1 Introduction

Compressed Sensing (CS) aims at recovering high dimensional sparse vectors from considerably fewer linear measurements. It refers to a problem of an economical recovery of an unknown vector $u \in \mathbb{R}^m$ from the information provided by linear measurements. Problem of sparse recovery through $l_0$ norm minimization (minimizes the solution set through $l_0$ norm) which is not tractable. Donoho with coauthors [1][2] made several pioneering contributions and reposed the problem as a simple LPP. They then established the equivalent conditions for a sparse recovery problem to become a LPP problem. RIP is one sufficient condition. Random matrices such as Gaussian or Bernouli as their entries are satisfies RIP. One of the verification procedure for these matrices, based on the Johnson-Lindenstrauss lemma [16] is given by R.Barianiuk [11].

R.Devore [12] was first to construct deterministic RIP matrices with 0’s and 1’s as elements. In the present work, we extend the ideas embedded in [12] and construct 0, 1−matrices possessing relatively better recovery properties. In particular, we show that by using homogeneous multivariable polynomials, we will get different size of 0, 1−matrices apart from the Devore’s matrices size. In some particular cases our matrices have better recovery properties.

2 Sparse recovery from linear measurements

As stated already CS refers to a problem of an economical recovery of an unknown vector $u \in \mathbb{R}^m$ from the information provided by linear measurements $\langle u, \phi_j \rangle, \phi_j \in \mathbb{R}^m, j = 1, 2, \ldots, n$. Where, $\langle u, \phi_j \rangle$ is inner product between $u, \phi_j$. The basic objective in CS is to design a recovery procedure based on the concept of sparsity is to that finds $u$ from the information $y = (\langle u, \phi_1 \rangle, \ldots, \langle u, \phi_n \rangle) \in \mathbb{R}^n$. We note that most important case is when the number of measurements $n$ is much smaller then $m$. Sparse representations seem to have merit for various applications in areas such as image/signal processing and numerical computation.

A vector $u \in \mathbb{R}^m$ $k$−sparse if it has at most $k$ nonzero coordinates. Mathe-
natically this problem can be posed as,

\[ P_0 : \min_v \|v\|_0 \text{ subject to } \Phi v = y. \]  

(1)

Here \( \|v\|_0 = |\{i \mid v_i \neq 0\}|. \)

D. Donoho with coauthors [1][2] have begun a systematic study of the following question: For which measurement matrices \( \Phi \), the highly non-convex combinatorial optimization problem \( P_0 \) remains equivalent to its convex relaxation problem

\[ P_1 : \min_v \|v\|_1 \text{ subject to } \Phi v = y. \]  

(2)

Here \( \|v\|_1 \) denotes the \( l_1 \)-norm of the vector \( v \in \mathbb{R}^m \). Denote the solution to \( P_1 \) by \( f_{\Phi}(y) \) and solution to \( P_0 \) by \( u_{\Phi}^0(y) \in \mathbb{R}^m \).

3 On the equivalence between \( P_0 \) and \( P_1 \) problems

Definition 3.1: The mutual-coherence \( \mu(\Phi) \) of a given matrix \( \Phi \) is the largest absolute normalized inner product between different columns of \( A \). Denoting the \( k \)-th column in \( A \) by \( a_k \), the mutual-coherence is given by

\[ \mu(\Phi) = \max_{1 \leq i,j \leq m, i \neq j} \frac{|\phi_i^T \phi_j|}{\|\phi_i\|_2 \|\phi_j\|_2}. \]  

(3)

It is known [2] that for \( \mu \)-coherent matrices \( \Phi \), one has

\[ u_{\Phi}^0(y) = f_{\Phi}(y) = u, \]  

(4)

provided \( u \) is \( k \)-sparse with \( k < \frac{1}{2} \left( 1 + \frac{1}{\mu} \right) \). D. Donoho [3] has given sufficient conditions on the matrix \( \Phi \) for (4) to hold.

