Explicit Matrices with Low Coherence Based on Algebraic Geometric Codes

Hamidreza Abin, Farzad Shahrivari and Arash Amini

Advanced Communication Research Institute (ACRI)
Department of Electrical Engineering
Sharif University of Technology, Tehran, Iran
E-mail: aamini@sharif.edu

Abstract

A key element in the performance of a compressed sensing (CS) setup is the so called sensing matrix. It is known that the success of CS-based methods strongly rely on the properties of the employed sensing matrix. Random matrices are the widely-adopted choice due to their order-optimal performance and flexibility in size. In real world applications, however, random structures are rarely feasible. For this reason, the deterministic design of sensing matrices has been an ongoing research topic. In this paper, we introduce new classes of deterministic complex-valued sensing matrices based on algebraic curves. In particular, we design a number of algebraic-geometric codes with large minimum distances specifically for the construction of sensing matrices. Our approach is to find maximal curves in the Galois field $\mathbb{F}_{p^{\widetilde{m}}}$, and transform them into $\mathbb{F}_p$ codes by a trace map. Invoking the Riemann-Roch theorem, we demonstrate that the resulting code has a large minimum distance compared to its length, which leads to a sensing matrix with small coherence value. For general $m \times n$ matrices, the Welch bound ($\approx \frac{1}{\sqrt{m}}$) sets a universal lower-bound on the coherence value, and the bound is achievable only when $n \leq m^2$. In our designs, we are able to construct $m \times n$ matrices with n ranging from around $8m$ to values larger than $\mathcal{O}(m^2)$ by tuning the parameters. Meanwhile, the coherence of the designed matrices differ from the Welch bound by only an $\mathcal{O}(\log m)$ factor. Simulation results indicate that the performance of our matrices in recovering sparse vectors from compressed

measurements is superior or equivalent to Gaussian random matrices.

Keywords: Algebraic-geometric code, coherence, compressed sensing, Galois field, trace mapping.

---

1. Introduction

Compressed sensing is a technique for reconstructing sparse signals from their projections onto low-dimensional subspaces [1, 2, 3, 4]. The result of the projections is widely regarded as linear samples/measurements of the original vector. Mathematically, if the sparse signal is represented via $\mathbf{x} \in \mathbb{R}^N$ that has at most k non-zero elements, the result of the projection/sampling process is found by $\mathbf{y} = \mathbf{\Phi x}$, where $\mathbf{\Phi}$ has m rows ($m < N$) and is called the measurement/sensing matrix. There are several methods proposed for recovering $\mathbf{x}$ from $\mathbf{y}$; the two main factors that determine the success of a recovery method are the sparsity level of the original vector and the low-dimensional subspaces generated by the columns of the sensing matrix. A widely studied property of the sensing matrix known as the Restricted Isometry Property (RIP) [5] implies that for every k-sparse vector $\mathbf{x} \in \mathbb{R}^N$,

$$(1 - \delta_k)\|\mathbf{x}\|_2^2 \leq \|\mathbf{\Phi} x\|_2^2 \leq (1 + \delta_k)\|\mathbf{x}\|_2^2.$$

It is known that the RIP of order $2k$ with small enough constant δ_{2k} provides a sufficient condition for stable recovery of all k-sparse vectors $\mathbf{x}$ even when measurements are noisy [6]. Random $m \times n$ matrices with various probability laws such as Gaussian and Bernoulli satisfy such RIP orders with high probability given that $m \gtrapprox \mathcal{O}\big(k \log(n/k)\big)$ [6]. Partial Fourier matrices obtained by random row selection from the DFT matrix are another class of matrices that satisfy RIP with high probability [6]. The story for deterministic matrices is completely different: verifying that a given matrix satisfies an RIP order is computationally NP-hard [7].

The coherence of an $m \times N$ matrix $\mathbf{\Phi}$ is defined as

$$\mu_{\mathbf{\Phi}} := \max_{1 \leq i \neq j \leq N} \frac{|< \boldsymbol{\phi}_i, \boldsymbol{\phi}_j >|}{\|\boldsymbol{\phi}_i\|_2 \cdot \|\boldsymbol{\phi}_j\|_2},$$

where $\boldsymbol{\phi}_i$ denotes the ith column of $\boldsymbol{\Phi}$. As the definition suggests, computing the coherence value of an $m \times N$ matrix requires $\mathcal{O}(mN^2)$ operations. Besides, a matrix with unit-norm columns that has a coherence value $\mu_{\boldsymbol{\Phi}}$ satisfies RIP of order k with constant δ_k as long as $\mu_{\boldsymbol{\Phi}}(k-1) \leq \delta_k < 1$ [6]. Therefore, it is desirable to design matrices with small coherence values. The well-known Welch bound introduces a universal lower bound on the coherence value: for any $m \times N$ matrix $\boldsymbol{\Phi}$ with $m \leq N$ we have that

$$\mu_{\boldsymbol{\Phi}} \geq \sqrt{\frac{N-m}{m(N-1)}}.$$

In addition, the equality is not achievable for $N > m^2$ [8]. One of the consequences of this bound is that sparse recovery guarantees based on the coherence value of the matrix are limited to $k \leq \mathcal{O}\big(\sqrt{m}\big)$ which is much more limiting than the RIP guarantees of random matrices. This fact is commonly referred to as the square-root bottleneck[1].

Even with the above limitation, minimizing the coherence value is the most common technique in deterministic design of sensing matrices. Indeed, the explicit construction of fat matrices with small coherence is an active field of research. The considered constrcutions mainly arise from structures in algebra or combinatorics. DeVore was among the pioneers of deterministic matrix design; in [11] he introduced an explicit construction of binary matrices based on polynomials of a given degree in a finite field. The same technique was later applied to finite geometry and algebraic codes in [12, 13, 14]. Various types of error correcting codes were considered in matrix design; the list includes BCH codes [15], [16], Reed-Muller codes [17], Reed-Solomon codes [18], Delsarte-Goethals codes [19], Kerdock codes [19] and LDPC codes [20]. Authors in [21] used specific linear and nonlinear to construct a family of deterministic measurement matrix. Many designs based on chirp signals are also studied [22, 10]. Partial Fourier submatrices are also popular due to efficient matrix multiplication techniques

[1] There are few deterministic constructions which marginally break the square-root bottleneck, but with orders that are not considerably better than $k \leq \mathcal{O}\big(\sqrt{m}\big)$ [9, 10].

[23]. Expander graphs are also useful in error correcting codes and measurement matrix design [24]. Recently, designs in combinatorics have become popular for matrix design [25, 26, 27, 28]. Binary measurement matrix design using unitary geometry was proposed in [29].A deterministic construction of sparse sensing matrices based on vector spaces over finite fields was provided in [30] . Authors in [31] provide a flexible construction of measurement matrices with low storage space and low coherence. Sequences with low correlation are used to design low coherence measurement matrix in [32]. Deterministic design of toeplitz matrices with small coherence based on Weyl sums are proposed in [33].

1.1. Road-map

In this paper, we follow the approach of [16] to construct a sensing matrix based on an error correcting code. More specifically, we need to design a linear p-ary code that includes the all-one codeword. Next, we partition the codewords into subsets of size p using a specific rule. Finally, we pick a vector from each subset (the choice is arbitrary) and apply an element-wise complex exponentiation to generate the columns of the overall sensing matrix. Using a result in [16], we can bound the coherence value of the resulting matrix in terms of the minimum distance of the code. To guarantee small coherence values, we need to have codes with minimum distances comparable to their block size. This is indeed a very restricting requirement on the code. In this work, we initially design an algebraic geometry code with a guaranteed minimum distance provided by the Riemann-Roch theorem. Unfortunately, the guaranteed minimum distance is not large enough to result in a matrix with small coherence. Here, we apply a trace mapping which increases the minimum distance by reducing the number of codewords. Fortunately, the remaining codewords are enough to form a fat sensing matrix suitable for compressed sensing purposes.

