1). A note on binary sensing matrices

2). Simple construction of Euler Squares using polynomials over finite field theory

Ramu Naidu R

IISc, SPC lab

July 16, 2016

Organization

- A note on binary sensing matrices
  - Basics of Compressed Sensing (CS)
  - On the solvability of P_0 problem
  - Conditions for equivalence between P_0 and P_1
  - Advantages with binary CS matrices and existing constructions
  - Motivation and objective
  - Extremal set theory for binary sensing matrices
- Part II: Simple construction of Euler Squares using polynomials over finite field theory
  - Euler Squares
  - Construction of Euler Squares
  - Example
- Part III: Conclusions and future work

Part I: A note on binary sensing matrices

A note on binary sensing matrices

Basics of Compressed Sensing

- A vector $x \in \mathbb{R}^M$ is $k-$**sparse** if it has k nonzero coordinates. That is, $\|x\|_0 := |\{i \mid x_i \neq 0\}| = k < M$
- One of the central problems in CS is that of reconstructing an unknown sparse vector $x \in \mathbb{R}^M$ from the linear measurements $y' = (\langle x, \phi_1 \rangle, \ldots, \langle x, \phi_M \rangle) \in \mathbb{R}^m$
- One can recover sparse x from its linear measurements by solving the following optimization problem:

$$P_0 : \min_x \|x\|_0 \text{ subject to } \quad \Phi x = y \qquad (1)$$

- This l_0-minimization problem is computationally not tractable[a] in general

[a] Simon Foucart and Holger Rauhut, "A Mathematical Introduction to Compressive Sensing," Birkhauser, Baseln, 2013.

A note on binary sensing matrices

On the solvability of P_0 problem

- There have been attempts to repose or solve P_0 problem via greedy and convex relaxation methods
- D.Donoho et.al.[a] posed an equivalent of this problem as

$$P_1 : \min_{x} \|x\|_1 \text{ subject to } \quad b = \Phi x \tag{2}$$

- Fast solvers are available
- The algorithms OMP, STOMP, WMP, MP, ROMP fall under greedy category. Among all, OMP is most popular algorithm

---

[a] S.S. Chen, D.L. Donoho, and M.A. Saunders, "Atomic Decomposition by Basis Pursuit," SIAM, 2001.

Sufficient conditions for equivalence between P_0 and P_1

- The general question of CS is: "when do both problems (1) and (2) admit same solution ?"

Definition

The mutual-coherence of a given matrix Φ is the largest absolute inner-product between different normalized columns of Φ. Denoting the k-th column in Φ by ϕ_k, the **mutual-coherence** is given by

$$\mu(\Phi) = \max_{1\leq\, i,j \leq\, m,\; i\neq j} \frac{|\, \phi_i^T \phi_j|}{\|\phi_i\|_2 \|\phi_j\|_2}. \tag{3}$$

A note on binary sensing matrices

- Terense Tao and Candes proposed an alternative approach establishing the stated equivalence

Definition

We say that a matrix Φ satisfies **Restricted Isometry Property (RIP)** of order k, if there is a $0 < \delta_k < 1$ such that

$$(1-\delta_k)\|z\|_{l_2} \leq \|\Phi_T z\|_{l_2} \leq (1+\delta_k)\|z\|_{l_2}, \quad z \in \mathcal{R}^k, \qquad (4)$$

holds for all T of cardinality k.

The following theorem [a] establishes the equivalence between P_0 and P_1 problems through RIP

[a] E. Candes, "The restricted isometry property and its implications for compressed sensing," Comptes Rendus Mathematique, 2008

A note on binary sensing matrices

Theorem

Suppose an $m \times M$ matrix Φ has the RIP of order $2k$ with constant $\delta_{2k} < \sqrt{2} - 1$, then P_0 and P_1 have same $k-$sparse solution if P_0 has a $k-$sparse solution.