Candes and Tao [8] introduced the following isometry condition on matrices \( \Phi \) and established its important role in CS. An \( n \times m \) matrix \( \Phi \) is said to satisfy the Restricted Isometry Property (RIP) of order \( k \) with constant \( \delta_k \) if, for all \( k \)-sparse vectors \( x \in \mathbb{R}^m \), we have

\[ (1 - \delta_k) \|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1 + \delta_k) \|x\|_2^2. \]  

(5)

Consider the \( n \times |T| \) matrices \( \Phi_T \) formed by the columns of \( \Phi \) with indices from \( T \). Then (5) is equivalent to showing that the Grammian matrices \( A_T = \Phi_T^T \Phi_T, |T| = k \), are bounded and boundedly invertible on \( l_2 \) with bounds as in (5), uniform for all \( T \) such that \( |T| = k \).

Candes and Tao [8] have shown that whenever \( \Phi \) satisfies the RIP of order \( 3k \) with \( \delta_{3k} < 1 \), then

\[ \|u - f_{\Phi}(\Phi u)\|_{l_2^T} \leq C k^{\frac{1}{2}} \sigma_k(u)_{l_1^m}, \]  

(6)

where \( \sigma_k(u)_{l_1^m} \) denotes the \( l_1 \) error of the best \( k \)-term approximation, and the constant \( C \) depends only on \( \delta_{3k} \). This means that the bigger the value of \( k \)
Deterministic construction of compressed sensing matrices using multivariable polynomials

for which we can verify the RIP then the better guarantee we have on the performance of $\Phi$.

How can we construct matrices $\Phi$ that satisfy the RIP for the largest possible range of $k$? The widest range possible is $k \leq Cn \log(mn)$ [11] [12] [6] [5]. To get the optimal result we want $\Phi$ to satisfy RIP of order $k = n \log(mn)$ [11] [12]. The only known constructions yielding matrices that satisfy the RIP for this range are based on random matrices

Richard Baraniuk and co-authors [11] have verified the RIP for random matrices with some probability using the following concentration of measure inequality:

$$\Pr(|\|\Phi(\omega)u\|_2^2 - \|u\|_2^2| \geq \epsilon \|u\|_2^2) \leq 2e^{-nc_0(\epsilon)}, \ 0 < \epsilon < 1.$$  (7)

Where the probability is taken over all $n \times m$ matrices $\Phi(\omega)$, and $c_0(\epsilon)$ is a constant dependent only on $\epsilon$ such that for all $\epsilon \in (0, 1)$, $c_0(\epsilon) > 0$.

However, there are no deterministic constructions for $k$ of this size. It is an open problem to design the good deterministic constructions of RIP matrices; see T. Tao’s weblog [14] for detailed discussion. R. DeVore [12], J. Nelson and V. N. Temlyakov [13] have constructed deterministic RIP matrices. Devore has constructed $0, 1$-RIP matrix using univariable polynomials. Nevertheless, in the present work, we attempt to extend the Devore’s work and construct $0, 1$-matrices based on multivariable homogeneous polynomials. In particular, we prove that such polynomials have the potential for constructing $0, 1$-matrices with better recovery properties. That is in our construction, matrices satisfy RIP of bigger order $k$ as compared to the Devore’s matrices RIP of $k$.

4 Deterministic construction of CS matrices using multivariable homogeneous polynomials

In this section, we present our deterministic construction procedure that is based on multivariable homogeneous polynomials. To begin with, we consider homogeneous polynomials in two variables and later on we extend our methodology using homogeneous polynomials in $n$ variables. As in [12], we shall consider only the case when $F$ has prime order and hence is field of integers modulo $p$ ($\mathbb{Z}_p$). The results we prove can be established for other finite fields as well.

Given any integer $2 < r < p$, define $\mathcal{P}_r$, a set of all homogeneous polynomials in two variables of degree $r$ over $\mathbb{Z}_p$. Let $Q(x, y) \in \mathcal{P}_r$, can be represented as $Q(x, y) = \sum_{i+j=r} a_{ij} x^i y^j$, where the coefficients $a_{ij} \in \mathbb{Z}_p$, $m = p^{r+1} - 1$ such polynomials are there. For any $Q(x, y) \in \mathcal{P}_r$, which is a mapping from $\mathbb{Z}_p \times \mathbb{Z}_p$ to $\mathbb{Z}_p$. The graph of $Q(x, y)$ is $\mathcal{G}(Q) = \{(x, y, Q(x, y)) \mid (x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, $|\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p| = p^3 = n$.