1.2. Outline

In Section 2, we review the basics of algebraic curves, rational points, Reimann-Roch space and extension curves. Further, we introduce algebraic geometry

codes and the trace of a code. In Section 3, we present our general technique to design codes with guaranteed minimum distances (Theorem 1–2). We follow the code design by the construction of the sensing matrix. Examples of algebraic curves and codes that are produced by our technique are studied in Section 3.1; the list includes curves of genus zero, elliptic curves, and norm-trace curves (including Hermitian curves). With numerical simulations, we evaluate the performance of our proposed matrices and compare them against Gaussian random matrices and an existing but different type of deterministic matrices based on algebraic curves in Section 4.

2. Preliminaries

Let $\mathcal{X}$ be an algebraic curve associated with a bivariate polynomial $\phi(x, y)$ over $\mathbb{F}_q$ and denote the genus of the curve by g. The degree of a point $P \in \mathcal{X}$ is said to be r if $P \in \left(\mathbb{F}_{q^r}\right)^2$. In particular, $P \in \mathcal{X}$ is called rational if $r = 1$.

For an algebraic curve $\mathcal{X}$, the function field $\mathbb{F}_q(\mathcal{X})$ on curve $\mathcal{X}$ is defined as the set of all bivariate rational functions (polynomial divided by polynomial) with coefficients in $\mathbb{F}_q$ such that the input domain is restricted to $\mathcal{X}$. For each $P \in \mathcal{X}$ and $f \in \mathbb{F}_q(\mathcal{X})$, the valuation $\nu_P(f)$ is defined as the multiplicity of point P as a root of f: if P is a zero of f with multiplicity $r \in \mathbb{N}$, then, $\nu_P(f) = r$. Similarly, if P is a pole of f with multiplicity $r \in \mathbb{N}$, then, $\nu_P(f) = -r$. When P is neither a zero nor a pole of f, then, $\nu_P(f) = 0$.

A divisor G of $\mathcal{X}$ is defined as $G = \sum_{P \in \mathcal{X}} n_P P$ where n_p is an integer number and only finite number of n_P are nonzero. The support and degree of a divisor G are defined respectively by $\mathrm{supp}(G) = \{P \in \mathcal{X} | n_P \neq 0\}$ and $\deg(G) = \sum_{P \in \mathcal{X}} n_P \deg(P)$. For a given divisor, the the Riemann-Roch space $\mathcal{L}(G)$ is defined as

$$\mathcal{L}(G) = \Big\{ f \in \mathbb{F}_q(\mathcal{X}) \;\Big|\; n_P + \nu_P(f) \geq 0 \Big\}. \tag{1}$$

$\mathcal{L}(G)$ is a finite dimensional vector space over $\mathbb{F}_q$ with dimension $\ell(G)$. According to the Riemann-Roch Theorem [34], $\ell(G) \geq \deg(G) + 1 - g$ and equality holds when $\deg(G) \geq 2g - 1$.

Let $P_1, P_2, \cdots P_{\widetilde{n}} \in \mathcal{X}$ be some of the rational points on curve $\mathcal{X}$ and set $D = P_1 + P_2 + \cdots + P_{\widetilde{n}}$. Choose $G \in \mathrm{Div}(\mathcal{X})$ such that $\mathrm{supp}(G) \subseteq \mathcal{X} \setminus \{P_1, \ldots, P_{\widetilde{n}}\}$. Next, we consider the evaluation map $\mathcal{T} : \mathcal{L}(G) \to (\mathbb{F}_q)^{\widetilde{n}}$:

$$\mathcal{T}(f) = \big(f(P_1), f(P_2), \cdots f(P_{\widetilde{n}})\big),\ f \in \mathcal{L}(G). \tag{2}$$

The range of this map forms a linear code known as the algebraic geometry (AG) code $\mathcal{C}(D, G)$ (in the rest of the paper, we simply write $\mathcal{C}$). If $\widetilde{n}, \widetilde{k}, d_{\min}$ represent the length, the dimension (alternatively, the uncoded length) and the minimum distance of this code, respectively, we have that [34]

$$\widetilde{k} = \ell(G) \geq \deg(G) - g + 1 \text{ and } d_{\min} \geq \widetilde{n} - \deg(G). \tag{3}$$

We define the trace operator $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ as the linear functional

$$\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = (\alpha) + (\alpha)^q + (\alpha)^{q^2} + \cdots + (\alpha)^{q^{r-1}}. \tag{4}$$

Let $\mathcal{C}$ be a code over the field $\mathbb{F}_{q^r}$ with parameters $[\widetilde{n}, \widetilde{k}, d_{\min}]$. We define the trace of $\mathcal{C}$ by applying the trace mapping in (4) to the code-words in an element-wise fashion:

$$\mathrm{Tr}(\mathcal{C}) = \Big\{ \big(\mathrm{Tr}(a_1), ..., \mathrm{Tr}(a_{\widetilde{n}})\big),\ \ \forall (a_1, ..., a_{\widetilde{n}}) \in \mathcal{C} \Big\},$$

where $\mathrm{Tr}(.) := \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(.)$. Oftentimes, the number of code-words in $\mathrm{Tr}(\mathcal{C})$ is less than in $\mathcal{C}$, because some of the code-words of $\mathcal{C}$ are mapped into the same code-word via Tr. The following theorem shows a connection between the dimension of a code and its trace.

Theorem 1 ([35]). *For any code $\mathcal{C}$ over the field $\mathbb{F}_{q^{\widetilde{m}}}$ with parameters $[\widetilde{n}, \widetilde{k}, d_{\min}]$, we have*

$$\widetilde{k} \leq \dim\big(\mathrm{Tr}(\mathcal{C})\big) \leq \widetilde{m} \times \widetilde{k}. \tag{5}$$

2.1. Matrix Design

So far, we explained the code structure using algebraic geometry curves. Our last step is to transform codes into deterministic compressed sensing matrices.

Design 1. Suppose $\mathcal{C}$ is a linear code over $\mathbb{F}_p$ with parameters $[\widetilde{n}, \widetilde{k}, d_{\min}]$ which contains the all-one code-word. We define the following equivalence relation:

$$a, b \in \mathcal{C}: \quad a \equiv b \;\Leftrightarrow\; \exists\, i \in \mathbb{F}_p: \; a - b = (i, i, ..., i). \tag{6}$$

From each of the $p^{\widetilde{k}-1}$ equivalence classes, we choose a code-word (arbitrary choice) such as $(c_{1,l}, \ldots, c_{\widetilde{n},l})$ (l represents the index of the equivalence class) and exponentiate it as

$$\left(\mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{1,l}}, \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{2,l}}, \cdots, \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{\widetilde{n},l}}\right). \tag{7}$$

Then, we normalize the code-words as vertical vectors and concatenate them to form the final matrix $\mathbf{\Phi}$:

$$\mathbf{\Phi} = \frac{1}{\sqrt{\widetilde{n}}} \begin{bmatrix} \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{1,1}} & \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{1,2}} & \ldots & \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{1,p^{\widetilde{k}}-1}} \\ \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{2,1}} & \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{2,2}} & \ldots & \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{2,p^{\widetilde{k}}-1}} \\ \vdots & \vdots & \vdots & \\ \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{\widetilde{n},1}} & \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{\widetilde{n},2}} & \ldots & \mathrm{e}^{\mathrm{j}\frac{2\pi}{p}c_{\widetilde{n},p^{\widetilde{k}}-1}} \end{bmatrix}. \tag{8}$$

In the following theorem, we present a general bound for the coherence of the constructed matrix based on code parameters.

