Serdica J. Computing **1** (2007), 193–206

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON THE AUTOMORPHISM GROUPS OF SOME AG-CODES BASED ON $C_{a,b}$ CURVES

Tanush Shaska* and Quanlong Wang

Abstract. We study $C_{a,b}$ curves and their applications to coding theory. Recently, Joyner and Ksir have suggested a decoding algorithm based on the automorphisms of the code. We show how $C_{a,b}$ curves can be used to construct MDS codes and focus on some $C_{a,b}$ curves with extra automorphisms, namely $y^3 = x^4 + 1$, $y^3 = x^4 - x$, $y^3 - y = x^4$. The automorphism groups of such codes are determined in most characteristics.

1. Introduction. In the design of new codes algebraic geometry codes (AG-codes), also known as Goppa codes, play an important part and have been well studied in the last few decades. In designing such codes an important fact is the number of points of the algebraic curve over a finite field. Hence, it is natural that the algebraic curves that have been used so far are curves for which such number of points can be computed. Is there a "nice" family of curves which can be used to construct good codes? Hermitian curves have been used successfully by many authors in addition to hyperelliptic curves and other families

ACM Computing Classification System (1998): E.4, H.1.1.
Key words: $C_{a,b}$ curves, AG-codes, automorphism groups.
*Partially supported by NATO.

of curves. In this paper we investigate a larger family of curves which contains the above families, namely the $C_{a,b}$ curves. C_{ab} curves are algebraic curves with very interesting arithmetic properties. There are algorithms suggested which count the number of points of these curves using the Monsky-Washnitzer cohomology; see [1]. In this paper we study how these properties can be used in constructing good algebraic geometry codes.

In Section 2, we give a brief introduction to algebraic geometry codes (AG-codes) and of C_{ab} curves. Such curves have degree a, b covers to $\mathbb{P}^1$. The existence of certain divisors makes these curves useful in coding theory.

In Section 3, we study the locus of genus g, $C_{a,b}$ curves for fixed a, b. Such curves have degree a, b covers to $\mathbb{P}^1$. Such covers are classified according to the ramification structure. We assume that the cover has the largest possible moduli dimension. This determines a ramification structure σ.

Denote the moduli spaces of these maximal moduli dimension degree a, b coverings by $\mathcal{M}_a$ and $\mathcal{M}_b$ respectively and let $g = \frac{1}{2}(a-1)(b-1)$. Then $\mathcal{M}_a, \mathcal{M}_b$ are algebraic varieties of $\mathcal{M}_g$ (not necessarily irreducible). The locus of $C_{a,b}$ curves in $\mathcal{M}_g$ is the intersection $\mathcal{M}_a \cap \mathcal{M}_b$. Studying this locus is the focus of section 3.

In the last section we use $C_{a,b}$ curves of genus 3 to construct AG-codes. Such codes are MDS codes. We focus on some genus 3 C_{ab} curves with extra automorphisms, namely $y^3 = x^4+1, y^3 = x^4-x, y^3-y = x^4$. The automorphism groups of such codes are determined for some characteristics.

Notation: Throughout this paper $\mathcal{X}$ will denote a smooth, projective curve defined over some field F. By Aut $(\mathcal{X})$ we denote the group of automorphisms of $\mathcal{X}$ defined over $\bar{F}$. By C we will denote a linear code. The permutation automorphism group of C will be denoted by PAut (C), the monomial automorphism group by MAut (C), and the automorphism group by ΓAut (C). $\mathbb{F}_q$ denotes a finite field of q elements.

2. Preliminaries.

Let $F/\mathbb{F}_q$ be an algebraic function field in one variable. Let $P_1, \ldots, P_n$ be places of degree one and let $D = P_1 + \cdots + P_n$. Furthermore let G be a divisor with $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. Then the **Goppa code** (respectively **AG code**) $C_{\mathcal{L}} \subseteq \mathbb{F}_q^n$ is defined by

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

Define the following linear **evaluation map**

$$\varphi: \quad \begin{cases} \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{cases}$$

Then the Goppa Code is given by $C_{\mathcal{L}}(D,G) = \varphi(\mathcal{L}(G))$, it is a linear code $[n,\, k,\, d]$ code with parameters

$$k = \dim G - \dim(G - D), \quad d \geq n - \deg G =: d_{des}.$$

The parameter d_{des} is called the **designed distance** of the Goppa code. The following result is well known, see [11, Thm. II.2.3] among many others.

