Construction of a Class of Algebraic-Geometric Codes via Gröbner Bases

Changyan Di, Zhuojun Liu
Institute of Systems Science
Academia Sinica, Beijing (100080), P. R. China
Email: {cdi,zliu}@mmrc.iss.ac.cn

Abstract. In this paper, a class of algebraic-geometric codes from affine varieties are constructed. This construction is presented via Gröbner bases computation. In particular, we can get some algebraic-geometric codes more efficient than the current algebraic geometric codes.

1. Introduction

The theory of algebraic-geometric codes is a fascinating topic where two extremes meet: the highly abstract and deep mathematics of modular curves and the very concrete problems in the engineering of the information transmission.

Algebraic curves over finite fields were used by Goppa [1], [2], [3] to construct codes. Nowadays these codes are called geometric Goppa codes or algebraic-geometric codes. At the beginning of 1980’s, Tsfasman, Vladut, and Zink proved the existence of curves over finite fields with many rational points, giving asymptotically good codes [4]. Since then, many papers dealing with algebraic-geometric codes and decoding procedure have followed. In [5], Feng and Rao presented a construction of improved geometric Goppa codes which are more efficient than the current geometric Goppa codes for some cases. In this paper, we construct a class of algebraic-geometric codes from affine varieties via Gröbner bases computation. Our construction meets the same results in [6].

First we give the definition of algebraic-geometric codes. Let $\mathcal{X}$ be a smooth, irreducible projective curve defined over the finite field $F_q$, $P_1, P_2, \cdots, P_n$ are distinct rational points on $\mathcal{X}$, $D$ is divisor $P_1 + P_2 + \cdots + P_n$. $G$ is another divisor with $supp(G) \cap supp(D) = \emptyset$.

Let $L(G)$ be the vector space of rational functions on $\mathcal{X}$ with poles and zeroes bounded by $G$:

$$L(G) := \{ f \in F_q(\mathcal{X})^* : (f) + G \geq 0 \} \cup \{0\}.$$
Definition 1.1 Let $\psi_L$ be a map:

$$\psi_L : L(G) \rightarrow F^n_q$$

$$f \mapsto (f(P_1), f(P_2), \ldots, f(P_n))$$

The image of the linear map $\text{Im}(\psi_L)$ is called the geometric Reed-Solomon code, denoted by $C_L(D, G)$.

Definition 1.2 We simply define the geometric Goppa code $C_\Omega(D, G)$ as the dual code of $C_L(D, G)$, i.e.,

$$C_\Omega(D, G) = C_L^\perp(D, G).$$

The parameters of $C_L(D, G)$ and $C_\Omega(D, G)$ can be easily estimated by applying Riemann-Rock theorem\cite{Riemann-Rock}, we have the following proposition:

Proposition 1.1 \cite{Riemann-Rock} if $2g - 2 < \deg(G) < n$, the geometric Reed-Solomon code $C_L(D, G)$ has dimension $k = \deg(G) - g + 1$, $d \geq n - \deg(G)$; the geometric Goppa code has dimension $k = n - \deg(G) + g - 1$, $d \geq \deg(G) - 2g + 2$.

Since $C_L(D, G)$ and $C_\Omega(D, G)$ are dual codes, any $k$ linearly independant codewords of $C_L(D, G)$ can be constructed as a parity check matrix of the code $C_\Omega(D, G)$. In this paper, we will consider the construction of a class of algebraic-geometric codes defined by the parity check matrixes consisting of $k$ linearly independant codewords of $C_L(D, G)$. For some cases, this new class of algebraic-geometric codes have the better parameters than the geometric Goppa codes.

The paper is organized as follows. In the next section, for easy reference, we include the knowledge of computer algebra and Gröbner bases. In Section 3, we present our construction of algebraic-geometric codes. In Section 4, two examples are given, one is the improved Klein code, the other is the improved Hermitian code.