Theorem 2. [16] *The coherence of matrix* $\mathbf{\Phi}$ *is bounded as*

$$\mu_{\mathbf{\Phi}} \leq \frac{p(p-1)\widetilde{n} - p^2 d_{min}}{2\widetilde{n}}. \tag{9}$$

Based on Theorem 2, for the coherence bound to become small, we need to have $p(p-1)\widetilde{n} \approx p^2 d_{\min}$, or equivalently, $d_{\min} \approx \frac{p-1}{p}\widetilde{n}$. This implies that the minimum distance of the code needs to be very large (comparable to the block length), which is not the case for the known code structures.

3. Main Contribution

As mentioned earlier, our goal in this paper is to construct matrices with small coherence. Our approach is to construct codes with large minimum distances first.

Theorem 3. *Let $\mathcal{X}$ be an algebraic curve of genus g over the finite field $\mathbb{F}_{p^{\widetilde{m}}}$, and let $P_1, P_2, \ldots, P_{\widetilde{n}} \in \mathcal{X}$. Further, let $D = P_1 + P_2 + \cdots + P_{\widetilde{n}}$, $G = rP_\infty$, and $\mathcal{C}(D,G)$ be the corresponding algebraic geometry code. Now, for the minimum distance of the code $\mathrm{Tr}\big(\mathcal{C}(D,G)\big)$, we have that*

$$d_{\min}\Big(\mathrm{Tr}\big(\mathcal{C}(D,G)\big)\Big) \geq \widetilde{n} - \frac{p^{\widetilde{m}} + 1 + g_\alpha \lfloor 2p^{\widetilde{m}/2} \rfloor}{p}, \tag{10}$$

where

$$g_\alpha = pg + \frac{(p-1)(r-1)}{2}. \tag{11}$$

The special case of Theorem 3 for genus zero curves was already studied in [35]. To facilitate reading of the paper, we have postponed the proof to Appendix C.

Theorem 4. *Let $\mathrm{Tr}\big(\mathcal{C}(D,G)\big)$ be the code introduced in Theorem 3 with the extra assumption that $r \geq 2g-1$. If we construct matrix $\mathbf{\Phi}$ via Design 1 based on the code $\mathrm{Tr}\big(\mathcal{C}(D,G)\big)$, then, $\mathbf{\Phi}$ has at least p^{r-g} columns and*

$$\mu(\mathbf{\Phi}) \leq \frac{p^{\widetilde{m}+1} + p + pg_\alpha \cdot \lfloor 2p^{\widetilde{m}/2} \rfloor - p\widetilde{n}}{2\widetilde{n}}. \tag{12}$$

Proof. Since $\deg(G) = r \geq 2g-1$, Riemann-Roch Theorem implies that

$$\widetilde{k} = \ell(G) = r - g + 1,$$

where $\widetilde{k}$ stands for the dimension of the AG code $\mathcal{C}(D,G)$. On one hand, Theorem 1 shows that the dimension of the code $\mathrm{Tr}\big(\mathcal{C}(D,G)\big)$ is at least $\widetilde{k}$. On the other hand, the matrix $\mathbf{\Phi}$ constructed in Design 1 has p^{k-1} columns, where k is the dimension of the employed code. Hence, $\mathbf{\Phi}$ has at least $p^{\widetilde{k}-1} = p^{r-g}$ columns.

To prove the coherence bound, we invoke Theorem 2 by using the bound in Theorem 3 for $d_{\min}$:

$$\begin{aligned}\mu(\mathbf{\Phi}) &\leq \frac{p(p-1)\widetilde{n} - p^2 d_{\min}}{2\widetilde{n}} \leq \frac{p(p-1)\widetilde{n} - p^2\big(\widetilde{n} - \frac{p^{\widetilde{m}}+1+g_\alpha\lfloor 2p^{\widetilde{m}/2}\rfloor}{p}\big)}{2\widetilde{n}} \\ &= \frac{p^{\widetilde{m}+1} + p + pg_\alpha \lfloor 2p^{\widetilde{m}/2} \rfloor - p\widetilde{n}}{2\widetilde{n}}. \end{aligned} \tag{13}$$

□

Remark 1. *If*

$$r > \max\big(2g-1\,,\,\widetilde{m}+g+\log_p(11)\big), \tag{14}$$

then, the matrix $\mathbf{\Phi}$ *in Theorem 4 is guaranteed to be a fat matrix. In fact, the Serre bound in Appendix A implies that*

$$\widetilde{n} \le p^{\widetilde{m}} + g\lfloor 2p^{\widetilde{m}/2}\rfloor. \tag{15}$$

It is now not difficult to check that

$$\begin{aligned} p^{\widetilde{m}} + g\lfloor 2p^{\widetilde{m}/2}\rfloor &\le p^{\widetilde{m}} + 2gp^{\widetilde{m}/2} < \max(2^{g-1}\,,\,11p^{\widetilde{m}}) \\ &\le \max(p^{g-1}\,,\,11p^{\widetilde{m}}) = p^{\max(g-1\,,\,\widetilde{m}+\log_p(11))}. \end{aligned}$$

This proves that

$$p^{r-g} > p^{\widetilde{m}} + g\lfloor 2p^{\widetilde{m}/2}\rfloor,$$

if r *satisfies* (14).

We should highlight that the use of algebraic curves for deterministic construction of sensing matrices was previously investigated in [12, 14, 21]. However, the structure and type of the resulting matrices are very different from those introduced in this work. In particular, the previously studied matrices were binary-valued (0–1), while in this work, we introduce complex-valued matrices with no zero elements that provide more flexibility in selection of their sizes.

3.1. Examples

In Theorem 3, we presented a general result regarding algebraic curves that could be used to construct compressed sensing matrices. In this section, we apply this result to particular classes of algebraic curves and construct a number of families of deterministic matrices.

Genus Zero Curves

Example 1. Let $\phi(x, y) = x - y + 1$. The associated curve has $p^{2\widetilde{m}}$ roots of the form $(a, a + 1)$ in $\mathbb{F}_{p^{2\widetilde{m}}} \times \mathbb{F}_{p^{2\widetilde{m}}}$ (we use $2\widetilde{m}$ instead of $\widetilde{m}$, to avoid $\sqrt{p^{\widetilde{m}}}$ in the following expressions). We denote these points by $P_1, \ldots, P_{p^{2\widetilde{m}}}$. We also represent the point at infinity of the projective curve by $P_\infty = [1, 1, 0]$. As $\phi(x, y)$ is a linear polynomial, the associated curve $\mathcal{X}$ has $g = 0$.