- The following proposition relates the RIP constant δ_k and μ

Proposition

[a] *Suppose that $\Phi_1, \ldots, \Phi_M$ are the unit norm columns of the matrix Φ with coherence μ. Then Φ satisfies RIP of order k with constant $\delta_k = (k-1)\mu$.*

[a] M. Elad, "Sparse and redundant representations; from theory to applications in signal and image processing," Springer, Berlin, 2010.

A note on binary sensing matrices

Advantages with binary CS matrices

- Binary matrices being sparse and possessing $0, 1$ as elements provide multiplier-less and faster dimensionality reduction operation, which is not possible with their dense counterparts
- These matrices have smaller density than Gaussian matrices. Here, by density, one refers to the ratio of number of nonzero entries to the total number of entries of the matrix

Definition

A binary matrix Φ is said to have a (r, k)-structure, if every column of Φ contains k ones and the inner product between any two columns is at most r, that is the mutual coherence of Φ is at most $\frac{r}{k}$.

Existing deterministic constructions

- The first constructions of binary sensing matrices has been given by R. Devore [4][a]. The sizes of the constructed matrices are $p^2 \times p^{l+1}$ with coherence $\frac{l}{p}$. This construction has (l, p)-structure,for a prime power p and $1 < l < p$.
- S. Li. et. al. [5] have generalized the work in [4] and constructed the matrices of $|\mathcal{P}|q \times q^{\mathcal{L}(G)}$, where q is any prime power and $\mathcal{P}$ is the set of all rational points on algebraic curve $\mathcal{X}$ over finite field $\mathbb{F}_q$ and G is a divisor of $\mathcal{X}$ such that $deg(G) < |\mathcal{P}|$. This construction has $(deg(G), \mathcal{P})$-structure.

[a] Ronald A. DeVore, "Deterministic constructions of compressed sensing matrices," Journal of Complexity, Volume 23,pp 918-925, 2007.

Existing deterministic constructions

- The authors in [5][a] have constructed binary sensing matrices using Euler squares with size being $nk \times n^2$ and coherence $\frac{1}{k}$, where $n = p_1^{r_1} p_2^{r_2} \dots p_l^{r_l}$ and $k = \min\{p_1^{r_1}, p_2^{r_2}, \dots, p_l^{r_l}\} - 1$ with p_i is a prime for $1 \leq i \leq l$ and r_i is a positive integer.This construction has $(1, k)-$structure.
- The authors in [4][b] have constructed binary sensing matrices using finite geometry. These matrices possess $(1, q)$, $(1, q+1)$ and $(2, q+1)$-structure for a prime power q.

[a] R. Ramu Naidu, P. V. Jampana and C. S. Sastry, "Deterministic compressed sensing matrices: Construction via Euler Squares and applications," IEEE Transactions on Sig. Proc., vol. 64, no. 14, pp. 3566-3575, 2016.

[b] S. Li and G. Ge, "Deterministic construction of sparse sensing matrices via finite geometry," IEEE Trans. Signal Process., vol. 62, 2850-2859, 2014.

A note on binary sensing matrices

Motivation

- All the existing constructions have (r, k)-structure for particular family of numbers

Objective

- To construct **general size** (r, k)**-structure and sparse binary sensing matrices** which are useful for fast processing

- The sparse CS matrix may contribute to fast processing with low computational complexity in Compressed Sensing[a]

[a] A. Gilbert et. al., "Sparse recovery using sparse matrices," Proceedings of IEEE, 2010.

A note on binary sensing matrices

A. Extremal set theory for binary sensing matrices

Let r, k, m be positive integers such that $r < k < m$ and X an m element set, that is, $X = \{1, 2, \ldots, m\}$. Define $[X]^k = \{H \subseteq X, |H| = k\}$. Any subset $\mathcal{F}$ of $[X]^k$ is called a $k-$uniform family.

Definition

Any subset $\mathcal{F}_d(r, k, m)$ of $[X]^k$ is called $r-$dense if any $r-$element subset of X is contained in at least one member of $\mathcal{F}_d$.

