# Compressed sensing matrices from function fields defined by linearized polynomials

Gretchen L. Matthews [*][†]    Justin D. Peachey[‡]

May 26, 2015

**Abstract**

Compressed sensing is a technique which allows for the reconstruction of a sparse signal even when few measurements of the signal are available. A key problem in compressed sensing is the deterministic constuction of sensing matrices. In this paper, we provide sensing matrices from function fields defined by linearized polynomials. Our approach relies on the determination of explicit bases for Riemann-Roch spaces on function fields defined by linearized polynomials. At times, it improves upon comparable known constructions. In addition to the sensing matrices, the bases yield explicit generator and parity check matrices for algebraic geometry codes. Previous results on the Hermitian function field as well as on the norm-trace function field can be obtained as special cases of those given here for function fields defined by linearized polynomials.

## 1 Introduction

The goal of compressed sensing is to reconstruct a discrete-time signal by taking as few measurements as possible. Let $\Phi$ be an $m \times n$ matrix and

[*] Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975 email: gmatthe@clemson.edu

[†] G. L. Matthews' work was supported in part by NSF DMS-0901693 and NSA H-98230-06-1-0008.

[‡] Mathematics Department, Davidson College, Davidson, NC 28036 email: jupeachey@davidson.edu

$\mathbf{y} = \mathbf{\Phi x}$ where the entries of both $\Phi$ and $\mathbf{x}$ are real numbers. Compressed sensing seeks to reconstruct $\mathbf{x}$ from $\mathbf{y}$. Here, $\mathbf{x}$ is considered as a discrete-time signal, $\mathbf{y}$ is thought of as the measurement vector, and $\Phi$ is called a sensing matrix. In groundbreaking works, Candes, Romberg, and Tao [4] and Donoho [8] show that a sparse signal can be reconstructed with few measurements. Furthermore, Candes et. al. provide criteria, such as the restricted isometry property defined below, which are desirable for sensing matrices.

While random matrices satisfy this criteria with high probability, it is difficult to verify the criteria for a particular matrix. In addition, the storage requirements for a random matrix may be problematic. Hence, there is a need for deterministic constructions. Recently, a new deterministic construction of sensing matrices using algebraic geometric (AG) codes from the Hermitian function field was given by Li, Gao, Ge, and Zhang [14]. By utilizing the structure of certain Riemann-Roch spaces, they provide an improvement on DeVore's construction from polynomials over $\mathbb{F}_p$ [7]. In this paper, we construct a larger class of sensing matrices from function fields defined by linearized polynomials. To demonstrate their advantages, we first give a brief overview of compressed sensing. For a more in-depth treatment, see [8] or [6].

To refine the search for good sensing matrices, we consider the following definition. Here, we say a vector $\mathbf{x} \in \mathbb{R}^{\mathbf{n}}$ is $k$-sparse to mean $\mathbf{x}$ has at most $k$ nonzero entries.

**Definition 1.1.** *An $m \times n$ matrix $\Phi$ satisfies the restricted isometry property (RIP) of order $k$ if there is a constant $0 \leq \delta_k < 1$ such that for all $k$-sparse vectors $\mathbf{x}$,*

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

If a matrix $\Phi$ satisfies the restricted isometry property, then a unique and exact solution $\mathbf{x}$ is guaranteed. Often, the notion of coherence is used as a proxy for RIP. The coherence of a matrix $\Phi$ with unit column vectors $\mathbf{u}_i$ is

$$\mu(A) = \max_{i \neq j} |\langle \mathbf{u}_i, \mathbf{u}_j \rangle|.$$

Then, the following is shown in [1].

**Theorem 1.2.** *If a matrix $\Phi$ has coherence $\mu$, then $\Phi$ satisfies the restricted isometry property of order $k$ with constant $\delta_k = (k - 1)\mu$.*

Note that as $\delta_k < 1$, we must have that $k < \frac{1}{\mu} + 1$. This leads one to consider matrices with small values of $\mu$ in order to handle larger values of $k$ (meaning less sparse vectors $\mathbf{x}$). In [14], the authors construct matrices from algebraic codes from the Hermitian function field which are better than those in [7].