Lemma 1. *Assume* $\deg G < n$ *and let* g *be the genus of* $F/\mathbb{F}_q$*. Then we have:*

(1) $\varphi : \mathcal{L}(G) \to C_{\mathcal{L}}(D,G)$ *is injective and* $C_{\mathcal{L}}(D,G)$ *is an* $[n,k,d]$ *code with*

$$k = \dim G \geq \deg G + 1 - g, \quad d \geq n - \deg G.$$

(2) *If in addition* $2g - 2 < \deg G < n$*, then* $k = \deg G + 1 - g$*.*

(3) *If* $(f_1, \ldots, f_k)$ *is a basis of* $\mathcal{L}(G)$*, then*

$$M \;=\; \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & & \vdots \\ f_k(P_1) & \cdots & f_k(P_n) \end{pmatrix}$$

is a generator matrix for $C_{\mathcal{L}}(D,G)$*.*

To characterize the dual code of a Goppa code we need to look at the original definitions of Goppa by means of differential forms and its relations to the code defined above. We define the code $C_\Omega(D,G)$ by

$$C_\Omega(D,G) := \{(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \mid \omega \in \Omega_F(G - D)\} \subseteq \mathbb{F}_q^n.$$

Lemma 2. *The code* $C_\Omega(D,G)$*, where* D *and* G *are as above has the following properties:*

(1) $C_{\mathcal{L}}(D,G)^\perp = C_\Omega(D,G)$*.*

(2) $C_\Omega(D,G) = a \cdot C_{\mathcal{L}}(D,H)$ *with* $H = D - G + (\eta)$ *where* η *is a differential,* $v_{P_i}(\eta) = -1$ *for* $i = 1, \ldots, n$*, and* $a = (\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta))$*.*

(3) $C_{\mathcal{L}}(D,G)^{\perp} = a \cdot C_{\mathcal{L}}(D,H)$.

The following proposition is cited from [11, Prop. VII.1.2]. It allows to construct differentials with special properties that help to construct a self-orthogonal code.

Lemma 3. *Let x and y be elements of F such that $v_{P_i}(y) = 1$, $v_{P_i}(x) = 0$ and $x(P_i) = 1$ for $i = 1, \ldots, n$. Then the differential $\eta := x \cdot \dfrac{dy}{y}$ satisfies*

$$v_{P_i}(\eta) = -1, \quad \textit{and} \quad \operatorname{res}_{P_i}(\eta) = 1$$

for $i = 1, \ldots, n$.

The **permutation automorphism group** of the code $C \subseteq F_q^n$ is the subgroup of S_n (acting on F_q^n by coordinate permutation) which preserves C. We denote such group by PAut (C). The set of monomial matrices that map C to itself forms the **monomial automorphism group**, denoted by MAut (C). Every monomial matrix M can be written as $M = DP$ where D is a diagonal matrix and P a permutation matrix. Let γ be a field automorphism of $\mathbb{F}_q$ and M a monomial matrix. Denote by M_γ the map $M_\gamma : C \to C$ such that $\forall \vec{x} \in C$ we have $M_\gamma(\vec{x}) = \gamma(M\vec{x})$. The set of all maps M_γ forms the **automorphism group** of C, denoted by ΓAut (C). It is well known that

$$\text{PAut } (C) \leq \text{MAut } (C) \leq \Gamma\text{Aut } (C)$$

Next we will define as admissible a class of curves which have some additional conditions on their divisors.

Definition 1. *A genus $g \geq 1$ curve $\mathcal{X}/F_q$ is called **admissible** if it satisfies:*

i) there exists a rational point P_∞ and two functions $x,\ y \in F(\mathcal{X})$ such that $(x)_\infty = kP_\infty,\ (y)_\infty = lP_\infty$, and $k,\ l \geq 1$;

ii) for $m \geq 0$, the elements $x^i y^j$ with $0 \leq i, 0 \leq j \leq k-1$, and $ki+lj \leq m$ form a basis of the space $\mathcal{L}(mP_\infty)$.