Definition

Any subset $\mathcal{F}_s(r, k, m)$ of $[X]^k$ is called $r-$sparse if any $r-$element subset of X is contained in at most one member of $\mathcal{F}_s$, that is, $|F_i \cap F_j| \leq r - 1, \forall F_i, F_j \in \mathcal{F}_s$. Define $n(m, k, r)$ to be the maximum possible cardinality of $\mathcal{F}_s$.

A. Extremal set theory for binary sensing matrices

Definition

Any subset $\mathcal{F}_S(r,k,m)$ of $[X]^k$ is called a Steiner system if every $r-$element subset of X is belongs to exactly one member of $\mathcal{F}_S$

- Some of the necessary 'divisibility conditions' for the existence of Steiner systems are as follows:

$$\binom{k-i}{r-i} \text{ divides } \binom{m-i}{r-i} \textit{ for all } 0 \leq i \leq r-1.$$

- Clearly the Steiner system $\mathcal{F}_S(r,k,m)$ is a subset of $r-$sparse set $\mathcal{F}_s(r,k,m)$.

A. Extremal set theory for binary sensing matrices

The following proposition relates the $r-$sparse sets and binary sensing matrices which possess $(r-1, k)-$structure.

Proposition

There is a one-one correspondence between the set of all $r-$sparse $k-$uniform families and binary sensing matrices which possess $(r-1, k)-$structure.

Therefore using $r-$sparse sets, one can construct binary sensing matrices with coherence at most $\frac{r-1}{k}$.

Proposition

If $\mathcal{F}$ is an $r-$sparse family with cardinality M on an m element set X, then the incidence matrix $\Phi_{m\times M}$ of $\mathcal{F}$ has coherence $\frac{r-1}{k}$ and $\Phi = \frac{1}{\sqrt{k}}\Phi$ satisfies RIP with $\delta_{k'} = (k'-1)(\frac{r-1}{k})$ for any $k' < \frac{k}{r-1} + 1$.

Some examples of r-sparse sets

- The binary construction in [4], has $(r, p)-$structure with sizes being $p^2 \times p^{r+1}$. This construction is a $(r+1)-$sparse p uniform family on a set $X = \{1, 2, \ldots, p^2\}$.
- The construction in [5], has $(1, k)-$structure with sizes being $nk \times n^2$. This construction is a $2-$sparse k uniform family set on a set $X = \{1, 2, \ldots, nk\}$.
- The construction in [4], has fall in the $r-$sparse family of $\mathcal{F}_s(2, q, q^3)$, $\mathcal{F}_s(2, q+1, (q^3+1))$ and $\mathcal{F}_s(3, q+1, (q^2+))$.
- The Steiner system $\mathcal{F}_S(r, k, m)$ is fall in the $r-$sparse family of $\mathcal{F}_s(r, k, m)$.

Remark 1: The $r-$sparse family is the super class of all the existing binary constructions which have the $(r-1, k)-$structure.

A note on binary sensing matrices

Extremal set theory for binary sensing matrices

Proposition

[a] *If $\mathcal{F}_s \subseteq [X]^k$ and $\mathcal{F}_s$ is an $r-$sparse family, then*

$$|\mathcal{F}_s| \leq \frac{\binom{m}{r}}{\binom{k}{r}}. \tag{5}$$

[a] G. Katona, T. Nemetz and M. Simonovits, "On a graph-problem of Turan," Mat. Lapok, 15, 228-238, 1964.

- Therefore, the maximum possible column size of a binary sensing matrix which possess $(r-1,k)-$structure is at most $\frac{\binom{m}{r}}{\binom{k}{r}}$, where m is the row size, k is the number of ones each column contains and $r-1$ is the inner product between any two columns.

A note on binary sensing matrices

Extremal set theory for binary sensing matrices

In [3] Vojtech Rodl has proved the following theorem.

Theorem

$\lim_{m\to\infty} n(m,k,r)\frac{\binom{k}{r}}{\binom{m}{r}} = 1$, *for every pair* (r,k) *with* $r < k$.