2. Gröbner Bases

Application of symbolic algebraic techniques to problems in coding theory have been considered for instance in \cite{Gröbner1}, \cite{Gröbner2} and \cite{Gröbner3}. The theory of Gröbner bases for polynomial ideals is one particularly powerful tool in this area. As a general reference, we suggest \cite{Gröbner4}. For the convenience of the reader, we give a brief exposition of Gröbner bases that are needed here. Let $F$ be any field, and consider the ring $F[X] = F[x_1, x_2, \ldots, x_m]$ of polynomials in $m$ variables over the field $F$. A monomials is a product of powers of variables $x_1^{i_1} \cdots x_m^{i_m}$. Monomial orders such as Lexicographical Order, Inverse Lexicographical Order and Total Degree Order are well defined in \cite{Gröbner4}. In the following, we define Weighted Lexicographical Order. First we present the definition of weight of monomial.
Definition 2.1 For each monomial $x_1^{i_1} \cdots x_m^{i_m}$, we let $\omega(x_\mu), \mu = 1, \cdots, m$ be the weight of $x_\mu, \mu = 1, \cdots, m$ respectively. We use lexicographical order

$$x_m \prec_L x_{m-1} \prec_L \cdots \prec_L x_1$$

The weight of monomial

$$\omega(x_1^{i_1} \cdots x_m^{i_m}) = \sum_{\mu=1}^m i_\mu \omega(x_\mu).$$

Definition 2.2 Consider any two monomials $x_1^{i_1} \cdots x_m^{i_m}$ and $x_1^{j_1} \cdots x_m^{j_m}$, using lexicographical order

$$x_m \prec_L x_{m-1} \prec_L \cdots \prec_L x_1$$

we can define Weighted Lexicographical Order of monomials and use a notation $\prec_\omega$.

Weighted Lexicographical Order:

$$x_1^{i_1} \cdots x_m^{i_m} \prec_\omega x_1^{j_1} \cdots x_m^{j_m}$$

if (1) $\omega(x_1^{i_1} \cdots x_m^{i_m}) < \omega(x_1^{j_1} \cdots x_m^{j_m})$,

or (2) $\omega(x_1^{i_1} \cdots x_m^{i_m}) = \omega(x_1^{j_1} \cdots x_m^{j_m})$,

$$x_1^{i_1} \cdots x_m^{i_m} \prec_L x_1^{j_1} \cdots x_m^{j_m}.$$ 

Let $F_q$ be a finite field, suppos $I$ is an ideal in the ring $F_q[x_1, x_2, \cdots, x_m]$, define

$$I_q = I + (x_1^q - x_1, \cdots, x_m^q - x_m).$$

Then $I_q$ is a radical ideal[?]. Let $V(I_q)$ be the variety of $I_q$. $F_q[x_1, x_2, \cdots, x_m]/I_q$ is called the coordinate ring of $I_q$. It is important to know that the dimension of the coordinate ring $F[x_1, x_2, \cdots, x_m]/I_q$ equals to the numeber of the elements of $V(I_q)$.

Proposition 2.1[?] $\dim F_q[x_1, \ldots, x_m]/I_q = |V(I_q)|$.

Macaulay’s theorem provides an efficient way to compute the monomial basis of $F[x_1, \ldots, x_m]/I$ which we need later.

Theorem 2.2 (Macaulay) [?] Let $\prec_\omega$ be a monomial order on $F[x_1, \ldots, x_m]$ and $B$ be a Gröbner basis of $I$. Then $\{ \prod_{i=1}^m x_i^{\alpha_i} | \forall f \in B, \text{lm}(f) \text{ is not a factor of } \prod_{i=1}^m x_i^{\alpha_i} \}$ is monomial basis of $F[x_1, \ldots, x_m]/I$, where $\text{lm}(f)$ is the leading monomial of $f$.

Remark 2.3 A software package WGBASIS on MapleV has been produced to calculate the Gröbner Bases with respect to weighted lexicographical order over finite fields.
3. New Construction of AG codes

Before giving the construction of a class of algebraic-geometric codes, we give a brief review of the notation and concepts from algebraic geometry we shall need later. We concentrate mainly on affine variety, since our goal is to construct algebraic-geometric codes from affine varieties.