Next we define

$$Aut_{D,G}(\mathcal{X}) := \{\sigma \in Aut(\mathcal{X}) | \sigma(D) = D \text{ and } \sigma(G) = G\}.$$

With the above notation we have the following:

Theorem 1. *Let $\mathcal{X}/F_q$ be an admissible curve over F_q of genus g where $l > k$. Assume that $m \geq l$. Let $D = \sum_{P \in J} P$ where $J \subseteq \mathbb{P} \backslash \{P_\infty\}$, $\mathbb{P}$ is the set of all rational points of $\mathcal{X}$. If*

$$n > \max\left\{2g+2, 2m, k\left(l + \frac{k-1}{\beta}\right), lk\left(1 + \frac{k-1}{m-k+1}\right)\right\},$$

where $n = |J|$, $\beta = \min\{k-1,\ r | y^r \in \mathcal{L}(mP_\infty)\}$ then

$$\text{Aut } (C_{\mathcal{L}}(D, mP_\infty)) \cong \text{Aut }_{D, mP_\infty}(\mathcal{X}).$$

P r o o f. See [15] for details. □

2.1. Introduction to C_{ab} curves. In this section, we introduce the notion of C_{ab} curves which constitute a wide class of algebraic curves including elliptic curves, hyperelliptic curves and superelliptic curves. They have been studied by many people due to their nice properties.

Definition 2. *Let a and b be relatively prime positive integers. Then a curve $\mathcal{X}$ is called an C_{ab} curve defined over a field F if it is a nonsingular plane curve defined by $f(X, Y) = 0$, where $f(X, Y)$ has the form*

$$f(X,Y) = \alpha_{0,a}Y^a + \alpha_{b,0}X^b + \sum_{ai+bj<ab} \alpha_{i,j}X^iY^j \in F[X,Y] \tag{1}$$

for nonzero $\alpha_{0,a},\ \alpha_{b,0} \in F$.

Let $\mathcal{X}$ be a C_{ab} curve defined over F. There exists exactly one F-rational place ∞ at infinity, which implies that the degree of ∞ is 1. Furthermore, the pole divisors of X and Y are $a \cdot \infty$ and $b \cdot \infty$, respectively. The genus of $\mathcal{X}$ is $g(\mathcal{X}) = \dfrac{(a-1)(b-1)}{2}$.

Hence, $C_{a,b}$ curves have fully ramified degree a and b covers to $\mathbb{P}^1$. Consider first the degree a cover $\pi_a : C_{a,b} \to \mathbb{P}^1$. Since the cover is fully ramified then there are at least $2g + a - 1$ other branch points. Thus, the total number of branch points is

$$d_1 := 2g + a = ab - b + 1 = b(a-1) + 1$$

The degree b cover has

$$d_2 := 2(g-1) + 2b - (b-1) = (a-1)(b-1) + b + 1 = a(b-1) + 1$$

branch points.

Corollary 1. *All hyperelliptic curves are $C_{a,b}$ curves.*

P r o o f. Every genus g hyperelliptic curve can be written as $Y^2 = f(X)$ such that $\deg f = 2g + 1$. Take $a = 2$ and $b = 2g + 1$. □

Example 1. Let $a = 3, b = 4$. Then the genus of the curve is $g = 3$ and we have

$$(2)\quad Y^3+\alpha_1X^4+\alpha_2X^3+\alpha_3X^2Y+\alpha_4XY^2+\alpha_5X^2+\alpha_6Y^2+\alpha_7XY+\alpha_8X+\alpha_9Y+\alpha_{10} = 0$$

Since the dimension of $\mathcal{M}_3$ is 5 then we should be able to write this curve in a "better" way; see the next section for details. The next proposition will be useful when we construct AG-codes from C_{ab} curves.

Proposition 1. *Let $\mathcal{X}$ be a C_{ab} curve defined by $f(X, Y) = 0$ with $f(X, Y) \in F[X, Y]$. Then*

$$\{X^iY^j \mid 0 \le j \le a-1,\ i \ge 0,\ ai + bj \le m\}$$

is a basis of a vector space $\mathcal{L}(m \cdot \infty)$ over F, where $m \in Z_{\ge 0}$.

Corollary 2. *$C_{a,b}$ curves are admissible curves.*

Hence we can use the results of the previous section when constructing codes from such curves.

2.1.1. Automorphism groups of C_{ab} curves. Let C_{ab} be a curve as above. The purpose of this section is to determine the automorphism group of C_{ab} over $\bar{F}$ in terms of a, b. For genus $g = 2, 3$ such groups can be determined by work of previous authors; see [9], [6].

Lemma 4. *Let $\mathcal{X}$ be a genus $g = 2$ algebraic curve as in Eq.* (1) *defined over F. Then* Aut $(\mathcal{X})$ *is isomorphic to one of the following:*

i) $p = 3$: $\mathbb{Z}_2, V_4, D_4, D_6, GL_2(3)$,

ii) $p = 5$: $\mathbb{Z}_2, \mathbb{Z}_{10}, V_4, D_4, D_6, GL_2(3)$,.

iii) $p \ge 5$: $\mathbb{Z}_2, V_4, D_4, D_6, SL_2(3)$.

