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 $O(\log m)$ factor. Moreover, our construction provides flexibility in setting the number of rows and columns.

I. BACKGROUND

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

$$\mu(\Phi) := \max_{1 \leq i \neq j \leq n} \frac{|\langle \phi_i, \phi_j \rangle|}{\|\phi_i\|_2 \|\phi_j\|_2},$$

where $\phi_i$ stands for the $i$th column of the matrix. For $m \leq n$, we know from Welch bound that $\mu(\Phi) \geq \sqrt{\frac{n-m}{m(n-1)}}$. 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 $\chi$ be an algebraic curve with genus $g_x$ defined by the polynomial $\varphi(x, y)$ over the finite field $\mathbb{F}_p$. If $N_x$ denotes the number of roots of $\varphi(x, y)$ in $\mathbb{F}_p$, the inequality implies that [13]

$$|N_x - p^{\alpha} - 1| \leq g_x |2p^{\alpha/2}|.$$

For a proper divisor $G$, of $\chi$ and distinct roots $r_1, r_2, \ldots, r_s \in \mathbb{F}_p$, the range of the linear mapping $T : \mathcal{L}(G) \rightarrow \mathbb{F}_p^s$ defined by

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

forms a linear code that is known as the algebraic geometry code $C(r_1, \ldots, r_s : G)$ [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]

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

III. MAIN RESULT

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

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

$$e \leq \tilde{e} \leq \alpha e, \quad \tilde{d} \geq s - \frac{p^{\alpha+1} + A |2p^{\alpha/2}|}{p},$$

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

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

$$\Phi_{s \times p^{d-1}} = \frac{1}{\sqrt{s}} \left[ e^{\beta c_{1,j}} \right]_{1 \leq j \leq s}^{1 \leq i \leq p^{d-1}}.$$  (4)

Theorem 1. Given $\max \{2y, \log_p n + g_x + 1\} \leq \beta < s$, the coherence of the above matrix can be bounded by

$$\mu(\Phi_{s \times p^{d-1}}) \leq \frac{p^{\alpha+1} + p + pA |2p^{\alpha/2}| - ps}{2s}.$$

For maximal curves with $s = p^\alpha + g_x |2p^{\alpha/2}|$, Theorem 1 could be simplified as $\mu(\Phi) \leq \frac{p^\alpha + g_x |2p^{\alpha/2}|}{2s}$. As an example of the above technique, we can obtain a $(3\alpha + 2.3^\alpha) \times 3^{2\alpha+2}$ matrix with

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

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

---

RELIMINARIES

II. P

1, f

\[\phi(x,y)\]
REFERENCES


