is linear for medium and high input SNR. Our new sensing matrix slightly outperforms the random partial Fourier matrix for high input SNR but shows almost the same trend with the chirp sensing code.

In addition to the above experiments, we attempted an elementary image reconstruction employing the Haar wavelet transform. An original sparsified image was
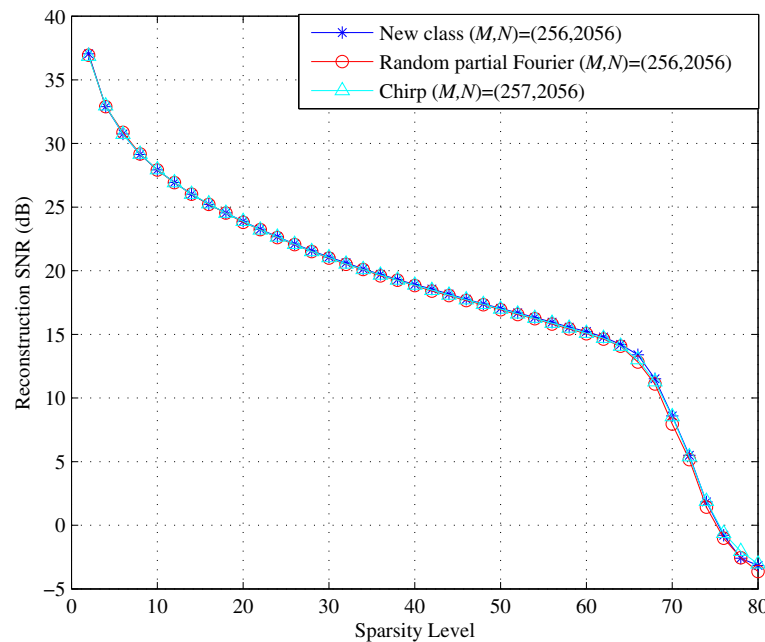

Figure 2 Successful recovery rates of the three sensing matrices from noiseless measurements. The figure displays successful recovery rates of our new class (asterisks), random partial Fourier (white circle), and chirp sensing (white triangle) matrices from noiseless measurements at various compression ratios of $\frac{M}{N}$, where the sparsity level is $s = 64$, $M = 256$ for our new sensing and random partial Fourier matrices, and $M = 257$ for chirp sensing codes.
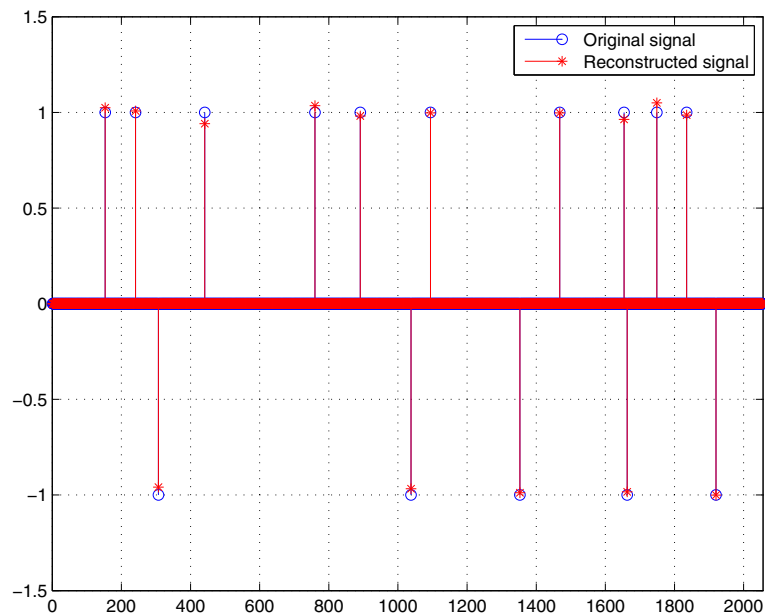
Figure 3 An example of original and reconstructed signals for our new sensing matrix in noisy compressed sensing. The figure shows an example of original (white circle) and reconstructed (asterisks) signals of length $N = 2,056$ from its noisy measurement of length $M = 256$ for our new sensing matrix, where $s = 15$ and $\text{SNR}_{input} = 15$ dB.

measured by the three sensing matrices and then reconstructed by the CoSaMP algorithm. We observed that the successfully reconstructed images from three different matrices are hard to distinguish, and show almost the same reconstruction SNR.