In this paper, we build sensing matrices from function fields defined by linearized polynomials. To do so, we provide explicit bases for Riemann-Roch spaces of divisors supported by certain places of degree one on function fields defined by linearized polynomials. These bases yield sensing matrices which, in certain cases, improve upon their Hermitian counterparts.

This paper is organized as follows. This section concludes with a summary of notation used throughout the paper. Section 2 contains relevant background on the function fields defined by linearized polynomials and includes the determination of bases for and dimension of certain Riemann-Roch spaces. These are applied to determine sensing matrices in Section 3. Closing observations are shared in Section 4.

**Notation.** Let $\mathbb{F}$ be a finite field and $F/\mathbb{F}$ be an algebraic function field of genus $g > 1$. The divisor of a function $f \in F \setminus \{0\}$ will be denoted by $(f)$. The Riemann-Roch space of a divisor $A$ of $F$ is

$$\mathcal{L}(A) := \ \{f \in F \setminus \{0\} : (f) \geq -A\} \cup \{0\},$$

which is a finite-dimensional vector space over $\mathbb{F}$. Let $\ell(A)$ denote the dimension of the vector space $\mathcal{L}(A)$ over $\mathbb{F}$. The Riemann-Roch Theorem states that

$$\ell(A) = \deg A + 1 - g + \ell(W - A)$$

where $W$ is any canonical divisor of $F$. Moreover, if the degree of $A$ is at least $2g - 1$, then $\ell(W - A) = 0$ and so $\ell(A) = \deg A + 1 - g$. For divisors $A$ of smaller degree, the dimension $\ell(A)$ is not necessarily easy to compute.

The set of positive integers is denoted by $\mathbb{Z}^+$. As usual, given $v \in \mathbb{Z}^m$ where $m \in \mathbb{Z}^+$, the $i^{th}$ coordinate of $v$ is denoted by $v_i$.

# 2 Function fields defined by linearized polynomials and bases for some Riemann-Roch spaces

Let $q$ be a power of a prime and $r$ be an integer with $r \geq 2$. Consider the function field $F := \mathbb{F}_{q^r}(x, y) / \mathbb{F}_{q^r}$ with defining equation

$$L(y) = x^u \tag{1}$$

where $u | \frac{q^r-1}{q-1}$ and $L(y) = \sum_{i=0}^{d} a_i y^{q^i}$ is a separable linearized polynomial which splits over $\mathbb{F}_{q^r}$ If one takes $u = \frac{q^r-1}{q-1}$ and $L(y) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$, the defining equation is

$$Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y) = N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x),$$

meaning the trace of $y$ with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is equal to the norm of $x$ with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$; this function field is called the norm-trace function field. As special cases, one may also obtain the Hermitian function field (by taking $r = 2$, $u = \frac{q^r-1}{q-1}$, and $L(y) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$) and a quotient of the Hermitian function field (by taking $r = 2$ and $L(y) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$). The norm-trace function field was first studied by Geil in [11] where he considered evaluation codes and one-point algebraic geometry codes constructed from this function field. More recently, Munuera, Tizziotti, and Torres [18] examined two-point algebraic geometry codes on this same function field.

The relevance of this function field to coding theory and other applications is tied to the abundance of rational places. Both the Hermitian function field and its quotient mentioned above are maximal function fields, meaning that the number of rational places meet the Hasse-Weil bound. The norm-trace function field and its infinite place, while not maximal, meet the Geil-Matsumoto bound [12]; certain places are used in the construction of algebraic geometry codes, and the Geil-Matsumoto bound takes this into account.