- In the proof of the above theorem, using probabilistic methods, the author has constructed $r-$ sparse family $\mathcal{F}_s(r,k,m)$, for sufficiently large m and every fixed r, k with $r < k$.

Remark 2: For sufficiently large m, by using the Rodl construction one can generate $(r,k)-$structure binary sensing matrices with asymptotically optimal column size for any r and k with $r < k$.

A note on binary sensing matrices

Extremal set theory for binary sensing matrices

Theorem

[a] *For fixed r, k there exist $m_0(r, k)$ such that if $m > m_0(r, k)$ satisfies the divisibility condition then a Stenier system $\mathcal{F}_S(r, k, m)$ exists.*

[a] P. Keevash, "The existence of designs," arXiv preprint arXiv:1401.3665, 2014.

Therefore using his construction and from Proposition-9, we conclude the following theorem:

Theorem

For every pair of integers (r, k) with $r < k$ there exist a $(r, k)-$structure binary sensing matrix Φ with optimal column size.

Extremal set theory for binary sensing matrices

In the above theorem, row size m is some integer which satisfies the divisibility condition and the column size $M = \frac{\binom{m}{r}}{\binom{k}{r}}$.

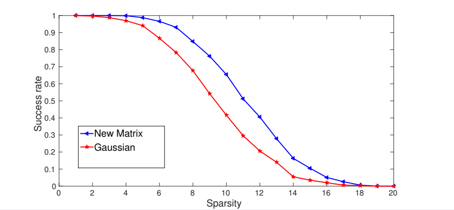

Figure : Comparison of the reconstruction performances of the synthesized matrices and Gaussian random matrices when the matrices are of size (a) 78×169 (top plot). These plot indicate that the matrices constructed from $r-$sparse sets show superior performance for some sparsity levels, while for other levels both matrices result in the same performance. The x and y axes in both plots refer respectively to the sparsity level and the success rate (in % terms).

Extremal set theory for binary sensing matrices

Figure : Original image

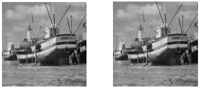

Figure : For the original image of size 256×256 in Figure 2, the image on the left is reconstructed via the matrix constructed from $r-$sparse sets and the right image is obtained via the corresponding Gaussian matrix with a down-sampling factor of two. This figure states that the constructed matrix provides competitive reconstruction performance.

Simple construction of Euler Squares using polynomials over finite field theory

Euler Squares

Definition

An Euler Square of order n, degree k and index n, k is a square array of $n^2, k-$ads, $(a_{ij1}, a_{ij2}, \ldots, a_{ijk})$, where $a_{ijr} = 1, 2, \ldots, n;\ r = 1, 2, \ldots, k;$ with $i, j = 1, 2, \ldots, n$ and $n > k$; $a_{ipr} \neq a_{iqr}$ and $a_{pjr} \neq a_{qjr}$ for $p \neq q$ and $(a_{ijr})(a_{ijs}) \neq (a_{pqr})(a_{pqs})$ for $i \neq p$ and $j \neq q$.

Harris F. MacNeish [a] has constructed Euler Squares by using group theoretical results for the following cases:

[a] H. F. MacNeish, "Euler squares," Ann. Math., 1922.

Simple construction of Euler Squares using polynomials over finite field theory

Construction of Euler Squares

- Index $p, p-1$, where p is a prime number, more generally Index $p^r, p^r - 1$, for a prime p
- Index n, k, where $n = 2^r p_1^{r_1} p_2^{r_2} \ldots, p_l^{r_l}$ for distinct odd primes $p_1, p_2, \ldots, p_l$ and $k = \min\{2^r, p_1^{r_1}, p_2^{r_2}, \ldots, p_l^{r_l}\} - 1$
- In the present work, we give a simpler construction of Euler Squares using polynomials over finite fields
- Let us first construct Euler Square of index p, k, where p is a prime or prime power
- Consider the polynomials of degree at most one over a finite field $\mathbb{F}_p = \{f_1 = 0, f_2 \ldots, f_p\}$ of order p. For sake of simplicity of notation in the later part, let us denote $f_i = i$ to form an order among the elements of $\mathbb{F}_p$.

