ADDITIVE CHARACTER SEQUENCES WITH SMALL ALPHABETS FOR COMPRESSED SENSING MATRICES

Nam Yul Yu

Department of Electrical Engineering, Lakehead University
Thunder Bay, Ontario, Canada

ABSTRACT

Compressed sensing is a novel technique where one can recover sparse signals from the undersampled measurements. In this paper, a $K \times N$ measurement matrix for compressed sensing is deterministically constructed via additive character sequences. The Weil bound is then used to show that the matrix has asymptotically optimal coherence for $N = K^2$, and that it is a tight frame. A sparse recovery guarantee for the incoherent tight frame is also discussed. Numerical results show that the deterministic sensing matrix guarantees empirically reliable recovery performance via an $l_1$-minimization method for noiseless measurements.

Index Terms— Additive characters, compressed sensing, sequences, Weil bound.

1. INTRODUCTION

Compressed sensing 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 $x \in \mathbb{R}^N$ with a $K \times N$ measurement matrix $A$ produces a $K$-dimensional vector $y = Ax$, where $K < N$. Imposing an additional requirement that $x$ is $s$-sparse or the number of nonzero entries in $x$ is at most $s$, one can recover $x$ exactly with high probability by an $l_1$-minimization method, which is computationally tractable.

Many research activities have been triggered on compressed sensing since Donoho [1], and Candes, Romberg, and Tao [2][3] published their marvelous theoretical works. The efforts revealed that a measurement matrix $A$ plays a crucial role in recovery of $s$-sparse signals. To facilitate the practical applications, we may consider a deterministic matrix, where a variety of techniques have been proposed for the construction [4]–[7]. Although the theoretical recovery bounds are worse than that of a random matrix, the deterministic matrices guarantee the recovery performance that is empirically reliable, allowing low cost implementation.

To enjoy the benefits of deterministic construction, this paper presents how to construct a $K \times N$ measurement matrix for compressed sensing via additive character sequences. Precisely, we construct the matrix by employing additive character sequences with small alphabets as its column vectors. The Weil bound [8] is then used to show that the matrix has asymptotically optimal coherence for $N = K^2$, and that it is a tight frame with the smallest possible redundancy. A sparse recovery guarantee for the incoherent tight frame is also discussed. Through numerical experiments, we observe that the deterministic matrix guarantees empirically reliable recovery performance via $l_1$-minimization for noiseless measurements. In particular, at least 99% successful recovery is empirically guaranteed for the sparsity level of $O(K / \log N)$.

Using additive character sequences with small alphabets, the matrix can be efficiently implemented by linear feedback shift registers (LFSR) [9].

2. PRELIMINARIES

The following notations will be used throughout this paper.

- $\omega_p = e^{\frac{2\pi i}{p}}$ where $p$ is a prime integer and $j = \sqrt{-1}$.
- $\mathbb{F}_q = \text{GF}(q)$ is the finite field with $q$ elements and $\mathbb{F}_q[x]$ is the polynomial ring over $\mathbb{F}_q$.

- Let $p$ be prime, and $m$ and $l$ be positive integers with $l | m$. A trace function is a linear mapping from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_p$ defined by

$$T_{p^m}(x) = \sum_{i=0}^{m/l-1} x^{p^i}, \quad x \in \mathbb{F}_{p^m}$$

where the addition is computed modulo $p$.

2.1. Additive characters

Let $p$ be prime and $m$ a positive integer. We define an additive character [10] of $\mathbb{F}_{p^m}$ as

$$\chi(x) = \exp \left( j \frac{2\pi T_{p^m}(x)}{p} \right), \quad x \in \mathbb{F}_{p^m} \quad (1)$$
where $\chi(x + y) = \chi(x)\chi(y)$ for $x, y \in \mathbb{F}_p^m$. The Weil bound \cite{weil} gives an upper bound on the magnitude of additive character sums. We introduce the bound as described in \cite{construction}.

**Proposition 1** \cite{construction} Let $f(x) \in \mathbb{F}_p^m[x]$ be a polynomial of degree $r \geq 1$ with $\gcd(r, p^m) = 1$. Let $\chi$ be the additive character of $\mathbb{F}_p^m$ defined in (1). Then,

$$\left| \sum_{x \in \mathbb{F}_p^m} \chi(f(x)) \right| \leq (r - 1) \sqrt{p^m}$$

where $\sum_{x \in \mathbb{F}_p^m} \chi(x) = 0$ is obvious.