For $G = rP_\infty$ with $r \in \mathbb{N}$ (later we use $r > 2\widetilde{m}$), it is easy to see that $\mathcal{L}(G)$ consists solely of polynomials (the rational functions cannot have non-trivial denominators) with degrees no more than r. According to Riemann-Roch Theorem, $\ell(G) = \dim\big(\mathcal{L}(G)\big) = r + 1$. Indeed, one can verify that $\{1, x, x^2, \ldots, x^r\}$ forms a basis for $\mathcal{L}(G)$. Now, if we define $D = P_1 + \cdots + P_{p^{2\widetilde{m}}}$ and follow the aforementioned procedure to generate matrix $\mathbf{\Phi}$, we will obtain a $p^{2\widetilde{m}} \times p^t$ matrix with $t \geq r$ that satisfies

$$\mu_{\mathbf{\Phi}} \leq \frac{1 + p^{\widetilde{m}}(p-1)(r-1)}{2p^{2\widetilde{m}-1}}. \tag{16}$$

For $r > 2\widetilde{m}$ the matrix is guaranteed to be fat. For large values of $r, \widetilde{m}$, the Welch bound μ_{Welch} for this matrix size is roughly equal to $\frac{1}{p^{\widetilde{m}}}$. This shows that the upper-bound on the coherence of the above matrix is worse than the Welch bound by a $\mathcal{O}(p^2 r)$ factor. However, we should mention that for $r > 4\widetilde{m}$, the Welch bound is not achievable by any matrix. By increasing r in the above construction, the number of columns in the matrix increases exponentially, while the coherence bound increases linearly.

Elliptic Curves

The general family of elliptic curves is defined by bivariate polynomials that are of degree 2 in terms of one variable and degree 3 in terms of the other variable. Below, we consider two examples of this family.

Example 2. Let $\phi(x, y) = y^2 + y - x^3 - x$ be the generating polynomial of the elliptic curve defined over fields with characteristic $p = 2$. This polynomial is irreducible and non-singular. Further, the genus of the resulting curve is given

by $g = 1$. The number $N_{\widetilde{m}}(\mathcal{X})$ of (x, y) roots of $\phi(x, y)$ in $\mathbb{F}_{2^{\widetilde{m}}} \times \mathbb{F}_{2^{\widetilde{m}}}$ is known to be [34]

$$N_{\widetilde{m}}(\mathcal{X}) = 2^{\widetilde{m}} - 2^{\frac{\widetilde{m}}{2}+1} \cos\left(\tfrac{3}{4}\pi\, \widetilde{m}\right). \tag{17}$$

Similar to the previous example, we use all the above points for the code construction, i.e., $\widetilde{n} = N_{\widetilde{m}}(\mathcal{X})$. The point at infinity of this curve is $P_\infty = [0, 1, 0]$. For $G = rP_\infty$ with $r \in \mathbb{N}$ (we use $r > \widetilde{m} + 4$), the Riemann-Roch space $\mathcal{L}(G)$ is formed by

$$\text{span}\Big\{x^i y^j \,\Big|\, 0 \leqslant i,\ 0 \leqslant j \leqslant 1,\ 2i + 3j \leqslant r\Big\}, \tag{18}$$

where $\{x^i y^j\}_{i,j}$ with $2i + 3j \leqslant r$ acts as a basis for this space. Riemann-Roch Theorem implies that $\ell(G) = \dim\big(\mathcal{L}(G)\big) = r$. Hence, the associated matrix $\mathbf{\Phi}$ shall have $\widetilde{n} = N_{\widetilde{m}}(\mathcal{X})$ rows and at least 2^{r-1} columns. The coherence of this matrix could be bounded via

$$\mu(\mathbf{\Phi}) \leq \frac{(2^{\widetilde{m}} + 1 - \widetilde{n}) + \frac{r+3}{2}\lfloor 2^{\frac{\widetilde{m}}{2}+1} \rfloor}{\widetilde{n}}. \tag{19}$$

As a special case, if $\widetilde{m} \equiv 2, 6 \pmod 8$, then,

$$\mu(\mathbf{\Phi}) \leq \frac{1 + 2^{\frac{\widetilde{m}}{2}}(r+3)}{2^{\widetilde{m}} + 1} \approx \frac{r+3}{2^{\frac{\widetilde{m}}{2}}}. \tag{20}$$

Finally, we set $r > \widetilde{m} + 4$ based on Remark 1 to guarantee that $\mathbf{\Phi}$ is a fat matrix. We should highlight that due to the construction based on $\mathbb{F}_2$, the resulting matrix is real-valued with $\pm\frac{1}{\sqrt{\widetilde{n}}}$ elements.

Example 3. The elliptic curve associated with $\phi(x, y) = y^2 - x^3 - 2x - 1$ is known to be maximal over $\mathbb{F}_3$. Similar to all elliptic curves, the genus of the resulting curve is $g = 1$. The number $N_{\widetilde{m}}(\mathcal{X})$ of roots of $\phi(x, y)$ in $\mathbb{F}_{3^{\widetilde{m}}} \times \mathbb{F}_{3^{\widetilde{m}}}$ is given by [34]

$$N_{\widetilde{m}}(\mathcal{X}) = 3^{\widetilde{m}} - 2 \times 3^{\widetilde{m}/2} \cos(\tfrac{5\pi}{6}\widetilde{m}). \tag{21}$$

It turns out that for $\widetilde{m} \equiv 6 \pmod{12}$, the curve is maximal. For the code construction, we use all the points on the curve ($\widetilde{n} = N_{\widetilde{m}}(\mathcal{X})$) and set $G = rP_\infty$ with $r \in \mathbb{N}$ (we use $r > \widetilde{m}+3$), where $P_\infty = [0, 1, 0]$ is again the point at infinity of the curve. The Riemann-Roch space $\mathcal{L}(G)$ is formed by

$$\text{span}\Big\{x^i y^j | 0 \leqslant i,\ 0 \leqslant j \leqslant 1,\ 2i + 3j \leqslant r\Big\}. \tag{22}$$

Since $\ell(G) = \dim\big(\mathcal{L}(G)\big) = r$, the resulting sensing matrix $\mathbf{\Phi}$ shall have $\widetilde{n} = N_{\widetilde{m}}(\mathcal{X})$ rows and at least 3^{r-1} columns. The coherence of this matrix could be bounded via

$$\mu(\mathbf{\Phi}) \leq \frac{3}{2}\frac{(3^{\widetilde{m}}+1-\widetilde{n})+(r+2)\lfloor 2\times 3^{\frac{\widetilde{m}}{2}}\rfloor}{\widetilde{n}}. \tag{23}$$

For the maximal curve of $\widetilde{m} \equiv 6 \pmod{12}$, this bound simplifies to

$$\mu(\mathbf{\Phi}) \leq 3\frac{1+3^{\frac{\widetilde{m}}{2}}(r+3)}{3^{\widetilde{m}}+2\times 3^{\frac{\widetilde{m}}{2}}} \approx \frac{3(r+3)}{3^{\frac{\widetilde{m}}{2}}}. \tag{24}$$

The condition $r > \widetilde{m}+3$ guarantees that $\mathbf{\Phi}$ is a fat matrix (Remark 1). Unlike the previous example regarding elliptic curves, the elements of this matrix are complex-valued.