Given $a, b \in \mathbb{F}_{q^r}$ such that $L(b) = a^u$, let $P_{ab}$ denote the unique place of $F$ of degree one with $x(P_{ab}) = a$ and $y(P_{ab}) = b$. The common pole of $x$ and $y$ will be denoted by $P_\infty$. Consider

$$\mathcal{B} := \{\beta \in \mathbb{F}_{q^r} : L(\beta) = 0\}.$$

Then $|\mathcal{B}| = q^d$, and for any $\beta \in \mathcal{B}$, $L(y) = L(y - \beta)$ which means $F$ has $q^d$ places of the form $P_{0\beta}$. Furthermore, one can show

$$(x) = \sum_{\beta \in \mathcal{B}} P_{0\beta} - q^d P_\infty \ \text{ and } \ (y - \beta) = uP_{0\beta} - uP_\infty. \tag{2}$$

We view $F$ as a Kummer extension of $\mathbb{F}_{q^r}(y)$. The place of the rational function field $\mathbb{F}_{q^r}(y)$ which corresponds to the irreducible polynomial $y - \beta$ is denoted $P_\beta$. If $\beta \in \mathcal{B}$, then $P_\beta$of $\mathbb{F}_{q^r}(y)$ is totally ramified in $F/\mathbb{F}_{q^r}(y)$ as is the infinite place $p_\infty$ of $\mathbb{F}_{q^r}(y)$. The genus of $F/\mathbb{F}_{q^r}$ is $g = \frac{(u-1)\left(q^d-1\right)}{2}$.

We now focus on bases for Riemann-Roch spaces $\mathcal{L}(a_\infty P_\infty + \sum_{\beta \in \mathcal{B}} a_\beta P_{0\beta})$. To do so, we make use of integral bases, which can be determined immediately from [20, Theorem III.5.10(b)]. The results given here generalize those in [15] and are obtained via a similar approach.

**Lemma 2.1.** *The functions $1, x, x^2, \ldots, x^{u-1}$ form an integral basis of the function field $\mathbb{F}_{q^r}(y, x)/\mathbb{F}_{q^r}(y)$ at any place of $\mathbb{F}_{q^r}(y)$ other than $p_\infty$.*

**Theorem 2.2.** *Consider the divisor $G := a_\infty P_\infty + \sum_{\beta \in \mathcal{B}} a_\beta P_{0\beta}$ on the function field $F/\mathbb{F}_{q^r}$ defined by $L(y) = x^u$ as in (1), where $a_\infty \in \mathbb{Z}$ and $a_\beta \in \mathbb{Z}$ for all $\beta \in \mathcal{B}$. Then*

$$\bigcup_{0 \le i \le u-1} \left\{ x^i f_{ic}(y) : c \in \mathbb{Z}, -\sum_{\beta \in \mathcal{B}} \left\lfloor \frac{a_\beta + i}{u} \right\rfloor \le c \le \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor \right\}$$

*is a basis for $\mathcal{L}(G)$ as a vector space over $\mathbb{F}_{q^r}$ where*

$$f_{ic}(y) \in \left\{ \prod_{\beta \in \mathcal{B}} (y - \beta)^{e_{\beta,i}} : e_{\beta,i} \in \mathbb{Z}, e_{\beta,i} \ge -\left\lfloor \frac{a_\beta + i}{u} \right\rfloor, \sum_{\beta \in \mathcal{B}} e_{\beta,i} = c \right\}.$$

*Furthermore, the dimension of $\mathcal{L}(G)$ is*

$$\ell(G) = \sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor + \sum_{\beta \in \mathcal{B}} \left\lfloor \frac{a_\beta + i}{u} \right\rfloor + 1, 0 \right\}.$$

*Proof.* Let $\mathcal{L} := \mathcal{L}(a_\infty P_\infty + \sum_{\beta \in \mathcal{B}} a_\beta P_{0\beta})$ and

$$S := \left\{ x^i \prod_{\beta \in \mathcal{B}} (y - \beta)^{e_{\beta,i}} : \begin{array}{l} e_{\beta,i} \in \mathbb{Z}, \ -a_\beta \le ue_{\beta,i} + i, \\ iq^d + u\sum_{\beta \in \mathcal{B}} e_{\beta,i} \le a_\infty \\ \forall i, \ 0 \le i \le u-1 \end{array} \right\}.$$

Notice that (2) implies $S \subseteq \mathcal{L}$ and the $\mathbb{F}_{q^r}$-linear span of $S$ is a subset of $\mathcal{L}$.