We order the elements of $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ lexicographically as $(0, 0, 0), \ldots, (0, p-1, p-1), (1, 0, 0), \ldots, (p-1, p-1)$, for any $Q(x, y) \in \mathcal{P}_r$, denote $V_Q$ the vector indexed on $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ which takes value one at any ordered pair from
the Graph of $Q(x, y)$ and takes the value zero otherwise. There are exactly $p^2$
ones in $V_Q$.

Define the matrix $\Phi_0$ with columns $V_Q, Q(x, y) \in \mathcal{P}_r$, with these columns
order lexicographically with respect to the coefficients of the polynomials. Then
the size of the matrix is $n \times m$, that is $p^3 \times (p^{r+1} - 1)$.

The following theorem provides an upper bound on the no.of zeros of a homogeneous polynomial $Q \in \mathcal{P}_r$
in $F_q^n$.

**Theorem 4.1** [15] Let $f \in F_q[x_1, \ldots, x_j]$ be homogeneous polynomial with $deg(f) = r \geq 1$.
Then the equation $f(x_1, \ldots, x_j) = 0$ has at most $r(q^{j-1} - 1) + 1$ solutions
in $F_q^j$, where the $F_q$ is finite field of characteristic $p$, $q = p^i, i \in \mathbb{Z}^+$.

Using the afore stated upper bound, we prove that the matrix $\Phi$ so constructed
satisfies RIP, as detailed below:

**Theorem 4.2** The matrix $\Phi = \frac{1}{p} \Phi_0$ satisfies the RIP with $\delta_k = \frac{k-1(r(p-1)+1)}{p^2}$,
for any $k < \frac{p^2}{r(p-1)+1} + 1$.

**Proof:** Let $T$ be any subset of column indices with $|T| = k$ and $\Phi_T$ a submatrix
of $\Phi$, the columns of $\Phi_T$ are columns of $\Phi$ correspondingly to the indices in $T$,
that is $\Psi_T = \frac{1}{p}[V_{Q_1}, \ldots, V_{Q_k}]$, where $T = \{i_1, \ldots, i_k\}$ and $Q_{i_1}, \ldots, Q_{i_k} \in \mathcal{P}_r$.
The Grammian matrix $\Psi_T = \Phi_T^T \Phi_T$ has entries $\frac{1}{p^2} V_{Q_{i_j}}^T V_{Q_{i_l}}$, where $i_j, i_l \in T$.
The matrix $\Psi_T$ has all ones as its diagonal entries. Since for any $Q_{i_j}, Q_{i_l} \in \mathcal{P}_r$
with $Q_{i_j} \neq Q_{i_l}$ there are atmost $r(p - 1) + 1$ values of $\mathbb{Z}_p \times \mathbb{Z}_p$ such that
$Q_{i_j}(x, y) = Q_{i_l}(x, y)$.

Therefore any off-diagonal entry of $\Psi_T$ is $\leq \frac{r(p-1)+1}{p^2}$. It follows that sum of
off-diagonal entries of any row or column of $\Psi_T$ is $\leq \frac{k-1(r(p-1)+1)}{p^2} = \delta_k < 1$
everwhen $k < \frac{p^2}{r(p-1)+1} + 1$. The matrix $\Psi_T$ can be written as $\Psi_T = I + \Theta_T$,
$\|\Theta_T\|_X \leq \delta_k$, where $X = 1$ or $\infty$ norm. Since
$\|\Theta_T\|_2 \leq \sqrt{\|\Theta_T\|_1 \|\Theta_T\|_\infty} \leq \delta_k$.

We have $\|\Psi_T\|_2 = \|I + \Theta_T\|_2 \leq \|I\|_2 + \|\Theta_T\|_2 \leq 1 + \delta_k$.