For the case $p = 2$ see [9] for details. For $g = 3$ see [6].

3. The locus of $C_{3,4}$ curves in the moduli space $\mathcal{M}_3$. In this section we want to focus on non-hyperelliptic genus 3 curves. More precisely, we

want to study the space of $C_{3,4}$ curves in the moduli space $\mathcal{M}_3$. Throughout this section all curves are defined over a characteristic zero field.

We first give a brief introduction to the Hurwitz spaces and projection of such spaces on $\mathcal{M}_g$. Let X be a curve of genus g and $f : X \to \mathbb{P}^1$ be a covering of degree n with r branch points. We denote the branch points by $q_1, \dots, q_r \in \mathbb{P}^1$ and let $p \in \mathbb{P}^1 \setminus \{q_1, \dots, q_r\}$. Choose loops γ_i around q_i such that

$$\Gamma := \pi_1(\mathbb{P}^1 \setminus \{q_1, \dots, q_r\},\ p) = \langle \gamma_1, \dots, \gamma_r \rangle, \quad \gamma_1 \cdots \gamma_r = 1.$$

Γ acts on the fiber $f^{-1}(p)$ by path lifting, inducing a transitive subgroup G of the symmetric group S_n (determined by f up to conjugacy in S_n). It is called the *monodromy group* of f. The images of $\gamma_1, \dots, \gamma_r$ in S_n form a tuple of permutations $\sigma = (\sigma_1, \dots, \sigma_r)$ called a tuple of *branch cycles* of f. We call such a tuple the *signature* of ϕ. The covering $f : X \to \mathbb{P}^1$ is of type σ if it has σ as tuple of branch cycles relative to some homotopy basis of $\mathbb{P}^1 \setminus \{q_1, \dots, q_r\}$.

Two coverings $f : X \to \mathbb{P}^1$ and $f' : X' \to \mathbb{P}^1$ are *weakly equivalent* (resp., *equivalent*) if there is a homeomorphism $h : X \to X'$ and an analytic automorphism g of $\mathbb{P}^1$ such that $g \circ f = f' \circ h$ (resp., $g = 1$). Such classes are denoted by $[f]_w$ (resp., $[f]$). The *Hurwitz space* $\mathcal{H}_\sigma$ (resp., *symmetrized Hurwitz space* $\mathcal{H}^s_\sigma$) is the set of weak equivalence classes (resp., equivalence) of covers of type σ, it carries a natural structure of an quasiprojective variety.

Let C_i denote the conjugacy class of σ_i in G and $C = (C_1, \dots, C_r)$. The set of Nielsen classes $\mathcal{N}(G, C)$ is

$$\mathcal{N}(G, \sigma) := \{(\sigma_1, \dots, \sigma_r) \mid \sigma_i \in C_i,\ G = \langle \sigma_1, \dots, \sigma_r \rangle,\ \sigma_1 \cdots \sigma_r = 1\}$$

The braid group acts on $\mathcal{N}(G, C)$ as

$$[\gamma_i] : \quad (\sigma_1, \dots, \sigma_r) \to (\sigma_1, \dots, \sigma_{i-1}, \sigma_{i+1}^{\sigma_i}, \sigma_i, \sigma_{i+2}, \dots, \sigma_r)$$

where $\sigma_{i+1}^{\sigma_i} = \sigma_i \sigma_{i+1} \sigma_i^{-1}$. We have $\mathcal{H}\sigma = \mathcal{H}_\tau$ if and only if the tuples σ, τ are in the same *braid orbit* $\mathcal{O}_\tau = \mathcal{O}_\sigma$.

Let $\mathcal{M}_g$ be the moduli space of genus g curves. We have morphisms

$$\begin{array}{c} \mathcal{H}_\sigma \xrightarrow{\Phi_\sigma} \mathcal{H}^s_\sigma \xrightarrow{\bar{\Phi}_\sigma} \mathcal{M}_g \\ [f]_w \to [f] \to [X] \end{array} \tag{3}$$

Each component of $\mathcal{H}_\sigma$ has the same image in $\mathcal{M}_g$. We denote by

$$\mathcal{L}_g := \bar{\Phi}_\sigma(\mathcal{H}^s_\sigma).$$

We say that the covering f or the ramification σ has *moduli dimension* $\delta := \dim \mathcal{L}_g$.

