COHERENCE OF SENSING MATRICES COMING FROM ALGEBRAIC-GEOMETRIC CODES

SEUNGKOOK PARK
Department of Mathematics
Sookmyung Women’s University
Cheongpa-ro 47 gil 100, Yongsan-Ku, Seoul 140-742, Korea

(Communicated by Gary McGuire)

Abstract. Compressed sensing is a technique which is used to reconstruct a sparse signal given few measurements of the signal. One of the main problems in compressed sensing is the deterministic construction of the sensing matrix. Li et al. introduced a new deterministic construction via algebraic-geometric codes (AG codes) and gave an upper bound for the coherence of the sensing matrices coming from AG codes. In this paper, we give the exact value of the coherence of the sensing matrices coming from AG codes in terms of the minimum distance of AG codes and deduce the upper bound given by Li et al. We also give formulas for the coherence of the sensing matrices coming from Hermitian two-point codes.

1. Introduction

Consider a discrete-time signal $x \in \mathbb{R}^n$. Let $y \in \mathbb{R}^m (m < n)$ be the measurement vector with $y = \Phi x$, where the $m \times n$ matrix $\Phi$ consists of $m$ linear projections of $x$. The $m \times n$ matrix $\Phi$ is called a sensing matrix. Compressed sensing is a technique which is used to reconstruct the original signal $x$ from the measurement vector $y$. Since $m < n$, $y = \Phi x$ is an underdetermined linear system. Nevertheless, Candès et al. [3] and Donoho [6] show that a sparse signal can be reconstructed from few measurements by solving an optimization problem. In [4], Candès and Tao provide a criterion for sensing matrices to guarantee a unique reconstruction of sparse signals which is named restricted isometry property (RIP). A signal $x$ is said to be $k$-sparse if $x$ has at most $k$ nonzero entries. An $m \times n$ matrix $\Phi$ is said to satisfy the RIP of order $k$ if there is a constant $0 \leq \delta_k < 1$ such that

$$(1 - \delta_k) \|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1 + \delta_k) \|x\|_2^2$$

holds for all $k$-sparse signals $x \in \mathbb{R}^n$. The smallest nonnegative number $\delta_k$ is called the restricted isometry constant (RIC). If the sensing matrix $\Phi$ satisfies the RIP, then a unique reconstruction of the sparse signal is possible. In [2], Bourgain et al.

2010 Mathematics Subject Classification: Primary: 11T71, 14G50; Secondary: 92C55, 11R58, 14H50.

Key words and phrases: Compressed sensing, coherence, algebraic-geometric code, minimum distance.

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2012R1A1A1015609).

©2016 AIMS
give a criterion for a matrix to satisfy the RIP using the notion of coherence. The coherence of a matrix $\Phi$ with columns $a_1, \ldots, a_n$ is
\[
\mu(\Phi) = \max_{i \neq j} \frac{|\langle a_i, a_j \rangle|}{\|a_i\|_2 \cdot \|a_j\|_2}, \quad \text{for } 1 \leq i, j \leq n.
\]
We now give the criterion that was given in [2].

**Theorem 1.1** ([2, Proposition 1]). If the coherence of the matrix $\Phi$ is $\mu$, then the matrix $\Phi$ satisfies the RIP of order $k$ with constant $\delta = (k - 1)\mu$.

Although a random matrix satisfies the RIP of order $k$ with high probability, there is no efficient algorithm that verifies whether a random matrix satisfies the RIP or not. Also, storing the random matrix requires a lot of storage space. To overcome these drawbacks, deterministic construction is inevitable. In [5], DeVore introduce a deterministic construction of sensing matrices using polynomials over finite fields. In [12], Li et al. generalize DeVore’s construction to algebraic curves over finite fields. They show that
\[
\mu(\Phi) \leq \deg G |P|,
\]
where $P$ is a set of rational points on an algebraic curve $X$ and $G$ is a divisor of $X$ such that supp($G$) \cap $P$ = $\emptyset$, and by computing the upper bound of coherence for appropriate curves obtain better sensing matrices than DeVore’s sensing matrices. In this paper, we prove that
\[
\mu(\Phi) = 1 - \frac{d(C)}{|P|},
\]
where $d(C)$ is the minimum distance of the AG code $C$, that is, we give the exact value of the coherence in terms of the minimum distance of the AG code and deduce the upper bound given in [12]. Finding the minimum distance of a code is a classical problem in coding theory and extensive research has been done to find the minimum distance of AG codes. In particular, the minimum distance of codes on Hermitian curve is given in [1, 7, 8, 9, 10, 11, 14]. Based on the formulas given in [14], we give formulas for the coherence of the sensing matrices coming from Hermitian two-point codes.