Hermitian Curves

Example 4. The Hermitian curves is an algebraic curve with generating polynomial $\phi(x,y) = y^p + y - x^{p+1}$ over $\mathbb{F}_{p^2}$. This curve has $g = \frac{p^2-p}{2}$ and p^3 rational points. As the number of rational points matches the Serre's upper-bound, this curve is called maximal. The number of roots of $\phi(x,y)$ in $\mathbb{F}_{p^{2\widetilde{m}}} \times \mathbb{F}_{p^{2\widetilde{m}}}$ is known to be $N_{2\widetilde{m}} = p^{2\widetilde{m}} + p^{\widetilde{m}+2} - p^{\widetilde{m}+1}$ (for $\widetilde{m} = 1$, we have $N_1 = p^3$) [36]. Interestingly, $N_{2\widetilde{m}}$ also matches the Serre's upper-bound. We base our code construction in the field $\mathbb{F}_{p^{2\widetilde{m}}}$ rather than $\mathbb{F}_{p^2}$; for this purpose, we use all the $N_{2\widetilde{m}}$ points on the curve and set $G = rP_\infty$ where $P_\infty = [0,1,0]$ is the point at infinity of the curve and $r \in \mathbb{N}$ is such that

$$r > \max\big(p^2-p-1\,,\, 2\widetilde{m}+\tfrac{p^2-p}{2}+4\big).$$

The corresponding Riemann-Roch space $\mathcal{L}(G)$ is formed by

$$\operatorname{span}\Big\{x^i y^j | 0 \leqslant i,\ 0 \leqslant j \leqslant p-1,\ ip+j(p+1) \leqslant r\Big\}. \tag{25}$$

The resulting sensing matrix has $N_{2\widetilde{m}} = p^{2\widetilde{m}} + p^{\widetilde{m}+2} - p^{\widetilde{m}+1}$ rows and at least p^{r-g} columns. The coherence of this matrix satisfies

$$\mu_{\mathbf{\Phi}} \leq \frac{p^3+(p-1)(r-1)-p^2+p^{-\widetilde{m}-1}}{2(p^{\widetilde{m}-1}+p-1)} \approx \frac{p^2(p^2+r)}{2p^{\widetilde{m}}}. \tag{26}$$

Table 1: Matrix Design 3

Curve	Field Size	Matrix Size	Coherence Bound	welch Bound
$x-y+1$	$p^{2\bar{m}}$	$p^{2\bar{m}} \times 2^t\ ,\ t \geq \widetilde{r}$	$\frac{1+p^{\bar{m}}(p-1)(r-1)}{2p^{2\bar{m}-1}}$	$\approx p^{-\bar{m}}$
y^2+y-x^3-x	$2^{\bar{m}}\ ,\ \widetilde{m} \overset{8}{\equiv} 4$	$\left(2^{\bar{m}}+2^{\bar{m}/2+1}\right) \times 2^{r-1}\ ,\ r \geq \widetilde{m}+3$	$\frac{r \times 2^{\bar{m}/2}+1}{2^{\bar{m}}+2^{\bar{m}/2+1}}$	$\approx 2^{-\bar{m}/2}$
y^2-x^3-ax-b	$p^{\bar{m}}$	$\left(p^{\bar{m}}-2p^{\frac{\bar{m}}{2}}\cos\left(\widetilde{m}\theta\right)\right) \times p^{r-1}\ ,\ r:\text{eq (14)}$	$\approx \frac{p(pr+2\cos(\widetilde{m}\theta))}{2(p^{\frac{\bar{m}}{2}}-\cos(\widetilde{m}\theta))}$	$\approx p^{-\bar{m}/2}$
y^p+y-x^{p+1}	$p^{2\bar{m}}\ ,\ \widetilde{m} \overset{2}{\equiv} 0\ ,\ \widetilde{m} < g/2$	$\left(p^{2\bar{m}}+p^{\bar{m}+2}-p^{\bar{m}}\right) \times p^g$	$\approx \frac{2p^2(p^2-p)}{p^{\bar{m}}+2g}$	$\approx p^{-\bar{m}}$

4. Simulation Results

In this section, we numerically examine the performance of some of the matrices based on the algebraic geometry codes in recovering sparse vectors using MATLAB.

In each experiment, we first construct deterministic and random sensing matrices of size $m \times n$. Then, we generate random k-sparse vectors $\mathbf{x}$ of dimension n; the support of the vector (non-zero locations) is chosen randomly among $\binom{n}{k}$ possibilities with equal probability. The value of non-zero elements are also determined by i.i.d. realizations of a standard normal distribution. Next, we compute $\mathbf{y}_{m\times 1} = \mathbf{\Phi}_{m\times n}\mathbf{x}_{n\times 1}$ for each sensing matrix $\mathbf{\Phi}$, and try to recover $\mathbf{x}_{n\times 1}$ from $\mathbf{y}_{m\times 1}$. We employ both LASSO and OMP as the recovery methods to achieve an estimate $\widehat{\mathbf{x}}_{n\times 1}$ of $\mathbf{x}_{n\times 1}$; we use the Lagrangian form of the LASSO

$$\widehat{\mathbf{x}}_{n\times 1} = \underset{\mathbf{z}_{n\times 1}}{\operatorname{argmin}}\ \|\mathbf{y}-\mathbf{\Phi}\mathbf{z}\|_2^2 + \lambda\|\mathbf{z}\|_1, \tag{27}$$

where λ is numerically optimized to yield the best solution. If the reconstruction SNR defined as

$$\text{SNR}_{\text{rec}} = 20 \times \log\left(\frac{\|\mathbf{x}\|_2}{\|\mathbf{x}-\widehat{\mathbf{x}}\|_2}\right) \tag{28}$$

exceeds 100dB, we consider the recovery procedure as successful. For each value of k, we repeat this procedure 8000 times (random generation of $\mathbf{x}$ followed by the recovery procedure), and evaluate the percentage of perfect recovery. By varying the value of k, we can obtain the curve of the perfect recovery percentage in terms of k (obviously, as k increases, this percentage decreases).

Gaussian ensembles are the most-studied choices of sensing matrices in the literature. Therefore, in each experiment, we compare the recovery percentage curve of the AGC-based deterministic matrix with that of a Gaussian ensemble of the same size. Whenever possible, we also include other deterministic designs in our comparisons. The main challenge in comparing deterministic matrices is the restriction on the available matrix sizes; on one hand, it is often very difficult to find matching matrices in terms of the number of rows and columns (equal or almost equal number of rows and columns). On the other hand, when the size of two deterministic sensing matrices do not match, it is not clear whether the difference in their performance reflects the size mismatch or superiority/inferiority of the design technique.

For constructing the AGC-based sensing matrices, we use Galois fields with $p = 2, 3, 5$. As explained earlier, $p = 2$ results in real-valued (bipolar) matrices, while $p > 2$ leads to complex-valued matrices. To make the comparisons fair, we use the same structure for the Gaussian ensemble; *i.e.*, we consider real-valued random Gaussian matrices when $p = 2$, and complex-valued random Gaussian matrices when $p > 2$.

In our first experiment, we consider the genus zero curve introduced in Example 1. We set $p = 2$, $\widetilde{m} = 2$ and $r = 5$ to achieve a bipolar sensing matrix of the size 16×32. Figure 1 shows the performance of this matrix compared to the real-valued Gaussian random matrix of the same size. The recovery in this experiment is via the OMP method. We observe that the performance of this bipolar matrix is superior to the Gaussian ensemble.

To study complex-valued matrices, we set $p = 3$, $\widetilde{m} = 4$ and $r = 5$ for the same genus zero curve (Example 1). The resulting matrix is of size 81×243. In Figures 2 and 3 we plot the recovery percentage of this matrix using LASSO and OMP recovery methods, respectively. While both curves confirm superiority of the deterministic matrix (compared to the Gaussian ensemble), it is counter-intuitive that OMP works better than LASSO for both the deterministic and random matrices.

