Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 299–304*

A family of codes on projective surface

Kouichi Sibaki shibaki@iwate-pu.ac.jp
Department of Management Information Science, Miyako college of Iwate Prefectural University, 1-5-1, Kanan Miyoko-shi, Iwate, 027-0039, Japan
Kiyoshi Nagata nagata@ic.daito.ac.jp
Department of Business Informatics, Daito Bunka University,
1-9-1, Takashimadaira, Itabashi-ku, Tokyo, 175-8571, Japan

Abstract. As an extension of Reed-Solomon Code, Goppa had proposed to use a family of fractional functions for constructing the so-called classical Goppa code in 1970. Goppa continued to investigate the relationship between error correcting codes and algebraic curves, and extended his idea to obtain the codes on algebraic curves. After the moment of his works, the research on algebraic geometric codes has been developed and several important results are published both in theoretical and in practical point of view. One of the most theoretical results in construction of code is codes on a projective scheme X over $\mathbb{F}_q$ defined using the germ map. In case of X being a projective surface, Hansen gave a lower bound of the minimum distance of codes defined on some irreducible curves with $\mathbb{F}_q$-rational points. In this paper, we propose a concrete construction of that type of codes over the typical projective surface $\mathbb{P}^2$, then give the dimension and a lower bound of the minimum distance which is better than Hansen's estimation in some cases.

1 Introduction

For a fixed integers k, n with $k \leq n \leq q$, and for a subset $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q$, Reed-Solomon Code is defined as the image of the subset of polynomials of $\mathbb{F}_q[X]$ with degree less than k into $\mathbb{F}_q^n$ under the map of substituting all the x_i to each polynomial. Although Reed-Solomon code is optimal in the sense of Singleton bound criteria and called maximum distance separable (MDS) code, the length of the code can not exceed the number of the elements of the base field. In 1970, V. D. Goppa had proposed to use a family of fractional functions for constructing the so-called classical Goppa code ([3]). Goppa continued to investigate the relationship between error correcting codes and algebraic curves, and extended his idea to obtain the codes on algebraic curves([4]).

The landmark of his work aroused many researchers to investigate the algebraic geometric codes, and several important results have been published both in theoretical and in practical point of view. One of important results is the existence of an infinite sequence of algebraic geometric codes which exceed the Varshamov-Gilbert bound. These codes are constructed using modular curves over a finite field $\mathbb{F}_q$ ([2]).

In view of construction of code, the most general definition is by the germ map which corresponds each global section of an invertible sheaf on a projective scheme X to an element of $\mathbb{F}_q^n$. In case that X is a projective surface, Hansen, in [5], gave a lower bound of the minimum distance of codes defined by some irreducible curves and an invertible sheaf corresponding to a divisor. For more practical use, it might be necessary to obtain other important parameters and to investigate much more properties. Lomont and Hansen, in [6], proposed to construct Hansen's type of code on a ruled surface over a non-singular curve of genus g, then gave some parameters. Zampolini, in [8], investigated more restricted case as the genus of the curve $g = 2$.

In this paper, we propose a concrete construction of Hansen's type of codes on the typical projective surface $\mathbb{P}^2$, and give the lower bound of the minimum distance which is better than Hansen's general result. The rest of this paper proceed as follows: an over view of known results and some notes come up in the next section, our proposed construction, estimation of some parameters of the code, and the comparison of our code with Hansen's general estimation are in the following section. Then the conclusion.

2 Overview of some known results

In this section, we start with the classical Goppa code which can be interpreted as a type of generalized Reed-Solomon code. The Reed-Solomon code was an image of polynomials over $\mathbb{F}_q$ of degree less than k, and it is extended to a family of codes whose length n and minimum distance at last $n-k+1$ using fixed vectors $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $v = (v_1, \ldots, v_n)$, where α_i's are distinct elements and v_i's are non-zero elements of $\mathbb{F}_{q^m}$. The generalized Reed-Solomon code, $GRS_k(\alpha, v)$, is defined as a set of all the images of polynomial $f(X)$ of $\mathbb{F}_{q^m}[X]$ with degree less than k, that is

$$(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)).$$

For a polynomial $g(X) \in \mathbb{F}_{q^m}[X]$ with $g(\alpha_i) \neq 0$ $(i = 1, \ldots, n)$, called Goppa polynomial, the classical Goppa code coincide with the restriction of $GRS_{n-r}(\alpha, v)$ to $\mathbb{F}_q^n$ where $r = \deg g(X)$ and $v_i = g(\alpha_i)/\prod_{j \neq i}(\alpha_i - \alpha_j)$ ([7, p.340]). Thus the classical Goppa code is considered as the image of rational function with non-positive degree whose numerator is divisible by the Goppa polynomial and the denominator is a fixed polynomial.