The organization of the paper is as follows. In Section 2, we give some background on AG codes that will be needed in the sequel sections. In Section 3, we review the construction of sensing matrices using algebraic curves over finite fields and give the exact value of the coherence of the sensing matrices. From the exact value of the coherence, we deduce the upper bound of the coherence given by Li et al. [12]. In Section 4, we give formulas for the coherence of the sensing matrices coming from Hermitian two-point codes.

## 2. Background on AG codes

We give the definition of the AG code and some properties. Let $X/\mathbb{F}$ be an algebraic curve (absolutely irreducible, smooth, projective) of genus $g$ over a finite field $\mathbb{F}$. Let $F(X)$ be the function field of $X/\mathbb{F}$ and let $\Omega(X)$ be the module of rational differentials of $X/\mathbb{F}$. Given a divisor $A$ on $X$ defined over $\mathbb{F}$, let $L(A)$ denote the vector space over $\mathbb{F}$ of functions $f \in F(X) \setminus \{0\}$ with $(f) + A \geq 0$ together with the zero function. The dimension of $L(A)$ is denoted by $l(A)$. Let $\Omega(A)$ denote the vector space over $\mathbb{F}$ of differentials $\omega \in \Omega(X) \setminus \{0\}$ with $(\omega) \geq A$ together with
the zero differential. Let $K$ represent the canonical divisor class. For $n$ distinct rational points $P_1, \ldots, P_n$ on $X$ and for disjoint divisors $D = P_1 + \cdots + P_n$ and $G$, the algebraic-geometric codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\alpha_L : L(G) \to \mathbb{F}^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)),$$

$$\alpha_\Omega : \Omega(G - D) \to \mathbb{F}^n, \quad \omega \mapsto (\text{Res}_{P_1}(\omega), \ldots, \text{Res}_{P_n}(\omega)).$$

The maps establish isomorphisms $L(G)/L(G - D) \simeq C_L(D, G)$ and $\Omega(G - D)/\Omega(G) \simeq C_\Omega(D, G)$. If $G = aQ$ is a multiple of some rational point $Q$ and $D$ is the sum of all the other rational points, then the codes $C_L(D, G)$ and $C_\Omega(D, G)$ are called one-point codes. If $G = a_1Q_1 + \cdots + a_mQ_m$ for $m$ distinct rational points $Q_1, \ldots, Q_m$ and $D$ is the sum of all the other rational points, then the codes $C_L(D, G)$ and $C_\Omega(D, G)$ are called $m$-point codes. The codes $C_L(D, G)$ and $C_\Omega(D, G)$ are dual to each other, that is, $C_\Omega(D, G) = C_L(D, G)^\perp$. The following theorem shows that $C_\Omega(D, G)$ can be represented as $C_L(D, G)$ with an appropriate divisor.

**Theorem 2.1** ([15, Proposition 2.2.10]). Let $\eta$ be a Weil differential such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for $i = 1, \ldots, n$. Then

$$C_L(D, G)^\perp = C_\Omega(D, G) = C_L(D, H) \text{ with } H = D - G + (\eta),$$

where $v_{P_i}(\eta)$ is the valuation of $\eta$ at $P_i$ and $\eta_{P_i}$ is a local component of $\eta$ at $P_i$.

The next theorem gives the parameters of $C_L(D, G)$.