Let a, b be fixed and $g = (a-1)(b-1)/2$. The generic $C_{a,b}$ curve of genus g has a degree a cover $\pi_a : C_{a,b} \to \mathbb{P}^1$ (resp. degree b cover $\pi_b : C_{a,b} \to \mathbb{P}^1$).

The ramification structure of $\pi_a : C_{a,b} \to \mathbb{P}^1$ is $(a, 2, \ldots, 2)$ where the number of branch points is $d_1 = b(a-1)+1$, as discussed in section 2. Let $\mathcal{H}_a$ denote the Hurwitz space of such covers and $\mathcal{M}_a$ its image in $\mathcal{M}_g$, as described above. Then, the dimension of $\mathcal{M}_a$ ia $\delta_1 \leq b(a-1)-2$. Similarly, we get that the dimension of $\mathcal{M}_b$ is $\delta_2 \leq a(b-1)-2$. Of course, the cover with smallest degree among π_a and π_b is the one of interest. From now on, we assume that $a < b$.

As mentioned above the goal of this section is to study the space $\mathcal{M}_{a,b}$ for fixed a and b, particularly on the case $a = 3$ and $b = 4$.

Theorem 2. *Every genus* 3 *curve is a* $C_{3,4}$ *curve. Moreover, every genus* $C_{3,4}$ *curve defined over a field* F*, is isomorphic (over* $\bar{F}$*) to a curve with equation*

$$f(x,y) = (x+b)y^3 + (cx+d)y^2 + (ex^2+fx)y + x^3 + kx^2 + lx = 0. \tag{4}$$

P r o o f. The case of hyperelliptic curves is obvious. Hence, we focus on non-hyperelliptic genus 3 curves. Let C be a non-hyperelliptic genus 3 curve, P be a Weierstrass point on C, and K the function field of C. Then exists a meromorphic function x which has P as a triple pole and no other poles. Thus, $[K : L(x)] = 3$. Consider x as a mapping of C to the Riemann sphere. We call this mapping $\psi : C \to \mathbb{P}^1$ and let ∞ be $\psi(P)$. From the Riemann-Hurwitz formula we have that ψ has at most 8 other branch points. There is also a meromorphic function y which has P as a pole of order 4 and no other poles. Thus the equation of K is given by

$$f(x,y) := \gamma_1(x)\, y^3 + \gamma_2(x)\, y^2 + \gamma_3(x)\, y + \gamma_0(x) = 0 \tag{5}$$

where $\gamma_0(x), \ldots, \gamma_3(x) \in L[x]$ and

$$\deg(\gamma_0) = 4,\ \deg(\gamma_1) = 0,\ \deg(\gamma_2) \leq 2,\ \deg(\gamma_3) \leq 3.$$

The discriminant of $F(x,y)$ with respect to y

$$D(f,y) := -27\,(\gamma_1\,\gamma_0)^2 + 18\,\gamma_0\,\gamma_1\,\gamma_2\,\gamma_3 + (\gamma_2\,\gamma_3)^2 - 4\,\gamma_0\,\gamma_2^3 - 4\,\gamma_1\,\gamma_3^3,$$

must have at most degree 8 since its roots are the branch points of $\psi : \mathbb{C} \to \mathbb{P}^1$. Thus, we have

$$\deg(\gamma_3\gamma_2) \leq 4, \quad \deg(\gamma_0\gamma_2^3) \leq 8, \quad \deg(\gamma_3^3\,\gamma_1) \leq 8.$$

If $\deg(\gamma_2) = 2$ then $\deg(\gamma_3) \leq 2$ and $\deg(\gamma_0) = 0$. Thus, $\deg(f, x) = 2$. Then, $f(x, y) = 0$ is not the equation of an genus 3 curve. Hence, $\deg(\gamma_2) \leq 1$. Clearly, $\deg(\gamma_3) \leq 1$. We denote:

$$\begin{aligned} &\gamma_1(x) := a, && \gamma_2(x) := cx + d \\ &\gamma_3(x) := ex + f, && \gamma_0(x) := gx^4 + hx^3 + kx^2 + lx + m \end{aligned} \tag{6}$$

Then, we have

$$f(x, y) = ay^3 + (cx + d)y^2 + (ex + f)y + (gx^4 + hx^3 + kx^2 + lx + m) = 0$$

which is obviously an $C_{3,4}$ curve. This completes the proof of the first statement.

Let C be a $C_{3,4}$ curve defined over F. Then, C is a non-hyperelliptic genus 3 curve. Hence, it is isomorphic over $\bar{F}$ to a curve with equation as in Eq. (4); see [7] for details. This completes the proof. □

Hence, the space of $C_{3,4}$ curves correspond to the moduli space $\mathcal{M}_3$. It is an interesting problem to see what happens for higher genus g.