Let \( F_q \) be the finite field with \( q \) elements. For any ideal \( I \) in the ring \( F_q[x_1,\ldots,x_m] \) of polynomials, define the variety of \( I, V(I) \), to be the set of \( m \)-tuples \( P \in F_q^m \) such that \( f(P) \) evaluates to zeroes for every \( f \in I \). A set \( \mathcal{X} \) of the form \( \mathcal{X} = V(I) \) for some ideal \( I \) in the ring \( F_q[x_1,\ldots,x_m] \) is called an affine variety defined over \( F_q \). Corresponding to any affine variety \( \mathcal{X} \) is the ideal \( I(\mathcal{X}) \) consisting of the set of polynomials \( f(x_1,\ldots,x_m) \) which vanish at every point of \( \mathcal{X} \). An affine variety is irreducible if it cannot be decomposed into two unions \( \mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 \) of two proper subvarieties \( \mathcal{X}_1 \) and \( \mathcal{X}_2 \). The ring \( F_q[x_1,\ldots,x_m]/I(\mathcal{X}) \) is called the coordinate ring of \( \mathcal{X} \). Assuming that \( \mathcal{X} \) is irreducible, the coordinate ring \( F_q[x_1,\ldots,x_m]/I(\mathcal{X}) \) is an integral domain.

Following is the our construction of AG codes from affine varieties. Feng and Rao proposed the definition of well-behaving sequence and the construction [2.1]. We follow their notation and give a construction of well-behaving sequence.

Let \( V \) be a variety defined by \( (g_1, g_2, \ldots, g_l) \) with \( g_i \in F_q[x_1,\ldots,x_m], i = 1,\ldots,l \). Suppose we can find a weight of variables, \( \omega(x_\mu) \) for \( 1 \leq \mu \leq m \), they must be consistent, i.e., for each polynomial \( g_i, i = 1,\ldots,l \), there are at least two monomial terms having the same maximal weight. Let \( H = \{h_1, h_2, \ldots, h_n\} \) be a linear independent monomial sequence with \( h_i \prec h_{i+1}, i = 1,\ldots,n, L(r) \) denotes the linear space over \( F_q \) spanned by the monomials \( h_1, h_1, \ldots, h_r, \) define \( h_{i,j} = h_i \ast h_j \).

**Definition 3.1** [?] Let \( h_{i,j} \) be a monomial with 

\[
\omega(h_i) + \omega(h_j) \leq \omega(h_n)
\]

and \( h_{i,j} \in L(r+1) - L(r) \) and \( \omega(h_{i,j}) = \omega(h_{r+1}) \). For any \( (u, v) < (i,j), r' < r + 1 \), provided

\[
h_{u,v} \in L(r') - L(r' - 1).
\]

Then \( h_{i,j} \) is referred to as a well-behaving term of \( H \), or is called a well-behaving term consistent with \( h_{r+1} \).

**Definition 3.2** [?] Let \( H \) be defined as above. For each monomial \( h_{i,j} \) with

\[
\omega(h_i) + \omega(h_j) \leq \omega(h_n)
\]

let

\[
h_{i,j} \in L(r+1) - L(r).
\]

We have \( h_{r+1} \prec \omega h_{i,j} \) or \( \omega(h_{r+1}) = \omega(h_{i,j}) \). Then, \( H \) is called a well-behaving sequence of the variety \( V \).
We construct the well-behaving sequence by using Gröbner Bases. For any variety $V$ defined by $(g_1, g_2, \ldots, g_l)$ with $g_i \in F_q[x_1, \ldots, x_m], i = 1, \ldots, l$, let

$$ I = (g_1, g_2, \ldots, g_l, x_q^i - x_1, \ldots, x_q^m - x_m), $$

we calculate the Gröbner Basis of $I$ with respect to weighted lexicographical order. With Macaulay theorem, we can get a monomial basis of $F_q[x_1, \ldots, x_m]/I$. Ordering the monomial basis with respect to weighted lexicographical order, we can get a monomial sequence $H$. From Theorem 2.1 [?], it is easy to prove that $H$ is a well-behaving sequence.

Algorithm 3.1 Algorithm for getting $H$ sequence.

Input : $g_1, g_2, \ldots, g_l$;  
Output : $H = \{h_1, \ldots, h_n\}$.

Step 1) Let $I = (g_1, g_2, \ldots, g_l, x_q^i - x_1, \ldots, x_q^m - x_m)$, $X = [x_1, x_2, \ldots, x_m]$ induces the ordering $x_1 > x_2 > \ldots > x_m$, $W = [\omega(x_1), \ldots, \omega(x_m)]$ be the weight list of $x_1, \ldots, x_m$.

Calculate the Gröbner basis $B = \text{wgbasis}(I, X, W)$.

Step 2) find the monomial base of $F_q[x_1, \ldots, x_m]/I$ and order it with the weighted lexicographical order, then get $H$.

stop.