Goppa generalized his result to obtain a family of codes on a non-singular algebraic curve C of genus g defined over $\mathbb{F}_q$. For distinct n number of $\mathbb{F}_q$-rational points $P_1, \ldots, P_n$, put a divisor $D = P_1 + \cdots + P_n$, and let E be any effective divisor such that $(\mathrm{Supp}E) \cap \{P_i\} = \emptyset$, then a functional type geometric Goppa code of length n associated with $C_L(C, D, E)$ is defined as the image of the following map:

$$\Phi_L \ : \ L(C, E) \to \mathbb{F}_q^n, \quad \Phi_L(f) = (f(P_1), \ldots, f(P_n)),$$

where $L(C,E)=\{f \in \mathbb{F}_q(X)^* \mid \mathrm{div}(f)+E \geq 0\}\cup\{0\}$. As the direct consequence of Riemann-Roch theorem, it is shown that if $2(g-1) < \mathrm{deg}E < n$, then the code has dimension $k = \mathrm{dim}E = \mathrm{deg}E - g + 1$ and the minimum distance $d \geq n-k-g+1$. Since the geometric Goppa is a code defined on an algebraic geometric curve, it is natural to extend it to codes on a surface, or on more general object in the algebraic geometry. One of most general definition of this kind of code is a code on projective scheme associated to a set of $\mathbb{F}_q$-rational point $\{P_1,\ldots,P_n\}$ and an invertible sheaf $\mathcal{L}=\mathcal{O}_X(E)$ for a divisor E, [1].

Definition 1. *Let X be a projective scheme over $\mathbb{F}_q$, $\mathcal{L}$ be an invertible sheaf, $\mathcal{P}=\{P_1,\ldots,P_n\}$ be a set of rational points. The germ map is defined by choosing trivialization $\phi : \bar{\mathcal{L}}_{P_i} \cong \mathcal{O}_{P_i}/m_{P_i} = \mathbb{F}_q$ for each i such as*

$$\alpha : \Gamma(X,\mathcal{L}) \to \mathbb{F}_q^n,\ \alpha(s) = (s(P_1),\ldots,s(P_n)),$$

where $s(P_i) := \phi(s_{P_i} + m_{P_i}\mathcal{L}_{P_i}) \in \mathbb{F}_q$ for any $s \in \Gamma(X,\mathcal{L})$.
Then the code on X corresponding to $(\mathcal{P},\mathcal{L})$ is defined as $C(X,\mathcal{P},\mathcal{L}) := \mathrm{Im}(\alpha)$.

Although the definition above seems to be inclusive and all-round, it is too general to calculate some important parameters such as the dimension, the minimum distance etc. Hansen, in [5], considered this type of code in case that X is a projective surface, and gave a lower bound for the minimum distance.

Proposition 1. *(Hansen) Let X be a projective surface over $\mathbb{F}_q$, and let $C_1,\cdots,C_m$ be irreducible curves on X with rational points $\mathcal{P}=\{P_1,\cdots,P_n\}$ such that there exists a positive integer N satisfying $\#C_i(\mathbb{F}_q) \leq N$. Let $\mathcal{L}=\mathcal{O}_X(E)$ be an invertible sheaf corresponding to a divisor E satisfying $E.C_i \geq 0$ for any i.*
Then the code $C(X,\mathcal{P},\mathcal{L})$ has minimal distance $\delta \geq n - lN - \sum_{i=1}^m E.C_i$, where $l = \sup\#\{i \mid \mathrm{Supp}Z(s) \supset C_i\}$ when s ranges in $\Gamma(X,\mathcal{O}_X(E))\backslash\{0\}$. Especially when $E.C_i = \eta \leq N$ for any i, then $\delta \geq n - lN - (m-l)\eta$.