In conclusion, our new sensing matrix showed empirically reliable recovery performance by the CoSaMP algorithm in both noiseless and noisy scenarios, which is comparable to those of chirp sensing and random partial Fourier matrices.

Figure 4 Reconstruction SNR of the three sensing matrices in noisy compressed sensing. The figure sketches the reconstruction SNR of our new class (asterisks), random partial Fourier (white circle), and chirp sensing (white triangle) matrices from noisy measurements with $\text{SNR}_{input} = 15$ dB, where $M = 256$ and $N = 2,056$ for our new sensing and random partial Fourier matrices, while $M = 257$ and $N = 2,056$ for chirp sensing codes.
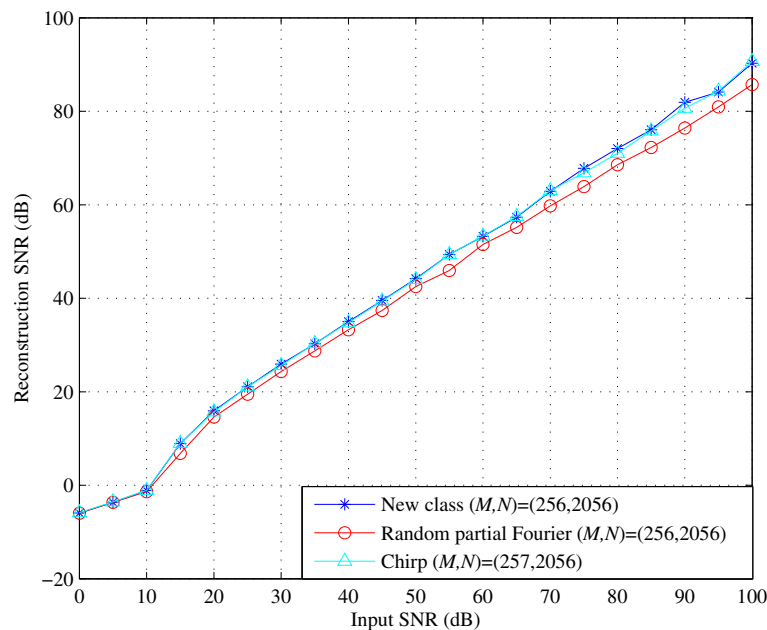
Figure 5 Reconstruction SNR versus input SNR in noisy compressed sensing for 70-sparse input signals. The figure displays reconstruction SNR versus input SNR of our new class (asterisks), random partial Fourier (white circle), and chirp sensing (white triangle) matrices in noisy compressed sensing for 70-sparse input signals, where $M = 256$ and $N = 2,056$ for our new sensing and random partial Fourier matrices, while $M = 257$ and $N = 2,056$ for chirp sensing codes.

6 Conclusions

This paper has constructed a new class of Fourier-based compressed sensing matrices using an almost difference set. We showed that a basic partial Fourier matrix, equivalent to the near-optimal partial Fourier codebook presented in [19], could be represented as a concatenation of DFT-based submatrices under row/column rearrangement. Choosing a full or a part of columns of the concatenated matrix, we then constructed a new sensing matrix which turns out to be an incoherent tight frame. The new sensing matrix guarantees unique sparse reconstruction with high probability for sparse signals with uniformly distributed supports. Moreover, experimental results revealed that our deterministic compressed sensing guarantees the empirically reliable recovery performance.

In conclusion, compared to existing chirp sensing and random partial Fourier matrices, our new sensing matrices have the benefits summarized:

1. Our new deterministic sensing matrices support various parameters of $M = p^r$ and $N = (M + 1)L$ for any prime p and positive integers r and L, $2 \leq L \leq M - 1$. They are incoherent tight frames for any such M and N. Compared to chirp sensing codes where M is generally restricted to a prime number, the new matrices therefore provide more options for the parameters M and N, permitting various compression ratios of $\frac{M}{N} \approx \frac{1}{L}$. A large number of new sensing matrices with a variety of admissible parameters may have many potential applications in compressed sensing.

2. The deterministic row index structure requires much less storage space than random partial Fourier matrices. Moreover, while the N-point FFT is required for random partial Fourier matrices, the DFT-based submatrix structure of our new sensing matrices allows the $(M + 1)$-point FFT processing, which enables efficient signal measurement and reconstruction with low complexity and fast processing. The benefits in implementation indicate the potential of our new sensing matrices in practical compressed sensing.