Also $\|\Psi_T\|_2 = \|I + \Theta_T\|_2 \geq \|I\|_2 - \|\Theta_T\|_2 \geq 1 - \delta_k$.

Which implies $(1 - \delta_k) \leq \|\Psi_T\|_2 \leq (1 + \delta_k)$.

Hence $\Phi$ satisfies RIP of order $k$.

The asymptotic bonds on the $k$ is $n^\frac{7}{4} < k(n, m) < n^\frac{7}{2}$.

**Note 1**: The asymptotic upper bound of our matrix on $k$ is bigger than the
asymptotic upper bounds on Devore’s $k$. The coherence of our matrix is $\frac{r(p-1)+1}{p^2}$
which is smaller than the coherence of Devore’s matrix $\frac{r}{p}$, therefore it has the
better recovery properties. Since the sizes of two matrices are different, so it is no meaning to compare, even though our matrix has small coherence. The size of Devore’s matrix is \( p^2 \times p^{(r+1)} \) and our matrix is \( p^3 \times p^{(r+1)} - 1 \), therefore we constructed different sizes of RIP 0,1−matrices. Here the considering field is \( Z_p \), if we consider any finite field \( F_p, q = p^i, i \in Z^+ \) then sizes of Devore’s and our matrix is \( p^{2n} \times p^{n(r+1)}, p^{3n} \times p^{n(r+1)} - 1 \). Therefore we constructed different sizes of 0,1−RIP matrices compare to Devore’s matrices.

5 On constructing circulant RIP matrices:

This construction has been extended to deal with circulant matrices \( \Phi = (\phi_{ij}) \).

In a circulant matrix first few columns describe it completely, in view of the following relation

\[
\phi_{i+1, j+i} = \phi_{ij}.
\]

As in the previous theorem, our construction uses the vectors \( V_Q, Q(x,y) \in P_r \), to generate the first \( l \) columns. For choosing these \( l \) polynomials, we define an equivalence relation on \( P_r \). For \( P, Q \in P_r \),

\[
P \sim Q \text{ iff } 0 \neq \lambda \in Z_p \text{ such that } P(x, y) = \lambda Q(x, y), \forall (x,y) \in Z_p \times Z_p.
\]

Clearly this is an equivalence relation. Given \( P \in P_r, [P] = \{ \lambda^{-1}P | \lambda \neq 0 \in Z_p \} \), \( |[P]| = p - 1, |P_r| = p^{r+1} - 1 \). Therefore there are \( \frac{p^{r+1} - 1}{p-1} \) distinct equivalence classes in \( P_r \). Let \( \Gamma_r \) consist of a set of representations from each of the equivalence classes. The cardinality of \( \Gamma_r \) is \( \frac{p^{r+1} - 1}{p-1} \). The polynomials from \( \Gamma_r \) will represent the first \( l \) columns. Hence \( l = |\Gamma_r| \). Since \( n = p^3 \) and these \( l \) columns can be shifted in cyclic way as \( p^3 \) times. Therefore \( m = (\frac{p^{r+1} - 1}{p-1})p^3 = p^{r+3} + p^{r+2} + \ldots + p^1 \).

Now define the circulant matrix \( \Phi_0 \) of size \( n \times m \), whose first \( l \) columns are the \( V_Q, Q(x,y) \in \Gamma_r \), written in lexicographic order with respect to the coefficients of the polynomials. We can find ones in shifted columns the following way.

The first \( l \) columns in \( \Phi_0 \) are defined by using the polynomials in \( \Gamma_r \), the next block of \( l \) columns each is obtained by a cyclic shift. The size of the vector \( V_Q \) is \( p^3 \times 1 \), therefore there will be \( n = p^3 \) such blocks. Consider the \( i^{th} \)-block, \( 0 \leq i \leq n-1 \). We can write \( i = a + bp + cp^2 \), where \( a, b, c \in \{0, \ldots, n-1 \} \). Each column in this block will be cyclic shift of the corresponding column \( V_Q \) from the first block. Recall that we index the columns of \( \Phi_0 \) by \( (x, y, z) \in Z_p \times Z_p \times Z_p \).