### 2.2. Coherence and redundancy

In compressed sensing, a $K \times N$ deterministic matrix $A$ is associated with two geometric quantities, coherence and redundancy \cite{coherence}. Assume that each column vector $a_n = (a_{0,n}, \cdots, a_{K-1,n})^T$, $0 \leq n \leq N - 1$, has unit $l_2$-norm, i.e., $\|a_n\|_2 = \sqrt{\sum_{k=0}^{K-1} |a_{k,n}|^2} = 1$, where $T$ denotes the transpose. The coherence $\mu$ is defined by

$$\mu = \max_{0 \leq n \neq m \leq N - 1} |a_n^H \cdot a_m|$$

where $a_n^H$ is the conjugate transpose of $a_n$. In general, the coherence is lower bounded by the Welch bound \cite{welch}, i.e.,

$$\mu \geq \sqrt{\frac{N - K}{K(N - 1)}}.$$

The redundancy, on the other hand, is defined as $\rho = ||A||^2$, where $|| \cdot ||$ denotes the spectral norm of $A$, or the largest singular value of $A$. We have $\rho \geq N/K$, where the equality holds if and only if $A$ is a tight frame. If $A$ is a tight frame with small coherence and redundancy, then it has been shown that the sparse solutions are necessarily unique \cite{unique}.

### 3. ADDITIVE CHARACTER COMPRESSED SENSING MATRICES

#### 3.1. Construction

**Construction 1** Let $p$ be an odd prime, and $m$ and $h$ be positive integers, where $h > 1$. Let $K = p^m$ and $N = K^h = p^{mh}$. Set a column index to $n = \sum_{i=1}^{h} u_i K^{i-1}$, where $u_i \equiv \left[ \frac{n}{K^{i-1}} \right] \mod K$. For each $i$, $1 \leq i \leq h$, let

$$b_i = \begin{cases} 0, & \text{if } u_i = 0, \\ \alpha^{u_i - 1}, & \text{if } 1 \leq u_i \leq p - 1, \end{cases}$$

where $b_i \in \mathbb{F}_p^m$ and $\alpha$ is a primitive element in $\mathbb{F}_p^m$. For a positive integer $d \geq h$, let $r_1, r_2, \cdots, r_h$ be $h$ distinct integers such that $1 = r_1 < r_2 < \cdots < r_h = d$ and $\gcd(r_i, p^m) = 1$ for each $i$, $1 \leq i \leq h$. Then, we construct a $K \times N$ compressed sensing matrix $A$ where each entry is given by

$$a_{k,n} = \begin{cases} \frac{1}{\sqrt{K}}, & \text{if } k = 0, \\ \frac{1}{\sqrt{K}} \omega_{p}^{\sum_{i=1}^{h} b_i \alpha^{r_i(k-1)}}, & \text{if } 1 \leq k \leq K - 1, \end{cases}$$

where $0 \leq n \leq N - 1$.

**Theorem 1** In the $K \times N$ matrix $A$ from Construction 1, the coherence is bounded by

$$\mu = \max_{0 \leq n_1 \neq n_2 \leq N - 1} |a_{n_1}^H \cdot a_{n_2}| \leq \frac{d - 1}{\sqrt{K}}$$

where if $d = 2$, the coherence is asymptotically optimal, achieving the equality of the Welch bound for large $K$.

**Proof.** Consider the column indices of $n_1 = \sum_{i=1}^{h} u_i K^{i-1}$ and $n_2 = \sum_{i=1}^{h} u_i' K^{i-1}$, where $n_1 \neq n_2$. According to (2), let $b_i = 0$ or $\alpha^{u_i-1}$, and $b_i' = 0$ or $\alpha^{u_i'-1}$, respectively. Similarly, from (3), let $x = 0$ if $k = 0$, or $x = \alpha^{r_i-1}$ otherwise. Then, the inner product of the pair of columns is given by

$$|a_{n_1}^H \cdot a_{n_2}| = \frac{1}{K} \left| \sum_{x \in \mathbb{F}_p^m} \omega_{p}^{\sum_{i=1}^{h} (b_i - b_i') x^{r_i}} \right| = \frac{1}{K} \left| \sum_{x \in \mathbb{F}_p^m} \chi \left( \sum_{i=1}^{h} (b_i - b_i') x^{r_i} \right) \right|.$$

In (5), if $n_1 \neq n_2$, then $f(x) = \sum_{i=1}^{h} (b_i - b_i') x^{r_i}$ is a nonzero polynomial in $\mathbb{F}_p^m[x]$, as there exists at least a pair of $(b_i, b_i')$ where $b_i \neq b_i'$. Since $\gcd(r_i, p^m) = 1$ for any $r_i$, the Weil bound in Proposition 1 gives $|a_{n_1}^H \cdot a_{n_2}| \leq \frac{(d - 1)\sqrt{K}}{K} = \frac{d - 1}{\sqrt{K}}$ from which the upper bound on the coherence $\mu$ in (4) is immediate. For given $K$ and $N$, the equality of the Welch bound is computed by $\sqrt{\frac{N - K}{K(N - 1)}} = \sqrt{\frac{N - K}{K(N - 1)}} \approx \frac{1}{\sqrt{K}}$ for large $K$. Therefore, if $d = 2$, the coherence asymptotically achieves the equality of the Welch bound for large $K$. \hfill $\Box$