Let $f \in \mathcal{L}\backslash\{0\}$. Given a place $P$ of $\mathbb{F}_{q^r}(y)$ where $P \notin \{p_\infty\} \cup \{P_\beta : \beta \in \mathcal{B}\}$, there exist $f_i \in \mathbb{F}_{q^r}(y)$ such that

$$f = f_0 + f_1 x + \cdots + f_{u-1} x^{u-1}$$

and no $f_i$ has a pole at $P$, according to Lemma 2.1. In fact, the only possible poles of $f_i$ in $\mathbb{F}_{q^r}(y)$ are $p_\infty$ and $P_\beta$ with $\beta \in \mathcal{B}$. To see this, consider a place $Q$ of $\mathbb{F}_{q^r}(y)$, $Q \notin \{p_\infty, P\} \cup \{P_\beta : \beta \in \mathcal{B}\}$. Notice that Lemma 2.1 also applies to $Q$, meaning there exist $h_i \in \mathbb{F}_{q^r}(y)$ such that $f = h_0 + h_1 x + \cdots + h_{u-1} x^{u-1}$ and no $h_i$ has a pole at $Q$. Because $\{1, x, \ldots, x^{u-1}\}$ is a basis of $F/\mathbb{F}_{q^r}(y)$, $f_i = h_i$ for all $i$, $0 \leq i \leq u-1$, which implies $f_i$ has no poles at $Q$. Consequently, the only possible poles of $f_i$ in $\mathbb{F}_{q^r}(y)$ are $p_\infty$ and $P_\beta$ with $\beta \in \mathcal{B}$, and

$$f_i = g_i(y) \prod_{\beta \in \mathcal{B}} (y - \beta)^{e_{\beta,i}},$$

where $e_{\beta,i} \in \mathbb{Z}$, $g_i \in \mathbb{F}_{q^r}[y]$, and $(y-\beta) \nmid g_i(y)$ for all $\beta \in \mathcal{B}$. It follows that $f$ is an $\mathbb{F}_{q^r}$-linear combination of functions

$$A_{i,j} := x^i y^{j+e_{0,i}} \prod_{\beta \in \mathcal{B}\backslash\{0\}} (y-\beta)^{e_{\beta,i}}$$

with $0 \leq j \leq \deg g_i$. It remains to verify that $A_{i,j} \in S$ for $0 \leq i \leq u-1$ and $0 \leq j \leq \deg g_i$. Since $P_{0\beta}$ is totally ramified in the extension $F/\mathbb{F}_{q^r}(y)$ for all $\beta \in \mathcal{B}$, $v_{P_{0\beta}}(f_i x^i) = u v_{P_\beta}(f_i) + i = u e_{\beta,i} + i$. Hence, for $0 \leq i, j \leq u-1$,

$$v_{P_{0\beta}}\left(f_i x^i\right) \not\equiv v_{P_{0\beta}}\left(f_j x^j\right) \mod u$$

unless $i = j$. As a result, $\min\{u e_{\beta,i} + i : 0 \leq i \leq u-1\} = v_{P_{0\beta}}(f) \geq -a_\beta$. Similarly, $\min\{v_{P_\infty}(f_i x^i) : 0 \leq i \leq u-1\} = v_{P_\infty}(f) \geq -a_\infty$ as

$$v_{P_\infty}\left(f_i x^i\right) = v_{P_\infty}(f_i) + v_{P_\infty}\left(x^i\right) = u v_{p_\infty}(f_i) - iq^d$$

are distinct modulo $u$ for $0 \leq i \leq u-1$. Since $v_{p_\infty}(f_i) = -\left(\deg g_i + \sum_{\beta \in \mathcal{B}} e_{\beta,i}\right)$, we conclude that

$$u\left(j + e_{0,i}\right) + \sum_{\beta \in \mathcal{B}\backslash\{0\}} e_{\beta,i} + iq^d \leq u\left(\deg g_i + \sum_{\beta \in \mathcal{B}} e_{\beta,i}\right) + iq^d \leq a_\infty.$$

Thus, $A_{ij} \in S$ and $f$ is in the $\mathbb{F}_{q^r}$-linear span of $S$, establishing that $S$ is a spanning set for $\mathcal{L}$.