The entry in the \((x, y, z)\) position of \( V_Q \) will now occupy the position \((x', y', z')\) in the \( i^{th} \)-block, where \( z' = z + i = z + a \, (mod \, p) \), \( y' = y + b \, or \, y + b + 1 \, (mod \, p) \), \( x' = x + c \, or \, x + c + 1 \, (mod \, p) \). Since the ones in \( V_Q \) occur precisely in the position \((x, y, Q(x,y))\), the new ones in the corresponding column of block \( i \) will occur in position \((x', y', z')\), where \( z' = Q(x, y) + a \, (mod \, p) \), \( y' = y + b \, or \, y + b + 1 \, (mod \, p) \), \( x' = x + c \, or \, x + c + 1 \, (mod \, p) \). The following lemma bounds the inner-product of any two columns of \( \Phi_0 \).
The following theorem provides an upper bound on the no. of zeros of a multivariable polynomial \( Q(x, y) \) in \( \mathbb{F}_q^2 \).

**Theorem 5.1:** [15] Let \( f \in \mathbb{F}_q[x_1, \ldots, x_n] \) be a polynomial with \( \text{deg}(f) = r \geq 1 \). Then the equation \( f(x_1, \ldots, x_n) = 0 \) has at most \( rq^{n-1} \) solutions in \( \mathbb{F}_q^n \), where the \( \mathbb{F}_q \) is finite field of characteristic \( p \), \( q = p^r, n \in \mathbb{Z}^+ \).

**Lemma 5.2:** Using above theorem, we derive bound on the inner product between any two different columns of the matrix \( \Phi_0 \) is \( |V.W| \leq 2^t \).

**Proof:** Let \( V \) and \( W \) be any to column of \( \Phi_0 \), then there exist \( Q, R \in \Gamma_r \) such that \( V \) and \( W \) are the cyclic shift of vectors \( V_Q, V_R \). As we have observed above, there are integers \( a_0, b_0, c_0 \) (depending only on \( V \)), such that any one in column \( V \) occurs at a position \( (x', y', z') \) iff \( z' = Q(x, y) + a_0 \pmod{p}, y' = y + b_0 + c_0 \pmod{p}, x' = x + c_0 + \epsilon_1 \pmod{p} \), with \( (x, y) \in Z_p \times Z_p, \epsilon_0, \epsilon_1 \in \{0, 1\} \). Similarly a one occurs in column \( W \) at position \( (x'', y'', z'') \) iff \( z'' = R(x, y) + a_1 \pmod{p}, y'' = y + b_1 + c_1 \pmod{p}, x'' = x + c_1 + \epsilon_1 \pmod{p} \), with \( (x, y) \in Z_p \times Z_p, \epsilon_0, \epsilon_1 \in \{0, 1\} \). The inner product \( V.W \) counts the number of row positions for which there is a one at common places of these two columns.

In other words, that is, \( (x', y', z') = (x'', y'', z'') \)

\[
x + c_0 + \epsilon_1 = x + c_1 + \epsilon_1, y + b_0 + \epsilon_0 = y + b_1 + \epsilon_0 \quad \text{and} \quad Q(x, y) + a_0 = R(x, y) + a_1.
\]

(9)

Case 1: Suppose \( Q \neq R \), we fix one of the \( 2^4 \) possibilities for \( \epsilon_0, \epsilon_0', \epsilon_1, \epsilon_1' \). (9) implies that \( \overline{x} = x + d, \overline{y} = y + e \) and \( R(x + d, y + e) = Q(x, y) + a \), where \( a = a_0 - a_1, d = c_0 + \epsilon_1 - c_1 - \epsilon_1' \). Since \( Q \neq R \) and \( Q, R \) are homogeneous imply that \( R(\overline{x} + (d, e)) \neq Q(\overline{x} + (d, e), \forall (x, y) \in Z_p \times Z_p \). In this case the only possible \( (x, y)'s \) which can satisfy (9) are zeros of \( R(\overline{x} + (d, e)) - Q(\overline{x}) - a \). It has at most \( rp \) roots. Since there are \( 2^4 \) possibilities for \( \epsilon_0, \epsilon_0', \epsilon_1, \epsilon_1' \). Hence \( |V.W| \leq 2^t \).

