Complex-valued Deterministic Matrices with Low Coherence based on Algebraic Geometric Codes

Hamidreza Abin and Arash Amini
Advanced Communications Research Institute (ACRI)
Sharif University of Technology, Tehran, Iran
Email: hamidreza.abin@gmail.com, aamini@sharif.ir

***Abstract*—In this work, we introduce new algebraic geometry (AG) curves that can generate extremely fat matrices with low coherence. The previous application of AG codes in matrix design has been limited to binary matrices. Here, we devise a different approach to achieve $m \times n$ complex-valued matrices. As $n > m^2$ in our matrices, the Welch bound is no longer achievable; however, the coherence of our matrices surpass the Welch bound only by a $\mathcal{O}(\log m)$ factor. Moreover, our construction provides flexibility in setting the number of rows and columns.**

I. Background

For a measurement matrix $\mathbf{\Phi}_{m\times n}$, the coherence value $\mu(\mathbf{\Phi})$ is defined as

$$\mu(\mathbf{\Phi}) := \max_{1\leq i\neq j\leq n} \frac{\big|\langle \boldsymbol{\phi}_i, \boldsymbol{\phi}_j\rangle\big|}{\|\boldsymbol{\phi}_i\|_2\,\|\boldsymbol{\phi}_j\|_2}, \tag{1}$$

where $\boldsymbol{\phi}_i$ stands for the ith column of the matrix. For $m \leq n$, we know from Welch bound that $\mu(\mathbf{\Phi}) \geq \sqrt{\frac{n-m}{m(n-1)}}$. Further, the equality is not achievable for $n > m^2$ [1].

Explicit construction of fat matrices with low coherence has been an active field of research in the past years. The introduced designs usually arise from structures in algebra or combinatorics: in [2] polynomials of certain degrees are used to construct binary measurements matrices. The same technique has been applied to finite geometry and algebraic codes in [3], [4], [5]. Various types of error correcting codes has been considered for matrix construction; the list includes BCH codes [6], [7], Reed-Muller codes [8], Reed-Solomon codes [9]. Expander graphs are also useful in error correcting codes and measurement matrix design [10]. Recently, designs in combinatorics have become popular tools for matrix design [11], [12].

II. Preliminaries

Let p be an integer prime and let χ be an algebraic curve with genus g_χ defined by the polynomial $\varphi(x,y)$ over the finite field $\mathbb{F}_{p^\alpha}$ (assuming $\alpha\in\mathbb{N}$). If N_χ denotes the number of roots of $\varphi(x,y)$ in $(\mathbb{F}_{p^\alpha})^2$ (point on χ), the Hasse-Weil-Serre bound implies that [13]

$$|N_\chi - p^\alpha - 1| \leq g_\chi \lfloor 2p^{\alpha/2}\rfloor.$$

For a proper divisor G_χ of χ and distinct roots $r_1, r_2, \dots, r_s \in (\mathbb{F}_{p^\alpha})^2$ of $\varphi(x,y)$, the range of the linear mapping $\mathcal{T}: \mathcal{L}(G) \to (\mathbb{F}_{p^\alpha})^s$ defined by

$$\mathcal{T}(f) = \big(f(r_1), f(r_2), \dots, f(r_s)\big), \quad f\in\mathcal{L}(G),$$

forms a linear code that is known as the algebraic geometry code $C(r_1,\dots,r_s : G)$ [13], [14]. Here, $\mathcal{L}(G)$ stands for the Riemann-Roch space associated with G. If s, e and d represent the length, dimension (uncoded length) and minimum distance of this code, respectively, we know that [13]

$$e \geq \deg(G) - g + 1 \quad \text{and} \quad d \geq s - deg(G). \tag{2}$$

III. Main Result

We denote the infinity point of χ by R_∞. If we set $G = \beta R_\infty$ for arbitrary integer β, and apply the element-wise trace mapping on $C(r_1,\dots,r_s{:}\beta R_\infty)$, we obtain a new code $\widetilde{C}(r_1,\dots,r_s{:}\beta R_\infty) \subset (\mathbb{F}_p)^s$ with parameters $(s, \tilde{e}, \tilde{d})$.

Lemma 1. *For the code $\widetilde{C}(p_1,\dots,p_s{:}\beta P_\infty)\subset(\mathbb{F}_p)^s$ we have that*

$$e \leq \tilde{e} \leq \alpha\, e \quad , \quad \tilde{d} \geq s - \tfrac{p^\alpha + 1 + A\lfloor 2p^{\alpha/2}\rfloor}{p}, \tag{3}$$

where $A = p\, g_\chi + \frac{1}{2}(p-1)(\beta-1)$.