For comparing our matrices with previous constructions using algebraic

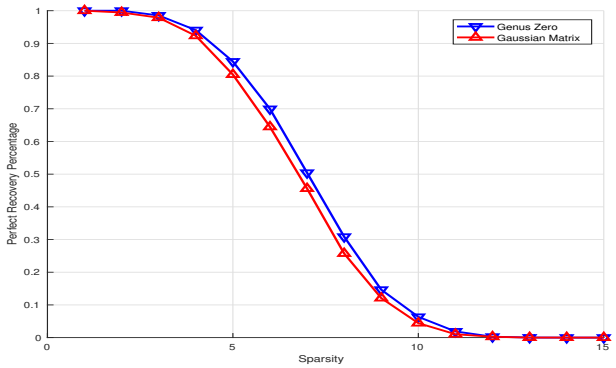


Figure 1: Perfect recovery percentage of a bipolar AGC-based matrix with $g = 0$ and size 16×32, as well as a random (real-valued) Gaussian matrix of the same size. The recovery method is OMP.

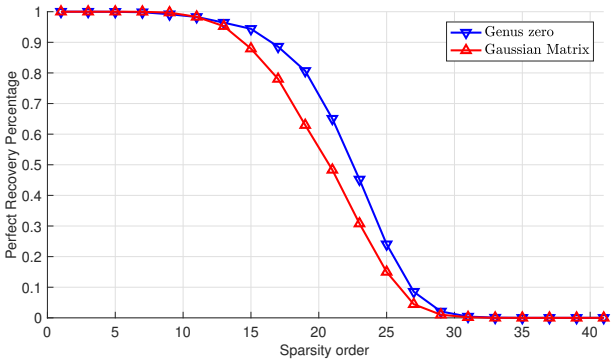


Figure 2: Perfect recovery percentage of a complex-valued AGC-based matrix with $g = 0$ and size 81×243, as well as a random (complex-valued) Gaussian matrix of the same size. The recovery method is LASSO.

curves, we focus on the binary matrices in [12]. With this binary design and using the elliptic curve in Example 2 ($\phi(x, y) = y^2 + y - x^3 - x$), we can construct $(|\rho| \times p^{\widetilde{m}}) \times p^{r\widetilde{m}}$ matrices where $|\rho|$ is the number of selected points on the curve. We set $p = 2$, $\widetilde{m} = 4$, $r = 2$ and $|\rho| = 4$ to achieve a 0/1-valued matrix of size 64×256; similarly, we set $p = 2$, $\widetilde{m} = 6$ and $r = 9$ in our design to obtain a bipolar (± 1-valued) matrix of the same size. We also include a similar size Gaussian random matrix in our comparison. The curves in Figure 4 are

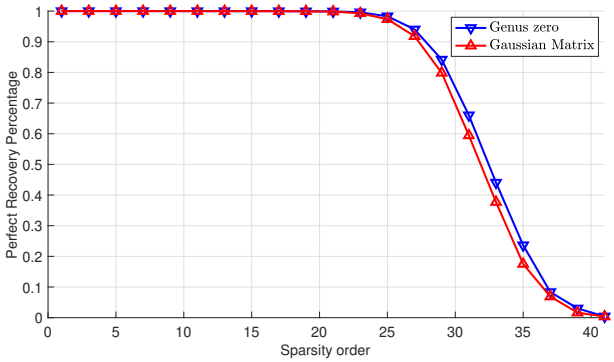


Figure 3: Perfect recovery percentage of a complex-valued AGC-based matrix with $g = 0$ and size 81×243, as well as a random (complex-valued) Gaussian matrix of the same size. The recovery method is OMP.

achieved by the LASSO method. The results reveal that the Gaussian random matrix in this setting slightly outperforms the proposed bipolar matrix, while both matrices perform substantially better than the binary matrix in [12]. The elliptic curve $\phi(x, y) = y^2 - x^3 - x - 2$ is maximal over $\mathbb{F}_{5^3}$. With this curve and by setting $\widetilde{m} = 3$ and $r = 5$, we obtain a 147×625 complex-valued matrix. The recovery curve of this matrix shown in Figure 5 using the LASSO method demonstrates significant improvement compared to the Gaussian random matrix of the same size. We further employ this matrix for recovering an image from low-dimensional linear projections using the OMP algorithm. For this purpose, we divide the 225×225-pixel image I of the Baboon (Figure 6-(a)) into 81 non-overlapping sub-images $I_{i,j} = I(25(i-1)+1, 25(j-1)+1),\ 1 \leq i, j \leq 9$ with size 25×25. Since images are often sparse in the DCT domain, we take the DCT of each $I_{i,j}$ and keep 8% of the largest entries to obtain $\widetilde{I}_{i,j}$ (sparsifying the images). Next, we reshape $\widetilde{I}_{i,j}$ to a column vector $\mathbf{v}_{i,j}$. Finally, we compute $\mathbf{u}_{i,j} = \mathbf{\Phi}_{147\times 625} \times \mathbf{v}_{i,j}$ and try to recovery $\mathbf{v}_{i,j}$ form $\mathbf{u}_{i,j}$ via the OMP algorithm. We repeat the same scenario by using a Gaussian ensemble instead of the designed sensing matrix. Figure 6 shows the results.

As a representative of Hermitian curves, we consider Example 4 with $p = 3$

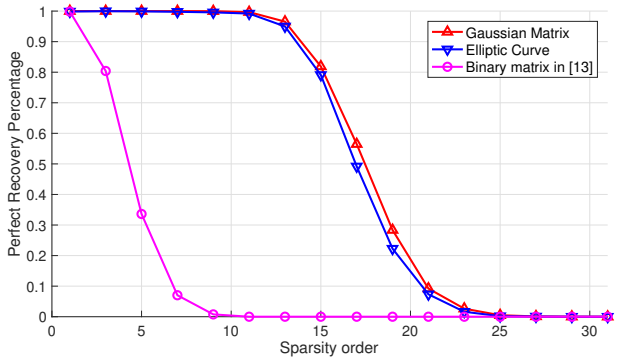


Figure 4: Perfect recovery percentage of binary ([12]) and bipolar (proposed matrices) matrices of size 64×256 formed by the elliptic curve $y^2 + y - x^3 - x$. The results also include the random Gaussian matrix of the same size, and are achieved by the LASSO method.

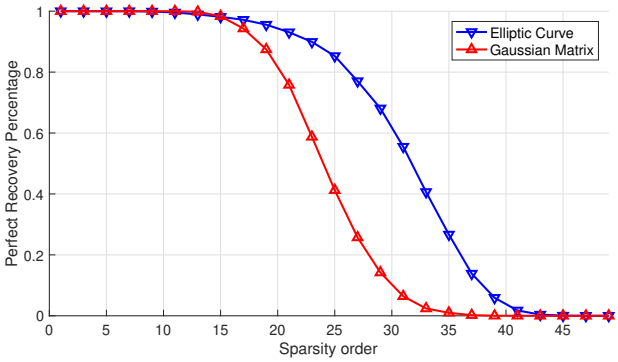
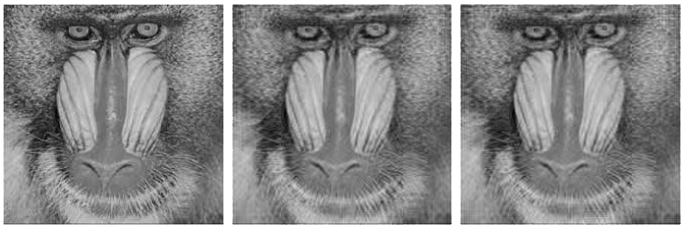


Figure 5: Perfect recovery percentage of a random Gaussian matrix and that of a matrix formed by elliptic curve $y^2 - x^3 - x - 2$ ($g = 1$) with the size 147×625. The recovery method is LASSO.