Simple construction of Euler Squares using polynomials over finite field theory

Construction of Euler Squares

- Let us denote the set of polynomials of degree at most one as $D_1^p = \{P_{ij}^1 = f_i x + f_j : i, j = 1, \ldots, ..., p\}$
- There are p^2 number of polynomials of degree at most one, that is cardinality of D_1^p is p^2
- Form a $k-$tuple $S_{k_p} = (f_2, ..., f_{k+1})$, for $1 \leq k \leq p-1$
- Evaluating a polynomial P_{ij}^1 of D_1^p at every point of S_{k_p}, we form an ordered $k-$tuple $P_{ij}^1(S_{k_p}) = (P_{ij}^1(f_2), \ldots, P_{ij}^1(f_{k+1})) \in \mathbb{F}_p^k$
- Let us denote $S_{k_p}^1 = \{P_{ij}^1(S_{k_p}) : i, j = 1, \ldots, p\} \subseteq \mathbb{F}_p^k$. Now $|S_{k_p}^1| = p^2$.

Simple construction of Euler Squares using polynomials over finite field theory

Construction of Euler Squares

- **Claim:** $S^1_{k_p}$ forms an Euler Square of index p, k.
- **Proof:** To show, $S^1_{k_p} = \{P^1_{ij}(S_{k_p}) = (P^1_{ij}(f_2), \ldots, P^1_{ij}(f_{k+1}) : i, j = 1, \ldots, p\}$ forms an Euler Square of index p, k, we need to show that, for $q, s = 2, \ldots, k+1$, $P^1_{in}(f_q) \neq P^1_{im}(f_q)$ and $P^1_{nj}(f_q) \neq P^1_{mj}(f_q)$ for $n \neq m$ and $P^1_{ij}(f_q)P^1_{ij}(f_s) \neq P^1_{nm}(f_q)P^1_{nm}(f_s)$ for $i \neq n$ and $j \neq m$.
- **Case 1:**For $n \neq m$, $P^1_{in} = f_i x + f_n$ and $P^1_{im} = f_i x + f_m$ doesn't have any common root and that shows that $P^1_{in}(f_q) \neq P^1_{im}(f_q)$.
- **Case 2:** For $n \neq m$, $P^1_{nj} = f_n x + f_j$ and $P^1_{mj} = f_m x + f_j$ have one common root at $f_1 = 0$ and that shows that $P^1_{nj}(f_r) \neq P^1_{mj}(f_r)$, as $1 \neq r$.

Construction of Euler Squares

- **Case 3:** For $i \neq n$ and $j \neq m$, P_{ij}^1 and P_{nm}^1 can have at most one common root and that shows that $P_{ij}^1(f_q)P_{ij}^1(f_s) \neq P_{nm}^1(f_q)P_{nm}^1(f_s)$.
- Therefore, using polynomials of degree at most one, we are able to construct an Euler Square of index p, k for p being prime or prime power and $k \leq p-1$.
- **Example:** To construct Euler Square of index $3, 2$, we consider field $F_3 = \mathbb{Z}_3 = \{0, 1, 2\}$.
- Then the set $D_3^1 = \{P_{ij}^1 : i, j = 0, 1, 2\}$ consist of all polynomials of degree at most one over $\mathbb{Z}_3$.
- Note that $|D_3^1| = 9$. Let us fix $S_{2_3} = (1, 2)$ as ordered $2-$tuple.

Construction of Euler Squares

- Evaluating every polynomial of D_3^1 at every point of S_{2_3}, we get the set $S_{2_3}^1 = \{(0,0),(1,2),(2,1);(1,1),(2,0),(0,2);(2,2),(0,1),(1,0)\} \subseteq \mathbb{Z}_3^2$.
- Now it is easy to check that $S_{2_3}^1$ forms an Euler Square of index $3,2$ after denoting $0=1, 1=2$ and $2=3$.