Appendix
Proof of procedure 1

First of all, Lemma 3 shows that the indices of D in Equation 1 are equivalently generated by cyclotomic cosets. In the proof, we use the well-known property that $(x + y)^{p^k} = x^{p^k} + y^{p^k}$ for $x, y \in \mathbb{F}_{p^m}$ and any integers m, k.

Lemma 3. *Consider all cyclotomic cosets modulo $p^r + 1$ over p. From Procedure 1, recall that if $p = 2$, $\Gamma_2(2^r + 1) \setminus \{0\} = \{u_1, \ldots, u_\delta\}$, and if $p > 2$, $\Gamma_p(p^r + 1) \setminus \{\frac{p^r+1}{2}\} = \{u_1, \ldots, u_\delta\}$, respectively. For each u_i, let C'_{u_i} be*

the cyclotomic coset having the coset leader u_i. Also, let $z_i \in \mathbb{Z}_{p^{2r}-1}$ be an integer satisfying Equation 8 for each u_i. Assume $z_i \in C_{s_i}$, where C_{s_i} is a cyclotomic coset modulo $p^{2r} - 1$ over p containing a coset leader s_i. Then,

1. In Equation 1 of Remark 1, $I = \bigcup_{1 \le i \le \delta} C'_{u_i}$.
2. $z_i = z_j$ if and only if $u_i = u_j$ for $1 \le i, j \le \delta$.
3. $|C_{s_i}| = |C'_{u_i}|$ for each i, $1 \le i \le \delta$.
4. Finally, the index set D of Equation 1 is given by

$$D = \bigcup_{1 \le i \le \delta} C_{s_i}. \tag{9}$$

Proof.
1. If $p = 2$, then $\bigcup_{1 \le i \le \delta} C'_{u_i} = \mathbb{Z}_{p^r+1} \setminus \{0\} = I$ is obvious. If $p > 2$, on the other hand, $\frac{p(p^r+1)}{2} - \frac{p^r+1}{2} = (p^r + 1) \times \frac{(p-1)}{2} \equiv 0 \pmod{p^r + 1}$ for odd p. Then, we have $\frac{p(p^r+1)}{2} \equiv \frac{p^r+1}{2} \pmod{p^r + 1}$, which means that $\frac{p^r+1}{2}$ is the only element of the cyclotomic coset containing it. Therefore, $\bigcup_{1 \le i \le \delta} C'_{u_i} = \mathbb{Z}_{p^r+1} \setminus \{\frac{p^r+1}{2}\} = I$ is also clear.
2. For given u_i, the solution $z_i \in \mathbb{Z}_{p^{2r}-1}$ of Equation 8 is unique from the structure of the finite field $\mathbb{F}_{p^{2r}}$. From the uniqueness, $z_i = z_j$ if and only if $u_i = u_j$ for $1 \le i, j \le \delta$.
3. For each i, let $|C'_{u_i}| = n_{u_i}$, where

$$u_i \equiv u_i p^{n_{u_i}} \pmod{p^r + 1}. \tag{10}$$

Also, let $|C_{s_i}| = n_{s_i}$. For $z_i \in C_{s_i}$,

$$z_i \equiv z_i p^{n_{s_i}} \pmod{p^{2r} - 1}. \tag{11}$$

Then, $1 + \alpha^{(p^r-1)u_i p^{n_{u_i}}} = \left(1 + \alpha^{(p^r-1)u_i}\right)^{p^{n_{u_i}}} = \alpha^{z_i p^{n_{u_i}}}$, where α is a primitive element in $\mathbb{F}_{p^{2r}}$. Since $1 + \alpha^{(p^r-1)u_i p^{n_{u_i}}} = 1 + \alpha^{(p^r-1)u_i} = \alpha^{z_i}$, we have $\alpha^{z_i p^{n_{u_i}}} = \alpha^{z_i}$, which implies

$$z_i \equiv z_i p^{n_{u_i}} \pmod{p^{2r} - 1}. \tag{12}$$

From Equations 11 and 12, n_{s_i} divides n_{u_i} since n_{s_i} is the smallest positive integer satisfying Equation 11. Similarly, $1 + \alpha^{(p^r-1)u_i p^{n_{s_i}}} = \left(1 + \alpha^{(p^r-1)u_i}\right)^{p^{n_{s_i}}} = \alpha^{z_i p^{n_{s_i}}} = \alpha^{z_i} = 1 + \alpha^{(p^r-1)u_i}$. Then,