which simplifies to the curve $y^3 + y - x^4$ with genus $g = 3$. Using $\widetilde{m} = 4$ and $r = 7$, we can generate a 27×81 matrix based on this curve. The performance curve of this matrix shown in Figure 7 using the OMP technique is again better than that of a Gaussian matrix. To examine the performance of sensing matrices based on AG codes with large genus values, we use Example 4 with $p = 5$ (the curve $y^5 + y - x^6$); this curve has $g = 10$. By setting $\widetilde{m} = 4$ and $r = 20$, we construct a complex-valued 125×5^{10} matrix based on this curve. Due to



(a) (b) (c)

Figure 6: (a) Orginal image. (b) Recovered image based on the proposed matrix formed by an elliptic curve; PSNR is 26.6990. (c) Recovered image based on a random Gaussian matrix; PSNR is 26.6323

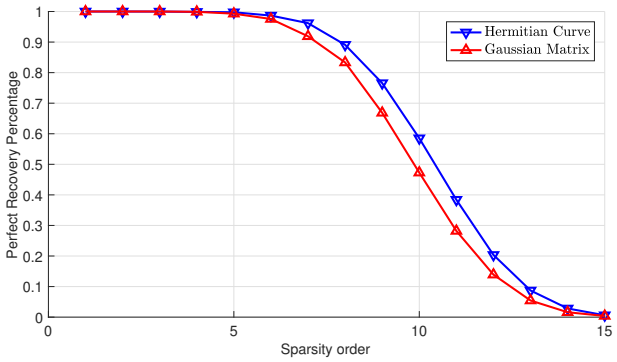


Figure 7: Perfect recovery percentage of a complex-valued matrix based on a Hermitian curve with $g = 3$ and size 27×81, as well as a random (complex-valued) Gaussian matrix of the same size. The recovery method is OMP.

computational complexity issues, we truncate this matrix by keeping only the first 500 columns, and depict the performance of this 125×500 matrix in Figure 8 using the OMP method.

5. Conclusion

The explicit construction of sensing matrices is desired in many applications of compressed sensing. In this paper, we presented a deterministic matrix design with small coherence based on algebraic geometry codes with large minimum distances (minimum distance comparable to the block size). The entries of the

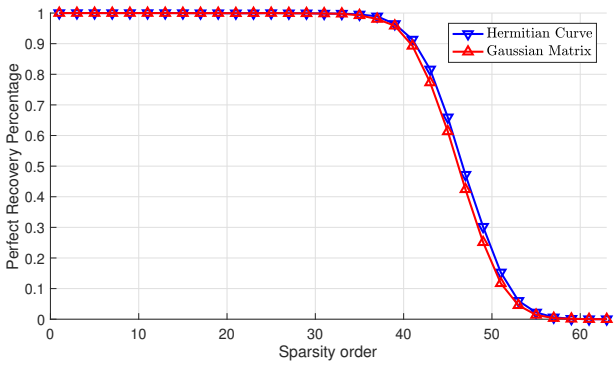


Figure 8: Perfect recovery percentage of a complex-valued based on a Hermitian curve with $g = 10$ and size 125×500, as well as a random (complex-valued) Gaussian matrix of the same size. The recovery method is OMP.

constructed $m \times n$ fat matrices take values on the complex unit circle; with this choice, the result ranges from binary-valued (± 1) matrices to more general complex-valued matrices. Besides the flexibility in the size of the matrix, the design technique allows for extremely fat matrices beyond $n > \mathcal{O}(m^2)$ for which the Welch bound on the coherence is no longer attainable. Interestingly, the coherence of the resulting matrices exceed the (possibly unachievable) Welch lower-bound only by an $\mathcal{O}(\log m)$ factor. Numerical experiments indicate that the constructed matrices perform equivalently or even better than the Gaussian matrices of the same size in recovering sparse vectors.

Appendix A. Number of Rational Points

Theorem 5 (Serre Bound)**.** *[34] Let $\mathcal{X}$ be an algebraic curve over F_q with genus g. Then, the number of rational points on $\mathcal{X}$ satisfies*

$$|N(\mathcal{X}) - q - 1| \leq g \, \lfloor 2q^{1/2} \rfloor \tag{A.1}$$

The useful point in the Serre bound is that it simultaneously provides lower and upper-bounds on the number of rational points. If the equality in the Serre bound holds for a given curve, it is called a maximal curve.

Appendix B. Extension Curves

Let $\mathcal{X}$ be an algebraic curve associated with $\phi(x, y) = 0$. The set of all triplets (x, y, z) that satisfy the following set of equations is called an extension curve:

$$\mathcal{X}_T = \big\{(x, y, z) \,\big|\, \Psi(x, y, z) = \phi(x, y) = 0\big\}, \tag{B.1}$$

where $\Psi(x, y, z)$ is a nonsingular and irreducible polynomial over $\mathbb{F}_q$ (which characteristic p). In particular, $\mathcal{X}_T$ is called the Artin-Schreier curve if $\Psi(x, y, z) = z^p - z - f(x, y)$. The genus of the Artin-Schreier curve is given by [37]:

$$g(\mathcal{X}_{T,f}) = p\, g(\mathcal{X}) - p + 1 + \frac{p-1}{2} \sum_{\substack{P:\ \text{rational} \\ \nu_P(f)<0}} \big(1 - \nu_P(f)\big).$$

Appendix C. Proof of Theorem 3

Consider $f \in \mathcal{L}(G)$. Since the supports of D and G are disjoint, for every point P_i in the support of D we have $\nu P_i(f) \geq 0$. Besides, the polynomial $\Psi(x, y, z) = z^p - z - f$ is irreducible over $\mathbb{F}_{p^{\widetilde{m}}}$, hence we can assume the extension curve $\mathcal{X}_{T,f}$, whose equation is

$$\mathcal{X}_{T,f} = \begin{cases} z^p - z = f(x, y), \\ \phi(x, y) = 0. \end{cases} \tag{C.1}$$

This extension is an Artin- Schreier extension(see Appendix B), therefore, using Arthur-Schreier theorem we have:

$$g(\mathcal{X}_{T,f}) = p\, g(\mathcal{X}) - p + 1 + \frac{p-1}{2} \sum_{\substack{P:\ \text{rational} \\ \nu_P(f)<0}} \big(1 - \nu_P(f)\big).$$

Now since $G = rP_\infty$, obviously f has only a pole at P_∞ of order at most r. Therefore

$$\sum_{P:\nu_P(f)<0} \deg(P)\big(1 - \nu_P(f)\big) - 2 \leq r - 1, \tag{C.2}$$

and as a result

$$g(\mathcal{X}_{T,f}) \leq g_\alpha = p\, g(\mathcal{X}) + \frac{(p-1)(r-1)}{2}. \tag{C.3}$$

We shall compute a lower bound for the weight of the word $\Big(\mathrm{Tr}\big(f(P_1)\big), \mathrm{Tr}\big(f(P_2)\big), ...\mathrm{Tr}\big(f(P_n)\big)\Big)$. If $\mathrm{Tr}\,(f(P_i)) = 0$, the equation has p simple roots, and the point P_i is ramified to exactly p rational points in $\mathcal{X}_{T,f}$. If $\mathrm{Tr}\,(f(P_i)) \neq 0$, the equation

$$\Psi(x, y, z) = z^p - z - f(P_i) = 0, \tag{C.4}$$

is irreducible; and, the point P_i is unramified in $\mathcal{X}_{T,f}$. If we denote the number of rational points in $\mathcal{X}_{T,f}$ by N and the weight of a codeword by w, we have

$$N \geq p(\widetilde{n} - w), \tag{C.5}$$

hence

$$w \geq \widetilde{n} - \frac{N}{p}. \tag{C.6}$$

Using Serre's bound

$$\begin{aligned} N &\leq p^{\widetilde{m}} + 1 + g(\mathcal{X}_{T,f})\lfloor 2p^{\widetilde{m}/2} \rfloor \\ &\leq p^{\widetilde{m}} + 1 + g_\alpha \lfloor 2p^{\widetilde{m}/2} \rfloor. \end{aligned} \tag{C.7}$$

Therefore

$$\mathrm{d}\Big(\mathrm{Tr}\big(\mathcal{C}(D, G)\big)\Big) \geq \widetilde{n} - \frac{p^{\widetilde{m}} + 1 + g_\alpha \lfloor 2p^{\widetilde{m}/2} \rfloor}{p}. \tag{C.8}$$

And the proof is complete.