**Theorem 2.2** ([15, Theorem 2.2.2]). $C_L(D, G)$ is an $[n, k, d]$ code with parameters

$$k = l(G) - l(G - D) \text{ and } d \geq n - \deg G.$$

3. MAIN RESULT

We review the construction of sensing matrices using algebraic curves over finite fields and find the values of the coherence of the sensing matrices coming from algebraic curves. Let $q$ be a prime power and let $X$ be an algebraic curve over a finite field $\mathbb{F}_q$. Let $P$ be a set of rational points on $X$ and let $G$ be a divisor of $X$ such that $\deg G < |P|$ and $\text{supp}(G) \cap P = \emptyset$. For each $f \in L(G)$, define the column vector $v_f$ whose entries are indexed by the pairs in $P \times \mathbb{F}_q$. Denote the entry indexed by $(P, a) \in P \times \mathbb{F}_q$ as $f_{P,a}$. Then we take $f_{P,a}$ as follows:

$$f_{P,a} = \begin{cases} 1, & \text{if } f(P) = a \\ 0, & \text{otherwise} \end{cases}$$

The column vectors $\{v_f | f \in L(G)\}$ form an $m \times n$ matrix $\Phi_0$, where $m = |P| \times q$ and $n = q^{\deg G}$. Now we state the theorem given by Li et al.

**Theorem 3.1** ([12, Theorem 3.2]). Suppose $\Phi = \frac{1}{\sqrt{|P|}}\Phi_0$. Then $\Phi$ is a sensing matrix with coherence

$$\mu(\Phi) \leq \frac{\deg G}{|P|}.$$

The following theorem gives the exact value of the coherence in terms of the minimum distance of AG codes.

**Theorem 3.2.** Let $\Phi = \frac{1}{\sqrt{|P|}}\Phi_0$. Then $\Phi$ is a sensing matrix with coherence

$$\mu(\Phi) = 1 - \frac{d(C)}{|P|}.$$
Proof. Let \( f, g \in L(G) \) be two distinct functions. Then \( \frac{1}{\sqrt{|P|}} \nu_f \) and \( \frac{1}{\sqrt{|P|}} \nu_g \) are two distinct columns of \( \Phi \) with unit norm. Let \( h = f - g \). Then

\[
\langle \nu_f, \nu_g \rangle = |\{ P \in \mathcal{P} : f(P) = g(P) \}| = |\{ P \in \mathcal{P} : (f - g)(P) = 0 \}| = |\{ P \in \mathcal{P} : h(P) = 0 \}| = |\mathcal{P} - \operatorname{wt}(\alpha_L(h))|.
\]

Thus

\[
\max_{f \neq g} \langle \nu_f, \nu_g \rangle = |\mathcal{P}| - \min \{ \operatorname{wt}(\alpha_L(h)) : 0 \neq h \in L(G) \} = |\mathcal{P}| - d(C).
\]

Hence

\[
\mu(\Phi) = \frac{|\mathcal{P}| - d(C)}{|\mathcal{P}|} = 1 - \frac{d(C)}{|\mathcal{P}|}.
\]

Note that Theorem 3.1 can be deduced from Theorem 3.2 and Theorem 2.2. Since \( d(C) \geq |\mathcal{P}| - \deg G \), we have

\[
\mu(\Phi) = \frac{|\mathcal{P}| - d(C)}{|\mathcal{P}|} \leq \frac{|\mathcal{P}| - (|\mathcal{P}| - \deg G)}{|\mathcal{P}|} = \frac{\deg G}{|\mathcal{P}|}.
\]