4. Codes obtained from $C_{a,b}$ curves. In this section we will give examples of codes which are constructed based on C_{ab} curves. We will focus on three curves, namely $y^3 = x^4 + 1$, $y^3 = x^4 - x$, and $y^3 - y = x^4$. All these curves are genus 3 non-hyperelliptic curves. For characteristic $p > 7$ these curves have automorphism group isomorphic to a group with GAP identity (48, 33), (9,1), and (96, 64) respectively; see [5] for details. Recall that an $[n, k, d]$ code with $d = n - k + 1$ is called **maximum distance separable** code or an MDS code.

4.1. The curve $y^3 = x^4 + 1$. Let $\mathcal{X}$ be the curve

$$y^3 = x^4 + 1$$

defined over $\mathbb{F}_q$. This is a $C_{3,4}$ curve of genus 3. For characteristic $p \neq 2, 3$ the automorphism group of $\mathcal{X}$ is $C_4 \rtimes A_4$, which has Gap identity $(48, 33)$. We denote the set of affine rational points of $\mathcal{X}$ over $\mathbb{F}_q$ by $\{P_1, \ldots, P_n\}$. Let $C = C_{\mathcal{L}}(D, G)$, where $n + 1$ is the number of rational points of $\mathcal{X}$ and

$$G = mP_\infty, \quad D = P_1 + \cdots P_n$$

We have the following result:

Theorem 3. *For the permutation automorphism group* PAut (C)*, one has*

i) If $0 \leq m < 3$ *or* $m > n + 4$ *then* PAut $(C) \cong S_n$.
ii) If $n > 24$ *and* $4 \leq m < n/2$ *then* PAut $(C) \cong$ Aut $_{D,mP_\infty}(\mathcal{X})$.

Proof. i) If $0 \leq m < 3$, then from Proposition 1 we know $(1, 1, \cdots, 1)$ is a basis of the vector space $\mathcal{L}(m \cdot P_\infty)$, thus $\dim G = 1$. Since $\dim(G - D) \geq 0$, $\dim C \geq 1$, together with $\dim C = \dim G - \dim(G - D)$ we have $\dim C = 1$. Therefore PAut $(C) \cong S_n$.

If $m > n+4$, then $\deg(G-D) > 2g-2$. Thus $\dim C = \dim G - \dim(G - D) = n$. C is the full space, therefore PAut $(C) \cong S_n$.

ii) With the notation of definition 1. In this case $k = 3$, $l = 4$, $g = 3$, $\beta = 1$, $m \geq 4$. For Theorem 1 to hold we need

$$n > \max\left\{8, 2m, 18, 12\left(1 + \frac{2}{m-2}\right)\right\}.$$

Since $m \geq 4$, $12\left(1 + \dfrac{2}{m-2}\right) \leq 24$. Thus when $n > 24$ and $4 \leq m < n/2$ Theorem 1 applies and PAut $(C) \cong$ Aut $_{D,mP_\infty}(\mathcal{X})$. □

It can be seen from the proof of theorem that $C_{\mathcal{L}}(D, G)$ is a $[n, 1, n]$ MDS code when $0 \leq m < 3$, and a $[n, n, 1]$ MDS code when $m > n + 4$.

Example 2. Let $\mathcal{X}$ be defined over F_{2^3}. Take $m = 4$. By computation using GAP, we find that $C_{\mathcal{L}}(D, G)$ is a $[8, 3, 6]$ MDS code with a generator matrix

$$\begin{pmatrix} \alpha^5 & \alpha^3 & \alpha^6 & 1 & \alpha^4 & \alpha & \alpha^2 & 0 \\ \alpha^3 & \alpha^6 & \alpha^5 & 0 & \alpha^2 & \alpha^4 & \alpha & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

where α is a primitive element of F_{2^3}. The permutation automorphism group is PAut $(C_{\mathcal{L}}(D, G)) \cong Z_{14}$.