Once we find well-behaving sequence $H$, we can use Construction2.1 [?] to get our new AG codes. The estimation of the parameters of these codes needs the concept of $N$ sequence.

Definition 3.3 [?] $N(h_r) = N_r$ = the number of $h_{i,j}$ which are consistent with $h_r$, and are well-behaving. The sequence $(N_1, N_2, N_3, \ldots)$ is called the $N$ sequence.

With the information, the parameters can be determined by Theorem 2.2 [?].

4. Examples

Example 4.1 Consider **Klein** quartic :

$$ X^3 * Y + Y^3 + X = 0 \text{ over } F_8. $$

Assign weights $\omega(x) = 2, \omega(y) = 3, y \prec_L x$,

$$ \text{wgbasis}\{x^3y + y^3 + x, x^8 + x, y^8 + y\}, [x, y], [2, 3] $$
From Macaulay Theorem, we get the basis of $F_8[x, y]/(x^3y + y^3 + x, x^8 + x, y^8 + y)$,

$$\{1, x, y, x^2, xy, y^2, x^2y, y^3, x^3y, y^4, x^3y^2, xy^3, y^5, x^4y, y^6, x^4y^2, xy^3, y^7, x^5y, y^8, x^5y^2, xy^4, y^9, x^6y, y^{10}, x^6y^2, xy^5, y^{11}, x^7y, y^{12}, x^7y^2, xy^6, y^{13}, x^8y, y^{14}, x^8y^2, xy^7, y^{15}, x^9y, y^{16}, x^9y^2, xy^8, y^{17}, x^{10}y, y^{18}, x^{10}y^2, xy^9, y^{19}, x^{11}y, y^{20}, x^{11}y^2, xy^{10}, y^{21}, x^{12}y, y^{22}, x^{12}y^2, xy^{11}, y^{23}, x^{13}y, y^{24}, x^{13}y^2, xy^{12}, y^{25} \}$$

After modifying the basis we get the H sequence as follows:

$$H = \{1, y, xy, y^2, x^2y, x^2y^2, xy^3, y^4, x^3y, y^5, x^4y, y^6, x^5y, y^7, x^6y, y^8, x^7y, x^8y \}$$

$$\dim F_8[x, y]/(x^3y + y^3 + x, x^8 + x, y^8 + y) = |H| = 22.$$  

Its weight sequence

$$W^* = \{0, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 \}.$$

The $N$ sequence

$$N^* = \{1, 2, 2, 3, 2, 4, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 \},$$

$V = \{P_1, \ldots, P_{22} \}$ is the rational point set of Klein quartic curve over $F_8$. Using $H_3^* = (1, xy, |x^2y|^T)$ as the parity check matrix, we get improved Klein code $[22, 18, 3]_8$, while the geometric Goppa code is $[22, 17, 3]_8$.

**Example 4.2** We consider the generalized Hermitian curve:

$$\begin{cases} 
  z^3 + y^2 + y = 0 \\
  y^3 + x^2 + x = 0
\end{cases} \quad \text{over } F_4.$$

Assign weights $\omega(x) = 9, \omega(y) = 6, \omega(z) = 4, z \prec_L y \prec_L x$.

$$\text{wgbasis}\{z^3 + y^2 + y, y^3 + x^2 + x, x^3 + y^4 + y, z^4 + z\}, [x, y, z], [9, 6, 4])$$

$$= \{z^3 + y^2 + y, z^4 + z, z^2 + z^3 + x^2 + y \}.$$

$$H = \{1, z, y, z^2, x, zy, z^3, z^2y, yz, z^2x, z^3y, z^2yx, z^3yx \}$$

Its weight sequence

$$W^* = \{0, 4, 6, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 27 \}.$$

The $N$ sequence

$$N^* = \{1, 2, 2, 3, 2, 4, 5, 6, 9, 8, 10, 12, 16 \},$$

$V = \{P_1, \ldots, P_{16} \}$ is all the rational points of the generalized Hermitian curve over $F_4$. Using $H_3^* = (1, z, y|x)^T$ as parity check matrix, we get improved Hermitian code $[16, 12, 3]_4$, while the geometric Goppa code is $[16, 8, 3]_4$.

Using $H_3^* = (1, z, y, z^2, x, zy|zx, xy)^T$ as parity check matrix, we get improved Hermitian code $[16, 8, 5]_4$, while the geometric Goppa code is $[16, 6, 5]_4$. 
References