When X is a non-singular projective variety with a local coordinates $\{(U_\lambda,\varphi_\lambda)\}_\lambda$. For the divisor E determined by local equations $R_\lambda(z_\lambda)=0$ on each U_λ, there is a $\mathbb{F}_q$-isomorphism

$$\begin{aligned} \Gamma(X,\mathcal{O}_X(E)) &\to L(X,E) = \{f \in \mathbb{F}_q(X)^* \mid \mathrm{div}(f)+E \geq 0\}\cup\{0\}, \\ s = \{s_\lambda(z_\lambda)\}_\lambda &\mapsto f_s(x) = s_\lambda(\varphi_\lambda(x))/R_\lambda(\varphi_\lambda(x)), \end{aligned}$$

where $s_\lambda = s \circ \varphi_\lambda^{-1}$. We note that this map is well-defined being independent on λ.

Here we also note that when we take $f_s \in L(X,E)$ corresponding to s, $Z(s)$ in the proposition above is identified as $Z(f_s) = \mathrm{div}(\{f_s(\varphi_\lambda^{-1}(z_\lambda))R_\lambda(z_\lambda)\}_\lambda)$ under this isomorphism.

Hansen proposed a family of codes on ruled surface associated to a non-singular curve C, and gave a formula for the dimension of the code related to the dimension of $0th$ oder cohomology, [6]. An explicit formulas for the dimension or the lower bound of δ are given in case of C being $\mathbb{P}^1$ or an elliptic curve by Lomont and Zampolini respectively, [8].

3 Code on $\mathbb{P}^2$

Before giving the definition of our proposed code on $\mathbb{P}^2$, we first mention a proposition on the $0th$ cohomology group $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E))$.

Proposition 2. *Let E be a divisor on $\mathbb{P}^2$ over $\mathbb{F}_q$, and express $E = E^+ - E^-$ with two effective divisors which has no common factors. Then*

1. *There exists homogeneous polynomials R^+ and R^- in $\mathbb{F}_q[x_0, x_1, x_2]$ such that $E^+ = \mathrm{div}(R^+)$ and $E^- = \mathrm{div}(R^-)$.*
2. *$H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E)) = \frac{1}{R}\{f \in \mathbb{F}_q[x_0, x_1, x_2] \,|\, f$ is homogeneous of $\deg E\} \cup \{0\}$, where $R := R^+/R^-$.*
3. $\dim H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E)) = \begin{cases} \frac{1}{2}(\deg E + 1)(\deg E + 2) & (\deg E \geq 0) \\ 0 & (\deg E < 0) \end{cases}$.

Proof. As E is defined over $\mathbb{F}_q$, E^+ and E^- are stable under any $\sigma \in G(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, then we have only to show the first assertion in case of E being effective. An effective divisor is a sum of irreducible divisors each of which corresponds to an absolutely irreducible homogeneous polynomial over $\bar{\mathbb{F}}_q$. Thus $E = \mathrm{div}(\bar{R})$ with a homogeneous polynomial $\bar{R}$ over $\bar{\mathbb{F}}_q$.

From the exact sequence $\{1\} \to \bar{\mathbb{F}}_q^* \to \bar{\mathbb{F}}_q(\mathbb{P}^2)^* \stackrel{\mathrm{div}}{\to} \mathrm{Div}(\mathbb{P}^2)$, $\mathrm{div}(\bar{R}^\sigma/\bar{R}) = E^\sigma - E = 0$ means $\bar{R}^\sigma/\bar{R} \in \bar{\mathbb{F}}_q$. Moreover Hilbert's Satz 90 implies that there exists $a \in \bar{\mathbb{F}}_q$ such that $(a\bar{R})^\sigma = a\bar{R}$, then $R = a\bar{R} \in \mathbb{F}_q[X]$ and $\mathrm{div}(R) = E$.