Next, we obtain a basis for $\mathcal{L}$ from $S$. For $0 \leq i \leq u-1$, set

$$V_i := \left\{ -iq^d - u \sum_{\beta \in \mathcal{B}} e_\beta : \begin{array}{l} e_\beta \in \mathbb{Z}, -a_\beta \leq ue_\beta + i, \text{ and} \\ iq^d + u \sum_{\beta \in \mathcal{B}} e_\beta \leq a_\infty \ \forall \beta \in B \end{array} \right\}$$

and $V := \cup_{i=0}^{u-1} V_i$. From above, $\{v_{P_\infty}(f) : f \in \mathcal{L} \setminus \{0\}\} \subseteq V$. If $n \in V$, then $n = v_{P_\infty}\left( x^i \prod_{\beta \in \mathcal{B}} (y-\beta)^{e_\beta} \right)$. Since $x^i \prod_{\beta \in \mathcal{B}} (y-\beta)^{e_\beta} \in \mathcal{L}$ by the previous argument, $V = \{v_{P_\infty}(f) : f \in \mathcal{L} \setminus \{0\}\}$. Moreover,

$$\dim \mathcal{L} = |V| = \sum_{i=0}^{u-1} |V_i|.$$

Here, the first equality holds due to [15, Lemma 3.5]. The latter equality follows from the observation that the sets $V_i$, $0 \leq i \leq u-1$, are disjoint; indeed, $u \mid (i-j)q^d$ implies $i = j$.

For $i$, $0 \leq i \leq u-1$, one can check that

$$| V_i | = | \left\{ c \in \mathbb{Z} : -\sum_{\beta \in \mathcal{B}} \left\lfloor \frac{a_\beta + i}{u} \right\rfloor \leq c \leq \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor \right\} | \, .$$

Hence,

$$|V_i| = \max \left\{ \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor + \sum_{\beta \in \mathcal{B}} \left\lfloor \frac{a_\beta + i}{u} \right\rfloor + 1, 0 \right\},$$

completing the proof. □

**Remark 2.3.** *Notice that one may set $a_\beta = 0$ for some (or all) $\beta \in \mathcal{B}$ or $a_\infty = 0$. In this way, Theorem 2.2 gives bases for divisors with support being any subset of $\{P_0\beta : \beta \in \mathcal{B}\} \cup \{P_\infty\}$. By setting $r = 2$, $u = q+1$, and $L(y) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$, one recovers bases for Riemann-Roch spaces of the Hermitian function field [15, Corollary 3.7]. In particular, setting $a_\beta = 0$ for all $\beta \in \mathcal{B}$ yields the original result of Stichtenoth [21, Satz 2] (see also [22, Proposition 1]).*

Our focus is the construction of sensing matrices which follow from Theorem 2.2; this is detailed in the next section. It is also worth noting that Theorem 2.2 has several immediate consequences for algebraic geometry codes defined by divisors whose support is contained in $\{P_\infty\} \cup \mathcal{B}$. For instance, we can obtain the floor of any divisor whose support is contained in $\{P_\infty\} \cup \mathcal{B}$, exact dimensions of algebraic geometry codes defined by divisors whose support is contained in $\{P_\infty\} \cup \mathcal{B}$, as well as bounds on the minimum distances of such codes. In addition, both generator and parity-check matrices of these codes are corollaries of Theorem 2.2.

# 3 Compressed Sensing Matrices

We now review the construction for sensing matrices due to Li et. al. [14]. Let $q$ be a prime power and consider a function field $F$ over $\mathbb{F}_q$. Let $\mathcal{P}$ denote a set of rational places of $F$ and $G$ be a divisor of $F$ such that $\deg(G) < |\mathcal{P}|$ and the support of $G$ does not include any places which are elements of $\mathcal{P}$. For each $f \in \mathcal{L}(G)$, define a column vector $v_f$ whose entries are indexed by pairs $(P, a) \in \mathcal{P} \times \mathbb{F}_q$ by

$$[v_f]_{(P,a)} := \mathbb{1}_{f(P)=a},$$

meaning that the entry of $v_f$ associated with the pair $(P, a)$ is an indicator function

$$\mathbb{1}_{f(P)=a} = \begin{cases} 1 & \text{if } f(P) = a \\ 0 & \text{otherwise.} \end{cases}$$

Define an $m \times n$ matrix $\Phi_0$ with columns $v_f$ where $f \in \mathcal{L}(G)$; here, $m = q|\mathcal{P}|$ and $n = q^{\ell(G)}$. Then the following result holds.