4. **Coherence of Sensing Matrix Coming from Hermitian Curve**

Matthews show that for codes on Hermitian curve, there are two-point codes that have better parameters than any comparable one-point codes [13]. For this reason, we will consider Hermitian two-point codes. Let \( X \) be a Hermitian curve defined by \( y^q + y = x^{q^2+1} \) over \( \mathbb{F}_{q^2} \). Then \( X \) has \( q^3 + 1 \) rational points and the genus is \( q(q - 1)/2 \). We denote by \( P_0 \) the point \((0,0)\) and by \( P_\infty \) the point at infinity. The canonical divisor \( K \) of a Hermitian curve is \( K = (q - 2)H \), where \( H \sim (q+1)P_\infty \sim (q+1)P_0 \). The action of the automorphism group of the Hermitian curve on the set of its rational points is doubly transitive, and therefore without loss of generality it can be assumed that the support of a two-point divisor consists of \( P_0 \) and \( P_\infty \). Let \( G = aP_\infty + bP_0 \) and \( D = P_1 + \cdots + P_n \) be divisors of \( X \), where \( \operatorname{supp}(G) \cap \operatorname{supp}(D) = \emptyset \) and \( P_1, \ldots, P_n \) are pairwise distinct. Then \( C_L(D, G) \) and \( C_\Omega(D, G) \) are Hermitian two-point codes. We state the formulas for the minimum distance of Hermitian two-point codes given in [14]. The formulas give the minimum distance of the Hermitian two-point codes for all ranges of \( G \). The ranges are divided into two parts as follows:

1. \( \{ G : \deg G > \deg K + q \} \cup \{ G : \deg K \leq \deg G \leq \deg K + q \land G \sim sP_\infty \land G \sim tP_0 \} \) and

2. \( \{ G : \deg G < \deg K \} \cup \{ G : (\deg K \leq \deg G \leq \deg K + q) \land (G \sim sP_\infty \lor G \sim tP_0) \} \), where \( s, t \in \mathbb{Z} \).

**Theorem 4.1** ([14, Theorem 6.5]). Let \( G = K + aP_\infty + bP_0 \), where \( K \) is a canonical divisor,

\[
a = a_0(q + 1) - a_1, \quad 0 \leq a_1 \leq q, \quad b = b_0(q + 1) - b_1, \quad 0 \leq b_1 \leq q.
\]

Let \( d^* = \deg(G) - (2g - 2) = a + b \). Suppose that \( G \) satisfies either
Theorem 4.2 ([14, Theorem 6.6]). Let \( G = aP_{\infty} + bP_0 \) with
\[
\begin{align*}
  a &= a_0(q + 1) + a_1, \ 0 \leq a_1 \leq q, \\
  b &= b_0(q + 1) + b_1, \ 0 \leq b_1 \leq q.
\end{align*}
\]
Suppose that \( G \) satisfies either
(1) \( \deg G < \deg K \) or
(2) \( \deg K \leq \deg G \leq \deg K + q \) with \( G \sim sP_{\infty} \) or \( G \sim tP_0 \) for all \( s, t \in \mathbb{Z} \),
then
\[
d(C(D, G)^\perp) = a_0 + b_0 + 2.
\]

We give the formulas for the coherence of the sensing matrices coming from the Hermitian two-point code.

Theorem 4.3. Let \( G = K + aP_{\infty} + bP_0 \), where \( K \) is a canonical divisor,
\[
\begin{align*}
  a &= a_0(q + 1) - a_1, \ 0 \leq a_1 \leq q, \\
  b &= b_0(q + 1) - b_1, \ 0 \leq b_1 \leq q.
\end{align*}
\]
Let \( d^* = \deg(G) - (2q - 2) = a + b \).
Suppose that \( G \) satisfies either
(1) \( \deg G > \deg K + q \) or
(2) \( \deg K \leq \deg G \leq \deg K + q \) and \( G \sim sP_{\infty} \) and \( G \sim tP_0 \) for all \( s, t \in \mathbb{Z} \),
then the coherence of the sensing matrix \( \Phi \) coming from \( C_L(D, G)^\perp \) is
\[
\mu(\Phi) = 1 - \frac{d^* + \max\{0, a_1 - (a_0 + b_0), b_1 - (a_0 + b_0), a_1 + b_1 - 2(a_0 + b_0)\}}{q^3 - 1},
\]
except for the case when \( (a_0 + b_0 < a_1, b_1) \) and \( a_1 = q, b_1 = q \), for which
\[
\mu(\Phi) = 1 - \frac{d^* + q - (a_0 + b_0)}{q^3 - 1}.
\]