Noticing that $H^0_{\bar{\mathbb{F}}_q}(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E)) = \{f \in \bar{\mathbb{F}}_q(\mathbb{P}^2)^* \mid \mathrm{div}(f) + E \geq 0\} \cup \{0\} = \frac{1}{\bar{R}}\{g \in \bar{\mathbb{F}}_q[x_0, x_1, x_2] \,|\, g$ is homogeneous, $\deg g = \deg E\} \cup \{0\}$ and $\mathbb{F}_q(\mathbb{P}^2) = \{f \in \bar{\mathbb{F}}_q(\mathbb{P}^2) \,|\, f^\sigma = f,\ \forall \sigma \in G(\bar{\mathbb{F}}_q/\mathbb{F}_q)\}$, we have the second assertion.

The dimension of $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E))$ is obtained by counting the number of $\{x_0^{e_0} x_1^{e_1} x_2^{e_2} \,|\, e_0 + e_1 + e_2 = \deg E, e_i \geq 0\}$. □

From now on, we always assume that curves and divisors are all defined over $\mathbb{F}_q$. For our proposed code, we focus on some curves on $\mathbb{P}^2$ with fixed number of $\mathbb{F}_q$-rational points.

Definition 2. *Let $C_1, \cdots, C_m$ be mutually distinct absolutely irreducible smooth plane projective curves of degree d. For each C_i, take n number of $\mathbb{F}_q$-rational points $P_{i1}, \cdots, P_{in}$. Then we call a set of these tuples $\mathcal{C} = \{(C_i, \{P_{i1}, \cdots, P_{in}\})\}_{1 \leq i \leq m}$ a system of m-tuple n-pointed curves of degree d.*

Here let E be an effective divisor of degree e such that $\mathrm{Supp}E \cap \{P_{ij}\} = \emptyset$, and $E = \mathrm{div}(R)$ with R in Prop. 2. Putting $P_i = P_{i1} + \cdots + P_{in}$ for each i, define $\Phi_i = \Phi_{C_i, P_i, E|_{C_i}} : H^0(C_i, \mathcal{O}_{C_i}(E|_{C_i})) \to \mathbb{F}_q^n$ by $\Phi_i(f_i) = (f_i(P_{i1}), \ldots, f_i(P_{in}))$, and define two $\mathbb{F}_q$-linear maps, $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E)) \stackrel{res}{\to} \prod_{i=1}^m H^0(C_i, \mathcal{O}_{C_i}(E|_{C_i})) \stackrel{\phi}{\to} \mathbb{F}_q^{nm}$ by $res(f) = (f|_{C_1}, \ldots, f|_{C_m})$ and by $\phi(f_1, \ldots, f_m) = (\Phi_1(f_1), \ldots, \Phi_m(f_m))$.

Definition 3. *If $\Phi_{\mathbb{P}^2,\mathcal{C},E} = \phi \circ res$ is injective, we call the image of this map, denoted by $C(\mathbb{P}^2,\mathcal{C},E)$, a functional type plane code associated to $(\mathbb{P}^2,\mathcal{C},E)$.*

The code defined above is just a code obtained by applying Hansen's construction to a system of pointed curves, however we can calculate some important parameters for this type of code.

Proposition 3. *If $n > de$ and $dm > e$, then $\Phi_{\mathbb{P}^2,\mathcal{C},E}$ is injective.*

Proof. If $n > de$, then $\deg(E|_{C_i} - P_i) = ed - n < 0$ and $\ker \Phi_i = H^0(C_i, \mathcal{O}_{C_i}(E|_{C_i} - P_i)) = 0$ for any i. Thus $\ker \phi = 0$. If $e < dm$, then $\deg(E - D) = e - dm < 0$, and $\ker(res) = H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E - D)) = 0$ with $D = C_1 + \cdots + C_m$. Therefore we have the result. □

Proposition 4. *When we suppose that $n > de$, let $I_f = \{i \mid w(\Phi_i(f|_{C_i})) < n - de\}$ with the Hamming weight w. Then $f \in H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E - \sum_{i \in I_f} C_i))$, and $w(\Phi_{\mathbb{P}^2,\mathcal{C},E}(f)) \geq (m - |\, I_f \,|)(n - de)$ for $f \in H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(E))$. If there exists non-zero f, then $|\, I_f \,| \, d \leq e$.*