**Lemma 3.1** ([14], Theorem 3.2)**.** *Let $\Phi = \frac{1}{\sqrt{|\mathcal{P}|}}\Phi_0$. Then $\Phi$ is a sensing matrix with coherence $\mu(\Phi) \leq \frac{\deg(G)}{|\mathcal{P}|}$.*

Applying this construction to the Hermitian function field over $\mathbb{F}_{q^2}$ with $G = sQ_\infty$ gives sensing matrices of size $m_H \times n_H$ where $m_H = q^2 \cdot |\mathcal{P}_H| = q^5$, $n_H = q^{2\ell(G)}$, and $2g_H - 1 \leq s < |\mathcal{P}| = q^3$. For certain values of $q$, this construction yields better parameters than previously known from DeVore's construction; indeed, better sensing matrices are obtained when $\frac{8(s-g_H+1)-2}{5} > q^{\frac{3}{2}}$. By applying this construction to function fields defined by linearized polynomials as in (1), we show that it is possible to construct larger classes of sensing matrices. In certain cases, they improve upon those associated with the Hermitian function field.

**Theorem 3.2.** *Let $s \in \mathbb{Z}^+$. Then there exists a sensing matrix $\Phi$ of size $m_{nt} \times n_{nt}$ where $m_{nt} := q^{3r-1}$ and $n_{nt} := q^{r\ell(sP_\infty)}$ with coherence bounded by $\mu(\Phi) \leq \frac{s}{q^{2r-1}}$.*

*Proof.* Take $F$ to be the norm-trace function field over $\mathbb{F}_{q^r}$. Then $F$ has exactly $q^{2r-1}+1$ places of degree one. Set $G = sP_\infty$. Then $|\mathcal{P}| = q^{2r-1}$. The result is then an immediate application of Lemma 3.1. □

**Corollary 3.3.** *There exists sensing matrices constructed from the norm-trace function field over $\mathbb{F}_{q^r}$ with the upper bound on coherence in Lemma 3.1 less than that of sensing matrices from the Hermitian function field of the same size.*

**Corollary 3.4.** *Let $k = \frac{3r-1}{5}$. If $\frac{s}{t} < q^{\frac{r-2}{5}}$, then the upper bound on the coherence of sensing matrices in Lemma 3.1 from the norm-trace function field is less than that of those from the Hermitian function field.*

*Proof.* Consider the Hermitian function field $H$ over $\mathbb{F}_{q^{2k}} = \mathbb{F}_{\left(q^k\right)^2}$ and the norm-trace function field $F$ over $\mathbb{F}_{q^r}$. Let $t \in \mathbb{Z}$ be so that $2g_H - 1 \leq t < q^{3k}$ and $\frac{2k}{r}(t+1-g_H) \in \mathbb{Z}$, where $g_H := \frac{q^k(q^k-1)}{2}$ is the genus of $H$. By the Riemann-Roch Theorem, $\ell\left(tQ_\infty\right) = t+1-\frac{q^k(q^k-1)}{2}$ where $Q_\infty$ is the infinite place of $H$. Because $\frac{2k}{r}(t+1-g_H) \in \mathbb{Z}^+$, Theorem 2.2 applies to give $s \in \mathbb{Z}^+$ so that