4.2. The curve $y^3 = x^4 - x$. Let $\mathcal{X}$ be the curve

$$y^3 = x^4 - x$$

defined over $\mathbb{F}_q$. For characteristic $p > 7$ the automorphism group of $\mathcal{X}$ is the cyclic group of order 9. Denote the set of affine rational points of $\mathcal{X}$ over $\mathbb{F}_q$ by $\{P_1, \ldots, P_n\}$. Let $C = C_{\mathcal{L}}(D, G)$, where $n+1$ is the number of rational points of $\mathcal{X}$ and

$$G = mP_\infty, \quad D = P_1 + \cdots P_n$$

We have the following result:

Theorem 4. *For the permutation automorphism group* PAut (C)*, one has*

i) If $0 \leq m < 3$ *or* $m > n + 4$ *then* PAut $(C) \cong S_n$.

ii) If $n > 24$ *and* $4 \leq m < n/2$ *then* PAut $(C) \cong Aut_{D,mP_\infty}(\mathcal{X})$.

P r o o f. i) If $0 \leq m < 3$, then from Proposition 1 we know $(1, 1, \cdots, 1)$ is a basis of the vector space $\mathcal{L}(m \cdot P_\infty)$, thus $\dim G = 1$. Since $\dim(G - D) \geq 0$, $\dim C \geq 1$, together with $\dim C = \dim G - \dim(G - D)$ we have $\dim C = 1$. Therefore PAut $(C) \cong S_n$.

If $m > n+4$, then $\deg(G-D) > 2g-2$. Thus $\dim C = \dim G - \dim(G - D) = n$. C is the full space, therefore PAut $(C) \cong S_n$.

ii) With the notation of definition 1. In this case $k = 3$, $l = 4$, $g = 3$, $\beta = 1$, $m \geq 4$. For Theorem 1 to hold we need

$$n > \max\left\{8, 2m, 18, 12\left(1 + \frac{2}{m-2}\right)\right\}.$$

Since $m \geq 4$, $12\left(1 + \dfrac{2}{m-2}\right) \leq 24$. Thus when $n > 24$ and $4 \leq m < n/2$ Theorem 1 applies and PAut $(C) \cong$ Aut $_{D,mP_\infty}(\mathcal{X})$. $\square$

It can be seen from the proof of theorem that $C_{\mathcal{L}}(D, G)$ is a $[n, 1, n]$ MDS code when $0 \leq m < 3$, and a $[n, n, 1]$ MDS code when $m > n + 4$.

Example 3. Let $\mathcal{X}$ be defined over F_{2^3}. Take $m = 3$. By computation using GAP, we find that $C_{\mathcal{L}}(D, G)$ is a $[8, 2, 7]$ code with permutation automorphism group $[56, 11]$(Gap identity), which is clearly an MDS code.

4.3. The curve $y^3 - y = x^4$. Let $\mathcal{X}$ be the curve

$$y^3 - y = x^4$$

defined over $\mathbb{F}_q$. Denote the set of affine rational points of $\mathcal{X}$ over $\mathbb{F}_q$ by $\{P_1, \ldots, P_n\}$. Let $C = C_{\mathcal{L}}(D, G)$, where $n + 1$ is the number of rational points of $\mathcal{X}$ and

$$G = mP_\infty, \quad D = P_1 + \cdots P_n$$

We have the following;

Theorem 4. *For the permutation automorphism group* PAut (C)*, one has*

i) If $0 \leq m < 3$ *or* $m > n + 4$ *then* PAut $(C) \cong S_n$.

ii) If $n > 24$ *and* $4 \leq m < n/2$ *then* PAut $(C) \cong$ Aut $_{D,mP_\infty}(\mathcal{X})$.

P r o o f. i) If $0 \leq m < 3$, then from Proposition 1 we know $(1, 1, \ldots, 1)$ is a basis of the vector space $\mathcal{L}(m \cdot P_\infty)$, thus $\dim G = 1$. Since $\dim(G - D) \geq 0$, $\dim C \geq 1$, together with $\dim C = \dim G - \dim(G - D)$ we have $\dim C = 1$. Therefore PAut $(C) \cong S_n$.

If $m > n + 4$, then $\deg(G - D) > 2g - 2$. Thus $\dim C = \dim G - \dim(G - D) = n$. C is the full space, therefore PAut $(C) \cong S_n$.

ii) With the notation of Definition 1. In this case $k = 3$, $l = 4$, $g = 3$, $\beta = 1$, $m \geq 4$. For Theorem 1 to hold we need

$$n > \max\left\{8, 2m, 18, 12\left(1 + \frac{2}{m-2}\right)\right\}.$$

Since $m \geq 4$, $12\left(1 + \frac{2}{m-2}\right) \leq 24$. Thus when $n > 24$ and $4 \leq m < n/2$ Theorem 1 applies and PAut $(C) \cong$ Aut $_{D,mP_\infty}(\mathcal{X})$. $\square$

It can be seen from the proof of theorem that $C_{\mathcal{L}}(D, G)$ is a $[n, 1, n]$ MDS code when $0 \leq m < 3$, and a $[n, n, 1]$ MDS code when $m > n + 4$.