$$u_i \equiv u_i p^{n_{s_i}} \pmod{p^r + 1}. \tag{13}$$

From Equations 10 and 13, n_{u_i} divides n_{s_i} since n_{u_i} is the smallest positive integer satisfying Equation 10. As n_{s_i} and n_{u_i} divide each other, it means $n_{u_i} = n_{s_i}$, or equivalently $|C'_{u_i}| = |C_{s_i}|$ for each i, $1 \le i \le \delta$.
4. With $z_i \in C_{s_i}$ and $u_i \in C'_{u_i}$ satisfying Equation 8, let us say that C_{s_i} is *associated* with C'_{u_i}. Recall that $\alpha^{(p^r+1)e_v} = \mathrm{Tr}_r^{2r}(\alpha^v)$ in Remark 1. For each index of

D in Equation 1,

$$\alpha^{d_k} = \alpha^{(p^r+1)e_v - v} = \alpha^{-v} \times \mathrm{Tr}_r^{2r}(\alpha^v)$$
$$= \alpha^{-v} \times (\alpha^v + \alpha^{vp^r}) = 1 + \alpha^{(p^r-1)v} \tag{14}$$

where $v \in I$ in Equation 1. In Equation 14, if $v = u_i$, then $d_k = z_i$ from Equation 8. Moreover,

$$\alpha^{z_i p^t} = \left(1 + \alpha^{(p^r-1)u_i}\right)^{p^t} = 1 + \alpha^{(p^r-1)u_i p^t} \tag{15}$$

for $1 \le t \le n_{u_i} = n_{s_i}$. Then, Equation 15 implies that each element of $C'_{u_i} = \{u_i, u_i p, \ldots, u_i p^{n_{u_i}-1}\}$ induces each element of $C_{s_i} = \{z_i, z_i p, \ldots, z_i p^{n_{s_i}-1}\}$ as a solution of Equation 15. For each element $v \in I = \bigcup_{1 \le i \le \delta} C'_{u_i}$, therefore, we conclude that the corresponding solution d_k of Equation 14 constitutes δ cyclotomic cosets of $C_{s_1}, \ldots, C_{s_\delta}$ each of which is associated with $C'_{u_1}, \ldots, C'_{u_\delta}$, respectively, which yields Equation 9. From item 2, $C_{s_1}, \ldots, C_{s_\delta}$ are disjoint, and the set D of Equation 9 has p^r distinct elements since $|D| = \sum_{i=1}^{\delta} |C_{s_i}| = \sum_{i=1}^{\delta} |C'_{u_i}| = |I| = p^r$. $\square$

From Lemma 3, if $p = 2$, Equation 9 directly presents the indices of D in Equation 2. If $p > 2$, on the other hand, we can simply add $\frac{M+1}{2}$ to each element of Equation 9, to obtain the indices of D in Equation 3. This verifies that Procedure 1 equivalently generates the row index set for our new sensing matrix.

Competing interests
The authors declare that they have no competing interests.

References
1. DL Donoho, Compressed sensing. IEEE Trans. Inf. Theory **52**(4), 1289–1306 (2006)
2. EJ Candes, J Romberg, T Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory **52**(2), 489–509 (2006)
3. EJ Candes, T Tao, Near-optimal signal recovery from random projections: Universal encoding strategies. IEEE Trans. Inf. Theory **52**(12), 5406–5425 (2006)
4. H Rauhut, Compressive sensing and structured random matrices, in *Theoretical Foundations and Numerical Methods for Sparse Recovery, Radon Series*. ed. by M. Fornasier. Computational and Applied Mathematics vol. 9 (deGruyter, Berlin, 2010), pp. 1–92
5. R Calderbank, S Howard, S Jafarpour, Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property. IEEE J. Sel. Topics Sig. Proc. **4**(2), 358–374 (2010)
6. L Applebaum, SD Howard, S Searle, R Calderbank, Chirp sensing codes: Deterministic compressed sensing measurements for fast recovery. Appl. Comput. Harmon. Anal. **26**, 283–290 (2009)
7. W Alltop, Complex sequences with low periodic correlations. IEEE Trans. Inf. Theory **26**(3), 350–354 (1980)