Proof. For any $i \in I_f$, put $D_{f,i} = \sum_{f(P_{ij})=0} P_{ij}$, then $\deg D_{f,i} > de$ and $\deg(E|_{C_i} - D_{f.i}) = de - \deg D_{f,i} < 0$. Thus $H^0(C_i, \mathcal{O}_{C_i}(E|_{C_i} - D_{f,i})) = 0$, which implies that $f|_{C_i} = 0$. If $i \notin I_f$, $w(\Phi_i(f|_{C_i})) \geq n - de$. This concludes the first two assertions. When there exists $f \neq 0$, then $0 \leq \deg(E - \sum_{i \in I_f} C_i) = e - |\, I_f \,| \, d$, and $|\, I_f \,| \, d \leq e$. □

Theorem 1. *If $n > de$ and $dm > e$, then*

$$\dim C(\mathbb{P}^2,\mathcal{C},E) = \frac{1}{2}(e+1)(e+2) \text{ and } \delta(\, C(\mathbb{P}^2,\mathcal{C},E)\,) \geq (\, m - \lfloor \frac{e}{d} \rfloor\,)(n - de),$$

where δ represents the minimum distance.

Now we apply Hansen's result in Prop.1 to our system. As we mentioned just after the proposition, $Z(s) = Z(f_s) = \mathrm{div}(\{f_s(\varphi_\lambda^{-1}(z_\lambda))R(\varphi_\lambda^{-1}(z_\lambda)\}_\lambda)$. Let g_i be a homogeneous polynomial which defines each C_i. The number $l = \sup\#\{i \mid \mathrm{Supp} Z(s) \supset C_i\} = \sup\#\{i \mid g_i \text{ divides } f_s R\}$, which is equal to the maximum number of g_i's whose multiple has degree less than or equal to e. That is $l = \lfloor \frac{e}{d} \rfloor$.

Then the Hansen's lower bound value for the minimum distance is

$$mn - \lfloor \frac{e}{d} \rfloor N - (m - \lfloor \frac{e}{d} \rfloor) de = (m - \lfloor \frac{e}{d} \rfloor)(n - de) - (N - n)\lfloor \frac{e}{d} \rfloor,$$

here n in Prop.1 is replaced by mn and $n \leq \#C_i(\mathbb{F}_q) \leq N$. Thus our resulted value is greater by $(N - n)\lfloor \frac{e}{d} \rfloor$ then Hansen's estimation value.

4 Conclusion

We proposed a family of algebraic geometric code over the projective surface $\mathbb{P}^2$ and gave explicit formulas for the dimension and the lower bound. Although our codes are special type of Hansen's codes, the estimation value of the minimum distance is better than in general case. As our construction method is simple, it can be possible to obtain other important properties.

In our future work, we will obtain the dual code of our type by applying several important theorems in algebraic geometry. The decoding method is also now under investigation.

Acknowledgment

We express great thanks to Prof. Kenichi Sugiyama of Chiba University for his suggestive comments. We would like to dedicate this paper to Emeritus Prof. Hideo Wada of Sophia University in Tokyo who passed away on 7th of January, 2012.

References

[1] M. T. Tsfasman and S. G. Vladut, *Algebraic Geometric Codes*, Kluwer Academic Publisher, 1991.

[2] M. T. Tsfasman, S. G. Vladut, and T. Zink, Modular Curves, Shimura Curves, and Goppa Codes Better than the Varshamov-Gilbert Bound, *Math. Nachr.,* **109**, 21–28, 1982.

[3] V. D. Goppa, A New Class of Linear Error-Correcting Codes, *Problems of Information Transmission,* **6** (3), 207–212, 1970.

[4] V. D. Goppa, Codes on Algebraic Curves, *Soviet Math. Dokl.,* **24** No.1, 170–172, 1981.

[5] S. H. Hansen, Error-Correcting Codes from higher-dimensional varieties, *PhD Thesis,* University of Aarhus, 2001.

[6] C. Lomot, Error-Correcting Codes on Algebraic surfaces, *PhD Thesis,* Purdue University, 2003.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[8] P. Zampolini, *Algebraic Geometric Codes on Curves and Surfaces*, Master Program in Mathematics Faculty of Science University of Padova, Italy, 2007.