$$\ell(sP_\infty) = \frac{2k}{r}(t+1-g_H)$$

where $P_\infty$ is the infinite place of the norm-trace function field. According to Theorem 3.1, we may construct an $m_{nt} \times n_{nt}$ sensing matrix $\Phi_{nt}$ where $m_{nt} = q^{3r-1}$, $n_{nt} = q^{r\ell(sP_\infty)} = q^{2k(t+1-g_H)}$, and $\mu\left(\Phi_{nt}\right) \leq \frac{s}{q^{2r-1}} =: \mu_{nt}$. Notice that the function field $H$ and divisor $G = tQ_\infty$ also give rise to a sensing matrix $\Phi_H$ of size $q^{3r-1} \times q^{2k(t+1-g_H)}$, because $\left(q^k\right)^5 = q^{5k} = q^{3r-1}$ and $q^{k^{2\ell(tQ_\infty)}} = q^{2k(t+1-g_H)}$. By Lemma 3.1, the coherence of $\Phi_H$ is $\mu\left(\Phi_H\right) \leq \frac{t}{q^{3k}} =: \mu_H$.

Comparing the bounds on the coherence of the matrices $\Phi_{nt}$ and $\Phi_H$, we see that

$$\mu_{nt} < \mu_H$$

as $\frac{s}{t} < q^{\frac{r-2}{5}}$. □

**Remark 3.5.** *If $s, t$ satisfy the given hypotheses, $\ell(sP_\infty) = \frac{k}{r}(t+1-g_H)$. Moreover, as $q \geq 2$ and $r \geq 7$, $q^k \leq q^{r-1}-1$ and $2q^{2k} \leq q^{2r-2}$. Hence,*

$$\frac{k}{r}(t+1-g_H) \leq \frac{k}{r}(q^{3k}-g_H) = \frac{(3r-1)(2q^{3k}-q^k+q^{\frac{k}{2}})}{10r} < g_{nt}.$$

*Thus, to find* $s$ *it is necessary to apply Theorem 2.2 since* $s < 2g_{nt} - 1$. *Also, as Theorem 2.2 provides a basis for* $\mathcal{L}(sP_\infty)$, *we may find an explicit description of all functions in the Riemann-Roch space. An explicit construction of these matrices is as given in the introduction to this section. Furthermore, provided that* $\frac{s}{t}q^{\frac{-11r+7}{10}} < 1$, *the sensing matrix constructed over the norm-trace function field has a smaller bound on the coherence than its Hermitian counterpart.*

**Example 3.6.** *Let* $q = 2$ *and* $r = 7$*; then,* $k = 4$. *Consider the norm-trace function field* $F$ *over* $\mathbb{F}_{2^7}$ *and the Hermitian function field* $F'$ *over* $\mathbb{F}_{2^4}$. *Then, if* $t = 4093 = 2^{12} - 3 < q^{3k} - 1$, $\frac{k}{r}(t + 1 - g_H) = 2336$. *Applying Theorem 2.2, we find* $\ell(6064P_\infty) = 2336$.

*Then the sensing matrix constructed over the Hermitian function field is a* $2^{20} \times 2^{16352}$ *matrix with* $\mu_H \leq \frac{4093}{2^6}$. *Moreover, the corresponding sensing matrix constructed over the norm-trace function field has the same dimensions, and* $\mu_{nt} \leq \frac{6064}{2^{13}} < \frac{4093}{2^6}$.

**Example 3.7.** *Let* $q = 5$ *and* $r = 7$*; then,* $k = 4$. *Consider the norm-trace function field* $F$ *over* $\mathbb{F}_{5^7}$ *and the Hermitian function field* $F'$ *over* $\mathbb{F}_{5^4}$. *Then, if* $t = 600 = 2g_H$, $\frac{k}{r}(t + 1 - g_H) = 2336$. *Using Sage and applying Theorem 2.2, we find* $\ell(304687P_\infty) = 172$.

*Then the sensing matrix constructed over the Hermitian function field is a* $5^{20} \times 5^{1204}$ *matrix with* $\mu_H \leq \frac{600}{5^6}$. *Moreover, the corresponding sensing matrix constructed over the norm-trace function field has the same dimensions, and* $\mu_{nt} \leq \frac{304687}{5^{13}} < \frac{600}{5^6}$.