Theorem 4.4. Let \( G = aP_{\infty} + bP_0 \) with
\[
\begin{align*}
  a &= a_0(q + 1) + a_1, \ 0 \leq a_1 \leq q, \\
  b &= b_0(q + 1) + b_1, \ 0 \leq b_1 \leq q.
\end{align*}
\]
Suppose that \( G \) satisfies either
(1) \( \deg G < \deg K \) or
(2) \( \deg K \leq \deg G \leq \deg K + q \) with \( G \sim sP_{\infty} \) or \( G \sim tP_0 \) for some \( s, t \in \mathbb{Z} \),
then the coherence of the sensing matrix \( \Phi \) coming from \( C_L(D, G)^\perp \) is
\[
\mu(\Phi) = 1 - \frac{a_0 + b_0 + 2}{q^3 - 1},
\]
We give a toy example in the following.
Example 4.5. Let $X$ be a Hermitian curve defined by $y^8 + y = x^9$ over $\mathbb{F}_{64}$. Then the genus of the curve is 28 and the canonical divisor $K = 54P_{\infty} \sim 54P_0$. There are 513 rational points on $X$. If $G = 82P_{\infty} + 27P_0$ and $D$ is the sum of all the other rational points on $X$, then the minimum distance of $C_L(D, G)_{\perp}$ is 56. By Theorem 2.1, $C_L(D, G)_{\perp} = C_L(D, H)$, where $H = 448P_{\infty} + 8P_0$. The dimension of the Riemann-Roch space $L(448P_{\infty} + 8P_0)$ is 429. By Theorem 3.2, the coherence of the $511 \cdot 64 \times 64$ sensing matrix $\Phi$ coming from Hermitian two-point code $C_L(D, H)$ is

$$\mu(\Phi) = 1 - \frac{56}{511} = \frac{455}{511} \leq \frac{456}{511}.$$  

If $G = 56P_{\infty} + 2P_0$ and $D$ is the sum of all the other rational points on $X$, then the minimum distance of $C_L(D, 501P_{\infty} + 6P_0) = C_L(D, G)_{\perp}$ is 14. The dimension of the Riemann-Roch space $L(501P_{\infty} + 6P_0)$ is 480. The coherence of the $511 \cdot 64 \times 64$ sensing matrix $\Phi$ coming from Hermitian two-point code $C_L(D, 501P_{\infty} + 6P_0)$ is

$$\mu(\Phi) = 1 - \frac{14}{511} = \frac{497}{511} \leq \frac{507}{511}.$$  

In [12], Li et al. construct sensing matrices from Hermitian one-point codes and improve the upper bound of the coherence of the DeVore’s sensing matrices. They compute the upper bound of the coherence using Theorem 3.1. In the next example, we use Theorem 3.2 to compute the coherence of the matrices constructed in [12] and compare the values of coherence obtained by both theorems.

Example 4.6. Let $X$ be a Hermitian curve defined by $y^{16} + y = x^{17}$ over $\mathbb{F}_{256}$. Then the genus of the curve is 120 and there are 4097 rational points on $X$. If $G = 4077P_{\infty}$ and $D$ is the sum of all the other rational points on $X$, then $C_L(D, G)$ is a $[4096, 3958, 32]$ code. By Theorem 3.2, the coherence of the $1048576 \times 256$ sensing matrix $\Phi$ coming from Hermitian one-point code $C_L(D, G)$ is

$$\mu(\Phi) = 1 - \frac{32}{4096} = \frac{4064}{4096} \leq \frac{4077}{4096}.$$  

If $G = 4087P_{\infty}$ and $D$ is the sum of all the other rational points on $X$, then $C_L(D, G)$ is a $[4096, 3968, 16]$ code. By Theorem 3.2, the coherence of the $1048576 \times 256$ sensing matrix $\Phi$ coming from Hermitian one-point code $C_L(D, G)$ is

$$\mu(\Phi) = 1 - \frac{16}{4096} = \frac{4080}{4096} \leq \frac{4087}{4096}.$$  

Theorem 3.2 states that we can improve the upper bound of the coherence of the sensing matrices coming from AG codes by improving the lower bound for the minimum distance of the AG codes. In [16], Xing and Chen show that by choosing specific divisors for the Hermitian codes, it is possible to improve the minimum distance of the Hermitian one-point codes. In Table 1, we give the parameters for the Hermitian one-point codes used in Example 4.6 and the parameters for the Improved Hermitian codes given by Xing and Chen. By applying Theorem 3.2 to

| Hermitian one-point codes | Improved Hermitian codes |
|--------------------------|--------------------------|
| [4096, 3958, 32]         | [4096, 3958, ≥ 64]       |
| [4096, 3968, 16]         | [4096, 3968, ≥ 59]       |

