Deterministic Construction of Binary and Bipolar Measurement Matrices Using BCH Codes

Shashank Ranjan[1] Dr. M. Vidyasagar FRS [2]

[1]PhD Scholar, IIT Hyderabad

[2]SERB National Science Chair and Distinguished Professor, IIT Hyderabad

December 12, 2023

IIT Hyderabad

Outline I

Outline II

Outline III

Outline IV

Compressed sensing refers to the recovery of high-dimensional but low-complexity data from a small number of linear measurements.

Two common applications

- Vector Recovery: Reconstruct a high-dimensional but sparse (or nearly sparse) vector.
- Matrix Recovery: Reconstruct a high-dimensional but low rank matrix.

- The objective is to recover a sparse or a nearly sparse vector $x \in \mathbb{R}^n$ from a lower-dimentional measurment vector

$$y = Ax + \eta,$$

where $A \in \mathbb{R}^{m \times n}$ $(m < n)$ is called the measurement matrix, and $\eta \in \mathbb{R}^m$ is the measurement noise with a known upper bound $\|\eta\|_2 \leq \epsilon$.

- In order to recover x, we need a decoder map $\Delta : \mathbb{R}^m \to \mathbb{R}^n$.

IIT Hyderabad

- Let $\Sigma_k \subseteq \mathbb{R}^n$ denote the set of k-sparse vectors, that is, the set of vectors with no more than k nonzero components. Given a norm $\|\cdot\|$, let

$$\sigma_k(x, \|\cdot\|) := \min_{z \in \Sigma_k} \|x - z\|$$

denote the k-sparsity index of x, which measures how close x is to being sparse.

- The decoder map (Δ) which is widely used in the recovery of x is the **Basis pursuit** decoder map (Δ_{BP}) i.e.,

$$\Delta_{\mathrm{BP}}(y) := \arg\min_z \|z\|_1 \text{ s.t. } \|y - Az\|_2 \leq \epsilon. \qquad (1)$$

Definition 1

The pair $(A, \Delta_{\mathrm{BP}})$ is said achieve **robust sparse recovery** of order k if, there exists constants C and D such that for all $\eta \in \mathbb{R}^m$ with $\|\eta\|_2 \leq \epsilon$, the following inequality holds

$$\|\Delta_{\mathrm{BP}}(Ax + \eta) - x\|_p \leq C\sigma_k(x, \|\cdot\|_1) + D\epsilon, \ \forall x \in \mathbb{R}^n. \qquad (2)$$

The usual choices for p in (2) are $p = 1$ and $p = 2$.

There are two widely used sufficient conditions on the matrix A that enable robust sparse recovery; namely, **Restricted Isometry Property (RIP)** and **Robust Null Space Property (RNSP)**.

IIT Hyderabad

Definition 2

A matrix $A \in \mathbb{R}^{m \times n}$ is said to satisfy the **restricted isometry property (RIP)** of order k with constant $\delta_k \in (0, 1)$ if

$$(1 - \delta_k)\|u\|_2^2 \leq \|Au\|_2^2 \leq (1 + \delta_k)\|u\|_2^2, \ \forall u \in \Sigma_k. \tag{3}$$

Definition 3

A matrix $A \in \mathbb{R}^{m \times n}$ is said to satisfy **robust null space property (RNSP)** of order k with constants $\rho \in (0, 1)$ and $\tau > 0$ if, for all $S \subseteq [n]$ with $|S| \leq k$, it is the case that

$$\|h_S\|_1 \leq \rho\|h_{S^c}\|_1 + \tau\|Ah\|_2, \ \forall h \in \mathbb{R}^n. \tag{4}$$

IIT Hyderabad

Ranjan and Vidyasagar, IEEE T-SP, 2019: RIP implies RNSP.

Theorem 4

Suppose $A \in \mathbb{R}^{m \times n}$ *satisfies* RIP *of order* tk *with* $\delta_{tk} < \sqrt{(t-1)/t}$ *for some* $t > 1$. *Define*

$$v := \sqrt{t(t-1)} - (t-1) \in (0, 0.5)$$

$$a := [v(1-v) - \delta(0.5 - v + v^2)]^{1/2},$$

$$b := v(1-v)\sqrt{1+\delta},\ c := \left[\frac{\delta v^2}{2(t-1)}\right]^{1/2}.$$

Then A *satisfies robust null space property of order* k *with*

$$\rho := \frac{c}{a},\ \tau := \sqrt{k}\frac{b}{a^2}.$$

- This finding lead to the conclusion that RNSP is a weaker condition than RIP.
- Subsequent to this result, in a recent work, Lotfi and Vidyasagar have proposed a class of binary matrices that directly satisfy RNSP while bypassing RIP.
- They have also shown that the value of k for which the RNSP is guaranteed to hold is $3\sqrt{3}/2 \approx 2.6$ times larger than for the RIP.