References

References

[1] D. L. Donoho, Compressed sensing, IEEE Transactions on Information Theory 52 (4) (2006) 1289–1306.

[2] E. J. Candes, J. Romberg, T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, IEEE Transactions on Information Theory 52 (2) (2006) 489–509.

[3] E. J. Candes, M. B. Wakin, An introduction to compressive sampling, IEEE Signal Processing Magazine 25 (2) (2008) 21–30.

[4] E. J. Candes, T. Tao, Near-optimal signal recovery from random projections: Universal encoding strategies?, IEEE Transactions on Information Theory 52 (12) (2006) 5406–5425.

[5] E. J. Candes, The restricted isometry property and its implications for compressed sensing, Comptes Rendus Mathematique 346 (9-10) (2008) 589–592.

[6] S. Foucart, H. Rauhut, A mathematical introduction to compressive sensing, Bull. Am. Math 54 (2017) 151–165.

[7] A. M. Tillmann, M. E. Pfetsch, The computational complexity of the restricted isometry property, the nullspace property, and related concepts in compressed sensing, IEEE Transactions on Information Theory 60 (2) (2014) 1248–1259.

[8] T. Strohmer, R. W. Heath, Grassmannian frames with applications to coding and communication, Appl. Comp. Harmonic Anal (2003) 257–275.

[9] S. Satake, Y. Gu, On compressed sensing matrices breaking the square-root bottleneck, in: 2020 IEEE Information Theory Workshop (ITW), IEEE, 2021, pp. 1–5.

[10] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, Explicit constructions of RIP matrices and related problems, Duke Math. J. 159 (1) (2011) 145–185. doi:10.1215/00127094-1384809.

[11] R. A. DeVore, Deterministic constructions of compressed sensing matrices, Journal of Complexity 23 (4) (2007) 918 – 925.

[12] S. Li, F. Gao, G. Ge, S. Zhang, Deterministic construction of compressed sensing matrices via algebraic curves, IEEE Transactions on Information Theory 58 (8) (2012) 5035–5041.

[13] S. Li, G. Ge, Deterministic construction of sparse sensing matrices via finite geometry, IEEE Transactions on Signal Processing 62 (11) (2014) 2850–2859.

[14] H. Chen, Explicit RIP matrices in compressed sensing from algebraic geometry, CoRR, arXiv:1505.07490vl.

[15] A. Amini, F. Marvasti, Deterministic construction of binary, bipolar, and ternary compressed sensing matrices, IEEE Transactions on Information Theory 57 (4) (2011) 2360–2370.

[16] A. Amini, V. Montazerhodjat, F. Marvasti, Matrices with small coherence using p -ary block codes, IEEE Transactions on Signal Processing 60 (1) (2012) 172–181.

[17] R. C. S. Howard, S. Searle, A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes, 2008, pp. 11–15.

[18] M. M. Mohades, A. Mohades, A. Tadaion, A Reed-Solomon code based measurement matrix with small coherence, IEEE Signal Processing Letters 21 (7) (2014) 839–843.

[19] R. Calderbank, S. Howard, S. Jafarpour, Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property, IEEE journal of selected topics in signal processing 4 (2) (2010) 358–374.

[20] A. G. Dimakis, R. Smarandache, P. O. Vontobel, Ldpc codes for compressed sensing, IEEE Transactions on Information Theory 58 (5) (2012) 3093–3114.

[21] G. Wang, M.-Y. Niu, F.-W. Fu, Deterministic constructions of compressed sensing matrices based on optimal codebooks and codes, Applied Mathematics and Computation 343 (2019) 128–136.

[22] L. Applebaum, S. D. Howard, S. Searle, R. Calderbank, Chirp sensing codes: Deterministic compressed sensing measurements for fast recovery, Applied and Computational Harmonic Analysis 26 (2) (2009) 283–290.

[23] N. Y. Yu, Y. Li, Deterministic construction of fourier-based compressed sensing matrices using an almost difference set, EURASIP Journal on Advances in Signal Processing 2013 (1) (2013) 155.

[24] S. Jafarpour, W. Xu, B. Hassibi, R. Calderbank, Efficient and robust compressed sensing using optimized expander graphs, IEEE Transactions on Information Theory 55 (9) (2009) 4299–4308.

[25] R. R. Naidu, P. Jampana, C. S. Sastry, Deterministic compressed sensing matrices: Construction via euler squares and applications, IEEE Transactions on Signal Processing 64 (14) (2016) 3566–3575.

[26] A. Amini, H. Bagh-Sheikhi, F. Marvasti, From paley graphs to deterministic sensing matrices with real-valued gramians, in: 2015 International Conference on Sampling Theory and Applications (SampTA), 2015, pp. 372–376.

[27] J. Liang, H. Peng, L. Li, F. Tong, Construction of structured random measurement matrices in semi-tensor product compressed sensing based on combinatorial designs, Sensors 22 (21) (2022) 8260.

[28] J. Liang, H. Peng, L. Li, F. Tong, Y. Yang, Flexible construction of measurement matrices in compressed sensing based on extensions of incidence matrices of combinatorial designs, Applied Mathematics and Computation 420 (2022) 126901.

[29] F. Tong, L. Li, H. Peng, Y. Yang, Deterministic constructions of compressed sensing matrices from unitary geometry, IEEE Transactions on Information Theory 67 (8) (2021) 5548–5561.

[30] Y. Jie, M. Li, C. Guo, B. Feng, T. Tang, A new construction of compressed sensing matrices for signal processing via vector spaces over finite fields, Multimedia Tools and Applications 78 (2019) 31137–31161.

[31] F. Tong, L. Li, H. Peng, Y. Yang, Flexible construction of compressed sensing matrices with low storage space and low coherence, Signal Processing 182 (2021) 107951.

[32] Z. Gu, Z. Zhou, Y. Yang, A. R. Adhikary, X. Cai, Deterministic compressed sensing matrices from sequences with optimal correlation, IEEE Access 7 (2019) 16704–16710.

[33] H. M. Dolatabadi, A. Amini, Deterministic design of toeplitz matrices with small coherence based on weyl sums, IEEE Signal Processing Letters 26 (10) (2019) 1501–1505.

[34] N. S. Harald, L. San, Advances in algebraic geometry codes, World Scientific, New Jersey, 2008.

[35] H. Stichtenoth, Algebraic function fields and codes, Vol. 254, Springer Science & Business Media, 2009.

[36] B. Malmskog, Maximal curves, zeta functions, and digital signatures, Ph.D. thesis, Colorado State University. Libraries (2011).

[37] S. Farnell, R. Pries, Families of artin–schreier curves with cartier–manin matrix of constant rank, Linear Algebra and its Applications 439 (7) (2013) 2158–2166.