Part III: Conclusions and Future Work

Conclusions and Future Work

- So far the objectives behind my work have centered around constructing binary sensing matrices
- I am now interested in constructing more general matrices, through Majorization and minimization methods
- In our present work we present a simple construction to generate Euler Square using polynomials of degree at most one over finite field
- Further we want to generalize our construction idea to define Generalized Euler Squares (GES) and construct them using higher degree polynomials over finite field
- As an application, compressed sensing matrices can be generate from Generalized Euler Squares

References

- A. Amini and F. Marvasti, "Deterministic construction of binary, bipolar and binary compressed sensing matrices," IEEE Trans. Inf. Theory, vol. 57, pp. 2360-2370, 2011.
- P. Indyk, "Explicit constructions for compressed sensing matrices," in Proc. 19th Annu. ACM-SIAM Symp. Discr. Algorithms, pp. 30-33, 2008.
- D. Donoho, "Compressed Sensing," IEEE Trans. Information Theory, 52, pp 1289-1306, 2006.
- Ronald A. DeVore, "Deterministic constructions of compressed sensing matrices," Journal of Complexity, Volume 23,pp 918-925, 2007.
- S. Li, F. Gao, G. Ge, and S. Zhang, Deterministic construction of compressed sensing matrices via algebraic curves, Information Theory, IEEE Transactions on, vol. 58, no. 8, pp. 5035-5041, 2012.

References

- E. Candes and T. Tao, "Decoding by linear programming," IEEE Trans. Inform. Theory 51, 415-424, 2005.
- Baraniuk.R, Davenport.M, De Vore.R, and Wakin.M, "A Simple Proof of the Restricted Isometry Property for Random Matrices," Constructive Approximation, 28(3),253-263, 2008.
- S. Foucart and H. Rauhut, "A mathematical introduction to compressive sensing," Birkhauser, Baseln, 2013.
- P. Keevash, "The existence of designs," arXiv preprint arXiv:1401.3665, 2014.
- J. L. Nelson, and Vladimir N. Temlyakov, "On the size of incoherent systems," Journal of Approximation Theory, 163(9),1238-1245, (2011).
- M. Elad, "Sparse and redundant representations; from theory to applications in signal and image processing," Springer, Berlin, 2010.

References

- A. Gilbert and P. Indyk, "Sparse recovery using sparse matrices," Proceedings of the IEEE, vol. 98, no. 6, pp. 937-947, 2010.
- H. F. MacNeish, "Euler squares," Ann. Math., vol. 23, pp. 221-227, 1922.
- Pradip Sasmal, R. Ramu Naidu, C. S.Sastry and P. V. Jamapana, "Composition of binary compressed sensing matrices," To be appear in IEEE Signal Processing Letters, 2016.
- S. Li and G. Ge, "Deterministic construction of sparse sensing matrices via finite geometry," IEEE Trans. Signal Process., vol. 62, 2850-2859, 2014.

References

- J. Bourgain, S. Dilworth, K. Ford, S. Konyagin and D. Kutzarova, "Explicit constructions of RIP matrices and related problems," Duke Math. J. 159, 145-185, 2011.
- G. Katona, T. Nemetz and M. Simonovits, "On a graph-problem of Turan," Mat. Lapok, 15, 228-238, 1964.
- Vojtech Rodl, "On a packing and covering problem," European journal of combinatorics, 5, 69-78, 1985.
- Calderbank Robert and Jafarpour Sina, "Reed Muller Sensing Matrices and the LASSO," Lecture Notes in Computer Science, SETA, 442-463, 2010.
- R. Ramu Naidu, P. V. Jampana and C. S. Sastry, "Deterministic compressed sensing matrices: Construction via Euler Squares and applications," IEEE Transactions on Sig. Proc., vol. 64, no. 14, pp. 3566-3575, 2016.

Thank you