- We present a deterministic construction method for designing the binary and bipolar compressed sensing matrices based on BCH codes.
- In our work, we adopt the methodology used in the construction of binary matrices proposed by Lotfi and Vidyasagar. Therefore, the matrices proposed here directly satisfy the RNSP while bypassing the RIP.
- For the matrices proposed here, the value of k for which the RNSP is guaranteed to hold is at least 1.3 times larger than for the RIP.

IIT Hyderabad

- If k is of the form 2^i, where $i \in \mathbb{N}$, then for below two cases

$$\frac{1}{2}\left(\sqrt[3]{n+\sqrt{n^2-1/27}}+\sqrt[3]{n-\sqrt{n^2-1/27}}\right) \leq k < \frac{1}{8}\left(\sqrt{n}+\sqrt{n+16(\sqrt{n}+1)}\right) \quad (5)$$

$$k \leq \frac{\sqrt[3]{n}}{2.83}, \quad (6)$$

the matrices proposed by us require fewer number of measurements than the binary matrices proposed by Lotfi and Vidyasagar.

Outline I

Outline II

Outline III

Outline IV

- A binary inear code denoted by $[\tilde{n}, \tilde{k}, d_{min}]_2$ is a linear subspace $\mathcal{C} \subseteq \mathbb{F}_2^{\tilde{n}}$ of dimension $\tilde{k}$, where $\mathbb{F}_2$ denotes the binary field, and $\tilde{n}$ is the code length.
- $|\mathcal{C}| = 2^{\tilde{k}}$
- The elements of $\mathcal{C}$ are called codewords.
- The **weight** of a codeword is the number of its non-zero elements.
- The **distance** d_{min} of a linear code is the minimum weight of its non-zero codewords.
- if vector $\mathbf{1}_m$ consisting of all ones is a codeword, then $\mathcal{C}$ is said to be **symmetric**.
- $\mathcal{C}$ is said to be cyclic if for every codeword, its circular shif is also a valid codeword.

IIT Hyderabad

- Narrow-sense primitive binary BCH codes are a class of cyclic binary codes with $\tilde{n} = 2^{\tilde{m}} - 1$ ($\tilde{m}$ is a positive integer) which are produced by a generating polynomial $g(x) \in GF(2)[x]$ such that $g(x) \mid x^{2^{\tilde{m}}-1} + 1$.
- In our work, when we say that a BCH code has the designed distance d, we mean that $\alpha^1,\ \alpha^2,\ \ldots, \alpha^{d-1}$ are different non-repeating roots of $g(x)$ (not necessarily all the roots), and $(x+1) \nmid g(x)$, where $\alpha \in GF(2^{\tilde{m}})$ is a primitive root of the field.
- Here, $d_{min} \geq d$. Since $(x+1) \nmid g(x)$, the code will be symmetric. Which means for every codeword its complement will aslo be a valid codeword.
- Since, $\tilde{n}$ is odd, each complement couple will have one even parity codeword and one odd parity codeword.

Outline I

Outline II

Outline III

IIT Hyderabad

Outline IV

Amini and Marvasti, IEEE T-IT, 2011

Theorem 5

Let $\mathcal{C} := [\tilde{n},\ \tilde{k}, d_{min}]_2$ *be a symmetric code. Let* $B \in \{0,1\}^{\tilde{n}\times 2^{\tilde{k}-1}}$ *be the matrix composed of code vectors as its column such that such that from each complement couple, exactly one is selected. Define*

$$A = \frac{1}{\sqrt{\tilde{n}}}\left(2B - \mathbf{1}_{\tilde{n}\times 2^{\tilde{k}-1}}\right). \tag{7}$$

Then A *satisfies the RIP with constant* $\delta_k = (k-1)\ (1 - 2\frac{d_{min}}{\tilde{n}})$ *for* $k < \frac{\tilde{n}}{\tilde{n}-2d_{min}} + 1$ *(* k *is the RIP order).*

The authors used BCH code in their construction.

IIT Hyderabad

Outline I

Outline II

Outline III

Outline IV