# 4 Conclusion

In this paper, we obtain compressed sensing matrices using function fields defined by linearized polynomials. To do so, we give explicit bases for Riemann-Roch spaces of these function fields which may be of independent interest (especially considering that this family of function fields includes the Hermitian function field and the norm-trace function field as well as certain quotients). Applications of the determined Riemann-Roch spaces are not limited those of sensing matrices and AG codes considered here. They are also relevant to the construction of low-discrepancy sequences [19], certain secret-sharing schemes [5, 10], and small-bias sets [17].

# References

[1] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, Explicit constructions of RIP matrices and related problems, Duke Math. J. **159** (2011), no. 1, 145–185.

[2] M. Bras-Amoros and M. E. O'Sullivan, Duality for some families of correction capability optimized evaluation codes, Adv. Math. Commun. **2** (2008), no. 1, 15–33.

[3] E.J. Candes, The restricted isometry property and its implications for compressed sensing, Comptes Rendus Math. Acad. Sci. Paris, **346** (2008), no. 9, 589–592.

[4] E.J. Candes, J. Romberg, and T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, IEEE Trans. Inform. Theory **52** (2006), no. 2, 489–509.

[5] H. Chen and R. Cramer, Algebraic geometric secret sharing schemes and secure multi-party computations over small fields, Advances in cryptology—CRYPTO 2006, 521–536, Lecture Notes in Comput. Sci. **4117** , Springer, Berlin, 2006.

[6] A. Cohen, W. Dahmen, R. DeVore, A taste of compressed sensing, in Independent Component Analyses, Wavelets, Unsupervised Nano-Biomimetic Sensors, and Neural Networks, Proceedings of SPIE **6576** (2007).

[7] R. A. DeVore, Deterministic constructions of compressed sensing matrices, J. Complexity, **23** (2007), 918–925.

[8] D.L. Donoho, Compressed sensing, IEEE Trans. Inform. Theory **52** (2006), no. 4, 1289–1306.

[9] I. Duursma, R. Kirov, and S. Park, Distance bounds for algebraic geometry codes, J. Pure Appl. Algebra **215** (2011), no. 8, pp. 1863-1878.

[10] I. Duursma and S. Park, Coset bounds for algebraic geometry codes, Finite Fields Appl. **16** (2010), no. 1, 36–55.

[11] O. Geil, On codes from norm-trace curves, Finite Fields Appl. **9** (2003), no. 3, 351–371.

[12] O. Geil and R. Matsumoto, Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups, J. Pure Appl. Algebra **213** (2009), 1152–1156.

[13] T. Høholdt, J. H. van Lint, and R. Pellikaan, Algebraic geometry codes, in Handbook of Coding Theory, V. Pless, W. C. Huffman, and R. A. Brualdi, Eds., **1**, Elsevier, Amsterdam (1998), 871–961.

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

[15] H. Maharaj, G. L. Matthews, and G. Pirsic, Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences, J. Pure Appl. Algebra. **195** (2005), 261–280.

[16] G. L. Matthews, Weierstrass semigroups and codes from a quotient of the Hermitian curve, Des. Codes Cryptogr. **37** (2005), no. 3, 473–492.

[17] G. L. Matthews and J. D. Peachey, Small-bias sets from extended norm-trace codes, Contemp. Math. (Proceedings of 11th International Conference on Finite Fields and their Applications) **579** (2012), 143-152.

[18] C. Munuera, G. C. Tizziotti, and F. Torres, Two-point codes on norm-trace curves, Coding Theory and Applications, Second International Castle Meeting, ICMCTA 2008 (A. Barbero Ed.), 128–136, Lecture Notes in Comput. Sci. **5228**, Springer-Verlag Berlin Heidelberg 2008.

[19] H. Niederreiter and C. Xing, Low discrepancy sequences and global function fields with many rational places, Finite Fields Appl. **2**(1996), no. 3, 241–273.

[20] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.

[21] H. Stichtenoth, Ober die automorphismengruppe eines algebraischen funktionenkorpers von primzahlcharackteristik, teil 2, Arch. Math. **24** (1973), 615–631.

[22] H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, IEEE Trans. Inform. Theory **34** (1988), no. 5, 1345–1348.

[23] H. J. Tiersma, Remarks on codes from Hermitian curves, IEEE Trans. Inform. Theory **IT-33** (1987), 605–609.