In Construction 1, $d$ should be chosen as a sufficiently small number for the coherence of $A$ to be small. A typical choice of $d = h \leq p - 1$ and $r_1 = 1, r_2 = 2, \cdots, r_h = h$ guarantees the condition of $\gcd(r_i, p^m) = 1$ for any $r_i$ as well as the small coherence for the matrix $A$ with $N = K^d$.

**Remark 1** Donoho and Elad \cite{donoho} revealed that $(2s - 1)\mu < 1$ ensures unique s-sparse recovery by l1-minimization. From the result and the coherence in Theorem 1, the matrix $A$ from Construction 1 guarantees a unique s-sparse solution by l1-minimization if

$$s < \frac{1}{2} \left( \frac{\sqrt{K}}{d - 1} + 1 \right).$$

2933
Table 1. Comparison of several $K \times N$ deterministic sensing matrices

<table>
<thead>
<tr>
<th>Method</th>
<th>$K$</th>
<th>$N$</th>
<th>Alphabet size</th>
<th>Coherence</th>
<th>Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chirp sensing [5]</td>
<td>$2^m$</td>
<td>$m$ is odd</td>
<td>$K^2$</td>
<td>$\frac{1}{\sqrt{K}}$</td>
<td>$N/K$</td>
</tr>
<tr>
<td>Delaunay-Goethals ($r \geq 0$) [4]</td>
<td>$2^m$, $m$ is odd</td>
<td>$K^{r+2}$</td>
<td>$K^2$</td>
<td>$\leq \sqrt{K}$</td>
<td>$N/K$</td>
</tr>
<tr>
<td>Dual of extended binary BCH [4][6]</td>
<td>$2^m$, $m$ is odd</td>
<td>$K^2$</td>
<td>$2$</td>
<td>$\leq (d-1)/\sqrt{K}$</td>
<td>$N/K$</td>
</tr>
<tr>
<td>Additive character ($h = d \geq 2$)</td>
<td>$p^m$, $p$ is an odd prime</td>
<td>$K^d$</td>
<td>$p$</td>
<td>$N/K$</td>
<td>$N/K$</td>
</tr>
</tbody>
</table>

In particular, if $d = h$, then $\log \left( \frac{K}{N} \right) = (h - 1) \log K = (d - 1) \log K$ with $N = K^d$, and thus $\frac{1}{d-1} = \frac{\log K}{\log(N/K)}$. For unique sparse recovery, (6) then yields $s < \frac{1}{2} \left( \sqrt{\frac{\log K}{\log(N/K)}} + 1 \right)$. Therefore, Construction 1 guarantees unique sparse recovery for the sparsity level of $s \leq C \sqrt{K} \log K / \log(N/K)$ with a constant $C$. The bound is the largest known sparse recovery guarantee for deterministic construction [7].

**Theorem 2** In Construction 1, $A$ is a tight frame with redundancy $\rho = N/K$.

**Proof.** Recall $n$ and $u_t$ in the column index representation of $A$ in Construction 1. For $0 \leq t \leq K^{h-1} - 1$, let $\sigma_t$ be a set of $K$ indices of $n = \sum_{t=1}^{h} u_t K^{t-1}$ where $u_t$ is varying for $0 \leq u_t \leq K - 1$, while $u_2, u_3, \ldots, u_h$ are fixed. That is, $\sigma_t = (tK, t(K + 1), \ldots, t(K + h - 1))$, where $t = u_2 + u_3 K + \ldots + u_h K^{h-2}$. Accordingly, note from (2) that $b_1$ runs through $\mathbb{F}_{p^m}$, while $b_2, b_3, \ldots, b_h$ are fixed in $\mathbb{F}_{p^m}$. Let $A_{\sigma_t}$ be a $K \times K$ submatrix of $A$ which contains a set of columns with the indices in $\sigma_t$. Then, $A_{\sigma_t}$ is a set of $K$ orthonormal bases $A$ is a concatenation of $A_{\sigma_t}$, i.e., $A = (A_{\sigma_0}, A_{\sigma_1}, \ldots, A_{\sigma_{K^{h-1}-1}})$.