To construct the sensing matrix, let $\{\tilde{\mathbf{c}}_j\}_{j=1}^{p^{\tilde{e}-1}} \subset (\mathbb{F}_p)^s$ with $\tilde{\mathbf{c}}_j = (c_{1,j},\dots,c_{s,j})$ be all code-words in $\widetilde{C}(r_1,\dots,r_s{:}\beta R_\infty)$ such that $c_{1,j}=0$. By mapping the elements of $\mathbb{F}_p$ to the integers $\{0,1,\dots,p-1\}$, we form the sensing matrix as

$$\mathbf{\Phi}_{s\times p^{\tilde{e}-1}} = \tfrac{1}{\sqrt{s}}\Big[\mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{i,j}}\Big]_{\substack{1\leq i\leq s\\ 1\leq j\leq p^{\tilde{e}-1}}}. \tag{4}$$

Theorem 1. *Given $\max\big\{2g_\chi - 1\,,\, \log_p n + g_\chi + 1\big\} \leq \beta < s$, the coherence of the above matrix can be bound by*

$$\mu\big(\mathbf{\Phi}_{s\times p^{\tilde{e}-1}}\big) \leq \frac{p^{\alpha+1} + p + pA\lfloor 2p^{\alpha/2}\rfloor - ps}{2s}.$$

For maximal curves with $s = p^\alpha + g_\chi\lfloor 2p^{\alpha/2}\rfloor$, Theorem 1 could be simplified as $\mu(\mathbf{\Phi}) \lessapprox \frac{\beta + 2g_\chi - 1}{2} p^{-\frac{\alpha-4}{2}}$.

As an example of the above technique, we can obtain a $(3^\alpha + 2.3^{\alpha/2}) \times 3^{2\alpha+2}$ matrix with

$$\mu(\mathbf{\Phi}) \leq \frac{3 + 3^{\alpha/2}(12\alpha + 24)}{2(3^\alpha + 3^{\alpha/2+1})}$$

by considering $\varphi(x,y) = y^2 - x^3 - 2x - 1$ over $\mathbb{F}_3$.

References

[1] T. Strohmer and R. W. Heath, "Grassmannian frames with applications to coding and communication,"*Appl. and Comp. Harm. Anal.*, vol. 14, no. 3, pp. 257-275, May 2003.

[2] R. A. DeVore, "Deterministic constructions of compressed sensing matrices,"*J. of Complexity*, vol. 23, no. 4-6, pp. 918–925, Aug.-Dec. 2007.

[3] S. Li, F. Gao, G. Ge and S. Zhang, "Deterministic construction of compressed sensing matrices via algebraic curves,"*IEEE Trans Inform. Theory*, vol. 58, no. 8, pp. 5035–5041, 2012.

[4] S. Li and G. Ge, "Deterministic construction of sparse sensing matrices via finite geometry,"*IEEE Trans. Sig. Proc.*, vol. 62, no. 11, pp. 2850–2859, Jun. 2014.

[5] H. Chen, "Explicit RIP matrices in compressed sensing from algebraic geometry,"*arXiv:1505.07490v1*, 2015.

[6] A. Amini and F. Marvasti, "Deterministic construction of binary, bipolar and ternary compressed sensing matrices,"*IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 2360–2370, Apr. 2011.

[7] A. Amini, V. Montazerhodjat and F. Marvasti, "Matrices with small coherence using p-ary block codes,"*IEEE Trans. Sig. Proc.*, vol. 60, no. 1, pp. 172–181, Jan. 2012.

[8] S. Howard, R. Calderbank and S. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes,"*Conf. on Info. Sciences and Systems (CISS)*, Princeton, New Jersey, 2008.

[9] M. Mohades, M. A. Mohades and A. Tadaion, "A Reed-Solomon code based measurement matrix with small coherence,"*IEEE Sig. Proc. Letters*, vol. 21, no. 7, pp. 839–843, 2014.

[10] S. Jafarpour, W. Xu, B. Hassibi and R. Calderbank, "Efficient and robust compressed sensing using optimized expander graphs", *IEEE Trans. Inform. Theory*, vol. 55, no.9, pp. 4299–4308, 2009.

[11] R. R. Naidu, P. Jampana and C. S. Sastry, "Deterministic compressed sensing matrices: Construction via Euler squares and applications,"*IEEE Trans. Sig. Proc.*, vol. 64, no. 14, pp. 3566–3575, 2015.

[12] A. Amini, H. Baghsheikhi and F. Marvasti, "From Paley graphs to deterministic sensing matrices with real-valued Gramians," *SAMPTA 2015*, Washington, USA, May 2015.

[13] H. Niederreiter, C. Xing and,"Algebraic Geometry in Coding Theory and Cryptography ,"*Princeton University Press*, New Jersey 2009.

[14] N. S. Harald and L. San,"Advances in algebraic geometry codes ,"*World Scientific*, New Jersey 2008