8. T Strohmer, R Heath, Grassmanian frames with applications to coding communication. Appl. Comput. Harmon. Anal. **14**(3), 257–275 (2003)
9. R Calderbank, S Howard, S Jafarpour, A sublinear algorithm for sparse reconstruction with l_2/l_2 recovery guarantees. 3rd IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), Aruba, 13–16 Dec 2009 (IEEE, Piscataway, 2009), pp. 209–212
10. S Howard, R Calderbank, S Searle, A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes. Conference on Information Systems and Sciences (CISS), Princeton, 19–21 March 2008 (IEEE, Piscataway, 2008), pp. 11–15
11. A Amini, V Montazerhodjat, F Marvasti, Matrices with small coherence using p-ary block codes. IEEE Trans. Sig. Proc. **60**, 172–181 (2012)
12. RA DeVore, Deterministic constructions of compressed sensing matrices. J. Complexity. **23**, 918–925 (2007)
13. S Gurevich, R Hadani, N Sochen, On some deterministic dictionaries supporting sparsity. J. Fourier Anal. Appl. **14**(5), 859–876
14. Z Xu, Deterministic sampling of sparse trigonometric polynomials. J. Complexity. **27**, 133–140 (2011)
15. NY Yu, Additive character sequences with small alphabets for compressed sensing matrices. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, 22–27 May 2011 (IEEE, Piscataway, 2011), pp. 2932–2935
16. S Li, F Gao, G Ge, S Zhang, Deterministic construction of compressed sensing matrices via algebraic curves. IEEE Trans. Inf. Theory. **58**(8), 5035–5041 (2012)
17. M Mishali, YC Eldar, Blind multiband signal reconstruction: Compressed sensing for analog signals. IEEE Trans. Sig. Proc. **57**(3), 993–1009 (2009)
18. ME Dominguez-Jimenez, N Gonzalez-Prelcic, G Vazquez-Vilar, R Lopez-Valcarce, Design of universal multicoset sampling patterns for compressed sensing of multiband sparse signals. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Kyoto, 25-30 March 2012 (IEEE, Piscataway, 2012), pp. 3337–3340
19. NY Yu, K Feng, A Zhang, A new class of near-optimal partial Fourier codebooks from an almost difference set. Des. Codes Cryptogr (2012). 10.1007/s10623-012-9753-8
20. D Needell, JA Tropp, CoSaMP: Iterative signal recovery from incomplete and inaccurate samples. Appl. Comput. Harmon. Anal. **26**, 301–321 (2009)
21. SW Golomb, G Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar.* (Cambridge University Press, Cambridge, 2005)
22. FJ MacWilliams, NJ Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977)
23. KT Arasu, C Ding, T Helleseth, PV Kumar, H Martinsen, Almost difference sets and their sequences with optimal autocorrelation. IEEE Trans. Inf. Theory **47**(7), 2934–2943 (2001)
24. DL Donoho, M Elad, Optimally sparse representation in general (nonorthogonal) dictionaries via l_1 minimization. Proc. Natl. Acad. Sci. **100**, 2197–2202 (2003)
25. LR Welch, Lower bounds on the maximum cross correlation of the signals. IEEE Trans. Inf. Theory **IT-20**, 397–399 (1974)
26. J Kovacević, A Chebira, *An Introduction to Frames: Foundations and Trends in Signal Processing*, vol. 2. (now Publishers, Hannover, 2008)
27. NY Yu, On statistical restricted isometry property of a new class of deterministic partial Fourier compressed sensing matrices. International Symposium on Information Theory and its Applications (ISITA), Honolulu, 28–31 Oct 2012 (IEEE, Piscataway, 2012), pp. 287–291
28. E Candes, Y Plan, Near-ideal model selection by l_1 minimization. Ann. Stat. **37**(5A), 2145–2177 (2009)
29. S Jafapour, MF Duarte, R Calderbank, Beyond worst-case reconstruction in deterministic compressed sensing. IEEE International Symposium on Information Theory Proceedings (ISIT), Cambridge, 1–6 July 2012 (IEEE, Piscataway, 2012), pp. 1862–1866
30. K Ni, S Datta, P Mahanti, S Roudenko, D Cochran, Efficient deterministic compressed sensing for images with chirps and Reed-Muller codes. SIAM J. Imaging Sci. **4**(3), 931–953 (2011)