For given $t$, let $w_{k_1}$ and $w_{k_2}$ be a pair of row vectors in $A_{\sigma_t}$, where $0 \leq k_1 \neq k_2 \leq K - 1$. For $l = 1$ and $2$, let $x_l = \alpha_l$ if $k_l = 0$, and $x_l = \alpha_k l - 1$ if $k_l \geq 1$. Then,

$$|w_{k_1}^H \cdot w_{k_2}| = \frac{1}{K} \left| \sum_{b_1 \in \mathbb{F}_{p^m}} Tr_{F_{p^m}}(\Sigma_{i=1}^{h} b_i (x_1^i - x_2^i)) \right|$$

$$= \frac{1}{K} \left| \sum_{b_1 \in \mathbb{F}_{p^m}} Tr_{F_{p^m}}(\Sigma_{i=2}^{h} b_i (x_1^i - x_2^i)) \right|$$

$$= 0$$

where $r_1 = 1$ and $x_1 \neq x_2$. Hence, a pair of rows in $A_{\sigma_t}$ is mutually orthogonal. The mutual orthogonality of a pair of rows in $A$ is obvious when $A_{\sigma_t}$ is concatenated for all $t$. From the orthogonality, $A A^H = \frac{N}{K} I_K$, where $I_K$ is a $K \times K$ identity matrix. Thus, $A$ is a tight frame with $\rho = N/K$.

Table 1 compares the geometric parameters of several deterministic matrices. It suggests that the additive matrix can be suitable for compressed sensing, providing low coherence and redundancy, and small alphabet size.

![Fig. 1. Successful recovery rates for additive, chirp sensing, and partial Fourier matrices.](image)

3.2. Recovery performance

In numerical experiments, taking $d = h = 2$ and $r_1 = 1$ and $r_2 = 2$, we consider the matrices of $N = K^2$ in Construction 1. For the noiseless recovery performance, we performed the l1-minimization by the complex basis pursuit solver in the SPGL1 package [14][15] to find a solution of $\min_{x \in \mathbb{C}^N} ||\tilde{x}||_1$ subject to $A\tilde{x} = y$, where $||\tilde{x}||_1 = \sum_{i=0}^{N-1} |\tilde{x}_i|$. We measured successful recovery rates of sparse signals, where total 1000 sample vectors were tested for each sparsity level. Each nonzero entry of an $s$-sparse signal has the magnitude of 1, where its position and sign are chosen uniformly at random. In the recovery process, a success is declared if the squared error is reasonably small, or $||x - \tilde{x}||_2 < 10^{-4}$.

Figure 1 shows successful recovery rates of $s$-sparse signals measured by the $81 \times 6561$ additive sensing matrix $A$. For comparison, it also displays the rates for a randomly chosen partial Fourier matrix of the same dimension, and the $79 \times 6241$ chirp sensing matrix [5], respectively. In the partial Fourier ensembles, we chose a new matrix at each instance of an $s$-sparse signal, in order to obtain the average rate. In the experiment, we observed that if $s \leq 4$, all $s$-sparse signals are successfully recovered for the matrix $A$, which confirms the sufficient condition for unique sparse recovery in Remark 1. Furthermore, the figure reveals that more than 99% successful recovery rates are observed for $s \leq 9$, which implies that...
our sensing matrix has fairly good recovery performance at the sparsity levels higher than that of the sufficient condition. The additive sensing matrix outperforms the randomly chosen partial Fourier matrix in sparse recovery, which has been also observed for $K = 125$ and $N = 15625$. Also, its recovery performance is similar to that of the chirp sensing code.

Figure 2 displays successful recovery rates of $K \times N$ additive sensing matrices for various $K$ and $N = K^2$. For each $K$, we observed 100% successful recovery of $s$-sparse signals if $s < \frac{\sqrt{\frac{K}{N}}+1}{2}$. Moreover, the maximum sparsity levels $s_{\text{max}}$ guaranteeing more than 99% successful recovery rates are 6, 9, 12, 16, 22 for $K = 49, 81, 125, 169, 243$, respectively, where $s_{\text{max}} \approx K/\log N$. Empirically, the additive sensing matrices guarantee more than 99% successful recovery for the sparsity level of $O(K/\log N)$.

4. CONCLUSION

This paper has presented how to deterministically construct a measurement matrix for compressed sensing via additive character sequences. We showed that the deterministic matrix achieves the optimal coherence for $N = K^2$ and it is a tight frame with the smallest redundancy. Through numerical experiments, we observed that the additive sensing matrices empirically guarantee at least 99% successful recovery from noiseless measurements for the sparsity level of $O(K/\log N)$. The deterministic construction allows an efficient LFSR implementation of the sensing matrix [9].

5. REFERENCES