Case 2: Suppose \( Q = R, (9) \) implies that \( \overline{x} = x + d, \overline{y} = y + e \) and \( Q(x + d, y + e) = Q(x, y) + a \). Suppose \( Q(\overline{x} + (d, e)) \equiv Q(\overline{x}) + a \), which implies that \( Q \) is non-homogeneous. Which is contradiction. Hence \( Q(\overline{x} + (d, e)) - Q(\overline{x}) - a \) has at most \( rp \) roots. Which implies \( |V.W| \leq 2^t \).

**Theorem 5.3:** The cyclic matrix \( \Phi = \frac{1}{p} \Phi_0 \) has the RIP with \( \delta = 2^k(k - 1) \frac{\epsilon}{p} \) whenever \( k - 1 < \frac{\epsilon}{2p} \).

**Proof:** Proof is same as that of Theorem 2.2.

## 6 Generalization from two variables to \( n \) variables

In the above construction, we have used homogeneous polynomials in two variables over \( \mathbb{Z}_p \). This idea can, however, be extended to deal with homogeneous polynomials in \( n \) variables over \( \mathbb{Z}_p \). Given any integer \( 2 < r < p \), define \( \mathcal{P}_r \) to be set of all homogeneous polynomials in \( n \) variables of degree \( r \) over \( \mathbb{Z}_p \). Using the recursive formula one may easily find the cardinality \( f_n(r) \) of \( \mathcal{P}_r \).

**Recursive formula:** \( f_2(r) = r + 1, f_3(r) = \sum_{i=0}^{r} f_2(r - 1), f_4(r) = \sum_{i=0}^{r} f_3(r -
Deterministic construction of compressed sensing matrices using multivariable polynomials

1,...,f_n(r) = \sum_{i=0}^{r} f_{n-1}(r-1). In this calculation, we use the following formula also.

\[ \sum_{k=1}^{n} k(k+1)(k+2)\ldots(k+m) = \frac{n(n+1)(n+2)(n+m+1)}{m+2} \]

\( \text{Hint: } \left( \frac{m+k}{m+2} \right) - \left( \frac{m+k}{m+2} \right) \). The cardinality of \( P_r = p^{f_n(r)} - 1 = p^{(r+n-1)} - 1 \). If we construct the matrix \( \Phi_0 \) using these polynomials just as in the two variable case, the size of the matrix is \( p^{n+1} \times p^{(r+n-1)} - 1 \).

**Note 2:** The coherence of these matrices is \( \frac{r(p^{n-1}+1)}{p} \), which is smaller than the coherence of Devore’s matrix \( \frac{r}{p} \), therefore it has the better recovery properties. Since the sizes of two matrices are different, so it is no meaning to compare, even though our matrix has small coherence. Any how in the case of two variables only we will get the smaller coherence and as \( n \) increases the coherence of corresponding matrix increase and finally it touches the Devore’s matrix coherence. Finally different sizes on no of variables, we will get different sizes of 0,1−RIP matrices with better recovery properties.

**Theorem 6.1:** The matrix \( \Phi = \frac{1}{\sqrt{p}} \Phi_0 \) satisfies the RIP with \( \delta_k = k - 1 \left( \frac{r}{p} \right) p^{n-1} - 1 \), for any \( k < \frac{p^n}{(p^{n-1}+1)} + 1 \).

Proof: Proof is same as that of Theorem 2.2.

Using above all ideas, if we construct the circulant matrices \( \Phi \) with respect to homogeneous \( r^{th} \) degree polynomials in \( n \) variables, then it satisfies RIP.

**Theorem 6.2:** The cyclic matrix \( \Phi = \frac{1}{\sqrt{p}} \Phi_0 \) has the RIP with \( \delta = 2^{2n}(k-1) \frac{r}{p} \) whenever \( k - 1 < \frac{p^n}{2^{2n}r} \).

Proof: Proof is same as that of Theorem 2.2.

**References**