Example 4. Let $\mathcal{X}$ be defined over F_{2^2}. Take $m = 6$. By computation using GAP, we find that $C_{\mathcal{L}}(D, G)$ is a $[4, 4, 1]$ code with a generator matrix

$$\begin{pmatrix} \alpha & \alpha^2 & 0 & 0 \\ \alpha^2 & \alpha & 0 & 0 \\ \alpha & \alpha^2 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

where α is a primitive element of F_{2^2}.

The permutation automorphism group is isomorphic to the group with GAP identity $[24, 12]$. In this case

$$\text{PAut } (C) \hookrightarrow \text{Aut } (\mathcal{X}).$$

This code is clearly an MDS code.

5. Concluding remarks. It is an open question to determine the automorphism groups of AG-codes obtained by $C_{a,b}$ curves, in all characteristics. Moreover, even determining the list of automorphism groups of $C_{a,b}$ curves seems to be a non-trivial problem.

Furthermore, to determine the locus of $C_{a,b}$ curves, defined over $\mathbb{C}$, in the moduli space $\mathcal{M}_g$, where $g = \frac{(a-1)(b-1)}{2}$, seems an interesting problem in its

own right. A $C_{a,b}$ curve has covers of degree a and b to $\mathbb{P}^1$. One has to take such covers in the most generic form. The space of $C_{a,b}$ curves in $\mathcal{M}_g$ will be the intersection of the corresponding Hurwitz spaces. To generalize this for any a, b would require a careful analysis of the corresponding Hurwitz spaces.

REFERENCES

[1] Denef J., F. Vercauteren. Counting points on $C_{a,b}$ curves using Monsky-Washnitz cohomology. Ppreprint.

[2] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.4, 2006, (`http://www.gap-system.org`).

[3] Joyner D. Conjectural permutation decoding of some AG codes. *SIGSAM Bull.* **39**, *1*,(2005), 26–32.

[4] Joyner D., A. Ksir. Automorphism Groups of Some AG Codes. *IEEE Tran. Inform. Theory* **52**, *7* (2006), 3325–3329.

[5] Magaard K., T. Shaska, S. Shpectorov, H. Völklein. The locus of curves with prescribed automorphism group. Communications in arithmetic fundamental groups, Kyoto, 1999/2001. *Sūrikaisekikenkyūsho Kōkyūroku* No. 1267 (2002), 112–141.

[6] Shaska T. Automorphism groups of genus 3 curves over finite fields (work in progress).

[7] Shaska T., J. Thompson. On the generic curves of genus 3. *Contemp. Math.* **369** (2005), 233–244.

[8] Shaska T. Quantum codes from algebraic curves with automorphisms. Proceedings of the International Conferences on Complex Systems, Kazimerz-Dolny, 2005, 2006. Journal of Condensed Matter, (to appear).

[9] Shaska T., H. Völklein. Elliptic subfields and automorphisms of genus two fields. In: Algebra, Arithmetic and Geometry with Applications. Papers from Shreeram S. Abhyankar's 70th Birthday Conference. Springer, 2004, 687–707.

[10] Shaska T., S. Wijesiri. Codes over rings of size four, Hermitian lattices, and corresponding theta functions. *Proc. Amer. Math. Soc.* 2008, (to appear).

[11] Stichtenoth H. Algebraic Function Fields and Codes. Springer, Berlin, 1993.

[12] Xing Chao-Ping. Hyperelliptic function fields and codes. *J. Pure Appl. Algebra* **74** (1991), 109–118.

[13] Xing C. On automorphism groups of the Hermitian codes. *IEEE Trans. Inform. Theory* **41** (1995), 1629–1635.

[14] Vardy A. Algorithmic complexity in coding theory and the minimum distance problem. STOC'97, 1997, 92–109.

[15] Wesemeyer S. On the automorphism group of various Goppa codes. *IEEE Trans. Inform. Theory* **44** (1998), 630–643.

Tanush Shaska
Department of Mathematics and Statistics
Oakland University
Rochester, MI, 48309-4485, USA
e-mail: `shaska@oakland.edu`

Quanlong Wang
LMIB, Department of Mathematics
School of Science
Beihang University
Beijing 100083, P. R. China
e-mail: `quanlongwang@yahoo.com.cn`

Received October 23, 2006
Final Accepted June 27, 2007