Table 1. Parameters of codes over $\mathbb{F}_{256}$.
the Improved Hermitian codes, we improve the bound of the coherence given by Li et al in [12]. In Table 2, we give the upper bound or the exact value of the coherence. For comparison we use the matrix of the same size. Also we denote the theorems used to compute the upper bound of the coherence.

| Size of the matrix | Hermitian one-point codes | Improved Hermitian codes |
|--------------------|---------------------------|---------------------------|
|                    | Theorem 3.1               | Theorem 3.2               | Theorem 3.2               |
| $1048576 \times 256^{3958}$ | $\leq 4077$ | $4064$ | $\leq 4096$ |
| $1048576 \times 256^{3968}$ | $\leq 4087$ | $4080$ | $\leq 4096$ |

Table 2. Comparison of the coherence of the matrices

5. Conclusion

The deterministic constructions of the sensing matrices are far from being optimal and to close this gap we need to find sensing matrices with smaller coherence. In this paper, we give the exact value of the coherence of the sensing matrices coming from AG codes in terms of the minimum distance of AG codes. Thus the value of the coherence can be computed by computing the minimum distance of the AG code. To get a small value of the coherence we need to find an AG code with large minimum distance which is a central problem in coding theory.

References

[1] P. Beelen, The order bound for general algebraic geometric codes, *Finite Fields Appl.*, 13 (2007), 665–680.
[2] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin and D. Kutzarova, Explicit constructions of RIP matrices and related problems, *Duke Math. J.*, 159 (2011), 145–185.
[3] E. J. Candès, J. Romberg and T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, *IEEE Trans. Inf. Theory*, 52 (2006), 489–509.
[4] E. J. Candès and T. Tao, Decoding by linear programming, *IEEE Trans. Inf. Theory*, 51 (2005), 4203–4215.
[5] R. A. DeVore, Deterministic constructions of compressed sensing matrices, *J. Complexity*, 23 (2007), 918–925.
[6] D. L. Donoho, Compressed sensing, *IEEE Trans. Inf. Theory*, 52 (2006), 1289–1306.
[7] M. Homma and S. J. Kim, Toward the determination of the minimum distance of two-point codes on a Hermitian curve, *Des. Codes Crypt.*, 37 (2005), 111–132.
[8] M. Homma and S. J. Kim, The complete determination of the minimum distance of two-point codes on a Hermitian curve, *Des. Codes Crypt.*, 40 (2006), 5–24.
[9] M. Homma and S. J. Kim, The two-point codes on a Hermitian curve with the designed minimum distance, *Des. Codes Crypt.*, 38 (2006), 55–81.
[10] M. Homma and S. J. Kim, The two-point codes with the designed distance on a Hermitian curve in even characteristic, *Des. Codes Crypt.*, 39 (2006), 375–386.
[11] C. Kirfel and R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Inf. Theory*, 41 (1995), 1720–1732.
[12] S. Li, F. Gao, G. Ge and S. Zhang, Deterministic construction of compressed sensing matrices via algebraic curves, *IEEE Trans. Inf. Theory*, 58 (2012), 5035–5041.
[13] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, *Des. Codes Crypt.*, 22 (2001), 107–121.
[14] S. Park, Minimum distance of Hermitian two-point codes, *Des. Codes Crypt.*, 57 (2010), 195–213.
[15] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd edition, Springer-Verlag, Berlin, 2009.
[16] C. P. Xing and H. Chen, Improvements on parameters of one-point AG codes from Hermitian curves, *IEEE Trans. Inf. Theory*, 48 (2002), 535–537.

Received for publication September 2014.

*E-mail address:* skpark@sookmyung.ac.kr